International Journal of Algebra, Vol. 3, 2009, no. 4, 157 - 171

Groups that Distribute over Mathematical Structures

Arthur Holshouser

3600 Bullard St., Charlotte, NC, USA

H. Reiter

Department of Mathematics
University of North Carolina Charlotte
Charlotte, NC 28223, USA
hbreiter@email.uncc.edu

1 Abstract

Suppose $(S,*)$ is a mathematical structure on a set S. As examples, $(S,*)$ might be a topological space on S, a topological group on S, an n-ary relation on S, an n-ary operator on S or a Steiner triple system on S. A *similarity* mapping on $(S,*)$ is a permutation of S that preserves the structure of $(S,*)$.

Such mappings $f:(S,*)\to(S,*)$ are called by different names. As examples, f might be called a homeomorphism or an automorphism on $(S,*)$. Suppose $(S,\cdot)$ is a group on S. For each t in S, the left and right translations on S are permutations $L_t(x)=t\cdot x$ and $R_t(x)=x\cdot t$, respectively. They are called the left and right translation by t. See [1].

We say that the group $(S,\cdot)$ left-distributes or right-distributes over $(S,*)$ if respectively for all t in S, $L_t(x):(S,*)\to(S,*)$ or $R_t(x):(S,*)\to(S,*)$ is a similarity mapping on $(S,*)$.

For example, suppose $(S,\cdot,T)$ is a topological group. Then for all t in S, both $L_t(x):(S,T)\to(S,T)$ and $R_t(x):(S,T)\to(S,T)$ are homeomorphisms on the topological space (S,T). This means that the group $(S,\cdot)$ both left-distributes and right-distributes over the topological space (S,T). See [1]. Note that the left and right distribution of the multiplicative group $(\mathbf{R}\setminus\{0\},\cdot)$ over addition $(\mathbf{R},+)$ is a pseudoexample since $\mathbf{R}\setminus\{0\}\neq\mathbf{R}$.

In this paper, we start with a given mathematical structure $(S,*)$ on S. We then find without redundancy all groups $(S,\cdot)$ on S such that $(S,\cdot)$ left-distributes over $(S,*)$. Analogous results hold for right-distribution by just defining $(S,\odot)$ from $(S,\cdot)$ by $a\odot b=b\cdot a$.

At the end, we briefly illustrate our results to study a very special class of Steiner triples. In the appendix, we discuss the converse problem in which the group $(S,\cdot)$ is given and we wish to find the structure $(S.*)$ on S such that $(S,\cdot)$ left-distributes over $(S,*)$. Of course, this will give many examples.

Mathematics Subject Classification: 22F50

Keywords: group, Steiner triples, permutations

2 Basic Concepts

The concepts of a structure $(S,*)$ on a set S and a similarity mapping $f:(S,*)\rightarrow(S,*)$ on the structure $(S,*)$ can be precisely defined in axiomatic set theory. In set theory, all objects can be defined as sets and elements of sets, and in some treatments of axiomatic set theory only sets are used. See [2].

From this point of view, a structure on a set S is an ordered pair $(S,*)$, where $*$ is a set whose atoms are members of S.

For example, if $S=\{a,b,c\}$, then $(S,*)$ might be

$$(S,*)=(\{a,b,c\},\{\{a,b\},b,c,\{a,c\}\}).$$

That is, $S=\{a,b,c\},*=\{\{a,b\},b,c,\{a,c\}\}$. Note that the atoms of $*$ are a,b,c. A structure $(S_1,S_2,\cdots,S_k,*)$ on several sets $S_1,S_2,\cdots,S_k$ where $S_i\cap S_j=\phi$ when $i\neq j$ is a $k+1$-tuple $(S_1,S_2,\cdots,S_k,*)$, where $*$ is a set whose atoms are members of $S_1\cup S_2\cup\cdots\cup S_k$. Thus, if $S_1=\{a,b\},S_2=\{c,d\}$, then $(S_1,S_2,*)=(\{a,b\},\{c,d\},\{a,b,\{a,d\}\})$ is an example.

Suppose $(S,*)$ is a structure on S and $f:S\rightarrow S$ is a permutation on S. We say that f is a similarity mapping on $(S,*)$ if replacing each $x\in S$ that appears in $*$ by $f(x)$ in $*$, leaves $(S,*)$ unchanged. Thus, in the above example, $(S,*)=(\{a,b,c\},\{\{a,b\},b,c,\{a,c\}\})$, the permutation $f:S\rightarrow S$ defined by $f(a)=a,f(b)=c,f(c)=b$ is a similarity mapping on $(S,*)$.

Suppose $(S_1,S_2,\cdots S_k,*)$ is a structure on several sets where $S_i\cap S_j=\phi$ when $i\neq j$. Suppose $f:S_1\rightarrow S_1$ is a permutation on S_1. We say that f is a similarity mapping on $(S_1,S_2,\cdots S_k,*)$ with respect to S_1 if the following is true. If each $x\in S_1$ that appears in $*$ is replaced by $f(x)$ in $*$ and each $x\in S_2\cup S_3\cup\cdots\cup S_k$ that appears $*$ is left the same, then $(S_1,S_2,\cdots S_k,*)$ remains unchanged.

Concept 1. A mathematical structure $(S,*)$ on a set S will be an undefined concept. Intuitively, a mathematical structure $(S,*)$ on S will mean any object that we can define by using S and the axioms of set theory.

Concept 2. Suppose $(S,*)$ is a structure on S and $f:S\rightarrow S$ is a permutation on S. Intuitively, $f:(S,*)\rightarrow(S,*)$ is a similarity mapping on

$(S,*)$ if f preserves the structure of $(S,*)$. However, similarity mapping will be an undefined concept.

We refer the reader to a book on axiomatic set theory for both Concept 1 and Concept 2. See [2].

The following three axioms are sufficient for our purposes.

Axiom 1. Suppose $(S,*)$ is a structure on S. Then $i:(S,*)\to(S,*)$ is a similarity mapping on $(S,*)$ where $i:S\to S$ denotes the identity permutation on S.

Axiom 2. Suppose $(S,*)$ is a given structure on S. If $f:S\to S$ is any permutation on S, we assume that we can use the axiom of specification to specify whether $f:(S,*)\to(S,*)$ is or is not a similarity mapping on $(S,*)$.

Axiom 3. Suppose $(S,*)$ is a structure on S and $f:S\to S,\ g:S\to S$ are permutations on S. Then if $f:(S,*)\to(S,*)$ and $g:(S,*)\to(S,*)$ are similarity mappings on $(S,*)$, then the permutation $f\circ g^{-1}:S\to S$ is a similarity mapping on $(S,*)$, where $\circ$ denotes the composition of functions.

Examples:

1. Suppose $(S,*)=(S,T)$ where T is a topology on S. Then a permutation $f:S\to S$ is a similarity mapping on (S,T) if and only if $f:(S,T)\to(S,T)$ is a homeomorphism on (S,T). This means that $\forall A\subseteq S, A\in T$ if and only if $f(A)\in T$.

2. Suppose $(S,*)$ is an n-ary operator $*$ on S. Then a permutation $f:S\to S$ is a similarity mapping on $(S,*)$ if and only if $f:(S,*)\to(S,*)$ is an automorphism on $(S,*)$. This means that $\forall a_1,a_2,\cdots,a_n\in S, f(a_1*a_2*\cdots*a_n)=f(a_1)*f(a_2)*\cdots*f(a_n)$.

3. Suppose $(S,*)=(S,R)$ is a binary relation R on S. This means that $\forall a,b\in S$, either aRb or $a\not Rb$. Then a permutation $f:S\to S$ is a similarity mappings on (S,R) if and only if for all $a,b\in S,\ aRb\leftrightarrow f(a)Rf(b)$.

4. Suppose $(S,*)=(S,\mathbf{A})$ is a collection of Steiner triples $\mathbf{A}$ on S. This means that $\mathbf{A}$ is a family of tripleton subsets of S having the following property: if $\{a,b\}\subseteq S$ is any doubleton subset of S, then $\exists$ a unique $A\in\mathbf{A}$ such that $\{a,b\}\subseteq A$. A permutation $f:S\to S$ is a similarity mapping on $(S,\mathbf{A})$ if and only if for each tripleton subset $\{a,b,c\}$ of $S, \{a,b,c\}\in\mathbf{A}$ if and only if $f(\{a,b,c\})\in\mathbf{A}$.

5. Suppose $(S,*)=(S,\cdot,\circ)$ where $\cdot$ and $\circ$ are binary operators on S. Then a permutation $f:S\to S$ is a similarity mapping on $(S,\cdot,\circ)$ if and only if $\forall a,b\in S, f(a\cdot b)=f(a)\cdot f(b)$ and $f(a\circ b)=f(a)\circ f(b)$.

6. Suppose $(S,*)=(S,*,\mathbf{A})$ where $*$ is a binary operator on S and $\mathbf{A}$ is a family of subsets of S. Then a permutation $f:S\to S$ is a similarity

mapping on $(S, *, \mathbf{A})$ if and only if (1) and (2) are true. (1) $\forall a, b \in S, f(a * b) = f(a) * f(b)$. (2) $\forall A \subseteq S, A \in \mathbf{A}$ if and only if $f(A) \in \mathbf{A}$.

Definition 1 Suppose $(S, \cdot)$ is a group on S. Then $\forall t \in S$, the permutation on S $L_t(x) = t \cdot x, \forall x \in S$, is called the *left translation* by t. Also, the permutation on S $R_t(x) = x \cdot t, \forall x \in S$, is called the *right translation* by t.

Definition 2 Suppose $(S, \cdot)$ is a group on S and $(S, *)$ is a structure on S. We say that $(S, \cdot)$ *left-distributes* over $(S, *)$ if $\forall t \in S, L_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$. Also, $(S, \cdot)$ *right-distributes* over $(S, *)$ if $\forall t \in S, R_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$. Also, $(S, \cdot)$ *distributes* over $(S, *)$ if $(S, \cdot)$ both left-distributes and right-distributes over $(S, *)$.

Examples:

1. Suppose $(S, *)$ is a binary operator on S. Then $(S, \cdot)$ left-distributes over $(S, *)$ if $\forall t \in S, L_t : (S, *) \to (S, *)$ is an automorphism on $(S, *)$. This means, $\forall t \in S, \forall a, b \in S, L_t(a * b) = L_t(a) * L_t(b)$. This means, $\forall t, a, b \in S, t \cdot (a * b) = (t \cdot a) * (t \cdot b)$. Likewise, $(S, \cdot)$ right-distributes over $(S, *)$ if $\forall t, a, b \in S, (a * b) \cdot t = (a \cdot t) * (b \cdot t)$.

2. Suppose $(S, *) = (S, R)$ is a binary relation on S. Then $(S, \cdot)$ left-distributes over (S, R) if $\forall t \in S, L_t : (S, R) \to (S, R)$ is a similarity mapping on (S, R). This means, $\forall t \in S, \forall a, b \in S, aRb$ if and only if $L_t(a) R L_t(b)$. This means, $\forall t \in S, \forall a, b \in S, aRb$ if and only if $(t \cdot a) R (t \cdot b)$. Likewise, $(S, \cdot)$ right-distributes over (S, R) if and only if $\forall t \in S, \forall a, b \in S, aRb$ if and only if $(a \cdot t) R (b \cdot t)$.

Definition 3 Let $(F, \circ)$ be a group of permutations on a set S where $\circ$ denotes the composition of functions. We say that $(F, \circ)$ is *transitive* on S if $\forall a, b \in S, \exists f \in F$ such that $f(a) = b$. Also, $(F, \circ)$ is *uniquely transitive* on S if $\forall a \in S, \forall b \in S, \exists$ a unique $f \in F$ such that $f(a) = b$.

Of course, if S is finite, then $(F, \circ)$ is uniquely transitive on S if and only if $(F, \circ)$ is transitive on S and $|S| = |F|$.

Theorem 1 $(F, \circ)$ is a group of permutations on a set S. Then $(F, \circ)$ is transitive on S if and only if $\exists a \in S$ such that $\forall b \in S, \exists f \in F$ such that $f(a) = b$. Also, $(F, \circ)$ is uniquely transitive on S if and only if $\exists a \in S$ such that $\forall b \in S, \exists a$ unique $f \in F$ such that $f(a) = b$.

Proof. The easy proof is left to the reader. ■

Note 1. If $(F, \circ)$ is uniquely transitive on S, then $|F| = |S|$. It will be convenient to index F by S and write $(F, \circ) = (\{f_t : t \in S\}, \circ)$.

Notation 1. Suppose $f : S \to S$, $g : S \to S$ are functions on S. Then $fg : S \to S$ is the composition of functions defined by $\forall x \in S, (fg)(x) = f(g(x))$. We also denote $fg : S \to S$ by $f \circ g : S \to S$.

3 Formally stating the problem

Main Problem. Suppose $(S, *)$ is a given structure on a set S. We wish to find without redundancy all groups $(S, \cdot)$ on S such that $(S, \cdot)$ left-distributes over $(S, *)$. This means we wish to find all groups $(S, \cdot)$ on S such that $\forall t \in S$, the left-translation by t, $L_t(x) = t \cdot x$, is a similarity mapping on $(S, *)$. The solution for right-distribution is analogous.

Note 2. Suppose $(S, *)$ is a given structure on S. From Axioms 1, 2, 3, we can define $(F, \circ)$ to be the group of all similarity mappings on $(S, *)$.

4 Basic Plan

Plan. In Section 4 we plan to proceed as follows. We are given a structure $(S, *)$ on S. We will arbitrarily choose and then fix an element $1 \in S$. We then find without redundancy all of the groups $(S, \cdot, 1)$ with identity 1 that left-distribute over $(S, *)$. If we then vary the $1 \in S$ that we choose, we will have completely solved the problem of finding without redundancy all of the groups $(S, \cdot)$ on S such that $(S, \cdot)$ left-distributes over $(S, *)$.

Suppose $1 = C_1 \in S$ is fixed and $C_2 \in S$ is arbitrary. In Section 5, we show how the collection of all groups $(S, \cdot, C_2)$ with identity C_2 that left-distribute over $(S, *)$ can be obtained without redundancy directly from the collection of all groups $(S, \cdot, 1)$ with identity $1 = C_1$ that left-distribute over $(S, *)$. We also find the corresponding equivalence relation on the collection of all groups $(S, \cdot)$ on S that left-distribute over $(S, *)$.

In Section 6 we give some concluding remarks on the main problem. As always, all of this work has an analogy for right-distribution by defining $(S, \odot)$ from $(S, \cdot)$ by $a \odot b = b \cdot a$.

In Section 7 we apply this work to briefly study a special class of Steiner triples, and in the appendix, we mention the converse problem.

5 Carrying out the Plan for the Main Problem

The following Theorems 2, 3, Lemmas 1, 2, Convention 1 and Observation 1 will solve the main problem.

In Theorem 2 and throughout the rest of the paper, it will be less confusing if we denote the left-translation by t to be $\forall t \in S, L_t(x) = f_t(x) = t \cdot x$.

Theorem 2 $(S, *)$ is a structure on S and $1 \in S$ is arbitrary but fixed. Suppose $(S, \cdot, 1)$ is a group with identity 1 that left-distributes over $(S, *)$.

For each $t \in S$, define the function (the left translation by t) $f_t : S \to S$ by $\forall x \in S, f_t(x) = L_t(x) = t \cdot x$. Then the following 8 statements are true.

1. (a) $\forall t \in S, f_t : S \to S$ is a permutation on S.

(b) $\forall t, \overline{t} \in S$, if $t \neq \overline{t}$ then $f_t \neq f_{\overline{t}}$.

2. $\forall t \in S, f_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$.

3. $\forall t \in S, f_t(1) = t$.

4. $\forall t, \overline{t} \in S, f_t \circ f_{\overline{t}} : (S, *) \to (S, *)$ is similarity mapping on $(S, *)$.

5. $\forall t, \overline{t} \in S, f_t \circ f_{\overline{t}} = f_{t \cdot \overline{t}}$.

6. $\forall t, \overline{t} \in S, (f_t \circ f_{\overline{t}})(1) = (f_t f_{\overline{t}})(1) = f_t(f_{\overline{t}}(1)) = f_t\left(\overline{t}\right) = t \cdot \overline{t} = f_{t \cdot \overline{t}}(1)$.

7. $(\{f_t : t \in S\}, \circ, f_1)$ is a group with identity $f_1 : S \to S$ that is isomorphic to the group $(S, \cdot, 1)$ through the 1-1 onto matching $f_t \leftrightarrow t, \forall t \in S$.

8. The group $(\{f_t : t \in S\}, \circ, f_1)$ is uniquely transitive on S.

Note 3. Theorem 2 is the key for solving the main problem.
Proof.
We prove statements 1, 2, 3, $\cdots$, 8 in order.

1. $\forall t \in S, f_t : S \to S$ is defined by $\forall x \in S, f_t(x) = L_t(x) = t \cdot x$, and it is a permutation on S since $(S, \cdot, 1)$ is a group. Also, if $t \neq \overline{t}$ then $f_t \neq f_{\overline{t}}$.

2. By Definition 2, the group $(S, \cdot)$ left-distributes over $(S, *)$ if and only if $\forall t \in S, L_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$. Since we are using the notation $L_t = f_t$, this means that $\forall t \in S, f_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$.

3. $\forall t \in S, f_t(1) = t \cdot 1 = t$ since 1 is the identity of $(S, \cdot, 1)$.

4. Now f_t and $f_{\overline{t}}$ are both similarity mappings on $(S, *)$. By Axiom 1, $i : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$. By Axiom 3, $i \circ f_{\overline{t}}^{-1} : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$. Now, $i \circ f_{\overline{t}}^{-1} = f_{\overline{t}}^{-1}$ and by Axiom 3, $f_t \circ \left(f_{\overline{t}}^{-1}\right)^{-1} = f_t \circ f_{\overline{t}}$ is a similarity mapping on $(S, *)$.

5. We show that $\forall x \in S, (f_t \circ f_{\overline{t}})(x) = f_{t \cdot \overline{t}}(x)$ which implies that $f_t \circ f_{\overline{t}} = f_{t \cdot \overline{t}}$. Now $(f_t \circ f_{\overline{t}})(x) = (f_t f_{\overline{t}})(x) = f_t(f_{\overline{t}}(x)) = f_t\left(\overline{t} \cdot x\right) = t \cdot \left(\overline{t} \cdot x\right) = \left(t \cdot \overline{t}\right) \cdot x = f_{t \cdot \overline{t}}(x)$.

6. This follows easily.

7. We know that $f_t \leftrightarrow t$, $\forall t \in S$, is a 1-1 onto matching of $\{f_t : t \in S\}$ and S since $f_t \neq f_{\overline{t}}$ if $t \neq \overline{t}$. Since $\forall t, \overline{t} \in S, f_t \circ f_{\overline{t}} = f_{t \cdot \overline{t}}$ and $t \cdot \overline{t} \in S$, we know that $(\{f_t : t \in S\}, \circ, f_1)$ is a binary operator. Also, since $\forall t, \overline{t} \in S, f_t \circ f_{\overline{t}} = f_{t \cdot \overline{t}}$ we know that $(\{f_t : t \in S\}, \circ, f_1)$ is isomorphic to the

group $(S,\cdot,1)$ through the 1-1 onto matching $f_t \leftrightarrow t, \forall t \in S$. Therefore, $(\{f_t : t \in S\}, \circ, f_1)$ is a group. Also, $\forall t \in S, f_t \circ f_1 = f_1 \circ f_t = f_{1\cdot t} = f_{t\cdot 1} = f_t$. Therefore, f_1 is the identity of the group $(\{f_t : t \in S\}, \circ, f_1)$.

8. Since $\forall t \in S, f_t(1) = t$, we know from Theorem 1 that the group $(\{f_t : t \in S\}, \circ, f_1)$ is uniquely transitive on S.

   As another proof, since $(S,\cdot,1)$ is a group, we can see directly that $\forall a \in S, \forall b \in S, \exists$ a unique f_t such that $f_t(a) = t \cdot a = b$. ■

Lemma 1. *Suppose $(S,\cdot,1)$ and $(S,\odot,1)$ are two unequal groups on S with the same identity 1. Unequal means $\exists a, b \in S$ such that $a \cdot b \neq a \odot b$. Then the two sets $\{f_t : t \in S\}$ and $\{f'_t : t \in S\}$ of permutations on S are different, where for each $t \in S$, f_t is defined by $\forall x \in S, f_t(x) = L_t(x) = t \cdot x$ and f'_t is defined by $\forall x \in S, f'_t(x) = L'_t(x) = t \odot x$. Of course, f_t, f'_t are the left translations by t.*

Proof. First, suppose $f_t = f'_{\overline{t}}$. Then $\forall x \in S, f_t(x) = t \cdot x = f'_{\overline{t}}(x) = \overline{t} \odot x$. Therefore, $t \cdot 1 = \overline{t} \odot 1$ which implies $t = \overline{t}$. This means that $f_t = f'_{\overline{t}}$ only if $t = \overline{t}$. Since $(S,\cdot) \neq (S,\odot)$, we easily show that for some $t \in S, f_t \neq f'_t$. Now $(S,\cdot) \neq (S,\odot)$ implies $\exists t, x \in S$, such that $f_t(x) = t \cdot x \neq t \odot x = f'_t(x)$ which implies that $f_t \neq f'_t$. ■

Using Theorem 2 as a guide, we will now reverse ourselves and start with a group of similarity mappings on the structure $(S,*)$.

Convention 1. $(S,*)$ is a structure on S with $1 \in S$ arbitrary but fixed.

Suppose $(\{f_t : t \in S\}, \circ)$ is a group of similarity mappings on $(S,*)$. Also, suppose $(\{f_t : t \in S\}, \circ)$ is uniquely transitive on S. Using Definition 3, this implies that the function $\{(x, f_x(1)) : x \in S\}$ is a permutation on S, and it also implies that $f_t \neq f_{\overline{t}}$ if $t \neq \overline{t}$. Using Theorem 2 as a guide, we agree to relabel (or reindex) the permutations $\{f_t : t \in S\}$ in such a way that $\forall i \in S, f_i(1) = i$. It is very important to point out that this relabeling is unique once we fix $1 \in S$.

Of course, this relabeling of the elements of the group $(\{f_t : t \in S\}, \circ)$ does not change the group itself since it just calls the elements of the group by different names and the permutations themselves are unchanged. Since $f_1(1) = 1$ we note that f_1 must now be the identity element of this group $(\{f_t : t \in S\}, \circ)$. Of course, for each different $1 \in S$ that we choose, the group $(\{f_t : t \in S\}, \circ)$ will be relabeled in a different way. Using Convention 1 and Note 2, we now state Theorem 3 which is the converse of Theorem 2.

Theorem 3 $(S,*)$ is a structure on S with $1 \in S$ arbitrary bit fixed. $(F,\circ)$ is the group of all similarity mappings of $(S,*)$.

Suppose $\left(\overline{F},\circ\right) = (\{f_t : t \in S\}, \circ)$ is a subgroup of $(F,\circ)$ that has the following two properties where (b) comes from Convention 1.

(a) $(\{f_t : t \in S\}, \circ)$ is uniquely transitive on S. Of course, this implies $f_t \neq f_{\overline{t}}$ when $t \neq \overline{t}$.

(b) $\forall i \in S, f_i(1) = i$. This implies that f_1 must be the identity permutation of this group $\left(\overline{F}, \circ\right)$.

Using Conclusion 6 of Theorem 2 as a guide, we define the binary operator $(S, \cdot)$ on S as follows. $\forall i, j \in S, (f_i \circ f_j)(1) = (f_i f_j)(1) = f_i(f_j(1)) = f_i(j) = i \cdot j$. Thus, $i \cdot j = f_i(j)$. Of course, $\forall t \in S$, the permutation $f_t : S \to S$ can now be defined from this binary operator $(S, \cdot)$ by $\forall x \in S, f_t(x) = t \cdot x$. Then (1), (2), and (3) are true.

1. $(S, \cdot, 1)$ is a group with identity 1.
2. $(S, \cdot, 1)$ left-distributes over $(S, *)$.
3. The 1-1 onto matching $t \leftrightarrow f_t, \forall t \in S$, defines an isomorphism between the groups $(S, \cdot, 1)$ and $(\{f_t : t \in S\}, \circ, f_1)$.

Note 4. Observe that $\forall i, j \in S, i \cdot j = k$ where k is defined by $f_i \circ f_j = f_k$. This is because $i \cdot j = (f_i \circ f_j)(1) = f_k(1) = k$.

Observation 1. Before giving the proof, we emphasize that $(S, \cdot, 1)$ is defined from $(\{f_t : t \in S\}, \circ, f_1)$ by $\forall i, j \in S, i \cdot j = f_i(j)$. Also, reversing ourselves, we see that $(\{f_t : t \in S\}, \circ)$ is defined from $(S, \cdot, 1)$ by $\forall t \in S, \forall x \in S, f_t(x) = t \cdot x$. This same observation could also have been made after Theorem 2.

Proof of Theorem 3. We first prove the isomorphism given in Statement 3. Since $f_t \neq f_{\overline{t}}$ when $t \neq \overline{t}$, it is obvious that the matching $t \leftrightarrow f_t, \forall t \in S$, is a 1-1 onto matching between S and $\{f_t : t \in S\}$. Now $\forall i, j \in S$, we have the matchings $i \leftrightarrow f_i, j \leftrightarrow f_j$. Now by Note 4, $i \cdot j = k$ where $f_i \circ f_j = f_k$.

Therefore, we have the matching $i \cdot j \leftrightarrow f_i \circ f_j$. Therefore, the 1-1 onto matching $t \leftrightarrow f_t, \forall t \in S$, defines an isomorphism between the binary operators $(S, \cdot)$ and $(\{f_t : t \in S\}, \circ)$. Also, we have the matching $1 \leftrightarrow f_1$ where f_1 is the identity of $(\{f_t : t \in S\}, \circ)$. To prove Statement 1, observe that the above isomorphism and the matching $1 \leftrightarrow f_1$ implies that $(S, \cdot, 1)$ is a group and $1 \in S$ is the identity of the group.

We now prove Statement 2. That is, we prove that $(S, \cdot, 1)$ left-distributes over $(S, *)$. From Definition 2, this is true if and only if $\forall t \in S, L_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$ where $L_t(x) = t \cdot x$ is the left-translation by t. Now $L_t(x) = t \cdot x = f_t(x)$. Now $f_t \in \overline{F} \subseteq F$, and by hypothesis this means that $L_t = f_t$ is a similarity mapping on $(S, *)$. ■

The following Lemma 2 plays the dual role of Lemma 1.

Lemma 2. *$(S, *)$ is a structure on S and $1 \in S$ is arbitrary but fixed. $(F, \circ)$ is the group of all similarity mappings of $(S, *)$. Suppose= $\left(\overline{F}, \circ\right) = (\{f_t : t \in S\}, \circ)$ and $(F', \circ) = (\{f'_t : t \in S\}, \circ)$ are two different subgroups of $(F, \circ)$. $\left(\overline{F}, \circ\right) \neq (F', \circ)$ means that $\overline{F} \neq F'$. Also, suppose $\left(\overline{F}, \circ\right)$ and $(F', \circ)$ satisfy hypothesis*

(a) of Theorem 3. Also, suppose Convention 1 has been used so that $\left(\overline{F},\circ\right)$ *and* $(F',\circ)$ *satisfy hypothesis (b) of Theorem 3 as well. This means that (a) and (b) are true and also (c) is true.*

(a) $\left(\overline{F},\circ\right) = (\{f_t : t \in S\},\circ)$ *is uniquely transitive on* S*, and* $(F',\circ) = (\{f'_t : t \in S\},\circ)$ *is uniquely transitive on* S*. This implies* $f_t \neq f_{\overline{t}}$ *and* $f'_t \neq f'_{\overline{t}}$ *when* $t \neq \overline{t}$*.*

(b) Both groups $\left(\overline{F},\circ\right)$ *and* $(F',\circ)$ *have been indexed by* S *so that* $\forall i \in S, f_i(1) = i$ *and* $f'_i(1) = i$*. This implies that* $f_1 = f'_1$ *is the identity permutation of both groups* $\left(\overline{F},\circ\right)$ *and* $(F',\circ)$*. It also implies that* $\forall i,j \in S, f_i \neq f'_j$ *if* $i \neq j$*.*

(c) $\overline{F} = \{f_t : t \in S\} \neq \{f'_t : t \in S\} = F'$*.*

Suppose the two groups $(S,\cdot,1),(S,\odot,1)$ *with identity 1 are defined as in Theorem 3. That is,* $\forall i,j \in S,\ i \cdot j = f_i(j)$ *and* $i \odot j = f'_i(j)$*. Then* $(S,\cdot,1) \neq (S,\odot,1)$*.*

Proof. Since $\{f_t : t \in S\} \neq \{f'_t : t \in S\}$, we know that $\exists i \in S$ such that $f_i \neq f'_i$. Since $f_i \neq f'_i, \exists j \in S$ such that $f_i(j) \neq f'_i(j)$. Therefore, $i \cdot j = f_i(j) \neq f'_i(j) = i \odot j$. Therefore, $(S,\cdot,1) \neq (S,\odot,1)$. ■

Solution to the Main Problem. *If we allow* $1 \in S$ *to vary over* S*, we see that Theorems 2 and 3, the unique relabeling of* $\{f_t : t \in S\}$ *in Convention 1 so that* $\forall i \in S, f_i(1) = i$ *and Observation 1 will give a complete solution to the main problem. The solution has no redundancy. However, for emphasis we have also included Lemmas 1, 2 which gives redundancy in the proof of the solution.* ■

In Section 5, we carry out the second part of our plan.

6 An Equivalence Relation on the Groups $(S,\cdot)$ that Left-distribute over $(S,*)$

Theorem 4 Suppose $(S,\cdot,C_1)$ is a group on S with identity $C_1 \in S$. Also, $f : S \to S$ is a permutation on S. Then $\exists$ a unique group $(S,\odot)$ on S such that $f : (S,\cdot,C_1) \to (S,\odot)$ is an isomorphism from $(S,\cdot,C_1)$ to $(S,\odot)$. Of course, $f(C_1)$ must be the identity element of $(S,\odot)$.

Proof. We must have $\forall a,b \in S, f(a \cdot b) = f(a) \odot f(b)$. Since $f : S \to S$ is a permutation on S, we have $\forall \overline{a},\overline{b} \in S, \overline{a} \odot \overline{b} = f\left(f^{-1}(\overline{a}) \cdot f^{-1}\left(\overline{b}\right)\right)$. ■

Discussion 1. Theorem 4 means that the group $(S,\odot)$ can be defined from the group $(S,\cdot,C_1)$ and the permutation $f : S \to S$ in either of two equivalent ways.

1. We define $(S, \odot)$ directly by $\forall a, b \in S, a \odot b = f\left(f^{-1}(a) \cdot f^{-1}(b)\right)$.

2. $(S, \odot)$ is the unique group on S such that $f : (S, \cdot, C_1) \to (S, \odot)$ is an isomorphism from $(S, \cdot, C_1)$ to $(S, \odot)$.

Application 1. $(S, \cdot, C_i)$ is a group on S with identity $C_i \in S$. For each $C_j \in S$, the permutation $f_{c_j} : S \to S$ is defined by $\forall x \in S$, $f_{c_j}(x) = x \cdot C_j$. Also, $f_{c_j}^{-1}(x) = x \cdot C_j^{-1}$. Therefore, if $f_{c_j} : (S, \cdot, C_i) \to (S, \odot)$ is an isomorphism from $(S, \cdot, C_i)$ to the group $(S, \odot)$, then $\forall a, b \in S, a \odot b = \left(a \cdot C_j^{-1} \cdot b \cdot C_j^{-1}\right) \cdot C_j = a \cdot C_j^{-1} \cdot b$, where C_j^{-1} is computed in $(S, \cdot, C_i)$.

Also, the identity of $(S, \odot)$ is $f_{c_j}(C_i) = C_i \cdot C_j = C_j$. Thus, $(S, \odot) = (S, \odot, C_j)$.

Theorem 5 Suppose $(S, \cdot, C_i)$ is a group with identity C_i that left-distributes over the structure $(S, *)$.

Also, the group $(S, \odot, C_j)$ with identity C_j is defined from $(S, \odot, C_i)$ by $\forall a, b \in S, a \odot b = a \cdot C_j^{-1} \cdot b$ where C_j^{-1} is computed in $(S, \cdot, C_i)$. Then $(S, \odot, C_j)$ also left-distributes over $(S, *)$.

Proof. We show that for the group $(S, \odot, C_j)$, $\forall t \in S, \overline{L}_t : (S, *) \to (S, *)$ is a similarity mapping on $(S, *)$ where $\overline{L}_t(x) = t \odot x, \forall x \in S$. Now $\overline{L}_t(x) = t \odot x = t \cdot C_j^{-1} \cdot x$,

Now $\overline{L}_t(x) = L_{t \cdot C_j^{-1}}(x)$ where $\overline{L}_t(x)$ is the left translation by t in the group $(S, \odot)$ and $L_{t \cdot C_j^{-1}}(x)$ is the left translation by $t \cdot C_j^{-1}$ in the group $(S, \cdot)$. Now $L_{t \cdot C_j^{-1}}(x)$ is a similarity mapping on $(S, *)$ since $(S, \cdot)$ left distributes over $(S, *)$. Therefore, $\overline{L}_t(x)$ is a similarity mapping on $(S, *)$. ■

Theorem 6 Suppose $(S, \cdot, C_1)$ is a group on S with identity $C_1 \in S$. Also, the group $(S, \odot, C_2)$ with identity $C_2 \in S$ is defined from the group $(S, \cdot, C_1)$ by the isomorphism $(x \cdot C_2) : (S, \cdot, C_1) \to (S, \odot, C_2)$. That is, $\forall a, b \in S, a \odot b = a \cdot C_2^{-1} \cdot b$ where C_2^{-1} is computed in $(S, \cdot, C_1)$. Then the group $(S, \cdot, C_1)$ can be defined from the group $(S, \odot, C_2)$ by the isomorphism $(x \odot C_1) : (S, \odot, C_2) \to (S, \cdot, C_1)$. That is, $\forall a, b \in S, a \cdot b = a \odot C_1^{-1} \odot b$ where C_1^{-1} is computed in $(S, \odot, C_2)$.

Proof. Let us denote $\forall x \in S, f(x) = x \cdot C_2$ and $\forall x \in S, g(x) = x \odot C_1$. Therefore, $f : (S, \cdot, C_1) \to (S, \odot, C_2)$ is an isomorphism from $(S, \cdot, C_1)$ to $(S, \odot, C_2)$ and $f^{-1} : (S, \odot, C_2) \to (S, \cdot, C_1)$ is an isomorphism from $(S, \odot, C_2)$ to $(S, \cdot, C_1)$. We now show that $f^{-1} = g$ which will imply that $g : (S, \odot, C_2) \to (S, \cdot, C_1)$ is an isomorphism from $(S, \odot, C_2)$ to$(S, \cdot, C_1)$. Since f and g are permutations on S, $f^{-1} = g$ is true if and only if $\forall x \in S, (g \circ f)(x) = x$. Now $\forall x \in S, (g \circ f)(x) = (x \cdot C_2) \odot C_1 = (x \cdot C_2) \cdot C_2^{-1} \cdot C_1 = x \cdot C_1 = x$ since C_2^{-1} is computed in $(S, \cdot, C_1)$ and C_1 is the identity of $(S, \cdot, C_1)$ ■.

Theorem 7 $(S, \cdot, C_1)$ is a group with identity C_1. Suppose the group $(S, \odot, C_2)$ with identity C_2 is defined from $(S, \cdot, C_1)$ by the isomorphism $(x \cdot C_2)$:

$(S,\cdot,C_1)\to(S,\odot,C_2)$. That is, $\forall a,b\in S, a\odot b=a\cdot C_2^{-1}\cdot b$ where C_2^{-1} is computed in $(S,\cdot,C_1)$. Also, the group $(S,\boxdot,C_3)$ with identity C_3 is defined from $(S,\cdot,C_1)$ by the isomorphism $(x\cdot C_3):(S,\cdot,C_1)\to(S,\boxdot,C_3)$. That is, $\forall a,b\in S, a\boxdot b=a\cdot C_3^{-1}\cdot b$ where C_3^{-1} is computed in $(S,\cdot,C_1)$. Then, $(S,\boxdot,C_3)$ can be defined from $(S,\odot,C_2)$ by the isomorphism $(x\odot C_3):(S,\odot,C_2)\to(S,\boxdot,C_3)$. That is, $\forall a,b\in S, a\boxdot b=a\odot C_3^{-1}\odot b$ where C_3^{-1} is computed in $(S,\odot,C_2)$.

Proof. From Theorem 6, we know that $(x\odot C_1):(S,\odot,C_2)\to(S,\cdot,C_1)$ is an isomorphism from $(S,\odot,C_2)$ to $(S,\cdot,C_1)$. Also, by hypothesis $(x\cdot C_3):(S,\cdot,C_1)\to(S,\boxdot,C_3)$ is an isomorphism from $(S,\cdot,C_1)$ to $(S,\boxdot,C_3)$. Therefore, $(x\odot C_1)\cdot C_3:(S,\odot,C_2)\to(S,\boxdot,C_3)$ is an isomorphism from $(S,\odot,C_2)\to(S,\boxdot,C_3)$. Therefore, we must show that $\forall x\in S,(x\odot C_1)\cdot C_3=x\odot C_3$.

Now, $\forall x\in S, x\odot C_3=x\cdot C_2^{-1}\cdot C_3$ where C_2^{-1} is computed in $(S,\cdot,C_1)$. Also, $\forall x\in S,(x\odot C_1)\cdot C_3=\left(x\cdot C_2^{-1}\cdot C_1\right)\cdot C_3=x\cdot C_2^{-1}\cdot C_3$ where C_2^{-1} is computed in $(S,\cdot,C_1)$ since C_1 is the identity of $(S,\cdot,C_1)$.

Therefore, $\forall x\in S,(x\odot C_1)\cdot C_3=x\odot C_3$. ■

We now summarize Theorems 4 - 7.

Summary 1. Calling $\cdot=\odot_1$, suppose $(S,\cdot,C_1)=(S,\odot_1,C_1)$ is a group on S with identity C_1 that left-distributes over the structure $(S,*)$ on S. $\forall C_i\in S$, define the group $(S,\odot_i,C_i)$ with identity C_i by $\forall a,b\in S, a\odot_i b=a\cdot C_i^{-1}\cdot b$ where C_i^{-1} is computed in $(S,\cdot,C_1)=(S,\odot_1,C_1)$. Then each $(S,\odot_i,C_i)$ left-distributes over $(S,*)$. Also, for each pair $(S,\odot_i,C_i),(S,\odot_j,C_j)$ we know that $(x\odot_i C_j):(S,\odot_i,C_i)\to(S,\odot_j,C_j)$ is an isomorphism from $(S,\odot_i,C_i)$ to $(S,\odot_j,C_j)$. This means that $\forall a,b\in S, a\odot_j b=a\odot_i C_j^{-1}\odot_i b$ where C_j^{-1} is computed in $(S,\odot_i,C_i)$. Using this let us suppose that the two groups $(S,\odot_i,C_i)$ and $(S,\odot_j,C_j)$ with identities C_i,C_j are any two groups on S that left-distributes over the structure $(S,*)$. We say that $(S,\odot_i,C_i)$ is R-related to $(S,\odot_j,C_j)$ if $(x\odot_i C_j):(S,\odot_i,C_i)\to(S,\odot_j,C_j)$ is an isomorphism from $(S,\odot_i,C_i)$ to $(S,\odot_j,C_j)$. Then R is an equivalence relation on the collection of all groups $(S,\cdot)$ that left-distributes over the structure $(S,*)$.

7 Concluding Remarks on the Main Problem

As in Theorem 3, $(S,*)$ is a structure on S with $1=C_1\in S$ arbitrary but fixed. Also, $(F,\circ)$ is the group of all similarity mappings of $(S,*)$. As in Theorem 3, we suppose that $\left(\overline{F},\circ\right)=\left(\{f_t:t\in S\},\circ\right)$ is a subgroup of $(F,\circ)$ that satisfies property (a) and has been indexed by S so that it also satisfies property (b).

(a) $(\{f_t:t\in S\},\circ)$ is uniquely transitive on S. This implies $f_t\neq f_{\overline{t}}$ when $t\neq\overline{t}$.

(b) $\forall i\in S, f_i(1)=f_i(C_1)=i$.

As in Theorem 3, the group $(S,\cdot,1)=(S,\cdot,C_1)$ with identity $1=C_1$ is defined as follows. $\forall i,j\in S, i\cdot j=(f_i\circ f_j)(1)=f_i(j)$. Of course, $(S,\cdot,1)=(S,\cdot,C_1)$ left-distributes over $(S,*)$

Let us now select a different $C_2\in S$. Using C_2, we wish to reindex $\{f_t:t\in S\}=\left\{\overline{f}_t:t\in S\right\}$ so that $\forall i\in S,\overline{f}_i(C_2)=i$. Now since $f_{C_2}(1)=f_{C_2}(C_1)=C_2$, we know that $f_{C_2}^{-1}(C_2)=1=C_1$. Therefore, $\forall i\in S,\left(f_i\circ f_{C_2}^{-1}\right)(C_2)=f_i(1)=i$.

Therefore, $\forall i\in S$, let us call $f_i\circ f_{C_2}^{-1}=\overline{f}_i$. Of course, the matching $f_i\leftrightarrow\overline{f}_i$, $\forall i\in S$, is a 1-1 onto matching on $\{f_i:i\in S\}$. Thus, $\forall i\in S,\overline{f}_i\in\{f_t:t\in S\}$ and $\overline{f}_i(C_2)=i$. Of course, $\left(\left\{\overline{f}_t:t\in S\right\},\circ\right)$ is also uniquely transitive on S.

By analogy to the above, we now use $\left(\left\{\overline{f}_t:t\in S\right\},\circ\right)$ to define the group $(S,\odot,C_2)$ with identity C_2 as follows, and again $(S,\odot,C_2)$ left-distributes over $(S,*)$. Note that $\forall i,j\in S, i\odot j=\left(\overline{f}_i\circ\overline{f}_j\right)(C_2)=\overline{f}_i(j)$. This means $\forall i,j\in S, i\odot j=\left(f_i\circ f_{C_2}^{-1}\right)(j)$.

From Theorem 3, we know that the 1-1 onto matching $t\leftrightarrow f_t,\forall t\in S$, defines an isomorphism between the two groups $(S,\cdot,1=C_1)$ and $(\{f_t:t\in S\},\circ)$. Therefore, $f_{C_2}^{-1}=f_{C_2^{-1}}$ where C_2^{-1} is computed in $(S,\cdot,1=C_1)$. Also, from this isomorphism (or from Note 4), $f_i\circ f_{C_2}^{-1}=f_i\circ f_{C_2^{-1}}=f_{i\cdot C_2^{-1}}$ where $i\cdot C_2^{-1}$ is computed in $(S,\cdot,1=C_1)$. Therefore, $i\odot j=\left(f_i\circ f_{C_2}^{-1}\right)(j)=\left(f_i\circ f_{C_2^{-1}}\right)(j)=f_{i\cdot C_2^{-1}}(j)=i\cdot C_2^{-1}\cdot j$. Thus, $(S,\odot,C_2)$ is defined from $(S,\cdot,1=C_1)$ in exactly the same way as was done in the preceding Section 5. What this means is that each of the different subgroups $\left(\overline{F},\circ\right)$ of $(F,\circ)$ that was defined in the first paragraph of this section gives rise to all of the groups (one for each $C_i\in S$) appearing in exactly one of the equivalency classes specified at the end of Summary 1 in Section 5.

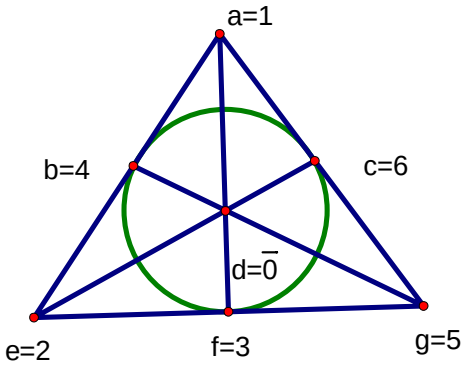
Note 5. Suppose $(S,*)$ is a given structure on S. Now a group $(S,\cdot)$ right-distributes over $(S,*)$ if and only if the group $(S,\odot)$ left-distributes over $(S,*)$ where $\forall a,b\in S, a\odot b=b\cdot a$. We have developed the machinery for finding all groups $(S,\cdot)$ such that $(S,\cdot)$ left-distributes over $(S,*)$. To find all groups $(S,\cdot)$ such that $(S,\cdot)$ distributes over $(S,*)$ we must test each $(S,\cdot)$ that left-distributes over $(S,*)$ to see whether its corresponding $(S,\odot)$ left-distributes over $(S,*)$.

8 An Application to Steiner Triples

A collection of Steiner triples on a set S is a collection of tripleton subsets of S having the property that each doubleton subset of $S,\{a,b\}\subseteq S$, is a subset of exactly one of these Steiner triples. We can easily show that a collection of Steiner triples on a set S is equivalent to a binary operator $(S,\cdot)$ on S

that satisfies $\forall a, b \in S$, (1) $a \cdot a = a$, (2) $a \cdot b = b \cdot a$, (3) $(a \cdot b) \cdot a = b$. Each doubleton subset $\{a, b\} \subseteq S$ is a member of the Steiner triple $\{a, b, a \cdot b\}$. Observe that $\{a, a \cdot b\}$ is a subset of $\{a, a \cdot b, a \cdot (a \cdot b) = b\}$ and $\{b, a \cdot b\}$ is a subset of $\{b, a \cdot b, b \cdot (a \cdot b) = a\}$.

Fig. 1 gives an example of a very special class of Steiner triples that was studied extensively by Marshall Hall. See [4].



In Fig. 1 any tripleton subset $\{x, y, z\}$ of $\{a, b, c, d, e, f, g\}$ is a Steiner-triple if and only if x, y, z lies on a straight line or on the circle. Thus, $\{a, d, f\}$ and $\{b, c, f\}$ are Steiner triples.

The general class of these Steiner triples is defined as follows. Let $(S, 0, +)$ be an Abelian group satisfying $\forall a \in S, a + a = 2a = 0$. We define Steiner triples on $S \backslash \{0\}$ as follows. Any tripleton subset $\{x, y, z\} \subseteq S \backslash \{0\}$ is a Steiner triple on $S \backslash \{0\}$ if and only if $x + y + z = 0$ in $(S, 0, +)$. Of course, this collection of Steiner triples on $S \backslash \{0\}$ is equivalent to the binary operator $(S \backslash \{0\}, \cdot)$ where $\forall x, y \in S \backslash \{0\}, x \cdot y = x = y$ if $x = y$ and $x \cdot y = -x - y = x + y$ if $x \neq y$.

It is easy to prove that the collection of automorphisms on this collection of Steiner triples $(S \backslash \{0\}, \cdot)$ is identical to the collection of automorphisms on the group $(S, 0, +)$ where we agree to ignore the 0 element since 0 maps to 0 in all automorphisms on $(S, 0, +)$.

Now if $(S, 0, +)$ satisfying $\forall a \in S, 2a = 0$ is finite, then $|S \backslash \{0\}| = 2^n - 1$.

Suppose $2^n - 1 = p$, a prime. This is the case in Fig. 1 since $2^3 - 1 = 7$.

Now the automorphism group of the Steiner triples $(S \backslash \{0\}, \cdot)$ has $(2^n - 1)(2^n - 2)(2^n - 4) \cdots (2^n - 2^{n-1})$ elements. Since $2^n - 1 = p$ is prime, we know from a Sylov theorem that $\exists$ a subgroup of automorphisms of $(S \backslash \{0\}, \cdot)$ that contains exactly p elements, and this subgroup is a cyclic group.

Since p is a prime, we know from elementary group theory that this cyclic group of permutations on $S \backslash \{0\}$ must be uniquely transitive on $S \setminus \{0\}$. Using Convention 1 and Theorem 3 of Section 3, we know that it is possible to label the p elements of $S \backslash \{0\}, \overline{0}, 1, 2, 3, \cdots, p - 1$ in such a way that $\forall t \in \left\{\overline{0}, 1, 2, 3, \cdots, p - 1\right\}$, if $\{x, y, z\}$ is a Steiner triple in $(S \backslash \{0\}, \cdot)$ then

$\{x+t, y+t, z+t\}$ is a Steiner triple in $(S\backslash\{0\}, \cdot)$ where $x+t, y+t, z+t$ is computed in the usual cyclic group $\left(\left\{\overline{0}, 1, 2, \cdots, p-1\right\}, \overline{0}, +\right)$. This cyclic group is defined by $\forall a, b \in \left\{\overline{0}, 1, 2, 3, \cdots, p-1\right\}, a+b \equiv a+b, (\text{mod } p,)$ where the right side + is the usual addition.

In Fig. 1 we have shown one possible labeling of the 7 vertices. In Fig. 1 it is possible to label the 7 vertices $\overline{0}, 1, 2, 3, \cdots, 6$ in at least 168 different ways, one for each of the $7 \cdot 6 \cdot 4 = 168$ different automorphisms on the Steiner triples $(S\backslash\{0\}, \cdot)$. We will not prove it here but it is fairly easy to show that this labeling can be done in only 168 different ways.

Appendix

We illustrate the converse problem for the cases where $(S, *)$ is an n-ary operator on S and $(S, *)$ is an n-ary relation on S. However, in general the converse problem will be more complex than this. First, suppose $(S, \cdot, 1)$ is a given group on S. We wish to find all n-ary, $n \geq 2$, operators $(S, *)$ on S such that $(S, \cdot)$ left-distributes over $(S, *)$. This means that we wish to find all n-ary operators $(S, *)$ on S such that $\forall x, a_1, a_2, \cdots, a_n \in S, x \cdot (a_1 * a_2 * \cdots * a_n) = (x \cdot a_1) * (x \cdot a_2) * \cdots * (x \cdot a_n)$. Let $f : S^{n-1} \to S$ be an arbitrary function from $S^{n-1} = S \times S \times \cdots \times S\,(n-1 \text{ times})$ to S.

If $(S, \cdot, 1)$ left-distributes over $(S, *)$ and $\forall x_2, x_3, \cdots, x_n \in S, 1 * x_2 * x_3 * \cdots * x_n = f(x_2, x_3, \cdots, x_n)$, then $(S, *)$ must be uniquely defined from $f : S^{n-1} \to S$. To see this, observe that $a_1 * a_2 * \cdots * a_n = (a_1 \cdot 1) * \left(a_1 \cdot \left(a_1^{-1} \cdot a_2\right)\right) * \cdots * \left(a_1 \cdot \left(a_1^{-1} \cdot a_n\right)\right) = a_1 \cdot \left[1 * \left(a_1^{-1} \cdot a_2\right) * \left(a_1^{-1} \cdot a_3\right) * \cdots * \left(a_1^{-1} \cdot a_n\right)\right] = a_1 \cdot f\left(a_1^{-1} \cdot a_2, a_1^{-1} \cdot a_3, \cdots, a_1^{-1} \cdot a_n\right)$. Also, this is compatible with $1 * x_2 * x_3 * \cdots * x_n = f(x_2, x_3, \cdots, x_n)$.

Next, suppose $(S, *)$ is defined by $\forall a_1, a_2, \cdots, a_n \in S$,

$$a_1 * a_2 * \cdots * a_n = a_1 \cdot f\left(a_1^{-1} \cdot a_2, a_1^{-1} \cdot a_3, \cdots, a_1^{-1} \cdot a_n\right).$$

We show that $(S, \cdot, 1)$ left-distributes over $(S, *)$. This is true if and only if $\forall x, a_1, a_2, \cdots, a_n \in S, x \cdot (a_1 * a_2 * \cdots * a_n) = (x \cdot a_1) * (x \cdot a_2) * \cdots * (x \cdot a_n)$. Now $x \cdot (a_1 * a_2 * \cdots * a_n) = x \cdot \left(a_1 \cdot f\left(a_1^{-1} \cdot a_2, a_1^{-1} \cdot a_3, \cdots, a_1^{-1} \cdot a_n\right)\right)$.

Also, $(x \cdot a_1) * (x \cdot a_2) * \cdots * (x \cdot a_n) = (x \cdot a_1) \cdot f\left((x \cdot a_1)^{-1} \cdot (x \cdot a_2), \cdots, (x \cdot a_1)^{-1} \cdot (x \cdot a_n)\right) = (x \cdot a_1) \cdot f\left(a_1^{-1} \cdot a_2, a_1^{-1} \cdot a_3, \cdots, a_1^{-1} \cdot a_n\right)$. ■

The solution for an n-ary relation on S is very similar and is left to the reader after we define what we mean by an n-ary relation (S, R, C) on S.

Definition 1. *Let $n \geq 2$ be a fixed positive integer. (S, R, C) denotes an n-ary relation R from a set S to a set C. This means that for each n-tuple $(a_1, a_2, \cdots, a_n)$, where each $a_i \in S$, we associate with $(a_1, a_2, \cdots, a_n)$ a member of C which we denote as $R(a_1, a_2, \cdots, a_n) \in C$.*

Notation 2 Given (S, R, C), we define an n-ary operator from S to C as follows. $\forall a_1, a_2, \cdots, a_n \in S, a_1 * a_2 * \cdots * a_n = R(a_1, a_2, \cdots, a_n)$. We say that $(S, R, C) = (S, *, C)$.

Definition 2. $(S, \cdot, 1)$ *is a group on* S *with identity 1. Also,* $(S, R, C) = (S, *, C)$ *is an* n*-ary relation from* S *to* C*. We say that* $(S, \cdot, 1)$ *left-distributes over* $(S, *, C)$ *if* $\forall x, a_1, a_2, \cdots, a_n \in S, a_1 * a_2 * \cdots * a_n = (x \cdot a_1) * (x \cdot a_2) * \cdots * (x \cdot a_n)$*. If the group* $(S, \cdot, 1)$ *and the set* C *are given, the problem of finding all* n*-ary relations* $(S, R, C) = (S, *, C)$ *from* S *to* C *such that* $(S, \cdot, 1)$ *left-distributes over* $(S, *, C)$ *is very similar to the previous problem and is left as an easy exercise for the reader*

References

[1] Kelly, John L., *General Topology*, D. Van Nostrard, New York, 1955, 105-106.

[2] Monk, Donald, *Introduction to Set Theory*, McGraw-Hill New York 1969.

[3] Maclagan, Diane and Ben Davis, The Card Game Set, The Mathematical Intelligencer, 2S, No. 3, 2003, 33-40.

[4] Hall, Marshall, *The Theory of Groups*, MacMillan - New York, 1959.

[5] Richard Hubert Bruck, *A Survey of Binary Systems*, Springer-Verlag, Berlin and New York, 1958.

Received: December 7, 2007