MINIMAL PERMUTATION REPRESENTATIONS OF SEMIDIRECT PRODUCTS OF GROUPS

DAVID EASDOWN AND MICHAEL HENDRIKSEN

ABSTRACT. The minimal faithful permutation degree $\mu(G)$ of a finite group $G$ is the least nonnegative integer $n$ such that $G$ embeds in the symmetric group $\text{Sym}(n)$. We make observations in varying degrees of generality about $\mu(G)$ when $G$ decomposes as a semidirect product, and provide exact formulae in the case that the base group is an elementary abelian $p$-group and the extending group a cyclic group of prime order $q$ not equal to $p$. For this class, we also provide a combinatorial characterisation of group isomorphism. These results contribute to the investigation of groups $G$ with the property that there exists a nontrivial group $H$ such that $\mu(G \times H) = \mu(G)$, in particular reproducing the seminal examples of Wright (1975) and Saunders (2010). Given an arbitrarily large group $H$ that is a direct product of elementary abelian groups (with mixed primes), we construct a group $G$ such that $\mu(G \times H) = \mu(G)$, yet $G$ does not decompose nontrivially as a direct product. In the case that the order of $H$ is a product of distinct primes, the group $G$ is a semidirect product such that the action of $G$ on each of its Sylow $p$-subgroups, where $p$ divides the order of $H$, is irreducible. This final construction relies on properties of generalised Mersenne prime numbers.

1. INTRODUCTION

Throughout this paper all groups are assumed to be finite and $C_n$ denotes a cyclic group of order $n$. The minimal faithful permutation degree $\mu(G)$ of a group $G$ is the smallest nonnegative integer $n$ such that $G$ embeds in the symmetric group $\text{Sym}(n)$. Note that $\mu(G) = 0$ if and only if $G$ is trivial. It is well known (and referred to as Karpilovsky’s theorem, see, for example, [11, 12]) that if $G$ is a nontrivial abelian group, then $\mu(G)$ is the sum of the prime powers that occur in a direct product decomposition of $G$ into cyclic factors of prime power order. Johnson proved (see [11, Theorem 1]) that the Cayley representation of a group $G$ is minimal, that is, $\mu(G) = |G|$, if and only if $G$ is cyclic of prime power order, the Klein four-group or a generalised quaternion 2-group. A number of other explicit calculations of minimal degrees and a variety of techniques appear in Johnson [11], Wright [21, 22], Neumann [15], Easdown and Praeger [3], Kovacs and Praeger [13], Easdown [2], Babai, Goodman and Pyber [1], Holt [9], Holt and Walton [10], Lemieux [14], Elias, Silbermann and Takloo-Bighash [5], Franchi [6], Saunders [17–20] and Easdown and Saunders [4]. This present article, building on work initiated by the second author in [8], focuses on minimal degrees of semidirect products of groups, characterises group isomorphism and provides exact formulae for minimal degrees in the case when the base group is an elementary abelian $p$-group and the extending group is cyclic of order $q$ where $p$ and $q$ are different primes.


Keywords: permutation groups, semidirect products, Mersenne numbers.
For any groups $G$ and $H$ and subgroups $S$ of $G$, we always have the inequalities
\[
\mu(S) \leq \mu(G) \tag{1}
\]
and
\[
\mu(G \times H) \leq \mu(G) + \mu(H). \tag{2}
\]
Many sufficient conditions are known for equality to occur in (2), for example, when $G$ and $H$ have coprime order (Johnson [11, Theorem 1]), when $G$ and $H$ are nilpotent (Wright [22]), when $G$ and $H$ are direct products of simple groups (Easdown and Praeger [3]), and when $G \times H$ embeds in $\text{Sym}(9)$ (Easdown and Saunders [4]). The first published example where the inequality in (2) is strict appears in Wright [22], where $G \times H$ is a subgroup of $\text{Sym}(15)$. Saunders [17, 18] describes an infinite class of examples, which includes the example in [22] as a special case, where strict inequality takes place in (2). The smallest example in his class occurs when $G \times H$ embeds in $\text{Sym}(10)$. In all of these examples of strict inequality, the groups $G$ and $H$ have the properties that $H$ is cyclic of prime order and
\[
\mu(G \times H) = \mu(G). \tag{3}
\]
As a consequence of our investigations below into semidirect products and our two main theorems, we are able to provide infinite classes of examples where (3) occurs, where $H$ may be a product of elementary abelian groups with an arbitrarily large number of factors and different prime exponents and $G$ does not decompose as a nontrivial direct product.

Recall that the core of a subgroup $H$ of $G$, denoted by core$_G(H)$, or just core$(H)$, is the largest normal subgroup of $G$ contained in $H$, and that $H$ is core-free if core$(H)$ is trivial. Thus, if $G$ is nontrivial then $\mu(G)$ is the smallest sum of indices for a collection of subgroups $\mathcal{C} = \{H_1, \ldots, H_k\}$ such $\cap_{i=1}^k H_i$ is core-free. In this case we say that $\mathcal{C}$ affords a minimal faithful representation of $G$. The subgroups $H_1, \ldots, H_k$ become the respective point-stabilisers for the action of $G$ on its orbits and letters in the $i$th orbit may be identified with cosets of $H_i$ for $i = 1, \ldots, k$. If $k = 1$ then the representation afforded by $\mathcal{C}$ is transitive and $H_1$ is a core-free subgroup.

**Lemma 1.1.** If a group $G$ has a unique (necessarily normal) subgroup of prime order $p$ then any collection of subgroups affording a faithful representation of $G$ must include a subgroup of order not divisible by $p$.

**Proof.** Suppose $G$ has a unique normal subgroup $N$ of order $p$ and $\{H_1, \ldots, H_k\}$ affords a faithful representation. If $p$ divides $|H_i|$ for each $i$ then $N \leq \text{core}(H_1 \cap \ldots \cap H_k)$, contradicting faithfulness. Hence $|H_1|$ is not divisible by $p$ for some $i$. \qed

**Corollary 1.2.** Let $G$ be a group with unique subgroups of orders $p_1, \ldots, p_k$ respectively, where $p_1, \ldots, p_k$ are distinct primes. Then $\mu(G) \geq |G|_{p_1} + \ldots + |G|_{p_k}$, where $|G|_p$ denotes the largest power of $p$ dividing $|G|$.

**Proof.** By Lemma 1.1, any collection of subgroups of $G$ affording a minimal faithful representation must contain subgroups $H_1, \ldots, H_k$ such that $p_i$ does not divide $|H_i|$ for $i = 1, \ldots, k$. Note that if $H_{i_1} = \ldots = H_{i_\ell}$ for $i_1 < \ldots < i_\ell$ then
\[
|G : H_{i_1}| \geq |G|_{p_{i_1}} \ldots |G|_{p_{i_\ell}} \geq |G|_{p_1} + \ldots + |G|_{p_k}.
\]
It follows that $\mu(G) \geq |G|_{p_1} + |G|_{p_2} + \ldots + |G|_{p_k}$. \qed
Example 1.3. Recall the generalised quaternion or dicyclic group of order 4n for n ≥ 2 is
\[ G = Q_{4n} = \langle a, b \mid a^{2n} = b^4 = 1, a^n = b^2, a^b = a^{-1} \rangle. \] (4)
Then \( b^2 \) is the unique subgroup of \( G \) of order 2. If \( n \) is a power of 2 then \( \mu(G) \geq |G|_2 = |G| \), by Corollary 1.2, whence \( \mu(G) = |G| \), the only nonabelian case where this is possible (see Johnson [11, Theorem 2]). Suppose then that \( n \) is not a power of 2 and let \( p_1, \ldots, p_k \) be the odd prime divisors of \( n \). Then \( \langle a^{2n/p_i} \rangle \) is the unique subgroup of \( G \) of order \( p_i \) for \( i = 1, \ldots, k \). By Corollary 1.2, \( \mu(G) \geq |G|_2 + |G|_{p_1} + \ldots + |G|_{p_k} \). Write \( |G| = 2^m p_1^{\alpha_1} \ldots p_k^{\alpha_k} \) where \( m \geq 2 \) and \( \alpha_1, \ldots, \alpha_k \geq 1 \), so \( n = 2^{m-2} p_1^{\alpha_1} \ldots p_k^{\alpha_k} \). Put
\[ H = \langle a^{2^{m-1}} \rangle \quad \text{and} \quad H_i = \langle a^{2^{m-1}}, b \rangle \]
for \( i = 1, \ldots, k \). Note that if \( k = 1 \) and \( m = 2 \) then \( a^{2^{m-1}} = a^n = b^2 \), so that \( H_1 = \langle b \rangle \). Clearly \( H \cap H_1 \cap \ldots \cap H_k = \{1\} \), so \( \{H, H_1, \ldots, H_k\} \) affords a faithful representation of \( G \) of degree
\[ |G : H| + |G : H_1| + \ldots + |G : H_k| = 2^m + p_1^{\alpha_1} + \ldots + p_k^{\alpha_k} = |G|_2 + |G|_{p_1} + \ldots + |G|_{p_k} \]
Thus \( \mu(G) = |G|_2 + |G|_{p_1} + \ldots + |G|_{p_k} \). Note that if \( m = 2 \) then \( |a^2| = n \) is odd and \( G = \langle a^2, b \rangle \). The presentation (4) simplifies, replacing \( a^2 \) by \( x \):
\[ G = \langle x, b \mid x^n = b^4 = 1, x^b = x^{-1} \rangle, \] (5)
so that \( G \) becomes a semidirect product (see the next section). If we put \( n = 3 \), then \( \mu(G) = 3 + 4 = 7 \) and \( G \) becomes the smallest group with the property that it does not have a nilpotent subgroup with the same minimal degree. The class of groups that do have nilpotent subgroups with the same degree was introduced by Wright [22], and its pervasiveness within the class of permutation groups of small degree was an important tool in the work of Easdown and Saunders [4].

2. Preliminaries on semidirect products

Recall that a group \( G \) is an internal semidirect product of a normal subgroup \( N \) by a subgroup \( H \) if \( G = NH \) and \( N \cap H \) is trivial, in which case the conjugation action of \( N \) on \( H \) induces a homomorphism \( \varphi : N \to \text{Aut}(H) \). Conversely, if \( N \) and \( H \) are any groups and \( \varphi : H \to \text{Aut}(N) \) any homomorphism then the cartesian product of sets
\[ N \ltimes H = N \ltimes \varphi H = \{ (n, h) \mid n \in N, h \in H \} \]
becomes a group, called the external semidirect product, under the binary operation
\[ (n_1, h_1)(n_2, h_2) = (n_1(n_2(h^{-1} \varphi)), h_1h_2) \],
in which case \( N \ltimes H \) becomes an internal semidirect product of the normal subgroup \( N \times \{1\} \) by the subgroup \( \{1\} \times H \). By identifying \( N \) with \( N \times \{1\} \) and \( H \) with \( \{1\} \times H \), it is common to move back and forth between external and internal semidirect products, and write \( N \ltimes H = NH \) without causing confusion. We refer to \( N \) as the base group and \( H \) as the extending group. The first two claims of the following proposition are probably well-known.
Proposition 2.1. Suppose that \( G \times H = G \rtimes_\varphi H \) is a semidirect product of groups \( G \) and \( H \), not necessarily finite, via a homomorphism \( \varphi : H \to \text{Aut}(G) \). Then

\[
G \times H \cong \text{Sym}(G) \times H.
\]

If \( \varphi \) is injective then \( G \times H \cong \text{Sym}(G) \). In particular, if \( G \) and \( H \) are finite then

\[
\mu(G \times H) \leq |G| + \mu(H).
\]

If \( G \) and \( H \) are finite and \( \varphi \) is injective then \( \mu(G \times H) \leq |G| \).

Proof. Define a homomorphism \( \sigma : G \times H \to \text{Sym}(G) \) by the following rule:

\[
(g, h)\sigma : x \mapsto (xg)(h\varphi) \quad \text{for } x, g \in G, \ h \in H.
\]

Now define a homomorphism \( \tau : G \times H \to \text{Sym}(G) \times H \) by the following rule:

\[
\tau : (g, h) \mapsto ((g, h)\sigma, h) \quad \text{for } g \in G, \ h \in H.
\]

If \( g \in G, \ h \in H \) and \((g, h)\tau = (id, 1)\), where \( id : G \to G \) denotes the identity mapping, then \((g, h)\sigma = id \) and \( h = 1 \), so, in particular,

\[
1 = 1((g, h)\sigma) = 1((g, 1)\sigma) = g(1\varphi) = g id = g
\]

whence \((g, h) = (1, 1)\), verifying that \( \tau \) is an embedding. Suppose now that \( \varphi \) is injective. Let \((g, h) \in \ker \sigma \), so \((g, h)\sigma = id \). In particular, \( 1 = 1((g, h)\sigma) = g(h\varphi) \), so that \( g = 1 \), since \( h\varphi \) is an automorphism of \( G \). Hence, for all \( x \in G \),

\[
x = x((g, h)\sigma) = (xg)(h\varphi) = x(h\varphi),
\]

so that \( h\varphi = id \in \text{Aut}(G) \). Hence \( h = 1 \), since \( \varphi \) is injective, so \((g, h) = (1, 1)\). This verifies that \( \sigma \) is injective, and all of the remaining claims follow. \( \square \)

Example 2.2. The bound \( |G| + \mu(H) \) in the previous proposition can easily be achieved, for example, whenever the semidirect product is direct (that is, \( \varphi \) is trivial), \( G \) any group for which the Cayley representation is minimal and \( H \) any group of order coprime to \( |G| \). For a class of semidirect products that are not direct, let \( G = C_p^n \) and \( H = C_{q^2} \), where \( p \) and \( q \) are distinct primes and \( n \) a positive integer such that \( q > p^{n-1} \). Put \( H = \langle c \rangle \) and suppose we have a homomorphism \( \varphi : H \to \text{Aut}(G) \) such that \( |c\varphi| = q \), so \( \varphi \) is neither trivial nor injective, and that the conjugation action induced on \( G \) is irreducible. A simple subclass of examples would be when \((p, q, n) = (p, 2, 1)\) and \( c\varphi \) the inversion automorphism of \( G \) (so of order 2). (An instance of this, when \((p, q, n) = (3, 2, 1)\), features in Example 2.9 below.) We claim that

\[
\mu(G \times H) = |G| + \mu(H) = p^n + q^2.
\]

Put \( S = G \rtimes H = GH \), regarded as an internal semidirect product. Certainly \( \mu(S) \leq p^n + q^2 \), either by Proposition 2.1, or directly by noting that \( \{G, H\} \) affords a faithful representation of \( S \) of degree \( p^n + q^2 \). Let \( \mathcal{C} = \{K_1, \ldots, K_i\} \) be a collection of subgroups of \( S \) affording a minimal faithful representation of \( S \). Observe that \( \langle c^p \rangle \) is the unique subgroup of \( S \) of order \( q \). If \( n = 1 \) then \( G \) is the unique subgroup of \( S \) of order \( p \), so \( \mu(S) \geq p + q^2 \), by Corollary 1.2, establishing (6), and we are done. Suppose then that \( n > 1 \). By Lemma 1.1, \(|K_i|\) is not divisible by \( q \), for some \( i \), so \( K_i \leq G \). If \( K_i \neq G \) then

\[
|S : K_i| \geq pq^2 = (p - 1)q^2 + q^2 > (p - 1)p^{2n-2} + q^2 \geq p^n + q^2,
\]
so that $\mu(S) > p^n + q^2$, which is impossible. Hence $K_i = G$. If some $|K_j|$ is not divisible by $q$, then $K_j = G$, by what we have just shown, so $j = i$, by minimality of $\mathcal{C}$. Without loss of generality, $K_1 = G$ and $q$ divides $|K_2|, \ldots, |K_i|$. Suppose that $q^2$ does not divide $|K_2|, \ldots, |K_i|$. By faithfulness, $\{1\} = \text{core}(\cap \mathcal{C}) = G \cap \text{core}(K_2 \cap \ldots \cap K_i)$, so that $K_j \cap G \neq G$ for some $j \geq 2$, giving

$$\mu(S) \geq |S : K_1| + |S : K_j| \geq q^2 + pq > q^2 + p^n,$$

which is impossible. Hence, without loss of generality, $q^2$ divides $K_2$, so $K_2$ contains some conjugate of $e$, the generator of $H$. If $K_2 \cap G \neq \{1\}$ then $K_2 \cap G = G$, since the conjugation action of $H$ (and hence also of any conjugate of $H$) on $G$ is irreducible, so that $K_2 = S$, contradicting minimality of $\mathcal{C}$. Hence $|K_2| = q^2$, so $\mu(S) \geq |S : K_1| + |S : K_2| = q^2 + p^n$, finally establishing (6). For example, if $(p, q, n) = (5, 2, 1)$ then $\mu(S) = 5 + 4 = 9$ and we get the intransitive representation

$$S \cong C_5 \times C_4 \cong \langle (1 2 3 4 5),(1 5)(2 4)(6 7 8 9) \rangle.$$

An alternative way of seeing the final conclusion of Proposition 2.1 is in terms of a transitive representation with respect to a core-free subgroup:

**Lemma 2.3.** Let $K$ be an internal semidirect product of $G$ by $H$. Then $\text{core}(H) = \text{ker } \varphi$, where $\varphi : H \to \text{Aut}(G)$ is the homomorphism induced by conjugation. In particular, if $\varphi$ is injective then $H$ is core-free and $\{1\}$ affords a transitive representation of $K$ of degree $|G|$, so that $\mu(K) \leq |G|$. 

**Proof.** Certainly $\text{ker } \varphi$ is a normal subgroup of $K$ contained in $H$, so $\text{ker } \varphi \leq \text{core}(H)$. Conversely, $G$ and $\text{core}(H)$ normalise each other and intersect trivially, so elements of $\text{core}(H)$ commute with elements of $G$, whence $\text{core}(H) \leq \text{ker } \varphi$, and all claims follow. \qed

It will be useful, for example, below in verifying the first alternative of formula (17), to note that, under certain conditions, the minimal degree of the semidirect product coincides with the minimal degree of the base group:

**Lemma 2.4.** Suppose that $G \rtimes \varphi H$ is a semidirect product of groups such $\varphi$ is injective. If $G$ has a minimal faithful representation afforded by a collection of subgroups that are invariant under the conjugation action of $H$, then $\mu(G \rtimes H) = \mu(G)$. 

**Proof.** We may regard $G \rtimes H = GH$ as an internal semidirect product. Since $\varphi$ is injective, $H$ is core-free by Lemma 2.3. Suppose that $\{B_1, \ldots, B_k\}$ is a collection of subgroups of $G$ that are invariant under conjugation by $H$ and affords a minimal faithful representation of $G$. In particular, $\text{core}_G(B_1 \cap \ldots \cap B_k) = \{1\}$. For $i = 1$ to $k$, put $D_i = B_iH$, which is a subgroup of $GH$ of index $|G : B_i|$. Then

$$\text{core}_{GH}(D_1 \cap \ldots \cap D_k) = \text{core}_{GH}((B_1 \cap \ldots \cap B_k)H) = \text{core}_{GH}(H) = \{1\},$$

so $\{D_1, \ldots, D_k\}$ affords a faithful representation of $GH$ of degree

$$|G : B_1| + \ldots + |G : B_k| = \mu(G).$$

But $\mu(GH) \geq \mu(G)$, so we have equality and the lemma is proved. \qed
Example 2.5. Let $p, q$ be primes such that the field $\mathbb{F}_p = \{0, \ldots, p - 1\}$ has a primitive $q$th root $\zeta$ of 1. Let $\varphi : C_q \to \text{Aut}(C_p^q)$ be the homomorphism induced by the map

$$c\varphi : (x_1, x_2, \ldots, x_q) \mapsto (x_1, x_2^c, x_3^{c^2}, \ldots, x_q^{c^{q-1}}),$$

where $c$ is a generator of $C_q$ and $x_1, \ldots, x_q \in C_p$. Put $G = C_p^q \rtimes \varphi C_q$. We may write $G = KC$ as an internal semidirect product of $K \cong C_p^q$ by $C \cong C_q$, where $K$ is an internal direct product $H_1 \ldots H_q$, where $H_i \cong C_p$ for $i = 1, \ldots, q$. Put $\hat{H}_i = H_1 \ldots H_{i-1}H_{i+1} \ldots H_q$, which is a subgroup of $K$ of index $p$, for $i = 1, \ldots, q$. Put $\mathcal{C} = \{\hat{H}_1, \ldots, \hat{H}_q\}$. Then $\cap \mathcal{C}$ is trivial, so $\mathcal{C}$ affords a faithful representation of $K$ of degree $pq$. But each $\hat{H}_i$ is invariant under the conjugation action by $C$, so $\mu(G) = pq$, by Lemma 2.4. We can also find a faithful transitive representation of $G$ by letting $a_i$ be a generator for $H_i$ for each $i$ and putting

$$H = \{a_1^{i_1} \ldots a_q^{i_q} \in H_1 \ldots H_q \mid i_1 + \ldots + i_q = 0\}.$$

Then $H$ is a core-free subgroup of $G$ (in fact, a canonical codimension 1 subspace of the additive vector space corresponding to the base group, in the sense of Lemma 3.11 below) of index $pq$. For example, if $p = 7$ and $q = 3$ then 4 is a cube root in $\mathbb{F}_7$ and $G = C_7^\times \rtimes C_3$, with presentation

$$\langle a_1, a_2, a_3, b \mid a_1^7 = b^3 = 1 = [a_i, a_j] = [a_1, b] \text{ for all } i \neq j, \quad a_2^4 = a_2^4, \quad a_3^b = a_3^3 \rangle,$$

an intransitive minimal representation:

$$\langle (1 2 3 4 5 6 7), (8 9 10 11 12 13 14), (15 16 17 18 19 20 21), (9 12 10)(11 13 14)(16 17 19)(18 21 20) \rangle,$$

and a contrasting transitive representation of the same degree:


Consider groups $H$ and $K$ of coprime order and $C$ a cyclic group such that $|C|$ and $|H||K|$ are also coprime. Let $\varphi : C \to \text{Aut}(H \rtimes K)$ be a homomorphism, so that we may form the semidirect product

$$G = (H \rtimes K) \rtimes C = (H \rtimes K) \rtimes \varphi C.$$

Let $\varphi_H : C \to \text{Aut}(H)$ and $\varphi_K : C \to \text{Aut}(K)$ where, for all $h \in H, k \in K, c \in C$,

$$(h, k)(c\varphi) = (h(c\varphi_H), k(c\varphi_K)),$$

so that we have the related semidirect products

$$H \rtimes C = H \rtimes \varphi_H C \quad \text{and} \quad K \rtimes C = K \rtimes \varphi_K C.$$

If $\varphi$ is trivial then $G \cong H \times K \times C$. If $\varphi_H$ is trivial then $G \cong H \times (K \rtimes C)$. If $\varphi_K$ is trivial then $G \cong (H \times C) \rtimes K$. Note that always $G$ embeds in $(H \times C) \times (K \times C)$ under the map

$$((h, k), c) \mapsto ((h, c), (k, c)).$$
for all \( h \in H, k \in K, c \in C \), so that, by (1) and (2),
\[
\mu(G) \leq \mu((H \rtimes C) \times (K \rtimes C)) \leq \mu(H \rtimes C) + \mu(K \rtimes C).
\]  
(8)

In Theorem 2.8 below, we show that equality occurs throughout (8) when both \( \varphi_H \) and \( \varphi_K \) are nontrivial and \( C \cong C_q \) for some prime \( q \). We first establish some useful general facts.

**Lemma 2.6.** Let \( G = HC \) be an internal semidirect product of a normal subgroup \( H \) by a cyclic subgroup \( C \cong C_q \) for some prime \( q \) not dividing \( |H| \). Let \( K \) be a subgroup of \( G \) that is not a subgroup of \( H \).

(a) There exists \( g \in G \) such that \( K = (H \cap K)C^g \) is an internal semidirect product of \( H \cap K \) by \( C^g \).

(b) If \( H \cap K \) is normal in \( H \) then \( H \cap K \) is normal in \( G \).

(c) If \( K \) is normal in \( G \) then \( K = (H \cap K)C \).

**Proof.** By Sylow theory, \( H = \{ g \in G \mid q \) does not divide \( |g| \} \), and it follows that \( H \cap K = \{ k \in K \mid q \) does not divide \( |k| \} \) is normal in \( K \). But \( q \) divides \( |K| \), since \( K \) is not a subgroup of \( H \), so \( |K| = |H||q \) and \( x \in K \) for some \( x \) of order \( q \). But \( C \) and \( \langle x \rangle \) are Sylow \( q \)-subgroups of \( G \), so that \( K = (H \cap K)/\langle x \rangle = (H \cap K)C^g \) for some \( g \in G \), and (a) is proved.

Suppose that \( H \cap K \) is normal in \( H \) and put \( C = \langle c \rangle \). To show \( H \cap K \) is normal in \( G \) it suffices to check \( (H \cap K)c = H \cap K \). But \( c^g = (g^{-1}cg^{-1})c = hc \) where \( h = g^{-1}cg^{-1} \in H \), since the derived subgroup \( G' \) is a subgroup of \( H \) as \( G/H \cong C_q \) is abelian. Hence, by (a), using the facts that \( H \cap K \) is normal in \( H \) and \( K \),
\[
(H \cap K)c = (H \cap K)hc = (H \cap K)c^g = H \cap K,
\]
and (b) is proved.

Suppose finally that \( K \) is normal in \( G \). Certainly \( H \cap K \) is normal in \( H \), so that (b) holds. Hence \( H \cap K \) is normal in \( G \) and
\[
K = K^{g^{-1}} = ((H \cap K)C^g)^{g^{-1}} = (H \cap K)^{g^{-1}}C = (H \cap K)C,
\]
proving (c). \( \square \)

**Lemma 2.7.** Let \( G = HC \) be an internal semidirect product that is not direct of a normal subgroup \( H \) by a cyclic subgroup \( C \cong C_q \) for some prime \( q \) not dividing \( |H| \). Then any collection \( \mathcal{C} \) affording a minimal faithful representation of \( G \) does not contain any normal subgroup of \( G \) that is a subgroup of \( H \).

**Proof.** Let \( \mathcal{C} = \{ K_1, \ldots, K_k \} \) afford a minimal faithful representation of \( G \). Suppose, by way of contradiction, that \( \mathcal{C} \) contains a subgroup of \( H \) that is normal in \( G \). Without loss of generality, \( K_1 \leq H \) and \( K_1 \) is normal in \( G \). If \( K_1 \neq H \) then \( \text{core}(K_1C \cap H) = K_1 \) and
\[
|G : K_1C| + |G : H| = |H : K_1| + q < |H : K_1|q = |G : K_1|,
\]
so that \( \{ K_1C, H, K_2, \ldots, K_k \} \) affords a faithful representation of degree smaller than that afforded by \( \mathcal{C} \), contradicting minimality. Hence \( K_1 = H \). If \( k = 1 \), then \( C = \{ H \} \) and \( \{ 1 \} = \text{core}(H) = H \), so that \( \mu(G) = |G| \) and, by a result of Johnson [11, Theorem 1], \( G \) must be cyclic of prime power order, a Klein four-group or a generalised quaternion 2-group, which is impossible. Hence \( k > 1 \) and \( \mathcal{C} = \{ H, K_2, \ldots, K_k \} \). Put \( N = \text{core}(K_2 \cap \ldots \cap K_k) \), so \( H \cap N = \{ 1 \} \). If \( q \) does not divide \( |N| \) then \( N \leq H \), so \( N = \{ 1 \} \) and \( \{ K_2, \ldots, K_k \} \)
affords a minimal representation, again contradicting minimality. Hence \(q\) divides \(|N|\), so, by Lemma 2.6(c), \(N = (H \cap N)C = C\), yielding a contradiction, since \(C\) is not normal in \(G\). This completes the proof.

The following theorem reduces calculations of minimal degrees of semidirect products by a \(q\)-cycle, where \(q\) is a prime that does not divide the order of the base group, to those cases where the base group is a \(p\)-group for \(p \neq q\).

**Theorem 2.8.** Let \(G = (H \times K) \rtimes C\) be a semidirect product where \(H\) and \(K\) are groups of coprime order and \(C \cong C_q\) for some prime \(q\) not dividing \(|H||K|\). Then

\[
\mu(G) = \begin{cases} 
\mu(H) + \mu(K) + q & \text{if } \varphi \text{ is trivial,} \\
\mu(H) + \mu(K \rtimes C) & \text{if } \varphi_H \text{ is trivial,} \\
\mu(H \rtimes C) + \mu(K) & \text{if } \varphi_K \text{ is trivial,} \\
\mu(H \rtimes C) + \mu(K \rtimes C) & \text{if neither } \varphi_H \text{ nor } \varphi_K \text{ is trivial.}
\end{cases}
\]

**Proof.** Note that the first case is a special case of the second and third cases, and the formulae for the first three cases follow by Johnson’s result [11, Theorem 1] that \(\mu\) is additive with respect to taking direct products of groups of coprime order.

Suppose then that neither \(\varphi_H\) nor \(\varphi_K\) are trivial. We may regard \(G = HKC\) as an internal semidirect product of \(HK\) by \(C\), where \(HK\) is an internal direct product of \(H\) and \(K\). By (8), it suffices to prove

\[
\mu(G) \geq \mu(HC) + \mu(KC).
\]

(9)

Let \(C\) be a collection of subgroups of \(G\) that affords a minimal faithful permutation representation of \(G\). Since \(|H|\) and \(|K|\) are coprime, subgroups of \(HK\) have the form \(H_0K_0\) for some \(H_0 \leq H\) and \(K_0 \leq K\). By Lemma 2.6(a), subgroups of \(G\) that are not subgroups of \(HK\) have the form \(H_0K_0C\) for some \(H_0 \leq H\), \(K_0 \leq K\) and \(g \in G\), such that \(H_0K_0\) is normal in \(H_0K_0C\). By a result of Johnson [11, Lemma 1], we may assume that all elements of \(C\) are meet irreducible, so therefore have the form

\[
H_0K_0, \quad H_0K_0C^x \quad \text{or} \quad H_1K_1C^y
\]

for some \(H_0, H_1 \leq H, K_0, K_1 \leq K\) and \(x, y \in G\). In these respective cases, note that

\[
\text{core}_G(H_0K) = \text{core}_{HC}(H_0)K, \quad \text{core}_G(HK_0) = H\text{core}_{KC}(K_0),
\]

and, by Sylow theory and Lemma 2.6(c),

\[
\text{core}_G(H_1KC^x) = \begin{cases} 
\text{core}_{HC}(H_1)KC & \text{if } q \text{ divides } |\text{core}_G(H_1KC^x)|, \\
\text{core}_{HC}(H_1)K & \text{otherwise},
\end{cases}
\]

and

\[
\text{core}_G(HK_1C^y) = \begin{cases} 
H\text{core}_{KC}(K_1)C & \text{if } q \text{ divides } |\text{core}_G(HK_1C^y)|, \\
H\text{core}_{KC}(K_1) & \text{otherwise}.
\end{cases}
\]
Put

\[ \mathcal{D}_H = \{ H_0 \mid H_0 \leq H \text{ and } H_0 K \in \mathcal{C} \}, \]
\[ \mathcal{E}_H = \{ H_1 C \mid H_1 \leq H \text{ and } H_1 K C^x \in \mathcal{C} \text{ for some } x \in G \}, \]
\[ \mathcal{D}_K = \{ K_0 \mid K_0 \leq K \text{ and } H K_0 \in \mathcal{C} \}, \]
\[ \mathcal{E}_K = \{ K_1 C \mid K_1 \leq K \text{ and } H K_1 C^y \in \mathcal{C} \text{ for some } y \in G \}. \]

By inspection, the index sum of elements of \( \mathcal{C} \) in \( G \) is equal to the index sum of elements of \( \mathcal{D}_H \cup \mathcal{E}_H \) in \( HC \) added to the index sum of elements of \( \mathcal{D}_K \cup \mathcal{E}_K \) in \( KC \). Hence, to complete the proof of (9), it suffices to show that \( \mathcal{D}_H \cup \mathcal{E}_H \) and \( \mathcal{D}_K \cup \mathcal{E}_K \) afford faithful representations of \( HC \) and \( KC \) respectively. Observe that

\[ \text{core}_{HC} \left( \bigcap_{H_0 \in \mathcal{D}_H} H_0 \cap \bigcap_{H_1 C \in \mathcal{E}_H} H_1 \right) K \cap \text{core}_{KC} \left( \bigcap_{K_0 \in \mathcal{D}_K} K_0 \cap \bigcap_{K_1 C \in \mathcal{E}_K} K_1 \right) \subseteq \text{core}_{G} \left( \bigcap \mathcal{C} \right) = \{1\}. \]

In particular,

\[ \text{core}_{HC} \left( \bigcap_{H_0 \in \mathcal{D}_H} H_0 \cap \bigcap_{H_1 C \in \mathcal{E}_H} H_1 \right) = \{1\}. \]

If \( \mathcal{D}_H \neq \emptyset \) then immediately we have

\[ \text{core}_{HC} \left( \bigcap (\mathcal{D}_H \cup \mathcal{E}_H) \right) = \{1\}. \]

Suppose that \( \mathcal{D}_H = \emptyset \). If \( \mathcal{E}_H = \emptyset \) then \( \mathcal{D}_K \cup \mathcal{E}_K \neq \emptyset \) so that \( H \subseteq \text{core}_G \left( \bigcap \mathcal{C} \right) = \{1\} \), which is impossible. Hence \( \mathcal{E}_H \neq \emptyset \) and

\[ \text{core}_{HC} \left( \bigcap_{H_1 C \in \mathcal{E}_H} H_1 \right) = \{1\}. \]

If \( \text{core}_{HC}(H_1 C) \) contains an element of order \( q \) for all \( H_1 C \in \mathcal{E}_H \) then, in each case, \( \text{core}_{HC}(H_1 C) = \text{core}_{HC}(H_1)C \), so that

\[ C = \text{core}_{HC} \left( \bigcap_{H_1 C \in \mathcal{E}_H} H_1 \right) C = \bigcap_{H_1 C \in \mathcal{E}_H} \text{core}_{HC}(H_1 C) \]

is a normal subgroup of \( HC \), contradicting that \( \varphi_H \) is nontrivial. Hence, for at least one \( H_1 C \in \mathcal{E}_H \), we have \( \text{core}_{HC}(H_1 C) = \text{core}_{HC}(H_1) \), so that

\[ \text{core}_{HC} \left( \bigcap \mathcal{E}_H \right) = \text{core}_{HC} \left( \bigcap_{H_1 C \in \mathcal{E}_H} H_1 C \right) = \text{core}_{HC} \left( \bigcap_{H_1 C \in \mathcal{E}_H} H_1 \right) = \{1\}. \]

This proves that \( \mathcal{D}_H \cup \mathcal{E}_H \) affords a faithful representation of \( HC \). Similarly \( \mathcal{D}_K \cup \mathcal{E}_K \) affords a faithful representation of \( KC \), and this completes the proof of (9).

□

Example 2.9. Let \( G \) be the holomorph of \( C_3 \times C_5 \), that is,

\[ G = (C_3 \times C_5) \rtimes_{\text{id}} \text{Aut}(C_3 \times C_5) \cong (C_3 \times C_5) \rtimes (C_2 \times C_4). \]
We may regard $G = HKCD$ as an internal semidirect product of a direct product $HK$ by another direct product $CD$, where $H = \langle h \rangle \cong C_3$, $K = \langle k \rangle \cong C_5$, $C = \langle c \rangle \cong C_2 \cong \text{Aut}(C_3)$ and $D = \langle d \rangle \cong C_4 \cong \text{Aut}(C_5)$. Then $\mu(G) \geq \mu(C_3 \times C_5) = 8$ and

$$G \cong \langle h, k, c, d \mid h^3 = k^5 = c^2 = d^4 = 1, [h, k] = [c, d] = [h, d] = [k, c], h^c = h^{-1}, k^d = k^2 \rangle \cong \langle (1 \, 2 \, 3), \ (4 \, 5 \, 6 \, 7 \, 8), \ (1 \, 2), \ (4 \, 5 \, 7 \, 6) \rangle,$$

which verifies that $\mu(G) = 8$. Put $C_1 = \langle cd^2 \rangle$, $C_2 = \langle cd \rangle$, $G_1 = HKC_1$ and $G_2 = HKC_2$. Then

$$G_1 \cong \langle C_3 \times C_5 \rangle \rtimes \varphi \cong \langle (1 \, 2 \, 3), \ (4 \, 5 \, 6 \, 7 \, 8), \ (1 \, 2)(4 \, 7)(5 \, 6) \rangle,$$

where $\varphi$ induces conjugation action that is inversion, and both $C_3 \rtimes \varphi_1 C_2$ and $C_5 \rtimes \varphi_2 C_2$ are dihedral, where $\varphi_1 = \varphi_{C_3}$ and $\varphi_2 = \varphi_{C_5}$ are defined by (7), and both nontrivial. As predicted by Theorem 2.8,

$$\mu(G_1) = 8 = 3 + 5 = \mu(C_3 \rtimes \varphi_1 C_2) + \mu(C_5 \rtimes \varphi_2 C_2).$$

However

$$G_2 \cong \langle C_3 \times C_5 \rangle \rtimes \psi \cong \langle (1 \, 2 \, 3), \ (4 \, 5 \, 6 \, 7 \, 8), \ (1 \, 2)(4 \, 5 \, 7 \, 6) \rangle,$$

where $C_3 \rtimes \psi_1 C_4$ is generalised quaternion of degree 7 (see Example 1.3) and $C_5 \rtimes \psi_2 C_4$ has degree $\mu(C_5) = 5$, by Lemma 2.4, where $\psi_1 = \psi_{C_3}$ and $\psi_2 = \psi_{C_5}$ are defined by (7). Here

$$\mu(G_2) = 8 < 12 = 7 + 5 = \mu(C_3 \rtimes \psi_1 C_4) + \mu(C_5 \rtimes \psi_2 C_4).$$

This is the smallest example where we do not get equality throughout in (8), yet all of the homomorphisms defining the semidirect products are nontrivial.

### 3. Preliminaries on group actions on a vector space

The aim in this section is to develop enough machinery to calculate, in the next section, the minimal degrees of all semidirect products of elementary abelian $p$-groups by cyclic groups of order $q$ where $p$ and $q$ are different primes. We exploit the fact that an elementary abelian $p$-group is a vector space over the field $\mathbb{F}_p$ of $p$ elements, so that group actions may be analysed using standard methods from linear algebra. The machinery also allows us, in this section, to characterise group isomorphism for this particular class of semidirect products.

Let $V$ be an $n$-dimensional vector space over $\mathbb{F}_p$, written additively, and $T : V \to V$ an invertible linear transformation. Define the semidirect product of $V$ by $\langle T \rangle$ (or more simply the semidirect product of $V$ by $T$) to be

$$V \rtimes T = V \rtimes \langle T \rangle = \{(v, T^i) \mid v \in V, i \in \mathbb{Z}\},$$

with binary operation

$$(v, T^i)(w, T^j) = (v + T^i(w), T^{i+j}),$$

for $v, w \in V$ and $i \in \mathbb{Z}$. Then $V \rtimes T$ becomes a group. A subspace of $V$ that is $T$–invariant is referred to simply as invariant. Thus invariant subspaces of $V$ become normal subgroups of $V \rtimes T$. We define the core of any subspace $W$ of $V$, denoted by $\text{core}(W)$, to be the largest invariant subspace of $V$ contained in $W$. Thus $\text{core}(W) = \text{core}_G(W)$, in the sense defined earlier, as the largest normal subgroup of $G$ contained in $W$, where $G = V \rtimes T$. 


We suppose throughout, unless stated otherwise, that \( T \neq \text{id} \) and \( T^q = \text{id} \), where \( \text{id} \) is the identity linear transformation and \( q \) is a prime different to \( p \). The characteristic and minimal polynomials of \( T \) are referred to as \( \chi_T = \chi_T(x) \) and \( \phi_T = \phi_T(x) \) respectively. By choosing a basis for \( V \) we may identify \( V \) with the vector space \( \mathbb{F}_p^n \) of column vectors of length \( n \) with entries from \( \mathbb{F}_p \) and \( T \) with the \( n \times n \) matrix of the linear transformation with respect to the basis, and so regard \( T(v) =Tv \) as a matrix product. Under these identifications \( V \times T \cong C_p \ltimes \varphi C_q \)

under the map

\[
\left( \begin{array}{c}
\lambda_1 \\
\vdots \\
\lambda_n
\end{array} \right), T^i \mapsto ((a^{\lambda_1}, \ldots, a^{\lambda_n}), b^{-i}),
\]

where we write \( C_p = \langle a \rangle \), \( C_q = \langle b \rangle \), and \( \varphi : C_q \to \text{Aut}(C_p^n) \) is the homomorphism induced by \( b\varphi : (a^{\lambda_1}, \ldots, a^{\lambda_n}) \mapsto (a^{\lambda_1'}, \ldots, a^{\lambda_n'}) \) where \( T \left[ \begin{array}{c}
\lambda_1 \\
\vdots \\
\lambda_n
\end{array} \right] = \left[ \begin{array}{c}
\lambda_1' \\
\vdots \\
\lambda_n'
\end{array} \right] \).

**Lemma 3.1.** Let \( T_1 \) and \( T_2 \) be \( n \times n \) matrices over \( \mathbb{F}_p \) of multiplicative order \( q \) and put \( V = \mathbb{F}_p^n \) for some positive integer \( n \). Then \( V \times T_1 \cong V \times T_2 \) if and only if \( T_1 \) and some power of \( T_2 \) are conjugate. In particular, if \( T_1 \) and \( T_2 \) are conjugate, then \( V \times T_1 \cong V \times T_2 \).

**Proof.** If \( T_1 \) and \( T_2^k \) are conjugate, for some \( k \in \mathbb{Z} \), then \( k \neq 0 \) modulo \( q \), \( T_1 = P^{-1}T_2^kP \) for some invertible matrix \( P \), and the mapping

\[
(v, T_1^i) \mapsto (Pv, T_2^{ki}), \quad (12)
\]

for \( v \in V \) and \( i \in \mathbb{Z} \), is an isomorphism from \( V \times T_1 \) to \( V \times T_2 \).

Suppose conversely that \( \theta : V \times T_1 \to V \times T_2 \) is an isomorphism. Then

\[
(0, T_1)\theta = (w, T_2^k)
\]

for some \( w \in V \) and integer \( k \). In fact, we will show \( T_1 \) and \( T_2^k \) are conjugate. Note that

\[
(v, I)\theta \in V \times \{ I \}
\]

for all \( v \in V \), since the order of \( (v, I) \) divides \( p \) and \( \theta \) is a homomorphism. For \( i = 1, \ldots, n \), denote by \( e_i \) the column vector with zero everywhere except for 1 in the \( i \)-th place (a standard basis vector). All vectors in \( V \) are linear combinations of \( e_1, \ldots, e_n \). For \( \lambda \in \mathbb{F}_p = \{0, \ldots, p-1\} \), define, for \( v \in V \),

\[
\lambda(v, I) = (\lambda v, I) = (v, I)^{\lambda}.
\]

Since \( \theta \) is a homomorphism, we have, for all \( v \in V \),

\[
(\lambda(v, I))\theta = \lambda((v, I)\theta).
\]

For each \( i = 1, \ldots, n \), we have

\[
(e_i, I)\theta = (p_i, I)
\]

for some \( p_i \in V \). Put

\[
P = [p_1 \ldots p_n],
\]
the matrix whose columns are just \( p_1, ..., p_n \). Observe that \( p_i = Pe_i \) for \( i = 1 \) to \( n \). Let \( v \in V \), so \( v = \sum_{i=1}^{n} \lambda_i e_i \) for some \( \lambda_i \in \mathbb{F}_p \). Then

\[
(v, I)\theta = \left( \sum_{i=1}^{n} \lambda_i e_i, I \right) \theta = \left( \prod_{i=1}^{n} \lambda_i (e_i, I) \right) \theta = \prod_{i=1}^{n} \lambda_i (p_i, I) = \left( \sum_{i=1}^{n} \lambda_i p_i, I \right) = \left( P \left( \sum_{i=1}^{n} \lambda_i e_i \right), I \right) = (Pv, I).
\]

It is immediate, since \( \theta \) is an isomorphism, that \( P \) is invertible. On the one hand,

\[
(v, T_1)\theta = ((v, I)(0, T_1))\theta = ((v, I)\theta)(0, T_1)\theta = (Pv, I)(w, T_2^k) = (Pv + w, T_2^k),
\]

whilst on the other hand,

\[
(v, T_1)\theta = ((0, T_1)(T_1^{-1}v, I))\theta = (0, T_1)\theta(T_1^{-1}v, I)\theta = (w, T_2^k)(PT_1^{-1}v, I) = (w + T_2^k PT_1^{-1}v, T_2^k).
\]

Hence, for all \( v \in V \), \( Pv = T_2^k PT_1^{-1}v \), so \( v = P^{-1}T_2^k PT_1^{-1}v \). Thus \( P^{-1}T_2^k PT_1^{-1} = I \), so \( T_1 = P^{-1}T_2^k P \), that is, \( T_1 \) and \( T_2^k \) are conjugate, completing the proof of the lemma. \( \square \)

Thus, in calculating minimal degrees later, we may assume \( T \) is in primary rational canonical form. By Maschke’s theorem, since \( p \) does not divide \( q = |\langle T \rangle| \), all invariant subspaces of \( V \) have invariant complements, so that the minimal polynomial \( \phi_T \) is square-free with regard to irreducible factors. All blocks in the primary rational canonical form of \( T \) become companion matrices of monic irreducible polynomials, and the restriction of \( T \) to an indecomposable subspace of \( V \) will always have an irreducible minimal polynomial. The canonical form is thus characterised uniquely, up to the order of blocks, by \( \chi_T \). The number of blocks corresponding to one particular irreducible factor is just the multiplicity of that factor in \( \chi_T \). An irreducible factor of \( \phi_T = \phi_T(x) \) divides \( x^q - 1 \), so is either \( x - 1 \) or a polynomial of the form

\[
\pi_\alpha(x) = (x - \alpha)(x - \alpha^p) \ldots (x - \alpha^{p^{s-1}})
\]

where \( s \) is the multiplicative order of \( p \) modulo \( q \) and \( \alpha \) is a primitive \( q^\text{th} \) root of 1 in an extension field \( \mathbb{F} = \mathbb{F}_p(\alpha) \) of \( \mathbb{F}_p \) (where \( \mathbb{F} = \mathbb{F}_p \) if \( s = 1 \)).

Fix \( \alpha \) and \( \mathbb{F} = \mathbb{F}_p(\alpha) \) from the previous paragraph. Then \( \beta \in \mathbb{F} \) is a primitive \( q^\text{th} \) root of 1 if and only if \( \beta \) is a nontrivial power of \( \alpha \). Recall that \( n = \dim V \). Let \( X_n \) be the set of nonnegative compositions of \( n \) in \( q \) parts:

\[
X_n = \{(k, k_1, \ldots , k_{q-1}) \mid k, k_1, \ldots , k_{q-1} \geq 0 \text{ and } k + k_1 + \ldots + k_{q-1} = n\}.
\]

Consider \( x = (k, k_1, \ldots , k_{q-1}) \in X_n \) and define the following polynomial \( P_x(y) \in \mathbb{F}_p[x, y] \), where \( x \) and \( y \) are indeterminates:

\[
P_x(y) = (x - 1)^k (x - y)^{k_1} (x - y^2)^{k_2} \ldots (x - y^{q-1})^{k_{q-1}}.
\]

Note, when \( x = (n, 0, \ldots , 0) \), that \( P_x(\alpha) = (x - 1)^n \), the characteristic polynomial of the \( n \times n \) identity matrix. In general, \( P_x(\alpha) \in \mathbb{F}[x] \), and \( P_x(\alpha) \in \mathbb{F}_p[x] \) if and only if \( P_x(\alpha) \) is a product of polynomials of the form \( x - 1 \) and \( \pi_\beta(x) \), defined as in (13), where \( \beta \) ranges over nontrivial powers of \( \alpha \). Further, if \( P_x(\alpha) \in \mathbb{F}_p[x] \), then \( P_x(\alpha) = \chi_T \), where \( T \) is the
matrix direct sum of companion matrices of irreducible polynomials, and it follows, by a
comparison of multiplicities of eigenvalues, that for \( i \in \{ 1, \ldots, q - 1 \} \),
\[
P_x(\alpha^i) = \chi_T^i.
\] (14)
Now put
\[
X_n^* = \{ x \in X_n \mid P_x(\alpha) \in \mathbb{F}_p[x] \text{ and } x \neq (n,0,\ldots,0) \}
\]
and
\[
\Pi_n = \{ P_x(\alpha) \mid x \in X_n^* \}.
\]
Then \( \Pi_n \) is precisely the set of characteristic polynomials of \( n \times n \) matrices over \( \mathbb{F}_p \) of
multiplicative order \( q \). Moreover, the map \( \theta : X_n^* \rightarrow \Pi_n, \ x \mapsto P_x(\alpha) \) is a bijection.

The field \( \mathbb{F}_q \) has a primitive element, so we can choose \( i \in \{ 1,\ldots,q-1 \} \) such that the
multiplicative order of \( i \) modulo \( q \) is \( q-1 \). Observe that, if \( x \in X_n^* \), then
\[
P_x(\alpha^i) = P_{x\nu}
\]
for some \( x\nu \in X_n^* \). Then \( \nu \) becomes a well-defined permutation of \( X_n^* \). This, in turn,
induces a permutation \( \hat{\nu} \) of \( \Pi_n \) given by the following rule
\[
\hat{\nu} : P_x(\alpha) \mapsto P_x(\alpha^i) = P_{x\nu}(\alpha).
\] (15)
Note that \( \nu, \hat{\nu} \) and \( \theta \) are intertwined, in the sense that \( \nu \theta = \theta \hat{\nu} \).

**Lemma 3.2.** Let \( x_1, x_2 \in X_n^* \). The following are equivalent:

(i) \( x_1 \) and \( x_2 \) lie in the same orbit of \( \nu \).

(ii) \( P_{x_1}(\alpha) \) and \( P_{x_2}(\alpha) \) lie in the same orbit of \( \hat{\nu} \).

(iii) There exists a matrix \( T \) of multiplicative order \( q \) and \( \ell \in \{ 1,\ldots,q-1 \} \) such that
\[
P_{x_1}(\alpha) = \chi_T^\ell \text{ and } P_{x_2}(\alpha) = \chi_T^{\ell i}.
\]

**Proof.** Certainly (i) and (ii) are equivalent since \( \nu, \hat{\nu} \) and \( \theta \) are intertwined. Suppose (ii)
holds. Hence there is some \( j \geq 0 \) such that
\[
P_{x_2}(\alpha) = (P_{x_1}(\alpha))^{\hat{\nu}^j} = P_{x_1^{\nu^j}}(\alpha) = P_{x_1}(\alpha^{i^j}) = P_{x_1}(\alpha^\ell),
\]
where \( \ell = i^j \). Certainly, \( \ell \in \{ 1,\ldots,q-1 \} \) and \( P_{x_1}(\alpha) = \chi_T^\ell \) for some matrix \( T \) of order \( q \).
Then \( P_{x_2}(\alpha) = \chi_T^{\ell i} \), by (14), so (iii) holds.

Suppose (iii) holds, so there exists a matrix \( T \) of order \( q \) and \( \ell \in \{ 1,\ldots,q-1 \} \) such that
\[
P_{x_1}(\alpha) = \chi_T^\ell \text{ and } P_{x_2}(\alpha) = \chi_T^{\ell i}.
\]
But, \( \ell = i^j \) for some \( j \in \{ 1,\ldots,q-1 \} \), by primitivity of \( i \). It follows, again by (14), that
\[
P_{x_2}(\alpha) = \chi_T^{\ell i} = P_{x_1}(\alpha^\ell) = P_{x_1}(\alpha^{i^j}) = P_{x_1^{\nu^j}}(\alpha),
\]
so that \( x_2 = x_1 \nu \), and (i) holds, completing the proof. \( \Box \)

Note that everything simplifies if \( q = 2 \): \( \alpha = -1 \in \mathbb{F} = \mathbb{F}_p \),
\[
\Pi_n = \{(x - 1)^k(x + 1)^{k_1} \mid k \geq 0, k_1 > 0 \text{ and } k + k_1 = n\}
\] (16)
and \( \nu \) and \( \hat{\nu} \) are identity permutations.

We can now characterise group isomorphism for our class of semidirect products:
Theorem 3.3. For \( i = 1 \) and \( 2 \), let \( V_i \) be an \( n_i \)-dimensional vector space over \( \mathbb{F}_{p_i} \) and \( T_i : V_i \to V_i \) be a linear transformation of order \( q_i \), where \( p_i \) and \( q_i \) are distinct primes. Then \( V_1 \times T_1 \cong V_2 \times T_2 \) if and only if \( p_1 = p_2 \), \( q_1 = q_2 \), \( n_1 = n_2 \) and both \( \chi_{T_1} \) and \( \chi_{T_2} \) lie in the same orbit of \( \hat{\nu} \), defined as above where \( n = n_1, p = p_1 \) and \( q = q_1 \).

Proof. Suppose that \( V_1 \times T_1 \cong V_2 \times T_2 \). Since neither semidirect products is direct, the base groups are isomorphic, and the extending groups are isomorphic. It follows that \( p_1 = p_2 \), \( q_1 = q_2 \) and \( n_1 = n_2 \). By Lemma 3.1, \( T_2 \) is conjugate to some power of \( T_1 \), say \( T_1^\ell \), for some \( \ell \in \{1, \ldots, q_1 - 1\} \). Hence \( \chi_{T_1} \) and \( \chi_{T_2} = \chi_{T_1}^\ell \) lie in the same orbit of \( \hat{\nu} \), by Lemma 3.2.

Suppose conversely that \( p_1 = p_2 = p \), \( q_1 = q_2 = q \), \( n_1 = n_2 = n \) and \( \chi_{T_1} \) and \( \chi_{T_2} \) lie in the same orbit of \( \hat{\nu} \). Then \( \chi_{T_1} = P_{x_1}(\alpha) \) and \( \chi_{T_2} = P_{x_2}(\alpha) \) for some \( x_1, x_2 \in X_n^\ast \).

By Lemma 3.2, \( P_{x_2}(\alpha) = \chi_{T_2} \) for some \( \ell \), so that \( T_2 \) and \( T_1^\ell \) are conjugate, since they have the same characteristic polynomial. Thus \( V_1 \times T_1 \cong V_2 \times T_2 \), by Lemma 3.1.

Example 3.4. Take \( n = 3 \), \( p > 2 \) and \( q = 2 \). This is an instance of (16), where \( X_n^3 = \{(2, 1), (1, 2), (0, 3)\} \).

\[ \Pi_3 = \{(x - 1)^2(x + 1), (x - 1)(x + 1)^2, (x - 1)^3\} \]

and \( \nu \) and \( \hat{\nu} \) are trivial. For each \( p \), there are three isomorphism classes, represented by the diagonal matrices

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & -1
\end{bmatrix},
\begin{bmatrix}
1 & 0 & 0 \\
0 & -1 & 0 \\
0 & 0 & -1
\end{bmatrix},
\begin{bmatrix}
-1 & 0 & 0 \\
0 & -1 & 0 \\
0 & 0 & -1
\end{bmatrix}.
\]

If \( T \) is any of these matrices and \( V = \mathbb{F}_{p_1}^3 \), then \( \mu(V \rtimes T) = 3p \), by Lemma 2.4 (or by Lemma 4.2 below).

Example 3.5. Take \( n = 2 \), \( p = 7 \) and \( q = 3 \). Then \( s = 1 \) and \( i = 2 \). We may take \( \alpha = 2 \). We have \( X_n^2 = \{(1, 1, 0), (1, 0, 1), (0, 1, 1)\} \).

\[ \Pi_2 = \{(x - 1)(x - 2), (x - 1)(x - 4), (x - 2)(x - 4)\} \]

and \( \nu \) and \( \hat{\nu} \) are transpositions that fix \((0, 1, 1)\) and \((x - 2)(x - 4)\) respectively, so each has two orbits. Thus there are two isomorphism classes, represented by the diagonal matrices

\[
\begin{bmatrix}
1 & 0 \\
0 & 2
\end{bmatrix}
\quad \text{and} \quad
\begin{bmatrix}
2 & 0 \\
0 & 4
\end{bmatrix}.
\]

If \( T \) is either of these matrices and \( V = \mathbb{F}_{p_1}^2 \), then \( \mu(V \rtimes T) = 14 \), by Lemma 2.4 (or by Lemma 4.2 below), and we get the following minimal permutation representations, for the group with the first matrix:

\[
\langle \langle 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \rangle, \langle 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \rangle, \langle 9 \ 10 \ 12 \rangle(11 \ 14 \ 13) \rangle,
\]

and for the second:

\[
\langle \langle 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \rangle, \langle 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \rangle, \langle 2 \ 3 \ 5 \rangle(4 \ 7 \ 6)(9 \ 12 \ 10)(11 \ 13 \ 14) \rangle.
\]

Example 3.6. Take \( n = 6 \), \( p = 13 \) and \( q = 7 \). Then \( s = 3 \) and, in generating \( \nu \) and \( \hat{\nu} \), we may take \( i = 2 \). The relevant irreducible polynomials, other than \( x - 1 \), have degree \((q - 1)/s = 2 \), and we may presume \( \alpha \) is chosen such that they are

\[
r_1 = r_1(x) = (x - \alpha)(x - \alpha^p) = (x - \alpha)(x - \alpha^6) = x^2 + 3x + 1,
\]

\[
r_2 = r_2(x) = (x - \alpha^2)(x - \alpha^{2p}) = (x - \alpha^2)(x - \alpha^5) = x^2 + 6x + 1,
\]

\[
r_3 = r_3(x) = (x - \alpha^3)(x - \alpha^{3p}) = (x - \alpha^3)(x - \alpha^4) = x^2 + 5x + 1.
\]
We denote a composition of 6 in 7 parts as a string of digits. Arranged in orbits of \( \nu \),

\[
X_6^\nu = \{4100001, 4010010, 4001100\} \cup \{2200002, 2020020, 2002200\} \\
\cup \{2110011, 2101101, 2011110\} \cup \{0300003, 0030030, 0003300\} \\
\cup \{0210012, 0021120, 0102201\} \cup \{0120021, 0012210, 0201102\} \cup \{0111111\},
\]

and, arranged in orbits of \( \hat{\nu} \),

\[
\Pi_6 = \{(x - 1)^4r_1, (x - 1)^4r_2, (x - 1)^4r_3\} \cup \{(x - 1)^2r_1^2, (x - 1)^2r_2^2, (x - 1)^2r_3^2\} \\
\cup \{(x - 1)^2r_1r_2, (x - 1)^2r_2r_3, (x - 1)^2r_1r_3\} \cup \{r_1^3, r_2^3, r_3^3\} \\
\cup \{r_1^2r_2, r_2^2r_3, r_1^2r_3\} \cup \{r_1r_2r_3\}.
\]

The intertwining bijection \( \theta \) maps elements of \( X_6^\nu \) to \( \Pi_6 \) exactly in the order listed above. Thus there are 7 isomorphism classes for \( V \rtimes T \), where \( V = F_{13}^3 \) and \( T \) is a 6 \( \times \) 6 matrix of order 7. Note that here \( q < p^{r-1} \) for purposes of reading alternatives in the formulae of Theorems 4.5 and 4.9 below. If \( G_1, G_2, G_3 \) are groups of the form \( V \rtimes T \) representing the first 3 isomorphism classes, in the order of orbits given above, then, by formula (24),

\[
\mu(G_1) = 3p + pq = 130, \quad \mu(G_2) = 2pq = 182 \quad \text{and} \quad \mu(G_3) = p + pq = 104.
\]

If \( G_4, G_5, G_6, G_7 \) represent the last 4 isomorphism classes, in order, then, by formula (17),

\[
\mu(G_4) = 3pq = 273, \quad \mu(G_5) = \mu(G_6) = 2pq = 182 \quad \text{and} \quad \mu(G_7) = pq = 91.
\]

Our techniques in principle allow us to determine when two groups in our class are isomorphic, but also to exhibit isomorphisms when they exist.

**Example 3.7.** Consider the following groups:

\[
H_1 = \langle a_1, \ldots, a_6, b \mid a_i^{13} = b^7 = 1 = [a_i, a_j] \text{ for all } i \text{ and } j \neq i, \quad \\
\quad a_i^b = a_2, a_i^b = a_1^{-1}a_2^{-3}, a_i^b = a_4, a_i^b = a_3^{-1}a_4^{-5}, a_i^b = a_6, a_i^b = a_5^{-1}a_6^{-6} \rangle,
\]

\[
H_2 = \langle a_1, \ldots, a_6, b \mid a_i^{13} = b^7 = 1 = [a_i, a_j] \text{ for all } i \neq j, \quad \\
\quad a_i^b = a_2, a_i^b = a_1^{-1}a_2^{-3}, a_i^b = a_4, a_i^b = a_3^{-1}a_4^{-5}, a_i^b = a_6, a_i^b = a_5^{-1}a_6^{-6} \rangle,
\]

\[
H_3 = \langle a_1, \ldots, a_6, b \mid a_i^{13} = b^7 = 1 = [a_i, a_j] \text{ for all } i \neq j, \quad \\
\quad a_i^b = a_2, a_i^b = a_1^{-1}a_2^{-3}, a_i^b = a_4, a_i^b = a_3^{-1}a_4^{-5}, a_i^b = a_6, a_i^b = a_5^{-1}a_6^{-6} \rangle.
\]

Then \( H_k \cong V \rtimes T_k \), for \( k = 1, 2, 3 \), where \( V = F_{13}^6 \) and, using \( r_1, r_2, r_3 \) from Example 3.6,

\[
T_1 = \begin{bmatrix}
0 & -1 & 0 & 0 & 0 & 0 \\
1 & -3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 1 & -3 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 1 & -6
\end{bmatrix},
\]
which is in rational canonical form, and clearly $\chi_{T_1} = r_1^2 r_2$.

$$T_2 = \begin{bmatrix} 1 & -5 & 1 & 1 & 1 & 1 \\ 1 & -4 & 3 & 1 & 3 & 1 \\ 0 & 0 & 0 & -6 & -1 & -1 \\ 0 & 0 & -2 & -5 & -3 & -1 \\ 0 & 0 & 0 & 0 & 1 & -5 \\ 0 & 0 & 0 & 0 & 1 & -4 \end{bmatrix} \quad \text{and} \quad T_3 = \begin{bmatrix} 1 & 6 & 3 & -2 & 3 & -2 \\ 1 & -6 & 5 & -2 & 5 & -2 \\ 0 & 0 & -2 & -5 & -3 & 2 \\ 0 & 0 & -4 & -4 & -5 & 2 \\ 0 & 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 1 & -6 \end{bmatrix}.$$ 

It is straightforward to verify that $\chi_{T_2} = r_1^2 r_3$ and $\chi_{T_3} = r_2 r_3^2$. These lie in the same orbit of $\hat{\nu}$ (see Example 3.6), so $H_2 \cong H_3$. However, $H_2 \ncong H_1$, since $\chi_{T_1}$ lies in a different orbit. To find an explicit isomorphism between $H_2$ and $H_3$, one can check that $T_2 = P^{-1}T_3^2 P$ where

$$P = \begin{bmatrix} -2 & -3 & -2 & -1 & -2 & -1 \\ 1 & -1 & 0 & 4 & 0 & 4 \\ 0 & 0 & 0 & -2 & 2 & 1 \\ 0 & 0 & 1 & -5 & 0 & -4 \\ 0 & 0 & 0 & 0 & -2 & -3 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}.$$

The mapping (12) translates into an isomorphism from $H_2$ to $H_3$, identifying the generators $a_1, \ldots, a_6$ with standard basis vectors and $b^{-1}$ with a matrix, induced by

$$a_1 \mapsto a_1^{-2} a_2, \quad a_2 \mapsto a_1^{-3} a_2^{-1}, \quad a_3 \mapsto a_1^{-2} a_4, \quad a_4 \mapsto a_1^{-1} a_2 a_3 a_4^{-2} a_5^{-5},$$
$$a_5 \mapsto a_1^{-2} a_3 a_5^{-2} a_6, \quad a_6 \mapsto a_1^{-1} a_2 a_3 a_4^{-1} a_5^{-3} a_6^{-1}, \quad b \mapsto b^2.$$

The following two lemmas are probably well-known, and the first part of the first lemma is a variation of the familiar modular law.

**Lemma 3.8.** Let $W$ be a subspace of a vector space $V$. Suppose that $V = K \oplus K'$ for some subspaces $K$ and $K'$ such that $K$ is also a subspace of $W$. Put $L = W \cap K'$. Then

$$W = K \oplus L.$$ 

The codimension of $L$ in $K'$ is the same as the codimension of $W$ in $V$. If, further, $T : V \to V$ is a linear transformation and $K$ is the core of $W$ with respect to $T$ then $L$ is core-free.

**Proof.** All of the claims follow quickly from the definitions.

**Lemma 3.9.** Let $T : V \to V$ be an invertible linear transformation such that $\phi_T$ has degree $d$. Let $W$ be a subspace of $V$ of codimension $k$. Then $\text{core}(W)$ has codimension at most $kd$. In particular, if $W$ has codimension 1 then $\text{core}(W)$ has codimension at most $d$.

**Proof.** The claim follows from the fact that $\text{core}(W) = W \cap T(W) \cap \ldots \cap T^{d-1}(W)$ and $W, T(W), \ldots, T^{d-1}(W)$ all have the same codimension in $V$, since $T$ is invertible.

**Proposition 3.10.** Let $T : V \to V$ be an invertible linear transformation of a finite dimensional vector space $V$ such that $\phi_T$ is a product of distinct irreducible factors. Let $W$ be a codimension 1 subspace of $V$. Then any invariant complement of $\text{core}(W)$ in $V$ is a sum of indecomposable subspaces with distinct minimal polynomials.
Proof. Let $\phi_T(x) = r_1(x)\ldots r_m(x)$ where $r_1,\ldots,r_m$ are the distinct irreducible factors. Put $V_i = \ker(r_i(T))$ and $W_i = \text{core}(W) \cap V_i$ for $i = 1,\ldots,m$. Then $\text{core}(W) = W_1 \oplus \ldots \oplus W_m$. Let $i \in \{1,\ldots,m\}$. Let $k_i$ be the number of indecomposable components of $V$ having minimal polynomial $r_i$, which is just the number of indecomposable components of $V_i$. To complete the proof, therefore, by the Krull-Schmidt theorem, it suffices to show that the number of indecomposable components of $W_i$ is $k_i$ or $k_i - 1$. Let $d_i$ be the degree of $r_i$. Observe that $W_i = \text{core}_{V_i}(W \cap V_i)$. But $W \cap V_i$ has codimension at most 1 in $V_i$. Thus $W_i$ has codimension at most $d_i$ in $V_i$, by Lemma 3.9. But $d_i$ is the dimension of any indecomposable component of $V_i$, so $W_i$ contains at least $k_i - 1$ indecomposable components, completing the proof. \hfill \square

Lemma 3.11. Let $T : V \to V$ be a linear transformation such that $\phi_T = r_1\ldots r_m$ for distinct irreducible polynomials $r_1,\ldots,r_m$. Suppose that $V = V_1 \oplus \ldots \oplus V_m$ where $V_i = \ker(r_i(T))$ is indecomposable for $i = 1,\ldots,m$. Let $B_i$ be a basis for $V_i$ for $i = 1,\ldots,m$ and put $B = B_1 \cup \ldots \cup B_m$, which is a basis for $V$. Put

$$\hat{V} = \left\{ \sum_{b \in B} \lambda_b b \in V \mid \sum_{b \in B} \lambda_b = 0 \right\}.$$ 

Then $\hat{V}$ is a core-free subspace of codimension 1. Conversely, if $W$ is a core-free subspace of codimension 1 then we can choose a basis $B_i$ for $V_i$ for $i = 1,\ldots,m$ such that $W = \hat{V}$.

Proof. Put $n = \dim(V)$. If $n = 1$ then all of the claims hold trivially, so we may suppose throughout that $n \geq 2$.

If $B = \{v_1,\ldots,v_n\}$ then $\{v_1 - v_2,\ldots,v_1 - v_n\}$ is a basis for $\hat{V}$, so $\dim(\hat{V}) = n - 1$. Because $r_1,\ldots,r_m$ are distinct, $V_1,\ldots,V_m$ are the unique indecomposable subspaces, and none of these is contained in $\hat{V}$, so $\text{core}(\hat{V}) = \{0\}$.

Conversely, let $W$ be a codimension 1 subspace of $V$ such that $\text{core}(W) = \{0\}$. Choose any basis $B'_i$ for $W \cap V_i$. Certainly, $W \cap V_1$ has codimension 1 in $V_1$, since $\text{core}(W) = \{0\}$. Hence $B'_1 \cup \{v_1\}$ is a basis for $V_1$ for some $v_1 \in V_1$. Put

$$B_1 = \{b + v_1 \mid b \in B'_1\} \cup \{v_1\}.$$ 

Then $B_1$ is also a basis for $V_1$. If $m = 1$ then $V = V_1$ and it follows quickly from the definition that $\hat{V} = W$. This starts an induction. Suppose $m > 1$ and put $\hat{V} = V_2 \oplus \ldots \oplus V_m$, so that $V = V_1 \oplus \hat{V}$. Certainly, $W \cap \hat{V}$ has codimension 1 in $\hat{V}$, since $\text{core}(W) = \{0\}$. Suppose, as an inductive hypothesis, that we have bases $B_2,\ldots,B_m$ for $V_2,\ldots,V_m$ respectively, such that

$$W \cap \hat{V} = \left\{ \sum_{c \in C} \lambda_c c \in \hat{V} \mid \sum_{c \in C} \lambda_c = 0 \right\},$$

where $C = B_2 \cup \ldots \cup B_m$. Observe that $(W \cap V_1) \oplus (W \cap \hat{V})$ has codimension 1 in $W$, so we may choose some $w \in W \setminus ((W \cap V_1) \oplus (W \cap \hat{V}))$. But $w = v + \hat{v}$ for some unique $v \in V_1$ and $\hat{v} \in \hat{V}$. If one of $v$ or $\hat{v}$ is in $W$ then both are, contradicting the choice of $w$. Hence $v, \hat{v} \not\in W$. But $\hat{v} = \sum_{c \in C} \lambda_c c$ for some scalars $\lambda_c$. Put

$$\lambda = \sum_{c \in C} \lambda_c.$$
By the inductive hypothesis, $\lambda \neq 0$. Now put 
\[ B_1 = \left\{ b - \frac{1}{\lambda} v \mid b \in B'_1 \right\} \cup \left\{ -\frac{1}{\lambda} v \right\}, \]
so that $B_1$ is a basis for $V_1$. Finally, put $B = B_1 \cup \ldots \cup B_m$ and form $\hat{V}$ with respect to $B$. But,
\[ w = v + \hat{v} = -\lambda \left( -\frac{1}{\lambda} v \right) + \sum_{c \in C} \lambda c c \]
and $-\lambda + \sum_{c \in C} \lambda c = -\lambda + \lambda = 0$, so that $w \in \hat{V}$, by definition. Noting that
\[ W = \langle w \rangle \oplus (W \cap V_1) \oplus (W \cap \hat{V}), \]
it is straightforward, using the inductive hypothesis, to verify that $W \subseteq V$. Because $\dim(W) = n - 1 = \dim(V)$, we have $W = \hat{V}$, establishing the inductive step, and completing the proof of the lemma. □

We call the subspace $V$ defined in the statement of the previous lemma, the canonical core-free subspace associated with $V$ (depending of course on the choice of basis).

**Proposition 3.12.** Let $W$ be a subspace of a finite dimensional vector space $V$ over $\mathbb{F}_p$ acted on by an invertible linear transformation $T : V \to V$ of order $q$, where $p$ and $q$ are distinct primes. Then $W$ has codimension 1 if and only if some (and hence every) invariant complement $\text{core}(W)'$ of $\text{core}(W)$ in $V$ is a sum of indecomposable components with distinct minimal polynomials and
\[ W = \text{core}(W) \oplus \text{core}(W)' \]
for some canonical core-free subspace $\text{core}(W)'$ of $\text{core}(W)'$.

**Proof.** Note first that the hypotheses guarantee that $T$ is invertible and $\phi_T$ is a product of distinct irreducible polynomials. The “if” direction is immediate by the construction of Lemma 3.11. Suppose then that $W$ has codimension 1, and, by Maschke’s theorem, choose some invariant complement $\text{core}(W)'$ of $\text{core}(W)$ in $V$. By Proposition 3.10, the indecomposable components of $\text{core}(W)'$ have distinct minimal polynomials. By Lemma 3.8,
\[ W = \text{core}(W) \oplus (W \cap \text{core}(W)'), \]
and $W \cap \text{core}(W)'$ is core-free of codimension 1 in $\text{core}(W)'$. By Lemma 3.11, there is a choice of basis for $\text{core}(W)'$ such that $W \cap \text{core}(W)' = \overline{\text{core}(W)'},$ and the proposition is proved. □

4. **Minimal degrees when the base group is elementary abelian**

Throughout this section $p$ and $q$ are distinct primes. Let
\[ V = \mathbb{F}_p^n \cong C_p^n \]
be an $n$-dimensional vector space over the field $\mathbb{F}_p$ of $p$ elements, for some fixed positive integer $n$, and $T$ an $n \times n$ matrix with entries from $\mathbb{F}_p$ of multiplicative order $q$. Recall that, if $W$ is a subspace of $V$ that is invariant under this action, then $W$ has an invariant complement $W'$ in $V$. The minimal polynomial $\phi_T$ is a product of distinct irreducible polynomials, all of degree $s$ where $s$ is the multiplicative order of $p$ modulo $q$, with the
possible exception (when \( s \geq 2 \)) of a factor \( x - 1 \). Note that \( s = 1 \) if and only if \( \mathbb{F}_p \) has a primitive \( q \)th root of unity, in which case all the irreducible factors of \( \phi_T \) are linear.

**Proposition 4.1.** Let \( G = V \rtimes T \). There exist nonnegative integers \( \ell \) and \( t \) and a collection \( \mathcal{C} = \mathcal{D} \cup \mathcal{E} \) affording a minimal faithful representation of \( G \) such that

\[
\mathcal{D} = \{ D_1, \ldots, D_\ell \} \quad \text{and} \quad \mathcal{E} = \{ E_1(T), \ldots, E_t(T) \}
\]

for some codimension 1 subspaces \( D_1, \ldots, D_\ell \) of \( V \), and invariant subspaces \( E_1, \ldots, E_t \) of \( V \), each of which complements an indecomposable subspace (where we interpret \( \ell = 0 \) and \( t = 0 \) to mean \( \mathcal{D} = \emptyset \) and \( \mathcal{E} = \emptyset \) respectively).

Note that it is possible to have \( t = 1 \) and \( E_1 = \{0\} \), the complement of \( V \) in the case that \( V \) is indecomposable.

**Proof.** There is no confusion in regarding \( G = VC \) as an internal semidirect product of \( V \) by \( C \cong \langle T \rangle \cong C_q \), but still retaining vector space terminology and additive notation for the group operation restricted to \( V \). By [11, Lemma 1] there exists a collection \( \mathcal{C} \) of meet-irreducible subgroups affording a minimal faithful representation of \( G \). Then \( \mathcal{C} = \mathcal{D} \cup \mathcal{E} \) where \( \mathcal{D} \), possibly empty, comprises all subgroups in \( \mathcal{C} \) of index divisible by \( q \), and \( \mathcal{E} \), possibly empty, consists of all subgroups in \( \mathcal{C} \) of order divisible by \( q \).

In particular, elements of \( \mathcal{D} \) are subgroups of \( V \). By Lemma 2.7, these must all be proper subgroups of \( V \), since \( V \) is normal in \( G \), so, being meet-irreducible, must have codimension 1 as subspaces of \( V \).

Let \( K \in \mathcal{E} \), so \( q \) divides \( |K| \). Put \( W = K \cap V \). Note that \( V \) is elementary abelian, so all of its subgroups are normal in \( V \). By (a) and (b) of Lemma 2.6, \( K = W(T)^g \) for some \( g \in G \) and \( W \) is an invariant subspace of \( V \) (being normal in \( G \)). Certainly \( W \neq V \) (for otherwise \( G = K \in \mathcal{C} \), contradicting minimality), so \( V = W \oplus W' \) for some nontrivial invariant subspace \( W' \) of \( V \). If \( W' \) is not indecomposable then \( W' = W'_1 \oplus W'_2 \) for some nontrivial invariant subspaces \( W'_1 \) and \( W'_2 \) of \( V \), so

\[
W = (W \oplus W'_1) \cap (W \oplus W'_2)
\]

and \( K = K_1 \cap K_2 \) where \( K \) is a proper subgroup of \( K_i = (W \oplus W'_i)(T)^g \) for \( i = 1, 2 \), contradicting that \( K \) is meet-irreducible. Hence \( W' \) is indecomposable, and the proposition is proved. \( \square \)

In what follows we develop a complete catalogue, namely, (17) and (24) below, of formulae for \( \mu(V \rtimes T) \). Note, throughout, that \( T \neq I \), so \( \phi_T(x) \neq x - 1 \). The next two theorems cover all possibilities, where \( s \) is the order of \( p \) modulo \( q \). In the first case (Theorem 4.5), we investigate what happens when all of the factors of the minimal polynomial have the same degree \( s \geq 1 \). In the second case (Theorem 4.9), we investigate the remaining possibilities, namely, when \( x - 1 \) is a factor and all other factors have the same degree \( s \geq 2 \).

**Lemma 4.2.** If \( G = V \rtimes T \), where all irreducible factors of \( \phi_T \) are linear, then \( \mu(G) = np \).

**Proof.** Suppose that all irreducible factors of \( \phi_T \) are linear. Without loss of generality, we may suppose \( T \) is diagonal and \( V = \langle v_1, \ldots, v_n \rangle \) where \( v_1, \ldots, v_n \) are eigenvectors for \( T \). For \( i = 1, \ldots, n \), put

\[
H_i = \langle v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n \rangle.
\]
Then \( \{H_1, \ldots, H_n\} \) affords a minimal faithful representation of \( V \) by \( T \)-invariant subspaces of degree \( np \). By Lemma 2.4, \( \mu(G) = \mu(V) = np \).

Illustrations of the phenomenon of Lemma 4.2 appear above in Examples 2.5 and 3.5.

**Lemma 4.3.** Let \( p \) and \( q \) be distinct primes and \( s \) the multiplicative order of \( p \) modulo \( q \). Suppose that \( s \geq 2 \). Let \( a \) be the smallest integer such that \( q < ap^{s-1} \). Then \( a = 1 \), or \( a = 2 \) and \( q = 1 + p + \ldots + p^{s-1} \). If \( s = a = 2 \) then \( p = 2 \) and \( q = 3 \).

**Proof.** Suppose that \( a > 1 \), so \( p^{s-1} < q \). Note that \( q \) divides \( p^s - 1 = (p-1)(1+p+\ldots+p^{s-1}) \). If \( q \) divides \( p-1 \) then \( q < p \leq p^{s-1} \), a contradiction. Hence \( q \) divides \( 1 + p + \ldots + p^{s-1} \) and \( p^{s-1} < q < 1 + p + \ldots + p^{s-1} \). It follows that \( q = 1 + p + \ldots + p^{s-1} < 2p^{s-1} \) and \( a = 2 \). \( \Box \)

**Remark 4.4.** A generalised Mersenne prime \( q \) has the form \( q = 1 + p + \ldots + p^{k-1} \) for some prime \( p \) and integer \( k \) (which includes the usual Mersenne primes of the form \( 2^k - 1 \)). The previous lemma asserts that, in our context, if \( a = 2 \) and \( s \geq 2 \) then \( q \) must be a generalised Mersenne prime. It is not known if there are infinitely many such primes.

**Theorem 4.5.** Suppose that \( r_1, \ldots, r_m \) are distinct irreducible polynomials over \( \mathbb{F}_p \) of degree \( s \), where \( s \) is the order of \( p \) modulo \( q \), such that

\[
\phi_T = r_1 \ldots r_m \quad \text{and} \quad \chi_T = r_1^{k_1} \ldots r_m^{k_m}.
\]

We may suppose \( k_1 \geq k_2 \geq \ldots \geq k_m \). Then

\[
\mu(V \rtimes T) = \begin{cases} 
np & \text{if } s = 1, \\
k_1pq & \text{if } s > 1 \text{ and } q < p^{s-1}, \\
k_1p^s & \text{if } s > 1, \ m = 1 \text{ and } q > p^{s-1}, \\
k_2pq + (k_1 - k_2)p^s & \text{if } s > 1, \ m > 1 \text{ and } q > p^{s-1}.
\end{cases}
\]  

**Proof.** The first alternative in (17) is given by Lemma 4.2, so we may suppose \( s > 1 \). Let \( a \) denote the smallest integer such that \( q < ap^{s-1} \). By Lemma 4.3, \( a = 1 \) or 2. It is convenient, throughout, to put \( k_{m+1} = 0 \). In particular, if \( m = 1 \) and \( a = 2 \) then \( k_1 = k_2 = 0 \). Put \( G = V \rtimes T = V(T) \) (regarded as an internal semidirect product, mixing addition and multiplication, without ever causing confusion). We have a direct sum decomposition

\[
V = \bigoplus_{i=1}^{m} \bigoplus_{i=1}^{k_i} V_{ij} = \bigoplus_{(i,j) \in I} V_{ij},
\]

where \( V_{ij} \) is an indecomposable subspace of \( V \) such that \( T|_{V_{ij}} \) has minimal polynomial \( r_i \) for each \( (i,j) \in I \), where \( I = \{(i,j) \mid 1 \leq i \leq m, 1 \leq j \leq k_i\} \). For \( J \subseteq I \), put

\[
V_J = \bigoplus_{(i,j) \in J} V_{ij},
\]

so that \( V = V_I = V_J \oplus V_{I \setminus J} \). If \( W = V_J \) for some \( J \subseteq I \) then put \( W' = V_{I \setminus J} \), so that \( V = W \oplus W' \).

Note that if \( k_a = 0 \) then \( m = 1 \) and \( a = 2 \). Suppose for the time being that \( k_a \geq 1 \), so either \( a = 1 \), or \( a = 2 \) and \( m \geq 2 \). Because \( k_a \geq k_{a+1} \geq \ldots \geq k_m > k_{m+1} = 0 \), we have that, for each \( j = 1 \) to \( k_a \), there exists some largest \( \ell_j \in \{a, \ldots, m\} \) such that

\[
k_{\ell_j} \geq j \geq k_{\ell_j+1}.
\]
and we put
\[ W_j = \bigoplus_{i=1}^{\ell_j} V_{ij}, \]
so that \( T|_{W_j} \) has minimal polynomial \( r_1 \ldots r_{\ell_j} \). In particular, \( \ell_1 = m \), since \( k_m \geq 1 > 0 = k_{m+1} \), and \( T|_{W_1} \) has minimal polynomial \( r_1 \ldots r_m \). Thus

\[ V = V_X \oplus \bigoplus_{j=1}^{k_a} W_j \]

where \( X = \{(1,j) \mid k_2 < j \leq k_1 \} \) if \( a = 2 \) and \( k_1 > k_2 \), and \( X = \emptyset \) otherwise, in which case we interpret \( V_X = \{0\} \). For \( j = 1 \) to \( k_a \), put

\[ H_j = \overline{W_j} \oplus W'_j, \]

where \( \overline{W_j} \) is a canonical codimension 1 subspace of \( W_j \) as described in Lemma 3.11, so that \( \text{core}(\overline{W_j}) = \{0\}, \text{core}(H_j) = W'_j \) and \( |G : H_j| = pq \). For \( (1,j) \in X \), put

\[ K_j = V'_{ij}(T), \]

so that \( \text{core}(K_j) = V'_j \) and \( |G : K_j| = p^s \). Now put

\[ \mathcal{C} = \{ H_1, \ldots, H_{k_a} \} \cup \{ K_j \mid (1,j) \in X \}. \]

Then

\[ \text{core} \left( \bigcap_{\mathcal{C}} \right) = \bigcap_{j=1}^{k_a} W'_j \cap \bigcap_{(1,j) \in X} V'_{ij} = V_X \cap V'_X = \{0\}, \]

so that \( \mathcal{C} \) affords a faithful representation of \( G \) of degree

\[ \sum_{j=1}^{k_a} |G : H_j| + \sum_{(1,j) \in X} |G : K_j| = k_a pq + (k_1 - k_a)p^s. \]

Note that if \( k_a = 0 \), so that \( m = 1 \) and \( a = 2 \), then (18) may be interpreted as \( V = V_I \) (since \( X = I \)) and (19) may be interpreted as \( \mathcal{C} = \{ K_j \mid (1,j) \in I \} \), and the conclusion about the faithfulness and degree of the representation afforded by \( \mathcal{C} \) still holds. This proves that, in all cases,

\[ \mu(G) \leq k_a pq + (k_1 - k_a)p^s. \]

We now prove that this formula is also a lower bound for \( \mu(G) \). By Proposition 4.1, there exists a collection \( \mathcal{C} = \mathcal{D} \cup \mathcal{E} \) affording a minimal faithful representation of \( G \) such that

\[ \mathcal{D} = \{ D_1, \ldots, D_\ell \} \quad \text{and} \quad \mathcal{E} = \{ E_1(T), \ldots, E_\ell(T) \} \]

for some codimension 1 subspaces \( D_1, \ldots, D_\ell \) of \( V \), and invariant subspaces \( E_1, \ldots, E_\ell \) of \( V \), each of which complements an indecomposable subspace. We interpret \( \ell = 0 \) and \( t = 0 \) to mean \( \mathcal{D} = \emptyset \) and \( \mathcal{E} = \emptyset \) respectively. By Proposition 3.12, for \( i = 1, \ldots, \ell \), we may write

\[ D_i = \text{core}(D_i) \oplus \overline{\text{core}(D_i)} = S_i \oplus S'_i, \]

where we put \( S_i = \text{core}(D_i)' \). The degree of the representation afforded by \( \mathcal{C} \) is \( \ell pq + tp^s \), so to complete the proof of the theorem it suffices to show

\[ \ell pq + tp^s \geq k_a pq + (k_1 - k_a)p^s. \]
As a stepping stone towards doing this, we will first prove \( \ell \geq k_a \). We use the following claim, which we will prove later:

**Claim:** We have a decomposition

\[
V = S_1 \oplus \ldots \oplus S_\ell \oplus T_1 \oplus \ldots \oplus T_t
\]

for some invariant subspaces \( S_1, \ldots, S_\ell, T_1, \ldots, T_t \) of \( V \) such that, after possible rewriting of \( D \),

\[
D_i = S_i' \oplus S_i \quad \text{and} \quad E_j = T_j',
\]

where \( S_i \) is a sum of indecomposable subspaces with distinct minimal polynomials for \( i = 1, \ldots, \ell \), and \( T_j \) is indecomposable for \( j = 1, \ldots, t \).

Suppose by way of contradiction that \( \ell < k_a \). Certainly, then, either \( a = 1 \) and \( \ell < k_1 \), or \( m > 1 \), \( a = 2 \) and \( \ell < k_2 \leq k_1 \). Hence, using the decomposition of \( V \) in the Claim, at most \( k_1 - 1 \) indecomposables with minimal polynomial \( r_1 \) appear in \( S_1 \oplus \ldots \oplus S_\ell \), and, when \( a = 2 \), at most \( k_2 - 1 \) indecomposables with minimal polynomial \( r_2 \) also appear. But \( k_1 \) and \( k_2 \) copies of indecomposables with minimal polynomial \( r_1 \) and \( r_2 \), respectively, appear in the decomposition of \( V \). Hence \( t \geq a \) and, without loss of generality, \( T_1 \) is indecomposable with minimal polynomial \( r_1 \), and, in the case \( a = 2 \), we may suppose \( T_2 \) is indecomposable with minimal polynomial \( r_2 \). Put

\[
S = \begin{cases} 
T_1' \oplus T_1' & \text{if } a = 1, \\
T_1 \oplus T_2' \oplus (T_1 \oplus T_2)' & \text{if } a = 2,
\end{cases}
\]

where, in the second case, \((T_1 \oplus T_2)' = T_1' \cap T_2' = E_1 \cap E_2\), which is indeed a complement for \( T_1 \oplus T_2 \). But core\((S) = E_1\), if \( a = 1 \), and core\((S) = E_1 \cap E_2\), if \( a = 2 \), so that the collection

\[
\mathcal{E}' = \begin{cases} 
\mathcal{D} \cup \{S\} \cup \mathcal{E} \setminus \{E_1(T)\} & \text{if } a = 1, \\
\mathcal{D} \cup \{S\} \cup \mathcal{E} \setminus \{E_1(T), E_2(T)\} & \text{if } a = 2,
\end{cases}
\]

affords a faithful representation of \( G \), but with degree less than the degree of the representation afforded by \( \mathcal{E} \), since

\[
|G : S| = pq < ap^S = \begin{cases} 
|G : E_1(T)| & \text{if } a = 1, \\
|G : E_1(T)| + |G : E_2(T)| & \text{if } a = 2.
\end{cases}
\]

This contradicts that \( \mathcal{E} \) is minimal. Hence \( \ell \geq k_a \).

There are at most \( \ell \) occurrences of indecomposables with minimal polynomial \( r_1 \) appearing in \( S_1 \oplus \ldots \oplus S_\ell \), so at least \( k_1 - \ell \) such indecomposables must occur amongst \( T_1, \ldots, T_t \), so that \( t \geq k_1 - \ell \). Thus

\[
\ell pq + tp^S = k_a pq + (\ell - k_a) pq + tp^S
\]

\[
\geq k_a pq + (\ell - k_a)(a - 1)p^S + p^S \begin{cases} 
0 & \text{if } a = 1, \\
k_1 - \ell & \text{if } a = 2,
\end{cases}
\]

\[
= k_a pq + (k_1 - k_a)p^S
\]
and (20) is proven. The statement of the theorem for \( s > 1 \) is therefore captured succinctly by the formula

\[
\mu(G) = k_apq + (k_1 - k_a)p^s.
\]  

(21)

To complete the proof of the theorem, it therefore remains to verify the Claim. As a first step we prove

\[
V = T_1 \oplus \ldots \oplus T_t \oplus (E_1 \cap \ldots \cap E_t)
\]

(22)

for some indecomposables \( T_i \) such that \( E_i = T_i' \) for \( i = 1, \ldots, t \). Note that \( V = E_1 \oplus T_1 \) for some indecomposable \( T_1 \), so \( E_1 = T_1' \), which starts an induction. Suppose, as inductive hypothesis, that for \( k \leq t \),

\[
V = T_1 \oplus \ldots \oplus T_{k-1} \oplus (E_1 \cap \ldots \cap E_{k-1})
\]

for some indecomposables \( T_1, \ldots, T_{k-1} \) such that \( E_i = T_i' \) for \( i = 1, \ldots, k-1 \). By minimality of \( \mathcal{C} \), \( E_1 \cap \ldots \cap E_k \) is a proper subspace of \( E_1 \cap \ldots \cap E_{k-1} \). Further,

\[
\frac{E_1 \cap \ldots \cap E_{k-1}}{E_1 \cap \ldots \cap E_k} \cong \frac{(E_1 \cap \ldots \cap E_{k-1}) + E_k}{E_k} = \frac{V}{E_k},
\]

which is indecomposable, so we may choose an indecomposable \( T_k \) such that

\[
E_1 \cap \ldots \cap E_{k-1} = (E_1 \cap \ldots \cap E_k) \oplus T_k.
\]

Certainly \( T_k \) is not a subspace of \( E_k \) (for otherwise \( E_1 \cap \ldots \cap E_k \cap T_k \neq \{0\} \)), so it follows that \( V = E_k \oplus T_k \), so we may write \( E_k = T_k' \). Then

\[
V = (T_1 \oplus \ldots \oplus T_{k-1}) \oplus (E_1 \cap \ldots \cap E_{k-1}) = T_1 \oplus \ldots \oplus T_k \oplus (E_1 \cap \ldots \cap E_k),
\]

which completes the inductive step and the proof of (22). Note that if \( \ell = 0 \) (so that \( \mathcal{D} = 0 \) then (22) proves the Claim (for then \( \mathcal{C} = \mathcal{D} \) and \( E_1 \cap \ldots \cap E_t = \{0\} \) so that \( V = T_1 \oplus \ldots \oplus T_t \)).

We may suppose in what follows that \( \ell > 0 \). Put \( E = E_1 \cap \ldots \cap E_t \). We next prove, by induction, that we can rewrite \( \mathcal{D} \) (if necessary) so that the following holds for \( k = 0, \ldots, \ell \):

\[
V = S_1 \oplus \ldots \oplus S_k \oplus T_1 \oplus \ldots \oplus T_t \oplus (S_1' \cap \ldots \cap S_k' \cap E)
\]

(23)

where \( D_i = \overline{S_i} \oplus S_i' \) and \( S_i \) is a sum of indecomposables with distinct minimal polynomials, for \( i = 1, \ldots, k \). This suffices to prove the Claim, because when \( k = \ell \) we have

\[
S_1' \cap \ldots \cap S_k' \cap E = S_1' \cap \ldots \cap S_k' \cap E = \bigcap \mathcal{C} = \{0\}.
\]

Note that (22) now becomes the initial case \( k = 0 \) in a proof by induction of (23). Suppose, as inductive hypothesis, that \( 0 < k \leq \ell \) and we can rewrite \( \mathcal{D} \) (if necessary) so that

\[
V = S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus (S_1' \cap \ldots \cap S_{k-1}' \cap E)
\]

where \( D_k = \overline{S_k} \oplus S_k' \) and \( S_i \) is a sum of indecomposables with distinct minimal polynomials for \( i = 1, \ldots, k-1 \). By minimality of \( \mathcal{C} \),

\[
\text{core}(D_1 \cap \ldots \cap D_{k-1} \cap E) \neq \text{core}(D_1 \cap \ldots \cap D_k \cap E),
\]

that is,

\[
S_1' \cap \ldots \cap S_{k-1}' \cap E \neq S_1' \cap \ldots \cap S_{k-1}' \cap E \cap \text{core}(D_k).
\]
But
\[ \frac{S'_1 \cap \ldots \cap S'_{k-1} \cap E}{S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(D_k)} \cong \frac{(S'_1 \cap \ldots \cap S'_{k-1} \cap E) + \text{core}(D_k)}{\text{core}(D_k)} \leq \frac{V}{\text{core}(D_k)} \cong \text{core}(D_k)' , \]
which is a sum of indecomposables with distinct minimal polynomials. Hence
\[ (S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(D_k)) \oplus S_k = S'_1 \cap \ldots \cap S'_{k-1} \cap E \]
for some invariant subspace \( S_k \) contained in \( E \), which is a sum of indecomposables with distinct minimal polynomials. Choose any complement \( (S'_1 \cap \ldots \cap S'_{k-1} \cap E)' \) and put
\[ S'_k = (S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(D_k)) \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E)' , \]
which is indeed a complement of \( S_k \). Put
\[ \widetilde{D}_k = \overline{S}_k \oplus S'_k . \]
Observe that \( \text{core}(\tilde{D}_k) = S'_k \) and
\[ S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(\tilde{D}_k) = S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap S'_k \]
\[ = (S'_1 \cap \ldots \cap S'_{k-1} \cap E) \cap \left[ (S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(D_k)) \right. \]
\[ \left. \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E)' \right] \]
\[ = S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(D_k) , \]
so we may replace \( D_k \) by \( \tilde{D}_k \) in \( D \) without disturbing faithfulness or the degree of the representation afforded by \( \psi \). Renaming \( \tilde{D}_k \) by \( D_k \), we get
\[ V = S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E) \]
\[ = S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus ((S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap \text{core}(D_k)) \oplus S_k) \]
\[ = S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus (S_k \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap S'_k)) \]
\[ = S_1 \oplus \ldots \oplus S_k \oplus T_1 \oplus \ldots \oplus T_t \oplus (S'_1 \cap \ldots \cap S'_k \cap E) , \]
completing the inductive step, and (23) is proved. This completes the proof of the Claim and therefore also the proof of the theorem. \( \square \)

Formula (21) captures the three alternatives in the previous theorem when \( s > 1 \). However, by Remark 4.4 and Theorem 4.5, we have the following further simplification (eventually) if there turn out to be only finitely many generalised Mersenne primes:

**Corollary 4.6.** With the hypotheses of Theorem 4.5, if \( s > 1 \) and there are only finitely many generalised Mersenne primes, then there is an integer \( N \) such that for all \( q \geq N \), \( \mu(V \rtimes T) = k_1pq \).

The first alternative in formula (17) is illustrated in Examples 3.4 and 3.5 and the intransitive case of Example 2.5. The second alternative is illustrated in Example 3.6 (and also occurs in Example 2.5 as an exceptional transitive case when \( s = 1 \) and \( np = pq = k_1pq \)). In the next two examples, we illustrate the third and fourth alternatives of (17).
Example 4.7. The smallest instance when \( q > p^{s-1} \), so that the third alternative of (17) is able to kick in, occurs when \( p = 2 \) and \( q = 3 \), so that \( s = 2 \). Let \( T = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \), so that \( \phi_T = x^2 + x + 1 \), and put \( G = \mathbb{F}_2^2 \rtimes T \cong C_2^2 \rtimes C_3 \cong \text{Alt}(4) \). As expected, (17) predicts correctly that \( \mu(G) = p^s = 4 \).

Example 4.8. Let \( p = 2 \) and \( q = 7 \). Then \( s = 3 \) and the monic irreducible polynomials over \( \mathbb{F}_2 \) with primitive 7th roots in an extension of \( \mathbb{F}_2 \) are \( \pi_1 = x^3 + x + 1 \) and \( \pi_2 = x^3 + x^2 + 1 \). Let \( T_1 \) and \( T_2 \) be the respective companion matrices, that is,

\[
T_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{and} \quad T_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.
\]

Now put \( T_3 = T_1 \oplus T_2 \), \( T_4 = T_1 \oplus T_1 \), \( T_5 = T_1 \oplus T_1 \oplus T_2 \), \( T_6 = T_1 \oplus T_1 \oplus T_2 \oplus T_2 \) and \( G_1 = V_i \rtimes T_i \), where \( V_i \) is of the appropriate dimension, for each \( i \). Then \( G_1 \cong G_2 \), by Lemma 3.1, and, by the third and fourth alternatives of (17), \( \mu(G_1) = p^s = 8 \), \( \mu(G_3) = pq = 14 \), \( \mu(G_4) = 2p^s = 16 \), \( \mu(G_5) = pq + p^s = 22 \) and \( \mu(G_6) = 2pq = 28 \). The underlying methods yield, for example, the following contrasting transitive minimal faithful representations:

\[
\begin{align*}
G_1 & \cong \langle (1 2)(3 4)(5 6)(7 8), (1 3)(2 4)(5 7)(6 8), (1 5)(2 6)(3 7)(4 8), (2 3 5 4 7 8 6) \rangle, \\
G_3 & \cong \langle (1 2)(5 6)(11 12)(13 14), (1 2)(3 4)(7 8)(13 14), (1 2)(3 4)(5 6)(9 10), (1 2)(7 8)(11 12)(13 14), (1 2)(3 4)(9 10)(13 14), (1 2)(3 4)(5 6)(11 12), (1 3 5 7 9 11 13)(2 4 6 8 10 12 14) \rangle.
\end{align*}
\]

Theorem 4.9. Suppose that \( r_1, \ldots, r_m \) are distinct irreducible polynomials over \( \mathbb{F}_p \) of degree \( s \geq 2 \), where \( s \) is the order of \( p \) modulo \( q \), such that

\[
\phi_T = (x-1)r_1 \cdots r_m \quad \text{and} \quad \chi_T = (x-1)^k r_1^{k_1} \cdots r_m^{k_m}.
\]

We may suppose \( k_1 \geq k_2 \geq \ldots \geq k_m \). Then

\[
\mu(V \rtimes T) = \begin{cases} 
  k_1 \pi & \text{if } k \leq k_1 \text{ and } q < p^{s-1}, \\
  k_1 \pi + (k-k_1) \pi & \text{if } k > k_1 \text{ and } q < p^{s-1}, \\
  k_1 \pi^s & \text{if } k \leq k_1, \ m = 1 \text{ and } q > p^{s-1}, \\
  k_1 \pi^s + kp & \text{if } k > k_1, \ m = 1 \text{ and } q > p^{s-1}, \\
  k_2 \pi q + (k_1-k_2) \pi & \text{if } k \leq k_2, \ m > 1 \text{ and } q > p^{s-1}, \\
  k_2 \pi q + (k_1-k_2) \pi^s + (k-k_2) \pi & \text{if } k > k_2, \ m > 1 \text{ and } q > p^{s-1}.
\end{cases}
\]

Proof. As before, let \( a \) be the smallest integer such that \( q < a p^{s-1} \). By Lemma 4.3, \( a = 1 \) or \( 2 \). We again put \( k_a = 0 \) when \( m = 1 \) and \( a = 2 \). Put \( G = V \rtimes T = V \langle T \rangle \). We have a decomposition \( V = \tilde{V} \oplus Z \), where

\[
\tilde{V} = \bigoplus_{(i,j) \in I} V_{ij} \quad \text{and} \quad Z = \bigoplus_{a=1}^{k} Z_a,
\]

where the \( V_{ij} \) are indecomposable subspaces of \( V \) with minimal polynomials from amongst \( r_1, \ldots, r_m \), adopting the notation of the proof of the previous theorem, and the \( Z_a \) are
Certainly, by (1), we have $\mu(\hat{V}(T)) = k_a^p q + p^s (k_1 - k_a)$.

(25)

\[ \mu(\hat{V}(T)) = k_a^p q + p^s (k_1 - k_a) . \]

\[ \text{Case 1: Suppose that } k_a \geq k . \]

Let $\mathcal{C}$ be the collection of subgroups described in the first part of the proof of Theorem 4.5 that affords a faithful representation of $\hat{V}(T)$ of degree $\mu(\hat{V}(T))$, replacing $V$ by $\hat{V}$ throughout. For $\alpha = 1, \ldots, k$, put

\[ U_\alpha = W_\alpha \oplus Z_\alpha \quad \text{and} \quad \hat{H}_\alpha = \overline{U}_\alpha \oplus W'_\alpha \oplus \bigoplus_{\beta \neq \alpha} Z_\beta , \]

where $\overline{U}_\alpha$ is a canonical codimension 1 subspace of $U_\alpha$ with trivial core (see Lemma 3.11), and here $W'_\alpha$ denotes a complement of $W_\alpha$ in $\hat{V}$, so that

\[ \text{core}(\hat{H}_\alpha) = W'_\alpha \oplus \bigoplus_{\beta \neq \alpha} Z_\beta . \]

Now put

\[ \hat{\mathcal{C}} = \{ \hat{H}_1, \ldots, \hat{H}_k, H_{k+1} \oplus Z, \ldots, H_{k_a} \oplus Z \} \cup \{ K_j \oplus Z \mid (1, j) \in X \} , \]

where the notation $K_j \oplus Z$ represents the internal semidirect product resulting from joining $K_j$ with $Z$ (since the action of $T$ on $Z$ is trivial). Then

\[ \text{core} \left( \bigcap \hat{\mathcal{C}} \right) = \text{core} \left( \bigcap \mathcal{C} \right) \oplus \bigcap_{\alpha=1}^{k} \bigoplus_{\beta \neq \alpha} Z_\beta = \{0\} , \]

so $\hat{\mathcal{C}}$ affords a faithful representation of $G$. Its degree is the same as the degree of the representation of $\hat{V}(T)$ afforded by $\mathcal{C}$, which is $\mu(\hat{V}(T))$, so

\[ \mu(G) \leq \mu(\hat{V}(T)) \leq \mu(G) , \]

whence we have equality. The formula (25) captures the first, third and fifth alternatives in the statement of the theorem.

\[ \text{Case 2: Suppose that } k > k_a . \]

We make the same definitions as in the previous case, except that we put

\[ \hat{\mathcal{C}} = \{ \hat{H}_1, \ldots, \hat{H}_{k_a} \} \cup \{ K_j \oplus Z \mid (1, j) \in X \} \cup \{ (\hat{V} \oplus \bigoplus_{\beta \neq \alpha} Z_\beta)(T) \mid \alpha = k_a + 1, \ldots, k \} . \]

Again the representation of $G$ afforded by $\hat{\mathcal{C}}$ is faithful. Its degree is

\[ k_a^p q + (k - k_a)p + p^s (k_1 - k_a) , \]

which therefore serves as a lower bound for $\mu(G)$.

By Proposition 4.1, there exists a collection $\mathcal{C} = \mathcal{D} \cup \mathcal{E}$ of subgroups affording a minimal representation of $G$, such that $\mathcal{D} = \{ D_1, \ldots, D_t \}$ and $\mathcal{E} = \{ E_1(T), \ldots, E_t(T) \}$, where $D_1, \ldots, D_k$ are codimension 1 subspaces of $V$ and, after reordering (if necessary), $E_1, \ldots, E_t$ are complements of indecomposables with minimal polynomials from amongst $r_1, \ldots, r_m$ and $E_{t_0+1}, \ldots, E_t$ are complements of one-dimensional indecomposables.
and, by the same reasoning as before, $t_0 \geq k_1 - \ell$ and $t - t_0 \geq k - \ell$. By definition of $a$, and since $p \neq q$, we have $(a - 1)p^{s - 1} < q$, so

$$pq \geq (a - 1)p^s + p.$$  

Hence

$$\mu(G) = \ell pq + (t - t_0)p + t_0p^s$$

$$= ka pq + (\ell - ka)pq + (t - t_0)p + t_0p^s$$

$$\geq ka pq + (\ell - ka)((a - 1)p^s + p) + (k - \ell)p + p^s \begin{cases} 0 & \text{if } a = 1, \\ k_1 - \ell & \text{if } a = 2, \end{cases}$$

$$\geq ka pq + (k - ka)p + p^s(k_1 - ka),$$

whence we have

$$\mu(G) = ka pq + (k - ka)p + p^s(k_1 - ka). \quad (26)$$

Formula (26) captures the second, fourth and sixth alternatives in the statement of theorem, and the proof is complete.

Illustrations of formula (24) are implicit in applications in the next section. \qed

5. Adding direct factors without increasing the degree

Results of the preceding section are applied now to investigate possible ways in which $\mu$ may fail to be additive with respect to taking direct products. The question of when additivity occurs is an important theme in the work of Johnson [11] and Wright [22]. The failure of additivity in general was demonstrated by a seminal example in [22] and explored further by Saunders [17–19]. In all their cases, nontrivial groups $G$ and $H$ are exhibited in which $G$ does not decompose nontrivially as a direct product, $H$ is a cyclic group of prime order and

$$\mu(G \times H) = \mu(G). \quad (27)$$

We reproduce these examples below as special cases of applications of the formulae in Theorems 4.5 and 4.9. We finish by exhibiting examples of groups $G$ that do not decompose nontrivially as direct products, but such that (27) holds for arbitrarily large direct products $H$ of elementary abelian groups (with mixed primes).

**Example 5.1.** Consider the groups $G_1 = F_3^2 \times T_1$, $G_2 = F_3^3 \times T_2$, $G_3 = F_3^4 \times T_3$, where

$$T_1 = \begin{bmatrix} 0 & 4 \\ 1 & 4 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 0 & 4 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad T_3 = \begin{bmatrix} 0 & 4 & 0 & 0 \\ 1 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$  

Then $|T_1| = |T_2| = |T_3| = 3$, $\phi_{T_1} = \chi_{T_1} = x^2 + x + 1$, $\phi_{T_2} = \chi_{T_2} = \phi_{T_3} = (x - 1)(x^3 + x + 1)$ and $\chi_{T_3} = (x - 1)^2(x^2 + x + 1)$. Then $G_1 \cong C_5^2 \rtimes C_3$ and $\mu(G_1) = 15$, by the second alternative of (17). A minimal faithful representation is afforded by a canonical core-free subspace of $F_3^2$ (see Lemma 3.11), yielding

$$G_1 \cong \langle a_1, a_2, b \mid a_1^3 = a_2^5 = b^3 = 1 = [a_1, a_2], a_1b = a_2, a_2b = a_1^{-1}a_2^{-1} \rangle \cong \langle \alpha_1, \alpha_2, \beta \rangle,$$
where
\[
\begin{align*}
\alpha_1 &= (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)(11\ 14\ 12\ 15\ 13), \\
\alpha_2 &= (1\ 2\ 3\ 4\ 5)(6\ 9\ 7\ 10\ 8)(11\ 12\ 13\ 14\ 15), \\
\beta &= (1\ 11\ 6)(2\ 12\ 7)(3\ 13\ 8)(4\ 14\ 9)(5\ 15\ 10).
\end{align*}
\]

By the first alternative of (24), we have \(\mu(G_2) = 15\). A minimal faithful representation is afforded by a canonical core-free subspace of \(\mathbb{F}_5^3\), yielding
\[
G_2 \cong G_1 \times C_5 \cong \langle \alpha_1, \alpha_2, \alpha_3, \beta \rangle,
\]
where \(\alpha_1, \alpha_2\) and \(\beta\) are as above, and
\[
\alpha_3 = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)(11\ 12\ 13\ 14\ 15).
\]

In fact, \(G_1\) and \(G_2\) are isomorphic to subgroups of the transitive permutation group introduced at the end of Wright’s paper [22], which was the first published counterexample to additivity of \(\mu\) with respect to direct product. By contrast, now using the second alternative of (24), \(\mu(G_3) = 15 + 5 = 20\). A faithful intransitive representation of \(G_3\) is given by the previous canonical core-free subspace of \(\mathbb{F}_5^3\), augmented in an obvious way in \(\mathbb{F}_5^4\), and a subgroup of index 3, yielding
\[
G_3 \cong G_2 \times C_5 \cong G_1 \times C_5^2 \cong \langle \alpha_1, \alpha_2, \alpha_3, \beta \rangle,
\]
where \(\alpha_1, \alpha_2, \alpha_3\) and \(\beta\) are as above, but fixing five new letters, and \(\alpha_4 = (16\ 17\ 18\ 19\ 20)\).

Observe that \(\mu(C_5)^2 = 10\), so that
\[
\max\{\mu(G_1), \mu(C_5^2)\} = 15 < \mu(G_1 \times C_3^2) = 20 < 25 = \mu(G_1) + \mu(C_5^2).
\]

This answers affirmatively a question of Saunders [17], whether there exist groups \(K\) and \(L\) such that
\[
\max\{\mu(K), \mu(L)\} < \mu(K \times L) < \mu(K) + \mu(L).
\]

Note that if \(G\) and \(H\) are groups such that \(\mu(H) < \mu(G)\) and \(\mu(G \times H) = \mu(G) < \mu(G) + \mu(H)\) (such as the example in [22]), then (29) holds easily by taking any group \(M\) of order coprime to \(|G \times H|\), putting \(K = G\) and \(L = M \times H\), and invoking Johnson’s result that \(\mu\) is additive with respect to taking direct products of groups of coprime order. However, the solution (28) given here appears to be novel in that only two primes, namely 3 and 5, divide \(|K \times L|\), taking \(K = G_1\) and \(L = C_5^2\). This example clearly generalises, by (24), to an infinite class of examples, where (29) holds and only two distinct primes \(p\) and \(q\) divide \(|K \times L|\). Note that (29) fails, if \(K \times L\) is a \(p\)-group, since \(\mu\) is additive with respect to taking direct products of nilpotent groups by a theorem of Wright [22].

Example 5.2. Let \(p\) and \(q\) be primes such that \(p\) has order \(s = q - 1\) modulo \(q\), so that \(\pi = 1 + x + \ldots + x^{q-1}\) is irreducible over \(\mathbb{F}_p\). Suppose also that \((p, q) \neq (2, 3)\), as this guarantees that \(q < p^{q-2} = p^q - 1\), so that the second alternative of (17) will apply. (The case \((p, q) = (2, 3)\) is explored above in Example 4.7 when illustrating the third alternative of (17).) The smallest case satisfying our conditions is \((p, q) = (2, 5)\). Consider the groups
\[
H_1 = \mathbb{F}_p^{q-1} \times T_1 \cong C_p^{q-1} \times C_q \quad \text{and} \quad H_2 = \mathbb{F}_p^{q} \times T_2 \cong C_p^q \times C_q \cong H_1 \times C_p,
\]
where $T_1$ and $T_2$ are matrices over $\mathbb{F}_p$ in rational canonical form having characteristic polynomials $\pi$ and $(1 + x)\pi$ respectively. Then

$$\mu(H_1) = pq = \mu(H_2) = \mu(H_1 \times C_p),$$

by the second alternative of (17) and the first alternative of (24). Observe that $H_1$ is a subgroup of the complex reflection group $C(p, p, q)$, a member of the infinite class of counterexamples studied by Saunders in [18]. In the smallest case, when $p = 2$ and $q = 5$, the groups become $H_1 \cong C_2^4 \text{ sd } C_5$ and $H_2 \cong C_5^2 \text{ sd } C_5 \cong H_1 \times C_2$, where

$$T_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad T_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\mu(H_1) = \mu(H_1 \times C_2) = 10 < 12 = \mu(H_1) + \mu(C_2).$$

The group $H_1$ and these properties appear for the first time in [17]. It is gratifying that the smallest example that comes from Saunders’ investigations, where he was motivated by questions about complex reflection groups, also coincides with the smallest example that arises as an application of Theorems 4.5 and 4.9. By results in [4], it is impossible to create a smaller example by any method, in the sense that $G \times H$ cannot embed in $\text{Sym}(9)$ and have $H$ nontrivial and $\mu(G) = \mu(G \times H)$.

In the final examples below, given an arbitrarily large direct product $H$ of elementary abelian groups built from any collection of primes and positive integer exponents, we can find a group $G$ that does not decompose nontrivially as a direct product, yet $\mu(G \times H) = H$. Example 5.10 below is a substantial simplification of Example 5.3, but relies on some number-theoretic preliminaries.

**Example 5.3.** Let $P = \{p_1, \ldots, p_k\}$ be a finite collection of distinct primes and $N = \{n_1, \ldots, n_k\}$ a collection of positive integers. Choose a prime $q \geq 5$ and larger than all of the primes in $P$. Consider $i \in \{1, \ldots, k\}$. Let $s_i$ be the multiplicative order of $p_i$ modulo $q$ and put $m_i = s_i n_i$. Then $s_i > 1$ and we can find a monic irreducible polynomial $\pi_i \in \mathbb{F}_{p_i}$ of degree $s_i$ such that its roots in an extension of $\mathbb{F}_{p_i}$ are primitive $q$th roots of 1. Let $a_i$ be the smallest integer such that $q < a_i p_i^{s_i - 1}$, so $a_i = 1$ or $a_i = 2$, by Lemma 4.3. Observe that if $a_i = 2$ then $s_i < q - 1$ (for otherwise $a_i = 1$, since $5 \leq q < p_i^{s_i - 2}$), so $\pi_i$ and $\pi_i \hat{\nu}_i$ are distinct, where $\hat{\nu}_i$ is the permutation defined by (15). Denote the companion matrix over a field $\mathbb{F}$ of a monic polynomial $\pi \in \mathbb{F}[x]$ by $M_{\pi}$. If $a_i = 1$, define $T_i$ to be the $m_i \times m_i$ matrix over $\mathbb{F}_p$ that is the matrix direct sum of $n_i$ copies of $M_{\pi_i}$. If $a_i = 2$, define $T_i$ to be the $(2m_i) \times (2m_i)$ matrix over $\mathbb{F}_p$ that is the matrix direct sum of $n_i$ copies of $M_{\pi_i} \oplus M_{\pi_i \hat{\nu}_i}$.

Now put

$$\hat{T}_i = T_i \oplus I_{n_i},$$
where $I_{n_i}$ is an identity matrix (over $\mathbb{F}_{p_i}$). Then $|T_i| = |\hat{T}_i| = q$.

$$
\phi_{T_i} = \begin{cases}
\pi_i & \text{if } a_i = 1, \\
\pi_i(\pi_i \hat{\nu}_i) & \text{if } a_i = 2,
\end{cases} \quad \chi_{T_i} = \begin{cases}
\pi_i^{n_i} & \text{if } a_i = 1, \\
\pi_i^{n_i}(\pi_i \hat{\nu}_i)^{n_i} & \text{if } a_i = 2,
\end{cases}
$$

$$
\phi_{\hat{T}_i} = \begin{cases}
(x - 1)\pi_i & \text{if } a_i = 1, \\
(x - 1)\pi_i(\pi_i \hat{\nu}_i) & \text{if } a_i = 2,
\end{cases} \quad \chi_{\hat{T}_i} = \begin{cases}
(x - 1)^n_i \pi_i^{n_i} & \text{if } a_i = 1, \\
(x - 1)^n_i \pi_i^{n_i}(\pi_i \hat{\nu}_i)^{n_i} & \text{if } a_i = 2.
\end{cases}
$$

Now let $G_i = V_i \times T_i$ and $\hat{G}_i = \hat{V}_i \times \hat{T}_i$, where

$$
V_i = \begin{cases}
\mathbb{F}_{p_i}^{m_i} & \text{if } a_i = 1, \\
\mathbb{F}_{p_i}^{m_i + n_i} & \text{if } a_i = 2,
\end{cases} \quad \hat{V}_i = \begin{cases}
\mathbb{F}_{p_i}^{m_i} & \text{if } a_i = 1, \\
\mathbb{F}_{p_i}^{m_i + n_i} & \text{if } a_i = 2.
\end{cases}
$$

Then

$$
\mu(G_i) = \mu(\hat{G}_i) = n_i p_i q_i,
$$

by Theorems 4.5 and 4.9. Observe that, because $I_{n_i}$ acts trivially on $\mathbb{F}_{p_i}^{m_i}$,

$$
\hat{G}_i \cong G_i \times C_{p_i}^{m_i}.
$$

Now put

$$
T = \oplus_{i=1}^k T_i, \quad \hat{T} = \oplus_{i=1}^k \hat{T}_i, \quad V = \oplus_{i=1}^k V_i, \quad \hat{V} = \oplus_{i=1}^k \hat{V}_i,
$$

where the zeros outside the matrix blocks down the diagonals act as formal zeros (not in any particular field) for the purpose of matrix multiplication, and the elements of $V$ and $\hat{V}$ may be regarded as column vectors over $\mathbb{F}_{p_1} \cup \ldots \cup \mathbb{F}_{p_k}$. Thus, because the construction respects direct sum decompositions, $T$ and $\hat{T}$ may be regarded as acting on $V$ and $\hat{V}$ (on the left) by usual matrix multiplication. Hence, as in (10) and (11), we may define

$$
G = V \rtimes T \quad \text{and} \quad \hat{G} = \hat{V} \rtimes \hat{T}.
$$

The actions of $T$ and $\hat{T}$ on the respective $i$th direct summands is nontrivial, for each $i$, and the orders of these direct summands are pairwise coprime and also coprime to $q$, so, by repeated application of the last alternative in the formula given in Theorem 2.8 and by (30), we have

$$
\mu(G) = \sum_{i=1}^k \mu(G_i) = \sum_{i=1}^k n_i p_i q_i = \sum_{i=1}^k \mu(\hat{G}_i) = \mu(\hat{G}).
$$

Also, by (31),

$$
\hat{G} \cong G \times C_{p_1}^{m_1} \times \ldots \times C_{p_k}^{m_k}.
$$

Finally, put $H = C_{p_1}^{m_1} \times \ldots \times C_{p_k}^{m_k}$, which is our arbitrarily large direct product of elementary abelian groups, using all of the primes $p_1, \ldots, p_k$. Then $\mu(G \times H) = \mu(G)$. By construction, the irreducible action on each direct summand guarantees that $G$ does not decompose nontrivially as a direct product.

**Remark** 5.4. If there are only finitely many generalised Mersenne primes, then the construction in Example 5.3 would simplify by choosing $q$ to be larger also than the largest Mersenne prime, for that would guarantee $a_i = 1$ for each $i$, by Remark 4.4.
To guarantee simplification in the construction of Example 5.3 (regardless of whether or not there are infinitely many generalised Mersenne primes), we invoke the following lemmas. We say that an integer \( m \geq 3 \) is Mersenne with respect to an integer \( n \geq 2 \) if 
\[
m = 1 + n + \ldots + n^\alpha
\]
for some integer \( \alpha \). Note that this implies 
\[
m = \frac{n^{\alpha+1} - 1}{n-1} < n^{\alpha+1}.
\]

**Lemma 5.5.** If \( m \) is Mersenne with respect to \( n \) then \( k \) is not Mersenne with respect to \( n \) for \( m < k \leq 2m \).

*Proof.* If \( m \) and \( k \) are Mersenne with respect to \( n \) and \( m < k \leq 2m \) then there exist positive integers \( \alpha \) and \( \beta \) such that 
\[
m = 1 + n + \ldots + n^\alpha \quad \text{and} \quad k = 1 + n + \ldots + n^{\alpha+\beta} = m + n^{\alpha+1} + \ldots + n^{\alpha+\beta},
\]
whence 
\[
n^{\alpha+1} \leq n^{\alpha+1} + \ldots + n^{\alpha+\beta} = k - m \leq m < n^{\alpha+1},
\]
which is impossible. \( \square \)

The following corollary is of independent interest and probably well-known.

**Corollary 5.6.** Given a positive integer \( n \), there exists infinitely many primes that are not Mersenne with respect to \( n \).

*Proof.* Let \( N \) be any positive integer, and choose any prime \( p_1 \geq N \). By Bertrand’s postulate, there exists a prime \( p_2 \) such that \( p_1 < p_2 \leq 2p_1 \). If \( p_1 \) is not Mersenne with respect to \( n \), then we are done. If \( p_1 \) is Mersenne with respect to \( n \) then \( p_2 \) is not Mersenne with respect to \( n \), by Lemma 5.5, and again we are done. \( \square \)

**Lemma 5.7.** Let \( n \geq 2 \), \( k \geq 3 \) and \( N \) any positive integer. Then any strictly increasing sequence of \( k \) integers between \( N \) and \( 2N \) contains a consecutive subsequence of \( \lfloor k/2 \rfloor \) elements, none of which are Mersenne with respect to \( n \).

*Proof.* Let \( t_1, \ldots, t_k \) be a strictly increasing sequence of integers between \( N \) and \( 2N \). If \( t_i \) is not Mersenne with respect to \( n \) for all \( i \), then we are done using the entire sequence. Suppose then that some element in the sequence is Mersenne with respect to \( n \), and let \( t_j \) be the least such element. Then, for all \( \ell \) such that \( j < \ell \leq k \), we have \( N < t_j < t_\ell < 2N < 2t_j \), so that \( t_\ell \) is not Mersenne with respect to \( n \), by Lemma 5.5. If \( j > \lfloor k/2 \rfloor \) then \( t_1, \ldots, t_{\lfloor k/2 \rfloor} \) is a consecutive subsequence of \( \lfloor k/2 \rfloor \) elements, none of which are Mersenne with respect to \( n \), and we are done. Otherwise \( j \leq \lfloor k/2 \rfloor \) and \( t_{j+1}, \ldots, t_k \) is a consecutive subsequence with \( k - j \geq k - \lfloor k/2 \rfloor \geq \lfloor k/2 \rfloor \) elements, none of which are Mersenne with respect to \( n \), and again we are done. \( \square \)

**Theorem 5.8.** If \( p_1, \ldots, p_k \) are prime numbers then there exist infinitely many primes that are not Mersenne with respect to \( p_i \) for each \( i \).

*Proof.* Let \( p_1, \ldots, p_k \) be primes and \( N \) any positive integer. By the Green-Tao theorem [7] there exists an arithmetic progression of primes 
\[
q - M, q - M + 1, \ldots, q_0 = q, q_1, \ldots, q_M
\]
for some \( M \geq \max\{N, 2^k\} \). We may suppose the common difference is \( s \) so that 
\[
q = q_\ell - M, q_\ell + 1 s \geq 2^k s \quad \text{and} \quad q_i = q + is \quad \text{for each} \quad i = 1, \ldots, M.
\]
In particular, 
\[
q < q_1 < \ldots < q_M < 2q.
\] (32)
By Lemma 5.7, there exists a consecutive subsequence of \( q_1, \ldots, q_M \), starting at \( q_{i_1} \) for some \( i_1 \geq 1 \), of length \( M_1 = \lfloor M/2 \rfloor \geq 2^{k-1} \) consisting of elements none of which are Mersenne with respect to \( p_1 \), which starts an induction. Suppose \( j \leq k \) and, as inductive hypothesis, that we have a consecutive subsequence starting at \( q_{i_{j-1}} \) of length \( M_{j-1} \geq 2^{k-j+1} \) consisting of elements none of which are Mersenne with respect to \( p_1, \ldots, p_{j-1} \). By Lemma 5.7, this contains a consecutive subsequence starting at \( q_{i_j} \) for some \( i_j \geq i_{j-1} \) of length \( M_j \geq \lfloor M_{j-1}/2 \rfloor \geq 2^{k-j} \) consisting of elements none of which are Mersenne with respect to \( p_1, \ldots, p_j \), establishing the inductive step. The lemma now follows by induction by observing that \( M_k \geq 2^{k-k} = 1 \), so that we have found at least one prime \( q_{i_k} \geq N \) that is not Mersenne with respect to \( p_1, \ldots, p_k \).

Remark 5.9. Ramanujan [16] showed that \( \pi(n) - \pi(n/2) \) tends to infinity as \( n \) does, where \( \pi(n) \) denotes the number of primes less than or equal to \( n \), generalising Bertrand’s postulate. This also guarantees the existence of an integer \( q \) and primes \( q_1, \ldots, q_M \) such that (32) holds, and the proof of Theorem 5.8 proceeds as above, but avoiding use of the Green-Tao theorem.

Example 5.10. Again let \( P = \{p_1, \ldots, p_k\} \) be a finite collection of distinct primes and \( N = \{n_1, \ldots, n_k\} \) a collection of positive integers. This time, we choose a prime \( q \) that is not Mersenne with respect to all of the primes in \( P \), and larger than all of the primes in \( P \), the existence of which is guaranteed by Theorem 5.8. For each \( i \), define \( T_i, \hat{T}_i = T_i \oplus I_{n_i}, V_i, \hat{V}_i, G_i = V_i \rtimes T_i \) and \( \hat{G}_i \rtimes \hat{T}_i \), as in Example 5.3, but noting that \( a_i = 1 \), since \( q \) is not Mersenne with respect to \( p_i \), by Lemma 5.5. Again, \( |T_i| = |\hat{T}_i| = q \), but now \( V_i = \mathbb{F}_{p_i}^{n_i}, \hat{V}_i = \mathbb{F}_{p_i}^{n_i+n_i} \), and we have the following simplifications:

\[
\phi_{T_i} = \pi_i, \quad \chi_{T_i} = \pi_i^{n_i}, \quad \phi_{\hat{T}_i} = (x - 1)\pi_i, \quad \chi_{\hat{T}_i} = (x - 1)^{n_i} \pi_i^{n_i}.
\]

Both (30) and (31) hold as before:

\[
\mu(G_i) = \mu(\hat{G}_i) = n_i p_i q_i \quad \text{and} \quad \hat{G}_i \cong G_i \times C_{p_i}^{n_i}.
\]

As before, putting \( T = \bigoplus_{i=1}^k T_i, \hat{T} = \bigoplus_{i=1}^k \hat{T}_i, V = \bigoplus_{i=1}^k V_i, \hat{V} = \bigoplus_{i=1}^k \hat{V}_i, G = V \rtimes T \) and \( \hat{G} = \hat{V} \rtimes \hat{T} \cong G \times C_{p_1}^{n_1} \times \ldots \times C_{p_k}^{n_k} \), we have

\[
\mu(G) = \sum_{i=1}^k \mu(G_i) = \sum_{i=1}^k n_i p_i q_i = \sum_{i=1}^k \mu(\hat{G}_i) = \mu(\hat{G}).
\]

Finally, as before, put \( H = C_{p_1}^{n_1} \times \ldots \times C_{p_k}^{n_k} \). Then \( \mu(G \times H) = \mu(G) \), so (27) holds, yet \( G \) does not decompose nontrivially as a direct product. Note that when \( H = C_{p_1} \times \ldots \times C_{p_k} \), the action of \( G \) on each Sylow \( p_i \)-subgroup is irreducible. The authors are not aware of any simpler method for achieving this last property, which appears to be inextricably linked to number-theoretic properties of the particular primes involved.
REFERENCES


School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia

E-mail address: david.easdown@sydney.edu.au

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia

E-mail address: michael.hendriksen@sydney.edu.au