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 $\mathrm{N}_G(H)$ 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 $\mathrm{O}_{p'}(G)$ et p-nilpotence)** Soient p un nombre premier et G un groupe.

(i) On note $\mathrm{O}_{p'}(G)$ 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 $P \in \mathrm{Syl}_p(G)$ — ou pour un seul, c'est pareil — $\mathrm{O}_{p'}(G)$ est un complément distingué de P dans G, autrement dit $G = \mathrm{O}_{p'}(G)P$.

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 $P \in \mathrm{Syl}_p(G)$. On suppose P abélien. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.
2) $\mathrm{N}_G(P)$ est p-nilpotent.
3) $P \leqslant \mathrm{Z}\big(\mathrm{N}_G(P)\big)$, ou encore $\mathrm{N}_G(P) = \mathrm{C}_G(P)$.

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 $P \in \mathrm{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.
2) Pour tout sous-groupe non trivial H de P, $\mathrm{N}_G(H)$ 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*, que je démontrerai à la fin de ce texte. 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 $P = \big\langle (1\ 2\ 3\ 4), (1\ 2) \big\rangle$, isomorphe au groupe diédral D_8, et les sous-groupes caractéristiques non triviaux de P sont P lui-même, son centre $\mathrm{Z}(P) = \big\langle (1\ 3)(2\ 4) \big\rangle$ et le sous-groupe cyclique $C = \big\langle (1\ 2\ 3\ 4) \big\rangle$. Or il n'est pas dur de vérifier que $\mathrm{N}_{S_4}(P) = \mathrm{N}_{S_4}\big(\mathrm{Z}(P)\big) = \mathrm{N}_{S_4}(C) = P$. 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 $\mathrm{J}(P)$ le sous-groupe de G engendré par les sous-groupes abéliens de G d'ordre maximal.

On pose en outre $\mathrm{ZJ}(P) = \mathrm{Z}\big(\mathrm{J}(P)\big)$.

Par exemple, si P est abélien : $\mathrm{J}(P) = P$. 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 $P \in \mathrm{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.
2) $\mathrm{N}_G\big(\mathrm{J}(P)\big)$ et $\mathrm{C}_G\big(\mathrm{Z}(P)\big)$ 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 $P \in \mathrm{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.
2) $\mathrm{N}_G\big(\mathrm{ZJ}(P)\big)$ 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 $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$. Alors pour tout $P \in \mathrm{Syl}_p(G)$: $\mathrm{ZJ}(P) \sqsubseteq G$.

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 $\mathrm{D}^*(P)$ de P que j'appellerai le *sous-groupe de Glauberman-Solomon de P* et qui paraît pouvoir remplacer avantageusement le sous-groupe de Thompson $\mathrm{J}(P)$ et son centre $\mathrm{ZJ}(P)$ dans les énoncés qui précèdent. Avantageusement en quel sens ? Le sous-groupe $\mathrm{D}^*(P)$ jouit d'une certaine propriété que les sous-groupes $\mathrm{J}(P)$ et $\mathrm{ZJ}(P)$ 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 $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$. Alors pour tout $P \in \mathrm{Syl}_p(G)$: $\quad \mathrm{D}^*(P) \sqsubseteq G$.

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 $P \in \mathrm{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.
2) $\mathrm{N}_G\big(\mathrm{D}^*(P)\big)$ est p-nilpotent.

Comme annoncé plus haut, la motivation historique du théorème de p-nilpotence de Thompson était un autre *théorème de Thompson* dont voici l'énoncé, précédé d'une définition.

Définition **(Automorphisme sans point fixe)** Soient G un groupe et $\varphi \in \mathrm{Aut}(G)$. 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 énonce souvent ce théorème en utilisant le vocabulaire des *groupes de Frobenius*. Les deux énoncés sont équivalents, mais je m'épargnerai toute digression à ce sujet. Les lecteurs intéressés trouveront de quoi satisfaire leur curiosité en (re)lisant mon texte « Le transfert et ses applications » dont un paragraphe est justement consacré aux groupes de Frobenius.

Ce texte est découpé en six 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 $\mathrm{D}^*(P)$ 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 qui n'est pas p-stable possède forcément une section isomorphe au groupe des quaternions, et également que $p = 3$ dans le cas p-séparable.

— La dernière partie de ce texte est enfin consacrée au *théorème de Thompson* de 1959 sur les automorphismes sans point fixe énoncé ci-dessus.

Nous terminerons cette introduction par le rappel de quelques notations.

$\lvert X\rvert$	Cardinal de l'ensemble X
$\lvert X\rvert_p$	Plus grande puissance du nombre premier p qui divise $\lvert X\rvert$
1	Double notation pour l'élément neutre d'un groupe et le sous-groupe trivial $\{1\}$
$H \leqslant G$	« H est un sous-groupe du groupe G »
$H < G$	« H est un sous-groupe propre du groupe G »
$H \trianglelefteqslant G$	« H est un sous-groupe distingué du groupe G »
$H \sqsubseteq G$	« H est un sous-groupe caractéristique du groupe G »
$\lvert G : H\rvert$	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
$\mathrm{N}_G(H)$	Normalisateur dans le groupe G du sous-groupe H
$\mathrm{C}_G(H)$	Centralisateur dans le groupe G du sous-groupe H
$\big[x,y\big]$	Commutateur $x^{-1}y^{-1}xy$ de x et y dans un groupe donné
$\big[X,Y\big]$	Sous-groupe engendré par les commutateurs $\big[x,y\big]$, x décrivant X et y décrivant Y
$\mathrm{D}(G)$	Sous-groupe dérivé $\big[G,G\big]$ du groupe G
$\mathrm{Syl}_p(G)$	Ensemble des p-Sylow du groupe G pour un nombre premier p
$\mathrm{Aut}(G)$	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
$\mathrm{GL}_n(q)$	Groupe général linéaire de degré n sur $\mathbb{F}_q$
$\mathrm{SL}_n(q)$	Groupe spécial linéaire de degré n sur $\mathbb{F}_q$

1 Groupes p-séparables

Définition-théorème 4 **(Sous-groupe $\mathrm{O}_\pi(G)$)** Soient G un groupe fini et π un ensemble de nombres premiers.

(i) On note $\mathrm{O}_\pi(G)$ le sous-groupe engendré par tous les π-sous-groupes distingués de G. Il est équivalent de dire que $\mathrm{O}_\pi(G)$ 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 : $\mathrm{O}_\pi(G) \sqsubseteq G$ et $\mathrm{O}_p(G) = \bigcap_{P\in\mathrm{Syl}_p(G)} P$.

Démonstration

(i) Le sous-groupe AB a pour ordre $\lvert AB\rvert = \dfrac{\lvert A\rvert\times\lvert B\rvert}{\lvert A\cap B\rvert}$, 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, donc $\mathrm{O}_p(G) \sqsubseteq G$. Ensuite, $\bigcap_{S\in\mathrm{Syl}_p(G)} P$ est un p-sous-groupe distingué de G car l'ensemble des p-Sylow de G est stable par conjugaison, donc : $\bigcap_{S\in\mathrm{Syl}_p(G)} P \leqslant \mathrm{O}_p(G)$. Inversement, $\mathrm{O}_p(G)$ 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 : $\mathrm{O}_p(G) \leqslant \bigcap_{S\in\mathrm{Syl}_p(G)} P$.

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 $1=H_0\trianglelefteqslant\dots\trianglelefteqslant H_n=G$ et tels que pour tout $i\in[\![0,n-1]\!]$, le quotient $\dfrac{H_{i+1}}{H_i}$ 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 : $1=H\cap H_0\trianglelefteqslant\dots\trianglelefteqslant H\cap H_n=H$. Ensuite, pour tout $i\in[\![0,n-1]\!]$, le morphisme de groupes $x\longmapsto(H\cap H_i)x$ de $H\cap H_{i+1}$ dans $\dfrac{H_{i+1}}{H_i}$ induit par quotient un morphisme injectif de $\dfrac{H\cap H_{i+1}}{H\cap H_i}$ dans $\dfrac{H_{i+1}}{H_i}$. En particulier, $\dfrac{H\cap H_{i+1}}{H\cap H_i}$ 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 : $1=\overline{H_0}\trianglelefteqslant\dots\trianglelefteqslant\overline{H_n}$. Ensuite, pour tout $i\in[\![0,n-1]\!]$, le morphisme de groupes $x\longmapsto\overline{H_i}\,\overline{x}$ de H_{i+1} dans $\dfrac{\overline{H_{i+1}}}{\overline{H_i}}$ induit par quotient un isomorphisme de $\dfrac{H_{i+1}}{H_{i+1}\cap NH_i}$ sur $\dfrac{\overline{H_{i+1}}}{\overline{H_i}}$. Comme $H_i\leqslant H_{i+1}\cap NH_i$, le groupe quotient $\dfrac{\overline{H_{i+1}}}{\overline{H_i}}$ est ainsi soit un p-groupe, soit un p'-groupe. Conclusion : $\dfrac{G}{N}$ est p-séparable. ∎

Théorème 6 (Sous-groupes $\mathrm{O}_p(G)$ et $\mathrm{O}_{p'}(G)$ d'un groupe p-séparable) Soient p un nombre premier et G un groupe p-séparable. Si G est non trivial, alors $\mathrm{O}_p(G)\neq1$ ou $\mathrm{O}_{p'}(G)\neq1$.

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 $n\geqslant1$. D'après **5**, H_{n-1} est p-séparable, donc $\mathrm{O}_p(H_{n-1})\neq1$ ou $\mathrm{O}_{p'}(H_{n-1})\neq1$ par hypothèse de récurrence. Or $\mathrm{O}_p(H_{n-1})\sqsubseteq H_{n-1}\trianglelefteqslant H_n=G$ et $\mathrm{O}_{p'}(H_{n-1})\sqsubseteq H_{n-1}\trianglelefteqslant H_n=G$, donc $\mathrm{O}_p(H_{n-1})\leqslant\mathrm{O}_p(G)$ et $\mathrm{O}_{p'}(H_{n-1})\leqslant\mathrm{O}_{p'}(G)$ — 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 $\mathrm{O}_p(G)\,\mathrm{O}_{p'}(G)$ dans un groupe p-séparable) Soient p un nombre premier et G un groupe p-séparable. Alors $\mathrm{C}_G\big(\mathrm{O}_p(G)\,\mathrm{O}_{p'}(G)\big)\leqslant\mathrm{O}_p(G)\,\mathrm{O}_{p'}(G)$.

Démonstration Posons : $O=\mathrm{O}_p(G)\,\mathrm{O}_{p'}(G)$, $C=\mathrm{C}_G(O)$ et $Z=\mathrm{Z}(O)$, et notons 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 $\dfrac{\Pi}{Z}=\mathrm{O}_\pi\left(\dfrac{C}{Z}\right)$. Aussitôt $Z\leqslant\Pi\leqslant C\leqslant\mathrm{C}_G(Z)$, donc $Z\leqslant\mathrm{Z}(\Pi)$. Par ailleurs, Z étant abélien : $Z=\mathrm{O}_p(Z)\,\mathrm{O}_{p'}(Z)$.

- Dans le cas où $\pi=\{p\}$, soit $P\in\mathrm{Syl}_p(\Pi)$. Le quotient $\dfrac{\Pi}{Z}$ étant un p-groupe : $\Pi=ZP=\mathrm{O}_{p'}(Z)\,P$, et comme $Z\leqslant\mathrm{Z}(\Pi)$: $P=\mathrm{O}_p(\Pi)\sqsubseteq\Pi\trianglelefteqslant G$, donc $P\leqslant\mathrm{O}_p(G)$. De la même façon $\mathrm{O}_{p'}(Z)\leqslant\mathrm{O}_{p'}(G)$, donc $\Pi=\mathrm{O}_{p'}(Z)\,P\leqslant O$. Or $\Pi\leqslant\mathrm{C}_G(O)$, donc $\Pi\leqslant Z$, et enfin $\mathrm{O}_p\left(\dfrac{C}{Z}\right)=1$.

- Dans le cas où π est le complémentaire de $\{p\}$ dans l'ensemble des nombres premiers, le quotient $\dfrac{\Pi}{Z}$ étant un p'-groupe : $\mathrm{O}_p(Z) \in \mathrm{Syl}_p(Z)$. Par ailleurs $\mathrm{O}_p(Z) \leqslant \mathrm{Z}(\Pi)$, donc Π est p-nilpotent d'après le théorème de p-nilpotence de Burnside, de sorte que $\Pi = \mathrm{O}_{p'}(\Pi)\,\mathrm{O}_p(Z)$. Or $\mathrm{O}_{p'}(\Pi) \sqsubseteq \Pi \trianglelefteqslant G$, donc $\mathrm{O}_{p'}(\Pi) \leqslant \mathrm{O}_{p'}(G)$. De même $\mathrm{O}_p(Z) \sqsubseteq Z \sqsubseteq O \sqsubseteq G$, donc $\mathrm{O}_p(Z) \leqslant \mathrm{O}_p(G)$. A fortiori $\Pi = \mathrm{O}_{p'}(\Pi)\,\mathrm{O}_p(Z) \leqslant O$, puis $\Pi \leqslant Z$, et enfin $\mathrm{O}_{p'}\left(\dfrac{C}{Z}\right) = 1$.

Au point où nous en sommes : $\mathrm{O}_p\left(\dfrac{C}{Z}\right) = 1$ et $\mathrm{O}_{p'}\left(\dfrac{C}{Z}\right) = 1$. Le quotient $\dfrac{C}{Z}$ étant p-séparable d'après **5** (ii), le théorème **6** montre que $\dfrac{C}{Z} = 1$, et donc $C = Z \leqslant O$.

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 classe des p-groupes finis dans elle-même satisfaisant les assertions suivantes :

— pour tout p-groupe P : $W(P) \sqsubseteq P$,

— 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 $P \in \mathrm{Syl}_p(G)$, la p-nilpotence de $\mathrm{N}_G\big(W(P)\big)$ 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 $\mathrm{O}_{p'}(G)$)** 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 $\mathrm{O}_{p'}(G)$, pour tout $P \in \mathrm{Syl}_p(G)$:

$$\mathrm{N}_{G^\circ}\big(W(P^\circ)\big) = \mathrm{N}_G\big(W(P)\big)^\circ.$$

Démonstration Il est d'abord clair que $\mathrm{N}_G\big(W(P)\big)^\circ \leqslant \mathrm{N}_{G^\circ}\big(W(P)^\circ\big)$. Inversement, soit $n \in G$ un élément pour lequel $n^\circ \in \mathrm{N}_{G^\circ}\big(W(P)^\circ\big)$. Aussitôt $\big(W(P)^\circ\big)^{n^\circ} = W(P)^\circ$, donc $W(P)^n \leqslant W(P)\,\mathrm{O}_{p'}(G)$. Or $W(P)$ et $W(P)^n$ sont deux p-Sylow de $W(P)\,\mathrm{O}_{p'}(G)$, donc d'après les théorèmes de Sylow : $W(P)^n = W(P)^\omega$ pour un certain $\omega \in \mathrm{O}_{p'}(G)$, donc $n\omega^{-1} \in \mathrm{N}_G\big(W(P)\big)$. A fortiori $n^\circ \in \mathrm{N}_G\big(W(P)\big)^\circ$.

Pour finir, l'application $x \longmapsto x^\circ$ est un isomorphisme de P sur P° car son noyau $P \cap \mathrm{O}_{p'}(G)$ est trivial, donc par définition de W : $W(P)^\circ = W(P^\circ)$. Conclusion : $\mathrm{N}_{G^\circ}\big(W(P^\circ)\big) = \mathrm{N}_{G^\circ}\big(W(P)^\circ\big) = \mathrm{N}_G\big(W(P)\big)^\circ$.

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

— pour tout $P \in \mathrm{Syl}_p(G)$: $W(P) \not\trianglelefteqslant G$,

— G est p-séparable et $\mathrm{O}_{p'}(G) = 1$ — donc d'après **7** : $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$,

— 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 classe $\mathscr{N}_W$ est composée de groupes a priori quelconques. Que Thompson ait réussi à se frayer un chemin dans cette classe 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 : $H < \mathrm{N}_G(H)$ avec inclusion stricte.

Démonstration La classe $\mathscr{N}_W$ étant non vide, nous pouvons nous en donner un élément G d'ordre minimal. Ainsi, le groupe G n'est pas p-nilpotent, mais $\mathrm{N}_G\big(W(P)\big)$ l'est pour un certain $P \in \mathrm{Syl}_p(G)$. Par conjugaison des p-Sylow de G et définition de W, $\mathrm{N}_G\big(W(P)\big)$ est donc p-nilpotent pour tout $P \in \mathrm{Syl}_p(G)$.

- Notons à présent $\mathscr{H}$ 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, $\mathscr{H}$ est non vide. Intéressons-nous alors aux éléments H de $\mathscr{H}$ pour lesquels $\big|\mathrm{N}_G(H)\big|_p$ 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.

  Donnons-nous ensuite un p-Sylow P de G contenant un p-Sylow de $\mathrm{N}_G(H)$ contenant lui-même H. Dans ces conditions $\mathrm{N}_P(H) \in \mathrm{Syl}_p\big(\mathrm{N}_G(H)\big)$, ou encore $\big|\mathrm{N}_G(H)\big|_p = \big|\mathrm{N}_P(H)\big|$, et par ailleurs $\mathrm{N}_G\big(W(P)\big)$ est p-nilpotent. Comme G ne l'est pas : $W(P) \not\trianglelefteq G$. Or $W(P) \sqsubseteq P$, donc $P \not\trianglelefteq G$. Conclusion : $\mathrm{O}_p(G) < P < G$.

- Montrons que $\mathrm{N}_G\Big(W\big(\mathrm{N}_P(H)\big)\Big)$ est p-nilpotent. Les relations $W\big(\mathrm{N}_P(H)\big) \sqsubseteq \mathrm{N}_P(H) \trianglelefteqslant \mathrm{N}_P\big(\mathrm{N}_P(H)\big)$ montrent que $\mathrm{N}_P\big(\mathrm{N}_P(H)\big) \leqslant \mathrm{N}_G\Big(W\big(\mathrm{N}_P(H)\big)\Big)$. Aussitôt, de deux choses l'une :

  — si $\mathrm{N}_P(H) = P$, nous savons déjà que $\mathrm{N}_G\Big(W\big(\mathrm{N}_P(H)\big)\Big) = \mathrm{N}_G\big(W(P)\big)$ est p-nilpotent,

  — dans le cas contraire : $\mathrm{N}_P(H) < \mathrm{N}_P\big(\mathrm{N}_P(H)\big)$ d'après **10**, donc :

  $$\Big|\mathrm{N}_G\Big(W\big(\mathrm{N}_P(H)\big)\Big)\Big|_p \geqslant \big|\mathrm{N}_P\big(\mathrm{N}_P(H)\big)\big| > \big|\mathrm{N}_P(H)\big| = \big|\mathrm{N}_G(H)\big|_p,$$

  donc $W\big(\mathrm{N}_P(H)\big) \notin \mathscr{H}$ par maximalité de H, autrement dit $\mathrm{N}_G\Big(W\big(\mathrm{N}_P(H)\big)\Big)$ est p-nilpotent.

- D'après le point précédent, $\mathrm{N}_{\mathrm{N}_G(H)}\Big(W\big(\mathrm{N}_P(H)\big)\Big)$ est p-nilpotent avec $\mathrm{N}_P(H) \in \mathrm{Syl}_p\big(\mathrm{N}_G(H)\big)$, mais pourtant, par définition de H, $\mathrm{N}_G(H)$ n'est pas p-nilpotent. Conclusion : $\mathrm{N}_G(H) = G$ par minimalité de G, donc $H \trianglelefteqslant \mathrm{O}_p(G)$.

  À présent, $\mathrm{O}_p(G) \in \mathscr{H}$ car $\mathrm{N}_G\big(\mathrm{O}_p(G)\big) = G$ n'est pas p-nilpotent, mais $\big|\mathrm{N}_G\big(\mathrm{O}_p(G)\big)\big|_p = |G|_p = \big|\mathrm{N}_G(H)\big|_p$, donc $\big|\mathrm{O}_p(G)\big| \leqslant |H|$ par maximalité de H. Conclusion : $H = \mathrm{O}_p(G)$.

- Montrons que G est p-séparable. Nous noterons désormais d'une barre les quotients par $\mathrm{O}_p(G)$. Notons V l'unique sous-groupe de G contenant $\mathrm{O}_p(G)$ pour lequel $\overline{V} = W\big(\overline{P}\big)$. L'inclusion stricte $\mathrm{O}_p(G) < P$ s'écrit aussi $\overline{P} \neq 1$, donc $\overline{V} \neq 1$ par définition de W, i.e. $H = \mathrm{O}_p(G) < V$. Cela dit $\overline{P} \trianglelefteqslant \mathrm{N}_{\overline{G}}\Big(W\big(\overline{P}\big)\Big)$, donc $P \leqslant \mathrm{N}_G(V)$. Ainsi $\big|\mathrm{N}_G(V)\big|_p = |G|_p = \big|\mathrm{N}_G(H)\big|_p$ et $|H| < |V|$, donc $V \notin \mathscr{H}$ par maximalité de H, i.e. $\mathrm{N}_G(V)$ est p-nilpotent. Comme $\mathrm{O}_p(G) \trianglelefteqslant V$, il en résulte que $\mathrm{N}_{\overline{G}}\Big(W\big(\overline{P}\big)\Big) = \mathrm{N}_{\overline{G}}\big(\overline{V}\big) = \overline{\mathrm{N}_G(V)}$ est p-nilpotent, et comme $\mathrm{O}_p(G) = H \neq 1$, la minimalité de G garantit finalement la p-nilpotence de $\overline{G}$. En particulier, $\overline{G}$ est p-séparable, mais donc G aussi a fortiori.

- Montrons que $\mathrm{O}_{p'}(G) = 1$. D'après **8**, si on on note d'un petit rond en exposant les quotients par $\mathrm{O}_{p'}(G)$: $\mathrm{N}_{G^\circ}\big(W(P^\circ)\big) = \mathrm{N}_G\big(W(P)\big)^\circ$, donc $\mathrm{N}_{G^\circ}\big(W(P^\circ)\big)$ est p-nilpotent puisque $\mathrm{N}_G\big(W(P)\big)$ l'est. Par l'absurde, si $\mathrm{O}_{p'}(G) \neq 1$, G° se trouve dès lors p-nilpotent par minimalité de G. Comme $\mathrm{O}_{p'}(G^\circ) = 1$ par définition de $\mathrm{O}_{p'}(G)$, 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 $\mathrm{O}_p(G)$ — et tâchons de montrer que $M = P$. Comme $\mathrm{O}_p(G)$ et $\mathrm{O}_{p'}(M)$ sont distingués dans M et d'ordres premiers entre eux : $\mathrm{O}_{p'}(M) \leqslant \mathrm{C}_G\big(\mathrm{O}_p(G)\big)$. Cela dit, G est p-séparable et $\mathrm{O}_{p'}(G) = 1$, donc $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$ d'après **7**. Conclusion : $\mathrm{O}_{p'}(M) \leqslant \mathrm{O}_p(G) \cap \mathrm{O}_{p'}(M) = 1$, i.e. $\mathrm{O}_{p'}(M) = 1$. Pourtant, $\mathrm{N}_M\big(W(P)\big)$ est p-nilpotent puisque $\mathrm{N}_G\big(W(P)\big)$ l'est, donc M lui-même est p-nilpotent par minimalité de G. Comme voulu : $M = \mathrm{O}_{p'}(M)\,P = P$.

- 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 $\mathrm{O}_p(G)$ est un q'-groupe et nous avons montré que $\overline{G}$ est p-nilpotent, i.e. que $\overline{G} = \mathrm{O}_{p'}\big(\overline{G}\big)\,\overline{P}$. Il nous suffit donc de montrer que $\mathrm{O}_{p'}\big(\overline{G}\big)$ est un q-groupe abélien.

  D'après les théorèmes de Sylow, $\mathrm{O}_{p'}\big(\overline{G}\big)$ a un nombre de q-Sylow qui divise $\big|\mathrm{O}_{p'}\big(\overline{G}\big)\big|$. L'action par conjugaison de $\overline{P}$ sur $\mathrm{Syl}_p\Big(\mathrm{O}_{p'}\big(\overline{G}\big)\Big)$ possède donc un point fixe d'après l'équation aux classes, disons $\overline{Q}$ avec $Q \in \mathrm{Syl}_q(G)$. En d'autres termes, $\overline{P}$ normalise $\overline{Q}$, donc PQ est un sous-groupe de G. Comme $Q \neq 1$, la maximalité de P montre que $G = PQ$. Or $\overline{\mathrm{D}(Q)}$ est lui aussi normalisé par $\overline{P}$, donc $\mathrm{D}(Q)\,P$ est un sous-groupe de G avec $\mathrm{D}(Q) < Q$. Par maximalité de P : $\quad \mathrm{D}(Q) = 1, \quad$ 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 $v, v' \in V$: $\quad (g,v)(g',v') = \big(\underbrace{gg'}_{\in G}, \underbrace{v^{g'}v'}_{\in V}\big)$.

Il est facile de vérifier que les applications $g \longmapsto (g,1)$ et $v \longmapsto (1,v)$ 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 $v \in V$: $\quad (1,v)^{(g,1)} = \big(1, v^g\big)$. 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 $\big[v,g\big] = v^{-1}v^g$ est quant à lui un élément de V, et on peut dire que v et g commutent quand $\big[v,g\big] = 1$, 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 $\mathrm{C}_G(V)$ 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 $\big[x,y,z\big] = \big[\big[x,y\big],z\big]$, et pour toutes parties X, Y, Z de G : $\quad \big[X,Y,Z\big] = \big[\big[X,Y\big],Z\big]$.

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 $\big[V,x,x\big] = 1$.

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 $v \in V$:

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

Dire que l'action de x est quadratique sur V revient alors à dire que l'endomorphisme $\mathbb{F}_p$-linéaire $(x - \mathrm{Id})^2$ 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 :

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

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 $\dfrac{G}{\mathrm{C}_G(V)}$ 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 de V induit par x est de la forme $\begin{pmatrix} I_n & & \\ & U & \\ & & \ddots \\ & & & U \end{pmatrix}$ dans une certaine base avec $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, or $U^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ pour tout $k \in \mathbb{Z}$ d'après un calcul classique, donc $U^p = I_2$. Conclusion : x^p agit trivialement sur V. Cela veut dire que $x^p \in \mathrm{C}_G(V)$, ou encore que l'image de x dans $\dfrac{G}{\mathrm{C}_G(V)}$ est d'ordre 1 ou p.

Démonstration

(i) Soit $k \in \mathbb{N}^*$ — c'est bien sûr suffisant. Pour tout $v \in V$: $\big[v, x^k\big] = \big[v,x\big]\big[v,x\big]^x\big[v,x\big]^{x^2}\dots\big[v,x\big]^{x^{k-1}}$, donc comme x est quadratique sur V : $\big[v,x^k\big] = \big[v,x\big]^k \in \big[V,x\big]$. Conclusion : $\big[V,x^k\big] \leqslant \big[V,x\big]$. Or x commute à $\big[V,x\big]$ par hypothèse, donc x^k aussi, donc $\big[V,x^k,x^k\big] = 1$.

(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 $x \in \mathrm{C}_G(V)$. Fixons pour cela $v \in V$. Comme x est quadratique sur V :

$$\big(\big[V,x\big]v\big)^x = \big[V,x\big]v^x = \big[V,x\big]\big[x,v^{-1}\big]v = \big[V,x\big]\big[v^{-1},x\big]^{-1}v = \big[V,x\big]v,$$

ce qui signifie que le q-groupe $\langle x\rangle$ agit sur $\big[V,x\big]v$. Or V est un p-groupe, donc la classe à gauche $\big[V,x\big]v$ de V modulo $\big[V,x\big]$ a pour cardinal une puissance de p. Comme $q \neq p$, l'équation aux classes montre que l'action de $\langle x\rangle$ sur $\big[V,x\big]$ a un point fixe, i.e. que pour un certain $w \in \big[V,x\big]$: $(wv)^x = wv$. 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 $i \in [\![1,r]\!]$,

— $x_0, \dots, x_r$ 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 $x_i \in \mathrm{C}_G(V)$ pour tout $i \in [\![1,r]\!]$ d'après le premier point. Conclusion : x a la même image dans $\dfrac{G}{\mathrm{C}_G(V)}$ 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 $\dfrac{G}{\mathrm{C}_G(V)}$. 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 $\mathrm{O}_p(G/N)$ l'unique sous-groupe — caractéristique — de G contenant N pour lequel $\dfrac{\mathrm{O}_p(G/N)}{N} = \mathrm{O}_p\left(\dfrac{G}{N}\right)$.

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 $x \in G$:
$$\big[V,x,x\big] = 1 \quad\Longrightarrow\quad x \in \mathrm{O}_p\big(G/\mathrm{C}_G(V)\big).$$
- 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 non p-stables) Soient p un nombre premier IMPAIR et G un groupe.

(i) Si G N'est PAS p-stable, il possède une section isomorphe au groupe des quaternions.

(ii) Si de plus G est p-séparable, alors $p=3$ et G possède une section isomorphe à $\mathrm{SL}_2(3)$.

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

1) G est p-séparable et $p \geqslant 5$.

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 $\mathrm{SL}_2(3)$ et le décrire. Pour commencer, le dénombrement suivant est classique : $\big|\mathrm{GL}_2(3)\big| = \big(3^2-1\big)\big(3^2-3\big) = 48$. On le démontre en remarquant que l'action naturelle de $\mathrm{GL}_2(3)$ 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 — $\big(3^2-1\big)$ possibilités — puis un vecteur quelconque qui ne lui est pas colinéaire — $\big(3^2-3\big)$ possibilités. Le déterminant étant un morphisme de groupes surjectif de $\mathrm{GL}_2(3)$ sur $\mathbb{F}_3^*$ de noyau $\mathrm{SL}_2(3)$, il en découle que $\big|\mathrm{SL}_2(3)\big| = 24$.

Introduisons à présent quatre élements de $\mathrm{SL}_2(3)$: $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $j = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$ 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 : $i^2 = j^2 = k^2 = -\mathrm{Id}$, $ij = k$ et $ji = -k$. Il n'est dès lors pas dur de se convaincre que $\langle i,j\rangle$ est isomorphe au groupe des quaternions : $\langle i,j\rangle = \big\{\pm\mathrm{Id}, \pm i, \pm j, \pm k\big\}$. 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 : $\mathrm{SL}_2(3) = \langle x\rangle \ltimes \langle i,j\rangle$.

Après ces modestes remarques, on comprend bien qu'un groupe d'ordre impair ou dont les 2-Sylow sont abéliens est forcément p-stable. Un tel groupe ne saurait en effet posséder une section isomorphe au groupe 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 $\big\{p,q\big\}$-groupe p-séparable dont les q-Sylow sont abéliens. Si p est impair, 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 $v \in V$:

$$\big[v,x\big]^x = x^{-1}\big(v^{-1}x^{-1}vx\big)x \overset{x^2=1}{=} x^{-1}v^{-1}xv = \big[x,v\big] = \big[v,x\big]^{-1} \overset{[v,x]^2=1}{=} \big[v,x\big], \qquad \text{donc } \big[v,x,x\big] = 1.$$

En résumé, toute involution de G est quadratique sur V. En particulier, G ne peut être 2-stable sur V que si $\mathrm{O}_2\big(G/\mathrm{C}_G(V)\big)$ 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 : $\mathrm{O}_2\big(G/\mathrm{C}_G(V)\big) = \mathrm{O}_2(G)$. Conclusion : pour que G soit 2-stable, il faut que $\mathrm{O}_2(G)$ contienne 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 : $\big[G,G\big] = \mathrm{D}(G)$. On a défini aussi $\big[G,G,G\big]$ dans la partie précédente. On définit de même $\big[G,G,G,G\big] = \big[\big[G,G,G\big],G\big]$, 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 $\overbrace{\big[G,G,\dots,G\big]}^{n+1 \text{ fois}} = 1$. Dans ce cas, le plus petit entier n pour lequel l'égalité est vraie est appelé la *classe de nilpotence de G* et notée $\mathrm{cl}(G)$.
  Par convention, si G n'est pas nilpotent, on pose $\mathrm{cl}(G) = +\infty$.
- 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 $\mathrm{D}(G) \leqslant \mathrm{Z}(G)$.

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 : $\forall H \leqslant G,\quad H < \mathrm{N}_G(H)$. 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 $x \in \mathrm{N}_G(A)$. Les assertions suivantes sont équivalentes :

1) $\mathrm{cl}\big(\langle A, x\rangle\big) \leqslant 2$.

2) x est quadratique sur A.

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

1) $\Longrightarrow$ 2) Par hypothèse : $\mathrm{cl}(B) \leqslant 2$, donc $\big[A, x, x\big] \leqslant \big[B, B, B\big] = 1$.

2) $\Longrightarrow$ 1) Faisons l'hypothèse que $\big[A, x, x\big] = 1$, i.e. que $\big[A, x\big] \leqslant \mathrm{C}_G(x)$. Comme x normalise A et comme A est abélien : $\big[A, x\big] \leqslant A \leqslant \mathrm{C}_B(A)$, donc $\big[A, x\big] \leqslant \mathrm{C}_B(x) \cap \mathrm{C}_B(A) = \mathrm{C}_B(B) = \mathrm{Z}(B)$, ce qui veut dire que $\overline{A}$ et $\overline{x}$ commutent si nous notons d'une barre les quotients par $\mathrm{Z}(B)$. Il en découle que $\overline{B}$ est abélien, et donc finalement $\mathrm{D}(B) \leqslant \mathrm{Z}(B)$, ou encore $\mathrm{cl}(B) \leqslant 2$. ∎

Ça y est, nous pouvons enfin définir le sous-groupe novateur que Glauberman et Solomon ont déniché en 2012 et qui finira peut-être un jour par détrôner l'incontournable $\mathrm{J}(P)$ de Thompson et son petit frère $\mathrm{ZJ}(P)$.

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

Il est équivalent d'exiger pour tout $x \in P$ l'implication : $\mathrm{cl}\big(\langle A, x\rangle\big) \leqslant 2 \quad\Longrightarrow\quad \big[A, x\big] = 1$.

(i) L'ensemble $\mathscr{D}^*(P)$ est stable par tout automorphisme de P.

(ii) Pour tous $A, A' \in \mathscr{D}^*(P)$, si A et A' se normalisent mutuellement, alors $AA' \in \mathscr{D}^*(P)$.

(iii) L'ensemble $\mathscr{D}^*(P)$ possède un maximum pour l'inclusion. On le note $\mathrm{D}^*(P)$ et on l'appelle le *sous-groupe de Glauberman-Solomon de P*.

En particulier, $\mathrm{D}^*(P)$ est abélien et $\mathrm{D}^*(P) \sqsubseteq P$. En outre : $\mathrm{D}^*(P) = \big\langle A \mid \ A \in \mathscr{D}^*(P)\big\rangle$.

(iv) $\mathrm{Z}(P) \leqslant \mathrm{D}^*(P)$. En particulier, si $P \neq 1$, alors $\mathrm{D}^*(P) \neq 1$.

(v) Pour tout sous-groupe P' de P contenant $\mathrm{D}^*(P)$: $\mathrm{D}^*(P) \leqslant \mathrm{D}^*(P')$.

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

Démonstration

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

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

(ii) Soient $A, A' \in \mathscr{D}^*(P)$. 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 $\big[A, A'\big] \leqslant A'$. Or A' est abélien, donc pour tout $x \in A'$: $\big[A, x, x\big] \leqslant \big[A, A', A'\big] \leqslant \big[A', A'\big] = 1$, puis $\mathrm{cl}\big(\langle A, x\rangle\big) \leqslant 2$ d'après **13**. Par définition de A enfin : $\big[A, x\big] = 1$ pour tout $x \in A'$, donc AA' est abélien.

Soit $x \in P$ pour lequel $\mathrm{cl}\big(\langle AA', x\rangle\big) \leqslant 2$. A fortiori $\mathrm{cl}\big(\langle A, x\rangle\big) \leqslant 2$ et $\mathrm{cl}\big(\langle A', x\rangle\big) \leqslant 2$, donc par définition de A et A' : $\big[A, x\big] = \big[A', x\big] = 1$, autrement dit x centralise à la fois A et A', ce dont on déduit que $\big[AA', x\big] = 1$. Conclusion : $AA' \in \mathscr{D}^*(P)$.

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

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

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

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

(v) Soit P' un sous-groupe de P contenant $\mathrm{D}^*(P)$. D'après (iii), il s'agit seulement de montrer l'inclusion $\mathscr{D}^*(P) \subset \mathscr{D}^*(P')$, 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 $\mathrm{D}^*(P)$ 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 $x \in P$: $\mathrm{cl}\big(\langle A, x\rangle\big)^\varphi = \mathrm{cl}\big(\langle A^\varphi, x^\varphi\rangle\big)$, donc $\mathscr{D}^*(P)^\varphi = \mathscr{D}^*(P')$. A fortiori, par unicité du maximum : $\mathrm{D}^*(P)^\varphi = \mathrm{D}^*(P')$. ∎

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 $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$. Alors pour tout $P \in \mathrm{Syl}_p(G)$: $\mathrm{D}^*(P) \sqsubseteq G$.

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

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

- Montrons que N est un sous-groupe abélien de P. Or $\mathrm{O}_p(G) \leqslant P$ et $\mathrm{D}^*(P) \trianglelefteqslant P$, donc $\big[\mathrm{O}_p(G), \mathrm{D}^*(P)\big] \leqslant \mathrm{D}^*(P)$, et comme $\mathrm{D}^*(P)$ est abélien : $\big[\mathrm{O}_p(G), \mathrm{D}^*(P), \mathrm{D}^*(P)\big] \leqslant \big[\mathrm{D}^*(P), \mathrm{D}^*(P)\big] = 1$. Aussitôt, par p-stabilité de G : $\mathrm{D}^*(P) \leqslant \mathrm{O}_p\Big(G/\mathrm{C}_G\big(\mathrm{O}_p(G)\big)\Big)$.

  Ensuite, par hypothèse : $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$, donc $\mathrm{C}_G\big(\mathrm{O}_p(G)\big)$ est un p-groupe. Par définition de $\mathrm{O}_p(G)$, il en découle que $\mathrm{O}_p\Big(G/\mathrm{C}_G\big(\mathrm{O}_p(G)\big)\Big) = \mathrm{O}_p(G)$.

  Conclusion : $\mathrm{D}^*(P) \leqslant \mathrm{O}_p(G)$, puis $\mathrm{D}^*(P) \leqslant \mathrm{D}^*\big(\mathrm{O}_p(G)\big)$ d'après **14** (v). Cela dit $\mathrm{D}^*\big(\mathrm{O}_p(G)\big) \sqsubseteq \mathrm{O}_p(G) \sqsubseteq G$. Ainsi $N \leqslant \mathrm{D}^*\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G) \leqslant P$, donc N est comme voulu un sous-groupe abélien de P.

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

  Soit $x \in P$ pour lequel $\mathrm{cl}\big(\langle N, x\rangle\big) \leqslant 2$. Comme $N \trianglelefteqslant G$, d'après **13** : $\big[N, x, x\big] = 1$. Posons $C = \mathrm{C}_G(N)$ et $O = \mathrm{O}_p(G/C)$. L'égalité $\big[N, x, x\big] = 1$ montre par p-stabilité de G que $x \in O$.

  À présent, pour montrer que $\big[N, x\big] = 1$, il nous suffit de prouver que $\big[\mathrm{D}^*(P)^g, x\big] = 1$ pour tout $g \in G$. Soit $g \in G$. Comme $O \trianglelefteqslant G$: $P^g \cap O \in \mathrm{Syl}_p(O)$, donc $O = C\big(P^g \cap O\big)$. Ainsi $x = cy$ pour certains $c \in C$ et $y \in P^g \cap O$. Il en découle que $\big[N, x\big] = \big[N, y\big] \leqslant N$, puis que $\big[\mathrm{D}^*(P)^g, y, y\big] \leqslant \big[N, y, y\big] = \big[N, x, x\big] = 1$. Or il se trouve que $\mathrm{D}^*(P)^g = \mathrm{D}^*\big(P^g\big) \in \mathscr{D}^*\big(P^g\big)$ et $y \in P^g$, donc par définition de $\mathscr{D}^*\big(P^g\big)$: $\big[\mathrm{D}^*(P)^g, y\big] = 1$. Comme voulu $\big[\mathrm{D}^*(P)^g, x\big] = 1$ puisque $\mathrm{D}^*(P)^g \leqslant N$ et $c \in C = \mathrm{C}_G(N)$. ∎

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.

5.1 Un chemin tortueux vers $\mathrm{SL}_2(q)$

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 $\mathrm{C}_G(W)\cap\mathrm{C}_G\left(\frac{V}{W}\right)$ 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 $x\in\mathrm{C}_G(W)\cap\mathrm{C}_G\left(\frac{V}{W}\right)$ et $v\in V$. Montrons que $\big[v,x,x\big]=1$. Or $(Wv)^x=Wv$ car $x\in\mathrm{C}_G\left(\frac{V}{W}\right)$, donc $v^x=wv$ pour un certain $w\in W$. Aussitôt $\big[w,x\big]=1$ car $x\in\mathrm{C}_G(W)$, donc $\big[v,x,x\big]=\big[w,x\big]=1$.

(ii) Notons W' le quotient de V par W. Soit $x\in G$ pour lequel $\big[V,x,x\big]=1$. Aussitôt $\big[W,x,x\big]=1$ et $\big[W',x,x\big]=1$, donc $x\in\mathrm{O}_p\big(G/\mathrm{C}_G(W)\big)\cap\mathrm{O}_p\big(G/\mathrm{C}_G(W')\big)$ par p-stabilité. Montrer que $x\in\mathrm{O}_p\big(G/\mathrm{C}_G(V)\big)$ revient dès lors à montrer l'inclusion : $\quad\mathrm{O}_p\big(G/\mathrm{C}_G(W)\big)\cap\mathrm{O}_p\big(G/\mathrm{C}_G(W')\big)\leqslant\mathrm{O}_p\big(G/\mathrm{C}_G(V)\big)$.

- Le morphisme de groupes $g\longmapsto\big(\mathrm{C}_G(W)g,\mathrm{C}_G(W')g\big)$ de G dans $\frac{G}{\mathrm{C}_G(W)}\times\frac{G}{\mathrm{C}_G(W')}$ a pour noyau l'intersection $\mathrm{C}_G(W)\cap\mathrm{C}_G(W')$ et envoie $\mathrm{O}_p\big(G/\mathrm{C}_G(W)\big)\cap\mathrm{O}_p\big(G/\mathrm{C}_G(W')\big)$ dans $\mathrm{O}_p\left(\frac{G}{\mathrm{C}_G(W)}\right)\times\mathrm{O}_p\left(\frac{G}{\mathrm{C}_G(W')}\right)$, lui-même inclus dans le p-sous-groupe distingué $\mathrm{O}_p\left(\frac{G}{\mathrm{C}_G(W)}\times\frac{G}{\mathrm{C}_G(W')}\right)$. Conclusion :
$$\mathrm{O}_p\big(G/\mathrm{C}_G(W)\big)\cap\mathrm{O}_p\big(G/\mathrm{C}_G(W')\big)\leqslant\mathrm{O}_p\big(G/\mathrm{C}_G(W)\cap\mathrm{C}_G(W')\big).$$
- Ensuite, d'après (i) et **11** (ii), $\frac{\mathrm{C}_G(W)\cap\mathrm{C}_G(W')}{\mathrm{C}_G(V)}$ est un p-sous-groupe distingué de $\frac{G}{\mathrm{C}_G(V)}$. Par ailleurs : $\frac{\mathrm{O}_p\big(G/\mathrm{C}_G(W)\cap\mathrm{C}_G(W')\big)}{\mathrm{C}_G(W)\cap\mathrm{C}_G(W')}=\mathrm{O}_p\left(\frac{G}{\mathrm{C}_G(W)\cap\mathrm{C}_G(W')}\right)$, donc $\frac{\mathrm{O}_p\big(G/\mathrm{C}_G(W)\cap\mathrm{C}_G(W')\big)}{\mathrm{C}_G(V)}$ est un p-sous-groupe distingué de $\frac{G}{\mathrm{C}_G(V)}$. Conclusion : $\quad\mathrm{O}_p\big(G/\mathrm{C}_G(W)\cap\mathrm{C}_G(W')\big)\leqslant\mathrm{O}_p\big(G/\mathrm{C}_G(V)\big)$ et le résultat en découle.

Par définition, un groupe est p-stable — tout court — s'il l'est sur tout p-groupe sur lequel il agit par automorphismes. Dire qu'un groupe N'est PAS p-stable revient donc à dire que son action par automorphismes sur certains p-groupes N'est PAS p-stable. Or que peut-on dire de ces p-groupes obstacles ? Qu'ont-ils de spécial ?

Théorème 18 (Première analyse d'un groupe non-p-stable) 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. Ainsi, pour un certain $x\in G$: $\quad\big[V,x,x\big]=1\quad$ mais $x\notin\mathrm{O}_p\big(G/\mathrm{C}_G(V)\big)$. En particulier $\mathrm{C}_G(V)\neq G$, donc $V\neq 1$, donc comme V est un p-groupe : $\quad\mathrm{Z}(V)\neq 1$.

- 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 $\mathrm{Z}(V) = V$, 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, $\big[V_q, x, x\big]$ est le sous-$\mathbb{F}_q$-espace vectoriel de V_q engendré par $\big[V, x, x\big]$, de sorte que $\big[V_q, x, x\big] = 1$. Également $\mathrm{C}_G(V_q) = \mathrm{C}_G(V) = 1$, donc $x \notin \mathrm{O}_p\big(G/\mathrm{C}_G(V)\big) = \mathrm{O}_p\big(G/\mathrm{C}_G(V_q)\big)$.

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) $x \in \mathrm{O}_p(G)$.
2) Pour tout $g \in G$, $\langle x, x^g \rangle$ est un p-groupe.

Démonstration

1) $\Longrightarrow$ 2) Si $x \in \mathrm{O}_p(G)$, alors pour tout $g \in G$: $x^g \in \mathrm{O}_p(G)$ car $\mathrm{O}_p(G) \trianglelefteqslant G$, donc $\big\langle x, x^g \big\rangle$ est un sous-groupe de $\mathrm{O}_p(G)$, a fortiori un p-groupe.

2) $\Longrightarrow$ 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) $\Longrightarrow$ 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 $\big\langle x^G \big\rangle \leqslant M$. Or par ailleurs, pour tous $g \in G$ et $m \in M$, $\langle x^g, x^{gm} \rangle = \big\langle x, x^{gmg^{-1}} \big\rangle^g$ est un p-groupe, donc $x^g \in \mathrm{O}_p(M)$ par hypothèse de récurrence. Ainsi $\big\langle x^G \big\rangle$ est un p-sous-groupe distingué de G, donc $x \in \big\langle x^G \big\rangle \leqslant \mathrm{O}_p(G)$.

Nous pouvons supposer désormais que x appartient à plusieurs sous-groupes maximaux de G. Donnons-nous-en deux M et M' pour lesquels $\big|M \cap M'\big|_p$ est maximal ainsi qu'un p-Sylow I de $M \cap M'$ contenant x. Si $I \trianglelefteqslant G$, $\big\langle x^G \big\rangle$ est un sous-groupe de I, donc un p-sous-groupe distingué de G, donc $x \in \big\langle x^G \big\rangle \leqslant \mathrm{O}_p(G)$.

Supposons $I \not\trianglelefteqslant G$. Dans ces conditions, $\mathrm{N}_G(I)$ est inclus dans un sous-groupe maximal M'' de G, qui bien sûr contient x. Soit $P \in \mathrm{Syl}_p(M)$ contenant I. Aussitôt $\mathrm{N}_P(I) = P \cap \mathrm{N}_G(I) \leqslant M \cap M''$, donc :

$$\big|M \cap M'\big|_p = |I| \leqslant \big|\mathrm{N}_P(I)\big| \leqslant \big|M \cap M''\big|_p,$$

d'où l'égalité $\mathrm{N}_P(I) = I$ grâce à notre choix des sous-groupes M et M'. Il en découle d'après **10** que $I = P$, autrement dit que $I \in \mathrm{Syl}_p(M)$, et pour la même raison $I \in \mathrm{Syl}_p(M')$. Retenons-en que $\mathrm{O}_p(M) \leqslant I$ et $\mathrm{O}_p(M') \leqslant I$.

À présent, pour tous $g \in G$ et $m \in M$, $\langle x^g, x^{gm} \rangle = \big\langle x, x^{gmg^{-1}} \big\rangle^g$ est un p-groupe, donc de nouveau, par hypothèse de récurrence : $x^G \cap M \subset \mathrm{O}_p(M) \subset I \subset M'$, ou encore $x^G \cap M \subset x^G \cap M'$, puis $x^G \cap M = x^G \cap M'$

par symétrie. En outre, $\langle x^G \cap M \rangle$ est un sous-groupe de $O_p(M)$, donc un p-groupe. Si $\langle x^G \cap M \rangle \trianglelefteqslant G$, il en découle que $x \in \langle x^G \cap M \rangle \subset O_p(G)$ et il en va de même si $\langle x^G \cap M' \rangle \trianglelefteqslant G$. Le cas contraire n'est pas possible, car on aurait par maximalité de M et M' : $M = N_G\big(\langle x^G \cap M \rangle\big) = N_G\big(\langle x^G \cap M' \rangle\big) = M'$.

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 $\dfrac{G}{C_G(V)}$ 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 $x \in G$: $\big[V, \overline{x}, \overline{x}\big] = \big[V, x, x\big]$, et de plus $\dfrac{\overline{G}}{C_{\overline{G}}(V)} = \overline{G} = \dfrac{G}{C_G(V)}$. Le résultat en découle par définition de la p-stabilité.

Théorème 21 (Tout groupe non-p-stable contient un morceau de $SL_2(q)$) 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 de $SL_2(q)$ dont les p-Sylow ne sont pas distingués.

Démonstration Ce n'est pas vraiment G qui nous intéresse, seulement l'une de ses sections. Nous pourrons ainsi nous permettre ci-dessous 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 $x \in G$: $\big[V, x, x\big] = 1$ mais $x \notin O_p\big(G/C_G(V)\big)$.

- 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**, $\dfrac{G}{C_G(V)}$ 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 $\big[V, x, x\big] = 1$ que $\big[V, y, y\big] = 1$. Nous supposerons désormais sans perte de généralité que $G = \langle x, y \rangle$. La proposition $x \notin O_p(G)$ montre également que $O_p(G)$ ne contient pas tous les p-éléments de G, et donc que les p-Sylow de G ne sont pas distingués dans G.
- 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 $GL\big(\mathbb{F}_q e\big)$, 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 actions quadratiques, l'égalité $\big[V, x, x\big] = 1$ s'écrit aussi $(x - \mathrm{Id})^2 = 0$ en termes plus linéaires. En particulier $\big(e^x\big)^x = 2e^x - e$, donc x stabilise le sous-$\mathbb{F}_q$-espace vectoriel $\mathbb{F}_q e + \mathbb{F}_q e^x$ de V. De même $\big[V, y, y\big] = 1$, donc y commute à $\big[e, y\big] = e^y - e$, donc : $\big(e^x\big)^y - e^x = \big(\lambda e^y\big)^y - \lambda e^y = \lambda\big(e^y - e\big)^y = \lambda\big(e^y - e\big) = e^x - \lambda e$, et enfin $\big(e^x\big)^y = 2e^x - \lambda e$. 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 $V = \mathbb{F}_q e + \mathbb{F}_q e^x$ par irréductibilité de V. En résumé, V est un $\mathbb{F}_q$-espace vectoriel de dimension 2.

5.2 Plongée dans $\mathrm{SL}_2(q)$

Pour avancer, nous avons maintenant besoin de connaître un peu plus finement le groupe $\mathrm{SL}_2(q)$.

Théorème 22 **(p-Sylow de $\mathrm{SL}_2(q)$)** Soient p un nombre premier et q une puissance non triviale de p.

(i) Tout élément de $\mathrm{SL}_2(q)\setminus\{I_2\}$ qui possède un point fixe dans $\mathbb{F}_q^2\setminus\{(0,0)\}$ est d'ordre p.

(ii) Les p-Sylow de $\mathrm{SL}_2(q)$ sont abéliens p-élémentaires d'ordre q.

(iii) Tout p-sous-groupe non trivial de $\mathrm{SL}_2(q)$ est inclus dans un unique p-Sylow.

(iv) Soit Γ un sous-groupe de $\mathrm{SL}_2(q)$. Si les p-Sylow de Γ ne sont pas distingués dans Γ, alors $\mathrm{O}_p(\Gamma)=1$.

Démonstration Le groupe $\mathrm{SL}_2(q)$ 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 : $\big|\mathrm{SL}_2(q)\big|=(q-1)q(q+1)$ et montre que les p-Sylow de $\mathrm{SL}_2(q)$ sont d'ordre q.

(i) Soit $s\in\mathrm{SL}_2(q)$. On suppose que s fixe un vecteur a de $\mathbb{F}_q^2\setminus\{(0,0)\}$. Complétons la famille libre (a) en une base (a,b) de $\mathbb{F}_q^2$. L'endomorphisme de $\mathbb{F}_q^2$ canoniquement associé à s a pour matrice $\begin{pmatrix}1&\alpha\\0&\beta\end{pmatrix}$ pour certains $\alpha,\beta\in\mathbb{F}_q$, et pour une raison de déterminant : $\beta=1$. Comme voulu $s^p=I_2$ car $\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}^p=I_2$.

(ii) Posons $i=(1,0)$. Alors $\mathrm{C}_{\mathrm{SL}_2(q)}(i)=\begin{pmatrix}1&\cdot\\0&1\end{pmatrix}$ où le symbole « $\cdot$ » désigne un élément quelconque de $\mathbb{F}_q$. L'application $\alpha\longmapsto\begin{pmatrix}1&\alpha\\0&1\end{pmatrix}$ étant un morphisme de groupes injectif du groupe additif $\mathbb{F}_q$ dans $\mathrm{SL}_2(\mathbb{F}_q)$, $\mathrm{C}_{\mathrm{SL}_2(q)}(i)$ est ainsi un p-Sylow de $\mathrm{SL}_2(q)$, qui plus est abélien p-élémentaire.

Pour tout $s\in\mathrm{SL}_2(q)$, $\mathrm{C}_{\mathrm{SL}_2(q)}\big(i^s\big)=\mathrm{C}_{\mathrm{SL}_2(q)}(i)^s$ est à son tour un p-Sylow de $\mathrm{SL}_2(q)$, et nous avons trouvé là en réalité tous les p-Sylow de $\mathrm{SL}_2(q)$ puisqu'ils sont conjugués d'après les théorèmes de Sylow. En résumé, l'action de $\mathrm{SL}_2(q)$ étant transitive sur $\mathbb{F}_q^2\setminus\{(0,0)\}$, les p-Sylow de $\mathrm{SL}_2(q)$ sont exactement les sous-groupes $\mathrm{C}_{\mathrm{SL}_2(q)}(x)$, x décrivant $\mathbb{F}_q^2\setminus\{(0,0)\}$ — attention, cette description occasionne des répétitions.

(iii) Tout p-sous-groupe de $\mathrm{SL}_2(q)$ 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 $\mathrm{SL}_2(q)$ est inclus dans un et un seul p-Sylow.

(iv) Supposons par contraposition que $\mathrm{O}_p(\Gamma)\neq 1$. D'après (iii), $\mathrm{O}_p(\Gamma)$ est alors inclus dans un unique p-Sylow P de $\mathrm{SL}_2(q)$. Or par ailleurs, $\mathrm{O}_p(\Gamma)$ est inclus dans tout p-Sylow de Γ. Conclusion : Γ ne possède qu'un seul p-Sylow, nécessairement distingué. ∎

Théorème 23 **(Un lemme de calcul matriciel dans $\mathrm{SL}_2(q)$)** Soient p un nombre premier IMPAIR, q une puissance non triviale de p, $x\in\mathrm{SL}_2(q)$ un élément d'ordre p et $u\in\mathrm{SL}_2(q)$ un p'-élément. Si u et u^x commutent, alors $u=I_2$ ou $u=-I_2$.

Ce petit résultat de rien du tout a l'air bien sage, mais c'est à cause de lui que le nombre premier 2 se trouve exclu des théorèmes de Thompson, Glauberman ou Glauberman-Solomon. Petit mais costaud !

Une remarque en passant. Toute involution de $\mathrm{SL}_2(q)$ 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 $\mathrm{SL}_2(q)$ que les matrices I_2 et $-I_2$. En particulier, $-I_2$ est donc la seule involution de $\mathrm{SL}_2(q)$.

Démonstration On peut supposer sans perte de généralité, quitte à conjuguer x et u, c'est-à-dire à changer de base, que $x=\begin{pmatrix}1&1\\0&1\end{pmatrix}$. Écrivons $u=\begin{pmatrix}\alpha&\gamma\\\beta&\delta\end{pmatrix}$ avec $\alpha,\beta,\gamma,\delta\in\mathbb{F}_q$ et notons n l'ordre de u. Après calcul, l'égalité $u^xu=uu^x$ implique que $2\beta^2=0$, donc $\beta=0$ car p est impair, mais aussi du coup que $\alpha=\delta$. Conclusion : $u=\begin{pmatrix}\alpha&\gamma\\0&\alpha\end{pmatrix}$, puis $\begin{pmatrix}\alpha^n&n\alpha^{n-1}\gamma\\0&\alpha^n\end{pmatrix}=u^n=I_2$ 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 : u est une homothétie, et comme $u\in\mathrm{SL}_2(q)$, forcément $u=I_2$ ou $u=-I_2$. ∎

Le résultat qui suit n'a rien à voir avec le groupe $\mathrm{SL}_2(q)$, mais il nous sera bientôt précieux. Rappelons tout d'abord que pour tout groupe G et pour tout $\varphi \in \mathrm{Aut}(G)$, on dit que φ est *sans point fixe* si son seul point fixe est l'élément neutre 1. Plus généralement, un sous-groupe A de $\mathrm{Aut}(G)$ est dit *sans point fixe* si tout élément de $A \setminus \{\mathrm{Id}\}$ est sans point fixe.

Théorème 24 (Structure d'un p-groupe d'automorphismes sans point fixe d'un groupe abélien) Soient G un groupe abélien, p un nombre premier et A un p-sous-groupe sans point fixe de $\mathrm{Aut}(G)$.

(i) Si $p \neq 2$, A est cyclique.

(ii) Si $p = 2$, soit A est cyclique, soit A possède un sous-groupe isomorphe au groupe des quaternions.

Dans l'assertion (ii), A est en fait soit cyclique, soit *quaternionien généralisé* — du nom d'une famille classique de 2-groupes — mais nous nous contenterons d'un énoncé léger.

L'hypothèse selon laquelle G est abélien est en réalité factice, mais nous ne le comprendrons qu'à l'extrême fin de ce texte.

Démonstration La preuve est assez longue. J'aurais pu la rédiger comme une liste de lemmes, mais cela aurait brisé l'élan général car les idées qui suivent diffèrent sensiblement de toutes celles qui traversent ce texte.

On peut supposer $A \neq \{\mathrm{Id}\}$ sans perte de généralité — mais donc aussi $G \neq 1$.

- D'après l'équation aux classes, A étant un p-groupe non trivial : $|G| \equiv \left|\mathrm{C}_A(G)\right| \ [p]$, mais A étant aussi sans point fixe : $|G| \equiv 1 \ [p]$. En particulier, $|G|$ et p sont premiers entre eux.
- Nous allons commencer par montrer que si A est d'ordre p^2, alors A est cyclique. Il est en tout cas bien connu que tout groupe d'ordre p^2 est soit cyclique, soit abélien p-élémentaire. Raisonnant par l'absurde, faisons l'hypothèse que A est abélien p-élémentaire d'ordre p^2, autrement dit que A est un $\mathbb{F}_p$-espace vectoriel de dimension 2. En tant que tel, A contient p^2-1 vecteurs non nuls, donc $p+1$ droites vectorielles, disons $D_1, \dots, D_{p+1}$, et : $A \setminus \{\mathrm{Id}\} = \bigsqcup_{1 \leqslant i \leqslant p+1} \left(D_i \setminus \{\mathrm{Id}\}\right)$ ♣.
  La commutativité de G va nous permettre à présent de multiplier ses éléments sans nous préoccuper de l'ordre dans lequel on le fait. Fixons $g \in G$. Pour tout sous-groupe non trivial B de A et pour tout $\beta \in B \setminus \{\mathrm{Id}\}$: $\left(\prod_{b \in B} g^b\right)^\beta = \prod_{b \in B} g^{b\beta} \overset{b' = b\beta}{=} \prod_{b' \in B} g^{b'} = \prod_{b \in B} g^b$, donc comme β est sans point fixe : $\prod_{b \in B} g^b = 1$, ou encore $\prod_{b \in B \setminus \{\mathrm{Id}\}} g^b = g^{-1}$. En particulier $\prod_{a \in A \setminus \{\mathrm{Id}\}} g^a = g^{-1}$ et pour tout $i \in [\![1, p+1]\!]$: $\prod_{d \in D_i \setminus \{\mathrm{Id}\}} g^d = g^{-1}$. Or d'après ♣ : $\prod_{a \in A \setminus \{\mathrm{Id}\}} g^a = \prod_{1 \leqslant i \leqslant p+1} \prod_{d \in D_i \setminus \{\mathrm{Id}\}} g^d$, donc $g^{-1} = g^{-(p+1)}$, et enfin $g^p = 1$. D'après le point précédent, il en découle que $g = 1$, et ceci pour tout $g \in G$, donc $G = 1$ — contradiction.
- Nous allons prouver à présent un lemme d'utilité générale valable dans n'importe quel groupe. Ci-dessous, x, y et z désignent des éléments quelconques d'un groupe. Alors :
  (i) $\big[x, yz\big] = \big[x, z\big]\big[x, y\big]^z$ et $\big[xy, z\big] = \big[x, z\big]^y\big[x, y\big]$.
  (ii) Si $\big[x, y\big]$ commute à x et y, alors pour tous $i, j \in \mathbb{N}$: $\big[x^i, y^j\big] = \big[x, y\big]^{ij}$.
  (iii) Si $\big[x, y\big]$ commute à x et y, alors pour tout $n \in \mathbb{N}$: $(xy)^n = x^n y^n \big[x, y\big]^{-\frac{n(n-1)}{2}}$ ♠.
  L'assertion (i) ne requiert qu'une vérification immédiate. Pour (ii), par récurrence, si $\big[x, y\big]$ commute à x et y et si $\big[x, y^j\big] = \big[x, y\big]^j$, alors : $\big[x, y^{j+1}\big] \overset{\text{(i)}}{=} \big[x, y^j\big]\big[x, y\big]^{y^j} = \big[x, y\big]^j\big[x, y\big] = \big[x, y\big]^{j+1}$, donc en particulier, $\big[x, y^j\big]$ commute à x et y. En retour : $\big[x^i, y^j\big] = \big[y^j, x^i\big]^{-1} = \big[y^j, x\big]^{-i} = \big[x, y^j\big]^i = \big[x, y\big]^{ij}$.
  Pour l'assertion (iii), par récurrence, si $(xy)^n = x^n y^n \big[x, y\big]^{-\frac{n(n-1)}{2}}$, alors :
  $$\begin{aligned}(xy)^{n+1} &= (xy)^n xy = x^n y^n \big[x, y\big]^{-\frac{n(n-1)}{2}} xy = x^{n+1}\big[x, y^{-n}\big]y^n x^{-1} xy \big[x, y\big]^{-\frac{n(n-1)}{2}} \\ &= x^{n+1}\big[x, y\big]^{-n} y^{n+1}\big[x, y\big]^{-\frac{n(n-1)}{2}} = x^{n+1} y^{n+1}\big[x, y\big]^{-\frac{n(n-1)}{2}-n} = x^{n+1} y^{n+1}\big[x, y\big]^{-\frac{n(n+1)}{2}}.\end{aligned}$$
- Après ces préparatifs, nous sommes en mesure de démontrer le théorème. Raisonnant par récurrence sur $|A| = p^n$, nous pouvons supposer que tout sous-groupe propre de A est cyclique ou possède un sous-groupe isomorphe au groupe des quaternions. Cela dit, de fait, si un sous-groupe propre de A possède un sous-groupe isomorphe au groupe des quaternions, il en va de même de A. Nous supposerons donc désormais que tout sous-groupe propre de A est cyclique, mais que A ne l'est pas — en particulier $n \geqslant 2$. À charge pour nous de montrer que A possède un sous-groupe isomorphe au groupe des quaternions.

Il est bien connu qu'en tant que p-groupe, A possède un sous-groupe M d'ordre p^{n-1}. Un tel sous-groupe est à la fois maximal dans A et distingué dans A, mais aussi cyclique par hypothèse de récurrence. En outre, d'après l'équation aux classes, l'action du p-groupe non trivial A sur M par conjugaison montre que : $\big|C_A(M)\big| \equiv |M| \equiv p^{n-1} \equiv 0\ [p]$, ce dont on déduit que $Z(A) \cap M \neq 1$. A fortiori, l'unique sous-groupe d'ordre p du groupe cycliqe M est inclus dans $Z(A)$.

Intéressons-nous maintenant à un élément a de $A \setminus M$ d'ordre minimal. Le quotient $\frac{A}{M}$ étant d'ordre p, le théorème de Lagrange montre que $a^p \in M$. Or A n'étant pas cyclique, a est d'ordre p^r pour un certain $r \in [\![1, n-1]\!]$, donc a^p d'ordre p^{r-1}. Le sous-groupe cyclique M contient alors un unique sous-groupe d'ordre p^r, et comme ce sous-groupe contient $\langle a^p \rangle$, on peut s'en donner un générateur b pour lequel $a^p = b^p$. En particulier, $a^{p^{r-1}} = b^{p^{r-1}}$ est d'ordre p dans M, donc appartient à $Z(A)$ d'après le paragraphe précédent. Nous noterons z cet élément.

Se peut-il qu'on ait $a^p = 1$, donc aussi $b^p = 1$? Si c'est le cas, b est d'ordre p dans M, donc appartient à $Z(A)$. Le sous-groupe $\langle a, b \rangle$ est alors abélien p-élémentaire d'ordre p^2, mais nous avons vu qu'aucun p-sous-groupe d'automorphismes sans point fixe de G ne peut avoir une telle structure. Conclusion : $a^p \neq 1$, ce qui veut dire aussi que $r \geqslant 2$. En particulier, a et b ne commutent pas car s'ils commutent : $\big(b^{-1}a\big)^p = b^{-p}a^p = 1$ et $b^{-1}a \in A \setminus M$, donc $a^p = 1$ par minimalité de l'ordre de a.

Comme a normalise M, il normalise aussi son unique sous-groupe $\langle b \rangle$ d'ordre p^r. L'automorphisme φ de $\langle b \rangle$ induit par a est non trivial car a et b ne commutent pas, mais φ^p au contraire, induit par $a^p = b^p \in \langle b \rangle$, fixe b donc $\langle b \rangle$ tout entier. Cela revient à dire que φ est un automorphisme d'ordre p de $\langle b \rangle$. Ce résultat nous conduit à nous pencher sur la structure du groupe $\mathrm{Aut}\big(\langle b \rangle\big)$. Or d'une part, l'application $k \longmapsto \big(x \longmapsto x^k\big)$ est un isomorphisme du groupe multiplicatif $\mathbb{Z}_{p^r}^*$ sur $\mathrm{Aut}\big(\langle b \rangle\big)$, mais d'autre part, la structure de $\mathbb{Z}_{p^r}^*$ est bien connue. Elle nous oblige à distinguer deux cas : $p \neq 2$ et $p = 2$.

— Supposons $p \neq 2$. Le groupe abélien $\mathbb{Z}_{p^r}^*$ est d'ordre $p^{r-1}(p-1)$ et son unique p-Sylow est cyclique engendré par $1+p$. La congruence $(1+p)^{p^k} \equiv 1 + p^{k+1}\big[p^{k+2}\big]$ pour tout $k \in \mathbb{N}$ montre en outre que l'unique sous-groupe d'ordre p de $\mathbb{Z}_{p^r}^*$ est engendré par $1 + p^{r-1}$. Quitte à remplacer a par l'une de ses puissances de même ordre, on peut donc faire l'hypothèse que φ est l'application $x \longmapsto x^{1+p^{r-1}}$. Conclusion : $b^a = b^{1+p^{r-1}}$, ou encore $\big[b^{-1}, a\big] = b\big(b^a\big)^{-1} = b^{-p^{r-1}} = z^{-1} \in Z(A)$, donc d'après ♠, p étant impair : $\big(b^{-1}a\big)^p = b^{-p}a^p\big[b^{-1}, a\big]^{-\frac{p(p-1)}{2}} = 1$. Cela dit $b^{-1}a \in A \setminus M$, donc $a^p = 1$ par minimalité de l'ordre de a — contradiction.

— Nous venons de montrer que $p = 2$. Si $r = 2$: $\mathbb{Z}_{p^r}^* = \mathbb{Z}_4^* = \big\{\pm 1\big\}$. Si au contraire $r \geqslant 3$, le groupe abélien $\mathbb{Z}_{2^r}^*$ est isomorphe à $\mathbb{Z}_{2^{r-2}} \times \mathbb{Z}_2$ et ses éléments sont tous les $\pm 5^k$, k décrivant $[\![0, 2^{r-1} - 1]\!]$. La congruence $5^{2^k} \equiv 1 + 2^{k+2}\ \big[2^{k+3}\big]$ pour tout $k \in \mathbb{N}$ montre que les involutions de $\mathbb{Z}_{2^r}^*$ sont les trois éléments -1, $1 + 2^{r-1}$ et $-1 + 2^{r-1}$. Conclusion : φ est soit l'application $x \longmapsto x^{-1}$, soit l'une des applications $x \longmapsto x^{1+2^{r-1}}$ ou $x \longmapsto x^{-1+2^{r-1}}$ si $r \geqslant 3$. En d'autres termes, soit $b^a = b^{-1}$, soit si $r \geqslant 3$: $b^a = b^{1+2^{r-1}} = bz$ ou $b^a = b^{-1+2^{r-1}} = b^{-1}z$.

  Supposons d'abord que $r \geqslant 3$ et $b^a = bz$. Dans ce cas : $\big[b^{-1}, a\big] = z^{-1} \in Z(A)$, donc d'après ♠ : $\big(b^{-1}a\big)^2 = b^{-2}a^2\big[b^{-1}, a\big]^{-1} = z$, puis $\big(b^{-1}a\big)^4 = 1$. Or $b^{-1}a \in A \setminus M$, donc $a^4 = 1$ par minimalité de l'ordre de a, donc $r \leqslant 2$ — contradiction.

  Ensuite, si $r \geqslant 3$ et $b^a = b^{-1}z$: $a^2 = \big(a^2\big)^a = \big(b^2\big)^a = \big(b^a\big)^2 = \big(b^{-1}z\big)^2 = b^{-2}z^2 = a^{-2}$, donc $a^4 = 1$, donc $r \leqslant 2$ — contradiction.

  Supposons enfin que $b^a = b^{-1}$. Aussitôt : $a^2 = \big(a^2\big)^a = \big(b^2\big)^a = \big(b^a\big)^2 = b^{-2} = a^{-2}$, donc $a^4 = 1$, et comme $a^2 \neq 1$, a est d'ordre 4 et $a^2 = b^2 = z$. Alors $\big[b, a\big] = b^{-2} = z^{-1} \in Z(A)$, donc d'après ♠ : $(ba)^2 = b^2a^2\big[b, a\big]^{-1} = z^3 = z$. Pour $c = ab$: $c^2 = (ab)^2 = a(ba)^2a^{-1} = aza^{-1} = z$, donc c est d'ordre 4, et de façon analogue : $bc = ab^ab = ab^{-1}b = a$ et $ca = a^2b^a = b^2b^{-1} = b$. Enfin : $ba = ab\big[b, a\big] = abz$, $cb = ab^2 = az$ et $ac = a^2b = bz$, donc $\langle a, b \rangle = \big\{\mathrm{Id}, z, a, az, b, bz, c, cz\big\}$ et il est assez clair que ce sous-groupe est isomorphe au groupe des quaternions. ■

Ouf ! Nous pouvons enfin reprendre l'étude du groupe $SL_2(q)$.

Théorème 25 (De l'art de faire surgir les quaternions dans $SL_2(q)$) Soient p un nombre premier IMPAIR, q une puissance non triviale de p et Γ un sous-groupe de $SL_2(q)$. Si les p-Sylow de Γ ne sont pas distingués dans Γ, Γ possède un sous-groupe isomorphe au groupe des quaternions.

Démonstration Quitte à remplacer Γ par l'un de ses sous-groupes, nous pouvons supposer sans perte de généralité que pour tout sous-groupe propre H de Γ, les p-Sylow de H sont distingués dans H. En outre, Γ n'étant pas un p-groupe, nous pouvons noter r le plus petit diviseur premier de $|\Gamma|$ autre que p et nous donner un r-Sylow R de Γ. En tant que groupe d'automorphismes de $\mathbb{F}_q^2$, R est sans point fixe d'après **22** (i), donc est cyclique ou possède un sous-groupe isomorphe au groupe des quaternions d'après **24**. Par l'absurde, supposons R cyclique.

- Si $N_\Gamma(R) = C_\Gamma(R)$, le théorème de r-nilpotence de Burnside montre que Γ est r-nilpotent. En particulier, $O_{r'}(\Gamma)$ est donc un sous-groupe propre de Γ et contient tous les p-Sylow de Γ. Il en découle que les p-Sylow de Γ sont distingués dans $O_{r'}(\Gamma)$, mais donc aussi dans Γ car $O_{r'}(\Gamma) \sqsubseteq \Gamma$ — contradiction. Conclusion : $N_\Gamma(R) \neq C_\Gamma(R)$.
- À présent, l'action de $N_\Gamma(R)$ sur R par conjugaison nous fournit un morphisme de groupes injectif de $\dfrac{N_\Gamma(R)}{C_\Gamma(R)}$ dans $\mathrm{Aut}(R)$, et comme R est cyclique d'ordre r^m pour un certain $m \in \mathbb{N}^*$: $\big|\mathrm{Aut}(R)\big| = r^{m-1}(r-1)$. En particulier, $\big|N_\Gamma(R) : C_\Gamma(R)\big|$ divise $r-1$ car R est abélien. Par définition de r, $\big|N_\Gamma(R) : C_\Gamma(R)\big|$ est ainsi forcément une puissance de p et de plus $r > p$. Donnons-nous alors un élément x d'ordre p de $N_\Gamma(R) \setminus C_\Gamma(R)$ et un générateur u de R. Aussitôt $u^x \in R^x = R$, donc u et u^x commutent, donc d'après **23**, u étant non trivial : $u = -I_2$. Il en découle que $r = 2$ — contradiction car $r > p \geqslant 3$. Conclusion : R n'est pas cyclique. Cela signifie à la fois que $r = 2$ et que R contient un sous-groupe isomorphe au groupe des quaternions. ∎

Le théorème qui suit prolonge le précédent dans le cas p-séparable.

Théorème 26 (De l'art de faire surgir $\mathrm{SL}_2(3)$ dans $\mathrm{SL}_2(q)$) Soient p un nombre premier IMPAIR, q une puissance non triviale de p et Γ un sous-groupe p-séparable de $\mathrm{SL}_2(q)$. Si les p-Sylow de Γ ne sont pas distingués dans Γ, Γ possède un sous-groupe isomorphe à $\mathrm{SL}_2(3)$.

Démonstration Par hypothèse, Γ n'est pas un p'-groupe, donc nous pouvons nous en donner une fois pour toutes un élément x d'ordre p. Posons en outre $Z = Z\big(\mathrm{SL}_2(q)\big) = \big\{I_2, -I_2\big\}$.

- D'après **22** (iv) : $O_p(\Gamma) = 1$, donc $O_{p'}(\Gamma) \neq 1$ d'après **6** car Γ est p-séparable, donc nous pouvons nous donner un diviseur premier quelconque r de $\big|O_{p'}(\Gamma)\big|$. Parce qu'il normalise $O_{p'}(\Gamma)$, x agit par conjugaison sur $\mathrm{Syl}_q\big(O_{p'}(\Gamma)\big)$, dont le cardinal est premier à p car il divise $\big|O_{p'}(\Gamma)\big|$ 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 $u \in Z(R)$, u et u^x commutent, donc $u \in Z$ d'après **23**. Comme $R \neq 1$, cela montre que $Z(R) = Z$. Mais cela montre aussi que $r = 2$, et comme r est quelconque, que $O_{p'}(\Gamma) = R$ est un 2-groupe.

  Ensuite, d'après **7**, Γ étant p-séparable : $C_G(R) = C_\Gamma\big(O_{p'}(\Gamma)\big) \leqslant O_{p'}(\Gamma) = R$, donc $C_\Gamma(R) \neq R$. A fortiori $R \neq Z$ car $Z = Z\big(\mathrm{SL}_2(q)\big)$.
- Intéressons-nous à présent au 2-groupe quotient non trivial $\dfrac{R}{Z}$. Son centre est lui-même non trivial et ses involutions forment un sous-groupe caractéristique de $\dfrac{R}{Z}$ 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 $k = i^{x^2}$, 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 $(ijk)^x = (ijk)^i$, donc $jki^{x^3} = jki$, 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. Il en découle que $p = 3$ car x est d'ordre p.

  Comme $ijk \in Z$: $jk = \pm i$, 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 $\langle i, j\rangle = \big\{\pm I_2, \pm i, \pm j, \pm k\big\}$, et il est clair à présent que $\langle i, j\rangle$ est isomorphe au groupe des quaternions. Le produit semi-direct $\langle x\rangle\langle i, j\rangle$ est enfin d'ordre $3 \times 8 = 24 = \big|\mathrm{SL}_2(3)\big|$ et il n'est pas difficile de se convaincre qu'il est isomorphe à $\mathrm{SL}_2(3)$. ∎

5.3 Une condition suffisante de p-stabilité

Théorème 27 (Groupes non p-stables) Soient p un nombre premier IMPAIR et G un groupe.

(i) Si G N'est PAS p-stable, il possède une section isomorphe au groupe des quaternions.

(ii) Si de plus G est p-séparable, alors $p=3$ et G possède une section isomorphe à $\mathrm{SL}_2(3)$.

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

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

Démonstration D'après **21**, 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 $\mathrm{SL}_2(q)$ dont les p-Sylow ne sont pas distingués. Cette section Γ possède elle-même un sous-groupe isomorphe au groupe des quaternions d'après **25**, donc G possède une section isomorphe au groupe des quaternions. Et si de plus G est p-séparable, Γ l'est aussi d'après **5**, donc possède une section isomorphe à $\mathrm{SL}_2(3)$ d'après **26**, ce qui est fortiori le cas de G.

Ça y est, les pièces du puzzle sont enfin en place et le théorème de p-nilpotence de Glauberman-Solomon est à notre portée.

Théorème 28 (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) $\mathrm{N}_G\big(\mathrm{D}^*(P)\big)$ 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 — éventuellement triviaux — est p-stable d'après **27**, donc d'après le théorème D^*, tout groupe p-séparable G pour lequel $\mathrm{C}_G\big(\mathrm{O}_p(G)\big) \leqslant \mathrm{O}_p(G)$ et dont les 2-Sylow sont abéliens satisfait la proposition universelle : $\forall P \in \mathrm{Syl}_p(G),\quad \mathrm{D}^*(P) \sqsubseteq G$. La réduction p-séparable de Thompson fournit la conclusion souhaitée.

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

Théorème 29 (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 maximal 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 $P \in \mathrm{Syl}_p(G)$, 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 : $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) = G$ ou $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) = P$.

- Si $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) = G$: $\mathrm{D}^*(P) \trianglelefteqslant G$. Or $P \neq 1$, donc $\mathrm{D}^*(P) \neq 1$, donc si nous notons d'une barre les quotients par $\mathrm{D}^*(P)$, $\overline{P}$ est un p-Sylow maximal dans $\overline{G}$, donc $\overline{G}$ est résoluble par hypothèse de récurrence. A fortiori, $\mathrm{D}^*(P)$ étant un p-groupe, G lui-même est résoluble.
- Supposons désormais que $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) = P$. En particulier, $\mathrm{N}_G\big(\mathrm{D}^*(P)\big)$ est p-nilpotent, donc G aussi d'après le théorème de p-nilpotence de Glauberman-Solomon : $G = \mathrm{O}_{p'}(G)\,P$ avec $\mathrm{O}_{p'}(G) \neq 1$. Donnons-nous alors un diviseur premier q de $\big|\mathrm{O}_{p'}(G)\big|$. L'action par conjugaison de P sur $\mathrm{Syl}_q\big(\mathrm{O}_{p'}(G)\big)$ possède un point fixe Q d'après l'équation aux classes, car $\big|\mathrm{O}_{p'}(G)\big|$ est premier à p. Or dans ces conditions, PQ est un sous-groupe de G, donc $PQ = G$ par maximalité de P, autrement dit $\mathrm{O}_{p'}(G) = Q$. Comme voulu, G est résoluble puisque P et $\mathrm{O}_{p'}(G) = Q$ 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 $G = \mathrm{GL}_3(2)$ comme contre-exemple. Ce groupe est pour commencer d'ordre $\big(2^3-1\big)\big(2^3-2\big)\big(2^3-2^2\big) = 168$. Ensuite, parce qu'on travaille sur le corps $\mathbb{F}_2$: $\quad G = \mathrm{GL}_3(2) = \mathrm{SL}_3(2) = \mathrm{PSL}_3(2),\quad$ 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 $P \leqslant \mathrm{N}_G(P) \leqslant \mathrm{C}_G(\tau)$, or après calcul $\mathrm{C}_G(\tau) = P$ donc $\mathrm{N}_G(P) = \mathrm{C}_G(\tau) = P$. L'égalité $\mathrm{C}_G(\tau) = P$ 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 $\big|S_{G/M}\big| = 6$ alors que $|G| = 168$.
- **Cas où $|M| = 24$:** D'après les théorèmes de Sylow : $\quad \big|\mathrm{Syl}_2(M)\big| = \big|M : \mathrm{N}_M(P)\big| = \big|M : P\big| = 3,\quad$ 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 $\big\{1, \sigma, \sigma^{-1}\big\}$ 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 $\sigma^\theta \in \big\{\sigma, \sigma^{-1}\big\}$, donc $\sigma^{\theta^2} = \sigma$, et comme $\theta^2 = \tau$: $\quad \sigma \in \mathrm{C}_G(\tau) = P\quad$ — contradiction.

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

6 Le théorème de Thompson sur les automorphismes sans point fixe

Nous démontrons dans cette dernière partie le théorème que Thompson visait dans sa thèse de 1959.

Théorème 30 (Propriétés des automorphismes sans point fixe) Soient G un groupe et $\varphi \in \mathrm{Aut}(G)$ sans point fixe.

(i) L'application $x \longmapsto \big[x, \varphi\big]$ est bijective de G sur G.

(ii) Pour tout nombre premier p, G possède un p-Sylow P stable par φ.

(iii) Soit N un sous-groupe distingué de G stable par φ. L'automorphisme $Nx \longmapsto Nx^\varphi$ de $\dfrac{G}{N}$ induit par φ est sans point fixe et son ordre divise celui de φ.

Démonstration

(i) Comme G est fini, nous pouvons nous contenter de montrer que $x \longmapsto \big[x, \varphi\big]$ est injective sur G. Or pour tous $x, y \in G$, si $\big[x, \varphi\big] = \big[y, \varphi\big]$: $\quad x^{-1}x^\varphi = y^{-1}y^\varphi,\quad$ donc $\big(xy^{-1}\big)^\varphi = xy^{-1}$. Ainsi $xy^{-1} = 1$ par définition de φ, i.e. $x = y$.

(ii) Soient p un nombre premier et $P \in \mathrm{Syl}_p(G)$. Alors P^φ est aussi un p-Sylow de G, donc d'après les théorèmes de Sylow : $\quad P^\varphi = P^g\quad$ pour un certain $g \in G$. Or d'après (i) : $\quad g = \big[x, \varphi\big]\quad$ pour un certain $x \in G$, donc $\big(P^{x^{-1}}\big)^\varphi = \big(P^\varphi\big)^{(x^\varphi)^{-1}} = \big(P^g\big)^{(x^\varphi)^{-1}} = P^{g(x^\varphi)^{-1}} = P^{x^{-1}}$.

(iii) L'application $Nx \overset{\overline{\varphi}}{\longmapsto} Nx^\varphi$ est un automorphisme de $\dfrac{G}{N}$ de réciproque $Nx \longmapsto Nx^{\varphi^{-1}}$ car N est stable par φ. En outre, pour tous $n \in \mathbb{N}$ et $x \in G$: $\quad (Nx)^{\overline{\varphi}^n} = Nx^{\varphi^n} = Nx,\quad$ donc l'ordre de $\overline{\varphi}$ divise n.

Montrons que $\overline{\varphi}$ est sans point fixe. Pour tout $g \in G$, si $(Ng)^{\overline{\varphi}} = Ng$: $\quad Ng^\varphi = Ng,\quad$ donc $\big[g, \varphi\big] \in N$. Or l'application $x \longmapsto \big[x, \varphi\big] = x^{-1}x^\varphi$ est injective d'après (i) et stabilise N. Elle est même bijective de N sur N car N est fini, donc $g \in N$, i.e. $Ng = N$. ∎

Quelques mots s'imposent sur le concept de *nilpotence*. Un groupe fini est dit *nilpotent* s'il possède un unique p-Sylow pour tout nombre premier p, ce qui le rend égal au produit de ses différents p-Sylow. Il est équivalent de dire qu'un tel groupe est p-nilpotent pour tout nombre premier p.

Théorème 31 (Théorème de Thompson) Soit G un groupe. Si G possède un automorphisme sans point fixe d'ordre premier, alors G est nilpotent.

Démonstration Par récurrence sur $|G|$, faisons l'hypothèse que le théorème est vrai de tout groupe d'ordre strictement inférieur à $|G|$. Nous noterons q l'ordre premier de φ. Si G est un p-groupe pour un certain nombre premier, il est nilpotent et c'est fini. Plaçons-nous désormais dans le cas contraire et donnons-nous un diviseur premier IMPAIR p de $|G|$. D'après **30** (ii), G possède un p-Sylow propre P pour lequel $P^\varphi = P$. Comme $\mathrm{D}^*(P) \sqsubseteq P$, a fortiori $\mathrm{D}^*(P)^\varphi = \mathrm{D}^*(P)$ et $\mathrm{N}_G\big(\mathrm{D}^*(P)\big)^\varphi = \mathrm{N}_G\big(\mathrm{D}^*(P)\big)$.

- Supposons d'abord que $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) < G$. Dans ce cas, $\varphi|_{\mathrm{N}_G(\mathrm{D}^*(P))}$ est un automorphisme sans point fixe de $\mathrm{N}_G\big(\mathrm{D}^*(P)\big)$ dont l'ordre divise q. Or $P \neq 1$, donc $\mathrm{D}^*(P) \neq 1$, donc $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) \neq 1$, donc $\varphi|_{\mathrm{N}_G(\mathrm{D}^*(P))} \neq \mathrm{Id}$. Finalement, $\varphi|_{\mathrm{N}_G(\mathrm{D}^*(P))}$ est d'ordre q, donc par hypothèse de récurrence, $\mathrm{N}_G\big(\mathrm{D}^*(P)\big)$ est nilpotent, donc p-nilpotent. Comme p est impair, G est a fortiori lui-même p-nilpotent d'après le théorème de p-nilpotence de Glauberman-Solomon, autrement dit $G = \mathrm{O}_{p'}(G)P$.

  Ensuite $\mathrm{O}_{p'}(G) \sqsubseteq G$, donc $\varphi|_{\mathrm{O}_{p'}(G)}$ est un automorphisme sans point fixe de $\mathrm{O}_{p'}(G)$ dont l'ordre divise q. Si $\mathrm{O}_{p'}(G) = 1$, G est un p-groupe et c'est fini. Plaçons-nous dans le cas contraire. Dans ce cas, $\varphi|_{\mathrm{O}_{p'}(G)}$ est d'ordre q, donc par hypothèse de récurrence, $\mathrm{O}_{p'}(G)$ est nilpotent. A fortiori, $G = \mathrm{O}_{p'}(G)P$ est résoluble.
- Supposons maintenant que $\mathrm{N}_G\big(\mathrm{D}^*(P)\big) = G$. Dans ce cas, d'après **30** (iii), l'automorphisme de $\dfrac{G}{\mathrm{D}^*(P)}$ induit par φ est sans point fixe et son ordre divise q, mais comme $\mathrm{D}^*(P) \neq G$, cet automorphisme est d'ordre q, donc par hypothèse de récurrence, $\dfrac{G}{\mathrm{D}^*(P)}$ est nilpotent. A fortiori, G est résoluble.

À ce stade, nous avons montré que G est résoluble dans tous les cas. Soit r un diviseur premier quelconque de $|G|$ — éventuellement $r = 2$. D'après **6** : $\quad \mathrm{O}_r(G) \neq 1 \quad$ ou $\quad \mathrm{O}_{r'}(G) \neq 1$.

- Si $\mathrm{O}_r(G) \neq 1$, l'automorphisme de $\dfrac{G}{\mathrm{O}_r(G)}$ induit par φ est sans point fixe et son ordre divise q d'après **30** (iii), mais comme $\mathrm{O}_r(G) \neq G$, cet automorphisme est d'ordre q, donc $\dfrac{G}{\mathrm{O}_r(G)}$ est nilpotent par hypothèse de récurrence. En particulier, $\dfrac{G}{\mathrm{O}_r(G)}$ possède un unique r-Sylow, mais il en va donc de même de G puisque tout r-Sylow de G contient $\mathrm{O}_r(G)$.
- Supposons à présent que $\mathrm{O}_{r'}(G) \neq 1$. Comme au point précédent avec $\dfrac{G}{\mathrm{O}_r(G)}$, $\dfrac{G}{\mathrm{O}_{r'}(G)}$ est nilpotent par hypothèse de récurrence, donc en particulier possède un unique r-Sylow. Fixons $R \in \mathrm{Syl}_r(G)$. Le quotient $\dfrac{\mathrm{O}_{r'}(G)R}{\mathrm{O}_{r'}(G)}$ est alors l'unique r-Sylow de $\dfrac{G}{\mathrm{O}_{r'}(G)}$, donc est caractéristique dans $\dfrac{G}{\mathrm{O}_{r'}(G)}$. A fortiori, $\mathrm{O}_{r'}(G)R$ est caractéristique dans G.

  Si G n'est pas r-nilpotent, i.e. si $\mathrm{O}_{r'}(G)R \neq G$, $\varphi|_{\mathrm{O}_{r'}(G)R}$ est un automorphisme sans point fixe de $\mathrm{O}_{r'}(G)R$ dont l'ordre divise q, mais comme $\mathrm{O}_{r'}(G)R \neq 1$, cet automorphisme est d'ordre q, donc $\mathrm{O}_{r'}(G)R$ est nilpotent par hypothèse de récurrence. A fortiori, R est l'unique r-Sylow de $\mathrm{O}_{r'}(G)R$, mais comme il est distingué dans G, $\mathrm{O}_{r'}(G)R$ contient tous les r-Sylow de G. Bref, R est l'unique r-Sylow de G.

Au point où nous en sommes, G possède un unique r-Sylow pour tout nombre premier r, sauf éventuellement s'il est r-nilpotent pour tout nombre premier r. Or dans ce cas, G est nilpotent comme voulu. ∎

Nous achèverons ce texte sur une généralisation du théorème **24**. Pour démontrer ce théorème, nous avons copieusement exploité le fait que le groupe G était supposé abélien, mais l'hypothèse est en réalité factice comme je l'avais d'ailleurs annoné.

Théorème 32 (Structure d'un p-groupe d'automorphismes sans point fixe d'un groupe abélien) Soient G un groupe, p un nombre premier et A un p-sous-groupe sans point fixe de $\mathrm{Aut}(G)$.

(i) Si $p \neq 2$, A est cyclique.

(ii) Si $p = 2$, soit A est cyclique, soit A possède un sous-groupe isomorphe au groupe des quaternions.

Démonstration On peut supposer $A \neq \{\mathrm{Id}\}$ — a fortiori $G \neq 1$. Dans tous les cas, A contient un élément d'ordre p, autrement dit un automorphisme sans point fixe de G d'ordre p, donc G est nilpotent d'après le théorème de Thompson. Donnons-nous un diviseur premier q de $|G|$. Notre groupe G possède alors un unique q-Sylow Q, lequel est forcément stable par tout élément de A, de même que son centre $\mathrm{Z}(Q)$. Grâce à cette réduction, A est un p-sous-groupe sans point fixe de $\mathrm{Aut}\big(\mathrm{Z}(Q)\big)$ et il ne nous reste plus qu'à appliquer **24**, car contrairement à G, $\mathrm{Z}(Q)$ est abélien. ∎