ANNALES MATHÉMATIQUES BLAISE PASCAL

RAFFAELE SCAPELLATO
LIBERO VERARDI

Bases of certain finite groups

Annales mathématiques Blaise Pascal, tome 1, n° 2 (1994), p. 85-93
<http://www.numdam.org/item?id=AMBP_1994__1_2_85_0>

Ann. Math. Blaise Pascal, Vol. 1, N° 2, 1994, pp. 85 - 93

BASES OF CERTAIN FINITE GROUPS

par Raffaele Scapellato and Libero Verardi

Résumé. Ce travail est consacré aux groupes dont les ensembles générateurs minimaux jouissent de propriétés proches à celles des bases d'une matroïde.

1 Introduction

Recently, considerable attention has been paid to problems on generators of groups. This concerns e.g. small generating sets of finite simple groups (see the survey [2]). Generating sets of groups are also relevant from the graph-theoretical point of view, because they give rise to connected Cayley digraphs (see e.g. [3]). Furthermore, Bénéteau [1] revisited Burnside basis theorem, by restating it in terms of matroids. Properties of this kind have also been studied by Jones [5] for semigroups, often reducing questions from semigroups to groups.

Therefore, it seems to be interesting to investigate groups whose behaviour with respect to generators is fairly similar to that of p-groups. This study can be performed with the help of an 'abstract' notion of independence. In order to make this idea more precise, we recall the definition of a matroid. Let S be a set, and let $c : \mathcal{P}(S) \to \mathcal{P}(S)$ be a mapping satisfying, for all $X \subseteq S$ and all $x, y \in S$, the following conditions:

1. $X \subseteq c(X)$;
2. $c(c(X)) = c(X)$;
3. $c(X)$ is the union of all $c(Y)$ for all finite $Y \subseteq X$;
4. if $y \notin c(X)$ and $x \notin c(Y, y)$ then $y \notin c(X, x)$.

[1]Work partially supported by the MURST.

The pair (S, c) is then called a *matroid*. This is one of the many equivalent definitions of a matroid (see e.g. [6]), and it seems to be the more appropriate for our purpose. A subset X of S is said to be *c-independent* if $c(Y) \neq c(X)$ for all $Y \subset X$. We say that X is a *generating set* if $c(X) = S$. Also, a *basis* is an independent generating set. We will make use of the above definitions even for the more general case of a mapping c satisfying only (1)-(3). For instance, let G be a finite group, and let $\Phi(G)$ be its Frattini subgroup (i.e. the intersection of its maximal subgroups). Setting $c(X) = < X, \Phi(G) >$ we obtain such a mapping. Following [7], [8], a subset X of a group is said to be *independent* if it is c-independent with respect to this c.

Accordingly with our previous paper [7], a finite group G is said to be a *matroid group* if it satisfies the following two axioms:

(M1) the minimal generating sets of G are exactly the bases of a matroid $\mathcal{M}(G)$;

(M2) each independent subset X of G is contained in a minimal generating set of G.

Note that in group theory the terms 'basis' and 'minimal generating set' are synonymous. In this paper we will use the latter, in order to avoid confusion with the 'basis' of a matroid.

As a consequence of Burnside basis theorem, all finite p-groups are matroid groups. We studied these groups in [7], [8], obtaining a characterization for them ([7], Lemma 1.1 and Theorem 2.5), that we summarize below in the following way. (Here $O_p(G)$ is the maximum normal p-subgroup of G).

Theorem 1.1 *Let G be a finite group, and let $H = G/\Phi(G)$. Then G is a matroid group if and only if one of the following holds:*

(1) *G is a p-group;*

(2) *there are two primes p, q with $p \equiv 1 \pmod q$ such that $|H : O_p(H)| = q$, $O_p(H)$ is elementary abelian and every subgroup of $O_p(H)$ is normal (but not central) in H.*

By the above, all matroid groups are solvable. But a finite simple group cannot even satisfy (M1), because its minimal generating sets have different numbers of elements. The situation is less obvious for (M2). We are aware of no non-solvable finite group satisfying this condition, and we conjecture that no such group exists. However, the solvable case is solved by Theorem 1.2 below. (Here $F(G)$ is the Fitting subgroup of G, i.e. its maximum normal nilpotent subgroup).

Theorem 1.2 *Let G be a finite solvable group, and let $H = G/\Phi(G)$. Then G satisfies (M2) if and only if one of the following holds:*

(1) *H is abelian;*

(2) *$F(H)$ has prime index in H and all its subgroups are normal in H.*

Another characterization of finite matroid groups will be given by using the following concept. Let (S, c) be a matroid and let $X \subseteq S$. Then X is said to be *c-hierarchical* if its elements can be ordered in a sequence $x_1, x_2, \ldots, x_m$ such that $c(x_1, x_2, \ldots, x_{k-1}) \neq c(x_1, x_2, \ldots, x_k)$ for all $k = 2, \ldots, m$, and $c(\emptyset) \neq c(x_1)$. For the case of groups (with $c(X) = < X >$), this concept was introduced by Hamidoune, Llado and Serra, who found in [4] the values of connectivity of Cayley digraphs associated with hierarchical generating sets.

At a first glance, most finite groups have hierarchical generating sets that are not minimal. On the other hand, we are able to describe the groups all whose hierarchical generating sets are minimal. This is the content of the following theorem, which will be proved as a corollary of a slighty more general result (Theorem 3.2).

Theorem 1.3 *Let G be a finite group. Then all hierarchical generating sets of G are minimal generating sets if and only if G is a matroid group with $\Phi(G) = 1$.*

The rest of the paper is mostly devoted to the proof of Theorems 1.2 and 1.3. Terminology and notation are standard, and can be found in [9] (but we write $\Phi(G)$ and $F(G)$ for the Frattini and Fitting subgroups). We will also use some obvious shortenings, such as $X \setminus x$ for $X \setminus \{x\}$.

2 Groups satisfying (M2)

First of all, we want to prove Theorem 1.2. Note that a group G satisfies (M2) if and only if $G/\Phi(G)$ does. Hence, in Lemmas 2.1-2.4, as well as in the proof of the theorem, we will assume that G is a finite solvable group satisfying (M2) and $\Phi(G) = 1$.

Lemma 2.1 *Every subgroup of $F(G)$ is normal in G.*

PROOF. As $\Phi(G) = 1$, $O_p(G)$ is elementary abelian. Let X be a minimal generating set of $O_p(G)$, and let $X \cup Y$ be a minimal generating set of G. Then $X \cup y$ is independent for all $y \in Y$. Hence for each $x \in X$, $< X \setminus x,\ y >$ is a subgroup of $O_p(G) < y >$, maximal of index p. Thus $< X \setminus x > \lhd < X \setminus x,\ y >$, so that $< X \setminus x > \lhd G$ for all $x \in X$. Since $F(G)$ is the direct product of the $O_p(G)$, we are done. ∎

Lemma 2.2 *The group G is supersolvable and metabelian. Also, $G' \leq F(G)$.*

PROOF. We know that $F(G)$ is abelian and all its subgroups are normal in G. Therefore, by conjugation, G induces on $F(G)$ universal power-automorphisms, that of course commute each other. Then this action corresponds to a homomorphism $G \to \mathrm{Aut}(F(G))$, whose kernel is $C_G(F(G))$ and whose image is abelian, so $G/C_G(F(G))$ is abelian. By [9], 7.4.7, p.187, $G/C_G(F(G)) = F(G)$, then

$G/F(G)$ is abelian. Hence $G' \leq F(G)$, and G is metabelian. Moreover it is obviously supersolvable, because every subgroup of G' is normal in G, so that G has a chief series with factors of prime order. ■

Lemma 2.3 *Every element of $G \setminus F(G)$ belongs to a complement of $F(G)$.*

PROOF. If $X = \{x_1, x_2, \ldots, x_r\}$ is a minimal generating set of $F(G)$ and $X \cup Y$ is a minimal generating set of G, then the subgroup $M = < Y >$ is a complement of $F(G)$. For otherwise, letting $L = M \cap F(G) \neq 1$, we can have $k = |\{x_1 L, x_2 L, \ldots, x_r L\}| < r$. Hence, $F(G) = < x_1, x_2, \ldots, x_r, L >$, and so $G = < x_1, x_2, \ldots, x_r, Y >$, a contradiction.

If $y \notin F(G)$ then $X' = X \cup y$ is independent, because $< X' \setminus y > = < X > = F(G)$. By Lemma 2.1, $< X' \setminus x_i > = < X \setminus x_i, y > = < X \setminus x_i >< y > \neq < X' >$ for all $x_i \in X$. Hence there is Y' such that $X' \cup Y'$ is a minimal generating set of G. Letting $Y = Y' \cup y$, also $X \cup Y$ is a minimal generating set of G. Thus $M = < Y >$ is a complement of G containing Y. ■

Lemma 2.4 *If G is nonabelian, then the index of $F(G)$ in G is prime.*

PROOF. By contradiction, suppose that $G/F(G)$ has not prime order. Let $X = \{x_1, \ldots, x_r\}$ be a minimal generating set of $F(G)$, and let $y \in G \setminus F(G)$. In view of Lemma 2.3, we can assume that y has prime order. Let $H = < X, y >$. By Lemma 2.2, we have $G' < F(G) < H$, so $H \lhd G$. Letting $X' = \{xy | x \in X\}$, we get $H = < X', y >$. Let us show that $X' \cup y$ is independent. Put $X_1 = \{x x_1^{-1} | x \in X \setminus x_1\}$, where $x_1 \in X$ is fixed. In view of Lemmas 2.1 and 2.3, we have $< X' > = < X_1, x_1 y > = < X_1 >< x_1 y > \neq H$. Similarly, for $x \in X$ we get $< X \setminus x, y > = < X \setminus x >< y > \leq H$.

By contradiction, suppose that $X' \cup y$ can be embedded in a minimal generating set. Then, in particular, there is $z \notin H$ such that $X' \cup \{y, z\}$ is independent. In view of Lemma 2.3, there is a complement M of $F(G)$ containing z. Suppose that $H \leq C_G(z)$. From Lemma 2.2 it follows that $M \cap G' = 1$, so M is abelian. Furthermore $HM = G$, and so $C_G(z) = G$. Therefore $z \in Z(G)$. But by [9], 7.4.7, p.167, $F(G)$ is self-centralizing, so in particular $Z(G) \leq F(G) \leq H$, hence $z \in H$, a contradiction. Then there is $w \in X' \cup y$ such that $[w, z] \neq 1$.

By Lemma 2.2 we have $G' \leq F(G)$, so $[w, z] \in F(G)$. If $[y, z] \neq 1$ we can choose $w = y$ and then there is $x_k \in X$ that may be replaced by a power of $[y, z]$ having prime order. This gives rise to another minimal generating set of $F(G)$. Therefore $< x_1, \ldots, x_r, y, z > = H < z > = < x_1 y, \ldots, x_{k-1} y, x_{k-1} y, \ldots, x_r y, y, z > = < X' \setminus x_k y, y, z >$, a contradiction. Thus $[y, z] = 1$. Since $w \in X' \cup y$, and by the above $w \neq y$, we have $w = x_i y$ for a suitable i.

Now $[w, z] = [x_i y, z] = [x_i, z]^y [y, z] = [x_i, z]^y \in < x_i >$, and so we get $x_i \in < x_i y, z >$, which implies $y \in < x_i y, z >$. Therefore

$$< X', y, z > = < x_1 y, \ldots, x_r y, y, z > = < x_1 y, \ldots, x_r y, z > = < X', z >,$$

a contradiction. ■

PROOF OF THEOREM 1.2. Let G be a group satisfying (M2). We may assume that $\Phi(G) = 1$. If G is nonabelian, we must prove (2). In view of Lemmas 2.1-2.4, it remains to show that the Sylow p-subgroups P of G are elementary abelian. If $P \leq F(G)$ this is clear. Otherwise, in view of Lemma 2.4, $P \cap F(G)$ has index p in P, then $\Phi(P) \leq F(G)$. A non-trivial cyclic subgroup C of $F(P)$ is normal in G and abelian, hence it has a complement in G ([9], 7.4.14, p.169). Thus C has also a complement in P, a contradiction because $C \leq \Phi(P)$. Hence $\Phi(P) = 1$ and we are done. Therefore (2) follows.

Conversely, let G be a group satisfying either (1) or (2). The former clearly imply (M2).

Assume now that (2) holds. Let X be independent and such that $H = < X >$ is different from G, and prove that there is $y \notin X$ such that $X \cup y$ is independent, too.

If $F(G)$ is not contained in H, choose any $y \in F(G) \setminus H$. Now $X \cup y$ is independent. In fact, for all $x \in X$ we have $< X \setminus x,\ y > = < X \setminus x > < y > \neq H < y >$, as $< X \setminus x > \neq H$.

If $F(G)$ is contained in H, then $H = F(G)$, because $F(G)$ is maximal in G. Let $y \in G \setminus F(G)$. Clearly, the set $X \cup y$ generates G. Moreover, for all $x \in X$, $K = < X \setminus x > \leq F(G)$, and so $K \lhd G$. It follows that $< X \setminus x, y > = K < y >$, which is a proper subgroup of G. This proves that $X \cup y$ is independent, and so G satisfies (M2). ■

By Theorem 1.2, an elementary example of a nonabelian group satisfying (M2) is given by any dihedral group.

It is worth to mention some consequences of Theorem 1.2.

Corollary 2.5 *Let G be a solvable group satisfying* (M2), *and let A be an abelian group with $(|A|.|F(G)|) = 1$. Then $G \times A$ satisfies* (M2).

Corollary 2.6 *Let G be a solvable group satisfying* (M2), *let p be the index of $F(G)$ in G. Then the Sylow p-subgroup of $F(G)$ is a direct factor of G. Also, if G has no abelian direct factors, then $F(G)$ is a Hall subgroup of G.*

PROOF. Let P be a p-Sylow subgroup of G. Since $Q = P \cap F(G)$, and P is abelian, we have $[Q, G] = [Q, F(G)P] = 1$, hence $Q \leq Z(G)$. Now Q is normal, abelian and $\Phi(G) = 1$, so Q has a complement C in G. From $Q \leq Z(G)$ we get $C \lhd G$ and $G = Q \times C$. ■

Yet another easy consequence of Theorem 1.2 is the following.

Corollary 2.7 *A finite solvable group G satisfying* (M2) *is a matroid group if and only if $F(G)/\Phi(G)$ is a p-group.*

The following proposition provides a criterion to prove that a group does not satisfy (M2). Note that a group does not satisfy (M2) if and only if it contains a maximal independent set that is not a minimal generating set.

Proposition 2.8 *Let G be a group with $\Phi(G) = 1$, let $K < G$ and let K^* be the intersection of all subgroups of G properly containing K. Assume that K^* is neither K nor G, and that K^* has a minimal generating set X, with $< X \cap K >= K$. Then G does not satisfy* (M2).

PROOF. Suppose $< X \cup Y >= G$ for some $Y \subseteq G$, and prove that the set $X \cup Y$ is dependent. By the hypothesis on X we have $K =< X \cap K > \subset < X' >$, where $X' =< X \cap K > \cup Y$. This inclusion is proper. In fact, $X \cap K$ is a minimal generating set of K and $Y \neq \emptyset$, otherwise we would have $K^* = G$. The definition of K^* gives us $K^* \subseteq < X' >$, so $X \subseteq < X' >$. Since $Y \subseteq X'$, it follows that $G =< X' >$. But $X \setminus K$ is non-empty, or else $K^* = K$. Hence X' is a proper subset of $X \cup Y$, and $X \cup Y$ is dependent. ■

We can apply Proposition 2.8 in order to prove that A_6 does not satisfy (M2). Let $x = (123456)$ and $K =< x >$. Then K^* is a dihedral group of order 12, and $K^* = N_G(K)$. Now $K^* =< x, y >$, where y has order 2, and $\{x, y\} \cap K = \{x\}$ is a minimal generating set of K.

3 Hierarchical generating sets

Unlike those of vector spaces, independent sets in finite groups cannot in general be embedded in bases. Namely, this happens only for groups satisfying (M2). On the other hand, each c-hierarchical subset X of a group G is contained in a c-hierarchical generating set of G.

Let G be a (finite) group and let F be a subgroup of G. Consider the mapping $c_F = c : \mathcal{P}(G) \to \mathcal{P}(G)$ defined by $c(X) =< F \cup X >$. A subset X of G will be said to be F-independent (F-hierarchical) if it is c_F-independent (resp. c_F-hierarchical). A set X is F-independent if and only if its is F-hierarchical for all of its total orders.

Clearly, c satisfies the conditions (1)-(3) of the definition of a matroid. We will prove that (4) holds exactly when G is a matroid group.

Note that (M1) does not imply (4) for the map c. A simple counterexample is provided by the group $G = A_4$. Letting Q be its Sylow 2-subgroup, define c_1 by $c_1(X) =< X >$ if $X \cap Q \subseteq 1$ and $c_1(X) =< X \cup Q >$ otherwise. Thus (G, c_1) is a matroid whose bases are the minimal generating sets of G, so (M1) holds. However, G does not satisfy (M2), because its c_1-independent subset $\{(12)(34), (14)(23)\}$ cannot be embedded in a minimal generating set of G.

Lemma 3.1 *A group G is a matroid group if and only if G is a $\Phi(G)$-matroid group.*

PROOF. A subset of G is independent if and only if it is $\Phi(G)$-independent. We will write $c = c_{\Phi(G)}$.

Let G be a matroid group. Let $X \subseteq G$ and $x, y \in G$. In order to show (4), we may assume that X is c-independent. Let $y \notin c(X)$. Then $X' = \{g\Phi(G) | g \in X\}$ is independent in $G/\Phi(G)$ and $y\Phi(G) \notin < X' >$. By [7], p.192, all subgroups of $G/\Phi(G)$ are matroid groups, hence also $< y\Phi(G), X' >$ is a matroid group. It contains the independent set X', so by (M2) each of its minimal generating subsets must have at least $|X'| + 1$ elements. It follows that $X' \cup \{y\Phi(G)\}$ is independent in $G/\Phi(G)$, hence $X \cup y$ is independent in G. By the same argument, if $x \notin c(X, y)$ then $\{x, y\} \cup X$ is independent, hence $y \notin c(X, x)$. Thus (G, c) is a matroid whose bases are the minimal generating sets of G, and so it coincides with $\mathcal{M}(G)$.

Conversely, let G a $\Phi(G)$-matroid group, and let X be a c-independent subset of G. Then X is contained in a basis B of the matroid (G, c). From $G = c(B) =< B \cup \Phi(G) >$, we get $G =< B >$. Furthermore $c(B \setminus y) \neq c(B) = G$ for all $y \in B$, hence B is a minimal generating set of G. Thus from $X \subseteq B$ we get(M2).

Finally, a minimal generating set B of G satisfies $< B >=< B, \Phi(G) >= G$ and for all proper subsets Y of B we have $< Y, \Phi(G) > \neq < B, \Phi(G) >$, so $c(B) = G$ but $c(Y) \neq G$. This proves (M1), with $\mathcal{M}(G) = (G, c)$. ■

Theorem 3.2 *Let G be a group and let $F \leq G$. Then G is an F-matroid group if and only if all of its F-hierarchical sets are independent.*

PROOF. Assume that G is an F-matroid group. Let $X = \{x_1, ..., x_m\}$ be an F-hierarchical subset of G. By contradiction, suppose that X is not F-independent. Let i such that $x_i \in c(x_1, ..., x_{i-1}, x_{i+1}, ..., x_m)$. There is k such that $x_i \in c(x_1, ..., x_{i-1}, x_{i+1}, ..., x_k)$ but $x_i \notin c(x_1, ..., x_{i-1}, x_{i+1}, ..., x_{k-1})$. Let $X' = \{x_1, ..., x_{i-1}, x_{i+1}, ..., x_{k-1}\}$. Then by the hypothesis on X we have $x_k \notin c(X', x_i)$, hence (4) implies $x_i \notin c(X', x_k)$, a contradiction. Thus X must be F-independent.

Conversely, assume that all F-hierarchical subsets of G are F-independent. We will prove (4) in the following form:

$$y \in c(X, x) \setminus c(X) \Rightarrow x \in c(X, y).$$

Once again, we may assume that X is F-independent. If X is F-hierarchical, both $X \cup x$ and $Y \cup y$ turn out to be F-hierarchical, so also F-independent. On the other hand, from $y \in c(X, x)$ it follows that $X \cup x \cup y$ is not F-independent, hence not even F-hierarchical. Thus $c(X, y) = c(X, y, x)$, and (4) follows. ■

PROOF OF THEOREM 1.3. By Lemma 3.1, G is a matroid group if and only if G is a $\Phi(G)$-matroid group. The assertion follows now from Theorem 3.2. ■

Proposition 3.3 *If G is an F-matroid group, then $\Phi(G) \leq F$.*

PROOF. If $y \in G \setminus F$, there is an F-basis $X \cup y$. Then $c(X, y) = G \neq c(X)$, that is $< F, X, y >= G \neq < F, X >$. Hence $y \notin \Phi(G)$. ■

Proposition 3.4 *If G is an F-matroid group and $F \leq H \leq G$, then G is also an H-matroid group.*

PROOF. In view of Theorem 3.2, we have to show that every H-hierarchical subset $\{y_1, \ldots, y_n\}$ of G is H-independent. Since G is an F-matroid group, it has an F-independent subset $\{x_1, \ldots, x_m\}$, such that $< F, x_1, \ldots, x_m >= H$. Then the set $\{x_1, \ldots, x_m, y_1, \ldots, y_n\}$ is F-hierarchical, so also F-independent by Theorem 3.2.

Suppose, by contradiction, that $\{y_1, \ldots, y_n\}$ is not H-independent. Then there is y_i such that

$$< H, y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n >=< H, y_1, \ldots, y_n >$$

but then

$$< F, x_1, \ldots, x_m, y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n >=< F, x_1, \ldots, x_m, y_1, \ldots, y_n >,$$

a contradiction, because $\{x_1, \ldots, x_m, y_1, \ldots, y_n\}$ is F-independent. ∎

The converse of Proposition 3.4 is not true. Obvious counter-examples arise from the fact that if H is a maximal subgroup of a group G, then G is always an H-matroid group.

Acknowledgement

We are grateful to the referee for his constructive remarks, that led to an improvement of the paper.

References

[1] L. Bénéteau, *Une classe particulière de matroïdes parfaits*, Ann. Discrete Math., **8** (1980), 229-232.

[2] L. Di Martino and C. Tamburini, *2-generation of finite simple groups and some related topics*, in: Generators and relations in groups and geometries, Barlotti et al. (eds.), Kluwer Acad. Publ., Amsterdam 1991, pp.195-232.

[3] J. L. Gross and A. Tucker, *Topological graph theory*, Wiley-Interscience, New York, 1987.

[4] Y. O. Hamidoune, A. S. Llado and O. Serra, *The connectivity of hierarchical Cayley digraphs*, Discrete Appl. Math. **37/38** (1992), 275-280.

[5] P. R. Jones, *Basis properties for inverse semigroups*, J. Algebra **50** (1978), 132-152.

[6] J. G. Oxley, *Matroid theory*, Oxford University Press, London 1992.

[7] R. Scapellato and L. Verardi, *Groupes finis qui jouissent d'une propriété analogue au théorème des bases de Burnside*, Boll. Un. Mat. It. (7), **5**-A (1991), 187-194.

[8] R. Scapellato and L. Verardi, *Sur les ensembles générateurs minimaux d'un groupe fini*, Ann. Sci. Univ. 'B. Pascal', Clermont II, Ser. Mat. **26** (1991), 51-60.

[9] W. R. Scott, *Group theory*, Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1964.

Raffaele Scapellato
Dipartimento di Matematica
Politecnico di Milano
Piazza Leonardo da Vinci 32,
20133 Milano ITALIA

Libero Verardi
Dipartemento di Matematica
Universita di Bologna
Piazza di Porta S. Donato 5,
40127 Bologna,ITALIA

manuscrit reçu le 28.04.94