ON SEMISIMPLE RINGS THAT ARE CENTRALIZER NEAR-RINGS

CARLTON JAMES MAXSON, MARTIN ROSS PETTET AND KIRBY C. SMITH
Let $G$ be a finite group with identity $0$ and let $\mathcal{A}$ be a group of automorphisms of $G$. The set $C(\mathcal{A}; G) = \{f: G \to G \mid f(0) = 0, f(\gamma v) = \gamma f(v) \text{ for every } \gamma \in \mathcal{A}, v \in G\}$ is the centralizer near-ring determined by $\mathcal{A}$ and $G$. In this paper we consider the following “representation” questions: (I) Which finite semisimple near-rings are of $C(\mathcal{A}; G)$-type? and (II) Which finite rings are of $C(\mathcal{A}; G)$-type?

1. Introduction. Let $G$ be a finite group and let $\Gamma$ denote a semigroup of endomorphisms of $G$. The set of functions $C(\Gamma; G) = \{f: G \to G \mid f(0) = 0 \text{ and } f(\gamma v) = \gamma f(v) \text{ for every } \gamma \in \Gamma, v \in G\}$ forms a zero-symmetric near-ring under function addition and function composition. (Since all near-rings in this paper will be zero-symmetric this adjective will henceforth be omitted.) Such “centralizer near-rings” are indeed general, for it is shown in [7] that if $N$ is any near-ring (with identity) then there exists a group $G$ and a semigroup of endomorphisms $\Gamma$ such that $N \cong C(\Gamma; G)$.

The structure of centralizer near-rings has been studied for various $G$'s and $\Gamma$’s, e.g. when $\Gamma = \mathcal{A}$ is a group of automorphisms of a finite group $G$ ([5]), or when $\Gamma$ is a finite ring with 1 and $G$ is a faithful, unital $\Gamma$-module ([6]). From a structure theorem due to Betsch [1] we have that a finite near-ring $N$, which is not a ring, is simple if and only if $N \cong C(\mathcal{A}; G)$ where $\mathcal{A}$ is a fixed point free group of automorphisms of a finite group $G$. (A group $\mathcal{A}$ of automorphisms is fixed point free if the identity map in $\mathcal{A}$ is the only element of $\mathcal{A}$ that fixes a nonidentity element of $G$.)

Since every finite simple nonring is of “$C(\mathcal{A}; G)$-type” it is natural to ask for which finite near-rings does there exist a finite group $G$ and a group of automorphisms $\mathcal{A}$ such that $N \cong C(\mathcal{A}; G)$, i.e. which finite near-rings are of $C(\mathcal{A}; G)$-type? In this paper we restrict our attention to the following more specific questions.

I. Which finite semisimple near-rings are of $C(\mathcal{A}; G)$-type?

II. Which finite rings are of $C(\mathcal{A}; G)$-type?

It will become clear in this paper that the “centralizer representation” problems I and II give rise to nontrivial group-theoretic, combinatoric problems.

In providing partial solutions to problems I and II we show that certain semisimple near-rings are not of $C(\mathcal{A}; G)$-type. Moreover
it is proven that the only possible rings of \( C(\mathcal{A}; G) \)-type are those that are direct sums of fields, but this is only a necessary condition. Information is obtained on which direct sums of fields are of \( C(\mathcal{A}; G) \)-type.

For definitions and basic results on near-rings the reader is referred to the book by Pilz [8]. A near-ring with 1 is simple if it has no nontrivial ideals. Since we are dealing exclusively with finite near-rings, we will regard a semi-simple near-ring as being one which is a direct sum of simple near-rings. For connections between our definition of semi-simplicity and near-ring radicals see [8], Chapters 4 and 5.

2. Rings of \( C(\mathcal{A}; G) \)-type. In this section we present results that characterize semisimple \( C(\mathcal{A}; G) \) near-rings. We also show that if a finite ring has a centralizer representation then this ring must be a direct sum of fields, a result that has been established independently by Zeller [10].

We begin by setting our notation and terminology. \( G \) will denote a finite group (normally written additively with identity 0) and \( \mathcal{A} \) a group of automorphisms of \( G \). For \( v \in G \), let \( C_{\mathcal{A}}(v) = \{ \alpha \in \mathcal{A} \mid \alpha v = v \} \), a subgroup of \( \mathcal{A} \), and let \( N(C_{\mathcal{A}}(v)) \) denote the normalizer of \( C_{\mathcal{A}}(v) \) in \( \mathcal{A} \). Also let \( C_0(C_{\mathcal{A}}(v)) = \{ v \in G \mid \alpha v = v \text{ for all } \alpha \in C_{\mathcal{A}}(v) \} \), a subgroup of \( G \). Finally for \( v \in G^* = G - \{0\} \) let \( \theta(v) = \{ \alpha v \mid \alpha \in \mathcal{A} \} \), the orbit of \( G^* \) determined by \( v \) under \( \mathcal{A} \).

The set \( \mathcal{S} = \{ C_{\mathcal{A}}(v) \mid v \in G^* \} \) is partially ordered by inclusion, and we say \( C_{\mathcal{A}}(v) \) is maximal if it is maximal in \( \mathcal{S} \). The following theorem appears in [5], but since it and its proof are basic to this paper we include it here for completeness.

**Theorem 1.** Let \( \mathcal{A} \) be a group of automorphisms of a finite group \( G \). The following are equivalent.

1. \( C(\mathcal{A}; G) \) is semi-simple.
2. Every element in \( \mathcal{S} \) is maximal.
3. The collection, \( \{ C_0(C_{\mathcal{A}}(v)) \mid v \in G^* \} \), of subgroups partitions \( G \).

**Proof.** Suppose \( C(\mathcal{A}; G) \) is semisimple and there exist elements \( u, v \in G^* \) with \( C_{\mathcal{A}}(v) \) properly contained in \( C_{\mathcal{A}}(u) \). Let

\[
M = \{ f \in C(\mathcal{A}; G) \mid C_{\mathcal{A}}(v) \subseteq C_{\mathcal{A}}(f(u)) \quad \text{and} \quad f \text{ is zero off } \theta(u) \}.
\]

Then \( M \) is a nonzero nilpotent \( C(\mathcal{A}; G) \)-subgroup and \( C(\mathcal{A}; G) \) is not semi-simple.

Suppose condition 2 holds, then if \( u \notin C_0(C_{\mathcal{A}}(v)), C_0(C_{\mathcal{A}}(v)) \cap C_0(C_{\mathcal{A}}(u)) = \{0\} \). So \( G \) is partitioned by the desired subgroups.
Assume now that condition 3 holds. For $v \in G^*$ let $T(v) = \cup \{ \theta(w) | C_{\mathcal{A}}(w) = C_{\mathcal{A}}(v) \}$, and let $M(v) = \{ f \in C(\mathcal{A}; G) | f \text{ is zero off } T(v) \}$. $M(v)$ is an ideal of $C(\mathcal{A}; G)$. We may select elements $v_1, \ldots, v_t \in G^*$ such that $G = T(v_1) \cup \cdots \cup T(v_t) \cup \{0\}$, a disjoint union. We have $C(\mathcal{A}; G) = M(v_1) \oplus \cdots \oplus M(v_t)$, a direct sum of ideals $M(v_i)$. It remains to show that each $M(v_i)$ is simple. For each $i$ let $\mathcal{A}_i = N(\mathcal{A}/(v_i))/\mathcal{A}$. Then $\mathcal{A}_i$ can be regarded as a group of automorphisms on $H_i = C(\mathcal{A}/(v_i))$ by defining $\beta w = \beta w$ for all $w \in H_i$, $\beta \in \mathcal{A}_i$. Moreover $M(v_i) \cong C(\mathcal{A}_i; H_i)$, and since $\mathcal{A}$ acts fixed point free on $H_i$, $C(\mathcal{A}_i; H_i)$ is a simple near-ring. So $C(\mathcal{A}; G)$ is semi-simple.

When $C(\mathcal{A}; G)$ is semi-simple the proof of Theorem 1 establishes that $C(\mathcal{A}; G)$ is a direct sum of simple near-rings of $C(\mathcal{A}; G)$-type. We record this in the following corollary.

**Corollary 1.** $C(\mathcal{A}; G)$ is semi-simple if and only if there exist elements $v_1, v_2, \ldots, v_t \in G^*$ with corresponding subgroups $H_1 \equiv C(\mathcal{A}/(v_1))$ of $G$ such that for every $i$, $\mathcal{A}_i \equiv N(\mathcal{A}/(v_i))/\mathcal{A}(v_i)$ acts fixed point free on $H_i$, and

$$C(\mathcal{A}; G) \cong C(\mathcal{A}_1; H_1) \oplus \cdots \oplus C(\mathcal{A}_t; H_t).$$

**Proposition 1.** Assume $C(\mathcal{A}; G)$ is simple. Then $C(\mathcal{A}; G)$ is a ring if and only if it is a field. Moreover every field is a near-ring of $C(\mathcal{A}; G)$-type.

**Proof.** Assume $C(\mathcal{A}; G)$ is a ring and suppose $\theta_1$ and $\theta_2$ are distinct orbits in $G^*$. Since $C(\mathcal{A}; G)$ is simple there exist elements $v_i \in \theta_i$ such that $C_{\mathcal{A}}(v_i) = C_{\mathcal{A}}(v_j)$. Let $e_{ij} : G \to G$, $i, j = 1, 2$ be defined by

$$e_{ij}(\alpha v_i) = \delta_{ij} \alpha v_i \quad \alpha \in \mathcal{A},
$$

$$e_{ij}(x) = 0 \quad x \in \theta_1 \cup \theta_2.$$

Then $e_{ij} \in C(\mathcal{A}; G)$. But $e_{12}(e_{12} + e_{22}) \neq e_{12}e_{12} + e_{12}e_{22}$ and $C(\mathcal{A}; G)$ is not a ring. So $G^*$ is an orbit and $C(\mathcal{A}; G)$ is a field.

If $F$ is a finite field, let $G = (F, +)$ and let $\mathcal{A} = F^*$, regarded as acting on $G$ by left multiplication. Then $F \cong C(\mathcal{A}; G)$.

**Theorem 2.** $C(\mathcal{A}; G)$ is a ring if and only if $C(\mathcal{A}; G)$ is a direct sum of fields.

**Proof.** Assume $C(\mathcal{A}; G)$ is a ring. We show first that $C(\mathcal{A}; G)$ is semisimple. Assume not; then there exist orbits $\theta_i(v_1), \theta_i(v_2)$ of $G^*$
such that $C_\omega(v_1) \cong C_\omega(v_2)$. If $e_{ij}$, $i = 1, 2$, $j = 1, 2$ are defined as above then $e_{11}, e_{22}, e_{21} \in C(\mathcal{A}; G)$, and $e_{23}(e_{11} + e_{12}) \neq e_{22}e_{11} + e_{22}e_{12}$. 

So $C(\mathcal{A}; G)$ is semi-simple and $C(\mathcal{A}; G) \cong C(\mathcal{A}_1; H_1) \oplus \cdots \oplus C(\mathcal{A}_n; H_n)$ as in the corollary to Theorem 1. This means each $C(\mathcal{A}_i; H_i)$ is a ring, and by Proposition 1 must be a field.

As a result of the arguments above we have the following structural result.

**Corollary 2.** If $N$ is a finite semi-simple near-ring with $N = S_1 \oplus \cdots \oplus S_t$ where each $S_t$ is simple, and if for some $j$, $S_j$ is a ring which is not a field, then $N$ is not of $C(\mathcal{A}; G)$-type.

3. **Centralizer representations of direct sums of fields.** From Theorem 2 the only time $C(\mathcal{A}; G)$ is a ring is when it is a direct sum of fields. Thus, it is natural to investigate the problem of when a direct sum of fields has a centralizer representation. We shall show that not all direct sums of fields are near-rings of $C(\mathcal{A}; G)$-type. For notation, let $GF(q)$ denote the finite field with $q$ elements where $q = p^t$ for some prime $p$. If $C(\mathcal{A}; G)$ is direct sum of fields then from Corollary 1 we have

$$C(\mathcal{A}; G) \cong C(\mathcal{A}_1; H_1) \oplus \cdots \oplus C(\mathcal{A}_n; H_n)$$

where each $C(\mathcal{A}_i; H_i)$ is a finite field. From Theorem 1 and its proof, and from Corollary 1, we have the following necessary and sufficient conditions for $GF(q_1) \oplus \cdots \oplus GF(q_t)$, $q_i = p_i^t$, to be a near-ring of $C(\mathcal{A}; G)$-type:

(i) There exists a finite group $G$ and a group of automorphisms $\mathcal{A}$ such that any one of the conditions of Theorem 1 is satisfied.

(ii) $G^*$ has exactly $t$ orbits under $\mathcal{A}$.

(iii) Every nonzero element in $G$ has prime order.

(iv) If $v, v' \in G^*$ belong to different orbits then $C_\omega(v)$ and $C_\omega(v')$ are not conjugate subgroups of $\mathcal{A}$.

(v) There exist elements $v_1, \ldots, v_t \in G^*$, no two in the same orbit, such that for each $i$, $N(C_\omega(v_i))/C_\omega(v_i) \cong GF(q_i)^*$. 

The following group theoretic result indicates that property (iii) places a rather strong restriction on the structure of the group $G$. The theorem is certainly known but we are not aware of any explicit reference in the literature so, for the reader's convenience, we have included a proof that is, for the most part, elementary.

**Theorem 3.** Let $G$ be a finite group such that every non-identity element of $G$ has prime order. Then one of the following holds:

(a) $G$ is a $p$-group of exponent $p$ for some prime $p$,

(b) $G$ is a Frobenius group with kernel of order $p^a$ and com-
(c) $G$ is isomorphic to $A_5$, the alternating group on five elements.

Proof Case 1. Assume $G$ is solvable and not a $p$-group. Then every minimal normal subgroup of $G$ is abelian ([4], page 23), so the Fitting subgroup $F(G)$ is nontrivial. The nilpotent group $F(G)$ must be a $p$-group for some prime $p$, for otherwise if $x$ and $y$ in $F(G)$ have distinct prime orders, $xy = yx$ has composite order. Let $G = G/F(G)$, and let $V = F(G)/\Phi(F(G))$, the Frattini factor group of $F(G)$. $V$ is a vector space over $GF(p)$ ([4], page 174, Theorem 1.3) and $G$ acts faithfully by conjugation as a group of linear transformations on $V$ ([4], page 229, Theorem 3.4).

Let $\bar{N} = N/F(G)$ be a minimal normal subgroup of $\bar{G}$, so $\bar{N}$ is an elementary abelian $q$-group for some prime $q \neq p$. Since all elements of $G$ have prime order, $\bar{N}$ acts fixed point freely on $V$. By Theorem 3.3, page 69 of [4] we have $|\bar{N}| = q$. It suffices now to prove $G = \bar{N}$.

Suppose $G \neq \bar{N}$ and let $\bar{M}/\bar{N}$ be a subgroup of prime order $r$ in $\bar{G}/\bar{N}$. Now $r \neq q$ for if so, then $\bar{M}$ would be elementary abelian of order $q^r$, which is not allowed by Theorem 3.3 of [4]. $\bar{M}$ must be a Frobenius group, so let $\bar{M} = \bar{N}\langle x \rangle$, where $x$ has order $r$.

Regarding $\bar{M}$ as a set of linear transformations on $V$, we see that $\sum_{n \in \bar{N}} n$ maps $V$ into $C_V(\bar{N}) = 1$, so $\sum n = 0$. Similarly, $\sum_{m \in \bar{M}} m = 0$. Since $\bar{M}^*$ is partitioned by $\bar{N}^*$ and the $q$ conjugates of $\langle x \rangle^*$ then

$$0 = \sum_{m \in \bar{M}} m = \sum_{n \in \bar{N}} n + \sum_{g} (x + x^g + \cdots + x^{r-1})^g$$

$$= 0 + \sum_{g} \left[ \sum_{i=0}^{r-1} x^i \right]^g - q^r.$$ 

Therefore $\sum_{i=0}^{r-1} x^i \neq 0$.

Let $v \in V^*$ such that $v^r \neq 1$ where $y = \sum_{i=0}^{r-1} x^i$. If $r = p$ then $v^p = vv^p \cdots v^{p^{p-1}} = v(x^{-i}vx)(x^{-2}vx)\cdots(x^{-i(p-1)}vx^{p-1}) = (vx^{-1})^p \neq 1$. So $vx^{-1}$ has order at least $p^2$ in the $p$-group $\langle x \rangle V$, impossible. On the other hand, if $r \neq p$, the fact that $x$ does not satisfy the polynomial $1 + \alpha + \cdots + \alpha^{r-1} = (\alpha^r - 1)/(\alpha - 1)$, but does satisfy $\alpha - 1$ means that $1$ is an eigenvalue for $x$ on $V$. Then $x^{-1}wx = w^r = w$ for some $w \in V^*$, so $wx$ has order $pr$, also impossible. Hence $G = \bar{N}$.

Case 2. Assume $G$ is not solvable. Then $G$ has even order by the Feit-Thompson theorem. Let $S$ be a Sylow 2-subgroup of $G$. Every element of $S^*$ has order 2 so $S$ is abelian. This means for every $x \in S^*$ we have $S \subseteq C(x)$ where $C(x)$ is the centralizer of $x$. On the other hand $C(x)$ is a 2-group if $x \in S^*$, otherwise $G$ has elements of composite order. Hence $C(x) = S$ for every $x \in X^*$. 
If \(|S| = 2\) then \(G\) has a normal 2-complement (see e.g. [4], Theorem 7.6.1, page 257) which implies \(G\) is solvable. Hence we may assume \(|S| > 2\). By a result of Brauer-Suzuki-Wall ([2], or for a more elementary reference see [3]), either \(S\) is a normal subgroup of \(G\) or else \(G\) isomorphic to \(SL(2, 2^n)\) where \(|S| = 2^n\). In the former situation, \(G/S\) has odd order so it is solvable. Then \(G\) is solvable, contradiction. Thus \(G\) is isomorphic to \(SL(2, 2^n)\) for some \(n \geq 2\). Since \(SL(2, 2^n)\) contains cyclic subgroups of order \(2^n - 1\) and \(2^n + 1\) ([4], Theorem 8.3 page 42) then \(2^n - 1\) and \(2^n + 1\) must be primes. But \(2^n - 1\) prime implies \(n\) is prime, and \(2^n + 1\) prime implies \(n\) is a power of 2. Hence \(n = 2\) and \(G\) is isomorphic to \(SL(2, 4) \cong A_5\).

**Remark.** By invoking a deep result of Suzuki on partitioned groups [9], the following stronger result can be proved: If the near-ring \(C(\mathcal{A}; G)\) is semi-simple and \(F(G) = 1\), then \(G \cong SL(2, 2^n)\) for some \(n\).

**Corollary 3.** Assume \(C(\mathcal{A}; G)\) is a direct sum of fields \(F_i, i = 1, \ldots, n\). Let \(S = \{p_i | p_i \text{ is the characteristic of } F_i\}\). Then

(i) \(|S| \leq 3\),

(ii) if \(|S| = 3\) then \(C(\mathcal{A}; G) \cong GF(2) \oplus GF(3) \oplus GF(5)\) where \(G \cong A_5\) and \(\mathcal{A} = \text{Aut}(G)\),

(iii) if \(|S| = 2\), then for some \(q \in S\), all components \(F_i\) of \(C(\mathcal{A}; G)\) with characteristic \(q\) are isomorphic to \(GF(q)\).

**Proof.** Part (i) is immediate from Theorem 3. For part (ii) we have \(G \cong A_5\) due to Theorem 3 and the remarks preceding it. If \(\mathcal{A} = \text{Aut}(A_5)\) then \(\Phi \in \mathcal{A}\) has the form \(\Phi(x) = yxy^{-1}\) where \(y\) is a fixed element in \(S_5\). Hence \(A_5\) has three nontrivial orbits, one for each type of cycle structure. We have

\[
\begin{align*}
C_0(C_{\mathcal{A}}(123)) &= \langle(123)\rangle \cong Z_3 \\
C_0(C_{\mathcal{A}}(12)(34)) &= \langle(12)(34)\rangle \cong Z_2 \\
C_0(C_{\mathcal{A}}(12345)) &= \langle(12345)\rangle \cong Z_6
\end{align*}
\]

Computations show that

\[
N(C_{\mathcal{A}}(123))/C_{\mathcal{A}}(123) \cong Z_3, \quad N(C_{\mathcal{A}}(12)(34))/C_{\mathcal{A}}(12)(34) \cong \{1\}
\]

and \(N(C_{\mathcal{A}}(12345))/C_{\mathcal{A}}(12345) \cong Z_4\). Hence \(C(\mathcal{A}; G) \cong GF(2) \oplus GF(3) \oplus GF(5)\).

It remains to show that no other group \(\mathcal{A}\) of automorphisms of \(G = A_5\) gives rise to a near-ring which is a direct sum of fields. We may assume \(\mathcal{A} \subseteq S_5\) where \(\mathcal{A}\) acts on \(A_5\) by conjugation. If \(x\) is a 5-cycle then \(x \in A_5\) and \(C_{\mathcal{A}}(x)\) is a subgroup of \(\langle x \rangle\). Since
ON SEMISIMPLE RINGS THAT ARE CENTRALIZER NEAR-RINGS

Let $A$ be semisimple we must have $G^x = \langle x \rangle$. Thus $\mathcal{A}$ contains all 5-cycles in $S_5$. Since the set of 5-cycles generates a normal subgroup of $A_5$, and $A_5$ is simple, we have $A_5 \subseteq \mathcal{A}$. Thus $\mathcal{A} = A_5$. The near ring $C(A_5; A_5)$ is semi-simple but is not a direct sum of fields. So we have $\mathcal{A} = S_5$.

Part (iii) follows from the fact that in part b) of Theorem 3, a Sylow $q$-subgroup of $G$ has order $q$.

The preceding theorem places a restriction on which direct sums of fields can be realized as a centralizer near-ring. The following two theorems give more information about when a direct sum of two fields with different characteristics is a centralizer near-ring.

**Theorem 4.** Let $G$ be a finite group and $\mathcal{A}$ a subgroup of $\text{Aut}(G)$ such that $\mathcal{A}$ has exactly two orbits in $G^*$. If $G$ does not have prime power order, then for distinct primes $p$ and $q$

(i) $G$ is a Frobenius group $[V]Q$, with $V$ an elementary abelian normal subgroup of order $p^r$ and $Q$ a cyclic group of order $q$, and

(ii) $p$ is a generator of $GF(q)^*$.

**Proof.** Since $G$ is not a $p$-group there exist distinct primes $p$ and $q$ such that the two orbits consist of the elements of order $p$ and the elements of order $q$ respectively. By Theorem 3, $G$ is a Frobenius group with a $p$-group $V$ as kernel and with a complement $Q$ of order $q$. Since $V$ is characteristic in $G$, the center of $V$ is $\mathcal{A}$-invariant so the transitivity of $\mathcal{A}$ on elements of order $p$ implies that $V$ is abelian. This proves (i).

If $\alpha \in \mathcal{A}$, $Q^\alpha$ is a Sylow $q$-subgroup of $G$ so $Q^\alpha = g^{-1}Qg$ for some $g \in G$. Since $G = VQ = QV$, $g$ can be selected to be in $V$ so $Q^\alpha = v^{-1}Qv = Q^\alpha$ where $v$ is the inner automorphism of $G$ induced by $v$. So $\alpha v^{-1} \in N_{\text{Aut}(G)}(Q) = N$ and $\alpha \in N_i$. We now have $\mathcal{A} \subseteq NI$ where $I_i$ is the group of inner automorphisms of $G$ induced by elements of $V$. Since $V$ is a characteristic subgroup of $G$ then $I_i$ is normal in $\text{Aut}(G)$ so $NI = I_iN$.

Since $\mathcal{A}$ acts transitively on $V^*$ so does $N$. We claim $N$ is also transitive on $Q^*$. For if $x, y \in Q^*$ then $x^\alpha = y$ for some $\alpha \in \mathcal{A}$. Writing $\alpha = v^n$ where $v \in V$, $n \in N$, we have $x^{v^n} = y$, so $x^{v^n} = y^{v^{-1}} \in Q^{v^{-1}} = Q$. Hence $x^{v^{-1}v^{-1}xv} = x^{-1}x^{v^n} \in Q$. On the other hand, since $V$ is normal in $G$, $x^{-1}v^{-1}xv \in V$, so $x^{-1}v^{-1}xv \in Q \cap V = \{1\}$. Therefore $x^{v^n} = x$ and $x^n = x^{v^n} = y$.

$Q$ acts faithfully on $V$ so we may let $Q = \langle T \rangle$ where $T$ is a linear transformation on $V$ regarded as a vector space over $GF(p)$. Suppose $W$ is an irreducible $Q$-submodule of $V$. Since $Q$ is invariant under $N$, $W^*$ is an irreducible $Q$-submodule for every $n \in N$. The
transitivity of $N$ on $V^*$ implies that every element of $V^*$ belongs to some irreducible $Q$-submodule $V$ and hence for every $v \in V^*$ there exists an irreducible polynomial (over $GF(p)$), $f_v(x)$, such that $f_v(T)v = 0$. If $v, w \in V^*$ then $f_v(T)f_w(T)(v + w) = 0$ so $f_{v+w}(x)$ divides $f_v(x)f_w(x)$. Hence we may assume $f_{v+w}(x) = f_v(x)$, implying $f_v(T)w = 0$ so $f_v(x) = f_w(x)$. Hence $f_v(x) = f_w(x)$ for all $v, w \in V^*$ and the minimal polynomial $f(x)$ of $T$ on $V$ is irreducible.

Since $T^q = I$, $f(x)$ divides $x^q - 1 = (x - 1)c(x)$ where $c(x) = x^{q-1} + \cdots + x + 1$. Since $T$ fixes no element of $V^*$, $f(x)$ divides $c(x)$. On the other hand if $\alpha$ is an eigenvalue of $T$ in some extension field of $GF(p)$ then the transitivity of $N$ on $Q^*$ implies $T$ is similar in $GL(V)$ to $T^\sigma$ for every $\sigma$ with $1 \leq k \leq q - 1$, so $\alpha^k$ is an eigenvalue for $T$ for every such $k$. Hence, all $q$th roots of $1$ (except 1) are eigenvalues for $T$ and thus roots of $f(x)$. It follows that $f(x) = x^{q-1} + \cdots + x + 1 = c(x)$ and $c(x)$ is irreducible over $GF(p)$. Therefore any extension of $GF(p)$ containing a $q$th root of $1$ has degree at least $q - 1$. Since $GF(p^n)$ contains a $q$th root of $1$ precisely when $q$ divides $|GF(p^n)| = p^n - 1$, this means that $p^{q-1}$ is the smallest power of $p$ which is congruent to $1$ modulo $q$. In other words, $p$ generates $GF(q)^*$. As an application of this group theoretic property we obtain the following centralizer representation result, the "if" part being established by Theorem 5 below.

**Corollary 4.** Let $p$ and $q$ be distinct primes. There is a group $G$ and a subgroup $\mathcal{A}$ of $Aut G$ such that $C(\mathcal{A}; G) \cong GF(p) \oplus GF(q)$ if and only if either $p$ generates $GF(q)^*$ or $q$ generates $GF(p)^*$.

Corollary 4 partially generalizes to the case in which $p^n$ generates $GF(q)^*$. This is given in the next theorem.

**Theorem 5.** Suppose $p$ and $q$ are distinct prime such that $p^n$ is a generator of $GF(q)^*$. Then there exists a group $G$ and a subgroup $\mathcal{A}$ of $Aut G$ such that $C(\mathcal{A}; G) \cong GF(p^n) \oplus GF(q)$.

**Proof.** Let $m$ be any integer divisible by $n(q - 1)$ and let $V = GF(p^n)$ considered as a vector space over $GF(p)$. Since $n$ divides $m$ we have $GF(p^n) \subseteq GF(p^m)$ and the Galois group $B = Gal(GF(p^m)/GF(p^n))$ is cyclic, generated by the automorphism $\vartheta: \alpha \to \alpha^n$, $\alpha \in GF(p^n)$.

For every $\alpha \in GF(p^n)^*$ and $\sigma \in B$ define the $GF(p^n)$-linear transformation $T_{\alpha, \sigma}$ of $V$ by $vT_{\alpha, \sigma} = \alpha v^\sigma$. Let $T = \{T_{\alpha, \sigma} | \alpha \in GF(p^n)^*, \sigma \in B\}$ and $M = \{T_{\alpha, \sigma} | \alpha \in GF(p^n)^*\}$. The set $T$ forms a group where $T_{\alpha, \sigma}T_{\beta, \delta} = T_{\sigma, \alpha}^{-1}T_{\beta, \delta}$, and $M \subseteq T$ with $M \cong GF(p^n)^*$ which is cyclic. Also, let $H = \{T_{\alpha, \sigma} | \sigma \in B\}$, a subgroup of $T$ isomorphic to $B$. We have $M \cap H = \{1\}$ and $T = MH$. 


Since \( q - 1 \) divides \( m \) then \( q \) divides \( p^m - 1 \). But \( M \) is cyclic of order \( p^m - 1 \) so \( M \) contains a characteristic subgroup \( Q \) of order \( q \). Also \( Q \) is normal in \( T \). Let \( G \) be the semidirect product \([V]Q\) so \( G \) is a Frobenius group and is a normal subgroup of the semidirect product \( A = [V]T \). We have \( C_A(G) \subseteq C_A(V) = \{1\} \), so \( A \) acts faithfully on \( G \) by conjugation as a group of automorphisms.

Since \( \theta: \alpha \rightarrow \alpha^p \) generates \( B \), the fact that \( p^m \) is a generator of \( GF(q)^* \) implies that the powers \( 1, p^m, p^{2m}, \ldots \) of \( p \) are congruent modulo \( q \) to the integers \( 1, 2, 3, \ldots, q - 1 \) (in some order) and hence, that \( H \) is transitive on \( Q^* \). Since \( G \subseteq A \) and since all Sylow \( q \)-subgroups of \( G \) are conjugate in \( G \), it follows \( A \) is transitive on elements of order \( q \). \( A \) is also transitive on elements of order \( p \) in \( G \) (i.e., on \( V^* \)), since \( M \) is. \( G \) is a Frobenius group so all its elements have order \( p \) or \( q \) (otherwise some nontrivial element of order \( q \) would centralize an element of order \( p \)). Thus, \( A \) has precisely two orbits in \( G \), of sizes \( |V^*| = p^m - 1 \) and \( |G| - |V| = p^mq - p^m = p^m(q - 1) \).

If \( v_0 \in V^* \) and \( x_o \in Q^* \), then \( V \subseteq C_A(v_o), C_A(x_o) = \{0\}, Q \subseteq C_A(x_o) \) and \( C_A(v_o) = \{1\} \). Hence, stabilizers in \( A \) of elements of \( G \) are incomparable and \( C(A; G) \) is semi-simple by Theorem 1. Also, if \( H_1 = \{x \in G | C_A(x) = C_A(x_o) = C_A(C_A(x_o)) \) and \( H_2 = C_O(C_A(v_o)) \), then \( C(A; G) \cong C(A_1; H_1) \oplus C(A_2; H_2) \) where \( A_1 = N_A(C_A(x_o))/C_A(x_o) \) and \( A_2 = N_A(C_A(v_o))/C_A(v_o) \).

Since \( x_o \in H_1 \) and the Sylow \( q \)-subgroups of \( G \) have order \( q \), \( H_i = Q \). Since \( A \) is transitive on \( Q^* \), so also is \( A_i \). Since \( Aut Q \) is abelian, \( A_i \) is abelian and \( C(A_i; H_i) \cong GF(q) \).

It remains to show that \( C(A_i; H_i) \cong GF(p^m) \). First we claim \( H_i \) is a \( n \)-dimensional subspace of \( V \). For this we may assume \( v_o \in GF(p^m) \subseteq GF(p^m) = V \) (since \( A \) is transitive on \( V^* \)), so \( H \subseteq C_A(v_o) \), and \( H_2 = C_O(C_A(v_o)) \subseteq C_O(H) = GF(p^m) \). On the other hand, the stabilizer in \( A \) of any element of \( GF(p^m)^* \) is \( VH \) since no element of \( M^* \) fixes an element of \( V^* \). So \( GF(p^m) \subseteq H_i \). Hence \( H_i = GF(p^m) \) if \( v_o \in GF(p^m) \) proving the claim.

Now \( A_i \) is transitive on \( H_i \) since \( A \) is, so \( C(A_i; H_i) \) is a near-field of order \( p^m \). But if \( v_o \in GF(p^m) \) we have \( C_A(v_o) = VH \) so \( A_2 = N_A(VH)/VH = VHN_M(VH)/VH \cong N_M(VH) \) using the facts that \( A = VMH \) and \( VH \cap M = \{1\} \). Since \( M \) is abelian, \( A_2 \) is abelian and \( C(A_2; H_2) \cong GF(p^m) \).

Note that, by Corollary 3, (iii), a proof of the converse of Theorem 5 would completely classify those near-rings of \( C(\mathcal{F}; G) \)-type which are a direct sum of two fields of different characteristic.

In our final representation theorem we show that a direct sum of a tower of finite fields can be obtained as a centralizer near-ring.
THEOREM 6. Let $F_i \subseteq F_2 \subseteq \cdots \subseteq F_t$ be fields. Then there exists a vector space $V$ over $F_i$ and a group $\mathcal{A}$ of linear transformations on $V$ such that $C(\mathcal{A}; V) \cong F_i \oplus F_2 \oplus \cdots \oplus F_t$.

Proof. Let $F_i = GF(p^{n_i})$, $i = 1, 2, \ldots, t$. Then $n_i$ divides $n_{i+1}$. We construct the vector space $V$ as follows. Let $W_i$ be a (finite dimensional) vector space over $F_i$, let $W_{i-1}$ be any vector space over $F_{i-1}$ that contains $W_i$ as a proper subspace, let $W_{i-2}$ be any vector space over $F_{i-2}$ that contains $W_{i-1}$ as a proper subspace, etc. Hence $W_i \subset W_{i-1} \subset \cdots \subset W_2 \subset W_1 = V$, where each containment is proper and $W_i$ is a vector space over $F_i$. Let $\mathcal{A}$ be the set of invertible $F_i$-linear transformations on $V$ defined as follows: $A \in \mathcal{A}$ if and only if for each $i$, $W_i$ is $A$-invariant and $A$ restricted to $W_i$ is $F_i$-linear.

We claim that $C(\mathcal{A}; V) \cong F_i \oplus \cdots \oplus F_t$. It is clear that $V^*$ has $t$ orbits under $\mathcal{A}$, namely $W_1^*$, $W_{i-1} - W_i$, $\cdots$, $W_1 - W_t$. If $v_i \in W_i - W_{i+1}$ then $C_r(C_\mathcal{A}(v_i)) = F_i v_i$. Let $\mathcal{A} = N_\mathcal{A}(C_\mathcal{A}(v_i))$. If $S \in \mathcal{A}$ and $A \in C_\mathcal{A}(v_i)$ then $S^{-1}ASv_i = v_i$, that is $ASv_i = Sv_i$. Hence $Sv_i \in C_r(C_\mathcal{A}(v_i))$ meaning $Sv_i = \alpha v_i$ for some $\alpha \in F_i^*$. This implies $\mathcal{A}n_{\mathcal{A}}(v_i) = \mathcal{A}/C_\mathcal{A}(v_i)$ is isomorphic to $F_i^*$. This implies

$$C(\mathcal{A}; V) \cong C(F_i^*; F_i v_i) \oplus \cdots \oplus C(F_t^*; F_t v_i) \cong F_i \oplus \cdots \oplus F_t.$$

We conclude this section (and the paper) with a couple of open problems relative to representing $C(\mathcal{A}; G)$ as the direct sum of two fields. The first question concerns the converse of Theorem 5 while the second question deals with the theorem above.

Problem 1. If $C(\mathcal{A}, G) \cong GF(p^n) \oplus GF(q)$, is $p^n$ a generator of $GF(q)^*$?

Problem 2. If $C(\mathcal{A}, G) \cong GF(p^n) \oplus GF(p^k)$ and $a < b$, does $a$ divide $b$?

REFERENCES


Received September 1, 1979.

Texas A & M University
College Station, TX 77843
Jean Bourgain, A Hausdorff-Young inequality for $B$-convex Banach spaces ................................................................. 255
J. L. Brenner and Lorraine L. Foster, Exponential Diophantine equations ................................................................. 263
Henry H. Glover and William Duncan Homer, II, Fixed points on flag manifolds ................................................................. 303
Lothar Hahn, A note on stochastic methods in connection with approximation theorems for positive linear operators ................. 307
James P. Henderson, Approximating cellular maps between low-dimensional polyhedra ......................................................... 321
V. K. Jain, Certain transformations of basic hypergeometric series and their applications ......................................................... 333
Charles David Keys, On the decomposition of reducible principal series representations of $p$-adic Chevalley groups .................. 351
M. S. Klamkin and A. Meir, Ptolemy’s inequality, chordal metric, multiplicative metric ......................................................... 389
Robert F. Lax, Independence of normal Weierstrass points under deformation ................................................................. 393
Leonid A. Luxemburg, On compactifications of metric spaces with transfinite dimensions ......................................................... 399
Carlton James Maxson, Martin Ross Pettet and Kirby C. Smith, On semisimple rings that are centralizer near-rings ......................... 451
Teodor C. Przymusiński, Extending functions from products with a metric factor and absolutes ......................................................... 463
Giorgio Talenti, A note on the Gauss curvature of harmonic and minimal surfaces ................................................................. 477
D. M. Terlinden, A spectral containment theorem analogous to the semigroup theory result $e^{t\sigma(A)} \subseteq \sigma(e^{tA})$ ......................... 493