Mathematica Pannonica
25/2 (2014–2015), 41–55

ON THE CENTRE OF A CENTRALIZER NEAR-RING

Martin R. **Pettet**

Department of Mathematics
The University of Toledo
Toledo, Ohio 43606
U.S.A.

Received: February 5, 2016

MSC 2000: 16 Y 30; Secondary 20 D 45, 20 D 15.

Keywords: automorphism, near-ring, centralizer near-ring, centre; nilpotent group, regular orbit, wreath product.

Abstract: Let $A \leq \mathrm{Aut}(G)$ where G is a finite group and let $M_A(G)$ be the near-ring of maps from G to itself that fix 0 and commute with A. We investigate the multiplicative structure of the centre $Z(M_A(G))$ and the consequences if $Z(M_A(G))$ is a subnear-ring of $M_A(G)$.

1. Introduction

In line with the terminology of groups and rings, the set of elements of a *near-ring* N that commute (multiplicatively) with all elements of N is called the *centre* of N, denoted here by $Z(N)$. However, in a *right* near-ring (as the near-rings considered here are), the lack of a left distributive law means that the centre fails, in general, to be additively closed. Thus, in addition to identifying the elements and multiplicative structure of the centre, the problem arises of characterizing those situations in which the centre is, in fact, a subnear-ring.

E-mail address: mpettet@math.utoledo.edu

These questions have been studied for several important classes of near-rings (including function near-rings) in [1], [3] and [5] but relatively few of the results apply specifically to *centralizer* near-rings. Here, our focus is exclusively on the centralizer near-ring $M_A(G)$, where G is a non-trivial finite group (written additively but not necessarily abelian) and A is a group of automorphisms of G. Thus, $M_A(G)$ consists of all maps $f : G \to G$ such that $f(0) = 0$ and $\alpha f = f\alpha$ for all $\alpha \in A$, with addition defined by the group operation in G and multiplication by composition.

We describe the multiplicative structure of $Z(M_A(G))$ in the context of a general direct sum decomposition of $M_A(G)$ into indecomposable ideals (Theorem 2.4). (It seems unlikely that this decomposition has not been described elsewhere but the author is unaware of an explicit reference.) From this decomposition, we conclude that the non-zero elements in each corresponding summand of $Z(M_A(G))$ form a multiplicative group, isomorphic to a subdirect product of certain abelian sections of A.

A consequence is that the obvious containment $Z(A) \cup \{0\} \subseteq Z(M_A(G))$ is an equality if A has a *regular orbit* in G (Theorem 3.1). In particular, by a result of B. B. Hargraves, this applies if A is nilpotent of order relatively prime to $|G|$ and $Z_p \wr Z_p$-free for $p = 2$ and all Mersenne primes (Theorem 3.3).

For arbitrary A but with the added assumption that $Z(M_A(G))$ is a subnear-ring, we show that $Z(M_A(G))$ is a direct sum of fields and G is a union of corresponding vector spaces (Theorem 4.2). A full characterization of this phenomenon is obtained in the case that A is nilpotent and $Z_p \wr Z_p$-free as above but not necessarily of order prime to G (Theorem 5.2).

We conclude by examining some known examples of coprime nilpotent actions without regular orbits, in some of which $Z(M_A(G))$ is strictly larger than $Z(A) \cup \{0\}$.

It is assumed throughout that $|G| > 1$ (so 0 and 1 are distinct elements of $M_A(G)$).

Notational remark. Let $G^{\#} = G\backslash\{0\}$ and if $x \in G$, let $C_A(x) = \{\alpha \in A : \alpha(x) = x\}$, the *centralizer* of x in A. More generally, if $S \subseteq G$, $C_A(S) = \{\alpha \in A : \alpha(s) = s \ \forall x \in S\}$. (This group theoretic terminology derives from the fact that within the semidirect product $G \rtimes A$, the action of A on G is conjugation and so $C_A(x)$ is the set of elements of A that commute with or *centralize* x. $C_A(x)$ is also often called the *stabilizer* of

x in A.) Similarly, if $B \subseteq A$, we define $C_G(B) = \{x \in G : \beta(x) = x \ \forall \beta \in B\}$.

Because it arises so frequently, the double stabilizer $C_G(C_A(x))$ is denoted here by G_x. Also, A_x will denote the automizer $N_A(G_x)/C_A(G_x)$, a section of A identified with a subgroup of $\mathrm{Aut}(G_x)$. If $x \in G$, $A(x)$ denotes the orbit of A containing x, namely $\{\alpha(x) : \alpha \in A\}$. More generally, if $X \subseteq G$, $A(X) = \{\alpha(x) : \alpha \in A, \ x \in X\}$.

The author thanks G. Alan Cannon for a correspondence that drew these problems to his attention.

2. A decomposition of $M_A(G)$

Lemma 2.1. If $A \leq \mathrm{Aut}(G)$ and $x \in G^\#$, then

(a) $G_x = \{f(x) : f \in M_A(G)\}$ (Betsch's Lemma).

(b) $C_A(x) = C_A(G_x)$.

Proof. If $f \in M_A(G)$ then $C_A(x) \leq C_A(f(x))$ so $f(x) \in G_{f(x)} \leq G_x$. But if $y \in G_x$, then $C_A(x) \leq C_A(y)$ and so there exists a function $f : G \to G$ such that $f(\alpha(x)) = \alpha(y)$ if $\alpha \in A$ and $f(u) = 0$ if $u \notin A(x)$. Moreover, f commutes with A and so $f \in M_A(G)$. This proves (a).

For (b), $C_A(G_x) \leq C_A(x)$ since $x \in G_x$. But suppose $\alpha \in C_A(x)$. If $y \in G_x$ then by (a), $f(x) = y$ for some $f \in M_A(G)$ and so, since A commutes with f, $\alpha \in C_A(y)$. Therefore, $C_A(x) \leq C_A(G_x)$, as required. $\diamondsuit$

We first consider the action of $Z(M_A(G))$ on double stabilizers. Clearly, $Z(A) \subseteq Z(M_A(G))^\#$. The gist of the next result is that actually, the whole of $Z(M_A(G))^\#$ is, in a sense, patched together from sections of A.

Proposition 2.2. Let $x \in G^\#$. If $z \in Z(M_A(G))$ and $z\big|_{G_x} \neq 0\big|_{G_x}$ then $z\big|_{G_x} = \alpha_z\big|_{G_x}$ for some $\alpha_z \in N_A(G_x)$. Moreover, $[\beta, \alpha_z^{-1}] \in C_A(G_x \cap G_{\beta(x)})$ for all $\beta \in A$ and in particular, $\bar{\alpha}_z = \alpha_z C_A(G_z) \in \bigcap_{y \in G_x} N_{Z(A_x)}(G_y)$.

Proof. Let $x \in G^\#$ and $z \in Z(M_A(G))$. We claim that if $z(x) \neq 0$ then $z(x) \in A(x)$. For if x and $z(x)$ lie in distinct A-orbits, there exists an $f \in M_A(G)$ such that $f(x) = x$ and $f(z(x)) = 0$ and so $z(x) = z(f(x)) = f(z(x)) = 0$.

If $z(x) = 0$, set $\alpha_z = 0$ and otherwise, let $\alpha_z \in A$ such that $z(x) = \alpha_z(x)$. We claim that $z(u) = \alpha_z(u)$ for all $u \in G_x$. For if $u \in G_x$, $u = f(x)$ for some $f \in M_A(G)$ and so $z(u) = z(f(x)) = f(z(x)) = f(\alpha_z(x)) = \alpha_z(f(x)) = \alpha_z(u)$. In particular, either $z\big|_{G_x} = 0$ or $z\big|_{G_x} = \alpha_z\big|_{G_x}$ for $\alpha_z \in N_A(G_x)$.

Assume that $0 \neq z\big|_{G_x} = \alpha_z\big|_{G_x}$ and $\beta \in A$. If $y \in G_x \cap G_{\beta(x)}$ then $\beta^{-1}(y) \in G_x$ and so $\alpha_z(\beta^{-1}(y)) = z(\beta^{-1}(y)) = \beta^{-1}(z(y)) = \beta^{-1}(\alpha_z(y))$. Therefore, $[\beta, \alpha_z^{-1}](y) = \beta\alpha_z^{-1}\beta^{-1}\alpha_z(y) = y$ so $[\beta, \alpha_z^{-1}] \in C_A(y)$. Thus, $[\beta, \alpha_z^{-1}] \in C_A(G_x \cap G_{\beta(x)})$. In particular, if $\beta \in N_A(G_x)$, $[\beta, \alpha_z^{-1}] \in C_A(G_x)$ so $\bar{\alpha}_z = \alpha_z C_A(G_x) \in Z(N_A(G_x)/C_A(G_x)) = Z(A_x)$. For all $y \in G_x$, $z(G_y) \subseteq G_y$ and so $\alpha_z \in N_A(G_y)$ and $\bar{\alpha}_z \in N_{Z(A_x)}(G_y)$. Thus, $\bar{\alpha}_z \in \bigcap_{y \in G_x} N_{Z(A_x)}(G_y)$. ◊

To set up the statement of the main result of this section, we introduce some *ad hoc* definitions and notation:

If $x, y \in G^{\#}$, we write $x \frown y$ if $A(G_x^{\#}) \cap A(G_y^{\#}) \neq \emptyset$.

Let $\sim$ be the transitive closure of the symmetric relation $\frown$.

Let $\Omega = G^{\#}/\sim$, using $[x]$ to denote the $\sim$ equivalence class containing x.

Proposition 2.3. Let $z \in Z(M_A(G))$. If $x \in G^{\#}$ and $z(x) \neq 0$, then $z(y) \neq 0$ for all $y \in [x]$ and z induces a permutation on $[x]$.

Proof. Proposition 2.2 implies that, for any double stabilizer G_u, if the restriction $z\big|_{G_u^{\#}}$ is not the zero map then z induces an automorphism on G_u (and thus, it maps G_u to itself with no non-trivial zeros). It follows that either $z\big|_{A(G_u^{\#})}$ is the zero map or it has no zeros and moreover, the same is true for $z\big|_{A(G_x^{\#}) \cup A(G_y^{\#})}$ provided that $x \frown y$. By an obvious induction, we see that if $z(x) \neq 0$ then z has no zeros in $[x]$.

Note that for any $y \in [x]$, $G_y^{\#} \subseteq [x]$. For if $u \in G_y^{\#}$, $G_u \leq G_y$ so certainly $y \frown u$. Since $x \sim y$, $x \sim u$ and so $u \in [x]$ as claimed. Thus, if $y \in [x]$, $z(y) \in z(G_y)^{\#} \subseteq G_y^{\#} \subseteq [x]$ so $z([x]) \subseteq [x]$.

To show that z induces a permutation on $[x]$, it suffices to show that $z\big|_{[x]}$ is injective. Suppose $u, v \in [x]$ with $z(u) = z(v) = w$. By Proposition 2.2, z induces an automorphism on each of G_u, G_v and G_w. In particular, $z(w') = w$ for some $w' \in G_w \leq G_u \cap G_v$. Thus, $u = w' = v$ by the injectivity of z on G_u and G_v. ◊

Recall that a near-ring is said to be *indecomposable* if it has no non-trivial near-ring direct summands (or equivalently, if it is not the direct sum of non-trivial ideals). By a *minimal stabilizer*, we shall mean a one-element stabilizer $C_A(x)$ that is minimal (with respect to inclusion) in the set of all such stabilizers.

Let $\mathcal{X}$ be a set of elements of G whose stabilizers are a complete set of representatives of the orbits of A on the collection of minimal stabilizers.

Theorem 2.4. Suppose that G is a finite group with $A \leq \mathrm{Aut}(G)$ and let $\mathcal{X}$, $\sim$ and Ω be as described above. For any $[x] \in \Omega$, let $M_A[x] = \{f \in M_A(G) : f(y) = 0 \text{ for all } y \notin [x]\}$. Then

(a) Each $M_A[x]$ is an indecomposable near-ring and an ideal of $M_A(G)$.

(b) $M_A(G) = \bigoplus_{[x]\in\Omega} M_A[x]$.

(c) $Z(M_A(G)) = \bigoplus_{[x]\in\Omega} Z(M_A[x])$ (as a multiplicative monoid).

(d) For each $x \in G^\#$, $Z(M_A[x])^\#$ is a multiplicative abelian group, isomorphic to a subdirect product of the groups $\bigcap_{y\in G_u} N_{Z(A_u)}(G_y)$, $u \in \mathcal{X} \cap [x]$.

Proof. It is routine to check that the $M_A[x]$'s are ideals and that $M_A[x] \cap (\Sigma_{[y]\neq[x]} M_A[y]) = \{0\}$ for all $[x] \in \Omega$. If $f \in M_A(G)$ and $[x] \in \Omega$ then $f([x]) \subseteq [x]$ by Lemma 2.1 (a). Because each $[x]$ is also A-invariant, there exist functions $f_{[x]} \in M_A[x]$ with $f_{[x]}(u) = f(u)$ for all $u \in [x]$. Since $f = \Sigma_{[x]\in\Omega} f_{[x]}$, $M_A(G) = \bigoplus_{[x]\in\Omega} M_A[x]$. This proves (b) and (c) follows.

If $z \in M_A[x]^\#$, by Proposition 2.3, $z\big|_{[x]}$ is a permutation and hence, for some $n > 0$, $z\big|_{[x]}^{-1} = z\big|_{[x]}^{n} \in Z(M_A[x])^\#$. Therefore, $Z(M_A[x])^\#$ is a multiplicative group. If $M_A[x]$ had a non-trivial direct summand, the projection of the multiplicative identity of $M_A[x]$ on that summand would yield a non-trivial idempotent in $Z(M_A[x])$, contradicting the fact that $Z(M_A[x])^\#$ is a multiplicative group. Thus, $M_A[x]$ is an indecomposable near-ring.

If $x \in G^\#$ then $[x] = \bigcup_{u\in[x]} G_u^\#$ and because every stabilizer contains a minimal stabilizer, $[x] = \bigcup_{u\in\mathcal{X}\cap[x]} \bigcup_{\alpha\in A} G_{\alpha(u)}^\#$ Let $Z = Z(M_A[x])^\#$. Because elements of A commute with $Z(M_A(G))$, $C_Z(G_u) = C_Z(G_{\alpha(u)})$ for all $\alpha \in A$ and so $\bigcap_{u\in\mathcal{X}\cap[x]} C_Z(G_u) = C_Z([x]) = 1_Z$. Therefore, $Z \cong Z/\bigcap_{u\in\mathcal{X}\cap[x]} C_Z(G_u)$ is a subdirect product of the groups $Z/C_Z(G_u)$

where u ranges over $\mathcal{X} \cap [x]$. But by Proposition 2.2, if $u \in \mathcal{X} \cap [x]$ the map $z \mapsto z\big|_{G_u}$ defines a group homomorphism $Z \to \bigcap_{y \in G_u} N_{Z(A_u)}(G_y)$ and so $Z/C_Z(G_u)$ is isomorphic to a subgroup of $\bigcap_{y \in G_u} N_{Z(A_u)}(G_y)$, proving (d). $\Diamond$

Corollary 2.5. If $A \leq \mathrm{Aut}(G)$ then the following conditions are equivalent:

(a) $M_A(G)$ is indecomposable.
(b) $[x] = G^{\#}$ for some (and hence, any) $x \in G^{\#}$.
(c) $Z(M_A(G))^{\#}$ is a multiplicative group.

Corollary 2.6. If $A \leq \mathrm{Aut}(G)$ and $C_G(A) \neq \{0\}$ then $Z(M_A(G))^{\#}$ is a multiplicative group.

Proof. $\{0\} < C_G(A) \leq C_G(C_A(x)) = G_x$ for all $x \in G$ and so $x \frown y$ for all $x, y \in G^{\#}$. Therefore, $G^{\#} = [x]$. $\Diamond$

For example, the previous corollary applies if A is a nilpotent group of *inner* automorphisms of a non-trivial group G. For since G is non-trivial, we may assume that $A \neq 1$. Identifying $\mathrm{Inn}(G)$ with the quotient $G/Z(G)$, A then corresponds to a non-trivial nilpotent subgroup $H/Z(G)$ acting on G by conjugation. But then H is itself nilpotent (since $Z(G) \leq Z(H)$) and so $1 \neq Z(H) \leq C_G(A)$.

Corollary 2.6 also applies if A is a p-group for some prime divisor p of $|G|$. For in this case, let R be a Sylow p-subgroup of the natural semidirect product $G \rtimes A$ such that $A \leq R$. If $P = R \cap G$ then $\{0\} \neq P \trianglelefteq R$ and so by [8, Theorem 1.19], $\{0\} \neq P \cap Z(R) \leq C_P(A) \leq C_G(A)$. We note also that by statement (d) of Theorem 2.4, $Z(M_A(G))^{\#}$ is a p-group in this case.

The following alternate description of $[x]$ will be useful when we consider the case that $Z(M_A(G))$ is a subnear-ring of $M_A(G)$.

Proposition 2.7. For any $x \in G^{\#}$, let $I_Z(x) = \{z \in Z(M_A(G)) : z(x) = 0\}$. Then $[x] = \{y \in G^{\#} : I_Z(y) = I_Z(x)\}$.

Proof. Suppose $y \in [x]$ so $[x] = [y]$. As in Proposition 2.3, $z(x) = 0$ if and only if $z(y) = 0$ and so $I_Z(x) = I_Z(y)$. Suppose $y \in G^{\#} \backslash [x]$ so $[x] \cap [y] = \emptyset$. Define $z \in Z(M_A(G))$ by setting $z(u) = u$ if $u \in [x]$ and $z(u) = 0$ if $u \in G \backslash [x]$. Then $z \in I_Z(y) \backslash I_Z(x)$ and so $I_Z(x) \neq I_Z(y)$. $\Diamond$

3. Regular orbits

By Proposition 2.2, elements of $Z(M_A(G))$ induce A_x-endomorphisms (and in fact, A_x-automorphisms) on G_x for any $x \in G$. Before stating the next result, we mention an abstract characterization of all such elements.

An element f of a right near-ring N is said to be *distributive* if, for all $g, h \in N$, $f(g+h) = fg + fh$. Such elements form a multiplicative monoid containing $Z(N)$, denoted by N_d. Clearly, $M_A(G)_d$ contains the set $\mathrm{End}_A(G)$ of A-endomorphisms of G. In fact, it is an easy consequence of Lemma 2.1 (a) that $M_A(G)_d$ consists precisely of those elements $f \in M_A(G)$ such that $f\big|_{G_x} \in \mathrm{End}_{A_x}(G_x)$ for all $x \in G$.

An orbit $A(x)$ is said to be *regular* if $C_A(x) = 1$. By Lemma 2.1 (a), such an element x has the property that for every $y \in G$, there is an $f \in M_A(G)$ such that $f(x) = y$.

Theorem 3.1. Let G be a non-trivial finite group and let A be a subgroup of $\mathrm{Aut}(G)$. If A has a regular orbit in G then $M_A(G)$ is indecomposable, $Z(M_A(G)) = Z(A) \cup \{0\}$ and $M_A(G)_d = \mathrm{End}_A(G)$.

Proof. If $C_A(x) = 1$, then $G_x = G$ and $A_x = A$. By Proposition 2.2, if $z \in Z(M_A(G))^\#$, $z = \alpha_z \in A$ where $[\alpha, \alpha_z^{-1}] \in C_A(G) = 1$ for all $\alpha \in A$. Thus, $z = \alpha_z \in Z(A)$. Since $Z(A) \subseteq Z(M_A(G))^\#$, $Z(M_A(G))^\# = Z(A)$. The indecomposability of $M_A(G)$ follows from Theorem 2.4 or Corollary 2.5. That $M_A(G)_d = \mathrm{End}_A(G)$ follows from the remarks above. $\Diamond$

Examples. (a) Of course, if $A = 1$, all orbits are regular. In this case, Theorem 3.1 generalizes two simple observations concerning $M_{\{1\}}(G)$ (usually denoted $M_0(G)$), namely that its centre is $\{0, 1\}$ [1, Proposition 1.1] and the set of distributive elements is $\mathrm{End}(G)$ [10, Lemma 9.6].

(b) If $M_A(G)$ is semisimple then as described in [9], $M_A(G)$ is a direct sum of centralizer near-rings of the form $N_x = M_{A_x}(G_x)$ so $Z(M_A(G))$ is correspondingly, a direct sum of the $Z(N_x)$'s. For each x, A_x is identified as a subgroup of $\mathrm{Aut}(G_x)$ with all non-trivial orbits of A_x in G_x being regular (so the natural semidirect product $G_x \rtimes A_x$ is a Frobenius group). By Theorem 3.1, $Z(N_x)^\# = Z(A_x)$ and, because the Sylow subgroups of a Frobenius complement are cyclic or generalized quaternion (see e.g. [8, Corollary 6.17]), this group is cyclic.

(c) If G is a vector space over a finite field F and A is the multiplicative group $F^{\#}$ of non-zero elements of F acting on G via scalar multiplication, all non-zero orbits are regular and so by Theorem 3.1, $Z(M_A(G)) = A \cup \{0\} = F$. In particular, in this situation $Z(M_A(G))$ is a subnear-ring of $M_A(G)$. As we shall see in Theorem 4.2, in a sense, this represents the simplest instance of this phenomenon.

Of course, the question immediately raised by Theorem 3.1 is: For which pairs (G, A) do regular orbits necessarily exist? For abelian coprime automorphism groups, they always exist, a fact that can be established by a relatively elementary argument. (See [8, 3.4] for the case that A is a p-group.) But for coprime actions of solvable or even nilpotent groups, regular orbits need not exist and identifying conditions under which they do can involve long and delicate represention theoretic arguments.

Example. S. Dolfi has shown [4] that if $A \leq \mathrm{Aut}(G)$ is solvable with $|A|$ and $|G|$ coprime then, while a regular orbit for A need not exist in G, the stabilizers of some pair of elements of G intersect trivially and so a regular orbit does exist for the standard action of A on $G \oplus G$. Thus, for any finite group G and any solvable, coprime group A of automorphisms of G, $M_A(G \oplus G)$ is indecomposable, $Z(M_A(G \oplus G))^{\#} = Z(A)$ and $M_A(G \oplus G)_d = \mathrm{End}_A(G \oplus G)$.

Extending an earlier result of T. R. Berger, the following orbit theorem for nilpotent coprime automorphism groups was established by B. B. Hargraves [7]. (A shorter proof appears in [6].) Recall that a group X is said to be *involved* in a group Y if X is isomorphic to a homomorphic image of a subgroup of Y.

Theorem 3.2. Let G be a non-trivial finite group and let A be a subgroup of $\mathrm{Aut}(G)$. If $A \leq \mathrm{Aut}(G)$ is nilpotent and $\gcd(|A|, |G|) = 1$ then A has a regular orbit except possibly if the wreath product $Z_p \wr Z_p$ is involved in A for $p = 2$ or a Mersenne prime.

(This result is stated in [7] for the case that G is a faithful, irreducible kA-module, where k is a field of characteristic not dividing $|A|$. However, by the Hartley-Turull theorem [8, 3.31], for G an arbitrary finite group, there is an abelian group G^* admitting A such that the groups G

and G^* are isomorphic as A-sets. The existence of a regular orbit in G^* (and hence, in G) follows from the module case by a standard argument.)

As an immediate consequence of Theorems 3.1 and 3.2, we have

Theorem 3.3. Let G be a non-trivial finite group and let A be a subgroup of $\mathrm{Aut}(G)$.

Suppose that $A \leq \mathrm{Aut}(G)$ is nilpotent with $\gcd(|A|, |G|) = 1$ and that the wreath product $Z_p \wr Z_p$ is not involved in A for $p = 2$ or a Mersenne prime. Then $M_A(G)$ is indecomposable, $Z(M_A(G)) = Z(A) \cup \{0\}$ and $M_A(G)_d = \mathrm{End}_A(G)$.

The wreath product hypothesis may not be easy to verify directly but because $Z_p \wr Z_p$ has nilpotence class p, it certainly holds if the Sylow p-subgroup of A has class less than p for $p = 2$ and all Mersenne primes dividing $|A|$.

4. Near-rings whose centres are subnear-rings

Not surprisingly, much more can be said about $M_A(G)$ if, to the hypotheses of Theorem 2.4 is added the assumption that $Z(M_A(G))$ is additively closed. Most of the following lemma was noted in [3].

Lemma 4.1. Suppose that $Z(M_A(G))$ is a subnear-ring of $M_A(G)$. Then
(a) For any $x \in G^{\#}$, G_x is an elementary abelian p-group for some prime p (so addition in $M_A(G)$ is commutative).
(b) One of the following three alternatives applies:
(i) G is a p-group of exponent p for some prime p
(ii) G is a Frobenius group with the Frobenius kernel a p-group of exponent p and complement of order q for distinct primes p and q, or
(iii) $G \cong A_5$

Proof. Since the identity map 1 is in $Z(M_A(G))$, the map $k1 : g \mapsto kg$ is in $Z(M_A(G))$ for any positive integer k. By Proposition 2.2, this map induces on each double stabilizer G_x either the zero map or an automorphism. Choosing $k = 2$ yields (in either case) that G_x is abelian. The additive commutativity of $M_A(G)$ follows since, if $f, g \in M_A(G)$ and $x \in G$, then $f(x), g(x) \in G_x$ so $(f + g)(x) = (g + f)(x)$. Choosing $k = p$ where p is a prime divisor of the exponent $\exp(G_x)$ of G_x yields that $p1\big|_{G_x} = 0$ so G_x has exponent p. Since G is the union of the double stabilizers, all non-zero elements of G have prime order and (b) follows, as in [9, Theorem 3]. $\Diamond$

Remark. As observed in [3, Corollary 2.3], the commutativity of addition follows, in fact, for *any* near-ring N with identity in which $Z(N)$ is a subnear-ring. Moreover, the set N_d of distributive elements is then a subring.

The following may be regarded as a generalization of [9, Corollary 3].

Theorem 4.2. Let G be a non-trivial finite group with $A \leq \mathrm{Aut}(G)$. Assume that $Z(M_A(G))$ is a subnear-ring of $M_A(G)$ and let $M_A(G) = \bigoplus_{[x]\in\Omega} M_A[x]$ as described in Theorem 2.4. Then

(a) Each $Z(M_A[x])$ is a field and for each $y \in [x]$, G_y is a vector space over $Z(M_A[x])$.

(b) If $x \in G^{\#}$, the action of $Z(M_A[x])^{\#}$ on G_x is induced by a cyclic subgroup of $Z(A_x)$.

(c) Corresponding to the three possibilities for G listed in Lemma 4.1 (b), (i) all $Z(M_A[x])$'s have the same characteristic p, (ii) all $Z(M_A[x])$'s are of characteristic p or of order q (with at least one of the latter occurring) or (iii) $G \cong A_5$, $A \cong \mathrm{Aut}(G) \cong S_5$ and $M_A(G) = Z(M_A(G)) \cong \mathbb{F}_2 \oplus \mathbb{F}_3 \oplus \mathbb{F}_5$.

Proof. By Lemma 4.1 (a), addition in $M_A(G)$ is commutative and so, if $Z(M_A(G))$ is a subnear-ring, it is a commutative ring, as is each summand $Z(M_A[x])$. But by Theorem 2.4 (d), $Z(M_A[x])^{\#}$ is a multiplicative abelian group and so $Z(M_A[x])$ is a field. If $x \in G^{\#}$, let $y \in [x]$. Then $I_Z(y) = I_Z(x)$ by Proposition 2.7 and so $Z(M_A[x])$ acts faithfully on G_y. Hence, G_y is a vector space over $Z(M_A[x])$ and (a) is proved.

Let $x \in G^{\#}$ and $Z = Z(M_A[x])^{\#}$, a cyclic multiplicative group. Because $Z(M_A[x])$ is a subnear-ring of $M_A(G)$, $z \in C_Z(x)$ if and only if $z - 1 \in I_Z(x)$. By Proposition 2.7, $C_Z(G_x) = C_Z(x) = C_Z([x]) = 1_{M_A[x]}$ and so the map $z \mapsto z\big|_{G_x}$, $Z \to Z(A_x)$ is a monomorphism, proving (b).

In view of (a), (i) and (ii) of statement (c) are consequences of the corresponding statements of Lemma 4.1 (b). In the remaining case (iii), by [9, Corollary 3] it remains only to prove that $A \cong S_5$. The following argument was communicated to the author by G. A. Cannon [2]: If $G = A_5$, $\mathrm{Aut}(G) \cong S_5$ and G is a non-abelian simple group. In particular, G may be identified with its inner automorphism group. By Lemma 4.1 (a), A has no regular orbit in G and so if x is any 5-cycle in G then $1 \neq C_A(x) = A \cap C_{S_5}(x) = A \cap \langle x \rangle$, whence $x \in A$. Therefore, the simplicity of G implies that $G \leq A$. But by (b) of this theorem, $Z(A_x)$ also contains an element of order 4. Since the Sylow 2-subgroups of G are isomorphic to $Z_2 \times Z_2$, $G \neq A$ and so $A = S_5$. $\diamondsuit$

Corollary 4.3. ([3, Theorem 5.2]) Let G be a non-trivial finite group and let A be a subgroup of $\mathrm{Aut}(G)$. If $Z(M_A(G))$ is a subnear-ring of $M_A(G)$, then for any $x \in G^{\#}$, $\langle x \rangle \backslash \{0\} \subseteq A(x)$. In particular, $Z(A_x)$ contains a cyclic subgroup of order $|x| - 1$.

Proof. Let $K = Z(M_A[x])$ and $p = \mathrm{char}(K) = \exp(G_x)$. $K^{\#}$ is transitive on $Kx\backslash\{0\}$ and if K_0 is the prime subfield of K, $Z_{p-1} \cong K_0^{\#} \leq K^{\#}$ and $K_0^{\#}$ is transitive on $K_0x\backslash\{0\} = \langle x \rangle \backslash \{0\}$. Theorem 4.2 (b) completes the proof. $\diamondsuit$

Theorem 4.2 (or Corollary 4.3) yields a generalization of one direction of [1, Proposition 1.1] (although, unfortunately, here without a converse).

Corollary 4.4. Let G be a non-trivial finite group and let A be a subgroup of $\mathrm{Aut}(G)$. Assume that $|A|$ is odd. If $Z(M_A(G))$ is a subnear-ring of $M_A(G)$ then G is an elementary abelian 2-group.

5. Two characterizations

Next, we note two cases in which the conditions under which $Z(M_A(G))$ is a subnear-ring of $M_A(G)$ are readily characterized. In each case, by Theorem 4.2 (c), we need only consider groups satisfying (i) or (ii) of Lemma 4.1 (b).

Theorem 5.1. Assume that $A \leq \mathrm{Inn}(G)$, the group of inner automorphisms. Then $Z(M_A(G))$ is a subnear-ring of $M_A(G)$ if and only if $A = \mathrm{Inn}(G)$ and

(i) G is an elementary abelian 2-group (of arbitrary rank) or

(ii) G is the semidirect product of an elementary abelian 3-group P (of arbitrary rank) and a group Q of order 2 acting on P by inversion. In case (i), $Z(M_A(G)) \cong \mathbb{F}_2$ and in case (ii), $Z(M_A(G)) \cong \mathbb{F}_3 \oplus \mathbb{F}_2$.

Proof. If G (and hence, A) has prime exponent p, Corollary 4.3 implies that $p = 2$ and so G is an elementary abelian 2-group and $A = 1$. By Theorem 3.1, $Z(M_A(G))^\# = 1$ so $Z(M_A(G)) \cong \mathbb{F}_2$. (See also [1, Proposition 1.1].)

Suppose that $G = PQ$ is Frobenius with a Frobenius kernel P of exponent p and complement $Q = \langle y \rangle \cong Z_q$ (so A may be regarded as a subgroup of G). Since $N_G(Q) = C_G(Q) = Q$, $A_y = 1$ so by Corollary 4.3, $q = 2$. By [8, Theorem 6.3], P is abelian and the element y conjugates each element of P to its inverse. Thus, if $x \in P^\#$, $G_x = P$ and since $C_G(P) = P$, $|A_x| = |A/A \cap P| \leq |G/P| = 2$. Again by Corollary 4.3, $p = 3$. By Lemma 4.1, each double stabilizer is abelian and so A has no regular orbit in G. Therefore, since $C_G(Q) = Q$, each conjugate of Q is contained in A and because G is generated by all such conjugates, $A = G$. In the notation of Theorem 2.4, $[x] = P^\#$ and because all elements of $G \backslash P$ are conjugate in $G = A$, $[y] = G \backslash P$. By Theorem 4.2, $Z(M_A[y])^\# \hookrightarrow Z(A_y) = 1$ so $Z(M_A[y]) \cong \mathbb{F}_2$. Similarly, $Z(M_A[x])^\# \hookrightarrow Z(A_x) \cong Z_2$ so $Z(M_A[x]) \cong \mathbb{F}_3$. Therefore, $Z(M_A(G)) = Z(M_A[x]) \oplus Z(M_A[y]) \cong \mathbb{F}_3 \oplus \mathbb{F}_2$. $\Diamond$

The second characterization concerns the case that A is nilpotent. In view of Theorem 3.3, it would seem redundant to explicitly state it but for the fact that, unlike the former theorem, this result does not require the *a priori* assumption that $|A|$ and $|G|$ be relatively prime.

Theorem 5.2. Let $A \leq \mathrm{Aut}(G)$ be nilpotent and assume A is $Z_p \wr Z_p$-free for $p = 2$ and all Mersenne primes. Then $Z(M_A(G))$ is a subnear-ring of $M_A(G)$ if and only if G is elementary abelian and $1 - \alpha \in Z(A)$ for all $\alpha \in Z(A) \backslash \{1\}$.

Proof. If G is elementary abelian and $1 - \alpha \in Z(A)$ for all $\alpha \in Z(A) \backslash \{1\}$, then $K = Z(A) \cup \{0\}$ is additively closed (and so is a field) and G is a K-module. If $p = \exp(G) = \mathrm{char}(K)$, $\gcd(|Z(A)|, p) = \gcd(|K| - 1, p) = 1$ and so, since A is nilpotent, $\gcd(|A|, p) = 1$. By Theorems 3.2 and 3.1, $Z(M_A(G)) = K$, a subnear-ring of $M_A(G)$ as claimed.

Assume now that $Z(M_A(G))$ is a subnear-ring of $M_A(G)$. Let P be the Fitting subgroup of G. Thus, according to whether (i) or (ii) of Lemma 4.1 (b) applies, P has exponent p for some prime p and either $P = G$ or $|G : P| = q$ for some prime $q \neq p$. We shall prove that A acts faithfully on P and p does not divide $|A|$, so Theorem 3.2 applies to the action of A on P.

We claim first that $C_A(P) = 1$. For this, we may assume that Lemma 4.1 (b)(ii) applies so let $Q = \langle y \rangle$ be a Frobenius complement in G. By Theorem 4.2 (a), all double stabilizers are abelian and so $G_x \leq P$ for all $x \in P^{\#}$ and $G_y = Q$. Then $Z(A) \leq N_A(C_A(y)) \leq N_A(G_y) = N_A(Q)$ so $[G, C_{Z(A)}(P)] = [QP, C_{Z(A)}(P)] = [Q, C_{Z(A)}(P)] \leq Q$. But Q contains no non-trivial normal subgroup of G so $[G, C_{Z(A)}(P)] = 1$, whence $C_{Z(A)}(P) = 1$. But A is nilpotent so any non-trivial normal subgroup of A has non-trivial intersection with $Z(A)$. Because $C_A(P) \trianglelefteq A$, it follows by [8, Theorem 1.19] that $C_A(P) = 1$ as claimed.

If $x \in P^{\#}$, $(Z(A)+I_Z(x))/I_Z(x) \leq (Z(M_A(G))/I_Z(x))^{\#} \cong Z(M[x])^{\#}$. But the map $\alpha C_{Z(A)}(x) \mapsto \alpha + I_Z(x)$ from $Z(A)/C_{Z(A)}(x)$ to $(Z(A) + I_Z(x))/I_Z(x)$ is well-defined and a multiplicative isomorphism. Therefore, $Z(A)/C_{Z(A)}(x)$ is isomorphic to a subgroup of $Z(M_A[x])^{\#}$.

By Theorem 4.2 (a), $Z(M_A[x])$ is a field of characteristic p and so $\gcd(|Z(A)/C_{Z(A)}(x)|, p) = 1$.

Because, as proved above, $\bigcap_{x \in P^{\#}} C_{Z(A)}(x) = C_A(P) = 1$, $Z(A)$ is isomorphic to a subgroup of the direct product $\prod_{x \in P^{\#}}(Z(A)/C_{Z(A)}(x))$. In particular, $\gcd(|Z(A)|, p) = 1$ and so, since A is nilpotent, $\gcd(|A|, p) = 1$.

We can now apply Theorem 3.2 to conclude that A has a regular orbit in P (and hence, in G). By Theorem 3.1, $Z(A) \cup \{0\}$ is a subnear-ring and so, if $1 \neq \alpha \in Z(A)$ then $1 - \alpha \in Z(M_A(G))^{\#} = Z(A)$. $\Diamond$

6. An example

One may reasonably ask if more direct proofs of Theorems 3.3 and 5.2 exist that sidestep the issue of regular orbits (and perhaps allow the wreath product hypotheses to be dropped or weakened). A natural first response to this question is to look at the examples that have been used (in [6] and elsewhere) to illustrate the necessity of these hypotheses in Theorem 3.2.

(Note: In what follows, G is a vector space over $\mathbb{F}_{q^r}$ and if $S \subseteq G^{\#}$, $\langle S \rangle$ denotes the $\mathbb{F}_{q^r}$-subspace of G spanned by S, *not* simply the additive subgroup that it generates.)

Example. Suppose p and q are primes with $q^r - p^s = 1$ (so the multiplicative group $\mathbb{F}_{q^r}^{\#} \cong Z_{p^s}$). The solutions of this equation are well-known (e.g. [11, Lemma 19.3]) and in all cases, p is either 2 or a Mersenne prime.

Let $G = \mathbb{F}_{q^r}^{\,p}$ with standard $\mathbb{F}_{q^r}$-basis $B = \{e_1, e_2, \ldots, e_p\}$. Let D be the multiplicative group of invertible diagonal (with respect to B) $\mathbb{F}_{q^r}$-linear transformations of G so $D \cong Z_{p^s}^{\,p}$. Define $\sigma \in \mathrm{Aut}(G)$ by $\sigma(e_i) = e_{i+1}$ for $1 \leq i < p$ and $\sigma(e_p) = e_1$ and let $A = D \rtimes \langle\sigma\rangle \cong Z_{p^s} \wr Z_p$ (so $Z(A) \cong Z_{p^s}$).

Let X be the set of vectors in $G^{\#}$ that have at least one zero component and let $u = (0, 1, 1, \ldots, 1) \in X$. X is A-invariant since the action of A preserves the number of zero components of a vector. Also, $C_A(u) = \{\mathrm{diag}(a, 1, 1, \ldots, 1) : a \in \mathbb{F}_{q^r}^{\#}\}$ and so $G_u = \langle e_2, e_3, \ldots, e_p\rangle$. In particular, $G_u^{\#} \subseteq X$. If x is any element of G whose first component is zero, then $C_A(u) \leq C_A(x)$ and so $G_x^{\#} \leq G_u^{\#} \subseteq X$. Since any vector with a zero component is $\langle\sigma\rangle$-conjugate to a vector with first component zero, it follows that $G_x^{\#} \subseteq X$ (and hence, $A(G_x^{\#}) \subseteq X$) for every $x \in X$, that A has no regular orbit in X and also, (recalling the notation used to formulate Theorem 2.4) that $X \subseteq [u]$.

Let $v = (1, 1, 1, \ldots, 1)$ Note that $G^{\#}\backslash X = D(v) = A(v)$. Also, $C_A(v) = \langle\sigma\rangle$ and so $G_v = C_G(\sigma) = \langle v\rangle$. (Thus, A also has no regular orbit outside X and so, no regular orbit anywhere in G.)

Since $G^{\#}\backslash X = A(v) = A(G_v)$, $A(y) = G^{\#}\backslash X$ for all $y \in G^{\#}\backslash X$. Since $A(x) \subseteq X$ for all $x \in X$, it follows that if $x \in X$ and $y \in G^{\#}\backslash X$ then $A(G_x^{\#}) \cap A(G_y^{\#}) = \emptyset$ so $x \not\sim y$. From the definition of $\sim$, it follows that $[u] \cap [v] = \emptyset$. Therefore, $X = [u]$ and $G^{\#}\backslash[u] = [v]$ and so Theorem 2.4 now yields that $M_A(G) = M_A[u] \oplus M_A[v]$ and $Z(M_A(G)) = Z(M_A[u]) \oplus Z(M_A[v])$.

Suppose that $f \in M_A(G)$. $C_A(e_1) = \{\mathrm{diag}(1, d_2, d_3, \ldots, d_p) : d_j \in \mathbb{F}_q^{\#}\}$ and so $G_{e_1} = \langle e_1\rangle$ and similarly, $G_{e_i} = \langle e_i\rangle$ for all i. Therefore, for all i, $f(e_i) \in \langle e_i\rangle$ and so $f(e_i) = \lambda_i e_i$ for some $\lambda_i \in \mathbb{F}_{q^r}$. But $\lambda_{i+1}e_{i+1} = f(e_{i+1}) = f(\sigma(e_i)) = \sigma(f(e_i)) = \sigma(\lambda_i e_i) = \lambda_i\sigma(e_i) = \lambda_i e_{i+1}$ and so $\lambda_{i+1} = \lambda_i$ for $1 \leq i \leq p-1$. Thus, there is a $\lambda \in \mathbb{F}_{q^r}$ such that $f(e_i) = \lambda e_i$ for all i.

Let $z \in Z(M_A(G))$. By Proposition 2.2, $z\big|_{G_u}$ is an endomorphism of G_u. Since $G_u = \langle e_2, e_3, \ldots, e_p\rangle$, the previous paragraph implies that there is a $\lambda \in \mathbb{F}_{q^r}$ such that $z(x) = \lambda x$ for all $x \in G_u$. Since every element of $[u]$ is $\langle\sigma\rangle$-conjugate to an element of G_u, $z(x) = \lambda x$ for all $x \in [u]$ and so $Z(M_A[u]) \cong \mathbb{F}_{q^r}$. Similarly, since $G_v = \langle v\rangle$, if $f \in M_A[v]$, there is a $\mu \in \mathbb{F}_{q^r}$ such that $f(v) = \mu v$ and since $[v] = A(v)$, $f(x) = \mu x$ for all $x \in [v]$. Thus, $M_A[v] = Z(M_A[v]) \cong \mathbb{F}_{q^r}$.

Therefore, $Z(M_A(G)) \cong \mathbb{F}_{q^r} \oplus \mathbb{F}_{q^r}$ and so, as with Theorem 3.2, the wreath product constraint (or something effectively similar) cannot be omitted from Theorem 3.3. However, this example is consistent with Theorem 5.2 since $Z(A) \cup \{0\} \cong \mathbb{F}_{q^r}$ so both $Z(A) \cup \{0\}$ and $Z(M_A(G))$ are subnear-rings.

We mention without details one further example from [6]. Let q be a Mersenne prime, G be the natural $GL_2(q)$-module and A be a Sylow 2-subgroup of $GL_2(q)$. A is semidihedral (so it involves $Z_2 \wr Z_2$) and indeed, there is no regular orbit. However, $M_A(G)$ is indecomposable and $Z(M_A(G)) = Z(A) \cup \{0\} = \{0, I, -I\}$. Thus, while it serves to show that the converse of Theorem 3.1 is false (even if A is nilpotent), this example too fails to clarify whether or not the wreath product hypothesis is really necessary in Theorem 5.2.

References

[1] AICHINGER, E. and FARAG, M.: On when the multiplicative center of a near-ring is a subnear-ring, *Aequationes Math.* **68** (2004), 46–59.

[2] CANNON, G. A.: *Personal communication.*

[3] CANNON, G. A., FARAG, M. and KABZA, L.: Centers and generalized centers of near-rings, *Comm. Algebra*, **35** (2) (2007), 443–453.

[4] DOLFI, S.: Large orbits in coprime actions of solvable groups, *Trans. Amer. Math. Soc.* **360** (1) (2008), 135–152.

[5] FARAG, M.: A new generalization of the center of a near-ring with applications to polynomial near-rings, *Comm. Algebra* **29** (6) (2001), 2377–2387.

[6] FLEISCHMANN, P.: Finite groups with regular orbits on vector spaces, *J. Algebra* **103** (1986), 211–215.

[7] HARGRAVES, B. B.: The existence of regular orbits for nilpotent groups, *J. Algebra* **72** (1981), 54–100.

[8] ISAACS, I. M.: *Finite Group Theory*, Graduate Studies in Mathematics 92, American Mathematical Society, Providence, RI 2008.

[9] MAXSON, C. J., PETTET, M. R. and SMITH, K. C.: *On semisimple rings that are centralizer near-rings*, *Pac. J. Math.* **101** (2) (1982), 451–461.

[10] MELDRUM, J. D. P.: *Near-Rings and Their Links with Groups*, Pitman Research Notes in Mathematics 134, Boston, 1985.

[11] PASSMAN, D. S.: *Permutation Groups*, W. A. Benjamin, Inc., New York, 1968.