THE UNIVERSITY OF
SYDNEY

Minimal Permutation Representations of Classes of Semidirect Products of Groups

Michael Hendriksen

A thesis submitted in fulfillment of
the requirements for the degree of
Master of Science

Pure Mathematics
University of Sydney

February 2016

CONTENTS

Introduction

This thesis provides an analysis of the topic of minimal permutation representations of finite groups. Given a finite group, we seek the smallest symmetric group it can be embedded into. If the smallest symmetric group that a group G can be embedded into is $\mathrm{Sym}(n)$, we say that G has a minimal degree equal to n, denoted $\mu(G) = n$. Much of the accumulated literature focuses on the interplay between minimal degrees and direct products. This thesis extends this to cover large classes of semidirect products. This is a useful step towards a catalogue of minimal degrees of small groups, due to the large number of small groups that can be constructed from cyclic groups using semidirect products.

Chapter 1 provides a background for minimal degrees - stating and proving a number of essential theorems and outlining the previous work on direct products by Johnson and Wright in the 1970s. Minimal degrees for a number of infinite classes of semidirect products are calculated using both established and original theory. The utility of the research into semidirect products is then demonstrated by producing some members of a special class of groups introduced by Wright, denoted $\mathcal{G}$, for which the minimal degree is additive with respect to taking direct products. The existence of this class of groups is one of the deeper results in the theory of minimal degrees.

Chapter 2 extends this to calculate minimal degrees for an infinite class of more complicated semidirect products - specifically the semidirect products of elementary abelian groups by groups of prime order not dividing the order of the base group, so that Maschke's theorem is available. This is established using vector space theory, including a number of novel techniques. Much of the time is spent establishing results on normal cores of subgroups of a semidirect product of elementary abelian groups with prime cyclic groups. The utility of this research is then demonstrated by answering an existing problem in the field of minimal degrees in a novel and potentially generalisable way. The class of examples introduced in this chapter include as special cases the seminal examples of Wright (1975) and Saunders (2010) where μ is not additive with respect to taking direct products.

Acknowledgements

I must first and foremost thank my supervisor, Associate Professor Dr David Easdown. His genuine interest in my work and life is an integral part of my continued interest in the topic, and his keen ability to differentiate the wheat from the chaff in my work has been invaluable in producing the work in my thesis.

Secondly, my associate supervisor Dr Anthony Henderson, whose amazing ability to produce useful and effective counterexamples and proofs in a matter of minutes saved countless hours of blundering on my part.

To my partner, Madison Tanner, I must also convey a deep and abiding thanks. She patiently listened to me ramble about mathematics that she had little-to-no interest in, endlessly supported me and propped me up when I lacked motivation - with no complaints and a lot of love.

Finally, I would like to thank my entire family, without whom I would literally not be here, as well as for supporting and nurturing my love of mathematics throughout my life.

CHAPTER 1

Preliminary Work

1.1. Historical Context

Permutation representations of finite groups are extremely useful for computation - composition of permutations with symmetric group elements is much easier to program than general group multiplication. A particularly interesting facet of this topic is the study of minimal permutation representations, in which we seek the most efficient way of representing a given finite group as a subgroup of a symmetric group. We define the *minimal degree* of a finite group G, denoted $\mu(G)$, to be the smallest integer n for which G can be embedded into the symmetric group on a set consisting of n elements. Denote the symmetric group on a set X by $\mathrm{Sym}(X)$, and write $\mathrm{Sym}(n)$ when $X = \{1, ..., n\}$. Unless otherwise stated, all groups will hereafter be assumed to be finite. We first dispose of the trivial group.

Example 1.1.1. The minimal degree of the trivial group is 0, as $\mathrm{Sym}(\varnothing) = \{\varnothing\}$ is trivial.

That the minimal degree is defined for finite groups is due to a single theorem named in honour of Cayley.

Theorem 1.1.2 (Cayley's Theorem)**.** *Any group G is isomorphic to a subgroup of the symmetric group* $\mathrm{Sym}(G)$.

The standard embedding (known as the *right regular representation* or *Cayley representation*) used to prove Cayley's Theorem is induced by multiplication on the right by group elements. In particular, when G is finite this establishes that $|G|$ is an upper bound for $\mu(G)$. However, with only a few exceptions, one can embed G into a much smaller symmetric group. By just examining the order of the group, we can easily establish some bounds on the minimal degree.

Remark 1.1.3. If $a(x)$ denotes the smallest number n such that x divides $|\mathrm{Sym}(n)| = n!$, then clearly $\mu(G) \geq a(|G|)$.

Example 1.1.4. Take any group G such that $|G| = p$ or 4, for p a prime. Then $\mu(G) \leq |G|$ by Cayley's Theorem. We can see that $a(|G|) = |G|$,

as 4 does not divide $3!$, and p certainly does not divide $(p-1)!$. Hence $\mu(C_2 \times C_2) = \mu(C_4) = 4$, and $\mu(C_p) = p$.

In this example, we saw some cases in which the regular representation is a minimal representation. The seminal work on minimal degrees [**7**], by D. L. Johnson, characterises completely for which groups this occurs.

Theorem 1.1.5 ([**7**], Theorem 1)**.** *If G is a group, then $\mu(G) = |G|$ if and only if G is isomorphic to a cyclic group of prime power order, a generalised quaternion 2-group, or $C_2 \times C_2$.*

For an important class of groups for which the minimal permutation representation is characterised, we have a theorem by Karpilovsky in [**8**] (and independently discovered by Johnson in [**7**]), which will be used implicitly throughout this thesis as well.

Theorem 1.1.6 (Karpilovsky)**.** *If $A = A_1 \times ... \times A_k$ is an abelian group, with each A_i prime power cyclic of order a_i, then $\mu(A) = a_1 + ... + a_k$.*

Corollary 1.1.7. *If $G = C_m$ is a cyclic group such that $m = p_1^{e_1}...p_n^{e_n}$ where $p_1, ..., p_n$ are distinct primes, then $\mu(G) = p_1^{e_1} + ... + p_n^{e_n}$.*

Example 1.1.8. Suppose $G = C_{210}$. Noting that $210 = 2 \times 3 \times 5 \times 7$, one easily produces that G is isomorphic to the following subgroup of $\mathrm{Sym}(17)$:

$$\langle (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9\ 10)(11\ 12\ 13\ 14\ 15\ 16\ 17) \rangle.$$

We will now examine how the minimal degree interacts with basic group theoretic concepts such as subgroups and the direct product.

Remark 1.1.9. Given two groups $H \leq G$, clearly $\mu(H) \leq \mu(G)$, as if there were some embedding $\varphi : G \to \mathrm{Sym}(n)$ for some n, then the restriction of φ to H provides an embedding of H into $\mathrm{Sym}(n)$.

Example 1.1.10. Let $G = D_{2p^\alpha}$ be a dihedral group of order $2p^\alpha$ where p is any prime and $\alpha \geq 1$:

$$D_{p^\alpha} = \langle a, b \mid a^{p^\alpha} = b^2 = 1, b^{-1}ab = a^{-1} \rangle.$$

Then, as $\langle a \rangle \cong C_{p^\alpha}$ is a subgroup of G, so by the previous remark and Theorem 1.1.5 we see that $\mu(G) \geq p^\alpha$. Put $n = p^\alpha$, and let

$$x = (1\ 2\ ...\ n),$$
$$y = (1\ n)(2\ (n-1))...(\left\lfloor \frac{n}{2} \right\rfloor\ \left\lceil \frac{n+2}{2} \right\rceil).$$

Then we observe that the map

$$\varphi : a \mapsto x, b \mapsto y$$

induces an embedding of G into $\mathrm{Sym}(p^a)$ and therefore $\mu(G) = p^\alpha$. This is a special case of the general fact that $\mu(D_{2n}) = \mu(C_n)$ for any $n \geq 3$, explored further below.

Suppose H embeds in $\mathrm{Sym}(m)$ and K embeds in $\mathrm{Sym}(n)$. Then clearly $H \times K$ embeds in $\mathrm{Sym}(m) \times \mathrm{Sym}(n)$, which is isomorphic to a subgroup of $\mathrm{Sym}(m+n)$. Thus we have the following simple fact.

Remark 1.1.11. If H and K are groups, then $\mu(H \times K) \leq \mu(H) + \mu(K)$.

Given the fact that a subgroup H of G has a minimal degree no larger than G, one might naively expect that a quotient group G/N might also have a minimal degree no larger than G. However, this is not the case, as we will see in the next section.

Now, a large section of the literature has examined the effect of the direct product on the minimal degree. The minimal degree is often additive with respect to taking direct products, for some familiar groups.

Proposition 1.1.12 ([**7**], Proposition 2)**.** *If G and H are two groups of coprime order, then*

$$\mu(G \times H) = \mu(G) + \mu(H).$$

This is the simplest to prove of the results on which groups have additive minimal degrees with respect to direct products. A deep work by Wright, [**19**], in 1975, outlines another large class of groups for which the minimal degree is additive with respect to taking direct products.

Theorem 1.1.13 (Wright's Theorem)**.** *Let $\mathcal{G}$ denote the class of groups G which have a nilpotent subgroup G_1 for which $\mu(G) = \mu(G_1)$. If $G, H \in \mathcal{G}$, then $G \times H \in \mathcal{G}$, and*

$$\mu(G \times H) = \mu(G) + \mu(H).$$

In [**19**], Wright goes on to outline a lot of familiar groups which belong to $\mathcal{G}$, including nilpotent groups, symmetric groups, dihedral groups, alternating groups and more, as well as showing that the class $\mathcal{G}$ is closed under direct products.

With such a wide variety of groups for which the direct product is additive, one might begin to think that all are! Indeed, Wright posed the question in [**19**] as to whether there were any groups for which the minimal degree is strictly subadditive with respect to the direct product. A referee for the paper provided groups G and H such that $G \times H$ embeds in

$\mathrm{Sym}(15)$, and $\mu(G \times H) < \mu(G) + \mu(H)$. Later, Saunders in [**17**], outlines an infinite class of finite reflection groups containing the referee's example and demonstrates that they form examples for which the minimal degree is strictly sub-additive. He provides an example where the direct product embeds in $\mathrm{Sym}(10)$, and proves (with the assistance of a computer search) that no example embeds in $\mathrm{Sym}(9)$ with the subadditive property.

Before moving any further, we shall outline the theory behind permutation representations.

Definition 1.1.14. A *permutation representation* of a group G is a homomorphism

$$\phi : G \to \mathrm{Sym}(X)$$

for some set X. A permutation representation is termed *faithful* if it is injective. If a permutation representation has the property that X has a single orbit under the induced $G\phi$-action, it is termed *transitive*. A permutation representation $\phi : G \to \mathrm{Sym}(X)$ is *finite* if X is finite. The *degree* of ϕ is $|X|$.

We shall restrict our attention in general to finite, faithful permutation representations. A useful concept for permutation representations is the direct sum.

Definition 1.1.15. A *direct sum* of permutation representations $\phi : G \to \mathrm{Sym}(X)$ and $\tau : G \to \mathrm{Sym}(Y)$, denoted $\phi \oplus \tau$ is a homomorphism

$$\phi \oplus \tau : G \to \mathrm{Sym}(X \sqcup Y)$$

such that for all $g \in G$, $x \in X, y \in Y$,

$$g(\phi \oplus \tau) : x \mapsto x(g\phi), y \mapsto y(g\tau).$$

This definition generalises in an obvious way to the direct sum of any number of permutation representations using disjoint sets. Transitive permutation representations are particularly useful as they form the building blocks for all other permutation representations.

Proposition 1.1.16. *Every finite permutation representation of G is a direct sum of transitive permutation representations.*

Definition 1.1.17. Let $\varphi : G \to \mathrm{Sym}(X)$ and $\psi : G \to \mathrm{Sym}(Y)$ be two permutation representations of G. We say φ and ψ are *equivalent* if there exists a bijection $\theta : X \to Y$ such that the following diagram commutes for all $g \in G$:

$$\begin{array}{ccc} X & \xrightarrow{\theta} & Y \\ \Big\downarrow{\scriptstyle g\varphi} & & \Big\downarrow{\scriptstyle g\psi} \\ X & \xrightarrow{\theta} & Y \end{array}$$

We will see that all transitive representations of G are equivalent to representations that arise by considering the action on right cosets of G.

Proposition 1.1.18. *Any group G acts transitively by right multiplication on the set G/H of right cosets of a subgroup H of G. In particular, the largest normal subgroup of G contained in H,*

$$\mathrm{core}(H) := \bigcap_{g \in G} g^{-1} H g,$$

is the kernel of the action.

In the case that $\mathcal{H}$ is a collection of subgroups, define $\mathrm{core}(\mathcal{H})$ to be the intersection of the cores of each subgroup in H.

Returning to the case at hand, more explicitly, we define a homomorphism

$$\phi_H : G \to \mathrm{Sym}(G/H),$$

by the rule

$$g\phi_H : Hh \to Hhg,$$

for all $g, h \in G$. Then, given a collection of subgroups $\{H_1, ..., H_k\}$ of G, we can define a permutation representation in terms of $\phi_{H_1}, ..., \phi_{H_k}$ as follows:

$$\phi = \phi_{H_1} \oplus ... \oplus \phi_{H_k} : G \to \mathrm{Sym}(G/H_1 \sqcup ... \sqcup G/H_k).$$

In this way, we can unambiguously refer to a collection of subgroups of G as affording a permutation representation of G. Indeed, one can see that the representation ϕ above, afforded by $\{H_1, ..., H_k\}$, will be faithful if and only if

$$\bigcap_i \ker(\phi_{H_i}) = \bigcap_i \mathrm{core}(H_i) = \mathrm{core}(\bigcap_i H_i) = \{1\}.$$

As promised, we see that any transitive permutation representation is equivalent to the permutation representations arising in the above way.

Theorem 1.1.19. *Let G be a group and X a non-empty set, and let $\varphi : G \to \mathrm{Sym}(X)$ be a transitive permutation representation of G. Then φ is equivalent to φ_H (as defined above) for some subgroup H of G.*

Proof. Let $x \in X$ and define $H := \{g \in G \mid x(g\varphi) = x\}$ to be the stabiliser of x in $G\varphi$. Let $y \in X$. Then there exists $g \in G$ such that $g\varphi : x \mapsto y$, which we can find as φ is transitive. Then define $\theta : X \to G/H$ so that

$$x\theta = Hg.$$

It is easy to show that θ is a bijection for which the diagram in Definition 1.1.17 is commutative, where $Y = G/H$ and $\psi = \varphi_H$. □

Corollary 1.1.20. *Every permutation representation ϕ of a non-trivial finite group G is equivalent to $\varphi_{H_1} \oplus ... \oplus \varphi_{H_K}$ for some collection $\{H_1, ..., H_k\}$ of subgroups of G. The degree of such a representation will be*

$$\deg(\phi) = \sum_{i=1}^{k} [G : H_i].$$

Hence we can reformulate the minimal degree of a non-trivial finite group in terms of a minimisation problem involving its lattice of subgroups.

Theorem 1.1.21. *For G finite and non-trivial, $\mu(G)$ is the minimum of $\sum_{i=1}^{k} [G : H_i]$ over all subgroup collections $\{H_1, ..., H_k\}$ for which*

$$\bigcap_{i=1}^{k} \mathrm{core}(H_i) = \{1\}.$$

Example 1.1.22. Let $A = A_1 \times ... \times A_k$ be an abelian group, with each A_i prime power cyclic of order a_i. Then if we define

$$H_i = A_1 \times ... \times A_{i-1} \times A_{i+1} \times ... \times A_k,$$

then the subgroup collection $\{H_1, ..., H_k\}$ has a trivial core intersection and an index sum of $a_1 + ... + a_k$. This is minimal by Karpilovsky's Theorem, and provides a nice example of a subgroup collection that affords a minimal representation.

In order to apply Theorem 1.1.21, we develop a useful few lemmas.

Lemma 1.1.23. *Suppose G is a finite group with a unique normal subgroup of prime order p. Then any collection of subgroups affording a faithful representation of G must include a subgroup H of order not divisible by p.*

Proof. Let N be the unique normal subgroup of G of order p. Let the subgroup collection $\{H_1, ..., H_k\}$ afford a faithful representation of G. If p divides $|H_i|$ for each i then, by Sylow theory, $N \subseteq H_i$, so that $\mathrm{core}(H_1 \cap ... \cap H_k) \supseteq N$ and is not trivial, contradicting faithfulness. Hence $|H_i|$ is not divisible by p for some i. □

For a finite group G and a prime number p, denote by $|G|_p$ the highest power of p dividing $|G|$.

Lemma 1.1.24. *Let G be a finite group with unique (necessarily normal) subgroups of order $p_1, ..., p_k$, where $p_1, .., p_k$ are distinct primes. Then*

$$\mu(G) \geq |G|_{p_1} + ... + |G|_{p_k}.$$

Proof. By 1.1.23, any collection of subgroups of G affording a minimal faithful representation of G must contain subgroups $H_1, ..., H_k$ such that p_i does not divide $|H_i|$ for $i = 1, ..., k$. Note that if $H_{i_1} = H_{i_2} = ... = H_{i_\ell}$ for $i_1 < i_2 < ... < i_\ell$ then

$$|G : H_{i_1}| \geq |G|_{p_{i_1}}|G|_{p_{i_2}}...|G|_{p_{i_\ell}} \geq |G|_{p_{i_1}} + |G|_{p_{i_2}} + ... + |G|_{p_{i_\ell}}.$$

It follows quickly that $\mu(G) \geq |G|_{p_1} + |G|_{p_2} + ... + |G|_{p_k}$. □

For example, we can quickly deduce a special case of Karpilovsky's Theorem.

Corollary 1.1.25. *Let $G = C_m$ be a cyclic group of order $m = p_1^{e_1}...p_k^{e_k}$, where p_i is a prime and e_i a positive integer. Then*

$$\mu(C_m) = p_1^{e_1} + ... + p_k^{e_k}.$$

Proof. Observe that G has a unique subgroup of order p_i, and therefore by the theorem $\mu(G) \geq |G|_{p_{i_1}} + |G|_{p_{i_2}} + ... + |G|_{p_{i_\ell}} = p_1^{e_1} + ... + p_k^{e_k}$. But if we let a be a generator of C_m, then the subgroup collection

$$\{\langle a^{m/p_1^{e_1}} \rangle, ..., \langle a^{m/p_k^{e_k}} \rangle\}$$

affords a faithful representation of degree $p_1^{e_1} + ... + p_k^{e_k}$. Therefore $\mu(G) \leq p_1^{e_1} + ... + p_k^{e_k}$, whence $\mu(G) = p_1^{e_1} + ... + p_k^{e_k}$. □

We demonstrate the utility of the lemma by calculating the minimal degree for a generalised quaternion group.

Definition 1.1.26. The *generalised quaternion group* or *dicyclic group* of order $4n$ for n a positive integer, is

$$Q_{4n} := \langle a, b \mid a^{2n} = b^4 = 1, a^n = b^2, b^{-1}ab = a^{-1} \rangle.$$

Proposition 1.1.27. *Let $G = Q_{4n}$ be a generalised quaternion group, where $n \geq 2$, and denote the odd prime divisors (if any) by $p_1, ..., p_k$. Then*

$$\mu(G) = |G|_2 + |G|_{p_1} + ... + |G|_{p_k}.$$

In particular, when n is a power of 2, this becomes $\mu(Q_{4n}) = |Q_{4n}| = 4n$.

Proof. Without causing confusion, we may write

$$G = Q_{4n} = \{a^i b^\varepsilon \mid 0 \leq i \leq 2n-1, 0 \leq \varepsilon \leq 1\},$$

where multiplication of group elements becomes:

$$a^i b^\varepsilon a^j b^\delta = \begin{cases} a^{i+j} b^\delta & \text{if } \varepsilon = 0, \\ a^{i-j} b^{1+\delta} & \text{if } \varepsilon = 1. \end{cases}$$

It follows quickly that $\langle b^2 \rangle$ is the unique subgroup of order 2 and is in fact the centre of G. Hence if n is a power of 2 then $|G|_2 = |G|$ so that, by the previous lemma, $\mu(G) \geq |G|$, whence we get the well-known result $\mu(Q_{4n}) = 4n$.

It is easy to see that if p is an odd prime dividing n, then $\langle a^{2n/p} \rangle$ is the unique (necessarily normal) subgroup of G of order p.

Therefore we can assume that n is not a power of 2 and that $p_1, ..., p_k$ are all of the distinct odd prime divisors of n. By the lemma,

$$\mu(G) \geq |G|_2 + |G|_{p_1} + ... + |G|_{p_k}.$$

Write

$$|G| = 2^m p_1^{\alpha_1} ... p_k^{\alpha_k}$$

where $m \geq 2$ and $\alpha_1, ..., \alpha_k \geq 1$. Then

$$|\langle a \rangle| = 2^{m-1} p_1^{\alpha_1} ... p_k^{\alpha_k}, \; |G|_2 = 2^m, \; |G|_{p_i} = p_i^{\alpha_i} \text{ for } i = 1, ..., k.$$

Put

$$H = \langle a^{2^{m-1}} \rangle \text{ and } H_i = \langle a^{p_i^{\alpha_i}}, b \rangle$$

for $i = 1, ..., k$. Note that if $k = 1$ and $m = 2$ then $a^{p_1^{\alpha_1}} = a^n = b^2$, so that $H_1 = \langle b \rangle$. Clearly $H_1 \cap ... \cap H_k = \langle b \rangle$, so

$$H \cap H_1 \cap ... \cap H_k = \{1\}.$$

Hence $\{H, H_1, ..., H_k\}$ affords a faithful representation of G of degree

$$|G : H| + |G : H_1| + ... + |G : H_k| = 2^m + p_1^{\alpha_1} + ... + p_k^{a_k}$$

and thus the result is proven. □

Example 1.1.28. Let $G = Q_{12} = \langle a, b | a^6 = 1, a^3 = b^2, a^b = a^{-1} \rangle$, the smallest generalised quaternion group that is not a 2-group. By the proposition, $\mu(G) = |G|_2 + |G|_3 = 4 + 3 = 7$. From the proof, a minimal faithful representation is afforded by $\{H, K\}$, noting $m = 2, k = 1$ and $p = 3$, where

$$H = \langle a^2 \rangle = \{1, a^2, a^4\} \text{ and } K = H_1 = \langle a^3, b \rangle = \{1, a^3, b, a^3 b\}.$$

Then $G/H = \{H, Ha, Hb, Hab\}$, $G/K = \{K, Ka, Ka^2\}$ and it is easy to check that

$$\begin{aligned}
a\varphi_H &: H \mapsto Ha \mapsto H, Hb \mapsto Hab \mapsto Hb, \\
b\varphi_H &: H \mapsto Hb \mapsto Ha \mapsto Hab \mapsto H, \\
a\varphi_K &: K \mapsto Ka \mapsto Ka^2 \mapsto K, \\
b\varphi_K &: K \mapsto K, Ka \mapsto Ka^2 \mapsto Ka.
\end{aligned}$$

Thus if we put $\varphi = \varphi_H \oplus \varphi_K$ and $\theta : G/H \sqcup G/K \to \{1, ..., 7\}$, where

$$\theta : K \mapsto 1, Ka \mapsto 2, Ka^2 \mapsto 3, H \mapsto 4, Hb \mapsto 5, Ha \mapsto 6, Hab \mapsto 7,$$

then $a(\theta^{-1} \circ \varphi \circ \theta) = (1\ 2\ 3)(4\ 6)(5\ 7), b(\theta^{-1} \circ \varphi \circ \theta) = (2\ 3)(4\ 5\ 6\ 7)$ and we get

$$G \cong \langle (1\ 2\ 3)(4\ 6)(5\ 7), (2\ 3)(4\ 5\ 6\ 7) \rangle = \langle (1\ 2\ 3), (2\ 3)(4\ 5\ 6\ 7) \rangle.$$

It is worth noting that this is the smallest example of a group that is not in Wright's class, $\mathcal{G}$. One sees Q_{12} cannot be in $\mathcal{G}$ as it is clearly not nilpotent and no proper subgroup of Q_{12} can have minimal degree 7. That Q_{12} is the smallest group outside of $\mathcal{G}$ can be seen easily, as all groups of order less than 12 are either abelian, a dihedral group covered by Example 1.1.10 or Q_8, which is nilpotent.

Note, in particular, our method verifies that the regular representation is minimal for both prime power cyclic groups and generalised quaternion 2-groups.

1.2. Minimal Degrees of Quotient Groups

Another substantial portion of the literature centres around the effect of taking quotient groups on the minimal degree. For example, one might naively expect that $\mu(G/N) \leq \mu(G)$ for N a normal subgroup of G, but this is quite false!

Definition 1.2.1. A group G with a normal subgroup N such that $\mu(G) < \mu(G/N)$ is referred to as *exceptional*. In such a case the subgroup N and corresponding quotient group G/N are referred to as the *distinguished subgroup* and *distinguished quotient* of G respectively.

In fact, as shown by Neumann ([**13**]), particularly aberrant groups can have $\mu(G/N)$ exponentially larger than $\mu(G)$. Take G to be the direct product of n copies of D_8, which by Wright's Theorem and the previously shown fact that $\mu(D_8) = 4$ gives us that $\mu(G) = 4n$. Neumann shows that certain subgroups N of G have the property that $\mu(G/N) = 2^{n-1}$, which becomes exponentially larger than $4n$ for increasing n. This topic was expanded upon by Holt and Walton, [**6**], who showed that for any finite group G, the minimal degree of a quotient group of G is bounded above by $c^{\mu(G)-1}$, where $c = 4.5$.

Easdown and Praeger [**4**] showed that the smallest possible exceptional groups occur at order 32 - finding two of them. They also provide several infinite classes of examples of exceptional groups, including p-groups and direct products of dihedral groups and quaternion 2-groups. The study of exceptional groups was continued by Lemieux in his Masters thesis ([**10**]) and, later, a paper ([**11**]), in which he showed that no p-groups of order less than p^4 can be exceptional, and provided an example of an exceptional p-group of order p^5.

It has been conjectured (see the survey article [**2**]) that if for a group G and a subgroup $N \trianglelefteq G$, G/N is abelian, then $\mu(G) \geq \mu(G/N)$, referred to as the Abelian Quotients Conjecture. They went on to show that a minimal counterexample, were it to exist, would be a p-group with the commutator subgroup N as its distinguished subgroup (again, see [**2**]). Kovacs and Praeger in [**9**] demonstrate that for a group G and a subgroup $N \trianglelefteq G$, that if G/N is elementary abelian then $\mu(G/N) \leq \mu(G)$.

Franchi in [**5**] continued this analysis, showing that a counterexample could not be a non-abelian p-group with an abelian maximal subgroup.

Theorem 1.2.2 ([**5**], Theorem 1)**.** *If G is a non-abelian finite p-group with an abelian maximal subgroup, and we denote the commutator subgroup by G', then $\mu(G/G') \leq \mu(G)$.*

1.3. Semidirect Products and Minimal Degrees

Semidirect products are a usual method of constructing large groups from smaller groups. As can be seen from browsing a catalogue of small groups, (see, for example, [**18**]), 88 of the 93 groups of order less than 32 can be constructed by starting with cyclic groups and nesting semidirect products. Similarly large proportions can also be seen in [**18**] for groups of order up to 100. If we develop a theory of how minimal degrees work with respect to semidirect products it would be a big step towards developing a catalogue of minimal degrees for finite groups up to a reasonable size.

Definition 1.3.1. Let G be a group with two subgroups N, H such that N is normal, $G = NH$ and $N \cap H$ is trivial. Then G is termed the *(internal) semidirect product* of N by H, and H is termed a *complement* of N in G.

It is immediate that $G/N \cong H$, so that G is an extension of N by H, called a *split extension*, because the image H arises as a complement of N.

A natural question is, given an internal semidirect product $G = NH$ of N by H, whether we can define a multiplication on $\overline{G} = N \times H$ such that $\overline{G}$ is the internal semidirect product of $N \times \{1\} \cong N$ by $\{1\} \times H \cong H$.

Suppose G is an internal semidirect product of N by H. Every element of G can be expressed uniquely as a product nh, with $n \in N, h \in H$ (because $N \cap H = \{1\}$). Since N is normal in G, for all $h \in G$ we can define an automorphism φ_h of N by $n \mapsto h^{-1}nh$. We can then construct a homomorphism $\varphi : H \to \mathrm{Aut}(N)$ by $h\varphi = \varphi_h$. Furthermore, for $n_1, n_2 \in N, h_1, h_2 \in H$,

$$(n_1h_1)(n_2h_2) = (n_1h_1n_2h_1^{-1})(h_1h_2) = (n_1(n_2\varphi_{h_1^{-1}}))(h_1h_2).$$

This observation motivates the following definition.

Definition 1.3.2. For two groups N, H and φ a group homomorphism $\varphi : H \to \mathrm{Aut}(N)$, the *(external) semidirect product of N and H with respect to φ*, denoted $N \rtimes_\varphi H$, is the Cartesian product $N \times H$, with multiplication defined by

$$(n_1, h_1) * (n_2, h_2) = (n_1(n_2\varphi_{h_1^{-1}}), h_1h_2)$$

for all $n_1, n_2 \in N, h_1, h_2 \in H$.

In what follows we use juxtaposition of ordered pairs (suppressing $*$) without causing confusion.

It is a simple exercise to show that $N \rtimes_\varphi H$ is a group, and in fact is an internal semidirect product of $N \times \{1\} \cong N$ by $\{1\} \times H \cong H$. Conversely,

if G is a semidirect product of N by H then $G \cong N \rtimes_\varphi H$ where φ is the homomorphism introduced above to motivate the definition.

Example 1.3.3. A common class of examples is the class of dihedral groups, which are the semidirect products $C_m \rtimes_\varphi C_2$ for each $m \in \mathbb{N}$, where φ maps the generator of C_2 to the inversion automorphism of C_m.

We can already establish an upper bound on the minimal degree of a semidirect product of two groups.

Theorem 1.3.4. *Suppose that $G \rtimes_\varphi H$ is a semidirect product of groups G and H, not necessarily finite, via a homomorphism $\varphi : H \to \mathrm{Aut}(G)$. Then*

$$G \rtimes_\varphi H \lesssim \mathrm{Sym}(G) \times H.$$

If φ is injective, then $G \rtimes_\varphi H \lesssim \mathrm{Sym}(G)$. In particular, if G and H are finite, then

$$\mu(G \rtimes_\varphi H) \leq |G| + \mu(H).$$

If further φ is injective, then $\mu(G \rtimes_\varphi H) \leq |G|$.

Proof. For $g \in G$, $h \in H$, define a mapping

$$\sigma_{(g,h)} : G \to G, x \mapsto (xg)\varphi_h \text{ for } x \in G.$$

It is easy to check $\sigma_{(g,h)}$ is bijective, so $\sigma_{(g,h)} \in \mathrm{Sym}(G)$. Now observe that if $x, g_1, g_2 \in G$ and $h_1, h_2 \in H$ then

$$\begin{aligned}
(x\sigma_{(g_1,h_1)})\sigma_{(g_2,h_2)} &= (((xg_1)\varphi_{h_1})g_2)\varphi_{h_2} \\
&= ((xg_1)\varphi_{h_1}\varphi_{h_2})(g_2\varphi_{h_2}) \\
&= ((xg_1)\varphi_{h_1h_2})(g_2\varphi_{h_1^{-1}}\varphi_{h_1}\varphi_{h_2}) \\
&= ((xg_1)\varphi_{h_1h_2})((g_2\varphi_{h_1^{-1}})\varphi_{h_1h_2}) \\
&= ((xg_1)(g_2\varphi_{h_1^{-1}}))\varphi_{h_1h_2} \\
&= (x(g_1(g_2\varphi_{h_1^{-1}})))\varphi_{h_1h_2} \\
&= x\sigma_{(g_1(g_2\varphi_{h_1^{-1}}),h_1h_2)} \\
&= x\sigma_{(g_1,h_1)(g_2,h_2)},
\end{aligned}$$

so that

$$\sigma : G \rtimes_\varphi H \to Sym(G), (g,h) \mapsto \sigma_{(g,h)}$$

is a homomorphism.

Now define $\tau : G \rtimes_\varphi H \to \mathrm{Sym}(G) \times H$ by

$$\tau : (g, h) \mapsto (\sigma_{(g,h)}, h) \text{ for } g \in G, H \in H,$$

which is clearly a homomorphism.

If $g \in G, h \in H$ and $(g, h)\tau = (id, 1)$ then $\sigma_{(g,h)} = id, h = 1$, so in particular

$$1 = 1\sigma_{(g,h)} = 1\sigma_{(g,1)} = g\varphi_1 = g,$$

so $g = 1$ and $h = 1$, verifying that τ is an embedding.

Suppose now that φ is injective. Let $(g, h) \in \ker(\sigma)$, so $\sigma_{(g,h)} = id$. In particular,

$$1 = 1\sigma_{(g,h)} = g\varphi_h,$$

so that $g = 1$, since φ_h is an automorphism of G. Hence, for all $x \in G$,

$$x = x\sigma_{(g,h)} = (xg)\varphi_h = x\varphi_h,$$

so that $\varphi_h = id \in \mathrm{Aut}(G)$. Hence $h = 1$, since φ is injective, so $(g, h) = (1, 1)$. This verifies that σ is injective. □

As a further introduction to semidirect products, we will characterise a number of easy semidirect products and then calculate the minimal degree for them using Theorem 1.1.21. Before we do, however, there is a simplifying lemma to make.

Lemma 1.3.5. *Let G be an internal semidirect product of N by H, and suppose that the induced homomorphism $\varphi : H \to \mathrm{Aut}(N)$ is injective. Then* $\mathrm{core}(H) = \{1\}$.

Proof. Let $h \in \mathrm{core}(H)$. Then for all $n \in N$,

$$h^{-1}nhn^{-1} \in N \cap \mathrm{core}(H) \subseteq N \cap H = \{1\},$$

so that $h^{-1}nhn^{-1} = 1$, yielding $n^h = h^{-1}nh = n$. Hence $h \in \ker(\varphi)$, so $h = 1$, since φ is injective. Thus $\mathrm{core}(H) = \{1\}$. □

Corollary 1.3.6. *If $G = N \rtimes_\varphi H$ is an external semidirect product and φ is injective, then H is core-free in G when regarding G as an internal semidirect product of N by H.*

Corollary 1.3.7. *If $G = N \rtimes_\varphi H$ is a semidirect product that is not direct and H is simple, then $\mu(G) \leq |N|$.*

Proof. Because G is not direct, φ is not the trivial homomorphism, so must be injective, since H is simple, so H is core-free and $\{H\}$ affords a faithful representation of G of degree $[G : H] = |N|$. □

We shall analyse a natural first case - the semidirect product of C_m with C_q with m, q relatively prime, and m square-free.

Proposition 1.3.8. *Let $p_1, ..., p_n, q$ be distinct primes and put $m = p_1...p_n$ (so m is square-free). Let $G = C_m \rtimes_\varphi C_q$ be a semidirect product that is not direct. Then*

$$\mu(G) = \mu(C_m) = p_1 + ... + p_n.$$

Proof. Write $C_m = \langle a \rangle$, $C_q = \langle c \rangle$. We may regard G as an internal semidirect product of $\langle a \rangle$ by $\langle c \rangle$ with induced homomorphism φ.

First note that

$$\mu(G) \geq \mu(\langle a \rangle) = p_1 + ... + p_n,$$

by Corollary 1.1.7. Also note that $\ker(\varphi) = \{1\}$, as the semidirect product is not direct and C_q is simple. Hence $\langle c \rangle$ is core-free, by Lemma 1.3.5. For $j = 1$ to n, put $H_j = \langle a^{p_j} \rangle$, the unique subgroup of $\langle a \rangle$ of index p_j, which is necessarily normal in G. Now put

$$K_j = \langle a^{p_j}, c \rangle = H_j \langle b \rangle,$$

which is the unique subgroup of G of index p_j. Observe that $\mathrm{core}(K_1 \cap ... \cap K_n) = \mathrm{core}(\langle c \rangle) = \{1\}$, so $\{K_1, ..., K_n\}$ affords a faithful representation of G of degree $p_1 + ... + p_n$. Hence $\mu(G) = p_1 + ... + p_n$. □

Example 1.3.9. Let $G = C_{35} \rtimes_\varphi C_3$ be a semidirect product that is not direct. We see that

$$\mathrm{Aut}(C_{35}) \cong \mathrm{Aut}(C_7) \times \mathrm{Aut}(C_5) \cong C_6 \times C_4,$$

which has a unique order 3 subgroup. Hence φ is non-trivial and uniquely determined, and it is quickly shown that

$$G \cong \langle a, b, c \mid a^7 = b^5 = c^3 = 1, a^c = a^2, a^b = a, b^c = b \rangle.$$

Then, from the proof of the above theorem, we find that after an appropriate identification of elements the subgroup collection $\{\langle a, c \rangle, \langle b, c \rangle\}$ affords a

minimal representation of G, from which we see that G is isomorphic to the following subgroup of $\mathrm{Sym}(12)$:

$$\langle (1\ 2\ 3\ 4\ 5\ 6\ 7), (8\ 9\ 10\ 11\ 12), (1\ 2\ 4)(3\ 6\ 5) \rangle.$$

We can change the order of the cyclic group on the right of the semidirect product.

Proposition 1.3.10. *Let $G = C_{p^n} \rtimes_\varphi C_{q^m}$ be a semidirect product with p,q distinct primes. Then*

$$\mu(G) = \begin{cases} p^n & \text{if } \varphi \text{ is injective,} \\ p^n + q^m & \text{otherwise.} \end{cases}$$

Proof. Let $C_{p^n} = \langle a \rangle, C_{q^m} = \langle b \rangle$. We may regard G as an internal semidirect product of $\langle a \rangle$ by $\langle b \rangle$. Now, G contains a subgroup isomorphic to C_{p^n}, and hence $\mu(G) \geq p^n$.

If φ is injective, then by Lemma 1.3.5 $\langle b \rangle$ is core-free, yielding a faithful representation of degree $[G : \langle b \rangle] = p^n$, whence $\mu(G) = p^n$.

Otherwise, suppose φ is not injective. Then $(b\varphi)^{q^{m-1}} = id \in \mathrm{Aut}(\langle a \rangle)$. It follows that $\langle a^{p^{n-1}} \rangle$ and $\langle b^{q^{m-1}} \rangle$ are normal and hence are the unique order p and unique order q subgroups of G respectively.

Hence by Lemma 1.1.23 there must be at least two subgroups in a minimal faithful representation, one of index at least p^n, and the other of index at least q^m. Hence the degree is bounded below by $p^n + q^m$.

Observing that the faithful representation afforded by $\{\langle a \rangle, \langle b \rangle\}$ is of degree $p^n + q^m$ we see $\mu(G) \leq p^n + q^m$. Thus $\mu(G) = p^n + q^m$. □

Example 1.3.11. A small, interesting example is $G = \langle a, b | a^5 = b^4 = 1, a^b = a^3 \rangle \cong C_5 \rtimes_\varphi C_4$. Since the homomorphism has order 4, we see that $\mu(G) = 5$. The subgroup collection $\{\langle b \rangle\}$ affords a minimal representation, yielding that G is isomorphic to the following subgroup of $\mathrm{Sym}(5)$:

$$\langle (1\ 2\ 3\ 4\ 5), (1\ 3\ 4\ 2) \rangle.$$

Alternatively, we can modify the right-hand side of the semidirect product to be a cyclic group of square-free order.

Proposition 1.3.12. *Let $p, q_1, ..., q_n$ be distinct primes and put $m = q_1 ... q_n$ (so m is square-free). Let $G = C_p \rtimes_\varphi C_m$ be a semidirect product, where $C_m = \langle b \rangle$. Put*

$$J = \{i | q_i \text{ divides } |b\varphi|\}$$

and write $k = \prod_{i \notin J} q_i$ *(interpreted as* 1 *if* $J = \{1, ..., n\}$*). Then*

$$\mu(G) = \mu(C_p \times C_k) = p + \sum_{i \notin J} q_i,$$

(interpreted as p *if* $J = \{1, ..., n\}$*).*

Proof. If $J = \varnothing$ then the result is immediate (by Karpilovsky's Theorem), so without loss of generality we may suppose $J = \{1, ..., j\}$ for some positive integer $j \leq n$. We may write $C_p = \langle a \rangle$ and suppose that $G = \langle a \rangle \langle b \rangle$ is an internal semidirect product. Put $H_0 = \langle b \rangle$ and

$$H_i = \langle a \rangle \langle b^{q_{j+i}} \rangle \text{ for } i = 1 \text{ to } n - j.$$

Then $[G : H_0] = p$ and $[G : H_i] = q_{j+i}$ for $i = 1$ to $n - j$. Also put

$$K = H_0 \cap H_1 \cap ... \cap H_{n-j}$$

(interpreted as H_0 if $j = n$), so that

$$K = \langle b^{q_{j+1} \cdots q_n} \rangle$$

(interpreted as $\langle b \rangle$ if $j = n$), a subgroup of G of order $q_1 ... q_j$. Suppose that the core of K is non-trivial, so K contains a minimal normal subgroup $N = \langle c \rangle$ of G, which must be cyclic of prime order. Without loss of generality we may assume $c = b^{q_2 \cdots q_n}$ and $|c| = |c\varphi| = q_1$. Hence $a^c = a^\ell$ for some integer $\ell \neq 1 \bmod p$, so $c^a = ca^{1-l} \in N$, from which it follows that $a^{1-\ell} \in N$. But $a^{1-\ell} \neq 1$, so $a \in N$, contradicting that $\langle a \rangle \cap \langle b \rangle = \{1\}$.

This proves that K has trivial core, so $\{H_0, H_1, ..., H_{n-j}\}$ affords a faithful permutation representation of G of degree $p + q_{j+1} + ... + q_n$. But G contains the internal direct product

$$\langle a \rangle \times \langle b^{m/q_{j+1}} \rangle \times ... \times \langle b^{m/q_n} \rangle \cong C_p \times C_{q_{j+1}} \times ... \times C_{q_n}$$

so that $\mu(G) \geq \mu(C_p \times C_{q_{j+1}} \times ... \times C_{q_n}) = p + q_{j+1} + ... + q_n$, whence equality holds, and the proposition is proved. □

Example 1.3.13. We provide three contrasting examples of the above class of groups.

a) Let $G_1 = \langle a, b | a^7 = b^6 = 1, a^b = a^3 \rangle \cong C_7 \rtimes_{\varphi_1} C_6$. The induced homomorphism φ_1 is injective, as one can easily check it has order 6. Thus $\langle b \rangle$ is core-free and the subgroup collection $\{\langle b \rangle\}$ affords a minimal representation. We therefore see that $\mu(G_1) = 7$, with G_1 isomorphic to the following subgroup of $\mathrm{Sym}(7)$:

$$\langle (1\,2\,3\,4\,5\,6\,7), (1\,3\,2\,6\,4\,5)\rangle.$$

b) Let $G_2 = \langle a, b | a^7 = b^6 = 1, a^b = a^2\rangle \cong C_7 \rtimes_{\varphi_2} C_6$, so that $|b\varphi_2| = 3$, $J = \{3\}$ and by the theorem $\mu(G_2) = 9$. The minimal representation is afforded by $\{\langle b\rangle, \langle a^2 b\rangle\}$, giving

$$\langle (1\,2\,3\,4\,5\,6\,7), (1\,2\,4)(3\,6\,5)(8\,9)\rangle.$$

c) Let $G_3 = \langle a, b | a^7 = b^6 = 1, a^b = a^{-1}\rangle \cong C_7 \rtimes_{\varphi_3} C_6$, so that $|b\varphi_3| = 2$, $J = \{2\}$ and by the theorem $\mu(G_3) = 10$. The minimal representation is afforded by $\{\langle b\rangle, \langle a^3 b\rangle\}$, giving

$$\langle (1\,2\,3\,4\,5\,6\,7), (1\,6)(2\,5)(3\,4)(8\,9\,10)\rangle.$$

A well-studied form of semidirect product is the holomorph.

Definition 1.3.14. The *holomorph* of a group G, denoted $\mathrm{Hol}(G)$, is $G \rtimes_\varphi \mathrm{Aut}(G)$ with φ being the identity mapping, so multiplication is given by

$$(g, \alpha)(h, \beta) = (g(h\alpha^{-1}), \alpha\beta).$$

Theorem 1.3.15. *Let G be a group and $\mathrm{Hol}(G)$ its holomorph. Then*

$$\mu(\mathrm{Hol}(G)) \leq |G|.$$

Proof. It is a well-known fact (see [**14**]) that the holomorph of a group is isomorphic to the normaliser of the image of G in $\mathrm{Sym}(G)$ under the Cayley representation. The result immediately follows. Alternatively, note that φ is injective as it is the identity mapping, and the result follows by Theorem 1.3.4. □

We can now produce a number of novel examples of groups in Wright's class, $\mathcal{G}$.

a) Any $G = C_{p^m} \rtimes_\varphi C_{q^n}$ (p, q prime, $m, n \in \mathbb{N}$) for φ with multiplicative order q^n, since $\mu(G) = \mu(C_{p^m})$ and C_{p^m} is nilpotent.
b) Any $G = C_p \rtimes_\varphi (\times_{i=1}^n C_{q_i})$ with q_i distinct primes and φ non-trivial, since $\mu(G) = \mu(H)$ for some abelian subgroup H of G.
c) Any $\mathrm{Hol}(G)$ for G with a minimal regular representation, as $G \leq \mathrm{Hol}(G)$ and all G with a minimal regular representation are p-groups and thus nilpotent.

We can produce more by examining the properties of injective homomorphisms further.

Lemma 1.3.16. *Let G be a group, H a simple group and $\varphi : H \to \mathrm{Aut}(G)$ an injective homomorphism. If G has a minimal faithful representation afforded by a collection of subgroups that are invariant under the action induced by φ then*

$$\mu(G \rtimes_\varphi H) = \mu(G).$$

Proof. We may regard $G \rtimes H$ as an internal semidirect product of G by H. Since φ is injective, H is core-free by Lemma 1.3.5. Suppose that $\{B_1, ..., B_k\}$ is a collection of subgroups of G that are invariant under the action induced by φ and affording a minimal representation of G.

For $i = 1$ to k, put $D_i = B_i H$ which is a subgroup of $G \rtimes H$ of index $[G : B_i]$. Then $\mathrm{core}(D_1 \cap ... \cap D_k) = \mathrm{core}(H) = \{1\}$, so $\{D_1, ..., D_k\}$ affords a faithful representation of $G \rtimes H$ of degree

$$[G : B_1] + ... + [G : B_k] = \mu(G).$$

But $\mu(G \rtimes H) \geq \mu(G)$ so we have equality and the lemma is proved. □

Corollary 1.3.17. *Suppose G_1 has a minimal regular representation, H is simple, and $G = G_1 \rtimes H$ is not a direct product. Then $\mu(G) = \mu(G_1)$.*

Proof. The regular representation is afforded by the trivial subgroup which is preserved by the action of H. □

Example 1.3.18. Let A be an abelian group and form $A \rtimes_\varphi C_2$, where the action of the generator of C_2 on A is inversion (under which all subgroups of A are invariant). It follows from Lemma 1.3.16 that $\mu(A \rtimes C_2) = \mu(A)$. In particular, $\mu(D_{2n}) = \mu(C_n)$.

However, this lemma fails in the general case - there are large classes of examples of $G = G_1 \rtimes C_q$ for which no minimal representation of G is preserved by the action, and the minimal degree of G is wildly different to $\mu(G_1)$. The next chapter outlines many cases for which this is true.

CHAPTER 2

Vector Space Theory for Semidirect Products

We aim to have a complete characterisation of the minimal degree of a well-behaved class of groups - the semidirect product of an elementary abelian group with a prime cyclic group. Throughout this chapter, unless otherwise stated, p and q are distinct primes. We shall henceforth use the following notation:

$$E := C_p^n$$

Then E is an elementary abelian p-group, which may be viewed as an n-dimensional vector space over $\mathbb{F}_p$, the field with p elements.

Let V be an n-dimensional vector space over $\mathbb{F}_p$, and $T : V \to V$ an invertible linear transformation. Define

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

with multiplication

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

Then $V \rtimes \langle T \rangle$ is a group, called the *semidirect product of* V *by* $\langle T \rangle$ (or just the *semidirect product of* V *by* T). We shall suppose throughout that $T \neq id$ and $T^q = id$, unless otherwise stated, where id is the identity linear transformation. 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 T with respect to the basis, and so regard $T(v) = Tv$ as a matrix product. Under these identifications

$$V \rtimes \langle T \rangle \cong C_p^n \rtimes_\varphi C_q$$

under the map

$$\left(\begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix}, T^i \right) \mapsto ((a^{\lambda_1}, ..., a^{\lambda_n}), b^{-i})$$

where we write $C_p = \langle a \rangle, C_q = \langle b \rangle$, and $\varphi : C_q \to \mathrm{Aut}(C_p^n)$ is the homomorphism induced by

$$b\varphi : (a^{\lambda_1}, ..., a^{\lambda_n}) \to (a^{\lambda'_1}, ..., a^{\lambda'_n})$$

wherever

$$T \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} = \begin{bmatrix} \lambda'_1 \\ \vdots \\ \lambda'_n \end{bmatrix}.$$

Therefore, in what follows, we identify the semidirect products and write $V \rtimes \langle T \rangle$ and $E \rtimes_\varphi C_q$ interchangeably.

2.1. Preliminary Work

We can exploit the fact that we are taking our semidirect product by a prime cyclic group to prove a pair of useful results.

Theorem 2.1.1. *Let $G = HC$ be an internal semidirect product of H by C that is not direct (so C is not normal in G), such that $C \cong C_q$ for some prime q not dividing $|H|$.*

(a) If $K \leq G$ and $K \not\leqslant H$ then $K = (H \cap K)C^g$ is an internal semidirect product of $H \cap K$ by C^g for some $g \in G$. If, in addition, $H \cap K \lhd H$ then $H \cap K \lhd G$. If $K \lhd G$ then $K = (H \cap K)C$.
(b) If $\mathcal{C}$ is a collection of subgroups affording a minimal faithful representation of G then $\mathcal{C}$ does not contain any subgroup of H that is normal in G.

Proof.

(a) Suppose that $K \leq G$ and $K \not\leqslant H$. By Sylow theory, $H = \{g \in G \mid q \text{ does not divide } |g|\}$ and it follows that $H \cap K = \{k \in K \mid q \text{ does not divide } |k|\} \lhd K$. But q divides $|K|$, since $K \not\leqslant H$, so $|K| = q|H \cap K|$ and $x \in K$ for some x of order q. Hence $\langle x \rangle \cap H \cap K = \{1\}$ and $|(H \cap K)\langle x \rangle| = |H \cap K|q = |K|$, so that $K = (H \cap K)\langle x \rangle = (H \cap K)C^g$ for some $g \in G$, since $\langle x \rangle$ and C are Sylow q-subgroups of G.

Suppose, in addition, that $H \cap K \lhd H$. Since $G = HC^g$, we have $H \cap K$ normalised by both H and C^g and hence by G. If, further, $K \lhd G$ then, using the fact that $H \cap K \lhd G$,

$$K = K^{g^{-1}} = ((H \cap K)C^g)^{g^{-1}} = (H \cap K)^{g^{-1}}C = (H \cap K)C,$$

and the proof of (a) is completed.

(b) Let $\mathcal{C} = \{K_1, ..., K_k\}$ 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 $K_1 \lhd G$. If $K_1 \neq H$ then $\mathrm{core}(K_1C \cap H) = K_1$ and

$$[G : K_1C] + [G : H] = [H : K_1] + q < [H : K_1]q = [G : K_1],$$

so that $\{K_1C, H, K_2, ..., K_k\}$ affords a faithful representation of degree smaller than that afforded by $\mathcal{C}$, contradicting minimality. Hence $K_1 = H$. If $k = 1$, then $\mathcal{C} = \{H\}$ and $\{1\} = \mathrm{core}(H) = H$, so that C is normal, contradicting our initial assumptions. Hence $k > 1$ and $\mathcal{C} = \{H, K_2, ..., K_k\}$. Put $N = \mathrm{core}(K_2 \cap ... \cap K_k)$, so $H \cap N = \{1\}$. If q does not divide $|N|$ then $N \leq H$, so $N = \{1\}$ and $\{K_2, ..., K_k\}$ affords a minimal representation, again contradicting minimality. Hence q divides $|N|$, so, by (a), $N = (H \cap N)C = C$, contradicting that C is not normal in G. This completes the proof of (b).

□

We will also further justify the choice to study the class of elementary abelian groups, by proving a result for semidirect products analogous to Johnson's result on the direct products of relatively prime groups, which is Proposition 1.1.12 in this document.

Let H and K be groups of coprime order and q a prime that does not divide $|H||K|$. Let $C = C_q$ be cyclic of order q. Let $\varphi : C \to \mathrm{Aut}(H \times K)$ be a homomorphism, so that we may form the semidirect product

$$G = (H \times K) \rtimes_\varphi C.$$

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

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

It is routine to check that φ_H and φ_K become well-defined homomorphisms, so that we have the related semidirect products

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

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

$$((h, k), c) \mapsto ((h, c), (k, c))$$

for all $h \in H$, $k \in K$, $c \in C$, so that

$$\mu(G) \leq \mu((H \rtimes C) \times (K \rtimes C)) \leq \mu(H \rtimes C) + \mu(K \rtimes C).$$

Theorem 2.1.2. *With G defined above, we have*

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

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 observations in the preamble and Johnson's result that μ is additive with respect to taking direct products of groups of coprime order.

Suppose then that neither φ_H not φ_K are trivial. We may write $G = HKC$ where HK is an internal direct product of H and K, and G is an internal semidirect product of HK by C. By the last observation in the preamble to the theorem, it suffices to prove that

$$\mu(G) \geq \mu(HC) + \mu(KC).$$

Let $\mathcal{C}$ be a collection of subgroups of G that affords a minimal faithful permutation representation of G. Note that, 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 Theorem 2.1.1(a), subgroups of G that are not subgroups of HK have the form $H_0K_0C^g$ for some $H_0 \leq H$, $K_0 \leq K$ and $g \in G$, such that H_0K_0 is normal in $H_0K_0C^g$. By Lemma 1 of [**7**], we may assume that all elements of $\mathcal{C}$ are meet-irreducible, so therefore have the form

$$H_0K\,, HK_0\,, H_1KC^x\,, HK_1C^y$$

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

$$\mathrm{core}_G(H_0K) = \mathrm{core}_{HC}(H_0)\,K\,, \mathrm{core}_G(HK_0) = H\ \mathrm{core}_{KC}(K_0),$$

and, by Sylow's theorem and the last part of Theorem 2.1.1(a),

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

and

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

Put

$$\begin{aligned} \mathcal{D}_H &= \{H_0 | H_0 \leq H \text{ and } H_0K \in \mathcal{C}\}, \\ \mathcal{E}_H &= \{H_1C | H_1 \leq H \text{ and } H_1KC^x \in \mathcal{C} \text{ for some } x \in G\}, \\ \mathcal{D}_K &= \{K_0 | K_0 \leq K \text{ and } HK_0 \in \mathcal{C}\}, \\ \mathcal{E}_K &= \{K_1C | K_1 \leq K \text{ and } HK_1C^y \in \mathcal{C} \text{ for some } y \in G\}. \end{aligned}$$

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 the theorem, 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

$$\operatorname{core}_{HC}\left(\bigcap_{H_0 \in \mathcal{D}_H} H_0 \cap \bigcap_{H_1C \in \mathcal{E}_H} H_1\right)K \cap H \operatorname{core}_{KC}\left(\bigcap_{K_0 \in \mathcal{D}_K} K_0 \cap \bigcap_{K_1C \in \mathcal{E}_K} K_1\right) \subseteq \operatorname{core}_G\left(\bigcap \mathcal{C}\right) = \{1\}.$$

In particular,

$$\operatorname{core}_{HC}\left(\bigcap_{H_0 \in \mathcal{D}_H} H_0 \cap \bigcap_{H_1C \in \mathcal{E}_H} H_1\right) = \{1\}.$$

If $\mathcal{D}_H \neq \emptyset$ then this immediately implies

$$\operatorname{core}_{HC}\left(\bigcap(\mathcal{D}_H \cup \mathcal{E}_H)\right) = \{1\}.$$

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

$$\operatorname{core}_{HC}\left(\bigcap_{H_1C \in \mathcal{E}_H} H_1\right) = \{1\}.$$

If $\operatorname{core}_{HC}(H_1C)$ contains an element of order q for all $H_1C \in \mathcal{E}_H$ then, in each case, $\operatorname{core}_{HC}(H_1C) = \operatorname{core}_{HC}(H_1)C$, so that

$$C = \mathrm{core}_{HC}\left(\bigcap_{H_1C\in\mathcal{E}_H} H_1\right)C = \bigcap_{H_1C\in\mathcal{E}_H} \mathrm{core}_{HC}(H_1C)$$

is a normal subgroup of HC, contradicting that φ_H is nontrivial. Hence, for at least one $H_1C \in \mathcal{E}_H$, we have $\mathrm{core}_{HC}(H_1C) = \mathrm{core}_{HC}(H_1)$, so that

$$\mathrm{core}_{HC}\left(\bigcap \mathcal{E}_H\right) = \mathrm{core}_{HC}\left(\bigcap_{H_1C\in\mathcal{E}_H} H_1C\right) = \mathrm{core}_{HC}\left(\bigcap_{H_1C\in\mathcal{E}_H} H_1\right) = \{1\}.$$

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 the theorem. □

We can now focus on $V \rtimes \langle T\rangle$.

Theorem 2.1.3. *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 $V \rtimes \langle T_1\rangle \cong V \rtimes \langle T_2\rangle$ 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 $E \rtimes_{T_1} C_q \cong E \rtimes_{T_2} C_q$.*

Proof. Suppose first that T_1 and T_2^k are conjugate for some $k \in \mathbb{Z}$, so that

$$T_1 = P^{-1}T_2^kP$$

for some invertible matrix P. Define the mapping

$$\theta : V \rtimes \langle T_1\rangle \to V \rtimes \langle T_2\rangle$$

by

$$(v, T_1^i)\theta = (Pv, T_2^{ki})$$

for all $v \in V$ and $i \in \mathbb{Z}$. Note that $k \neq 0 \mod q$, and it follows quickly that θ is a bijection. Further, for all $v, w \in V$ and $i, j \in \mathbb{Z}$,

$$\begin{aligned}((v,T_1^i)(w,T_1^j))\theta &= (v+T_1^i w, T_1^{i+j})\theta \\ &= (P(v+T_1^i w), T_2^{(i+j)k}) \\ &= (Pv + (PT_1^iP^{-1})Pw, T_2^{ki+kj}) \\ &= (Pv + T_2^{ki}Pw, T_2^{ki+kj}) \\ &= (Pv, T_2^{ki})(Pw, T_2^{kj}) \\ &= (v,T_1^i)\theta(w,T_1^j)\theta,\end{aligned}$$

which verifies that θ is an isomorphism.

Suppose conversely that $\theta : V \rtimes \langle T_1\rangle \to V \rtimes \langle T_2\rangle$ is an isomorphism. We have

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

for some $w \in V$ and integer k. From the homomorphism property, we have

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

for all $v \in V$. In fact, we will show T_1 and T_2^k are conjugate. For $i = 1,...,n$, denote by e_i the column vector with zero everywhere except for 1 in the i-th place (a standard basis vector). Hence all vectors in V are linear combinations of $e_1,...,e_n$. For $\lambda \in \mathbb{F}_p$, define, for $v \in V$,

$$\begin{aligned}\lambda(v,I) &= (\lambda v, I) \\ &= \left(\sum^{\lambda} v, I\right) \\ &= \prod^{\lambda}(v,I)\end{aligned}$$

where we take $\lambda \in \{0,...,p-1\}$. Since θ is a homomorphism, we have, for all $v \in V$,

$$(\lambda(v,I))\theta = \lambda((v,I)\theta).$$

For each $i = 1,...,n$, we have

$$(e_i,I)\theta = (p_i,I)$$

for some $p_i \in V$. Put

$$P = [p_1 ... p_n],$$

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

$$\begin{aligned}
(v, I)\theta &= \left(\sum_{i=1}^{n} \lambda_i e_i, I \right) \theta \\
&= \left(\prod_{i=1}^{n} \lambda_i (e_i, I) \right) \theta \\
&= \prod_{i=1}^{n} \lambda_i \left((e_i, I)\theta \right) \\
&= \prod_{i=1}^{n} \lambda_i (p_i, I) \\
&= \left(\sum_{i=1}^{n} \lambda_i p_i, I \right) \\
&= \left(\sum_{i=1}^{n} \lambda_i P e_i, I \right) \\
&= \left(P \left(\sum_{i=1}^{n} \lambda_i e_i \right), I \right) \\
&= (Pv, I).
\end{aligned}$$

On the one hand,

$$\begin{aligned}
(v, T_1)\theta &= ((v, I)(0, T_1))\theta \\
&= ((v, I)\theta)((0, T_1)\theta) \\
&= (Pv, I)(w, T_2^k) \\
&= (Pv + w, T_2^k),
\end{aligned}$$

whilst, on the other hand,

$$\begin{aligned}(v, T_1)\theta &= ((0, T_1)(T_1^{-1}v, I))\theta \\ &= (0, T_1)\theta(T_1^{-1}v, I)\theta \\ &= (w, T_2^k)(PT_1^{-1}v, I) \\ &= (w + T_2^k PT_1^{-1}v, T_2^k).\end{aligned}$$

Hence, for all $v \in V$,

$$Pv = T_2^k PT_1^{-1}v,$$

so

$$v = P^{-1}T_2^k PT_1^{-1}v.$$

It follows that $P^{-1}T_2^k PT_1^{-1} = I$, so

$$T_1 = P^{-1}T_2^k P,$$

that is, T_1 and T_2^k are conjugate, completing the proof of the theorem. □

This allows us to focus on a single representative from each conjugacy class of matrices. Fortunately, there exists a usual representative for conjugacy classes of matrices over finite fields - the primary rational canonical form.

Definition 2.1.4. Let $m = \sum_{i=0}^{n} m_i x^i \in \mathbb{F}_p[x]$ be a monic polynomial (so $m_n = 1$). The *companion matrix* P_m of m is

$$P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -m_0 \\ 1 & 0 & \cdots & 0 & -m_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -m_{n-2} \\ 0 & \cdots & 0 & 1 & -m_{n-1} \end{pmatrix}.$$

Theorem 2.1.5 ([**12**], Theorem 10.14)**.** *There exist matrices T and L for each $M \in GL(n, p)$ such that $T = LML^{-1} = \mathrm{diag}(P_{r_1}, ..., P_{r_k})$ is a block matrix of companion matrices of powers of irreducible polynomials, and T is unique up to reordering of the blocks. Furthermore, $\mathrm{lcm}(r_1, ..., r_k)$ is the minimal polynomial of M.*

This motivates the following definition.

Definition 2.1.6. A matrix T is said to be in *primary rational canonical form* if it is a block diagonal matrix of companion matrices of powers of irreducible polynomials.

We shall now begin with a special case, again using Theorem 1.1.21 - semidirect products corresponding to diagonal matrices.

Proposition 2.1.7. *Let $G = V \rtimes \langle T \rangle$ for a vector space $V = \mathbb{F}_p^n$ and invertible linear transformation T of order q, for p and q distinct primes. If T is diagonal, then $\mu(G) = np$.*

Proof. Suppose T is diagonal, so V is the direct sum of T-invariant one-dimensional subspaces. Under the identification of V with E these may be regarded as direct factors $\langle a_1 \rangle, ..., \langle a_n \rangle$, say, of E. For $i = 1, ..., n$, put

$$H_i = \langle a_1, ..., a_{i-1}, a_{i+1}, ..., a_n \rangle.$$

Then $\{H_1, ..., H_n\}$ affords a minimal faithful representation of E by T-invariant subspaces. By Lemma 1.3.16, $\mu(G) = \mu(E) = np$. □

Example 2.1.8. Suppose $G = C_5^3 \rtimes_T C_2$, where

$$T = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and the entries of T come from $\mathbb{F}_5$.Then, regarding the additive action of T on $\mathbb{F}_5$ multiplicatively on C_5^3, and denoting the generators of C_5^3 by g_1, g_2, g_3 and the generator of C_2 by b, one can see that the subgroup collection $\{\langle g_1, g_2, b \rangle, \langle g_1, g_3, b \rangle, \langle g_2, g_3, b \rangle\}$ affords a minimal representation of G. Thus G is isomorphic to the following subgroup of $\mathrm{Sym}(15)$:

$$\langle (1\ 2\ 3\ 4\ 5), (6\ 7\ 8\ 9\ 10), (11\ 12\ 13\ 14\ 15), (1\ 4)(2\ 3)(6\ 9)(7\ 8) \rangle.$$

Observe that $\mu(G) = \mu(E)$, and that E is nilpotent, so $G \in \mathcal{G}$, as defined in Wright's work.

In addition to only examining matrices in rational canonical form, we can use the restriction that T must have order q to further simplify things.

Theorem 2.1.9. *Suppose $T \in GL(n, p)$ is a matrix in primary rational canonical form of order q such that p has order s modulo q and $\mathbb{F}_p$ does not have a primitive q-th root of unity. Then T is composed of companion matrix blocks of irreducible polynomials where each polynomial is either*

$x-1$ or one of the $(q-1)/s$ irreducible polynomials of degree s whose roots constitute the primitive q-th roots of 1 in an extension of $\mathbb{F}_p$.

Proof. As T is an $n \times n$ matrix over $\mathbb{F}_p$ such that $T^q = I$, T gives a representation of the cyclic group C_q over $\mathbb{F}_p$. Then, by Maschke's Theorem, as the order of C_q is not divisible by p, every representation of C_q over $\mathbb{F}_p$ is semisimple. Thus the minimal polynomial of T has no repeated irreducible factors.

As $T^q = I$, we see that the eigenvalues are q-th roots of 1. Suppose α is a non-trivial q-th root of 1 in some finite extension of $\mathbb{F}_p$. Then so are $\alpha^p, \alpha^{p^2}, ..., \alpha^{p^{s-1}}$ noting that s is minimal such that $\alpha^{p^s} = \alpha$. The Frobenius automorphism generates the Galois group of the extension and so the minimal polynomial of α over $\mathbb{F}_p$ is $(x-\alpha)...(x-\alpha^{p^{s-1}})$, and thus has degree s. The result follows. □

Corollary 2.1.10. *If q does not divide $p-1$, $p^2-1, ..., p^n-1$, then $G = C_p^n \rtimes C_q$ is abelian, and hence must be the direct product $G = C_p^n \times C_q$.*

This corollary is also a consequence of the fact that the order of $GL(n,p)$ is $p^{n(n-1)/2}\Pi_{i=1}^{n}(p^i-1)$

Example 2.1.11. Let $p = 11, q = 7$, so that the order of p mod q is $s = 3$. Therefore $(q-1)/s = 2$, so there are 2 irreducible polynomials of degree 3, $P_1(x)$ and $P_2(x)$, which are derived from the 7-th roots of unity. Therefore, by the previous theorem, any invertible linear transformation of $\mathbb{F}_p^n$ of order 7 has a rational canonical form that is composed of companion matrices of some or all of the irreducible polynomials $x-1$, $P_1(x)$ and $P_2(x)$. We now calculate these irreducible polynomials.

Suppose α is a non-trivial 7-th root of 1 in some finite extension of $\mathbb{F}_{11}$. As in the proof of the previous theorem, the minimal polynomial of α is $(x-\alpha)...(x-\alpha^{p^{s-1}})$, so

$$\begin{aligned} P_1(x) &= (x-\alpha)(x-\alpha^{11})(x-\alpha^{11^2}) \\ &= (x-\alpha)(x-\alpha^2)(x-\alpha^4) \\ &= x^3 - (\alpha+\alpha^2+\alpha^4)x^2 + (\alpha^3+\alpha^5+\alpha^6)x - 1 \end{aligned}$$

which is an irreducible degree 3 polynomial and hence $\alpha+\alpha^2+\alpha^4$ and $\alpha^3+\alpha^5+\alpha^6$ must be in $\mathbb{F}_{11}$. A useful trick to find them is by calculating that

$$(x-(\alpha+\alpha^2+\alpha^4))(x-(\alpha^3+\alpha^5+\alpha^6)) = x^2+x+2,$$

and then finding that the roots of x^2+x+2 are 4 and 6 in $\mathbb{F}_{11}$. Thus we find that $\alpha+\alpha^2+\alpha^4=4$ or 6, yielding that $\alpha^3+\alpha^5+\alpha^6=6$ or 4 respectively. These give us that

$$P_1(x)=x^3+7x^2+6x-1 \text{ and } P_2(x)=x^3+5x^2+4x-1$$

are irreducible. Hence we can see that any invertible linear transformation of $\mathbb{F}_{11}$ of order 7 is a block matrix composed of diagonal 1's and the following two companion matrices:

$$A=\begin{pmatrix}0&0&1\\1&0&5\\0&1&4\end{pmatrix},\quad B=\begin{pmatrix}0&0&1\\1&0&7\\0&1&6\end{pmatrix}.$$

The following theorem characterises our semidirect products even further.

Theorem 2.1.12. *Let V_1, V_2 be finite dimensional vector spaces over $\mathbb{F}_p$, and $T_1 : V_1 \to V_1$ and $T_2 : V_2 \to V_2$ be invertible linear transformations of order q such that $T_1 \neq id$ and ϕ_{T_1}, the minimal polynomial of T_1, is irreducible of degree d. Then $V_1 \rtimes \langle T_1\rangle \cong V_2 \rtimes \langle T_2\rangle$ if and only if $\dim(V_1) = \dim(V_2)$ and φ_{T_2} is irreducible of degree d.*

Proof. If $V_1 \rtimes \langle T_1\rangle \cong V_2 \rtimes \langle T_2\rangle$ then clearly $\langle T_1\rangle \cong \langle T_2\rangle$ and $V_1 \cong V_2$ as a module, so, in particular, $\dim(V_1)=\dim(V_2)=dk$ where there are k summands and the action of T_2 is irreducible on each summand, so φ_{T_2} is irreducible of degree d. Suppose conversely that $\dim(V_1)=\dim(V_2)$ and φ_{T_2} is irreducible of degree d. Then, by the proof of Theorem 2.1.15, the eigenvalues of some power of T_2 coincide with the eigenvalues of T_1, so that T_1 and some power of T_2 are conjugate. Hence $V_1 \rtimes \langle T_1\rangle \cong V_2 \rtimes \langle T_2\rangle$ by Theorem 2.1.3. □

Example 2.1.13. Consider the groups

$$\begin{aligned}G_1 = \langle a_1,a_2,a_3,b \mid a_1^{11}=a_2^{11}=a_3^{11}=b^7=1, a_1^{a_2}=a_1^{a_3}=a_1, a_2^{a_3}=\\ a_2, a_1^b=a_2, a_2^b=a_3, a_3^b=a_1a_2^5a_3^4\rangle,\\ G_2 = \langle a_1,a_2,a_3,b \mid a_1^{11}=a_2^{11}=a_3^{11}=b^7=1, a_1^{a_2}=a_1^{a_3}=a_1, a_2^{a_3}=\\ a_2, a_1^b=a_2, a_2^b=a_3, a_3^b=a_1a_2^7a_3^6\rangle\end{aligned}$$

Then $G_1 \cong \mathbb{F}_{11}^3 \rtimes \langle A\rangle$ and $G_2 \cong \mathbb{F}_{11}^3 \rtimes \langle B\rangle$, where A, B are given in Example 2.1.11, so ϕ_A and ϕ_B are irreducible of degree 3. By the theorem $G_1 \cong G_2$.

Now we shall characterise some cases for small primes p and q. In the case that $(q-1)/s = 1$, we see that the unique irreducible polynomial must be

$$(x^q - 1)/(x - 1) = x^{q-1} + x^{q-2} + ... + x + 1.$$

Below is a table of cases for prime p and q for which $(q-1)/s \neq 1$ and $\mathbb{F}_p$ does not have a primitive q-th root of unity, for $p, q \leq 13$, obtained using MAGMA. The cases for which $p, q \leq 13$ and $\mathbb{F}_p$ does have a primitive q-th root of unity are $q = 2$; $p = 7, q = 3$; $p = 11, q = 5$ and $p = 13, q = 3$.

TABLE 1. Irreducible Polynomials of Degree s

p	q	s	$(q-1)/s$	**Irreducible Polynomials**
2	7	3	2	$x^3 + x + 1, x^3 + x^2 + 1$
3	11	5	2	$x^5 + 2x^3 + x^2 + 2x + 2, x^5 + x^4 + 2x^3 + x^2 + 2$
3	13	3	4	$x^3 + 2x + 2, x^3 + x^2 + 2, x^3 + x^2 + x + 2,$ $x^3 + 2x^2 + 2x + 2$
5	11	5	2	$x^5 + 2x^4 + 4x^3 + x^2 + x + 4,$ $x^5 + 4x^4 + 4x^3 + x^2 + 3x + 4$
5	13	4	3	$x^4 + x^3 + 4x^2 + x + 1, x^4 + 2x^3 + x^2 + 2x + 1,$ $x^4 + 3x^3 + 3x + 1$
11	7	3	2	$x^3 + 5x^2 + 4x + 10, x^3 + 7x^2 + 6x + 10$
13	7	2	3	$x^2 + 3x + 1, x^2 + 5x + 1, x^2 + 6x + 1$

By Corollary 2.1.10, the only 'interesting' semidirect products occur when q divides $p^i - 1$ for some positive integer i. In fact, as an aside, we can generalise this.

Proposition 2.1.14. *If $G = H \rtimes K$ where H is a p-group of order p^n and K is a q-group, where p and q are different primes, then G is a direct product if q does not divide $p - 1, p^2 - 1, ..., p^n - 1$.*

Proof. Observe that K is a Sylow q-subgroup of G, and the number of Sylow q-subgroups is congruent to 1 mod q and divides the index of K in G, which is p^n. Hence, by Sylow's theorems, K is unique and therefore normal. □

As the primary rational canonical form is comprised of companion matrix blocks corresponding to irreducible polynomials, it would be useful to find the minimal degree of a semidirect product corresponding to a single companion matrix block. The following theorem implies the minimal degree of such a group as a corollary.

Theorem 2.1.15. *Suppose $G = N \rtimes C_q$ where N is a non-trivial p-group and the action of C_q on N is non-trivial and irreducible (so, in particular, N is elementary abelian). Then*

$$\mu(G) = \begin{cases} |N| & \text{if } q > |N|/p \\ pq & \text{otherwise.} \end{cases}$$

Proof. Let H be a maximal subgroup of N, so H has index p in N and thus index pq in G. We see that the proper subgroups of G are subgroups of N or conjugates of C_q. Then the cores of H and C_q are both trivial, in the former case as the action of C_q is irreducible, and the latter because G is non-abelian and C_q has prime order.

Therefore any minimal representation is transitive. By H's maximality, it has the minimal index of any subgroup of N. Therefore, as we can provide a subgroup of index pq or $|N|$, which representation is minimal only depends on the relative sizes of pq and $|N|$ and the result follows. □

Corollary 2.1.16. *Let $G = E \rtimes_T C_q$. Suppose T is in primary rational canonical form and composed of a single non-trivial companion matrix block of an irreducible polynomial. Then*

$$\mu(G) = \begin{cases} p^n & \text{if } q > p^{n-1} \\ pq & \text{otherwise.} \end{cases}$$

Now we have a class of examples, as promised at the end of Chapter 1, for which $G = G_1 \rtimes C_q$ is not a direct product and $\mu(G) > \mu(G_1)$: any semidirect product of a p-group, N, by C_q with an irreducible, non-trivial action, for which $q < |N|/p$.

Example 2.1.17. A quick computer check on the values of p, q and s, combined with our results in Table 1, yields that the smallest such example by order of the group is $G = C_5^2 \rtimes_T C_3$ with

$$T = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

for which $|G| = 75$ and $\mu(G) = 15 > 10 = \mu(C_5^2)$. The smallest such example by minimal degree is $G = C_2^4 \rtimes_T C_5$, where

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

for which $|G| = 80$ and $\mu(G) = 10 > 8 = \mu(C_2^4)$.

We also note that this provides a proof of the minimal degree of the crucial group $G = A \rtimes C_q$ in Saunders' work in [**17**], where $A \cong C_p^{q-1}$. The group G is shown to be isomorphic to the case from the above corollary where $n = q - 1$ and T is the $(q-1) \times (q-1)$ matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -1 \\ 1 & 0 & \cdots & 0 & -1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -1 \\ 0 & \cdots & 0 & 1 & -1 \end{pmatrix}.$$

In the case that $q < p^{q-2}$ with $p \geq 2, q \geq 5$, by the above corollary such a group has minimal degree pq.

Saunders proves that G provides an example of a group for which there is a group H such that $\mu(G \times H)$ is strictly less than $\mu(G) + \mu(H)$. We shall independently provide a proof for this by the end of the chapter.

2.2. Normal Cores

Let $G = V \rtimes \langle T \rangle$, and suppose T has order q. If W is a subspace of V, then finding the core of W is equivalent to finding the largest T-invariant subspace of W. Thus we can talk about cores of subspaces of V with no ambiguity.

Throughout this section, unless otherwise stated, V is an n-dimensional vector space over $\mathbb{F}_p$ and T is an order q element of $GL(n, p)$, with minimal polynomial ϕ_T.

Additionally, as the context demands, we may identify T^i with the semidirect product element $(0, T^i)$ and v with the element (v, I). We shall also refer to T-invariant subspaces as just invariant subspaces, as we shall henceforth only be discussing subspaces under one potential action.

First we find a lower bound on the size of the core of a given subspace.

Lemma 2.2.1. *Suppose ϕ_T is of degree d. Let S be an $(n-i)$-dimensional subspace of V. Then $\mathrm{core}(S) = S \cap S^T \cap ... \cap S^{T^{d-1}}$ and $\mathrm{core}(S)$ has dimension at least $n - di$.*

Proof. Let

$$W = S \cap S^T \cap ... \cap S^{T^{d-1}}.$$

Then W is invariant because T^d is a linear combination of the lower powers of T. Since each subspace has codimension i as T is invertible, their intersection has codimension at most di. Additionally, this intersection is obviously the largest invariant subspace of S. □

Characterisation of invariant subspaces usually involves the decomposition of these subspaces.

Definition 2.2.2. Suppose that S is a non-trivial invariant subspace of V and S cannot be expressed as the direct sum of two (or more) proper invariant subspaces. Then we say that S is an *indecomposable* subspace.

We now provide a technical lemma for our subsequent calculations.

Lemma 2.2.3 ([**1**], Theorem 4.14)**.** *Let $\phi_T(x) = r_1^{d_1}...r_k^{d_k}(x)$, where the r_i are distinct and monic irreducible polynomials. Let $V_i = \ker(r_i^{d_i}(T))$ and let W be an invariant subspace of V. Then*

$$W = (W \cap V_1) \oplus (W \cap V_2) \oplus ... \oplus (W \cap V_t).$$

Now we are equipped to examine the cores of subspaces much more effectively.

Theorem 2.2.4. *Let $\phi_T(x) = r_1...r_k(x)$, with $r_1, ..., r_k$ distinct irreducible polynomials over $\mathbb{F}_p$. Let V be the direct sum of t indecomposable subspaces, and let S be an $(n-i)$-dimensional subspace of V. Then S contains at least $t - ik$ pairwise non-intersecting indecomposable subspaces.*

Proof. Let

$$V_j = \ker(r_j(T))$$

and suppose V_j contains ℓ_j indecomposable subspaces. We see $\dim(V_j) = \deg(r_j)\ell_j$, so $S \cap V_j$ is a subspace of V_j of dimension at least $(\deg(r_j)\ell_j - i)$. Therefore, by Lemma 2.2.1, we see $\mathrm{core}(S) \cap V_j$ has a dimension of at least

$$\deg(r_j)\ell_j - \deg(r_j)i = \deg(r_j)(\ell_j - i).$$

As an indecomposable subspace of V_j can only be $\deg(r_j)$-dimensional, this means $\mathrm{core}(S) \cap V_j$ contains at least $\ell_j - i$ distinct indecomposable subspaces, and as $V = V_1 \oplus ... \oplus V_k$ and the sum of the ℓ_j's must be t, the result follows. □

2.3. Minimal Subgroup Collections

We now aim to use the theory we have developed in the preceding section to find a minimal representation for a given group $G = V \rtimes \langle T \rangle$. Fortunately, we can immediately remove a substantial class of subgroups of G from the list of subgroups that can be used to create a minimal representation.

Theorem 2.3.1. *Suppose $G = V \rtimes \langle T \rangle$, where V is the direct sum of t indecomposable subspaces. Then there exists a minimal faithful representation of G afforded by a collection of subgroups such that for any subgroup H in the collection with an order divisible by q, $H \cap V$ is an invariant subspace that is the direct sum of $t - 1$ indecomposable subspaces.*

Proof. Let $\mathcal{C}$ be a collection of subgroups affording a minimal faithful representation of G. By Lemma 1 in Johnson [**7**], we may suppose that all elements of $\mathcal{C}$ are meet-irreducible. Let $K \in \mathcal{C}$ such that q divides $|K|$. By part (a) of Theorem 2.1.1, noting V is elementary abelian so all of its subgroups are normal, $K = W\langle T^g \rangle$ where $W = K \cap V$ is an invariant subspace of V.

Certainly $W \neq V$ (for otherwise $K = G \in \mathcal{C}$, contradicting minimality), so, by Maschke's Theorem, $V = W \oplus W'$ for some non-trivial invariant subspace W' of V. If W' is not indecomposable then $W' = W'_1 \oplus W'_2$ for some non-zero invariant subspaces W'_1, 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 $K_i = (W \oplus W'_i)\langle T^g \rangle$ for $i = 1, 2$, contradicting that K is meet-irreducible. Hence W' is indecomposable, so W is the sum of $t - 1$ indecomposable subspaces and the theorem is proved. □

Subgroups in any collection affording a minimal faithful representation with indexes divisible by q require a slightly more delicate handling. These subgroups are subspaces of V, and in light of Theorem 2.1.1, we focus only on subspaces which are non-invariant.

Definition 2.3.2. Let W be a subspace of V. Then a collection $\mathcal{C}$ of subspaces of V is called *W-exchangeable* if W is contained in each subspace in $\mathcal{C}$, $\mathrm{core}(\cap\mathcal{C}) \subseteq \mathrm{core}(W)$ and the index sum of $\mathcal{C}$ is at most the index of W. If $\mathcal{C} = \{W'\}$ is W-exchangeable, where W' is a subspace of V then we say that W' is W-exchangeable.

Note in particular the following transitivity property: if W' is a W-exchangeable subgroup and further W'' is W'-exchangeable, then $W'' \subseteq W' \subseteq W$, so certainly

$$\mathrm{core}(W'') \subseteq \mathrm{core}(W') \subseteq \mathrm{core}(W)$$

and

$$[V : W''] \leq [V : W'] \leq [V : W],$$

so that W'' is also W-exchangeable.

In fact, we can prove a more general property of W-exchangeability.

Lemma 2.3.3. *Let $W' \in \mathcal{C}$ where $\mathcal{C}$ is W-exchangeable. Suppose that $\mathcal{C}'$ is W'-exchangeable. Then $\mathcal{C}' \cup \mathcal{C}\backslash\{W'\}$ is W-exchangeable.*

Proof. Observe that W is contained in every subspace of $\mathcal{C}' \cup \mathcal{C}\backslash\{W'\}$,

$$\begin{aligned}
\mathrm{core}\left(\cap(\mathcal{C}' \cup \mathcal{C}\backslash\{W'\})\right) &= \mathrm{core}(\cap\mathcal{C}') \cap \mathrm{core}(\cap(\mathcal{C}\backslash\{W'\}) \\
&\subseteq \mathrm{core}(W') \cap \mathrm{core}(\cap(\mathcal{C}\backslash\{W'\})) \\
&= \mathrm{core}(\cap\mathcal{C}) \\
&\subseteq \mathrm{core}(W),
\end{aligned}$$

and the index sum of $\mathcal{C}' \cup \mathcal{C}\backslash\{W'\}$ is bounded by the index sum of $\mathcal{C}\backslash\{W'\}$ plus the index of W' (since $\mathcal{C}'$ is W'-exchangeable), which is just the index sum of $\mathcal{C}$, which is bounded above by the index of W. □

Another useful property of W-exchangeability follows.

Lemma 2.3.4. *Suppose $W = W_1 \cap W_2$, where W is a proper subspace of both W_1 and W_2 (so W is meet reducible). Then $\{W_1, W_2\}$ is W-exchangeable.*

Proof. Immediately $\mathrm{core}(W) = \mathrm{core}(W_1 \cap W_2)$ and

$$\begin{aligned}[V : W] &= [V : W_1 \cap W_2] = [V : W_1][W_1 : W_1 \cap W_2] \\ &= [V : W_1][W_1 + W_2 : W_2] \\ &\leq [V : W_1] + [W_1 + W_2 : W_2] \\ &\leq [V : W_1] + [V : W_2]\end{aligned}$$

which verifies that $\{W_1, W_2\}$ is W-exchangeable. □

Lemma 2.3.5. *Any subspace W of V of codimension greater than or equal to 2 is meet reducible.*

Proof. If W has codimension greater than or equal to 2, then $W \oplus \langle v_1 \rangle \oplus \langle v_2 \rangle$ is a subspace of V for some $v_1, v_2 \in V$, so that $W = W_1 \cap W_2$ where we put $W_i = W + \langle v_i \rangle$, noting W is a proper subspace of W_i for $i = 1, 2$. □

Proposition 2.3.6. *Let $G = V \rtimes \langle T \rangle$ and $W \leq V$. Then there exists a W-exchangeable collection $\mathcal{W}$ of subspaces of V of codimension 1.*

Proof. If W has codimension 1 then $\mathcal{W} = \{W\}$ is W-exchangeable trivially, which starts an induction.

Suppose W has codimension ≥ 2, so W is meet reducible, say $W = W_1 \cap W_2$, where W is a proper subspace of W_1 and W_2. Then $\{W_1, W_2\}$ is W-exchangeable. By an inductive hypothesis (since W_1, W_2 have codimension less than the codimension of W) there exists a W_i-exchangeable collection $\mathcal{W}_i$ of subspaces of V of codimension 1, for $i = 1, 2$. Put $\mathcal{W} = \mathcal{W}_1 \cup \mathcal{W}_2$. By Lemma 2.3.3, $\mathcal{W}$ is W-exchangeable, and the proposition follows by induction. □

Theorem 2.3.7. *Let $G = V \rtimes \langle T \rangle$. Suppose $\phi_T = r_1 ... r_k$, with r_i all distinct and irreducible. Suppose $V_i = V \cap \ker(r_i(T))$ is the direct sum of t_i indecomposables for each i. Then there exists a minimal representation of G afforded by a subgroup collection $\mathcal{W}$ such that every subgroup W in $\mathcal{W}$ of index divisible by q is a $(n-1)$-dimensional subspace so that $\mathrm{core}(W) = \mathrm{core}(W_1) \oplus ... \oplus \mathrm{core}(W_k)$ where $W_i = W \cap V_i$ and $\mathrm{core}(W_i)$ is the direct sum of at least $(t_i - 1)$ indecomposables for each i.*

Proof. Let $\mathcal{C}$ be any subgroup collection that affords a minimal faithful representation of G. By applying the previous proposition to any member of $\mathcal{C}$ that is a subgroup of G whose order is not divisible by q, we may suppose any such subgroup is a subspace W of V of codimension 1. But then

$$\begin{aligned}\dim(W \cap V_i) &= \dim W + \dim V_i - \dim(W + V_i) \\ &\geq n - 1 + \dim V_i - n \\ &= \dim V_i - 1,\end{aligned}$$

so that $W_i := W \cap V_i$ has codimension at most 1 in V_i. By the proof of Theorem 2.2.4, $\mathrm{core}(W_i)$ contains at least $t_i - 1$ indecomposables. $\square$

Before moving on to the final result, we shall establish a canonical way to construct an $(n-1)$-dimensional subspace with the above properties.

Lemma 2.3.8. *Let $V = V_1 \oplus ... \oplus V_m$ where $\phi_T = r_1...r_m$ for distinct irreducible $r_1, ..., r_m$, such that $V_i = \ker(r_i(T))$ is indecomposable for $i = 1, ..., m$. Let B_i be a basis for V_i for $i = 1, ..., m$ and put $B = B_1 \cup ... \cup B_m$, which is a basis for V. Let*

$$\overline{V} = \{v = \sum_{b \in B} \lambda_b b \in V \mid \sum_{b \in B} \lambda_b = 0\}.$$

Then $\overline{V}$ has codimension 1 and $\mathrm{core}(\overline{V}) = \{0\}$. Conversely, if W is a codimension 1 subspace of V such that $\mathrm{core}(W) = \{0\}$ then we can choose a basis B_i for V_i for $i = 1, ..., m$ such that $W = \overline{V}$.

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

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

$$B_i = \{b + v_i \mid b \in B_i'\} \cup \{v_i\}.$$

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

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

where $C = B_2 \cup ... \cup B_m$. Observe that $(W \cap V_1) \oplus (W \cap \widehat{V})$ has codimension 1 in W, so we may choose some $w \in W \backslash ((W \cap V_1) \oplus (W \cap \widehat{V}))$. But $w = v + \widehat{v}$ for some unique $w \in V_1$ and $\widehat{v} \in \widehat{V}$. If one of v or $\widehat{v}$ is in W then both are, contradicting the choice of w. Hence $v, \widehat{v} \notin W$. But $\widehat{v} = \sum_{c \in C} \lambda_c c$ for some scalars λ_c. Put $\lambda = \sum_{c \in C} \lambda_c$. By the inductive hypothesis, $\lambda \neq 0$. Now put

$$B_1 = \{b - \tfrac{1}{\lambda} v \mid bb \in B_1'\} \cup \{-\tfrac{1}{\lambda} v\},$$

so that B_1 is a basis for V_1. Finally, put $B = B_1 \cup ... \cup B_m$ and form $\widehat{V}$ with respect to B. But,

$$w = v + \widehat{v} = -\lambda\big(-\frac{1}{\lambda} v\big) + \sum_{c \in C} \lambda_c c$$

and $-\lambda + \sum_{c \in C} \lambda_c = -\lambda + \lambda = 0$, so that $w \in \overline{V}$, by definition. Noting that

$$W = \langle w \rangle \oplus (W \cap V_1) \oplus (W \cap \widehat{V}),$$

it is straightforward, using the inductive hypothesis, to verify that $W \subseteq \overline{V}$. Because $\dim(W) = n - 1 = \dim(\overline{V})$, we have $W = \overline{V}$, establishing the inductive step, and completing the proof of the lemma.

□

2.4. Final Results

We have now accumulated enough knowledge to prove a full theorem for the semidirect product of elementary abelian groups with prime cyclic groups. Recall that by Theorem 2.1.9 the minimal polynomial of an action T on E has a square-free polynomial.

Theorem 2.4.1. *Let $G = V \rtimes \langle T \rangle$ and suppose that*

$$\phi_T(x) = r_1 ... r_m(x) \neq x - 1$$

is a product of distinct irreducible polynomials $r_1, .., r_m$ of degree s, where s is the order of p modulo q. Suppose, for $i = 1$ to m, that $\ker(r_i(T))$ is the direct sum of k_i indecomposable subspaces, and reorder $r_1, ..., r_m$ (if necessary) so that $k_1 \geq ... \geq k_m$. Let a be the smallest integer such that $q < ap^{s-1}$ and put $k_j = 0$ for $j \geq m + 1$. Then

$$\mu(G) = k_a pq + \sum_{i=1}^{a-1}(k_i - k_a)p^s.$$

Proof. Suppose first that $s = 1$, so that $\mathbb{F}_p$ has q-th roots of unity. Then $a = q + 1$, $m \leq q$, $k_a = 0$ and all indecomposables are 1-dimensional. Hence T is diagonal, and $T \neq I$ since $\varphi_T(x) \neq x - 1$. By Lemma 2.1.7,

$$\mu(G) = \mu(V) = np,$$

which verifies the formula in the statement of the theorem, since $k_a = 0$ and

$$\sum_{i=1}^{a-1}(k_i - k_a)p^s = (k_1 + ... + k_{n-1})p = (k_1 + ... + k_m)p = np.$$

Suppose now that $s \geq 2$. We first prove that the above formula is an upper bound for $\mu(G)$. We have

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

where V_{ij} is indecomposable with $T|_{V_{ij}}$ having minimal polynomial r_i, for each $(i, j) \in I$, where

$$I = \{(i, j)|1 \leq i \leq m, 1 \leq j \leq k_i\}.$$

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 $V = W \oplus W'$. For $j = 1$ to k_a, we have $k_{\ell_j} \geq j \geq k_{\ell_j+1}$ for some largest $\ell_j \in \{a, ..., m\}$, and we put

$$W_j = \bigoplus_{i=1}^{\ell_j} V_{ij},$$

so that $T|_{W_j}$ has minimum polynomial $r_1...r_{\ell_j}$. In particular, $\ell_1 = m$, since $k_m \geq 1 > 0 = k_{m+1}$, and $T|_{W_1}$ has minimum polynomial $r_1...r_m$.

Thus

$$V = V_X \oplus (\bigoplus_{j=1}^{k_a} W_j)$$

where

$$X = \{(i,j) | i < a, k_a < j \leq k_i\}.$$

If W is a direct sum of N indecomposable subspaces such that $T|_W$ has minimal polynomial $r_1...r_N$ then let $\overline{W}$ denote a canonical codimension 1 subspace of W as described in Lemma 2.3.8, so $\mathrm{core}(\overline{W}) = \{0\}$.

For $j = 1$ to k_a, put

$$H_j = \overline{W_j} \oplus W_j',$$

so $\mathrm{core}(H_j) = W_j'$ and $|G : H_j| = pq$. For $(i,j) \in X$, put

$$K_{ij} = V_{ij}' \langle T \rangle,$$

so $\mathrm{core}(K_{ij}) = V_{ij}'$ and $|G : K_{ij}| = p^s$.

Let $\mathcal{C} = \{H_1, ..., H_{k_a}\} \cup \{K_{ij} \mid (i,j) \in X\}$. Then

$$\mathrm{core}(\bigcap \mathcal{C}) = (\bigcap_{j=1}^{k_a} W_j') \cap (\bigcap_{(i,j) \in X} V_{ij}') = V_X \cap V_X' = \{0\},$$

so $\mathcal{C}$ affords a faithful representation of G of degree

$$\sum_{j=1}^{k_a} |G : H_j| + \sum_{(i,j) \in X} |G : K_{ij}| = k_a pq + \sum_{i=1}^{a-1} (k_i - k_a) p^s.$$

This proves that

$$\mu(G) \leq k_a pq + \sum_{i=1}^{a-1} (k_i - k_a) p^s.$$

We now prove that the formula is a lower bound for $\mu(G)$.

By Theorem 2.3.1 and the proof of 2.3.7 there exists a collection $\mathcal{C}$ affording a minimal faithful representation of G such that $\mathcal{C} = \mathcal{D} \cup \mathcal{E}$,

where $\mathcal{D} = \{D_1, ..., D_\ell\}$ and $\mathcal{E} = \{E_1\langle T\rangle, ..., E_t\langle T\rangle\}$ for some codimension 1 subspaces $D_1, ..., D_\ell$ of V, and invariant subspaces $E_1, ..., E_t$ of V, each of which complements an indecomposable subspace. We interpret $\ell = 0, t = 0$ to mean $\mathcal{D} = \varnothing$, $\mathcal{E} = \varnothing$ respectively.

Throughout if X is an invariant subspace of V then X' denotes some invariant subspace such that $V = X \oplus X'$, and we call X' a complement of X, guaranteed to exist by Maschke's Theorem. Further, $\overline{X}$ denotes a canonical codimension 1 subspace of X in the case that X is a sum of indecomposables with distinct minimum polynomials, which can be used to represent any codimension 1 subspsace by Lemma 2.3.8. Theorem 2.3.7 tells us that, for $i = 1, ..., \ell$, $(\mathrm{core}(D_i))'$ is a sum of indecomposables with distinct minimum polynomials and

$$D_i = (\mathrm{core}(D_i)) \oplus (\overline{\mathrm{core}(D_i)'}).$$

The degree of the representation afforded by $\mathcal{C}$ is $\ell pq + tp^s$ (because $|G : D_i| = pq$ and $|G : E_j\langle T\rangle| = p^s$ for each i, j), so to complete the proof of the theorem it suffices to show

$$\ell pq + tp^s \geq k_a pq + \sum_{i=1}^{a-1}(k_i - k_a)p^s.$$

As a stepping stone we will first prove $\ell \geq k_a$. We use the following claim, which we will prove later.

Claim: $V = S_1 \oplus ... \oplus S_\ell \oplus T_1 \oplus ... \oplus T_t$ for some invariant subspaces $S_1, ..., S_\ell, T_1, ..., T_t$ of V such that, after possible rewriting of $\mathcal{D}$ and $\mathcal{E}$, $D_i = \overline{S_i} \oplus S_i'$, $E_j = T_j'$ where S_i is a sum of indecomposables with distinct minimal polynomials, for $i = 1, ..., \ell$, and T_j is indecomposable for $j = 1, ..., t$.

Suppose by way of contradiction that $\ell < k_a$. Hence, using the decomposition of V in the claim, at most $k_a - 1$ indecomposables with minimum polynomial r_i appear in $S_1 \oplus ... \oplus S_\ell$ for $i = 1, ..., a$. But at least k_a copies of indecomposables with minimum polynomial r_i appear in the decomposition of V for each i. Hence $t \geq a$ and, without loss of generality, $T_1, ..., T_a$ are indecomposables with minimum polynomials $r_1, ..., r_a$ respectively. Put

$$S = \overline{T_1 \oplus ... \oplus T_a} \oplus (T_1 \oplus ... \oplus T_a)'$$

where $(T_1 \oplus ... \oplus T_a)' = T_1' \cap ... \cap T_a' = E_1 \cap ... \cap E_a$, which is indeed a complement for $T_1 \oplus ... \oplus T_a$. But $\mathrm{core}(S) = E_1 \cap ... \cap E_a$, so the collection

$$\mathcal{C}' = \mathcal{D} \cup \{S\} \cup (\mathcal{E} \backslash \{E_1\langle T\rangle, ..., E_a\langle T\rangle\})$$

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

$$|G : S| = pq < ap^s = |G : E_1\langle T\rangle| + ... + |G : E_a\langle T\rangle|.$$

This contradicts that $\mathcal{C}$ is minimal. Hence $\ell \geq k_a$.

For $i = 1$ to $a - 1$, there are at most ℓ occurrences of indecomposables with minimum polynomial r_i appearing in $S_1 \oplus ... \oplus S_\ell$, so at least $k_i - \ell$ such indecomposables must occur amongst $T_1, ..., T_t$. Hence $t \geq (k_1 - \ell) + ... + (k_{a-1} - \ell)$.

Thus

$$\begin{aligned}
\ell pq + tp^s &= k_a pq + (\ell - k_a)pq + tp^s \\
&\geq k_a pq + (\ell - k_a)pq + p^s \sum_{i=1}^{a-1} (k_i - \ell) \\
&\geq k_a pq + (\ell - k_a)(a-1)p^s + p^s \sum_{i=1}^{a-1} (k_i - \ell) \\
&= k_a pq + p^s \sum_{i=1}^{a-1} (k_i - k_a)
\end{aligned}$$

and the equality given before the claim is proven.

To prove the theorem it therefore suffices to prove the claim. As a first step we prove

$$V = T_1 \oplus ... \oplus T_t \oplus (E_1 \cap ... \cap E_t)$$

for some indecomposables T_i such that $E_i = T_i'$ for $i = 1, ..., t$. 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 $k \leq t$,

$$V = T_1 \oplus ... \oplus T_{k-1} \oplus (E_1 \cap ... \cap E_{k-1}),$$

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

$$\frac{E_1 \cap ... \cap E_{k-1}}{E_1 \cap ... \cap E_k} \cong \frac{(E_1 \cap ... \cap E_{k-1}) + E_k}{E_k} = \frac{V}{E_k},$$

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

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

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

$$\begin{aligned} V &= (T_1 \oplus ... \oplus T_{k-1}) \oplus (E_1 \cap ... \cap E_{k-1}) \\ &= (T_1 \oplus ... \oplus T_{k-1}) \oplus ((E_1 \cap ... \cap E_k) \oplus T_k) \\ &= T_1 \oplus ... \oplus T_k \oplus (E_1 \cap ... \cap E_k), \end{aligned}$$

which completes the inductive step. This proves the first step given above when $k = t$.

Observe that the first step starts a new induction, and also proves the claim when $\ell = 0$ (for then $\mathcal{C} = \mathcal{E}$ and $E_1 \cap ... \cap E_t = \{0\}$ so that $V = T_1 \oplus ... \oplus T_t$). Suppose $\ell > 0$ and, as inductive hypothesis, that, for $1 \leq k \leq \ell$, we can rewrite $\mathcal{D}$ if necessary so that

$$V = S_1 \oplus ... \oplus S_{k-1} \oplus T_1 \oplus ... \oplus T_t \oplus (S_1' \cap ... \cap S_{k-1}' \cap E)$$

where $E = E_1 \cap ... \cap E_t$ and, for $i = 1$ to $k-1$, $D_i = \overline{S_i} \oplus S_i'$ where S_i is a sum of indecomposables with distinct minimum polynomials.

By minimality of $\mathcal{C}$,

$$\operatorname{core}(D_1 \cap ... \cap D_{k-1} \cap E) \neq \operatorname{core}(D_1 \cap ... \cap D_k \cap E),$$

that is,

$$S_1' \cap ... \cap S_{k-1}' \cap E \neq S_1' \cap ... \cap S_{k-1}' \cap (\operatorname{core} D_k) \cap E.$$

But

$$\begin{aligned}\frac{S'_1 \cap \ldots \cap S'_{k-1} \cap E}{S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} D_k)} &\cong \frac{(S'_1 \cap \ldots \cap S'_{k-1} \cap E) + (\operatorname{core} D_k)}{\operatorname{core} D_k} \\ &\leq \frac{V}{\operatorname{core} D_k} \\ &\cong (\operatorname{core} D_k)',\end{aligned}$$

which is a sum of indecomposables with distinct minimum polynomials. Hence

$$(S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} D_k)) \oplus S_k = S'_1 \cap \ldots \cap S'_{k-1} \cap E$$

for some invariant subspace S_k contained in E, which is a sum of indecomposables with distinct minimum polynomials. Choose any complement $(S'_1 \cap \ldots \cap S'_{k-1} \cap E)'$ of $S'_1 \cap \ldots \cap S'_{k-1} \cap E$ and let

$$S'_k = (S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} D_k)) \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E)'.$$

Put

$$\widetilde{D_k} = \overline{S_k} \oplus S'_k.$$

Observe that $\operatorname{core} \widetilde{D_k} = S'_k$ and

$$\begin{aligned}S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} \widetilde{D_k}) &= S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap S'_k \\ &= (S'_1 \cap \ldots \cap S'_{k-1} \cap E) \cap [(S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} D_k)) \\ &\quad \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E)'] \\ &= S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} D_k),\end{aligned}$$

so we may replace D_k by $\widetilde{D_k}$ in $\mathcal{C}$ without disturbing faithfulness or degree of the representation afforded by $\mathcal{C}$. Renaming $\widetilde{D_k}$ by D_k, we get

$$\begin{aligned}V &= S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap E) \\ &= S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus \big((S'_1 \cap \ldots \cap S'_{k-1} \cap E \cap (\operatorname{core} D_k)) \oplus S_k\big) \\ &= S_1 \oplus \ldots \oplus S_{k-1} \oplus T_1 \oplus \ldots \oplus T_t \oplus \big(S_k \oplus (S'_1 \cap \ldots \cap S'_{k-1} \cap S'_k \cap E)\big) \\ &= S_1 \oplus \ldots \oplus S_k \oplus T_1 \oplus \ldots \oplus T_t \oplus (S'_1 \cap \ldots \cap S'_k \cap E).\end{aligned}$$

This completes the inductive step. Taking $k = \ell$ gives

$$\begin{aligned} V &= S_1 \oplus ... \oplus S_\ell \oplus T_1 \oplus ... \oplus T_t \oplus (S_1' \cap ... \cap S_\ell' \cap E) \\ &= S_1 \oplus ... \oplus S_\ell \oplus T_1 \oplus ... \oplus T_t, \end{aligned}$$

since $S_1' \cap ... \cap S_\ell' \cap E = \{0\}$ (by faithfulness), completing the proof of the claim. □

We are now equipped to prove our final theorem.

Theorem 2.4.2. *Let $G = V \rtimes \langle T \rangle$, where*

$$\phi_T(x) = (x-1)r_1...r_m(x)$$

with $r_1, ..., r_m$ distinct irreducible polynomials of degree $s \geq 2$, where s is the order of p modulo q. Suppose that $\ker(T-I)$ and $\ker(r_i(T))$ are direct sums of k and k_i indecomposable subspaces respectively for each i, and reorder $r_1, ..., r_m$ (if necessary) so that $k_1 \geq ... \geq k_m$. Let a be the smallest integer such that $q < ap^{s-1}$ and put $k_j = 0$ for $j \geq m+1$. Then

$$\mu(G) = \begin{cases} k_a pq + \sum_{i=1}^{a-1}(k_i - k_a)p^s & \text{if } k_a \geq k \\ (k-k_a)p + k_a pq + \sum_{i=1}^{a-1}(k_i - k_a)p^s & \text{if } k_a < k. \end{cases}$$

Proof. Here we have $G = V\langle T \rangle$ where $V = \widetilde{V} \oplus Z$, where $\widetilde{V} = \oplus_{(i,j)\in I} V_{ij}$ and $Z = \oplus_{\alpha=1}^{k} Z_\alpha$, where the V_{ij} are indecomposables with minimum polynomials from amongst $r_1, ..., r_m$ and the Z_α are one-dimensional indecomposables on which the action of T is trivial (so $Z_\alpha\langle T \rangle \cong C_p \times C_q$). By the previous theorem

$$\mu(\widetilde{V}\langle T \rangle) = k_a pq + p^s \textstyle\sum_{i=1}^{a-1}(k_i - k_a).$$

Certainly we have $\mu(G) \geq \mu(\widetilde{V}\langle T \rangle)$. There are two cases, according to whether $k_a \geq k$ or $k_a < k$.

Case 1: $k_a \geq k$**.**

Let $\mathcal{C}$ be the collection of subgroups described in Theorem 2.4.1 that affords a faithful representation of $\widetilde{V}\langle T \rangle$ of degree $\mu(\widetilde{V}\langle T \rangle)$, replacing V by $\widetilde{V}$ throughout. For $\alpha = 1, ..., k$, let $U_\alpha = W_\alpha \oplus Z_\alpha$ and

$$\widehat{H}_\alpha = \overline{U}_\alpha \oplus W_\alpha' \oplus (\bigoplus_{\beta \neq \alpha} Z_\beta).$$

Put

$$\widehat{\mathcal{C}} = \{\widehat{H_1}, ..., \widehat{H_k}, H_{k+1} \oplus Z, ..., H_{k_a} \oplus Z\} \cup \{K_{ij} \oplus Z \mid (i,j) \in X\}.$$

As before, $\mathrm{core}(\cap\widehat{\mathcal{C}}) = \{0\}$, so $\widehat{\mathcal{C}}$ affords a faithful representation of G. Its degree is the same as the degree of the representation of $\widetilde{V}\langle T\rangle$ afforded by $\mathcal{C}$, which is $\mu(\widetilde{V}\langle T\rangle)$, so

$$\mu(G) \leq \mu(\widetilde{V}\langle T\rangle) \leq \mu(G),$$

whence we have equality and we are done.

Case 2: $k > k_a$**.**

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

$$\widehat{\mathcal{C}} = \{\widehat{H_1}, ..., \widehat{H_{k_a}}\} \cup \{K_{ij} \oplus Z \mid (i,j) \in X\}$$
$$\cup\{\left(\widetilde{V} \oplus (\oplus_{\beta\neq\alpha} Z_\beta)\right)\langle T\rangle \mid \alpha = k_a + 1, ..., k\}.$$

The degree of the representation of G afforded by $\widehat{\mathcal{C}}$ is

$$k_a pq + (k - k_a)p + p^s \sum_{i=1}^{a-1} (k_i - k_a),$$

which therefore serves as a lower bound for $\mu(G)$. Now let $\mathcal{C} = \mathcal{D} \cup \mathcal{E}$ be any collections of subgroups affording a minimal representation of G, where, by Theorems 2.3.1 and 2.3.7, we may assume $\mathcal{D} = \{D_1, ..., D_\ell\}$ and $\mathcal{E} = \{E_1\langle T\rangle, ..., E_k\langle T\rangle\}$, where $D_1, ..., D_k$ are codimension 1 subspaces of V and, after reordering (if necessary), $E_1, ..., E_{t_0}$ are complements of indecomposables with minimum polynomials from amongst $r_1, ..., r_m$ and $E_{t_0+1}, ..., E_t$ are complements of one-dimensional indecomposables. As before, $\ell \geq k_a$ and, by the same reasoning as before, $t_0 \geq \sum_{i=1}^{a-1}(k_i - \ell)$ and $t - t_0 \geq k - \ell$.

By minimality of a we have

$$(a-1)p^{s-1} \leq q.$$

If $(a-1)p^{s-1} = q$ then p divides q (since $s \geq 2$), which is impossible. Hence $(a-1)p^{s-1} < q$, so $(a-1)p^{s-1} \leq q - 1$, so

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

Hence

$$\begin{aligned}
\mu(G) &= \ell pq + t_0 p^s + (t - t_0)p \\
&= k_a pq + (\ell - k_a)pq + t_0 p^s + (t - t_0)p \\
&\geq k_a pq + (\ell - k_a)[(a-1)p^s + p] + p^s \sum_{i=1}^{a-1} (k_i - \ell) + (k - \ell)p \\
&= k_a pq + (k - k_a)p + p^s \sum_{i=1}^{a-1} (k_i - k_a),
\end{aligned}$$

so that we get equality, and the theorem is proven.

□

Remark 2.4.3. Since submission of this thesis it was noticed that the parameter a in Theorems 2.4.1 and 2.4.2 can only take the values 1 and 2. For details, the reader is referred to [**3**].

By Theorem 2.1.9, all semidirect products $E \rtimes C_q$ satisfy the hypotheses of Theorems 2.4.1 and 2.4.2, so we have found all of their minimal degrees.

As an illustration of the usefulness of the above work, we discuss a problem posed by Saunders in [**15**], following on from [**17**], where he provides an infinite class of examples of groups for which the direct product is strictly sub-additive, generalising an example given by the referee at the end of Wright's paper [**19**]. (Relevant subgroups of the examples of Saunders and Wright are reproduced below, up to isomorphism, within the discussion of Examples 2.4.4 and 2.4.5, using the constructions of this chapter). However, all of these examples are pairs of groups G and H such that $\max\{\mu(G), \mu(H)\} = \mu(G \times H)$. They also have the property that G does not have a proper direct product decomposition and H is cyclic of prime order. Saunders asks whether there exist groups G and H, such that

$$\max\{\mu(G), \mu(H)\} < \mu(G \times H) < \mu(G) + \mu(H).$$

There are in fact natural methods to generate many groups with this property. Suppose that K and L are given nontrivial groups such that

$$\mu(K \times L) = \mu(K) < \mu(K) + \mu(L),$$

such as any of the examples in [**15**], [**17**] or [**19**].

Suppose that M is any nontrivial group such that

$$\mu(L \times M) = \mu(L) + \mu(M)$$

and

$$\mu(K \times L \times M) = \mu(K \times L) + \mu(M) = \mu(K) + \mu(M).$$

Choices for M are plentiful. For example, we can choose M to be any nontrivial group with order coprime to the orders of K and L, and then these equations hold by a result of Johnson [**7**] (Proposition 1.1.12 in this thesis). Then

$$\mu(K) < \mu(K) + \mu(M) < \mu(K) + \mu(L) + \mu(M) = \mu(K) + \mu(L \times M),$$

and so

$$\max\{\mu(K), \mu(L \times M)\} < \mu\left(K \times (L \times M)\right) < \mu(K) + \mu(L \times M),$$

provided we choose M such that $\mu(L \times M) \leq \mu(K)$, thus solving the problem posed by Saunders.

An alternative method for choosing K, L and M is by exploiting the overlap of the formulae in Theorems 2.4.1 and 2.4.2. Let p and q be distinct primes such that the order of p modulo q is s, and assume $s \geq 2$. Assume also that $q < p^{s-1}$, so that $a \geq 1$ in the hypotheses of Theorems 2.4.1 and 2.4.2. Let T be an invertible $n \times n$ matrix over $\mathbb{F}_p$ of order q having an irreducible minimal polynomial of degree s, so that $n = ks$ for some fixed $k \geq 1$. Let V be the direct sum of k (isomorphic) indecomposable modules with respect to the action induced by T (so V has dimension n), and put

$$K = V \rtimes \langle T \rangle \cong C_p^n \rtimes C_q.$$

By Theorem 2.4.1,

$$\mu(K) = kpq.$$

Let V_ℓ be the direct sum of ℓ one-dimensional spaces and I_ℓ the $\ell \times \ell$ identity matrix, where ℓ is a positive integer. Put

$$\overline{V} = V \oplus V_\ell, \qquad \overline{T} = T \oplus I_\ell$$

and

$$G_\ell = \overline{V} \rtimes \langle \overline{T} \rangle \cong C_p^{n+\ell} \rtimes C_q,$$

where the action induced by I_ℓ is trivial. By Theorem 2.4.2,

$$\mu(G_\ell) = \begin{cases} kpq \text{ if } \ell \leq k \\ kpq + (\ell - k)p \text{ if } \ell > k. \end{cases}$$

Now put $L = V_k \cong C_p^k$ and $M = V_\ell \cong C_p^\ell$ for any $\ell \geq 1$. Then

$$\mu(L \times M) = (k + \ell)p = \mu(L) + \mu(M).$$

Observe also that

$$K \times L \cong G_k \quad \text{and} \quad K \times L \times M \cong G_{k+\ell},$$

so that $\mu(K \times L) = kpq = \mu(K)$ and

$$\mu(K \times L \times M) = kpq + \ell p = \mu(K \times L) + \mu(M) = \mu(K) + \mu(M).$$

Hence the earlier equations relating the minimal degrees of K, L and M are satisfied. Thus, if we choose ℓ such that $k + \ell \leq kq$ then $\mu(L \times M) = (k+\ell)p \leq kpq = \mu(K)$ and we have another large class of examples where

$$\max\{\mu(K), \mu(L \times M)\} < \mu\left(K \times (L \times M)\right) < \mu(K) + \mu(L \times M).$$

A novel feature of this class is that we can make the group L as large as we like whilst the group K retains the property of not having a proper direct product decomposition. The following problem arises naturally from our investigations:

Problem: *Characterise groups G that have no proper direct product decomposition but for which there exists a group H such that $\mu(G) = \mu(G \times H)$. For such groups G find the maximal such H.*

The problem of Saunders may be refined as follows:

Problem (Saunders): *Find groups G and H, if they exist, such that G and H both have no proper direct product decomposition, but*

$$\max\{\mu(G), \mu(H)\} < \mu(G \times H) < \mu(G) + \mu(H).$$

Example 2.4.4. Consider the groups

$$G_1 = \mathbb{F}_5^2 \rtimes \langle T_1 \rangle, G_2 = \mathbb{F}_5^3 \rtimes \langle T_2 \rangle, G_3 = \mathbb{F}_5^4 \rtimes \langle T_3 \rangle$$

where

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

so that

$$\phi_{T_1}(x) = x^2 + x + 1, \phi_{T_2}(x) = \phi_{T_3}(x) = (x - 1)(x^2 + x + 1)$$

and

$$\langle T_1\rangle \cong \langle T_2\rangle \cong \langle T_2\rangle \cong C_3.$$

Then $G_1 \cong C_5^2 \rtimes C_3$ and $\mu(G_1) = 15$, by Theorem 2.4.1. From the proof, a minimal faithful representation is afforded by a single subgroup corresponding to a codimension 1 subspace of $\mathbb{F}_5^2$ with trivial core. We get the following transitive representation:

$$\begin{aligned} G_1 &\cong \langle x_1, x_2, y | x_1^5 = x_2^5 = y^3 = 1, x_1^{x_2} = x_1, x_1^y = x_2, x_2^y = x_1^{-1}x_2^{-1}\rangle \\ &\cong \langle \alpha_1, \alpha_2, \beta\rangle, \end{aligned}$$

where

$$\begin{aligned} \alpha_1 &= (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9\ 10)(11\ 14\ 12\ 15\ 13), \\ \alpha_2 &= (1\ 2\ 3\ 4\ 5)(6\ 9\ 7\ 10\ 8)(11\ 12\ 13\ 14\ 15), \\ \beta &= (1\ 11\ 6)(2\ 12\ 7)(3\ 13\ 8)(4\ 14\ 9)(5\ 15\ 10). \end{aligned}$$

By Theorem 2.4.2, $\mu(G_2) = 15$, by a minimal faithful transitive representation induced by a subgroup corresponding now to a codimension 1 subspace of $\mathbb{F}_5^3$ with trivial core, yielding

$$G_2 \cong G_1 \times C_5 \cong \langle \alpha_1, \alpha_2, \alpha_3, \beta\rangle,$$

where α_1, α_2 and β 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 subgroups of the transitive permutation group introduced at the end of Wright's paper [**19**] yielding the first published counterexample to additivity of μ with respect to direct product. By contrast, $\mu(G_3) = 15 + 5 = 20$, again by Theorem 2.4.2, but by an intransitive faithful representation, afforded by the codimension 1 subspace of the previous case, augmented in the obvious way, and a subgroup of index 5, yielding

$$G_3 \cong G_2 \times C_5 \cong G_1 \times C_5^2 \cong \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \beta\rangle,$$

where α_1, α_2, α_3 and β are as above, but fixing five new letters, and

$$\alpha_4 = (16\ 17\ 18\ 19\ 20).$$

Now we have an illustration of the phenomenon described earlier where

$$\max\{\mu(K), \mu(L \times M)\} < \mu\left(K \times (L \times M)\right) < \mu(K) + \mu(L \times M)$$

by taking $K = G_1$ and $M = C_5^2$, and noting that $\mu(M) = 10$.

Example 2.4.5. Let p and q be primes such that p has order $q-1$ modulo q, so that $\phi(x) = 1 + x + \ldots + x^{q-1}$ is irreducible over F_p, and also such that $q < p^{q-2}$ (to ensure that $a \geq 1$ in the hypotheses of Theorems 2.4.1 and 2.4.2 when they are applied below). The smallest case is $p = 2$ and $q = 5$. Consider the groups

$$H_1 = \mathbb{F}_p^{q-1} \rtimes \langle U_1 \rangle \qquad \text{and} \qquad H_2 = \mathbb{F}_p^q \rtimes \langle U_2 \rangle,$$

where U_1 and U_2 are matrices over $\mathbb{F}_p$ in rational canonical form having minimal polynomials $\phi(x)$ and $(1+x)\phi(x)$ respectively. Then

$$H_1 \cong C_p^{q-1} \rtimes C_q, H_2 \cong C_p^q \rtimes C_q \cong H_1 \times C_p,$$

and $\mu(H_1) = \mu(H_2) = pq$, by Theorems 2.4.1 and 2.4.2. 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 [**17**]. In the smallest case, when $p = 2$ and $q = 5$, the groups become $H_1 \cong C_2^4 \rtimes C_5$ and $H_2 \cong C_2^5 \rtimes C_5 \cong H_1 \times C_2$, where

$$U_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

$$U_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and

$$\mu(H_1) = \mu(H_2) = \mu(H_1 \times C_2) = 10 < 12 = \mu(H_1) + \mu(C_2).$$

The group H_1 and these properties appear for the first time in [**15**]. In his thesis [**16**], Saunders shows, by an elaborate argument and some computer checking, that the subadditive property cannot occur for a direct product embedded in the symmetric group on less than 10 letters. 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 2.4.1 and 2.4.2.

References

[1] COOPERSTEIN, B. *Advanced Linear Algebra.* Taylor and Francis Group LLC, 2010.

[2] EASDOWN, D. *Minimal faithful permutation and transformation representations of groups and semigroups.* Contemporary Mathematics, Volume 131, (1992), Part 3, pp. 75-84.

[3] EASDOWN, D. & HENDRIKSEN, M. *Minimal permutation representations of semidirect products of groups.* Preprint. School of Mathematics and Statistics, University of Sydney, 2015.

[4] EASDOWN, D. & PRAEGER, C.E. *On minimal faithful permutation representations of finite groups.* (1998) Bulletin of the Australian Mathematical Society, 38, pp. 207-220.

[5] FRANCHI, C. *On minimal degrees of permutation representations of abelian quotients of finite groups.* (2011) Bulletin of the Australian Mathematical Society, 84, pp. 408-413.

[6] HOLT, D.F. & WALTON, J. *Representing the Quotient Groups of a Finite Permutation Group.* Journal of Algebra 248, pp. 307-333 (2002).

[7] JOHNSON, D.L. *Minimal permutation representations of finite groups.* Amer. J. Math. 93 (1971), pp. 857-866.

[8] KARPILOVSKY, G. I. *The least degree of a faithful representation of abelian groups.* Vestnik Khar'kov Gos. Univ, 53:107-115, 1970.

[9] KOVACS, L. G. & PRAEGER, C. E. *Finite permutation groups with large abelian quotients.* Pacific J. Math. 136 (1989), pp. 283-292.

[10] LEMIEUX, S. *Minimal Degree of Faithful Permutation Representations of Finite Groups.* Masters Thesis, Carleton University, Ottawa, 1999.

[11] LEMIEUX, S. *Finite exceptional p-groups of small order.* Comm. Algebra, 35 (6):1890-1894, 2007.

[12] LIPSCHUTZ, S., & LIPSON, M. *Schaum's Outline of Linear Algebra.* McGraw Hill Professional, 1 Jan 2000.

[13] NEUMANN, P.M. *Some algorithms for computing with finite permutation groups.* In Robertson, E.F. and Campbell, C.M. (eds), Proceedings of Groups-St Andrews 1985. London Math. Soc. Lecture Notes 121, Cambridge University Press (1987), 59-92.

[14] ROBINSON, DEREK *A Course in the Theory of Groups.* Springer Science & Business Media, 1996.

[15] SAUNDERS, N. *Strict inequalities for minimal degrees of direct products.* Bulletin of the Australian Mathematical Society, (2009), 79, pp 23-30.

[16] SAUNDERS, N. *Minimal Faithful Permutation Representations of Finite Groups.* Ph.D. Thesis, University of Sydney, 2010.

[17] SAUNDERS, N. *The minimal degree for a class of finite complex reflection groups.* Journal of Algebra 323, (2010), pp. 561-573.

[18] *Schaps, M., Weil, M., Shlomo, O. & Hasan Ali, M.* DATABASE OF GROUP CHARACTER TABLES. Sourced from http://u.cs.biu.ac.il/~mschaps/DATA/database.html on 25/08/13.

[19] WRIGHT, D. *Degrees of minimal embeddings for some direct products.* Amer. J. Math. 97 (1975), pp. 897-903.