COMPOSITIO MATHEMATICA

CARLTON J. MAXSON

On well-ordered groups and near-rings

Compositio Mathematica, tome 22, nº 2 (1970), p. 241-244

<http://www.numdam.org/item?id=CM_1970__22_2_241_0>

COMPOSITIO MATHEMATICA, Vol. 22, Fasc. 2, 1970, pag. 241-244
Wolters-Noordhoff Publishing
Printed in the Netherlands

ON WELL-ORDERED GROUPS AND NEAR-RINGS

by

Carlton J. Maxson *

1. Introduction

The major result of this note is the following theorem

If $\langle G, \cdot \rangle$ is a group with a partition $G = P \cup P^{-1} \cup \{e\}$ such that P has property (W): every non-empty subset S (of P) contains an element l such that $Sl^{-1} \subseteq \{e\} \cup P$ then $\langle G, \cdot \rangle$ is cyclic. $(P^{-1} = \{x^{-1} | x \in P\})$.

The proof of this theorem is given in Section 2. We note that in the case of abelian groups the result is well-known (see [2], [6]).

As an immediate corollary we find that well-ordered groups (see Section 2) are abelian.

In Section 3 the above result is applied to near-rings and a new characterization of the integers is obtained. Recall that a unitary (right) near-ring $\langle N, +, \cdot \rangle$ is a set N with two binary operations $+$ and $\cdot$ such that

(i) $\langle N, + \rangle$ is a group with identity 0,
(ii) $\langle N, \cdot \rangle$ is a semigroup with unit 1 ($\neq 0$),
(iii) For all $x, y, z \in N$, $(x+y)z = xz+yz$.

In the final section new characterizations of finite prime fields are obtained. In particular a generalization of the theorem of [5] is given.

2. Main result

THEOREM 1. *If $\langle G, \cdot \rangle$ is a group with a partition $G = P \cup P^{-1} \cup \{e\}$ such that P has property (W): every non-empty subset S (of P) contains an element l such that $Sl^{-1} \subseteq \{e\} \cup P$ then $\langle G, \cdot \rangle$ is cyclic.*

PROOF. If $P = \emptyset$ the result is clear so we assume $P \neq \emptyset$. Then, by (W), there exists an $a \in P$ such that $Pa^{-1} \subseteq \{e\} \cup P$. Let $A = \{a^m | m \in Z\}$. If $A \neq G$ then $U = G - A \neq \emptyset$ and since $e = a^0 \in A$ there exists some $x \neq e$ in U. Hence $x^{-1} \in U$ for otherwise $x \in A$ since A is a group. Thus

* The author was supported in part by the research foundation of State University of New York.

$U \cap P \neq \emptyset$ and so by (W) there exists $b \in U \cap P$ such that $(U \cap P)b^{-1} \subseteq \{e\} \cup P$. Since $a \in A$, $a^{-1}b \neq e$. If $b^{-1}a \in P$ then $b^{-1}a = a$ or $b^{-1}aa^{-1} \in P$; that is, $b = e$ or $b^{-1} \in P$. But $b \in P$ so we must conclude that $a^{-1}b \in P$. Now if $a^{-1}b \in U$ then $a^{-1}b \in U \cap P$ which implies $a^{-1}b = b$ or $a^{-1}bb^{-1} \in P$. Since $a \in P$ we conclude that $a^{-1}b \notin U$. Thus $a^{-1}b \in A$, hence $b \in A$, contradicting $b \in U \cap P$. This shows that $U = \emptyset$.

We note that both the partition of the group and the property (W) are needed for the conclusion of the above theorem. For, if we take the non-cyclic group of real numbers $\langle R, + \rangle$ under the usual ordering (i.e., $P = \{x \in R | x > 0\}$ then $\langle R, + \rangle$ is a group with a partition $P \cup P^{-1} \cup \{e\}$ but (W) is not satisfied. On the other hand, if we again take the group $\langle R, + \rangle$ of real numbers under addition and take $P = R$ then clearly (W) is satisfied but $P \cap P^{-1} \neq \emptyset$.

A group $\langle G, \cdot \rangle$ is said to be *fully ordered* (see [1]) if there exists a non-empty subset P of G such that (i) P is closed under the group operation, (ii) $xPx^{-1} = P$, for all $x \in G$, and (iii) G is a group with a partition $G = P \cup \{e\} \cup P^{-1}$. (This set P is called the set of *positive elements of* G.) $\langle G, \cdot \rangle$ is said to be *well-ordered* if it is fully ordered and the set P of its positive elements satisfies property (W) of Theorem 1.

COROLLARY 1. *The only well-ordered group (up to isomorphism) is the additive group of integers with the usual ordering.*

PROOF. If $\langle G, \cdot \rangle$ is fully ordered then G is infinite [1] and so by Theorem 1, $\langle G, \cdot \rangle$ is an infinite cyclic group.

EXAMPLE ([2]). There are groups satisfying the hypotheses of Theorem 1 which are not fully ordered. In fact the cyclic groups $\langle Z_{2n+1}, + \rangle$, $n \in Z$, $n \geqq 1$ where $Z_{2n+1} = \{0, 1, 2, \cdots, 2n\}$ with $P = \{m | 1 \leqq m \leqq n\}$ provide examples.

3. Application

In [4] we found that every unitary near-ring with cyclic additive group is a commutative ring. This proof also established the well-known fact that there are only two distinct unitary rings with additive group isomorphic to the integers; i.e., the usual ring of integers $\langle Z, +, \cdot \rangle$ and the ring $\langle Z, +, \circ \rangle$ where $a \circ b = -(a \cdot b)$, $a, b \in Z$. Both of these rings are ordered rings and the map $\theta : x \to -x$ is an order isomorphism.

We now use Theorem 1 to give a new characterization of the integers.

THEOREM 2. *If $\langle N, +, * \rangle$ is a unitary near-ring such that $\langle N, + \rangle$ satisfies the hypotheses of Theorem* 1 *then $\langle N, +, * \rangle$ is a commutative ring. If N is infinite then $\langle N, +, * \rangle$ is order isomorphic to the ring of integers.*

PROOF. The first statement follows immediately from Theorem 1 and Proposition 1 of [4]. If N is infinite, $\langle N, +\rangle \cong \langle Z, +\rangle$ and so from the preceding remarks $\langle N, +, *\rangle$ is order isomorphic to $\langle Z, +, \cdot\rangle$.

The above theorem contains as a special case the last corollary of [2]. Moreover, the above result shows that in the usual characterization of the integers as a fully ordered ring in which the positive elements are well-ordered ([3], Theorem 5, p. 169) many of the axioms are redundant. In particular, only one distributive law is required, commutativity of addition is not needed and, relative to order, only the partition property and the well-ordering of the positive elements (W) are needed.

4. On finite prime fields

We recall that a *near-field* is a unitary near-ring in which every non-zero element has a multiplicative inverse.

THEOREM 3. *Let N be a set with cardinality $||N|| \geqq 3$. The following are equivalent*:

(a) $\langle N, +, \cdot\rangle$ *is a finite prime field.*

(b) $\langle N, +, \cdot\rangle$ *is a finite unitary near-ring such that* $\langle N, +\rangle$ *is a simple group.*

(c) $\langle N, +, \cdot\rangle$ *is a finite near-field such that* $\langle N, +\rangle$ *satisfies the hypotheses of Theorem* 1.

(d) $\langle N, +, \cdot\rangle$ *is a unitary near-ring such that* $\langle N, +\rangle$ *is a simple group satisfying the hypotheses of Theorem* 1.

PROOF. Clearly (a) $\Rightarrow$ (b) and in [5] we showed that (b) $\Rightarrow$ (a) under the additional assumption that $x \cdot 0 = 0$ for all $x \in N$. Let $S = \{x \in N | x \cdot 0 = 0\}$. S is a normal subgroup of $\langle N, +\rangle$ and since $1 \in S$ we have $S = N$. Hence (b) $\Rightarrow$ (a). If $\langle N, +, \cdot\rangle$ is a finite prime field then the examples following Corollary 1 show that $\langle N, +\rangle$ satisfies the hypotheses of Theorem 1. Thus (a) $\Rightarrow$ (c) and (a) $\Rightarrow$ (d). If we assume (c), then $\langle N, +\rangle$ is an elementary abelian p-group and cyclic from Theorem 1. Thus $\langle N, +\rangle$ is a simple group and (c) $\Rightarrow$ (d). The proof is completed by showing that (d) $\Rightarrow$ (b). But assuming (d), $\langle N, +\rangle$ is cyclic and consequently finite since $\langle N, +\rangle$ is simple.

BIBLIOGRAPHY

L., FUCHS
[1] Partially ordered Algebraic Systems, Addison-Wesley, Reading, Mass., 1963.
A. HANNA,
[2] On the ring of integers, Amer. Math. Monthly, 74 (1967), 1242–1243.

S. MACLANE AND G. BIRKHOFF
[3] Algebra, Macmillan, New York, 1967.

C. MAXSON
[4] On finite near-rings with identity, Amer. Math. Monthly, 74 (1967), 1228–1230.
[5] On a new characterization of finite prime fields, Can. Math. Bull., 11 (1968), 381–382.

S. WARNER
[6] Modern Algebra, Vol. 1, Prentice Hall, Englewood Cliffs, N. J., 1965.

(Oblatum 26-VI-69)

Department of Mathematics
Texas A & M University
College Station, Texas 77893