A NOTE ON FINITE ABELIAN GROUPS[1]

L. J. PAIGE

1. Introduction. R. H. Bruck[2] has pointed out that every finite group of odd order is isotopic to an idempotent quasigroup. It can be shown that a necessary and sufficient condition that a group G be isotopic to an idempotent quasigroup is that there exist one-to-one mappings θ and η of G upon G satisfying the relationship $\eta(x) = x \cdot \theta(x)$, for all x of G. The same condition is sufficient to prove the existence of a loop M whose automorphism group contains G as a subgroup. We shall not attempt to show either of these applications; but, since there may be others, the present paper is concerned with the existence of suitable θ and η for any finite abelian group G. For this we have a complete answer. Our methods are constructive, but (unfortunately from the standpoint of generalization) they make considerable use of the commutative law.

2. Notation. We shall consider a finite abelian group G of order $n = n(G)$.

The product of the n distinct elements of G will be designated by $p = p(G)$.

Let $x \rightarrow \theta(x)$ be any one-to-one mapping (*not* necessarily an automorphism) of G upon G. Consider the derived mapping $x \rightarrow \eta(x) = x\theta(x)$. The *order* of η, denoted by $O(\eta)$, is the number of distinct elements $\eta(x)$, for x in G.

It is our purpose to prove the following theorem:

THEOREM 1. *There exists a θ for which $O(\eta) = n(G)$ unless G possesses exactly one element of order 2. In the latter case there exists a θ for which $O(\eta) = n(G) - 1$.*

3. Evaluation of p.

LEMMA 1. *$p(G) = 1$ unless G possesses exactly one element of order 2. In the latter case, $p(G)$ is the unique element of order 2.*

PROOF. The set H consisting of the identity and all elements of G of order 2 is a uniquely defined subgroup of G. If $a \in G$ is of order

Presented to the Society, November 30, 1946; received by the editors October 17, 1946, and, in revised form, December 5, 1946.

[1] The author wishes to thank the referee for his suggestions which added considerably to the clarity of the paper.

[2] R. H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 19–52, especially pp. 35, 36.

greater than 2, $a \neq a^{-1}$; thus both a and a^{-1} appear in $p(G)$ and hence $p(G) = p(H)$.

If H has order 1, $p(H) = 1$. If H has order 2, elements 1, g, then $p(H) = 1 \cdot g = g$, and $p(H)$ is the unique element of H (and hence of G) of order 2.

Now suppose H has order greater than 2; so that H has order 2^k, $k > 1$. Then H has k generators $g_1, \cdots, g_k$ and every element of H has a unique representation in the form $g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k}$ where n_i is 0 or 1. Hence $p(H) = \prod (g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k})$, where the product is over the distinct ordered sets $(n_1, \cdots, n_k)$ with n_i taking the values 0 or 1. By symmetry $p(H) = (g_1 g_2 \cdots g_k)^m$ where $m = 2^{k-1}$ and since $k > 1$ we have $p(H) = 1$.

4. **A necessary condition.** It is easily shown that there are abelian groups for which a suitable θ does not exist.

LEMMA 2. *A necessary condition that $O(\eta) = n(G)$ is that $p(G) = 1$.*

COROLLARY. *If $p(G) \neq 1$, $O(\eta) < n(G)$ for all θ.*

PROOF. Suppose there exists a θ for which $O(\eta) = n(G)$. Then if we denote the elements of G by x_i $(i = 1, 2, \cdots, n)$,

$$\prod_{i=1}^{n} [x_i \theta(x_i)] = \prod_{i=1}^{n} \eta(x_i),$$

and since G is abelian, θ and η one-to-one mappings of G upon G, we have $p^2 = p$ or $p = 1$. The corollary should be obvious.

5. **The main theorem.** In order to avoid complexity, we prove the following lemma before proceeding with the proof of Theorem 1.

LEMMA 3. *If for θ, $O(\eta) \leqq n - 2$, where $n = n(G)$, there exists a θ' such that $O(\eta') > O(\eta)$.*

COROLLARY. *There exists a θ for which $O(\eta) = n(G) - 1$.*

PROOF. Let θ be a mapping for which $O(\eta) = r \leqq n - 2$. Denoting the elements of G by x_i $(i = 1, \cdots, n)$, let $\eta(x_i)$ $(i = 1, \cdots, r)$ be the r distinct elements of $\eta(x)$, for x in G. If there exist integers $h, k > r$ such that $x_h \theta(x_k) \neq \eta(x_i)$ $(i \leqq r)$, the problem is solved by setting $\theta'(x_h) = \theta(x_k)$, $\theta'(x_k) = \theta(x_h)$ and $\theta'(x) = \theta(x)$ for the remaining elements of G. Hence, assume that this is not the case. Since $\eta(x_{r+1}) = \eta(x_i)$ for some $i \leqq r$, there is no loss in generality in assuming that $\eta(x_{r+1}) = \eta(x_1)$. If $x_1 \theta(x_{r+2}) \neq \eta(x_i)$ $(i \leqq r)$, we can set $\theta'(x_1) = \theta(x_{r+2})$, $\theta'(x_{r+2}) = \theta(x_1)$ leaving $\theta'(x) = \theta(x)$ for the remaining elements of G

and thus construct a θ' with $O(\eta')>r$. But if $x_1\theta(x_{r+2})=\eta(x_i)$ for some $i\leqq r$, we note that $x_1\theta(x_{r+2})\neq\eta(x_1)$. Hence we may assume without loss of generality that $x_1\theta(x_{r+2})=\eta(x_2)$.

Now $x_2\theta(x_1)\neq\eta(x_1)$, $\eta(x_2)$. If $x_2\theta(x_1)\neq\eta(x_i)$ $(i\leqq r)$, we could change θ by setting $\theta'(x_1)=\theta(x_{r+2})$, $\theta'(x_2)=\theta(x_1)$, $\theta'(x_{r+2})=\theta(x_2)$ and thus construct θ' with $O(\eta')>r$. Otherwise we may assume without loss of generality that $x_2\theta(x_1)=\eta(x_3)$.

Continue in this manner and suppose we have reached the point where

$$(1)\qquad x_1\theta(x_{r+2}) = \eta(x_2), \qquad x_{i+1}\theta(x_i) = \eta(x_{i+2}) \qquad (i = 1, 2, \cdots, k).$$

From (1) we derive the equations

$$(2)\qquad \eta(x_1)\theta(x_{r+2}) = \eta(x_{i+1})\theta(x_i) \qquad (i = 1, 2, \cdots, k+1).$$

In fact $\eta(x_1)\theta(x_{r+2})=x_1\theta(x_1)\theta(x_{r+2})=x_1\theta(x_{r+2})\theta(x_1)=\eta(x_2)\theta(x_1)$; so assume $\eta(x_1)\theta(x_{r+2})=\eta(x_{j+1})\theta(x_j)$ for some j, with $1\leqq j\leqq k$. Then $\eta(x_{j+1})\theta(x_j)=x_{j+1}\theta(x_j)\theta(x_{j+1})=\eta(x_{j+2})\theta(x_{j+1})$; and the result follows by induction.

Now $x_{k+2}\theta(x_{k+1})\neq\eta(x_i)$ $(i\leqq k+2)$, for using (2) this would imply $\eta(x_i)\theta(x_{k+2}) = x_{k+2}\theta(x_{k+1})\theta(x_{k+2}) = \eta(x_{k+2})\theta(x_{k+1}) = \eta(x_i)\theta(x_{i-1})$, or $\theta(x_{k+2})=\theta(x_{i-1})$, which is impossible since $i\leqq k+2$. If $x_{k+2}\theta(x_{k+1})\neq\eta(x_i)$ $(i\leqq r)$, we could change θ by setting $\theta'(x_1)=\theta(x_{r+2})$, $\theta'(x_{i+1})=\theta(x_i)$ $(i=1, 2, \cdots, k+1)$, $\theta'(x_{r+2})=\theta(x_{k+2})$ and thus construct a θ' with $O(\eta')>r$. If $x_{k+2}\theta(x_{k+1})=\eta(x_i)$ for some $i\leqq r$ we may assume without loss of generality that $i=k+3$ and add to (1) the equation $x_{k+2}\theta(x_{k+1})=\eta(x_{k+3})$. However, since $O(\eta)$ is finite, we must reach a product $x_j\theta(x_{j-1})\neq\eta(x_i)$ $(i\leqq r)$. This completes the proof of Lemma 3. The corollary is obvious.

In order to prove Theorem 1 we may assume, by the corollary of Lemma 3, a θ for which $O(\eta)=n(G)-1$. Hence, let $\eta(x_i)$ $(i=1, \cdots, n-1)$ be the $n-1$ distinct elements of $\eta(x)$, for x in G; z the unique element of G not equal to some $\eta(x_i)$. Then since

$$\prod_{i=1}^{n-1} [x_i\theta(x_i)] = \prod_{i=1}^{n-1} \eta(x_i)$$

we have $px_n^{-1}p\theta(x_n)^{-1}=pz^{-1}$, where $p=p(G)$ as defined in §2. Thus $p^{-1}x_n\theta(x_n)=z$ or $p^{-1}\eta(x_n)=z$. Hence if $p(G)=1$, we see that $O(\eta)=n(G)$. But if $p(G)\neq 1$ we know by Lemma 2 that $O(\eta)<n(G)$ for all θ. This completes the proof.

Although there exist groups G for which a θ, such that $O(\eta)=n(G)$, is easily represented explicitly (for example, if G is of odd order let $\theta(x)=x$), the author found it necessary to use repeated applications of Lemma 3 to obtain suitable θ's for groups of the form $Z_1 \times Z_2 \times Z_3$ where Z_i are cyclic of order 2^{n_i}. However, it should be noted that if $G \cong G_1 \times G_2$, a one-to-one mapping θ of G upon G may be defined by

$$\theta[(x, y)] = [\theta_1(x), \theta_2(y)]$$

where θ_1 and θ_2 are one-to-one mappings of G_1 upon G_1 and G_2 upon G_2 respectively. Moreover θ satisfies the relationship $O(\eta) \geqq O(\eta_1) \cdot O(\eta_2)$. Thus if $O(\eta_1) = n(G_1)$, $O(\eta_2) = n(G_2)$ we would have $O(\eta) = n(G_1 \times G_2)$ and θ is represented explicitly in terms of θ_1 and θ_2.

UNIVERSITY OF WISCONSIN

ON RINGS WHOSE ASSOCIATED LIE RINGS ARE NILPOTENT

S. A. JENNINGS

1. **Introduction.** With any ring R we may associate a Lie ring $(R)_l$ by combining the elements of R under addition and commutation, where the commutator $x \circ y$ of two elements $x, y \in R$ is defined by

$$x \circ y = xy - yx.$$

We call $(R)_l$ the Lie ring associated with R, and denote it by $\mathfrak{R}$. The question of how far the properties of $\mathfrak{R}$ determine those of R is of considerable interest, and has been studied extensively for the case when R is an algebra, but little is known of the situation in general. In an earlier paper the author investigated the effect of the nilpotency of $\mathfrak{R}$ upon the structure of R if R contains a nilpotent ideal N such that R/N is commutative.[1] In the present note we prove that, for an arbitrary ring R, the nilpotency of $\mathfrak{R}$ implies that the commutators of R of the form $x \circ y$ generate a nil-ideal, while the commutators of R of the form $(x \circ y) \circ z$ generate a nilpotent ideal (cf. §3). If R is finitely generated, and $\mathfrak{R}$ is nilpotent then the ideal generated by the commutators $x \circ y$ is also nilpotent (cf. §4).

2. **A lemma on L-nilpotent rings.** We recall that the Lie ring $\mathfrak{R}$ is said to be nilpotent of class γ if we have

Received by the editors December 23, 1946.

[1] *Central chains of ideals in an associative ring*, Duke Math. J. vol. 9 (1942) pp. 341–355, Theorem 6.5.