JOURNAL OF ALGEBRA 54, 27–41 (1978)

The Centralizer of a Group Automorphism

CARLTON J. MAXSON AND KIRBY C. SMITH

Texas A & M University, College Station, Texas 77843

Communicated by A. Fröhlich

Received May 31, 1977

Let G be a finite group. The structure of the near-ring $C(A)$ of identity preserving functions $f: G \to G$, which commute with a given automorphism A of G, is investigated. The results are then applied to the case in which G is a finite vector space and A is an invertible linear transformation.

INTRODUCTION

Let A be a linear transformation on a finite-dimensional vector space V over a field F. The problem of determining the structure of the ring of linear transformations on V which commute with A has been studied extensively (e.g., [3, 5, 8]). In this paper we consider a nonlinear analogue to this well-known problem which arises naturally in the study of automorphisms of a linear automaton [6].

Specifically let G be a finite group, written additively, and let A be an automorphism of G. If $C(A) = \{f: G \to G \mid fA = Af$ and $f(0) = 0$ where 0 is the identity of $G\}$, then $C(A)$ forms a near ring under the operations of pointwise addition and function composition. That is $\langle C(A), + \rangle$ is a group, $\langle C(A), \cdot \rangle$ is a monoid, $(f + g)h = fh + gh$ for all $f, g, h \in C(A)$ and $f \cdot 0 = 0 \cdot f = 0$, $f \in C(A)$. It is the purpose of this paper to investigate the structure of the near-ring $C(A)$.

Near-rings of group mappings have previously been investigated. In fact, if A is the identity on G then $C(A)$ is the near-ring $M_0(G) = \{f: G \to G \mid f(0) = 0\}$, first investigated by Blackett [1]. Moreover, if A is an automorphism of G then the near-ring $C(A)$ is the centralizer of A in $M_0(G)$. We also mention that Betsch has considered a related problem. In [2] he studied the near-ring $M_H{}^0(G)$ of identity preserving functions on G that commute with every element in a group H of fixed point free automorphisms. For other references to $M_0(G)$, $M_H{}^0(G)$, and to near-rings in general we mention the recent book by Pilz [7].

In this paper we deal exclusively with finite groups. In Section 1 we characterize those $C(A)$ that are simple. We find the rather surprising result that

0021-8693/78/0541-0027$02.00/0

those semisimple $C(A)$ are precisely the ones that are simple. In Section 2 we describe the radical $J(C(A))$ for those $C(A)$ that are not semisimple. In the final section we apply our results to the case in which A is an invertible linear transformation on a finite vector space V. Here we find that in most cases $J(C(A))$ has a very explicit characterization.

1. Structure of $C(A)$

As in the Introduction, let G be a finite group written additively, but not necessarily Abelian, and let A be an automorphism of G. The set $C(A) = \{f\colon G \to G \mid fA = Af, f(0) = 0\}$ forms a near-ring under the operations of pointwise addition and composition of functions. In this section we investigate the structure of $C(A)$.

We fix some notation and terminology used throughout. Let $G^* = G - \{0\}$, and for $v \in G^*$ let $\theta(v)$ denote the orbit of v in G determined by A. So $\theta(v) = \{v, Av, \ldots, A^{k-1}v\}$ where k is the least positive integer such that $A^k v = v$. We denote the cardinality of $\theta(v)$ by $|\theta(v)|$ and refer to this as the *length* (or size) of $\theta(v)$. We define a partial order on the set of all orbits in G^* as follows: the orbit $\theta(w)$ is "less than" the orbit $\theta(v)$ if $|\theta(w)|$ is a proper divisor of $|\theta(v)|$. Thus $\theta(v)$ is a *minimal orbit* if G^* contains no orbits whose length is a proper divisor of $|\theta(v)|$. We extend this ordering to G by defining the orbit $\{0\}$ to be less than every nonzero orbit. The reason for this ordering will become clear in the sequel.

We now consider the problem of characterizing those $C(A)$ that are simple near-rings. We note that if $f \in C(A)$ then the values of f on an orbit $\theta(v)$ are completely determined once $f(v)$ is known, and $f(\theta(v))$ must also be an orbit of G, namely $\theta(f(v))$.

Lemma 1.1. *Let θ_1 and θ_2 be orbits in G of lengths n and m, respectively. Then there exists an $f \in C(A)$ such that $f(\theta_1) = \theta_2$ if and only if m divides n.*

Proof. Suppose $f \in C(A)$ with $f(\theta_1) = \theta_2$. Let $n = qm + r$, $0 \leqslant r < m$ and let $v_1 \in \theta_1$. Since $|f(\theta_1)| = m$ we have $A^m f(v_1) = f(v_1)$ and m is minimal with this property. On the other hand,

$$f(v_1) = f(A^n v_1) = A^n f(v_1) = A^r A^{qm} f(v_1) = A^r f(v_1),$$

which implies $r = 0$.

Conversely suppose m divides n and choose $v_1 \in \theta_1$, $v_2 \in \theta_2$. Define $f\colon G \to G$ by $f(0) = 0$, $f(A^j v_1) = A^j v_2$, $j = 1, 2, \ldots, n$, and $f(v) = 0$ otherwise. Since m divides n, f is well-defined, and clearly $f \in C(A)$.

We recall that if $N \equiv \langle N, +, \cdot\rangle$ is a near-ring then an additive subgroup H is N-invariant if $NH \subseteq H$ and $HN \subseteq H$.

LEMMA 1.2. *Let H be a $C(A)$-invariant subgroup of $C(A)$. If there exists an $h \in H$ with the property that $| h(\theta)| = | \theta |$ for some orbit θ in G^*, then H contains the idempotent function $e: G \to G$ where e is the identity on θ and 0 elsewhere.*

Proof. Choose $v \in \theta$ and let $\bar{v} = hv$, an element of $h(\theta)$. Define $f: G \to G$ by $f(A^s\bar{v}) = A^s v$, $s = 0, 1, \ldots$, and 0 elsewhere. Then $f \in C(A)$ and $e = fhe \in H$.

THEOREM 1.1. *$C(A)$ is simple if and only if all the orbits of G^* have the same length.*

Proof. Assume $C(A)$ is simple. Among all the orbits of G^* let θ be an orbit of minimal length, say k. Let $I = \{f \in C(A) \mid f(\theta) = \{0\}$ for all orbits of length $k\}$, an ideal of $C(A)$. Since $C(A)$ contains the identity map, $I \neq C(A)$. If G^* contains an orbit $\bar{\theta}$ of length greater than k, then the map $\bar{e}$ which is the identity on $\bar{\theta}$ and zero elsewhere belongs to I. So in order for $C(A)$ to be simple, all orbits of G^* must have length k.

Conversely suppose all the orbits of G^* have the same length k. If I is a nonzero ideal then there exists an $f \in I$ with $|f(\theta_i)| = | \theta_i |$ for some orbit θ_i in G^*. By Lemma 1.2 the associated idempotent e_i belongs to I. If θ_j is another orbit of G^*, define e_{ji} by $e_{ji}(\theta_j) = \theta_i$ and 0 elsewhere. Then $e_i e_{ji} = e_{ji} \in I$ and by Lemma 1.2, $e_j \in I$. Hence the identity map $1 = \Sigma e_j$ belongs to I, so $I = C(A)$.

We remark that when A is the identity map the above is a new proof to the known result that for a finite group G, $M_0(G) = \{f: \to G \mid f(0) = 0\}$ is a simple near-ring.

Recall that a permutation A on a group G is called *regular* if A has no fixed points other than the identity of G and A is a product of cycles of the same order.

COROLLARY 1.1. *$C(A)$ is simple if and only if either A is a regular permutation on G or A is the identity map.*

Betsch has shown that if H is a fixed point free group of automorphisms of a finite group G then the near-ring of zero preserving maps of G which commute with all the automorphisms in H is a simple near-ring. (See [2] or [7].) In our situation we have the cyclic group $H = \langle A \rangle$ of automorphisms of G generated by A. The proof of the following corollary is immediate from Theorem 1.1.

COROLLARY 1.2. *$C(A)$ is simple if and only if $\langle A \rangle$ is fixed point free.*

COROLLARY 1.3. *The following are equivalent:*

(a) *$C(A)$ is a field,*

(b) *$C(A)$ is a near-field,*

(c) *G^* has only one orbit.*

Proof. If $C(A)$ is a near-field then $C(A)$ is simple and all the orbits of G^*

have the same length, say k. Since every nonzero element of $C(A)$ is invertible, Lemma 1.2 implies that G^* has only one orbit.

If G^* has only one orbit, θ, then $C(A)$ is simple. Further, for a nonzero f in $C(A)$, $|f(\theta)| = |\theta|$ and so f is invertible. This implies that $C(A)$ is a near-field. Since a near-field always has commutative addition ([7], p. 240) and since the multiplication in $C(A)$ is clearly commutative, $C(A)$ is a field.

When $C(A)$ is a simple near-ring much can be said about its structure. Some of the more immediate results are contained in the following remarks.

The minimal left ideals of a simple $C(A)$ can be characterized. In particular, the $C(A)$-subgroups $C(A)\,e_i$, where e_i is the idempotent associated with the orbit θ_i, are the minimal left ideals. The equations $(h + fe_i + h) = (h + f - h)\,e_i$ and $h(fe_i + g) - hg = (h(f + g) - hg)\,e_i$, f, g, $h \in C(A)$ establish that $C(A)\,e_i$ is a left ideal. If K is a nonzero left ideal contained in $C(A)\,e_i$ then for $h \in K$, $h \neq 0$, we have $h(\theta_i) = \theta_j$ where $|\theta_j| = |\theta_i|$. Hence $e_i \in K$ and $C(A)\,e_i$ is minimal. On the other hand if M is a minimal left ideal in $C(A)$ then for a nonzero f in M there exist orbits θ_i and θ_j such that $f(\theta_i) = \theta_j$. As above we find that $e_i \in M$ and hence $M = C(A)\,e_i$. Therefore if $e_1, e_2, \ldots, e_t$ are the idempotents associated with the nonzero orbits of G then it is easily verified that $C(A) = C(A)\,e_1 \oplus C(A)\,e_2 \oplus \cdots \oplus C(A)\,e_t$.

As a final remark concerning the structure of the simple near-rings $C(A)$, we determine when the additive group $\langle C(A), +\rangle$ is abelian. Since $C(A)$ is simple, all nonzero orbits have the same length and thus for each nonzero x and y in G there exists a function f in $C(A)$ such that $f(x) = y$. Now if $\langle C(A), +\rangle$ is abelian then $y + x = (f + e_i)\,x = (e_i + f)\,x = y + x$ where $x \in \theta_i$. Thus G is abelian. Hence for the simple near-rings $C(A)$, $\langle CA), +\rangle$ is Abelian if and only if G is abelian.

One of our primary applications of this work is to the study of functions on a finite vector space which commute with a given invertible linear transformation. We now interpret the above results in this setting.

Let V be a finite-dimensional vector space over a finite field F and let A be an invertible linear transformation on V. For $v \in V^*$, $\theta(v) = \{v, Av, \ldots, A^{k-1}\}$ where $A^k v = v$, k minimal. So $(x^k - 1)\,v = (A^k - I)\,v = 0$ and hence $m(x; v)$ divides $x^k - 1$ where $m(x; v)$ is the minimal polynomial of v. This means that the orbit of v has length k where k is minimal such that $m(x; v)$ divides a polynomial of the form $x^k - 1$.

In general for $f(x) \in F[x]$ with $(x, f(x)) = 1$, let k be the least positive integer such that $f(x)$ divides $x^k - 1$, and call k the order of $f(x)$. Thus the length of the orbit containing $v \in V^*$ is the order of $m(x; v)$.

COROLLARY 1.4. *Let A be an invertible linear transformation on the finite vector space V. Then $C(A)$ is simple if and only if the minimal polynomial for A, $m(x; V)$, is the product of distinct irreducible polynomials having the same order.*

Proof. Assume $m(x; V)$ has the above form. If $v \in V^*$ then $m(x; v)$ is the product of distinct irreducibles of the same order, say k. Hence the order of $m(x; v)$ is k and $|\theta(v)| = k$. This is true for all $v \in V^*$ so $C(A)$ is simple.

Conversely if the minimal polynomial for A has factors (not necessarily irreducible) $f_1(x)$ and $f_2(x)$ of orders k_1 and k_2, respectively, with $k_1 \neq k_2$, then $f_1(x) = m(x; v_1)$ and $f_2(x) = m(x; v_2)$ for some $v_1, v_2 \in V^*$. Hence $k_1 = |\theta(v_1)| \neq |\theta(v_2)| = k_2$, and $C(A)$ is not simple.

Back to the general setting, suppose that θ is not a minimal orbit (recall the definitions preceding Lemma 1.1) of G^*. Then there exists a nonzero orbit $\theta_1 < \theta$. Let $M = \{f \in C(A) \mid f(\theta) < \theta_1 \text{ or } |f(\theta)| = |\theta_1| \text{ and } f(v) = 0 \text{ for } v \notin \theta\}$, a nonzero $C(A)$-subgroup of $C(A)$. Since $f_1 f_2 = 0$ for all $f_1, f_2 \in M$ then M is nilpotent. Since a near-ring N is defined to be semisimple whenever N satisfies the descending chain condition on N-subgroups and has no nonzero nilpotent N-subgroups, we have established the following.

Theorem 1.2. *If $C(A)$ is semisimple then all the orbits of G^* are minimal.*

The converse of Theorem 1.2 is also true but in this case we find the rather surprising result that all orbits in G^* must have the same size. This implies that $C(A)$ is semisimple if and only if it is simple. Our result follows from the following group theory result due to S. Garrison and M. Pettet (oral communication).

Lemma 1.3 (Garrison–Pettet). *Suppose $A: G \to G$ is a fixed point free automorphism of G and suppose $\theta(x)$, $\theta(y)$ are minimal orbits. Then either $x + y = 0$ or $|\theta(x + y)| = \text{l.c.m.}\{|\theta(x)|, |\theta(y)|\}$.*

Proof. Clearly $\text{l.c.m.}\{|\theta(x)|, |\theta(y)|\} \geqslant |\theta(x + y)|$. Suppose $x + y \neq 0$ and let $k = |\theta(x + y)|$. Then $A^k(x + y) = A^k(x) + A^k(y) = x + y$, so

$$-x + A^k(x) = y - A^k(y).$$

If A^t fixes x then it also fixes $-x + A^k(x)$ and hence $|\theta(-x + A^k(x))|$ divides $|\theta(x)|$. By the minimality of $\theta(x)$ either $|\theta(-x + A^k(x))| = |\theta(x)|$ or 1.

If $|\theta(-x + A^k(x))| = |\theta(x)|$ then $|\theta(x)| = |\theta(y - A^k(y))|$ and this divides $|\theta(y)|$. By the minimality of $\theta(y)$ either $|\theta(x)| = |\theta(y)|$ or $|\theta(x)| = 1$. (If $|\theta(x)| = 1$ then $x = 0$ since A is fixed point free.) In either case we are done.

If $|\theta(-x + A^k(x))| = 1$ then $-x + A^k(x) = 0 = y - A^k(y)$, that is, $A^k(x) = x$ and $A^k(y) = y$. This implies both $|\theta(x)|$ and $|\theta(y)|$ divide k. So $k = |\theta(x + y)| \geqslant \text{l.c.m.}\{|\theta(x)|, |\theta(y)|\}$.

Corollary 1.5. *If $A: G \to G$ is an automorphism of G such that all the orbits of G^* are minimal, then they all have the same size. Hence $C(A)$ is semisimple if and only if $C(A)$ is simple.*

Proof. If A has a fixed point then by definition of minimality all the orbits have length 1. If A has no fixed point assume $\theta(x)$ and $\theta(y)$ are minimal orbits such that $|\theta(x)| \neq |\theta(y)|$. Then $y + x \neq 0$ and by the lemma $|\theta(x+y)| = \text{l.c.m.}\{|\theta(x)|, |\theta(y)|\}$, so $\theta(x+y)$ is not a minimal orbit. Hence $|\theta(x)| = |\theta(y)|$ as desired.

The above implies that if $C(A)$ has a nontrivial ideal then the radical $J(C(A))$ of $C(A)$ is nontrivial. In the next section we describe this radical.

2. The Radical of $C(A)$

Recall that the radical of a near-ring N with identity is the intersection of all strictly maximal left ideals of N, that is, the intersection of all left ideals of N which are also maximal as N-subgroups. Thus to describe $J(C(A))$ it suffices to find all strictly maximal left ideals of $C(A)$. To this end we first consider certain maximal $C(A)$-subgroups.

Lemma 2.1. *For an orbit θ of G^* let $N(\theta) = \{n \in C(A)\colon n(\theta)$ is less than $\theta\}$. If $N(\theta)$ is a subgroup then $N(\theta)$ is a maximal $C(A)$-subgroup.*

Proof. It is straightforward to verify that $N(\theta)$ is a $C(A)$-subgroup. Suppose $\bar{N}$ is a $C(A)$ subgroup that properly contains $N(\theta)$. It is clear that for each orbit $\theta_j \neq \theta$, $N(\theta)$ contains the associated idempotent e_j. To show $\bar{N} = C(A)$ it suffices to show the idempotent e associated with θ belongs to $\bar{N}$.

Since $\bar{N} \neq N(\theta)$ there exists an $f \in \bar{N}$ with $|f(\theta)| = |\theta|$, say $f(\theta) = \theta_j$. Using the $C(A)$-subgroup property of $\bar{N}$ there exists a $g \in \bar{N}$ such that $g(\theta) = \theta$ and the range of g is $\theta \cup \{0\}$. Suppose $g(\bar{\theta}) = \theta$, $\bar{\theta} \neq \theta$. Define $h\colon G \to G$ by $h(\bar{v}) = g(\bar{v})$ for $\bar{v} \in \bar{\theta}$ and 0 otherwise. Then $h \in N(\theta)$ and $g - h$ has the property that $(g - h)(\bar{\theta}) = \{0\}$ and $(g - h)(\theta) = \theta$. Continuing in this fashion if necessary shows $e \in \bar{N}$, hence $\bar{N} = C(A)$.

The following example shows that there are maximal $C(A)$-subgroups not of the form $N(\theta)$ for some orbit θ in G^*.

Example. Let $G = Z_3 \oplus Z_3$ and $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The orbits in G^* are $\theta_1 = \{(1, 0)\}$, $\theta_2 = \{(2, 0)\}$, $\theta_3 = \{(1, 1), (2, 1), (0, 1)\}$ and $\theta_4 = \{(0, 2), (2, 2), (1, 2)\}$. If $M = \{f \in C(A) \mid f(\theta_1) = f(\theta_2)\}$ then it is easily verified that M is a $C(A)$-subgroup and one can check that M is also maximal.

We show now that if M is a maximal $C(A)$-subgroup which is not of the form $N(\theta)$ for any orbit θ in G^* then M cannot be a left ideal. As a consequence we will have that a strictly maximal left ideal of $C(A)$ must be of the form $N(\theta)$ for some orbit θ and to characterize $J(C(A))$ it will suffice to determine those $N(\theta)$ that are left ideals.

Assume M is a strictly maximal left ideal of $C(A)$. Let $\theta_1, \theta_2, \ldots, \theta_s$ be the orbits of G^*. Since $M \neq C(A)$ not all of the idempotents e_i, $i = 1, 2, \ldots, s$, are in M, say $e_1 \notin M$. Since M is a left ideal then M is a normal subgroup and consequently $M + C(A)\, e_1$ is a $C(A)$-subgroup ([7], pg. 46). The maximality of M means $M + C(A)\, e_1 = C(A)$, and so there exist $m \in M$, $n \in C(A)$ such that $m + ne_1 = 1$. We note that m is the identity on $\theta_2, \theta_3, \ldots, \theta_s$, i.e., $me_i = e_i$ for $i \geqslant 2$. Assume $m(\theta_1) = \theta_2$. Then for $j \geqslant 3$ we have $e_j m = e_j \in M$. Consider $m_1 = m - (me_3 + \cdots + me_s) \in M$, which has the following properties: $m_1(\theta_1) = \theta_2$, $m_1(\theta_2) = \theta_2$, $m_1(\theta_j) = \{0\}$ for $j \geqslant 3$.

Two situations arise. Either there exists an $f \in M$ such that $f(\theta_1) = \theta_i$ with $|\theta_1| = |\theta_i|$ or else $f(\theta_1) < \theta_1$ for every $f \in M$.

If we have the first situation, then for $f \in M$ such that $f(\theta_1) = \theta_i$ with $|\theta_1| = |\theta_i|$ consider $f_1 = f - (fe_3 + \cdots + fe_s) \in M$. The function f_1 has the following properties:

$$f_1(\theta_1) = \theta_i, \qquad f_1(\theta_2) = \theta_j, \qquad f_1(\theta_k) = \{0\} \qquad \text{for } k \geqslant 3 \quad \text{and some} \quad j.$$

We have $e_{i1} f_1 \in M$ where $e_{i1}(\theta_i) = \theta_1$ and 0 otherwise. Moreover $e_{i1} f_1(\theta_1) = \theta_1$, $e_{i1} f_1(\theta_2) = e_{i1}(\theta_j)$, and $e_{i1} f_1(\theta_k) = \{0\}$ for $k \geqslant 3$. If $\theta_j \neq \theta_i$ then $e_{i1} f_1(\theta_2) = \{0\}$ and $e_1 \in M$, a contradiction. Hence $\theta_j = \theta_i$ and this means $|\theta_j| = |\theta_i| = |\theta_1| = |\theta_2|$.

Since M is an ideal we have $g = e_1(m_1 + e_1) - e_1 \in M$, which annihilates each θ_j, $j \geqslant 2$. If $v \in \theta_1$ with $m_1(v) + v \notin \theta_1$ then $g(v) = -v$, hence $e_1 \in M$. On the other hand, if $m_1(v) + v \in \theta_1$ then $g(v) = m_1(v) \in \theta_2$, and 0 off θ_1. Since $e_{21} g \in M$ then $e_1 \in M$, giving a contradiction.

Suppose the second situation holds, namely $f(\theta_1) < \theta_1$ for all $f \in M$. Then M is a subset of $N(\theta_1)$. We have seen above that $e_3, \ldots, e_s$ belong to M and we now show e_2 belongs to M. Suppose not, then the maximality of M means $M + C(A)\, e_2 = C(A)$. But for each $f \in M$, $g \in C(A)$ we have $(f + ge_2)\, \theta_1 = f(\theta_1) < \theta_1$. This means $M + C(A)\, e_2 \subseteq N(\theta_1)$ which is impossible, so $e_2 \in M$. This means that whether or not a function belongs to M depends only on its action on θ_1, i.e., functions in M can be arbitrarily defined off θ_1 (subject to being in $C(A)$).

Let $M(\theta_1) = \{f(x) \in G \mid f \in M \text{ and } x \in \theta_1\}$, a subgroup of the group $G(\theta_1) = \{x \in G \mid \theta(x) < \theta_1 \text{ or } |\theta(x)| = |\theta_1|\}$. We note that $M(\theta_1)$ has the following properties:

(i) $M(\theta_1)$ is a union of orbits in G,

(ii) if the orbit θ is a subset of $M(\theta_1)$ then so is every orbit $\tilde{\theta}$ with $|\tilde{\theta}| = |\theta|$.

For convenience we will call such subgroups of $G(\theta_1)$ s-subgroups. We note that s-subgroups give rise to $C(A)$-subgroups in a natural way. Thus, since M is a maximal $C(A)$-subgroup, $M(\theta_1)$ is a maximal s-subgroup of $G(\theta_1)$.

If θ_1 is a minimal orbit then necessarily $M(\theta_1) = \{0\}$. But in this case $N(\theta_1)$ is a maximal $C(A)$-subgroup so $M = N(\theta_1)$.

We may now assume θ_1 is not minimal. Let $\hat{\theta}$ be an orbit in G^* such that $\hat{\theta} < \theta_1$. Then $\{f \in C(A) \mid f(\theta_1) < \hat{\theta}$ or $|f(\theta)| = |\hat{\theta}|\}$ is a $C(A)$-subgroup and this means $M(\theta_1) \neq \{0\}$, due to the maximality of M. We now show that M must equal $N(\theta_1)$.

If this is not the case then there exists an orbit $\tilde{\theta} < \theta_1$ with $\tilde{\theta} \cap M(\theta_1) = \varnothing$. Choose $\tilde{\theta}$ minimal with respect to this property. Let $H = M(\theta_1) \cup \{x \in G \mid |\theta(x)| = |\tilde{\theta}|\}$. Since $M(\theta_1)$ is a maximal s-subgroup there exists an x in $M(\theta_1)$ and a y in $H - M(\theta_1)$ such that $x + y \notin H$ (otherwise H would be a group). Choose $z \in \theta_1$ and define functions $f, g \in C(A)$ as follows:

$$\begin{aligned} f(A^i z) &= A^i x, \qquad & i &= 0, 1, \ldots, \\ f(\theta_j) &= \{0\}, \qquad & j &\neq 1, \end{aligned}$$

and

$$\begin{aligned} g(A^i z) &= A^i y, \qquad & i &= 0, 1, \ldots, \\ g(\theta_j) &= \{0\}, \qquad & j &\neq 1. \end{aligned}$$

Then both f and $\bar{e}(f + g) - \bar{e}g$ belong to M where $\bar{e}$ is the idempotent associated with $\theta(y)$. But $(\bar{e}(f + g) - \bar{e}g)(z) = -y$ and $-y$ does not belong to $M(\theta_1)$, a contradiction. This means $M(\theta_1) = \{x \mid \theta(x) < \theta_1\}$ which in turn implies that $M = N(\theta_1)$.

This establishes the following result.

Lemma 2.2. *If M is a strictly left ideal of $C(A)$ then $M = N(\theta)$ for some orbit θ in G^*.*

It remains to characterize those $N(\theta)$ that are left ideals. Let θ be an orbit of G^*, say $|\theta| = k$, and let $G_k = \cup\theta_i$, where the union is over all orbits of G whose order divides k and let $U_k = \{v \in G \mid \theta(v)$ is less than $\theta\}$. Clearly $A(G_k) = G_k$ and $G_k = (\cup\theta_j) \cup U_k$ where $|\theta_j| = k$.

Lemma 2.3. *Let θ_1 and θ_2 be distinct orbits of the same length. Then $N(\theta_1)$ is a left ideal of $C(A)$ if and only if $N(\theta_2)$ is.*

Proof. Let $\theta_1 = \theta(v_1)$, $\theta_2 = \theta(v_2)$ and define $\alpha: G \to G$ by $\alpha(A^i v_1) = A^i v_2$, $\alpha(A^i v_2) = A^i v_1$, $i = 1, 2, \ldots$, and $\alpha(v) = v$ otherwise. Clearly $\alpha \in C(A)$. Define $R_\alpha: C(A) \to C(A)$ by $R_\alpha(f) = f\alpha$. It is easily verified that R_α is an automorphism of $\langle C(A), + \rangle$ and $R^2 = 1$. Moreover $R_\alpha(N(\theta_1)) = N(\theta_2)$, and $N(\theta_1)$ is a normal subgroup of $C(A)$ if and only if $N(\theta_2)$ is.

Suppose $N(\theta_2)$ is a left ideal. For $f, g \in C(A)$, $n_1 \in N(\theta_1)$ we have

$(f(n_1 + g) - fg)\,\alpha = f(n_1\alpha + g\alpha) - fg\alpha \in N(\theta_2)$ since $n_1\alpha \in N(\theta_2)$. Thus $f(n_1 + g) - fg \in N(\theta_1)$. By symmetry the lemma is proven.

THEOREM 2.1. *Let θ be an orbit of length k. Then $N(\theta)$ is a strictly maximal left ideal if and only if U_k is a normal subgroup of G_k and every orbit of length k is a union of cosets of U_k in G_k.*

Proof. We first show the conditions are sufficient. Since U_k is a group, $N(\theta)$ is a group and thus from Lemma 2.1, $N(\theta)$ is a maximal $C(A)$-subgroup. Let $f \in C(A)$, $n \in N(\theta)$. Then for $v \in \theta$ we have $(f + n - f)\,v \in U_k$ since $f(v) \in G_k$ and U_k is normal in G_k. Hence $f + n - f \in N(\theta)$ and $N(\theta)$ is a normal subgroup. To show that $N(\theta)$ is a left ideal, let $f, g \in C(A)$, $n \in N(\theta)$ and consider $(f(n + g) - fg)\,v$, $v \in \theta$. If $g(v) \in U_k$ then both $f(n(v) + g(c))$ and $fg(v)$ belong to U_k so $(f(n + g) - fg)\,v \in U_k$ and $f(n + g) - fg \in N(\theta)$. Assume $g(v) \notin U_k$. Since $n(v) \in U_k$ then $n(v) + g(v)$ and $g(v)$ belong to the same coset of U_k in G_k and thus belong to the same orbit $\theta(g(v))$. Let $s > 0$ be minimal such that $A^s v - v$ belongs to U_k. Then $\theta(v)$ is the union of s cosets, namely,

$$\begin{aligned} v + U_k &= \{A^{st}(v) \mid t = 0, 1, 2,\ldots\},\\ Av + U_k &= \{A^{st}(Av) \mid t = 0, 1, 2,\ldots\},\\ &\vdots\\ A^{s-1}v + U_k &= \{A^{st}(A^{s-1}v) \mid t = 0, 1, 2,\ldots\}. \end{aligned}$$

We have $n(v) + g(v) = A^{st}(g(v))$ for some t. Thus $(f(n + g) = fg)\,(v) = f(A^{st}(g(v))) - f(g(v)) = A^{st}fg(v) - fg(v) = (A^{st} - I)\,fg(v)$. But $A^{st}fg(v))$ and $fg(v)$ belong to the same coset of U_k so $(A^{st} - I)\,fg(v) \in U_k$. Hence $f(n + g) - fg \in N(\theta)$ as desired.

For the necessity, suppose $N(\theta)$ is a strictly maximal left ideal. If U_k is not a subgroup, say $w_1, w_2 \in U_k$ but $w_1 + w_2 = v \notin U_k$, then we must have $|\,\theta(v)| = k$. Let $f = g = e_1$ where e_1 is the identity on $\theta(v)$ and 0 elsewhere. Define $n\colon G \to G$ by $n(A^i v) = -A^i w_1$ and $n(\bar{v}) = 0$, $\bar{v} \notin \theta(v)$. Then $n \in N(\theta(v))$ which must be a left ideal by Lemma 2.3. But $(e_1(n + e_1) - e_1)\,v = -v$ which means $e_1(n + e_1) - e_1 \notin N(\theta(v))$. This contradiction implies that U_k is a subgroup. If U_k is not normal in G_k then there exist $v \in G_k$, $w \in U_k$ such that $v + w - v \notin U_k$. Defining n by $n(A^i v) = A^i w$, $i = 0, 1,\ldots,$ and $n(\bar{v}) = 0$ if $\bar{v} \notin \theta$ then $e_1 + n - e_1 \notin N(\theta)$. Thus U_k is normal. If $w \in U_k$, $\bar{v} \in \theta(v)$ then we must have $w + \bar{v} \in \theta(v)$, otherwise using an argument similar to the above it can be shown that $N(\theta)$ is not a left ideal.

It is immediate from the theorem that if θ is a minimal orbit in G^* then $N(\theta)$ is a strictly maximal left ideal in $C(A)$. We note also that even though U_k is a normal subgroup of G_k and some of the orbits of length k are unions of cosets of U_k, it need not be the case that all orbits of length k are unions of cosets.

EXAMPLE. Let $G = (Z_2)^4$ with

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

G has two orbits of length 1, a unique orbit of length 2, and three orbits of length 4. One of the orbits of length 4 is a coset of U_4, while the other two are not. Note that if θ is the unique orbit of length 2 then necessarily $N(\theta)$ is a left ideal.

From the above discussion, in order to determine $J(C(A))$ one needs to investigate the sets $N(\theta)$. By definition, $N(\theta_1) = N(\theta_2)$ if and only if $\theta_1 = \theta_2$, so in order to find the strictly maximal left ideals in $C(A)$ one is left with the straightforward but tedious task of determining which orbits satisfy the criteria of Theorem 2.1. From Lemma 2.3, if one orbit of length k determines a strictly maximal left ideal then so does every orbit of length k. Moreover, as the next proposition shows, the length of an orbit θ determines the isomorphism class of the left ideal $N(\theta)$.

PROPOSITION 2.1. *If $N(\theta_1)$ and $N(\theta_2)$ are left ideals then $N(\theta_1)$ and $N(\theta_2)$ are $C(A)$-isomorphic if and only if $|\theta_1| = |\theta_2|$.*

Proof. If $|\theta_1| = |\theta_2|$ then the group automorphism R_α defined in the proof of Lemma 2.3 is easily verified to be a $C(A)$-isomorphism. Conversely, let $\phi: N(\theta_1) \to N(\theta_2)$ be a $C(A)$-isomorphism and define $H(\theta_i) = \{f \in N(\theta_i) \mid e_1 f = f\}$ for $i = 1, 2$. That is, $H(\theta_i) = \{f \in N(\theta_i) \mid \text{range} f \subseteq \theta_1 \cup \{0\}\}$, $i = 1, 2$. Now ϕ induces a bijection between $H(\theta_1)$ and $H(\theta_2)$. Suppose $|\theta_1| \neq |\theta_2|$, say $|\theta_2| < |\theta_1|$. Then $H(\theta_1) = \{f \in C(A) \mid f(\theta_1) = f(\theta_2) = \{0\}$ and $f(\theta_i) \subseteq \theta_1 \cup \{0\}$, $i \notin \{1, 2\}\}$ while $H(\theta_2) = \{f \in C(A) \mid f(\theta_2) = \{0\}$ and $f(\theta_i) \subseteq \theta_1 \cup \{0\}, i \neq 2\}$. Thus $|H(\theta_1)| \lneqq |H(\theta_2)|$, contradicting the fact that there is a bijection between $H(\theta_1)$ and $H(\theta_2)$.

We now let $L_1, L_2, \ldots, L_n$ denote the collection of strictly maximal left ideals of $C(A)$ and define $I_1 = \cap\{L_i \mid L_i \simeq L_1\}$. From the above proposition, $I_1 = \{f \in C(A) \mid f(\theta_i) < \theta_i$ for all orbits of length $|\theta_1|\}$ and consequently it is easy to show that I_1 is an ideal of $C(A)$. Suppose J is an ideal of $C(A)$ such that $J \supsetneqq I_1$. For $a_j \in J - I_1$, we have $a_j \notin L_j$ for some $L_j \simeq L_1$. Hence $|a_j(\theta_j)| = |\theta_j|$ and so, using the ideal property of J, $e_j \in J$. But also from the ideal property of J we find that there exists $a_i \in J - I_1$, $a_i \notin L_i$ for each $L_i \simeq L_1$ and so $e_i \in J$ for each nonzero orbit θ_i of G. Hence $1 \in J$. This shows that I_1 is a maximal ideal of $C(A)$.

COROLLARY 2.1. *Let $\{K_1, K_2, \ldots, K_t\}$ be a partition of the set of strictly* *maximal left ideals into isomorphism classes and let* $I_j = \cap \{L \mid L \in K_j\}$, $j = 1, 2, \ldots, t$. *Then* I_j *is a maximal ideal and* $J(C(A)) = \bigcap_{j=1}^{t} I_j$.

One of the more interesting properties of the radical $J(N)$ of a finite near-ring N is that, in contrast to the situation for rings, $J(N)$ is not necessarily nilpotent. We answer the natural question as to when $J(N)$ is nilpotent in the next proposition.

PROPOSITION 2.2. *$J(C(A))$ is nilpotent if and only if for every nonzero orbit θ, $N(\theta)$ is a strictly maximal left ideal.*

Proof. Let $J(C(A))$ be nilpotent. Suppose there is a nonzero orbit θ such that $N(\theta)$ is not a strictly maximal left ideal. Then the function f defined by $f(\theta) = \theta$ and $f(\bar{\theta}) = \{0\}$ for $\bar{\theta} \neq \theta$ is in $J(C(A))$ and for each positive integer n, $f^n \neq 0$. This contradicts the fact that $J(C(A))$ is nilpotent which in turn gives the desired result. Conversely if $N(\theta)$ is a strictly maximal left ideal for every nonzero orbit θ then $J(C(A)) = \{f \in C(A) \mid f(\theta) < \theta \text{ for } \theta \neq \{0\}\}$. Since the number of orbits is finite, $J(C(A))$ is nilpotent.

From the above proposition and results in [7, Chap. 5] we obtain several relationships among the various well-known radical-like objects of near-ring theory. Some of these are given in the following.

COROLLARY 2.2. *Let A be an automorphism of G such that for every nonzero orbit θ, $N(\theta)$ is a strictly maximal left ideal of $C(A)$. The following are equivalent to $J(C(A))$ being nilpotent:*

(i) $J(C(A))$ *is nilpotent,*

(ii) $J(C(A))$ *is quasiregular,*

(iii) $J(C(A)) = \cap \{L \mid L$ *is a maximal left ideal*$\}$,

(iv) $J(C(A)) = \cap \{K \mid K$ *is a maximal* $C(A)$*-subgroup*$\}$,

(v) $J(C(A)) = \cap \{M \mid M$ *is a maximal ideal*$\}$.

In the example following Theorem 2.1, there is an orbit θ, $\theta \neq \{0\}$, such that $N(\theta)$ is *not* a strictly maximal left ideal. Thus in this case $J(C(A))$ satisfies none of the characterizations of Corollary 2.1. On the other hand, we now give an example showing that the above situation can arise. Thus we observe that the structure of $J(C(A))$ is intimately associated with the orbit structure of the group G as determined by the automorphism A.

EXAMPLE. Let $G = (Z_2)^3$ with

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

G has a unique orbit of length 4, a unique orbit of length 2, and a unique nonzero orbit of length 1. Hence $N(\theta)$ is a strictly maximal left ideal for each nonzero orbit and so $J(C(A))$ is nilpotent.

This concludes our general study of $C(A)$. In the next section we specialize to the near-ring $C(A)$ where A is an invertible linear transformation on a finite vector space. In this situation we give a complete description, in terms of minimal polynomials, of those $N(\theta)$ that are strictly maximal left ideals.

3. The Centralizer of an Invertible Linear Transformation

Throughout this section $G = V$ is a vector space over a finite field F and A is an invertible linear transformation on V. As above we let θ be an orbit of V^*, $|\theta| = k$, then $V_k = \cup\theta_i$ where the union is over all orbits of V whose length divides k, and U_k is the union of all orbits which are less than θ. V_k is an A-invariant subspace of V. Theorem 2.1 states that $N(\theta)$ is a left ideal of $C(A)$ if and only if U_k is a subspace and every orbit of length k is a union of cosets of U_k. We now seek a description of such vector spaces V_k.

Let A_k be the restriction of A to V_k.

Lemma 3.1. *If $N(\theta)$ is a left ideal of $C(A)$ and θ is not a minimal orbit then V_k is indecomposable relative to A_k.*

Proof. Since $N(\theta)$ is a left ideal of $C(A)$, then Theorem 2.1 applies. Suppose $V_k = W_1 \oplus W_2$ where W_1, W_2 are A_k-invariant subspaces. Since U_k is a proper subspace of V_k it cannot contain both W_1 and W_2. Suppose $w_1 \in W_1$ with $w_1 \notin U_k$. Then $|\theta(w_1)| = k$ and so $w_1 + U_k \subseteq \theta(w_1) \subseteq W_1$. Thus $U_k \subseteq W_1$. If $W_2 \neq \{0\}$ then there is a $w_2 \in W_2$ such that $|\theta(w_2)| = k$. Again this means $U_k \subseteq W_2$, a contradiction since $U_k \neq \{0\}$. Hence V_k is indecomposable.

Since V_k is indecomposable the minimal and characteristic polynomials for A_k are equal, and moreover this polynomial must be a power of an irreducible polynomial, say $m(x; V_k) = p(x)^n$ [4, p. 129].

Lemma 3.2. *Suppose $N(\theta)$ is a left ideal of $C(A)$ where θ is not minimal and $|\theta| = k$. Let $v \in \theta$. Then*

(a) *$m(x; v) = m(x; w)$ for every $w \in V$ such that $|\theta(w)| = k$,*

(b) *F is a prime field,*

(c) *$m(x; V_k) = (x - a)^n$ for some $a \neq 0 \in F$.*

Proof. As above we have V_k is indecomposable, so $m(x; V_k) = p(x)^n$ where $p(x)$ is irreducible. We also have

$$\{0\} \subset V_k^{(1)} \subset \cdots \subset V_k^{(m-1)} \subset V_k^{(m)} \subset \cdots \subset V_k^{(n)}$$

where $V_k^{(i)} = \ker p(A_k)^i$, $U_k = V_k^{(m-1)}$ and every orbit in $V_k^{(n)} - V_k^{(m-1)}$ has size k and is the union of cosets of U_k. Consider $W = V_k^{(n)}/U_k$ with the induced linear transformation $\bar{A}_k$. We have $m(x; W) = p(x)^{n-m+1}$ and

$$\{0\} \subset W^{(1)} \subset \cdots \subset W^{(n-m+1)} = W,$$

where $W^{(i)} = \ker p(\bar{A}_k)^i$ and all the orbits of W^* have the same size. Since $o(p(x)) < o(p(x)^2)$ the above implies $n = m$. This proves part (a).

We now have

$$\{0\} \subset V_k^{(1)} \subset \cdots \subset V_k^{(n-1)} \subset V_k^{(n)},$$

where $U_k = V_k^{(n-1)}$. Suppose first that $n = 2$. Then $V_k^{(2)} - V_k^{(1)}$ contains orbits of length $k = o(p(x)^2) = o(p(x))\, \rho = h\rho$ where $\rho = \operatorname{char} F$ and $(h, \rho) = 1$. Since each orbit in $V_k^{(2)} - V_k^{(1)}$ is the union of cosets of $U_k = V_k^{(1)}$ then

$$| U_k | = | F |^{\deg p(x)}$$

must divide $h\rho$. Since $(h, \rho) = 1$ then we must have $| F | = \rho$ and $\deg p(x) = 1$.

If $n > 2$ then again consider $W = V_k^{(n)}/V_k^{(n-2)}$ with the induced linear transformation $\bar{A}_k$. We have $m(x; W) = p(x)^2$ and

$$\{0\} \subset W^{(1)} \subset W,$$

where $W^{(1)} = \ker p(\bar{A}_k)$. Moreover the orbits of $W - W^{(1)}$ are unions of cosets of $W^{(1)}$. Thus as in the above, $| F | = \rho$ and $\deg p(x) = 1$.

We now turn to the main result of this section, the characterization of the strictly maximal ideals in $C(A)$ and hence the description of $J(C(A))$. We continue our notation that $o(f(x))$ is the order of $f(x) \in F[x]$, $m(x; V)$ is the minimal polynomial, and $c(x; V)$ is the characteristic polynomial for A.

THEOREM 3.1. *Let A be an invertible linear transformation on a finite vector space over a field F. For $v \in V^*$, $N(\theta(v))$ is a strictly maximal left ideal of $C(A)$ if and only if exactly one of the following holds:*

(a) *$\theta(v)$ is a minimal orbit,*

(b) *$m(x; v) = (x - 1)^3$, $F = Z_2$, $m(x; V) = (x - 1)^3 g_1(x)$ and $c(x; V) = (x - 1)^3 g_2(x)$ where $g_2(x)$ has no linear factors,*

(c) *$m(x; v) = (x - 1)^2$, $F = Z_2$, $m(x; V) = (x - 1)^s g_1(x)$ and $c(x; V) = (x - 1)^s g_2(x)$ where $s \geq 2$ and $g_2(x)$ has no linear factors,*

(d) *$m(x; v) = (x - a)^2$, $F = Z_\rho$, $\rho \neq 2$, $m(x; V) = (x - a)^2 g_1(x)$ where $g_1(x)$ has no linear factors $x - b$ with $o(x - b)$ dividing $o(x - a)$, $c(x; V) = (x - a)^2 g_2(x)$.*

Proof. Suppose that $N(\theta(v))$ is a left ideal. We will assume that $\theta(v)$ is not a minimal orbit and show that one of (b)–(d) must hold. From Lemma 3.2 we have $m(x; v) = (x - a)^n$ and $F = Z_\rho$. If $|\,\theta(v)| = s$ then U_s is a group and $\theta(v)$ is a union of cosets of U_s. We have $o(x - a) = k$, $1 \leqslant k \leqslant \rho - 1$, and so $x^k - 1 = (x - a)\, q(x)$. For any $t > 0$, $(x^k - 1)^{\rho^t} = x^{k\rho^t} - 1 = (x - a)^{\rho^t} q(x)^{\rho^t}$. Hence the length of $\theta(v)$ is $k\rho^t$ where t is minimal such that $\rho^t \geqslant n$. Also, from Lemma 3.2, we have $|\, U_s \,| = \rho^{n-1}$.

In order for $\theta(v)$ to be a union of cosets of U_s we must have

$$\rho^{n-1} \mid k\rho^t, \qquad (k, \rho) = 1, \tag{1}$$

where t is minimal such that $\rho^t \geqslant n$. This means ρ^{n-1} divides ρ^t, or $n - 1 \leqslant t$.

Assume $n \geqslant 5$. Then it can be shown that $n \leqslant \rho^{n-2}$ and this means $t \leqslant n - 2 < n - 1$ and (1) does not hold. If $n = 4$ and $\rho > 2$, the above argument is still valid and (1) does not hold. If $n = 4$, $\rho = 2$ then $t = 2$ and $t < n - 1$ so (1) does not hold.

Assume $n = 3$. If $\rho > 2$ then $t = 1$ and (1) does not hold. If $\rho = 2$ then $t = 2$ and (1) is satisfied. This means $m(x; v) = (x - 1)^3$ and $c(x; V)$ has the form $c(x; V) = (x - 1)^k g_1(x)$ where $g_1(x)$ has no linear factors. Lemma 3.1 forces the minimal polynomial to have the form $m(x; V) = (x - 1)^k g_2(x)$. If $k \geqslant 3$ then there exists a $v_1 \in V$ such that $m(x; v_1) = (x - 1)^4$ and $|\,\theta(v_1)| = 4$. By Lemma 2.3 and Theorem 2.1, $\theta(v_1)$ is a union of cosets of U_4. Since $|\, U_4 \,| = 4$ then $v_1 + U_4 = \theta(v_1)$, but $Av_1 - v_1 \in U_4$ implies $(x - 1)^3 v_1 = 0$, a contradicition. Thus $k = 3$ and we have part (b) of the theorem.

If $n = 2$, $\rho = 2$ then $t = 1$ and (1) is satisfied. As above $c(x; V) = (x - 1)^k g_1(x)$ and $m(x; V) = (x - 1)^k g_2(x)$ where $g_1(x)$ has no linear factors. This gives (c).

If $n = 2$, $\rho \geqslant 3$ then $t = 1$ and (1) is satisfied. Again $c(x; V) = (x - a)^k g_1(x)$ and $m(x; V) = (x - a)^k g_2(x)$ where $x - a$ does not divide $g_1(x)$. Suppose $g_1(x)$ has a linear factor $x - b$ such that $o(x - b)$ divides $o(x - a)$. Then for $w \in U_s$ with $m(x; w) = x - a$ we have $w + v \notin \theta(v)$, a contradiction to Lemma 3.1. We now show $k = 2$. If $k \geqslant 3$ then there is an element $v_1 \in V$ such that $m(x; v_1) = (x - a)^3$ and $|\,\theta(v_1)| = |\,\theta(v)|$, say $k\rho$. The orbit $\theta(v_1)$ is a union of cosets of U_k and this means $(A^l - I)\, v_1 \in U_k$ for some $l < k\rho$. But then $(A - aI)(A^l - I)\, v_1 = 0$ so $(x - a)^2$ divides $x^l - 1$ which is impossible since $l < k$. Hence we have (d).

If $n = 1$ then $t = 0$ and (1) is satisfied. Then $m(x; v) = x - a$ and it is easily seen that $\theta(v)$ must be a minimal orbit.

It remains to show that situations (a)–(d) actually give rise to left ideals of $C(A)$. Part (a) is obvious.

Assume part (b) holds. Then $\theta(v)$ has size 4 and $U_4 = \ker(A - I)^2$. If $\theta(v_1)$ is any orbit of size 4 then $w = (A - I)\, v_1 \in U_4$ since $(A - I)^2 w = 0$. Since $m(x; w) = (x - 1)^2$ it is easy to see that $v_1 + U_4 = \theta(v_1)$. By Theorem 2.1, $N(\theta(v))$ is a left ideal.

Assume (c) is true. Then $|\theta(v)| = 2$ and $U_2 = \ker(A - I)$. If $\theta(v_1)$ has size 2 then $m(x; v_1) = (x - 1)^2$ and as above $(A - I)v_1 \neq 0 \in U_2$, so $v_1 + U = \theta(v_1)$.

Assume (d) is true. Let $|\theta(v)| = kp$ then $U_{kp} = \ker(A - aI)$, $|U_{kp}| = p$. Let $\theta(v_1)$ be any orbit of length k. Then $m(x; v_1) = (x - a)^2$ and since $w = (A^k - I)v_1 \in U_{kp}$ we have

$$A^k v_1 = v_1 + w,$$
$$A^{2k} v_1 = A^k v_1 + A^k w = v_1 + 2w,$$

and in general $A^{ik}v_1 = v_1 + iw$, $i = 1, 2, \ldots, p$. So $\theta(v_1) = v_1 + U_k$ and now apply Theorem 2.1.

From Theorem 3.1 we note that in most cases (the exceptional cases being (b)–(d)) the radical of $C(A)$ is the intersection of those $N(\theta)$ where θ is a minimal orbit. This characterizes the radical as the set of functions that annihilate all minimal orbits.

Summarizing our results for the situation of this section we have the following.

THEOREM 3.2. *Let V be a finite vector space over the field F and let A be an invertible linear transformation on V. Then*

(i) *$C(A)$ is semisimple if and only if it is simple;*

(ii) *$C(A)$ is simple if and only if $m(x; V)$ is a product of distinct irreducible polynomials all having the same order;*

(iii) *If $C(A)$ is not simple and F is not a prime field then $J(C(A)) = \cap\{N(\theta) \mid \theta$ is a minimal orbit of $V^*\}$.*

REFERENCES

1. D. BLACKETT, "Simple and Semisimple Near-Rings," Ph.D. Dissertation, Princeton University, 1950.
2. G. BETSCH, Some structure theorems on 2-primitive near-rings, *in* "Rings, Modules and Radicals," Coll. Math. Soc. Janus Bolyai 6, Keszthely, Hungary/North-Holland, New York, 1973.
3. K. HOFFMAN AND R. KUNZE, "Linear Algebra," Prentice-Hall, Englewood Cliffs, N.J., 1961.
4. N. JACOBSON, "Lectures in Abstract Algebra," Vol. II, Van Nostrand, Princeton, N.J., 1953.
5. N. JACOBSON, "Theory of Rings," Amer. Math. Soc. Surveys, Vol. II, Amer. Math. Soc., Providence, R.I., 1943.
6. C. MAXSON AND K. SMITH, Automorphisms of linear automata, *J. Comput.*, to appear.
7. G. PILZ, "Near-Rings," North-Holland, New York, 1977.
8. D. SUPRUNENKO AND R. TYSHKEVICH, "Commutative Matrices," Academic Press, New York, 1968.