PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 87, Number 3, March 1983

DISTRIBUTIVELY GENERATED CENTRALIZER NEAR-RINGS

C. J. MAXSON AND K. C. SMITH

ABSTRACT. Let G be a finite group, $\mathcal{A}$ a group of automorphisms of G and $\mathcal{C}(\mathcal{A}; G)$ the centralizer near-ring determined by the pair $(\mathcal{A}, G)$. In this paper we investigate the structure of those centralizer near-rings $\mathcal{C}(\mathcal{A}; G)$ which are distributively generated. Particular attention is given to the situation in which G is a solvable group.

1. Introduction. Let G be a group written additively with identity 0, but not necessarily abelian and let $M_0(G)$ denote the near-ring of zero-preserving functions on G. For any near-ring N contained in $M_0(G)$, we say N is distributively generated (d.g.) if there exists a monoid $\mathcal{S}$ of endomorphisms of G that additively generates N. Thus if N is d.g. by $\mathcal{S}$ then every function f in N has the form $f = \sum_{i=1}^{t} \varepsilon_i \sigma_i$, $\varepsilon_i \in \{-1, 1\}$, $\sigma_i \in \mathcal{S}$. For any group $\mathcal{A}$ of automorphisms of G, the set of functions $\mathcal{C}(\mathcal{A}; G) = \{f: G \to G \mid f(0) = 0, f\alpha(x) = \alpha f(x), \alpha \in \mathcal{A}, x \in G\}$ is a subnear-ring of $M_0(G)$ called the *centralizer near-ring* determined by $\mathcal{A}$ and G. It is the purpose of this paper to initiate a study of the characterization of those centralizer near-rings that are distributively generated.

In this paper all groups will be finite, all near-rings will be finite, zero-symmetric and have an identity element. As in **[3]**, when $\mathcal{A}$ is a group of automorphisms of a group G, $\theta(v) = \{\alpha v \mid v \in G\}$ is the $\mathcal{A}$-orbit containing v and e_v is the map in $\mathcal{C}(\mathcal{A}; G)$ which is the identity on $\theta(v)$ and zero off $\theta(v)$. Further, for $v \in G$, $\operatorname{stab}(v) = \{\beta \in \mathcal{A} \mid \beta v = v\}$. For basic definitions and results concerning near-rings we refer the reader to the book by Pilz **[5]**.

Fröhlich, **[1]**, in 1958 determined the structure of the near-ring N generated by all inner automorphisms of a finite, nonabelian simple group H. This near-ring is simple and in fact $N = M_0(H)$. Later, Laxton **[2]** generalized Fröhlich's result to the following: Let $N \subseteq M_0(G)$ be a finite, simple d.g. near-ring with identity which is not a ring, then $N = M_0(G)$ and G is a finite, nonabelian invariantly simple group. (Recall that a subgroup H of a group G is fully invariant if $\sigma(H) \subseteq H$ for each endomorphism of G.) As an application of Laxton's result we let $N = \mathcal{C}(\mathcal{A}; G)$ be a simple d.g. centralizer near-ring which is not a ring. Thus $\mathcal{C}(\mathcal{A}; G) = M_0(G)$ so $\mathcal{A} = \{1_G\}$ and G is a nonabelian, invariantly simple group. Thus, as we shall see the work in this paper initiates a study of the problem suggested by Fröhlich that one investigate d.g. near-rings of $M_0(G)$ where G is not invariantly simple.

Received by the editors February 17, 1982.
1980 *Mathematics Subject Classification*. Primary 16A76; Secondary 16A44, 16A48.
Key words and phrases. Centralizer-near rings, distributively generated near-rings.

0002-9939/82/0000-0861/$02.25

The results here are also related to the recent work of the authors and M. R. Pettet [4]. There we considered the question "When is a centralizer near-ring a ring?". It was found that the only rings that occur as centralizer near-rings $\mathcal{C}(\mathcal{A}; G)$, $\mathcal{A}$ a group of automorphisms of G, are direct sums of fields. In the d.g. case we find a similar situation when G is a solvable group. In this special case in which $\mathcal{C}(\mathcal{A}; G)$ is d.g. we find that $\mathcal{C}(\mathcal{A}; G)$ is either a field or a direct sum of fields. This situation is illustrated in the following example.

EXAMPLE 1. Let $G = S_3$ and $\mathcal{A} = \operatorname{Aut} S_3$ ($= \operatorname{Inn} S_3$). Under the action of $\mathcal{A}$ on G we have $S_3 = \{(1)\} \cup \theta_1 \cup \theta_2$ where $\theta_1 = \{(12), (23), (13)\}$ and $\theta_2 = \{(123), (132)\}$. Further $\operatorname{stab}(12) = \{I, I(12)\}$, $\operatorname{stab}(13) = \{I, I(13)\}$, $\operatorname{stab}(23) = \{I, I(23)\}$ and $\operatorname{stab}(123) = \operatorname{stab}(132) = \{I, I(123), I(132)\}$ where $I(a)$ is the inner automorphism determined by a. Let $e_i \in \mathcal{C}(\mathcal{A}; G)$ denote the identity function on θ_i and zero off θ_i, $i = 1, 2$. Then using the results of [3] it is easily seen that

$$\mathcal{C}(\mathcal{A}; G) = \{0, 1, e_1, e_2, \alpha e_2, e_1 + \alpha e_2\}$$

where $\alpha(123) = (132)$. Thus $\mathcal{C}(\mathcal{A}; G) = S_1 \oplus S_2$, $S_1 = \{0, e_1\}$, $S_2 = \{0, e_2, \alpha e_2\}$, and so $\mathcal{C}(\mathcal{A}; G)$ is a direct sum of fields. We note that $\mathcal{C}(\mathcal{A}; G)$ is distributively generated by $\mathcal{S} = \{I\}$. Hence distributively generated centralizer near-rings do occur.

We conclude this section with a short summary of the remainder of the paper. In the next section we present some general results about d.g. centralizer near-rings. In the final section we specialize to the case in which G is a solvable group and apply our results to completely determine when $\mathcal{C}(\mathcal{A}; G)$ is d.g., G solvable.

2. Preliminary results. In this section we develop general results needed for our study of d.g. centralizer near-rings. As we indicated above, the setting is as follows: G is a finite group, $\mathcal{A}$ a group of automorphisms of G and N is a subnear-ring of $\mathcal{C}(\mathcal{A}; G)$. For convenience we shall call N a *basic* subnear-ring of $\mathcal{C}(\mathcal{A}; G)$ if $e_v \in N$ for every $\mathcal{A}$-orbit $\theta(v)$ of G.

PROPOSITION 1. *Let N be a basic d.g. subnear-ring of $\mathcal{C}(\mathcal{A}; G)$. If H is a fully invariant subgroup of G then every $\mathcal{A}$-orbit of $G - H$ is a union of cosets of H in G.*

PROOF. Let $\mathcal{S}$ be the set of endomorphisms of G which are the generators for N. If $f \in N$ then $f = \sum \varepsilon_i \Phi_i$ where $\varepsilon_i = \pm 1$, $\Phi_i \in \mathcal{S}$. For $v \in G - H$, $h \in H$, we have

$$f(v + h) = \sum \varepsilon_i \Phi_i(v + h) = \sum \varepsilon_i(\Phi_i(v) + \Phi_i(h)) = \sum \varepsilon_i \Phi_i(v) + h'$$

for some $h' \in H$, using the normality of H in G. Thus $f(v + h) = f(v) + h'$.

Suppose v, $v + h$ belong to different orbits. Then, since $e_v \in N$, $0 = e_v(v + h) = e_v(v) + h' = v + h'$ which would mean $v \in H$, a contradiction. So $v + h \in \theta(v)$ for every $h \in H$ and $\theta(v)$ is a union of cosets of H.

PROPOSITION 2. *Let N be a basic d.g. subnear-ring of $\mathcal{C}(\mathcal{A}; G)$. Suppose H is a fully invariant subgroup of G and let $\bar{\mathcal{A}}$ be the automorphism group of H which is obtained by restricting the elements of $\mathcal{A}$ to H. If $\bar{N}$ is the subnear-ring of $\mathcal{C}(\bar{\mathcal{A}}; H)$ consisting of the elements of N restricted to H, then $\bar{N}$ is basic and d.g.*

PROOF. The map ψ: $N \to \bar{N}$ defined by $\psi(f)$ is the restriction of f to H and is a homomorphism of N onto $\bar{N}$. Since N is basic in $\mathcal{C}(\mathcal{A}; G)$, $\bar{N}$ is basic in $\mathcal{C}(\bar{\mathcal{A}}; H)$. Since N is d.g., so is $\bar{N}$.

PROPOSITION 3. *Let N be a basic d.g. subnear-ring of $\mathcal{C}(\mathcal{A}; G)$. If $H \neq \{0\}$ is a fully invariant abelian subgroup of G, then H^* is an orbit.*

PROOF. By Proposition 2, $\bar{N}$ is a basic d.g. subnear-ring of $\mathcal{C}(\bar{\mathcal{A}}; H)$. Since H is abelian, the set $\mathrm{End}(H)$ of all endomorphisms of H is a ring. Hence $\bar{N}$ is a ring of endomorphisms of H.

Assume H^* has two distinct orbits $\theta(h)$, $\theta(\tilde{h})$. If $h + \tilde{h} \notin \theta(h)$, then since $e_h \in \bar{N}$ we have $0 = e_h(h + \tilde{h}) = e_h(h) + e_h(\tilde{h}) = h$, a contradiction. On the other hand, if $h + \tilde{h} \in \theta(h)$ then $h + \tilde{h} = e_h(h + \tilde{h}) = h$, and $\tilde{h} = 0$, again a contradiction. So H^* is one orbit.

PROPOSITION 4. *Let N be a basic d.g. subnear-ring of $\mathcal{C}(\mathcal{A}; G)$. If H is a fully invariant subgroup of G such that G/H is abelian, then $G - H$ is one orbit.*

PROOF. Since G/H is abelian then for every $v, w \in G - H$, $v + w = w + v + h$ for some $h \in H$. Since N is d.g. then as in the proof of Proposition 1, $f(v + w) = f(v) + f(w) + h'$ for every $v, w \in G - H, f \in N$ and some $h' \in H$.

Suppose $\theta(v)$, $\theta(w)$ are distinct orbits in $G - H$. If $v + w \notin \theta(v)$ then $0 = e_v(v + w) = e_v(v) + e_v(w) + h' = v + h'$ and $v \in H$, a contradiction. A similar contradiction is reached if $v + w \in \theta(v)$. So $G - H$ is an orbit.

PROPOSITION 5. *Let G be a nilpotent group. If N is a basic d.g. subnear-ring of $\mathcal{C}(\mathcal{A}; G)$ then N is a field, G is an abelian p-group of exponent p and $\mathcal{A}$ acts transitively on G^*.*

PROOF. Every nilpotent group contains a fully invariant subgroup $H \neq \{0\}$ such that H is a subgroup of the center of G. Since N is d.g. then $f(v + h) = f(v) + f(h)$ for all $f \in N$, $v \in G - H$, $h \in H$. By Proposition 1, $v + h \in \theta(v)$. We have $v + h = e_v(v + h) = e_v(v) + e_v(h) = v + 0 = v$ and $h = 0$. This gives a contradiction unless $G = H$, hence G is abelian and N is a ring. By Proposition 3, G^* is an orbit, so G is an abelian p-group of exponent p and $\mathcal{C}(\mathcal{A}; G)$ is a near-field. As a subring of $\mathcal{C}(\mathcal{A}; G)$, N must be a field.

3. Distributively generated $\mathcal{C}(\mathcal{A}; G)$, G solvable. Throughout this section G is assumed to be a finite solvable group. It is our goal to show that if $\mathcal{C}(\mathcal{A}; G)$ is distributively generated with G solvable then $\mathcal{C}(\mathcal{A}; G)$ is a ring and thus a direct sum of fields (see [**4**]).

Since G is solvable, its series of higher commutator subgroups $G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{0\}$, where as usual $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$, $i = 1, 2, \ldots, n$, forms a normal series whose factor groups are abelian. For our purposes it is important to observe that each higher commutator subgroup $G^{(i)}$ is a fully invariant subgroup of G. If G is a solvable group such that $G^{(n)} = \{0\}$, $G^{(n-1)} \neq \{0\}$ then we shall say G has derived length n.

If G has derived length 1 then G is abelian and $\mathcal{C}(\mathfrak{A}; G)$ d.g. implies $\mathcal{C}(\mathfrak{A}; G)$ is a field by Proposition 3. The length 2 case is handled in the following theorem, and is illustrated by the example in §1.

THEOREM 1. *Suppose G is a solvable group with derived length 2 and $\mathcal{C}(\mathfrak{A}; G)$ is d.g. for some automorphism group $\mathfrak{A}$ of G. Then $\mathcal{C}(\mathfrak{A}; G)$ is a ring and G is a Frobenius group of order qp^n, p and q distinct primes.*

PROOF. As a consequence of Proposition 5 we may assume G is not a nilpotent group, and hence not a p-group. Let $H = G^{(1)}$, a fully invariant nonzero subgroup of G. Since G has length 2, H is abelian and G/H is abelian. By Propositions 3 and 4, G^* has two orbits under $\mathfrak{A}$, namely $G - H$, H^*. It is known [**4**, Theorem 4] that since G is not a p-group, G must be a Frobenius group of order qp^n with p, q distinct primes. Moreover H is the Frobenius kernel of G and H is an elementary abelian group with order p^n. A Frobenius complement for G is a cyclic group Q of order q. From a result of S. Garrison (see the following lemma) we find that if $v \in G - H$ and $h \in H^*$ then $\operatorname{stab}(v) \not\subseteq \operatorname{stab}(h)$. Since $\mathcal{C}(\mathfrak{A}; G)$ is distributively generated, H is $\mathcal{C}(\mathfrak{A}; G)$-invariant and $\operatorname{stab}(v) \not\supseteq \operatorname{stab}(h)$. So there are no proper stabilizer containments among elements of G^*, and by [**3**, Theorem 4], $\mathcal{C}(\mathfrak{A}; G)$ is semisimple. Since there are two orbits in G^*, $\mathcal{C}(\mathfrak{A}; G)$ is a direct sum of two near-fields. Since $\mathcal{C}(\mathfrak{A}; G)$ is d.g. it is a direct sum of two fields and hence a ring.

LEMMA (GARRISON). *For distinct primes p and q let G be a Frobenius group of order qp^n having kernel H, $|H| = p^n$, and complement Q, $|Q| = q$. Suppose $\mathfrak{A}$ is a group of automorphisms of G which acts transitively on both H^* and $G - H$. If $v \in G - H$ and $h \in H^*$ then* $\operatorname{stab}(v) \not\subseteq \operatorname{stab}(h)$.

PROOF. Suppose $v \in G - H$, $h \in H^*$ with $\operatorname{stab}(v) \subseteq \operatorname{stab}(h)$. We have $|\theta(v)| = (q-1)p^n = |\mathfrak{A} : \operatorname{stab}(v)|$. Let $\mathfrak{B} = \{\alpha \in \mathfrak{A} \mid \alpha(nv + H) = nv + H$ for all n, $n = 0, 1, \ldots, q-1\}$ a subgroup of $\mathfrak{A}$. We note that $\operatorname{stab}(v) \subseteq \mathfrak{B}$, $\mathfrak{B}$ is a normal subgroup of $\mathfrak{A}$ and $|\mathfrak{A} : \mathfrak{B}| = q - 1$. Let $I = \operatorname{stab}(h) \cap \mathfrak{B}$, then $|\mathfrak{B} : I|$ divides $|\mathfrak{B} : \operatorname{stab}(v)| = p^n$. Also $|\mathfrak{B} : I|$ divides $|\mathfrak{A} : \operatorname{stab}(h)| = p^n - 1$ and so $\mathfrak{B} = I$, and $\operatorname{stab}(h) \supseteq \mathfrak{B}$. We have $q - 1 = |\mathfrak{A} : \mathfrak{B}| = |\mathfrak{A} : \operatorname{stab}(h)|\,|\operatorname{stab}(h) : \mathfrak{B}| = (p^n - 1)|\operatorname{stab}(h) : \mathfrak{B}|$, and $|\mathfrak{A} : \operatorname{stab}(h)| = p^n - 1 < q - 1$. This is impossible since

$$(q-1)p^n = |\mathfrak{A} : \operatorname{stab}(v)| = |\mathfrak{A} : \operatorname{stab}(h)|\,|\operatorname{stab}(h) : \operatorname{stab}(v)|$$
$$= (p^n - 1)\,|\operatorname{stab}(h) : \operatorname{stab}(v)|$$

and $q - 1$ divides $p^n - 1$.

PROPOSITION 6. *If G is a solvable group with derived length 3 which is not a p-group and if $\mathfrak{A}$ is any automorphism group of G, then $\mathcal{C}(\mathfrak{A}; G)$ is not distributively generated.*

PROOF. Assume G is a solvable group with derived length 3 and with an automorphism group $\mathfrak{A}$ such that $\mathcal{C}(\mathfrak{A}; G)$ is distributively generated. Then $G \supset G^{(1)} \supset G^{(2)} \supset G^{(3)} = \{0\}$. Let $H = G^{(1)}$ and $K = G^{(2)}$. From Propositions 2, 3, 4 and Theorem 1, the orbits of G^* are $G - H$, $H - K$ and K^*. Moreover if $\bar{\mathfrak{A}}$ is $\mathfrak{A}$ restricted to H then $\mathcal{C}(\bar{\mathcal{A}}; H)$ is distributively generated by Proposition 2. From the proof of Theorem 1, H is a Frobenius group of order qp^n with $[H: K] = q$ and K is an elementary abelian group of order p^n. Since $\mathcal{A}$ acts transitively on $G - H$ we must have $[G: H] = r^m$ for some prime r.

Assume $r \neq p, q$. Then $G - H$ contains an element of order r and since $G - H$ is an orbit, then every element in $G - H$ has order r. Hence every element in G^* would have order either r, p or q. By Theorem 3 of **[4]**, the only finite groups having the property that every nonidentity element has prime order are p-groups of exponent p, Frobenius groups of order qp^n, and the alternating group A_5. None of these is possible in this case. (A_5 is excluded because it is not solvable.)

Assume $r = q$. Then $\tilde{G} \equiv G/K$ is a q-group. If $\tilde{\mathcal{A}}$ is the automorphism group on $\tilde{G}$ induced by $\mathcal{A}$, then $\tilde{G}^*$ has two $\tilde{\mathcal{A}}$-orbits. The function Φ: $\mathcal{C}(\mathcal{A}; G) \to \mathcal{C}(\tilde{\mathcal{A}}; \tilde{G})$ defined by $\Phi: f \to \tilde{f}$ where $\tilde{f}(a + G) = f(a) + G$, is a homomorphism of $\mathcal{C}(\mathcal{A}; G)$ into $\mathcal{C}(\tilde{\mathcal{A}}; \tilde{G})$. The image of Φ is a basic d.g. subnear-ring of $\mathcal{C}(\tilde{\mathcal{A}}; \tilde{G})$. By Proposition 5, $\tilde{\mathcal{A}}$ acts transitively on $\tilde{G}^*$, a contradiction.

Assume $r = p$, which is the remaining possibility. The group G/K has two nonzero orbits under the automorphism group induced by $\mathcal{A}$. By Theorem 4 of **[4]**, the order of G/K must be pq. This means $[G: H] = p$. We now have $|G| = qp^{n+1}$ with $[G: H] = p$, $[H: K] = q$, $|K| = p^n$ and H is a Frobenius group of order qp^n. To prove no such group exists we use an argument suggested by S. Gagola. Let Q be a Sylow q-subgroup of H, a cyclic group of order q. By the Frattini argument **[6**, p. 88], $G = N_G(Q)H$. We have $|N_G(Q) \cap H|\,|G| = |N_G(Q)|\,|H|$, or

$$|N_G(Q) \cap H|\, qp^{n+1} = |N_G(Q)|\, qp^n$$

and so p divides $|N_G(Q)|$. We claim $N_G(Q) \cap K = \{0\}$. Assume $v \in N_G(Q) \cap K$, $v \neq 0$. Then for $x \in Q$, $v + x - v = ix$, $1 \leqslant i < q$. Hence $v + x - v - x \in Q \cap K = \{0\}$. So $v + x = x + v$ which is impossible because $v + x$ would have order pq. So $N_G(Q) \cap K = \{0\}$ and $N_G(Q)$ contains an element of order p not in K and therefore in $G - H$. This means every element in $G - H$ has order p and thus every element in G^* has order p or q, and G is Frobenius by Theorem 3 of **[4]**. But such a Frobenius group would have a normal Sylow subgroup and our group does not, again a contradiction. Since none of the possibilities can occur we conclude that $\mathcal{C}(\mathcal{A}; G)$ cannot be distributively generated.

THEOREM 2. *Suppose $\mathcal{C}(\mathcal{A}; G)$ is distributively generated and G is solvable. Then $\mathcal{C}(\mathcal{A}; G)$ is a ring and G has derived length* 2.

PROOF. From Theorem 1 and Proposition 6 it suffices to show that the derived length of G cannot be larger than 3. Assume $\mathcal{C}(\mathcal{A}; G)$ is d.g. with G having derived length 4. Let H be the commutator subgroup of G and let $\bar{\mathcal{A}}$ be the automorphism group on H induced by $\mathcal{A}$. Then H has derived length 3 and $\mathcal{C}(\bar{\mathcal{A}}; H)$ is d.g., an impossible situation due to Proposition 6. Inductively it is seen that the derived length of G cannot be larger.

References

1. A Fröhlich, *The near-ring generated by the inner automorphisms of a finite simple group*, J. London Math. Soc. **33** (1958), 95–107.

2. R. R. Laxton, *Primitive distributively generated near-rings*, Mathematika **8** (1961), 143–158.

3. C. J. Maxson and K. C. Smith, *The centralizer of a set of group automorphisms*, Comm. Algebra **8** (1980), 211–230.

4. C. J. Maxson, M. R. Pettet and K. C. Smith, *On semisimple rings that are centralizer near-rings*, Pacific J. Math. (to appear).

5. G. Pilz, *Near-rings*, North-Holland, New York, 1977.

6. J. J. Rotman, *The theory of groups, an introduction*, 2nd ed., Allyn & Bacon, Boston, Mass., 1973.

Department of Mathematics, Texas A & M University, College Station, Texas 77843-3368