A NOTE ON THE UNIT GROUP OF ZS_3

P. J. ALLEN AND C. HOBBY

ABSTRACT. The group $V(ZS_3)$ of units of augmentation 1 in ZS_3 is characterized as the group of all doubly stochastic matrices in $GL(3, Z)$. Two normal complements are presented, one of which is torsion free while the other contains elements of order 2.

Hughes and Pearson [3] characterized the group $V = V(ZS_3)$ of units of augmentation 1 in ZS_3 by showing that V is isomorphic to the subgroup of $GL(2, Z)$ consisting of matrices whose column sums are 1 modulo 3. Their approach was to construct a 6×6 matrix from a full set of irreducible representations of S_3 , invert the matrix, then solve a system of six linear congruences modulo 6. The same approach, with slight modifications, was used subsequently by Polcino Milies [4] to describe units in ZD_4 and by the authors [1] to describe units in ZA_4 .

In this paper we use a different method to obtain a new description of $V(ZS_3)$ as the group of all doubly stochastic matrices in $GL(3, Z)$. Working in $GL(3, Z)$ instead of $GL(2, Z)$ permits us to exploit the fact that a convex combination of permutation matrices is always doubly stochastic; it is not necessary to invert a 6×6 matrix or to solve a system of linear congruences.

It is well known that S_3 has a torsion free normal complement in $V(ZS_3)$. (This is a special case of a theorem of Passman and Smith [6] and of a more general theorem of Cliff, Sehgal, and Weiss [2].) On the other hand, it is easy to see that the doubly stochastic matrices which are the identity modulo 2 are a normal complement to S_3 in our presentation, and that this complement contains elements of order 2.

We represent $S_3 = \langle a, b \mid a^2 = b^3 = 1 \text{ and } a^{-1}ba = b^2 \rangle$ by

$$\rho(a) = A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \rho(b) = B = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

and extend ρ linearly to ZS_3 . Whenever $\alpha = \sum c_{ij}a^ib^j \in ZS_3$, it is clear that

$$(1) \quad \rho(\alpha) = \begin{bmatrix} c_{00} + c_{12}, & c_{01} + c_{10}, & c_{02} + c_{11} \\ c_{02} + c_{10}, & c_{00} + c_{11}, & c_{01} + c_{12} \\ c_{01} + c_{11}, & c_{02} + c_{12}, & c_{00} + c_{10} \end{bmatrix}.$$

In addition, if α is a unit of augmentation 1, then $\rho(\alpha)$ is clearly a doubly stochastic matrix in $GL(3, Z)$.

Received by the editors December 9, 1985.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20C05; Secondary 20C10.

©1987 American Mathematical Society
0002-9939/87 \$1.00 + \$.25 per page

Whenever $M \in \text{GL}(3, \mathbb{Z})$, we agree that $t_{ij} = t_{ij}(M)$ will denote the sum of the entries in M which occur in the locations where the permutation matrix $A^i B^j$ has 1's. Moreover, we let

$$\delta_M = \begin{cases} 1 & \text{if } t_{00}(M) \equiv 1 \pmod{3}, \\ 0 & \text{otherwise,} \end{cases}$$

and use the equations

$$(2) \quad c_{0j} = (t_{0j} - \delta_M)/3 \quad \text{and} \quad c_{1j} = (t_{1j} + \delta_M - 1)/3$$

to obtain coefficients c_{ij} from M and then associate with M the group ring element

$$(3) \quad \alpha_M = \sum c_{ij} a^i b^j.$$

It is clear that an arbitrary $M \in \text{GL}(3, \mathbb{Z})$ may produce coefficients c_{ij} that are not integers. The next two lemmas show that the c_{ij} will be integers if M is in $\rho(V)$ or if M is merely doubly stochastic.

LEMMA 1. *If $\alpha = \sum c_{ij} a^i b^j \in V(ZS_3)$ and $M = \rho(\alpha)$, then the group ring element α_M determined from equations (2) has integer coefficients and $\alpha_M = \alpha$.*

PROOF. In view of (1), we have

$$t_{0j} = 3c_{0j} + \sum_k c_{1k} \quad \text{and} \quad t_{1j} = 3c_{1j} + \sum_k c_{0k}.$$

The homomorphism $\sigma: ZS_3 \rightarrow Z\langle a \rangle$ defined by

$$(4) \quad \sigma\left(\sum c_{ij} a^i b^j\right) = \sum c_{ij} a^i = \left(\sum c_{0j}\right) + \left(\sum c_{1j}\right)a$$

must map units in ZS_3 to units in $Z\langle a \rangle$. Since $Z\langle a \rangle$ has only trivial units, it is clear that one of $\sum c_{0j}, \sum c_{1j}$ is 0 and the other is 1. Consequently, if we solve the above equations for the coefficients c_{ij} we immediately obtain equations (2).

LEMMA 2. *Let M be a doubly stochastic matrix in $\text{GL}(3, \mathbb{Z})$ and let $\alpha_M = \sum c_{ij} a^i b^j$ be the group ring element defined from equations (2). Then*

- (i) α_M has integer coefficients,
- (ii) one of $\sum c_{0j}, \sum c_{1j}$ is 0 and the other is 1, and,
- (iii) $\rho(\alpha_M) = M$.

PROOF. We first write M in the form

$$M = \begin{bmatrix} s, & t, & 1-s-t \\ u, & v, & 1-u-v \\ 1-s-u, & 1-t-v, & -1+s+t+u+v \end{bmatrix},$$

where s, t, u , and v are integers. Use elementary row and column operations to evaluate the determinant of M modulo 3 as follows: add the first two rows to the third row, next add the first two columns to the third column, and finally subtract the second column from the first column obtaining

$$|M| \equiv \begin{vmatrix} s-t & t & 1 \\ u-v & v & 1 \\ 0 & 1 & 0 \end{vmatrix} \pmod{3}.$$

Since $M \in \text{GL}(3, Z)$, we can expand the above determinant along the third row to obtain

$$\pm 1 = |M| \equiv t - s + u - v \pmod{3}.$$

Consequently, if we let $n = t - s + u - v$ it is clear that $n \equiv \pm 1 \pmod{3}$. From the form of the matrix M it follows that $t_{0j} \equiv -1 + n \pmod{3}$ and $t_{1j} \equiv -1 - n \pmod{3}$. Therefore, regardless of whether $n \equiv 1 \pmod{3}$ or $n \equiv -1 \pmod{3}$, the definition of δ_M ensures that the numerators in equations (2) are multiples of 3 and part (i) follows.

We next write $M = [m_{ij}]$ and calculate the coefficients c_{1j} according to equation (2). Observe that

$$\sum c_{0j} = (\sum m_{ij} - 3\delta_M)/3 = 1 - \delta_M$$

and

$$\sum c_{1j} = (\sum m_{ij} + 3\delta_M - 3)/3 = \delta_M.$$

Since δ_M is either 0 or 1, part (ii) follows.

We see from equation (1) that the i, j entry of $\rho(\alpha_M)$ is of the form

$$\rho(\alpha_M)_{ij} = (t_{0u} + t_{1v} - 1)/3,$$

where t_{0u} and t_{1v} each include m_{ij} while the remaining summands in t_{0u} and t_{1v} are the entries of M which lie outside the i th row and j th column of M . Since the column sums of M are 1,

$$t_{0u} + t_{1v} = 2m_{ij} + (1 - m_{ij_1}) + (1 - m_{ij_2}),$$

where j_1 and j_2 are the indices of the columns other than the j th. Consequently,

$$t_{0u} + t_{1v} = 3m_{ij} + 2 - \sum m_{ik} = 3m_{ij} + 1$$

and it follows that $\rho(\alpha_M)_{ij} = m_{ij}$.

We can now easily obtain the following characterization.

THEOREM 1. *The group $V(ZS_3)$ of units of augmentation 1 in ZS_3 is isomorphic to the group of doubly stochastic matrices in $\text{GL}(3, Z)$.*

PROOF. Let S denote the set of all $\alpha = \sum c_{ij}a^ib^j$ in ZS_3 such that the map σ of equation (4) sends α to a unit of augmentation 1. It is clear that S is closed under multiplication and that $V(ZS_3) \subseteq S$. As noted after equation (4), if $\alpha \in S$ then one of $\sum c_{0j}$, $\sum c_{1j}$ is 0 and the other is 1. Thus it follows from (1) that if $\alpha \in S$, then $\rho(\alpha) = I$ if and only if $\alpha = 1$. Therefore the restriction of ρ to $V(ZS_3)$ is an isomorphism into the group of doubly stochastic matrices. On the other hand, if M is doubly stochastic, then it follows from (i) and (ii) of Lemma 2 that α_M and $\alpha_{M^{-1}}$ are in S , so $\alpha_M\alpha_{M^{-1}} \in S$. Since (iii) of Lemma 2 implies that $\rho(\alpha_M\alpha_{M^{-1}}) = I$, and since $\alpha_M\alpha_{M^{-1}} \in S$, we see that $\alpha_M \in V(ZS_3)$. Therefore ρ is onto.

In view of Theorem 1, we may think of $V = V(ZS_3)$ as the set of all doubly stochastic matrices in $\text{GL}(3, Z)$ and identify S_3 with its image $\rho(S_3)$. We let

$$\mathcal{J}_k = \{X \in \text{GL}(3, Z) \mid X \equiv I \pmod{k}\}.$$

It is well known (see Newman [5, p. 176]) that $\mathcal{J}_k$ is a torsion free group when $k > 2$.

THEOREM 2. *If $N = V \cap \mathcal{J}_2$, then*

- (i) *N is a complement of S_3 in V , and*
- (ii) *N contains elements of order 2.*

PROOF. It is clear that N is a subgroup of V and that $S_3 \cap N = \{I\}$. Let $X \in V$. Since $|X| = \pm 1$, at least one of the “diagonals” followed in computing $|X|$ must consist only of odd integers. If these are not the only odd entries in X , then it follows from the fact that X is doubly stochastic that every entry in X must be odd; one argues that a row or column with two odds must contain three odds, and so on. But then X is congruent to the matrix of all ones modulo 2 and thus $|X| \equiv 0 \pmod{2}$, a contradiction. Therefore, X contains just one “diagonal” of odd entries and consequently multiplying by one of the permutation matrices in S_3 produces I modulo 2. Therefore $V = S_3 N$. It is now clear that N is normal in V and part (i) follows. Moreover,

$$X = \begin{bmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 2 & -2 & 1 \end{bmatrix}$$

is in N and $X^2 = I$.

Theorem 1 also permits us to give an explicit description of a torsion free normal complement. Let $\mathcal{M}_3(\mathbb{Z})$ denote the set of all 3×3 matrices with integer entries and agree to denote the trace of the matrix X by $\text{tr}(X)$. We let

$$\mathcal{D} = \{D \in \mathcal{M}_3(\mathbb{Z}) \mid D \text{ is diagonal and } \text{tr}(D) = 0\}.$$

Moreover, we let J denote the 3×3 matrix with all entries 1.

THEOREM 3. *Let N denote the set of all $X \in V$ such that $X \equiv (I + DJ) \pmod{3}$ for some $D \in \mathcal{D}$. Then N is a torsion free normal complement to S_3 in V .*

PROOF. If three integers have sum 1, then two of them must be equal modulo 3. Thus, if $X \in V$ then the set of entries in the i th row of X modulo 3 must consist of $\{n_i, n_i, n_i + 1\}$. No two of the $n_i + 1$ can occur in the same column of X modulo 3 since, if that happens, the other two columns of X would be identical modulo 3 and we would have the immediate contradiction $|X| \equiv 0 \pmod{3}$. Therefore some permutation of the rows of X must produce a matrix PX of the form

$$PX = I + D_1 J + 3M_1,$$

where D_1 is diagonal. The column sums of $D_1 J$ are $\text{tr}(D_1)$, thus $\text{tr}(D_1)$ is a multiple of 3. Consequently, we can subtract $\text{tr}(D_1)$ from each entry of the third row of $D_1 J$ and add $\text{tr}(D_1)$ to each entry of the third row of $3M_1$ to obtain

$$PX = I + DJ + 3M,$$

where $D \in \mathcal{D}$. The matrices in S_3 provide a full set of permutations of the rows of X , thus P can be chosen to be an element of S_3 . Consequently, $V = S_3 N$. It is clear that $S_3 \cap N = \{I\}$. Also, N is normalized by S_3 since conjugating the diagonal matrix D by an element of S_3 merely rearranges the entries on the diagonal.

We still must show that N is a group and that it is torsion free. If X_1 and X_2 are elements of N with $X_i \equiv (I + D_i J) \pmod{3}$, then

$$X_1 X_2 \equiv I + (D_1 + D_2)J \pmod{3}$$

since $\text{tr}(D_2) = 0$ implies that $JD_2J = 0$. Thus, N is closed under multiplication. Multiplying both sides of $X \equiv (I + DJ) \pmod{3}$ on the right by X^{-1} gives $I \equiv (X^{-1} + DJ) \pmod{3}$ since $JY = J$ for any doubly stochastic matrix Y . Consequently, $X^{-1} \in N$ whenever $X \in N$ and we have shown that N is a group.

Finally, suppose that X is a nontrivial element of prime order in N . Since X is a 3×3 integer matrix it must have order 2 or 3. As noted above, if $X \equiv (I + DJ) \pmod{3}$, then

$$X^2 \equiv (I + 2DJ) \pmod{3}.$$

If $X^2 = I$, then $2DJ \equiv 0 \pmod{3}$ and it follows that $DJ \equiv 0 \pmod{3}$ which forces $X \in \mathcal{J}_3$, a contradiction since $\mathcal{J}_3$ is torsion free. Suppose that $X^3 = I$. We see from the above expressions for X and X^2 that $I + X + X^2 \equiv 0 \pmod{3}$. Multiplying $X = I + DJ + 3M$ by $I + X + X^2$ gives

$$I + X + X^2 = I + X + X^2 + 3DJ + 3M(I + X + X^2).$$

The last term on the right is 0 modulo 9, so $DJ \equiv 0 \pmod{3}$ and we reach the same contradiction as before.

REMARKS. We expected the N of Theorem 2 to be torsion free and tried to construct a proof by showing that $X^2 = I$ implies that $X \equiv I \pmod{4}$. The only difficult case arose when

$$X \equiv \begin{bmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix} \pmod{4}$$

and we then found the X given in Theorem 2. That X corresponds to $b - b^2 + a + ab - ab^2$ in ZS_3 , thus it is one of the elements of order 2 described by Olga Taussky in [7]. It is remarkable that the elements she discovered play an important role both in our work and in the quite different approach followed by Hughes and Pearson.

Our permutation representation of degree 3 is necessarily reducible. In fact, if

$$S = \frac{1}{3} \begin{bmatrix} 1 & -2 & 1 \\ -2 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$

then

$$S^{-1} \rho(g) S = \left[\begin{array}{c|c} T(g) & \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \\ \hline 0 & 1 \end{array} \right],$$

where T is the representation of degree 2 used by Hughes and Pearson. Moreover, X is a doubly stochastic matrix in $\text{GL}(3, Z)$ if and only if

$$S^{-1} X S = \left[\begin{array}{c|c} Y & \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \\ \hline 0 & 1 \end{array} \right],$$

where $Y \in \text{GL}(2, \mathbb{Z})$ and the column sums of Y are 1 modulo 3. If $Y \in \text{GL}(2, \mathbb{Z})$, then

$$X = S \left[\begin{array}{cc|c} & & 0 \\ & Y & \\ \hline & & 0 \\ 0 & 0 & 1 \end{array} \right] S^{-1}$$

is always doubly stochastic; the column sum condition is exactly what is needed to ensure that X has integer entries.

REFERENCES

1. P. J. Allen and C. Hobby, *A characterization of units in $\mathbb{Z}[A_4]$* , J. Algebra **66** (1980), 534–543.
2. G. H. Cliff, S. K. Sehgal, and A. R. Weiss, *Units of integral group rings of metabelian groups*, J. Algebra **73** (1981), 167–185.
3. I. Hughes and K. R. Pearson, *The group of units of the integral group ring $\mathbb{Z}S_3$* , Canad. Math. Bull. **15** (1972), 529–534.
4. C. Milies, *The units of the integral group ring $\mathbb{Z}D_4$* , Bol. Soc. Brasil. Mat. **4** (1972), 85–92.
5. M. Newman, *Integral matrices*, Academic Press, New York, 1972.
6. D. S. Passman and P. F. Smith, *Units in integral group rings*, J. Algebra **69** (1981), 213–239.
7. O. Taussky, *Matrices of rational integers*, Bull. Amer. Math. Soc. **66** (1960), 327–345.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ALABAMA, UNIVERSITY, ALABAMA 35486