

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`

March 22, 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 [6], who considered it in the context of inverse semigroups. The basis property for groups has been considered by a number of authors [1, 2, 6] 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 [8, 9] (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 [8, Lemma 1.1 and Theorem 2.5] and it follows from [8, 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 $Q = 1$ in our theorem. To say that an element x in Q acts *fixed-point-freely* on P is to require that the centraliser $C_P(x)$ is trivial. When $Q \neq 1$, 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 [6, 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 [6], 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, 10]).

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 3.6) and note that, in general, such a group G need not have the basis property. However, our construction appears in Proposition 3.5 which provides the link between fixed-point-free action and groups with the basis property. This is the 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 $C_G(x)$ and $N_G(H)$ denote the centraliser of an element and a subgroup, respectively, in 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} . \square

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*

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

PROOF: When G splits over M , this follows from Lemma 2.2 and its proof. Let us assume then that G does not split over M and write $Q = G/M$. Let x_1, x_2, \dots, x_d be elements of G such that $A = \{Mx_1, Mx_2, \dots, Mx_d\}$ is a minimal generating set for Q . Let $X = \langle x_1, x_2, \dots, x_d \rangle$. Then $G = MX$ and by assumption $M \cap X \neq \mathbf{1}$. Since $M \cap X \trianglelefteq X$ and M is abelian, we conclude $M \cap X \trianglelefteq MX = G$. Hence $M \cap X = M$ and we conclude $G = MX \leq X$. Therefore $\{x_1, x_2, \dots, x_d\}$ is a generating set for G and it is minimal, since it projects onto the minimal generating set A for Q . We conclude that $d = d(G)$ and as A is an arbitrary minimal generating set for Q , the proof is complete. \square

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, $|T_0| \geq 3$, 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 $n \geq 4$, 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 $d(G \times H) = d + e$. It follows then that G and H have property \mathcal{B} with $d(G) = d$ and $d(H) = e$, for if G were to have minimal generating set of size d' we could construct an analogous minimal generating set for $G \times H$ of cardinality $d' + e$ and hence conclude $d' = d$.

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 .

We now show that G is a p -group. Suppose there exists a prime $q \neq p$ that divides the order of G . Let x be an element of q -power order and let Z be a subset of G such that $\{x\} \cup Z$ generates G . Apply the processes of the previous paragraph to first construct $X^* = \{x\} \cup Z^*$ and then a subset X' that generates minimally. We have observed that $x \notin X'$ and hence $X' \subseteq Z^*$. It follows that Z^* , and hence Z , generates G . We conclude that x is a non-generator of G and so belongs to $\Phi(G)$. Hence if P is a Sylow p -subgroup of G , then $G = P\Phi(G)$ and so $G = P$. By the same argument, H is also a p -group and the proof is complete. \square

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 3.6). This description has much in common with the observations made by Scapellato and Verardi concerning matroidal groups (see [8, Theorem 3.1]). However, most significant will be the observation made in Proposition 3.5 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 $p^n - 1$. Let H be the unique subgroup of order q^m in the multiplicative group of \mathbb{F}_{p^n} . Define a homomorphism $\phi: H \rightarrow \text{Aut } V$ by defining $h\phi$ (for $h \in H$) to be the automorphism $v \mapsto vh$ given by multiplying by h . We may then construct the semidirect product $G = V \rtimes_{\phi} H$ using the resulting action of H on V . 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 denote elements in G by ordered pairs (v, h) where $v \in V$ and $h \in H$.

We can view V as a vector space over \mathbb{F}_p and in this setting ϕ becomes a linear representation. Let us write R for the group algebra $\mathbb{F}_p H$. Then ϕ induces the structure of an R -module upon V and, by Maschke's Theorem, $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ is a direct sum of irreducible R -submodules. If $v_1, v_2,$

\dots, v_k are non-zero elements of V_1, V_2, \dots, V_k , respectively, then these generate V as an R -module. Hence G is generated by the set

$$\{(v_1, 1), (v_2, 1), \dots, (v_k, 1), (0, x)\},$$

where x is a generator for H . We shall demonstrate that G has property \mathcal{B} by showing that every generating set for G contains a subset of cardinality $k+1$ that also generates G .

Lemma 3.1 *The group G possesses no elements of order pq^i with $i \geq 1$.*

PROOF: An element of V has order dividing p . If (v, h) is an element of G not in V then $h \neq 1$ and we calculate

$$(v, h)^{q^m} = \left(\sum_{i=0}^{q^m-1} vh^{-i}, h^{q^m} \right) = (0, 1),$$

since the first entry is a geometric sum in \mathbb{F}_{p^n} that sums to zero. Hence every element in G but not in V has q -power order. \square

If $v \in V$, we shall write vR for the R -submodule generated by v .

Lemma 3.2 *Let v and w be non-zero elements of V . Then $vR \cong wR$. In particular, all non-zero cyclic submodules of V are irreducible.*

PROOF: There is a surjective module homomorphism $\theta_v: R \rightarrow vR$ given by $r \mapsto vr$. If $v \neq 0$, then the kernel of θ_v consists of those elements $r = \sum_{h \in H} \lambda_h h$ in R such that the sum $\sum_{h \in H} \lambda_h h$ equals 0 when evaluated in the field \mathbb{F}_{p^n} . In particular, $\ker \theta_v$ is independent of the choice of v . Hence if v and w are non-zero elements of V , then $\ker \theta_v = \ker \theta_w$ and so $vR \cong R/\ker \theta_v = R/\ker \theta_w \cong wR$.

The final assertion holds as V possesses at least one irreducible submodule and this is necessarily of the form vR for some non-zero $v \in V$. \square

Theorem 3.3 *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 $\mathbb{F}_p H$ -submodules;
- (iii) $\Phi(G) = \mathbf{1}$.

PROOF: We retain the notation already established in this section. 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 $\pi: G \rightarrow H$ be the natural map. Then $A\pi$ generates H and since H is cyclic of order q^m , there exists some $a_0 \in A$ such that $H = \langle a_0\pi \rangle$. Any other element of A has the form $a = va_0^j$ for some $v \in V$ and $j = j(a) \geq 0$. Let $B = \{aa_0^{-j(a)} \mid a \in A\} \subseteq V$. Then $B \cup \{a_0\}$ generates G and if W is the R -submodule of V generated by B , then $G = W\langle a_0 \rangle$. Hence $V = W\langle a_0 \rangle \cap V = W(\langle a_0 \rangle \cap V) = W$, since $\langle a_0 \rangle \cap V = \mathbf{1}$ by Lemma 3.1. It follows that V is the sum of the irreducible submodules bR for $b \in B \setminus \{0\}$ (using Lemma 3.2) and we may therefore find $B_0 \subseteq B \setminus \{0\}$ such that $V = \bigoplus_{b \in B_0} bR$. As the number of composition factors occurring in the module V is an invariant, we conclude $|B_0| = k$.

Let $a_1, a_2, \dots, a_k \in A$ such that $B_0 = \{a_i a_0^{-j(a_i)} \mid i = 1, 2, \dots, k\}$. Then $G = \langle B_0, a_0 \rangle = \langle a_0, a_1, \dots, a_k \rangle$. This establishes the claim and so G has property \mathcal{B} and $d(G) = k + 1$.

All that remains is to show that $\Phi(G) = \mathbf{1}$. The subgroups of the form $(V_1 \oplus \dots \oplus V_{i-1} \oplus V_{i+1} \oplus \dots \oplus V_k) \rtimes H$ are all maximal, so $\Phi(G)$ is contained in their intersection, which is H . On the other hand, a straightforward calculation shows that if $\mathbf{1} \neq K \leq H$, then $N_G(K) = H$. Hence no non-trivial subgroup of H is normal in G and we conclude $\Phi(G) = \mathbf{1}$. \square

In order to link our construction fully with groups with property \mathcal{B} and with the basis property, we need to have a complete description of the irreducible submodules occurring in Lemma 3.2. In the following lemma, V , H and R retain the same meaning established earlier in this section.

Lemma 3.4 (i) *There is a unique finite field of characteristic p generated by a subgroup of order q^m of its multiplicative group, namely the field \mathbb{F}_{p^r} where r is minimal such that \mathbb{F}_{p^r} has a multiplicative subgroup of order q^m .*

(ii) *Any irreducible submodule of V is isomorphic to the additive group of \mathbb{F}_{p^r} (with r as in (i)) viewed as an R -module via the field multiplication in \mathbb{F}_{p^r} .*

PROOF: (i) First note that if r is minimal such that \mathbb{F}_{p^r} has a multiplicative subgroup H of order q^m , then the subfield generated by H must be \mathbb{F}_{p^r} . Now suppose K and L are finite fields of characteristic p both generated by a multiplicative subgroup of order q^m . There exists a finite field F that contains K and L and we deduce that $K = L$ since they are both generated by the unique subgroup of F^* of order q^m .

(ii) We return to the notation of the earlier parts of this section and, in particular, that appearing in Lemma 3.2. Let v be a non-zero element of V .

We consider the homomorphism $\theta_v: R \rightarrow vR$ introduced in that lemma. The kernel I of θ_v is a maximal ideal of R (since R is commutative) and so the quotient ring R/I has the structure of a field. If $h \in H \cap (1 + I)$, then $v(h - 1) = 0$ in the field \mathbb{F}_{p^n} and we conclude $h = 1$. Hence H embeds in the multiplicative group of the finite field R/I . Note that R/I is generated by the image of H and so we conclude that $R/I \cong \mathbb{F}_{p^r}$ by part (i).

The induced action of H on the additive subgroup of R/I is given by

$$(I + r)h = I + rh = (I + r)(I + h)$$

and so, as modules, $vR \cong R/I$, where the additive group of R/I is viewed as an R -module via the field multiplication in R/I . This completes the proof of the lemma. \square

Proposition 3.5 *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, when $G = V \rtimes H$ is constructed via the field multiplication in some finite field \mathbb{F}_{p^n} , then $h \in H$ fixes $v \in V$ when $v(h - 1) = 0$. From this it follows that either $v = 0$ or $h = 1$ in the field \mathbb{F}_{p^n} . Therefore if a semidirect product $P \rtimes Q$ is constructed via the field multiplication in \mathbb{F}_{p^n} , then every non-identity element of Q acts fixed-point-freely on P .

(i) \Rightarrow (ii): Assume every non-identity element of Q acts fixed-point-freely on P . View P as an $\mathbb{F}_p Q$ -module and write it as a direct sum of irreducible submodules

$$P = V_1 \oplus V_2 \oplus \cdots \oplus V_k.$$

Each V_i is a homomorphic image of the group algebra $\mathbb{F}_p Q$, so $V_i \cong \mathbb{F}_p Q / I_i$ where I_i is a maximal ideal. Therefore each quotient ring $\mathbb{F}_p Q / I_i$ naturally has the structure of a finite field. Since every non-identity element of Q acts fixed-point-freely on V_i , it follows that $Q \cap (1 + I_i) = \mathbf{1}$. Therefore Q embeds in the multiplicative group of the field $\mathbb{F}_p Q / I_i$ and does so such that the image generates the field. It follows that each $\mathbb{F}_p Q / I_i$ is isomorphic to \mathbb{F}_{p^r} where r is as in Lemma 3.4(i).

Hence P is the direct sum of k copies of the finite field \mathbb{F}_{p^r} where Q acts on each summand via its embedding in the multiplicative group $\mathbb{F}_{p^r}^*$. The same is true, by Lemma 3.4(ii), for the additive group $\mathbb{F}_{p^{rk}}$ when it appears as the base group in our group constructed from its field multiplication. Hence the two semidirect products $P \rtimes Q$ and $V \rtimes Q$ (when V is the additive group of $\mathbb{F}_{p^{rk}}$) are isomorphic. \square

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 3.6 *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 so is normal in $G/\Phi(G)$. Hence $P\Phi(G) \trianglelefteq G$. By the Frattini Argument, $G = N_G(P)P\Phi(G) = N_G(P)\Phi(G)$ and we conclude $G = N_G(P)$ and $P \trianglelefteq G$.

(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 $\bar{G}/\Phi(\bar{G}) \cong G/\Phi(G)$. Therefore \bar{G} satisfies the hypotheses of this theorem, but by construction $\Phi(\bar{G}) = \Phi(G)/(P \cap \Phi(G))$ has trivial Sylow p -subgroup. Therefore $\Phi(\bar{G})$ is a q -group and so $\Phi(\bar{G}) \leq \bar{Q}$.

Now let W be any maximal subgroup of Q . Then PW is maximal in G and so $\Phi(G) \leq PW$. Since \bar{W} is the Sylow q -subgroup of $\bar{P}\bar{W}$ and $\Phi(\bar{G}) \leq \bar{P}\bar{W}$, we conclude that $\Phi(\bar{G})$ is contained in some, and hence every, conjugate of \bar{W} . Therefore $\Phi(\bar{G}) \leq \bar{W}$. Consequently $\Phi(\bar{G})$ is contained in every maximal subgroup of \bar{Q} , so $\Phi(\bar{G}) \leq \Phi(\bar{Q})$. 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 $Q = \langle x, \Phi(Q) \rangle$ for some x and hence $Q = \langle x \rangle$.

(iii) First consider the quotient group $G/\Phi(P) \cong (P/\Phi(P)) \rtimes Q$. By Maschke's Theorem, $P/\Phi(P)$ is the direct sum of irreducible $\mathbb{F}_p Q$ -modules $V_1 \oplus V_2 \oplus \cdots \oplus V_k$. Define M_i to be the subgroup of G such that

$$M_i/\Phi(P) = (V_1 \oplus \cdots \oplus V_{i-1} \oplus V_{i+1} \oplus \cdots \oplus V_k) \rtimes Q.$$

Then M_i is a maximal subgroup of G and the intersection of the M_i is contained in $\Phi(P) \rtimes Q$. Hence

$$\Phi(G) \cap P \leq \bigcap_{i=1}^k (M_i \cap P) \leq \Phi(P).$$

Conversely, [7, 5.2.13(ii)] tells us that $\Phi(P) \leq \Phi(G)$ and so we conclude $\Phi(P) = \Phi(G) \cap P$.

Let $\theta: Q \rightarrow \text{Aut } P$ be the homomorphism determined by the action of Q on P . Since $\Phi(P) \leq \Phi(G)$, there are two natural homomorphisms $\pi_1: G \rightarrow G/\Phi(P)$ and $\pi_2: G/\Phi(P) \rightarrow G/\Phi(G)$. These quotients have the following structures

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

and so $\ker \pi_2 = \Phi(P)\langle x^{q^m} \rangle/\Phi(P)$. It follows that $\Phi(P)\langle x^{q^m} \rangle$ is a normal subgroup of G and hence

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

It follows that $\langle x^{q^m} \rangle\theta \leq C_{\text{Aut } P}(P/\Phi(P))$. A theorem of Philip Hall (see [7, (5.3.3)]) says that this centraliser is a p -group and hence $\langle x^{q^m} \rangle \leq \ker \theta$; that is, x^{q^m} centralises P . It now follows that $\Phi(G) = \Phi(P) \times \langle x^{q^m} \rangle$. \square

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 $\phi: C_9 \rightarrow \text{Aut}(C_2 \times C_2)$ is the composite of the natural map $C_9 \rightarrow C_3$ and the homomorphism $C_3 \rightarrow \text{Aut}(C_2 \times C_2)$ arising in our construction via the field multiplication in \mathbb{F}_4 . Let $K = \ker \phi \cong C_3$. Then $K = Z(G)$, the centre of G , and this is the unique subgroup of G of order 3. If M were a maximal subgroup of G not containing K , then $G = MK$, $M \cap K = \mathbf{1}$ (as K is a minimal normal subgroup of G) and so $G = K \rtimes M$. However, this contradicts K being the unique subgroup of order 3. Hence K is contained in every maximal subgroup of G , so $K \leq \Phi(G)$. 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 3.3(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 $\mathbb{F}_p Q$ -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 $\{vb, a\}$. \square

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 . Then $G = P \rtimes Q$ and G is soluble. If G were to have property \mathcal{B} , then so would every quotient of G by Corollary 2.4. We could first pass to the quotient of G by the Frattini subgroup of P and so assume that P is elementary abelian. Then P would be the direct sum $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ of irreducible $\mathbb{F}_p Q$ -modules. We could then factor by $P_2 \oplus \cdots \oplus P_k$ and so produce a quotient of the form $P_i \rtimes Q$. Lemma 4.1 tells us that this quotient does not have property \mathcal{B} and hence our original group G does not have property \mathcal{B} . \square

Groups with metacyclic quotient

Lemma 4.3 *Let H be the semidirect product of a cyclic group of order q^b by a cyclic group of order p^a where every non-identity element of the Sylow p -subgroup of H acts fixed-point-freely on the Sylow q -subgroup. Let V be an irreducible $\mathbb{F}_p H$ -module. Then either V is a trivial module or is free when viewed as an $\mathbb{F}_p C_{p^a}$ -module.*

PROOF: Let x be a generator for a Sylow p -subgroup and y be a generator for the Sylow q -subgroup of H . Let $R = \mathbb{F}_p \langle x \rangle$ be the group algebra of $\langle x \rangle$. Then R is a uniserial module of dimension p^a with submodules

$$R = R_0 > R_1 > R_2 > \cdots > R_{p^a} = \mathbf{0}$$

and each quotient R_i/R_{i+1} is a trivial R -module.

Now let $S = \mathbb{F}_p H$ and observe that S possesses a chain of submodules

$$S = S_0 > S_1 > S_2 > \cdots > S_{p^a} = \mathbf{0}$$

where $S_i = \bigoplus_{j=0}^{q^b-1} R_i y^j$ is the submodule of S generated by R_i . We shall now establish the structure of each quotient S_i/S_{i+1} .

Let $\Omega = \{ \omega_{y^j} \mid 0 \leq j \leq q^b - 1 \}$ be a set in one-one correspondence with the elements of $\langle y \rangle$. We let $\langle y \rangle$ act regularly on Ω and $\langle x \rangle$ act according to the conjugation in H :

$$\omega_{y^j} \cdot y = \omega_{y^{j+1}}, \quad \omega_{y^j} \cdot x = \omega_{(y^j)^x}.$$

This then defines an action of H on Ω . Let W be the vector space with basis Ω , viewed as an S -module via this action. Let $\theta: R_i \rightarrow \mathbb{F}_p$ be the natural map with kernel R_{i-1} . We define a linear map $\phi: S_i \rightarrow W$ by

$$\left(\sum_{j=0}^{q^b-1} r_j y^j \right) \phi = \sum_{j=0}^{q^b-1} (r_j \theta) \omega_{y^j}.$$

It is straightforward to check that y commutes with the map ϕ , while

$$\begin{aligned} \left(\left(\sum_{j=0}^{q^b-1} r_j y^j \right) x \right) \phi &= \left(\sum_{j=0}^{q^b-1} (r_j x) (y^j)^x \right) \phi = \sum_{j=0}^{q^b-1} ((r_j x) \theta) \omega_{(y^j)^x} \\ &= \left(\sum_{j=0}^{q^b-1} (r_j \theta) \omega_{y^j} \right) \cdot x = \left(\sum_{j=0}^{q^b-1} r_j y^j \right) \phi \cdot x, \end{aligned}$$

since x acts trivially on R_i/R_{i+1} . Thus ϕ is an S -module homomorphism and the kernel is S_{i+1} . Hence $S_i/S_{i+1} \cong W$ for all i .

We now determine the structure of W . Since $\langle y \rangle$ acts regularly on Ω , as an $\mathbb{F}_p \langle y \rangle$ -module W is isomorphic to the quotient $\mathbb{F}_p[Y]/(Y^{q^b} - 1)$, where $\mathbb{F}_p[Y]$ is the polynomial algebra and the action of y on this quotient is induced by multiplication by the indeterminate Y . Let us factorise

$$Y^{q^b} - 1 = f_1(Y) f_2(Y) \cdots f_k(Y)$$

as a product of irreducible polynomials. Since the derivative of $Y^{q^b} - 1$ is coprime to the original polynomial, these factors are distinct. Then

$$W \cong \mathbb{F}_p[Y]/(Y^{q^b} - 1) \cong \bigoplus_{i=1}^k W_i,$$

where $W_i = \mathbb{F}_p[Y]/(f_i(Y))$, a direct sum of irreducible $\mathbb{F}_p \langle y \rangle$ -modules. Moreover, as the irreducible polynomials $f_i(Y)$ are distinct, these summands are pairwise non-isomorphic.

By hypothesis, every non-identity element of $\langle x \rangle$ acts fixed-point-freely on $\langle y \rangle$. Consequently, in the action of $\langle x \rangle$ on Ω , there is one orbit of length 1, namely that containing the identity element and every other orbit corresponds to a trivial stabiliser and so has length p^a . Hence, as an $\mathbb{F}_p\langle x \rangle$ -module, W is isomorphic to the direct sum of a trivial module and $(q^b - 1)/p^a$ copies of the group algebra R .

Now as they are pairwise non-isomorphic, the W_i are the unique k irreducible $\mathbb{F}_p\langle y \rangle$ -submodules of W and Clifford's Theorem tells us that $\langle x \rangle$ permutes them. Consequently, if $\{W_{i_1}, W_{i_2}, \dots, W_{i_m}\}$ is a $\langle x \rangle$ -orbit of such submodules, then

$$U = W_{i_1} \oplus W_{i_2} \oplus \dots \oplus W_{i_m}$$

is an irreducible S -module. It now follows that as an S -module, W is completely reducible, say

$$W = U_1 \oplus U_2 \oplus \dots \oplus U_n.$$

Without loss of generality, U_1 is the trivial S -module. Moreover, the direct sum decomposition of W as an R -module must be a refinement of this decomposition. Hence, each U_i , for $i \geq 2$, is a direct sum of copies of the group algebra R as an R -module.

As an irreducible S -module is isomorphic to some irreducible quotient of W and hence isomorphic to some U_i , the claimed result now holds. \square

Proposition 4.4 *Let H be the semidirect product of a cyclic group of order q^b by a cyclic group of order p^a where every non-identity element of the Sylow p -subgroup of H acts fixed-point-freely on the Sylow q -subgroup and where $a, b \geq 1$. Let $G = P \rtimes H$ where P is a non-trivial p -subgroup. Then G does not have property \mathcal{B} .*

PROOF: This group G is soluble and so if G were to have property \mathcal{B} , then so would every quotient of G . By passing to an appropriate quotient, we can then assume that P is an elementary abelian p -group and that P is irreducible when viewed as an $\mathbb{F}_p H$ -module.

If x is a generator for the Sylow p -subgroup of H , y is a generator for the Sylow q -subgroup of H , and z is a non-identity element of P , then $\{x, y, z\}$ is a minimal generating set for G . (Note that here we use $a, b \geq 1$.)

If P were a trivial $\mathbb{F}_p H$ -module, then y and z commute and have coprime order, so we would deduce that $\{x, yz\}$ is also a minimal generating set for G .

If P is a non-trivial module, then as an $\mathbb{F}_p\langle x \rangle$ -module, P is a direct sum of copies of $\mathbb{F}_p\langle x \rangle$, by Lemma 4.3. Let us then choose z to actually be a generator of one of these summands. Then $\langle x, z \rangle$ is isomorphic to the wreath product $C_p \text{ wr } C_{p^a}$ and it follows that xz is an element of order p^{a+1} . Let $L = \langle xz, y \rangle$. Then $L \cap P$ contains $(xz)^{p^a}$ and so is non-trivial. Since $LP = G$, we deduce $P = \langle L \cap P \rangle^{LP} = \langle L \cap P \rangle^L \leq L$. Hence $L = G$ and so $\{xz, y\}$ is a minimal generating set for G .

This now gives us a contradiction and establishes the proposition. \square

Classification of groups with the basis property

We now describe the structure of finite groups with the basis property.

Lemma 4.5 (Jones [6, Theorem 5.4]) *A finite group with the basis property is soluble.*

PROOF: Let G be a minimal counterexample. As observed earlier, a non-abelian simple group does not have property \mathcal{B} . It follows that G is not simple and, if M is a minimal normal subgroup of G , then M is elementary abelian. By Proposition 2.3, the quotient G/M has property \mathcal{B} . If H/M is a proper subgroup of G/M , then H has the basis property and is soluble by induction. Consequently, the quotient H/M has property \mathcal{B} by Corollary 2.4. It follows that G/M has the basis property and hence is soluble by induction. We can then deduce that G is soluble, which contradicts the assumption that G is a minimal counterexample. This completes the proof. \square

Proposition 4.6 *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 either conclusion then trivially so does G . Any element of G has prime-power order, since a cyclic group of non-prime-power order would not have property \mathcal{B} . 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 $kp^a + 1$.

We shall show that, apart from trivial examples, Cases (ii) and (iii) are impossible and then show that Case (i) leads to the forms claimed in the theorem.

Case (ii): A group G as in Case (ii) does not have the basis property by Proposition 4.2.

Case (iii): Assume that our minimal counterexample G is as in Case (iii). If $b = 0$, then $G = P$ and our group is as in Case (i) with $k = 0$. Equally if $a = 0$, then G is also in Case (i), so we shall assume $a, b \neq 0$. As $\Phi(G) = \mathbf{1}$, we deduce $\Phi(P) = \mathbf{1}$ (see [7, (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 and is not a p -group as $b \neq 0$. Therefore G/M satisfies the conclusion and so G/M has a unique Sylow p -subgroup by Theorem 3.6. Consequently, G/P has normal Sylow subgroups for both primes p and q . It is therefore the direct product of these Sylow subgroups and so does not have the basis property, contrary to assumption.

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 $P \rtimes H$. Here H has order $p^a q^b$, has cyclic Sylow subgroups and, as $q = kp^a + 1$, the Sylow q -subgroup is normal in H . Moreover, H has no element of non-prime-power order, so it follows that H is as in Proposition 4.4. 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 so P is elementary abelian. If any non-identity element of Q centralises a non-identity element of P , then we would have an element of non-prime-power order contrary to G having the basis property. Therefore every non-identity element of Q acts fixed-point-freely on P . Proposition 3.5 establishes that G is constructed via the field multiplication in some finite field.

This completes the proof of Proposition 4.6. □

We can now finish the proof of Theorem 1.1.

If G has the basis property, then $G/\Phi(G)$ is a semidirect product constructed via the multiplication in some finite field. Theorem 3.6 says that $G = P \rtimes Q$ where P is a p -group and Q is a cyclic q -group. The basis property ensures that no non-identity element of Q centralises a non-identity element of P and so 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 . If H is a subgroup of G , then its Sylow p -subgroup $H \cap P$ is normal and all its Sylow q -subgroups are cyclic. Moreover, since every non-identity element of Q acts fixed-point-freely on P , we deduce the same holds for non-trivial subgroups of Sylow q -subgroups of H . Hence subgroups

of G inherit the hypothesis, so in order to show that G has the basis property, it is sufficient to show that it has property \mathcal{B} .

We first show that every non-identity element of Q acts fixed-point-freely on $P/\Phi(P)$. If this were not the case, then there exists a non-trivial subgroup R of Q whose generator has a fixed-point in $P/\Phi(P)$. Let U be the set of fixed-points of the generator of R . When we view $P/\Phi(P)$ as an $\mathbb{F}_p R$ -module, this U is a submodule and hence $P/\Phi(P) = U \oplus W$ for some submodule W by Maschke's Theorem. Then $[P/\Phi(P), R] \leq W$ and so $[P, R] < P$. Since $P = C_P(R)[P, R]$ by [3, Theorem 5.3.5], we conclude $C_P(R) \neq \mathbf{1}$. In particular, the generator of R has a fixed-point in P , contrary to hypothesis.

Hence every non-identity element of Q acts fixed-point-freely on $P/\Phi(P)$. Proposition 3.5 tells us that $G/\Phi(P) \cong P/\Phi(P) \rtimes Q$ is constructed via the multiplication in some finite field. Theorem 3.3(iii) together with [7, (5.2.13)(ii)] show that $\Phi(G) = \Phi(P)$. Hence $G/\Phi(G)$ has property \mathcal{B} by Theorem 3.3(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.

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] P. R. Jones, "Basis properties for inverse semigroups," *J. Algebra* **50** (1978), 135–152.
- [7] Robinson, *A Course in the Theory of Groups, Second Edition*, Graduate Texts Math. **80**, Springer, New York, 1996.

- [8] Raffaele Scapellato and Libero Verardi, “Groupes finis qui jouissent d’une propriété analogue au théorème des bases de Burnside”, *Boll. Un. Mat. Ital. A (7)* **5** (1991), 187–194.
- [9] Raffaele Scapellato and Libero Verardi, “Bases of certain finite groups,” *Annales mathématiques Blaise Pascal* **1** (1994), 85–93.
- [10] J. G. Thompson, Finite groups with fixed-point-free automorphisms of prime order, *Proc. Nat. Acad. Sci. U.S.A.* **45** (1959), 578–581.