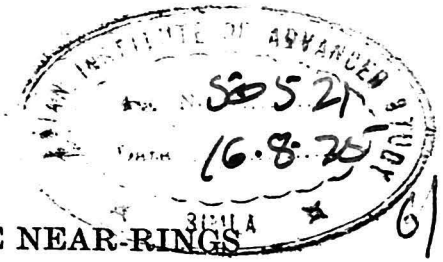
MATH. SCAND. 19 (1966), 146–160



THE NEAR-RINGS WITH IDENTITIES ON CERTAIN FINITE GROUPS

JAMES R. CLAY and JOSEPH J. MALONE, JR.

In the theory of near-rings the near-rings with identities occupy a role analogous to that in ring theory of rings with identities. Specifically, every near-ring may be embedded in a near-ring with identity. This result is given in [1]. (Although the proof given in [1] is erroneous, the result is valid.) This paper investigates near-rings with identities, demonstrating some implications of the existence of the identity element.

Throughout this paper the term "near-ring" shall mean "left-near-ring".

THEOREM 1. *Let $(G,+)$ be a cyclic group. If $(G,+,*)$ is a near-ring with identity, then $(G,+,*)$ is a commutative ring with identity.*

PROOF. Let the elements of G be given as equivalence classes of integers and let a be contained in a generator of $(G,+)$. Choose the notation so that $1'$ designates $(1\cdot a)'$ — the class containing a, $2'$ designates $(1\cdot a)'+(1\cdot a)'=(2\cdot a)'$, etc. Let e' be the identity of $(G,+,*)$ and let $1'*1'=c'$. Then

$$\begin{aligned} 1' = 1'*e &= 1'*(\overbrace{1'+\ldots+1'}^{e\text{ terms}}) \\ &= (1'*1')+\ldots+(1'*1') \\ &= e\cdot(1'*1') = e\cdot c' = (e\cdot c)' . \end{aligned}$$

If $G=I$, the integers, $a=\pm 1$ and, hence, $e=\pm 1$. If $G=I_n$, the integers modulo n, $e\cdot c\cdot a=1\cdot a \pmod n$ or $n \mid (e\cdot c-1)\cdot a$. Since a is contained in a generator of $(I_n,+)$, $(n,a)=1$ and $n \mid (e\cdot c-1)$. But this implies $(n,e)=1$. Thus the class containing e is a generator of $(I_n,+)$.

Whether $G=I$ or $G=I_n$, the class containing e is a generator of $(G,+)$ and, in the notation, the generator containing a may be replaced by the generator containing e so that $1'$ designates the class containing e, that is, $1'$ is the multiplicative identity. Then, for x', y' in G,

---

Received August 16, 1966.
The second author was supported in part by NASA Research Grant NGR 44-005-037.

$$\begin{aligned} x'*y' &= x'*(\overbrace{1'+\ldots+1'}^{y \text{ terms}}) \\ &= (x'*1')+\ldots+(x'*1') \\ &= y\cdot x' = (y\cdot x)' = (x\cdot y)' = x\cdot y' = y'*x' . \end{aligned}$$

Thus the near-ring multiplication is commutative and it follows that the right-distributive law holds. Therefore, $(G, +, *)$ is a commutative ring with identity.

COROLLARY. *Let $(G, +)$ be a cyclic group. There is, to an isomorphism, a unique near-ring (ring) with identity whose additive group is $(G, +)$.*

PROOF. Let $R_1=(G, +, *_1)$ and $R_2=(G, +, *_2)$ be near-rings whose identities contain, respectively, a and b. By the theorem, $(1\cdot a)'$ and $(1\cdot b)'$ generate, respectively, the additive groups of R_1 and R_2. Consider π: $R_1 \to R_2$ such that $(1\cdot a)'\pi=(1\cdot b)'$. Since π is known to be an isomorphism of $(G, +)$, it need only be shown that π preserves multiplication. For w', x' in R_1 the following equations establish this:

$$(w'*_1x')\pi = [(w\cdot a)'*_1(x\cdot a)']\pi = ((w\cdot x)\cdot a)'\pi = ((w\cdot x)\cdot b)' ,$$
$$w'\pi*_2x'\pi = (w\cdot a)'\pi*_2(x\cdot a)'\pi = (w\cdot b)'*_2(x\cdot b)' = ((w\cdot x)\cdot b)' .$$

THEOREM 2. *Let $(G, +)$ be a simple (non-trivial) group of finite order. If $(G, +, *)$ is a near-ring with identity, then $(G, +, *)$ is a field.*

PROOF: For an arbitrary near-ring $(G, +, *)$, the maximal sub-C-ring $(G_c, +, *)$ consists of all c in G such that $0*c=0$ and the maximal sub-Z-ring $(G_z, +, *)$ consists of all z in G such that $g*z=z$ for every g in G. In addition, G may be expressed bi-uniquely (see p. 27 of [1]) as a sum of these sub-near-rings. Note that $(G_c, +)$ is a normal subgroup of $(G, +)$ since

$$0*(g+c-g) = 0*g-0*g = 0 ,$$

g in G, c in G_c.

If, as in the statement of the theorem, $(G, +)$ is simple, the note above implies $G=G_c$ or $G=G_z$, i.e. G is a C-ring or G is a Z-ring. If $(G, +, *)$ has an identity e and is a Z-ring, then $z=z*e=e$, for every z in G. Thus, in this case, G contains only one element.

In any near-ring, for a fixed g in G, $(A_g, +)$ is a normal subgroup of $(G, +)$ if $A_g=\{a \mid a\in G, g*a=0\}$. If $(G, +)$ is simple and finite, each row of the multiplication table must contain all 0's or else only the 0 entry corresponding to the right-multiplication by 0. As a matter of fact, in the latter case each row — except for the 0 entry — is a permu-

tation of the non-zero entries since $g*a=g*b$ implies $g*(a-b)=0$ which, in turn, implies $a-b=0$.

If $(G,+)$ has prime order, $G=I_p$, Theorem 1 provides all that is needed except the multiplicative inverses. Since $(G,+,*)$ has an identity, there is a non-zero entry in each row (except the row corresponding to the left-multiplications by 0) and the last remark of the previous paragraph assures us that the identity occurs once, and only once, in each row of the multiplication table (except the row of left-multiplications by 0). So the needed multiplicative inverses exist and the theorem holds in this case.

If $(G,+)$ has composite order, then the result of [3] implies that $(G,+)$ has even composite order. Since the prime 2 divides the order of G, the Sylow theory assures us that G contains an element of order 2. If x is the element of order 2 and e is the identity, we see that e is also of order 2 since

$$0 = x+x = e*(x+x) = e*x+e*x = x*e+x*e = x*(e+e)\,.$$

Then, for g in G, $g\neq 0$,

$$g = e*g = -(e*(-g)) = -((-g)*e) = (-g)*(-e) = (-g)*e = -g\,.$$

Thus every non-zero element of G is of order 2 and $(G,+)$ must be commutative. The subgroup of $(G,+)$ generated by x is then a proper normal subgroup. This contradiction completes the proof of the theorem and yields the following

COROLLARY. *A simple group of composite order cannot be the additive group of a near-ring with identity.*

LEMMA. *Let $(G,+)$ be a finite group. If $*$ is a left distributive binary operation on $(G,+)$ there exists a function f: $G\to \mathrm{Hom}(G,G)$ such that $f(x)=f_x$ and $f_x(y)=x*y$ for each $y\in G$.*

This lemma is contained in theorem 1.1 of [2].

THEOREM 3. *Let $(G,+)$ be a finite group. Suppose $*$ is a left distributive binary operation defined on $(G,+)$. If $e\in G$ is an identity with respect to $*$, and if $x\in G$, then the order of x, $O(x)$, divides the order of e, $O(e)$.*

PROOF. For the identity e, $x=x*e=f_x(e)$ for each $x\in G$. Consequently $0=x*0=f_x(0)=f_x(O(e)\cdot e)=O(e)\cdot f_x(e)=O(e)\cdot x$. Hence $O(x)\mid O(e)$.

COROLLARY. *Let $(G,+)$ be a non-cyclic group whose order is a product of distinct primes. Then $(G,+)$ cannot be the additive group of a near-ring with identity.*

PROOF. Assume $(G, +, *)$ is a near-ring with an identity e. Since the order of G is a product of distinct primes $p_1, p_2, \ldots, p_n$ and since there are elements in G of order p_i for each i, $1 \leqq i \leqq n$, it follows that $p_1 p_2 \ldots p_n \mid O(e)$, and consequently $O(e) = p_1 p_2 \ldots p_n$. But $(G, +)$ is not cyclic.

LEMMA A. *Let x, y be integers $\geqq 2$. Then $xy \geqq x + y$.*

LEMMA B. *Let $s(n)$ denote the sum of the primes $\leqq n$, n an integer $\geqq 3$. Then $s(n) > n$.*

PROOF. Note that $s(3) = 5$, $s(4) = 5$, and $s(5) = 10$. We assume that $s(k) > k$ for $3 \leqq k < n$ and show that $s(n) > n$.

CASE I. Let n be even and $\geqq 6$. Then $3 \leqq \frac{1}{2}n < n$, where $\frac{1}{2}n$ is an integer. By Bertrand's postulate (Theorem 8.3 of [5]) there exists a prime p such that $\frac{1}{2}n < p \leqq n$. Hence,

$$s(n) \geqq p + s(\tfrac{1}{2}n) > \tfrac{1}{2}n + \tfrac{1}{2}n = n .$$

CASE II. Let n be odd and > 6. Then $n-1$ is even and $\geqq 6$. There exists a prime p such that $\frac{1}{2}(n-1) < p \leqq n-1$. Hence,

$$\begin{aligned} s(n) \geqq s(n-1) \geqq p + s\big(\tfrac{1}{2}(n-1)\big) &> p + \tfrac{1}{2}(n-1) \\ &\geqq 1 + \tfrac{1}{2}(n-1) + \tfrac{1}{2}(n-1) = n . \end{aligned}$$

THEOREM 4. *Let $(S_n, +)$ be the permutation group on n symbols. There exists no near-ring with identity whose additive group is $(S_n, +)$ $n \geqq 3$.*

PROOF. S_n has elements of order t for $1 \leqq t \leqq n$. By Theorem 3, if $(S_n, +)$ is the additive group of a near-ring with identity e, then $t \mid O(e)$, $1 \leqq t \leqq n$. Then $D(n) \mid O(e)$, where $D(n) = \operatorname{lcm}[2, 3, \ldots, n]$. Note that $D(n) = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, where the p_i are the primes $\leqq n$ and a_i is the maximum power of p_i such that $p_i^{a_i} \leqq n$.

Let $x \in S_n$ and write x as a product of disjoint cycles. The lengths of the cycles give a partition of n, say $n = r_1 + r_2 + \ldots + r_m$. By Theorem 5.1.2 of [4],

$$O(x) = \operatorname{lcm}[r_1, r_2, \ldots, r_m] .$$

We show that $O(x) < D(n)$. Consequently, there exists no $y \in S_n$ such that $D(n) \mid O(y)$. Hence the assumption that there is an identity will lead to a contradiction.

Let $N = \{P \mid P \text{ is a partition on } n\}$. If $P = \{r_1, r_2, \ldots, r_m\}$, let $\operatorname{lcm} P$ denote $\operatorname{lcm}[r_1, r_2, \ldots, r_m]$. If $L(n)$ is the maximum $\operatorname{lcm} P$ for $P \in N$, it is sufficient to show that $L(n) < D(n)$. For $r_i \in P$, let $p_1^{a_{1i}} p_2^{a_{2i}} \ldots p_k^{a_{ki}}$ be the prime factorization of r_i. Then

$$\text{lcm}\,[r_1, r_2, \ldots, r_m] = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$
$$b_j = \max\{a_{j1}, a_{j2}, \ldots, a_{jm}\}.$$

Thus $L(n) \leqq D(n)$.

Suppose there is an n such that $L(n) = D(n)$. Then there exists a partition of n, $P = \{r_1, r_2, \ldots, r_m\}$ such that $\text{lcm}\, P = D(n)$. Consider

$$\begin{aligned}
n &< p_1 + p_2 + \ldots + p_k && \text{(by Lemma B)} \\
&\leqq p_1^{a_1} + p_2^{a_2} + \ldots + p_k^{a_k} && \text{(since each } a_i \geqq 1) \\
&\leqq \textstyle\sum p_j^{a_{j1}} + \sum p_j^{a_{j2}} + \ldots + \sum p_j^{a_{jm}} && \text{(by the hypothesis. Only} \\
&\qquad \text{the terms for which } a_{ji} \neq 0 \text{ are included in the sum)} \\
&\leqq r_1 + r_2 + \ldots + r_m = n && \text{(by Lemma A)}.
\end{aligned}$$

Thus we have the contradiction $n < n$.

REFERENCES

1. G. Berman and R. J. Silverman, *Near-rings*, Amer. Math. Monthly 66 (1959), 23–34.
2. J. R. Clay, *Construction of all near-rings on a finite group*, to appear.
3. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 771–1029.
4. M. Hall, *The theory of groups*, Macmillan, New York, 1959.
5. I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, Wiley, New York, 1960.

UNIVERSITY OF ARIZONA
UNIVERSITY OF HOUSTON