THE GROUP RING FOR S_3

by

Earle Peter Botta

B.A., The University of British Columbia, 1961

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in the Department
of
Mathematics

We accept this thesis as conforming to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

April, 1963

Department of Mathematics

The University of British Columbia,
Vancouver 8, Canada.

Date April 30, 1963

Abstract

The units in the group ring for S_3 over the integers are investigated. It is shown that the only units of finite order are of order two, three or six. Infinite classes of units of each of these orders are constructed as well as an infinite class of units of infinite order.

The equation $G = AA^T$, where G is a unimodular group matrix of rational integers and A a matrix of rational integers, is investigated in the ring of group matrices for S_3. It is shown that $A = CP$, where C is a unimodular group matrix of rational integers and P a generalized permutation matrix. It is also shown that if H is a positive definite symmetric unimodular group matrix then $H = H_1H_1^T$ where H_1 is a group matrix of rational integers and H is of infinite order except in the trivial case when $H = I$.

I hereby certify that this abstract is satisfactory.

Acknowledgment

The author would like to thank his supervisor, Dr. R. C. Thompson, for his patient assistance in the preparation of this thesis.

He would also like to thank the National Research Council of Canada for their financial support.

Table of Contents

1. Group Rings

Let G be any multiplicative group and Z the ring of rational integers. The set of all finite formal sums $\sum_{i=1}^{n} x_{g_i} g_i$, $x_{g_i} \in Z$, $g_i \in G$ will be denoted by Z(G). Z(G) can be made into a ring by defining addition (+) and multiplication (•) as follows.

Suppose $x, y \in Z(G)$; $x = \sum_{i=1}^{n} x_{g_i} g_i$, $y = \sum_{j=1}^{n} y_{g_j} g_j$

then (a) $x \cdot y = \sum_{i=1}^{n} \sum_{j=1}^{n} (x_{g_i} y_{g_j}) g_i g_j$

(b) $x + y = \sum_{i=1}^{n} (x_{g_i} + y_{g_i}) g_i$

It is not hard to verify that $\{Z(G), +, \cdot\}$ is an associative ring with identity 1e, where e is the identity in G.

Definition. $\{Z(G), +, \cdot\}$ is called the group ring for G over Z or simply the group ring for G.

In what follows the identity matrix will be denoted by I. The phrase "if and only if" will be abbreviated to "iff".

2. The left regular representation of a finite group

Let G be a finite group of order n and suppose the elements of G are $(g_1, \cdots, g_n)$ in some fixed order. For each $g_s \in G$ consider the ordered set $(g_s g_1, \cdots, g_s g_n)$. This set is some permutation of $(g_1, \cdots, g_n)$ so $(g_s g_1, \cdots, g_s g_n) = (g_1, \cdots, g_a)P(g_s)$ where $P(g_s)$ is a permutation matrix associated with g_n. The (i, j) element of $P(g_s)$ is 1 if $g_i = g_s g_j$ and is 0 otherwise. Define the symbol

$$g_s(i, j) = \begin{cases} 1 & \text{if } g_i g_j^{-1} = g_s \\ 0 & \text{otherwise} \end{cases}$$

then $P(g_s) = (g_s(i, j))$ and $P(g_s)P(g_t) = P(g_s g_t)$ since $\sum_{r=1}^{n} g_s(i, r)g_t(r, j) = g_s g_t(i, j)$, for $g_s(i, r) = 1$ iff

$g_r = g_s^{-1} g_i$ and $g_t(r, j) = 1$ iff $g_r = g_t g_j$ so $\sum_{r=1}^{n} g_s(i, r)g_s(r, j) = 1$ if $g_s g_t = g_i g_j^{-1}$ and 0 otherwise.

It is clear that $P(g_i) = P(g_j)$ iff $g_i = g_j$. Define a map $f: G \rightarrow M_n(Z)$, where $M_n(Z)$ is the ring of n-square matrices over Z, by $f(g_i) = P(g_i)$. It is clear from the above discussion that f is an isomorphism.

Definition. The set of n-square permutation matrices $P(g_i)$, $i = 1, \cdots, n$, $g_i \in G$ is called a left regular representation of G in $M_n(Z)$.

The matrices $P(g_i)$ are linearly independent since $g_s(i, j) = g_t(i, j) = 1$ for some i, j implies $g_t = g_i g_j^{-1} = g_s$.

Let $x = \sum_{t=1}^{n} x_{g_t} g_t \in Z(G)$ and define a map $F: Z(G) \to M_n(Z)$ by $F(x) = \sum_{t=1}^{n} x_{g_t} P(g_t)$. Then $F(x) = (x_{g_i g_j^{-1}})$ since the matrices $P(g_t)$ do not have non-zero elements in sommon positions. Since the matrices $P(g_t)$ are linearly independent $F(x) = 0$ iff $x = 0$ so the map is 1 - 1. Further $F(x + y) = (x_{g_i g_j^{-1}} + y_{g_i g_j^{-1}}) = (x_{g_i g_j^{-1}}) + (y_{g_i g_j^{-1}})$ $= F(x) + F(y)$, and $F(xy) = F(x)F(y)$ since $F(g_i g_j)$ $= P(g_i g_j) = P(g_i)P(g_j) = F(g_i)F(g_j)$. Hence F is a ring isomorphism of $Z(G)$ into $M_n(Z)$ and the image of F is the set of matrices of the form $(x_{g_i g_j^{-1}})$.

Definition. Let $x = \sum_{t=1}^{n} x_{g_t} g_t \in Z(G)$. The matrix $X = (x_{g_i g_j^{-1}}) \in M_n(Z)$ is called the group matrix for x.

3. Units in a group ring

Definition. Let G be a group and $Z(G)$ the group ring for G. An element $x \in Z(G)$ is a *left* (right) *unit* iff there exists a $y \in Z(G)$ such that $xy = 1e$ $(yx = 1e)$ where $1e$ is the identity in $Z(G)$. An element $x \in Z(G)$ is a *unit* iff it is both a left and right unit.

Definition. Let X be an n-square matrix. X is *unimodular* iff $\det X = \pm 1$.

Theorem 1. Let G be a finite group. If $x \in Z(G)$ then x is a unit iff the group matrix for x is unimodular.

Proof. Suppose x is a unit in $Z(G)$. Then there exists a $y \in Z(G)$ such that $xy = 1e$. Let X and Y be the group matrices for x and y respectively. Then $XY = I$ so $\det XY = \det X \cdot \det Y = 1$. Hence $\det X = \det Y = \pm 1$ since $\det X$, $\det Y$ are rational integers.

Conversely, suppose that X is the group matrix for an element $x \in Z(G)$ and X is unimodular. Let $X = (x_{g_i g_j^{-1}})$, $x = \sum_{t=1}^{n} x_{g_t} g_t$. Let $y = \sum_{r=1}^{n} y_{g_r} g_r$ be any other element of $Z(G)$. Then $xy = \sum_{s=1}^{n} z_{g_s} g_s$ where $z_{g_s} = \sum_{r=1}^{n} x_{g_s g_r^{-1}} y_{g_r}$.

So

$$\text{(I)} \quad \begin{pmatrix} z_{g_1} \\ \vdots \\ z_{g_n} \end{pmatrix} = X \begin{pmatrix} y_{g_1} \\ \vdots \\ y_{g_n} \end{pmatrix} .$$

Take $z_{g_i} = 1$ if g_i is the identity and $z_{g_i} = 0$ otherwise. Since X^{-1} is a matrix of rational integers the above system of equations (I) can be solved for $y_{g_1}, \ldots, y_{g_n}$ in integers. Then $xy = 1e \in Z(G)$. Let Y be the group matrix for y. Then $XY = I$ so $Y = X^{-1}$ and since $XX^{-1} = X^{-1}X = YX = I$ it follows that $yx = 1e$. Hence x is both a left and right unit.

The above proof can be found in [6].

If G is a finite group then every left (right) unit is also a right (left) unit. Suppose x is a left unit. Then there exists a y such that $xy = 1e$. Let X and Y be the group matrices for x and y respectively. Then $XY = XX^{-1} = X^{-1}X = YX = I$ so $yx = 1e$ and x is a right unit.

If G is any finite group then the set of units in $Z(G)$ form a multiplicative group. Suppose x and y are units. Then there exist x^{-1}, y^{-1} such that $x^{-1}x = xx^{-1} = 1e$ and $y^{-1}y = yy^{-1} = 1e$ so $y^{-1}x^{-1}xy = xyy^{-1}x^{-1}$ and xy is a unit.

4. The existence of non-trivial units in a group ring

Definition. Let G be any group and $Z(G)$ the group ring for G. A unit $x \in Z(G)$ is *trivial* if it is of the form $\pm 1g$ for some $g \in G$. If x is not of this form it is *non-trivial*.

Definition. If $x \in Z(G)$ is a unit then x is of *finite order* iff $x^n = 1 \cdot e$ for some positive integer n. If n is the least such integer x is said to have *order n*. If no such integer n exists x is said to be of *infinite order*.

If G is a finite group the question of the existence of non-trivial units in $Z(G)$ has been completely solved. Higman [1] proves the following theorem.

Theorem. If all elements of a group G have finite order, $Z(G)$ has non-trivial units unless G is either

(i) an Abelian group the orders of whose elements all divide four

or (ii) an Abelian group the orders of whose elements all divide six

or (iii) the direct product of a quaternion group and an Abelian group, the orders of whose elements all divide two.

In these cases $Z(G)$ has only trivial units.

5. The group ring for S_3

Let S_3 be the symmetric group on three symbols and $Z(S_3)$ the group ring for S_3. If the elements of S_3 are $g_1 = (1)$, $g_2 = (123)$, $g_3 = (132)$, $g_4 = (12)$, $g_5 = (13)$ and $g_6 = (23)$ then the group matrix $X = (x_{g_i g_j^{-1}})$ for an element $x = \sum_{i=1}^{6} x_{g_i} g_i \in Z(S_3)$ is (letting $x_{g_i} = x_i$)

$$X = \begin{pmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_6 & x_4 & x_5 \\ x_3 & x_2 & x_1 & x_5 & x_6 & x_4 \\ x_4 & x_6 & x_5 & x_1 & x_2 & x_3 \\ x_5 & x_4 & x_6 & x_3 & x_4 & x_2 \\ x_6 & x_5 & x_4 & x_2 & x_3 & x_1 \end{pmatrix}$$

Suppose the elements of S_3 are taken in some order other than $(g_1, \ldots, g_6)$, say $(g_{r_1}, \ldots, g_{r_6})$. Consider the matrix $X' = (x_{g_{r_i} g_{r_j}^{-1}})$. Let P be the permutation matrix with a one in row i, column r_i, $i = 1, \ldots, 6$. Then $P^T X' P = X$.

Definition. Let A and B be square matrices and let $C = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. Then C is called the direct sum of A and B and we write $C = A \dotplus B$.

Note that $X = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$ where A, B, A^T, and B^T are 3-square circulants.

Let $$U = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega^2 & \omega & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & \omega & 1 \\ 0 & 0 & 0 & \omega & \omega^2 & 1 \\ \omega & \omega^2 & 1 & 0 & 0 & 0 \\ -\alpha & -\alpha & -\alpha & \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha & \alpha & \alpha & \alpha \end{pmatrix}$$

where $\omega = \frac{-1 + \sqrt{3}\, i}{2}$, $\alpha = \frac{1}{\sqrt{2}}$. Then U is unitary and $UXU^{-1} = Y \dotplus Y \dotplus \varepsilon_1 \dotplus \varepsilon_2$ where

$$Y = \begin{pmatrix} x_1 - x_2 + \omega(x_3 - x_2) & x_4 - x_6 + \omega(x_5 - x_6) \\ x_4 - x_6 + \omega^2(x_5 - x_6) & x_1 - x_2 + \omega^2(x_3 - x_2) \end{pmatrix}$$

$$\varepsilon_1 = x_1 + x_2 + x_3 - x_4 - x_5 - x_6$$
$$\varepsilon_2 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6.$$

<u>Definition</u>. Let X be a n-square matrix. The <u>trace of</u> X, denoted by tr$X$, is the sum of the main diagonal elements of X.

Let $E_2(x_i, x_j, x_k) = x_i x_j + x_i x_k + x_j x_k$. Then

$$\det Y = x_1^2 + x_2^2 + x_3^2 - (x_4^2 + x_5^2 + x_6^2) - E_2(x_1, x_2, x_3) + E_2(x_4, x_5, x_6)$$

$$\operatorname{tr} Y = 2x_1 - x_2 - x_3.$$

Since x_i $(i = 1, \ldots, 6)$ is a rational integer, $\det Y$, $\operatorname{tr} Y$, ε_1 and ε_2 are rational integers.

6. Units in the group ring for S_3

Theorem 2. The only units of finite order in $Z(S_3)$ are of order two, three or six.

Proof. By theorem 1, to determine the units in $Z(S_3)$ it is sufficient to determine the unimodular group matrices for S_3. If $X = (x_{g_i g_j^{-1}})$ is a group matrix for $x \in Z(S_3)$ then X is similar to $Y \dotplus Y \dotplus \varepsilon_1 \dotplus \varepsilon_2$, where Y, ε_1 and ε_2 are as in Section 5. If $\det Y = \pm 1$, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$ then since $\det X = (\det Y)^2 \varepsilon_1 \varepsilon_2$, X is unimodular. Conversely, if X is unimodular then $\det Y = \pm 1$, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$ since $\det Y$, ε_1 and ε_2 are rational integers. Since X is similar to $Y \dotplus Y \dotplus \varepsilon_1 \dotplus \varepsilon_2$, $X^n = I$ iff $Y^n = I$, $\varepsilon_1^n = 1$ and $\varepsilon_2^n = 1$.

Lemma 1. If $\det X = \pm 1$ then
$E_2(x_1, x_2, x_3) = E_2(x_4, x_5, x_6)$ where
$E_2(x_i, x_j, x_k) = x_i x_j + x_i x_k + x_j x_k$.

Proof. $\det X = \pm 1$ iff $\det Y = \pm 1$, $\varepsilon_1 = \pm 1$ and $\varepsilon_2 = \pm 1$. $\pm 1 = \det Y = x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2$

$$- E_2(x_1,x_2,x_3) + E_2(x_4,x_5,x_6)$$

$$\pm 1 = \varepsilon_1\varepsilon_2 = x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2 + 2E_2(x_1, x_2, x_3)$$
$$- 2E_2(x_4, x_5, x_6).$$

So $\varepsilon_1\varepsilon_2 - \det Y = 3[E_2(x_1,x_2,x_3) - E_2(x_4,x_5,x_6)] = 0, \pm 2$.

Since $E_2(x_1, x_2, x_3)$ and $E_2(x_4, x_5, x_6)$ are rational integers the only solution is $E_2(x_1, x_2, x_3) = E_2(x_4, x_5, x_6)$.

<u>Lemma</u> 2. Let X be unimodular with integral entries. Then $Y = cI$ iff $X = cI$.

<u>Proof</u>. Suppose $Y = cI$. Since Y has algebraic integers as elements c is an algebraic integer. Since $\operatorname{tr} Y = 2x_1 - x_2 - x_3 = 2c$ is rational, c is a rational integer. Then $\det Y = \pm 1 = c^2$ implies $c = \pm 1$. The condition $Y = cI$ implies $x_2 = x_3$, $x_4 = x_5 = x_6$, and $x_1 - x_2 = c$. Since X is unimodular

$\varepsilon_1 = x_1 + x_2 + x_3 - x_4 - x_5 - x_6 = \pm 1$ and

$\varepsilon_2 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = \pm 1$.

Hence $x_1 + x_2 + x_3 = \dfrac{\varepsilon_1 + \varepsilon_2}{2}$ $(= 0, \pm 1)$

and $x_4 + x_5 + x_6 = \dfrac{\varepsilon_2 - \varepsilon_1}{2}$ $(= 0, \pm 1)$. Since $x_1 - x_2 = c$ and $x_2 = x_3$, $\dfrac{\varepsilon_1 + \varepsilon_2}{2} - c = x_1 + x_2 + x_3 - (x_1 - x_2) = 3x_2$. But $\dfrac{\varepsilon_1 + \varepsilon_2}{2} - c = 0, \pm 2$. Hence $x_2 = 0$. Since $x_4 = x_5 = x_6$, $x_4 + x_5 + x_6 = 3x_4 = \dfrac{\varepsilon_2 - \varepsilon_1}{2}$. But $\dfrac{\varepsilon_2 - \varepsilon_1}{2} = 0, \pm 1$. Hence $x_4 = 0$. Thus $x_2 = x_3 = x_4 = x_5 = x_6 = 0$. Then $x_1 = \varepsilon_1 = \varepsilon_2$ and $0 = \dfrac{\varepsilon_1 + \varepsilon_2}{2} - c$. Hence $x_1 = c$ and $X = cI$.

If $X = cI$ then, since X is a matrix of rational integers, if X is unimodular $c = \pm 1$. Since $UXU^{-1} = cI = Y \dotplus Y \dotplus \varepsilon_1 + \varepsilon_2$, $Y = cI$.

<u>Lemma</u> 3. Let $m(\lambda)$ be the minimal polynomial for Y. Then $m(\lambda)$ is a monic polynomial with rational integers as coefficients and is of degree one or two. If $m(\lambda)$ is of degree two it is the characteristic polynomial for Y.

<u>Proof</u>. If $m(\lambda)$ is linear then $Y = cI$ so by lemma 2 $c = \pm 1$ and $m(\lambda) = \lambda \pm 1$.

If $m(\lambda)$ is of degree two then since it is monic and divides the characteristic polynomial $\lambda^2 - (\mathrm{tr}\ Y)\lambda + \det Y$ of Y, $m(\lambda) = \lambda^2 - (\mathrm{tr}\ Y)\lambda + \det Y$. Therefore since $\mathrm{tr}\ Y$ and $\det Y$ are rational integers $m(\lambda)$ has rational integer coefficients.

Since $m(\lambda)$ divides the characteristic polynomial the degree of $m(\lambda)$ cannot be greater than two.

<u>Lemma</u> 4. Suppose $x \in Z(S_3)$ satisfies $x^p = 1e$, where p is a prime greater than three. Then $x = 1e$.

<u>Proof</u>. Let X be the group matrix for x. Then $X^p = I$. Let $m(\lambda)$ be the minimal polynomial for Y. By lemma 3 $m(\lambda)$ is a monic polynomial with rational integer coefficients of degree one or two.

Case (i): $m(\lambda)$ is linear. Then $Y = cI$ so by lemma 1 $X = cI$ and $c = \pm 1$. If $c = -1$ then $X^p = -I$ contradicting $X^p = I$. Hence $X = I$ and $x = 1e$.

Case (ii): $m(\lambda)$ is of degree two. As $X^p = I$, $Y^p = I$. Hence $\lambda^p - 1$ is an annihilating polynomial for Y

and $m(\lambda)$ divides $\lambda^p - 1$. The unique factorization of $\lambda^p - 1$ over the rational number field into irreducible factors is [5]:

$$\lambda^p - 1 = (\lambda - 1)(\lambda^{p-1} + \cdots + \lambda + 1).$$

Hence $m(\lambda) = (\lambda - 1)^{e_1}(\lambda^{p-1} + \cdots + \lambda + 1)^{e_1}$ where e_1 and e_2 are 0 or 1. If $p > 3$ there is no choice of exponents e_1, e_2 that makes deg $m(\lambda)$ two.

Suppose $x \in Z(S_3)$ is of order n and $n = \prod_{i=1}^{k} p_i^{e_i}$ $(e_i > 0)$ is the canonical factorization of n into prime power factors. Let $m = \prod_{\substack{i=1 \\ i \neq j}}^{k} p_i^{e_i}$ then $(x^m)^{p_j^{e_j}} = x^n = 1e$.

Hence if $x^n = 1e$ and $p|n$ for some prime $p > 3$ then $x^m = 1e$ where $m = \frac{n}{p}$. Hence if a unit of order n exists then $n = 2^i3^j$.

<u>Lemma</u> 5. Suppose $x^{2^i3^j} = 1e$, $i \geq 2$. Then $x^{2^{i-1}3^j} = 1e$.

<u>Proof</u>. Let $x' = x^{2^{i-2}3^j}$. Then $(x')^4 = 1e$. Let X be the group matrix for x' and $m(\lambda)$ the minimal polynomial for the associated Y. Then deg $m(\lambda)$ is one or two.

Case (i): $m(\lambda)$ is linear. Then $Y = cI$ so by lemma 2 $X = cI$ and $c = \pm 1$. Hence $X^2 = I$ and $(x')^2 = 1e$. Since $(x')^2 = x^{2^{i-1}3^j}$ this implies the result.

Case (ii): $m(\lambda)$ is of degree two. Since $X^4 = I$, $Y^4 = I$ so $\lambda^4 - 1$ is an annihilating polynomial for Y. The unique factorization of $\lambda^4 - 1$ into factors irreducible over the rational number field is $\lambda^4 - 1 = (\lambda - 1)(\lambda + 1)(\lambda^2 + 1)$. By lemma 3 $m(\lambda) = \lambda^2 - (\text{tr } Y)\lambda + \det Y$ has rational coefficients so we have two possibilities (a) $m(\lambda) = \lambda^2 - 1$

(b) $m(\lambda) = \lambda^2 + 1$.

Case (a): If $m(\lambda) = \lambda^2 - 1$ then $Y^2 = I$ so $Y^2 \dotplus Y^2 \dotplus \varepsilon_1^2 \dotplus \varepsilon_2^2 = I$. Hence $X^2 = I$ so

$(x')^2 = x^{2^{i-1}3^j} = 1e$.

Case (b): If $m(\lambda) = \lambda^2 + 1$ then since $m(\lambda) = \lambda^2 - (\text{tr } Y)\lambda + \det Y$ it follows that $\text{tr } Y = 2x_1 - x_2 - x_3 = 0$ and $\det Y = 1$. Since $\text{tr } X = 6x_1 = 2 \text{ tr } Y + \varepsilon_1 + \varepsilon_2$; $\text{tr } Y = 0$, $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$ implies $\text{tr } X = 0$ so $x_1 = 0$ and $\varepsilon_1 = -\varepsilon_2$. Since $\varepsilon_1 = x_1 + x_2 + x_3 - x_4 - x_5 - x_6$ and $\varepsilon_2 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6$, $\varepsilon_1 + \varepsilon_2 = 0 = x_1 + x_2 + x_3$ and $x_4 + x_5 + x_6 = \pm 1$. Hence $x_2 = -x_3$. Using lemma 1 and the above results gives

(1) $\det Y = 2x_2^2 - (x_4^2 + x_5^2 + x_6^2) = 1$

(2) $E_2(x_1, x_2, x_3) = -x_2^2 = x_4x_5 + x_4x_6 + x_5x_6 = E_2(x_4, x_5, x_6)$.

Multiplying equation (2) by two and adding it to equation (1) gives

$$-[(x_4^2 + x_5^2 + x_6^2) + 2(x_4x_5 + x_4x_6 + x_5x_6)] = -[(x_4 + x_5 + x_6)^2] = 1$$

but this is a contradiction since $-(x_4 + x_5 + x_6)^2 \leq 0$. Hence case (b) cannot occur and the proof is complete.

Lemma 6. Suppose $x^{2^i 3^j} = 1e$, $j \geq 2$, then $x^{2^i 3^{j-1}} = 1e$.

Proof. Let $x' = x^{2^i 3^{j-2}}$. Then $(x')^9 = x^{2^i 3^j} = 1e$. Let X be the group matrix for x'. Then $X^9 = I$ so $Y^9 = I$. Let $m(\lambda)$ be the minimal polynomial for Y. Since $\lambda^9 - 1$ is an annihilating polynomial for Y, $m(\lambda)$ divides $\lambda^9 - 1$. The unique factorization of $\lambda^9 - 1$ into factors irreducible over the rational number field is [5]

$$\lambda^9 - 1 = (\lambda - 1)(\lambda^2 + \lambda + 1)(\lambda^6 + \lambda^3 + 1).$$

Since by lemma 3 $m(\lambda)$ is a monic polynomial with rational integer coefficients of degree one or two it follows that $m(\lambda) = \lambda - 1$ or $m(\lambda) = \lambda^2 + \lambda + 1$.

Case (i): $m(\lambda) = \lambda - 1$. Then $Y = I$ so by lemma 2 $X = I$ so $x' = 1e$. Hence $(x')^3 = x^{2^i 3^{j-1}} = 1e$.

Case (ii): $m(\lambda) = \lambda^2 + \lambda + 1$. Then $Y^2 + Y + I = 0$, $(Y - I)(Y^2 + Y + I) = 0 = Y^3 - I$. Hence $Y^3 = I$. Since $X^9 = I$, $\varepsilon_1^9 = \varepsilon_2^9 = 1$ so that since 9 is odd $\varepsilon_1 = \varepsilon_2 = 1$. Hence $Y^3 \dotplus Y^3 \dotplus \varepsilon_1^3 \dotplus \varepsilon_2^3 = X^3 = I$. Therefore $(x')^3 = x^{2^i 3^{j-1}} = 1e$.

Combining lemmas 5 and 6 it follows that if $x \in Z(S_3)$ is a unit of order $n = 2^i 3^j$ then $i, j = 0$ or 1. Hence the only units of finite order are of order two, three or six.

We will now proceed to find infinitely many units of each of these orders as well as infinitely many units of infinite order.

The following equations will be useful in further investigation of units of finite order. Using the same notation as before,

(1) $x_1 + x_2 + x_3 = \frac{\varepsilon_1 + \varepsilon_2}{2}$ $(= 0, \pm 1)$

(2) $x_4 + x_5 + x_6 = \frac{\varepsilon_2 - \varepsilon_1}{2}$ $(= 0, \pm 1)$

(3) $6x_1 = \mathrm{tr}\ X = 2\ \mathrm{tr}\ Y + \varepsilon_1 + \varepsilon_2$

(4) $\mathrm{tr}\ Y = 2x_1 - x_2 - x_3$.

Suppose x is a unit of order two and X the group matrix for x. Then $Y^2 = I$ and $m(\lambda)|\lambda^2 - 1$. Hence $m(\lambda) = \lambda - 1, \lambda + 1$ or $\lambda^2 - 1$. If $m(\lambda)$ is linear then by lemma 2 $X = \pm I$ since $Y = \pm I$.

Suppose $m(\lambda) = \lambda^2 - 1$. Then by lemma 3 $m(\lambda)$ is the characteristic polynomial for Y, $\lambda^2 - (\mathrm{tr}\ Y)\lambda + \det Y$. Hence $\mathrm{tr}\ Y = 0$ and from (3) $\mathrm{tr}\ X = 0$, $x_1 = 0$. Since $\mathrm{tr}\ Y = 2x_1 - x_2 - x_3 = 0$ it follows that $x_2 = x_3$. From (1) and (2) it is clear that $x_4 + x_5 + x_6 = \pm 1$. Hence if $X^2 = I$ either $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = m$, $x_5 = n$, $x_6 = \pm 1 - m - n$, where k, m and n are rational integers, or $X = -I$. Since x is a unit, $\det X = \pm 1$ by Theorem 1. Hence by lemma 1 $E_2(0, k, -k) = E_2(m, n, \pm 1 - m - n)$. Hence k, m and n must satisfy (I) $k^2 - m^2 - mn - n^2 \pm m \pm n = 0$.

Conversely suppose k, m and n satisfy (I). Then if $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = m$, $x_5 = n$, $x_6 = \pm 1 - m - n$; $E_2(x_1, x_2, x_3) = E_2(x_4, x_5, x_6)$ so

$\det Y = x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2 = -1$,

$\text{tr } Y = 2x_1 - x_2 - x_3 = 0$, $\varepsilon_1 = x_1 + x_2 + x_3 - x_4 - x_5 - x_6 = \mp 1$, $\varepsilon_2 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = \pm 1$. Hence $\det X = (\det Y)^2 \varepsilon_1 \varepsilon_2 = -1$ and $\lambda^2 - 1$ is the characteristic polynomial for Y. Therefore $Y^2 = I$ so $X^2 = I$ and x is of order two.

If $m = k$, $n = -k$ equation (I) is satisfied. Hence infinitely many units of order two are given by $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = k$, $x_5 = -k$, $x_6 = \pm 1$, where k is any rational integer. Since the choice of two of x_4, x_5 and x_6 was arbitrary, two other infinite classes of units of order two are given by $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = \pm 1$, $x_5 = k$, $x_6 = -k$ and $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = k$, $x_5 = \pm 1$, $x_6 = -k$.

Suppose x is a unit of order three and X is the group matrix for x. Then $Y^3 = I$ and $m(\lambda) | \lambda^3 - 1$. Since $\lambda^3 - 1 = (\lambda - 1)(\lambda^2 + \lambda + 1)$ this implies, using lemma 3, that $m(\lambda) = \lambda - 1$ or $m(\lambda) = \lambda^2 + \lambda + 1$. It was shown above that $m(\lambda) = \lambda - 1$ then $X = I$. Suppose $m(\lambda) = \lambda^2 + \lambda + 1$. Since $\deg m(\lambda) = 2$, $m(\lambda)$ is the characteristic polynomial for Y, $\lambda^2 - (\text{tr } Y)\lambda + \det Y$. Hence $\text{tr } Y = -1$. Using this together with (3) it follows that $x_1 = 0$ and $\varepsilon_1 = \varepsilon_2 = 1$. From (1) and (2) it now follows that $x_1 + x_2 + x_3 = 1$, $x_4 + x_5 + x_6 = 0$. Hence if x is a unit of order three, $x_1 = 0$, $x_2 = k$, $x_3 = 1 - k$, $x_4 = m$, $x_5 = n$, $x_6 = -m - n$; where k, m and n are rational integers. Since x is a unit $\det X = \pm 1$ so by lemma 1 k, m and n must satisfy

(II) $k(1 - k) + m^2 + mn + n^2 = 0$.

Conversely suppose k, m and n satisfy (II). If $x_1 = 0$, $x_2 = k$, $x_3 = 1 - k$, $x_4 = m$, $x_5 = n$, $x_6 = -m - n$, then $E_2(x_1, x_2, x_3) = E_2(x_4, x_5, x_6)$ so
$\det Y = x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2 = 1$,
$\operatorname{tr} Y = 2x_1 - x_2 - x_3 = -1$, $\varepsilon_1 = x_1 + x_2 + x_3 - x_4 - x_5 - x_6 = 1$, $\varepsilon_2 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 1$. Hence $\det X = (\det Y)^2\varepsilon_1\varepsilon_2 = 1$ and $\lambda^2 + \lambda + 1$ is the characteristic polynomial for Y. Therefore $Y^2 + Y + I = 0$. Hence $(Y - I)(Y^2 + Y + K) = Y^3 - I = 0$, $Y^3 = I$ so $I = Y^3 \dotplus Y^3 \dotplus \varepsilon_1^3 \dotplus \varepsilon_2^3 = X^3$ and x is of order three.

Suppose $x \in Z(S_3)$ is such that for some rational integer k, $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = k$, $x_5 = -k$ and $x_6 = \pm 1$. Then as was shown above x is a unit of order two. Recall $g_2 = (123) \in S_3$. Consider $y = xg_2x$, $y_1 = 0$, $y_2 = -3k^2$, $y_3 = 3k^2 + 1$, $y_4 = -3k^2 \pm k$, $y_5 = \mp 2k$ and $y_6 = 3k \pm k$. Clearly $y \neq 1e$ and $y^3 = (xg_2x)^3 = xg_2xxg_2xxg_2x = 1e$ so y is a unit of order three. This gives an infinite class of units of order three. Using g_3 will give another class as will using different classes of units of order two.

This technique for obtaining units of order three from units of order two is discussed in Taussky's paper [6].

Suppose x is a unit of order six and X is the group matrix for x. Then $X^6 = I$, so $Y^6 = I$ and $m(\lambda)|\lambda^6 - 1$.

Since $\lambda^6 - 1 = (\lambda - 1)(\lambda^2 + \lambda + 1)(\lambda + 1)(\lambda^2 - \lambda + 1)$ this implies $m(\lambda) = \lambda - 1, \lambda + 1, \lambda^2 - 1, \lambda^2 + \lambda + 1$ or $\lambda^2 - \lambda + 1$. If $m(\lambda)$ is linear then by lemma 2 $X = \pm I$ so X is not of order six. If $m(\lambda) = \lambda^2 - 1$ then as above $X^2 = I$ and X is not of order six. Suppose $m(\lambda) = \lambda^2 + \lambda + 1$. Then since $m(\lambda)$ is the characteristic polynomial for Y, $\operatorname{tr} Y = -1$. Using this together with (3) it follows that $x_1 = 0$, $\varepsilon_1 = \varepsilon_2 = 1$. Since $m(\lambda) = \lambda^2 + \lambda + 1$ it follows that $(Y - I)(Y^2 + Y + I) = Y^3 - I = 0$. Hence $X^3 = Y^3 \dotplus Y^3 \dotplus \varepsilon_1^3 \dotplus \varepsilon_2^3 = I$, a contradiction. Suppose $m(\lambda) = \lambda^2 - \lambda + 1$. Then since $m(\lambda)$ is the characteristic polynomial for Y, $\operatorname{tr} Y = 1$. Using this together with (3) it follows that $x_1 = 0$, $\varepsilon_1 = \varepsilon_2 = -1$. Since $(Y + I)(Y^2 - Y + I) = Y^3 + I = 0$ it follows that $X^3 = Y^3 \dotplus Y^3 \dotplus \varepsilon_1^3 \dotplus \varepsilon_2^3 = -I$. Hence $(-X)^3 = I$ so $-X$ is a unit of order three. If Z is a unit of order three clearly $-Z$ is a unit of order six. Hence every unit of order six is of the form $-Z$ where Z is a unit of order three.

There exist infinitely many units of infinite order in $Z(S_3)$. Suppose $x \in Z(S_3)$ is such that $x_1 = 0$, $x_2 = k$, $x_3 = -k$, $x_4 = k$, $x_5 = -k$, $x_6 = \pm 1$ for some rational integer k. Then x is of order two. Let X be the group matrix for X. Consider the unit y corresponding to the group matrix $Y = X^T X$. If $y = \sum_{i=1}^{6} y_i g_i$ then $y_1 = 4k^2 + 1$, $y_2 = -2k^2$, $y_3 = -2k^2$, $y_4 = 2k^2 \pm 2k$, $y_5 = 2k^2 \mp 2k$, $y_6 = -4k^2$. Since all units y of finite order except $\pm I$ have $y_1 = 0$, y

cannot be of finite order unless $k = 0$. This gives an infinite class of units of infinite order.

7. The equation $G = AA^T$ in the ring of group matrices for S_3

Let H be any finite group and suppose G is a unimodular group matrix for H. If $G = AA^T$, where A is a matrix of rational integers, is it possible to find a group matrix C such that $G = CC^T$? This question has been answered in the affirmative for cyclic groups by Newman and Taussky [4] and for abelian groups by Thompson [7]. This question will now be investigated for the group S_3.

Let $G = AA^T$ be a unimodular group matrix for S_3 where A is a matrix of rational integers. As discussed in section 5 the group matrix depends on the numbering of the elements of S_3. If another numbering of elements is used the matrix X in section 5 is converted to P^TXP, P a permutation matrix. Since if $D = P^TCP$, $DD^T = P^TCC^TP = P^TGP$, without loss of generality G may be taken in the form $\begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$ where A, B, A^T and B^T are 3-square circulants.

Let $P_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

$$Q_1 = \begin{pmatrix} P_1 & 0 \\ 0 & P_1 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 0 & P_2 \\ P_2 & 0 \end{pmatrix}.$$

Definition. The permutation $\sigma = (12\cdots(n-1)n) \in S_n$ is the n-cycle. The matrix $P \in M_n(Z)$ defined by $P_{ij} = \varepsilon_{ij}\delta_{i\sigma(j)}$ $(\varepsilon_{ij} = \pm 1)$ is a generalized n-cycle.

The following lemmas will be needed.

Lemma 7. If C is any 3-square circulant then $P_2CP_2 = C^T$.

Proof. The result follows by direct computation.

Lemma 8. The matrices Q_1 and Q_2 commute with the matrix G.

Proof. The result follows by computation, the fact that P_1 commutes with all 3-square circulants, and lemma 7.

Lemma 9. The matrices $A^{-1}Q_1A$ and $A^{-1}Q_2A$ are orthogonal.

Proof. For $i = 1, 2$; $(A^{-1}Q_iA)(A^{-1}Q_iA)^T = A^{-1}Q_iAA^TQ_i^T(A^{-1})^T = AA^{-1}A^TQ_iQ_i^T(A^T)^{-1} = A^T(A^T)^{-1} = I$ by lemma 8.

Lemma 10. There exist generalized permutation matrices M_1 and M_2 such that $Q_1A = AM_1$ and $Q_2A = AM_2$.

Proof. The only orthoganal matrices of rational integers are the generalized permutation matrices so by lemma 9 there exist generalized permutation matrices M_1 and M_2 such that $A^{-1}Q_1A = M_1$ and $A^{-1}Q_2A = M_2$.

Lemma 11. Let M be a generalized permutation matrix. Then M is similar, via a permutation matrix, to a direct sum of generalized m-cycles.

Proof. The result is obviously true if M is a 1-square matrix. Assume the result true for all $r < n$ and suppose M is a n-square generalized permutation matrix. If there is a non-zero entry in the (1, 1) position of M the result follows by induction on the matrix obtained by deleting the first row and first column of M. If $M_{11} = 0$ then there is a non-zero element in the first row of M. Suppose the non-zero element is M_{1j}. By post multiplying M by a permutation matrix P_1 interchange the second column and the j^{th} column. Since left multiplication of MP_1 by P_1^{-1} does not affect the first row of MP_1, $P_1^{-1}MP_1$ has a ± 1 in the (1, 2) position. If $P_1^{-1}MP_1$ has a ± 1 in the (2, 1) position the result follows by induction. If not, then there exists a ± 1 in position $(2, j)$ for some $j \geq 3$. Interchange columns 3 and j and rows 3 and j. Then either the (3, 1) element is a ± 1 in which case the cycle closes off and the result follows by induction, or there is a non-zero element $(3, j)$ for some $j \geq 4$. In this case repeat the above process. Since M is a generalized permutation matrix a ± 1 must eventually appear in column 1. If this happens for some $i < n$ the result follows by induction. If this happens for $i = n$ M is similar to the n-cycle.

Lemma 12. Let R be the ring of matrices over Z generated by P_1 and P_2. Then

$$R = \{X \in M_3(Z): X = x_1 I + x_2 P_1 + x_3 P_1^2 + x_4 P_2 + x_5 P_1 P_2 + x_6 P_1^2 P_2,\ x_i \in Z\}.$$

<u>Proof</u>. Clearly R contains I, P_1, P_1^2, P_2, P_1P_2 and $P_1^2P_2$ $(= P_2P_1)$. Since these six matrices form a representation of S_3 in $M_3(Z)$ this set is closed multiplicitively. Since R is a ring of matrices over Z it must contain all linear combinations of the above six matrices. The set

$$\{X \in M_3(Z): X = x_1I + x_2P_1 + x_3P_1^2 + x_4P_2 + x_5P_1P_2 + x_6P_1^2P_2, \; x_i \in Z\}$$

is a ring. Since R is the smallest ring containing P_1 and P_2 it is of the desired form.

Let A_i denote the i^{th} row of A and write A as a matrix of its rows: $A = \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \\ A_5 \\ A_6 \end{pmatrix}$

Then $Q_1A = \begin{pmatrix} A_2 \\ A_3 \\ A_1 \\ A_5 \\ A_6 \\ A_4 \end{pmatrix}$ $\qquad AM_1 = \begin{pmatrix} A_1M_1 \\ A_2M_1 \\ A_3M_1 \\ A_4M_1 \\ A_5M_1 \\ A_6M_1 \end{pmatrix}$

so, since $Q_1A = AM_1$ by lemma 10, $A_2 = A_1M_1$, $A_3 = A_2M_1 = A_1M_1^2$ and $A_5 = A_4M_1$, $A_6 = A_5M_1 = A_4M_1^2$, hence

$$A = \begin{pmatrix} A_1 \\ A_1M_1 \\ A_1M_1^2 \\ A_4 \\ A_4M_1 \\ A_4M_1^2 \end{pmatrix}$$

By lemma 11 there exists a permutation matrix S such that $S^TM_1S = P_{n_1} \dotplus \cdots \dotplus P_{n_k}$ where P_{n_j} $(j = 1, \cdots, k)$ is a generalized n_j cycle. Hence $Q_1AS = AS\ (P_{n_1} \dotplus \cdots \dotplus P_{n_k})$. Since $(AS)(AS^T) = ASS^TA^T = AA^T = G$ we may assume without loss of generality that $M_1 = P_{n_1} \dotplus \cdots \dotplus P_{n_k}$.

Since $Q_1^3 = I$, $(A^{-1}Q_1A)^3 = M_1^3 = P_{n_1}^3 \dotplus \cdots \dotplus P_{n_k}^2 = I$ so $P_{nj}^2 = I$ for all j. If $n_j > 3$ $P_{n_j}^3 \neq I$ so none of the P_{n_j} are generalized 4, 5 or 6 cycles. If $n_j = 2$ for some j then $P_{n_j} = \begin{pmatrix} 0 & \sigma_1 \\ \sigma_2 & 0 \end{pmatrix}$ $\sigma_1 = \pm 1$, $\sigma_2 = \pm 1$

and $P_{n_j}^3 = \pm P_{n_j} \neq I$. Hence M_1 cannot contain any 2-cycles. Since $n_j = 1$ or 3 and $n_1 + \cdots + n_k = 6$ if M_1 contains a 1-cycle it must contain three.

To show M_1 cannot contain any 1-cycles a technique due to Newman and Taussky is used [4]. Suppose M_1 contains a 1-cycle. Then it contains three 1-cycles. Two 1-cycles must appear either in the (1, 1) and (2, 2) positions or in the

(5, 5) and (6, 6) positions. Without loss of generality assume they appear in the (1, 1) and (2, 2) positions. Then M_1 (mod 2) has the following form.

$$M_1 \equiv \left(\begin{array}{cc:c} 1 & 0 & \\ 0 & 1 & 0 \\ \hdashline & 0 & P \end{array}\right) \pmod 2.$$

where P is a 4-square permutation matrix. Since $A_2 = A_1M_1$, $A_3 = A_1M_1^2$, $A_5 = A_4M_1$ and $A_6 = A_4M_1^2$, A (mod 2) has the following form.

$$A \equiv \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{11} & a_{12} & * & * & * & * \\ a_{11} & a_{12} & * & * & * & * \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} \\ a_{41} & a_{42} & * & * & * & * \\ a_{41} & a_{42} & * & * & * & * \end{pmatrix} \pmod 2$$

The elements in rows 2 and 3 and columns 3, ..., 6 are just $(a_{13}, a_{14}, a_{15}, a_{16})$ permuted by P and P^2 respectively. Similarly, the elements in rows 5 and 6 and columns 3, ..., 6 are just $(a_{43}, a_{44}, a_{45}, a_{46})$ permuted by P and P^2 respectively.

The determinant of A is now computed modulo two. First add column 4, 5 and 6 to column 3. This leaves det A (mod 2) unchanged and

$$\det A \equiv \det \begin{pmatrix} a_{11} & a_{12} & c_1 & * & * & * \\ a_{11} & a_{12} & c_1 & * & * & * \\ a_{11} & a_{12} & c_1 & * & * & * \\ a_{41} & a_{42} & c_2 & * & * & * \\ a_{41} & a_{42} & c_2 & * & * & * \\ a_{41} & a_{42} & c_2 & * & * & * \end{pmatrix} \pmod 2$$

where $c_1 = a_{13} + a_{14} + a_{15} + a_{16}$, $c_2 = a_{43} + a_{44} + a_{45} + a_{46}$ all sums being modulo two.

Now add row one to rows two and three and add row four to rows five and six. Then det A (mod 2) is unchanged and

$$\det A \equiv \det \begin{pmatrix} a_{11} & a_{12} & c_1 & * & * & * \\ 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \\ a_{41} & a_{42} & c_2 & * & * & * \\ 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & * & * & * \end{pmatrix} \pmod 2$$

Columns 1, 2 and 3 are essentially 2-vectors over the field of residue classes modulo two. Since there are three such vectors they are linearly dependent. Hence $\det A \equiv 0 \bmod 2$. Since $G = AA^T$ is unimodular, $\det A \equiv 1 \pmod 2$, $\det A \equiv 0 \pmod 2$ is a contradiction and M_1 cannot contain any 1-cycles.

Since M_1 cannot contain any 1, 2, 4, 5 or 6 cycles $M_1 = R_1 \dotplus R_2$ where R_1 and R_2 are generalized 3-cycles.

Let $R_1 = \begin{pmatrix} 0 & \tau_1 & 0 \\ 0 & 0 & \tau_2 \\ \tau_3 & 0 & 0 \end{pmatrix}$, $R_2 = \begin{pmatrix} 0 & \sigma_1 & 0 \\ 0 & 0 & \sigma_2 \\ \sigma_3 & 0 & 0 \end{pmatrix}$

where $\tau_i = \pm 1$, $\sigma_i = \pm 1$.

Since $I = (A^{-1}Q_1A)^3 = M_1^3 = R_1^3 \dotplus R_2^3$ and $R_1^3 = \tau_1\tau_2\tau_3 I$, $R_2^3 = \sigma_1\sigma_2\sigma_3 I$; $\tau_1\tau_2\tau_3 = 1$ and $\sigma_1\sigma_2\sigma_3 = 1$.

Let $S_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \tau_1 & 0 \\ 0 & 0 & \tau_1\tau_2 \end{pmatrix}$, $S_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sigma_1 & 0 \\ 0 & 0 & \sigma_1\sigma_2 \end{pmatrix}$.

Then $S_1^T R_1 S_1 = P_1$ and $S_2^T R_2 S_2 = P_1$. Let $S = S_1 \dotplus S_2$, then $S^T M_1 S = P_1 \dotplus P_1 = Q_1$. Hence $Q_1AS = ASQ_1$. Since $(AS)(AS)^T = AA^T = G$ without loss of generality let $M_1 = Q_1$ so $Q_1A = AQ_1$.

Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ where the A_{ij} are 3-square matrices of rational integers. Then

$$Q_1A = \begin{pmatrix} P_1A_{11} & P_1A_{12} \\ P_1A_{21} & P_1A_{22} \end{pmatrix} = \begin{pmatrix} A_{11}P_1 & A_{12}P_1 \\ A_{11}P_1 & A_{22}P_1 \end{pmatrix} = AQ_1.$$

Hence $P_1A_{ij} = A_{ij}P_1$ (i, j = 1, 2) and since any matrix that commutes with P_1 is a circulant, each of the A_{ij} is a 3-square circulant.

Since A^{-1} is a polynomial in A and the sum and product of circulants are circulants, A^{-1}, when considered as a 2-square matrix with 3-square matrices as elements, has elements that are circulants. Also A^{-1} has rational integer elements as $\det A = \pm 1$. Every 3-square circulant of rational integers is a linear combination of I, P_1 and P_1^2. Since

$$Q_2 = \begin{pmatrix} 0 & P_2 \\ P_2 & 0 \end{pmatrix} \quad \text{and} \quad A^{-1}Q_2A = M_2,$$

M_2 may be considered as a 2-square matrix with elements in the ring R of 3-square matrices over the rational integers generated by P_1 and P_2.

Let $M_2 = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$ where M_{ij} = (i, j = 1, 2) is a 3-square matrix of rational integers.

Consider the first row of M_2. Since M_2 is a generalized permutation matrix there is a ± 1 either in M_{11} or M_{12}. Suppose it is in M_{11}. If the non-zero element is not in the (1, 1) position of M_{11} by post multiplying M_2 by a matrix of the form $P \dotplus P$, where $P = P_1$ or P_1^2, bring the non-zero element to the (1, 1) position.

Note that since $\begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix} = \begin{pmatrix} M_{11}P & M_{21}P \\ M_{21}P & M_{22}P \end{pmatrix}$

post multiplication by $P \dotplus P$ does not shift elements from one block M_{ij} to another, and since $M_{ij} \in R$, $M_{ij}P \in R$.

Since $M_{11} \in R$, the ring of matrices over Z generated by P_1 and P_2, by lemma 12

$$M_{11}P = x_1I + x_2P_1 + x_3P_1^2 + x_4P_2 + x_5P_1P_2 + x_6P_1^2P_2$$

$$= \begin{pmatrix} x_1 + x_4 & x_2 + x_6 & x_3 + x_5 \\ x_3 + x_6 & x_1 + x_5 & x_1 + x_4 \\ x_2 + x_5 & x_3 + x_4 & x_1 + x_6 \end{pmatrix}$$

Since M_2 is a generalized permutation matrix there is at most one non-zero entry in each row and column of $M_{11}P$. Since it was assumed that $x_1 + x_4 = \pm 1$ this observation results in the following equations:

(1) $x_1 + x_4 = \pm 1$

(2) $x_3 + x_6 = 0$

(3) $x_2 + x_5 = 0$

(4) $x_2 + x_6 = 0$

(5) $x_3 + x_5 = 0$

Equations (2) and (4) yield $x_1 = x_3$ and equations (2) and (5) yield $x_5 = x_6$. Using these facts $M_{11}P$ has the form

$$M_{11}P = \begin{pmatrix} x_1 + x_4 & 0 & 0 \\ 0 & x_1 + x_5 & x_3 + x_4 \\ 0 & x_3 + x_4 & x_1 + x_5 \end{pmatrix}$$

If $x_1 + x_5 = 0$ and $x_3 + x_4 = 0$, these equations together with equation (5) above yield $x_1 + x_4 = 0$, contradicting $x_1 + x_4 = \pm 1$. Hence $M_{11}P = \pm I$ or $\pm P_2$ and since $P = I$, P_1 or P_1^2; $M_{11} = \pm I, \pm P_1, \pm P_1^2, \pm P_2,$ $\pm P_1P_2$ or $\pm P_1^2P_2$. Since M_2 is a generalized permutation matrix $M_{11} \neq 0$ implies $M_{12} = M_{21} = 0$ so M_{22} is a 3-square generalized permutation matrix. Similarly if $M_{21} \neq 0$

$M_{11} = M_{22} = O$ and M_{12} is a 3-square generalized permutation matrix. Hence $M_2 = \begin{pmatrix} E_1 & O \\ O & E_2 \end{pmatrix}$ or $M_2 = \begin{pmatrix} O & E_1 \\ E_2 & O \end{pmatrix}$ where E_i $(i = 1, 2)$ is a 3-square generalized permutation matrix.

Suppose $M_2 = \begin{pmatrix} E_1 & O \\ O & E_1 \end{pmatrix}$. By lemma 6

$$Q_2A = \begin{pmatrix} P_2A_{11} & P_2A_{12} \\ P_2A_{21} & P_2A_{22} \end{pmatrix} = \begin{pmatrix} A_{11}E_1 & A_{12}E_2 \\ A_{21}E_1 & A_{22}E_2 \end{pmatrix} = AM_2$$

so $A_{21} = P_2A_{11}E_1$ and $A_{22} = P_2A_{12}E_2$. Then

$$A = \begin{pmatrix} I & O \\ O & P_2 \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ A_{11}E_1 & A_{12}E_2 \end{pmatrix}.$$

Consider det A (mod 2). Since $\det \begin{pmatrix} I & O \\ O & P_2 \end{pmatrix} \equiv 1 \pmod 2$

$$\det A \equiv \det \begin{pmatrix} A_{11} & A_{12} \\ A_{11}E_1 & A_{12}E_2 \end{pmatrix} \pmod 2.$$

Post multiplication of A_{11} by E_1 interchanges the columns of A_{11} in some way (mod 2), since E_1 is a permutation matrix modulo 2. Similarly post multiplication of A_{12} by E_2 interchanges the columns of A_{12} in some way (mod 2).

Add columns 2 and 3 to column 1 and columns 5 and 6 to column 4. The determinant of A modulo 2 is unchanged and

$$\det A \equiv \det \begin{pmatrix} C_1 & * & * & D_1 & * & * \\ C_1 & * & * & D_1 & * & * \\ C_1 & * & * & D_1 & * & * \\ C_1 & * & * & D_1 & * & * \\ C_1 & * & * & D_1 & * & * \\ C_1 & * & * & D_1 & * & * \end{pmatrix} \pmod 2$$

where C_1 denotes the row sum of A_{11} and D_1 the row sum of A_{12}. Since A_{11} and A_{12} are circulants the row sums are the same for each row of A_{11} and each row of A_{12}.

Now add the first row to each of the others to obtain

$$\det A \equiv \det \begin{pmatrix} C_1 & * & * & D_1 & * & * \\ 0 & * & * & 0 & * & * \\ 0 & * & * & 0 & * & * \\ 0 & * & * & 0 & * & * \\ 0 & * & * & 0 & * & * \\ 0 & * & * & 0 & * & * \end{pmatrix} \pmod 2$$

Columns 1 and 4 are essentially two 1-vectors of the field of integers modulo 2 so are linearly dependent and $\det A \equiv 0 \pmod 2$ which is a contradiction. Hence M_2 is of the form $\begin{pmatrix} 0 & E_1 \\ E_2 & 0 \end{pmatrix}$.

By lemma 10 $M_2 = A^{-1}Q_2A$ and since $Q_2^2 = I$

$$(A^{-1}Q_2A)^2 = M_2^2 = \begin{pmatrix} E_1E_2 & 0 \\ 0 & E_2E_1 \end{pmatrix} = I.$$

Hence $E_2 = E_1^{-1} = E_1^T$.

Since $Q_1A = AQ_1$ and $Q_2A = AM_2$ it follows that $Q_1Q_2Q_1A = Q_1Q_2AQ_1 = Q_1AM_2Q_1 = AQ_1M_2Q_1$. Since $Q_1Q_2Q_1 = Q_2$ this implies $Q_2A = AM_2 = AQ_1M_2Q_1$ and since A is non-singular,

$$Q_1M_2Q_1 = \begin{pmatrix} 0 & P_1E_1P_1 \\ P_1E_1^TP & 0 \end{pmatrix} = \begin{pmatrix} 0 & E_1 \\ E_1^T & 0 \end{pmatrix} = M_2.$$

Hence $P_1E_1P_1 = E_1$. It has already been proved that E_1 is one of $\pm I$, $\pm P_1$, $\pm P_1^2$, $\pm P_2$, $\pm P_1P_2$, $\pm P_1^2P_2$. Since $P_1E_1P_1 = E_1$, E_1 cannot be any of $\pm I$, $\pm P_1$, $\pm P_1^2$. Since $P_1P_2 = P_2P_1^2$ and $P_1^2P_2 = P_2P_1$ it follows that $E_1 = \pm P_2P_1^j$ $(1 \leq j \leq 3)$. Hence since $(P_2P_1^j)^T = P_2P_1^j$,

$$M_2 = \pm \begin{pmatrix} 0 & P_2P_1^j \\ P_2P_1^j & 0 \end{pmatrix}$$

By lemma 6,

$$Q_2A = \begin{pmatrix} P_2A_{21} & P_2A_{22} \\ P_2A_{11} & P_2A_{12} \end{pmatrix} = \pm \begin{pmatrix} A_{12}P_2P_1^j & A_{11}P_2P_1^j \\ A_{22}P_2P_1^j & A_{21}P_2P_1^j \end{pmatrix} = AM_2.$$

Hence $A_{21} = \pm P_2A_{12}P_2P_1^j$ and $A_{22} = \pm P_2A_{11}P_2P_1^j$. Recall A_{11} and A_{12} are 3-square circulants so by lemma 7 $A_{21} = \pm A_{12}^TP_1^j$ and $A_{22} = \pm A_{11}^TP_1^j$. Since A_{12}^T and A_{11}^T are circulants they commute with P_1^j so $A_{21} = \pm P_1^jA_{12}^T$ and $A_{22} = \pm P_1^jA_{11}^T$.

Choose k such that $j + k = 3$, then $P_1^{j+k} = I$. Let $K = \begin{pmatrix} \pm I & 0 \\ 0 & P_1^k \end{pmatrix}$. Then

$$AK = \begin{pmatrix} I & 0 \\ 0 & \pm P_1^k \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} \\ \pm P_1^j A_{12}^T & \pm P_1^j A_{11}^T \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} \\ P_1^{j+k} A_{12}^T & P_1^{j+k} A_{11}^T \end{pmatrix}$$

$$= \begin{pmatrix} A_{11} & A_{12} \\ A_{12}^T & A_{11}^T \end{pmatrix} = C.$$

Since A_{11} and A_{12} are circulants C is a group matrix. Further $CC^T = AKK^TA^T = AA^T = G$, since K is a generalized permutation matrix.

Theorem 3. Let G be a unimodular group matrix for the group S_3 and suppose $G = AA^T$ where A is a matrix of rational integers. Then there exists a group matrix C such that $G = CC^T$.

Definition. Suppose $x \in Z(S_3)$ is a unit. Then x is positive definite symmetric iff the group matrix for x is positive definite symmetric.

This definition is independent of the order in which the group elements are taken since it was shown in section 4 that group matrices for a fixed element $x \in Z(S_3)$ corresponding to different orderings of group elements are similar via a permutation matrix.

Since it is known [2] that any n-square unimodular positive definite symmetric matrix of rational integers is of the form AA^T if $n \leq 7$ (this is false if $n > 7$) the following result is also clear.

Theorem 4. If H is any unimodular positive definite symmetric group matrix of rational integers for the group S_3 then $H = H_1 H_1^T$ where H_1 is a group matrix of rational integers for S_3.

It is known [3] that if H is positive definite then $H_{11} > 0$. Since H is a group matrix $H_{ii} = H_{11}$, $i = 1, \dots, 6$. It was established in section 6 that the group matrix for a unit of finite order has a zero diagonal. Hence the following result is clear.

Theorem 5. The positive definite units in $Z(S_3)$ are all of infinite order.

There are infinitely many positive definite units of infinite order. Explicit formulas for an infinite number of positive definite units may be found on page 18.

Bibliography

1. G. Higman, The units of group rings, Proc. London Math. Soc. vol. 46 (1940) pp. 231-248.

2. M. Kneser, Klassenzählen definiter quadratischer Formen, Arch. Math. vol. 8 (1957) pp. 76-80.

3. M. Marcus, Basic Theorems in Matrix Theory, National Bureau of Standards, Applied Mathematics Series 57. (1960) p. 3.

4. M. Newman and O. Taussky, On a generalization of the normal basis in abelian algebraic number fields, Comm. Pure Appl. Math. vol. 9 (1956) pp. 85-91.

5. H. Pollard, The Theory of Algebraic Numbers, Carus Monograph No. 9. Math. Assoc. of America, 1950. p. 31.

6. O. Taussky, Matrices of rational integers, Bul. Amer. Math. Soc. vol. 66 (1960) pp. 327-345.

7. R. C. Thompson, Normal matrices and the normal basis in abelian number fields, Pacific Journal of Math. vol. 12, No. 3 (1962) pp. 1115-1124.