A NOTE ON HOMOMORPHIC MAPPINGS OF QUASIGROUPS INTO MULTIPLICATIVE SYSTEMS

GRACE E. BATES AND FRED KIOKEMEISTER

The study of normality theories for general quasigroups and loops became productive when that study was restricted to a study of homomorphisms of quasigroups on quasigroups.[1] The existence of a loop with homomorphic image which is not a quasigroup is then pertinent to this study. In this note we exhibit such a loop and show that certain properties of our example are necessary. In particular, if the homomorphic image of a quasigroup is a finite or an associative multiplicative system, this image is a quasigroup. A deeper statement is that of Theorem 4—finiteness of the kernel of a loop homomorphism into a multiplicative system is a sufficient condition for the image of this homomorphism to be a loop.

We make use of the following definitions: A *multiplicative system* M is a nonvacuous set of elements $a, b, c, \cdots$ such that to each ordered pair of elements a, b, there corresponds in M a uniquely defined element ab called the product. If the product is defined for a (possibly vacuous) subset of the set of ordered pairs, then M is called a *partial multiplicative system*. If M_1 and M_2 are partial multiplicative systems, M_1 is said to be *imbedded* in M_2 if $M_1 \subseteq M_2$ and products in M_2 coincide with those in M_1 whenever they are defined in M_1. A partial multiplicative system has an *identity element* e if the products ea and ae are defined for each element a and $ea = ae = a$. A mapping of a multiplicative system M on a multiplicative system $\overline{M}$ which preserves products is called a *homomorphism* of M. A multiplicative system G in which the equations $ax = b$ and $ya = b$ have unique solutions for each pair of elements a, b in G is called a *quasigroup*. A *loop* is a quasigroup with identity element.

THEOREM 1. *If J is a partial multiplicative system, then J can be imbedded in a multiplicative system M which has the additional properties:*

(1) *If a and b are elements of M, there is at least one x and at least one y in M such that $ax = b$ and $ya = b$.*

(2) *If $x \neq y$ but $ax = ay$ (or $xa = ya$) in M, then a, x, y, and $ax = ay$ (or $xa = ya$) are all in J.*

Presented to the Society, December 31, 1948; received by the editors January 26, 1948.

[1] Cf. [1, p. 513]; [2, p. 450]; [3, p. 769]; [4, Theorem 10A]; and [5]. (Numbers in brackets refer to the bibliography.)

(Note that (1) asserts that all equations are solvable in M, while (2) states that the solutions are unique except possibly for those equations possessing in J more than one solution. Hence, in particular, if J has both cancellation laws, M is a quasigroup.)

We define first an elementary extension K of a partial multiplicative system J as follows: Let K consist of all elements of J together with new elements z_{ab}, x_{ab}, y_{ab} defined in the following manner:

Each ordered pair of elements a, b in J for which ab is not in J gives rise to an element z_{ab} in K, the element z_{ab} being uniquely defined by the relation $z_{ab}=ab$ and the requirement that $z_{ab}=z_{cd}$ if and only if $a=c$ and $b=d$. Similarly, to each ordered pair of elements in J for which there is no x in J satisfying $xa=b$, there corresponds an element x_{ab} in K for which $(x_{ab})a=b$ is the defining relation, and to each ordered pair of elements a, b in J for which there is no y in J satisfying $ay=b$, there corresponds an element y_{ab} in K defined by the relation $a(y_{ab})=b$. Again, $x_{ab}=x_{cd}$ or $y_{ab}=y_{cd}$ if and only if $a=c$ and $b=d$.

The set K is a partial multiplicative system having the following properties:

(i) If a, b is an ordered pair of elements in J, ab is a uniquely defined element of K.

(ii) If a and b are elements of J, there is at least one x and at least one y in K such that $ax=b$ and $ya=b$.

(iii) If $x\neq y$, but $ax=ay$ (or $xa=ya$) in M, then a, x, y, and $ax=ay$ (or $xa=ya$) are all in J.

Consider the chain of partial multiplicative systems

$$J = J_0 \subseteq J_1 \subseteq J_2 \subseteq \cdots \subseteq J_i \subseteq J_{i+1} \subseteq \cdots$$

where J_{i+1} is an elementary extension of J_i for $i=1, 2, \cdots$. Let

$$M = \bigcup J_i$$

be the set-theoretic sum[2] of the J_i.

If a and b are elements of M, there exists an integer k such that a and b are elements of J_k, and therefore there exists a unique element ab in J_{k+1}. Thus to each ordered pair of elements a, b in M there corresponds a product ab in M. Furthermore, if a and b are in J_k, then J_{k+1} contains elements x and y such that $ax=b$ and $ya=b$.

If $x\neq y$, but $ax=ay$ in M, then a, x, y, and $ax=ay$ all lie in some J_k and $x\neq y$ in J_k. It follows that a, x, y, and $ax=ay$ are elements of J_i, $i=k-1, k-2, \cdots, 0$; that is, these elements lie in J. This proves the theorem.

[2] Clearly M is countable if J is countable.

COROLLARY 1. *If J is a partial multiplicative system with identity element e, then J may be imbedded in a multiplicative system M with identity e, having properties* (1) *and* (2) *of the theorem.*

For, in the construction of the elementary extension K of J, we require now only the additional condition imposed on the symbols z_{ab}, x_{ab}, and y_{ab} that they satisfy the relations $(z_{ab})e=e(z_{ab})=z_{ab}$, and so forth.

Suppose, now, that J is commutative (that is, ab is in J if and only if ba is in J, and $ab=ba$). Then if ab is undefined in J, ba is also undefined, and we may let $z_{ab}=ab=ba$ in K. Similarly, if there is in J no solution x of the equation $xa=b$, there is no solution of $ay=b$, and we may define $s_{ab}=x_{ab}=y_{ab}$ in K by the relations $(s_{ab})a=a(s_{ab})=b$. Hence we have the following corollary.

COROLLARY 2. *If J is a partial multiplicative system which is commutative, then J may be imbedded in a commutative multiplicative system M having properties* (1) *and* (2) *of the theorem.*

We shall employ Theorem 1 in constructing an example as follows:

Let J be the set consisting of the four elements β_1, β_2, β_3, β_4 with the following products defined:

$$\beta_1\beta_k = \beta_k\beta_1 = \beta_k, \qquad k = 1, 2, 3, 4,$$
$$\beta_2\beta_2 = \beta_2\beta_4 = \beta_4\beta_2 = \beta_4\beta_4 = \beta_3.$$

It is to be noted that J is a commutative partial multiplicative system with identity element β_1. The equation $\beta_2 x=\beta_3$ has two distinct solutions in J, and thus J cannot be imbedded in a quasigroup.

Let J be imbedded in a system M, as in Theorem 1, with elements β_k, $k=1, 2, 3, \cdots$. By Corollary 1, β_1 may be taken to be the identity element of M. Then M is a multiplicative system with the following properties:

(1) There exist positive integers h and k such that for each pair β_i and β_m, $\beta_i\beta_h=\beta_m$ and $\beta_k\beta_i=\beta_m$.

(2) If $\beta_i\beta_h=\beta_i\beta_k$, or if $\beta_h\beta_i=\beta_k\beta_i$, where $h<k$, then $h=2$, $k=4$, and $i=2$ or $i=4$.

Let A be a countably infinite loop[3] with elements α_1, α_2, α_3, $\cdots$ where α_1 is the identity of A. We construct a system G whose elements are the ordered pairs of elements (β_i, α_j), $i, j=1, 2, 3, \cdots$, with β_i in M and α_j in A.[4] The product of two elements in G is defined by:

[3] A may be a group.

[4] A similar construction has been employed by Bruck; see [4, p. 166].

(P) $$(\beta_i, \alpha_j)(\beta_h, \alpha_k) = (\beta_i\beta_h, \alpha_n)$$

where the subscript n of α_n is determined in the following way: Let α_q be the uniquely determined element $\alpha_j\alpha_k$ in A; then in (P)

(1) If $i=h=2$, or if $i=h=4$, let $n=2q-1$,

(2) If $i=2$, $h=4$, or if $i=4$, $h=2$, let $n=2q$,

(3) In all other cases, let $n=q$.

It is easily verified that G is a loop with identity (β_1, α_1). The set H of elements (β_1, α_i), $i=1, 2, 3, \cdots$, is a loop isomorphic with A under the correspondence

$$(\beta_1, \alpha_i) \leftrightarrow \alpha_i, \qquad i = 1, 2, 3, \cdots .$$

The definition of product in G implies that the correspondence

$$(\beta_i, \alpha_j) \to \beta_i, \qquad i, j = 1, 2, 3, \cdots ,$$

is a homomorphism of G on M. The kernel of this homomorphism is H.

By Corollary 2 of Theorem 1, M may be chosen to be commutative. If, furthermore, A is commutative, then G will have the same property. Commutativity, then, is not a sufficient condition that a quasigroup have only quasigroup images.

It is to be noted that in the example M is neither finite nor associative, and H is not finite. We shall show that these are necessary properties of the example.

In general, let the quasigroup G be homomorphic to the multiplicative system G'. If the elements of G are $a, b, c, \cdots$, let $a', b', c', \cdots$ be their corresponding images in G'. We have immediately the following lemmas:

LEMMA 1. *If a' and b' are any two elements of G', then x' and y' exist in G' such that $a'x'=b'$ and $y'a'=b'$.*

LEMMA 2. *The system G' is a quasigroup if and only if $a'b'=a'c'$ and $b'a'=c'a'$ each implies $b'=c'$.*

THEOREM 2. *If the homomorphic image G' of a quasigroup G is finite, then G' is a quasigroup.*[5]

Let $b_1', b_2', \cdots, b_n'$ be the elements of G', n a positive integer. Then by Lemma 1, for given i, $b_i'b_1', b_i'b_2', \cdots, b_i'b_n'$ are n distinct elements of G'. Right-hand cancellation is similarly established.

THEOREM 3. *If the homomorphic image G' of a quasigroup G is associative, then G' is a quasigroup.*

[5] Cf. [5, Theorem 4.13].

A multiplicative system which satisfies Lemma 1 and is associative is known to be a group (see [7, p. 19]).

If S is a subset of G, let $O[S]$ be the cardinal number of elements in S. Obviously

$$O[S] = O[aS] = O[Sa] \tag{A}$$

if a is any element of G.

We define $R(a)$ to be the set of elements g in G such that $g' = a'$ in G'. Then

$$\text{(B)} \qquad \begin{aligned} R(a)b &\subseteq R(ab), \quad \text{and} \\ aR(b) &\subseteq R(ab); \end{aligned}$$

for if $g = d_1 b$ where $d_1' = a'$, then $g' = d_1' b' = a'b' = (ab)'$, and g lies in $R(ab)$. The second statement follows in the same way.

Let a and b be any elements of G. There exists x in G such that $a = bx$. By (B), $R(b)x \subseteq R(bx) = R(a)$, and thus $O[R(b)x] \leqq O[R(a)]$. By (A), $O[R(b)] = O[R(b)x]$. It follows that $O[R(b)] \leqq O[R(a)]$. But a and b were any elements of G. We have proved the following lemma.

LEMMA 3. *If a and b are any elements of G, then $O[R(a)] = O[R(b)]$.*[6]

LEMMA 4. *If G' is the homomorphic image of the quasigroup G, then G' is a quasigroup if and only if $R(ab) = aR(b) = R(a)b$.*

Let $R(ab) = aR(b) = R(a)b$. If $a'b' = a'c'$, then ac is an element of $R(ab) = aR(b)$, and c lies in $R(b)$, that is, $c' = b'$. By Lemma 2, G' is a quasigroup.

Conversely, let G' be a quasigroup. Let $g = xb$ be an element of $R(ab)$. Then $g' = x'b' = a'b'$, and by Lemma 2, $x' = a'$. Thus x lies in $R(a)$, and g lies in $R(a)b$. It follows that $R(a)b \supseteq R(ab)$. By (B), however, $R(a)b \subseteq R(ab)$. Then $R(a)b = R(ab)$, and by a similar argument $aR(b) = R(ab)$.

LEMMA 5. *If $O[R(a)]$ is finite, G' is a quasigroup.*

By (B), $R(ab) \supseteq aR(b)$. By Lemma 3 and (A), $O[R(ab)] = O[R(b)] = O[aR(b)]$. Since this order is finite, $R(ab) = aR(b)$. Similarly, $R(ab) = R(a)b$, and by Lemma 4, G' is a quasigroup.

THEOREM 4. *If G is a loop homomorphic to the multiplicative system G', and if the kernel of the homomorphism is finite, then G' is a loop.*

If e is the identity of G, then $R(e)$ is the kernel of the homomorphism. The theorem follows by Lemma 5.

[6] Cf. [3, p. 770].

Bibliography

1. A. A. Albert, *Quasigroups*. I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–520.
2. R. Baer, *The homomorphism theorems for loops*, Amer. J. Math. vol. 67 (1945) pp. 450–460.
3. R. H. Bruck, *Simple quasigroups*, Bull. Amer. Math. Soc. vol. 50 (1944) pp. 769–781.
4. ———, *Some results in the theory of linear non-associative algebras*, Trans. Amer. Math. Soc. vol. 56 (1944) pp. 141–199.
5. G. H. Garrison, *Quasigroups*, Ann. of Math. vol. 41 (1940) pp. 474–487.
6. F. Kiokemeister, *A theory of normality for quasigroups*, Amer. J. Math. vol. 70 (1948) pp. 99–106.
7. B. L. van der Waerden, *Moderne Algebra*, Berlin, 1930, 1st ed.

Mt. Holyoke College

A CONJECTURE OF KRISHNASWAMI

D. H. LEHMER

Let $T(N)$ denote the number of right triangles whose perimeters do not exceed $2N$, and whose sides are relatively prime integers. A list of all such triangles whose perimeters do not exceed 10000 has been given by A. A. Krishnaswami.[1] On the basis of this table he conjectured that

$$T(N) \sim N/7. \tag{1}$$

The asymptotic formula

$$T(N) \sim \pi^{-2}N \log 4 \tag{2}$$

follows from the general theory of "totient points," as developed by D. N. Lehmer in 1900. A statement equivalent to (2) will be found in his paper[2] (p. 328).

The conjecture (1) is not far wrong since

$$\pi^2/\log 4 = 7.11941466.$$

Presented to the Society, April 17, 1948; received by the editors January 29, 1948.

[1] A. A. Krishnaswami, *On isoperimetrical Pythagorean triangles*, Tôhoku Math. J. vol. 27 (1926) pp. 332–348. Two omissions in Table I may be noted: For $s=3450$, $a=50$, $b=19$; for $s=3465$, $a=55$, $b=8$. This table is the basis for the one at the end of the present paper.

[2] D. N. Lehmer, *Asymptotic evaluation of certain totient sums*, Amer. J. Math. vol. 22 (1900) pp. 293–335.