Pacific Journal of Mathematics

ON SEMISIMPLE RINGS THAT ARE CENTRALIZER NEAR-RINGS

Carlton James Maxson, Martin Ross Pettet and Kirby C. Smith

Vol. 101, No. 2 December 1982

PACIFIC JOURNAL OF MATHEMATICS
Vol. 101, No. 2, 1982

ON SEMISIMPLE RINGS THAT ARE CENTRALIZER NEAR-RINGS

CARLTON J. MAXSON, MARTIN R. PETTET AND KIRBY C. SMITH

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

1. Introduction. Let G be a finite group and let Γ denote a semigroup of endomorphisms of G. The set of functions $C(\Gamma; G) = \{f: G \to G \mid f(0) = 0$ and $f(\gamma v) = \gamma f(v)$ 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 Γ such that $N \cong C(\Gamma; G)$.

The structure of centralizer near-rings has been studied for various G's and Γ's, e.g. when $\Gamma = \mathscr{A}$ is a group of automorphisms of a finite group G ([5]), or when Γ is a finite ring with 1 and G is a faithful, unital Γ-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 $N \cong C(\mathscr{A}; G)$ where $\mathscr{A}$ is a fixed point free group of automorphisms of a finite group G. (A group $\mathscr{A}$ of automorphisms is fixed point free if the identity map in $\mathscr{A}$ is the only element of $\mathscr{A}$ that fixes a nonidentity element of G.)

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

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

II. Which finite rings are of $C(\mathscr{A}; G)$-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 $C(\mathscr{A}; G)$-type. Moreover it is proven that the only possible rings of $C(\mathscr{A}; G)$-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 $C(\mathscr{A}; G)$-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 $C(\mathscr{A}; G)$-type. In this section we present results that characterize semisimple $C(\mathscr{A}; G)$ 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 $\mathscr{A}$ a group of automorphisms of G. For $v_0 \in G$, let $C_{\mathscr{A}}(v_0) = \{\alpha \in \mathscr{A} \mid \alpha v_0 = v_0\}$, a subgroup of $\mathscr{A}$, and let $N(C_{\mathscr{A}}(v_0))$ denote the normalizer of $C_{\mathscr{A}}(v_0)$ in $\mathscr{A}$. Also let $C_G(C_{\mathscr{A}}(v_0)) = \{v \in G \mid \alpha v = v \text{ for all } \alpha \in C_{\mathscr{A}}(v_0)\}$, a subgroup of G. Finally for $v \in G^* \equiv G - \{0\}$ let $\theta(v) = \{\alpha v \mid \alpha \in \mathscr{A}\}$, the orbit of G^* determined by v under $\mathscr{A}$.

The set $\mathscr{S} = \{C_{\mathscr{A}}(v) \mid v \in G^*\}$ is partially ordered by inclusion, and we say $C_{\mathscr{A}}(v)$ is maximal if it is maximal in $\mathscr{S}$. 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 $\mathscr{A}$ be a group of automorphisms of a finite group G. The following are equivalent.*

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

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

$$M = \{f \in C(\mathscr{A}; G) \mid C_{\mathscr{A}}(v) \subseteqq C_{\mathscr{A}}(f(u)) \quad \text{and} \quad f \text{ is zero off } \theta(u)\} .$$

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

Suppose condition 2 holds, then if $u \notin C_G(C_{\mathscr{A}}(v))$, $C_G(C_{\mathscr{A}}(v)) \cap C_G(C_{\mathscr{A}}(u)) = \{0\}$. So G is partitioned by the desired subgroups.

Assume now that condition 3 holds. For $v \in G^*$ let $T(v) = \cup \{\theta(w) \mid C_{\mathscr{A}}(w) = C_{\mathscr{A}}(v))\}$, and let $M(v) = \{f \in C(\mathscr{A}; G) \mid f$ is zero off $T(v)\}$. $M(v)$ is an ideal of $C(\mathscr{A}; G)$. We may select elements $v_1, \cdots, v_t \in G^*$ such that $G = T(v_1) \cup \cdots \cup T(v_t) \cup \{0\}$, a disjoint union. We have $C(\mathscr{A}; G) = M(v_1) \oplus \cdots \oplus M(v_t)$, a direct sum of ideals $M(v_i)$. It remains to show that each $M(v_i)$ is simple. For each i let $\bar{\mathscr{A}_i} = N_{\mathscr{A}}\{C_{\mathscr{A}}(v_i))/C_{\mathscr{A}}(v_i)$. Then $\bar{\mathscr{A}_i}$ can be regarded as a group of automorphisms on $H_i = C_G(C_{\mathscr{A}}(v_i))$ by defining $\bar{\beta} w = \beta w$ for all $w \in H_i$, $\bar{\beta} \in \bar{\mathscr{A}_i}$. Moreover $M(v_i) \cong C(\bar{\mathscr{A}_i}; H_i)$, and since $\bar{\mathscr{A}_i}$ acts fixed point free on H_i, $C(\bar{\mathscr{A}_i}; H_i)$ is a simple near-ring. So $C(\mathscr{A}; G)$ is semisimple.

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

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

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

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

Proof. Assume $C(\mathscr{A}; G)$ is a ring and suppose θ_1 and θ_2 are distinct orbits in G^*. Since $C(\mathscr{A}; G)$ is simple there exist elements $v_i \in \theta_i$ such that $C_{\mathscr{A}}(v_1) = C_{\mathscr{A}}(v_2)$. Let $e_{ij}: G \to G$, $i, j = 1, 2$ be defined by

$$e_{ij}(\alpha v_k) = \delta_{jk} \alpha v_i \qquad \alpha \in \mathscr{A}$$
$$e_{ij}(x) = 0 \qquad x \notin \theta_1 \cup \theta_2 .$$

Then $e_{ij} \in C(\mathscr{A}; G)$. But $e_{11}(e_{12} + e_{22}) \neq e_{11}e_{12} + e_{11}e_{22}$ and $C(\mathscr{A}; G)$ is not a ring. So G^* is an orbit and $C(\mathscr{A}; G)$ is a field.

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

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

Proof. Assume $C(\mathscr{A}; G)$ is a ring. We show first that $C(\mathscr{A}; G)$ is semisimple. Assume not; then there exist orbits $\theta_1(v_1)$, $\theta_2(v_2)$ of G^*

such that $C_{\mathscr{A}}(v_1) \subsetneqq C_{\mathscr{A}}(v_2)$. If e_{ij}, $i = 1, 2$, $j = 1, 2$ are defined as above then $e_{11}, e_{22}, e_{21} \in C(\mathscr{A}; G)$, and $e_{22}(e_{21} + e_{11}) \neq e_{22}e_{21} + e_{22}e_{11}$.

So $C(\mathscr{A}; G)$ is semi-simple and $C(\mathscr{A}; G) \cong C(\bar{\mathscr{A}_1}; H_1) \oplus \cdots \oplus C(\bar{\mathscr{A}_t}; H_t)$ as in the corollary to Theorem 1. This means each $C(\bar{\mathscr{A}_i}; H_i)$ 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_i is simple, and if for some j, S_j is a ring which is not a field, then N is not of $C(\mathscr{A}; G)$-type.*

3. Centralizer representations of direct sums of fields. From Theorem 2 the only time $C(\mathscr{A}; G)$ 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 $C(\mathscr{A}; G)$-type. For notation, let $GF(q)$ denote the finite field with q elements where $q = p^t$ for some prime p. If $C(\mathscr{A}; G)$ is direct sum of fields then from Corollary 1 we have

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

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

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

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

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

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

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

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-*

plement of order q, where p and q are distinct primes,

(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 $\bar{G} = G/F(G)$, 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 $\bar{G}$ acts faithfully by conjugation as a group of linear transfoamations 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 $\bar{G} = \bar{N}$.

Suppose $\bar{G} \neq \bar{N}$ 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^2, 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

$$0 = \sum_{m \in M} m = \sum_{n \in N} n + \sum_{g} (x + x^2 + \cdots + x^{r-1})^g$$
$$= 0 + \sum_{g} \left[\sum_{i=0}^{r-1} x^i\right]^g - q^I .$$

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

Let $v \in V^*$ such that $v^y \neq 1$ where $y = \sum_{i=0}^{r-1} x^i$. If $r = p$ then $v^y = vv^x \cdots v^{x^{p-1}} = v(x^{-1}vx)(x^{-2}vx^2) \cdots (x^{-(p-1)}vx^{p-1}) = (vx^{-1})^p \neq 1$. 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 $\alpha^r - 1$ means that 1 is an eigenvalue for x on V. Then $x^{-1}wx = w^x = w$ for some $w \in V^*$, so wx has order pr, also impossible. Hence $\bar{G} = \bar{N}$.

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 $S \subseteqq C(x)$ 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 $n \geqq 2$. 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 $C(\mathscr{A}; G)$ is semi-simple and $F(G) = 1$, then $G \cong SL(2, 2^n)$ for some n.

COROLLARY 3. *Assume $C(\mathscr{A}; G)$ is a direct sum of fields F_i, $i = 1, \cdots, n$. Let $S = \{p_i \mid p_i$ is the characteristic of $F_i\}$. Then*

(i) $|S| \leqq 3$,

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

(iii) *if $|S| = 2$, then for some $q \in S$, all components F_i of $C(\mathscr{A}; G)$ 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 $\mathscr{A} = \mathrm{Aut}(A_5)$ then $\Phi \in \mathscr{A}$ 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

$$C_G(C_{\mathscr{A}}(123)) = \langle(123)\rangle \cong Z_3$$
$$C_G(C_{\mathscr{A}}(12)(34)) = \langle(12)(34)\rangle \cong Z_2$$
$$C_G(C_{\mathscr{A}}(12345)) = \langle(12345)\rangle \cong Z_5$$

Computations show that

$$N(C_{\mathscr{A}}(123))/C_{\mathscr{A}}(123) \cong Z_2,\ N(C_{\mathscr{A}}(12)(34)/C_{\mathscr{A}}(12)(34) \cong \{I\}$$

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

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

$C(\mathscr{A}; A_5)$ is semisimple we must have $C_{\mathscr{A}}(x) = \langle x \rangle$. Thus $\mathscr{A}$ 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 $A_5 \subseteqq \mathscr{A}$. Thus $\mathscr{A} = A_5$. The near ring $C(A_5; A_5)$ is semi-simple but is not a direct sum of fields. So we have $\mathscr{A} = S_5$.

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 $\mathscr{A}$ a subgroup of* $\operatorname{Aut} G$ *such that $\mathscr{A}$ 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^n 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 $\mathscr{A}$-invariant so the transitivity of $\mathscr{A}$ on elements of order p implies that V is abelian. This proves (i).

If $\alpha \in \mathscr{A}$, Q^α 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 $Q^\alpha = v^{-1}Qv = Q^{i_v}$ where i_v is the inner automorphism of G induced by v. So $\alpha i_v^{-1} \in N_{\operatorname{Aut} G}(Q) \equiv N$ and $\alpha \in N i_v$. We now have $\mathscr{A} \subseteqq NI_v$ where I_v is the group of inner automorphisms of G induced by elements of V. Since V is a characteristic subgroup of G then I_v is normal in $\operatorname{Aut} G$ so $NI_v = I_vN$.

Since $\mathscr{A}$ 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 $\alpha \in \mathscr{A}$. Writing $\alpha = i_v n$ where $v \in V$, $n \in N$, we have $x^{i_v n} = y$, so $x^{i_v} = y^{n^{-1}} \in Q^{n^{-1}} = Q$. Hence $x^{-1}v^{-1}xv = x^{-1}x^{i_v} \in Q$. 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 $x^{i_v} = x$ and $x^n = x^{i_v n} = y$.

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^n 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 α 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^k for every k with $1 \leqq k \leqq q-1$, so α^k is an eigenvalue for T for every such k. Hence, all qth 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 qth root of 1 has degree at least $q-1$. Since $GF(p^k)$ contains a qth root of 1 precisely when q divides $|GF(p^k)^*| = p^k - 1$, 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 $\mathscr{A}$ of* Aut G *such that $C(\mathscr{A}; G) \cong GF(p) \oplus GF(q)$ 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 $\mathscr{A}$ of* Aut G *such that $C(\mathscr{A}; G) \cong GF(p^n) \oplus GF(q)$.*

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

For every $\alpha \in GF(p^m)^*$ and $\sigma \in B$ define the $GF(p^n)$-linear transformation $T_{\sigma,\alpha}$ of V by $vT_{\sigma,\alpha} = \alpha v^\sigma$. Let $T = \{T_{\sigma,\alpha} \mid \alpha \in GF(p^m)^*, \sigma \in B\}$ and $M = \{T_{1,\alpha} \mid \alpha \in GF(p^m)^*\}$. The set T forms a group where $T_{\sigma,\alpha}T_{\tau,\beta} = T_{\sigma\tau,\alpha^\tau\beta}$, and $M \trianglelefteq T$ with $M \cong GF(p^m)^*$ which is cyclic. Also, let $H = \{T_{\sigma,1} \mid \sigma \in B\}$, 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 $\theta: \alpha \to \alpha^{p^n}$ generates B, the fact that p^n is a generator of $GF(q)^*$ implies that the powers $1, p^n, p^{2n}, \cdots$ of p^n are congruent modulo q to the integers $1, 2, 3, \cdots, q-1$ (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 $|G| - |V| = p^m q - p^m = p^m(q-1)$.

If $v_0 \in V^*$ and $x_0 \in Q^*$, then $V \subseteq C_A(v_0)$, $C_V(x_0) = \{0\}$, $Q \subseteq C_A(x_0)$ and $C_Q(v_0) = \{1\}$. Hence, stabilizers in A of elements of G are incomparable and $C(A; G)$ is semi-simple by Theorem 1. Also, if $H_1 = \{x \in G \mid C_A(x) = C_A(x_0)\} = C_G(C_A(x_0))$ and $H_2 = C_G(C_A(v_0))$, then $C(A; G) \cong C(A_1; H_1) \oplus C(A_2; H_2)$ where $A_1 = N_A(C_A(x_0))/C_A(x_0)$ and $A_2 = N_A(C_A v_0))/C_A(v_0)$.

Since $x_0 \in H_1$ and the Sylow q-subgroups of G have order q, $H_1 = Q$. Since A is transitive on Q^*, so also is A_1. Since Aut Q is abelian, A_1 is abelian and $C(A_1; H_1) \cong GF(q)$.

It remains to show that $C(A_2; H_2) \cong GF(p^n)$. First we claim H_2 is an n-dimensional subspace of V. For this we may assume $v_0 \in GF(p^n) \subseteq GF(p^m) = V$ (since A is transitive on V^*), so $H \subseteq C_A(v_0)$, and $H_2 = C_G(C_A(v_0)) \subseteq C_G(H) = GF(p^n)$. On the other hand, the stabilizer in A of any element of $GF(p^n)^*$ is VH since no element of M^* fixes an element of V^*. So $GF(p^n) \subseteq H_2$. Hence $H_2 = GF(p^n)$ if $v_0 \in GF(p^n)$ proving the claim.

Now A_2 is transitive on H_2 since A is, so $C(A_2; H_2)$ is a near-field of order p^n. But if $v_0 \in GF(p^n)$ we have $C_A(v_0) = VH$ 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 $C(A_2; H_2) \cong GF(p^n)$.

Note that, by Corollary 3, (iii), a proof of the converse of Theorem 5 would completely classify those near-rings of $C(\mathscr{A}; G)$-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 $F_1 \subseteqq F_2 \subseteqq \cdots \subseteqq F_t$ be fields. Then there exists a vector space V over F_1 and a group $\mathscr{A}$ of linear tranformations on V such that $C(\mathscr{A}; V) \cong F_1 \oplus F_2 \oplus \cdots \oplus F_t$.*

Proof. Let $F_i = GF(p^{n_i})$, $i = 1, 2, \cdots, t$. Then n_i divides n_{i+1}. We construct the vector space V as follows. Let W_t be a (finite dimensional) vector space over F_t, let W_{t-1} be any vector space over F_{t-1} that contains W_t as a proper subspace, let W_{t-2} be any vector space over F_{t-2} that contains W_{t-1} as a proper subspace, etc. Hence $W_t \subset W_{t-1} \subset \cdots \subset W_2 \subset W_1 \equiv V$, where each containment is proper and W_i is a vector space over F_i. Let $\mathscr{A}$ be the set of invertible F_1-linear transformations on V defined as follows: $A \in \mathscr{A}$ 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 $C(\mathscr{A}; V) \cong F_1 \oplus \cdots \oplus F_t$. It is clear that V^* has t orbits under $\mathscr{A}$, namely W_t^*, $W_{t-1} - W_t, \cdots, W_1 - W_2$. If $v_i \in W_i - W_{i+1}$ then $C_V(C_{\mathscr{A}}(v_i)) = F_i v_i$. Let $\mathscr{A}_i = N_{\mathscr{A}}(C_{\mathscr{A}}(v_i))$. If $S \in \mathscr{A}_i$ and $A \in C_{\mathscr{A}}(v_i)$ then $S^{-1}ASv_i = v_i$, that is $ASv_i = Sv_i$. Hence $Sv_i \in C_V(C_{\mathscr{A}}(v_i))$ meaning $Sv_i = \alpha v_i$ for some $\alpha \in F_i^*$. This implies $\bar{\mathscr{A}_i} \equiv \mathscr{A}_i / C_{\mathscr{A}}(v_i)$ is isomorphic to F_i^*. This implies

$$\begin{aligned} C(\mathscr{A}; V) &\cong C(F_t^*; F_t v_t) \oplus \cdots \oplus C(F_1^*; F_1 v_1) \\ &\cong F_t \oplus \cdots \oplus F_1 . \end{aligned}$$

We conclude this section (and the paper) with a couple of open problems relative to representing $C(\mathscr{A}; G)$ 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 $C\mathscr{A}, G) \cong GF(p^n) \oplus GF(q)$, is p^n a generator of $GF(q)^*$?

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

REFERENCES

1. G. Betsch, *Some structure theorems on 2-primitive near-rings*, Coll. Math. Soc. Janus Bolyai 6, Rings, Modules and Radicals, Keszthely (Hungary) North Holland, New York, 1973.
2. R. Brauer, M. Suzuki, and G. E. Wall, *A characterization of the one-dimensional unimodular groups over finite fields*, Illinois. J. Math., **2** (1958), 718-745.
3. D. Goldschmidt, *Elements of order two in finite groups*, Delta, **4** (1974), 45-58.
4. D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.
5. C. Maxson and K. Smith, *The centralizer of a set of group automorphisms*, Communications in Algebra, **8** (1980), 211-230.
6. C. Maxson and K. Smith, *Simple near-ring centralizers of finite rings*, Proc. Amer. Math. Soc., **75** (1979), 8-12.

7. C. Maxson and K. Smith, *Near-ring centralizers*, Proc. of the Ninth Annual USL Mathematics Conference, Res. Ser. No. 48, Univ. of Southwestern Louisiana, (1979), 49-58.

8. G. Pilz, *Near-Rings*, North Holland, New York, 1977.

9. M. Suzuki, *On a finite group with a partition*, Arch. Math., **12** (1961), 241-254.

10. M. Zeller, Oral Communication.

Received September 1, 1979.

TEXAS A & M UNIVERSITY
COLLEGE STATION, TX 77843

PACIFIC JOURNAL OF MATHEMATICS

Mathematical parers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Please propose a heading for the odd unmbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

50 reprints to each author are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966, Regular subscription rate: $114.00 a year (6 Vol., 12 issues). Special rate: $57.00 a year to individual members of supporting institution.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address shoud be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.).
8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics
Vol. 101, No. 2 December, 1982