LE TRANSFERT ET SES APPLICATIONS

La détermination des groupes finis simples non abéliens, qui sont ce que les atomes sont aux molécules et les nombres premiers aux entiers, a été l'un des enjeux majeurs de la théorie des groupes finis depuis sa naissance. Il n'est malheureusement pas souvent facile de savoir si un groupe est simple ou non. Il est en tout cas bien connu que le noyau d'un morphisme de groupes est distingué dans son groupe de départ, mais bien connu aussi que tout sous-groupe distingué N d'un groupe G est le noyau du morphisme $x \longmapsto Nx$ de G sur $\dfrac{G}{N}$. La recherche des sous-groupes distingués d'un groupe G se ramène ainsi à la recherche des morphismes de groupes qu'on peut définir sur G.

Est-il cependant facile de construire des morphismes de groupes qui ne soient pas donnés d'emblée comme des surjections canoniques ? En dépit des apparences, nous allons voir que oui, c'est assez facile. À tout sous-groupe H d'un groupe fini G, nous allons associer dans ce texte un morphisme de groupes $V_{G\to H}$ appelé le *transfert de G dans H*. Ce morphisme, introduit par Schur en 1902, ne sera pas défini de G dans H, mais de G dans le groupe abélien $\dfrac{H}{\mathrm{D}(H)}$ où $\mathrm{D}(H)$ désigne le groupe dérivé de H. Le problème de ces morphismes de transfert $V_{G\to H}$, c'est qu'ils ont beau être nombreux — un par sous-groupe H de G — leur construction n'exclut pas qu'ils soient nuls, i.e. de noyau G lui-même.

Ce texte est découpé en sept parties.

— La première est consacrée à la seule définition du transfert, déroutante au premier abord.

— On s'intéresse dans la deuxième partie aux carrés de $\mathbb{Z}_p$ pour tout nombre premier p impair. Le symbole de Legendre est interprété comme un simple transfert, remarque dont on tire à la fois la *loi de réciprocité quadratique* de Gauss et sa *loi complémentaire*.

— On étudie ensuite le transfert d'un groupe dans son centre, dont on tire un joli théorème de finitude de Schur.

— La quatrième partie prolonge la première de par sa généralité et introduit, en lien avec le transfert, les concepts importants de *sous-groupe focal* et de *fusion* des classes de conjugaison.

— On s'intéresse ensuite au transfert d'un groupe dans un p-Sylow. Cette partie, de loin la plus riche, est un peu le point de départ de l'*analyse p-locale*, une branche essentielle de la théorie des groupes finis dont les enjeux et les méthodes ne seront cependant qu'esquissés.

— On démontre ensuite partiellement un *théorème de Frobenius* sur les groupes éponymes dont la seule démonstration complète à ce jour requiert la *théorie des caractères*, une branche de la théorie des représentations.

— Trois cas particuliers du *théorème Z^* de Glauberman* sont finalement démontrés. Ce résultat décrit l'impact de certaines involutions sur la structure d'un groupe qui en contient et constitue un puissant critère de non-simplicité. Étape majeure de la classification des groupes finis simples, ce théorème n'est aujourd'hui démontré complètement que dans le cadre de la *théorie des caractères modulaires*, une adaptation de la théorie des caractères ordinaires au cas d'un corps de caractéristique non nulle.

Nous terminerons cette introduction par le rappel de quelques notations.

$\lvert X\rvert$	Cardinal de l'ensemble X
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 »
G/H	Ensemble des classes à droite de G modulo H
$\lvert G : H\rvert$	Indice du sous-groupe H dans le groupe G
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
H^g	Conjugué $g^{-1}Hg$ du sous-groupe H par l'élément g
$\mathrm{N}_G(H)$	Normalisateur dans le groupe G du sous-groupe H
$\mathrm{C}_G(H)$	Centralisateur dans le groupe G du sous-groupe H
$\langle X\rangle$	Sous-groupe engendré par l'ensemble X dans un groupe donné

$[x,y]$	Commutateur $x^{-1}y^{-1}xy$ de x et y
$\mathrm{D}(G)$	Sous-groupe dérivé du groupe G
$\mathrm{Syl}_p(G)$	Ensemble des p-Sylow du groupe fini G pour un nombre premier p
$\mathrm{Aut}(G)$	Groupe des automorphismes du groupe G
$A \ltimes G$	Produit semi-direct du (sous-)groupe G par le (sous-)groupe A
$\mathbb{Z}_n$	Quotient du groupe $\mathbb{Z}$ par son sous-groupe $n\mathbb{Z}$ pour un entier naturel non nul n
$\mathbb{F}_q$	Corps fini de cardinal q où q est une puissance non triviale d'un nombre premier

1 Définition du transfert

Nous partons d'un groupe quelconque G et d'un sous-groupe d'indice fini H de G. Dans la plupart de nos applications, le groupe G sera fini, mais la construction du transfert requiert seulement la finitude de $\big|G : H\big|$. Le groupe G opère par translation sur l'ensemble G/H de ses classes à droite modulo H. Donnons-nous alors une transversale à droite quelconque θ de H dans G, autrement dit, pour toute classe $\alpha \in G/H$, un élément α^θ de α. L'ensemble $\big\{\alpha^\theta\big\}_{\alpha\in G/H}$ est aussi ce qu'on appelle souvent un ensemble de représentants des classes à droite de G modulo H. Pour tout $\alpha \in G/H$, on a donc : $\alpha = H\alpha^\theta$.

Remarquons à présent que l'action de G sur G/H ne nous fournit aucune action de G sur l'ensemble des représentants $\big\{\alpha^\theta\big\}_{\alpha\in G/H}$. Pour tous $g \in G$ et $\alpha \in G/H$, en effet, alors que le produit $\alpha^\theta g$ appartient à la classe αg, rien ne nous dit qu'il coïncide avec le représentant $(\alpha g)^\theta$. Ce n'est pas le cas en général. Quoi qu'il en soit, l'égalité : $H\alpha^\theta g = \alpha g = H(\alpha g)^\theta$ montre que le produit $\alpha^\theta g\big((\alpha g)^\theta\big)^{-1}$ appartient à H. Si nous notons $h_\theta(\alpha, g)$ ce produit, alors :

$$\boxed{\alpha^\theta g = h_\theta(\alpha,g)\,(\alpha g)^\theta,}$$

relation que nous noterons ♠. On comprend sur cette relation le sens de la fonction h_θ. Cette fonction mesure l'écart qui sépare $\alpha^\theta g$ de $(\alpha g)^\theta$.

L'associativité du produit dans G donne à h_θ une propriété fonctionnelle bien particulière. Pour tous $g, g' \in G$ et $\alpha \in G/H$, en effet : $h_\theta(\alpha, gg')\,(\alpha gg')^\theta \overset{\spadesuit}{=} \alpha^\theta gg' \overset{\spadesuit}{=} h_\theta(\alpha,g)\,(\alpha g)^\theta g' \overset{\spadesuit}{=} h_\theta(\alpha,g)\,h_\theta(\alpha g,g')\,(\alpha gg')^\theta$. Finalement :

$$\boxed{h_\theta(\alpha,gg') = h_\theta(\alpha,g)\,h_\theta(\alpha g,g'),}$$

relation que nous noterons ♣. Cette identité n'est pas loin de faire de h_θ un morphisme de groupes par rapport à sa première variable, mais la deuxième variable fait obstacle. Pour la faire disparaître, l'idéal serait qu'on puisse écrire un produit de ce genre :

$$\prod_{\alpha\in G/H} h_\theta(\alpha,gg') = \prod_{\alpha\in G/H} h_\theta(\alpha,g) \prod_{\alpha\in G/H} h_\theta(\alpha g,g'),$$

qui deviendrait après changement d'indice : $\displaystyle\prod_{\alpha\in G/H} h_\theta(\alpha,gg') = \prod_{\alpha\in G/H} h_\theta(\alpha,g) \prod_{\alpha\in G/H} h_\theta(\alpha,g')$. La fonction $\displaystyle g \longmapsto \prod_{\alpha\in G/H} h_\theta(\alpha,g)$ serait ainsi un morphisme de groupes de G dans H.

Le problème des calculs qui précèdent, c'est que le groupe H n'est pas commutatif. Or nous avons utilisé la commutativité du produit à deux endroits ci-dessus :

— une première fois avec la notation « $\displaystyle\prod_{\alpha\in G/H}$ » qui requiert un ordre d'énumération,

— une deuxième fois avec la règle implicite « $\displaystyle\prod_{\alpha\in G/H}(x_\alpha y_\alpha) = \prod_{\alpha\in G/H} x_\alpha \prod_{\alpha\in G/H} y_\alpha$ ».

Finalement, il suffirait qu'on travaille dans le groupe abélien $\dfrac{H}{\mathrm{D}(H)}$ et tout irait bien. Le *transfert de G dans H* est par définition l'application $\displaystyle g \overset{V_{G\to H}}{\longmapsto} \overline{\prod_{\alpha\in G/H}} h_\theta(\alpha,g)$ de G dans $\dfrac{H}{\mathrm{D}(H)}$, où le symbole « $\overline{\prod}$ » désigne un produit d'éléments de H calculé dans $\dfrac{H}{\mathrm{D}(H)}$. Cette application $V_{G\to H}$ est comme annoncé un morphisme de groupes car pour tous $g, g' \in G$:

$$\begin{aligned} V_{G\to H}(gg') &= \overline{\prod_{\alpha\in G/H}} h_\theta(\alpha,gg') \overset{\clubsuit}{=} \overline{\prod_{\alpha\in G/H}} \Big(h_\theta(\alpha,g)\,h_\theta(\alpha g,g')\Big) = \overline{\prod_{\alpha\in G/H}} h_\theta(\alpha,g) \overline{\prod_{\alpha\in G/H}} h_\theta(\alpha g,g') \overset{\alpha'=\alpha g}{=} \overline{\prod_{\alpha\in G/H}} h_\theta(\alpha,g) \overline{\prod_{\alpha'\in G/H}} h_\theta(\alpha',g') \\ &= V_{G\to H}(g)\,V_{G\to H}(g'). \end{aligned}$$

Alors que $h_\theta(\alpha,g)$ mesure l'écart qui sépare $\alpha^\theta g$ de $(\alpha g)^\theta$, $V_{G\to H}(g)$ est en résumé la « somme » de ces écarts et mesure une sorte d'écart total qui sépare l'ensemble de représentants $\left\{\alpha^\theta\right\}_{\alpha\in G/H}$ de son produit $\left\{\alpha^\theta g\right\}_{\alpha\in G/H}$ par g.

Le transfert de G dans H semble d'ailleurs dépendre tout à fait de la transversale θ qu'on a choisie pour le définir. Ce n'est pourtant pas le cas. Donnons-nous en effet une transversale θ' de H dans G et notons $V'_{G\to H}$ le transfert de G dans H associé. Pour tout $\alpha\in G/H$: $\quad H\alpha^{\theta'}=\alpha=H\alpha^\theta,\quad$ donc : $\quad\alpha^{\theta'}=\eta_\alpha\alpha^\theta\quad$ pour un certain $\eta_\alpha\in H$. Les transferts $V_{G\to H}$ et $V'_{G\to H}$ coïncident car pour tout $g\in G$:

$$V'_{G\to H}(g)=\overline{\prod_{\alpha\in G/H}}h_{\theta'}(\alpha,g)=\overline{\prod_{\alpha\in G/H}}\alpha^{\theta'}g\left((\alpha g)^{\theta'}\right)^{-1}=\overline{\prod_{\alpha\in G/H}}\eta_\alpha\alpha^\theta g\left((\alpha g)^\theta\right)^{-1}\eta_{\alpha g}^{-1}=\left(\overline{\prod_{\alpha\in G/H}}\eta_\alpha\right)\overline{\prod_{\alpha\in G/H}}h_\theta(g,\alpha)\left(\overline{\prod_{\alpha\in G/H}}\eta_{\alpha g}\right)^{-1}$$
$$\overset{\alpha'=\alpha g}{=}\left(\overline{\prod_{\alpha\in G/H}}\eta_\alpha\right)V_{G\to H}(g)\left(\overline{\prod_{\alpha'\in G/H}}\eta_{\alpha'}\right)^{-1}=V_{G\to H}(g).$$

L'énoncé suivant résume notre construction du transfert.

Définition-théorème 1 **(Transfert dans un sous-groupe d'indice fini)** Soient G un groupe et H un sous-groupe d'indice fini de G. Le symbole « $\overline{\prod}$ » désigne ci-dessous un produit d'éléments de H calculé dans $\dfrac{H}{\mathrm{D}(H)}$.

- Pour tout $g\in G$ et pour toute transversale à droite θ de H dans G, l'élément : $\overline{\prod_{\alpha\in G/H}}\alpha^\theta g\left((\alpha g)^\theta\right)^{-1}$ de $\dfrac{H}{\mathrm{D}(H)}$ ne dépend pas de θ. On le note $V_{G\to H}(g)$.
- L'application $V_{G\to H}$ est un morphisme de groupes de G dans $\dfrac{H}{\mathrm{D}(H)}$ appelé le *transfert de G dans H*.

Deux petites remarques. Premièrement, le transfert de G dans H ne présente aucun intérêt si H est un groupe *parfait*, i.e. si : $\mathrm{D}(H)=H$. Deuxièmement, le quotient $\dfrac{H}{\mathrm{D}(H)}$ étant abélien, $\mathrm{Ker}\,V_{G\to H}$ contient toujours $\mathrm{D}(G)$.

Le moins qu'on puisse dire en tout cas, c'est que cette définition classique du transfert ne brille pas par son évidence calculatoire. Nous venons de construire une foule de morphismes, mais est-il possible de les calculer concrètement ? Le résultat qui suit montre que oui. S'il semble obscur au premier abord, c'est vraiment grâce à lui que le transfert est toujours calculé.

Théorème 2 **(Calcul du transfert)** Soient G un groupe, H un sous-groupe d'indice fini de G et $g\in G$.

L'action de $\langle g\rangle$ sur G/H possède un certain nombre r d'orbites dont on se donne des représentants $Hx_1^{-1},\dots,Hx_r^{-1}$ avec $x_1,\dots,x_r\in G$. Pour tout $i\in[\![1,r]\!]$, le cardinal de la $\langle g\rangle$-orbite de Hx_i^{-1} est noté n_i. En particulier : $\quad\left|G:H\right|=\sum_{1\leqslant i\leqslant r}n_i.$

Avec ces notations : $\quad\left(g^{n_i}\right)^{x_i}\in H\quad$ pour tout $i\in[\![1,r]\!]$ et : $\quad V_{G\to H}(g)=\overline{\prod_{1\leqslant i\leqslant r}}\left(g^{n_i}\right)^{x_i}.$

Démonstration Les éléments de G/H sont exactement les ensembles $Hx_i^{-1}g^j$, i décrivant $[\![1,r]\!]$ et j décrivant $[\![0,n_i-1]\!]$. Le transfert ne dépendant pas de la transversale choisie pour le définir, nous allons calculer $V_{G\to H}(g)$ grâce à la transversale θ définie pour tous i et j par : $\quad\left(Hx_i^{-1}g^j\right)^\theta=x_i^{-1}g^j.$

Remarquons tout d'abord que pour tout $i\in[\![1,r]\!]$, par définition de n_i : $\quad Hx_i^{-1}g^{n_i}=Hx_i^{-1},\quad$ autrement dit : $\left(g^{n_i}\right)^{x_i}\in H$. À présent, pour tous $i\in[\![1,r]\!]$ et $j\in[\![0,n_i-1]\!]$, la contribution de $Hx_i^{-1}g^j$ au produit qui définit $V_{G\to H}(g)$ vaut dans H :

$$\left(Hx_i^{-1}g^j\right)^\theta g\left(\left(Hx_i^{-1}g^{j+1}\right)^\theta\right)^{-1}=\begin{cases}\left(Hx_i^{-1}g^{n_i-1}\right)^\theta g\left(\left(Hx_i^{-1}g^{n_i}\right)^\theta\right)^{-1}=\left(x_i^{-1}g^{n_i-1}\right)g\left(\left(Hx_i^{-1}\right)^\theta\right)^{-1}=\left(g^{n_i}\right)^{x_i} & \text{si } j=n_i-1\\ \left(x_i^{-1}g^j\right)g\left(x_i^{-1}g^{j+1}\right)^{-1}=1 & \text{sinon.}\end{cases}$$

Par produit, comme voulu : $\quad V_{G\to H}(g)=\overline{\prod_{1\leqslant i\leqslant r}}\left(g^{n_i}\right)^{x_i}.$ ■

Dans le cas où G est abélien, ce calcul du transfert peut être simplifié davantage. L'application $V_{G\longrightarrow H}$ est dans ce cas définie de G dans H, et avec les notations du théorème précédent : $\quad V_{G\to H}(g)=\prod_{1\leqslant i\leqslant r}\left(g^{n_i}\right)^{x_i}=\prod_{1\leqslant i\leqslant r}g^{n_i}=g^{|G:H|}.\quad$ À

vrai dire, G étant abélien et d'après le théorème de Lagrange, il était clair à l'avance que l'application $g \longmapsto g^{|G:H|}$ était un morphisme de groupe de G dans H, mais la définition du transfert nous donne une expression différente de cette fonction puissance.

Théorème 3 (Transfert dans un groupe abélien) Soient G un groupe abélien et H un sous-groupe d'indice fini de G. Pour tout $g \in G$: $V_{G\to H}(g) = g^{|G:H|}$.

Ce résultat simple peut servir à démontrer déjà de jolis résultats, par exemple la fameuse *loi de réciprocité quadratique* de Gauss ainsi que sa non moins fameuse *loi complémentaire*.

2 Le symbole de Legendre comme transfert

Pour tout $n \in \mathbb{N}^*$, les ensembles $\mathbb{Z}$ et $\mathbb{Z}_n$ ont beau être distincts, nous noterons de la même manière tout élément de $\mathbb{Z}$ et son image dans $\mathbb{Z}_n$.

Définition-théorème 4 (Symbole de Legendre) Soit p un nombre premier impair. On appelle *symbole de Legendre sur* $\mathbb{Z}_p^*$ l'application $\left(\frac{\cdot}{p}\right)$ de $\mathbb{Z}_p^*$ dans lui-même définie pour tout $x \in \mathbb{Z}_p^*$ par : $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$.

(i) Plus explicitement, pour tout $x \in \mathbb{Z}_p$: $\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{Z}_p \\ -1 & \text{si } x \text{ n'est pas un carré dans } \mathbb{Z}_p. \end{cases}$

(ii) Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ coïncide avec le transfert de $\mathbb{Z}_p^*$ dans son sous-groupe $\{1,-1\}$.

Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ étant un morphisme de groupes, le calcul de ses valeurs nous ramène au calcul des nombres $\left(\frac{q}{p}\right)$, q décrivant l'ensemble des nombres premiers. Par exemple : $\left(\frac{60}{113}\right) = \left(\frac{2}{113}\right)\left(\frac{3}{113}\right)^2\left(\frac{5}{113}\right) = \left(\frac{2}{113}\right)\left(\frac{5}{113}\right)$, mais que valent $\left(\frac{2}{113}\right)$ et $\left(\frac{5}{113}\right)$?

Démonstration

(i) L'application $x \longmapsto x^2$ est surjective de $\mathbb{Z}_p^*$ dans l'ensemble de ses carrés et donne à chaque carré de $\mathbb{Z}_p^*$ exactement deux antécédents — opposés. D'après le lemme des bergers, $\mathbb{Z}_p^*$ contient ainsi exactement $\frac{p-1}{2}$ carrés.

Ensuite, d'après le théorème de Lagrange dans le groupe $\mathbb{Z}_p^*$, le polynôme $X^{p-1}-1$ de $\mathbb{Z}_p[X]$ admet tout élément de $\mathbb{Z}_p^*$ pour racine. Or : $X^{p-1}-1 = \left(X^{\frac{p-1}{2}}-1\right)\left(X^{\frac{p-1}{2}}+1\right)$, donc le polynôme $X^{\frac{p-1}{2}}-1$ possède exactement $\frac{p-1}{2}$ racines dans $\mathbb{Z}_p^*$ et les $\frac{p-1}{2}$ éléments restants sont racines de $X^{\frac{p-1}{2}}+1$.

Remarquons enfin que pour tout carré $x = y^2 \in \mathbb{Z}_p^*$ avec $y \in \mathbb{Z}_p^*$: $x^{\frac{p-1}{2}} = y^{p-1} = 1$. Les carrés de $\mathbb{Z}_p^*$ sont ainsi tous racines de $X^{\frac{p-1}{2}}-1$, et comme ils sont au nombre de $\frac{p-1}{2}$, ils sont exactement les racines de $X^{\frac{p-1}{2}}$. Les non-carrés de $\mathbb{Z}_p^*$ sont a fortiori exactement les racines de $X^{\frac{p-1}{2}}+1$.

(ii) D'après **3**, pour tout $g \in \mathbb{Z}_p^*$: $V_{\mathbb{Z}_p^*\to\{1,-1\}}(x) = x^{|\mathbb{Z}_p^*:\{1,-1\}|} = x^{\frac{p-1}{2}} = \left(\frac{x}{p}\right)$. ∎

Que le symbole de Legendre soit un transfert nous permet d'envisager de le calculer comme tel grâce au théorème **2**. Les classes à droite de $\mathbb{Z}_p^*$ modulo $\{1,-1\}$ sont les ensembles $\{x,-x\}$, x décrivant $\mathbb{Z}_p^*$, dont les éléments $1, 2, \dots, \frac{p-1}{2}$ peuvent servir de représentants. Nous noterons θ_p la transversale associée à cet ensemble $R_p = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ de représentants. L'application θ_p associe à toute classe à droite α de $\mathbb{Z}_p^*$ modulo $\{1,-1\}$ l'unique élément de $\alpha \cap R_p$.

Pour tout $x \in \mathbb{Z}_p^*$, posons enfin : $R_p(x) = \Big\{r \in R_p / \quad rx \notin R_p\Big\} = \Big\{r \in R_p / \quad -rx \in R_p\Big\}$.

Théorème 5 **(Le symbole de Legendre comme transfert)**
Soit p un nombre premier impair. Pour tout $x \in \mathbb{Z}_p^*$: $\left(\dfrac{x}{p}\right) = (-1)^{|R_p(x)|}$.

Démonstration Soit $x \in \mathbb{Z}_p^*$ fixé. Il s'agit de calculer $V_{\mathbb{Z}_p^* \to \{1,-1\}}(x)$. Pour toute classe à droite α de $\mathbb{Z}_p^*$ modulo $\{1,-1\}$, sachant que : $\alpha x = \{\alpha^{\theta_p} x, -\alpha^{\theta_p} x\}$, deux situations peuvent se présenter :

— si $\alpha^{\theta_p} x \in R_p$: $(\alpha x)^{\theta_p} = \alpha^{\theta_p} x$, donc : $\alpha^{\theta_p} x \big((\alpha x)^{\theta_p}\big)^{-1} = 1$,

— si $\alpha^{\theta_p} x \notin R_p$: $(\alpha x)^{\theta_p} = -\alpha^{\theta_p} x$, donc : $\alpha^{\theta_p} x \big((\alpha x)^{\theta_p}\big)^{-1} = -1$.

Comme voulu, par définition du transfert : $V_{\mathbb{Z}_p^* \to \{1,-1\}}(x) = \prod_\alpha \alpha^{\theta_p} x \big((\alpha x)^{\theta_p}\big)^{-1} = (-1)^{|R_p(x)|}$. ■

Théorème 6 **(Loi complémentaire)** Soit p un nombre premier impair. Alors : $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Par exemple, 2 est un carré modulo 17 mais pas modulo 11 car : $(-1)^{\frac{17^2-1}{8}} = 1$ alors que : $(-1)^{\frac{11^2-1}{8}} = -1$. On peut vérifier que : $2 \equiv 6^2\ [17]$.

Démonstration

- Si $\dfrac{p-1}{2}$ est pair : $R_p(2) = \left\{\dfrac{p-1}{4}+1, \dfrac{p-1}{4}+2, \dots, \dfrac{p-1}{2}\right\}$, donc : $\big|R_p(2)\big| = \dfrac{p-1}{4}$, donc d'après **5**, sachant que $\dfrac{p+1}{2}$ est impair : $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}\times\frac{p+1}{2}} = (-1)^{\frac{p^2-1}{8}}$.
- Si $\dfrac{p-1}{2}$ est impair : $R_p(2) = \left\{\dfrac{p+1}{4}, \dfrac{p+1}{4}+1, \dots, \dfrac{p-1}{2}\right\}$, donc : $\big|R_p(2)\big| = \dfrac{p+1}{4}$, donc d'après **5**, sachant que $\dfrac{p-1}{2}$ est impair : $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p+1}{4}} = (-1)^{\frac{p+1}{4}\times\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}$. ■

Si la loi complémentaire de Gauss est un joli théorème, le résultat le plus surprenant sur les carrés de $\mathbb{Z}_p^*$ reste quand même la *loi de réciprocité quadratique* qui, pour deux nombres premiers impairs p et q, énonce un lien inattendu entre les carrés de $\mathbb{Z}_p^*$ et ceux de $\mathbb{Z}_q^*$.

Théorème 7 **(Loi de réciprocité quadratique)**
Soient p et q deux nombres premiers impairs. Alors : $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Par exemple : $\left(\dfrac{5}{113}\right) = (-1)^{\frac{(5-1)(113-1)}{4}}\left(\dfrac{113}{5}\right) = \left(\dfrac{3}{5}\right) = (-1)^{\frac{(3-1)(5-1)}{4}}\left(\dfrac{5}{3}\right) = \left(\dfrac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$, donc 5 n'est pas un carré modulo 113.

Démonstration Posons : $E = \left\{(x,y) \in \mathbb{Z}^2 / \quad 1 \leqslant x \leqslant \dfrac{p-1}{2} \quad \text{et} \quad 1 \leqslant y \leqslant \dfrac{q-1}{2}\right\}$,

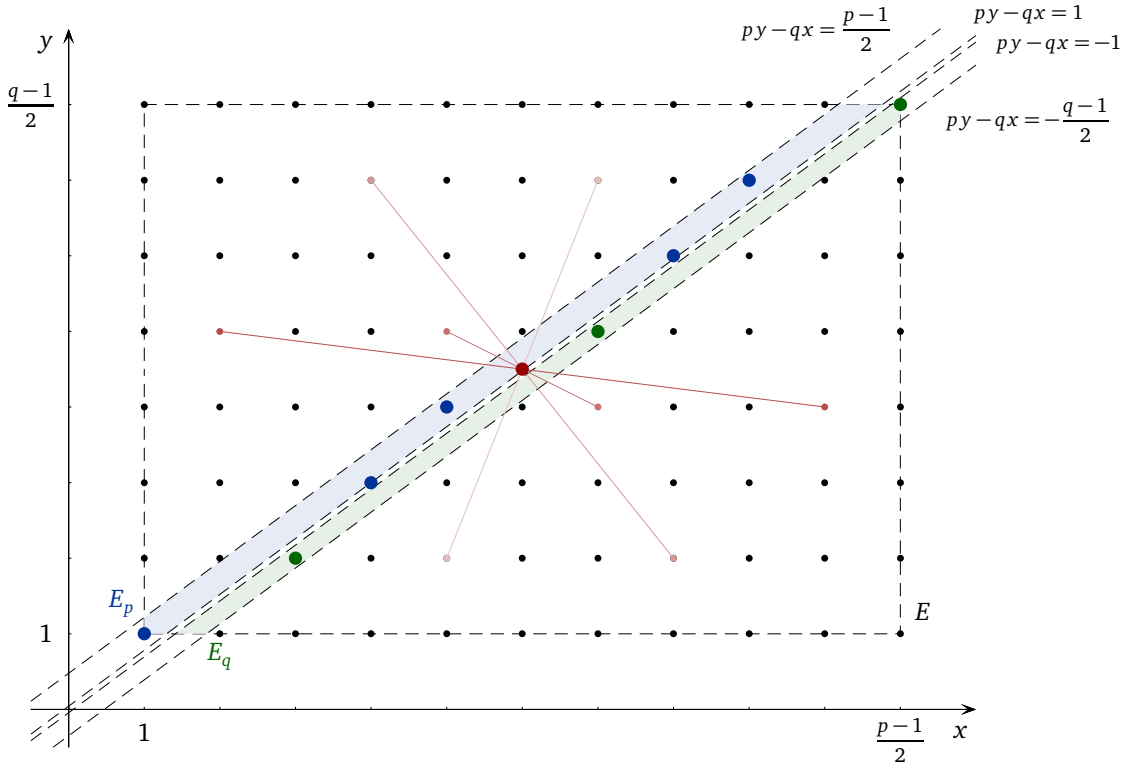
$$E_p = \left\{(x,y) \in \mathbb{Z}^2 / \quad 1 \leqslant x \leqslant \frac{p-1}{2}, \quad 1 \leqslant y \leqslant \frac{q-1}{2} \quad \text{et} \quad 1 \leqslant py - qx \leqslant \frac{p-1}{2}\right\},$$

$$E_q = \left\{(x,y) \in \mathbb{Z}^2 / \quad 1 \leqslant x \leqslant \frac{p-1}{2}, \quad 1 \leqslant y \leqslant \frac{q-1}{2} \quad \text{et} \quad -\frac{q-1}{2} \leqslant py - qx \leqslant -1\right\}$$

et : $E_{pq} = \left\{(x,y) \in \mathbb{Z}^2 / \quad 1 \leqslant x \leqslant \dfrac{p-1}{2}, \quad 1 \leqslant y \leqslant \dfrac{q-1}{2} \quad \text{et} \quad -\dfrac{q-1}{2} \leqslant py - qx \leqslant \dfrac{p-1}{2}\right\}$. L'ensemble E_{pq} ne contient aucun couple (x,y) pour lequel : $py - qx = 0$ car x n'est pas divisible par p. Il en découle que E_{pq} est en fait la réunion disjointe des ensembles E_p et E_q.

Nous noterons enfin σ l'involution $(x,y)\longmapsto\left(\frac{p+1}{2}-x,\frac{q+1}{2}-y\right)$ de E.

- Nous allons montrer d'abord que l'application $(x,y)\longmapsto x$ est bijective de E_p sur $R_p(q)$. Cela montrera en particulier que : $\left|E_p\right|=\left|R_p(q)\right|$. Pour une raison analogue : $\left|E_q\right|=\left|R_q(p)\right|$.
  Pour commencer, pour tout $(x,y)\in E_p$: $x\in R_p$ et $-qx\in R_p$, donc : $x\in R_p(q)$.
  Ensuite, soit $x\in\mathbb{Z}$ pour lequel : $x\in R_p(q)$. On peut choisir x de manière unique entre 1 et $\frac{p-1}{2}$. Par division euclidienne, il existe un unique $y\in\mathbb{Z}$ pour lequel : $0\leqslant py-qx\leqslant p-1$, et en fait : $1\leqslant py-qx\leqslant\frac{p-1}{2}$ car d'une part x n'est pas divisible par p, et d'autre part : $-qx\in R_p$. Dans ces conditions : $py\geqslant qx+1>0$ donc : $y\geqslant 1$, et : $py\leqslant qx+\frac{p-1}{2}\leqslant\frac{(p-1)(q+1)}{2}<\frac{p(q+1)}{2}$, donc : $y<\frac{q+1}{2}$. Finalement, q étant impair : $1\leqslant y\leqslant\frac{q-1}{2}$. Conclusion : $(x,y)\in E_p$.
- Montrons que σ stabilise E_{pq}. Or pour tout $(x,y)\in E_{pq}$:
$$p\left(\frac{q+1}{2}-y\right)-q\left(\frac{p+1}{2}-x\right)=\frac{p-1}{2}-\frac{q-1}{2}-(py-qx).$$
  L'encadrement : $-\frac{q-1}{2}\leqslant py-qx\leqslant\frac{p-1}{2}$ devient : $-\frac{q-1}{2}\leqslant\frac{p-1}{2}-\frac{q-1}{2}-(py-qx)\leqslant\frac{p-1}{2}$, donc comme voulu : $\sigma(x,y)\in E_{pq}$.
- Montrons que E_{pq} contient tous les points fixes de σ. Or σ ne possède en fait qu'un seul point fixe, à savoir : $\left(\frac{p+1}{4},\frac{q+1}{4}\right)$. Clairement : $1\leqslant\frac{p+1}{4}\leqslant\frac{p-1}{2}$ et $1\leqslant\frac{q+1}{4}\leqslant\frac{q-1}{2}$, et par ailleurs : $p\times\frac{q+1}{4}-q\times\frac{p+1}{4}=\frac{p-q}{4}$, donc : $-\frac{q-1}{2}\leqslant p\times\frac{q+1}{4}-q\times\frac{p+1}{4}\leqslant\frac{p-1}{2}$. Comme voulu : $\left(\frac{p+1}{4},\frac{q+1}{4}\right)\in E_{pq}$.
- Au point où nous en sommes, les σ-orbites de E sont toutes de cardinal 2, sauf une qui est dans E_{pq}. Conclusion : $\frac{(p-1)(q-1)}{4}=|E|\equiv\left|E_{pq}\right|\equiv\left|E_p\right|+\left|E_q\right|\equiv\left|R_p(q)\right|+\left|R_q(p)\right|$ [2], donc d'après **5** : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{|R_q(p)|}(-1)^{|R_p(q)|}=(-1)^{\frac{(p-1)(q-1)}{4}}$.
- On a représenté ci-dessous la situation géométrique dont vient de découler la loi de réciprocité quadratique dans le cas où : $p=23$ et $q=17$. Le point rouge au centre est le point fixe $\left(\frac{p+1}{4},\frac{q+1}{4}\right)$ de l'involution σ, qui n'est finalement que la symétrie centrale par rapport à ce point. Certaines orbites de cardinal 2 ont été représentés comme des segments entre deux points de même nuance de rouge. ■



3 TRANSFERT CENTRAL

D'après **3**, le transfert $V_{G\to H}$ d'un groupe G dans un sous-groupe d'indice fini H est facile à calculer quand G est abélien. Le théorème qui suit est un peu plus général. Nous le démontrerons dans le cas où : $H = \mathrm{Z}(G)$, mais H pourrait être en fait n'importe quel sous-groupe de $\mathrm{Z}(G)$.

Théorème 8 **(Transfert central)** Soit G un groupe. Si $\mathrm{Z}(G)$ est d'indice fini dans G, alors pour tout $g \in G$:

$$V_{G\to \mathrm{Z}(G)}(g) = g^{|G:\mathrm{Z}(G)|}.$$

En particulier, tout élément de $\mathrm{D}(G)$ est d'ordre un diviseur de $\big|G : \mathrm{Z}(G)\big|$.

Le fait que l'application $g \longmapsto g^{|G:\mathrm{Z}(G)|}$ soit à valeurs dans $\mathrm{Z}(G)$ découle simplement du théorème de Lagrange. Ce que le transfert ajoute ici — et c'est non trivial — c'est que pour tous $x, y \in G$: $(xy)^{|G:\mathrm{Z}(G)|} = x^{|G:\mathrm{Z}(G)|} y^{|G:\mathrm{Z}(G)|}$.

Démonstration Avec les notations du théorème **2**, pour tout $g \in G$: $V_{G\to \mathrm{Z}(G)}(g) = \prod_{1\leqslant i\leqslant r} \big(g^{n_i}\big)^{x_i}$, avec pour tout $i \in [\![1, r]\!]$: $\big(g^{n_i}\big)^{x_i} = g^{n_i}$ car : $\big(g^{n_i}\big)^{x_i} \in \mathrm{Z}(G)$. Comme voulu : $V_{G\to \mathrm{Z}(G)}(g) = \prod_{1\leqslant i\leqslant r} g^{n_i} = g^{|G:\mathrm{Z}(G)|}$.
Pour la deuxième assertion, ne pas oublier que $\mathrm{Ker}\, V_{G\to \mathrm{Z}(G)}$ contient $\mathrm{D}(G)$. ■

La deuxième assertion du théorème précédent ne permet pas d'affirmer que $\mathrm{D}(G)$ est fini. C'est pourtant le cas.

Théorème 9 **(Théorème de Schur)** Soit G un groupe. Si $\mathrm{Z}(G)$ est d'indice fini dans G, alors $\mathrm{D}(G)$ est fini.

Démonstration On pose : $n = \big|G : \mathrm{Z}(G)\big|$. On va montrer que $\mathrm{D}(G)$ est fini en montrant qu'il contient au plus n^{2n^3} éléments. On pourrait affiner très légèrement cette majoration en étant plus fin dans la preuve qui suit, mais le résultat resterait des plus grossiers.

- Pour tous $x, y \in G$, le commutateur $\big[x, y\big]$ ne dépend en réalité que des classes de x et y modulo $\mathrm{Z}(G)$. L'application $(x, y) \longmapsto \big[x, y\big]$ de $G \times G$ dans G ne peut ainsi prendre que n^2 valeurs au plus.
- Soit $d \in \mathrm{D}(G)$. Faisons l'hypothèse que d est le produit de k commutateurs avec : $k > n^3$. L'un de ces commutateurs, disons c, apparaît alors au moins n fois dans ce produit. Or pour tous $x_1, \dots, x_{n-1} \in G$: $cx_1cx_2c \dots cx_{n-1}c = c^n x_1^{c^{n-1}} x_2^{c^{n-2}} \dots x_{n-2}^{c^2} x_{n-1}^{c}$. Le produit de k termes qui définit d peut ainsi être réécrit comme un autre produit de k termes qui sont toujours des commutateurs — car tout conjugué d'un commutateur est encore un commutateur — mais dont n occurrences de c ont été regroupées. À présent, comme : $c^n = 1$ d'après **8**, d est aussi le produit de $k - n$ commutateurs. Conclusion : quitte à répéter ce procédé de simplification, on peut toujours écrire d comme un produit d'au plus n^3 commutateurs. Le sous-groupe $\mathrm{D}(G)$ contient finalement au plus $\big(n^2\big)^{n^3} = n^{2n^3}$ éléments, donc en particulier est fini. ■

On pourrait croire que le transfert central est au cœur du théorème de Schur. Il n'en est rien. Le transfert central contrôle l'ordre des éléments de $\mathrm{D}(G)$ dans les deux théorèmes qui précèdent, mais on peut démontrer le théorème de Schur sans cette information. En quelques mots, deux éléments x et y de G étant donnés, on peut montrer par récurrence que pour tout $k \in \mathbb{N}^*$: $\big[x, y\big]^k = (yx)^{-k}(xy)^k p_k$ où p_k est un produit de $k-1$ commutateurs. Le théorème de Lagrange montre par ailleurs que : $(yx)^n \in \mathrm{Z}(G)$, toujours avec : $n = \big|G : \mathrm{Z}(G)\big|$. En particulier : $(xy)^n = x(yx)^n x^{-1} = (yx)^n$, donc $\big[x, y\big]^n = p_n$ est le produit de $n-1$ commutateurs. C'est évidemment moins fort que l'égalité : $\big[x, y\big]^n = 1$ que le transfert central établit, mais on peut en tirer malgré tout la finitude de $\mathrm{D}(G)$ de la même manière que dans la preuve précédente.

4 TRANSFERT ET FUSION

D'après **3**, le transfert d'un groupe abélien G dans un sous-groupe d'indice fini H est simple à calculer, c'est seulement l'application $g \longmapsto g^{|G:H|}$. Il est en fait assez courant, en dépit sa définition complexe, que le transfert $V_{G\to H}(g)$ se ramène pour certaines valeurs de g à cette forme simple $g^{|G:H|}$, et ce n'est pas si étonnant. Comme $V_{G\to H}(g)$ mesure l'écart total qui sépare l'ensemble de représentants $\{\alpha^\theta\}_{\alpha\in G/H}$ de son produit $\{\alpha^\theta g\}_{\alpha\in G/H}$ par g, on comprend assez bien que ces écarts puissent se compenser. Dans ce cas, sans aucune rigueur : $V_{G\to H}(g) = \overline{\prod_{\alpha\in G/H}} \alpha^\theta g\big((\alpha g)^\theta\big)^{-1} = \overline{\prod_{\alpha\in G/H}} g = g^{|G:H|}$.

Le plus souvent, c'est seulement pour les éléments de H qu'on arrive à cette simplification. Reprenons ici les notations du théorème **2** mais dans le cas d'un élément h de H — et non plus g quelconque. Alors pour tout $i\in[\![1,r]\!]$: $\big(h^{n_i}\big)^{x_i}\in H$ et : $V_{G\to H}(h) = \overline{\prod_{1\leqslant i\leqslant r}} \big(h^{n_i}\big)^{x_i}$, mais comme $h\in H$, il est également vrai que pour tout $i\in[\![1,r]\!]$: $h^{n_i}\in H$. Dès lors :

$$V_{G\to H}(h) = \overline{\prod_{1\leqslant i\leqslant r}} \big(h^{n_i}\big)^{x_i} = \overline{\prod_{1\leqslant i\leqslant r}} h^{n_i}\Big(\underbrace{h^{-n_i}\big(h^{n_i}\big)^{x_i}}_{\in H}\Big) = \overline{\prod_{1\leqslant i\leqslant r}} h^{n_i} \overline{\prod_{1\leqslant i\leqslant r}} \big[h^{n_i},x_i\big] = h^{|G:H|} \overline{\prod_{1\leqslant i\leqslant r}} \big[h^{n_i},x_i\big].$$

Dans cette relation, le produit $\overline{\prod_{1\leqslant i\leqslant r}} \big[h^{n_i},x_i\big]$ mesure le défaut du transfert $V_{G\to H}(h)$ par rapport à sa valeur équilibrée $h^{|G:H|}$ dans le quotient $\dfrac{H}{\mathrm{D}(H)}$. La définition suivante du *sous-groupe focal* devrait maintenant paraître naturelle.

Rappelons qu'un sous-groupe A d'un groupe fini B est dit *de Hall dans B* si $|A|$ et $\big|B:A\big|$ sont premiers entre eux.

Définition-théorème 10 (Sous-groupe focal) Soient G un groupe fini et H un sous-groupe de G. On appelle *sous-groupe focal de H dans G*, noté $\mathrm{Foc}_G(H)$, le sous-groupe de H engendré par les commutateurs $\big[h,g\big] = h^{-1}h^g$ pour lesquels : $h\in H$, $g\in G$ et $h^g\in H$.

(i) Le sous-groupe $\mathrm{Foc}_G(H)$ est distingué dans H. Par ailleurs : $\mathrm{D}(H)\leqslant \mathrm{Foc}_G(H)\leqslant H\cap \mathrm{D}(G)$.

(ii) Pour tout $h\in H$, si on travaille modulo $\mathrm{Foc}_G(H)$: $V_{G\to H}(h)\,\mathrm{Foc}_G(H) = h^{|G:H|}\,\mathrm{Foc}_G(H)$.

(iii) Si $|H|$ est de Hall dans G, le morphisme de groupes $h\longmapsto V_{G\to H}(h)\,\mathrm{Foc}_G(H)$ est surjectif de H sur $\dfrac{H}{\mathrm{Foc}_G(H)}$ de noyau $\mathrm{Foc}_G(H)$.

Démonstration

(i) Montrons d'abord que $\mathrm{Foc}_G(H)$ est distingué dans H. Soit $x\in\mathrm{Foc}_G(H)$, disons : $x=\big[h,g\big]$ avec : $h\in H$, $g\in G$ et $h^g\in H$. Pour tout $\eta\in H$: $x^\eta = \big[h^\eta,g^\eta\big]$ avec : $h^\eta\in H$, $g^\eta\in G$ et $\big(g^\eta\big)^{-1}h^\eta g^\eta = \big(g^{-1}hg\big)^\eta\in H$, donc : $x^\eta\in\mathrm{Foc}_G(H)$.
Ensuite, pour tous $h,h'\in H$: $h^{h'}\in H$, donc : $\big[h,h'\big]\in\mathrm{Foc}_G(H)$. A fortiori : $\mathrm{D}(H)\leqslant\mathrm{Foc}_G(H)$. Il est enfin clair que : $\mathrm{Foc}_G(H)\leqslant H\cap\mathrm{D}(G)$.

(ii) On a vu plus haut, avec les notations du théorème **2**, que : $V_{G\to H}(h) = h^{|G:H|}\overline{\prod_{1\leqslant i\leqslant r}}\big[h^{n_i},x_i^{-1}\big]$ pour tout $h\in H$, et clairement : $\prod_{1\leqslant i\leqslant r}\big[h^{n_i},x_i^{-1}\big]\in\mathrm{Foc}_G(H)$ — d'où le résultat.

(iii) Notons φ le morphisme $h\longmapsto V_{G\to H}(h)\,\mathrm{Foc}_G(H)$ de H dans $\dfrac{H}{\mathrm{Foc}_G(H)}$. D'après (ii) : $\mathrm{Foc}_G(H)\leqslant\mathrm{Ker}\,\varphi$.
Ensuite, H étant de Hall dans G, d'après le théorème de Bézout : $u|H|+v\big|G:H\big|=1$ pour certains $u,v\in\mathbb{Z}$. Il en découle d'une part que : $\mathrm{Ker}\,\varphi\leqslant\mathrm{Foc}_G(H)$ car pour tout $h\in\mathrm{Ker}\,\varphi$, d'après (ii) : $h^{|G:H|}\in\mathrm{Foc}_G(H)$, donc : $h = h^{u|H|+v|G:H|} = \big(h^{|G:H|}\big)^v\in\mathrm{Foc}_G(H)$. Mais d'autre part, pour tout $h\in H$: $h\,\mathrm{Foc}_G(H) = \big(h^v\big)^{|G:H|}\,\mathrm{Foc}_G(H) = V_{G\to H}\big(h^v\big)\,\mathrm{Foc}_G(H) = \varphi\big(h^v\big)$. ■

Le sous-groupe focal de H dans G mesure la manière dont G conjugue les éléments de H. Pour tout $h\in H$, la classe de conjugaison h^H de h dans H est incluse dans la classe de conjugaison h^G de h dans G, et plus précisément : $h^H\subset h^G\cap H$, mais cette inclusion n'est pas une égalité en général. Il arrive souvent que deux éléments de H non conjugués dans H le soient dans G. Plus c'est vrai, plus $\mathrm{Foc}_G(H)$ est gros par rapport à $\mathrm{D}(H)$. Au contraire, plus G respecte les classes de conjugaison de H, plus $\mathrm{Foc}_G(H)$ est proche de $\mathrm{D}(H)$. En particulier : $\mathrm{Foc}_H(H)=\mathrm{D}(H)$.

Définition-théorème 11 **(Classes de conjugaison fusionnées)** Soient G un groupe fini et H un sous-groupe de G.

(i) Pour tous $h,h' \in H$, on dit que les classes de conjugaison h^H et h'^H de H sont *fusionnées dans G* ou *G-fusionnées* si : $h^G = h'^G$.

(ii) Soit K un sous-groupe de G contenant H. On dit que *K contrôle la G-fusion de H* si pour tous $h,h' \in H$, la G-fusion des classes h^H et h'^H implique leur K-fusion : $h^G = h'^G \implies h^K = h'^K$. Cela revient à exiger que deux éléments de H conjugués dans G le sont en fait déjà toujours dans K.

Dans ce cas : $\mathrm{Foc}_G(H) = \mathrm{Foc}_K(H)$.

(iii) Dire que H contrôle sa propre G-fusion revient à dire que pour tout $h \in H$: $h^G \cap H = h^H$.

Dans ce cas : $\mathrm{Foc}_G(H) = \mathrm{D}(H)$ et pour tout $h \in H$: $V_{G\to H}(h) = h^{|G:H|}\,\mathrm{D}(H)$.

Démonstration

(ii) Clairement : $\mathrm{Foc}_K(H) \leqslant \mathrm{Foc}_G(H)$. Inversement, soient $h \in H$ et $g \in G$ pour lesquels : $h^g \in H$. Aussitôt : $\left(h^g\right)^G = h^G$, donc comme K contrôle la G-fusion de H : $\left(h^g\right)^K = h^K$, autrement dit : $h^g = h^k$ pour un certain $k \in K$. A fortiori : $\left[h,g\right] = h^{-1}h^g = h^{-1}h^k = \left[h,k\right] \in \mathrm{Foc}_K(H)$.

(iii) Si pour tout $h \in H$: $h^G \cap H = h^H$, alors clairement : $h^G = h'^G \implies h^H = h'^H$.

Supposons réciproquement que H contrôle sa propre G-fusion. Soit $h \in H$. Il est alors toujours vrai que : $h^H \subset h^G \cap H$. Ensuite, soit $h' \in h^G \cap H$. En particulier : $h^G = h'^G$, donc par hypothèse : $h^H = h'^H$, donc en particulier : $h' \in h^H$. Conclusion : $h^G \cap H = h^H$.

À présent, d'après (ii), si H contrôle sa propre G-fusion : $\mathrm{Foc}_G(H) = \mathrm{Foc}_H(H) = \mathrm{D}(H)$. Les autres points ont été démontrés dans le théorème **10**. ■

Ce fut un peu long, mais nous pouvons enfin comprendre à grands traits la manière dont le transfert est le plus souvent utilisé. Un groupe fini G et un sous-groupe H de G étant donnés, faisons l'hypothèse que : $\mathrm{Foc}_G(H) \neq H$ et que H est de Hall dans G. Le morphisme de groupes $g \overset{\varphi}{\longmapsto} V_{G\to H}(g)\,\mathrm{Foc}_G(H)$ est alors surjectif de G sur $\dfrac{H}{\mathrm{Foc}_G(H)}$ car sa restriction à H l'est. Les quotients $\dfrac{G}{\mathrm{Ker}\,\varphi}$ et $\dfrac{H}{\mathrm{Foc}_G(H)}$ se trouvent ainsi isomorphes, et comme le deuxième est non trivial par hypothèse, il en découle que G n'est pas simple.

5 Introduction à l'analyse p-locale

5.1 Transfert dans un p-Sylow

Nous avons vu dans le théorème **10**, où l'on étudie le transfert d'un groupe fini G dans un sous-groupe H, l'importance que peut revêtir le fait que H soit de Hall dans G. Les sous-groupes de Sylow constituent bien sûr le premier exemple naturel de sous-groupes de Hall, avec deux avantages majeurs — ils existent universellement d'une part, ils ne sont pas parfaits d'autre part, i.e. pas égaux à leur sous-groupe dérivé.

Deux sous-groupes vont apparaître beaucoup dans ce paragraphe, que nous introduisons ci-dessous.

Définition-théorème 12 **(Sous-groupes $\mathrm{O}^p(G)$ et $\mathrm{A}^p(G)$)** Soient G un groupe fini et p un nombre premier.

(i) On note $\mathrm{O}^p(G)$ l'intersection des sous-groupes distingués N de G pour lesquels $\dfrac{G}{N}$ est un p-groupe. Il est équivalent de dire que $\mathrm{O}^p(G)$ est le plus petit sous-groupe distingué de G par le quotient duquel on obtient un p-groupe, car pour tous sous-groupes distingués A et B de G, si $\dfrac{G}{A}$ et $\dfrac{G}{B}$ sont des p-groupes, $\dfrac{G}{A\cap B}$ est lui aussi un p-groupe.

Pour tout $P \in \mathrm{Syl}_p(G)$: $G = \mathrm{O}^p(G)P$.

(ii) On note $\mathrm{A}^p(G)$ l'intersection des sous-groupes distingués N de G pour lesquels $\dfrac{G}{N}$ est un p-groupe abélien.

Pour tout $P \in \mathrm{Syl}_p(G)$: $G = \mathrm{A}^p(G)P$ et $\mathrm{A}^p(G) = \mathrm{O}^p(G)\mathrm{D}(G) = \mathrm{O}^p(G)\mathrm{D}(P)$.

Par ailleurs, si les p-Sylow de G sont abéliens : $\mathrm{A}^p(G) = \mathrm{O}^p(G)$.

Démonstration

(i) Le morphisme de groupes $g \longmapsto (Ag, Bg)$ de G dans le p-groupe $\dfrac{G}{A} \times \dfrac{G}{B}$ induit un morphisme injectif de $\dfrac{G}{A \cap B}$ dans $\dfrac{G}{A} \times \dfrac{G}{B}$.
Ensuite, pour tout $P \in \mathrm{Syl}_p(G)$: $G = \mathrm{O}^p(G)P$ car $\mathrm{O}^p(G)P$ est d'ordre divisible par $\big|G : P\big|$ par définition de $\mathrm{O}^p(G)$, ainsi que par $|P|$, donc par $|G|$.

(ii) Un sous-groupe distingué de G par le quotient duquel on obtient un p-groupe abélien contient toujours $\mathrm{O}^p(G)\mathrm{D}(G)$, lequel est lui-même un sous-groupe distingué de G par le quotient duquel on obtient un p-groupe abélien. Conclusion : $\mathrm{A}^p(G) = \mathrm{O}^p(G)\mathrm{D}(G)$. Ensuite, $\mathrm{O}^p(G)\mathrm{D}(P)$ est un sous-groupe distingué de $\mathrm{O}^p(G)P = G$ par le quotient duquel on obtient un p-groupe abélien, donc : $\mathrm{A}^p(G) \leqslant \mathrm{O}^p(G)\mathrm{D}(P)$. Inversement : $\mathrm{O}^p(G)\mathrm{D}(P) \leqslant \mathrm{O}^p(G)\mathrm{D}(G) = \mathrm{A}^p(G)$, donc comme voulu : $\mathrm{A}^p(G) = \mathrm{O}^p(G)\mathrm{D}(P)$. ■

Théorème 13 **(Noyau du transfert dans un p-Sylow)** Soient G un groupe fini, p un nombre premier et $P \in \mathrm{Syl}_p(G)$.

(i) $P \cap \mathrm{Ker}\, V_{G\to P} = \mathrm{Foc}_G(P) = P \cap \mathrm{D}(G) = P \cap \mathrm{A}^p(G)$.

(ii) $\mathrm{Ker}\, V_{G\to P} = \mathrm{A}^p(G)$.

Démonstration

(i) D'après **10** (i) et (iii), P étant de Hall dans G : $P \cap \mathrm{Ker}\, V_{G\to P} = \mathrm{Foc}_G(P) \leqslant P \cap \mathrm{D}(G)$. Ensuite, $\dfrac{G}{\mathrm{Ker}\, V_{G\to P}}$ est isomorphe à un sous-groupe du p-groupe abélien $\dfrac{P}{\mathrm{D}(P)}$, donc : $\mathrm{A}^p(G) \leqslant \mathrm{Ker}\, V_{G\to P}$. Finalement : $P \cap \mathrm{D}(G) \leqslant P \cap \mathrm{A}^p(G) \leqslant P \cap \mathrm{Ker}\, V_{G\to P} = \mathrm{Foc}_G(P) \leqslant P \cap \mathrm{D}(G)$.

(ii) L'inclusion : $\mathrm{A}^p(G) \leqslant \mathrm{Ker}\, V_{G\to P}$ et l'égalité : $G = \mathrm{A}^p(G)P$ montrent que :

$$\mathrm{Ker}\, V_{G\to P} = \mathrm{A}^p(G)\big(P \cap \mathrm{Ker}\, V_{G\to P}\big) \overset{\text{(i)}}{=} \mathrm{A}^p(G)\big(P \cap \mathrm{D}(G)\big) = \mathrm{A}^p(G).$$ ■

Théorème 14 **(Contrôle de fusion d'un p-Sylow et quotient $\dfrac{G}{\mathrm{A}^p(G)}$)** Soient G un groupe fini, p un nombre premier, $P \in \mathrm{Syl}_p(G)$ et H un sous-groupe de G contenant P. Si H contrôle la G-fusion de P, alors : $H \cap \mathrm{A}^p(G) = \mathrm{A}^p(H)$ et les groupes $\dfrac{H}{\mathrm{A}^p(H)}$ et $\dfrac{G}{\mathrm{A}^p(G)}$ sont isomorphes.

Ce théorème n'a bien sûr d'intérêt que si on est capable de trouver explicitement des sous-groupes qui contrôlent la fusion d'un p-Sylow. Nous étudierons notamment, plus loin, le cas d'un p-Sylow abélien.

L'hypothèse selon laquelle H contrôle la G-fusion de P porte une information sur la manière dont H est plongé dans G, mais le quotient $\dfrac{H}{\mathrm{A}^p(H)}$, à la différence d'un quotient comme $\dfrac{H}{\mathrm{Foc}_G(H)}$, ne dépend quant à lui que de H.

Démonstration Nous avons déjà vu que : $H = \mathrm{A}^p(H)P$ et $G = \mathrm{A}^p(G)P$. En outre, d'après **11** et **13** : $P \cap \mathrm{A}^p(G) = \mathrm{Foc}_G(P) = \mathrm{Foc}_H(P) = P \cap \mathrm{A}^p(H)$. Ainsi :

$$\big|G : \mathrm{A}^p(G)\big| = \big|\mathrm{A}^p(G)P : \mathrm{A}^p(G)\big| = \big|P : P \cap \mathrm{A}^p(G)\big| = \big|P : P \cap \mathrm{A}^p(H)\big| = \big|\mathrm{A}^p(H)P : \mathrm{A}^p(H)\big| = \big|H : \mathrm{A}^p(H)\big|.$$

De même : $G = \mathrm{A}^p(G)H$ car H contient P, donc : $\big|G : \mathrm{A}^p(G)\big| = \big|\mathrm{A}^p(G)H : \mathrm{A}^p(G)\big| = \big|H : H \cap \mathrm{A}^p(G)\big|$. En résumé : $\big|\mathrm{A}^p(H)\big| = \big|H \cap \mathrm{A}^p(G)\big|$ et $\big|G : \mathrm{A}^p(G)\big| = \big|H : \mathrm{A}^p(H)\big|$.
Remarquons à présent que $\dfrac{H}{H \cap \mathrm{A}^p(G)}$ est un p-groupe abélien. Il en découle que : $\mathrm{A}^p(H) \leqslant H \cap \mathrm{A}^p(G)$, et même mieux : $\mathrm{A}^p(H) = H \cap \mathrm{A}^p(G)$ pour une raison de cardinal. Le morphisme de groupes $h \longmapsto \mathrm{A}^p(G)\,h$ de H dans $\dfrac{G}{\mathrm{A}^p(G)}$ a ainsi pour noyau $H \cap \mathrm{A}^p(G) = \mathrm{A}^p(H)$. Il induit donc un morphisme injectif de $\dfrac{H}{\mathrm{A}^p(H)}$ dans $\dfrac{G}{\mathrm{A}^p(G)}$, qui est en fait bijectif pour une raison de cardinal. ■

5.2 p-NILPOTENCE ET FUSION

La première application classique du transfert dans un p-Sylow concerne un concept que nous n'avons pas encore introduit — celui de *p-nilpotence*. Rappelons que pour tout nombre premier p, un groupe fini est appelé un *p'-groupe* si son ordre est premier à p.

Définition-théorème 15 **(Sous-groupe $O_{p'}(G)$ et p-nilpotence)** Soient G un groupe fini et p un nombre premier.

(i) On note $O_{p'}(G)$ le sous-groupe engendré par tous les p'-sous-groupes distingués de G. Il est équivalent de dire que $O_{p'}(G)$ est le plus grand p'-sous-groupe distingué de G, car pour tous p'-sous-groupes distingués A et B de G, AB est aussi un p'-sous-groupe distingué de G.

Il est toujours vrai que : $O_{p'}(G) \leqslant O^p(G)$.

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

1) $O^p(G) = O_{p'}(G)$.

2) $G = O_{p'}(G)P$. En d'autres termes, $O_{p'}(G)$ est un complément distingué de P dans G.

On dit dans ce cas que G est *p-nilpotent*.

(iii) Si G est p-nilpotent, ses sous-groupes le sont tous également.

Démonstration

(i) Le sous-groupe AB a pour ordre : $|AB| = \dfrac{|A| \times |B|}{|A \cap B|}$, donc en effet c'est un p'-groupe.

Ensuite, $\dfrac{G}{O^p(G)}$ est un p-groupe, donc $\dfrac{O^p(G)O_{p'}(G)}{O^p(G)}$ aussi. Or $\dfrac{O^p(G)O_{p'}(G)}{O^p(G)}$ est aussi un p'-groupe car : $\left|O^p(G)O_{p'}(G) : O^p(G)\right| = \left|O_{p'}(G) : O_{p'}(G) \cap O^p(G)\right|$. Conclusion : $O^p(G)O_{p'}(G) = O^p(G)$, i.e. : $O_{p'}(G) \leqslant O^p(G)$.

(ii) De 1) vers 2), il est toujours vrai que : $G = O^p(G)P$, donc ici : $G = O_{p'}(G)P$.

De 2) vers 1), $\dfrac{G}{O_{p'}(G)}$ est un p-groupe, donc : $O^p(G) \leqslant O_{p'}(G)$, et il est toujours vrai d'après (i) que : $O_{p'}(G) \leqslant O^p(G)$.

(iii) Soit H un sous-groupe de G. Il est toujours vrai que : $O_{p'}(H) \leqslant O^p(H)$. Inversement, $H \cap O_{p'}(G)$ est un p'-sous-groupe distingué de H, donc : $H \cap O_{p'}(G) \leqslant O_{p'}(H)$, et $\dfrac{H}{H \cap O^p(G)}$ est isomorphe à un sous-groupe du p-groupe $\dfrac{G}{O^p(G)}$, donc : $O^p(H) \leqslant H \cap O^p(G)$. Finalement, G étant p-nilpotent : $O^p(H) \leqslant H \cap O^p(G) = H \cap O_{p'}(G) \leqslant O_{p'}(H)$. ■

Le résultat qui suit, intéressant en soi malgré tout, ne sera pour nous qu'un lemme.

Théorème 16 **(Commutateurs dans un p-groupe fini)** Soient p un nombre premier, G un p-groupe fini et H un sous-groupe non trivial distingué de G. Dans ces conditions : $\big[H, G\big] \leqslant H$ avec inclusion stricte.

Démonstration Pour commencer, pour tous $h \in H$ et $g \in G$, H étant distingué dans G : $\big[h, g\big] = h^{-1}h^g \in H$, donc : $\big[H, G\big] \leqslant H$.

Pour l'inclusion stricte, raisonnons par récurrence sur $|G|$ en supposant le résultat vrai de tout groupe d'ordre strictement inférieur satisfaisant les mêmes hypothèses que G. Par hypothèse : $H \neq 1$ donc : $G \neq 1$, donc comme G est un p-groupe : $Z(G) \neq 1$. Nous noterons alors d'une barre les quotients dans $\dfrac{G}{Z(G)}$. Si : $\overline{H} = 1$, alors : $H \leqslant Z(G)$ donc : $\big[H, G\big] = 1 < H$. Si au contraire : $\overline{H} \neq 1$, alors par hypothèse de récurrence, l'inclusion : $\big[\overline{H}, \overline{G}\big] \leqslant \overline{H}$ est stricte, donc aussi l'inclusion : $\big[H, G\big] \leqslant H$ car : $\big[\overline{H}, \overline{G}\big] = \overline{\big[H, G\big]}$. ■

Théorème 17 **(p-nilpotence et auto-fusion)** Soient G un groupe fini, p un nombre premier et $P \in \mathrm{Syl}_p(G)$. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.

2) P contrôle sa propre G-fusion.

Démonstration

1) $\Longrightarrow$ 2) Soient $x \in P$ et $g \in G$ pour lesquels : $x^g \in P$. Par hypothèse : $G = \mathrm{O}_{p'}(G)P$, donc : $g = \omega u$ pour certains $\omega \in \mathrm{O}_{p'}(G)$ et $u \in P$. Il en découle que : $x^\omega = \left(x^g\right)^{u^{-1}} \in P$, mais du coup : $\left[\omega, x\right] = \left(x^\omega\right)^{-1} x = \omega^{-1}\omega^x \in P \cap \mathrm{O}_{p'}(G) = 1$, de sorte que ω et x commutent. On en déduit que : $x^g = \left(x^\omega\right)^u = x^u \in x^P$, ce qui montre bien que G contrôle sa propre G-fusion.

2) $\Longrightarrow$ 1) Tout d'abord : $P \cap \mathrm{O}^p(G) \in \mathrm{Syl}_p\left(\mathrm{O}^p(G)\right)$ car : $\left|\mathrm{O}^p(G) : P \cap \mathrm{O}^p(G)\right| = \left|\mathrm{O}^p(G)P : P\right| = \left|G : P\right|$. Pour montrer que G est p-nilpotent, nous allons ainsi montrer que : $P \cap \mathrm{O}^p(G) = 1$.

Ensuite, parce qu'il est caractéristique dans $\mathrm{O}^p(G)$, $\mathrm{A}^p\left(\mathrm{O}^p(G)\right)$ est un sous-groupe distingué de G par le quotient duquel on obtient un p-groupe. Cela suffit à montrer que : $\mathrm{A}^p\left(\mathrm{O}^p(G)\right) = \mathrm{O}^p(G)$, puis d'après **13**, que : $\mathrm{Foc}_{\mathrm{O}^p(G)}\left(P \cap \mathrm{O}^p(G)\right) = \left(P \cap \mathrm{O}^p(G)\right) \cap \mathrm{A}^p\left(\mathrm{O}^p(G)\right) = P \cap \mathrm{O}^p(G)$.

Soient $x \in P \cap \mathrm{O}^p(G)$ et $g \in G$ pour lesquels : $x^g \in P \cap \mathrm{O}^p(G)$. Comme P contrôle sa propre G-fusion : $x^g = x^u$ pour un certain $u \in P$, donc : $\left[x, g\right] = x^{-1}x^g = x^{-1}x^u = \left[x, u\right] \in \left[P \cap \mathrm{O}^p(G), P\right]$. Conclusion : $P \cap \mathrm{O}^p(G) = \mathrm{Foc}_{\mathrm{O}^p(G)}\left(P \cap \mathrm{O}^p(G)\right) \leqslant \left[P \cap \mathrm{O}^p(G), P\right]$, ce que contredit **16**. ■

5.3 Transfert dans un p-Sylow abélien

Théorème 18 **(Contrôle de fusion d'un p-Sylow abélien)** Soient G un groupe fini, p un nombre premier et $P \in \mathrm{Syl}_p(G)$. Si P est abélien, $\mathrm{N}_G(P)$ contrôle la G-fusion de P.

Démonstration Soient $x \in P$ et $g \in G$ pour lesquels : $x^g \in P$. Il s'agit de montrer que : $x^g = x^n$ pour un certain $n \in \mathrm{N}_G(P)$. Or : $x^g \in P^g$, donc P étant abélien : $P^g \leqslant \mathrm{C}_G\left(x^g\right)$ et $P^g \leqslant \mathrm{C}_G\left(x^g\right)$. D'après les théorèmes des Sylow, les p-Sylow P et P^g sont ainsi conjugués dans $\mathrm{C}_G\left(x^g\right)$, donc : $P^g = P^d$ pour un certain $d \in \mathrm{C}_G\left(x^g\right)$, ou encore : $P^{gd^{-1}} = P$, i.e. : $gd^{-1} \in \mathrm{N}_G(P)$. Posons : $n = gd^{-1}$. Comme voulu : $x^g = \left(x^g\right)^{d^{-1}} = x^n$ avec $n \in \mathrm{N}_G(P)$. ■

Le *théorème de p-nilpotence de Burnside*, établi en 1900 deux ans avant la naissance officielle du transfert, collecte et relie une bonne partie des résultats que nous avons démontrés à ce stade. Il caractérise efficacement la p-nilpotence d'un groupe fini, mais dans le seul cas où ses p-Sylow sont abéliens.

Théorème 19 **(Théorème de p-nilpotence de Burnside)** Soient G un groupe fini, p un nombre premier et $P \in \mathrm{Syl}_p(G)$. On suppose P abélien. Les assertions suivantes sont alors équivalentes :

1) G est p-nilpotent.

2) $\mathrm{N}_G(P)$ est p-nilpotent.

3) $P \leqslant \mathrm{Z}\left(\mathrm{N}_G(P)\right)$, ou encore : $\mathrm{N}_G(P) = \mathrm{C}_G(P)$ — ce qui implique que P est abélien.

En pratique, ce qui compte, c'est que si : $\mathrm{N}_G(P) = \mathrm{C}_G(P)$, ou encore : $P \leqslant \mathrm{Z}\left(\mathrm{N}_G(P)\right)$, alors G est p-nilpotent.

Démonstration Tout d'abord, P étant abélien : $\mathrm{A}^p(G) = \mathrm{O}^p(G)$ et $\mathrm{A}^p\big(\mathrm{N}_G(P)\big) = \mathrm{O}^p\big(\mathrm{N}_G(P)\big)$.

1) $\Longrightarrow$ 2) Simple conséquence de **15** (iii).

2) $\Longrightarrow$ 3) Si $\mathrm{N}_G(P)$ est p-nilpotent : $\mathrm{N}_G(P) = \mathrm{O}_{p'}\big(\mathrm{N}_G(P)\big)P$. Or P et $\mathrm{O}_{p'}\big(\mathrm{N}_G(P)\big)$ sont à la fois distingués dans $\mathrm{N}_G(P)$ et d'ordres premiers entre eux, donc pour tous $x \in P$ et $y \in \mathrm{O}_{p'}\big(\mathrm{N}_G(P)\big)$:

$$\big[x,y\big] = x^{-1}x^y = \big(y^x\big)^{-1}y \in P \cap \mathrm{O}_{p'}\big(\mathrm{N}_G(P)\big) = 1,$$

autrement dit P et $\mathrm{O}_{p'}\big(\mathrm{N}_G(P)\big)$ commutent. Abélien, P est donc centralisé à la fois par $\mathrm{O}_{p'}\big(\mathrm{N}_G(P)\big)$ et par lui-même. Conclusion : $P \leqslant \mathrm{Z}\big(\mathrm{N}_G(P)\big)$.

3) $\Longrightarrow$ 1) Il nous suffit de montrer que P contrôle sa propre G-fusion d'après **17**. Soient $x \in P$ et $g \in G$ pour lesquels : $x^g \in P$. Comme P est abélien, $\mathrm{N}_G(P)$ contrôle la G-fusion de P d'après **18**, donc : $x^g = x^n$ pour un certain $n \in \mathrm{N}_G(P)$. Or : $x \in P \leqslant \mathrm{Z}\big(\mathrm{N}_G(P)\big)$, donc : $x^g = x^n = x \in x^P$. ■

Exemple Aucun groupe d'ordre 252 n'est simple.

Démonstration Intéressons-nous par l'absurde à un groupe simple G d'ordre $252 = 2^2 \times 3^2 \times 7$. Les théorèmes de Sylow ne nous fournissent hélas aucune contradiction à eux seuls, mais parce qu'il est simple, ils imposent tout de même à G de posséder exactement 36 7-Sylow. Soit $S \in \mathrm{Syl}_7(G)$. Il est bien connu qu'alors : $\big|G : \mathrm{N}_G(S)\big| = 36$, donc ici : $\mathrm{N}_G(S) = S$. Or S est d'ordre 7 donc abélien, donc : $S \leqslant \mathrm{Z}\big(\mathrm{N}_G(S)\big)$. D'après le théorème de p-nilpotence de Burnside, G s'avère ainsi 7-nilpotent, ce qui contredit sa simplicité.

Théorème 20 (Corollaire cyclique du théorème de p-nilpotence de Burnside) Soit G un groupe fini. On note p le plus petit diviseur premier de $|G|$. Si les p-Sylow de G sont cycliques, G est p-nilpotent.

Démonstration Soit P un p-Sylow de G. D'après le théorème de p-nilpotence de Burnside, il nous suffit de montrer l'égalité : $\mathrm{N}_G(P) = \mathrm{C}_G(P)$, i.e. : $\big|\mathrm{N}_G(P) : \mathrm{C}_G(P)\big| = 1$. Or l'action par conjugaison de $\mathrm{N}_G(P)$ sur P a pour noyau $\mathrm{C}_G(P)$ et plonge le quotient $\dfrac{\mathrm{N}_G(P)}{\mathrm{C}_G(P)}$ dans le groupe $\mathrm{Aut}(P)$. En particulier, $\big|\mathrm{N}_G(P) : \mathrm{C}_G(P)\big|$ divise $\big|\mathrm{Aut}(P)\big|$. Le résultat découle ainsi des trois remarques qui suivent.

— Pour commencer, P étant cyclique, disons d'ordre p^n : $\big|\mathrm{Aut}(P)\big| = p^{n-1}(p-1)$.

— Ensuite, $\mathrm{C}_G(P)$ contient P car P est abélien, donc $\big|\mathrm{N}_G(P) : \mathrm{C}_G(P)\big|$ est premier à p.

— Pour finir, p étant le plus petit diviseur premier de $|G|$, $\big|\mathrm{N}_G(P) : \mathrm{C}_G(P)\big|$ est premier à $p-1$. ■

En particulier, tout groupe fini dont l'ordre est divisible par 2 mais pas par 4 est 2-nilpotent — donc n'est pas simple à moins d'être abélien. On pourrait tirer du théorème de p-nilpotence de Burnside un résultat plus fort, à savoir que l'ordre d'un groupe fini simple non abélien d'ordre pair est divisible par 8 ou 12, mais nous obtiendrons mieux au prochain paragraphe, alors patience.

Rappelons en vue de l'exemple qui suit qu'un groupe G est résoluble si : $\mathrm{D}^n(G) = 1$ pour un certain $n \in \mathbb{N}$, où l'on a posé : $\mathrm{D}^0(G) = G$ et pour tout $k \in \mathbb{N}$: $\mathrm{D}^{k+1}(G) = \mathrm{D}\big(\mathrm{D}^k(G)\big)$. Il est équivalent de dire que G possède une suite de sous-groupes $G_0, \dots, G_n$ pour lesquels : $1 = G_0 \leqslant G_1 \leqslant \dots \leqslant G_n = G$ et tels que pour tout $i \in [\![0, n-1]\!]$, G_i est distingué dans G_{i+1} et le quotient $\dfrac{G_{i+1}}{G_i}$ est abélien. Pour tout nombre premier p, en particulier, tout p-groupe est résoluble.

Exemple Tout groupe fini dont tous les sous-groupes de Sylow sont cycliques est résoluble.

En particulier, pour tous nombres premiers distincts $p_1, \dots, p_n$, tout groupe d'ordre $p_1 \dots p_n$ est résoluble.

Démonstration Soit G un groupe fini dont tous les sous-groupes de Sylow sont cycliques. On raisonne par récurrence en supposant le résultat vrai de tout groupe d'ordre strictement inférieur à $|G|$ satisfaisant les mêmes hypothèses que G. On peut supposer G non trivial et noter p le plus petit diviseur premier de G. D'après **20**, G est p-nilpotent, mais $\mathrm{O}^p(G)$ n'a lui aussi que des sous-groupes de Sylow cycliques, donc il est résoluble par hypothèse de récurrence. Comme $\dfrac{G}{\mathrm{O}^p(G)}$ est résoluble en tant que p-groupe, G l'est à son tour par empilement.

Le théorème de p-nilpotence de Burnside étudie spécifiquement le cas d'un p-Sylow P d'un groupe fini G pour lequel : $P \leqslant \mathrm{Z}\big(\mathrm{N}_G(P)\big)$. Que se passe-t-il, toujours sous l'hypothèse que P est abélien, si on ne suppose plus que P est totalement inclus dans $\mathrm{Z}\big(\mathrm{N}_G(P)\big)$? Que dire du sous-groupe : $P \cap \mathrm{Z}\big(\mathrm{N}_G(P)\big) = \mathrm{C}_P\big(\mathrm{N}_G(P)\big)$?

Théorème 21 **(Transfert dans un p-Sylow abélien)** Soient G un groupe fini, p un nombre premier et $P \in \mathrm{Syl}_p(G)$. Si P est abélien : $\mathrm{D}(G) \cap \mathrm{C}_P\big(\mathrm{N}_G(P)\big) = 1$. En particulier, si G est simple non abélien : $\mathrm{C}_P\big(\mathrm{N}_G(P)\big) = 1$.

Démonstration Soit $g \in \mathrm{D}(G) \cap \mathrm{C}_P\big(\mathrm{N}_G(P)\big)$. Avec les notations du théorème **2** : $V_{G\to P}(g) = \prod_{1\leqslant i\leqslant r} \big(g^{n_i}\big)^{x_i}$ avec pour tout $i \in [\![1,r]\!]$: $\big(g^{n_i}\big)^{x_i} \in P$.

- Comme : $\mathrm{D}(G) \leqslant \mathrm{Ker}\, V_{G\to P}$, alors : $V_{G\to P}(g) = 1$.
- Ensuite, P étant abélien, $\mathrm{N}_G(P)$ contrôle la G-fusion de P d'après **18**. Pour tout $i \in [\![1,r]\!]$, les éléments g^{n_i} et $\big(g^{n_i}\big)^{x_i}$ de P sont donc conjugués dans $\mathrm{N}_G(P)$, mais comme : $g \in \mathrm{C}_P\big(\mathrm{N}_G(P)\big)$, cela montre tout simplement que : $\big(g^{n_i}\big)^{x_i} = g^{n_i}$.

Conclusion : $1 = \prod_{1\leqslant i\leqslant r} g^{n_i} = g^{|G:P|}$, mais comme $\big|G:P\big|$ est premier à p : $g = 1$. ■

En guise de corollaire, le résultat suivant généralise le corollaire cyclique **20** du théorème de p-nilpotence de Burnside.

Théorème 22 **(Exemples de p-Sylow abéliens qui empêchent la simplicité)** Soit G un groupe fini. On note p le plus petit diviseur premier de $|G|$ et on suppose que les p-Sylow de G sont le produit de groupes cycliques dont l'un d'ordre strictement supérieur aux autres. Alors : $\mathrm{O}^p(G) \neq G$, donc en particulier n'est pas simple.

Les 2-Sylow d'un groupe fini simple ne peuvent donc pas être isomorphes aux groupes : $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$, etc.

Démonstration Soit $P \in \mathrm{Syl}_p(G)$. Par hypothèse : $P = \langle c\rangle \times A$ où c est d'ordre p^γ et où A est abélien avec pour tout $a \in A$: $a^{p^{\gamma-1}} = 1$. Aussitôt : $\big\langle c^{p^{\gamma-1}}\big\rangle = \big\{x^{p^{\gamma-1}}\big\}_{x\in P}$, donc $\big\langle c^{p^{\gamma-1}}\big\rangle$ est stable par conjugaison par tout élément de $\mathrm{N}_G(P)$. Or ce sous-groupe est d'ordre p, donc $\Big|\mathrm{N}_G\big(\big\langle c^{p^{\gamma-1}}\big\rangle\big) : \mathrm{C}_G\big(\big\langle c^{p^{\gamma-1}}\big\rangle\Big|$ divise $p-1$, donc par définition de p : $\mathrm{N}_G\big(\big\langle c^{p^{\gamma-1}}\big\rangle\big) = \mathrm{C}_G\big(\big\langle c^{p^{\gamma-1}}\big\rangle\big)$. Conclusion : $\mathrm{N}_G(P)$ centralise $c^{p^{\gamma-1}}$, autrement dit : $c^{p^{\gamma-1}} \in \mathrm{C}_P\big(\mathrm{N}_G(P)\big)$. Le théorème **21** montre alors que : $c^{p^{\gamma-1}} \notin \mathrm{D}(G)$, donc en effet : $\mathrm{O}^p(G) \neq G$. ■

5.4 Le théorème de p-nilpotence de Frobenius

Le théorème de p-nilpotence de Burnside a beau être riche en applications, l'hypothèse d'un p-Sylow abélien sur laquelle il repose n'en demeure pas moins une restriction majeure. Un théorème analogue est-il envisageable dans le cas général ? La réponse est oui, mais il faut pour appréhender cette généralisation bien comprendre en quoi le théorème de p-nilpotence de Burnside est surprenant. En pratique, ce sont l'hypothèse : $P \leqslant \mathrm{Z}\big(\mathrm{N}_G(P)\big)$ et sa sœur : $\mathrm{N}_G(P) = \mathrm{C}_G(P)$ que l'on vérifie quand on veut utiliser le théorème, mais ces hypothèses masquent l'essentiel. Ce qui est fort dans le cas où P est abélien, c'est que la p-nilpotence du sous-groupe $\mathrm{N}_G(P)$ implique celle du groupe G tout entier. On mesure ici l'importance du transfert dans un p-Sylow, qui rend finalement globale une information a priori locale. Frobenius a découvert un analogue non abélien du théorème de Burnside, qui est l'objet de ce paragraphe.

Définition **(Sous-groupe p-local)** Soient G un groupe fini et p un nombre premier. 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.

Théorème 23 **(Théorème de p-nilpotence de Frobenius)** Soient G un groupe fini et p un nombre premier. Les assertions suivantes sont équivalentes :

1) G est p-nilpotent.
2) Tout sous-groupe p-local de G est p-nilpotent.
3) Le quotient $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ est un p-groupe pour tout p-sous-groupe H de G.

Le théorème de Frobenius ne généralise pas à proprement parler celui de Burnside, car on y demande à tout sous-groupe p-local d'être p-nilpotent, et non plus à un seul. Le principe des deux théorèmes est néanmoins le même, une information p-locale est convertie en une information globale.

Démonstration

1) $\Longrightarrow$ 2) Simple conséquence du théorème **15** (iii).

2) $\Longrightarrow$ 3) Si H est trivial : $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)} = 1$. Dans le cas contraire, $\mathrm{N}_G(H)$ est un sous-groupe p-local, donc est p-nilpotent, autrement dit : $\mathrm{N}_G(H) = \mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big)(H \cap P)$ pour un certain $P \in \mathrm{Syl}_p(G)$ pour lequel : $H \cap P \in \mathrm{Syl}_p\big(\mathrm{N}_G(H)\big)$. Or H et $\mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big)$ sont d'ordres premiers entre eux, donc : $H \cap \mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big) = 1$, et ils distingués dans $\mathrm{N}_G(H)$, donc pour tous $h \in H$ et $g \in \mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big)$:

$$\big[h, g\big] = h^{-1}h^g = \big(g^h\big)^{-1} g \in H \cap \mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big) = 1,$$

autrement dit H et $\mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big)$ commutent. Conclusion : $\mathrm{O}^p\big(\mathrm{N}_G(H)\big) = \mathrm{O}_{p'}\big(\mathrm{N}_G(H)\big) \leqslant \mathrm{C}_G(H)$, donc $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ est un p-groupe.

3) $\Longrightarrow$ 1) C'est l'implication difficile du théorème, à laquelle nous allons maintenant nous attaquer. ■

Pour préparer le terrain, fixons $P \in \mathrm{Syl}_p(G)$. D'après **17**, G est p-nilpotent si et seulement si P contrôle sa propre G-fusion, mais quel lien cela a-t-il avec le fait que le quotient $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ soit un p-groupe pour tout p-sous-groupe H ? Donnons-nous pour le comprendre des éléments $x \in P$ et $g \in G$ pour lesquels : $x^g \in P$, ou encore : $x \in P \cap P^{g^{-1}}$. De quelle manière les quotients $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ peuvent-ils forcer l'appartenance : $x^g \in x^P$?

Commençons par la situation simple où : $g \in \mathrm{N}_G(P)$ et où le seul quotient $\dfrac{\mathrm{N}_G(P)}{\mathrm{C}_G(P)}$ est un p-groupe. Dans ce cas, P étant un p-Sylow de $\mathrm{N}_G(P)$: $\mathrm{N}_G(P) = \mathrm{C}_G(P)P$, donc : $g = cy$ pour certains $c \in \mathrm{C}_G(P)$ et $y \in P$. Aussitôt : $x^g = \big(x^c\big)^y = x^y \in x^P$ comme voulu.

Dans un deuxième temps, il est facile de remplacer l'hypothèse précédente : $g \in \mathrm{N}_G(P)$ par l'hypothèse assouplie : $g \in \mathrm{C}_G\big(P \cap P^{g^{-1}}\big)\mathrm{N}_G(P)$, car de toute façon : $x \in P \cap P^{g^{-1}}$. Il est équivalent d'exiger l'égalité : $P^g = P^c$ pour un certain $c \in \mathrm{C}_G\big(P \cap P^g\big)$. En résumé, si d'une part P et P^g sont conjugués par un élément de $\mathrm{C}_G\big(P \cap P^g\big)$ et si d'autre part le quotient $\dfrac{\mathrm{N}_G(P)}{\mathrm{C}_G(P)}$ est un p-groupe, alors : $x^g \in x^P$. Il nous suffit dès lors pour atteindre le théorème de Frobenius de démontrer le résultat suivant.

Théorème 24 **(Un lemme pour le théorème de Frobenius)** Soient G un groupe fini et p un nombre premier. Si le quotient $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ est un p-groupe pour tout p-sous-groupe H de G, alors pour tous $P, P' \in \mathrm{Syl}_p(G)$, P et P' sont conjugués par un élément de $\mathrm{C}_G(P \cap P')$.

Ce lemme repose lui-même en grande partie sur un autre petit lemme de grand intérêt pour l'étude des p-groupes.

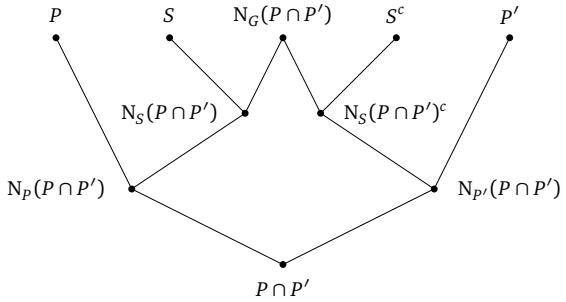
Théorème 25 **(Normalisateurs dans un p-groupe fini)** Soient p un nombre premier, G un p-groupe fini et H un sous-groupe propre de G. Dans ces conditions, l'inclusion : $H \leqslant \mathrm{N}_G(H)$ est stricte.

Démonstration On s'intéresse à l'action par translation de H sur G/H. Les orbites non ponctuelles de cette action sont nécessairement de cardinal divisible par p. D'après l'équation aux classes, le nombre d'orbites ponctuelles est dès lors congru à $\big|G : H\big|$ modulo p, donc est divisible par p puisque H est propre dans G.

Or que sont précisément les orbites ponctuelles ? Pour tout $x \in G$, l'orbite de Hx est ponctuelle si et seulement si pour tout $h \in H$: $Hxh = Hx$, i.e. : $x^{-1}Hx = H$, ou encore : $x \in \mathrm{N}_G(H)$. L'action étudiée possède ainsi $\big|\mathrm{N}_G(H) : H\big|$ orbites ponctuelles. Conclusion : $\big|\mathrm{N}_G(H) : H\big|$ est divisible par p, donc : $\big|\mathrm{N}_G(H)\big| > |H|$. ■

Démonstration **(du théorème 24)** On raisonne par récurrence descendante sur $\big|P \cap P'\big|$ en supposant le résultat vrai, à G fixé, de tout couple $(S, S') \in \mathrm{Syl}_p(G)$ pour lequel : $\big|P \cap P'\big| < \big|S \cap S'\big|$. Le cas d'initialisation où : $P = P'$ est sans enjeu car : $P = P^1$ et $1 \in \mathrm{C}_G(P \cap P)$. Nous supposerons désormais : $P \neq P'$.

- Donnons-nous pour commencer un p-Sylow S de G contenant un p-Sylow de $\mathrm{N}_G(P\cap P')$ contenant lui-même $\mathrm{N}_P(P\cap P')$. Dans ces conditions : $\mathrm{N}_S(P\cap P')\in\mathrm{Syl}_p\big(\mathrm{N}_G(P\cap P')\big)$. D'après les théorèmes de Sylow, $\mathrm{N}_{P'}(P\cap P')$ est inclus dans un conjugué $\mathrm{N}_S(P\cap P')^n$ de $\mathrm{N}_S(P\cap P')$ dans $\mathrm{N}_G(P\cap P')$ avec $n\in\mathrm{N}_G(P\cap P')$. Or le quotient $\dfrac{\mathrm{N}_G(P\cap P')}{\mathrm{C}_G(P\cap P')}$ est un p-groupe par hypothèse, donc : $\mathrm{N}_G(P\cap P')=\mathrm{N}_S(P\cap P')\mathrm{C}_G(P\cap P')$, donc : $n=sc$ avec $s\in\mathrm{N}_S(P\cap P')$ et $c\in\mathrm{C}_G(P\cap P')$, et enfin : $\mathrm{N}_S(P\cap P')^n=\mathrm{N}_S(P\cap P')^{sc}=\mathrm{N}_S(P\cap P')^c$.



- À présent, comme : $P\neq P'$, $P\cap P'$ est propre dans $\mathrm{N}_P(P\cap P')$ et $\mathrm{N}_{P'}(P\cap P')$ d'après **25**, donc a fortiori : $\big|P\cap P'\big|<\big|P\cap S\big|$ et $\big|P\cap P'\big|<\big|P\cap S^c\big|$. Par hypothèse de récurrence, on peut donc dire que : $S=P^{c'}$ pour un certain $c'\in\mathrm{C}_G(P\cap S)\leqslant\mathrm{C}_G(P\cap P')$ et que : $P'=\big(S^c\big)^{c''}$ pour un certain $c''\in\mathrm{C}_G\big(S^c\cap P'\big)\leqslant\mathrm{C}_G(P\cap P')$. Enfin : $P'=S^{cc''}=P^{c'cc''}$ avec : $c'cc''\in\mathrm{C}_G(P\cap P')$. ■

Dans la preuve qui précède et dans son application au théorème de Frobenius, l'hypothèse que le quotient $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ est un p-groupe pour TOUT p-sous-groupe H de G est en réalité utilisée avec parcimonie pour un nombre très restreint de sous-groupes H. À bien y regarder, les seuls sous-groupes H évoqués sont tous des intersections de deux p-Sylow. C'est manifestement suffisant.

Le théorème suivant mériterait dans un autre contexte de plus amples approfondissements. Nous n'en dévoilerons ici qu'un énoncé condensé car ce ne sera pour nous qu'un lemme.

Définition-théorème 26 (Sous-groupe de Frattini et ordre du groupe des automorphismes d'un p-groupe) Soient p un nombre premier, $\alpha\in\mathbb{N}^*$ et G un p-groupe fini d'ordre p^α.

(i) On appelle *sous-groupe de Frattini de G* et on note $\Phi(G)$ l'intersection des sous-groupes maximaux de G. Ce sous-groupe est caractéristique dans G et le quotient $\dfrac{G}{\Phi(G)}$ est abélien p-élémentaire.

(ii) L'entier $\big|\mathrm{Aut}(G)\big|$ divise le produit $p^\beta\displaystyle\prod_{k=1}^{\alpha}\big(p^k-1\big)$ pour un certain $\beta\in\mathbb{N}$.

Démonstration

(i) L'ensemble des sous-groupes maximaux de G est stable par tout automorphisme de G, donc leur intersection aussi, ce qui montre bien que $\Phi(G)$ est caractéristique dans G. Posons alors : $V=\dfrac{G}{\Phi(G)}$.

Nous admettrons ensuite le résultat clasique selon lequel, parce que G est un p-groupe fini, ses sous-groupes maximaux sont exactement ses sous-groupes d'indice p, tous distingués dans G. Notons-les $M_1,\dots,M_r$, de sorte que : $\Phi(G)=M_1\cap\dots\cap M_r$. Le morphisme de groupes $g\longmapsto(M_1g,\dots,M_rg)$ induit aussitôt un morphisme injectif de V dans $\dfrac{G}{M_1}\times\dots\times\dfrac{G}{M_r}$, lequel est isomorphe à $\mathbb{Z}_p^r$. Comme voulu, V est abélien p-élémentaire.

(ii) Parce que $\Phi(G)$ est caractéristique dans G d'après (i), nous pouvons associer à tout automorphisme φ de G un automorphisme $\overline{\varphi}$ de V en posant pour tout $x\in G$: $\overline{\varphi}\big(\Phi(G)x\big)=\Phi(G)\varphi(x)$. L'application $\varphi\longmapsto\overline{\varphi}$ est alors un morphisme de groupes de $\mathrm{Aut}(G)$ dans $\mathrm{Aut}(V)$. Il nous suffit pour conclure de montrer que son noyau est un p-groupe et que $\big|\mathrm{Aut}(V)\big|$ divise $p^\gamma\displaystyle\prod_{k=1}^{\alpha}\big(p^k-1\big)$ pour un certain $\gamma\in\mathbb{N}$.

- Parce que V est abélien p-élémentaire d'après (i), la loi externe $\big(\lambda,\Phi(G)x\big)\longmapsto\Phi(G)x^\lambda$ de $\mathbb{F}_p\times V$ dans V munit V d'une structure de $\mathbb{F}_p$-espace vectoriel, disons de dimension $r\in[\![1,\alpha]\!]$. Il n'est alors pas dur

de comprendre que tout automorphisme DE GROUPE de V est de fait un automorphisme LINÉAIRE de V, autrement dit : $\mathrm{Aut}(V) = \mathrm{GL}(V)$. Or le calcul de $\big|\mathrm{GL}(V)\big|$ est un grand classique :

$$\big|\mathrm{Aut}(V)\big| = \big|\mathrm{GL}(V)\big| = \prod_{k=0}^{r-1}\big(p^r - p^k\big) = p^{\frac{r(r+1)}{2}}\prod_{k=1}^{r}\big(p^k - 1\big).$$

- Supposons maintenant par l'absurde que le noyau du morphisme $\varphi \longmapsto \overline{\varphi}$ ne soit pas un p-groupe. Nous pouvons alors nous donner un automorphisme $\varphi \in \mathrm{Aut}(G)$ d'ordre premier $q \neq p$ pour lequel : $\overline{\varphi} = \mathrm{Id}_V$, ou encore pour tout $x \in G$: $\varphi\big(\Phi(G)x\big) = \Phi(G)x$. En d'autres termes, φ stabilise chacune des classes à droite de G modulo $\Phi(G)$, disons $\Phi(G)x_1, \dots, \Phi(G)x_s$ avec $x_1, \dots, x_s \in G$. D'après l'équation aux classes, q étant distinct de p, φ fixe alors au moins un élément de chacune de ces classes et on peut supposer sans perte de généralité que φ fixe $x_1, \dots, x_s$. A fortiori, φ fixe le sous-groupe $\big\langle x_1, \dots, x_s\big\rangle$, mais comme : $\varphi \neq \mathrm{Id}_G$, ce sous-groupe est propre dans G, donc inclus dans un sous-groupe maximal M de G, lequel contient $\Phi(G)$ par définition. Finalement : $\dfrac{G}{\Phi(G)} = V = \Big\{\Phi(G)x_1, \dots, \Phi(G)x_s\Big\} \leqslant \dfrac{M}{\Phi(G)}$, donc : $G \leqslant M$ — contradiction. ■

Théorème 27 (Théorème 12-16-56 de Burnside)

(i) Soient p un nombre premier, $m \in \mathbb{N}^*$ premier à p, $\alpha \in \mathbb{N}^*$ et G un groupe fini d'ordre $p^\alpha m$. Si m premier à tous les entiers $p^k - 1$, k décrivant $[\![1, \alpha]\!]$, alors G est p-nilpotent.

(ii) Tout groupe fini simple non abélien d'ordre pair est d'ordre divisible par 12, 16 ou 56.

(iii) Soit G un groupe fini simple non abélien d'ordre impair. On note p le plus petit diviseur premier de $|G|$. Alors $|G|$ est divisible par p^3.

Le résultat de l'assertion (iii) est un peu artificiel car le théorème de Feit-Thompson affirme que tout groupe fini simple non abélien est d'ordre pair, mais le théorème de Feit-Thompson est hélas TRÈS difficile à prouver.

Démonstration

(i) Soit H un p-sous-groupe de G. L'action par conjugaison de $\mathrm{N}_G(H)$ sur H plonge le quotient $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ dans le groupe $\mathrm{Aut}(H)$. Par hypothèse sur m et d'après **26** (ii), il en découle aussitôt que $\dfrac{\mathrm{N}_G(H)}{\mathrm{C}_G(H)}$ est un p-groupe. Il ne reste alors plus qu'à conclure grâce au théorème de p-nilpotence de Frobenius.

(ii) Soit G un groupe fini simple non abélien d'ordre pair. En particulier, G n'est pas 2-nilpotent. D'après (i), il est aussitôt impossible que $|G|$ soit divisible par 2 mais pas par 4. Pour la même raison, si $|G|$ est divisible par 4 mais pas par 8, $|G|$ a un diviseur premier en commun avec $2^2 - 1 = 3$, donc $|G|$ est divisible par 12. Si $|G|$ est divisible par 8 mais pas par 16, $|G|$ a un diviseur premier en commun avec $2^2 - 1 = 3$ ou $2^3 - 1 = 7$, donc $|G|$ est divisible par 24 ou 56. C'est exactement le résultat voulu.

(iii) Simple non abélien, G n'est pas p-nilpotent. D'après (i), il est aussitôt impossible que $|G|$ soit divisible par p mais pas par p^2. Pour la même raison, si $|G|$ est divisible par p^2 mais pas par p^3, $|G|$ a un diviseur premier en commun avec $p^2 - 1 = (p-1)(p+1)$, donc avec $p+1$ par minimalité de p, mais c'est impossible car : $p \neq 2$. Comme voulu, $|G|$ est divisible par p^3. ■

Exemple Soient $p_1, \dots, p_n$ des nombres premiers distincts supérieurs ou égaux à 5. Tout groupe d'ordre $2^2 p_1 \dots p_n$ est résoluble.

Démonstration On raisonne par récurrence sur n en supposant le résultat vrai de tout rang strictement inférieur. Soit G un groupe d'ordre $2^2 p_1 \dots p_n$ où $p_1, \dots, p_n$ sont des nombres premiers distincts supérieurs ou égaux à 5. D'après le théorème 12-16-56, G n'est pas simple et nous pouvons nous en donner un sous-groupe distingué N à la fois propre et non trivial.

— Si les groupes N et $\dfrac{G}{N}$ sont tous les deux d'ordre pair, ils sont résolubles d'après un exemple précédent.

— Dans le cas contraire, l'un de ces deux groupes est résoluble d'après le même exemple tandis que l'autre l'est par hypothèse de récurrence.

Dans les deux cas, G est résoluble par empilement.

Exemple Soient p, q et r trois nombres premiers distincts avec : $q < r$. S'il existe un groupe simple G d'ordre p^2qr, alors : $p = 2$, $q = 3$ et $r = 5$, et G est isomorphe au groupe symétrique A_5 d'ordre 60.

Démonstration D'après le théorème 12-16-56 : $p = 2$ et $q = 3$. Ensuite, d'après les théorèmes de Sylow et par simplicité de G, G possède un nombre n_r de r-Sylow avec : $n_r = 6$ si $r = 5$ et : $n_r = 12$ si $r = 11$.

— Si $r = 11$: $|G| = 132 = 2^2 \times 3 \times 11$. Les 11-Sylow de G étant cycliques, ils sont deux à deux d'intersection triviale, donc représentent collectivement $(11-1) \times 12 = 120$ éléments d'ordre 11. Les théorèmes de Sylow montrent par ailleurs que G possède au moins 4 3-Sylow, qui représentent quand à eux au moins $(3-1) \times 4 = 8$ éléments d'ordre 3. Les 128 éléments ainsi collectés ne permette à G qu'un unique 2-Sylow, ce qui contredit sa simplicité.

— Si $r = 5$: $|G| = 60$ et il est bien connu que A_5 est le seul groupe d'ordre 60 à isomorphisme près.

5.5 Pour aller plus loin

Comme on l'a vu, les théorèmes de p-nilpotence de Burnside et Frobenius énoncent tous les deux de quelle manière une information p-locale peut être convertie en une information globale. Avec le temps, ces théorèmes ont ouvert la voie à une branche complète de la théorie des groupes finis qualifiée parfois d'*analyse p-locale*, et dont nous allons présenter rapidement quelques résultats emblématiques supplémentaires.

Thompson a introduit au début des années 1960 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 fini.

- 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 : $\mathrm{ZJ}(P) = \mathrm{Z}\big(\mathrm{J}(P)\big)$.

Si P est abélien, il est clair que : $\mathrm{J}(P) = P$.

Le résultat qui suit généralise les deux théorèmes de p-nilpotence de Burnside et Frobenius. Publié en 1964, il a fait date dans l'histoire de la théorie des groupes finis et nous y reviendrons d'ailleurs quand nous parlerons des groupes de Frobenius. Nous n'énoncerons le théorème que dans le cas où p est impair. Une condition supplémentaire est requise pour $p = 2$.

Théorème 28 **(Théorème de p-nilpotence de Thompson)** Soient G un groupe fini, p un nombre premier IMPAIR 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.

Résumons-nous. Burnside a prouvé que si P est abélien, la p-nilpotence de $\mathrm{N}_G(P)$ implique celle de G. Dans le cas général, Frobenius a établi que la p-nilpotence de tout sous-groupe p-local de G implique celle de G. Thompson a réconcilié les deux théorèmes pour $p \neq 2$ en montrant que dans le théorème de Frobenius, la p-nilpotence de DEUX sous-groupes p-locaux bien choisis est suffisante. Quelques années plus tard, en 1968, Glauberman a même trouvé mieux.

Théorème 29 **(Théorème de p-nilpotence de Glauberman, ou théorème ZJ)** Soient G un groupe fini, p un nombre premier IMPAIR 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.

Ici aussi, la restriction au cas où p est impair peut être levée au moyen d'une hypothèse supplémentaire.

Alors que le théorème de Frobenius nous a demandé un peu de travail, le théorème de Thompson nous en demanderait davantage et le théorème de Glauberman plus encore. Glauberman et Solomon ont cela dit découvert en 2012 un nouveau sous-groupe universel susceptible de remplacer à terme le sous-groupe de Thompson et nettement plus facile d'utilisation.

Si ces divers théorèmes de p-nilpotence sont naturels à présenter dans une discussion sur le transfert dans un p-Sylow, une autre question se pose tout aussi naturellement. Dans le cas où P est abélien, nous avons vu que le sous-groupe $\mathrm{N}_G(P)$ contrôle la G-fusion de P, et c'est d'ailleurs grâce à ce résultat que nous avons démontré le théorème de p-nilpotence de Burnside. Quel contrôle de fusion de P pouvons-nous espérer dans le cas général ?

Théorème 30 **(Théorème ZJ de Glauberman, version « fusion »)** Soient G un groupe fini, p un nombre premier IMPAIR et $P \in \mathrm{Syl}_p(G)$. Alors $\mathrm{N}_G\big(\mathrm{ZJ}(P)\big)$ contrôle la G-fusion de P.

Dans une autre direction, Yoshida a trouvé une condition sur la structure du p-Sylow P pour que le sous-groupe $\mathrm{N}_G(P)$ lui-même contrôle la G-fusion de P. Notons pour l'énoncer $\mathbb{Z}_p \wr \mathbb{Z}_p$ le produit semi-direct $\mathbb{Z}_p \ltimes \mathbb{Z}_p^{\mathbb{Z}_p}$ défini par l'action de décalage de $\mathbb{Z}_p$ sur $\mathbb{Z}_p^{\mathbb{Z}_p}$. Précisément, pour tous $k \in \mathbb{Z}_p$ et $(x_0, \dots, x_{p-1}) \in \mathbb{Z}_p^{\mathbb{Z}_p}$: $\quad (x_0, \dots x_{p-1})^k = (x_k, \dots, x_{p-1}, x_0, \dots, x_{k-1})$.

Théorème 31 **(Théorème de Yoshida)** Soient G un groupe fini, p un nombre premier et $P \in \mathrm{Syl}_p(G)$. Si $\mathrm{N}_G(P)$ NE contrôle PAS la G-fusion de P, alors P a un quotient isomorphe à $\mathbb{Z}_p \wr \mathbb{Z}_p$.

En particulier, si : $\quad |P| \leqslant p^p, \quad$ alors $\mathrm{N}_G(P)$ contrôle la G-fusion de P.

6 Le théorème de Frobenius

Un groupe fini G et un sous-groupe H de G étant donnés, les conjugués de H dans G occupent une certaine place dans G. Si H est distingué dans G ce territoire est H lui-même, car alors pour tout $g \in G$: $\quad H^g = H$. $\quad$ À l'extrême inverse, on peut se demander ce qu'il advient de G dans le pire des cas, i.e. dans le cas où H et ses conjugués occupent le plus de place possible. C'est précisément cette situation extrémale que la notion de *sous-groupe de Frobenius* entend décrire.

Définition **(Groupe de Frobenius, sous-groupe de Frobenius)** Soit G un groupe fini. On dit que G est un *groupe de Frobenius* s'il existe un sous-groupe non trivial et propre H de G pour lequel pour tout $g \in G \setminus H$: $\quad H \cap H^g = 1$. $\quad$ Le sous-groupe H est dans ce cas appelé un *complément* (*de Frobenius*) *de* G, ou encore un *sous-groupe de Frobenius de* G.

Définition-théorème 32 **(Premières propriétés d'un sous-groupe de Frobenius)** Soit G un groupe de Frobenius de complément H.

(i) H contrôle sa propre G-fusion.

(ii) $\quad \mathrm{N}_G(H) = H$. $\qquad$ En particulier, H possède $\big|G : H\big|$ conjugués dans G.

(iii) $\quad \big|G : H\big| \equiv 1 \big[|H|\big]$. $\qquad$ En particulier, H est un sous-groupe de Hall de G.

Démonstration

(i) Simple conséquence de **11** (ii).

(ii) Pour montrer que : $\quad \mathrm{N}_G(H) = H, \quad$ il nous suffit de montrer que : $\quad \mathrm{N}_G(H) \leqslant H, \quad$ or pour tout $g \in G \setminus H$: $H \cap H^g = 1, \quad$ donc : $\quad H^g \neq H$.

Pour calculer le nombre de conjugués de H dans G, on peut simplement remarquer que G opère transitivement par conjugaison sur leur ensemble et que le stabilisateur de H pour cette action est $\mathrm{N}_G(H) = H$. Comme voulu, H possède $\big|G : H\big|$ conjugués dans G.

(iii) Montrons pour finir que : $\big|G : H\big| \equiv 1 \big[|H|\big]$. Faisons pour cela agir H par translation à droite sur $(G/H) \setminus \big\{H\big\}$. Pour tout $x \in G \setminus H$, le stabilisateur de Hx pour cette action vaut $H \cap H^x = 1$, donc l'orbite de Hx est de cardinal $|H|$. D'après l'équation des classes, comme voulu, $\big|(G/H) \setminus \{1\}\big| = \big|G : H\big| - 1$ est divisible par $|H|$. ■

Les groupes de Frobenius décrivent par définition une situation extrémale, mais plutôt courante. Le théorème suivant se penche sur une classe de groupes de Frobenius dont nous verrons par la suite qu'elle contient en réalité à isomorphisme près tous les groupes de Frobenius.

Définition-théorème 33 (Automorphismes sans point fixe et groupes de Frobenius) Soient G un groupe fini non trivial et A un sous-groupe non trivial de $\mathrm{Aut}(G)$.

- Pour tout $\varphi \in \mathrm{Aut}(G)$, on dit que φ est *sans point fixe* (*dans* G) si pour tous $g \in G$: $\quad \varphi(g) = g \quad \Longrightarrow \quad g = 1$.
  On dit alors que A est *sans point fixe* (*dans* G) si tous ses éléments non triviaux sont eux-mêmes sans point fixe.
- Si A est sans point fixe dans G, le produit semi-direct $A \ltimes G$ défini par l'action naturelle de A sur G est un groupe de Frobenius de complément A.

Un rappel sur les produits semi-directs s'impose ici peut-être. Les groupes A et G peuvent être vus comme des sous-groupes de $A \ltimes G$ et tout élément de $A \ltimes G$ s'écrit d'une et une seule manière sous la forme αg avec $\alpha \in A$ et $g \in G$. Pour définir la loi de $A \ltimes G$, il est suffisant de savoir conjuguer tout élément g de G par un élément α de A : $\quad g^\alpha = \alpha(g)$. Cette relation énonce en particulier que G est normalisé par A, donc distingué dans $A \ltimes G$. Pour tous $\alpha, \alpha' \in A$ et $g, g' \in G$, enfin :

$$(\alpha g)(\alpha' g') = (\alpha\alpha')\big(\alpha'^{-1} g \alpha' g'\big) = (\alpha\alpha')\big(g^{\alpha'} g'\big) = \underbrace{(\alpha\alpha')}_{\in A}\big(\underbrace{\alpha'(g) g'}_{\in G}\big).$$

Démonstration Montrons que A est un sous-groupe de Frobenius de $A \ltimes G$. Soit $x \in (A \ltimes G) \setminus A$, disons : $x = \varphi g \quad$ avec $\varphi \in A$ et $g \in G \setminus \big\{1\big\}$. Nous voulons montrer que : $\quad A \cap A^x = 1, \quad$ i.e. : $\quad A \cap A^g = 1$.

Soit $\alpha \in A \cap A^g$. Alors : $\quad g\alpha g^{-1} \in A, \quad$ donc : $\quad \alpha(g) g^{-1} = g^\alpha g^{-1} = \alpha^{-1}\big(g\alpha g^{-1}\big) \in A \cap G = 1, \quad$ donc : $\alpha(g) = g$. Finalement, comme : $\quad g \neq 1 \quad$ et comme α est sans point fixe : $\quad \alpha = 1$. ■

Exemple Pour tout entier q puissance d'un nombre premier, le produit semi-direct $\mathbb{F}_q^* \ltimes \mathbb{F}_q$ défini par l'action multiplicative de $\mathbb{F}_q^*$ sur $\mathbb{F}_q$ est un groupe de Frobenius de complément $\mathbb{F}_q^*$.

Le théorème **33** a été énoncé en termes de produit semi-direct externe, i.e. en termes d'action d'un groupe sur un autre par automorphismes. On aurait pu, de manière équivalente, l'énoncer en termes de produit semi-direct interne. C'est ce que fait justement le théorème qui suit.

Théorème 34 (Groupes de Frobenius définis comme des produits semi-directs internes) Soient G un groupe fini, K un sous-groupe distingué non trivial de G et H un sous-groupe non trivial de G. Si G est le produit semi-direct de K par H, i.e. si : $\quad G = HK \quad$ et $H \cap K = 1, \quad$ et si de plus pour tout $k \in K \setminus \big\{1\big\}$: $\quad \mathrm{C}_G(k) \leqslant K, \quad$ alors G est un groupe de Frobenius de complément H.

Démonstration Par hypothèse, d'une part : $\quad G = H \ltimes K, \quad$ où le produit semi-direct est défini par l'action de H sur K par conjugaison, mais d'autre part, tout élément non trivial de H est sans point fixe dans K, car pour tous $h \in H$ et $k \in K \setminus \big\{1\big\}$, si : $\quad k^h = k, \quad$ alors : $\quad h \in \mathrm{C}_G(k) \leqslant K, \quad$ donc : $\quad h \in H \cap K = 1$. Le théorème **33** montre que dans ces conditions, G est comme voulu un groupe de Frobenius de complément H. ■

Exemple Pour tout $n \geqslant 3$ impair, le groupe diédral D_n de degré n peut être défini abstraitement comme le produit semi-direct $\mathbb{Z}_2 \ltimes \mathbb{Z}_n$ issu de l'action par inversion de $\mathbb{Z}_2$ sur $\mathbb{Z}_n$. Plus explicitement, cela veut dire que : $\quad D_n = \langle\tau\rangle\langle\sigma\rangle \quad$ où τ est une involution, σ un élément d'ordre n, et : $\quad \sigma^\tau = \sigma^{-1}$. Remarquons alors que pour tout $k \in Z$: $\quad k \not\equiv -k\,[n] \quad$ car n étant impair, donc : $\quad \big(\sigma^k\big)^\tau = \sigma^{-k} \neq \sigma^k, \quad$ donc τ est sans point fixe dans $\langle\sigma\rangle$. Conclusion : D_n est un groupe de Frobenius de complément $\langle\sigma\rangle$.

Exemple Le groupe symétrique S_3 de degré 3 est isomorphe à D_3, c'est donc un groupe de Frobenius — de noyau $\big\langle(1\ 2)\big\rangle$.

Dans chacun de ces exemples, tous issus des théorèmes **33** et **34**, le sous-groupe de Frobenius proposé se trouve toujours acquiné avec un sous-groupe distingué dans une situation de produit semi-direct — G dans le théorème **33** et K dans le théorème **34**. Avec les notations du théorème **34**, le fait que K soit distingué dans G et qu'on ait : $H \cap K = 1$ implique qu'en réalité pour tout $g \in G$: $H^g \cap K = 1$. Conclusion : $K \subset \left(G \setminus \bigcup_{g \in G} H^g \right) \cup \{1\}$.

Définition-théorème 35 **(Noyau de Frobenius)** Soit G un groupe de Frobenius de complément H. On appelle *noyau (de Frobenius) de G* l'ensemble : $\left(G \setminus \bigcup_{g \in G} H^g \right) \cup \{1\}$. Cet ensemble a pour cardinal $\big|G : H\big|$.

Démonstration Donnons-nous un ensemble de représentants $\{g_1, \dots, g_n\}$ des classes à droite de G modulo H, avec : $n = \big|G : H\big|$. Les conjugués de H dans G sont alors les sous-groupes H^{g_k}, k décrivant $[\![1, n]\!]$. N'oublions pas par ailleurs que les ensembles $H^{g_k} \setminus \{1\}$, k décrivant $[\![1, n]\!]$, sont deux à deux disjoints. Aussitôt :

$$\left| \left(G \setminus \bigcup_{g \in G} H^g \right) \cup \{1\} \right| = \big|G \setminus \{1\}\big| - \sum_{k=1}^{n} \big|H^{g_k} \setminus \{1\}\big| + 1 = |G| - \sum_{k=1}^{n} \big(|H| - 1\big) = |G| - \big|G : H\big|\big(|H| - 1\big) = |G|. \qquad \blacksquare$$

Avec les notations du théorème **34**, il apparaît maintenant pour une raison d'inclusion et de cardinal que K coïncide avec le noyau de Frobenius de G. Nous tenons là, en d'autres termes, une description du sous-groupe distingué K à partir du sous-groupe de Frobenius H. Pourquoi est-ce intéressant ? Parce que la définition d'un groupe de Frobenius stipule l'existence d'un sous-groupe de Frobenius mais ne le relie pas naturellement à un sous-groupe distingué.

Ce que Frobenius a découvert, contre toute attente, c'est que le noyau d'un groupe de Frobenius G est **TOUJOURS** un sous-groupe de G. C'est plus précisément un sous-groupe distingué de G car clairement le noyau de Frobenius de G est stable par conjugaison dans G, mais le miracle de cette affaire, c'est vraiment que le noyau de Frobenius soit un **SOUS-GROUPE**. Sa définition comme complémentaire d'une réunion ne laissait rien présager de ce genre.

Théorème 36 **(Théorème de Frobenius)** Soit G un groupe de Frobenius de complément H et de noyau K.

(i) Le noyau K est un sous-groupe de G.

(ii) Plus précisément, K est un sous-groupe de Hall distingué dans G et G est le produit semi-direct de K par H. En outre, dans ce produit semi-direct, H est sans point fixe dans K.

Démonstration Nous travaillerons sur l'assertion (i) plus tard. Admettons-la pour le moment et déduisons-en (ii). La définition de K en fait clairement une partie de G stable par conjugaison, donc K est un sous-groupe distingué de G d'après l'assertion (i). Ensuite, d'après **32** et **35** : $|K| = \big|G : H\big| \equiv 1 \big[|H|\big]$, donc K est de Hall dans G. Pour finir, par définition de K : $H \cap K = 1$ et pour une raison de cardinal : $G = HK$, donc en effet, G est le produit semi-direct de K par H. Se peut-il, dans ce produit semi-direct, qu'un élément non trivial h de H fixe un élément non trivial k de K ? Non, car dans ce cas : $k \in G \setminus H$, donc : $h^k = h \in H \cap H^k = 1$. $\blacksquare$

Nous ne pourrons hélas pas démontrer ici l'assertion (i) du théorème de Frobenius dans sa pleine mesure. Pour la prouver, Frobenius a eu recours à la *théorie des caractères*, une branche de la *théorie des représentations* qui s'est avérée cruciale dans le développement de la théorie des groupes finis, mais dont les méthodes sont peu compatibles avec les outils de ce texte. Si personne n'a encore jamais de trouvé de preuve du théorème de Frobenius indépendante de la théorie des représentations, on sait au moins l'établir dans deux situations importantes — lorsque H est résoluble d'une part grâce au transfert, et lorsque H est d'ordre pair d'autre part, situations que nous allons étudier à présent.

Un théorème hautement non trivial, le *théorème de Feit-Thompson*, énonce que tout groupe d'ordre impair est résoluble. Selon ce théorème, les deux situations du théorème de Frobenius que nous allons traiter ci-dessous — résolubilité et ordre pair — couvrent donc en fait tous les cas possibles. Le problème, hélas, c'est que le théorème de Feit-Thompson requiert lui aussi la théorie des caractères, et à un niveau nettement plus difficile.

Démonstration **(de l'assertion (i) du théorème de Frobenius dans le cas résoluble)** Les notations sont celles du théorème **36** et on suppose H résoluble. Par récurrence, l'assertion (i) est en outre supposée vraie de tout groupe de Frobenius d'ordre strictement inférieur à $|G|$ dont le complément résoluble.

- D'après **32**, le sous-groupe H contrôle sa propre G-fusion, donc d'après **11** (iii) : $V_{G\to H}(h) = h^{|G:H|}\,\mathrm{D}(H)$ pour tout $h \in H$. Ensuite, H est de Hall dans G d'après **32**, donc $V_{G\to H}$ est surjectif de G sur $\dfrac{H}{\mathrm{D}(H)}$ d'après **10**. Son noyau contient $\mathrm{D}(H)$, mais plus précisément : $H \cap \mathrm{Ker}\, V_{G\to H} = \mathrm{D}(H)$, car : $h^{|G:H|} \in \mathrm{D}(H)$ pour tout $h \in H \cap \mathrm{Ker}\, V_{G\to H}$, donc grâce à une relation de Bézout : $h \in \mathrm{D}(H)$.
- Montrons à présent que $\mathrm{D}(H)$ est un sous-groupe de Frobenius de $\mathrm{Ker}\, V_{G\to H}$. C'est immédiat car pour tout $g \in \mathrm{Ker}\, V_{G\to H} \setminus \mathrm{D}(H)$, on vient de voir que : $g \in G \setminus H$, donc : $\mathrm{D}(H) \cap \mathrm{D}(H)^g \leqslant H \cap H^g = 1$. Or le complément H étant résoluble : $\mathrm{Ker}\, V_{G\to H} \neq G$, donc par hypothèse de récurrence, le noyau de Frobenius K' de $\mathrm{Ker}\, V_{G\to H}$ est un sous-groupe de G. D'après **35**, son ordre vaut :

$$|K'| = \big|\mathrm{Ker}\, V_{G\to H} : \mathrm{D}(H)\big| = \frac{\big|\mathrm{Ker}\, V_{G\to H}\big|}{\big|\mathrm{D}(H)\big|} = \frac{|G|}{\big|H : \mathrm{D}(H)\big|} \times \frac{1}{\big|\mathrm{D}(H)\big|} = \big|G : H\big|,$$

  or c'est aussi le cardinal du noyau de Frobenius K de G. Il n'est pas difficile de comprendre par ailleurs que : $K' \subset K$. Conclusion : $K = K'$. En particulier, K est un sous-groupe de G. ■

Démonstration **(de l'assertion (i) du théorème de Frobenius dans le cas pair)** Les notations sont celles du théorème **36** et on suppose H d'ordre pair. Posons : $n = \big|G : H\big|$. D'après **32**, nous pouvons noter $H_1, \dots, H_n$ les conjugués distincts de H — avec par exemple : $H_1 = H$ — et nous donner une involution t_k de H_k pour tout $k \in [\![1, n]\!]$.

- Soient $i, j \in [\![1, n]\!]$ distincts. Se peut-il qu'on ait : $t_i t_j \in H_k$? Comme : $(t_i t_j)^{t_i} = t_j t_i = (t_i t_j)^{-1}$: on aurait dans ce cas : $(t_i t_j)^{t_i} \in H_k \cap H_k^{t_i}$. Pourtant : $t_i \in H_i$ donc : $t_i \in G \setminus H_k$, donc : $(t_i t_j)^{t_i} = 1$, i.e. : $t_i = t_j$, ce qui est faux car i et j sont distincts.
- Le point précédent montre que pour tous $i, j \in [\![1, n]\!]$: $t_i t_j \in K$. Pour tout $i \in [\![1, n]\!]$, l'application $j \longmapsto t_i t_j$ est alors injective de $[\![1, n]\!]$ dans K, mais c'est donc une bijection pour une raison de cardinal. Pour tout $i \in [\![1, n]\!]$, tout élément de K peut donc être écrit : $t_i t_j$ pour un certain $j \in [\![1, n]\!]$.
- Montrons enfin que K est un sous-groupe de G. Soient $k, k' \in K$, disons : $k = t_1 t_i$ et $k' = t_1 t_j$ pour certains $i, j \in [\![1, n]\!]$. Alors : $k^{-1}k' = (t_1 t_i)^{-1}(t_1 t_j) = t_i t_j \in K$. ■

Nous achèverons cette partie par l'énoncé sans preuve de quelques résultats supplémentaires importants sur les groupes de Frobenius. Tous ne sont pas faciles à démontrer, loin s'en faut. Le *théorème de Thompson* demande ainsi un gros travail d'analyse p-locale. C'est d'ailleurs à cette occasion que Thompson a démontré le théorème de p-nilpotence éponyme que nous avons évoqué plus haut dans ce texte.

Rappelons ici qu'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 direct de ses différents p-Sylow. En réalité, cette définition de la nilpotence manque un peu de généralité mais elle est ici suffisante.

Théorème 37 **(Résultats supplémentaires sur les groupes de Frobenius)** Soit G un groupe de Frobenius de complément H et de noyau K.

(i) Pour tout nombre premier p impair, les p-Sylow de H sont cycliques. Ses 2-Sylow sont quant à eux soit cycliques, soit d'un type particulier appelé *quaternionien généralisé*. Également, pour tous nombres premiers p et q distincts, tout sous-groupe de H d'ordre pq est cyclique.

(ii) **Théorème de Thompson :** K est nilpotent.

Dans le cas où H est d'ordre pair, on peut même dire que K est abélien.

(iii) H et ses conjugués sont les seuls sous-groupes de Frobenius de G.

Démonstration Le cas pair de l'assertion (ii) est très facile à démontrer. Sous l'hypothèse que H est d'ordre pair, donnons-nous-en une involution t.

- Montrons que l'application $k \longmapsto \big[k, t\big]$ est injective de K dans K. Pour commencer, elle est bien définie de K dans K car K est distingué dans G. Ensuite, pour tous $k, k' \in K$, si : $\big[k, t\big] = \big[k', t\big]$, alors : $k^{-1}tk = k'^{-1}tk'$ donc : $\big(k'k^{-1}\big)^t = k'k^{-1}$, or t agit sans point fixe sur K d'après **36**, donc : $k'k^{-1} = 1$, i.e. : $k = k'$.

- Comme K est fini, l'injectivité de l'application $k \longmapsto \big[k,t\big]$ en fait une bijection de K sur K. Pour tout $k \in K$, dès lors : $k = \big[k',t\big]$ pour un certain $k' \in K$, donc : $k^t = \big[k',t\big]^t = \big[t,k'\big] = \big[k',t\big]^{-1} = k^{-1}$. En résumé, t agit sur K par inversion.
- Pour finir, pour tous $x, y \in G$: $(xy)^t = (xy)^{-1} = y^{-1}x^{-1} = y^t x^t = (yx)^t$, donc : $xy = yx$. ■

7 Le théorème Z^* de Glauberman

S'il y a bien une chose que la théorie des groupes finis a observé tout au long de son long développement jusqu'à nous, c'est le rôle central que les involutions y occupent. Le monstrueux *théorème de Feit-Thompson*, pour ne citer que lui, énonce ainsi qu'un groupe fini simple non abélien est forcément d'ordre pair. Le *théorème de Brauer-Fowler* montre de son côté qu'il n'existe qu'un nombre fini de groupes finis simples non abéliens dont le centralisateur d'une involution est prescrit. La classification des groupes finis simples, aujourd'hui achevée, a ainsi consisté en grande partie à comprendre de quelle manière les centralisateurs d'involution, information locale, voient leur structure se diffuser au sein d'un groupe. Le *théorème* Z^* *de Glauberman*, publié en 1966, est l'un des résultats les plus importants dans cette direction.

Définition **(Involution isolée, sous-groupes $O(G)$ et $Z^*(G)$)** Soit G un groupe fini.

- On dit qu'une involution t de G est *isolée dans* G si : $t^G \cap C_G(t) = \{t\}$.
- Le sous-groupe $O_{2'}(G)$ est aussi souvent noté $O(G)$.
- On note $Z^*(G)$ l'unique sous-groupe de G contenant $O(G)$ dont le quotient par $O(G)$ est $Z\left(\frac{G}{O(G)}\right)$.

Le sous-groupe $Z^*(G)$ est distingué dans G car $Z\left(\frac{G}{O(G)}\right)$ l'est dans $\frac{G}{O(G)}$.

Théorème 38 **(Théorème Z^* de Glauberman)** Soit G un groupe fini.

(i) Si G contient une involution isolée : $G = O(G)C_G(t)$. En particulier, G n'est pas simple.

(ii) $Z^*(G)$ contient toutes les involutions isolées de G.

La preuve du théorème Z^* dépasse largement le cadre de ce texte. Alors que le théorème de Frobenius de la partie précédente requérait la théorie des caractères ordinaires, i.e. définis sur le corps $\mathbb{C}$, le théorème Z^* découle de certains résultats de Brauer en *théorie des caractères modulaires*, i.e. sur un corps fini. Notre objectif sera seulement de démontrer le théorème dans certains cas particuliers accessibles aisément par transfert.

Démonstration Nous pouvons au moins montrer que l'assertion (ii) découle de l'assertion (i). Soit t une involution isolée de G. D'après (i) : $G = O(G)C_G(t)$, donc pour tout $g \in G$ donné sous la forme : $g = \omega c$ avec $\omega \in O(G)$ et $c \in C_G(t)$: $\big[g^{-1},t\big] = t^{g^{-1}}t = t^{\omega^{-1}}t = \omega\big(\omega^t\big)^{-1} \in O(G)$. En d'autres termes, $O(G)g$ et $O(G)t$ commutent dans $\frac{G}{O(G)}$ pour tout $g \in G$, donc : $O(G)t \in Z\left(\frac{G}{O(G)}\right)$, i.e. : $t \in Z^*(G)$. ■

Théorème 39 **(Deux exemples sur les involutions isolées)** Soit G un groupe fini d'ordre pair. Si les 2-Sylow de G sont cycliques ou isomorphes au groupe des quaternions Q_8, toute involution de G y est isolée.

Les 2-groupes cycliques et le groupe des quaternions Q_8 ont ceci de commun qu'ils ne contienne qu'une seule involution chacun. C'est cette propriété d'unicité, on va le voir, qui fait fonctionner le théorème.

Démonstration Soient t une involution de G et $g \in G$. Faisons l'hypothèse que : $t^g \in C_G(t)$. Le sous-groupe $\langle t, t^g\rangle$ est alors un 2-sous-groupe de G, donc est inclus dans un 2-Sylow de G, lequel ne contient qu'une seule involution par hypothèse. Conclusion : $t^g = t$, ce qui montre bien que t est isolée dans G. ■

Le théorème Z* montre en particulier, grâce au théorème **39**, qu'un groupe fini simple ne peut pas avoir le groupe Q_8 pour 2-Sylow. Il ne peut pas non plus avoir un groupe cyclique pour 2-Sylow, mais c'est un résultat que nous avons déjà tiré du théorème de p-nilpotence de Burnside dans le théorème **20**. Si l'on y réfléchit bien, le théorème **20** est même un peu plus fort que le théorème Z* dans ce cas particulier.

Théorème 40 **(Quelques propriétés des involutions isolées)** Soit G un groupe fini. On suppose que G contient une involution isolée t. On pose pour tout $x \in G$: $\widehat{x} = [t,x]$ et $\widehat{G} = \{\widehat{x}\}_{x\in G}$.

(i) $C_G(t)$ contient un 2-Sylow de G.

(ii) Pour tous $x, y \in G$: $\widehat{x}^t = \widehat{x}^{-1}$ et $\widehat{x}\widehat{y}\widehat{x} = \widehat{yx}$, donc en particulier : $\widehat{\widehat{x}} = \widehat{x}^2$.

(iii) $\widehat{G}$ est stable par exponentiation et ses éléments sont tous d'ordre impair.

(iv) $\widehat{G}$ est un ensemble de représentants des classes à droite de G modulo $C_G(t)$. En particulier : $\left|\widehat{G}\right| = \left|G : C_G(t)\right|$.

(v) $C_G(t)$ contrôle sa propre G-fusion.

(vi) 1 est le seul élément de G conjugué à la fois à un élément de $\widehat{G}$ et à un élément de $C_G(t)$.

(vii) $\operatorname{Ker} V_{G\to C_G(t)}$ contient $\widehat{G}$ et le sous-groupe $\left(\operatorname{Ker} V_{G\to C_G(t)}\right)\langle t\rangle$ est distingué dans G.

(viii) Le sous-groupe $\left\langle \widehat{G}\right\rangle$ est distingué dans G.

Démonstration

(i) L'action par translation à droite du groupe $\langle t\rangle$ sur l'ensemble $G/C_G(t)$ admet la classe $C_G(t)$ pour unique point fixe. En effet, pour tout $x \in G$:

$$C_G(t)xt = C_G(t)x \iff t^{x^{-1}} \in t^G \cap C_G(t) \iff t^{x^{-1}} = t \iff x \in C_G(t).$$

On déduit alors de l'équation aux classes que $\left|G : C_G(t)\right|$ est impair, autrement dit que $C_G(t)$ contient un 2-Sylow de G.

(ii) Pour tous $x, y \in G$: $\widehat{x}^t = [t,x]^t = [x,t] = [t,x]^{-1} = \widehat{x}^{-1}$ et :

$$\widehat{x}\widehat{y}\widehat{x} = \widehat{x}ty^{-1}tyx = t\widehat{x}^{-1}y^{-1}tyx = t(yx)^{-1}t(yx) = [t,yx] = \widehat{yx}.$$

En particulier : $\widehat{\widehat{x}} = \widehat{x}\widehat{1}\widehat{x} = \widehat{x}^2$.

(iii) Soit $x \in G$. Notons $(x_n)_{n\in\mathbb{N}}$ la suite d'éléments de G définie par : $x_0 = 1$, pour tout $n \in \mathbb{N}^*$: $x_{2n} = \widehat{x_n}$, et pour tout $n \in \mathbb{N}$: $x_{2n+1} = x\widehat{x_n}$. Nous allons montrer que pour tout $n \in \mathbb{N}$: $\widehat{x}^n = \widehat{x_n}$.

Initialisation : $\widehat{x}^0 = 1 = \widehat{x_0}$.

Hérédité : Soit $n \in \mathbb{N}$. On suppose pour tout $k \in [\![0,n]\!]$: $\widehat{x}^k = \widehat{x_k}$.

— Si n est pair, disons : $n = 2p$ avec $p \in [\![0,n]\!]$: $\widehat{x}^{n+1} = \widehat{x}^{2p+1} \overset{\text{HDR}}{=} \widehat{x_p}\widehat{x}\widehat{x_p} \overset{\text{(ii)}}{=} \widehat{x\widehat{x_p}} = \widehat{x_{2p+1}} = \widehat{x_{n+1}}$.

— Si n est impair, disons : $n = 2p-1$ avec $p \in [\![1,n]\!]$, alors : $\widehat{x}^{n+1} = \left(\widehat{x}^p\right)^2 \overset{\text{HDR}}{=} \widehat{x_p}^2 \overset{\text{(ii)}}{=} \widehat{\widehat{x_p}} = \widehat{x_{n+1}}$.

Nous pouvons maintenant montrer que $\widehat{x}$ est d'ordre impair. Supposons-le d'ordre pair — par l'absurde. L'une de ses puissances est alors d'ordre 2, disons : $\widehat{x}^n = \widehat{x_n}$ avec $n \in \mathbb{N}$. Ainsi : $\widehat{\widehat{x_n}} \overset{\text{(ii)}}{=} \widehat{x_n}^2 = 1$, donc : $[t,\widehat{x_n}] = 1$, ou encore : $\widehat{x_n} \in C_G(t)$. Aussitôt : $t^{x_n} \in t^G \cap C_G(t)$, donc comme t est isolée : $t^{x_n} = t$, et enfin : $\widehat{x_n} = 1$ — alors que $\widehat{x_n}$ a été supposé d'ordre 2.

(iv) Soit $g \in G$. Nous souhaitons montrer que tout élément de G peut être écrit d'une et une seule manière sous la forme : $g = c\widehat{x}$ pour certains $c \in C_G(t)$ et $x \in G$.

D'après (iii), $\widehat{g}$ est d'ordre impair n, disons : $n = 2k-1$ avec $k \in \mathbb{N}^*$, et : $\widehat{g}^k = \widehat{g_k}$ pour un certain $g_k \in G$. Aussitôt : $t\widehat{g_k}^{-1}t\widehat{g_k} = [t,\widehat{g_k}] = \widehat{\widehat{g_k}} = \widehat{g_k}^2 = \widehat{g}^{2k} = \widehat{g} = tg^{-1}tg$, donc : $g\widehat{g_k}^{-1} \in C_G(t)$. C'est bien l'existence annoncée.

Pour l'unicité, soient $c, c' \in C_G(t)$ et $x, x' \in G$ pour lesquels : $c\widehat{x} = c'\widehat{x'}$. Aussitôt :

$$\widehat{x}^2 \overset{\text{(ii)}}{=} \widehat{\widehat{x}} = [t,\widehat{x}] = [t,c\widehat{x}] = \widehat{c\widehat{x}} = \widehat{c'\widehat{x'}} = [t,c'\widehat{x'}] = [t,\widehat{x'}] = \widehat{\widehat{x'}} \overset{\text{(ii)}}{=} \widehat{x'}^2,$$

or $\widehat{x}$ et $\widehat{x'}$ sont tous deux d'ordre impair d'après (iii), donc : $\widehat{x} = \widehat{x'}$ et enfin : $c = c'$.

(v) Soient $c', c'' \in \mathrm{C}_G(t)$. On suppose c' et c'' conjugués dans G. D'après (iv) que : $c'' = c'^{c\widehat{x}}$ pour certains $c \in \mathrm{C}_G(t)$ et $x \in G$. Aussitôt : $\widehat{x}c'' = c'^c\widehat{x}$, ou encore : $c''\widehat{x^{c''}} = c'^c\widehat{x}$, donc par unicité dans (iv) : $c'' = c'^c \in c'\mathrm{C}_G(t)$.

(vi) Soit $g \in G$. On suppose $\widehat{g}$ conjugué à un élément de $\mathrm{C}_G(t)$. Il s'agit de montrer qu'alors : $\widehat{g} = 1$. D'après (iv) : $\widehat{g} = c^{\widehat{x}}$ pour un certain $x \in G$, ou encore : $\widehat{x}\widehat{g} = c\widehat{x}$. A fortiori : $\widehat{g\widehat{x}} \overset{\text{(ii)}}{=} \widehat{x}\widehat{g}\widehat{x} = c\widehat{x}^2 \overset{\text{(ii)}}{=} c\widehat{\widehat{x}}$, donc par unicité dans (iv) : $c = 1$, donc en effet : $\widehat{g} = 1$.

(vii) Clairement : $\widehat{G} \subset \mathrm{D}(G) \leqslant \mathrm{Ker}\, V_{G\to\mathrm{C}_G(t)}$. Montrons ensuite que $\big(\mathrm{Ker}\, V_{G\to\mathrm{C}_G(t)}\big)\langle t\rangle$ est distingué dans G. Or $\mathrm{Ker}\, V_{G\to\mathrm{C}_G(t)}$ l'est déjà, et pour tout $g \in G$: $t^g = \big[g,t\big]t = \widehat{g}^{-1}t \in \big(\mathrm{Ker}\, V_{G\to\mathrm{C}_G(t)}\big)\langle t\rangle$.

(viii) Pour tous $x \in G$ et $g \in G$: $\widehat{x}^g = \big(g^{-1}tgt\big)\big(tg^{-1}x^{-1}txg\big) = \big[t,g\big]^{-1}\big[t,xg\big] = \widehat{g}^{-1}\widehat{xg}$, donc : $\widehat{x}^g \in \big\langle\widehat{G}\big\rangle$, ce qui montre bien que $\big\langle\widehat{G}\big\rangle$ est distingué dans G. ■

Nous allons maintenant établir le théorème Z^* dans trois cas particuliers par des méthodes de transfert. Les deux premières preuves, en particulier, se ressembleront beaucoup et reposent en partie sur le petit lemme suivant.

Théorème 41 **(Une situation parfaite)** Soit G un groupe. Si : $G = \mathrm{D}(G)\mathrm{Z}(G)$, alors $\mathrm{D}(G)$ est parfait, autrement dit : $\mathrm{D}^2(G) = \mathrm{D}(G)$.

Démonstration Pour tous $x, x' \in G$, disons : $x = dz$ et $x' = d'z'$ avec $d, d' \in \mathrm{D}(G)$ et $z, z' \in \mathrm{Z}(G)$: $\big[x,x'\big] = \big[d,d'\big]$, donc tout commutateur de G est un commutateur de $\mathrm{D}(G)$. On en déduit l'inclusion : $\mathrm{D}(G) \leqslant \mathrm{D}^2(G)$, et l'autre est évidente. ■

Théorème 42 **(Un premier cas particulier du théorème Z^*)** Soit G un groupe fini. On suppose que G contient une involution isolée t et que $\mathrm{C}_G(t)$ est à la fois de Hall dans G et résoluble.

(i) $\widehat{G}$ est un sous-groupe distingué de G.

(ii) G est le produit semi-direct de $\widehat{G}$ par $\mathrm{C}_G(t)$. En particulier : $G = \mathrm{O}(G)\mathrm{C}_G(t)$.

(ii) $\widehat{G}$ est abélien. A fortiori, G est résoluble.

Démonstration

(i) D'après **40** (viii), il nous suffit de montrer que $\widehat{G}$ est un sous-groupe de G.

Par récurrence, l'assertion (i) est supposée vraie de tout groupe d'ordre strictement inférieur à $|G|$ satisfaisant les mêmes hypothèses que G. Nous noterons par souci de simplicité V le transfert $V_{G\to\mathrm{C}_G(t)}$.

Nous savons d'une part que $\mathrm{C}_G(t)$ est de Hall dans G, mais d'autre part qu'il contrôle sa propre G-fusion d'après **40** (v). D'après **10** (iii) et **11** (iii), V est donc surjectif de $\mathrm{C}_G(t)$ sur $\dfrac{\mathrm{C}_G(t)}{\mathrm{D}\big(\mathrm{C}_G(t)\big)}$. En particulier, $\mathrm{C}_G(t)$ étant résoluble : $\mathrm{Ker}\, V \neq G$, et d'autre part : $G = (\mathrm{Ker}\, V)\mathrm{C}_G(t)$.

- Faisons l'hypothèse que : $(\mathrm{Ker}\, V)\langle t\rangle \neq G$ et posons : $N = (\mathrm{Ker}\, V)\langle t\rangle$, distingué dans G d'après **40** (vii). Comme le quotient $\dfrac{\mathrm{C}_G(t)}{\mathrm{C}_N(t)}$ se plonge dans $\dfrac{G}{N}$, $\big|N : \mathrm{C}_N(t)\big|$ divise $\big|G : \mathrm{C}_G(t)\big|$, donc $\mathrm{C}_N(t)$ est de Hall dans N — et bien sûr résoluble. Par ailleurs, t est une involution isolée de N. Par hypothèse de récurrence, l'ensemble $\widehat{N} = \big\{\widehat{n}\big\}_{n\in N}$ est donc un sous-groupe de N. Or : $\widehat{G} \subset \mathrm{Ker}\, V$ d'après **40** (vii), donc : $\widehat{N} = \widehat{G}$ et $\widehat{G}$ est un sous-groupe de G.
- Faisons maintenant l'hypothèse que : $(\mathrm{Ker}\, V)\langle t\rangle = G$. Comme : $\mathrm{Ker}\, V \neq G$, cela veut dire que : $t \notin \mathrm{Ker}\, V$ et $\big|G : \mathrm{Ker}\, V\big| = 2$. Or $\mathrm{Ker}\, V$ contient $\mathrm{D}\big(\mathrm{C}_G(t)\big)$, donc : $t \notin \mathrm{D}\big(\mathrm{C}_G(t)\big)$. Ensuite, comme V induit un isomorphisme de $\dfrac{G}{\mathrm{Ker}\, V}$ sur $\dfrac{\mathrm{C}_G(t)}{\mathrm{D}\big(\mathrm{C}_G(t)\big)}$: $\mathrm{C}_G(t) = \mathrm{D}\big(\mathrm{C}_G(t)\big)\langle t\rangle$, donc d'après le lemme **41** : $\mathrm{D}^2\big(\mathrm{C}_G(t)\big) = \mathrm{D}\big(\mathrm{C}_G(t)\big)$. Mais $\mathrm{C}_G(t)$ étant résoluble : $\mathrm{D}\big(\mathrm{C}_G(t)\big) = 1$, et enfin : $\mathrm{C}_G(t) = \langle t\rangle$. En particulier, d'après **40** (iv) : $\big|\widehat{G}\big| = \big|G : \mathrm{C}_G(t)\big| = \dfrac{|G|}{2} = \big|\mathrm{Ker}\, V\big|$, mais par ailleurs : $\widehat{G} \subset \mathrm{Ker}\, V$, donc $\widehat{G} = \mathrm{Ker}\, V$ est comme voulu un sous-groupe de G.

(ii) D'après le théorème **40** (iv), G est le produit semi-direct de $\widehat{G}$ par $C_G(t)$. Pour finir : $\left|\widehat{G}\right| = \left|G : C_G(t)\right|$ et $C_G(t)$ contient un 2-Sylow de G d'après **40** (i), donc $\widehat{G}$ est d'ordre impair, et comme il est distingué dans G : $\widehat{G} \leqslant O(G)$, et donc : $G = \widehat{G}C_G(t) = O(G)C_G(t)$.

(iii) Pour tous $x, y \in G$: $\widehat{x}\widehat{y} \in \widehat{G}$ d'après (i), donc : $\widehat{y}^{-1}\widehat{x}^{-1} = \left(\widehat{x}\widehat{y}\right)^{-1} = \left(\widehat{x}\widehat{y}\right)^t = \widehat{x}^{-1}\widehat{y}^{-1}$ d'après **40** (i), i.e. $\widehat{x}$ et $\widehat{y}$ commutent. Conclusion : $\widehat{G}$ est abélien. Or d'après (i), le quotient $\dfrac{G}{\widehat{G}}$ est isomorphe à $C_G(t)$ qui est résoluble, donc G lui-même est résoluble. ■

Exemple Soient $p_1, \dots, p_n$ des nombres premiers distincts supérieurs ou égaux à 5. Tout groupe d'ordre $2^3 p_1 \dots p_n$ dont les 2-Sylow sont isomorphes au groupe des quaternions Q_8 est résoluble.

Démonstration Soit G un tel groupe. On raisonne par récurrence en supposant le résultat vrai de tout groupe d'ordre strictement inférieur à $|G|$ satisfaisant les mêmes hypothèses que G. Soient $S \in \mathrm{Syl}_2(G)$. L'unique involution t de S est isolée dans G et la factorisation première de $|G|$ force $C_G(t)$ d'une part à être de Hall dans G, mais d'autre part à satisfaire les mêmes hypothèses que G.

- Supposons : $C_G(t) \neq G$. Par hypothèse de récurrence, $C_G(t)$ est alors à la fois de Hall dans G et résoluble. Le théorème **42** montre aussitôt que G est le produit semi-direct d'un groupe abélien par $C_G(t)$, donc en particulier qu'il est résoluble.
- Si au contraire : $C_G(t) = G$, l'involution t est centrale dans G et le quotient $\dfrac{G}{\langle t\rangle}$ est d'ordre $2^2 p_1 \dots p_n$, donc est résoluble d'après un exemple précédent. Par empilement, G est ainsi résoluble.

Notre deuxième cas particulier du théorème Z^* ressemble beaucoup aux théorèmes de p-nilpotence que nous avons rencontrés dans notre précédente partie sur le transfert dans un p-Sylow.

Théorème 43 **(Un deuxième cas particulier du théorème Z^*)** Soit G un groupe fini. On suppose que G contient une involution isolée t.

(i) Soit p un nombre premier qui ne divise pas $\left|G : C_G(t)\right|$. Si $C_G(t)$ est p-nilpotent, G est p-nilpotent.

(ii) En particulier, si $C_G(t)$ est 2-nilpotent, G est 2-nilpotent et : $G = O(G)C_G(t)$.

Démonstration

(i) Par récurrence, l'assertion (i) est supposée vraie de tout groupe d'ordre strictement inférieur à $|G|$ satisfaisant les mêmes hypothèses que G. Nous noterons par souci de simplicité V le transfert $V_{G\to C_G(t)}$.

Soit $P \in \mathrm{Syl}_p\big(C_G(t)\big)$, qu'on peut supposer non trivial. Par p-nilpotence de $C_G(t)$: $C_G(t) = O_{p'}\big(C_G(t)\big)P$, donc : $D(P) \leqslant D\big(C_G(t)\big) \leqslant O_{p'}\big(C_G(t)\big)D(P)$ On en déduit aisément, $O_{p'}\big(C_G(t)\big)$ étant un p'-groupe, que : $P \cap D\big(C_G(t)\big) = D(P)$.

Ensuite, $C_G(t)$ contrôle sa propre G-fusion d'après **40** (v), donc d'après **11** (iii) : $V(c) = c^{|G:C_G(t)|}\, D\big(C_G(t)\big)$ pour tout $c \in C_G(t)$. En particulier, pour tout $x \in P \cap \mathrm{Ker}\, V$: $x^{|G:C_G(t)|} \in D\big(C_G(t)\big)$, donc par hypothèse sur p : $x \in P \cap D\big(C_G(t)\big) = D(P)$. Conclusion : $P \cap \mathrm{Ker}\, V = D(P)$. Or : $P \neq 1$ donc : $D(P) \neq P$, donc $\left|G : \mathrm{Ker}\, V\right|$ est divisible par $\left|P : D(P)\right|$, donc par p.

- Faisons l'hypothèse que : $(\mathrm{Ker}\, V)\langle t\rangle = G$. Comme : $\mathrm{Ker}\, V \neq G$, cela veut dire que : $t \notin \mathrm{Ker}\, V$ et $\left|G : \mathrm{Ker}\, V\right| = \left|P : D(P)\right| = 2$, donc : $p = 2$ et $t \notin P \cap \mathrm{Ker}\, V = D(P)$. Or t centralise le 2-Sylow P, donc $P\langle t\rangle$ est un 2-sous-groupe de G, donc : $t \in P$. Ainsi : $P = D(P)\langle t\rangle$, donc d'après le lemme **41** : $D^2(P) = D(P)$, puis : $D(P) = 1$. Finalement : $G = (\mathrm{Ker}\, V)\langle t\rangle = (\mathrm{Ker}\, V)P$ avec : $P \cap \mathrm{Ker}\, V = D(P) = 1$, donc en effet G est 2-nilpotent et : $\mathrm{Ker}\, V = O_{2'}(G) = O(G)$.
- Faisons maintenant l'hypothèse que : $(\mathrm{Ker}\, V)\langle t\rangle \neq G$ et posons : $N = (\mathrm{Ker}\, V)\langle t\rangle$. Ce sous-groupe N est p-nilpotent par hypothèse de récurrence, mais il est par ailleurs distingué dans G et contient $\widehat{G}$ d'après **40** (viii). Or d'après un résultat classique : $P \cap N \in \mathrm{Syl}_p(N)$, donc on déduit de **40** (iv) que : $G = \widehat{G}C_G(t) = NC_G(t) = O_{p'}(N)(P \cap N)O_{p'}\big(C_G(t)\big)P = O_{p'}(N)O_{p'}\big(C_G(t)\big)P$. Il n'est pas dur de comprendre sur cette égalité que le sous-groupe $O_{p'}(N)O_{p'}\big(C_G(t)\big)$ est à la fois un p'-groupe et qu'il est distingué dans G, ce qui achève de montrer que G est p-nilpotent.

(ii) Simple conséquence de (i) car $\left|G : C_G(t)\right|$ est impair d'après **40** (i). Ainsi, pour tout $S \in \mathrm{Syl}_2\big(C_G(t)\big)$: $G = O(G)S = O(G)C_G(t)$. ■

Notre dernier cas particulier est plus rassurant que profond. Fondamentalement, le théorème Z^* est un théorème de non-simplicité. Le démontrer dans le cas des groupes résolubles peut dès lors paraître léger, mais c'est tout de même ce que nous allons faire. Les groupes résolubles représentent après tout une classe importante de groupes.

Théorème 44 **(Un troisième cas particulier du théorème Z^*)** Soit G un groupe fini. Si G est résoluble et contient une involution isolée t, alors : $G = O(G)C_G(t)$.

Démonstration D'après **40** (iv) et (viii), il nous suffit de montrer que $\langle \widehat{G} \rangle$ est un groupe d'ordre impair.

Par récurrence, le résultat est supposé vrai de tout groupe d'ordre strictement inférieur à $|G|$ satisfaisant les mêmes hypothèses que G. Comme G est résoluble, un résultat classique affirme que N possède un sous-groupe distingué abélien p-élémentaire pour un certain nombre premier p.

- Si : $\langle \widehat{G} \rangle \langle t \rangle \neq G$, alors comme : $\widehat{\langle \widehat{G} \rangle \langle t \rangle} = \widehat{G}$, le groupe $\langle \widehat{G} \rangle$ est d'ordre impair par hypothèse de récurrence. Nous supposerons désormais que : $\langle \widehat{G} \rangle \langle t \rangle = G$.
- Si $t \in N$: $t^G \subset N$ car N est distingué dans G. Comme N est abélien, t commute ainsi avec tous ses conjugués, donc : $t^G = t^G \cap C_G(t) = \{t\}$. Conclusion : $t \in Z(G)$, donc : $\widehat{G} = 1$, donc $\langle \widehat{G} \rangle = 1$ est d'ordre impair. Nous supposerons désormais que : $t \notin N$.
- Intéressons-nous au quotient $\frac{G}{N}$ dont Nt est une involution et montrons que Nt est isolée dans $\frac{G}{N}$. Soit $g \in G$ pour lequel : $(Nt)^{Ng} \in C_{\frac{G}{N}}(Nt)$. Aussitôt :

$$N\widehat{g} = Ntt^g = (Nt)(Nt)^{Ng} = (Nt)^{Ng}(Nt) = Nt^g t = N\widehat{g}^{-1},$$

donc : $\widehat{g}^2 \in N$, donc comme $\widehat{g}$ est d'ordre impair : $\widehat{g} = \widehat{x}^{-2}$ pour un certain $x \in G$ d'après **40** (iii) et : $\widehat{x} \in N$. Or : $\left[t, g\widehat{x}\right] = t\widehat{x}^{-1}g^{-1}tg\widehat{x} = \widehat{x}\widehat{g}\widehat{x} = 1$, donc : $tg\widehat{x} = g\widehat{x}t$, donc : $Ntg = Ngt$, et enfin : $(Nt)^{Ng} = Nt$. Comme voulu : $(Nt)^{\frac{G}{N}} \cap C_{\frac{G}{N}}(Nt) = \{Nt\}$.

Il est par ailleurs clair que pour tout $x \in G$: $\widehat{Nx} = N\widehat{x}$, donc : $\widehat{\left(\frac{G}{N}\right)} = \{N\widehat{x}\}_{x \in G} = \frac{N\widehat{G}}{N}$. Par hypothèse de récurrence, nous pouvons donc affirmer que $\left\langle \frac{N\widehat{G}}{N} \right\rangle = \frac{N\langle \widehat{G} \rangle}{N}$ est un groupe d'ordre impair.

De nouveau, deux cas se présentent.

- Tout d'abord, si p est impair, $N\langle \widehat{G} \rangle$ est d'ordre impair d'après le point précédent, donc $\langle \widehat{G} \rangle$ aussi.
- Faisons désormais l'hypothèse que : $p = 2$. Comme : $N \leqslant O_2(G)$ et comme $C_G(t)$ contient un 2-Sylow de G d'après **40** (i) : $N \leqslant C_G(t)$. Ainsi, pour tous $n \in N$ et $x \in G$: $n^{\widehat{x}} \in N \leqslant C_G(t)$ car N est distingué dans G, donc : $n^{\widehat{x}^{-1}} = \left(n^{\widehat{x}}\right)^t = n^{\widehat{x}}$, autrement dit n et $\widehat{x}^2$ commutent. On peut même dire que n et $\widehat{x}$ commutent d'après **40** (iii). Conclusion : $\langle \widehat{G} \rangle \leqslant C_G(N)$, et même : $G = \langle \widehat{G} \rangle \langle t \rangle \leqslant C_G(N)$, donc : $N \leqslant Z(G)$.

  Posons enfin : $M = N\langle \widehat{G} \rangle$. Comme $\frac{M}{N}$ est d'ordre impair : $N \in \mathrm{Syl}_2(M)$. Ensuite : $N \leqslant Z(M)$ donc : $\mathrm{Foc}_M(N) = 1$, donc $V_{M \to N}$ est surjectif de M sur N d'après **10** (iii). Il en découle d'une part que : $\langle \widehat{G} \rangle \leqslant \mathrm{Ker}\, V_{M \to N}$ d'après **40** (iii), mais aussi que : $\left|\mathrm{Ker}\, V_{M \to N}\right| = |M : N|$. Conclusion : $\langle \widehat{G} \rangle$ est d'ordre impair. ■