On a construction of Hosszú.

By SHERMAN K. STEIN (Davis, California).

M. HOSSZÚ's method of constructing selfdistributive quasigroups from groups[1]) provides a meeting point for various investigations in groups and quasigroups. Relations between right distributive quasigroups, special automorphisms of groups, complete functions and characterizations of abelian groups, exhibited in part by his construction, will be discussed here.

In what follows, G will be a finite group, Q a finite quasigroup. An automorphism of G leaving only the unity, e, fixed will be called *special.* If $f: Q \to Q$ is onto Q and so is $g: Q \to Q$, defined by $g(x) = xf(x)$, then f is *complete.*

Theorem 1. *The following statements concerning $w: G \to G$ are equivalent:*

(a) *w is a special automorphism;*

(b) *the function $f: G \to G$, defined by $f(x) = w(x^{-1})$ is a complete antiautomorphism;*

(c) *the groupoid $R(\circ)$ defined by $x \circ y = w(x)\,w(y^{-1})y$ is a right distributive quasigroup, and $w(e) = e$.*

PROOF. We prove only that (c) implies (a).

(The equivalence of (a) and (b) is clear, and the implication, (a) implies (c), describes HOSSZÚ's construction). Since R is a quasigroup every element ot R is of the form $w(x)$ and also $w(y^{-1})y$.

Since R satisfies

$(a \circ c) \circ (b \circ c) = (a \circ b) \circ c$

G satisfies

$$w(w(a)w(c^{-1})c)w(c^{-1}(w(b))^{-1}(w(c^{-1}))^{-1})w(b)w(c^{-1})c = w(w(a)w(b^{-1})b)\,w(c^{-1})c.$$

Cancelling and setting $b = e$, we obtain

$$w(w(a)w(c^{-1})c)w(c^{-1}(w(c^{-1}))^{-1}) = w(w(a)) \tag{1}$$

[1]) See § 2 in [3] and Theorem 1 (c) of the present paper.

But for any $x, y \in G$ the simultaneuous equations

$$w(a)\, w(c^{-1})c = x$$
$$c^{-1}(w(c^{-1}))^{-1} = y$$

have unique solutions a, c. Equation (1) then implies that for all $x, y \in G$, $w(x)w(y) = w(xy)$. Thus w is an automorphism. Since every element of G has a unique representation in the form $w(y^{-1})y$, $e = w(y^{-1})y$ implies $y = e$; that is, $w(y) = y$ implies $y = e$, so w is special. Thus (c) implies (a).

It might be mentioned that S_4, for example, has no special automorphism (since every automorphism of S_4 is inner) but does have a complete function ([2], p. 544).

Since B. H. NEUMANN ([5]; p. 4) gives an example of a special automorphism of a finite non-abelian group, the Theorems 1 and 2 of HOSSZÚ [3] provide a negative answer to question 3 in [9] (p. 253) in the form of

Theorem 2. *There exists a Q which is right-but not left-distributive.*

From HOSSZÚ's construction and the fact that there are no right-distributive quasigroups of order $4k+2$ ([9]; p. 236) we deduce

Theorem 3. *A group of order $4k+2$ has no special automorphism.*[2])

BURNSIDE ([1]; pp. 90, 334) was the first to study special automorphisms, w. He proved, among other things, that if $w^2 = 1$ then $w(x) = x^{-1}$ and that G is therefore abelian. B. H. NEUMANN (in [5]) generalized this result to infinite groups:

A group in which every element has a unique square root and which possesses a special automorphism w with $w^2 = 1$ is abelian and $w(x) = x^{-1}$.

It is well known that a group is abelian if and only if the function $x \to x^{-1}$ is an endomorphism or the function $x \to x^2$ is an endomorphism. In this direction F. W. LEVI ([3]; p. 5) proved that the function $x \to x^3$ is an endomorphism of the group H if and only if for every pair of elements $a, b \in H$

$[[a, b], b] = [a, b]^3 = e$

Related to these results is:

Theorem 4. *If in a group H the function $x \to x^3$ is an automorphism then H is abelian.*[3])

[2]) This result is actually a special case of the following theorem proved by HALL and PAIGE ([2]; p. 548) in a study of orthogonal quasigroups: If G is a group of even order and its 2-sylow subgroups are cyclic then G has no complete function.

[3]) Compare to part 3 in the proposition of E. SHENKMAN and L. T. WADE [8]. Note that the map $x \to x^3$ is an automorphism of the group with two elements.

PROOF. For $x, y \in H, (xy)^3 = x^3y^3$. Cancellation yields $(yx)^2 = x^2y^2$. Replacing x by x^{-1} and y by y^{-1} be obtain $(xy)^{-2} = x^{-2}y^{-2}$. Thus the function $x \to x^{-2}$ is a homomorphism. Hence the function $x \to (x^{-2})^{-2} = x^4$ is also a homomorphism. Thus $x^4 y^4 = (xy)^4 = (xy)^3 xy = x^3 y^3 xy$. Cancellation implies $xy^3 = y^3x$ and that H is therefore abelian.

By a method employed in [6] (p. 2) one can establish

Theorem 5. *If w is a special automorphism of G and $w^n = 1, n \geqq 2$ then for all $x \in G, xw(x)w^2(x)..w^{n-1}(x) = e$.*[4])

The proof follows easily if x is written in the form $yw(y^{-1})$.

For $n = 2$ one obtains BURNSIDE's result.

DEFINITION. If w is an automorphism of period n of the group G such that w^i is special for $1 \leqq i \leqq n-1$, then w is called a *regular* automorphism.

Theorem 6. *If w is a regular automorphism of period n of the group G, then the n quasigroups $Q_i, 0 \leqq i \leqq n-1$, are mutually orthogonal* ([7] p. 245.), *where the law of composition of Q_i is defined by*

$$x \otimes_i y = w^i(x)\, w^i(y^{-1})\, y \qquad 1 \leqq i \leqq n-1$$
$$x \otimes_i y = xy^{-1} \qquad i = 0.$$

PROOF. To show that Q_i is orthogonal to Q_j, $1 \leqq i < j \leqq n-1$, it is sufficient to exhibit solutions to the simultaneous equations

$$w^i(x)\, w^i(y^{-1})\, y = a \tag{1}$$

$$w^j(x)\, w^j(y^{-1})\, y = \mathrm{b} \tag{2}$$

for any $a, b \in G$.

Let $j = i + k$. Then from (1) follows

$$w^j(x)\, w^j(y^{-1})\, w^k(y) = w^k(a). \tag{1'}$$

Equations (2) and (1′) yield

$$b^{-1} w^k(a) = y^{-1} w^k(y),$$

an equation having a unique solution for y. Then determine x from either (1) or (2).

To show Q_0 is orthogonal to $Q_i, 1 \leqq i \leqq n-1$, consider the simultaneous equations

$$xy^{-1} = a \tag{3}$$

$$w^i(x)\, w^i(y^{-1})\, y = b. \tag{4}$$

Clearly y then satisfies $w^i(a)y = b$; then either (3) or (4) determines x.

[4]) It is interesting to compare this theorem with the following, due to PAIGE [7]: A necessary condition that G possess a complete function is that there exist an ordering of the elements of G such that $g_1 g_2 \dots g_n = 1$ $(g_i \in G)$.

It is a long standing conjecture[5]) that if the integer m has the factorization into primes $m = \Pi p_j^{e_j}$, where the p_j are distinct primes and $e_j \geqq 1$, and if p^e is the smallest of the $p_j^{e_j}$, then there are at most $p^e - 1$ mutually orthogonal quasigroups of order m. In accord with this conjecture is.

Theorem 7. *If G is a group of order $n = \Pi p_i^{e_i}$, $e_i > 0$, the p_i are distinct primes, and $T: G \rightarrow G$ is a regular automorphism of period e then $e | p_i^{e_i} - 1$ for each i.*

Proof. If the theorem were established for e equal to a prime power then it would follow for arbitrary e. For if $e = \Pi q_j^{f_j}, f_j > 0$, the q_j's being distinct primes, then for each j let $U_j = T^{e/q_j^{f_j}}$. U_j is a regular automorphism of period $q_j^{f_j}$ so $q_j^{f_j} | p_i^{e_i} - 1$ for each j. Thus $e | p_i^{e_i} - 1$. So it is now assumed that $e = q_j^{f_j}$. Let there be s_i p_i-Sylow subgroups of G. Let S_i be this set with s_i elements. Then T induces a permutation $T_* : S_i \rightarrow S_i$. Since $(T_*)^e =$ identity, the number of elements of S_i in any orbit of T_* divides $e = q_j^{f_j}$.

If there is an orbit of T_* with only one element, say H, then $T(H) = H$, and $H - \{1\}$ is union of orbits of T. Thus it would follow that $e | p_i^{e_i} - 1$.

If each orbit of T_* has more than one element then q_j divides the cardinality of each such orbit. Thus $q_j | s_i$. But $s_i | n$; thus $q_j | n$. On the other hand $q_j | e$ and $e | n - 1$. Thus $q_j | n - 1$. Since $q_j > 1$ this is a contradiction.

Theorem 10 puts a severe restriction on the regular automorphisms that can operate on G. For example, if G is non abelian of odd order and gcd $\{p_i^{e_i} - 1\}_i = 2$ then G possesses no regular automorphisms.[6])

Bibliography.

[1] W. Burnside, Theory of groups of finite order, *Cambridge*, 1897.

[2] M. Hall—L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **5** (1955), 541—549.

[3] M. Hosszú, Nonsymmetric means, *Publ. Math. Debrecen* **6** (1959), 1—9.

[4] F. W. Levi, Notes on group theory I, II, *J. Indian Math. Soc.* (new series) **8** (1944), 1—9.

[5] B. H. Neumann, On the commutativity of addition, *J. London Math. Soc.* **15** (1940), 203—208.

[5]) E. T. Parker has recently shown that this conjecture is false for $n = 21$.

[6]) J. G. Thompson has announced that G must be nilpotent. In particular this would imply Theorem 7.

[6] B. H. Neumann, Groups with automorphism that leave only the neutral element fixed, *Arch. Math.* **7** (1956), 1–5.

[7] L. J. Paige, Complete mappings of finite groups, *Pacific J. Math.* **1** (1951), 111—116.

[8] E. Shenkman—L. T. Wade, The mapping which takes each element of a group onto its nth power, *Amer. Math. Monthly* **65** (1958), 33—34.

[9] S. K. Stein, On the foundations of quasigroups, *Trans. Amer. Math. Soc.* **85** (1957), 228—256.

(Recieved September 26, 1957.)