In presenting the dissertation as a partial fulfillment of the requirements for an advanced degree from the Georgia Institute of Technology, I agree that the Library of the Institute shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to copy from, or to publish from, this dissertation may be granted by the professor under whose direction it was written, or, in his absence, by the Dean of the Graduate Division when such copying or publication is solely for scholarly purposes and does not involve potential financial gain. It is understood that any copying from, or publication of, this dissertation which involves potential financial gain will not be allowed without written permission.

_____

3/17/65
b

# GROUP-THEORETIC CONSTRUCTIONS OF SPECIAL QUASIGROUPS

A THESIS

Presented to the

Faculty of the Graduate Division

by

Evelyn Frances Veal

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Applied Mathematics

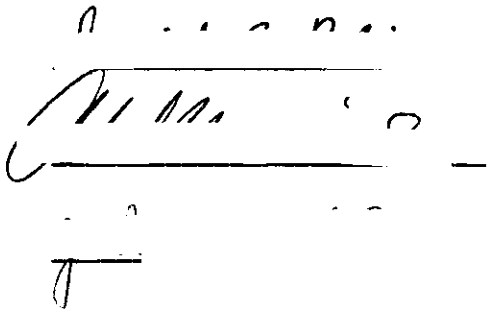
Georgia Institute of Technology

December, 1965

GROUP-THEORETIC CONSTRUCTIONS OF

SPECIAL QUASIGROUPS

Approved:



Date approved by Chairman: Dec. 17, 1965

# ACKNOWLEDGMENTS

I wish to express my sincere appreciation to Dr. D. A. Robinson, my thesis advisor, for his guidance and help in the preparation of this thesis. I also wish to thank Dr. John C. Currie and Dr. Andrew W. Marris for their reading of the thesis.

TABLE OF CONTENTS

# LIST OF TABLES

# CHAPTER I

## INTRODUCTION

The main purpose of this paper is to study group-theoretic constructions of special quasigroups. A quasigroup $(S,o)$ is considered to be constructed from a group $(T,\cdot)$ if $S \subseteq T$ and the operation $o$ can be defined in terms of the $\cdot$ operation.

In Chapter II some types of quasigroups are defined and examples of them given. These types are left-distributive, right-distributive, associative, commutative, and medial. Groups from which the examples could be constructed are not given. Some preliminary theorems on quasigroups are presented.

In Chapter III two theorems of S. K. Stein [5] are presented and illustrated. One of them is that for any left-distributive quasigroup $(S,o)$ there exists a group $(T,\cdot)$ such that $(S,o)$ can be constructed from $(T,\cdot)$ by conjugation. The other theorem is that, if $(T,\cdot)$ is a group and $S \subseteq T$ has certain properties, a left-distributive quasigroup $(S,o)$ can be constructed from $(T,\cdot)$ by conjugation.

In Chapter IV the concept of the core of a group is introduced. The core is a left-distributive closed binary system. Theorems which relate properties of the group to properties of its core are developed. These theorems permit a negative answer to the following two questions raised by S. K. Stein [6].

Question A. Is a left-distributive quasigroup right-distributive?

Question B. Does any combination of the hypotheses left-distributivity, right distributivity, and commutativity imply mediality?

# CHAPTER II

## TYPES OF QUASIGROUPS

Definition 2.1. A binary system is a non-empty set $Q$ and a function $f$ which assigns a value to each ordered pair of elements of $Q$.

If $Q$ and $f$ are a binary system and $x, y \in Q$, $f((x,y))$ is written $x \circ y$ and the binary system is written $(Q,\circ)$. Whenever a binary system $(Q,\circ)$ is under discussion in this paper and $x, y \in Q$; $xy$ will be written in place of $x \circ y$. If the operation is denoted by some other symbol, as in the binary systems $(Q,o)$ and $(Q,\otimes)$, no shorter method of writing $x\,o\,y$ and $x \otimes y$ will be employed.

Definition 2.2. A closed binary system $(Q,\circ)$ is a binary system such that if $x, y \in Q$ then $xy \in Q$.

Definition 2.3. A quasigroup is a closed binary system $(Q,\circ)$ such that for every $a, b \in Q$ there exists unique elements $x, y \in Q$ so that $ax = b = ya$.

An equivalent definition is that a quasigroup $(Q,\circ)$ is a binary system in which $xy = z$ has a unique solution in $Q$ for the third whenever two of $x,y,z$ are given elements of $Q$. Clearly if $Q$ is a finite set, $(Q,\circ)$ is a quasigroup if and only if each element of $Q$ appears exactly once in each row and each column of the table defining the operation.

Example 2.1. Let $Q = \{a,b,c\}$ and define $\circ$ and $o$ by Table 1. Then $(Q,\circ)$ and $(Q,o)$ are quasigroups.

Table 1. Example 2.1

| $\circ$ | a | b | c |
|---|---|---|---|
| a | a | c | b |
| b | c | b | a |
| c | b | a | c |

| o | a | b | c |
|---|---|---|---|
| a | a | b | c |
| b | b | c | a |
| c | c | a | b |

Definition 2.4. A binary system $(Q,\cdot)$ is left-cancellative if $x,y,z \in Q$ and $xy = xz$ imply that $y = z$. Similarly $(Q,\circ)$ is right-cancellative if $x,y,z \in Q$ and $xy = zy$ imply that $x = z$. The binary system $(Q,\circ)$ is said to be cancellative if it is both left and right cancellative.

Theorem 2.1. If $(Q,\cdot)$ is a quasigroup, $(Q,\circ)$ is cancellative.

Proof. If $x,y,z \in Q$ and $xy = xz$, let $w = xy$. Then $y$ and $z$ are solutions to $w = xa$ but the solution is unique. Thus $y = z$. The proof that $yx = zx$ implies $y = z$ is similar.

Definition 2.5. A closed binary system $(Q,\cdot)$ is associative if $(xy)z = x(yz)$ for every $x,y,z \in Q$.

Clearly every group is an associative quasigroup. In the next theorem it will be shown that the converse of this is also true.

Theorem 2.2. A closed binary system $(Q,\circ)$ is a group if and only if $(Q,\circ)$ is an associative quasigroup.

Proof. As stated above, one direction is clear. If $(Q,\cdot)$ is an associative quasigroup and $x \in Q$, there exists $e,f \in Q$ such that

$xe = x$ and $fx = x$. If $y \in Q$, $x(ey) = (xe)y = xy$ and $(yf)x = y(fx) = yx$. So, by Theorem 2.1, $ey = y = yf$ for every $y \in Q$. Thus, in particular, $ef = e = ee$. By Theorem 2.1, $f = e$. Hence, $e$ is an identity in $Q$. For $x \in Q$ there exists $y,z \in Q$ such that $xy = e = zx$. Since $x(zx) = xe = x = ex = (xy)x = x(yx)$, $zx = yx$ so $z = y$. Thus, for each $x \in Q$ there exists an element $y \in Q$ so that $xy = yx = e$. Therefore $(Q,\cdot)$ is a group.

Definition 2.6. If $(Q,\cdot)$ is a closed binary system and $a \in Q$, the left-translation $L_a$ is defined by $(x)L_a = ax$ and the right-translation $R_a$ is defined by $(x)R_a = xa$ for every $x \in Q$.

Theorem 2.3. A closed binary system $(Q,\cdot)$ is a quasigroup if and only if every left-translation and every right translation is a one-to-one function from $Q$ onto $Q$.

Proof. Let $(Q,\cdot)$ be a quasigroup. Then $L_a$ is a function from $Q$ into $Q$. If $a,x,y \in Q$ and $(x)L_a = (y)L_a$, then $ax = ay$ and, by Theorem 2.1, $x = y$. Thus each $L_a$ is one-to-one. For each $x \in Q$ there is an element $z \in Q$ such that $x = az = (z)L_a$. Hence, $L_a$ is a one-to-one function from $Q$ onto $Q$. Similarly $R_a$ is also a one-to-one function from $Q$ onto $Q$.

Conversely, assume that $L_a$ and $R_a$ are one-to-one functions from $Q$ onto $Q$ for every $a \in Q$. Then for $a,b \in Q$ there exists unique $x,y \in Q$ such that $ax = (x)L_a = b$ and $ya = (x)R_a = b$. Thus $(Q,\cdot)$ is a quasigroup.

Definition 2.7. A closed binary system $(Q,\cdot)$ is left-distributive if $x(yz) = (xy)(xz)$ for all $x,y,z \in Q$. It is right-distributive if $(xy)z = (xz)(yz)$ for all $x,y,z \in Q$.

Example 2.2. Let $P = \{(x,x^2): x \text{ is a real number}\}$. $P$ is a

parabola. Define $\circ$ by $(x,x^2) \circ (y,y^2) = (z,z^2)$ where $(z,z^2) \in P$ and the line from $(y,y^2)$ to $(z,z^2)$ is parallel to the tangent at $(x,x^2)$. Let $(x,x^2)(x,x^2) = (x,x^2)$. This common geometric definition of the operation is equivalent to $(x,x^2)(y,y^2) = (2x - y, (2x-y)^2)$. The quasigroup $(P,\circ)$ is both left-distributive and right-distributive.

Theorem 2.4. If $(Q,\circ)$ is a left-distributive or a right-distributive quasigroup and $x \in Q$, then $xx = x$.

Proof. If $(Q,\circ)$ is left-distributive, $x(xx) = (xx)(xx)$ which implies $x = xx$ by cancellation. If $(Q,\circ)$ is right-distributive, the proof is similar.

Example 2.3. The quasigroup $(Q,\circ)$ defined in Example 2.1 is a left-distributive and a right-distributive quasigroup. From the remark preceding Example 2.1 about a quasigroup in which the set is finite and Theorem 2.4, it is easily seen that the $(Q,\circ)$ of Example 2.1 is the only left-distributive and the only right-distributive quasigroup with three elements. It will be shown in Chapter IV that a quasigroup may be left-distributive and not right-distributive.

Theorem 2.5. If $(S,\otimes)$ is a left-distributive quasigroup, either $S$ is the group with one element or $S$ has no left identity.

Proof. Let $u$ be a left identity of $S$ and $x$ an element of $S$. By Theorem 2.4, $x \otimes x = x = u \otimes x$ so by cancellation $x = u$ for every $x \in S$.

Definition 2.8. A closed binary system $(Q,\circ)$ is medial if $(xy)(zw) = (xz)(yw)$ for all $x,y,z,w \in Q$.

Example 2.4. The quasigroup $(Q,\circ)$ defined in Example 2.1 is a

medial quasigroup. The quasigroup $(Q,o)$ defined in Example 2.1 is a medial quasigroup but it is neither left nor right distributive. Many averaging processes result in medial quasigroups. Let $A$ be the real numbers and $B$ be the positive real numbers. Define $\cdot$ by $a \cdot b = 1/2(a+b)$ for all $a,b \in A$. Define $o$ by $a \circ b = \sqrt{ab}$ for all $a,b \in B$ where $ab$ is the normal multiplication of $a$ and $b$. Define $\otimes$ by $a \otimes b = \frac{2}{1/a + 1/b}$ for all $a,b \in B$. Then $(A,\cdot)$ and $(B,o)$ are medial quasigroups. The binary system $(B,\otimes)$ is medial but is not a quasigroup. The quasigroup $(P,\cdot)$ in Example 2.2 is also medial. In Chapter IV an example of a quasigroup which is not medial will be given.

Definition 2.9. A closed binary system $(Q,\cdot)$ is commutative if $xy = yx$ for every $x, y \in Q$.

Example 2.5. $(Q,o)$ of Example 2.1 is a commutative quasigroup but it is shown in Example 2.3 that $(Q,o)$ is neither left nor right distributive.

# CHAPTER III

## CONJUGATION AND QUASIGROUPS

Let $(G,\cdot)$ be a group. If $x,y \in G$, $x^{-1}yx$ is called the conjugate of $y$ by $x$. A close relationship between group conjugation and left-distributive quasigroups will be shown in this chapter. Theorem 3.2 appears with the proof outlined in a paper by S. K. Stein [5]. A theorem similar to Theorem 3.1 appears in the same paper without proof. It seems that hypotheses not given by Mr. Stein are necessary for the proof. The hypothesis used here is sufficient but may be stronger than is necessary.

Definition 3.1. If $(T,\cdot)$ is a group and $a \in T$, the normalizer of $a$ is the set of all $x \in T$ such that $ax = xa$.

Definition 3.2. If $(T,\cdot)$ is a group, $S \subseteq T$, and $a \in T$, the set of all elements $ax$ with $x \in S$ is a left coset of $S$.

In the group $(T,\cdot)$ the normalizer of $a \in T$ is written $N_T(a)$. A left coset of the normalizer of $a$ would be written $bN_T(a)$.

From group theory it is known that if $a,b,c \in T$ either $bN_T(a) = cN_T(a)$ or $bN_T(a)$ and $cN_T(a)$ have no elements in common. Since the identity of $T$ is clearly in $N_T(a)$ for each $a \in T$, every element of $T$ is in one and only one distinct left coset of $N_T(a)$.

Theorem 3.1. Let $(T,\cdot)$ be a group and $S \subseteq T$ satisfy the following conditions for all $a,b,c \in S$ and $b \neq c$. (i) $b$ and $c$ are in distinct left cosets of the normalizer of $a$. (ii) $aba^{-1}, a^{-1}ba \in S$.

(iii) there exists $d \in S$ such that $d^{-1}ad = b$. Then $(S,\otimes)$ where $\otimes$ is defined by $a \otimes b = a^{-1}ba$ is a left-distributive quasigroup.

Proof. Let $a$ and $b$ be given elements of $S$. Since $T$ is a group $a \otimes b = a^{-1}ba$ is uniquely determined and by (ii) it is an element of $S$. By (ii) $aba^{-1} \in S$. Also $a \otimes (aba^{-1}) = a^{-1}(aba^{-1})a = b$. Thus, $aba^{-1}$ is a solution in $S$ to $a \otimes c = b$. If $c \in S$ is a solution to $a \otimes c = b$, $a^{-1}ca = b$ so $c = aba^{-1}$. Thus, the solution $c$ of $a \otimes c = b$ is uniquely determined in $S$. By (iii) there exists $d \in S$ such that $d \otimes a = d^{-1}ad = b$. If $e \in S$ and $e \otimes a = b$, $b = e^{-1}ae$ so $ebe^{-1} = a = dbd^{-1}$. Thus, $(d^{-1}e)b = b(d^{-1}e)$ and hence $d^{-1}e \in N_T(b)$. Let $1_T$ be the identity of $T$. Then $e \in dN_T(b)$ and $d = d1_T \in dN_T(b)$ which by (i) means that $e = d$. This shows that the solution $x$ of $x \otimes a = b$ is uniquely determined in $S$. Therefore, $(S, \otimes)$ is a quasigroup. Let $x,y$ and $z$ be elements of $S$. Then $x \otimes (y \otimes z) = x \otimes (y^{-1}zy) = x^{-1}(y^{-1}zy)x = x^{-1}y^{-1}x\,(x^{-1}zx)x^{-1}yx = (x^{-1}yx) \otimes (x^{-1}zx) = (x \otimes y)(x \otimes z)$. Therefore, $(S, \otimes)$ is a left-distributive quasigroup.

Example 3.1. Let $T = \{I,a,b,c,d,e\}$ and $S = \{a,b,e\}$. Define $\cdot$ by Table 2. Then $(T,\cdot)$ is a group isomorphic to the symmetric group of degree three, the left cosets of the normalizers of the elements of $S$ are the sets shown in Table 3, and the operation $\otimes$ defined in $S$ by $x \otimes y = x^{-1}yx$ is the operation shown in Table 4.

From Table 3 it is obvious that condition (i) of Theorem 3.1 holds. For $x \in S$, $x = x^{-1}$ so $xyx^{-1} = x^{-1}yx = x \otimes y$ so from Table 4 conditions (ii) and (iii) are clear. Hence, by Theorem 3.1 $(S, \otimes)$ is a left-distributive quasigroup. Clearly, $(S, \otimes)$ is isomorphic to the left-distributive quasigroup $(Q,\cdot)$ of Example 2.3.

Table 2. The Group $(T,\cdot)$

| o | I | a | b | c | d | e |
|---|---|---|---|---|---|---|
| I | I | a | b | c | d | e |
| a | a | I | d | e | b | c |
| b | b | c | I | a | e | d |
| c | c | b | e | d | I | a |
| d | d | e | a | I | c | b |
| e | e | d | c | b | a | I |

Table 3. Left Cosets of the Normalizers

| · | $N_T(a)$ | $N_T(b)$ | $N_T(e)$ |
|---|---|---|---|
| I | I,a | I,b | I,e |
| a | I,a | a,d | a,c |
| b | b,c | I,b | b,d |
| c | b,c | c,e | a,c |
| d | d,e | a,d | b,d |
| e | d,e | c,e | I,e |

Table 4. The Quasigroup $(S,\otimes)$

| $\otimes$ | a | b | e |
|---|---|---|---|
| a | a | e | b |
| b | e | b | a |
| e | b | a | e |

Theorem 3.2. If $(S,\otimes)$ is a left-distributive quasigroup, then there is a group $(T,\cdot)$ such that $S \subseteq T$ and for $a, b \in S$, $a \otimes b = a^{-1}ba$.

Proof. If $S$ has only one element, the theorem is obvious. If $S$ has more than one element, let $T'$ be the set of all one-to-one mappings from $S$ onto $S$. Define $o$ on $T'$ by $(x)F \,o\, G = [(x)F]G$ for all $F,G \in T'$. Then $(T',o)$ is a group. By Theorem 2.3 $L_a$ is a one-to-one function from $S$ onto $S$ for every $a \in S$ so $L_a \in T'$ for every $a \in S$. For $x \in S$, $(x)L_a \,o\, L_{a\otimes b} = (a \otimes x)L_{a\otimes b} = (a\otimes b)\otimes(a\otimes x) = a \otimes (b \otimes x) = (b\otimes x)L_a = (x)L_b \,o\, L_a$. Since any $x \in S$ can be written $(y)L_a^{-1}$ for some $y$ this is equivalent to $L_{a\otimes b} = L_a^{-1} \,o\, L_b \,o\, L_a$. Define $f$ on $S$ by $(a)f = L_a$. Define $T = (T'-[S]f) \cup S$. For $x \in T-S$, let $\bar{x} = x$ and for $x \in S$, let $\bar{x} = L_x$. Define $\circ$ on $T$ by $xy = \bar{x} \,o\, y$ if $\bar{x} \,o\, y \in [S]f$ and $xy = [\bar{x} \,o\, \bar{y}]f^{-1}$ if $\bar{x} \,o\, \bar{y} \in [S]f$. Routine calculations show that the identity of $T'$, which by Theorem 2.5 is not $L_a$ for any $a \in S$, is an identity of $T$ and that for $x \in T$ the inverse of $x$ in $(T,\circ)$ is either the inverse of $\bar{x}$ in $T'$ or $b$ if the inverse of $\bar{x}$ is $L_b$ for some $b \in S$. Let $x,y$, and $z$ be elements of $T$. If $\bar{x} \,o\, \bar{y} \,o\, \bar{z} \in [S]f$,

$$x(yz) = \begin{cases} x(\bar{y} \,o\, \bar{z}) & \text{if } \bar{y} \,o\, \bar{z} \notin [S]f \\ x(\bar{y} \,o\, \bar{z})f^{-1} & \text{if } \bar{y} \,o\, \bar{z} \in [S]f \end{cases} = \bar{x} \,o\, \bar{y} \,o\, \bar{z} =$$

$$\begin{cases} (\bar{x} \,o\, \bar{y})z & \text{if } \bar{x} \,o\, \bar{y} \notin [S]f \\ [(\bar{x} \,o\, \bar{y})f^{-1}]z & \text{if } \bar{x} \,o\, \bar{y} \in [S]f \end{cases} = (xy)z$$

If $\bar{x} \,o\, \bar{y} \,o\, \bar{z} \in [S]f$,

$$x(yz) = \left\{ \begin{array}{ll} x(\bar{y} \circ \bar{z}) & \text{if } \bar{y} \circ \bar{z} \notin [S]f \\ x[(\bar{y} \circ \bar{z})f^{-1}] & \text{if } \bar{y} \circ \bar{z} \in [S]f \end{array} \right\} = f^{-1}[\bar{x} \circ \bar{y} \circ \bar{z}] =$$

$$\left\{ \begin{array}{ll} (\bar{x} \circ \bar{y})z & \text{if } \bar{x} \circ \bar{y} \notin [S]f \\ [(\bar{x} \circ \bar{y})f^{-1}]z & \text{if } \bar{x} \circ \bar{y} \in [S]f \end{array} \right\} = (xy)z \ .$$

Hence $(T,\circ)$ is associative. Therefore $(T,\circ)$ is a group and $S \subseteq T$. If $u,v \in S$, then $\overline{\overline{u^{-1}}} = L_a^{-1}$ so $\overline{\overline{u^{-1}}} \circ \bar{v} \circ \bar{u} = L_u^{-1} \circ L_v \circ L_u = L_{u \otimes v}$. Thus $u^{-1}vu = [\overline{\overline{u^{-1}}} \circ \bar{v} \circ \bar{u}]f^{-1} = [L_{u \otimes v}]f^{-1} = u \otimes v$.

Theorem 3.3. If $(S, \otimes)$ is a left-distributive quasigroup then there is a group $(T,\circ)$ such that $S \subseteq T$, for $a,b \in S$ $a \otimes b = a^{-1}ba$, and conditions (ii) and (iii) of Theorem 3.1 hold.

Proof. By Theorem 3.2 there exists a group $(T,\circ)$ such that $S \subseteq T$ and, for $a,b \in S$, $a \otimes b = a^{-1}ba$. If $a,b \in S$, then $aba^{-1} = a \otimes b \in S$ and there exists $c \in S$ such that $a^{-1}ca = a \otimes c = b$ so $a^{-1}ba = c \in S$. Hence, condition (ii) is verified. There exists $d \in S$ such that $b = d \otimes a = d^{-1}ad$ so condition (iii) holds.

Theorem 3.3 is almost the converse of Theorem 3.1.

# CHAPTER IV

## THE CORE OF A GROUP AS A QUASIGROUP

In this chapter the concepts of core, Engel groups of type two, and nilpotent groups of class at most two will be introduced. The notion of core was first introduced by R. H. Bruck [2] in the study of Moufang loops. It was used by V.D. Belousov [1] D. A. Robinson [4] to obtain theorems which provide a negative answer to the following questions raised by S. K. Stein [6].

Question A. Is a left-distributive quasigroup right-distributive?

Question B. Does any combination of the hypotheses left-distributivity, right distributivity and commutativity imply mediality?

The theorems in this chapter are due to D. A. Robinson and show that the core of a group has certain properties if and only if the group has certain properties.

Definition 4.1. If $(G,\circ)$ is a group, the commutator, $[x,y]$, of $x, y \in G$ is $x^{-1}y^{-1}xy$.

Lemma 4.1. If $(G,\circ)$ is a group, then for all $x,y,z \in G$ the following hold:

$$xy = yx[x,y] \tag{1}$$

$$[x,y]^{-1} = [y,x] \tag{2}$$

$$y^{-1}xy = x[x,y] \tag{3}$$

$$y^{-1}[x,z]y = [y^{-1}xy, y^{-1}zy] \tag{4}$$

Proof. The proof follows directly from Definition 4.1.

Definition 4.2. Let $(G,\circ)$ be a group with the identity denoted by $e$. Then $(G,\circ)$ is an Engel group of type two if $[[x,y],x] = e$ for all $x,y \in G$. The group $(G,\circ)$ is a nilpotent group of class at most two if $[[x,y],z] = e$ for all $x,y,z \in G$.

Lemma 4.2. If $(G,\circ)$ is an Engel group of type two, then for all $x,y \in G$ the following hold.

$$[x,y]^{-1} = [x^{-1},y] \tag{5}$$

$$[x,y] = [x^{-1},y^{-1}] \tag{6}$$

$$[x,y^{-1}xy] = e \tag{7}$$

Proof. For all $x,y \in G$, $e = y^{-1}(xx^{-1}y) = (y^{-1}xy)(y^{-1}x^{-1}y) = x[x,y]x^{-1}[x^{-1},y] = [x,y][x^{-1},y]$ since $[x,y]x = x[x,y]$. Thus $[x,y]^{-1} = [x^{-1},y]$ and (5) is established. Replacing $y$ by $y^{-1}$ in (5), $[x^{-1},y^{-1}] = [x,y^{-1}]^{-1} = [y^{-1},x]$. By (5) $[y^{-1},x] = [y,x]^{-1}$. Thus $[x^{-1},y^{-1}] = [x,y]$ for all $x,y \in G$ and (6) is established. Finally, for all $x,y \in G$, $(y^{-1}xy)x = x[x,y]x = xx[x,y] = x(y^{-1}xy)$ and (7) holds.

Definition 4.3. If $(G,\circ)$ is a group, then the binary system $(G,o)$ with $o$ defined by $x\,o\,y = xy^{-1}x$ for all $x,y \in G$ is called the core of $(G,\circ)$.

Lemma 4.3. If $(G,\circ)$ is a group and $(G,o)$ is the core of $(G,\circ)$, then $(G,o)$ is left-distributive.

Proof. If $x,y,z \in G$, $(x \circ y) \circ (x \circ z) = (xy^{-1}x) \circ (xz^{-1}x) = xy^{-1}x(x^{-1}zx^{-1})\ xy^{-1}x = xy^{-1}zy^{-1}x = x \circ (yz^{-1}y) = x \circ (y \circ z)$.

Theorem 4.1. The core $(G,\circ)$ of a group $(G,\cdot)$ is a quasigroup if and only if the function $f$ defined by $(x)f = x \cdot x$ for all $x \in G$ is a one-to-one function from $G$ onto $G$.

Proof. If $(G,\circ)$ is a quasigroup and $y,z \in G$, there is a unique solution $x$ to $z = xy^{-1}x = x \circ y$. Let $y$ be the identity of $G$. Then $x \cdot x = z$ has a unique solution for every $z \in G$. Hence, $f$ is a one-to-one function from $G$ onto $G$.

If $f$ is one-to-one and onto $G$ and $y,\ z \in G$, there is a unique $w$ such that $ww = zy^{-1}$. Thus $(wy)y^{-1}(wy) = wwy = zy^{-1}y = z$. If $uy^{-1}u = z$, $(uy^{-1})(uy^{-1}) = zy^{-1}$ so $w = uy^{-1}$ and $u = wy$. Thus, $x = wy$ is the unique solution to $x \circ y = z$. If $y,z \in G$, $y \circ z = yz^{-1}y$ is uniquely determined and $x = yz^{-1}y$ is the unique solution to $y \circ x = z$. Hence $(G,\circ)$ is a quasigroup.

Theorem 4.2. The core $(G,\circ)$ of a group $(G,\cdot)$ is commutative if and only if $x^3 = e$ for all $x \in G$.

Proof. $xy^{-1}x = yx^{-1}y$ for all $x,y \in G$ if and only if $(y^{-1}x)^3 = e$ for all $x,y \in G$.

Theorem 4.3. A group $(G,\cdot)$ is an Engel group of type two if and only if its core $(G,\circ)$ is right-distributive.

Proof. The core $(G,\circ)$ is right-distributive if and only if the following is true for all $x,y,z \in G$.

$$y^{-1}xz^{-1}xy^{-1} = z^{-1}xy^{-1}zy^{-1}xz^{-1} \tag{8}$$

If $(G,\circ)$ is right distributive, set $z = e$ and replace $y$ by

$xy^{-1}$ in (8). Then $y(xyx^{-1}) = (xyx^{-1})y$. Replacing $x$ by $x^{-1}$ in this expression, gives $y(x^{-1}yx) = (x^{-1}yx)y$ for all $x,y \in G$. Then $yy[y,x] = y[y,x]y$ and $y[y,x] = [y,x]y$ for all $x,y \in G$. Thus $y[y,x][[y,x],y] = y[y,x][y,x]^{-1}y^{-1}[y,x]y = [y,x]y = y[y,x]$. Hence $[[y,x],y] = e$ for all $x,y \in G$ and $(G,\circ)$ is an Engel group of type two.

If $(G,\cdot)$ is an Engel group of type two, for all $x,y,z \in G$ $e = [xy^{-1},(zx^{-1})^{-1}(xy^{-1})(zx^{-1})]$ by (7). Then $e = x^{-1}[xy^{-1},(zx^{-1})^{-1}(xy^{-1})(zx^{-1})]x = [y^{-1}x, z^{-1}xy^{-1}z]$ for all $x,y,z \in G$. Hence $y^{-1}xz^{-1}xy^{-1}z = z^{-1}xy^{-1}zy^{-1}x$ for all $x,y,z \in G$ and multiplying both sides on the right by $z^{-1}$, gives (8). Thus $(G,o)$ is right-distributive.

Theorem 4.4. A group $(G,\circ)$ is nilpotent of class at most two if and only if its core $(G,o)$ is medial.

Proof. The core $(G,o)$ is medial if and only if for all $x,y,z,w \in G$ the following is true.

$$y^{-1}xz^{-1}wz^{-1}xy^{-1} = z^{-1}xy^{-1}wy^{-1}xz^{-1} \qquad (9)$$

If $(G,o)$ is medial, let $y = xz^{-1}$ in (9). Then $w(z^{-1}xzx^{-1}) = (z^{-1}xzx^{-1})w$ for all $x,z,w \in G$. That is, $[[z,x^{-1}],w] = e$ for all $x,z,w \in G$ and $(G,\circ)$ is nilpotent of class at most two.

If $(G,\circ)$ is nilpotent of class at most two, then $(G,\cdot)$ is also an Engel group of type two and Lemma 4.2 applies. Hence for all $x,y,z \in G$, $[xy^{-1},yz^{-1}] = [(xy^{-1})^{-1},(yz^{-1})^{-1}] = y^{-1}[yx^{-1},zy^{-1}]y = [x^{-1}y,y^{-1}z]$. But since $(G,\cdot)$ is nilpotent of class at most two, $[[xy^{-1},yz^{-1}],w] = e$ for all $x,y,z,w \in G$. Thus $[xy^{-1},yz^{-1}]w = w[xy^{-1},yz^{-1}] = w[x^{-1}y,y^{-1}z]$ for all $x,y,z,w \in G$ and (9) holds so $(G,o)$ is medial.

There exist groups $(G,\cdot)$ which are not Engel groups of type two

in which $x \to x \circ x$ is a one-to-one function from G onto G. One example of such a group appears as Part I in the Appendix. Therefore, by Lemma 4.3, Theorem 4.1, and Theorem 4.3 there exist quasigroups which are left-distributive but not right-distributive.

There also exist groups $(G,\circ)$ which are Engel groups of type two in which $x \to x \circ x$ is a one-to-one function from G onto G and $x^3 = e$ but which are not nilpotent of class at most two (see Appendix, Part II). Therefore, by Lemma 4.3 and Theorems 4.1, 4.2, 4.3, and 4.4 there exist quasigroups which are left-distributive, right-distributive, and commutative but not medial.

# APPENDIX

## PART I

Let $G$ be all ordered pairs with the first member 0, 1, or 2 and the second member 0, 1, 2, 3, 4, 5, or 6. Define $\circ$ by $(u,v)\circ(x,y) = (u+x, 2^x v + y)$ where for the first coordinate addition is modulo three and for the second coordinate addition is modulo seven $(u,v)\cdot(0,0) = (u+0, 2^0 v + 0) = (u,v)$ and $(0,0)\cdot(u,v) = (0+u, 2^u(0)+v) = (u,v)$ so $(0,0)$ is an identity for $(G,\cdot)$. Also $(u,v)\cdot(-u,-2^{-u}v) = (u+(-u), 2^{-u}v + (-2^{-u}v)) = (0,0)$ and $(-u,-2^{-u}v)\cdot(u,v) = (-u+u, 2^u(-2^{-u}v)+v) = (0,-v+v) = (0,0)$ so every element has an inverse. Since $[(u,v)\cdot(x,y)]\cdot(w,z) = (u+x, 2^x v + y)\cdot(w,z) = (u+x+w, 2^w(2^x v + y) + z) = (u+x+w, 2^{w+x}v + 2^w y + z) = (u,v)\cdot(x+w, 2^w y + z) = (u,v)\cdot[(x,y)\cdot(w,z)]$, $(G,\cdot)$ is associative. Therefore, $(G,\cdot)$ is a group.

If $(x,y)\cdot(x,y) = (u,v)\cdot(u,v)$, $(2x, 2^x y + y) = (2u, 2^u v + v)$. Since $2x = 2u$ modulo the prime three and $2^x y + y = 2^u v + v$ modulo the prime seven, $x = u$ and $y = v$. Hence $x \to xx$ is a one-to-one function from $G$ onto $G$.

Assume $[[(1,0),(0,1)],(1,0)] = (0,0)$. Then $(0,0) = [(2,0)(0,6)(1,0)(0,1)(1,0)] = [(0,6),(1,0)] = (0,1)(2,0)(0,6)(1,0)$ so $(1,5) = (1,0)(0,6) = (1,6)$. This is a contradiction so $[[(1,0)(0,1)],(1,0)] \neq (0,0)$ and $(G,\circ)$ is not an Engel group of type two.

Therefore, there exist groups $(G,\cdot)$ which are not Engel groups of type two in which $x \to x\cdot x$ is a one-to-one function from $G$ onto $G$.

PART II

Let $r$ be a positive integer larger than two. Let $G$ be all ordered $r + \frac{r!}{2(r-2)!} + \frac{r!}{6(r-3)!}$ tuples of 0, 1, and 2. If $a \in G$, the first $r$ members of $a$ will be denoted by $a_1, a_2, \cdots, a_r$; the next $\frac{r!}{2(r-2)!}$ by $a_{1,2}, a_{1,3}, \cdots, a_{r-1,r}$; and the last $\frac{r!}{6(r-3)!}$ by $a_{1,2,3}, a_{1,2,4}, \cdots, a_{r-2,r-1,r}$. The operation will be defined on $G$ by $(a \circ b)_i = a_i + b_i$, $(a \circ b)_{i,j} = a_{i,j} + b_{i,j} - [b_i \oplus a_j]$ and $(a \circ b)_{i,j,k} = a_{i,j,k} + b_{i,j,k} + (b_i \oplus a_{j,k}) - (b_i \oplus a_j \oplus a_k) - (b_j \oplus a_{i,k}) + (b_j \oplus b_i \oplus a_k) + (b_k \oplus a_{i,j}) - (b_k \oplus b_i \oplus a_j)$ where $+$, and hence $-$, is addition modulo 3 and $\oplus$ is defined by Table 5.

Table 5. The Operation $+$.

| $\oplus$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

By considering all cases it is seen that $a_i \oplus (a_j + a_k) = (a_i \oplus a_j) + (a_i \oplus a_k)$, $a_i \oplus (-a_j) = -(a_i \oplus a_j) = (-a_i) \oplus a_j$, and that $\oplus$ is associative. It is obvious from the table defining $\oplus$ that the operation is commutative. Using these facts about $\oplus$, it is easily verified that $\circ$ is associative, that the ordered tuple every element of which is 0 is an identity of $(G, \cdot)$, and that the inverse of $a \in G$ is $a \circ a$. Therefore

$(G,\cdot)$ is a group. The identity will be denoted by $I$ and the inverse of $a$ by $a^{-1}$.

It will now be shown that $(G,\cdot)$ is an Engel group of type two. If $x,y,z \in G$, $I = (xy)(xy)(xy)$ so $yxy = x^{-1}y^{-1}x^{-1}$. Applying this to $x^{-1}yxzx^{-1}$ gives $x^{-1}yxzx^{-1} = x^{-1}y(x^{-1}x^{-1})zx^{-1} = (y^{-1}xy^{-1})(z^{-1}xz^{-1}) = y^{-1}(zyx^{-1}zy)z^{-1}$, hence $x^{-1}yxzx^{-1} = y^{-1}zyx^{-1}zyz^{-1}$. In particular, letting $z = y$ gives $x^{-1}yxyx^{-1} = yx^{-1}y$. Thus $(x^{-1}yx)y = y(x^{-1}yx)$ so that $[y,x]y = (y^{-1}x^{-1}yx)y = y^{-1}y(x^{-1}yx) = y(y^{-1}x^{-1}yx) = y[y,x]$. Therefore, $[[y,x],y] = [y,x]^{-1}y^{-1}[y,x]y = I$.

For $i = 1,2,3$ let $x_i \in G$ have $(x_i)_i = 1$ and all other members of the tuple be 0. Then $([[x_1,x_2],x_3])_{1,2,3} = 1$ so $[[x_1,x_2],x_3] \neq I$. Hence $(G,\cdot)$ is not nilpotent of class at most two.

Therefore, there exist groups $(G,\cdot)$ which are Engel groups of type two in which $x \to x \cdot x$ is a one-to-one function from $G$ onto $G$ and $x^3$ is the identity but which are not nilpotent of class at most two.

## REFERENCES

1. V. D. Belousov, The Structure of Distributive Quasigroups (in Russian), Matematicheskie Sbornik, Vol. 92 (1960) pp. 267-298.

2. R. H. Bruck, A Survey of Binary Systems, Ergebnisse Series, Springer - Verlag, Berlin-Gottingen-Heideberg, 1958.

3. Marshall Hall, The Theory of Groups, MacMillan, New York, 1959.

4. D. A. Robinson, Concerning Two Questions of S. K. Stein, Notices of the American Mathematical Society, Vol. 9, No. 2 (1962) p. 149.

5. S. K. Stein, Left-Distributive Quasigroups, Proceedings of the American Mathematical Society, Vol. 10, No. 4 (1959) pp. 577-578.

6. _____, On the Foundations of Quasigroups, Transactions of the American Mathematical Society, Vol. 85 (1957) pp. 228-256.