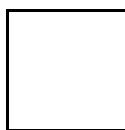


**A NEW PROOF OF  
THE FOUR COLOUR THEOREM**

BY

**ASHAY DHARWADKER**



INSTITUTE OF MATHEMATICS

H-501 PALAM VIHAR  
DISTRICT GURGAON  
HARYANA 122017  
INDIA

[ashay@धारwadker.org](mailto:ashay@धारwadker.org)



COPYRIGHT © 2000 ASHAY DHARWADKER

<http://www.dधारwadker.org>

## ACKNOWLEDGEMENTS

Thanks to the **Canadian Mathematical Society** for selecting this website as a "cool math site of the week" and knot No. 221 in their popular braid of links on October 5, 2000; Thanks to the editors of the **The Math Forum** at Drexel University for providing an elegant review of this website and its classification in both their Group Theory and Graph Theory categories; Thanks to the editors of **Tölvunot Fréttahorn** at Akureyri University for writing an article about this proof; Thanks to Dominic Verderaine for citing this proof in his essay on the **History of the Four Color Theorem**; Thanks to Anita Pasotti for citing this proof in her article on the **Teorema dei Quattro Colori e la Teoria dei Grafi**; This proof has also been cited in **Applications of Graph Theory** published by the Korean Society for Industrial and Applied Mathematics; Thanks to the editors of Yahoo! for featuring this website in their list of **Famous Mathematics Problems**; We are pleased to announce that this proof will now appear as the fourteenth chapter of the book *Graph Theory* to be published by Orient Longman and Universities Press of India.

## CONTENTS

### INTRODUCTION

### I. MAP COLOURING

### II. STEINER SYSTEMS

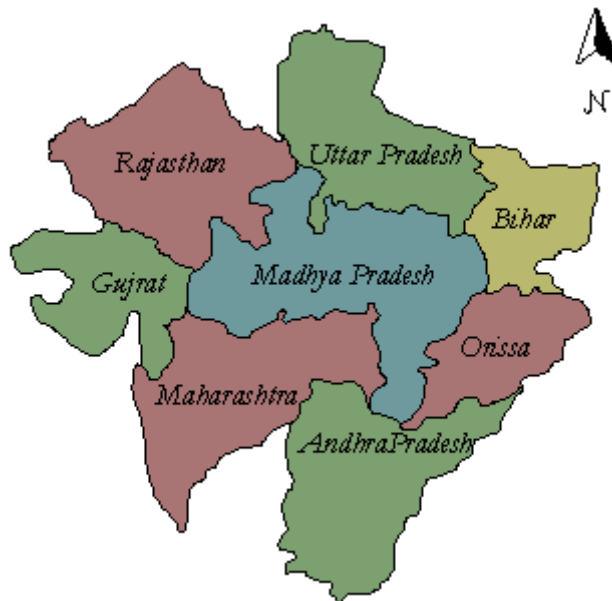
### III. EILENBERG MODULES

### IV. HALL MATCHINGS

### V. RIEMANN SURFACES

### VI. MAIN CONSTRUCTION

### REFERENCES



*Figure 0. Map of Madhya Pradesh and adjoining states in India*

## INTRODUCTION

The famous four colour theorem seems to have been first proposed by Möbius in 1840, later by DeMorgan and the Guthrie brothers in 1852, and again by Cayley in 1878. The problem of proving this theorem has a distinguished history, details of which abound in the literature. The statement of the theorem may be introduced as follows. In colouring a geographical map it is customary to give different colours to any two countries that have a segment of their boundaries in common. It has been found empirically that any map, no matter how many countries it contains nor how they are situated, can be so coloured by using only four different colours. The map of India requires four colours in the states bordering Madhya Pradesh. The fact that no map was ever found whose colouring requires more than four colours suggests the mathematical theorem.

**FOUR COLOUR THEOREM.** *For any subdivision of the plane into non-overlapping regions, it is always possible to mark each of the regions with one of the numbers 0, 1, 2, 3 in such a way that no two adjacent regions receive the same number.*

**STEPS OF THE PROOF:** We shall outline the strategy of the new proof given in this paper. In section I on **MAP COLOURING**, we define maps on the sphere and their proper colouring. For purposes of proper colouring it is equivalent to consider maps on the plane and furthermore, only maps which have exactly three edges meeting at each vertex. Lemma 1 proves the six colour theorem using Euler's formula, showing that any map on the plane may be properly coloured by using at most six colours. We may then make the following basic definitions.

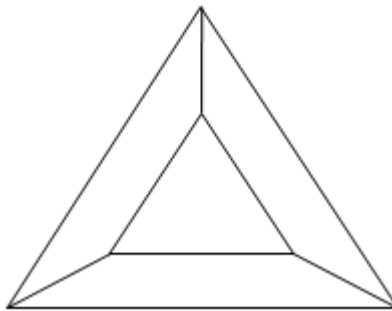
- Define  $N$  to be the minimal number of colours required to properly colour any map from the class of all maps on the plane.
- Based on the definition of  $N$ , select a specific map  $m(N)$  on the plane which requires no fewer than  $N$  colours to be properly coloured.
- Based on the definition of the map  $m(N)$ , select a proper colouring of the regions of the map  $m(N)$  using the  $N$  colours  $0, 1, \dots, N-1$ .

The whole proof works with the fixed number  $N$ , the fixed map  $m(N)$  and the fixed proper colouring of the regions of the map  $m(N)$ . In section II we define **STEINER SYSTEMS** and prove Tits' inequality and its consequence that if a Steiner system  $S(N+1, 2N, 6N)$  exists, then  $N$  cannot exceed 4. Now the goal is to demonstrate the existence of such a Steiner system. In section III we define **EILENBERG MODULES**. The regions of the map  $m(N)$  are partitioned into disjoint, nonempty equivalence classes  $\underline{0}, \underline{1}, \dots, \underline{N-1}$  according to the colour they receive. This set is given the structure of the cyclic group  $\mathbf{Z}_N = \{\underline{0}, \underline{1}, \dots, \underline{N-1}\}$  under addition modulo  $N$ . We regard  $\mathbf{Z}_N$  as an Eilenberg module for the symmetric group  $S_3$  on three letters and consider the split extension  $\mathbf{Z}_N]S_3$  corresponding to the trivial representation of  $S_3$ . By section IV on **HALL MATCHINGS** we are able to choose a common system of coset representatives for the left and right cosets of  $S_3$  in the full symmetric group on  $|\mathbf{Z}_N]S_3|$  letters. For each such common representative and for each ordered pair of elements of  $S_3$ , in section V on **RIEMANN SURFACES** we establish a certain action of the two-element cyclic group on twelve copies of the partitioned map  $m(N)$  by using the twenty-fourth root function of the sheets of the complex plane. Using this action, section VI gives the details of the

**MAIN CONSTRUCTION.** The  $6N$  elements of  $\mathbb{Z}_N \wr S_3$  are regarded as the set of points and lemma 23 builds the blocks of  $2N$  points with every set of  $N+1$  points contained in a unique block. This constructs a Steiner system  $S(N+1, 2N, 6N)$  which implies by Tits' inequality that  $N$  cannot exceed 4, completing the proof. The lemmas 1-23 and theorem 24 below are written in logical sequence.  $\square$

## I. MAP COLOURING

A *map* on the sphere is a subdivision of the surface into finitely many regions. A map is regarded as *properly coloured* if each region receives a colour and no two regions having a whole segment of their boundaries in common receive the same colour. Since deformations of the regions and their boundary lines do not affect the proper colouring of a map, we shall confine ourselves to maps whose regions are bounded by simple closed polygons. For purposes of proper colouring it is equivalent to consider maps drawn on the plane. Any map on the sphere may be represented on the plane by boring a small hole through the interior of one of the regions and deforming the resulting surface until it is flat. Conversely, by a reversal of this process, any map on the plane may be represented on the sphere. Furthermore, it suffices to consider *3-regular maps*, i.e. maps with exactly three edges meeting at each vertex, by the following argument. Replace each vertex at which more than three edges meet by a small circle and join the interior of each such circle to one of the regions meeting at the vertex. A new map is obtained which is 3-regular. If this new map can be properly coloured by using at most  $n$  colours, then by shrinking the circles down to points, the desired colouring of the original map using at most  $n$  colours is obtained.



**Figure 1.** A map that requires four colours to be properly coloured

**1. LEMMA.** Any map on the sphere can be properly coloured by using at most six colours.

**PROOF:** Assume that the given map is 3-regular. First show that there must be at least one region whose boundary is a polygon with fewer than six sides, as follows. Let  $E$  be the number of edges,  $V$  the number of vertices,  $F$  the number of regions and  $F_n$  the number of regions whose boundary is a polygon with  $n$  sides in the given map. Then

$$F = F_2 + F_3 + F_4 + \dots$$

$$2E = 3V = 2F_2 + 3F_3 + 4F_4 + \dots$$

since a region bounded by  $n$  edges has  $n$  vertices and each vertex belongs to three regions. By Euler's formula  $V - E + F = 2$ ,

$$\begin{aligned} \Rightarrow & 6V - 6E + 6F = 12 \\ \Rightarrow & 4E - 6E + 6F = 12 \\ \Rightarrow & 6F - 2E = 12 \\ \Rightarrow & 6(F_2 + F_3 + F_4 + \dots) - (2F_2 + 3F_3 + 4F_4 + \dots) = 12 \\ \Rightarrow & 4F_2 + 3F_3 + 2F_4 + F_5 + 0 + \text{NEGATIVE TERMS} = 12. \end{aligned}$$

Hence, at least one of  $F_2, F_3, F_4, F_5$  must be positive. Now, if a region  $R$  with fewer than six sides is removed from the map and the resulting map coloured with six colours inductively, there is always a colour left for  $R$ .  $\square$

By lemma 1, the minimal number of colours required to properly colour any map from the class of all maps on the sphere is a well-defined natural number. We may now make the following basic definition.

#### DEFINITION

- Define  $N$  to be the minimal number of colours required to properly colour any map from the class of all maps on the sphere. That is, given any map on the sphere, no more than  $N$  colours are required to properly colour it and there exists a map on the sphere which requires no fewer than  $N$  colours to be properly coloured.
- Based on the definition of  $N$ , select a specific map  $m(N)$  on the sphere which requires no fewer than  $N$  colours to be properly coloured.
- Based on the definition of the map  $m(N)$ , select a proper colouring of the regions of the map  $m(N)$  using the  $N$  colours  $0, 1, \dots, N-1$ .

The natural number  $N$ , the map  $m(N)$  and the proper colouring of the regions of  $m(N)$  is fixed for all future reference. By the example shown in figure 1 and lemma 1,  $4 \leq N \leq 6$ . The goal is to show that  $N \leq 4$ .

## II. STEINER SYSTEMS

A Steiner system  $S(t, k, v)$  is a set  $P$  of points together with a set  $B$  of blocks such that

- There are  $v$  points.
- Each block consists of  $k$  points.
- Every set of  $t$  points is contained in a unique block.

Note that by definition  $t, k, v$  are nonnegative integers with  $t \leq k \leq v$ . Steiner systems

with  $v = k$  (only one block that contains all the points) or  $k = t$  (every  $k$ -element subset of points is a block) are called trivial. An example of a nontrivial Steiner system is  $S(5, 8, 24)$  due to Witt, whose blocks are known as Golay codewords of weight eight [see an explicit construction cf. 7]. The group of automorphisms of  $S(5, 8, 24)$  (permutations of points which permute blocks) is the largest of the Mathieu groups,  $M_{24}$ .

**2. LEMMA.** [J. TITS] *If there exists a nontrivial Steiner system  $S(t, k, v)$  then*

$$v \geq (t+1)(k-t+1).$$

PROOF: First show that there exists a set  $X_0$  of  $t+1$  points that is not contained in any block, as follows. Suppose that for every set  $X$  of  $t+1$  points there is a block  $B_X$  that contains it. Then, this block  $B_X$  must be the unique block containing  $X$ , since  $X$  has more than  $t$  points. Let  $b$  denote the total number of blocks. Count in two ways the number of pairs  $(X, B_X)$  where  $X$  is a set of  $t+1$  points and  $B_X$  is the unique block containing it. One finds

$$\binom{v}{t+1} = b \binom{k}{t+1}.$$

Count in two ways the number of pairs  $(Y, B_Y)$  where  $Y$  is a set of  $t$  points and  $B_Y$  is the unique block containing it, by definition of a Steiner system. One finds

$$\binom{v}{t} = b \binom{k}{t}.$$

Hence

$$\frac{\binom{v}{t+1}}{\binom{k}{t+1}} = \frac{\binom{v}{t}}{\binom{k}{t}} = b.$$

and it follows that  $b = 1$  and  $k = v$ , contradicting the hypothesis that the Steiner system is nontrivial. Now choose a fixed set  $X_0$  of  $t+1$  points that is not contained in any block. For each set  $Z$  of  $t$  points contained in  $X_0$  there is a unique block  $B_Z$  containing  $Z$ . Each such  $B_Z$  has  $k-t$  points not in  $X_0$  and any point not in  $X_0$  is contained in at most one such  $B_Z$ , since two such blocks already have  $t-1$  points of  $X_0$  in common. The union of the blocks  $B_Z$  contains  $(t+1)+(t+1)(k-t)$  points and this number cannot exceed the total number of points  $v$ .  $\square$

Recall the definition from section I that  $N$  is the minimal number of colours required to properly colour any map from the class of all maps on the sphere and  $m(N)$  is a specific map which requires all of the  $N$  colours to properly colour it. The regions of the map

$m(N)$  have been properly coloured using the  $N$  colours  $0, 1, \dots, N-1$ . From the map  $m(N)$  and its fixed proper colouring, we shall construct a Steiner system  $S(N+1, 2N, 6N)$  by defining the points and blocks in a certain way. The next lemma shows that this construction would force  $N \leq 4$ .

**3. LEMMA.** *Referring to the definition of  $N$  in section I, if there exists a Steiner system  $S(N+1, 2N, 6N)$  then  $N \leq 4$ .*

PROOF: Since  $4 \leq N \leq 6$  by definition, the Steiner system is nontrivial if it exists. By lemma 2,  $6N \geq (N+1+1)(2N-N-1+1) = (N+2)N$ . Hence  $6 \geq N+2$  and it follows that  $4 \geq N$ .  $\square$

Now, the goal is to demonstrate the existence of the Steiner system  $S(N+1, 2N, 6N)$  based upon the definition of the map  $m(N)$ .

### III. EILENBERG MODULES

Let  $G$  be a group with identity element  $e$  and let  $\mathbf{Z}$  denote the integers. The *integral group algebra*  $(\mathbf{Z}G, +, -)$  is a ring whose elements are formal sums

$$\sum_{g \in G} n_g g$$

with  $g$  in  $G$  and  $n_g$  in  $\mathbf{Z}$  such that  $n_g = 0$  for all but a finite number of  $g$ . Addition and multiplication in  $\mathbf{Z}G$  are defined by

$$\begin{aligned} \sum_{g \in G} n_g g + \sum_{g \in G} m_g g &= \sum_{g \in G} (n_g + m_g)g, \\ \sum_{g \in G} n_g g \cdot \sum_{g \in G} m_g g &= \sum_{g \in G} \left( \sum_{h \in G} n_{gh^{-1}} m_h \right) g. \end{aligned}$$

The element  $n$  of  $\mathbf{Z}$  is identified with the element  $n \cdot e$  of  $\mathbf{Z}G$  and the element  $g$  of  $G$  is identified with the element  $1 \cdot g$  of  $\mathbf{Z}G$ , so that  $\mathbf{Z}$  and  $G$  are to be regarded as subsets of  $\mathbf{Z}G$ . The underlying additive abelian group  $(\mathbf{Z}G, +)$  is the direct sum of copies of the integers  $\mathbf{Z}$  indexed by elements of  $G$ . If  $Q$  is a subgroup of  $G$  then  $\mathbf{Z}Q$  is a subring of  $\mathbf{Z}G$  in a natural way. For each element  $g$  of  $G$ , the right multiplication  $R(g): G \rightarrow G; x \rightarrow xg$  and the left multiplication  $L(g): G \rightarrow G; x \rightarrow gx$  are permutations of the set  $G$ . Denote the group of all permutations of the set  $G$  by  $\text{Sym}(G)$ . Then

$$\begin{aligned} R : G &\rightarrow \text{Sym}(G); g \rightarrow R(g) \\ L^{-1} : G &\rightarrow \text{Sym}(G); g \rightarrow L^{-1}(g) = L(g^{-1}) \end{aligned}$$

are embeddings of the group  $G$  in  $\text{Sym}(G)$ . The images  $R(G), L^{-1}(G)$  are called the *Cayley right and left regular representations of  $G$* , respectively. The subgroup of  $\text{Sym}(G)$  generated by the set  $R(G) \cup L^{-1}(G) = \{R(g), L(g^{-1}) | g \in G\}$  is called the

combinatorial multiplication group  $Mlt(G)$  of  $G$ . There is an exact sequence of groups

$$1 \rightarrow C(G) \xrightarrow{\Delta} G \times G \xrightarrow{T} Mlt(G) \rightarrow 1$$

where  $T(x, y) = R(x)L(y^{-1})$  and  $\Delta c = (c, c)$  for an element  $c$  of the center  $C(G)$  of  $G$ . If  $Q$  is a subgroup of  $G$  then the *relative combinatorial multiplication group*  $Mlt_G(Q)$  of  $Q$  in  $G$  is the subgroup of  $Mlt(G)$  generated by the set  $R(Q) \cup L^{-1}(Q) = \{R(q), L^{-1}(q) | q \in Q\}$ . The orbits of the action of  $Mlt_G(Q)$  on  $G$  are the double cosets  $QgQ$  of the subgroup  $Q$  in  $G$ . The stabilizer of the identity element  $e$  is the subgroup of  $Mlt_G(Q)$  generated by the set  $\{T(q) = R(q)L^{-1}(q) | q \in Q\}$ . A *representation* of the group  $Q$  is usually defined as a module, i.e. an abelian group  $(M, +)$ , for which there is a homomorphism  $T: Q \rightarrow Aut(M, +)$  showing how  $Q$  acts as a group of automorphisms of the module. Another approach due to Eilenberg, views a module  $M$  for the group  $Q$  as follows. The set  $M \times Q$  equipped with the multiplication

$$(m_1, q_1)(m_2, q_2) = (m_1 + m_2T(q_1), q_1q_2)$$

becomes a group  $M]Q$  known as the *split extension of  $M$  by  $Q$* . There is an exact sequence of groups

$$1 \rightarrow M \xrightarrow{\iota} M]Q \xrightarrow{\pi} Q \rightarrow 1$$

with  $\iota: M \rightarrow M]Q; m \rightarrow (m, e)$  and  $\pi: M]Q \rightarrow Q; (m, q) \rightarrow q$  split by  $0: Q \rightarrow M]Q; q \rightarrow (0, q)$ . The group action  $T$  is recovered from the split extension  $M]Q$  by  $mT(q)\iota = mR((0, q))L^{-1}((0, q))$  for  $m$  in  $M$  and  $q$  in  $Q$ . In this context we shall call  $M$  an *Eilenberg module for the group  $Q$* . For example, the trivial representation for the group  $Q$  is obtained by defining  $T: Q \rightarrow Aut(M, +); q \rightarrow 1_M$ , the identity automorphism of  $(M, +)$  and the corresponding split extension is the group direct product  $M \times Q$ . The Cayley right regular representation for the group  $Q$  is obtained by defining

$$T: Q \rightarrow Aut(\mathbf{Z}Q, +); q \rightarrow \left( \sum_{g \in Q} n_g g \rightarrow \sum_{g \in Q} n_g g R(q) \right).$$

Here  $T(q) = R(q)L^{-1}(q)$  with  $L^{-1}(q)$  acting trivially on the module elements and  $R(q)$  acting as the usual right multiplication. The split extension  $\mathbf{Z}Q]Q$  has multiplication given by

$$(m_1, q_1)(m_2, q_2) = (m_1 + m_2R(q_1), q_1q_2)$$

for  $m_1, m_2$  in  $\mathbf{Z}Q$  and  $q_1, q_2$  in  $Q$ .

Referring to the definition in section I,  $N$  is the minimal number of colours required to properly colour any map from the class of all maps on the sphere and  $\mathbf{m}(N)$  is a specific map that requires all of  $N$  colours to be properly coloured. Note that  $\mathbf{m}(N)$  has been properly coloured by using the  $N$  colours  $0, 1, \dots, N-1$  and this proper colouring is fixed. The set of regions of  $\mathbf{m}(N)$  is then partitioned into subsets  $\underline{0}, \underline{1}, \dots, \underline{N-1}$  where the subset

$\underline{m}$  consists of all the regions which receive the colour  $m$ . Note that the subsets  $\underline{0}, \underline{1}, \dots, \underline{N-1}$  are each nonempty (since  $\mathbf{m}(N)$  requires all of the  $N$  colours to be properly coloured) and form a partition of the set of regions of  $\mathbf{m}(N)$  (by virtue of proper colouring). Identify the set  $\{\underline{0}, \underline{1}, \dots, \underline{N-1}\}$  with the underlying set of the  $N$ -element cyclic group  $\mathbf{Z}_N$  under addition modulo  $N$ . Let  $S_3$  denote the symmetric group on three letters, identified with the dihedral group of order six generated by  $\rho, \sigma$  where  $|\rho| = 3$  and  $|\sigma| = 2$ .

**4. LEMMA.**  $(\mathbf{Z}_N, +)$  is an Eilenberg module for the group  $S_3$  with the trivial homomorphism

$$T_1: S_3 \rightarrow \text{Aut}(\mathbf{Z}_N, +); \alpha \rightarrow \mathbf{1}_{\mathbf{Z}_N}$$

where  $\mathbf{1}_{\mathbf{Z}_N}$  denotes the identity automorphism of  $\mathbf{Z}_N$ . The corresponding split extension  $\mathbf{Z}_N[S_3]$  has multiplication given by

$$(\underline{m}_1, \alpha_1) \cdot (\underline{m}_2, \alpha_2) = (\underline{m}_1 + \underline{m}_2, \alpha_1 \alpha_2)$$

and is a group isomorphic to the direct product  $\mathbf{Z}_N \times S_3$ .

PROOF: Follows from definition.  $\square$

Referring to section II, the goal is to construct a Steiner system  $S(N+1, 2N, 6N)$ . We shall take the point set of the Steiner system to be the underlying set of the split extension  $\mathbf{Z}_N[S_3]$ . The following lemma is used in section V.

**5. LEMMA.** Let  $(\mathbf{Z}(\mathbf{Z}_N[S_3]), +)$  and  $(\mathbf{Z}S_3, +)$  denote the underlying additive groups of the integral group algebras  $\mathbf{Z}(\mathbf{Z}_N[S_3])$  and  $\mathbf{Z}S_3$ , respectively. Then  $(\mathbf{Z}(\mathbf{Z}_N[S_3]), +)$  is an Eilenberg module for the group  $(\mathbf{Z}S_3, +)$  with the trivial homomorphism

$$T_2: (\mathbf{Z}S_3, +) \rightarrow \text{Aut}(\mathbf{Z}(\mathbf{Z}_N[S_3]), +); \sum_{\alpha \in S_3} n_\alpha \alpha \rightarrow \mathbf{1}_{\mathbf{Z}(\mathbf{Z}_N[S_3])}$$

where  $\mathbf{1}_{\mathbf{Z}(\mathbf{Z}_N[S_3])}$  denotes the identity automorphism of  $(\mathbf{Z}(\mathbf{Z}_N[S_3]), +)$ . The corresponding split extension  $\mathbf{Z}(\mathbf{Z}_N[S_3])[\mathbf{Z}S_3]$  has multiplication given by

$$\begin{aligned} & \left( \sum_{(\underline{m}, \beta) \in \mathbf{Z}_N[S_3]} n_{(\underline{m}, \beta)} (\underline{m}, \beta), \sum_{\alpha \in S_3} n_\alpha \alpha \right) \left( \sum_{(\underline{m}', \beta') \in \mathbf{Z}_N[S_3]} n'_{(\underline{m}', \beta')} (\underline{m}', \beta'), \sum_{\alpha' \in S_3} n'_{\alpha'} \alpha' \right) \\ &= \left( \sum_{(\underline{m}, \beta) \in \mathbf{Z}_N[S_3]} (n_{(\underline{m}, \beta)} + n'_{(\underline{m}, \beta)}) (\underline{m}, \beta), \sum_{\alpha \in S_3} (n_\alpha + n'_\alpha) \alpha \right) \end{aligned}$$

and is a group isomorphic to the direct product  $(\mathbf{Z}(\mathbf{Z}_N[S_3]) \times \mathbf{Z}S_3, +)$ .

PROOF: Follows from definition.  $\square$

#### IV. HALL MATCHINGS

Let  $\Gamma$  be a bipartite graph with vertex set  $V = XUY$  and edge set  $E$  (every edge has one end in  $X$  and the other end in  $Y$ ). A *matching from  $X$  to  $Y$  in  $\Gamma$*  is a subset  $M$  of  $E$  such that no vertex is incident with more than one edge in  $M$ . A matching  $M$  from  $X$  to  $Y$  in  $\Gamma$  is called *complete* if every vertex in  $X$  is incident with an edge in  $M$ . If  $A$  is a subset of  $V$  then let  $adj(A)$  denote the set of all vertices adjacent to a vertex in  $A$ .

**6. LEMMA.** [P. HALL] *If  $|adj(A)| \geq |A|$  for every subset  $A$  of  $X$  then there exists a complete matching from  $X$  to  $Y$  in  $\Gamma$ .*

PROOF: A matching from  $X$  to  $Y$  in  $\Gamma$  with  $|M| = 1$  always exists by choosing a single edge in  $E$ . Let  $M$  be a matching from  $X$  to  $Y$  in  $\Gamma$  with  $m$  edges,  $m < |X|$ . Let  $x_0 \in X$  such that  $x_0$  is not incident with any edge in  $M$ . Since  $|adj(\{x_0\})| \geq 1$ , there is a vertex  $y_1$  adjacent to  $x_0$  by an edge in  $E \setminus M$ . If  $y_1$  is not incident with an edge in  $M$ , then stop. Otherwise, let  $x_1$  be the other end of such an edge. If  $x_0, x_1, \dots, x_k$  and  $y_1, \dots, y_k$  have been chosen, then since  $|adj(\{x_0, x_1, \dots, x_k\})| \geq k+1$ , there is a vertex  $y_{k+1}$ , distinct from  $y_1, \dots, y_k$ , that is adjacent to at least one vertex in  $\{x_0, x_1, \dots, x_k\}$ . If  $y_{k+1}$  is not incident with an edge in  $M$ , then stop. Otherwise, let  $x_{k+1}$  be the other end of such an edge. This process must terminate with some vertex, say  $y_{k+1}$ . Now build a simple path from  $y_{k+1}$  to  $x_0$  as follows. Start with  $y_{k+1}$  and the edge in  $E \setminus M$  joining it to, say  $x_{i_1}$  with  $i_1 < k+1$ . Then add the edge in  $M$  from  $x_{i_1}$  to  $y_{i_1}$ . By construction,  $y_{i_1}$  is joined by an edge in  $E \setminus M$  to some  $x_{i_2}$  with  $i_2 < i_1$ . Continue adding edges in this way until  $x_0$  is reached. One obtains a path  $y_{k+1}, x_{i_1}, y_{i_1}, x_{i_2}, y_{i_2}, \dots, x_{i_r}, y_{i_r}, x_0$  of odd length  $2r+1$  with the  $r+1$  edges  $\{y_{k+1}, x_{i_1}\}, \{y_{i_1}, x_{i_2}\}, \dots, \{y_{i_r}, x_0\}$  in  $E \setminus M$  and the  $r$  edges  $\{x_{i_1}, y_{i_1}\}, \dots, \{x_{i_r}, y_{i_r}\}$  in  $M$ . Define

$$M' = (M \setminus \{\{x_{i_1}, y_{i_1}\}, \dots, \{x_{i_r}, y_{i_r}\}\}) \cup \{\{y_{k+1}, x_{i_1}\}, \{y_{i_1}, x_{i_2}\}, \dots, \{y_{i_r}, x_0\}\}.$$

Then  $M'$  is a matching from  $X$  to  $Y$  in  $\Gamma$ , with  $|M'| = |M| - r + r + 1 = |M| + 1$ . Repeating this process a finite number of times must yield a complete matching from  $X$  to  $Y$  in  $\Gamma$ .  $\square$

**7. LEMMA.** *Referring to section III, let  $Sym(\mathbf{Z}_N]S_3)$  denote the group of all permutations of the underlying set of the split extension  $\mathbf{Z}_N]S_3$  of lemma 4. Then  $S_3$  embeds in  $Sym(\mathbf{Z}_N]S_3)$  via the Cayley right regular representation.*

PROOF: Note that  $S_3 = \{(\underline{0}, \alpha) | \alpha \in S_3\}$  is a subgroup of  $\mathbf{Z}_N]S_3$ . Since  $S_3$  embeds in  $Sym(S_3)$  via the Cayley right regular representation  $\alpha \rightarrow R(\alpha)$  and  $Sym(S_3)$  is a subgroup of  $Sym(\mathbf{Z}_N]S_3)$ , the lemma follows.  $\square$

**8. LEMMA.** *By lemma 7, regard  $S_3$  as a subgroup of  $Sym(\mathbf{Z}_N]S_3)$ . There exists a common system of coset representatives  $\phi_1, \dots, \phi_k$  such that  $\{\phi_1 S_3, \dots, \phi_k S_3\}$  is the family of left cosets of  $S_3$  in  $Sym(\mathbf{Z}_N]S_3)$  and  $\{S_3 \phi_1, \dots, S_3 \phi_k\}$  is the family of right cosets of  $S_3$  in  $Sym(\mathbf{Z}_N]S_3)$ .*

PROOF: By Lagrange's theorem the left cosets of  $S_3$  partition  $Sym(\mathbf{Z}_N]S_3)$  into  $k = [Sym(\mathbf{Z}_N]S_3):S_3]$  disjoint nonempty equivalence classes of size  $|S_3| = 6$ . The same is true of the right cosets. Define a bipartite graph  $\Gamma$  with vertices  $XUY$  where  $X = \{\psi_1S_3, \dots, \psi_kS_3\}$  is the family of left cosets of  $S_3$  in  $Sym(\mathbf{Z}_N]S_3)$  and  $Y = \{S_3\psi'_1, \dots, S_3\psi'_k\}$  is the family of right cosets of  $S_3$  in  $Sym(\mathbf{Z}_N]S_3)$  with an edge  $\{\psi_iS_3, S_3\psi'_j\}$  if and only if  $\psi_iS_3$  and  $S_3\psi'_j$  have nonempty intersection. Note that we can select representatives of the left cosets that belong to distinct right cosets [see a proof of this fact cf. 8]. For any subset  $A = \{\psi_{i_1}S_3, \dots, \psi_{i_r}S_3\}$  of  $X$ , one has  $\psi_{i_1} \in \psi_{i_1}S_3, \dots, \psi_{i_r} \in \psi_{i_r}S_3$  and there exist distinct  $j_1, \dots, j_r$  such that  $\psi_{i_1} \in S_3\psi'_{j_1}, \dots, \psi_{i_r} \in S_3\psi'_{j_r}$ . Hence, in the graph  $\Gamma$ ,  $|adj(A)| \geq |A|$ . Hall's hypothesis of lemma 6 is satisfied and there exists a complete matching from  $X$  to  $Y$  in  $\Gamma$ . This is precisely the statement that a common system of coset representatives  $\phi_1, \dots, \phi_k$  exists.  $\square$

## V. RIEMANN SURFACES

Let  $C$  denote the complex plane. Consider the function  $C \rightarrow C; z \rightarrow w = z^n$ , where  $n \geq 2$ . There is a one-to-one correspondence between each sector

$$\{z|(k-1)2\pi/n < \arg z < k2\pi/n\} \quad (k = 1, \dots, n)$$

and the whole  $w$ -plane except for the positive real axis. The image of each sector is obtained by performing a cut along the positive real axis; this cut has an upper and a lower edge. Corresponding to the  $n$  sectors in the  $z$ -plane, take  $n$  identical copies of the  $w$ -plane with the cut. These will be the *sheets of the Riemann surface* and are distinguished by a label  $k$  which serves to identify the corresponding sector. For  $k = 1, \dots, n-1$  attach the lower edge of the sheet labeled  $k$  with the upper edge of the sheet labeled  $k+1$ . To complete the cycle, attach the lower edge of the sheet labeled  $n$  to the upper edge of the sheet labeled 1. In a physical sense, this is not possible without self-intersection but the idealized model shall be free of this discrepancy. The result of the construction is a *Riemann surface* whose points are in one-to-one correspondence with the points of the  $z$ -plane [see a geometric model cf. 15]. This correspondence is continuous in the following sense. When  $z$  moves in its plane, the corresponding point  $w$  is free to move on the Riemann surface. The point  $w = 0$  connects all the sheets and is called the *branch point*. A curve must wind  $n$  times around the branch point before it closes. Now consider the  $n$ -valued relation

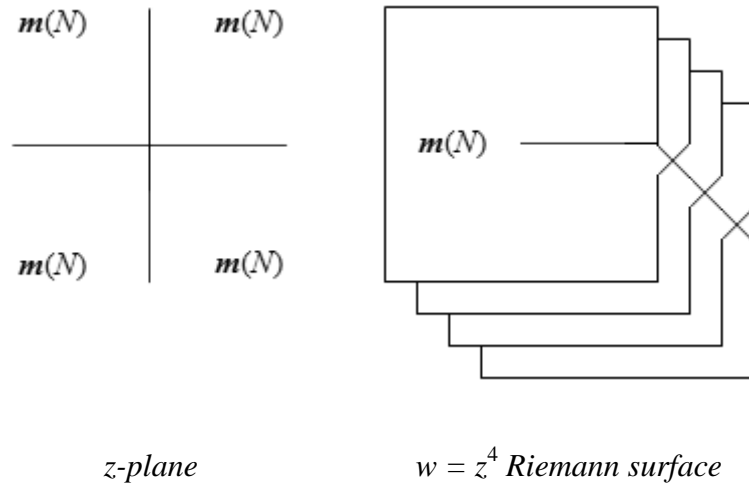
$$z = \sqrt[n]{w}.$$

To each  $w \neq 0$ , there correspond  $n$  values of  $z$ . If the  $w$ -plane is replaced by the Riemann surface just constructed, then each complex number  $w \neq 0$  is represented by  $n$  points of the Riemann surface at superposed positions. Let the point on the uppermost sheet represent the principal value and the other  $n-1$  points represent the other values. Then  $z = \sqrt[n]{w}$  becomes a single-valued, continuous, one-to-one correspondence of the points of the Riemann surface with the points of the  $z$ -plane. Now recall the definition of the map  $m(N)$  from section I. The map  $m(N)$  is on the sphere. Pick a region and deform the sphere so that both 0 and  $\infty$  are two distinct points inside this region when the sphere is

regarded as the extended complex plane. Using the stereographic projection one obtains the map  $m(N)$  on the complex plane  $C$  with the region containing 0 and  $\infty$  forming a “sea” surrounding the other regions which form an “island”. Put this copy of  $C$  on each sheet of the Riemann surface corresponding to  $w = z^n$ . The branch point lies in the “sea”. The inverse function  $z = \sqrt[n]{w}$  results in  $n$  copies of the map  $m(N)$  on the  $z$ -plane in the sectors

$$\{z|(k-1)2\pi/n < \arg z < k2\pi/n\} \quad (k = 1, \dots, n).$$

The origin of the  $z$ -plane lies in the  $n$  “seas”.



**Figure 2.** An example with  $n = 4$

Referring to section III, the full symmetric group  $Sym(\mathbf{Z}_N]S_3)$  acts faithfully on the set  $\mathbf{Z}_N]S_3$ . The action of an element  $\psi$  of  $Sym(\mathbf{Z}_N]S_3)$  on an element  $(\underline{m}, \alpha)$  of  $\mathbf{Z}_N]S_3$  will be written as  $(\underline{m}, \alpha)\psi$ . This action extends to the integral group algebra  $\mathbf{Z}(\mathbf{Z}_N]S_3)$  by linearity

$$\left( \sum_{(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3} n_{(\underline{m}, \alpha)} (\underline{m}, \alpha) \right) \psi = \sum_{(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3} n_{(\underline{m}, \alpha)} ((\underline{m}, \alpha)\psi).$$

Referring to lemma 8, fix a common coset representative  $\phi_i$  of  $S_3$  in  $Sym(\mathbf{Z}_N]S_3)$  and fix a pair  $(\beta, \gamma) \in S_3 \times S_3 = Mlt(S_3)$ . There are two cases depending on whether  $\beta = \gamma$  or whether  $\beta \neq \gamma$ .

**CASE 1.** Suppose  $\beta \neq \gamma$ . Consider the composition of the functions

$$C \rightarrow C; z \rightarrow t = z^2 \text{ and } C \rightarrow C; t \rightarrow w = t^{12}.$$

The composite is given by the assignment

$$z \rightarrow t = z^2 \rightarrow w = t^{12} = z^{24}.$$

There are twenty-four superposed copies of the map  $m(N)$  on the  $w$ -Riemann surface corresponding to the sectors

$$\{z|(k-1)2\pi/24 < \arg z < k2\pi/24\} \quad (k = 1, \dots, 24)$$

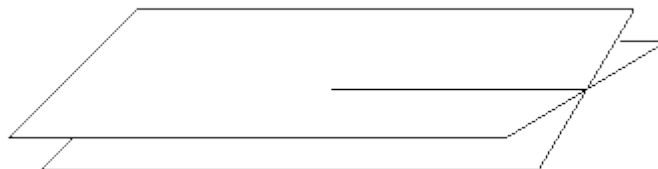
on the  $z$ -plane. These are divided into two sets. The first set consists of twelve superposed copies of the map  $m(N)$  corresponding to the sectors

$$\{z|(k-1)2\pi/24 < \arg z < k2\pi/24\} \quad (k = 1, \dots, 12)$$

of the upper half of the  $z$ -plane which comprise the upper sheet of the  $t$ -Riemann surface. The second set consists of twelve superposed copies of the map  $m(N)$  corresponding to the sectors

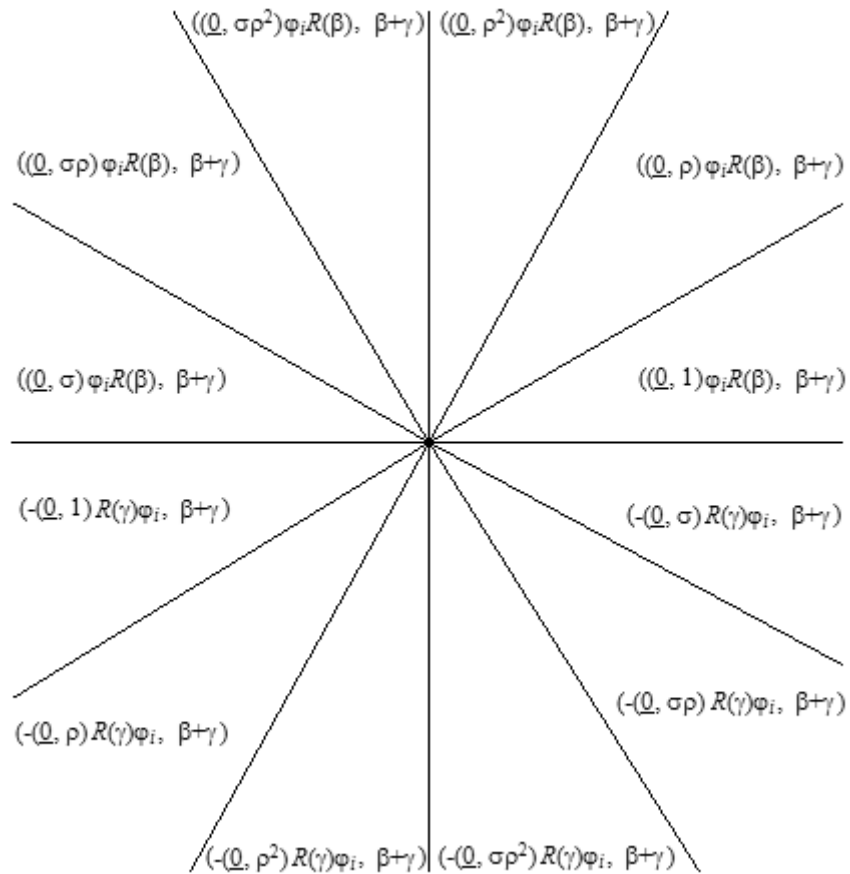
$$\{z|(k-1)2\pi/24 < \arg z < k2\pi/24\} \quad (k = 13, \dots, 24)$$

of the lower half of the  $z$ -plane which comprise the lower sheet of the  $t$ -Riemann surface.



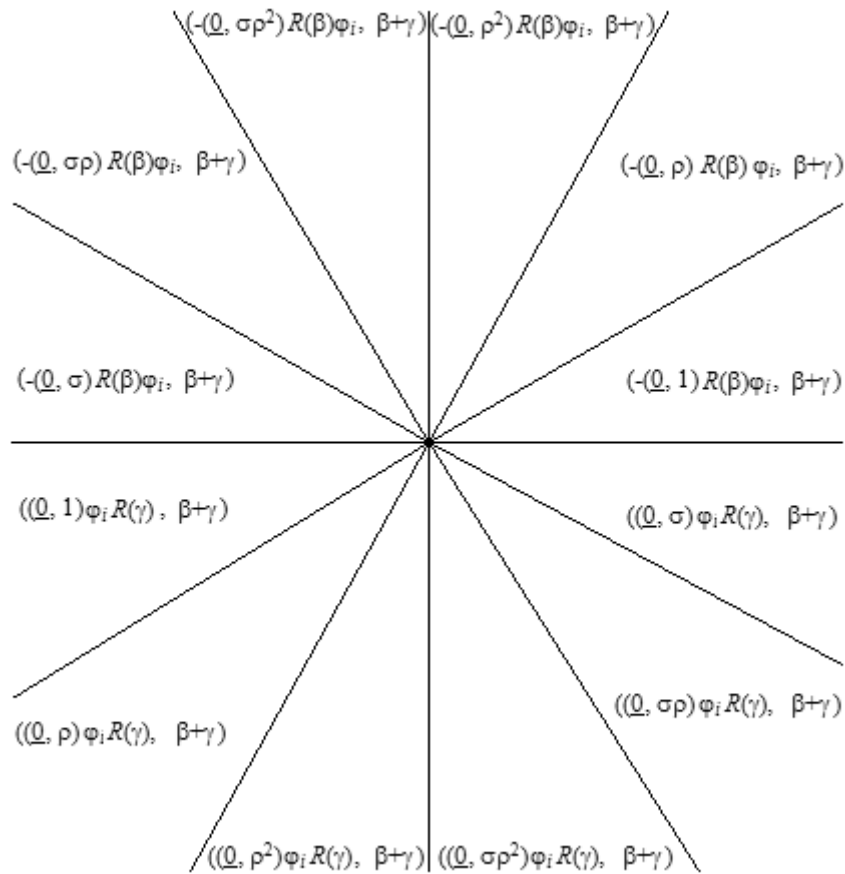
**Figure 3.** *Sheets of the  $t$ -Riemann surface*

Label the twelve sectors of the upper sheet of the  $t$ -Riemann surface by elements of  $Z(Z_N]S_3)]ZS_3$  as shown:



**Figure 4.** Upper sheet of the  $t$ -Riemann surface

Label the twelve sectors of the lower sheet of the  $t$ -Riemann surface by elements of  $Z(Z_N]S_3)]ZS_3$  as shown:



**Figure 5.** Lower sheet of the  $t$ -Riemann surface

Referring to section II, the regions of the map  $m(N)$  have been partitioned into disjoint, nonempty equivalence classes  $\underline{0}, \underline{1}, \dots, \underline{N-1}$  and this set of equivalence classes forms the underlying set of the cyclic group  $\mathbf{Z}_N$ . Hence there are twelve copies of  $\mathbf{Z}_N$  on the upper sheet and twelve copies of  $\mathbf{Z}_N$  on the lower sheet of the  $t$ -Riemann surface. The copies of  $\mathbf{Z}_N$  are indexed by the elements of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$  which label the sectors on a particular sheet. The branch point of the  $t$ -Riemann surface is labeled by the element  $(0, \beta+\gamma)$  of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$  where 0 denotes the zero element of  $\mathbf{Z}(\mathbf{Z}_N]S_3)$ .

**9. LEMMA.** *Referring to lemma 8, fix a common representative  $\varphi_i$  of the left and right cosets of  $S_3$  in  $\text{Sym}(\mathbf{Z}_N]S_3)$ . Fix a pair  $(\beta, \gamma) \in S_3 \times S_3$  with  $\beta \neq \gamma$ . Referring to lemma 5, define a subset  $T_{(\beta, \gamma)}$  of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$  as follows:*

$$T_{(\beta, \gamma)} = \left\{ ((\underline{m}, \alpha), \beta+\gamma) \mid (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3 \right\} \\ \cup \\ \left\{ (0, \beta+\gamma) \right\} \\ \cup \\ \left\{ (-(\underline{m}, \alpha), \beta+\gamma) \mid (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3 \right\}.$$

Referring to the preceding discussion, consider the composite function

$$z \rightarrow t = z^2 \rightarrow w = t^{12} = z^{24}$$

of the complex  $z$ -plane to the  $w$ -Riemann surface. There is a copy of the set  $T_{(\beta, \gamma)}$  on the upper sheet and a copy of the set  $T_{(\beta, \gamma)}$  on the lower sheet of the  $t$ -Riemann surface according to the labels of the sectors in figures 4 and 5 with the branch point labelled by the element  $(0, \beta+\gamma)$  of both copies. The rotation of the  $z$ -plane by  $\pi$  radians induces a permutation

$$p: T_{(\beta, \gamma)} \rightarrow T_{(\beta, \gamma)}$$

given by

$$\begin{aligned} (-(\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma)p &= ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma) \\ (0, \beta+\gamma)p &= (0, \beta+\gamma) \\ ((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma)p &= (-(\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma) \end{aligned}$$

for all  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$ , such that each point of the copy of  $T_{(\beta, \gamma)}$  on the upper sheet moves continuously along a circular curve that winds exactly once around the branch point, to the point superposed directly below it on the copy of  $T_{(\beta, \gamma)}$  on the lower sheet of the  $t$ -Riemann surface.

PROOF:  $T_{(\beta, \gamma)}$  is seen to be a well-defined subset of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$  by setting the appropriate coefficients to zero in a typical element as described in lemma 5. Each of

$R(\gamma)\varphi_i, \varphi_iR(\gamma), \varphi_iR(\beta), R(\beta)\varphi_i$  are permutations of the set  $\mathbf{Z}_N]S_3$  and the rotation of the  $z$ -plane by  $\pi$  radians clearly induces a permutation  $p$  of the set  $T_{(\beta, \gamma)}$  as described.  $\square$

**10. LEMMA.** Referring to lemma 9, let  $Sym(T_{(\beta, \gamma)})$  denote the full permutation group of the set  $T_{(\beta, \gamma)}$ . Let  $\langle p \rangle$  denote the cyclic subgroup of  $Sym(T_{(\beta, \gamma)})$  generated by  $p$ . Then  $\langle p \rangle$  is nontrivial and acts faithfully on the set  $T_{(\beta, \gamma)}$ .

PROOF: If  $p = 1$ , then  $(-\underline{0}, 1)R(\gamma)\varphi_i, \beta+\gamma) = (-\underline{0}, 1)R(\gamma)\varphi_i, \beta+\gamma)p = ((\underline{0}, 1)\varphi_iR(\gamma), \beta+\gamma)$  which implies that  $(-\underline{0}, 1)R(\gamma)\varphi_i = (\underline{0}, 1)\varphi_iR(\gamma)$  in  $\mathbf{Z}(\mathbf{Z}_N]S_3)$ . This is impossible since  $1 \neq -1$  in  $\mathbf{Z}$ . Hence  $p \neq 1$ . Since the full permutation group  $Sym(T_{(\beta, \gamma)})$  acts faithfully on  $T_{(\beta, \gamma)}$ , so does its subgroup  $\langle p \rangle$ .  $\square$

**11. LEMMA.** Referring to lemma 9 and lemma 10, let  $1: \mathbf{C} \rightarrow \mathbf{C}; z \rightarrow z$  denote the identity and  $\pi: \mathbf{C} \rightarrow \mathbf{C}; z \rightarrow -z$  denote the rotation through an angle of  $\pi$  radians of the  $z$ -plane. Then the two-element cyclic group  $\{1, \pi\}$  acts faithfully on the set  $\langle p \rangle$  as follows:  $p^n 1 = p^n$  and  $p^n \pi = p^{1-n}$ , for all  $n$  in  $\mathbf{Z}$ .

PROOF: The set  $\{1, \pi\}$  forms a two-element cyclic group  $\langle \pi \rangle$  under function composition. To show that  $\{1, \pi\}$  acts on  $\langle p \rangle$  as defined, observe that  $(p^n \pi)\pi = (p^{1-n})\pi = p^{1-(1-n)} = p^{1-1+n} = p^n = p^n 1 = p^n(\pi\pi)$ , for all  $n$  in  $\mathbf{Z}$ . To show that the action is faithful, let  $\theta \in \{1, \pi\}$ . If  $\theta$  belongs to the kernel of the action then  $p^n \theta = p^n$  for all  $n$  in  $\mathbf{Z}$  so that  $p\theta = p$  which implies that  $\theta = 1$ , since  $p \neq 1$  by lemma 10.  $\square$

**12. LEMMA.** Putting together lemma 9, lemma 10 and lemma 11, there is a well-defined action of the two-element cyclic group  $\{1, \pi\}$  on the set  $T_{(\beta, \gamma)}$  given by

$$\begin{aligned} ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma)1 &= ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma) \\ (0, \beta+\gamma)1 &= (0, \beta+\gamma) \\ (-\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma)1 &= (-\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma) \end{aligned}$$

and

$$\begin{aligned} ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma)\pi &= (-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma) \\ (0, \beta+\gamma)\pi &= (0, \beta+\gamma) \\ (-\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma)\pi &= ((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma) \end{aligned}$$

for all  $(\underline{m}, \alpha)$  in  $\mathbf{Z}_N]S_3$ . This action is faithful.

PROOF: For each  $x \in T_{(\beta, \gamma)}$ , let  $Orb(x) = \{xp^n | n \in \mathbf{Z}\}$  denote the orbit of  $x$  under  $\langle p \rangle$ . The collection  $\{Orb(x) | x \in T_{(\beta, \gamma)}\}$  forms a partition of the set  $T_{(\beta, \gamma)}$  as follows. Let  $x, y \in T_{(\beta, \gamma)}$ . If  $z \in Orb(x) \cap Orb(y)$  then  $z = xp^n = yp^m$  for some  $m, n \in \mathbf{Z}$ . This implies  $xp^{n-m} = y \Rightarrow y \in Orb(x) \Rightarrow Orb(y) \subseteq Orb(x)$  and  $yp^{m-n} = x \Rightarrow x \in Orb(y) \Rightarrow Orb(x) \subseteq Orb(y)$ . Hence  $Orb(x) = Orb(y)$ . Also each  $x \in T_{(\beta, \gamma)}$  belongs to an orbit, namely  $x \in Orb(x)$ . Hence the orbits are disjoint, nonempty and their union is all of the set  $T_{(\beta, \gamma)}$ . For each fixed  $x \in T_{(\beta, \gamma)}$  define

$$\pi: Orb(x) \rightarrow Orb(x); (xp^n)\pi = xp^{1-n}.$$

Then  $\pi$  is well-defined, since  $xp^n = xp^m \Rightarrow xp^{n-m} = x \Rightarrow xp^{-m} = xp^{-n} \Rightarrow xp^{l-m} = xp^{l-n} \Rightarrow (xp^n)\pi = (xp^m)\pi$ . Also,  $\pi$  is a permutation of  $Orb(x)$  with  $\pi^2 = 1$ , since for each  $xp^n \in Orb(x)$  we have  $((xp^n)\pi)\pi = (xp^{1-n})\pi = xp^{1-(1-n)} = xp^n$ . Now define

$$\pi: T_{(\beta, \gamma)} \rightarrow T_{(\beta, \gamma)}; (xp^n)\pi = xp^{1-n}$$

orbit by orbit. Then, since  $\{Orb(x)|x \in T_{(\beta, \gamma)}\}$  forms a partition of  $T_{(\beta, \gamma)}$ ,  $\pi$  is a well-defined permutation of  $T_{(\beta, \gamma)}$  with  $\pi^2 = 1$ , the identity permutation of  $T_{(\beta, \gamma)}$ . Hence, using the definition of  $p$  in lemma 9, we obtain an action of the two-element cyclic group  $\{1, \pi\}$  on  $T_{(\beta, \gamma)}$  as follows. For all  $(\underline{m}, \alpha)$  in  $\mathbf{Z}_N]S_3$  define

$$\begin{aligned} ((-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma)p)1 &= (-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma)p \\ ((0, \beta+\gamma)p)1 &= (0, \beta+\gamma)p \\ (((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma)p)1 &= ((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma)p \end{aligned}$$

and

$$\begin{aligned} ((-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma)p)\pi &= (-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma) \\ ((0, \beta+\gamma)p)\pi &= (0, \beta+\gamma) \\ (((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma)p)\pi &= ((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma). \end{aligned}$$

Now, using the definition of  $p$  in lemma 9, the action of  $\{1, \pi\}$  on  $T_{(\beta, \gamma)}$  may be rewritten

$$\begin{aligned} ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma)1 &= ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma) \\ (0, \beta+\gamma)1 &= (0, \beta+\gamma) \\ (-\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma)1 &= (-\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma) \end{aligned}$$

and

$$\begin{aligned} ((\underline{m}, \alpha)\varphi_iR(\gamma), \beta+\gamma)\pi &= (-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta+\gamma) \\ (0, \beta+\gamma)\pi &= (0, \beta+\gamma) \\ (-\underline{m}, \alpha)R(\beta)\varphi_i, \beta+\gamma)\pi &= ((\underline{m}, \alpha)\varphi_iR(\beta), \beta+\gamma) \end{aligned}$$

for all  $(\underline{m}, \alpha)$  in  $\mathbf{Z}_N]S_3$ , as in the statement of this lemma. To verify that the action of  $\{1, \pi\}$  on  $T_{(\beta, \gamma)}$  is faithful, note that

$$\begin{aligned} 1: T_{(\beta, \gamma)} &\rightarrow T_{(\beta, \gamma)}; x \rightarrow x \\ \pi: T_{(\beta, \gamma)} &\rightarrow T_{(\beta, \gamma)}; x \rightarrow x\pi \end{aligned}$$

are permutations of the set  $T_{(\beta, \gamma)}$ . If  $\theta \in \{1, \pi\}$  and  $\theta$  belongs to the kernel of the action then  $x\theta = x$  for all  $x \in T_{(\beta, \gamma)}$ . Then  $\theta = 1$ , since  $\pi$  moves  $((0, 1)\varphi_iR(\gamma), \beta+\gamma)$  to  $(-\underline{0}, 1)R(\gamma)\varphi_i, \beta+\gamma)$  which are distinct elements of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$ .  $\square$

**CASE 2.** Suppose  $\beta = \gamma$ . Note that in the labelling of the sectors of the sheets of the

$t$ -Riemann surface in figures 4 and 5,  $R(\beta) = R(\gamma)$  and  $\beta + \gamma = 2\beta$  in the group algebra  $\mathbf{Z}S_3$ .

**13. LEMMA.** *Referring to lemma 8, fix a common representative  $\varphi_i$  of the left and right cosets of  $S_3$  in  $\text{Sym}(\mathbf{Z}_N]S_3)$ . Fix a pair  $(\beta, \beta) \in S_3 \times S_3$ . Referring to lemma 5, define a subset  $T_{(\beta, \beta)}$  of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$  as follows:*

$$T_{(\beta, \beta)} = \left\{ ((\underline{m}, \alpha), 2\beta) \mid (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3 \right\} \cup \left\{ (0, 2\beta) \right\} \cup \left\{ (-\underline{m}, \alpha), 2\beta \mid (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3 \right\}.$$

Referring to the preceding discussion, consider the composite function

$$z \rightarrow t = z^2 \rightarrow w = t^{12} = z^{24}$$

of the complex  $z$ -plane to the  $w$ -Riemann surface. There is a copy of the set  $T_{(\beta, \beta)}$  on the upper sheet and a copy of the set  $T_{(\beta, \beta)}$  on the lower sheet of the  $t$ -Riemann surface according to the labels of the sectors in figures 4 and 5. Note that in this case  $R(\beta) = R(\gamma)$  and  $\beta + \gamma = 2\beta$  with the branch point labelled by the element  $(0, 2\beta)$  of both copies. The rotation of the  $z$ -plane by  $\pi$  radians induces a permutation

$$p: T_{(\beta, \beta)} \rightarrow T_{(\beta, \beta)}$$

given by

$$\begin{aligned} (-\underline{m}, \alpha)R(\beta)\varphi_i, 2\beta)p &= ((\underline{m}, \alpha)\varphi_iR(\beta), 2\beta) \\ (0, 2\beta)p &= (0, 2\beta) \\ ((\underline{m}, \alpha)\varphi_iR(\beta), 2\beta)p &= (-\underline{m}, \alpha)R(\beta)\varphi_i, 2\beta \end{aligned}$$

for all  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$ , such that each point of the copy of  $T_{(\beta, \beta)}$  on the upper sheet moves continuously along a circular curve that winds exactly once around the branch point, to the point superposed directly below it on the copy of  $T_{(\beta, \beta)}$  on the lower sheet of the  $t$ -Riemann surface. Then  $p = p^{-1}$  so that  $\langle p \rangle = \{1, p\}$  is a two-element cyclic subgroup of the full permutation group  $\text{Sym}(T_{(\beta, \beta)})$  and  $\langle p \rangle$  acts faithfully on the set  $T_{(\beta, \beta)}$ .

PROOF: As in the proof of lemma 9,  $T_{(\beta, \beta)}$  is seen to be a well-defined subset of  $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$  by setting the appropriate coefficients to zero in a typical element as described in lemma 5. Both  $\varphi_iR(\beta)$ ,  $R(\beta)\varphi_i$  are permutations of the set  $\mathbf{Z}_N]S_3$  and the rotation of the  $z$ -plane by  $\pi$  radians clearly induces a permutation  $p$  of the set  $T_{(\beta, \beta)}$  as described. Furthermore, it is clear from the definition that  $p = p^{-1}$  by chasing elements of  $T_{(\beta, \beta)}$ . Then  $\langle p \rangle = \{1, p\}$  as a subgroup of  $\text{Sym}(T_{(\beta, \beta)})$  and  $\langle p \rangle$  acts faithfully on the set  $T_{(\beta, \beta)}$ .  $\square$

**14. LEMMA.** *Referring to lemma 13, let  $1: C \rightarrow C$ ;  $z \rightarrow z$  denote the identity and*

$\pi: \mathbb{C} \rightarrow \mathbb{C}; z \rightarrow -z$  denote the rotation through an angle of  $\pi$  radians of the  $z$ -plane. Then there is a well-defined action of the two-element cyclic group  $\{1, \pi\}$  on the set  $T_{(\beta, \beta)}$  given by

$$\begin{aligned} ((\underline{m}, \alpha)\varphi_i R(\beta), 2\beta)1 &= ((\underline{m}, \alpha)\varphi_i R(\beta), 2\beta) \\ (0, 2\beta)1 &= (0, 2\beta) \\ (-\underline{m}, \alpha)R(\beta)\varphi_i, 2\beta)1 &= (-\underline{m}, \alpha)R(\beta)\varphi_i, 2\beta) \end{aligned}$$

and

$$\begin{aligned} ((\underline{m}, \alpha)\varphi_i R(\beta), 2\beta)\pi &= (-\underline{m}, \alpha)R(\beta)\varphi_i, 2\beta) \\ (0, 2\beta)\pi &= (0, 2\beta) \\ (-\underline{m}, \alpha)R(\beta)\varphi_i, 2\beta)\pi &= ((\underline{m}, \alpha)\varphi_i R(\beta), 2\beta) \end{aligned}$$

for all  $(\underline{m}, \alpha)$  in  $\mathbf{Z}_N]S_3$ . This action is faithful.

PROOF: The isomorphism  $1 \rightarrow 1, p \rightarrow \pi$  of the two-element cyclic groups  $\{1, p\}$  and  $\{1, \pi\}$  establishes the lemma.  $\square$

## VI. MAIN CONSTRUCTION

**RÉSUMÉ.** Let us review the final goal. Recall the definition made in section I. We have defined  $N$  to be the minimal number of colours required to properly colour any map from the class of all maps on the sphere. We know that  $4 \leq N \leq 6$ . We have chosen a specific map  $\mathbf{m}(N)$  on the sphere which requires all of the  $N$  colours  $0, 1, \dots, N-1$  to properly colour it. The map  $\mathbf{m}(N)$  has been properly coloured and the regions of  $\mathbf{m}(N)$  partitioned into disjoint, nonempty equivalence classes  $\underline{0}, \underline{1}, \dots, \underline{N-1}$  according to the colour they receive. The set  $\{\underline{0}, \underline{1}, \dots, \underline{N-1}\}$  is endowed with the structure of the cyclic group  $\mathbf{Z}_N$  under addition modulo  $N$ . In section III we have built the split extension  $\mathbf{Z}_N]S_3$ . The underlying set  $\mathbf{Z}_N]S_3$  of cardinality  $6N$  is taken to be the point set of a Steiner system  $S(N+1, 2N, 6N)$  which will be constructed in this section. We are required to define the blocks of size  $2N$  and show that every set of  $N+1$  points is contained in a unique block. Once this goal is achieved, lemma 3 shows that  $N \leq 4$ .

**15. LEMMA.** Let  $\mathbf{Z}_N]S_3$  denote the split extension defined in lemma 4 and  $\text{Sym}(\mathbf{Z}_N]S_3)$  denote the full permutation group on the set  $\mathbf{Z}_N]S_3$ . Define

$$\mu: \text{Sym}(\mathbf{Z}_N]S_3) \rightarrow \text{Sym}(\mathbf{Z}_N]S_3)$$

by

$$\psi = R(\gamma)\varphi_i \rightarrow \varphi_i R(\gamma) = \psi^\mu.$$

Then  $\mu$  is a bijection of the set  $\text{Sym}(\mathbf{Z}_N]S_3)$  with itself.

PROOF: Referring to lemma 8,  $\mu$  is well-defined since each  $\psi \in \text{Sym}(\mathbf{Z}_N]S_3)$  may be written uniquely as  $\psi = R(\gamma)\phi_i$  for some  $\gamma \in S_3$  and some  $\phi_i$ . Then  $\mu$  is a surjection because for any  $\psi \in \text{Sym}(\mathbf{Z}_N]S_3)$  one may also write  $\psi = \phi_i R(\gamma)$  uniquely for some  $\gamma \in S_3$  and some  $\phi_i$ , whence  $R(\gamma)\phi_i \rightarrow \phi_i R(\gamma) = \psi$ . Since  $\text{Sym}(\mathbf{Z}_N]S_3)$  is a finite set,  $\mu$  must be a bijection by counting.  $\square$

**16. LEMMA.** *Define the set  $G$  as follows:*

$$G = \left\{ \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} \middle| \psi \in \text{Sym}(\mathbf{Z}_N]S_3) \right\} = \left\{ \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \middle| \begin{matrix} \gamma \in S_3 \\ i = 1, \dots, k \end{matrix} \right\}.$$

*Define multiplication in  $G$  as follows:*

$$\begin{pmatrix} \psi_1 \\ \psi_1^\mu \end{pmatrix} \begin{pmatrix} \psi_2 \\ \psi_2^\mu \end{pmatrix} = \begin{pmatrix} (\psi_1 \psi_2) \\ (\psi_1 \psi_2)^\mu \end{pmatrix}$$

*i.e.*

$$\begin{pmatrix} R(\gamma_1)\phi_{i_1} \\ \phi_{i_1} R(\gamma_1) \end{pmatrix} \begin{pmatrix} R(\gamma_2)\phi_{i_2} \\ \phi_{i_2} R(\gamma_2) \end{pmatrix} = \begin{pmatrix} R(\gamma_3)\phi_{i_3} \\ \phi_{i_3} R(\gamma_3) \end{pmatrix}$$

*where  $R(\gamma_3)\phi_{i_3}$  is the unique expression for  $R(\gamma_1)\phi_{i_1}R(\gamma_2)\phi_{i_2}$  according to the right coset decomposition of  $S_3$  in  $\text{Sym}(\mathbf{Z}_N]S_3)$ . Then  $G$  is a group.*

PROOF: Referring to lemma 8 and lemma 15, the set  $G$  is well-defined by the decomposition of  $\text{Sym}(\mathbf{Z}_N]S_3)$  into the left and right cosets of  $S_3$  by the  $\phi_i$ . Define

$$\mu': \text{Sym}(\mathbf{Z}_N]S_3) \rightarrow G; \psi \rightarrow \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix}.$$

Then  $\mu'$  is a well-defined bijection of the set  $\text{Sym}(\mathbf{Z}_N]S_3)$  with  $G$  since  $\mu$  is a bijection by lemma 15. The definition of multiplication in  $G$  mirrors the multiplication in  $\text{Sym}(\mathbf{Z}_N]S_3)$  via  $\mu'$  and is designed to make  $G$  a group and  $\mu'$  an isomorphism.  $\square$

**17. LEMMA.** *Consider the set  $\mathbf{Z}_N]S_3$  and let*

$$\begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} = \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \in G.$$

*Define*

$$\uparrow \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix}: \mathbf{Z}_N]S_3 \rightarrow \mathbf{Z}_N]S_3 \text{ by}$$

$$(\underline{m}, \alpha) \rightarrow (\underline{m}, \alpha) \uparrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha) \uparrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} = (\underline{m}, \alpha) R(\gamma)\phi_i.$$

Define

$$\downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix}: \mathbf{Z}_N]S_3 \rightarrow \mathbf{Z}_N]S_3 \text{ by}$$

$$(\underline{m}, \alpha) \rightarrow (\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha) \downarrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} = (\underline{m}, \alpha)\phi_i R(\gamma).$$

Then

$$(\underline{m}, \alpha) \uparrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \text{ for all } (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3.$$

Both  $\uparrow$  and  $\downarrow$  are well-defined, faithful and  $|\mathbf{Z}_N]S_3|$ -transitive right actions of the group  $G$  on the set  $\mathbf{Z}_N]S_3$ .

PROOF: Referring to lemma 12 and lemma 14, put  $\beta = 1$ . Working in the set  $T_{(1, \gamma)}$ , for each  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$  we have

$$\begin{aligned} & ((\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix}, 1+\gamma) \\ &= ((\underline{m}, \alpha) \downarrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix}, 1+\gamma) \\ &= ((\underline{m}, \alpha)\phi_i R(\gamma), 1+\gamma) \\ &= (-\underline{m}, \alpha)R(\gamma)\phi_i, 1+\gamma)\pi \\ &= (-\underline{m}, \alpha\gamma)\phi_i, 1+\gamma)\pi \\ &= (-\underline{m}, \alpha\gamma)R(1)\phi_i, 1+\gamma)\pi \\ &= (\underline{m}, \alpha\gamma)\phi_i R(1), 1+\gamma) \\ &= (\underline{m}, \alpha\gamma)\phi_i, 1+\gamma) \\ &= (\underline{m}, \alpha)R(\gamma)\phi_i, 1+\gamma) \\ &= ((\underline{m}, \alpha) \uparrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix}, 1+\gamma) \\ &= ((\underline{m}, \alpha) \uparrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix}, 1+\gamma) \end{aligned}$$

using the action of the two-element cyclic group  $\{1, \pi\}$  on the set  $T_{(1, \gamma)}$  according to lemma 12 and lemma 14. Hence

$$(\underline{m}, \alpha) \uparrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \text{ for all } (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3.$$

Since the action  $\uparrow$  is the usual action of  $Sym(\mathbf{Z}_N]S_3)$  on the set  $\mathbf{Z}_N]S_3$ , it is faithful and  $|\mathbf{Z}_N]S_3|$ -transitive. By the last equality, so is the  $\downarrow$  action.  $\square$

**18. LEMMA.** *Let  $(\underline{m}_1, \alpha_1), \dots, (\underline{m}_r, \alpha_r)$  be any  $r$  distinct elements of  $\mathbf{Z}_N]S_3$  and let  $(\underline{n}_1, \beta_1), \dots, (\underline{n}_s, \beta_s)$  be any  $s$  distinct elements of  $\mathbf{Z}_N]S_3$ . Let*

$$H_{r, s} = \left\{ \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in G \left| \begin{array}{l} (\underline{m}_i, \alpha_i) \uparrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}_i, \alpha_i) \text{ for } i = 1, \dots, r \text{ and} \\ (\underline{n}_j, \beta_j) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{n}_j, \beta_j) \text{ for } j = 1, \dots, s \end{array} \right. \right\}$$

then  $H_{r, s}$  is a subgroup of  $G$ .

PROOF: Note that if  $\psi = R(\gamma)\varphi_i = 1$  then  $\varphi_i = R(\gamma)^{-1}$  so that  $\psi^\mu = \varphi_i R(\gamma) = R(\gamma)^{-1} R(\gamma) = 1$ . Then

$$\begin{pmatrix} 1 \\ 1^\mu \end{pmatrix} \in H_{r, s}$$

since

$$(\underline{m}_i, \alpha_i) \uparrow \begin{pmatrix} 1 \\ 1^\mu \end{pmatrix} = (\underline{m}_i, \alpha_i) 1 = (\underline{m}_i, \alpha_i)$$

for  $i = 1, \dots, r$  and

$$(\underline{n}_j, \beta_j) \downarrow \begin{pmatrix} 1 \\ 1^\mu \end{pmatrix} = (\underline{n}_j, \beta_j) 1^\mu = (\underline{n}_j, \beta_j) 1 = (\underline{n}_j, \beta_j)$$

for  $j = 1, \dots, s$ . If

$$\begin{pmatrix} \Psi_1 \\ \Psi_1^\mu \end{pmatrix} \text{ and } \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} \in H_{r, s}$$

then

$$\begin{aligned} (\underline{m}_i, \alpha_i) \uparrow \left( \begin{pmatrix} \Psi_1 \\ \Psi_1^\mu \end{pmatrix} \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} \right) &= (\underline{m}_i, \alpha_i) \uparrow \begin{pmatrix} \Psi_1 \\ \Psi_1^\mu \end{pmatrix} \uparrow \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} \\ &= (\underline{m}_i, \alpha_i) \uparrow \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} = (\underline{m}_i, \alpha_i) \text{ for } i = 1, \dots, r \end{aligned}$$

and

$$\begin{aligned} (\underline{n}_j, \beta_j) \downarrow \left( \begin{pmatrix} \Psi_1 \\ \Psi_1^\mu \end{pmatrix} \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} \right) &= (\underline{n}_j, \beta_j) \downarrow \begin{pmatrix} \Psi_1 \\ \Psi_1^\mu \end{pmatrix} \downarrow \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} \\ &= (\underline{n}_j, \beta_j) \downarrow \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} = (\underline{n}_j, \beta_j) \text{ for } j = 1, \dots, s. \end{aligned}$$

Hence

$$\begin{pmatrix} \Psi_1 \\ \Psi_1^\mu \end{pmatrix} \begin{pmatrix} \Psi_2 \\ \Psi_2^\mu \end{pmatrix} \in H_{r,s}$$

Since  $G$  is finite,  $H_{r,s}$  is a subgroup of  $G$ .  $\square$

Note that  $\mathbf{Z}_N$  is embedded as the subgroup  $\{(\underline{m}, 1) | \underline{m} \in \mathbf{Z}_N\}$  in  $\mathbf{Z}_N]S_3$  and  $S_3$  is embedded as the subgroup  $\{(\underline{0}, \alpha) | \alpha \in S_3\}$  in  $\mathbf{Z}_N]S_3$ . Since  $\mathbf{Z}_N]S_3 = \mathbf{Z}_N \times S_3$  is the direct product of groups by lemma 4, both  $\mathbf{Z}_N$  and  $S_3$  are normal subgroups. Recall the notation

$$S_3 = \langle \sigma, \rho \rangle = \{1, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}.$$

**19. LEMMA.** *Define*

$$H = \left\{ \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in G \left| \begin{array}{l} (\underline{m}, 1) \uparrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, 1) \text{ for all } \underline{m} \in \mathbf{Z}_N \text{ and} \\ (\underline{0}, \sigma) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{0}, \sigma) \end{array} \right. \right\}.$$

Then given

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in H$$

either

$$(\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha) \text{ for all } (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$$

or

$$(\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha^\sigma) \text{ for all } (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3.$$

PROOF:  $H$  is a well-defined subgroup of  $G$  according to lemma 18. Let

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = \begin{pmatrix} R(\gamma)\varphi_i \\ \varphi_i R(\gamma) \end{pmatrix} \in H$$

and  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$  be given. Referring to lemmas 12 and 14, put  $\beta = \gamma^{-1}\alpha\gamma$ . Working in the set  $T_{(\beta, \gamma)}$  we have

$$\begin{aligned} & ((\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix}, \beta + \gamma) \\ &= (\underline{m}, \alpha) \downarrow \begin{pmatrix} R(\gamma)\varphi_i \\ \varphi_i R(\gamma) \end{pmatrix}, \beta + \gamma) \\ &= (\underline{m}, \alpha)\varphi_i R(\gamma), \beta + \gamma) \\ &= (-\underline{m}, \alpha)R(\gamma)\varphi_i, \beta + \gamma)\pi \\ &= (-\underline{m}, \alpha\gamma)\varphi_i, \beta + \gamma)\pi \\ &= (-\underline{m}, \gamma\beta)\varphi_i, \beta + \gamma)\pi \\ &= (-\underline{m}, \gamma)R(\beta)\varphi_i, \beta + \gamma)\pi \\ &= (\underline{m}, \gamma)\varphi_i R(\beta), \beta + \gamma) \\ &= (\underline{m}, 1)R(\gamma)\varphi_i R(\beta), \beta + \gamma) \\ &= (\underline{m}, 1)R(\beta), \beta + \gamma) \\ &= (\underline{m}, \beta), \beta + \gamma) \end{aligned}$$

using the definition of  $H$  and the action of the two-element cyclic group  $\{1, \pi\}$  on the set  $T_{(\beta, \gamma)}$ . Hence

$$(\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \beta) = (\underline{m}, \gamma^{-1}\alpha\gamma) = (\underline{m}, \alpha^\gamma).$$

Now since

$$(\underline{0}, \sigma) = (\underline{0}, \sigma) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{0}, \sigma^\gamma)$$

by hypothesis, we have  $\sigma = \sigma^\gamma$ . Hence  $\gamma\sigma = \sigma\gamma$  so that either  $\gamma = 1$  or  $\gamma = \sigma$ .  $\square$

**20. LEMMA.** *Let  $H$  be the subgroup of  $G$  defined in lemma 19. Then  $H$  is a nontrivial group of involutions of the set  $\mathbf{Z}_N]S_3$ . In particular, every nontrivial element of  $H$  is of order 2.*

PROOF: Define

$$\psi: \mathbf{Z}_N]S_3 \rightarrow \mathbf{Z}_N]S_3; (\underline{m}, \alpha) \rightarrow (\underline{m}, \alpha^\sigma).$$

Then

$$(\underline{m}, 1)\uparrow \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} = (\underline{m}, 1)\psi = (\underline{m}, 1^\sigma) = (\underline{m}, 1) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

and

$$(\underline{0}, \sigma)\downarrow \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} = (\underline{0}, \sigma)\uparrow \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} = (\underline{0}, \sigma)\psi = (\underline{0}, \sigma^\sigma) = (\underline{0}, \sigma).$$

Now  $\psi \neq 1$ , so

$$\begin{pmatrix} 1 \\ 1^\mu \end{pmatrix} \neq \begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} \in H,$$

hence  $H$  is nontrivial. To show that each nontrivial element of  $H$  is of order 2, let

$$\begin{pmatrix} \psi \\ \psi^\mu \end{pmatrix} = \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \in H.$$

Then by the proof of lemma 19,  $\gamma = 1$  or  $\gamma = \sigma$ . In particular  $\gamma^2 = 1$ . Hence, for any  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$

$$\begin{aligned} & (\underline{m}, \alpha)\downarrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix}^2 \\ &= (\underline{m}, \alpha)\downarrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \downarrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \\ &= (\underline{m}, \alpha^\gamma)\downarrow \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \\ &= (\underline{m}, (\alpha^\gamma)^\gamma) = (\underline{m}, \alpha). \end{aligned}$$

Since the  $\downarrow$  action of  $G$  on the set  $\mathbf{Z}_N]S_3$  is faithful,

$$\begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix}^2 = \begin{pmatrix} 1 \\ 1^\mu \end{pmatrix}$$

the identity element of  $G$ .  $\square$

**21. LEMMA.** Denote the right cosets of  $\mathbf{Z}_N$  in  $\mathbf{Z}_N]S_3$  by

$$\mathbf{Z}_N, \mathbf{Z}_{N\rho}, \mathbf{Z}_{N\rho^2}, \mathbf{Z}_{N\sigma}, \mathbf{Z}_{N\sigma\rho}, \mathbf{Z}_{N\sigma\rho^2}.$$

Define

$$\text{Fix}\downarrow(H) = \left\{ (\underline{m}, \alpha) \in \mathbf{Z}_N]S_3 \mid (\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha) \text{ for all } \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in H \right\}.$$

Then  $\text{Fix}\downarrow(H) = \{(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3 \mid \alpha = 1 \text{ or } \alpha = \sigma\}$ . The  $\downarrow$  action of a nontrivial element of  $H$  transposes the coset  $\mathbf{Z}_{N\rho}$  with the coset  $\mathbf{Z}_{N\rho^2}$  and transposes the coset  $\mathbf{Z}_{N\sigma\rho}$  with the coset  $\mathbf{Z}_{N\sigma\rho^2}$ .

PROOF: By lemmas 19 and 20, the elements

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in H$$

are of two kinds:

(i)  $(\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha)$  for all  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$

in which case

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = \begin{pmatrix} 1 \\ 1^\mu \end{pmatrix}$$

the identity element of  $H$ , and

(ii)  $(\underline{m}, \alpha) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \alpha^\sigma)$  for all  $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$

in which case

$$\begin{pmatrix} 1 \\ 1^\mu \end{pmatrix} \neq \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix}$$

is an element of order 2 in  $H$ . In the second case, compute according to the cosets of  $\mathbf{Z}_N$  in  $\mathbf{Z}_N]S_3$ :

$$(\underline{m}, 1) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, 1^\sigma) = (\underline{m}, 1) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

$$(\underline{m}, \sigma) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \sigma^\sigma) = (\underline{m}, \sigma) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

$$(\underline{m}, \rho) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, \rho^\sigma) = (\underline{m}, \rho^2) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

$$(\underline{m}, \rho^2) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, (\rho^2)^\sigma) = (\underline{m}, \rho) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

$$(\underline{m}, \sigma\rho) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, (\sigma\rho)^\sigma) = (\underline{m}, \sigma\rho^2) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

$$(\underline{m}, \sigma\rho^2) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}, (\sigma\rho^2)^\sigma) = (\underline{m}, \sigma\rho) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

and the lemma follows.  $\square$

**22. LEMMA.** *Let  $\text{Norm}_G(H)$  denote the normalizer of  $H$  in  $G$ . The action  $\downarrow$  of  $G$  on  $\mathbf{Z}_N]S_3$  restricts to an action  $\downarrow$  of  $\text{Norm}_G(H)$  on  $\text{Fix}\downarrow(H)$  which is  $(|\mathbf{Z}_N|+1)$ -transitive.*

PROOF: Let

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in G.$$

First show that

$$\text{Fix}\downarrow \left( \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} H \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right) = \text{Fix}\downarrow(H) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix}$$

as follows:

$$\begin{aligned} (\underline{m}, \alpha) &\in \text{Fix}\downarrow \left( \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} H \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right) \\ \Leftrightarrow (\underline{m}, \alpha) &\downarrow \left( \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} \begin{pmatrix} \Psi^* \\ \Psi^{*\mu} \end{pmatrix} \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right) = (\underline{m}, \alpha) \text{ for all } \begin{pmatrix} \Psi^* \\ \Psi^{*\mu} \end{pmatrix} \in H \end{aligned}$$

$$\begin{aligned} &\Leftrightarrow (\underline{m}, \alpha) \downarrow \left( \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} \begin{pmatrix} \Psi^* \\ \Psi^{*\mu} \end{pmatrix} \right) = (\underline{m}, \alpha) \downarrow \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} \text{ for all } \begin{pmatrix} \Psi^* \\ \Psi^{*\mu} \end{pmatrix} \in H \\ &\Leftrightarrow (\underline{m}, \alpha) \downarrow \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} \downarrow \begin{pmatrix} \Psi^* \\ \Psi^{*\mu} \end{pmatrix} = (\underline{m}, \alpha) \downarrow \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} \text{ for all } \begin{pmatrix} \Psi^* \\ \Psi^{*\mu} \end{pmatrix} \in H \\ &\Leftrightarrow (\underline{m}, \alpha) \downarrow \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} \in \text{Fix} \downarrow (H) \\ &\Leftrightarrow (\underline{m}, \alpha) \in \text{Fix} \downarrow (H) \downarrow \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right). \end{aligned}$$

Now let

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in \text{Norm}_G(H) = \left\{ \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in G \mid \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} H \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = H \right\}.$$

Then

$$\text{Fix} \downarrow (H) = \text{Fix} \downarrow \left( \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)^{-1} H \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right) = \text{Fix} \downarrow (H) \downarrow \left( \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \right)$$

showing that the action restricts to an action of  $\text{Norm}_G(H)$  on  $\text{Fix} \downarrow (H)$ . Now to show that the action  $\downarrow$  of  $\text{Norm}_G(H)$  on  $\text{Fix} \downarrow (H) = \mathbf{Z}_N \cup \mathbf{Z}_N \sigma$  is  $(|\mathbf{Z}_N|+1)$ -transitive, label the elements of  $\mathbf{Z}_N$  as  $(\underline{m}_1, \alpha_1), \dots, (\underline{m}_N, \alpha_N)$  and label  $(\mathbf{0}, \sigma) = (\underline{m}_{N+1}, \alpha_{N+1})$ . Let  $(\underline{m}^*_1, \alpha^*_1), \dots, (\underline{m}^*_{N+1}, \alpha^*_{N+1})$  be any  $|\mathbf{Z}_N|+1$  distinct points of  $\text{Fix} \downarrow (H)$ . It is enough to show that there exists

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in \text{Norm}_G(H)$$

such that

$$(\underline{m}^*_i, \alpha^*_i) \downarrow \begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} = (\underline{m}_i, \alpha_i) \text{ for } i = 1, \dots, N+1.$$

Now there exists

$$\begin{pmatrix} \Psi \\ \Psi^\mu \end{pmatrix} \in G$$

such that

$$(\underline{m}_i^*, \alpha_i^*) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) = (\underline{m}_i, \alpha_i) \text{ for } i = 1, \dots, N+1.$$

Hence

$$(\underline{m}_i^*, \alpha_i^*) = (\underline{m}_i, \alpha_i) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \text{ for } i = 1, \dots, N+1.$$

Note that for every

$$\left( \begin{array}{c} \Psi^* \\ \Psi^{\mu*} \end{array} \right) \in H$$

and for  $i = 1, \dots, N+1$ :

$$\begin{aligned} & (\underline{m}_i, \alpha_i) \downarrow \left( \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \left( \begin{array}{c} \Psi^* \\ \Psi^{\mu*} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \right) \\ &= (\underline{m}_i, \alpha_i) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \downarrow \left( \begin{array}{c} \Psi^* \\ \Psi^{\mu*} \end{array} \right) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \\ &= (\underline{m}_i^*, \alpha_i^*) \downarrow \left( \begin{array}{c} \Psi^* \\ \Psi^{\mu*} \end{array} \right) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \\ &= (\underline{m}_i^*, \alpha_i^*) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \end{aligned}$$

$$= (\underline{m}_i, \alpha_i).$$

Hence

$$\left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \left( \begin{array}{c} \Psi^* \\ \Psi^{\mu*} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \in H \text{ for all } \left( \begin{array}{c} \Psi^* \\ \Psi^{\mu*} \end{array} \right) \in H \Rightarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \in \text{Norm}_G(H). \square$$

**23. LEMMA.** *There exists a Steiner system  $S(N+1, 2N, 6N)$ , where the points are the elements of the set  $\mathbf{Z}_N]S_3$  and the set of blocks is*

$$\left\{ \text{Fix} \downarrow (H) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \mid \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \in G \right\}.$$

PROOF: There are  $6N = |\mathbf{Z}_N]S_3|$  points. Each block, for a fixed

$$\left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \in G$$

contains

$$2N = |\mathbf{Z}_N \cup \mathbf{Z}_N \sigma| = |\text{Fix} \downarrow(H)| = \left| \text{Fix} \downarrow(H) \downarrow \left( \begin{matrix} \Psi \\ \Psi^\mu \end{matrix} \right) \right|$$

points. Label the elements of  $\mathbf{Z}_N$  as  $(\underline{m}_1, \alpha_1), \dots, (\underline{m}_N, \alpha_N)$  and label  $(\underline{0}, \sigma) = (\underline{m}_{N+1}, \alpha_{N+1})$ . Let  $(\underline{m}^*_1, \alpha^*_1), \dots, (\underline{m}^*_{N+1}, \alpha^*_{N+1})$  be any  $|\mathbf{Z}_N|+1$  distinct points of  $\mathbf{Z}_N]S_3$ . Then there exists

$$\left( \begin{matrix} \Psi \\ \Psi^\mu \end{matrix} \right) \in G$$

such that

$$(\underline{m}_i, \alpha_i) \downarrow \left( \begin{matrix} \Psi \\ \Psi^\mu \end{matrix} \right) = (\underline{m}^*_i, \alpha^*_i) \text{ for } i = 1, \dots, N+1.$$

Hence, there is at least one block, namely  $\text{Fix} \downarrow(H)$ , that contains the points  $(\underline{m}^*_1, \alpha^*_1), \dots, (\underline{m}^*_{N+1}, \alpha^*_{N+1})$ . It remains to show that this is the unique block that contains the points  $(\underline{m}^*_1, \alpha^*_1), \dots, (\underline{m}^*_{N+1}, \alpha^*_{N+1})$ . Suppose  $(\underline{m}^*_1, \alpha^*_1), \dots, (\underline{m}^*_{N+1}, \alpha^*_{N+1})$  are contained in

$$\text{Fix} \downarrow(H) \downarrow \left( \begin{matrix} \Psi^* \\ \Psi^{*\mu} \end{matrix} \right) \text{ for some } \left( \begin{matrix} \Psi^* \\ \Psi^{*\mu} \end{matrix} \right) \in G.$$

Then there exist points  $(\underline{m}^{**}_1, \alpha^{**}_1), \dots, (\underline{m}^{**}_{N+1}, \alpha^{**}_{N+1})$  in  $\text{Fix} \downarrow(H)$  such that

$$(\underline{m}^*_i, \alpha^*_i) = (\underline{m}^{**}_i, \alpha^{**}_i) \downarrow \left( \begin{matrix} \Psi^* \\ \Psi^{*\mu} \end{matrix} \right) \text{ for } i = 1, \dots, N+1.$$

By lemma 22, there exists

$$\left( \begin{matrix} \Psi^{**} \\ \Psi^{**\mu} \end{matrix} \right) \in \text{Norm}_G(H)$$

such that

$$(\underline{m}^{**}_i, \alpha^{**}_i) = (\underline{m}_i, \alpha_i) \downarrow \left( \begin{matrix} \Psi^{**} \\ \Psi^{**\mu} \end{matrix} \right) \text{ for } i = 1, \dots, N+1.$$

Hence for  $i = 1, \dots, N+1$

$$\begin{aligned}
 & (\underline{m}_i, \alpha_i) \downarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \\
 &= (\underline{m}_i^*, \alpha_i^*) \\
 &= (\underline{m}_i^{**}, \alpha_i^{**}) \downarrow \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \\
 &= (\underline{m}_i, \alpha_i) \downarrow \left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right) \downarrow \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \\
 &\Rightarrow (\underline{m}_i, \alpha_i) = (\underline{m}_i, \alpha_i) \downarrow \left( \left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right) \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \right) \text{ for } i = 1, \dots, N+1.
 \end{aligned}$$

Then by lemma 17

$$(\underline{m}_i, \alpha_i) = (\underline{m}_i, \alpha_i) \uparrow \left( \left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right) \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \right) \text{ for } i = 1, \dots, N$$

and

$$(\underline{m}_{N+1}, \alpha_{N+1}) = (\underline{m}_{N+1}, \alpha_{N+1}) \downarrow \left( \left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right) \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \right).$$

Hence

$$\left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right) \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \in H.$$

Now  $H$  is a subgroup of  $Norm_G(H)$

$$\begin{aligned}
 &\Rightarrow \left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right) \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \in Norm_G(H) \\
 &\Rightarrow \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \in \left( \begin{array}{c} \Psi^{**} \\ \Psi^{**\mu} \end{array} \right)^{-1} Norm_G(H) = Norm_G(H) \\
 &\Rightarrow \left( \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \right) H \left( \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} \right)^{-1} = H \\
 &\Rightarrow \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right) \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} H \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right)^{-1} = H \\
 &\Rightarrow \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right)^{-1} H \left( \begin{array}{c} \Psi \\ \Psi^\mu \end{array} \right) = \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right)^{-1} H \left( \begin{array}{c} \Psi^* \\ \Psi^{*\mu} \end{array} \right).
 \end{aligned}$$

Now, using the first fact in the proof of lemma 22

$$\begin{aligned}
 & \text{Fix}\downarrow(H)\downarrow\left(\begin{array}{c} \Psi^* \\ \Psi^*\mu \end{array}\right) \\
 &= \text{Fix}\downarrow\left(\left(\begin{array}{c} \Psi^* \\ \Psi^*\mu \end{array}\right)^{-1} H\left(\begin{array}{c} \Psi^* \\ \Psi^*\mu \end{array}\right)\right) \\
 &= \text{Fix}\downarrow\left(\left(\begin{array}{c} \Psi \\ \Psi^\mu \end{array}\right)^{-1} H\left(\begin{array}{c} \Psi \\ \Psi^\mu \end{array}\right)\right) \\
 &= \text{Fix}\downarrow(H)\downarrow\left(\begin{array}{c} \Psi \\ \Psi^\mu \end{array}\right).
 \end{aligned}$$

This establishes the uniqueness of the block.  $\square$

**24. THEOREM.** *Any map on the sphere can be properly coloured by using at most four colours.*

PROOF: Referring to section I, we have defined  $N$  to be the minimal number of colours required to properly colour any map from the class of all maps on the sphere. Based on the definition of  $N$ , we have selected a specific map  $\mathbf{m}(N)$  on the sphere which requires no fewer than  $N$  colours to be properly coloured. Based on the definition of the map  $\mathbf{m}(N)$  we have selected a proper colouring of its regions using the  $N$  colours  $0, 1, \dots, N-1$ . Working with the fixed number  $N$ , the fixed map  $\mathbf{m}(N)$ , and the fixed proper colouring of the regions of the map  $\mathbf{m}(N)$ , lemma 23 has explicitly constructed a Steiner system  $S(N+1, 2N, 6N)$ . Now lemma 3 implies that  $N$  cannot exceed four.  $\square$

## REFERENCES

### WEBSITES

1. **Canadian Mathematical Society** - A New Proof of The Four Colour Theorem by Ashay Dharwadker, Knot No.221, Knot a Braid of Links, 5 October 2000. <http://www.cms.math.ca/cgi/kabol/browse.pl?Number=221>
2. **The Math Forum** - A New Proof of The Four Colour Theorem by Ashay Dharwadker, Internet Mathematics Library, Group Theory and Graph Theory, 2000. <http://mathforum.org/library/view/16622.html>
3. **Tölvunot Fréttahorn** - Ný sönnun á setningunni um fjóra liti, Ashay Dharwadker, 2000. <http://www.tolvunot.is/adal.Frettahorn.htm>
4. **Four Color Theorem: A Brief Historical Insight** – An essay by Dominic Verderaime, 2005. <http://student.adams.edu/~verderaimedj/finalEssay/>
5. **Il Teorema dei Quattro Colori e la Teoria dei Grafi** - An article by Anita Pasotti, 2007. <http://www.matematicamente.it/magazine/ottobre2007/Numero04.pdf>

6. **Yahoo! Famous Mathematics Problems** - A New Proof of The Four Colour Theorem by Ashay Dharwadker, 2000. [http://dir.yahoo.com/Science/Mathematics/Problems\\_\\_Puzzles\\_\\_and\\_Games/Famous\\_Problems/Four\\_Color\\_Theorem/](http://dir.yahoo.com/Science/Mathematics/Problems__Puzzles__and_Games/Famous_Problems/Four_Color_Theorem/)
7. **The Witt Design** - The Steiner system  $S(5,8,24)$  explicitly computed by Ashay Dharwadker, 2002. <http://www.geocities.com/dharwadker/witt.html>
8. **Common Systems of Coset Representatives** - Proof of existence of common systems of representatives for the left and right cosets of a finite subgroup of a group by Ashay Dharwadker, 2005. <http://www.geocities.com/dharwadker/coset.html>

## BOOKS

9. AHLFORS, L.V. *Complex Analysis*, McGraw-Hill Book Company, 1979.
10. DHARWADKER, A. & PIRZADA, S. *Graph Theory*, Orient Longman and Universities Press of India, 2008.
11. LAM, T.Y. *A First Course in Noncommutative Rings*, Springer-Verlag, 1991.
12. ROTMAN, J.J. *An Introduction to the Theory of Groups*, Springer-Verlag, 1995.
13. VAN LINT, J.H. & WILSON, R.M. *A Course in Combinatorics*, Cambridge University Press, 1992.

## PAPERS

14. APPEL, K. & HAKEN, W. *Every Planar Map is Four Colorable*, Bull. Amer. Math. Soc. 82(711-712), 1976.
15. DHARWADKER, A. **Riemann Surfaces**, Electronic Geometry Models, Model 2002.05.001, 2003. [http://www.eg-models.de/models/Surfaces/Riemann\\_Surfaces/2002.05.001/\\_preview.html](http://www.eg-models.de/models/Surfaces/Riemann_Surfaces/2002.05.001/_preview.html)
16. DHARWADKER, A. & SMITH, J.D.H. *Split Extensions and Representations of Moufang Loops*, Comm. in Alg.23(11),4245-4255, 1995.
17. EILENBERG, S. *Extensions of General Algebras*, Ann.Soc.Polon.Math. 21, 1948.
18. EULER, L. *Elementa Doctrinae Solidorum*, Novi comment. acad. sci. Petrop., 4(109-140), 1752.
19. HALL, P. *On Representatives of Subsets*, J. London Math. Soc. 10, 26-30, 1935.
20. RIEMANN, G.F.B. *Grundlagen für eine allgemeine Theorie der Funktionen einer veränderlichen complexen Grösse*, 1851, Reprinted in Gesammelte Mathematische Werke, Dover, 1953.
21. TITS, J. *Sur les systèmes de Steiner associés aux trois grands groupes de Mathieu*, Rend. Math. e Appl.(5)23, 166-184, 1964.
22. WITT, E. *Die 5-fach transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg 12, 256-264, 1938.
23. NIEUWOUDT, I. **On the Maximum Degree Chromatic Number of a Graph**, Ph.D. Thesis, Department of Mathematical Sciences, Stellenbosch University, 2007.
24. DHARWADKER, A. & PIRZADA, S. **Applications of Graph Theory**, Journal of the Korean Society for Industrial and Applied Mathematics (KSIAM), Vol. 11, No. 4, 2007.