MATH. SCAND. 23 (1968), 54–56

NEAR-RINGS WITH IDENTITY ON ALTERNATING GROUPS

JAMES R. CLAY and DONNA K. DOI

In [1] it was shown that the symmetric groups $(S_n, +)$ cannot be the additive group of a near-ring with identity if $n \geqq 3$. A natural question arises as to what happens in the corresponding alternating groups $(A_n, +)$. In this paper we shall see that similar results are obtained for the alternating group $(A_n, +)$ for $n \geqq 4$. Our main result is

THEOREM A. *For $n \geqq 4$, the alternating groups $(A_n, +)$ cannot be the additive group of a near-ring with identity.*

PROOF. The corollary to Theorem 2 of [1] shows that every simple group of composite order cannot be the additive group of a near-ring with identity. From Theorem 5.4.3 of [4] we know that each alternating group $(A_n, +)$ is simple for $n \geqq 5$. There remains to show the result holds for $n=4$ and does not hold for $n=3$.

If $n=3$, $(A_3, +)$ is cyclic and Theorem 1 of [1] shows that the near-rings with identities on cyclic groups are actually commutative rings with identity.

In A_4, the orders of the elements are 1, 2, and 3. But by Theorem 3 of [1], the order of each element must divide the order of the identity, so $(A_4, +)$ cannot be the additive group of a near-ring with identity.

REMARK. Theorem 2 of [1] and its corollary depends heavily upon 1) associativity of the multiplication of a near-ring, and 2) the fact that simple groups of composite order are of even order. The proof of this latter result, see [3], is based on advanced techniques. We shall now give a generalization of Theorem A based on elementary techniques. We will first need some results concerning the order of elements of A_n.

OBSERVATION. If $x \in S_n$ and the order of x is $O(x)=q_1^{\beta_1}q_2^{\beta_2}\ldots q_s^{\beta_s}$ where the q_i are distinct primes, then in the cycle decomposition of x, there are cycles of length $q_i^{\beta_i}$, $i=1,2,\ldots,s$. This follows directly from Theorems 5.1.1 and 5.1.2 in [4].

Received December 12, 1967.

We now introduce some notation to be used in the sequel. If G is a finite group, let

$$\Phi(G) = \text{l.c.m.}\{O(x) \mid x \in G\}.$$

(Here l.c.m. means least common multiple.) Let

$$\Psi(n) = \text{l.c.m.}\{k \mid 1 \leqq k \leqq n \text{ and } k \text{ is odd}\}.$$

In what follows, n will be an integer $\geqq 4$.

LEMMA 1. *If n or $n-1$ is not a power of 2, then*

$$\Phi(S_n) = \Phi(A_n) = \text{l.c.m.}\{1,2,3,\ldots,n\} = 2^{a_1}\Psi(n),$$

where $2^{a_1} \leqq n$ but $2^{a_1+1} > n$.

PROOF. It follows directly from Theorem 5.1.2 of [4] that

$$\Phi(S_n) = \text{l.c.m.}\{1,2,3,\ldots,n\} = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$$

where the p_i are the primes $\leqq n$ and a_i is the maximum power of p_i such that $p_i^{a_i} \leqq n$. We will assume that $2 = p_1 < p_2 < p_3 < \ldots < p_k$.

If $p_i \neq 2$, then the cycle $(1,2,\ldots,p_i^{a_i}) \in A_n$ and has order $p_i^{a_i}$. Therefore $p_i^{a_i} \mid \Phi(A_n)$. Since $2^{a_i} \leqq n-2$,

$$x = (1,2,3,\ldots,2^{a_i})(2^{a_i}+1, 2^{a_i}+2) \in A_n$$

and x has order 2^{a_i}. Hence $\Phi(S_n) = \Phi(A_n)$.

LEMMA 2. *In S_n, there are no elements of order $\Phi(S_n)$.*

PROOF. This follows from the proof of Theorem 4 in [1].

LEMMA 3. *If n or $n-1$ is a power of 2, say 2^α, then $\Phi(A_n) = 2^{\alpha-1}\Psi(n)$.*

PROOF. If $k \in \{1,2,\ldots,n\}$ is odd, then $(1,2,\ldots,k) \in A_n$ and has order k. Hence $\Psi(n) \mid \Phi(A_n)$. Similarly,

$$(1,2,\ldots,2^{\alpha-1})(2^{\alpha-1}+1, 2^{\alpha-1}+2) \in A_n$$

has order $2^{\alpha-1}$, so $2^{\alpha-1} \mid \Phi(A_n)$. If there is an $x \in A_n$ with order $O(x)$ such that $O(x) \nmid 2^{\alpha-1}\Psi(n)$, then by Lemma 1, the element x has a cycle of length 2^α. Hence $x = (x_1, x_2, \ldots, x_{2^\alpha})$, contrary to $x \in A_n$.

LEMMA 4. *If $x \in A_n$ and $2^\alpha \in \{n, n-1\}$, then $O(x) < 2^{\alpha-1}\Psi(n)$.*

PROOF. If there is an $x \in A_n$ such that $O(x) \geqq 2^{\alpha-1}\Psi(n)$, then in the cycle decomposition for x, there are cycles of length 2^α and p where p

is a prime and $2^{\alpha-1} < p \leqq n$. (There is such a prime p by Bertrand's postulate, Theorem 8.3 of [6].) Hence

$$n \geqq 2^{\alpha-1}+p > 2^{\alpha-1}+2^{\alpha-1} = 2^{\alpha},$$

a contradiction if $n=2^{\alpha}$. If $n-1=2^{\alpha}$, then x has a cycle decomposition $x=(x_1,\ldots,x_{2^\alpha})(y_1,\ldots,y_p)$ contrary to $x \in A_n$.

THEOREM B. *If $*$ is a left distributive binary operation with identity on an alternating group $(A_n, +)$, then $n \leqq 3$.*

PROOF. By Theorem 3 of [1], if an element e of a finite group $(G, +)$ is an identity with respect to a left distributive binary operation, then the order $O(e)$ of e is $\Phi(G)$. Then Lemmas 1 and 2 eliminate all $n>3$ where neither n nor $n-1$ are powers of 2, and Lemmas 3 and 4 eliminate all $n>3$ where either n or $n-1$ is a power of 2.

Theorem B generalizes Theorem A in that associativity of multiplication is not needed, whereas it is needed for the proof of the corollary to Theorem 2 in [1] and the proof of Theorem A depends upon this corollary

The infinite alternating group $A_\infty = \bigcup_{n=1}^{\infty} A_n$ is simple, and an element of A_∞ is of finite order. But since the orders of elements of A_∞ are not bounded above by some integer N, Theorem B, hence Theorem A extends to A_∞; that is, *there is no left distributive binary operation with identity definable on the infinite alternating group* $(A_\infty, +)$. The proof of this follows directly from the above remarks and Theorem 3 of [1] mentioned earlier in this paper. This argument also extends to the infinite symmetric group $S_\infty = \bigcup_{n=1}^{\infty} S_n$, hence extends Theorem 4 of [1]; that is, *there is no left distributive binary operation with identity definable on the infinite symmetric group* $(S_\infty, +)$.

REFERENCES

1. J. R. Clay and J. J. Malone, Jr., *The near-rings with identities on certain finite groups*, Math. Scand. 19 (1966), 146–150.
2. J. R. Clay and C. J. Maxon, *The near-rings with identities on generalized quaternion groups*. To be submitted.
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. C. J. Maxon, *On finite near-rings with identity*, Amer. Math. Monthly 74 (1967), 1228–1230.
6. I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, Wiley, New York, 1960.

UNIVERSITY OF ARIZONA, TUCSON, ARIZONA, U.S.A.