Salut Dude,

Tu te rappelles de nous ?... (clin clin)
En tout cas, on n'est pas prêtes de t'oublier... (clin clin)
Depuis notre dernière rencontre, on a décidé avec quelques copines d'ouvrir un site très très spécial ! (clin)
Rejoins-nous sur http://www.yenaurapourtout-le-monde.com, tu pourras voir qu'on est plutôt mignonnes !
Alors à l'avenir, pour toute commande de plâtre, béton armé, ciment hydrolique et mastic de vitrier, une seule adresse (clin clin) :
http://www.yenaurapourtout-le-monde.com !!!
Cette semaine, promotion spéciale sur le gravier "Da Costa" : Gravier Da Costa, votre béton en redemandera ! Démonstration d'utilisation ce lundi, par RADU MIHAI STANCU Da Costa, qui nous parlera

ÜBER P-GRUPPEN.

Date: Lundi 27 mai 2002
Heure: 16h00
Lieu: Salle 623
Tenue du conférencier: Tourneur-fraiseur.

Béton-man bienvenu.
Mastic-boy s'abstenir.

M.Baillif (selles de singe)
D.Cimasoni (merde de chimpanzé)

"Suis-je mieux ou moins bien entouré que George W Bush ?"
T.G.

P.S. L'enveloppe corporelle de le premier poulpor organisator étant dans l'impossibilité de participer à ce raout, elle a mandaté une marionnette en mousse pour la représenter.

ÜBER p-GRUPPEN

MIHAI-RADU “DA COSTA” STANCU

Introduction

Qui dit algèbre, dit classification et qui dit groupes finis, dit la classification des groupes finis simples. La compréhension des groupes finis simples a occupé et occupe toujours l'esprit de beaucoup d'algébristes. Leur classification a été achevée au début des années '80, mais D. Gorenstein, un des grands artisans de la preuve, a immédiatement reconnu la nécessité d'un projet de ‘révision’. Celle-ci s'avère, en effet, nécessaire car la preuve existante de la classification s'étend sur dix à quinze mille pages de journal, partagées entre quelques 500 articles tous écrits entre 1950 et le début des années '80. Les révisionnistes[1], dans le rang desquels on compte aujourd'hui R. Lyons et R. Solomon, avec une vision globale de la classification, qui permet d'aborder différemment certains points clef de la démarche mathématique, espèrent obtenir une réduction du nombre de pages nécessaires pour la preuve à trois-quatre mille. En même temps, ils sont convaincus qu'une preuve substantiellement plus courte ne peut être obtenue qu'avec des méthodes radicalement nouvelles.

Dans ce qui suit, on ne part pas à la recherche de méthodes nouvelles. On se contente d'approfondir certains aspects d'une des anciennes méthodes, qui est l'étude de la structure p-locale d'un groupe fini G, où p est un nombre premier qui divise l'ordre de G, c'est-à-dire l'étude des normalisateurs dans G des p-sous-groupes de G. Notons $O_{p'}(G)$ le plus grand sous-groupe normal de G d'ordre premier à p. On peut démontrer que les structures p-locales de G et $G/O_{p'}(G)$ sont isomorphes. Donc, la maîtrise de la structure p-locale de G fournit, tout au plus, la connaissance de $G/O_{p'}(G)$. Le théorème suivant, dû à Frobenius, montre qu'en partant de la structure p-locale, on peut avoir des informations précises sur $G/O_{p'}(G)$.

Théorème (Frobenius).
Soit G un groupe fini. Supposons que, pour tout p-sous-groupe P de G, le groupe $N_G(P)/C_G(P)$ est un p-groupe. Alors $G/O_{p'}(G)$ est un p-groupe.

[1] Dis-donc, Radu, tu cherches à nous attirer des ennuis ou quoi ? N.d.E.

Catégorie de Frobenius et contrôle de la p-fusion

Pour l'étude p-locale de G on organise les p-sous-groupes non-triviaux en une catégorie, appelée (au vu du théorème précédent) la *catégorie de Frobenius*. Cette catégorie, notée $F_p(G)$ aura donc comme objets les p-sous-groupes de G et comme morphismes, les morphismes de groupes donnés par les conjugaisons par les éléments de G. On appelle ces morphismes des p-fusions. Si R et Q sont deux p-sous-groupes de G on note $R \xrightarrow{g} Q$ le morphisme de R dans Q induit par la conjugaison par g, c'est-à-dire $x \mapsto {}^g x$, étant sous-entendu que ${}^g R \leq Q$. Une autre notation équivalente est $\mathrm{conj}(g) : R \longrightarrow Q$.

Remarque. On a bien sûr $(R \xrightarrow{g} Q) = (R \xrightarrow{h} Q)$ si et seulement si $h^{-1}g \in C_G(R)$. Par conséquent,

$$\mathrm{Hom}_{F_p(G)}(R, Q) = \{g \in G \mid {}^g R \leq Q\}/C_G(R)\,.$$

Soit P un p-sous-groupe de Sylow de G. On dit que deux sous-groupes de P *p-fusionnent* dans G s'ils sont conjugués par un élément de G. On va s'intéresser aux phénomènes de p-fusion dans G et, surtout, au problème du contrôle de la p-fusion dans G, c'est à dire trouver un sous-groupe H de G qui réalise par conjugaison à l'intérieur de H toutes les p-fusions données par G.

Définition. *Soit H un sous-groupe de G. On dit que H contrôle la p-fusion, ou que H est un sous-groupe de p-contrôle, si $p \nmid |G : H|$ et pour tout p-sous-groupe R de H et tout $g \in G$ tel que ${}^g R \leq H$, on a $g = hc$ avec $h \in H$ et $c \in C_G(R)$.*

Autrement dit, le contrôle de la p-fusion par un sous-groupe H de G est équivalent au fait que H contient un p-sous-groupe de Sylow de G et que tout morphisme par conjugaison par un élément de G entre des p-sous-groupes de H peut être donné par la conjugaison par un élément de H.

Exemple. Voici deux exemples de contrôle de fusion.

1) (Burnside) Si un p-sous-groupe de Sylow P de G est abélien, alors $N_G(P)$ contrôle la p-fusion dans G.

Preuve. Evidemment, p ne divise pas $|G : N_G(P)|$. Soient Q un p-sous-groupe de $N_G(P)$ et $g \in G$ tels que ${}^g Q \leq N_G(P)$. Comme P est normal dans $N_G(P)$, on a que P est l'unique p-sous-groupe de Sylow de $N_G(P)$ et donc Q, ${}^g Q \leq P$. De plus P est abélien et, comme $Q \leq {}^{g^{-1}}P$, on a P, ${}^{g^{-1}}P \leq C_G(Q)$. Maintenant P et ${}^{g^{-1}}P$ sont des p-sous-groupes de Sylow de $C_G(Q)$, donc ils sont conjugués par un élément c de $C_G(Q)$. Autrement dit, ${}^c P = {}^{g^{-1}}P$ ce qui implique qu'il existe $h \in N_G(P)$, tel que $gc = h$. Ceci nous donne $g = hc^{-1}$, avec $h \in N_G(P)$ et $c \in C_G(Q)$. Donc $N_G(P)$ contrôle la p-fusion dans G. $\square$

2) Si $p \nmid n$ alors S_{n-1} contrôle la p-fusion dans S_n.

Preuve. On fixe $S_{n-1} := \{\gamma \in S_n | \gamma(1) = 1\}$. Comme $|S_n : S_{n-1}| = n$, on a par hypothèse que $p \nmid |S_n : S_{n-1}|$. Soient $Q \leq S_{n-1}$ et $\sigma \in S_n$ tels que ${}^\sigma Q \leq S_{n-1}$. On construit explicitement une permutation $\tau \in S_{n-1}$ telle que ${}^{\tau}\beta = {}^{\sigma}\beta$, pour tout $\beta \in Q$. Posons

$$\begin{aligned} \tau(1) &:= 1\,, \\ \tau(\sigma^{-1}(1)) &:= \sigma(1) \text{ et} \\ \tau(i) &:= \sigma(i) \text{ pour } i \neq 1, \sigma^{-1}(1)\,. \end{aligned}$$

On a clairement que $\tau \in S_{n-1}$ car $\tau(1) = 1$. Vérifions que ${}^{\tau}\beta = {}^{\sigma}\beta$, pour tout $\beta \in Q$. Soit $\beta \in Q$.

$$\begin{aligned} \tau\beta\tau^{-1}(1) = 1 \text{ car } \beta \in Q \leq S_{n-1} \qquad &\text{et} \qquad \sigma\beta\sigma^{-1}(1) = 1 \text{ car } {}^{\sigma}\beta \in {}^{\sigma}Q \leq S_{n-1}\,; \\ \tau\beta\tau^{-1}(\sigma(1)) = \tau\beta\sigma^{-1}(1) = \tau\sigma^{-1}(1) = \sigma(1) \qquad &\text{et} \qquad \sigma\beta\sigma^{-1}\sigma(1) = \sigma\beta(1) = \sigma(1)\,; \end{aligned}$$

pour $i \neq 1, \sigma(1)$ on a $\tau^{-1}(i) = \sigma^{-1}(i)$ donc $\beta\tau^{-1}(i) = \beta\sigma^{-1}(i) \neq 1, \sigma^{-1}(1)$ ce qui entraîne

$$\tau\beta\tau^{-1}(i) = \sigma\beta\sigma^{-1}(i)\,.$$

Donc ${}^{\tau}\beta = {}^{\sigma}\beta$. Il s'ensuit que $\sigma = \tau\chi$ avec $\chi \in C_{S_n}(Q)$. Donc S_{n-1} contrôle la p-fusion dans S_n. □

Théorème 'essentiel' d'Alperin

Dans ce qui suit, on va donner quelques définitions qui nous seront utiles par la suite.

DÉFINITION. *Soit $\mathcal{S}_p(G)$ l'ensemble des p-sous-groupes non-triviaux de G ordonné par l'inclusion. C'est un poset, c'est-à-dire un ensemble partiellement ordonné pour l'inclusion. On dit que $Q, R \in \mathcal{S}_p(G)$ sont liés s'il existe une suite $S_i \in \mathcal{S}_p(G)$, $i = 1 \ldots n$ avec $Q \leq S_1 \geq S_2 \leq S_3 \geq \cdots \geq S_{n-1} \leq S_n \geq R$. Ceci définit une relation d'équivalence sur $\mathcal{S}_p(G)$. Les classes d'équivalence sont appelées les composantes connexes. On dit que $\mathcal{S}_p(G)$ est connexe s'il y a une seule composante connexe.*

DÉFINITION. *On dit que Q est un p-sous-groupe essentiel de G si son centre $Z(Q)$ est un p-sous-groupe de Sylow de $C_G(Q)$ et $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ est non-connexe.*

Le phénomène de fusion est de nature locale. Le théorème suivant, dû à ALPERIN [1] en 1967 et raffiné par PUIG [10] en 1976, en est la preuve.

THÉORÈME (ALPERIN).
Tout morphisme de la catégorie $F_p(G)_{\leq P}$ peut être décomposé comme une suite de morphismes de deux types:

i) Conjugaison par un élément de $N_G(E)$, où E est un p-sous-groupe essentiel de G contenu dans P et complètement normalisé dans P.

ii) Conjugaison par un élément de $N_G(P)$,

suivies d'une inclusion. Plus précisément si Q, ${}^{g}Q$ sont des sous-groupes de P alors il existe une décomposition $g = g_1 g_2 \ldots g_n g_{n+1} c$, où *a)* $g_i \in N_G(E_i)$, *où* E_i *est un* p*-sous-groupe essentiel de* G*, contenu dans* P *et complètement normalisé dans* P*, pour tout* $i = 1, \ldots, n$,

b) $g_{n+1} \in N_G(P)$,

c) $c \in C_G(Q)$.

La preuve est donnée dans [12] dans le même cadre général des groupes pointés locaux. En remplaçant groupe pointé local par p-sous-groupe, $\mathcal{L}_G(b)_{\leq P}$ par $F_p(G)_{\leq P}$ et groupe de défaut par p-sous-groupe de Sylow, on spécialise cette preuve à notre cas.

Les notions de p-contrôle de fusion et p-sous-groupe essentiel sont fortement liées. Par le théorème précédent, si G ne contient pas de p-sous-groupes essentiels alors le normalisateur de P dans G contrôle la p-fusion. En fait, comme le montre le résultat suivant, la réciproque est aussi vraie.

Proposition. *Le normalisateur* $N_G(P)$ *contrôle la* p*-fusion si et seulement s'il n'y a pas de* p*-sous-groupes essentiels dans* G.

Preuve. Clairement, par le théorème d'Alperin, la condition est suffisante. Prouvons le fait qu'elle est aussi nécessaire. Soit Q un p-sous-groupe centrique de G. Sans restreindre la généralité on peut supposer que Q est un sous-groupe de P. En fait, Q est sous-groupe de tout p-sous-groupe de Sylow de $N_G(Q)$. Soit $T := N_P(Q)$ et R un p-sous-groupe de Sylow de $N_G(Q)$ qui contient T. Un autre p-sous-groupe de Sylow R', contenu dans $N_G(Q)$, est conjugué à R par un élément $h \in N_G(Q)$. Comme $Q = {}^hQ < N_G(P)$, la conjugaison par h est un morphisme dans $F_p(N_G(P))$. Par le fait que $N_G(P)$ contrôle la p-fusion dans G, on a $h = gc$ avec $g \in N_G(P)$ et $c \in C_G(Q)$. Ainsi $h, c \in N_G(Q)$, donc $g = hc^{-1} \in N_G(P) \cap N_G(Q) \subset N_G(T)$. Comme le normalisateur grossit dans un p-groupe, Q est un sous-groupe propre de T et $C_P(Q) \leq Q$ (Q est centrique) l'image $\overline{T}$ de T dans $N_G(Q)/Q$ est un groupe non trivial. Donc, les images de R et ${}^gR$ dans $N_G(Q)/Q$ sont connectées par $\overline{T}$. D'autre part, on peut passer de ${}^hR$ à ${}^gR$ en utilisant la conjugaison par $c \in C_G(Q)$. Ceci implique que $C_G(Q)$ agit transitivement sur les composantes connexes de $\mathcal{S}_p(N_G(Q)/Q)$ et ainsi Q n'est pas un p-sous-groupe essentiel de G. □

Y a-t-il des p-sous-groupes essentiels?

Concernant le groupe d'automorphismes d'un p-groupe Q, Martin [9] a démontré que, pour presque tout p-groupe Q, le groupe des automorphismes $\mathrm{Aut}(Q)$ est un p-groupe. D'autre part, Gorenstein, Lyons [8] et Aschbacher [2] ont trouvé la liste complète des groupes finis ayant un sous-groupe fortement p-plongé. Il est vrai que le fait que la liste est complète se base entièrement sur la classification des groupes finis simples.

Ceci nous pousse, plutôt, à chercher des familles de p-groupes qui ne peuvent jamais être des p-sous-groupes essentiels. Les premiers exemples pour $p = 2$ sont les groupes des quaternions, les groupes diédraux et les groupes semi-diédraux.

Exemple. Les groupes d'automorphismes des groupes des quaternions Q_{2^m}, pour $m > 3$, des groupes diédraux D_{2^n}, pour $n > 2$ et des groupes semi-diédraux SD_{2^s}, pour $s > 2$ sont des 2-groupes. En effet, en étudiant les images des générateurs par un automorphisme quelconque, on obtient $|\mathrm{Aut}(Q_{2^m})| = 2^{2m-3}$, $|\mathrm{Aut}(D_{2^n})| = 2^{2n-3}$ et $|\mathrm{Aut}(SD_{2^s})| = 2^{2s-4}$, pour $m > 3$, $n > 2$ et $s > 2$. Donc, si Q est un p-groupe d'un des trois types plus haut, pour tout $X \leq \mathrm{Out}(Q)$ on a que $\mathcal{S}_p(X)$ n'a qu'une seule composante connexe, donc il est connexe. Un tel p-groupe Q ne peut pas être réalisé comme p-sous-groupe essentiel d'un groupe G car $N_G(Q)/QC_G(Q)$ est un sous-groupe de $\mathrm{Out}(Q)$.

Dans ce qui suit, on donne une condition suffisante pour qu'un p-groupe ne puisse pas être réalisé comme p-sous-groupe essentiel, pour p impair. Pour ceci, on a besoin de quelques propriétés du sous-groupe de Frattini d'un p-groupe.

Définition. *Soit Q un p-groupe. Le sous-groupe de Frattini de Q, noté $\Phi(Q)$, est le sous-groupe engendré par les commutateurs et les puissances p-ièmes.*

Le sous-groupe de Frattini de Q est caractéristique dans Q. Le quotient de Q par $\Phi(Q)$ est un p-groupe abélien (car on passe au quotient par les commutateurs) élémentaire (car on passe au quotient par les puissances p-ièmes) de rang n (où n est le cardinal minimal d'un système de générateurs de Q). Donc on peut regarder $Q/\Phi(Q)$ comme un espace vectoriel de dimension n sur le corps $\mathbb{F}_p$. Par conséquent, $\mathrm{Aut}(Q/\Phi(Q))$ peut être interprété comme le groupe $\mathrm{GL}(n, \mathbb{F}_p)$ des matrices inversibles de dimension n, à coefficients dans $\mathbb{F}_p$. On a la propriété suivante.

Proposition. *Soit* $\phi : \mathrm{Aut}(Q) \longrightarrow \mathrm{Aut}(Q/\Phi(Q))$ *l'application canonique induite par la projection* $Q \longrightarrow Q/\Phi(Q)$. *Alors* $\mathrm{Ker}\phi$ *est un p-groupe.*

Preuve. Un résultat de Burnside, dont une preuve se trouve dans le livre de Gorenstein [7, Thm. 5.1.4], affirme que tout p'-automorphisme de Q qui induit l'identité sur $Q/\Phi(Q)$ est, en fait, l'identité sur Q. Donc $\mathrm{Ker}(\phi)$ ne contient pas de p'-éléments, ce qui entraîne que $\mathrm{Ker}(\phi)$ est un p-groupe. □

Voici quelques rappels sur le sous-groupe des matrices triangulaires inférieures dans $\mathrm{GL}(n, \mathbb{F}_p)$.

Les matrices triangulaires inférieures sont de la forme $B := \left\{ \begin{pmatrix} * & 0 & \dots & 0 \\ * & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & * \end{pmatrix} \right\}$; le nombre d'éléments de B est $\#B = p^{\frac{n(n-1)}{2}}(p-1)^n$. Donc $P := \left\{ \begin{pmatrix} 1 & 0 & \dots & 0 \\ * & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & 1 \end{pmatrix} \right\}$, qui a $p^{\frac{n(n-1)}{2}}$ éléments, est un p-sous-groupe de Sylow de B. Il est unique car c'est un sous-groupe normal de B.

Soient G un groupe, $H, N \lhd G$ et $K := G/N$. Si P est l'unique p-sous-groupe de Sylow de G, alors $P \cap H$ est l'unique p-sous-groupe de Sylow de H et $P/(P \cap N)$ est l'unique p-sous-groupe de Sylow de K. Si N est un p-groupe on a une bijection entre les p-sous-groupes de Sylow de G et de K.

La proposition précédente nous aide à trouver des informations sur $\mathrm{Aut}(Q)$, à partir de l'image de ϕ, comme l'indique le lemme suivant.

Lemme. *Soient p un nombre premier, Q un p-groupe, $\Phi(Q)$ son sous-groupe de Frattini et n le rang du groupe abélien élémentaire $Q/\Phi(Q)$. Supposons que l'image du morphisme canonique $\phi : \mathrm{Aut}(Q) \longrightarrow \mathrm{Aut}(Q/\Phi(Q))$ induite par la projection canonique est isomorphe à un sous-groupe du groupe multiplicatif B des matrices inversibles triangulaires inférieures, de dimension n, à coefficients dans $\mathbf{F_p}$. Alors Q ne peut pas être réalisé comme p-sous-groupe essentiel dans un groupe fini G.*

Preuve. On note $\mathrm{Im}\phi$ l'image et $\mathrm{Ker}\phi$ le noyau du morphisme ϕ. On a que $\mathrm{Im}\phi$ est isomorphe à un sous-groupe de B, donc il a un unique p-sous-groupe de Sylow. Comme $\mathrm{Im}\phi \simeq \mathrm{Aut}(Q)/\mathrm{Ker}\phi$ et $\mathrm{Ker}\phi$ est un p-groupe, $\mathrm{Aut}(Q)$ a aussi un unique p-sous-groupe de Sylow et il en est de même pour $\mathrm{Out}(Q)$, car il est le quotient de $\mathrm{Aut}(Q)$ par le groupe des automorphismes intérieurs de Q, qui est un p-groupe. D'autre part, $N_G(Q)/QC_G(Q)$ est un sous-groupe de $\mathrm{Out}(Q)$ donc il a un unique p-sous-groupe de Sylow. Ainsi $\mathcal{S}_p(N_G(Q)/QC_G(Q))$ est connexe et Q ne peut jamais être réalisé comme p-sous-groupe essentiel dans un groupe fini G. □

On va conclure avec une application du lemme précedent :

Proposition. *Soient p un nombre premier et $\alpha_1 \neq \alpha_2$ deux nombres entiers positifs. Alors $Q := C_{p_1^\alpha} \times C_{p_2^\alpha}$ ne peut pas être réalisé comme un p-sous-groupe essentiel d'un groupe G.*

Preuve. Soient x et y deux générateurs de Q d'ordres p_1^α, respectivement p_2^α et σ un automorphisme de Q. On a $\sigma(x) = x^a y^b$ et $\sigma(y) = x^c y^d$. Par le lemme précédent, une condition suffisante pour que Q ne puisse pas être réalisé comme p-sous-groupe essentiel est que l'image du groupe d'automorphismes de Q dans $\mathrm{Aut}(Q/\Phi(Q))$ soit plongée dans le groupe des matrices triangulaires inférieures. Donc il suffit de montrer que, pour tout $\sigma \in \mathrm{Aut}(Q)$, comme avant, on a que p divise b ou p divise c.

Supposons, sans restreindre la généralité, que $\alpha_1 > \alpha_2$. Maintenant, l'ordre de $\sigma(y)$ est le même que l'ordre de y, donc égal à p_2^α. Ainsi $\sigma(y)^{p_2^\alpha} = 1$. Comme $y^{p_2^\alpha} = 1$, on en déduit que $x^{cp_2^\alpha} = 1$. Ceci implique que p divise c car l'ordre de x est plus grand que p_2^α. □

Avec des méthodes de même type on arrive à démontrer que d'autres familles de groupes comme par exemple les p-groupes métacycliques, pour p impair, ne peuvent pas être réalisés comme p-sous-groupes essentiels dans un groupe fini G.

References

[1] J. Alperin, Sylow intersections and fusion. *J. Algebra 6* (1967), pp. 222–241.

[2] M. Aschbacher, Simple connectivity on p-group complexes. *Israel J. of Math. 83* nos. 1–3 (1993) pp. 1–43.

[3] W. Burnside, *Theory of groups of finite order.* Cambridge Univ. Press, London 1897.

[4] J. A. Dieudonné, *La géométrie des groupes classiques.* Springer-Verlag, Berlin, third edition, 1971.

[5] J. Dietz, Automorphisms of p-groups, given as cyclic-by-elementary abelian central extension. *J. Algebra 242* (2001), pp. 417-432.

[6] D. M. Goldschmidt, A conjugation family for finite groups. *J. Algebra 16* (1970), pp. 138–142.

[7] D. Gorenstein, *Finite groups.* Harper's Series in Modern Math. U.S.A, 1968.

[8] D. Gorenstein et R. Lyons, The local structure of finite groups of characteristic 2 type. *Mem. Amer. Math. Soc. 42* no. 276 (1983).

[9] U. Martin, Allmost all p-groups have automorphism group a p-group. *Bull. Amer. Math. Soc (N.S.) 15* (1986), no. 1, pp. 78–82.

[10] L. Puig, Structure locale dans les groupes finis. *Bul. Soc. Math. France*, Mémoire no. 47, PH thesis, 1976.

[11] M. Suzuki, *Group Theory I*, Springer-Verlag, 1982

[12] J. Thévenaz, *G-Algebras et Modular Representation Theory.* Oxford Science Publications, 1995.