PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 6, Pages 1649–1653
S 0002-9939(03)06839-4
Article electronically published on January 15, 2003

BICYCLIC UNITS OF $\mathbb{Z}S_n$

AURORA OLIVIERI AND ÁNGEL DEL RÍO

(Communicated by Stephen D. Smith)

ABSTRACT. We prove that the group generated by the bicyclic units of $\mathbb{Z}S_n$ has torsion for $n \geq 4$. This answers a question of Sehgal (1993).

Let G be a finite group. For every $x \in G$ of order k let $\hat{x} = \sum_{i=0}^{k-1} x^i \in \mathbb{Z}G$. The bicyclic units of $\mathbb{Z}G$ are the units of the form

$$b(x, y) = 1 + \hat{x}y(1 - x)$$

for $x, y \in G$. The following appears in [5] as Problem 19:

> **Problem**: Is the group $\langle b(x, y) : x, y \in G\rangle$, generated by the bicyclic units of $\mathbb{Z}G$, torsionfree?

As a consequence of [5, Theorem 31.3] it is easy to prove that the problem has a positive answer for several groups, including dihedral groups.

The units of the form $b'(x, y) = 1 + (1 - x)y\hat{x}$ are also called bicyclic units and in fact the problem was stated in [5] for the group generated by the $b'(x, y)$'s. It is obvious that both versions are equivalent. We have chosen the $b(x, y)$'s for computational reasons.

In this paper we show that the problem has a negative answer proving the following theorem.

Theorem 1. *For every positive integer n let S_n be the symmetric group on n letters and $\mathcal{B}_n$ the group generated by the bicyclic units of the symmetric group ring $\mathbb{Z}S_n$. Then*

$$\mathcal{B}_n \cap S_n = \begin{cases} 1 & \text{if } n \leq 3, \\ \langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle & \text{if } n = 4, \\ A_n \text{ or } S_n & \text{if } n \geq 5. \end{cases}$$

Since S_2 is abelian and $\mathcal{B}_3$ is free [3] Theorem 1 is clear of $n \leq 3$. We consider S_n embedded in S_{n+1} in the obvious way so that $\mathcal{B}_n \subseteq \mathcal{B}_{n+1}$. If $g, x, y \in G$, then $g^{-1}b(x, y)g = b(g^{-1}xg, g^{-1}yg)$. Therefore $\mathcal{B}_n$ is normalized by S_n and hence $\mathcal{B}_n \cap S_n$ is a normal subgroup of S_n. Thus to prove Theorem 1 it is enough to prove

$$\langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle = \mathcal{B}_4 \cap S_4. \tag{1}$$

In the remainder of the paper we prove this equality and in the way we obtain a full description of $\mathcal{B}_4$ in terms of some groups of integral matrices.

Received by the editors May 16, 2001 and, in revised form, July 17, 2001.
2000 *Mathematics Subject Classification.* Primary 20C05; Secondary 16U60.
The second author was partially supported by the D.G.I. of Spain and Fundación Séneca of Murcia.

Consider the following four elements of S_4:

$$a = (1\,2)(3\,4), \quad b = (1\,3)(2\,4), \quad c = (1\,2\,3), \quad d = (1\,2).$$

Recall that $S_4 = \langle a, b \rangle \rtimes \langle c, d \rangle$ and $\langle c, d \rangle = S_3$. Let $\tau : S_4 \to S_3$ be the projection given by the previous decomposition, that is, τ is the identity in $\langle c, d \rangle$ and Ker $\tau = \langle a, b \rangle$. Extend τ by linearity to a homomorphism of rational algebras $\mathbb{Q}S_4 \to \mathbb{Q}S_3$, also denoted by τ. S_4 has two inequivalent representations of degree 3. We take from [1] ρ_1 and ρ_2 given by

$$\rho_1(a) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \rho_1(b) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

$$\rho_1(c) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \qquad \rho_1(d) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

and

$$\rho_2(g) = \begin{cases} \rho_1(g), & \text{if } g \in A_4, \\ -\rho_1(g), & \text{if } g \notin A_4. \end{cases}$$

(The representation ρ_1 and ρ_2 are denoted ρ and ρ' in [1]. Note that there is an error in the definition of ρ in [1] where $\rho(a)$ and $\rho(b)$ should be interchanged.)

Extend ρ_1 and ρ_2 to homomorphisms of rational algebras $\mathbb{Q}S_4 \to M_3(\mathbb{Q})$ and let $\rho : \mathbb{Q}S_4 \to M_3(\mathbb{Q})^2$ be the direct sum of ρ_1 and ρ_2. It is well known that $\tau \oplus \rho : \mathbb{Q}S_4 \to \mathbb{Q}S_3 \oplus M_3(\mathbb{Q})^2$ is an isomorphism.

For an arbitrary finite group G, $V(\mathbb{Z}G)$ denotes the group of units of $\mathbb{Z}G$ of augmentation 1. The homomorphisms τ and ρ induce group homomorphisms $\tau : V(\mathbb{Z}S_4) \to V(\mathbb{Z}S_3)$ and $\rho : V(\mathbb{Z}S_4) \to \mathrm{GL}_3(\mathbb{Z})^2$. Clearly $\tau(\mathcal{B}_4) = \mathcal{B}_3$. Since $\mathcal{B}_3$ is free [3], one has that

$$\mathcal{B}_4 = (\mathcal{B}_4 \cap K) \rtimes \mathcal{B}_3, \tag{2}$$

where $K = \{\alpha \in V(\mathbb{Z}S_4) : \tau(\alpha) = 1\}$. Moreover, ρ is an isomorphism between K and $\rho(K)$ (because $\tau \oplus \rho$ is an isomorphism) and the last has been described in [1]. Since we need this description we are going to recall it.

Let $\hat{E}(n)$ denote the principal congruence group of level n, of $\mathrm{SL}_3(\mathbb{Z})$ $(n \in \mathbb{Z})$; that is,

$$\hat{E}(n) = \{A \in \mathrm{SL}_3(\mathbb{Z}) : A \equiv 1 \mod n\}.$$

Let

$$X = \{(x_{ij}) \in \hat{E}(2) : x_{12} + x_{23} + x_{31} \equiv x_{13} + x_{21} + x_{32} \mod 4\}$$

and

$$X_1 = \{(x_{ij}) \in \hat{E}(2) : x_{12} + x_{23} + x_{31} \equiv x_{13} + x_{21} + x_{32} \equiv 0 \mod 4\}.$$

Let $\mathbb{G} = \langle Q, R, Q^t, R^t, \hat{E}(8) \rangle$ where

$$Q = \begin{pmatrix} 1 & 0 & 4 \\ 4 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}, \quad R = \begin{pmatrix} 5 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 4 & 5 \end{pmatrix},$$

and A^t denotes the transpose of a matrix A. Finally let

$$T = \begin{pmatrix} 17 & 0 & -4 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix}.$$

(Note that the matrices Q and R are different from the corresponding matrices in [1]. This does not affect the definition of $\mathbb{G}$ because our Q and R are congruent to the Q and R in [1] modulo 8.)

Now we are ready to give the description of $\rho(K)$ in terms of integral matrices.

Theorem 2 ([1])**.**

$$\rho(K) = \{(A, T^s AG) : A \in X, G \in \mathbb{G}, s = 0, \textit{if } A \in X_1 \textit{ and } s = 1, \textit{otherwise}\}.$$

For a permutation $\sigma \in S_n$ and a matrix $A \in M_n(R)$ let A^σ denote the matrix obtained by permuting the rows and columns of A by σ, that is, $A^\sigma = P_\sigma^{-1} A P_\sigma$ where P_σ is the permutation matrix defined by

$$P_\sigma(i,j) = \begin{cases} 1, & \text{if } j = \sigma(i), \\ 0, & \text{otherwise.} \end{cases}$$

For every $x, y \in S_4$ let

$$\kappa_{x,y} = b(x,y) \cdot \tau(b(x,y))^{-1} \in \mathcal{B}_4 \cap K$$

and let K_0 be the group generated by all the $\kappa_{x,y}$'s.

Remark 3. Let H be a group of units of $\mathbb{Z}S_4$ normalized by $S_3 = \langle c, d \rangle$. Then $\rho_i(H)$ is normalized by $\rho_i(S_3)$ $(i = 1, 2)$. This implies that $A^\sigma \in \rho_i(H)$ for every $A \in \rho_i(H)$ and $\sigma \in S_3$.

Some groups normalized by S_3 are $\mathcal{B}_4$, K and Ker ρ_i $(i = 1, 2)$. Another example is K_0 because τ acts as the identity in S_3. □

For every $1 \leq i \neq j \leq 3$ and n an integer let $e_{ij}(n)$ be the 3×3 matrix having n in the (i,j) entry and zeroes elsewhere. Set $E_{ij}(n) = I + e_{ij}(n)$. Let $E(n) = \langle E_{ij}(n) : 1 \leq i \neq j \leq 3 \rangle$.

Lemma 4. (1) *$SL_3(\mathbb{Z}) = E(1)$.*

(2) *$\hat{E}(n)$ is the normal subgroup of $SL_3(\mathbb{Z})$ generated by $E_{12}(n)$.*

(3) *$E(n) = \{(a_{ij}) \in \mathrm{SL}_3(\mathbb{Z}) : n | a_{ij}$ if $i \neq j$ and $a_{ii} \equiv 1 \mod n^2\}$, in particular $\hat{E}(n^2) \subseteq E(n)$.*

(4) *$\hat{E}(n) = \langle A_n, A_n^c, E(n) \rangle$ (recall that $c = (1\,2\,3)$), where*

$$A_n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+n & n \\ 0 & -n & 1-n \end{pmatrix}.$$

(5) *$X = \langle {A_2}^\sigma, B^\sigma, \hat{E}(4) : \sigma \in S_3 \rangle$ where $B = E_{23}(2) \cdot E_{12}(2)$.*

Proof. (1) See [4, 1.2.11].

(2) See [4, 1.2.26] and [2, Corollary 4.3] or the proof of [4, 4.3.1].

(3) We first prove $\hat{E}(n^2) \subseteq E(n)$. By 1 and 2 it is enough to show that $E_{ij}(1)E_{12}(n^2)E_{ij}(1)^{-1}$ belongs to $E(n)$ for every $i \neq j$. This is obvious if $(i,j) \neq (2,1)$. Finally

$$\begin{aligned} E_{21}(1)E_{12}(n^2)E_{21}(1)^{-1} &= E_{21}(1)[E_{13}(n), E_{32}(n)]E_{21}(1)^{-1} \\ &= [E_{21}(1)E_{13}(n)E_{21}(1)^{-1}, E_{21}(1)E_{32}(n)E_{21}(1)^{-1}] \\ &= [E_{23}(n)E_{13}(n), E_{31}(-n)E_{32}(n)]. \end{aligned}$$

Let $E = \{(a_{ij}) \in \mathrm{SL}_3(\mathbb{Z}) : n|a_{ij} \text{ if } i \neq j \text{ and } a_{ii} \equiv 1 \mod n^2\}$. Plainly $\hat{E}(n^2) \subseteq E(n) \subseteq E$. Now notice that if $A = I + n(a_{ij})$ and $B = I + n(b_{ij})$, then $AB \equiv I + n(a_{ij}+b_{ij}) \mod n^2$. Using this it is easy to see that $E(n)/\hat{E}(n^2) \simeq \mathbb{Z}_n^6 \simeq E/\hat{E}(n^2)$, so that $E(n)/\hat{E}(n^2) = E/\hat{E}(n^2)$ and hence $E(n) = E$.

(4) and (5). A trivial verification shows that $\hat{E}(n)/\hat{E}(n^2) = \langle A_n, A_n^c, E(n)\rangle/\hat{E}(n^2)$ and $X/\hat{E}(4) = \langle {A_2}^\sigma, B^\sigma, \hat{E}(4) : \sigma \in S_3\rangle/\hat{E}(4)$. □

Remark 5. Let H be as in Remark 3. By Lemma 4 to prove that $E(n) \subseteq \rho_i(H)$ it is enough to show that $E_{ij}(n) \in \rho_i(H)$ for some $i \neq j$, and to prove that $\hat{E}(n) \subseteq \rho_i(H)$ it is enough to additionally prove that $A_n \in \rho_i(H)$. □

Lemma 6. *$\rho_1(K_0) = X$.*

Proof. By Theorem 2, $\rho_1(K_0) \subseteq X$. To prove the other inclusion we are going to use Lemma 4 and Remarks 3 and 5 several times without specific mention.

Note that $\rho_1(\kappa_{a,cd}) = E_{21}(4)$ and $A_2 = \rho_1(\kappa_{bc^2d,a})$. Since $A_4 = A_2^2$, $\hat{E}(4) \subseteq \rho_1(K_0)$.

The proof is completed by showing that $B \in \rho_1(K_0)$. Let $C = \rho_1(\kappa_{abcd,ac^2})$ and $D = \rho_1(\kappa_{ac^2,abc^2d})$. Consider $B_1 = C \cdot (D \cdot A_2)^c$. Then $B \in B_1\hat{E}(4)$ and therefore $B \in \rho_1(K_0)$. This completes the proof. □

Lemma 7. *$\mathbb{G} = \rho_2(K_0 \cap \mathrm{Ker}\ \rho_1)$.*

Proof. Let $N = K_0 \cap \mathrm{Ker}\ \rho_1$. By Theorem 2, $\rho_2(N) \subseteq \rho_2(K \cap \ker \rho_1) \subseteq \mathbb{G}$. We obtain the other embedding by proving $\hat{E}(8) \subseteq \rho_2(N)$ and $Q, Q^t, R, R^t \in \rho_2(N)$. Again we are going to use Lemma 4 and Remarks 3 and 5 without specific mention.

Note that N is normalized by S_3 and $\rho(\kappa_{b,bc} \cdot \kappa_{b,cd}^{-1}) = (1, E_{12}(8))$, so that $E(8) \subseteq \rho_2(N)$. Let $b = (\kappa_{bc^2,ad} \cdot \kappa_{abcd,a}^{-1})^2 \cdot (\kappa_{ab,ad} \cdot \kappa_{ab,ac^2})^{-1} \in N$ and $B = \rho_2(b)$. Then

$$B \equiv \begin{pmatrix} 41 & 48 & 0 \\ 48 & 25 & 0 \\ 56 & 16 & 1 \end{pmatrix} \mod 64$$

and hence $A_8 \in (B^3)^{c^2d}E(8)$. Thus $A_8 \in \rho_2(N)$ and we conclude $\hat{E}(8) \subseteq \rho_2(N)$.

Consider the following elements of $\rho_2(N)$:

$$\begin{aligned} Q_1 &= \rho_2(\kappa_{c^2d,ac^2} \cdot \kappa_{ac^2d,ad}^{-1}), \\ Q_2 &= \rho_2(\kappa_{d,ac^2}.\kappa_{d,b}^{-1}), \\ Q_3 &= \rho_2(\kappa_{cd,ac^2d}.\kappa_{bcd,ac^2}^{-1}). \end{aligned}$$

Then

$$R \equiv Q_1 \cdot Q_2 \mod 8 \quad \text{and} \quad R^t \equiv Q_2 \cdot Q_3 \mod 8$$

and hence $R, R^t \in \rho_2(N)$. Since $Q = R^{c^{-1}}$, we have that $Q, Q^t \in \rho_2(N)$. □

Proposition 8. *$\mathcal{B}_4 = K \rtimes \mathcal{B}_3$.*

Proof. By (2), it is enough to show that $K \subseteq \mathcal{B}_4$. Since $K_0 \subseteq \mathcal{B}_4 \cap K \subseteq K$ and the restriction of ρ to K is injective, it is enough to prove that $\rho(K) \subseteq \rho(K_0)$. By Theorem 2, any element of $\rho(K)$ is of the form (A, T^sAG) with $A \in X$, $G \in \mathbb{G}$ and $s = 0$ if $A \in X_1$ and $s = 1$ otherwise. By Lemma 6, $A \in \rho_1(K_0)$. Thus, by Theorem 2, we have that $(A, T^sAG_1) \in \rho(K_0)$ for some $G_1 \in \mathbb{G}$. By Lemma 7, $(1, G)$ and $(1, G_1)$ belong to $\rho(K_0)$. Then

$$(A, T^sAG) = (A, T^sAG_1) \cdot (1, G_1)^{-1} \cdot (1, G) \in \rho(K_0). \qquad \square$$

Proposition 8 contains the announced description of $\mathcal{B}_4$. Indeed, $\mathcal{B}_3$ is isomorphic to the congruence subgroup of level 3 of $\mathrm{SL}_2(\mathbb{Z})$, which is free of rank 3 [3]. Moreover we have already mentioned that ρ is an isomorphism between K and $\rho(K)$ and the last has been described in Theorem 2.

Proof of (1). By Proposition 8, $\langle a, b\rangle \subseteq K \cap S_4 \subseteq \mathcal{B}_4 \cap S_4$. Since the last is a normal subgroup of S_4, then $\mathcal{B}_4 \cap S_4$ is either $\langle a, b\rangle$, A_4 or S_4. We prove $\mathcal{B}_4 \cap S_4 = \langle a, b\rangle$ by proving that $\mathcal{B}_4$ has only 2-torsion (that is, every torsion element of $\mathcal{B}_4$ has order ≤ 2).

By Proposition 8, $\mathcal{B}_4 = (K \cap \mathcal{B}_4) \rtimes \mathcal{B}_3$. Let b be a torsion element of $\mathcal{B}_4$. Then $b = gh$ with $g \in K \cap \mathcal{B}_4$ and $h \in \mathcal{B}_3$. However, h is a torsion element of $\mathcal{B}_3$ and hence $h = 1$, because $\mathcal{B}_3$ is torsionfree. Therefore $b = g$ is a torsion element of K. Since $K \simeq \rho(K) \subseteq \hat{E}(2)^2$, the order of $b = g$ is ≤ 2. □

Final remark

After this paper was accepted, we received a note from Martin Hertweck with the following two remarks.

First $\mathcal{B}_n \cap S_n \subseteq A_n$ because $\mathcal{B}_n$ is embedded in the kernel of the sign representation of S_n. Therefore, by Theorem 1, $\mathcal{B}_n \cap S_n = A_n$ if $n \geq 5$. This improves Theorem 1.

Second he has expressed the group element $b \in S_4$ as a product of seven bicyclics:

$$b = b(b, c^2) \cdot b(ab, bc) \cdot b(d, abc^2) \cdot b(d, bc^2) \cdot b(abd, c) \cdot b(bc^2d, c^2) \cdot b(c^2d, abc).$$

Motivated by this we have performed an exhaustive search, using Mathematica, looking for a shorter product of bicyclic units of $\mathbb{Z}S_4$ of finite order and this search has produced the following expression of a as a product of four bicyclics:

$$a = b(cd, c) \cdot b(bc^2d, abc) \cdot b(c^2d, abc^2) \cdot b(cd, ac^2).$$

References

[1] P.J. Allen and C. Hobby, *A characterization of units of* $\mathbb{Z}S_4$, Comm. in Algebra 16 (1988), 1479-1505. MR **89g:**20005

[2] H. Bass, J. Milnor and J.P. Serre *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Publ. Math. IHES 33 (1967), 59-137. MR **39:**5574

[3] E. Jespers and M.M. Parmenter, *Bicyclic units in* $\mathbb{Z}S_3$, Bull. Belg. Math. Soc. 44 (1992), 141-146. MR **95j:**16035

[4] A.J. Hahn and O.T. O'Meara, *The classical groups and K-Theory*, Springer-Verlag, 1989. MR **90i:**20002

[5] S.K. Sehgal, *Units of integral group rings*, Longman Scientific and Technical Essex, 1993. MR **94m:**16039

Departamento de Matemáticas, Universidad Simón Bolívar, Apartado Postal 89000, Caracas 1080-A, Venezuela

E-mail address: `olivieri@usb.ve`

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain

E-mail address: `adelrio@um.es`