Proceedings of the Edinburgh Mathematical Society (1979), 22, 241–245 ©

INVOLUTION NEAR-RINGS

by S. D. SCOTT

(Received 10th April 1978)

Throughout this paper all near-rings considered will be zero-symmetric and left distributive. All groups will be written additively, but this does not imply commutativity. The near-ring of all zero-fixing maps of a group V into itself will be denoted by $M_0(V)$. If N is a near-ring with an identity and $\alpha \neq 1$ is an element of N such that $\alpha^2 = 1$, then α will be called an *involution* of N. Let V be a group. An involution α of $M_0(V)$ will be called an involution on V.

If S is a subset of a near-ring N, then $N(S)$ will denote the subnear-ring of N generated by S. If S consists of the single element γ, we write $N(\gamma)$ for $N(\{\gamma\})$. We shall call a near-ring N with identity an *involution near-ring*, if N contains an involution α such that $N(\alpha) = N$. We are now in a position to state our main theorem.

Theorem 1. *If V is a non-trivial finite group, then $M_0(V)$ is an involution near-ring if, and only if, V is neither an elementary abelian 2-group nor a cyclic group of order three.*

To prove this theorem we will require certain lemmas, propositions and definitions. Also we shall clarify and explain some notation.

If S is a set, then $|S|$ will denote the cardinal of S. We shall, on the whole, be concerned only with finite sets. If K is a subset of S we write $S \setminus K$ for the complement of K in S.

From now on all groups considered will be finite. Let G be a group. As for sets, $|G|$ is the order of G. If S is a subset of G, then $\langle S \rangle$ will denote the subgroup of G generated by S (if S is empty, $\langle S \rangle$ is taken as $\{0\}$ and if S consists of the single element g, we write $\langle g \rangle$ for $\langle \{g\} \rangle$). The order $|\langle g \rangle|$ of an element g of G will be denoted by $|g|$. The set of all g in G such that $|g| = 2$ will be denoted by $\eta(G)$. To avoid confusion the elements of $\eta(G)$ will not be referred to as involutions. We denote the set $G \setminus \{0\}$ by G^*. A subgroup of G that will play an important role in what follows is $\lambda(G)$, which is defined to be $\langle G^* \setminus \eta(G) \rangle$. Thus $\lambda(G)$ is the subgroup of G generated by all elements g of G such $|g| > 2$. We define the centraliser of a subgroup H of G in the normal manner. Thus $C_G(H)$ will denote the subgroup of G consisting of all elements b of G such that $-b + h + b = h$ for all h in H.

Proposition 2. *If G is a non-trivial group and $\lambda(G) = \{0\}$, then G is an elementary abelian 2-group.*

Proposition 3. *If G is a group, then $\lambda(G)$ is a normal subgroup of G.*

Proof. We shall in fact show that $\lambda(G)$ is characteristic in G. Assume $\lambda(G) \neq \{0\}$. Let g in G be such that $|g| > 2$ and let μ be an automorphism of G. Then $|g\mu| = |g| > 2$. So μ maps $G^* \setminus \eta(G)$ into $G^* \setminus \eta(G)$ and $\lambda(G)$ is characteristic in G.

Lemma 4. *Let G be a group and suppose $\{0\} < \lambda(G) < G$. The following hold:*
(i) $G\setminus\lambda(G) \subseteq \eta(G)$;
(ii) *if b is in $G\setminus\lambda(G)$ and g in $\lambda(G)$, then $-b+g+b=-g$;*
(iii) *$\lambda(G)$ is abelian;*
(iv) *$C_G(\lambda(G)) = \lambda(G)$; and*
(v) $|G/\lambda(G)| = 2$.

Proof. (i) This is obvious.

(ii) Since b is in $G\setminus\lambda(G)$ and g in $\lambda(G)$, $b+g$ is in $G\setminus\lambda(G)$. By (i) $b+g+b+g=0$. By (i) $b=-b$ and (ii) follows.

(iii) Let b be in $G\setminus\lambda(G)$. By (ii) the inner automorphism induced by b maps every element of $\lambda(G)$ to its inverse. This is an automorphism of $\lambda(G)$ only if $\lambda(G)$ is abelian.

(iv) Since $\lambda(G)$ is abelian, $C_G(\lambda(G)) \geqslant \lambda(G)$. Suppose $C_G(\lambda(G)) > \lambda(G)$ and let b be an element of $C_G(\lambda(G))\setminus\lambda(G)$ and g an element of $\lambda(G)$ such that $|g| \neq 2$. But, by (ii), it would then follow that $-b+g+b=-g\neq g$. Hence $C_G(\lambda(G)) = \lambda(G)$.

(v) If b_1 and b_2 are in $G\setminus\lambda(G)$ and g in $\lambda(G)$, then

$$-b_1+g+b_1=-g$$

and

$$-b_2-b_1+g+b_1+b_2=g$$

by (ii). Hence b_1+b_2 is in $C_G(\lambda(G)) = \lambda(G)$. Thus $b_1 \equiv -b_2 \bmod \lambda(G)$ and (v) follows. The proof of the lemma is now complete.

Definition. Let G be a group and S a collection of subgroups of G. A bijection β of G onto G will be said to *confuse* S, if for any H in S, $H\beta \not\subseteq H$.

Lemma 5. *Let G be a non-zero group which is neither an elementary abelian 2-group nor a group of order three. There exists an involution α on G which confuses proper subgroups of G and is such that*
(i) *if $|G|$ is even, then α has a unique fixed element $h\neq 0$.*
(ii) *if $|G|$ is odd, then α fixes only two non-zero elements b_1, b_2 and $b_1+b_2\neq 0$.*

Proof. Let $A_1,\ldots,A_n$ be the distinct non-zero cyclic subgroups of G of order greater than two, and let g_i generate A_i for $1\leqslant i\leqslant n$. Set $S=\{g_1,-g_1,\ldots,g_n,-g_n\}$. Clearly $g_i\neq -g_i$ as $|g_i|>2$. If $|G|$ is even, let $a_1,\ldots,a_{2k+1}$, be the elements of $\eta(G)$ (note that $|\eta(G)|$, the number of subgroups of G of order two, is odd by the Sylow Theorems). By (i) of Lemma 4 we may assume that if $\lambda(G)<G$, then a_{2k+1} is in $G\setminus\lambda(G)$.

Finally partition the elements of $G\setminus\{S\cup\eta(G)\}=T$ by $\{g,-g\}$. Define α by:
α interchanges g_i and $-g_{i+1}$ for $1\leqslant i\leqslant n-1$ (vacuous if $n=1$), and α interchanges g and $-g$ for g in T.

(a) if $|G|$ is odd an $n>1$, α fixes $-g_1$ and g_n,

(a)′ if $|G|$ is odd and $n=1$, then $|G|$ is a prime p greater than three and thus $G^*=\{a_1,\ldots,a_{p-1}\}$, where we may assume that $a_{p-1}\neq -a_{p-2}$. Let α fix a_{p-1} and a_{p-2} and interchange the rest in pairs.

(b) if $|G|$ is even, let α interchange a_{2k+1} and $-g_1$, a_{2i-1} and a_{2i} for $1 \leqslant i \leqslant k$ (vacuous if $k = 0$), and fix g_n.

Then $\alpha \neq 1$, $\alpha^2 = 1$ and α is an involution. Let H be a non-zero subgroup of G such that $H\alpha \subseteq H$. If H contains an element of order greater than two, then some g_i is in H. Thus $-g_i$ is in H and, by the definition of α, $H \supseteq \{g_1, \ldots, g_n\}$. If $|G|$ is odd and $n > 1$, then $H = G$. If $|G|$ is odd and $n = 1$, then $H = G$ anyway. If $|G|$ is even, then $\lambda(G) \leqslant H$ and by the definition of α, a_{2k+1} is in H. Thus $H = G$ since, if $G > \lambda(G)$, then $\lambda(G)$ is a maximal subgroup of G by Lemma 4.

We may therefore assume that $H\alpha \subseteq H$ and $H^* \subseteq \eta(G)$. Clearly a_{2k+1} is not in H, otherwise g_1 is in H. By the definition of α, a_{2i} is in H if, and only if, a_{2i-1} is in H. Thus $|H^*|$ is even. However, H is an elementary abelian 2-group and $|H^*| = |H| - 1$ is odd. This contradiction completes the proof.

The question remains as to whether or not elementary abelian 2-groups are a genuine exception to Lemma 5.

Proposition 6. *If A is an elementary abelian 2-group and α an involution on A, then there exists a proper subgroup H of A such that $H\alpha \subseteq H$.*

Proof. As a cyclic group of order two has no involutions we may assume that $|A| \geqslant 4$. Let S be the set of all b in A^* such that $b\alpha = b$. Since $A^* \setminus S$ is partitioned by two element subsets of the form $\{g, g\alpha\}$ where G is in $A^* \setminus S$, it follows that $|A^* \setminus S|$ is even. Since $|A^*|$ is odd, $|S|$ is odd. Thus S is non-empty. Let h be in S. We have $h\alpha = h$ and $h \neq 0$. Let $H = \langle h \rangle$. Clearly H is a proper subgroup of A and $H\alpha \subseteq H$. The proposition is now proved.

There remains the case of a cyclic group of order three.

Proposition 7. *If G is a group of order three, then there exists a unique involution α on G and α is an automorphism.*

Proof. Let h_1 and h_2 be the non-zero elements of G. Since an involution α on G is such that $0\alpha = 0$ and distinct from 1, it is clear that $h_1\alpha = h_2$ and $h_2\alpha = h_1$. Thus α is the unique involution on G. Also $h_2 = -h_1$ and $h\alpha = -h$ for all h in G. Thus α is an automorphism.

If G is a non-trivial group which is not an elementary abelian 2-group, it follows from Lemma 5 that there exists an involution α on G that confuses proper subgroups, provided $|G| \neq 3$. In the case where $|G| = 3$ the involution α of Proposition 7 may be considered to confuse proper subgroups. Proposition 6 tells us that this is an "if, and only if" result. Thus we have:

Theorem 8. *A non-zero group G has an involution α on G that confuses proper subgroups if, and only if, G is not an elementary abelian 2-group.*

We are now in a position to prove Theorem 1.

Proof of Theorem 1. Let V be a non-zero group and β an involution of $M_0(V)$ that confuses proper subgroups of V. Set $N = M_0(V)$. We make three straightforward observations:

(a) V is a unitary $N(\beta)$-group;

(b) $N(\beta)$ is 2-primitive on V (see (**2**, 4.2, p. 103)); and

(c) if β is distributive in $N(\beta)$, then β is an automorphism of V.

Firstly, we prove these results. Clearly $N(\beta) \leq N$ and, since the identity of N is in $N(\beta)$, V is a unitary $N(\beta)$-group. Thus (a) holds. If H is an $N(\beta)$-subgroup of V, then $HN(\beta) \subseteq H$. However β confuses proper subgroups of V and thus $H = \{0\}$ or $H = V$. Hence (b) holds. If v is a non-zero element of V, then $vN(\beta)$ is an $N(\beta)$-subgroup of V. Also $vN(\beta)$ is non-zero by (a) and $vN(\beta) = V$ by (b). Let v_1 and v_2 be two elements of V. We have $v_i = v\gamma_i$, $i = 1, 2$, where γ_i is in $N(\beta)$. Thus

$$\begin{aligned}(v_1 + v_2)\beta &= v(\gamma_1 + \gamma_2)\beta \\ &= v\gamma_1\beta + v\gamma_2\beta \\ &= v_1\beta + v_2\beta.\end{aligned}$$

Since β is a bijection on V, it is an automorphism of V and (c) holds.

We now assume that V is not an elementary abelian 2-group and $|V|$ is even. By Lemma 5 there exists an involution α on V, that confuses proper subgroups of V and is such that $h\alpha = h$ for some unique non-zero element h of V. By (b) $N(\alpha)$ is 2-primitive on V. If $N(\alpha)$ is a ring, then α is an automorphism of V by (c), and all v in V such that $v\alpha = v$ form a subgroup of V. Thus $\{0, h\}$ is a subgroup of V such that $\{0, h\}\alpha = \{0, h\}$. Hence $\{0, h\} = V$. But, since V is not an elementary abelian 2-group, this cannot happen. Hence $N(\alpha)$ is not a ring. Let μ be an $N(\alpha)$-automorphism of V. By (**2**, 4.61, p. 132) we need only show that μ is the identity. If $\mu \neq 1$, it acts fixed point freely on V. Since $h\alpha = h$, it follows that $h\mu\alpha = h\mu$ and, by the uniqueness of h, $h\mu = h$. Thus $\mu = 1$ and $N(\alpha) = N$ in this case.

Assume $|V|$ is odd and $|V| > 3$. By Lemma 5 there exists an involution α on V, that confuses proper subgroups of V and is such that $b_1\alpha = b_1$ and $b_2\alpha = b_2$ for a unique non-zero pair of elements b_1 and b_2 of V. Furthermore we may assume that $b_1 \neq -b_2$. Now $N(\alpha)$ is 2-primitive on V by (b). If $N(\alpha)$ is a ring, then by (c) we have the set of all v in V such that $v\alpha = v$ is a subgroup of V. It would then follow that $\{0, b_1, b_2\}$ is a subgroup of V fixed by α and this in turn implies that $\{0, b_1, b_2\} = V$. Since $|V| \neq 3$, we conclude that $N(\alpha)$ is not a ring. Let μ be an $N(\alpha)$-automorphism of V. Again by (**2**, 4.61, p. 132) we need only show that μ is the identity. Now $b_1\alpha = b_1$ and thus $b_1\mu\alpha = b_1\mu$. If $\mu \neq 1$, then it is fixed point free on V and $b_1\mu = b_2$. Similarly $b_2\mu = b_1$. Thus $b_1\mu^2 = b_1$ and it follows that $\mu^2 = 1$. By (**1**, 1.4, p. 336) $b_1\mu = -b_1 \neq b_2$. This contradiction establishes that $N(\alpha) = N$.

Conversely, if V is an elementary abelian 2-group and α an involution of $M_0(V)(= N)$, then by Proposition 6 $H\alpha \subseteq H$ for some proper subgroup H of V. Thus $HN(\alpha) \subseteq H$ and $N(\alpha)$ is not 2-primitive on V as is N. Hence $N(\alpha) \neq N$. Finally, if V is a cyclic group of order three and α an involution of $M_0(V)$, then by Proposition 7, α is an automorphism of V. Since V is abelian, $N(\alpha)$ is a ring. However, $N = M_0(V)$ is a non-ring. The proof is complete and Theorem 1 is established.

Corollary. *A finite non trivial near-ring N may be embedded in the involution near-ring $M_0((N,+)\oplus C_3$ $(=N')$ where C_3 is a cyclic group of order three.*

Proof. By (2, 1.86, p. 33) N can be embedded in N'. By Theorem 1 N' is an involution near-ring.

Let V be a group satisfying the conditions of Theorem 1. It is natural to ask how many involutions α in $M_0(V)(=N)$ exist such that $N(\alpha)=N$? It is not difficult to show that if α is such an involution and μ an automorphism of V, then $\beta=\mu^{-1}\alpha\mu$ is an involution of N distinct from α and such that $N(\beta)=N$. From this we conclude that the number of such involutions is at least $|A|$, where A is the automorphism group of V.

Another question is whether or not the above corollary holds for infinite near-rings. In fact it does not hold. Indeed, let N_1 be the near-ring with identity generated by a single element α and where the only defining relationship is $\alpha^2=1$. Let N be any near-ring such that $|N|>|N_1|$. The near-ring N cannot be embedded in an involution near-ring.

Also, what can be said about a near-ring generated by an involution which is distributive? Such near-rings may have a surprisingly complex structure. There are, for example, an infinite number of such near-rings which are finite, 0-primitive but not 2-primitive (3). In particular such a finite near-ring N may have a non-nilpotent radical $(J_2(N))$.

Yet another question that arises naturally from Theorem 1 is the following:

If n is a fixed integer, then which of the near-rings $M_0(V)$ (V a finite group) are generated by a single element α such that $\alpha^n=1$? Theorem 1 answers this question for $n=2$. Even for $n=3$, this question seems difficult. If, for example, V is the symmetric group on three letters, then $M_0(V)$ is not generated by such an α as, in this case, V has four proper subgroups intersecting in zero and β can permute at most three elements of V.

The author wishes to thank the referee for his comments which helped condense the proof of Theorem 1.

REFERENCES

(1) D. Gorenstein, *Finite Groups* (Harper & Row).

(2) G. Pilz, *Near-rings* (North-Holland).

(3) S. D. Scott, A construction of monogenic near-ring groups and some applications, *Bull. Australian Math. Soc.* **19**, (1978), 1–4.

Department of Mathematics,
University of Auckland,
Auckland,
New Zealand.