Groups with the basis property

Jonathan McDougall-Bagnall and Martyn Quick

Mathematical Institute, University of St Andrews, North Haugh,
St Andrews, Fife, Scotland, KY16 9SS

jbagnall@mcs.st-and.ac.uk, martyn@mcs.st-and.ac.uk

August 15, 2011

1 Introduction

The Burnside Basis Theorem tells us that generating sets for p-groups share many properties with bases for vector spaces. In particular, if G is a p-group then minimal generating sets (that is, generating sets for which no proper subset also generates G) all have the same cardinality. We shall say that an arbitrary group has *property $\mathcal{B}$* if its minimal generating sets have the same cardinality. A group G is said to have the *basis property* if G and all its subgroups have property $\mathcal{B}$. The basis property was introduced by P. R. Jones [7], who considered it in the context of inverse semigroups. The basis property for groups has been considered by a number of authors [1, 2, 7] and we shall mention some of this work below.

A variant of these properties is the concept of a *matroid group*. This is a group G which satisfies property $\mathcal{B}$ and also an additional condition that every independent subset of G is contained in a minimal generating set. Matroid groups have been studied in detail by Scapellato and Verardi [11, 12] (and the reader can also consult these papers for the definition of the term "independent"). In particular, they provide a full characterisation of matroid groups [11, Lemma 1.1 and Theorem 2.5] and it follows from [11, Theorem 1.2] that a matroid group has the basis property. (This latter result also appears in [1]).

The purpose of this paper is to initiate a study of groups with property $\mathcal{B}$, to provide a pleasant characterisation of groups with the basis property, and to draw attention to the links between property $\mathcal{B}$, the basis property and matroid groups. The characterisation is our main theorem and the various links between these properties will appear in the course of its proof:

Theorem 1.1 *Let G be a finite group. Then G has the basis property if and only if G is a semidirect product $P \rtimes Q$, where P is a p-group, Q is a* *cyclic q-group, for some prime $q \neq p$, and every non-identity element of Q acts fixed-point-freely on P.*

We retrieve the case of a p-group having the basis property by taking $Q = \mathbf{1}$ in our theorem. To say that an element x in Q acts *fixed-point-freely* on P is to require that the centraliser $\mathrm{C}_P(x)$ is trivial. When $Q \neq \mathbf{1}$, to achieve this condition that every non-identity element acts fixed-point-freely on P, it is of course sufficient that a generator of the unique subgroup of Q of order q acts fixed-point-freely on P.

In view of the isomorphism $C_{mn} \cong C_m \times C_n$ for m and n coprime, it follows that a group with the basis property has all its elements of prime-power order. Jones [7, Lemma 5.3 and Theorem 5.4] established that the basis property is inherited by quotients and that a group with the basis property is soluble. He notes that Higman [5] classified the soluble groups with all elements of prime-power order. A classification of groups with the basis property based on Higman's result was announced by N. K. Dickson and Jones in [7], but as far as we can tell this has yet to appear and work has continued on this topic. More recently, A. Al'Khalaf has announced a classification of groups with the basis property, but this is different to our theorem and involves a technical condition on the module structure of various quotients of the p-group P appearing above. The current authors have seen some parts of Al'Khalaf's proof and the methods employed are considerably different to those we employ although, as would be expected, both rely on Higman's result. It therefore seems worthwhile to demonstrate how our classification on the one hand follows from a construction of groups with property $\mathcal{B}$ and, on the other, links to classic results on groups with fixed-point-free automorphisms (see, for example, [4, 13]).

The structure of the paper is as follows. Section 2 contains some theoretical observations concerning groups possessing property $\mathcal{B}$. In particular, we are able to observe that under certain circumstances, property $\mathcal{B}$ is inherited by quotients and that a direct product of non-trivial groups has property $\mathcal{B}$ if and only if the groups involved are p-groups. In Section 3, we demonstrate a method of constructing, from a finite field, groups with property $\mathcal{B}$ and trivial Frattini subgroups. We classify groups G with $G/\Phi(G)$ as given by our construction (Theorem 3.4) and note that, in general, such a group G need not have the basis property. However, our construction appears in Proposition 3.3 which provides the link between fixed-point-free action and groups with the basis property. This is a key tool used in the final step of the proof of our main theorem in Section 4.

We shall use standard notation. In particular, $\Phi(G)$ denotes the Frattini subgroup of a group G, while $\mathrm{C}_G(x)$ and $\mathrm{N}_G(H)$ denote the centraliser of an element and a subgroup, respectively, in G. We shall use $d(G)$ to denote the minimal number of generators of a group G.

2 Theoretical observations concerning property $\mathcal{B}$

The purpose of this section is to initiate a study of groups satisfying property $\mathcal{B}$. This property is sufficiently weak that a full analysis of such groups appears to be rather challenging. Nevertheless, we are able to make some observations and these will be of use in our classification of groups with the basis property.

Our first observation is elementary and depends only on the fact that the Frattini subgroup is the set of non-generators in a group.

Lemma 2.1 *A group G has property $\mathcal{B}$ if and only if $G/\Phi(G)$ has property $\mathcal{B}$.*

Lemma 2.2 *If G is a group with property $\mathcal{B}$ and G splits over a normal subgroup N, then G/N has property $\mathcal{B}$.*

PROOF: By hypothesis, $G = N \rtimes H$ for some subgroup H. Choose a set $B = \{b_1, b_2, \dots, b_k\}$ of elements of N with k minimal such that $N = \langle B \rangle^H$. If $A = \{a_1, a_2, \dots, a_d\}$ is a minimal generating set for H, then $A \cup B$ is a minimal generating set for G. Hence every minimal generating set for G contains $k + d$ elements and we conclude that, in particular, d is uniquely determined. Hence H has property $\mathcal{B}$. □

Proposition 2.3 *Let G be a group with property $\mathcal{B}$ and M be an elementary abelian minimal normal subgroup of G. Then G/M has property $\mathcal{B}$ and*

$$d(G/M) = \begin{cases} d(G) - 1 & \textit{if } G \textit{ splits over } M, \\ d(G) & \textit{if } G \textit{ does not split over } M. \end{cases}$$

PROOF: When G splits over M, this follows from Lemma 2.2 and its proof. Assume then that G does not split over M. Let $x_1, x_2, \dots, x_d \in G$ such that $A = \{Mx_1, Mx_2, \dots, Mx_d\}$ is a minimal generating set for G/M. Let $X = \langle x_1, x_2, \dots, x_d \rangle$. Our assumptions ensure $\mathbf{1} \neq M \cap X \trianglelefteqslant MX = G$ and, from the minimality of M, we conclude $M \leqslant X$ and $G = X$. Consequently, $\{x_1, x_2, \dots, x_d\}$ is a minimal generating set for G. Hence $d = d(G)$ and as A is an arbitrary minimal generating set for G/M, the proof is complete. □

Corollary 2.4 *If G is a soluble group with property $\mathcal{B}$, then every quotient of G has property $\mathcal{B}$.*

We shall see from our construction in Section 3 that there exist groups having property $\mathcal{B}$ with subgroups that do not inherit the property. This indicates a principal difference between this property and the more restrictive basis property.

It is tempting to ask whether, in the case of finite groups, property $\mathcal{B}$ is always inherited by quotients or even whether a group with $\mathcal{B}$ is necessarily soluble. Indeed, it is well-known (via the Classification of Finite Simple Groups) that every non-abelian finite simple group G is 2-generated. On the other hand, if T is the set of involutions in G, then $G = \langle T \rangle$ and some subset T_0 of T is a minimal generating set for G. Necessarily, $|T_0| \geqslant 3$, since a group generated by two involutions is dihedral. Consequently, no non-abelian finite simple group has property $\mathcal{B}$. In addition, it is easy to see that a symmetric group S_n never has property $\mathcal{B}$ for $n \geqslant 4$, since it is minimally generated by $n-1$ transpositions $\{(1\ 2), (2\ 3), \dots, (n{-}1\ n)\}$ and also by $(1\ 2)$ together with $(1\ 2 \dots n)$.

To make progress on whether property $\mathcal{B}$ is inherited by quotients and whether it implies solubility, the likely next step would be to establish whether or not a finite almost simple group can have property $\mathcal{B}$. Such an investigation would take us on some detour from our final goal, so we choose to leave that to another time.

Theorem 2.5 *A direct product $G \times H$ of two non-trivial groups G and H has property $\mathcal{B}$ if and only if both G and H are p-groups for some prime p.*

Proof: If G and H are p-groups, then so is $G \times H$ and this then has property $\mathcal{B}$ by the Burnside Basis Theorem. Conversely, suppose $G \times H$ has property $\mathcal{B}$ and let $A = \{a_1, a_2, \dots, a_d\}$ and $B = \{b_1, b_2, \dots, b_e\}$ be minimal generating sets for G and H, respectively. Then

$$C = \{(a_1, 1), (a_2, 1), \dots, (a_d, 1), (1, b_1), (1, b_2), \dots, (1, b_e)\}$$

is a minimal generating set for $G \times H$ and hence $d(G \times H) = d + e$. The hypothesis then ensures d and e are fixed and so G and H have property $\mathcal{B}$.

Now let X be any generating set for G. We describe two processes to apply to X. First if X contains elements of coprime order, exploit the isomorphism $C_{mn} \cong C_m \times C_n$ for m and n coprime, to produce a new generating set X^* for G consisting entirely of elements of prime-power order. Secondly, let X' be any minimal generating set for G contained in X^*. If Y is any generating set for H, we apply the same steps to produce a minimal generating set Y' for H consisting of elements of prime-power order. We take $A = X'$ and $B = Y'$ in the previous paragraph to produce a minimal generating set C for $G \times H$. Since $G \times H$ has property $\mathcal{B}$ it now follows that there is a prime p such that every element in X' and Y' is of p-power order. For otherwise, there would exist $a \in X'$ and $b \in Y'$ of coprime order and we could replace $(a, 1)$ and $(1, b)$ in C by the element (a, b) to produce a smaller generating set for $G \times H$. If we started with a different generating set for G but applied the same steps to the generating set Y for H, we must necessarily still end up with elements of p-power order. Consequently, the prime p is an invariant of $G \times H$ and does not depend on the initial choice of X and Y.

Suppose there exists a prime $q \neq p$ that divides the order of G. Let x be an element of q-power order and $G = \langle x, Z \rangle$ for some subset Z. Applying the above process to $X = \{x\} \cup Z$, we note $X^* = \{x\} \cup Z^*$ and $x \notin X'$ by the previous paragraph. It follows that Z^*, and hence Z, generates G. We conclude that x is a non-generator of G and so belongs to $\Phi(G)$. It follows that $G/\Phi(G)$, and hence G, is a p-group. This is enough to complete the proof. □

3 Constructing groups with property $\mathcal{B}$

In this section, we provide a standard method for constructing a group with property $\mathcal{B}$ and trivial Frattini subgroup. We shall give a structural description of groups G such that $G/\Phi(G)$ is isomorphic to a group arising from our construction (Theorem 3.4). This description has much in common with the observations made by Scapellato and Verardi concerning matroid groups (see [11, Theorem 3.1]). However, most significant will be the observation made in Proposition 3.3 linking our construction to fixed-point-free actions. This will turn out to be key in our characterisation of groups with the basis property.

Let V be the additive group of some finite field $\mathbb{F}_{p^n}$ and let q^m be a prime-power that divides $p^n - 1$. If H is the unique subgroup of order q^m in the multiplicative group of $\mathbb{F}_p^n$, then there is a natural action $\phi\colon H \to \operatorname{Aut} V$ via multiplication, $h\phi\colon v \mapsto vh$, and we can construct the semidirect product $G = V \rtimes_\phi H$. In what follows we shall refer to such a semidirect product as being constructed *via the field multiplication in* $\mathbb{F}_{p^n}$.

We shall observe that G is a group with property $\mathcal{B}$ and to do this we shall exploit the structure of V as an $\mathbb{F}_pH$-module. The facts given in Lemma 3.1 will be of use. They are all established via standard methods, though it is worth pointing out that they also occur naturally when viewed through the lens of Singer cycles. If t is a generator for the multiplicative group of $\mathbb{F}_{p^n}$, then the automorphism $v \mapsto vt$ of V is known as a *Singer cycle*. In this context, our group G is a subgroup of the semidirect product of V by the cyclic group generated by the Singer cycle. Much of the lemma can be deduced from the standard theory (see, for example, Huppert [6, Satz II.7.3] and Neumann–Praeger [9, Lemmas 2.1 and 2.2]).

Let R denote the group algebra $\mathbb{F}_pH$ and write vR for the submodule of V generated by a vector v.

Lemma 3.1 (i) *Every element in G has order equal to p or a power of q.*

(ii) *If $v \in V$, then the kernel of the homomorphism $R \to V$ given by $r \mapsto vr$ is independent of the choice of v. Hence, if v and w are non-zero vectors in V, then $vR \cong wR$ and vR is irreducible.*

Theorem 3.2 *Let $G = V \rtimes_\phi H$ be the semidirect product of an elementary abelian p-group by a cyclic q-group constructed via the field multiplication in $\mathbb{F}_{p^n}$. Then*

(i) *G has property $\mathcal{B}$;*

(ii) *$d(G) = k+1$ where V is a direct sum of k irreducible $\mathbb{F}_pH$-submodules;*

(iii) *$\Phi(G) = \mathbf{1}$.*

PROOF: Let A be an arbitrary generating set for G. We shall show that A possesses a subset of cardinality $k+1$ that also generates G. Parts (i) and (ii) will then follow.

Let $\pi \colon G \to H$ be the natural map. Then $A\pi$ generates $H \cong C_{q^m}$, so there exists some $a_0 \in A$ such that $H = \langle a_0\pi \rangle$. Note that $V \cap \langle a_0 \rangle = \mathbf{0}$ by Lemma 3.1(i). Any further element of A has the form $a = va_0^j$ for some $v \in V$ and $j = j(a) \geqslant 0$. Let $B = \{\, aa_0^{-j(a)} \mid a \in A \,\} \subseteq V$. Then $B \cup \{a_0\}$ generates G and it is straightforward to verify that V is the sum of the R-submodules bR for $b \in B$. As each non-zero bR is irreducible by Lemma 3.1(ii), we conclude $V = \bigoplus_{b \in B_0} bR$ for some $B_0 \subseteq B \setminus \{0\}$ of cardinality k. If $a_1, a_2, \dots, a_k \in A$ are such that $B_0 = \{\, a_ia_0^{-j(a_i)} \mid i = 1, 2, \dots, k \,\}$, then $G = \langle a_0, a_1, \dots, a_k \rangle$. This establishes the claim and so G has property $\mathcal{B}$ and $d(G) = k+1$.

Finally, if $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ as a direct sum of irreducible submodules, then the subgroups of the form $(V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_k) \rtimes H$ are all maximal, so $\Phi(G)$ is contained in their intersection, which is H. On the other hand, a straightforward calculation show that if $\mathbf{1} \neq K \leqslant H$, then $\mathrm{N}_G(K) = H$. Hence no non-trivial subgroup of H is normal in G and we conclude $\Phi(G) = \mathbf{1}$. □

The main link between the basis property and semidirect products constructed via field multiplication is the following. Again, it can easily be understood within the theory of Singer cycles, so we keep our proof brief.

Proposition 3.3 *Let G be the semidirect product of an elementary abelian p-subgroup P by a cyclic q-subgroup Q. Then the following are equivalent:*

(i) *every non-identity element of Q acts fixed-point-freely on P;*

(ii) *$G = P \rtimes Q$ is constructed via the field multiplication in some finite field $\mathbb{F}_{p^n}$.*

PROOF: (ii) $\Rightarrow$ (i): In the notation of our construction, the fact that every $h \in H$ acts fixed-point-freely on V follows immediately from the fact that if $v(h-1) = 0$ in $\mathbb{F}_{p^n}$, then either $v = 0$ or $h = 1$.

(i) $\Rightarrow$ (ii): Suppose $Q \cong C_{q^m}$. If V is an irreducible $\mathbb{F}_pQ$-module upon which every non-identity element of Q acts fixed-point-freely, then $V \cong \mathbb{F}_pQ/I$ for some maximal ideal I with $Q \cap (1+I) = \mathbf{1}$. This quotient ring has the structure of a field such that Q embeds in the multiplicative group as a set of generators for the field. Consequently, $V \cong \mathbb{F}_{p^r}$ where r is minimal subject to q^m dividing $p^r - 1$ and Q acts on $\mathbb{F}_{p^r}$ via the field multiplication. Therefore, if $G = P \rtimes Q$ satisfies our assumption (i), then we conclude P is the direct sum of k copies, say, of $\mathbb{F}_{p^r}$ as an $\mathbb{F}_pQ$-module and we deduce G is isomorphic to the semidirect product constructed via the field multiplication in $\mathbb{F}_{p^{rk}}$. □

Finally in this section, we provide a description of all groups G for which $G/\Phi(G)$ is a semidirect product as constructed from a finite field as above.

Theorem 3.4 *Let G be a finite group such that $G/\Phi(G)$ is a semidirect product of an elementary abelian p-group by a cyclic group of order q^m constructed via the multiplication in a finite field. Then*

(i) *G has a unique Sylow p-subgroup P;*

(ii) *$G = P \rtimes Q$ for any Sylow q-subgroup Q and all Sylow q-subgroups of G are cyclic;*

(iii) *$\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$ where x is a generator for Q. Moreover, x^{q^m} centralises P.*

Proof: (i) Let P be a Sylow p-subgroup of G. Then $P\Phi(G)/\Phi(G)$ is a Sylow p-subgroup of $G/\Phi(G)$ and our hypothesis tells us $P\Phi(G) \trianglelefteqslant G$. Applying the Frattini Argument, we conclude $G = \mathrm{N}_G(P)$ and $P \trianglelefteqslant G$.

(ii) Let Q be a Sylow q-subgroup. Our hypothesis on $G/\Phi(G)$ ensures that $G = PQ\Phi(G)$ and hence $G = PQ$. We conclude $G = P \rtimes Q$.

Now consider the quotient group $\bar{G} = G/(P \cap \Phi(G))$. We shall use the bar notation for subgroups of this quotient. Every maximal subgroup of G contains $P \cap \Phi(G)$ and so we conclude $\bar{G}/\Phi(\bar{G}) \cong G/\Phi(G)$. By construction $\Phi(\bar{G}) = \Phi(G)/(P \cap \Phi(G))$ has trivial Sylow p-subgroup and so is a q-group. Hence $\Phi(\bar{G}) \leqslant \bar{Q}$.

Now let W be any maximal subgroup of Q. Then PW is maximal in G and so $\Phi(G) \leqslant PW$. Since $\bar{W}$ is the Sylow q-subgroup of $\bar{P}\bar{W}$ and $\Phi(\bar{G}) \leqslant \bar{P}\bar{W}$, we conclude that $\Phi(\bar{G})$ is contained in some, and hence every, conjugate of $\bar{W}$. We deduce $\Phi(\bar{G})$ is contained in every maximal subgroup of $\bar{Q}$, so $\Phi(\bar{G}) \leqslant \Phi(\bar{Q})$. It follows that $\bar{Q}/\Phi(\bar{Q})$ is a quotient of $\bar{Q}/\Phi(\bar{G})$, which is isomorphic to the image of Q in $G/\Phi(G)$ and so is cyclic. Therefore $Q = \langle x, \Phi(\bar{Q}) \rangle$ for some x and hence $Q = \langle x \rangle$.

(iii) Let $\theta \colon Q \to \operatorname{Aut} P$ be the homomorphism determined by the action of Q on P. Since $\Phi(P) \leqslant \Phi(G)$, there is a natural homomorphism

$\pi\colon G/\Phi(P) \to G/\Phi(G)$. The quotients appearing here have the following structures

$$G/\Phi(P) \cong (P/\Phi(P)) \rtimes Q, \qquad G/\Phi(G) \cong (P/\Phi(P)) \rtimes Q/\langle x^{q^m} \rangle$$

and so $\ker \pi = \Phi(P)\langle x^{q^m} \rangle / \Phi(P)$. It follows that $\Phi(P)\langle x^{q^m} \rangle$ is a normal subgroup of G and hence

$$[P, \Phi(P)\langle x^{q^m} \rangle] \leqslant P \cap \Phi(P)\langle x^{q^m} \rangle = (P \cap \langle x^{q^m} \rangle)\Phi(P) = \Phi(P).$$

It follows that $\langle x^{q^m} \rangle \theta \leqslant \mathrm{C}_{\mathrm{Aut}\,P}(P/\Phi(P))$. A theorem of Philip Hall (see [10, (5.3.3)]) says that this centraliser is a p-group and hence $\langle x^{q^m} \rangle \leqslant \ker \theta$; that is, x^{q^m} centralises P. It now follows that $\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$. □

We can now easily construct examples of groups with property $\mathcal{B}$ that do not satisfy the basis property. For example, let $G = (C_2 \times C_2) \rtimes_\phi C_9$ where $\phi\colon C_9 \to \mathrm{Aut}(C_2 \times C_2)$ is the composite of the natural map $C_9 \to C_3$ and the homomorphism $C_3 \to \mathrm{Aut}(C_2 \times C_2)$ arising in our construction via the field multiplication in $\mathbb{F}_4$. Let $K = \ker \phi \cong C_3$. Then $K = \mathrm{Z}(G)$, the centre of G, and this is the unique subgroup of G of order 3. We can then observe K is contained in every maximal subgroup of G, so $K \leqslant \Phi(G)$. On the other hand, G/K is the semidirect product constructed via the field multiplication in $\mathbb{F}_4$, so $\Phi(G/K) = \mathbf{1}$ by Theorem 3.2(iii). Hence $\Phi(G) = K$. Thus $G/\Phi(G)$ has property $\mathcal{B}$ and so therefore also does G. It clearly does not have the basis property since it contains a subgroup isomorphic to $C_2 \times C_2 \times C_3$.

4 Proof of the main theorem

In this section, we shall prove our main theorem. The proof depends upon Higman's result [5] classifying soluble groups where every element has prime-power order. In view of this, we shall first establish various results concerning the groups arising, specifically that certain of them never have the basis property.

Groups with generalised quaternion quotient

Lemma 4.1 *Let Q be a generalised quaternion group and V be an irreducible $\mathbb{F}_pQ$-module for an odd prime p upon which Q acts faithfully. Then the semidirect product $V \rtimes Q$ constructed from this action has minimal generating sets of cardinality* 2 *and* 3. *In particular, $V \rtimes Q$ does not have property $\mathcal{B}$.*

Proof: Suppose $Q = \langle a, b \rangle$ where $a^{2^{n-1}} = 1$, $b^2 = a^{2^{n-2}}$ and $b^{-1}ab = a^{-1}$. Let $H = V \rtimes Q$ and we shall denote the action of Q on V by exponentiation.

If v is a non-zero vector in V, then certainly $\{a, b, v\}$ is a minimal generating set for H.

On the other hand, since Q acts faithfully on V, the action of a on V does not commute with the action of b. This means that b is not represented by $-I$ (where I is the identity map), so there exists some $v \neq 0$ such that $v^b \neq -v$. Consider $L = \langle vb, a \rangle$. Certainly $VL = H$. We calculate that $(vb)^2 = (v + v^{b^{-1}})b^2$ and so it follows that L contains $v + v^{b^{-1}} \neq 0$. Hence L contains $\langle v + v^{b^{-1}} \rangle^L = \langle v + v^{b^{-1}} \rangle^{VL} = V$. Therefore $L = H$ and so H has a minimal generating set of cardinality 2, namely $\{vb, a\}$. □

Proposition 4.2 *Let G be a group with a non-trivial normal p-subgroup P such that G/P is a generalised quaternion group. Then G does not have property $\mathcal{B}$.*

Proof: Let Q be the Sylow 2-subgroup of G, so $G = P \rtimes Q$ and G is soluble. There exists $N \trianglelefteqslant G$ such that $\Phi(G) \leqslant N < P$ and P/N is irreducible when viewed as an $\mathbb{F}_p Q$-module. If G were to have property $\mathcal{B}$, then so would $G/N \cong (P/N) \rtimes Q$, by Corollary 2.4, and this contradicts Lemma 4.1. □

Groups with metacyclic quotient

Proposition 4.3 *Let H be the semidirect product of a cyclic group C of order q^b by a cyclic group D of order p^a where every non-identity element of D acts fixed-point-freely on C and where $a, b \geqslant 1$. Let $G = P \rtimes H$ where P is a non-trivial p-subgroup. Then G does not have the basis property.*

Proof: Assume G has the basis property. By passing to a quotient, we can assume P is elementary abelian and irreducible as an $\mathbb{F}_p H$-module. Let $C = \langle x \rangle$, $D = \langle y \rangle$ and let $z \in P \setminus \mathbf{1}$. Then $\{x, y, z\}$ is a minimal generating set for G. (Here we use $a, b \geqslant 1$.)

However, as G has the basis property, it follows that if $h \in C$, then $\mathrm{C}_P(h) = \mathbf{1}$, so PC is a Frobenius group. We may therefore apply part (5b) of Lemma 1 in Mazurov [8] to deduce that G contains an element g of order p^{a+1}. Let $L = \langle y, g \rangle$. Then $PL = G$ and g^{p^a} is a non-identity element of P, so L contains $\langle g^{p^a} \rangle^{PL} = P$. Hence $L = G$ and we deduce $\{y, g\}$ is also a minimal generating set, contrary to assumption. □

Remark: In fact, the group G in Proposition 4.3 does not have property $\mathcal{B}$. To establish this, a similar argument is used and the principal tool is the observation that, in the notation of the proposition, an irreducible $\mathbb{F}_p H$-module is either a trivial module or is free when viewed as an $\mathbb{F}_p D$-module.

Classification of groups with the basis property

We now describe the structure of finite groups with the basis property. We use the fact that a finite group with the basis property is soluble, as observed by Jones [7, Theorem 5.4].

Proposition 4.4 *Let G be a finite group with the basis property. Then $G/\Phi(G)$ is a semidirect product constructed via the multiplication in some finite field.*

Proof: Let G be a minimal counterexample. Then G is soluble and every quotient of G has the basis property. Therefore minimality forces $\Phi(G) = \mathbf{1}$, since if $G/\Phi(G)$ satisfies the conclusion then trivially so does G. In addition, any element of G has prime-power order and we may therefore apply Theorem 1 of Higman [5]. Let p be a prime such that G has a non-trivial normal p-subgroup and let P be a maximal normal p-subgroup of G. Then one of the following cases occurs:

(i) G/P is cyclic of order q^k where q is a prime distinct from p;

(ii) p is odd and G/P is a generalised quaternion group;

(iii) G/P is a group of order $p^a q^b$ with cyclic Sylow subgroups where q is a prime of the form $kp^a + 1$.

Proposition 4.2 shows that Case (ii) cannot occur. We shall show that, apart from trivial examples, Case (iii) are impossible and then show that Case (i) leads to the forms claimed in the theorem.

Case (iii): Assume that our minimal counterexample G is as in Case (iii). We shall assume $a, b \neq 0$, since otherwise G is actually as in Case (i). As $\Phi(G) = \mathbf{1}$, we deduce $\Phi(P) = \mathbf{1}$ (see [10, (5.2.13)(ii)]) and so P is an elementary abelian p-group. We claim that P is a minimal normal subgroup of G. If it were not, there is a minimal normal subgroup M of G such that $M < P$. Then G/M is, by assumption, not a counterexample, is not a p-group as $b \neq 0$, and so has a normal Sylow subgroup by Theorem 3.4. If G/M has a unique Sylow p-subgroup, then G/P has normal Sylow subgroups for both primes p and q. Therefore G/P possesses commuting elements of p-power and q-power order, contradicting it having the basis property. If G/M has a unique Sylow q-subgroup, then as P/M is a normal p-subgroup, we obtain a similar contradiction.

Hence P is a minimal normal subgroup of G. As $\Phi(G) = \mathbf{1}$, there is a maximal subgroup H of G such that $P \not\leq H$. Then $H \cap P = \mathbf{1}$ and G is the semidirect product $P \rtimes H$. As H has no element of non-prime-power order, it follows that H is as in Proposition 4.3. Therefore $G = P \rtimes H$ does not have the basis property.

Case (i): It remains that G is as in Case (i) and so is a semidirect product of a p-subgroup P by a cyclic q-subgroup Q. Since $\Phi(G) = \mathbf{1}$, so we deduce $\Phi(P) = \mathbf{1}$ and P is elementary abelian. As G has no elements of non-prime-power order, we deduce every non-identity element of Q acts fixed-point-freely on P. Proposition 3.3 establishes that G is constructed via the field multiplication in some finite field.

This completes the proof of Proposition 4.4. □

We can now finish the proof of Theorem 1.1.

If G has the basis property, then applying Proposition 4.4 and Theorem 3.4 tells us that $G = P \rtimes Q$ where P is a p-group and Q is a cyclic q-group. The basis property ensures that every non-identity element of Q acts fixed-point-freely on P.

Conversely, suppose $G = P \rtimes Q$, where P is a p-group, Q is a cyclic q-group for some prime $q \neq p$ and every non-identity element of Q acts fixed-point-freely on P. These properties are inherited by any subgroup of G, and so in order to show that G has the basis property, it is sufficient to show that it has property $\mathcal{B}$.

First, it is straightforward to apply the theory of p'-automorphisms of p-groups (see, for example, Section 5.3 in Gorenstein [3]) to deduce that every non-identity element of Q acts fixed-point-freely on $P/\Phi(P)$. Proposition 3.3 tells us that $G/\Phi(P) \cong P/\Phi(P) \rtimes Q$ is constructed via the multiplication in some finite field. Theorem 3.2(iii) together with [10, (5.2.13)(ii)] show that $\Phi(G) = \Phi(P)$. Hence $G/\Phi(G)$ has property $\mathcal{B}$ by Theorem 3.2(i) and so G has property $\mathcal{B}$.

This completes the proof of the main theorem.

Acknowledgements: The first author is supported by an EPSRC Doctoral Training Grant. The authors are grateful to Dr. A. Al'Khalaf for helpful discussions and sharing the details of his recent work on this topic. They would also like to thank Prof. N. Ruškuc for his contributions which led to this line of investigation and the referee for, in particular, drawing their attention to the link with Singer cycles and Lemma 1 in Mazurov [8].

References

[1] A. Aljouiee & F. Alrusaini, “Matroid groups and basis property,” *Internat. J. Algebra* **4** (2010), 535–540.

[2] A. Al'Khalaf, “Finite groups with the basis property”, *Dokl. Akad. Nauk BSSR* **33** (1989), no. 11, 972–974, 1051. (Russian)

[3] Daniel Gorenstein, *Finite Groups, Second Edition* (Chelsea, New York, 1980).

[4] Graham Higman, “Groups and rings having automorphisms without non-trivial fixed elements,” *J. London Math. Soc.* **32** (1957), 321–334.

[5] Graham Higman, “Finite groups in which every element has prime power order,” *J. London Math. Soc.* **32** (1957), 335–342.

[6] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenchaften **134**, Springer-Verlag, Berlin, 1967.

[7] P. R. Jones, “Basis properties for inverse semigroups,” *J. Algebra* **50** (1978), 135–152.

[8] V. D. Mazurov, “The set of orders of elements in a finit group,” *Algebra and Logic* **33** (1994), 49–55.

[9] Peter M. Neumann & Cheryl E. Praeger, “A recognition algorithm for special linear groups,” *Proc. London Math. Soc. (3)* **65** (1992), 555–603.

[10] Robinson, *A Course in the Theory of Groups, Second Edition*, Graduate Texts Math. **80**, Springer, New York, 1996.

[11] Raffaele Scapellato and Libero Verardi, “Groupes finis quis jouissent d’une propriété analogue au théorème des bases de Burnside”, *Boll. Un. Mat. Ital. A (7)* **5** (1991), 187–194.

[12] Raffaele Scapellato and Libero Verardi, “Bases of certain finite groups,” *Annales mathématiques Blaise Pascal* **1** (1994), 85–93.

[13] J. G. Thompson, Finite groups with fixed-point-free automorphisms of prime order, *Proc. Nat. Acad. Sci. U.S.A.* **45** (1959), 578–581.