ZERO DIVISORS AND FINITE NEAR-RINGS

S. LIGH and J. J. MALONE, Jr.

(Received 25 March 1969, revised 6 June 1969)

Communicated by G. B. Preston

A *near-ring* is a triple $(R, +, \cdot)$ such that $(R, +)$ is a group, $(R, \cdot)$ is a semigroup, and $\cdot$ is left distributive over $+$; *i.e.* $w(x+z) = wx+wz$ for each w, x, $z \in R$. The most comprehensive work on near-rings is [1]. A near-ring R is *distributively generated* if there exists $S \subset R$ such that $(S, \cdot)$ is a sub-semigroup of $(R, \cdot)$, each element of S is right distributive, and S is an additive generating set for $(R, +)$. Distributively generated near-rings, first treated in [3], arise out of consideration of the system generated by the endomorphisms of an (not necessarily commutative) additive group. A *near-field* is a near-ring such that the nonzero elements form a group under multiplication. Near fields are discussed in [9]. An element $x \neq 0$ in R is a *left (right) zero divisor* if there is $a \neq 0$ in R such that $xa = 0$ ($ax = 0$). A zero divisor is an element that is either a left or a right zero divisor. In a near-ring R it will be assumed that $0x = 0$ for each $x \in R$.

In Section 1 near-rings with no zero divisors are studied. In Section 2 it is shown that a near-ring with a finite number of zero divisors is finite. This generalizes a ring theoretic result. In Section 3 a ring theoretic result concerning elements that are not zero divisors is generalized to distributively generated near-rings.

1. Near-rings with no zero divisors

In this section it is assumed that all near-rings dealt with are finite and have no zero divisors.

LEMMA 1.1. Let R be a near-ring. For each nonzero $x \in R$ there exists a least positive integer n such that $x^{n+1} = x$ and, for this n, x^n is a left identity. In particular, if $x^2 = x$ then x is a left identity.

PROOF. Since $\{x^n | n \text{ a positive integer}\}$ is finite, it follows that for each nonzero x there exists a least positive integer n such that $x^n x = x$. As in the case of rings without zero divisors, one proves, by using left distributivity, that $R = xR$. But $R = xR$ and $x^n x = x$ imply that x^n is a left identity. In particular, if $n = 1$ then x is a left identity.

THEOREM 1.2. *If R has a nonzero right distributive element, then R is a near-field and $(R, +)$ is a commutative group.*

PROOF. Let $x \in R$, $x \neq 0$, be right distributive. By Lemma 1.1 there exists a positive integer n such that x^n is a left identity. From $(wx^n - w)\,x = 0$, $w \in R$, it follows that x^n is also a right identity. For an arbitrary nonzero $w \in R$, $R = wR$ so that there exists $z \in R$ such that $x^n = wz$. Thus $(R - \{0\}, \cdot)$ is a group. It was proved in [8] that the additive group of a near-field is commutative. (H. Zassenhaus [10] had previously shown that the additive group of a finite near-field is commutative.)

COROLLARY 1.3. *If R has a unique left identity, then R is a near-field.*

PROOF. Let e be the unique left identity. For nonzero $x \in R$, $x^n x = x = xx^n$ and $x^n y$ for each $y \in R$. Thus $e = x^n$ and $x = xe$ so that e is a right identity. But, as a right identity, e is right distributive.

LEMMA 1.4. [5, p. 60] *Let $(G, +)$ be a finite group with an automorphism α such that $\alpha^2 = I$ and such that 0 is the only fixed point for α. Then G is commutative.*

THEOREM 1.5. *Let R be a near-ring such that $(R, +)$ is noncommutative. Then for each $x \in R$ there is a unique $y \in R$ such that $x = y^2$.*

PROOF. Let $x \in R$, $x \neq 0$, and let n be the positive integer of Lemma 1.1. Assume $n = 2k$, where $k \geqq 1$. Consider the map α: $(R, +) \to (R, +)$ defined by $(y)\alpha = x^k y$. It is immediate that α is an automorphism and that $\alpha^2 = I$. Suppose there exists a nonzero $y \in R$ such that $x^k y = y$. Since $yR = R$ there exists $y' \in R$ such that $yy' = x^{2k}$. Then $x^k yy' = yy' = x^{2k}$, and $x^k = x^{2k}$. From this contradiction it follows that such a y does not exist. Thus α satisfies the conditions of Lemma 1.4 and $(R, +)$ is commutative. This contradiction implies that n is odd. Thus $n+1$ is even, say $n+1 = 2m$, and $(x^m)^2 = x$. Also if $(x^t)^2 = x$, then $t \geqq m$.

It remains to be shown that if $y^2 = x$, then $y = x^m$. From the first part of the proof, there exists a least positive integer t such that $(y^t)^2 = y$. Since $y^2 = x$, it follows that $y = y^{2t} = x^t$. This implies that the order of y (in the multiplicative group generated by x), namely $2t-1$, divides $2m-1$. Thus $t \leqq m$, so that $t = m$, and $y = x^m$.

EXAMPLE 1.6. The near-ring on $(Z_5, +)$ gives as $\neq 7$ in [2, Section 2.3] shows that Theorem 1.5 cannot be extended to near-rings defined on commutative groups.

On the elements of any group $(G, +)$ the multiplication defined by $0g = 0$ and $g_1 g = g$ for $g_1 \neq 0$ and $g \in G$ is such that $(G, +, \cdot)$ is a near-ring. This is one of the "trivial" multiplications discussed in [7]. For several classes of groups, this is the only near-ring with no zero divisors definable on the groups. Some such classes are given below.

Let R be a near-ring and let $x \in R$, $x \neq 0$. The map $\alpha_x : R \to R$ defined by $(y)\alpha_x = xy$ is an automorphism of $(R, +)$. Thus each row in the multiplication table of R may be considered to be (the images under) an automorphism. If x is

such that there exists a nonzero $y \in R$ so that $xy = y$, then $xz = z$ for each $z \in R$. This follows since $R = yR$ and z may be written as yw for some $w \in R$. This leads to

THEOREM 1.7. *If $(R, +)$ is a complete group, then the near ring R has the trivial multiplication.*

PROOF. Since the inner automorphism determined by conjugation by a nonzero x leaves x fixed, this result follows from the discussion above.

It is clear that in order for R to have a non-trivial multiplication, $(R, +)$ must have at least one fixed point free automorphism. The dihedral group D_8 has no fixed point free automorphism and so admits only the trivial multiplication. Also, a group with a unique element of order 2 such as the quaternion group Q_8 would admit only the trivial multiplication.

Again, for $x \neq 0$, in R, let n be the positive integer of Lemma 1.1. Then for $1 \leqq t < k \leqq n$, there cannot be a nonzero y such that $x^k y = x^t y$. For if $k = t+c$, it would follow that $x^c y = y$, with $c \leqq n-1$. From this contradiction it is seen that $xy, x^2y, \cdots, x^n y = y$ are distinct. Recalling that the $\alpha_x i$, $i = 1, \cdots, n$, where $(y)\alpha_x i = x^i y$, are automorphisms, one sees that the elements $(y)\alpha_x i$, $i = 1, \cdots, n$, are distinct elements of order $|y|$. Therefore n is less than or equal to the number of elements of order $|y|$ for each nonzero $y \in R$. Of course, n is the order (in the group of automorphisms of $(R, +)$) of the automorphism associated with left multiplication by x.

2. Near-rings with a finite number of zero divisors

In this section the zero element is also taken to be a zero divisor. K. Koh [6] has shown that a ring having $n+1$ left (right) zero divisors, n a positive integer, is finite and does not contain more than $(n+1)^2$ elements. In this section Koh's result is extended to near-rings.

THEOREM 2.1. *Let R be a near-ring with $n+1$ right zero divisors. Then R is finite and does not contain more than $(n+1)^2$ elements.*

PROOF. For each $y \in R$, define $R_y = \{x \in R | yx = 0\}$. Clearly R_y is a subgroup of R. Since R has $n+1$ right zero divisors, there is $a \in R$ such that $R_a \neq 0$ and the order of R_a is at most $n+1$. For otherwise R has more than $n+1$ right zero divisors. Let $w \neq 0$ be an element of R_a. The subgroup wR is contained in R_a since $a(wx) = (aw)x = 0x = 0$. Hence the order of wR is at most $n+1$. Consider the map $f: R \to wR$ defined by $(x)f = wx$ for each $x \in R$. It easily follows that f is a homomorphism, that the kernel of f is R_w, and that f is an onto map. Thus, using the fundamental homomorphism theorem in group theory, it follows that $R/R_w \cong wR$. Since the order of wR is the order of R/R_w, the order of R is the product of the order of wR and the order of R_w, which is less than or equal $(n+1)^2$.

https://doi.org/10.1017/S1446788700006807 Published online by Cambridge University Press

If in Theorem 2.1 right is changed to left, the conclusion does not follow. This is illustrated by

EXAMPLE 2.2. Let $(G, +)$ be an infinite group. Let H be a finite subset of G which contains 0 and has nonzero elements. Define $hg = 0$ for each $h \in H$, $g \in G$ and define $xg = g$ for each $x \in G-H$, $g \in G$. Then $(G, +, \cdot)$ is a near-ring [7]. Each element in H is a left zero divisor and H is finite; but G is not finite.

However, the conclusion may still be obtained if one of the left zero divisors is right distributive. This is shown in

THEOREM 2.3. *Let R be a near-ring with $n+1$ left zero divisors, at least one of which is right distributive. Then R is finite and does not contain more than $(n+1)^2$ elements.*

PROOF. For each $x \in R$, define $L_x = \{y \in R | yx = 0\}$. Note that L_x is a subgroup if x is right distributive. Let w be a right distributive element that is a left zero divisor. Then there is $z \neq 0$ in R such that $wz = 0$. Since there is only a finite number of left zero divisors, it is seen that the order of L_z is less than or equal to $n+1$. Since w is right distributive, $Rw = \{xw | x \in R\}$ is a subgroup of R. Furthermore, $Rw \subseteq L_z$ since $(xw)z = x(wz) = x0 = 0$. Hence the order of Rw is less than or equal to $n+1$. Consider the map $f: R \to Rw$ defined by $(x)f = xw$. Because w is right distributive, f is a homomorphism from R onto Rw. Thus $R/\mathrm{Ker} f \cong Rw$. But $\mathrm{Ker} f = R_w$. Since the order of L_w is less than or equal to $n+1$, it follows that the order of $\mathrm{Ker} f$ is less than or equal $n+1$. Consequently the order of R is less than or equal to $(n+1)^2$. This completes the proof.

3. Integral elements

In this section a result of N. Ganesan [4] is generalized.

DEFINITION 3.1. *Let R be a near-ring. An element $x \neq 0$ in R is said to be an integral element if x is not a zero divisor.*

Ganesan showed that the integral elements of a finite ring R determine a multiplicative group whose identity is also the identity element for R. This result cannot be extended to arbitrary near-rings (see Example 3.3 below) but can be extended to distributively generated near-rings.

THEOREM 3.2. *Let R be a distributively generated near-ring with a finite number of right zero divisors and at least one integral element. Then the set of integral elements of R is a multiplicative group whose identity is also the identity element for R.*

PROOF. According to Theorem 2.1, R is finite. If x is an integral element, then $xR = R$ and there is $e \in R$ such that $xe = x$. But $x(ex-x) = 0$ and this implies that $ex = x$. Hence e is an identity for x. For each $y \in R$, $x(ey-y) = 0$ and this implies $ey = y$. Since R is a distributively generated near-ring, $x = x_1 + x_2 + \cdots$

https://doi.org/10.1017/S1446788700006807 Published online by Cambridge University Press

$+x_n$ where x_i is either a right or anti-right distributive element. Thus

$$\begin{aligned}(ye-y)x &= (ye-y)x_1+(ye-y)x_2+\cdots+(ye-y)x_n\\ &= \pm(yex_1-yx_1)\pm(yex_2-yx_2)\pm\cdots\pm(yex_n-yx_n)\\ &= \pm(yx_1-yx_1)\pm(yx_2-yx_2)\pm\cdots\pm(yx_n-yx_n)\\ &= 0,\end{aligned}$$

with $+$ chosen if x_i is right distributive and $-$ chosen if x_i is anti-right distributive. The fact that x is not a zero divisor implies that $ye = y$. Thus e is an identity element for R.

It remains to be shown that the set N of integral elements forms a multiplicative group and e is the identity. Suppose $z, w \in N$. If there is $y \in R$ such that $(zw)y = 0$, then either z or w is a zero divisor. Thus N is closed under multiplication. Since e is an identity for R and $e \in N$, it follows that e is the identity for N. Now suppose $w \in N$. Since R is finite, $wR = R$ and there is a $z \in R$ such that $wz = e$. Since $w(zw-e) = 0$, it follows that z is the multiplicative inverse of w. Suppose there is $x \neq 0$ in R such that $zx = 0$. Then $x = wzx = w0 = 0$, which is a contradiction. Thus N is a multiplicative group and the theorem is proved.

If a near-ring is not d.g. then the integral elements may not form a multiplicative group. This is shown by

EXAMPLE 3.3. In the near-ring given as $\neq 10$ in [2, Section 2.1] the elements 1 and 3 are the integral elements, but they do not determine a multiplicative group.

References

[1] J. C. Beidleman, *On near-rings and near-ring modules*, Doctoral dissertation, The Pennsylvania State University, 1964.
[2] J. R. Clay, 'The near-rings on groups of low order', *Math. Z.* 104 (1968), 364–371.
[3] A. Fröhlich, 'Distributively generated near-rings', *Proc. London Math. Soc.* (3) 8 (1958), 76–108.
[4] N. Ganesan, 'Properties of rings with a finite number of zero divisors', *Math. Ann.* 157 (1964) 215–218.
[5] I. N. Herstein, *Topics in algebra* (Blaisdell, New York, 1964).
[6] K. Koh, 'On properties of rings with a finite number of zero divisors', *Math. Ann.* 171 (1967), 79–80.
[7] J. J. Malone, 'Near-rings with trivial multiplications', *Amer. Math. Monthly* 74 (1967), 1111–1112.
[8] B. H. Neumann, 'On the commutativity of addition', *J. London Math. Soc.* 15 (1940), 203–208.
[9] H. Wefelscheid, 'Vervollständigung topologischer Fastkörper', *Math. Z.* 99 (1967), 279–298.
[10] H. Zassenhaus, 'Über endliche Fastkörper', *Abh. Math. Sem. Univ. Hamburg* 11 (1935), 187–220.

Department of Mathematics, Texas A & M University
College Station, Texas 77843, United States of America