ANNALES SCIENTIFIQUES
DE L'UNIVERSITÉ DE CLERMONT-FERRAND 2
Série Mathématiques

RAFFAELE SCAPELLATO
LIBERO VERARDI

Sur les ensembles générateurs minimaux d'un groupe fini

Annales scientifiques de l'Université de Clermont-Ferrand 2, tome 95, série *Mathématiques*, n° 26 (1990), p. 51-60

<http://www.numdam.org/item?id=ASCFM_1990__95_26_51_0>

Ann. Sci. Univ. "Blaise Pascal", Clermont II, Sér. Math., Fasc. 26eme, pp. 51-60

Sur les ensembles générateurs minimaux d'un groupe fini

par

RAFFAELE SCAPELLATO (*)

Dipartimento di Matematica,
Università di Parma, Via d'Azeglio 85, 43100 PARMA

LIBERO VERARDI (*)[1]

Dipartimento di Matematica,
Piazza Porta S. Donato 5, 40127 BOLOGNA

I - Introduction

Soit g un groupe fini. Considérons les propriétés suivantes :

(M1') Les ensembles générateurs minimaux (ou bases) de G ont tous le même cardinal ;

(M1") Si X et Y sont deux ensembles générateurs minimaux de G et si $|X| = |Y|$, pour tout $x \in X$ il existe $y \in Y \setminus \{x\}$ tel que $(X \setminus \{x\}) \cup \{y\}$ soit encore un ensemble générateur minimal de G.

Nous disons **indépendant** tout sous-ensemble X de G tel que pour tout $x \in X$, $< X \setminus \{x\}, \phi(G) > \neq < X, \phi(G) >$ (où $\phi(G)$ est le sous-groupe de Frattini de G). Introduisons la propriété suivante :

(M2) Tout sous-ensemble indépendant X de G est contenu dans une base de G.

1. (*) Lavoro parzialmente finanziato su fondi M P I

Nous appelons **matroïdal** un groupe fini jouissant des propriétés (M1') , (M1") et (M2) . Le théorème des bases de Burnside (ou mieux un complément de ce résultat) peut être énoncé en disant que tout p-groupe fini est matroïdal (c.f. aussi [2] et [8]) .

Nous avons donné dans [9] une caractérisation et une construction des groupes finis matroïdaux . L'un de nos résultats [9, Théorème 1.2] dit que si G est un groupe matroïdal avec $\phi(G) = 1$, alors G satisfait aux propriétés suivantes (où $\delta(H)$ est le **rang** de H) :

(L1) Pour tout sous-groupe H de G et pour tout sous-ensemble indépendant X de H on a : $|X| \leq \delta(H)$;

(L2) Pour tout sous-groupe propre H de G on a : $\delta(H) < \delta(G)$.

(Ce résultat dit aussi que toutes les bases des sous-groupes H ont le même cardinal, mais ceci est une conséquence de (L1)).

Le présent travail est consacré à ces propriétés ; il aboutira au résultat suivant :

Théorème :

Soit G *un groupe fini avec* $\phi(G) = 1$.

Alors : G *est matroïdal* <=====> G *vérifie* (L1) et (L2) .

Les propriétés (M1') , (M1"), (M2) , (L1) et (L2) peuvent être considérées dans un contexte plus général que celui de la théorie des groupes. Soit en effet A une structure algébrique (ou algèbre : c.f. [5]) finie. L'intersection $\phi(A)$ des sous-algèbres maximales de A est encore l'ensemble des "non-générateurs" de A (la preuve est la même que pour les groupes) .

On peut remarquer, à ce propos , que :

- d'une part, la preuve de l'implication " =====> " est obtenue dans [9 , Théorème 1.2] avec des considérations d'algèbre universelle ; elle est donc valable pour n'importe quelle algèbre ;

- et d'autre part, l'implication " $<=====$ " est prouvée dans le présent travail par une démonstration plus longue et complexe, qui utilise des résultats de théorie des groupes (soit [3] , [7] et [9]).

Il est ainsi naturel de se demander si ce Théorème peut être généralisé à n'importe quelle algèbre. Dans le troisième paragraphe nous donnerons une réponse négative.

II - Preuve du Théorème

Dans le présent paragraphe on notera G **un groupe fini, avec** $\phi(G) = 1$ **, qui satisfait aux conditions (L1) et (L2)** . On notera $F(G)$ le sous-groupe de Fitting de G.

Le résultat suivant concerne les groupes vérifiant (L2) .

Lemme 2.1. :

Si A *est un sous-groupe normal, maximal et abélien élémentaire de* G, *alors tout sous-groupe* K *de* A *est normal dans* G.

Preuve :

Soit $y \in G \setminus A$. Il s'agit de prouver que $y \in N_G(K)$.

Procédant par l'absurde, soit $K^y \neq K$. Soit $x_1, \ldots, x_n$ une base de A , telle que $K = < x_1, \ldots, x_i >$ et $x_{i+1} \in K^y \setminus K$, où $i+1 \leq n$.

Le groupe $M = < x_1, \ldots x_i , y, x_{1+2}, \ldots, x_n >$ contient K^y, donc $x_{i+1} \in M$. Ainsi A est un sous-groupe propre de M, ce qui implique $M = G$. Il s'ensuit que $\delta(G) \leq n$. Mais ceci est contradictoire avec (L2), car n est le rang du sous-groupe A.

Par conséquent $y \in N_G(K)$, donc K est normal dans G.

Les preuves des deux lemmes suivants sont similaires à celles de [9, Lemme 2.1 et Lemme 2.4]. Elles ne sont placées ici que pour rendre ce travail complet.

Lemme 2.2 :

L'ordre de tout élément de G *est une puissance d'un nombre premier* .

Preuve :

Procédant par l'absurde, soit x un élément de G d'ordre pq (p, q premiers différents). Soient $y, z \in \langle x \rangle$, tels que $x = yz$, $o(y) = p$, $o(z) = q$. L'ensemble $\{y, z\}$ est indépendant, mais $\delta(\langle x \rangle) = 1$. Ceci contredit (L1).

Lemme 2.3. :

G est résoluble.

Preuve :

Procédons par l'absurde. L'ordre de tout élément de G est une puissance d'un nombre premier (Lemme 2.2), donc d'après un résultat de Brandl [3] (l'auteur nous a prévenu que (iii) avait été oublié dans [3]) on a l'un des trois cas suivants :

(i) G est simple, donc engendré par deux éléments ([1, Théorème B]). En vertu de (L2) tous ses sous-groupes propres sont cycliques, ainsi ([6, 2.8 , page 420]) G est un super-soluble, ce qui est contradictoire.

(ii) G possède un 2-sous-groupe normal et abélien élémentaire P, tel que G/P soit simple. Si $N = \langle x,y \rangle \cap P$, où $x \in P$ et y d'ordre premier $q \geq 5$, alors N est abélien élémentaire et normal dans $\langle x,y \rangle$. Comme y agit sur $N \setminus \{1\}$ sans point fixe, $|N| \equiv 1$ (modulo q). Il s'ensuit $|N| \geq 8$ car $q \geq 5$. Ainsi il existe dans $\langle x,y \rangle$ un ensemble indépendant de cardinal 3. Ceci contredit (L1).

(iii) G est isomorphe à M_{10} (le stabilisateur d'un point dans le groupe de Mathieu M_{11}. Ainsi G contient un sous-groupe maximal isomorphe au groupe alterné $Alt(6)$. On a $\delta(Alt(6)) = 2$, mais $\{(123), (124), (125)\}$ est un sous-ensemble indépendant de $Alt(6)$. Ceci contredit (L1).

Grâce au Lemme 2.2. l'ordre de tout élément de G est une puissance d'un nombre premier. Comme G est aussi résoluble (Lemme 2.3), il découle de [7, Théorème 1] qu'il existe deux nombres premiers p,q tels que $H = G/F(G)$ **satisfait l'une des conditions suivantes** :

(1) L'ordre de H est $p^a q^b$, où $a \geq 1$, $b \geq 1$, $q \equiv 1$ modulo p^a, et ses sous-groupes de Sylow sont cycliques.

(2) L'ordre de H est q^b, où $b \geq 1$ et H est cyclique ou un groupe quaternionien généralisé.

On remarque que $F(G)$ est abélien élémentaire, car $\phi(G) = 1$.

Lemme 2.4 :

G *ne vérifie pas* (1).

Preuve :

Procédons par l'absurde. Ainsi, en particulier, q est plus grand que p.

Soit y un élément de G, où $o(y) = q$, soit $M = \langle F(G), y \rangle$, soit $x \in F(G) \setminus \{1\}$. Si l'ordre de $\langle x,y \rangle$ est pq, ce groupe n'est pas abélien, sinon $o(xy)$ serait égal à pq. Or $\langle x \rangle = \langle x,y \rangle \cap F(G)$ est normal dans $\langle x,y \rangle$, donc $q < p$, ce qui est absurde. Il s'ensuit que l'ordre de $\langle x,y \rangle$ est plus grand que pq.

Si l'ordre de $\langle x,y \rangle$ est plus grand que $p^2 q$, alors celui de $\langle x,y \rangle \cap F(G)$ est plus grand que p^2, car $F(G)$ est le seul p-sous-groupe de Sylow de M. Alors il existe un sous-ensemble indépendant de $\langle x,y \rangle$, de cardinal 3. Ceci viole (L1). L'ordre de $\langle x,y \rangle$ est donc $p^2 q$. Or q est un diviseur de $p+1$, nombre des p-sous-groupes cycliques de $\langle x,y \rangle$, (en effet, le p-sous-groupe de Sylow de ce groupe est contenu dans $F(G)$, donc abélien élémentaire). Puisque q est congruent à 1 modulo p^a, nous avons $q = p+1$. Donc $p = 2$, $q = 3$, et $a = 1$. Ainsi l'ordre de $\langle x,y \rangle$ est 12.

Montrons que $F(G)$ est contenu dans $\langle x,y \rangle$. Supposons, par contradiction, qu'il existe $x' \in F(G) \setminus \langle x,y \rangle$. Par le même argument utilisé par rapport à x, l'ordre de $\langle x',y \rangle$ est 12. Soient $L = \langle x,y \rangle \cap F(G)$ et $L' = \langle x',y \rangle \cap F(G)$. Les groupes L, L' sont normalisés par y, donc $L \cap L'$ est aussi normalisé par y. Ce groupe n'est pas cyclique. Par conséquent $L \cap L' = 1$ car L, L' sont différents.

Le groupe $\langle x,x',y \rangle = L\,L' \langle y \rangle$ contient $L\,L'$, qui est abélien élémentaire d'ordre 2^4. Ceci contredit (L1). Par conséquent, $F(G)$ est contenu dans $\langle x,y \rangle$. Il s'ensuit que $M = \langle x,y \rangle$. Il s'agit d'un groupe d'ordre 12, évidemment isomorphe à Alt(4).

Or $G/F(G)$ est d'ordre $2^a 3^b$ (nous avons déjà prouvé que $a = 1$), donc il y a un 3-sous-groupe de Sylow normal. Ainsi G possède un sous-groupe N d'index 2, qui contient $F(G)$.

Soit Q un 3-sous-groupe de Sylow de G. Il est isomorphe à un 3-sous-groupe de Sylow de $G/F(G)$, car $Q \cap F(G) = 1$. Donc Q est cyclique.

Soit $z \in G \setminus N$, soit y' un générateur de Q. Il existe une puissance y de y' qui appartient à M. Nous avons $z^2 \in N$ donc $z^2 \in F(G)$. Si z^2 est différent de 1, alors $M = < y, z^2 >$, ce qui entraîne $N = < y', z^2 >$, ainsi $G = < y', z >$. Ceci contredit (L1). Par conséquent, tous les éléments de $G \setminus N$ ont pour ordre 2. Les 2-sous-groupes de Sylow de G sont nécessairement abéliens élémentaires, et chacun d'eux est d'ordre 8. Donc G possède des sous-groupes propres de rang 3. Mais si $x \in F(G)$ et y', z sont comme ci-dessus, nous avons $G = < x, y', z >$, ce qui contredit (L2).

Lemme 2.5 :

Si G *est résoluble, mais non abélien élémentaire, alors il existe deux nombres premiers* p,q (*où* $p \equiv 1$ modulo q) *tels que* $|G : F(G)| = q$. *En outre,* $F(G)$ *est abélien élémentaire et tout sous-groupe de* $F(G)$ *est normal dans* G.

Preuve :

En vertu du Lemme 2.4, G satisfait à (2). Comme p et q sont différents, un q-sous-groupe de Sylow Q de G est disjoint de $F(G)$ et isomorphe à H : ainsi Q est cyclique ou un groupe quaternionien généralisé.

Montrons que les q-sous-groupes de Sylow de G sont deux à deux à intersection triviale. Soient Q_1 et Q_2 des q-sous-groupes de Sylow distincts de G, soient $x_1 \in Q_1 \setminus Q_2$ et $x_2 \in Q_2 \setminus Q_1$. Si $Q_1 \cap Q_2 \neq 1$, il existe dans cette intersection un élément y d'ordre q. Alors y commute avec tout élément de Q_1 et de Q_2, ainsi $y \in Z(< x_1, x_2 >)$. Mais le groupe $< x_1, x_2 >$ a une intersection non-vide avec $F(G)$, donc y commute avec un élément d'ordre p, ce qui est une contradiction (à cause de (L1)).

Montrons, par l'absurde, que $N_G(Q) = Q$ **pour tout q-sous-groupe de Sylow Q de G.** Si $x \in F(G) \cap N_G(Q) \setminus \{1\}$, on a $x \in N_G(< y >)$, où $o(y) = q$, $y \in Q$. Or $< x > = < x, y > \cap F(G)$, donc $< x >$ est normal dans $< x, y >$; mais $< y >$ aussi est normal dans $< x, y >$, ainsi $< x, y >$ est cyclique d'ordre pq, ce qui est contradictoire.

Par conséquent l'ordre de $F(G)$ est égal au nombre des conugués de Q. **Soit E l'ensemble des éléments de G d'ordre q et soit $k = < E >$.**

Si $z \in E$, l'ensemble $\{g z g^{-1} z^{-1} \mid g \in F(G)\}$ a pour cardinal $|F(G)|$ et il est contenu dans $F(G)$, donc il est égal à $F(G)$.
En outre, il est clair que $\{g z g^{-1} z^{-1} \mid g \in F(G)\}$ est contenu dans $< E >$. Ceci entraîne $F(G) \leq K$.

Prouvons que $G = K$. Procédons par l'absurde, supposons K strictement contenu dans G ; ainsi les q-sous-groupes de Sylow de G sont d'ordre plus grand que q .
Soit X une base de K , où $X \leq E$. Pour tout $x \in X$ nous pouvons fixer un élément y de G , d'ordre égal à l'exposant des q-sous-groupes de Sylow de G, tel que $x \in < y >$. Soit Y l'ensemble de ces éléments y . Nous avons $|Y| = |X|$, et K est contenu strictement dans $< Y >$.
Soit Q un q-sous-groupe de Sylow de G . Si Q était cyclique, nous aurions $G = < Y >$ et $\delta(G) \leq |Y| = \delta(K)$, ce qui contredirait (L2) . Donc Q est un groupe quaternionien généralisé , $q = 2$ et $M = < Y >$ est un sous-groupe maximal de G.
Soit $y \in Y$, soit Q un 2-sous-groupe de Sylow de G , tel que $y \in Q$. Soit $x \in F(G) \setminus \{1\}$; si $|Y|$ est plus grand que 2, nous pouvons supposer que $x \in F(G) \cap Y \setminus \{y\} >$. Soit z l'élément d'ordre 2 de Q, soit $Q_1 = x^{-1} Q x$, soit $y_1 = x^{-1} y x$, soit $z_1 \in Q_1 \setminus < y_1 >$, où $o(y_1) = o(z_1)$. Comme $Q \cap Q_1$ est trivial, z_1 est différent de y.
Les ensembles Y et $Y_1 = (Y \cup \{z_1\}) \setminus \{y\}$ ont le même cardinal.
En outre $Q \leq < Y_1 >$, car $y_1, z_1 \in Y_1$.
Si $|Y| \geq 3$ alors $x \in < Y \setminus \{y\} >$, donc $y = x y_1 x^{-1} \in < Y_1 >$. Il s'ensuit que $Y \leq < Y_1 >$.
Ainsi M est contenu strictement dans $< Y_1 >$, et $< Y_1 > = G$. Mais alors $\delta(G) \leq \delta(K)$, ce qui contredit (L2).
Par conséquent $|Y| = 2$. Comme $\delta(M) = 2$, l'ordre de $F(G)$ est au plus p^2 . Or l'ordre de K est $2p^2$, et tout élément d'ordre 2 agit sur $F(G)$ comme l'inversion $x \dashrightarrow x^{-1}$ (un automorphisme d'ordre 2 sans point fixe doit être de cette forme, c.f. [4 , page 334]) .
Alors, si $\{x_1, x_2\}$ est une base de $F(G)$, nous avons $K = < x_1, x_2, y >$ où y est un élément d'ordre 2. Il est clair que l'ensemble $\{x_1, x_2, y\}$ est indépendant, ce qui est une contradiction car $\delta(K) = |E| = 2$.
Par conséquent $G = K$ et l'indexe de $F(G)$ dans G est q . Tout élément de $G \setminus F(G)$ a pour ordre q .
En vertu du Lemme 2.1, tous les sous-groupes de $F(G)$ sont normaux dans G.

Les groupes qui satisfont aux conditions établies dans le Lemme 2.5 sont exactement les groupes matroïdaux. La preuve du Théorème est ainsi complète.

Nous remarquons, enfin, que les groupes matroïdaux d'ordre pair (soit $q = 2$) ont été étudiés en détail, par un autre point de vue, dans [10].

III - Un exemple

Soient X un ensemble de cardinal ≥ 3 et α une involution sur X, sans point fixe. Fixons un sous-ensemble Y de X, tel que $|Y \cap T| = 1$ pour toute trajectoire T de α. Alors $X = Y \cup \alpha(Y)$ et $Y \cap \alpha(Y) = \varnothing$.

Pour tout couple $x,y \in Y$ nous poserons $x * y = \alpha(y)$ si $x \neq y$ et $\{x,y\}$ est contenu dans Y ou dans $\alpha(Y)$; sinon , nous poserons $x * y = y$.

Le tableau suivant illustre le cas où $X = \{a, b, c, a', b', c'\}$, $\alpha = (a\,a')\,(b\,b')\,(c\,c')$ et $Y = \{a, b, c\}$.

*	a	b	c	a'	b'	c'
a	a	b'	c'	a'	b'	c'
b	a'	b	c'	a'	b'	c'
c	a'	b'	c	a'	b'	c'
a'	a	b	c	a'	b	c
b'	a	b	c	a	b'	c
c'	a	b	c	a	b	c'

Les sous-algèbres maximales du groupoïde $G = (X, *)$ sont les ensembles de la forme $X \setminus \{x, \alpha(x)\}$ pour $x \in X$; d'où $\phi(G) = \varnothing$.

Les bases de G sont les sous-ensembles Z tels que $|Z \cap T| = 1$ pour toute trajectoire T de α, et G vérifie (L1) et (L2). Il satisfait aussi à (M1'), qui (en général) est une conséquence de (L1) et (L2), et à (M1"). En outre, quelque soit $x \in X$, l'ensemble $\{x, \alpha(x)\}$ est indépendant, mais il n'est contenu dans aucune base. Ainsi G ne vérifie pas (M2).

REFERENCES

[1] M. ASCHBACHER et R. GURALNICK :
Some applications of the first cohomology group , J. Algebra 90 (1984), 446-460.

[2] L. BENETEAU :
Une classe particulière de matroïdes parfaites, Ann. Discrete Math. 8 - (1980), 229-232.

[3] R. BRANDL :
Finite groups all of whose elements are of prime power order, Boll. Un. Mat. It. (5) 18-A (1981), 491-493.

[4] D. GORENSTEIN :
Finite groups , Harper & Row, 1968.

[5] G. GRÂTZER :
Universal algebra , Van Nostrand, 1968.

[6] B. HUPPERT :
Endliche Gruppen, I, Springer-Verlag, Berlin, 1967.

[7] G. HIGMAN :
Groups in which every element has prime-power order , J. London Math. Soc. , 32, (1957), 335-342.

[8] P.R. JONES :
Basis properties for inverse semigroups , J. Algebra 50 (1978), 135-152.

[9] R. SCAPELLATO et L. VERARDI :
Groupes finis qui jouissent d'une propriété analogue au théorème de la base de Burnside, présenté pour publication.

[10] R. SCAPELLATO :

Sur les groupes engendrés par une classe de p-involutions, Archiv der Mathematik, à paraître.

RAFFAELE SCAPELLATO (*)

Dipartimento di Matematica, Università di Parma, Via d'Azeglio 85, 43100 PARMA

LIBERO VERARDI (*)

Dipartimento di Matematica, Piazza Porta S. Donato 5, 40127 BOLOGNA

(*) Lavoro parzialmente finanziato su fondi MPI .

Manuscrit reçu le 11 Juillet 1990.