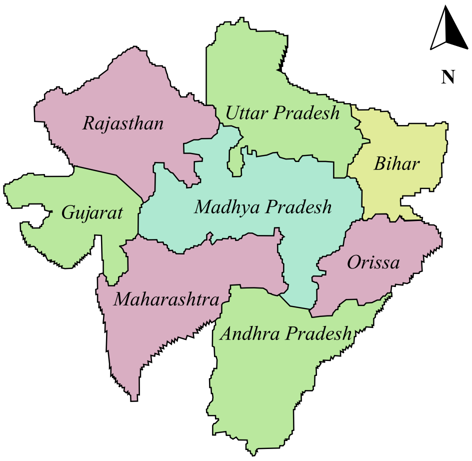
12. The Four Colour Theorem



Map of Madhya Pradesh and adjoining states in India, circa 2000

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.

The 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 chapter. In section 12.1 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 12.1 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 $\boldsymbol{m}(N)$ on the plane, which requires no fewer than N colours to be properly coloured.
- Based on the definition of the map $\boldsymbol{m}(N)$, select a proper colouring of the regions of the map $\boldsymbol{m}(N)$ using the N colours $0, 1, \dots, N-1$.

The whole proof works with the fixed number N, the fixed map $\boldsymbol{m}(N)$ and the fixed proper colouring of the regions of the map $\boldsymbol{m}(N)$. In Section 12.2, 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 12.3, we define *Eilenberg Modules*. The regions of the map $\boldsymbol{m}(N)$ are partitioned into disjoint, nonempty equivalence classes $0, 1, \dots, N-1$ according to the colour they receive. This set is given the structure of the cyclic group $\mathbf{Z}_N = \{0, 1, \dots, N-1\}$ 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 12.4 on *Hall Matchings*, we choose a common system of coset representatives for the left and right cosets of S_3 in the full symmetric group on $|Z_N]S_3|$ letters. In Section 12.5, for each such common representative and for each ordered pair of elements of S_3, on *Riemann surfaces*, we establish a certain action of the two-element cyclic group on twelve copies of the partitioned map $\boldsymbol{m}(N)$ by using the twenty-fourth root function of the sheets of the complex plane. In Section 12.6, we give the details of the *Main Construction* using this action. The $6N$ elements of $\mathbf{Z}_N]S_3$ are regarded as the set of points and Lemma 12.23 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.

12.1 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, this is equivalent to considering 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. Example of a map that requires four colours to be properly coloured is shown in Figure 12.1.

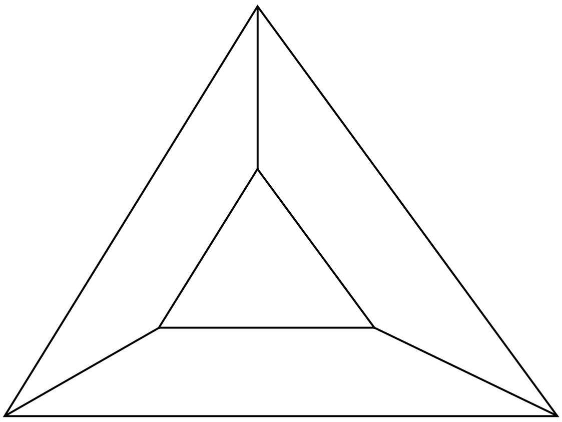


Fig. 12.1 *A map that requires four colours to be properly coloured*

Lemma 12.1 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 $V - E + F = 2$

$$\begin{array}{rrcl}
\Rightarrow & 6V-6E+6F & = & 12\\
\Rightarrow & 4E-6E+6F & = & 12\\
\Rightarrow & 6F-2E & = & 12\\
\Rightarrow & 6(F_2+F_3+F_4+\ldots)-(2F_2+3F_3+4F_4+\ldots) & = & 12\\
\Rightarrow & 4F_2+3F_3+2F_4+F_5+0+\text{ negative terms} & = & 12.
\end{array}$$

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. ❑

By Lemma 12.1 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 $\boldsymbol{m}(N)$ on the sphere, which requires no fewer than N colours to be properly coloured.
- Based on the definition of the map $\boldsymbol{m}(N)$, select a proper colouring of the regions of the map $\boldsymbol{m}(N)$ using the N colours $0, 1, \ldots, N-1$.

The natural number N, the map $\boldsymbol{m}(N)$ and the proper colouring of the regions of $\boldsymbol{m}(N)$ is fixed for all future reference. By the example shown in Figure 12.1 and Lemma 12.1, $4 \leq N \leq 6$. The goal is to show that $N \leq 4$.

12.2 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 non-negative 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. The group of automorphisms of $S(5, 8, 24)$ (permutations of points which permute blocks) is the largest of the Mathieu groups, M_{24}.

Lemma 12.2 (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 that

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

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

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

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 atmost 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. ❑

Recall the definition from section 12.1 that N is the minimal number of colours required to properly colour any map from the class of all maps on the sphere and $\boldsymbol{m}(N)$ is a specific map which requires all of the N colours to properly colour it. The regions of the map $\boldsymbol{m}(N)$ have been properly coloured using the N colours $0, 1, \ldots, N-1$. From the map $\boldsymbol{m}(N)$ 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 $N \leq 4$.

Lemma 12.3 Referring to the definition of N in section 12.1, 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 12.2, $6N \geq (N+1+1)(2N-N-1+1) = (N+2)N$. Hence $6 \geq N+2$ and it follows that $4 \geq N$. ❑

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

12.3 Eilenberg Modules

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

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

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

$$\sum_{g\in G} n_g g + \sum_{g\in G} m_g g = \sum_{g\in G} (n_g + m_g) g$$

$$\sum_{g\in G} n_g g \cdot \sum_{g\in G} m_g g = \sum_{g\in G} \sum_{n\in G} h \in G(n_{gh} - 1 m_h) g$$

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

$$R : G \to Sym(G);\ g \to R(g)$$

$$L^{-1} : G \to Sym(G);\ g \to L^{-1}(g) = L(g^{-1})$$

are embeddings of the group G in Sym(G). The images $R(G), L^{-1}(G)$ are called the *Cayley right and left regular representations of* G, respectively. The subgroup of 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

$$\begin{tikzcd} 1 \arrow[r] & C(G) \arrow[r, "\Delta"] & G\times G \arrow[r, "T"] & Mlt(G) \arrow[r] & 1 \end{tikzcd}$$

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

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

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

$$\begin{tikzcd} 1 \arrow[r] & M \arrow[r, "\iota"] & M]Q \arrow[r, "\pi"] & Q \arrow[r] & 1 \end{tikzcd}$$

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 $mT(q)\iota=m\iota R((0,\ q))L^{-1}((0,\ q))$ 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

$$T:Q\rightarrow Aut(ZQ,+);\ q\rightarrow\Big(\sum_{g\in Q}n_gg\rightarrow\sum_{g\in Q}n_ggR(q)\Big).$$

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

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

for $m_1,\ m_2$ in $\boldsymbol{ZQ}$ and $q_1,\ q_2$ in Q.

Referring to the definition in section 12.1, N is the minimal number of colours required to properly colour any map from the class of all maps on the sphere and $\boldsymbol{m}(N)$ is a specific map that requires all of N colours to be properly coloured. Note that $\boldsymbol{m}(N)$ has been properly coloured by using the N colours $0,\ 1,\ \ldots,\ N-1$ and this proper colouring is fixed. The set of regions of $\boldsymbol{m}(N)$ is then partitioned into subsets $\underline{0},\underline{1},\ \ldots,\ \underline{N-1}$ where the subset $\underline{m}$ consists of all the regions which receive the colour m. Note that the subsets $\underline{0}$, $\underline{1}$, ..., $\underline{N-1}$ are each nonempty (since $\boldsymbol{m}(N)$ requires all of the N colours to be properly coloured) and form a partition of the set of regions of $\boldsymbol{m}(N)$ (by virtue of proper colouring). Identify the set $\{\underline{0}, \underline{1}, \ldots, \underline{N-1}\}$ 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 ρ, σ where $|\rho| = 3$ and $|\sigma| = 2$.

Lemma 12.4 $(\mathbf{Z}_N, +)$ is an Eilenberg module for the group S_3 with the trivial homomorphism

$$T_1 : S_3 \to Aut\ (\mathbf{Z}_N, +); a \to 1\ \mathbf{Z}_N$$

where $1\ \mathbf{Z}_N$ 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. ❑

Referring to section 12.2, 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 12.5.

Lemma 12.5 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

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

where $1\ \mathbf{Z}(\mathbf{Z}_N]S_3)$ denotes the identity automorphism of $(\mathbf{Z}(\mathbf{Z}_N]S_3),\ +)$. The corresponding split extension $\mathbf{Z}(\mathbf{Z}_N]S_3)]ZS_3$ has multiplication given by

$$\Big(\sum_{(\underline{m},\beta)\in Z_N]S_3} n_{(\underline{m},\ \beta)}(\underline{m},\beta),\ \sum_{\alpha\in S_3} n_\alpha\alpha\Big)\Big(\sum_{(\underline{m},\ \beta)\in Z_N]S_3} n'_{(m,\ \beta)}(m,\ \beta),\ \sum_{\alpha\in S_3} n'_\alpha\alpha\Big)$$

$$= \Big(\sum_{(\underline{m},\ \beta)\in Z_N]S_3} (n_{\underline{m},\ \beta)} + n'_{(\underline{m}\,\beta)})(\underline{m},\ \beta),\ \sum_{\alpha\in S_3} (n_\alpha + n'_\alpha)\alpha\Big)$$

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.

12.4 Hall Matchings

Let Γ be a bipartite graph with vertex set $V = X \cup Y$ and edge set E (every edge has one end in X and the other end in Y). A *matching from X to Y in Γ* 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 Γ 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.

Lemma 12.6 (P. Hall) If $|adj(A)| \geq |A|$ for every subset A of X, then there exists a complete matching from X to Y in Γ.

Proof A matching from X to Y in G with $|M| = 1$ always exists by choosing a single edge in E. Let M be a matching from X to Y in G 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/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 $x_0, x_1, \ldots, x_k$ and $y_1, \ldots, y_k$ have been chosen, since $|adj(\{x_0, x_1, \ldots, x_k\})| \geq k+1$, there is a vertex y_{k+1}, distinct from $y_1, \ldots, y_k$, that is adjacent to at least one vertex in $\{x_0, x_1, \ldots, x_k\}$. 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/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/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 $y_{k+1}, x_{i_1}, y_{i_1}, x_{i_2}, y_{i_2}, \ldots, x_{i_r}, y_{i_r}, x_0$ of odd length $2r+1$ with the $r+1$ edges $\{y_{k+1}, x_{i_1}\}, \{y_{i_1}, x_{i_2}\}, \ldots, \{y_{i_r}, x_0\}$ in E/M and the r edges $\{x_{i_1}, y_{i_1}\}, \ldots, \{x_{i_r}, y_{i_r}\}$ in M. Define

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

Then M' is a matching from X to Y in Γ, 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 Γ.

Lemma 12.7 Referring to section 12.3, 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 12.4. 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 $\alpha \to R(\alpha)$ and $Sym(S_3)$ is a subgroup of $Sym(\mathbf{Z}_N]S_3)$, the lemma follows.

Lemma 12.8 By Lemma 12.7, regard S_3 as a subgroup of $\mathrm{Sym}(\mathbf{Z}_N]S_3)$. There exists a common system of coset representatives $\phi_1, \ldots, \phi_k$ such that $\{\phi_1 S_3, \ldots, \phi_k S_3\}$ is the family of left cosets of S_3 in $Sym(\mathbf{Z}_N]S_3)$ and $\{S_3\phi_1, \ldots, S_3\phi_k\}$ 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 Γ with vertices $X \cup Y$ where $X = \{\psi_1 S_3, \ldots, \psi_k S_3\}$ is the family of left cosets of S_3 in $Sym(\mathbf{Z}_N]S_3)$ and $Y = \{S_3\psi'_1, \ldots, S_3\psi'_k\}$ is the family of right cosets of S_3 in $Sym(\mathbf{Z}_N]S_3)$ with an edge $\{\psi_i S_3, S_3\psi'_j\}$ if and only if $\psi_i S_3$ and $S_3\psi'_j$ have nonempty intersection. For any subset $A = \{\psi i_1 S_3, \ldots, \psi i_r S_3\}$ of X, one has $\psi i_1 \in \psi i_1 S_3, \ldots, \psi i_r \in \psi i_r S_3$ and there exist distinct $j_1, \ldots, j_r$ such that $\psi i_1 \in S_3\psi' j_1, \ldots, \psi i_r \in S_3\psi' j_r$. Hence in the graph $\Gamma, |adj(A)| \geq |A|$. Hall's hypothesis of Lemma 12.6 is satisfied and there exists a complete matching from X to Y in Γ. This is precisely the statement that a common system of coset representatives $\phi_1, \ldots, \phi_k$ exists.

12.5 Riemann Surfaces

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

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

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 $k = 1, \ldots, n-1$ attach the lower edge of the sheet labelled k with the upper edge of the sheet labelled $k+1$. To complete the cycle, attach the lower edge of the sheet labelled n to the upper edge of the sheet labelled 1. In a physical sense, this is not possible without self-intersection but the idealised 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. 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 $\boldsymbol{m}(N)$ from section 12.1. The map $\boldsymbol{m}(N)$ is on the sphere. Pick a region and deform the sphere so that both 0 and ∞ 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 $\boldsymbol{m}(N)$ on the complex plane C with the region containing 0 and ∞ 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 $\boldsymbol{m}(N)$ on the z-plane in the sectors

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

The origin of the z-plane lies in the n "seas". An example with $n = 4$ is given in Figure 12.2.

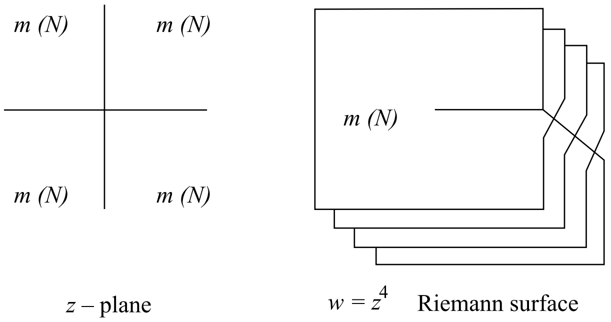


Fig. 12.2 *An example with* $n = 4$

Referring to section 12.3, 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 ψ 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

$$(\sum_{(\underline{m}\alpha)\in Z_N]S_3} n_{(\underline{m},\ \alpha)}(\underline{m},\ \alpha)) = \sum_{(\underline{m},\ \alpha)\in Z_N]S_3} n_{(\underline{m},\ \alpha)}((\underline{m},\ \alpha)\psi).$$

Referring to Lemma 12.8, fix a common coset representative ϕ_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

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

The composite is given by the assignment

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

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

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

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

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

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 $\boldsymbol{m}(N)$ corresponding to the sectors

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

of the lower half of the z-plane which comprise the lower sheet of the t-Riemann surface. Figure 12.3 shows sheets of the t-Riemann surface.

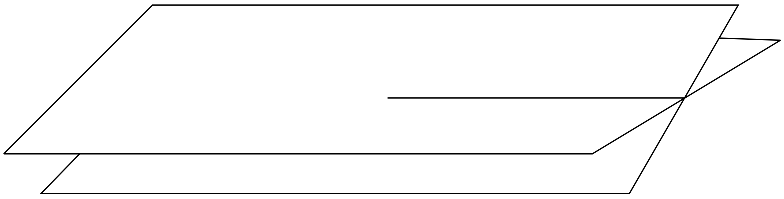
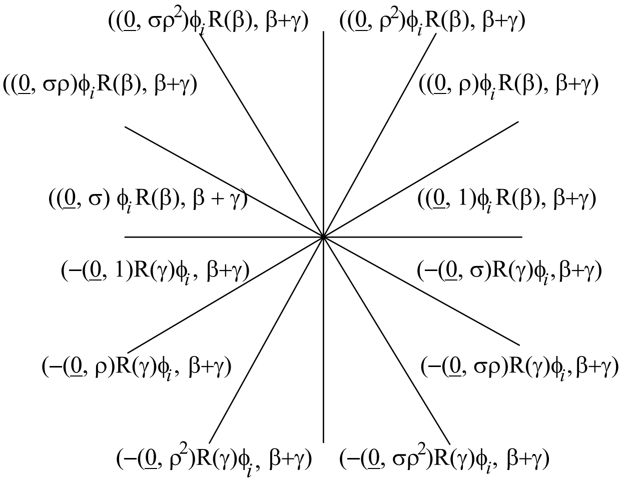


Fig. 12.3 *Sheets of the t-Riemann surface*

Label the twelve sectors of the upper sheet of the t-Riemann surface by elements of $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$ as shown in Figure 12.4.



$((\underline{0}, \sigma\rho^2)\phi_i R(\beta), \beta+\gamma)$
$((\underline{0}, \rho^2)\phi_i R(\beta), \beta+\gamma)$
$((\underline{0}, \sigma\rho)\phi_i R(\beta), \beta+\gamma)$
$((\underline{0}, \rho)\phi_i R(\beta), \beta+\gamma)$
$((\underline{0}, \sigma)\ \phi_i R(\beta), \beta + \gamma)$
$((\underline{0}, 1)\phi_i R(\beta), \beta+\gamma)$
$(-(\underline{0}, 1)R(\gamma)\phi_i, \beta+\gamma)$
$(-(\underline{0}, \sigma)R(\gamma)\phi_i, \beta+\gamma)$
$(-(\underline{0}, \rho)R(\gamma)\phi_i, \beta+\gamma)$
$(-(\underline{0}, \sigma\rho)R(\gamma)\phi_i, \beta+\gamma)$
$(-(\underline{0}, \rho^2)R(\gamma)\phi_i, \beta+\gamma)$
$(-(\underline{0}, \sigma\rho^2)R(\gamma)\phi_i, \beta+\gamma)$

Fig. 12.4 *Upper sheet of the t-Riemann surface*

Label the twelve sectors of the lower sheet of the t-Riemann surface by elements of $\mathbf{Z}(\mathbf{Z}_N]S_3)]\mathbf{Z}S_3$ as shown in Figure 12.5.

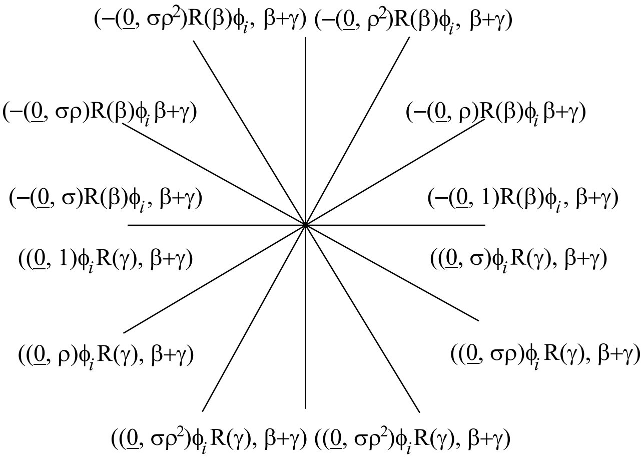


Fig. 12.5 *Lower sheet of the t-Riemann surface*

Referring to section 12.2, the regions of the map $\boldsymbol{m}(N)$ have been partitioned into disjoint, nonempty equivalence classes $0, 1, \ldots, N-1$ 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 labelled 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 $\mathbf{Z}(\mathbf{Z}_N]S_3)$.

Lemma 12.9 Referring to Lemma 12.8, fix a common representative ϕ_i of the left and right cosets of S_3 in $Sym(\mathbf{Z}_N]S_3)$. Fix a pair $(\beta, \gamma) \in S_3 \times S_3$ with $\beta \neq \gamma$. Referring to Lemma 12.5, define a subset $T_{(\beta,\gamma)}$ of $\mathbf{Z}(\mathbf{Z}_N]S_3)]\ \mathbf{Z}S_3$ as follows.

$$T_{(\beta,\,\gamma)} = \{((\underline{m},\ \alpha),\ \beta+\gamma) | (\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3\}$$

$$\cup$$

$$\{(0, \beta+\gamma)\}$$

$$\cup$$

$$\{(-(\underline{m},\ \alpha),\ \beta+\gamma) | (\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3\}.$$

Referring to the preceding discussion, consider the composite function

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

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 12.4 and 12.5 with the branch point labelled by the element $(0, \beta+\gamma)$ of both copies. The rotation of the z-plane by p radians induces a permutation

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

given by

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

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

Lemma 12.10 Referring to Lemma 12.9, let $Sym(T_{(\beta,\,\gamma)})$ denote the full permutation group of the set $T_{(\beta,\,\gamma)}$. Let $< \mathrm{p} >$ denote the cyclic subgroup of $Sym(T_{(\beta,\,\gamma)})$ generated by p. Then $< p >$ is nontrivial and acts faithfully on the set $T_{(\beta,\,\gamma)}$.

Proof If $p = 1$, then $(-(\underline{0}, 1)R(\gamma)\phi_i,\ \beta+\gamma) = (-(\underline{0},\ 1)R(\gamma)\phi_i, \beta+\gamma)p = ((\underline{0},\ 1)\phi_i R(\gamma),\ \beta+\gamma)$ which implies that $-(\underline{0},\ 1)R(\gamma)\phi_i = (0,\ 1)\phi_i R(\gamma)$ 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 $< p >$. ❑

Lemma 12.11 Referring to Lemma 12.9 and Lemma 12.10, let $1 : C \to C$; $z \to z$ denote the identity and $\pi : C \to C$; $z \to -z$ denote the rotation through an angle of p radians of the z-plane. Then the two-element cyclic group $\{1, \pi\}$ acts faithfully on the set $< p >$ as follows: $p^n \cdot 1 = p^n$ and $p^n \cdot \pi = p^{1-n}$, for all n in Z.

Proof The set $\{1,\ \pi\}$ forms a two-element cyclic group $< \pi >$ under function composition. To show that $\{1, \pi\}$ acts on $< p >$ as defined, observe that $(p^n \cdot \pi) \cdot \pi = (p^{1-n}) \cdot \pi = p^{1-(1-n)} = p^{1-1+n} = p^n = p^n \cdot 1 = p^n \cdot (\pi\pi)$, for all n in $\mathbf{Z}$. To show that the action is faithful, let $\theta \in \{1,\ \pi\}$. If θ belongs to the kernel of the action, then $p^n \cdot \theta = p^n$ for all n in $\mathbf{Z}$, so that $p \cdot \theta = p$ which implies that $\theta = 1$, since $p \neq 1$ by Lemma 12.10. ❑

Lemma 12.12 Putting together Lemma 12.9, Lemma 12.10 and Lemma 12.11, there is a well-defined action of the two-element cyclic group $\{1,\, \pi\}$ on the set $T_{(\beta,\,\gamma)}$ given by

$$((\underline{m},\, \alpha)\phi_i R(\gamma),\, \beta+\gamma)\cdot 1 \;= ((\underline{m},\, \alpha)\; \phi_i R(\gamma),\, \beta+\gamma)$$

$$(0,\, \beta+\gamma)\cdot 1 \;= (0,\, \beta+\gamma)$$

$$(-(\underline{m},\, \alpha)R(\beta)\phi_i,\, \beta+\gamma)\cdot 1 = (-(\underline{m},\, \alpha)R(\beta)\phi_i,\, \beta+\gamma)$$

and

$$((\underline{m},\, \alpha)\phi_i R(\gamma),\, \beta+\gamma)\cdot \pi = (-(\underline{m},\, \alpha)R(\gamma)\phi_i,\, \beta+\gamma)$$

$$(0,\, \beta+\gamma)\cdot \pi \;= (0,\, \beta+\gamma)$$

$$(-(\underline{m},\, \alpha)R(\beta)\phi_i,\, \beta+\gamma)\cdot \pi = ((\underline{m},\, \alpha)\phi_i R(\beta),\, \beta+\gamma)$$

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 $< p >$. 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

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

Then, π is well-defined since $xp^n = xp^m \Rightarrow xp^{n-m} = x \Rightarrow xp^{-m} = xp^{-n} \Rightarrow xp^{1-m} = xp^{1-n} \Rightarrow (xp^n)\pi = (xp^m)\pi$. Also, π 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

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

orbit by orbit. Then, since $\{Orb(x)|x \in T_{(\beta,\,\gamma)}\}$ forms a partition of $T_{(\beta,\,\gamma)}$, π 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 12.9, 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

$$((-(\underline{m},\, \alpha)R(\gamma)\phi_i,\, \beta+\gamma)p)\cdot 1 \;= (-(\underline{m},\, \alpha)R(\gamma)\phi_i,\, \beta+\gamma)p$$

$$((0,\, \beta+\gamma)p)\cdot 1 \;= (0,\beta+\gamma)p$$

$$(((\underline{m},\, \alpha)\phi_i R(\beta),\, \beta+\gamma)p)\cdot 1 \;= ((\underline{m},\, \alpha)\phi_i R(\beta),\, \beta+\gamma)p$$

and

$$\begin{aligned}((-(\underline{m},\,\alpha)R(\gamma)\phi_i,\,\beta+\gamma)p)\cdot\pi\ &=(-(\underline{m},\,\alpha)R(\gamma)\phi_i,\,\beta+\gamma)\\ ((0,\,\beta+\gamma)p)\cdot\pi\ &=(0,\,\beta+\gamma)\\ (((\underline{m},\,\alpha)\phi_iR(\beta),\,\beta+\gamma)p)\cdot\pi\ &=((\underline{m},\,\alpha)\phi_iR(\beta),\,\beta+\gamma)\end{aligned}$$

Now, using the definition of p in Lemma 12.9, the action of $\{1,\pi\}$ on $T_{(\beta,\gamma)}$ may be rewritten as

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

and

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

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

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

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

Case 2 Suppose $\beta=\gamma$. Note that in the labelling of the sectors of the sheets of the t-Riemann surface in Figures. 12.4 and 12.5, $R(\beta)=R(\gamma)$ and $\beta+\gamma=2\beta$ in the group algebra $\mathbf{Z}S_3$. ❑

Lemma 12.13 Referring to Lemma 12.8, fix a common representative ϕ_i of the left and right cosets of S_3 in $Sym(\mathbf{Z}_N]S_3)$. Fix a pair $(\beta,\,\beta)\in S_3\times S_3$. Referring to Lemma 12.5, define a subset $T_{(\beta,\,\beta)}$ of $\mathbf{Z}(\mathbf{Z}_N]S_3)\mathbf{Z}S_3$ as follows.

$$T_{(\beta,\beta)} = \{((\underline{m},\ \alpha),\ 2\beta)|(\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3\}$$

$$\cup$$

$$\{(0,\ 2\beta)\}$$

$$\cup$$

$$\{(-(\underline{m},\ \alpha),\ 2\beta)|(\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3\}.$$

Referring to the preceding discussion, consider the composite function

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

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 12.4 and 12.5. 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 p radians induces a permutation

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

given by

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

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 $< p > = \{1,\ p\}$ is a two-element cyclic subgroup of the full permutation group $Sym(T_{(\beta,\beta)})$ and $< p >$ acts faithfully on the set $T_{(\beta,\beta)}$.

Proof As in the proof of Lemma 12.9, $T_{(\beta,\beta)}$ 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 12.5. Both $\phi_i R(\beta)$, $R(\beta)\phi_i$ are permutations of the set $\mathbf{Z}_N]S_3$ and the rotation of the z-plane by p 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, $< p > = \{1,\ p\}$ is a subgroup of $Sym(T_{(\beta,\beta)})$ and $< p >$ acts faithfully on the set $T_{(\beta,\beta)}$. ❑

Lemma 12.14 Referring to Lemma 12.13, let $1 : C \to C; z \to z$ denote the identity and $\pi : C \to C$; $z \to -z$ denote the rotation through an angle of p 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

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

and

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

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

Proof The isomorphism $1 \to 1$, $p \to \pi$ of the two-element cyclic groups $\{1,\ p\}$ and $\{1,\ \pi\}$ establishes the lemma. ❑

12.6 Main Construction

Let us review the final goal with a brief résumé. In section 12.1, 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 $4 \le N \le 6$. We have chosen a specific map $\boldsymbol{m}(N)$ on the sphere that requires all of the N colours $0,\ 1,\ \ldots,\ N-1$ to properly colour it. The map $\boldsymbol{m}(N)$ has been properly coloured and the regions of $\boldsymbol{m}(N)$ partitioned into disjoint, nonempty equivalence classes $0,\ 1,\ \ldots,\ N-1$ according to the colour they receive. The set $\{0,\ 1,\ \ldots,\ N-1\}$ is endowed with the structure of the cyclic group $\mathbf{Z}_N$ under addition modulo N. In section 12.3, 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 12.3 shows that $N \le 4$.

Lemma 12.15 Let $\mathbf{Z}_N]S_3$ denote the split extension defined in Lemma 12.4 and $\mathrm{Sym}(\mathbf{Z}_N]S_3)$ denote the full permutation group on the set $\mathbf{Z}_N]S_3$.

Define

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

by

$$\Psi = R(\gamma)\phi_i \to \phi_i(\gamma) = \Psi^{\mu}.$$

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

Proof Referring to Lemma 12.8, μ is well-defined since each $\Psi \in Sym(\mathbf{Z}_N]S_3)$ may be written uniquely as $\Psi = R(\gamma)\phi_i$ for some $\gamma \in S_3$ and some ϕ_i. Then, μ is a surjection because for any $\Psi \in Sym(\mathbf{Z}_N]S_3)$ one may also write $\Psi = \phi_i R(\gamma)$ uniquely for some $\gamma \in S_3$ and some ϕ_i, whence $R(\gamma)\phi_i \to \phi_i R(\gamma) = \Psi$. Since $Sym(\mathbf{Z}_N]S_3)$ is a finite set, μ must be a bijection by counting. ❑

Lemma 12.16 Define the set G as follows.

$$G = \left\{ \begin{pmatrix} \Psi \\ \Psi^{\mu} \end{pmatrix} \middle| \Psi \in \mathrm{Sym}(Z_N]S_3) \right\} = \left\{ \begin{pmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{pmatrix} \middle| \begin{matrix} \gamma \in S_3 \\ i = 1, \ldots, k \end{matrix} \right\}$$

Define multiplication in G as follows:

$$\begin{bmatrix} \Psi_1 \\ (\Psi_1^{\mu}) \end{bmatrix} \begin{bmatrix} \Psi_2 \\ (\Psi_2^{\mu}) \end{bmatrix} = \begin{bmatrix} \Psi_1\Psi_2 \\ (\Psi_1\Psi_2)^{\mu} \end{bmatrix}$$

i.e.,

$$\begin{bmatrix} R(\gamma_1)\phi i_1 \\ \phi i_1 R(\gamma_1) \end{bmatrix} \begin{bmatrix} R(\gamma_2)\phi i_2 \\ \phi i_2 R(\gamma_2) \end{bmatrix} = \begin{bmatrix} R(\gamma_3)\phi i_3 \\ \phi i_3 R(\gamma_3) \end{bmatrix},$$

where $R(\gamma_3)\phi_3$ 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 $Sym(\mathbf{Z}_N S_3)$. Then, G is a group.

Proof Referring to Lemma 12.8 and Lemma 12.15, the set G is well-defined by the decomposition of $Sym(Z_N]S_3)$ into the left and right cosets of S_3 by the ϕ_1. Define

$$\mu' : Sym(\mathbf{Z}_N]S_3) \to G;\ \Psi \to \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix}.$$

Then, μ' is a well-defined bijection of the set $Sym(\mathbf{Z}_N]S_3)$ with G since m is a bijection by Lemma 12.15. The definition of multiplication in G mirrors the multiplication in $Sym(\mathbf{Z}_N]S_3)$ via μ' and is designed to make G a group and μ' an isomorphism. ❑

Lemma 12.17 Consider the set $\mathbf{Z}_N]S_3$ and let

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

Define

$$\uparrow \begin{bmatrix} \Psi \\ \Psi^\mu \end{bmatrix} : Z_N]s_3 \to Z_N]S_3 \text{ by}$$

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

Define

$$\downarrow \begin{bmatrix} \Psi \\ \Psi^\mu \end{bmatrix} : Z_N]S_3 \text{ by}$$

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

Then

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

Both ↑ and ↓ 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 12.12 and Lemma 12.12, put $\beta = 1$. Working in the set $T_(1,\ \gamma)$, for each $(\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3$, we have

$$((\underline{M},\ \alpha) \downarrow \begin{bmatrix} \Psi \\ \Psi^\mu \end{bmatrix},\ 1+\gamma)$$

$$= ((\underline{m},\ \alpha) \downarrow \begin{bmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{bmatrix},\ 1+\gamma)$$

$$= (\,(\underline{m},\ \alpha)\phi_i R(\gamma),\ 1+\gamma)$$

$$= (\,-(\underline{m},\ \alpha)R(\gamma)\phi_i,\ 1+\gamma)\pi$$

$$= (\,-(\underline{m},\ \alpha\gamma)\phi_i,\ 1+\gamma)\pi$$

$$= (\,-(\underline{m},\ \alpha\gamma)R(1)\phi_i,\ 1+\gamma)\pi$$

$$= (\,(\underline{m},\ \alpha\gamma)\phi_i R(1),\ 1+\gamma)$$

$$= (\,(\underline{m},\ \alpha\gamma)\phi_i,\ 1+\gamma)$$

$$= (\,(\underline{m},\ \alpha)R(\gamma)\phi_i,\ 1+\gamma)$$

$$= (\,(\underline{m},\ \alpha)\uparrow \begin{bmatrix} R(\gamma)\phi_i, \\ \phi_i R(\gamma) \end{bmatrix},\ 1+\gamma)$$

$$= (\,(\underline{m},\ \alpha)\uparrow \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix},\ 1+\gamma)$$

using the action of the two-element cyclic group $\{1,\ \pi\}$ on the set $T_{(1,\ \gamma)}n$ according to Lemma 12.12 and Lemma 12.12. Hence

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

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. ❑

Lemma 12.18 Let $(\underline{m}_1,\ \alpha_1),\ \cdots,\ (\underline{m}_r,\ \alpha_r)$ be any r distinct elements of $\mathbf{Z}_N]S_3$ and let $(\underline{n}_1,\ \beta_1),\ \ldots,\ (\underline{n}_s,\ \beta_s)$ be any s distinct elements of $\mathbf{Z}_N]S_3$. Let

$$H_{r,\,s} = \left\{ \begin{pmatrix} \Psi \\ \Psi^{\mu} \end{pmatrix} \in G \;\middle|\; \begin{array}{l} (\underline{m_i}, \alpha_i)\uparrow \begin{pmatrix} \Psi \\ \Psi^{\mu} \end{pmatrix} = (\underline{m_i},\ \alpha_i) \text{ for } i=1,\ \ldots,\ r \\ \text{and} \\ (\underline{n_j}, \beta_i)\downarrow \begin{pmatrix} \Psi \\ \Psi^{\mu} \end{pmatrix} = (\underline{n_j},\ \beta_i) \text{ for } j=1,\ \ldots, s \end{array} \right\},$$

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

Proof Note that if $\Psi = R(\gamma)\phi_i = 1$ then $\phi_i = R(\gamma)^{-1}$, so that

$$\Psi^{\mu} = \phi_i R(\gamma) = R(\gamma)^{-1}R(\gamma) = 1.$$

Then

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

since

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

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

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

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

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

then

$$(\underline{m}_i,\ \alpha_i) \uparrow \left[\begin{bmatrix} \Psi_1 \\ \Psi_1^\mu \end{bmatrix} \begin{bmatrix} \Psi_2 \\ \Psi_2^\mu \end{bmatrix} \right] = (\underline{m}_i,\ \alpha_i) \uparrow \begin{bmatrix} \Psi_1 \\ \Psi_1^\mu \end{bmatrix} \begin{bmatrix} \Psi_2 \\ \Psi_2^\mu \end{bmatrix}$$

$$= (\underline{m}_i,\ \alpha_i) \uparrow \begin{bmatrix} \Psi_2 \\ \Psi_2^\mu \end{bmatrix} = (\underline{m}_i,\ \alpha_i) \text{ for } i = 1, \ldots, r$$

and

$$(\underline{n}_j,\ \beta_j) \downarrow \left[\begin{bmatrix} \Psi_1 \\ \Psi_1^\mu \end{bmatrix} \begin{bmatrix} \Psi_2 \\ \Psi_2^\mu \end{bmatrix} \right] = (\underline{n}_j,\ \beta_j) \downarrow \begin{bmatrix} \Psi_1 \\ \Psi_1^\mu \end{bmatrix} \downarrow \begin{bmatrix} \Psi_2 \\ \Psi_2^\mu \end{bmatrix}$$

$$= (\underline{n}_j,\ \beta_j) \downarrow \begin{bmatrix} \Psi_2 \\ \Psi_2^\mu \end{bmatrix} = (\underline{n}_j,\ \beta_j) \text{ for } j = 1, \ldots, s.$$

Hence

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

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

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

$$S_3 = < \sigma, \rho > = \{1,\ \rho, \rho^2,\ \sigma,\ \sigma\rho,\ \sigma\rho_2\}.$$

Lemma 12.19 Define

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

Then given

$$\begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} \in H,$$

either

$$(\underline{m},\ \alpha) \downarrow \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} = (\underline{m},\ \alpha) \text{ for all } (\underline{m},\ \alpha) \in Z_N]S_3$$

or

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

Proof H is a well-defined subgroup of G according to Lemma 12.18. Let

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

and $(\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3$ be given. Referring to Lemmas 12.12 and 12.14, put $\beta = \gamma^{-1}\alpha\gamma$. Working in the set $T_{(}\beta,\ \gamma)$, we have

$$\left((\underline{m},\ \alpha) \downarrow \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix},\ \beta + \gamma\right)$$

$$= \left((\underline{m},\ \alpha) \downarrow \begin{bmatrix} R(\gamma)\phi_i \\ \phi_i R(\gamma) \end{bmatrix},\ \beta + \gamma\right)$$

$$= ((\underline{m},\ \alpha)\phi_i R(\gamma),\ \beta + \gamma)$$

$$= (-(\underline{m},\ \alpha)R(\gamma),\ \phi_i\beta + \gamma)\pi$$

$$= (-(\underline{m},\ \alpha\gamma)\phi_i,\ \beta + \gamma)\pi$$

$$= (-(\underline{m},\ \gamma\beta)\phi_i,\ \beta + \gamma)\pi$$

$$= (-(\underline{m},\ \gamma)R(\beta)\phi_i,\ \beta + \gamma)\pi$$

$$= ((\underline{m},\ \gamma)\phi_i R(\beta),\ \beta + \gamma)$$

$$= ((\underline{m},\ 1)R(\gamma)\phi_i R(\beta),\ \beta + \gamma)$$

$$= ((\underline{m},\ 1)R(\beta),\ \beta + \gamma)$$

$$= ((\underline{m},\ \beta),\ \beta + \gamma)$$

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

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

Now since

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

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

Lemma 12.20 Let H be the subgroup of G defined in Lemma 12.19. 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

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

Then

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

and

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

Now $\Psi^1 \neq 1$, so

$$\begin{bmatrix} 1 \\ 1^{\mu} \end{bmatrix} \neq \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} \in H,$$

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

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

Then, by the proof of Lemma 12.19, $\gamma = 1$ or $\gamma = \sigma$. In particular, $\gamma^2 = 1$. Hence, for any $(\underline{m}, \alpha) \in \mathbf{Z}_N]S_3$

$$(\underline{m},\ \alpha) \downarrow \begin{bmatrix} R(\gamma)\phi^{i} \\ \phi_{i}R(\gamma) \end{bmatrix}^{2}$$

$$= (\underline{m},\ \alpha) \downarrow \begin{bmatrix} R(\gamma)\phi^{i} \\ \phi_{i}R(\gamma) \end{bmatrix} \downarrow \begin{bmatrix} R(\gamma)\phi^{i} \\ \phi_{i}R(\gamma) \end{bmatrix}$$

$$= (\underline{m},\ \alpha^{\gamma}) \downarrow \begin{bmatrix} R(\gamma)\phi^{i} \\ \phi_{i}R(\gamma) \end{bmatrix}$$

$$= (\underline{m},\ (\alpha^{\gamma})^{\gamma}) = (\underline{m},\ \alpha).$$

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

$$\begin{bmatrix} R(\gamma)\phi_{i} \\ \phi_{i}R(\gamma) \end{bmatrix}^{2} = \begin{bmatrix} 1 \\ 1^{\mu} \end{bmatrix},$$

the identity element of G.

Lemma 12.21 Denote the right cosets of $\mathbf{Z}_N$ in $\mathbf{Z}_N]S_3$ by

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

Define Fix↓(H) =

$$\left\{ (\underline{m},\ \alpha) \in Z_N]S_3 \,\middle|\, (\underline{m}\alpha) \downarrow \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} = (\underline{m}\alpha) \text{ for all } \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} \in H \right\}.$$

Then Fix $\downarrow(H)$ = $\{(\underline{m},\ \alpha) \in \mathbf{Z}_N]S_3 | a = 1$ or $\alpha = \sigma$. The ↓ 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 12.19 and 12.20, the elements

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

are of two kinds:

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

in which case

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

the identity element of H, and

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

in which case

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

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

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

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

$$(\underline{m}, \rho) \downarrow \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} = (\underline{m},\ \rho^{\sigma}) = (\underline{m},\ \rho_2) \text{ for all } \underline{m} \in \mathbf{Z}_N$$

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

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

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

and the lemma follows.

Lemma 12.22 Let $Norm_G(H)$ denote the normaliser of H in G. The action$\downarrow$ of G on $\mathbf{Z}_N]S_3$ restricts to an action $\downarrow$ of $Norm_G(H)$ on Fix$\downarrow$ (H) which is $(|Z_N|+1)$-transitive.

Proof Let

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

First show that

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

as follows.

$$(\underline{m},\ \alpha) \in Fix\downarrow \left[\overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}} H \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right]$$

$$\Leftrightarrow (\underline{m},\ \alpha)\downarrow \left[\overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}} \begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix} \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right] = (\underline{m},\ \alpha) \text{ for all } \begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix} \in H$$

$$\Leftrightarrow (\underline{m},\alpha)\downarrow \left[\overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}} \begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}\right] = \overset{-1}{(\underline{m},\alpha)}\downarrow \begin{bmatrix}\Psi\\ \Psi\end{bmatrix} \text{ for all } \begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix} \in H$$

$$\Leftrightarrow (\underline{m},\ \alpha)\downarrow \overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}} \downarrow \begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix} = \overset{-1}{(\underline{m},\ \alpha)}\downarrow \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \text{ for all } \begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix} \in H$$

$$\Leftrightarrow (\underline{m},\ \alpha)\downarrow \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \in \text{Fix}\downarrow(H) \Leftrightarrow (\underline{m},\ \alpha) \in \text{Fix}\downarrow(H)\downarrow \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}.$$

Now let

$$\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \in\ Norm_G(H) = \left\{ \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \overset{-1}{\in} G \,\middle|\, \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} H \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} = H \right\}.$$

Then

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

showing that the action restricts to an action of $Norm_G(H)$ on Fix $\downarrow(H)$. Now to show that the action ↓ of $Norm_G(H)$ on 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 $(\underline{m}_1,\alpha_1),\ldots,(\underline{m}_N,\alpha_N)$ and label $(\underline{0},\sigma) = (\underline{m}_{N+1},\ \alpha_{N+1})$. Let $(\underline{m}_1^*,\ \alpha_1^*),\ \ldots,\ (\underline{m}_{N+1}^*,\ \alpha_{N+1}^*)$ be any $|Z_N|+1$ distinct points of Fix$\downarrow(H)$. It is enough to show that there exists

$$\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \in Norm_G(H)$$

such that

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

Now there exists

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

such that

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

Hence

$$(\underline{m}_i^*,\ \alpha_i^*) = (\underline{m}_i,\ \alpha_i)\overset{-1}{\downarrow}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \text{ for } I = 1,\ \ldots,\ N+1.$$

Note that for every

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

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

$$(\underline{m}_i,\ \alpha_i)\downarrow\left[\overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}}\begin{bmatrix}\Psi *\\ \Psi *^{\mu}\end{bmatrix}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right]$$

$$= (\underline{m}_i,\ \alpha_i)\downarrow\overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}}\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}$$

$$= (\underline{m}_i^*,\ \alpha_i^*)\downarrow\begin{bmatrix}\Psi *\\ \Psi *^{\mu}\end{bmatrix}\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}$$

$$= (\underline{m}_i^*,\ \alpha_i^*)\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} = (\underline{m}_i,\ \alpha_i).$$

Hence

$$\overset{-1}{\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}}\begin{bmatrix}\Psi *\\ \Psi *^{\mu}\end{bmatrix}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \in H \text{ for all } \begin{bmatrix}\Psi *\\ \Psi *^{\mu}\end{bmatrix} \in H \Rightarrow \begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \in \ Norm_G(H). \qquad ❑$$

Lemma 12.23 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

$$\left\{\text{Fix}\downarrow(H)\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\middle|\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix} \in G\right\}.$$

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

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

contains $2N = |\,\mathbf{Z}_N \cup \mathbf{Z}_N\sigma| = |\,\text{Fix} \downarrow (H)| =$

$$\left| Fix \downarrow (H) \downarrow \begin{bmatrix} \Psi \\ \Psi^{\mu} \end{bmatrix} \right|$$

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

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

such that

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

Hence there is at least one block, namely Fix↓ (H), that contains the points $(\underline{m}_1^*,\ \alpha_1^*),\ \ldots,\ (\underline{m}_{N+1}^*,\ \alpha_{N+1}^*)$. It remains to show that this is the unique block that contains the points $(\underline{m}_1^*,\ \alpha_1^*),\ \ldots,\ (\underline{m}_{N+1}^*, \alpha_{N+1}^*)$. Suppose $(\underline{m}_1^*,\ \alpha_1^*),\ \ldots, (\underline{m}_{N+1}^*,\ \alpha_{N+1}^*)$ are contained in

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

Then there exist points $(\underline{m}_1^{**},\ \alpha_1^{**}),\ \ldots,\ (\underline{m}_{N+1}^{**},\ \alpha_{N+1}^{**})$ in Fix↓ (H) such that

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

By Lemma 12.22, there exists

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

such that

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

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

$$(\underline{m}_i,\ \alpha_i)\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}$$

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

$$=(\underline{m}_i^{**},\ \alpha_i^{**})\downarrow\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}$$

$$=(\underline{m}_i,\ \alpha_i)\downarrow\begin{bmatrix}\Psi**\\ \Psi**^{\mu}\end{bmatrix}\downarrow\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}$$

$$\Leftrightarrow(\underline{m}_i,\ \alpha_i)=(\underline{m}_i,\ \alpha_i)\downarrow\left[\begin{bmatrix}\Psi**\\ \Psi**^{\mu}\end{bmatrix}\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right]\text{ for } i=1,\ \ldots,\ N+1.$$

Then, by Lemma 12.17

$$(\underline{m}_i,\ \alpha_i)=(\underline{m}_i,\ \alpha_i)\uparrow\left[\begin{bmatrix}\Psi**\\ \Psi**^{\mu}\end{bmatrix}\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right]\text{ for } i=1,\ \ldots,\ N,$$

and

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

Hence

$$\begin{bmatrix}\Psi**\\ \Psi**^{\mu}\end{bmatrix}\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\in H.$$

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

$$\Leftrightarrow\begin{bmatrix}\Psi**\\ \Psi**^{\mu}\end{bmatrix}\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\in Norm_G(H)$$

$$\Leftrightarrow\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}^{-1}\in\begin{bmatrix}\Psi**\\ \Psi**^{\mu}\end{bmatrix}^{-1}Norm_G(H)=Norm_G(H)$$

$$\left[\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}^{-1}\right]H\left[\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1-1}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right]=H$$

$$\Leftrightarrow\begin{bmatrix}\Psi^{*}\\ \Psi^{*\mu}\end{bmatrix}\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}^{-1}H\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}^{-1}\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}=H$$

$$\Leftrightarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}^{-1}H\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}=\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1}H\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}.$$

Now, using the first fact in the proof of Lemma 12.22

$$\text{Fix}\downarrow(H)\downarrow\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}$$

$$=\text{Fix}\downarrow\left[\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}^{-1}H\begin{bmatrix}\Psi*\\ \Psi*^{\mu}\end{bmatrix}\right]$$

$$=\text{Fix}\!\downarrow\left[\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}^{-1}H\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}\right]$$

$$=\text{Fix}\!\downarrow(H)\downarrow\begin{bmatrix}\Psi\\ \Psi^{\mu}\end{bmatrix}$$

This establishes the uniqueness of the block.

Theorem 12.1. Any map on the sphere can be properly coloured by using at most four colours.

Proof Referring to section 12.1, 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 $\boldsymbol{m}(N)$ on the sphere that requires no fewer than N colours to be properly coloured. Based on the definition of the map $\boldsymbol{m}(N)$ we have selected a proper colouring of its regions using the N colours $0, 1, \ldots, N-1$. Working with the fixed number N, the fixed map $\boldsymbol{m}(N)$, and the fixed proper colouring of the regions of the map $\boldsymbol{m}(N)$, Lemma 12.23 has explicitly constructed a Steiner system $S(N+1, 2N, 6N)$. Now Lemma 12.3 implies that N cannot exceed four.