Generalized Groups that Distribute over Stars

Harold Reiter

Department of Mathematics,

University of North Carolina Charlotte,

Charlotte, NC 28223, USA

hbreiter@email.uncc.edu

Arthur Holshouser

3600 Bullard St.

Charlotte, NC,

USA

1 Abstract

In the paper "Groups that Distribute over Mathematical Structures", [5], we stated that a group $(S, \cdot)$ on a set S left (or right) distributes over an arbitrary mathematical structure $(S, *)$ on the same set S if and only if respectively for all fixed $t \in S$ the permutation $L_t(x) = t \cdot x$ (or $R_t(x) = x \cdot t$) is a similarity mapping on $(S, *)$. A similarity mapping f on $(S, *)$ is a permutation on S that preserves the structure of $(S, *)$ such as a homeomorphism on a topological space, an automorphism on a binary operator or a similarity mapping on a binary relation. Also, $L_t(x)$ and $R_t(x)$ are called the left and right translations by t. For example, the group $(\mathbb{R}, \circ, +)$ both left and right distributes over the space of real numbers $(\mathbb{R}, T)$ with the usual topology. In other words, for all subsets U of $\mathbb{R}$, and for all $x \in \mathbb{R}$, $U + x = x + U$ is an open subset of $\mathbb{R}$ if and only if U is an open subset of $\mathbb{R}$. See [5] for the details.

In this paper we define and give a reasonably complete solution for a naturally occurring example that involves what we call an n-star which is structurally the same as n lines in the plane intersecting in $\binom{n}{2}$ district points.

However, an equally important purpose of this paper is to show that if a structure $(S, *)$ is given, then a fundamental idea is to see if a group $(S, \cdot)$ exists such that $(S, \cdot)$ left-distributes or right-distributes over $(S, *)$.

This paper takes the reader on a long journey, but we hope that it is a reasonably fast and easy journey.

2 Introduction

Suppose $(S,*)$ is an arbitrary structure on a set S. In the paper [5] which the reader can easily access electronically, we show how to construct all groups $(S,\cdot)$ on S such that $(S,\cdot)$ left-distributes or right-distributes over $(S,*)$ if such a group exists. However, usually such a group $(S,\cdot)$ will not exist. Our construction used the group of all similarity mappings on $(S,*)$ which we now call $\left(\overline{F},\circ\right)$. We showed that a group $(S,\cdot)$ exists such that $(S,\cdot)$ left-distributes over $(S,*)$ if and only if there exists a subgroup $\left(\overline{G},\circ\right)$ of $\left(\overline{F},\circ\right)$ such that $\left(\overline{G},\circ\right)$ is uniquely transitive on S. This means that for every $a,b\in S$, there exists a unique $f\in\overline{G}$ such that $f(a)=b$. If such a $\left(\overline{G},\circ\right)$ exists then a group $(S,\cdot)$ that left-distributes over $(S,*)$ was defined in theorem 3, [5] as follows.

First, we arbitrarily choose $1\in S$ to be the identity of $(S,\cdot)$. Then we index $\overline{G}=\{f_t : t\in S\}$ so that $\forall i\in S, f_i(1)=i$. We can do this since $\left(\overline{G},\circ\right)$ is uniquely transitive on S, and we can do it by either renaming the members of S or renaming the members of $\overline{G}$. A group $(S,\cdot)$ with identity 1 that left-distributes over $(S,*)$ is then defined by $\forall i,j\in S, i\cdot j=f_i(j)$. It is also very important to emphasize that in theorem 3, [5] we also proved that the groups $(S,\cdot)$ and $\left(\overline{G},\circ\right)$ are isomorphic (i.e., $(S,\cdot)\cong\left(\overline{G},\circ\right)$) through the isomorphism $f_i\circ f_j=f_{i\cdot j}$.

It is also obvious that if the group $(S,\cdot)$ left-distributes over $(S,*)$ then the group $(S,\odot)$ defined by $a\odot b=b\cdot a$ will right-distribute over $(S,*)$.

By studying the paper [5], it becomes obvious that intuitively a necessary condition on $(S,*)$ is that the structure of $(S,*)$ must be fairly homogeneous and symmetric. This follows from the transitive property of $(\overline{G},\circ)$ We cannot tell just by looking at a structure $(S,*)$ whether it is homogeneous and symmetric enough or not. However, any time that we encounter a structure $(S,*)$ that appears to be fairly homogeneous and symmetric then it is natural to ask if a group $(S,\cdot)$ exists which left (or right) distributes over $(S,*)$. We now proceed to illustrate this by studying n-stars. Intuitively these stars look alike. But some have groups that left (or right) distribute over them and some do not, and this illustrates the delicate balance that must exist. We will show that a necessary condition is that $n=p^t$ where p is a prime of the form $p=4k+3$ and t is odd. Also, we will construct **all types of groups** (up to isomorphism) that left (or right) distribute over the n-star. This **construction** uses an Abelian group on the set $\{1,2,\cdots,n=p^t\}$ and a group of automorphisms on this Abelian group.

3 Generalized n-Stars

In sections 3-5 we study n-stars using one set of definitions, and in sections 6-7 we use a different set of definitions. Also, in section 7 we state an axiom. Then in sections 8-10 we use the material in sections 3-7 including the axiom of section 7 to construct all types of groups that left (or right) distribute over the n-stars. In section 11 we use different techniques to prove the axiom of section 7 and also to prove deeper properties of the n-stars. For example, we prove that a necessary condition on the n-stars is that $n = p^t$ where p is a prime of the form $p = 4k + 3$ and t is odd. Then in section 12 we give some applications.

Suppose n lines in the plane called $L = \{l_1, l_2, \cdots, l_n\} = \{1, 2, \cdots, n\}$ intersect each other in $\binom{n}{2} = \frac{n(n-1)}{2}$ distinct points which we call $D_L = \{\{l_i, l_j\} : i \neq j, l_i, l_j \in L\} = \{\{i, j\} : i \neq j, i, j \in \{1, 2, \cdots, n\}\}$. D_L stands for doubleton sets on L. If these n lines are the sides of a regular n-gon, then these $\binom{n}{2}$ points can be viewed as generalized n-stars. However, we must allow points at infinity when n is even. In Fig. 1 we show the n-stars for $n = 3, 4, 5, 6$ and in Fig. 2 we show the n-star for $n = 7$. We denote the n-star by $(D_L, *)$.

Let us define the group $(F, \circ)$ of all permutations on $L = \{l_1, l_2, \cdots, l_n\} = \{1, 2, \cdots, n\}$ using composition of functions. This group $(F, \circ)$ which contains $n!$ permutations is the standard symmetric group on L. It is almost obvious that each permutation f on L defines a corresponding line preserving permutation $\overline{f}$ on D_L when $\forall \{i, j\} \in D_L, \overline{f}(\{i, j\}) = \{f(i), f(j)\}$. For example if $f = \begin{pmatrix} l_1 & l_2 & l_3 & l_4 & l_5 \\ l_3 & l_1 & l_5 & l_2 & l_4 \end{pmatrix}$,

$$\text{then } \overline{f} = \begin{pmatrix} \{l_1l_2\} & \{l_1l_3\} & \{l_1l_4\} & \{l_1l_5\} & \{l_2l_3\} & \{l_2l_4\} & \{l_2l_5\} & \{l_3l_4\} & \{l_3l_5\} & \{l_4l_5\} \\ \{l_1l_3\} & \{l_3l_5\} & \{l_2l_3\} & \{l_3l_4\} & \{l_1l_5\} & \{l_1l_2\} & \{l_1l_4\} & \{l_2l_5\} & \{l_4l_5\} & \{l_2l_4\} \end{pmatrix}.$$

This line preserving permutation $\overline{f}$ is shown in Fig. 3, and the reader should study this carefully. In Fig. 3 we note that line l_1 is moved to l_3, line l_2 is moved to l_1, line l_3 is loved to l_5, line l_4 is moved to l_2 and line l_5 is moved to l_4. This changes the positions of the points $\{i, j\}$ as shown. The important thing to notice is that if 4 points in the first drawing lie in a straight line then these same 4 points lie in a straight line in the second drawing. This is why we call $\overline{f}$ a line preserving permutation on D_L. In Lemmas 1, 2 we show that these $n!$ line preserving permutations on D_L form a group using composition of functions. Lemmas

1, 2 also relate this group of line preserving permutations on D_L and the symmetric group on L.

Lemma 1 *Suppose, f, g are permutations on $L = \{l_1, l_2, \cdots, l_n\} = \{1, 2, \cdots, n\}$ where $n \geq 3$. Also, $\overline{f}, \overline{g}$ are the corresponding line preserving permutations on D_L. Then $f \neq g$ implies $\overline{f} \neq \overline{g}$. Thus, the mapping $f \to \overline{f}$ is $1-1$.*

Proof. Since $f \neq g, \exists a \in L$ such that $f(a) \neq g(a)$.

Suppose $b \in L \setminus \{a\}$. Now if $\overline{f}(\{a,b\}) = \{f(a), f(b)\} \neq \overline{g}(\{a,b\}) = \{g(a), g(b)\}$ then there is nothing to prove.

Therefore, suppose $\{f(a), f(b)\} = \{g(a), g(b)\}$.

Therefore, $f(a) \neq g(a)$ implies $f(a) = g(b)$ and $f(b) = g(a)$.

Since $n \geq 3$ suppose $c \in L \setminus \{a, b\}$.

Now, $f(a) = g(b)$ implies $f(a) \neq g(c)$.

Therefore, since $f(a) \neq g(a)$ we see that $\overline{f}(\{a,c\}) = \{f(a), f(c)\} \neq \{g(a), g(c)\} = \overline{g}(\{a,c\})$. Therefore, $\overline{f}(\{a,c\}) \neq \overline{g}(\{a,c\})$ which implies $\overline{f} \neq \overline{g}$. ■

Lemma 2 *If f, g are permutations on $L = \{l_1, l_2, \cdots, l_n\}$ and $\overline{f}, \overline{g}$ are the corresponding line preserving permutations on D_L then $\overline{f \circ g} = \overline{f} \circ \overline{g}$.*

Note 1 Thus when $n \geq 3$ the symmetric group of all permutations on L which we call $(F, \circ)$ is isomorphic to the corresponding group of line preserving permutations on D_L which we now call $(\overline{F}, \circ)$. That is, $(F, \circ) \cong (\overline{F}, \circ)$.

Proof of Lemma 2 $\overline{(f \circ g)}(\{i,j\}) = \{(f \circ g)(i), (f \circ g)(j)\}$. Also, $(\overline{f} \circ \overline{g})(\{i,j\}) = \overline{f}(\overline{g}(\{i,j\})) = \overline{f}(\{g(i), g(j)\}) = \{f(g(i)), f(g(j))\} = \{(f \circ g)(i), (f \circ g)(j)\}$. Therefore, $\overline{f \circ g} = \overline{f} \circ \overline{g}$. ■

4 Groups that Distribute over n-Stars

We say that a permutation $\overline{f}$ on D_L is a similarity mapping on the n-star $(D_L, *)$ if and only if $\overline{f}$ maps lines onto lines. It is easy to show that this is true if and only if $\overline{f}$ corresponds to some permutation f on $L = \{l_1, l_2, \cdots, l_n\}$ as defined above. Thus, $(\overline{F}, \circ)$ is also the group of all similarity mappings on $(D_L, *)$ and as above we have $(\overline{F}, \circ) \cong (F, \circ)$. The reason that the above is true is that the $n-1$ points on the line l_1 can be mapped in $(n-1)!$ different ways onto the $n-1$ points of any line l_i. Also, once the $n-1$ points on line l_1 have been mapped onto l_i, the mapping of the other points of the n-star are uniquely determined from this. This gives a total of $n \cdot (n-1)! = n!$ different mappings which is the same number as the $n!$ permutations on L.

Of course, from the paper [5] this means that a group $(D_L, \cdot)$ with operator $(\cdot)$ on the set D_L left-distributes over the n-star $(D_L, *)$ if and only if for all fixed $t \in D_L$, the permutation $\{(x_i, t \cdot x_i) : x_i \in D_L\}$ is a line preserving permutation on D_L.

If we examine the 5 stars shown in Fig. 1 and Fig. 2, we see that the points on these 5 stars intuitively seem to be fairly homogeneous and symmetric. As always in such a case, it is natural to ask if there exists a group $(D_L, \cdot)$ that left (or right) distributes over the n-star $(D_L, *)$ as n ranges over $\{3, 4, 5, 6, \cdots\}$.

In sections 5-11 we give a reasonably complete solution to the following Main Problem.

Main Problem Find all n-stars $(D_L, *)$ on the set $L = \{l_1, l_2, \cdots, l_n\}$ that have groups $(D_L, \cdot)$ that left (or right) distribute over them. Also, for each n-star $(D_L, *)$ that has a group $(D_L, \cdot)$ that left (or right) distributes over it, find all of the different types of groups $(D_L, \cdot)$, up to isomorphism, that left (or right) distribute over $(D_L, *)$.

5 A Necessary Condition on $(D_L, *)$

Lemma 3 *If $|D_L| = \frac{n(n-1)}{2}$ is even, then there does not exist a group $(D_L, \cdot)$ that left (or right) distributes over the n-star $(D_L, *)$ when $L = \{l_1, l_2, \cdots, l_n\}$.*

Proof. As always let $(\overline{F}, \circ)$ be the group of all line preserving permutations on D_L. Using the introduction, suppose there exists a subgroup $(\overline{G}, \circ)$ of $(\overline{F}, \circ)$ such that $(\overline{G}, \circ)$ is uniquely transitive on D_L. Of course, $(\overline{G}, \circ)$ must have exactly $|\overline{G}| = n(n-1)/2$ permutations since $(\overline{G}, \circ)$ is uniquely transitive on D_L and $|D_L| = \frac{n(n-1)}{2}$. Since $|\overline{G}|$ is even, by the Syloe theorems of group theory we know that $\exists \overline{f} \in \overline{G}$ such that $\overline{f} \neq i$ and $\overline{f} \circ \overline{f} = i$, the identity permutation on D_L. By the isomorphism $\overline{f \circ g} = \overline{f} \circ \overline{g}$ stated in lemmas 1, 2, this implies that $\exists$ a permutation f on $L = \{l_1, l_2, \cdots, l_n\}$, such that (1) $f \neq I$, (2) $f \circ f = I$, the identity permutation on L, and (3) $f, \overline{f}$ correspond to each other as defined earlier by $\overline{f}(\{i, j\}) = \{f(i), f(j)\}$. Since $f \neq I$ and $f \circ f = I$, this implies that $\exists i, j \in L, i \neq j$, such that $f(i) = j$ and $f(j) = i$. Therefore, $\overline{f}(\{i, j\}) = \{f(i), f(j)\} = \{i, j\}$.

But since $\overline{f} \neq i$, the identity permutation on D_L, and since $i\left(\{i,j\}\right) = \{i,j\}$, we see that $\left(\overline{G}, \circ\right)$ cannot be uniquely transitive on D_L since $\overline{f}\left(\{i,j\}\right) = i\left(\{i,j\}\right) = \{i,j\}$. ■

Corollary 1 *If $|L| = n$ is a positive integer of the form $n = 4k$ or $n = 4k+1$, then there does not exist a group $(D_L, \cdot)$ that left (or right) distributes over the n-star $(D_L, *)$ since $\frac{n(n-1)}{2}$ would be even.*

6 Alternate Definitions for the n-Star

In this section we develop a bilingual approach by studying the n-stars $(D_L, *)$ in terms of a new set of definitions. As always, $(F, \circ)$ is the group of all permutations on L.

Definition 1 *Suppose $(G, \circ) \subseteq (F, \circ)$ is a group of permutations on $L = \{1, 2, \cdots, n\}$ where $n \geq 3$. We say that $(G, \circ)$ is 2-transitive* on L if and only if $\forall$ doubleton subsets $\{a, b\}, \left\{\overline{a}, \overline{b}\right\} \subseteq L, \exists f \in G$ such that $f\left(\{a, b\}\right) = \{f(a), f(b)\} = \left\{\overline{a}, \overline{b}\right\}$. Also, $(G, \circ)$ is uniquely 2-transitive* on L if and only if $\forall$ doubleton subsets $\{a, b\}, \left\{\overline{a}, \overline{b}\right\} \subseteq L, \exists$ a unique $f \in G$ such that $f\left(\{a, b\}\right) = \left\{\overline{a}, \overline{b}\right\}$.*

Lemma 4 *Suppose $(G, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}$. Then $|G| = \frac{n(n-1)}{2}$.*

Proof. There are exactly $\binom{n}{2}^2$ ordered pairs $\left(\{a, b\}, \left\{\overline{a}, \overline{b}\right\}\right)$ where $\{a, b\}, \left\{\overline{a}, \overline{b}\right\}$ are doubleton subsets of L. Also, each permutation $f \in G$ generates exactly $\binom{n}{2}$ ordered pairs $(\{a, b\})$, $f\left(\{a, b\}\right)$ since $\{a, b\}$ can be chosen in $\binom{n}{2}$ different ways. Therefore, $|G| = \frac{\binom{n}{2}^2}{\binom{n}{2}} = \binom{n}{2} = \frac{n(n-1)}{2}$. ■

Lemma 5 *Suppose $(G, \circ) \subseteq (F, \circ)$ is a group of permutations on $L = \{1, 2, 3, \cdots, n\}$ and $\left(\overline{G}, \circ\right) \subseteq \left(\overline{F}, \circ\right)$ is the corresponding isomorphic group of line preserving permutations on D_L as defined previously. This means that $g \in G$ and $\overline{g} \in \overline{G}$ correspond to each other (which we write as $\overline{g} \leftrightarrow g$) if and only if $\forall$ doubleton subset $\{a, b\} \subseteq L$, $\overline{g}\left(\{a, b\}\right) = \{g(a), g(b)\}$. Then the group $\left(\overline{G}, \circ\right)$ is uniquely transitive on D_L if and only if the group $(G, \circ)$ is uniquely 2-transitive* on L.*

Proof. The proof follows immediately from the fact that $D_L = \{\{a,b\} : \{a,b\}$ is a doubleton subset of $L\}$ and from the fact that $\forall \{a,b\} \in D_L, \overline{g}(\{a,b\}) = \{g(a), g(b)\}$. ■

Note 2 Suppose $(\overline{G}, \circ)$ and $(G, \circ)$ are from lemma 5 and suppose $(G, \circ)$ is uniquely 2-transitive* on L. From lemma 5 this implies that $(\overline{G}, \circ)$ is uniquely transitive on D_L. Thus $(\overline{G}, \circ)$ is a uniquely transitive group of similarity mappings on the n-star (D_L*). As summarized in section 2 (The Introduction) this implies that there exists a group $(D_L, \cdot)$ that left-distributes over the n-star $(D_L, *)$. From section 2 we also know that $(D_L, \cdot) \cong (\overline{G}, \circ)$, and as always we know that $(\overline{G}, \circ) \cong (G, \circ)$. Therefore, $(G, \circ) \cong (\overline{G}, \circ) \cong (D_L, \cdot)$. This triple isomorphism means that many of the properties that we develop for one of these three groups will also be true for the other two groups.

Observation 1 Suppose f is a permutation on $L = \{1, 2, \cdots, n\}$. Then f can be partitioned (i.e., broken down) into the cycles k_1-cycle, k_2-cycle, $\cdots$, k_m-cycle where $\sum_{i=1}^{m} k_i = |L| = n$ and where each k_i-cycle satisfies the following. $\forall x \in k_i$-cycle, $f(x), f^2(x), f^3(x), \cdots, f^{k_i}(x)$ are all distinct and $f^{k_i}(x) = x$. If $k_1 \leq k_2 \leq \cdots \leq k_m$, we say that f is of type $(k_1, k_2, \cdots, k_m)$. Two permutations f, g on L are said to be similar if they are of the same type. Also, if f, g are permutations on L then it is a standard lemma that f and g are similar if and only if there exists a permutation h on L such that $f = h^{-1} \circ g \circ h$.

Lemma 6 *Suppose $(G, \circ) \subseteq (F, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, , n\}$, then*

1. $|G| = \frac{n(n-1)}{2}$ *and* $\frac{n(n-1)}{2}$ *is odd.*
2. *Each $f \in G$ is of type (a), (b) or (c).*

Type (a) $(k, k, k, \cdots, k)$ *where $k \neq 1, k|n$ and k is odd. Thus, $\forall x \in L, f(x), f^2(x), \cdots, f^k(x)$ are all distinct and $f^k(x) = x$.*

Type (b) $(1, , k, k, \cdots, k)$ *where $k \neq 1, k|n-1$ and k is odd. Thus, $\exists a \in L$ such that $f(a) = a$ and $\forall x \in L \setminus \{a\}, f(x), f^2(x), \ldots, f^k(x)$ are all distinct and $f^k(x) = x$.*

Type (c) $(1, 1, 1, \cdots, 1)$ *which is the identity permutation I.*

Proof. (1) follows from Lemmas 3, 4 and 5. We now prove (2). First, suppose $f \in G$ is of type $(k_1, k_2, \cdots, k_m)$ and at least one k_i is even. This implies that there exist an even positive integer m such that $f, f^2, f^3, \cdots, f^m = I$ are all distinct which implies that $(\{f^i : i = 1, 2, \cdots, m\}, \circ)$ is a subgroup of $(G, \circ)$ having m elements. But this implies $m | \frac{n(n-1)}{2}$ which is impossible since m is even and $\frac{n(n-1)}{2}$ is odd. Therefore, $k_1, k_2, \cdots, k_m$ are all odd.

Next, suppose $f \in G \backslash \{I\}$ and f has two self-loops. That is $k_1 = k_2 = 1$. This means that $\exists a \neq b, a, b \in L$ such that $f(a) = a, f(b) = b$. Therefore, $f(\{a, b\}) = \{f(a), f(b)\} = \{a, b\}$.

Also, $I(\{a, b\}) = \{a, b\}$. But since $f \neq I$, this implies that $(G, \circ)$ is not uniquely 2-transitive* on L. Therefore, if $f \in G \backslash \{I\}$ then f can have at most one self-loop.

Next, suppose $f \in G \backslash \{I\}$ and f has no self-loops and $2 \leq k_i < k_j$ for some $i < j$. This implies that $\exists x \in L$ such that $f(x), f^2(x), \cdots, f^{k_i}(x) = x$ are all distinct. Also, $f^{k_i} \neq I$ since $k_i < k_j$.

Also, of course, $f^{k_i} \in (G, \circ)$ since $(G, \circ)$ is a group.

Using the above x, we know that $x \neq f(x)$ since $k_i \geq 2$. Also, $f^{k_i}(\{x, f(x)\}) = \left\{f^{k_i}(x), f^{k_i+1}(x)\right\} = \{x, f(x)\}$. Also, $I(\{x, f(x)\}) = \{x, f(x)\}$. However, since $f^{k_i} \neq I$ this implies that $(G, \circ)$ is not uniquely 2-transitive* on L. Thus, f must be of type (a) when it has no self-loops.

Likewise, if $f \in G \backslash \{I\}$ has one self-loop then f must be of type (b). ■

In Corollaries 2, 3, $(G, \circ)$ is uniquely 2-transitive* on $L = \{1, 2, \cdots, n\}$.

Corollary 2 *$\forall g \in (G, \circ)$, define the order of g to be the smallest positive integer m such that $g^m = I$. If g is of type (a) then order (g) is odd and order $(g) | n$. Also, order $(g) \neq 1$. Furthermore, if g is of type (b) then order (g) is odd and order $(g) | n-1$. Also, order $(g) \neq 1$.*

Corollary 3 *Suppose $|L| = n \geq 4$. Then $(G, \circ)$ cannot be an Abelian group.*

Proof. The proof is the same as the proof of lemma 39. Corollary 3 is not used in this paper. ■

Definition 2 *$(G, \circ)$ is a group of permutations on L and $A \subseteq G$. We say that A is a normal subset of $(G, \circ)$ if $\forall f \in G, f^{-1} \circ A \circ f = \{f^{-1} \circ g \circ f : g \in A\} = A$.*

Notation 1 *$(G, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots .n\}$. Using Lemma 6, let us partition $G = G_a \cup G_b \cup \{I\}$ where G_a consists of those permutations in G of type (a), G_b consists of those permutations in G of type (b) and I is the identity permutation on L.*

Lemma 7 *Each of $G_a, G_b, \{I\}$ is a normal subset of $(G, \circ)$.*

Proof. Since $\forall f, g \in G, f^{-1} \circ g \circ f$ is of the same type as g and since each $g \in G$ is of type (a), (b) or $\{I\}$, it is obvious that G_a, G_b and $\{I\}$ are normal subsets of $(G, \circ)$. ■

Lemma 8 *Suppose a group $(G, \circ)$ of permutations on $L = \{1, 2, 3, \cdots, n\}$ is 2-transitive* on L. Then $(G, \circ)$ is transitive on L when $|L| = n \geq 3$. Transitive means that $\forall a, b \in L, \exists g \in G$ such that $g(a) = b$.*

Proof. Let $a, b \in L$ be arbitrary. We show that $\exists g \in G$ such that $g(a) = b$. Therefore, suppose that there does not exist $g \in G$ such that $g(a) = b$. Since $|L| \geq 3$, let $c \in L \backslash \{a, b\}$. Now, $\exists \overline{g} \in G$ such that $\overline{g}(\{a, c\}) = \{\overline{g}(a), \overline{g}(c)\} = \{b, c\}$ since $\{a, c\}$ and $\{b, c\}$ are doubleton subsets of L. Since $\overline{g}(a) \neq b$ we must have $\overline{g}(a) = c, \overline{g}(c) = b$. Now, $g = \overline{g}^2 = \overline{g} \circ \overline{g} \in (G, \circ)$ satisfies $g(a) = (\overline{g}^2)(a) = (\overline{g} \circ \overline{g})(a) = \overline{g}(\overline{g}(a)) = \overline{g}(c) = b$. Therefore, $(G, \circ)$ is transitive on L. ■

Lemma 9 *Suppose a group $(G, \circ)$ of permutations on $L = \{1, 2, \cdots, n\}$ where $n \geq 3$ is uniquely 2-transitive* on L. Then n is odd.*

Proof. Since $(G, \circ)$ is uniquely 2-transitive* on $L = \{1, 2, \cdots, n\}$, we know by Lemma 4 that $|G| = \frac{n(n-1)}{2}$.

Also, by Lemma 8 we know that $(G, \circ)$ is transitive on L since $n \geq 3$. Let us fix $a \in L$ and define $(K_a, \circ)$ to be the subgroup of $(G, \circ)$ that consisted those members $g \in G$ that map a to a. That is, $K_a = \{g \in G : g(a) = a\}$. $(K_a, \circ)$ is called the stabilizer subgroup of a.

For $b \in L$ suppose we wish to compute all $f \in (G, \circ)$ that satisfy $f(a) = b$. Since $(G, \circ)$ is transitive on L we know that $\exists$ at least one $\overline{f} \in (G, \circ)$ such that $\overline{f}(a) = b$. Then the set $\overline{f} \circ K_a = \{\overline{f} \circ g : g \in K_a\}$ gives all $f \in (G, \circ)$ that satisfy $f(a) = b$.

Now $\overline{f} \circ K_a$ is just a left coset of the subgroup $(K_a, \circ)$ of the group $(G, \circ)$. Therefore, $\forall b \in L, \exists$ exactly $|K_a|$ members $f \in (G, \circ)$ that satisfy $f(a) = b$.

Therefore, $|G| = \frac{n(n-1)}{2} = |K_a| \cdot n$ since $|L| = n$ and each $f \in G$ maps $f(a)$ somewhere in L. Therefore, $|K_a| = \frac{n-1}{2}$ which implies that n is odd. ■

Corollary 4 *Combining Lemma 6-(1) and Lemma 9 we know the following. Suppose $(G, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, 3, \cdots, n\}$ where $n \geq 3$. Then $|G| = \frac{n(n-1)}{2}$. Also, $\frac{n(n-1)}{2}$ is odd and n is odd.*

This implies that n must be of the form $n = 4k + 3$.

Corollary 5 *Suppose* $(G, \circ)$ *is a uniquely 2-transitive** *group of permutations on* $L = \{1, 2, 3, \cdots, n\}$ *where* $n \geq 3$*.* $\forall a \in L$*, define* $(K_a, \circ) = (\{g \in G : g(a) = a\}, \circ)$ *to be the stabilizer subgroup of* a*.*

Then $|K_a| = \frac{n-1}{2}$ *and* $|K_a|$ *is odd.*

Also, $\forall a, b \in L$*, there exists exactly* $\frac{n-1}{2}$ *members* $f \in (G, \circ)$ *satisfying* $f(a) = b$*.*

Proof. Given in the proof of Lemma 9. ■

Applications 1 Suppose $(G, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}$ where $n \geq 3$. From Lemma 6, we know that each $f \in (G, \circ)$ is of type (a), (b), or (c).

(a) $(k, k, k, \cdots, k)$ where $k \neq 1, k|n$ and k is odd.

(b) $(1, k, k, \cdots, k)$ where $k \neq 1, k|n-1$ and k is odd. Since $n-1$ is even, we now know that $k|\frac{n-1}{2}$, and we also know $\frac{n-1}{2}$ is odd.

(c) $(1, 1, 1, 1, \cdots, 1)$ which is the identity permutation I.

If $f \in (G, \circ)$ is of type (a) then $\forall a \in L, f(a) \neq a$. This means that f maps no $a \in L$ to itself. If $f \in (G, \circ)$ is of type (b), then $\exists$ exactly one $\overline{a} \in L$ such that $f(\overline{a}) = \overline{a}$. $\forall \overline{a} \in L$, as always define $(K_{\overline{a}}, \circ) = (\{g \in G : g(\overline{a}) = \overline{a}\}, \circ)$ to be the stabilizer subgroup of $\overline{a}$.

Since $L = \{1, 2, \cdots .n\}$ we see that $(K_1, \circ), (K_2, \circ), \cdots, (K_n, \circ)$ are the n stabilizers of $(G, \circ)$. Of course, $\forall i, j \in L$, if $i \neq j$ then $K_i \cap K_j = \{I\}$. We easily see that each $f \in (G, \circ)$ that is of type (b) is a member of exactly one of $(K_1, \circ), (K_2, \circ), \cdots, (K_n, \circ)$. Also, if $f \in (G, \circ)$ is of type (a) then $f \notin (K_1 \cup K_2 \cup \cdots \cup K_n)$. Of course, I (which is of type (c)) is a member of each $K_i, i = 1, 2, \cdots, n$. Since $|K_i \backslash \{I\}| = \frac{n-1}{2} - 1 = \frac{n-3}{2}$ for each $i = 1, 2, \cdots, n$, since $|G| = \frac{n(n-1)}{2}$ and since $(K_i \backslash \{I\}) \cap \{K_j \backslash \{I\}\} = \phi$ when $i \neq j$, we see that the number of members $f \in (G, \circ)$ that are of type (a) or type (c) equals $\frac{n(n-1)}{2} - \frac{n(n-3)}{2} = n$.

Since each $f \in (G, \circ)$ is of type (a), (b) or (c), we know the following. The order of each permutation $f \in (G, \circ)$ divides n or it divides $\frac{n-1}{2}$ and the order of I (which is 1) is the only order that divides both n and $\frac{n-1}{2}$. Therefore, exactly $n-1$ non-identity members $f \in (G, \circ)$ have an order that divides n, and these $n-1$ permutations make up $G_a = H \backslash \{I\}$ where $H = G_a \cup \{I\}$. Also, exactly $\frac{n(n-1)}{2} - n = \frac{n(n-3)}{2}$ non-identity members $f \in (G, \circ)$ have an order that divides $\frac{n-1}{2}$ and these $\frac{n(n-3)}{2}$ permutations make up $G \backslash H = (\cup_{i=1}^{n} K_i) \backslash \{I\}$.

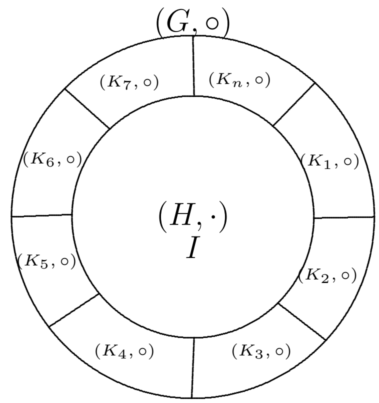


Fig. 4. $(G,\circ), (H,\circ) = (G_a \cup \{I\}, \circ)$ and the stabilizers $(K_i,\circ), i = 1, 2, \cdots, n.$

As stated above, we are defining $H = \{f \in G : f = I$ or f is of type (a)$\} = G_a \cup \{I\}$ where G_a is from Notation 1, and we again note that $|H| = n$. Also, note that $K_1 \cup K_2 \cup \cdots \cup K_n = G_b \cup \{I\}$ from Notation 1.

Of course, $\forall a \in L$ we immediately know that the stabilizer $(K_a,\circ)$ is a group. Also, since $|H| = n$ we immediately suspect that $(H,\circ)$ is a group as well. However, this fact is much harder to prove, and in section 11 we use different techniques to prove it. In section 11 we also show that $(H,\circ)$ is an Abelian p-group of order $|H| = p^t$ where p is a prime of the form $p = 4k + 3$ and t is odd. We also show that $\forall f \in H \backslash \{I\}$, order $(f) = p$. Thus, we see that $(H,\circ)$ is not a very complicated group.

Lemma 10 *Suppose $(G,\circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}$ where $n \geq 3$. Then $\forall a \in L, \forall f, g \in (K_a,\circ)$ if $f \neq g$ then f and g are totally different on $L \backslash \{a\}$. That is, $\forall x \in L \backslash \{a\}, f(x) \neq g(x)$.*

Proof. If $f \neq g$ and $f(x) = g(x)$ for some $x \in L \backslash \{a\}$, then $f(\{a, x\}) = \{f(a), f(x)\} = \{a.f(x)\} = \{g(a), g(x)\} = g(\{a, x\})$. This implies that $(G,\circ)$ is not uniquely 2-transitive * on L. ■

Lemma 11 *$(G,\circ)$ is a uniquely 2-transitive * group of permutations on $L = \{1, 2, \cdots, n\}$ where $n \geq 3$.*

Then the set $H = G_a \cup \{I\}$ is a normal subset of $(G,\circ)$.

Thus, if $(H,\circ)$ is a subgroup of $(G,\circ)$ then $(H,\circ)$ is a normal subgroup of $(G,\circ)$.

Proof. This follows from Lemma 7. ■

The triple isomorphism $(G,\circ) \cong (\overline{G},\circ) \cong (D_L,\cdot)$ of Note 2 means that many of the properties that we prove for $(G,\circ)$ will also be true for $(\overline{G},\circ)$ and $(D_L,\cdot)$. For this reason we believe that it is worthwhile to prove a few more lemmas before we continue the main business of solving the Main Problem. Lemmas 12-16 can be omitted in a short reading of this paper. Lemmas 12-14 will suggest that we must develop different techniques if we hope to prove that $(H,\circ)$ is a group. This is because Lemmas 12-14 have proved futile to us in proving that $(H,\circ)$ is a group. These new techniques are given in Section 11.

Lemma 12 *$(G,\circ)$ is a uniquely 2-transitive* group of permutations on $L=\{1,2,\cdots,n\}, n \geq 3$, and as always $H = G_a \cup \{I\}$. If $(H,\circ)$ is a subgroup of $(G,\circ)$ then it is uniquely transitive on L.*

Proof. Suppose $f \neq g, f,g \in (H,\circ)$ and $\exists a \in L$ such that $f(a) = g(a)$. Now $(f^{-1}\circ g)(a) = a$ and also $f^{-1}\circ g \in H$ and $f^{-1}\circ g \neq I$. However, $(f^{-1}\circ g)(a) = a$ and $f^{-1}\circ g \neq I$ implies that $f^{-1}\circ g \in K_a \backslash \{I\}$ which is impossible since $(K_a\backslash\{I\}) \cap (H\backslash\{I\}) = \phi$. Therefore, $\forall a \in L, f(a) \neq g(a)$. From this and from the fact that $|H| = |L| = n$, we see that $\forall a,b \in L, \exists f \in (H,\circ)$ such that $f(a) = b$. Thus, $(H,\circ)$ is transitive on L which implies that $(H,\circ)$ is uniquely transitive on L. ■

Lemma 13 *$(G,\circ)$ is a uniquely 2-transitive* group of permutations on $L=\{1,2,\cdots,n\}$, $n \geq 3$, and as always $H = G_a \cup \{I\}$. Suppose $\forall a,b \in L, \exists$ a unique $f \in H$ such that $f(a) = b$. Then $(H,\circ)$ is a subgroup of $(G,\circ)$.*

Proof. Suppose $f,g \in H$ and $f\circ g \in G\backslash H$. Therefore, $\exists a \in L$ such that $f\circ g \in K_a\backslash\{I\}$. Now $f \neq I$ and $g \neq I$. Also, $f \in H$ is true if and only if $f^{-1} \in H$ since $H = G_a \cup \{I\}$. Now $(f\circ g)(a) = f(g(a)) = a$ since $f\circ g \in K_a$. Therefore, $g(a) = f^{-1}(a)$. Now $g \neq f^{-1}$ since $f\circ f^{-1} = I \notin G\backslash H$.

However, $g \neq f^{-1}, g \in H, f^{-1} \in H$ and $g(a) = f^{-1}(a)$ contradicts the hypothesis. This contradiction implies that $f,g \in H$ and $f\circ g \in G\backslash H$ is impossible. Therefore, $(H,\circ)$ is a closed operator. Therefore, since $|H| = n$ is finite and $I \in H$ we see that $(H,\circ)$ must be a group. ■

Lemma 14 *Suppose $(G,\circ)$ is a uniquely 2-transitive* group of permutations on $L=\{1,2,\cdots,n\}$, $n \geq 3$. Also, suppose there exists a subgroup $(\overline{H},\circ)$ of $(G,\circ)$ of order $|\overline{H}| = n$. Then $(\overline{H},\circ) = (H,\circ)$ which implies that $(H,\circ)$ is a subgroup of $(G,\circ)$.*

Proof. Of course, $I \in \overline{H}$ and $I \in H$. Suppose, $f \in \overline{H} \backslash \{I\}$. Now, order $(f) \neq 1$ and order $(f) | n$. Also, $\left|\overline{H} \backslash \{I\}\right| = n - 1$. Now from Applications 1 we know that exactly $n - 1$ non-identity members $f \in (G, \circ)$ have an order that divides n, and these $n - 1$ permutations make up $H \backslash \{I\} = G_a$. Therefore, $\overline{H} \backslash \{I\} = H \backslash \{I\}$ which implies that $\overline{H} = H$. ■

Corollary 6 *Suppose* $(G, \circ)$ *is a uniquely 2-transitive** *group of permutations on* $L = \{1, 2, 3, \cdots, n = p^t\}, p^t \geq 3$, *where* p *is a prime. Since by Corollary 4,* $p^t = 4k + 3$ *is necessary we must have* $p = 4\overline{k} + 3$ *and* t *is odd. As always,* $H = G_a \cup \{I\}$. *Then* $(H, \circ)$ *is a subgroup of* $(G, \circ)$.

Proof. Since $|G| = \frac{p^t(p^t-1)}{2}$ we know by the Syloe theorems that $(G, \circ)$ has a subgroup $\left(\overline{H}, \circ\right)$ of order $\left|\overline{H}\right| = p^t$. By Lemma 14, $\left(\overline{H}, \circ\right) = (H, \circ)$ which implies that $(H, \circ)$ is a subgroup of $(G, \circ)$. ■

Lemma 15 $(G, \circ)$ *is a uniquely 2-transitive** *group of permutations on* $L = \{1, 2, \cdots, n\}, n \geq 3$. *Then* $\forall a, b \in L$, *the groups* $(K_a, \circ)$ *and* $(K_b, \circ)$ *are conjugates. This means that* $\exists f \in (G, \circ)$ *such that* $f^{-1} K_a f = K_b$. *Thus,* $\forall a, b \in L, (K_a, \circ) \cong (K_b, \circ)$.

Proof. Let $g \in K_a$ be arbitrary. Now $g \in K_a$ is true if and only if $g(a) = a$.

By Lemma 8, we know that $(G, \circ)$ is transitive on L. Therefore, $\exists f \in (G, \circ)$ such that $f(b) = a$. Now $(f^{-1} \circ g \circ f)(b) = (f^{-1} \circ g)(f(b)) = (f^{-1} \circ g)(a) = f^{-1}(g(a)) = f^{-1}(a) = b$. Thus, by using this f we see that $\forall g \in K_a, f^{-1} \circ g \circ f \in K_b$. Since $|K_b| = |K_a| = \frac{n-1}{2}$ and since the function $\{(g, f^{-1} \circ g \circ f) : g \in K_a\}$ is 1-1 we see that $f^{-1} \circ K_a \circ f = K_b$. ■

Lemma 16 $(G, \circ)$ *is a uniquely 2-transitive** *group of permutations on* $L = \{1, 2, \cdots, n\}, n \geq 3$. *Then* $\forall f \in (G, \circ), \forall a \in L, \exists b \in L$ *such that* $f^{-1} \circ K_a \circ f = K_a$.

Proof. The proof is the same as the proof of Lemma 15 since the fact that f is a permutation on L implies that $\exists b \in L$ such that $f(b) = a$. ■

Comments 1 $\forall f \in G$, the function $\{(g, f^{-1} \circ g \circ f) : g \in G\}$ will map I to I, map H to H and map the K_a's (as a varies over L) 1-1 among themselves.

Also, $\forall a \in L$, it is true that $\{f \in G : f^{-1} \circ K_a \circ f = K_a\} = K_a$. We can write more of these lemmas, but we believe that the reader has been exposed to a good sample of what is going on in all groups $(G, \circ) \cong \left(\overline{G}, \circ\right) \cong (D_L, \cdot)$. So we are now going to get down to the main business of finding all of the types of groups $(D_L, \cdot)$ that left (or right) distribute over the n-stars $(D_L, *)$ as n ranges over $n \in \{3, 4, 5, 6, \cdots\}$.

We now use Section 6 to help us solve this Main Problem.

7 Using Section 6 to Solve the Main Problem

In this section $(G, \circ)$ is a uniquely 2-transitive* group of permutations on $\{L = 1, 2, \cdots, n\}$, $n \geq 3$. As always $H = G_a \cup \{I\}$.

Also, $\forall a \in L, (K_a, \circ) = (\{f \in G : f(a) = a\}, \circ)$ is the stabilizer subgroup of a.

Since we need different techniques to prove that $(H, \circ)$ is always a subgroup of $(G, \circ)$, we will temporarily add this fact as Axiom 1 and postpone the proof of Axiom 1 to Section 11.

Axiom 1 $(H, \circ) = (G_a \cup \{I\}, \circ)$ *is a subgroup of* $(G, \circ)$.

Note 3 Of course, by Lemma 11, $(H, \circ)$ is a normal subgroup of $(G, \circ)$. Therefore, the left cosets of $(H, \circ)$ are identical to the right cosets of $(H, \circ)$.

Lemma 17 *Assuming that Axiom 1 is true, we have* $(H \circ K_a, \circ) = (\{h \circ k : h \in H, k \in K_a\}, \circ) = (G, \circ)$ *where* $a \in L$ *is arbitrary but fixed. Also, the* $\frac{n-1}{2}$ *permutations* $f \in (K_a, \circ)$ *lie in distinct cosets of* $(H, \circ)$*. Also, the* n *permutations* $f \in (H, \circ)$ *lie in distinct left cosets of* $(K_a, \circ)$ *and the* n *permutations* $f \in (H, \circ)$ *also lie in distinct right cosets of* $(K_a, \circ)$.

Proof. Follows from elementary group theory since $(H, \circ)$ is a normal subgroup of $(G, \circ)$, $|G| = \frac{n(n-1)}{2} = |H| \cdot |K_a|$ and $H \cap K_a = \{I\}$. ■

Notation 2 *Assuming that* $a \in L$ *is fixed, denote* $K_a = \left\{g_1, g_2, \cdots, g_{\frac{n-1}{2}}\right\}$ *where* $g_1 = I$*. Thus, each* g_i *is a permutation on* L *and* $g_1, g_2, \cdots, g_{\frac{n-1}{2}}$ *lie in distinct cosets of the normal subgroup* $(H, \circ)$ *of* $(G, \circ)$*. Also,* $\forall g_i \in (K_a, \circ)$ *define* $F_{g_i} : (H, \circ) \to (H, \circ)$ *to be the permutation on the normal set* H *defined by* $\forall f \in H, F_{g_i}(f) = g_i \circ f \circ g_i^{-1}$*. Since* $(H, \circ)$ *is a normal subgroup of* $(G, \circ)$ *we see that* $\forall g_i \in K_a, F_{g_i} : (H, \circ) \to (H, \circ)$ *is an automorphism on* $(H, \circ)$*. Also, Lemma 18 is easy to prove.*

Lemma 18 $\forall g_i, g_j \in (K_a, \circ), F_{g_i} \circ F_{g_j} = F_{g_i \circ g_j}$.

Proof. For all f in H, $\left(F_{g_i} \circ F_{g_j}\right)(f) = g_i \circ \left(g_j \circ f \circ g_j^{-1}\right) \circ g_i^{-1} = (g_i \circ g_j) \circ f \circ (g_i \circ g_j)^{-1} = F_{g_i \circ g_j}(f)$. ■

Note 4 Of course, $\forall g_i \in (K_a, \circ), F_{g_i}(I) = I$.

Lemma 19 *$\forall g_i, g_j \in (K_a, \circ)$ if $g_i \neq g_j$ then $F_{g_i} : (H, \circ) \to (H, \circ)$ and $F_{g_j} : (H, \circ) \to (H, \circ)$ are totally different on $H \backslash \{I\}$. That is, $\forall f \in H \backslash \{I\}, F_{g_i}(f) \neq F_{g_j}(f)$.*

Proof. Suppose $F_{g_i}(f) = F_{g_j}(f)$ for $g_i \neq g_j$ and $f \in H \backslash \{I\}$. Then $g_i \circ f \circ g_i^{-1} = g_j \circ f \circ g_j^{-1}$. Therefore, $\left(g_j^{-1} \circ g_i\right) \circ f = f \circ \left(g_j^{-1} \circ g_i\right)$.

Let $g_j^{-1} \circ g_i = g_t$. Now $g_t \in K_a \backslash \{I\}$ since $g_j^{-1} \circ g_i \in K_a$ and $g_i \neq g_j$.

Therefore, $g_t \circ f = f \circ g_t$ which implies $g_t = f \circ g_t \circ f^{-1}$. Now $f \in H \backslash \{I\}$ implies $f \notin K_a$. Therefore, $f(a) = b$ where $a \neq b$.

Now, $g_t(b) \neq b$ since $g_t \in K_a \backslash \{I\}$ and $K_b \cap (K_a \backslash \{I\}) = \phi$. See Fig. 4. Now $g_t = f \circ g_t \circ f^{-1}$ implies that $g_t(b) = (f \circ g_t \circ f^{-1})(b) = (f \circ g_t)(f^{-1}(b)) = (f \circ g_t)(a) = f(g_t(a)) = f(a) = b$, which is a contradiction to $g_t(b) \neq b$. This contradiction proves that the initial assumption in this proof must be incorrect which proves the lemma. ■

Note that Axiom 1 was not used to prove Lemma 19.

Corollary 7 *$\forall g_i, g_j \in (K_a, \circ)$, if $g_i \neq g_j$ then $F_{g_i} \neq F_{g_j}$.*

Proof. This is obvious since g_i and g_j are totally different on $H \backslash \{I\}$. ■

Lemma 20 *From Lemma 18 and Corollary 7 we see that $\left(\left\{F_{g_i} : F_{g_j} \in K_a\right\}, \circ\right) \cong (K_a, \circ)$ by the isomorphism $F_{g_i} \circ F_{g_j} = F_{g_i \circ g_j}$.*

Discussion 1 If $(G, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}, n \geq 3$, and $(H, \circ) = (G_a \cup \{I\}, \circ)$ satisfies Axiom 1, then we now know the following about $(H, \circ)$. There must exist a group of automorphisms on $(H, \circ)$ which we momentarily call $(A, \circ) = \left(\left\{a_1, a_2, \cdots, a_{\frac{n-1}{2}}\right\}, \circ\right)$ that satisfies the following conditions which we will later call the Standard Hypothesis.

First, of course $|A| = \frac{n-1}{2}$. Also, $\forall a_i, a_j \in A$, if $a_i \neq a_j$ then a_i and a_j are totally different on $H \backslash \{I\}$. That is, $\forall f \in H \backslash \{I\}, a_i(f) \neq a_j(f)$.

Also, of course, we know that $|H| = n$ where n is odd and also $|A| = \frac{n-1}{2}$ satisfies $\frac{n-1}{2}$ is odd. From the triple isomorphism $(G, \circ) \cong \left(\overline{G}, \circ\right) \cong (D_L, \cdot)$ that we discussed in Note 2, we know that all three of these groups must have a subgroup that is analogous to $(H, \circ)$ and that has properties analogous to the above.

We will soon drop to a lower level and use the notation $(L, \cdot)$ instead of $(H, \circ)$, where $L = \{1, 2, \ldots, n\}$ is our original set of lines. We show that if the above statements about $(H, \circ)$ hold true for any group $(L, \cdot)$ on $L = \{1, 2, \cdots, n\}, n \geq 3$, then we can use $(L, \cdot)$ to construct a group $(D_L, \cdot)$ on $D_L = \{\{i, j\} : i \neq j, i, j \in L\}$ such that $(D_L, \cdot)$ left (or right) distributes over the n-star $(D_L, *)$ on L. However, in order to do this we need a little more information which we give in Observation 2 and in Lemmas 21-23. Before we continue we need to emphasize one thing. In the Main Problem, we are not trying to find all of the groups $(D_L, \cdot)$ that left or right distribute over the n-stars $(D_L, *)$ on L. What we are trying to do is find all of the different types of groups (up to isomorphism) that left (or right) distribute over the n-stars $(D_L, *)$ on $L = \{1, 2, \cdots, n\}$. The point is that two isomorphic groups can act on $(D_L, *)$ in different ways.

Observation 2 Since $H \circ K_a = G$ from Lemma 17 and since $H \cap K_a = \{I\}$, it is obvious that each $f \in G$ can be uniquely written as $f = h \circ g$ where $h \in h, g \in K_a$. Suppose $f, \overline{f} \in G$ and $f = h \circ g, \overline{f} = \overline{h} \circ \overline{g}, h, \overline{h} \in H, g, \overline{g} \in K_a$.

Now $f \circ \overline{f} = (h \circ g) \circ \left(\overline{h} \circ \overline{g}\right) = \left[h \circ \left(g \circ \overline{h} \circ g^{-1}\right)\right] \circ [g \circ \overline{g}] = \left[h \circ F_g\left(\overline{h}\right)\right] \circ [g \circ \overline{g}]$. That is, $(h \circ g) \circ \left(\overline{h} \circ \overline{g}\right) = \left[h \circ F_g\left(\overline{h}\right)\right] \circ [g \circ \overline{g}]$ where $h \circ F_g\left(\overline{h}\right) \in H$ and $g \circ \overline{g} \in K_a$.

If we write each $f \in G$ as the ordered pair $f = (h, g), h \in H, g \in K_a$, then $(h, g) \circ \left(\overline{h}, \overline{g}\right) = \left(h \circ F_g\left(\overline{h}\right), g \circ \overline{g}\right)$ where $h \circ F_g\left(\overline{h}\right) \in H, g \circ \overline{g} \in K_a$.

Of course, $F_g \circ F_{\overline{g}} = F_{g \circ \overline{g}}$ from Lemma 18. Therefore, instead of using ordered pairs $(h, g), h \in H, g \in K_a$, let us use the ordered pairs $(h, F_g), h \in H, g \in K_a$ where as always $F_g(f) = g \circ f \circ g^{-1}$ is an automorphism on $(H, \circ)$.

Also, let us define the operation $(\{(h, F_g) : h \in H, g \in K_a\}, \cdot)$ by $\forall (h, F_g), \left(\overline{h}, F_{\overline{g}}\right) \in H \times \{F_g : g \in K_a\}, (h, F_g) \cdot \left(\overline{h}, F_{\overline{g}}\right) = \left(h \circ F_g\left(\overline{h}\right), F_g \circ F_{\overline{g}}\right)$, where $F_g \circ F_{\overline{g}} = F_{g \circ \overline{g}}$. Note that $F_g^{-1} = F_{g^{-1}}$.

The following Lemma 21 has an easy straight forward proof, and we also prove essentially the same thing in Lemmas 31, 32.

Lemma 22 and Lemma 23 should then be almost obvious.

Of course, $(\{F_g : g \in K_a\}, \circ)$ is a group of automorphisms on $(H, \circ)$ and if $g \neq \overline{g}$ then F_g and $F_{\overline{g}}$ are totally different on $H \backslash \{I\}$.

Lemma 21 $(\{(h, F_g) : h \in H, g \in K_a\}, \cdot)$ *is a group with identity* (I, F_I) *and* $(h, F_g)^{-1} =$

$(F_{g^{-1}}(h^{-1}), F_{g^{-1}})$.

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

Lemma 22 $(\{(h, F_g) : h \in H, g \in K_a\}, \cdot) \cong (G, \circ)$.

The proof follows from the discussion in Observation 2.

Lemma 23 *Since* $(D_L, \cdot) \cong (\overline{G}, \circ) \cong (G, \circ)$ *from Note 2, we see that the following Standard Hypothesis gives necessary conditions that must be satisfied in order for a group* $(D_L, \cdot)$ *on* D_L *to exist such that* $(D_L, \cdot)$ *left-distributes over the* n*-star* $(D_L, *)$ *on* $L = \{1, 2, \cdots .n\}, n \geq 3$*, if we also assume that* $(D_L, \cdot)$ *must satisfy the analogy of Axiom 1. From the triple isomorphism* $(G, \circ) \cong (\overline{G}, \circ) \cong (D_L, \cdot)$*, Axiom 1 means that for the group* $(D_L, \cdot)$ *there exists a subgroup* $(H, \cdot)$ *of* $(D_L, \cdot)$ *of order* $|H| = n$*, and, of course,* $(H, \cdot)$ *is a normal subgroup of* $(D_L, \cdot)$ *by Lemma 11.*

In the Standard Hypothesis we are changing the notation and calling $(H, \cdot) = (L, \cdot)$ *and we are denoting* $(A, \circ) = \left(\left\{g_1, g_2, \cdots, g_{\frac{n-1}{2}}\right\}, \circ\right)$.

Standard Hypothesis The following structure exists. Also, we have reason for changing the notation, which will soon become clear.

(a) $L = \{1, 2, \cdots, n\}, n \geq 3$.

(b) $n = 4k + 3$.

(c) $\exists$ a structure $((L, 1, \cdot), (A, \circ))$ on L having Properties 1-4.

  (1) $(L, 1, \cdot)$ is a group on L with identity 1. In section 11 we prove that $(L, 1, \cdot)$ is an Abelian p-group, but this is not needed now.

  (2) $(A, \circ)$ is a group of automorphisms on $(L, 1, \cdot)$ where $\circ$ is composition of functions.

  (3) $|A| = \frac{n-1}{2}$ and, of course, $|L| = n$.

  (4) $\forall g, \overline{g} \in A$ if $g \neq \overline{g}$ then g and $\overline{g}$ are totally different on $L \setminus \{I\}$. This means that $\forall x \in L \setminus \{I\}, g(x) \neq \overline{g}(x)$.

Remark 1. Note that if $((L,1,\cdot),(A,\circ))$ satisfies the Standard Hypothesis, we show in Section 8-10 that a group $(D_L,\cdot)$ exists such that (1) $(D_L,\cdot)$ is isomorphic to the group stated in Lemma 21 when $((L,\cdot),(A,\circ))$ and $((H,\circ),(\{F_g : g\in K_a\},\circ))$ correspond, and (2) $(D_L,\cdot)$ left-distributes over the n-star $(D_L,*)$ on $L=\{l_1,l_2,\cdots,l_n\}=\{1,2,\cdots,n\}, n\geq 3$. We will state (1) very clearly in the last paragraph of Section 10. Note that in (1) we could also write $((L,\cdot),(A,\circ))\cong((H,\circ),(\{F_g : g\in K_a\},\circ))$, which means that the structures are identical except that the entities have just been give different names.

Properties (1) and (2) mean that we are constructing (up to isomorphism) all of the different types of groups $(D_L,\cdot)$ that left-distribute over the n-star $(D_L,*)$.

In Section 8-10, $((L,1,\cdot),(A,\circ))$ always denotes a structure that satisfies the Standard Hypothesis, and we can think of $L=\{l_1,l_2,\cdots .l_n\}$ or $L=\{1,2,\cdots,n\}$.

In Section 11, we prove additional facts about $((L,1,\cdot),(A,\circ))$ such as $(L,1,\cdot)$ is Abelian, but we do not need any of this now.

8 Stating the Main Theorem

Theorem 1 Suppose $((L,1,\cdot),(A,\circ))$ satisfies the Standard Hypothesis where $L=\{1,2,\cdots,n\}$, $n\geq 3$. Then there exists a group $(D_L,\cdot)$ that left-distributes over the n-star $(D_L,*)$. Also, this group $(D_L,\cdot)$ is isomorphic to the group $(\{(h,F_g) : h\in H, g\in K_a\},\cdot)$ dealt with in Lemma 21 where we are now using the notation $((L,\cdot),(A,\circ))$ in the place of $((H,\circ),(\{F_g : g\in K_a\},\circ))$.

Of course, the group $(D_L,\odot)$ defined by $a\odot b=b\cdot a$ will right-distribute over $(D_L,*)$.

In Section 9 we develop the algebraic machinery that is needed to prove Theorem 1. Then in Section 10 we prove Theorem 1, and in the last paragraph of Section 10 we clearly show that $(D_L,\cdot)\cong(\{(h,F_g) : h\in H, g\in K_a\},\cdot)$. Then in Section 11 in addition to proving Axiom 1 we show that the isomorphic groups $(H,\circ)\cong(L,\cdot)$ must be Abelian p-groups with $\mid H\mid=|L|=p^t$ where p is a prime of the form $p=4k+3$ and t is odd. We also show that $\forall x\in L\backslash\{1\}$, the order of x is p. However, we do not need this now.

9 Algebraic Machinery that we need

Lemma 24 *If the structure $((L,1,\cdot),(A,\circ))$, satisfies the Standard Hypothesis then for all $a\in L$, $a\cdot a=a^2=1$ if and only if $a=1$.*

Proof. Suppose $a^2 = 1, a \neq 1$. Then $(\{1, a\}, 1, \cdot)$ is a two-element subgroup of $(L, 1, \cdot)$. This implies $|L|$ is even which is impossible since $|L| = 4k + 3$ ■

Lemma 25 *In the structure* $((L, 1, \cdot), (A, \circ))$, $\quad \forall g \in A, g^2 = g \circ g = I$ *if and only if* $g = I$ *where* I *is the identity permutation on* L.

Proof. Suppose $g \neq I$ and $g \circ g = I$. Then $(\{g, I\}, \circ)$ is a two element subgroup of $(A, \circ)$. This implies $2| \mid A \mid$ which is impossible since $|A| = \frac{n-1}{2} = 2k + 1$. ■

Lemma 26 *In the structure* $((L, 1, \cdot), (A, \circ))$ *it is true that* $\forall g \in (A, \circ), \forall x \in L \backslash \{1\}, g(x) \neq x^{-1}$.

Proof. Suppose $x \in L \backslash \{1\}$ and $g(x) = x^{-1}$. First, suppose $g = I$, the identity permutation on L. Then $g(x) = x^{-1}$ implies $x = x^{-1}$ which implies $x^2 = 1$. However, by Lemma 24, $x^2 = 1$ is impossible when $x \neq 1$.

Second, suppose $g \neq I$, and $g(x) = x^{-1}$ where $x \in L \backslash \{1\}$. Now $g \circ g \in (A, \circ)$.

Also, $(g \circ g)(x) = g(g(x)) = g(x^{-1}) = (g(x))^{-1} = (x^{-1})^{-1} = x$ since g is an automorphism on $(L, 1, \cdot)$.

Now $g \circ g = g^2 \neq I$ by Lemma 25 since $g \neq I$.

Therefore, $g^2 \neq I, g^2(x) = x$ and $I(x) = x$ where $x \in L \backslash \{1\}$. However, this contradicts condition c-4 of the Standard Hypothesis. ■

Definition 3 *In the structure* $((L, 1, \cdot), (A, \circ)), \forall x, y \in L$, *define the diameter of the set* $\{x, y\}$ *as* $D(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$.

Lemma 27 *The following is true in* $((L, 1, \cdot), (A, \circ))$.

(a) $\forall x, y \in L$, *if* $x = y$ *then* $D(\{x, y\}) = \{1\}$. *If* $x \neq y$ *then* $D(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$ *is a doubleton subset of* $L \backslash \{1\}$.

(b) $\forall x, y, \overline{x}, \overline{y} \in L, D(\{x, y\}) = D(\{\overline{x}, \overline{y}\})$ *or* $D(\{x, y\}) \cap D(\{\overline{x}, \overline{y}\}) = \phi$.

(c) Suppose, $x, y, \overline{x}, \overline{y} \in L$ *and* $D(\{x, y\}) = D(\{\overline{x}, \overline{y}\})$. *Then* $\exists$ *a unique* $t \in L$ *such that* $\{x, y\} \cdot t = \{x \cdot t, y \cdot t\} = \{\overline{x}, \overline{y}\}$.

Proof. (a) Suppose $x \neq y$ and $xy^{-1} = yx^{-1}$. This implies $(xy^{-1})(xy^{-1}) = (xy^{-1})^2 = 1$ which implies $xy^{-1} = 1$ by Lemma 24. This is a contradiction since $x \neq y$.

(b) Now $D(\{x, y\}) = \{xy^{-1}, yx^{-1}\}$ and $D(\{\overline{x}, \overline{y}\}) = \{\overline{xy}^{-1}, \overline{yx}^{-1}\}$. Suppose, $D(\{x, y\}) \cap D(\{\overline{x}, \overline{y}\}) \neq \phi$. Now, if $xy^{-1} = \overline{xy}^{-1}$ then $yx^{-1} = \overline{yx}^{-1}$. Also, if $xy^{-1} = \overline{yx}^{-1}$ then $yx^{-1} = \overline{xy}^{-1}$. Likewise, if $yx^{-1} = \overline{xy}^{-1}$ then $xy^{-1} = \overline{yx}^{-1}$. Also, if $yx^{-1} = \overline{yx}^{-1}$ then $xy^{-1} = \overline{xy}^{-1}$.

(c) We first prove that $\exists$ at least one $t \in L$ such that $\{x \cdot t, y \cdot t\} = \{\overline{x}, \overline{y}\}$. Since $\{xy^{-1}, yx^{-1}\} = \{\overline{xy}^{-1}, \overline{yx}^{-1}\}$ by symmetry let us suppose $xy^{-1} = \overline{xy}^{-1}$. Therefore, $\overline{x}^{-1}x = \overline{y}^{-1}y = t^{-1}$. Therefore, $\overline{x}^{-1}x = t^{-1}, \overline{y}^{-1}y = t^{-1}$ which implies $xt = \overline{x}, yt = \overline{y}$. We now show that t is unique. Therefore, suppose $\exists t, \bar{t} \in L, t \neq \bar{t}$, such that $\{xt, yt\} = \left\{x\bar{t}, y\bar{t}\right\}$. Therefore, $\left\{xt\bar{t}^{-1}, yt\bar{t}^{-1}\right\} = \{x, y\}$. Since $t\bar{t}^{-1} \neq 1$ we must have, $xt\bar{t}^{-1} = y$ and $yt\bar{t}^{-1} = x$. Therefore, $y^{-1}x = \bar{t}t^{-1} = t\bar{t}^{-1}$. Therefore, $\left(\bar{t}t^{-1}\right)\left(\bar{t}t^{-1}\right) = \left(\bar{t}t^{-1}\right)^2 = 1$ which by Lemma 24 implies $\bar{t}t^{-1} = 1$. This is a contradiction since $t \neq \bar{t}$. ■

Lemma 28 *The following is true in $((L, 1, \cdot), (A, \circ))$. Suppose $i \neq j$ and $i, j \in L$ are arbitrary but fixed. Then $D(\{g(i), g(j)\})$, as g ranges over $g \in A$, are pairwise disjoint doubleton subsets of $L \backslash \{1\}$. Since $\frac{|L|-1}{2} = \frac{n-1}{2} = |A|$ this implies that these doubleton sets $D(\{g(i), g(j)\}), g \in A$, will partition $L \backslash \{1\}$.*

Proof. First, we show that each $D(\{g(i), g(j)\}), g \in A$, is a doubleton subset of $L \backslash \{1\}$. We know that $\forall g \in A, g(i) \neq g(j)$ since g is a permutation on L since $g : (L, 1, \cdot) \to (L, 1, \cdot)$ is an automorphism on $(L, 1, \cdot)$. Therefore, by Lemma 27 (a) we know that $D(\{g(i), g(j)\})$ is a doubleton subset of $L \backslash \{1\}$.

Next, suppose $g \neq \overline{g}, g, \overline{g} \in A$. We show that $D(\{g(i), g(j)\}) \cap D(\{\overline{g}(i), \overline{g}(j)\}) = \phi$. Now,

$$\begin{aligned} D(\{g(i), g(j)\}) &= \left\{g(i) \cdot (g(j))^{-1}, g(j) \cdot (g(i))^{-1}\right\} \\ &= \left\{g(i) \cdot g\left(j^{-1}\right), g(j) \cdot g\left(i^{-1}\right)\right\} \\ &= \left\{g\left(i \cdot j^{-1}\right), g\left(j \cdot i^{-1}\right)\right\} \end{aligned}$$

since g is an automorphism on $(L, 1, \cdot)$.

Likewise, $D(\{\overline{g}(i), \overline{g}(j)\}) = \{\overline{g}(i \cdot j^{-1}), \overline{g}(j \cdot i^{-1})\}$. By Lemma 27(b) we show that $D(\{g(i), g(j)\}) \cap D(\{\overline{g}(i), \overline{g}(j)\}) = \phi$ by showing the following. First, we show that

$g\left(i\cdot j^{-1}\right)\neq\overline{g}\left(i\cdot j^{-1}\right)$. Since $i\cdot j^{-1}\neq 1$ and $g\neq\overline{g}$ we know from property c-4 of the Standard Hypothesis that $g\left(i\cdot j^{-1}\right)\neq\overline{g}\left(i\cdot j^{-1}\right)$. Second, we show that $g\left(i\cdot j^{-1}\right)\neq\overline{g}\left(j\cdot i^{-1}\right)$. Therefore, suppose $g\left(i\cdot j^{-1}\right)=\overline{g}\left(j\cdot i^{-1}\right)$.

Now $j\cdot i^{-1}=\left(i\cdot j^{-1}\right)^{-1}$. Therefore, if we call $i\cdot j^{-1}=x$ we have $x\neq 1$ and $g\left(x\right)=\overline{g}\left(x^{-1}\right)$. Therefore, $\left(\overline{g}^{-1}\circ g\right)\left(x\right)=x^{-1}$. However, since $\overline{g}^{-1}\circ g\in A$ and $x\neq 1$ this contradicts Lemma 26. ■

Definition 4 *Using* $\left(\left(L,1,\cdot\right),\left(A,\circ\right)\right)$, *for each fixed* $x\in L$ *and each fixed* $g\in A$ *we define the permutation* $f_{(x,g)}$ *on* L *by* $\forall t\in L, f_{(x,g)}\left(t\right)=g\left(t\right)\cdot x$.

These permutations $f_{(x,g)}, x\in L, g\in A$, *form a uniquely 2-transitive* group of permutations on* L. *However, we will instead deal with* $f_{(x,g)}$ *by using the definitions given in Sections 3-5.*

Also, it is important to note that we could just as well have defined $f_{(x,g)}=x\cdot g\left(t\right)$ *and this definitions is more analogous to the definitions in Section 7. However, since we prove in Section 11 that* $\left(L,1,\cdot\right)$ *is an Abelian group anyway, then* $x\cdot g\left(t\right)=g\left(t\right)\cdot x$ *and we can see no compelling reason to change it.*

For $f_{(x,g)}=g\left(t\right)\cdot x$, *we note that* $x\in L, g\in A$ *gives a total of* $\left|L\right|\cdot\left|A\right|=\frac{n(n-1)}{2}$ *permutations on* L. *Definition 4 forms the common hypothesis for Lemmas 29-34.*

Lemma 29 $\forall x\in L,\forall g\in A, f_{(x,g)}\left(t\right)=g\left(t\right)\cdot x$ *is a permutation on* L.

Proof. Obvious. ■

Lemma 30 *All of the* $\frac{n(n-1)}{2}$ *permutations* $f_{(x,g)}\left(t\right)=g\left(t\right)\cdot x$, *where* $x\in L, g\in A$ *are distinct.*

Proof. Suppose $\left(x,g\right)\neq\left(\overline{x},\overline{g}\right)$. First, suppose $x\neq\overline{x}$. Now $f_{(x,g)}\left(1\right)=g\left(1\right)\cdot x=1\cdot x=x$. Also, $f_{(\overline{x},\overline{g})}\left(1\right)=\overline{g}\left(1\right)\cdot\overline{x}=\overline{x}$. Therefore, $f_{(x,g)}\left(1\right)\neq f_{(\overline{x},\overline{g})}\left(1\right)$ which implies $f_{(x,g)}\neq f_{(\overline{x},\overline{g})}$.

Second, suppose $x=\overline{x}, g\neq\overline{g}$. Also suppose $\forall t\in L, f_{(x,g)}\left(t\right)=f_{(\overline{x},\overline{g})}\left(t\right)$. Then $\forall t\in L, g\left(t\right)\cdot x=\overline{g}\left(t\right)\cdot\overline{x}$ which implies $\forall t\in L, g\left(t\right)=\overline{g}\left(t\right)$. Since $g\neq\overline{g}$ this contradicts condition $c-4$ of the Standard Hypothesis. ■

Lemma 31 $f_{(x,g)}\circ f_{(\overline{x},\overline{g})}=f_{(g(\overline{x})\cdot x,g\circ\overline{g})}$ *where* $\circ$ *is the composition of functions.*

Note 5 Compare this to the equation $\left(h,F_g\right)\cdot\left(\overline{h},F_{\overline{g}}\right)=\left(h\circ F_g\left(\overline{h}\right),F_g\circ F_{\overline{g}}\right)$ given in Observation 2. Also, we note that the operation $g\circ\overline{g}$ is carried out in $\left(A,\circ\right)$ and $g\left(\overline{x}\right)\cdot x$ is carried out in $\left(L,1,\cdot\right)$.

Lemma 31 implies that $\circ$ is a closed operator on $\left\{f_{(x,g)} : x \in L, g \in A\right\}$.

Proof.

$$\begin{aligned}\left(f_{(x,g)} \circ f_{(\overline{x},\overline{g})}\right)(t) &= f_{(x,g)}\left(f_{(\overline{x},\overline{g})}(t)\right) \\ &= f_{(x,g)}(\overline{g}(t) \cdot \overline{x}) \\ &= g\left[\overline{g}(t) \cdot \overline{x}\right] \cdot x \\ &= (g \circ \overline{g})(t) \cdot (g(\overline{x}) \cdot x) \\ &= f_{(g(\overline{x}) \cdot x, g \circ \overline{g})}(t) . \blacksquare\end{aligned}$$

Lemma 32 $\left(\left\{f_{(x.g)} : x \in L, g \in A\right\}, \circ\right)$: *is a group where $\circ$ is the composition of functions. See Lemma 21 which has the same proof.*

Proof. (1) From Lemma 31, $\circ$ is a closed operator on $\left\{f_{(x.g)} : x \in L, g \in A\right\}$.

(2) We prove $f_{(1,I)}$ is the identity permutation on L where 1 is the identify of $(L, 1, \cdot)$ and $I \in A$ is the identity permutation on L.

Now $f_{(1,I)}(t) = I(t) \cdot 1 = t \cdot 1 = t$.

Therefore, $f_{(1,I)}$ is the identity permutation on L.

(3) Of course, the composition of functions is always associative.

(4) We show that $f_{(x,g)}$ and $f_{(g^{-1}(x^{-1}),g^{-1})}$ are inverse permutations on L where g^{-1} is the inverse permutation of g. See Lemma 21 noting that $F_{g^{-1}} = (F_g)^{-1}$.

Now, $f_{(x,g)} \circ f_{(g^{-1}(x^{-1}),g^{-1})} = f_{(g[g^{-1}(x^{-1})] \cdot x, g \circ g^{-1})} = f_{(x^{-1} \cdot x, I)} = f_{(1,I)}$. $\blacksquare$

Using the permutations $f_{(x,g)}(t) = g(t) \cdot x$ on $L = \{l_1, l_2, l_3, \cdots, l_n\} = \{1, 2, \cdots, n\}$, as in section 3-5, let $\overline{f}_{(x,g)} = \overline{f}_{(x,g)}(\{i,j\}) = \left\{f_{(x,g)}(i), f_{(x,g)}(j)\right\} = \{g(i) \cdot x, g(j) \cdot x\}$ be the corresponding line preserving permutations on
$D_L = \{\{l_i, l_j\} : l_i \neq l_j, l_i, l_j \in L\} = \{\{i,j\} : i \neq j, i, j \in L\}$. From Lemma 32 and from the isomorphism $\overline{f \circ h} = \overline{f} \circ \overline{h}$ of Lemmas 1,2 where $f \neq h$ implies $\overline{f} \neq \overline{h}$, we know that these line preserving permutations $\overline{f}_{(x,g)}(\{i,j\})$ on D_L where $x \in L, g \in A$ form a group under composition of functions.

Lemma 33 *The groups* $\left(\left\{f_{(x,g)} : x \in L, g \in A\right\} . \circ\right)$ *and* $\left(\left\{\overline{f}_{(x,g)} : x \in L, g \in A\right\}, \circ\right)$ *are isomorphic.*

Proof. Follows from Lemmas 1,2 since $\overline{f \circ h} = \overline{f} \circ \overline{h}$ and $f \neq h$ implies $\overline{f} \neq \overline{h}$. $\blacksquare$

Lemma 34 *The group* $\left(\left\{\overline{f}_{(x,g)} : x \in L, g \in A\right\}, \circ\right)$ *of line preserving permutations on* D_L *is uniquely transitive on* D_L. *Therefore, from Lemma 5, the group* $\left(\left\{f_{(x,g)} : x \in L, g \in A\right\}, \circ\right)$ *of permutations on* L *is uniquely 2-transitive** *on* L.

Proof. We must show that $\forall \{i,j\}, \left\{\bar{i},\bar{j}\right\} \in D_L, \exists$ a unique (x,g) with $x \in L, g \in A$ such that $\overline{f}_{(x,g)}(\{i,j\}) = \left\{\bar{i},\bar{j}\right\}$. That is, $\{g(i)\cdot x, g(j)\cdot x\} = \left\{\bar{i},\bar{j}\right\}$. Now $D\left(\left\{\bar{i},\bar{j}\right\}\right)$ is a doubleton subset of $L\setminus\{1\}$ by Lemma 27-a since $\bar{i} \neq \bar{j}$. Also, $D(\{g(i)\cdot x, g(j)\cdot x\}) = D(\{g(i), g(j)\})$. Therefore, a necessary condition on g is that $D(\{g(i), g(j)\}) = D\left(\left\{\bar{i},\bar{j}\right\}\right)$. Since $i \neq j$, from Lemma 28, the sets $D(\{g(i), g(j)\})$, $g \in A$, are pairwise disjoint doubleton sets that partition $L\setminus\{1\}$. Also, from Lemma 27-b we know that $\forall g \in A, D(\{g(i), g(j)\}) \cap D\left(\left\{\bar{i},\bar{j}\right\}\right) = \phi$ or $D(\{g(i), g(j)\}) = D\left(\left\{\bar{i},\bar{j}\right\}\right)$. Therefore, it follows that $\exists$ a unique $g \in A$ such that $D(\{g(i), g(j)\}) = D\left(\left\{\bar{i},\bar{j}\right\}\right)$. Using this unique $g \in A$, from Lemma 27-c $\exists$ a unique $x \in L$ such that $\{g(i), g(j)\}\cdot x = \{g(i)\cdot x, g(j)\cdot x\} = \left\{\bar{i},\bar{j}\right\}$. ■

10 Constructing the group $(D_L, \cdot)$ of Theorem 1.

Proof of Theorem 1 Calling our collection of n lines $L = \{l_1, l_2, \cdots, l_n\} = \{1, 2, \cdots, n\}$, we use the machinery developed in Section 9 to construct a group $(D_L, \cdot)$ that left-distributes over the n-star $(D_L, *)$ when $((L, 1, \cdot), (A, \circ))$ satisfies the Standard Hypothesis. We know that $\forall x \in L, \forall g \in A$, the permutation $\overline{f}_{(x,g)}(\{i,j\}) = \{g(i)\cdot x, g(j)\cdot x\}$ on D_L is a similarity mapping on the n-star $(D_L, *)$ since it is a line preserving permutation on $(D_L.*)$. Also, from Lemma 34, this collection of similarity mappings on $(D_L, *)$ is a uniquely transitive group of permutations on D_L under composition of functions.

We are now in a position to use Theorem 3, [5] to construct a group $(D_L, \cdot)$ that left-distributes over the n-star $(D_L, *)$. We have summarized this construction in the second paragraph of the introduction.

First, we must arbitrarily choose and then fix an element of D_L to be the identity of $(D_L, \cdot)$. Let $\{1, \theta\}$ be the identity where $1 \in L$ is the identity of $(L, 1, \cdot)$ and $\theta \in L\setminus\{1\}$ is arbitrarily chosen and then fixed. In the notation of Theorem 3, [5] that we are using in the Introduction, we have $S = D_L$ and $\left(\overline{G}, \circ\right) = \left(\left\{\overline{f}_{(x,g)} : x \in L, g \in A\right\}, \circ\right)$. Since $\left(\overline{G}, \circ\right)$ is uniquely transitive on $S = D_L$, we know that $\forall \{i,j\} \in D_L$, $\exists$ a unique (x,g) with $x \in L$ and $g \in A$ such that $\overline{f}_{(x,g)}(\{1,\theta\}) = \{g(1)\cdot x, g(\theta)\cdot x\} \equiv \{x, g(\theta)\cdot x\} = \{i,j\}$. Therefore, let us write each $\{i,j\} \in D_L$ as $\{i,j\} = \{x, g(\theta)\cdot x\} = (x,g)$ where $x \in L, g \in A$. This gives a 1-1 correspondence $\{i,j\} \leftrightarrow (x,g)$ where $\{i,j\} \in D_L$ and $x \in L, g \in A$. If we write each $\{i,j\} \in D_L$ in this unique way, then $\overline{G}$ is automatically indexed as required in Theorem 3, b, [5] and which we have stated in paragraph 2 of the Introduction. This is because

Arthur, the next line does not make sense. Is there an extra = sign? What follows does not make logical sense to me either.

$$\begin{aligned} \forall \{i,j\} &= \{x, g(\theta) \cdot x\} = (x,g) \in S = D_L, \overline{f}_{(x,g)}(\{1,\theta\}) \\ &= \{g(1) \cdot x, g(\theta) \cdot x\} = \{x, g(\theta) \cdot x\} = (x,g). \end{aligned}$$

The group $(D_L, \cdot)$ with identity $\{1,\theta\} = \{1, I(\theta) \cdot 1\} = (1, I)$ that left-distributes over the n-star $(D_L, *)$ is now defined in Theorem 3, [5] and also stated in paragraph 2 of the Introduction as follows.

$$\begin{aligned} \forall \{x, g(\theta) \cdot x\} &= (x,g), \{\overline{x}, \overline{g}(\theta) \cdot \overline{x}\} \\ &= (\overline{x}, \overline{g}) \in S = D_L, \{x, g(\theta) \cdot x\} \cdot \{\overline{x}, \overline{g}(\theta) \cdot \overline{x}\} \\ &= (x,g) \cdot (\overline{x}, \overline{g}) = \overline{f}_{(x,g)}(\{\overline{x}, \overline{g}(\theta) \cdot \overline{x}\}) \\ &= \{g(\overline{x}) \cdot x, [g(\overline{g}(\theta) \cdot \overline{x})] \cdot x\} \\ &= \{(g(\overline{x}) \cdot x), (g \circ \overline{g})(\theta) \cdot (g(\overline{x}) \cdot x)\} \\ &= (g(\overline{x}) \cdot x, g \circ \overline{g}) \text{ where} \\ g \circ \overline{g} &\in A \text{ and } g(\overline{x}) \cdot x \in L. \end{aligned}$$

Note that we are also calling this $(x,g) \cdot (\overline{x}, \overline{g}) = (g(\overline{x}) \cdot x, g \circ \overline{g})$.

Compare this to Lemma 31. In section 11 we prove that $(H, \circ) \cong (L . \cdot)$ is an Abelian group. Therefore the claim that we made in Remark 1 and in Theorem 1 that $(D_L, \cdot) \cong (\{(h, F_g) : h \in H, g \in K_a\}, \cdot)$ when $((L, \cdot), (A, \circ))$ and $((H, \circ), (\{F_g : g \in K_a\}, \circ))$ correspond, where $(\{(h, F_g) : h \in H, g \in K_a\}, \cdot)$ is the group we dealt with in Lemma 21, should now be clear.

11 Proving Axiom 1 and Other Properties of $(H, \circ)$

We will now use different techniques to prove Axiom 1 and also to derive other properties of $(H, \circ)$.

We begin by summarizing the ideas from Section 6 that we will use. In Section 6, $(G, \circ)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}, n \geq 3$.

From Lemma 4, $|G| = \frac{n(n-1)}{2}$ and from Corollary 4, n is odd and $\frac{n-1}{2}$ is odd. In Corollary 5, we defined $\forall a \in L, (K_a, \circ) = (\{g \in G : g(a) = a\}, \circ)$ to be the stabilizer subgroup of a. Also, see Fig. 4. From Corollary 5, we know that $\forall a \in L, |K_a| = \frac{n-1}{2}$.

We defined $H = G_a \cup \{I\}$ in Applications 1 and we showed in Lemma 11 that H is a normal subset of $(G, \circ)$. This means that $\forall g \in G, g^{-1} \circ h \circ g = H$. We also showed in Applications 1 that $|H| = n$ and $\forall f \in H \setminus \{I\}$, order $(f) \geq 2$ and order $(f) \,|n$.

Also, $\forall f \in G \setminus H$, order $(f) \geq 2$ and order $(f) \,|\frac{n-1}{2}$. Of course, order $(I) = 1$.

In section 7 we gave Axiom 1 which stated that $(H, \circ) = (G_a \cup \{I\}, \circ)$ is a subgroup of $(G, \circ)$ and, therefore, $(H, \circ)$ is a normal subgroup of $(G, \circ)$.

We now prove Axiom 1, and for convenience we use the notation $(G, I, \circ) = (G, 1, \cdot)$ interchangeably. Definitions 5, 6 and Lemmas 35-38 are standard.

Lemma 35 *Suppose $(G, 1, \cdot)$ is any finite group and suppose $x, y \in G$ satisfy (1) and (2). (1). $xy = yx$. (2) order (x) and order (y) are relatively prime. Then order $(x \cdot y) =$ order $(x) \cdot$ order (y).*

Definition 5 *Suppose $(G, 1, \cdot)$ is any finite group. $\forall a, b \in G$, we say that a and b are conjugates (which we denote by $a \sim b$) if and only if $\exists x \in G$ such that $b = x^{-1}ax$.*

Observe that if $a \sim b$ then order $(a) =$ order (b).

Lemma 36 *$(G, \sim)$ is an equivalence relation on G and partitions G into $G = \{1\} \cup S_1 \cup S_2 \cup \cdots \cup S_k$ where $\forall i \in \{1, 2, \cdots, k\}, \forall a \in S_i, \forall x \in G, a \sim x$ is true if and only if $x \in S_i$. Also, $1 \sim x$ is true if and only if $x = 1$.*

Definition 6 *Suppose $(G, 1, \cdot)$ is any finite group. $\forall a \in G$, define $C_a = \{x \in G : ax = xa\}$. Thus, C_a consists of those elements x of G that commute with a.*

Lemma 37 *$\forall a \in G, (C_a, \cdot)$ is a subgroup of $(G, 1, \cdot)$.*

Lemma 38 *$\forall a \in G$ define $S_a = \{x \in G : a \sim x\}$. Then $|S_a| = \frac{|G|}{|C_a|}$.*

Proof. For all $x, y \in G, x^{-1}ax = y^{-1}ay$ is true if and only if $yx^{-1} \in C_a$ which is true if and only if x, y lie in the same right coset of C_a. The lemma follows from this. ■

Corollary 8 *$\forall a, b \in G$, if $a \sim b$ then obviously $S_a = S_b$ is true and this implies that $|S_a| = |S_b| = \frac{|G|}{|C_a|} = \frac{|G|}{|C_b|}$. Therefore, $|C_a| = |C_b|$ is true.*

Lemma 39 *$(G, I, \circ) = (G, 1, \cdot)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}$. As always $H = G_a \cup \{I\} = G_a \cup \{1\}$. Then $\forall x \in H \backslash \{1\}, \forall y \in G \backslash H, xy \neq yx$.*

Proof. Suppose $xy = yx$. From section 6, order $(x) \geq 2$ and order $(x) | n$. Also, order $(y) \geq 2$ and order $(y) | \frac{n-1}{2}$. Since n and $\frac{n-1}{2}$ are relatively prime we know that order (x) and order (y) are relatively prime. Therefore, from Lemma 35, order $(x \cdot y) =$ order $(x) \cdot$ order (y). From section 6, we know that order $(xy) | n$ or order $(xy) | \frac{n-1}{2}$. But this is impossible since order (x) does not divide $\frac{n-1}{2}$ and order (y) does not divide n. Therefore, $xy = yx$ is impossible. ■

Lemma 40 *$(G, I, \circ) = (G, 1, \cdot)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}$.*

As always, $H = G_a \cup \{I\} = G_a \cup \{1\}$. Suppose $\forall x, y \in H, xy = yx$. Then $(H, \circ) = (H, \cdot)$ is a subgroup of $(G, \circ) = (G, \cdot)$.

Proof. Of course, $I = 1 \in H$. Also, $\forall x \in H$, order $(x) =$ order (x^{-1}) which implies that $x^{-1} \in H$. We now show that $(H, \cdot) = (H, \circ)$ is a closed operator on H.

Therefore, suppose $x, y \in H$ and $xy \in G \backslash H$. Of course, this implies that $x \in H \backslash \{1\}$ and $y \in H \backslash \{1\}$. Now if $xy \in G \backslash H$ and $x \in H \backslash \{1\}$, then from Lemma 39 we know that $(xy) \cdot x \neq x \cdot (xy)$. But this is a contradiction since $xy = yx$ implies that $(xy) \cdot x = x \cdot (xy)$.

Therefore, $x, y \in H$ and $x \cdot y \in G \backslash H$ is impossible. Therefore, $(H, \circ) = (H, \cdot)$ is a closed operation on H and we know that $(H, \circ) = (H, \cdot)$ must be a subgroup of $(G, \circ) = (G, \cdot)$. ■

Lemma 41 *$(G, I, \circ) = (G, 1, \cdot)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}$. Also, $H = G_a \cup \{I\} = G_a \cup \{1\}$. $\forall a \in H \backslash \{I\} = H \backslash \{1\}$ let $S_a = \{x \in G : a \sim x\}$ where $(G, \sim)$ is defined in Definitions 5. Now, $\forall a \in H \backslash \{1\}, S_a \subseteq H \backslash \{1\}$ is true since $\forall x \in S_a$, order $(x) =$ order (a). $S_a \subseteq H \backslash \{1\}$ is also true since $H \backslash \{1\} = G_a$ is a normal subset of $(G, \circ) = (G, \cdot)$. Also, from Lemma 38, $|S_a| = \frac{|G|}{|C_a|}$ is true. We now prove that $|C_a|$ and $\frac{n-1}{2}$ are relatively, prime.*

Proof. Suppose $|C_a|$ and $\frac{n-1}{2}$ are not relatively price. Therefore, $\exists$ a prime p such that $p | \, |C_a|$ and $p | \frac{n-1}{2}$.

Of course, p is odd since $\frac{n-1}{2}$ is odd. Since $(C_a, \circ) = (C_a, \cdot)$ is a group and $p|\,|C_a|$ we know by the Syloe theorems that $\exists x \in C_a$ such that order $(x) = p$. However, since $p \mid \frac{n-1}{2}$ and since order $(x) \geq 2$, we know from section 6 that $x \in G\backslash H$.

Now by the definition $C_a = \{x \in G : ax = xa\}$ we know that $x \in C_a$ implies that $ax = xa$. But since $a \in H\backslash\{1\}$ and $x \in G\backslash H$ we know from Lemma 39 that $ax \neq xa$. This contradiction proves that our initial assumption is false which proves that $|C_a|$ and $\frac{n-1}{2}$ must be relatively prime. ■

Lemma 42 $(G, I, \circ) = (G, 1, \cdot)$ *is a uniquely 2-transitive* group of permutations on* $L = \{1, 2, \cdots, n\}, n \geq 3$. *As always,* $H = G_a \cup \{I\}$. *Then* $\forall a \in H\backslash\{I\} = H\backslash\{1\}, C_a \cap (G\backslash H) = \phi$ *which implies that* $C_a \subseteq H$.

Proof. Suppose $x \in G\backslash H$. Since $a \in H\backslash\{I\}$ and $x \in G\backslash H$, from Lemma 39 $ax \neq xa$. Therefore, $x \notin C_a$. ■

Corollary 9 $(G, I, \circ) = (G, 1, \cdot)$ *is a uniquely 2-transitive* group of permutations on* $L = \{1, 2, \cdots, n\}, n \geq 3$. *Also,* $H = G_a \cup \{I\}$. *Then* $\forall x, y \in H, xy = yx$.

Proof. Suppose $a \in H\backslash\{1\}$. From Lemma 38, $|S_a| = \frac{|G|}{|C_a|} = \frac{\frac{n(n-1)}{2}}{|C_a|}$. Since from Lemma 41 $|C_a|$ and $\frac{n-1}{2}$ are relatively prime, we know that $|C_a|$ divides n and $|S_a| = \left[\frac{n}{|C_a|}\right] \cdot \left[\frac{n-1}{2}\right]$.

Now $S_a \subseteq H\backslash\{1\}$ and $|H\backslash\{1\}| = n - 1$. Therefore, $|S_a| \leq n - 1$. From section 6, $|H| = n$ is odd. Therefore, if $|C_a| \neq n$ then $\frac{n}{|C_a|} \geq 3$ and this implies $|S_a| \geq \frac{3}{2}(n-1)$. However, $n - 1 \geq |S_a| \geq \frac{3}{2}(n-1)$ is impossible. Therefore, $|C_a| = n = |H|$. Therefore, since from Lemma 42, $C_a \subseteq H$ when $a \in H\backslash\{1\}$, we know that $\forall a \in H\backslash\{1\}, C_a = H$. Since $1 = I$ commutes with all $x \in H$ and since a$\in H\backslash\{1\}$ is arbitrary, we see that $\forall x, y \in H, xy = yx$.

■

Lemma 43 (Axiom 1) $(G, I, \circ) = (G, 1, \cdot)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}, n \geq 3$. As always, $H = G_a \cup \{I\}$. From Corollary 9 and Lemma 40, we know that $(H, I, \circ) = (H, 1, \cdot)$ is an Abelian subgroup of $(G, \circ) = (G, \cdot)$.

We now prove that $(H, I, \circ) = (H, 1, \cdot)$ is not only an Abelian group but it is also an Abelian p-group of order $|H| = p^t$ where p is a prime of the form $p = 4k + 3$ and t is odd. Also, we prove that $\forall x \in H\backslash\{I\}$, order $(x) = p$.

In order to do this, we use the following definitions from Notation 2 of section 7. As always, $(G, I, \circ) = (G, 1, \cdot)$ is a uniquely 2-transitive* group of permutations on $L = \{1, 2, \cdots, n\}, n \geq 3$.

For all $g_i \in (K_a, \circ), F_{g_i} : (H, \circ) \to (H, \circ)$ was an automorphism on the normal group $(H, \circ)$ defined by $\forall f \in H, F_{g_i}(f) = g_i \circ f \circ g_i^{-1}$.

Lemma 19 stated that $\forall g_i, g_j \in (K_a, \circ)$, if $g_i \neq g_j$ then $F_{g_i} : (H, \circ) \to (H, \circ)$ and $F_{g_j} : (H, \circ) \to (H, \circ)$ are totally different on $H \backslash \{I\}$. Also, $\forall f \in H, \forall g_i \in (K_a, \circ)$, it is obvious that order $(f) =$ order $(F_{g_i}(f))$ since F_{g_i} is an automorphism on $(H, \circ)$.

Also, of course $\forall g_i \in (K_a, \circ), F_{g_i}(I) = I$. Suppose that $f \in H \backslash \{I\}$. Since (1) - (4) are true, then Lemma 44 is obvious.

(1) $F_{g_i}(f) \neq F_{g_j}(f)$ when $g_i \neq g_j$ and $g_i, g_j \in (K_a, \circ)$.

(2) $F_{g_i}(f) \in H \backslash \{I\}, F_{g_j}(f) \in H \backslash \{I\}$.

(3) Order $(f) =$ order $(F_{g_i}(f)) =$ order $\left(F_{g_j}(f)\right)$.

(4) $|K_a| = \frac{n-1}{2}$ and $|H \backslash \{I\}| = n - 1$.

Lemma 44 $(G, I, \circ) = (G, I, \cdot)$ *is a uniquely 2-transitive* group of permutations on* $L = \{1, 2, \cdots, n\}, n \geq 3$. *Also,* $H = G_a \cup \{I\}$. *Suppose* $f \in H \backslash \{I\}$ *and define*

$$\overline{O}_f = \{g \in H \backslash \{I\} : \textit{ order } (g) = \textit{ order } (f)\}.$$

Then $\left|\overline{O}_f\right| \geq \frac{n-1}{2}$.

Applications 2 Lemma 44 implies that the elements $f \in H \backslash \{I\}$ can have at most 2 different orders. Now $(H, I, \circ) = (H, 1, \cdot)$ is a normal Abelian subgroup of $(G, \circ) = (G, \cdot)$. Also, $|H| = n$ and n is odd.

Suppose p, q are distinct odd primes and $p|n, q|n$. Since $p|\,|H|, q|\,|H|$ we know that $\exists f, g \in H \backslash \{I\}$ such that order $(f) = p$ and order $(g) = q$. Therefore, by Lemma 35, order $(f \circ g) = p \cdot q$. Also, $f \circ g \in H \backslash \{I\}$ since $(H, \circ)$ is a group. Therefore, since $p, q, p \cdot q$ are distinct, we have a contradiction to the above statement that the elements of $H \backslash \{I\}$ can have at most two different orders. This contradiction implies that $(H, I, \circ) = (H, 1, \cdot)$ must be a p-group. Since from Corollary 4 we know that $n = 4k + 3$ we see that $|H| = p^t$ where p is a prime of the form $p = 4k + 3$ and t is odd. We now show that if $|H| = p^t$ then $\forall f \in H \backslash \{I\}$, order $(f) = p$.

Lemma 45 $(G, I, \circ) = (G, I, \cdot)$ *is a uniquely 2-transitive* group of permutations on* $L = \{1, 2, \cdots, n\}, n \geq 3$. *Of course,* $|H| = n = p^t$ *where* p *is a prime of the form* $p = 4k+3$ *and* t *is odd. We prove that* $\forall x \in H \backslash \{I\}$, *order* $(x) = p$.

Proof. Suppose $\exists t \in H\backslash\{I\}$ such that order $(t) \neq p$. Of course, since $(H, \circ)$ is a p-group, we know that $\exists x \in H\backslash\{I\}$ such that order $(x) = p$ and $\exists y \in H\backslash\{I\}$ such that order $(y) = p^2$. Of course from Applications 2 we know that $\forall t \in H\backslash\{I\}$, order $(t) = p$ or order $(t) = p^2$.

From Applications 2 and Lemma 44, we can partition H into $H = \{I\} \cup \overline{O}_p \cup \overline{O}_{p^2}$ such that

(1) $\left|\overline{O}_p\right| = \left|\overline{O}_{p^2}\right| = \frac{n-1}{2} = \frac{p^t-1}{2}$,

(2) $\forall x \in \overline{O}_p$, order $(x) = p$ and

(3) $\forall x \in \overline{O}_{p^2}$, order $(x) = p^2$.

Suppose $x \in \overline{O}_{p^2}$ and as always let $(g(x), \circ)$ be the subgroup of $(H, \circ)$ that is generated by x. Now (1) $|g(x)| = p^2$, (2) exactly $p(p-1)$ elements of $(g(x), \circ)$ have an order of p^2, (3) exactly $p-1$ elements of $(g(x), \circ)$ have an order of p and (4) one element (namely I) has order 1. For all $x \in \overline{O}_{p^2}$ define $\overline{g}(x) = \{y \in g(x) : \text{ order } (y) = p^2\}$. We easily see that $\forall x \in \overline{O}_{p^2}, \forall y \in \overline{g}(x)$ it is true that $y \in \overline{O}_{p^2}, g(x) = g(y)$ and $\overline{g}(x) = \overline{g}(y)$.

Indeed, $\forall x, y \in \overline{O}_{p^2}$, let us define $x \approx y$ if and only if $y \in \overline{g}(x)$. It is easy to prove that $\left(\overline{O}_{p^2}, \approx\right)$ is an equivalence relation on $\overline{O}_{p^2}$. Therefore, $\left(\overline{O}_{p^2}, \approx\right)$ induces a partition of $\overline{O}_{p^2}$ which we call $\overline{O}_{p^2} = A_1 \cup A_2 \cup \cdots \cup A_r$ such that $\forall i \in \{1, 2, \cdots, r\}, |A_i| = p(p-1)$. This implies that $\left|\overline{O}_{p^2}\right| = r \cdot p(p-1)$ which is obviously impossible since $\left|\overline{O}_{p^2}\right| = \frac{p^t-1}{2}$. Therefore, the initial assumption in the proof must be wrong, and this proves Lemma 45. ■

12 Applications

1. Suppose p is a prime of the form $p = 4k+1$. Then by Corollary 1 there does not exist a group $(D_L, \cdot)$ that left (or right) distributes over the p-star $(D_L, *)$ when $L = \{1, 2, 3, \cdots, p\}$.

2. Suppose p is a prime of the form $p = 4k+3$. We show that there does exist a group $(D_L, \cdot)$ that left-distributes over the p-star $(D_L, *)$ when $L = \{0, 1, 2, \cdots, p-1\}$. Note that we are calling $L = \{0, 1, 2, \cdots, p-1\}$ and not $L = \{1, 2, \cdots, p\}$. As suggested by the theory, to prove this we use the mod p field $Z_p = (\{0, 1, 2, \cdots, p-1\}, 0, 1, +, -, \cdot, \div)$.

   Also, by that theory, we define $(L, 0, +) = (\{0, 1, 2, 3, \cdots, p-1\}, 0, +)$ where $(L, 0, +)$ is the mod p cyclic group on $\{0, 1, 2, \cdots, p-1\}$, using mod p addition $(+)$. Note that we are using the notation $(L, 0, +)$ in the place of $(L, 1, \cdot)$. By elementary number theory, we also know that the mod p Abelian group $(\{1, 2, \cdots, p-1\}, 1, \cdot)$, using mod p multiplication $(\cdot)$, is a cyclic group.

Therefore, since $2|p-1$ we know that $(\{1, 2, \cdots, p-1\}, 1, \cdot)$ has a cyclic subgroup containing $\frac{p-1}{2}$ elements.

This implies that $\exists m \in \{1, 2, \cdots, p-1\}$ such that $m^{\frac{p-1}{2}} = 1$ and the elements of the set $\left\{m, m^2, m^3, \cdots, m^{\frac{p-1}{2}} = 1\right\} \subseteq \{1, 2, \cdots, p-1\}$ are all distinct. Define $((L, 0, +), (A, \circ))$ as follows. First, of course, $(L, 0, +) = (\{0, 1, 2, \cdots, p-1\}, 0, +)$. Also, let $(A, \circ) = \left(\left\{g_1, g_2, \cdots, g_{\frac{p-1}{2}}\right\}, \circ\right)$ where each automorphism $g_i : (L, 0, +) \rightarrow (L, 0, +)$ is defined by $\forall t \in L, g_i(t) = m^i \cdot t$ and where $m^i \cdot t$ is carried out in the field Z_p.

From the properties of the mod p field Z_p, it is straightforward to prove that $((L, 0, +), (A, \circ))$ satisfies the conditions of the Standard Hypothesis. Therefore, the construction in Section 10 produces a group $(D_L, \cdot)$ that left-distributes over the p-star $(D_L, *)$ when $p = 4k+3$. Of course, $(D_L, \odot)$ defined by $a \odot b = b \cdot a$ will right-distribute over $(D_L, *)$.

3. Let $Z_3 = (\{0, 1, 2\}, 0, 1, +, -, \cdot, \div)$ denote the mod 3 field on the set $\{0, 1, 2\}$. We consider the n-star where $n = 3^k$, where $k \in \{3, 5, 7, 9, \cdots\}$ and $\frac{3^k-1}{2} = p$ and p is an odd prime.

   Let $\left(V_3^k, 0, +\right)$ denote the k-dimensional vector space in this field Z_3 that consists of all $k \times 1$ column vectors whose entries are in Z_3.

   Define $(L, 1, \cdot) = \left(V_3^k, 0, +\right)$ where $|L| = \left|V_3^k\right| = 3^k$.

   The group of all automorphisms on $(V_3^k, 0, +)$ has $(3^k-1)(3^k-3)(3^k-9)(3^k-27)\cdots(3^k-3^{k-1})$ elements. Since $3^k - 1 = p$, by the Syloe theorems it is, it is reasonably easy to show that there exists a group $(A, \circ)$ of automorphisms on $\left(V_3^k, 0, +\right)$ such that the structure $((L, 1, \cdot), (A, \circ)) = \left(\left(V_3^k, 0, +\right), (A, \circ)\right)$ satisfies the conditions of the Standard Hypothesis when $L = V_3^k, 1 = 0$ and $\cdot = +$. Therefore, there exists a group $(D_L \cdot \cdot)$ that left-distributes over the $n - star\,(D_L, *)$ when $n = 3^k$ and $\frac{3^k-1}{2} = p$ where p is an odd prime. Also, $(D_L, \odot)$ where $a \odot b = b \cdot a$ right-distributes over $(D_L, *)$.

13 Discussion

If $((L,1,\cdot),(A,\circ))$ satisfies the conditions of the Standard Hypothesis, then $|L| = p^k$ where p is a prime of the form $p = 4\overline{k}+3$ and k is odd. Also, $(L,1,\cdot)$ is Abelian and $\forall x \in L\backslash\{1\}$, order $x = p$. This follows from $(L,1,\cdot) \cong (H,I,\circ)$ and it can also be proved directly from the properties of $((L,1,\cdot),(A,\circ))$ itself.

From group theory, we easily see that $(L,1,\cdot)$ must be isomorphic to the k-dimensional vector space in the field Z_p that consists of all $k \times 1$ column vectors whose entries are in Z_p. We denote this vector space by $(L,1,\cdot) \cong \left(V_p^k,0,+\right)$. Also, of course, all automorphisms $g_i : \left(V_p^k,0,+\right) \to \left(V_p^k,0,+\right)$ can be represented by the linear transformation MV where M is any $k \times k$ non-singular matrix in the field Z_p and V is any $k \times k$ column vector in $\left(V_p^k,0,+\right)$.

The problem that we have not been able to completely solve is to find all groups $(A,\circ) = (\{M_1, M_2, \ldots, M_{(p^k-1)/2}\},\cdot)$ where $M_i \circ M_j = M_i \cdot M_j$(matrix multiplication) that satisfy conditions c-2,c-3 and c-4, of the Standard Hypothesis. Note that $\forall i \neq j, M_iV$ is totally different from M_jV on $V_p^k\backslash\{0\}$ if and only if $M_i - M_j$ is non-singular.

Also, it seems plausible to us that a deeper analysis using the same ideas in this paper would find not only all of the types of groups that left (or right) distribute over the n-stars but also find all of these groups as well.

References

[1] Kelly, John L., General Topology, D. Van Nostrand, New York, 1955, 105-16.

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

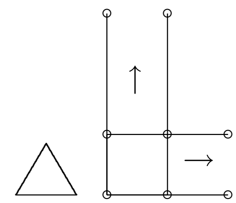
[3] Hall, Marshall, The Theory of Groups, MacMillan, New York, 1959.

[4] Bruck, Richart Hubert, A Survey of Binary Systems, Springer-Verlag, Berlin and New York, 1958.

[5] Holshouser, Arthur and Harold Reiter, "Groups that Distribute over Mathematical Structures," to appear in *International Journal of Algebra*. This paper can be accessed electronically at `http://www.math.uncc.edu/~hbreiter/researchindex.htm`

[6] Holshouser, Arthur and Harold Reiter, "Groups that Distribute over n-Stars," to appear in *International Journal of Algebra*. This paper can be accessed electronically at `http://www.math.uncc.edu/~hbreiter/researchindex.htm`

Fig. 1 Stars for $n = 3, 4, 5, 6$.



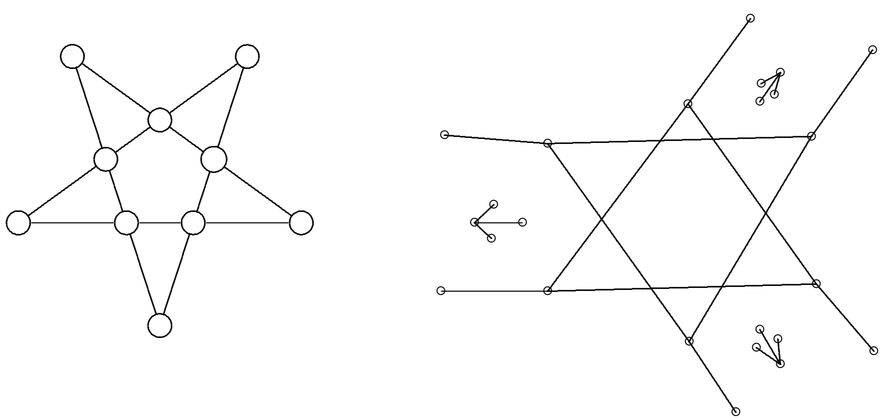


Fig. 2 A 7-star.

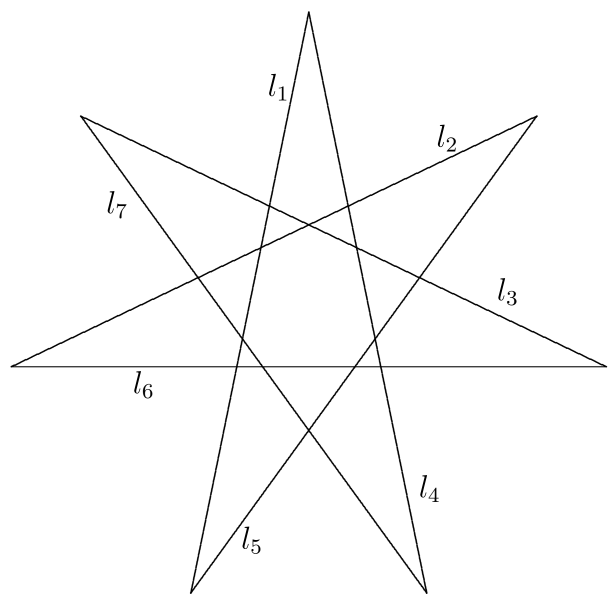


Fig. 3 A line preserving permutation.