PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 59, Number 1, August 1976

AUTOMORPHISMS OF THE INTEGRAL GROUP RING OF S_n

GARY L. PETERSON

ABSTRACT. In this paper it is shown that every normalized automorphism of the integral group ring of S_n can be written as a group automorphism followed by conjugation by a unit in the group algebra of S_n over the rationals.

1. **Introduction.** Throughout we will use $Z(G)$ to denote the integral group ring of a group G and $\mathcal{N}\mathcal{A}(G)$ to denote the group of normalized automorphisms of $Z(G)$. That is, $\mathcal{N}\mathcal{A}(G)$ is the group of ring automorphisms of $Z(G)$ such that $f(g)$ has augmentation one for all g in G. It is well known (see [2] or [3]) that it suffices to study normalized automorphisms over arbitrary automorphisms of $Z(G)$.

The major purpose of this paper is to consider $\mathcal{N}\mathcal{A}(G)$ when $G = S_n$, the symmetric group on n letters. In [2], Brown showed that S_n is an $\mathcal{G}.\mathcal{R}.$ *group* for every $n = 1, 2, \ldots, 10$. That is, every normalized automorphism of $Z(G)$ can be written in the form $f = \tau_u\sigma$ where σ is a group automorphism, u is a unit in $Q(G)$ (the group algebra of G over the rationals), and τ_u denotes conjugation by u when $G = S_n$, $n = 1, \ldots, 10$. In this paper, it will be shown that S_n is an $\mathcal{G}.\mathcal{R}.$ group for any positive integer n.

It should be remarked that the study of $\mathcal{G}.\mathcal{R}.$ groups is not limited to S_n. The reader can find several types of metabelian $\mathcal{G}.\mathcal{R}.$ groups in [2], [4] and [6].

2. **Action on class sums**. Before looking at the case $G = S_n$, we will need some facts concerning the action of $\mathcal{N}\mathcal{A}(G)$ on the class sums of a finite group G.

If f is an element of $\mathcal{N}\mathcal{A}(G)$ and $\overline{C}_g$ denotes the class sum of an element g of G, then $f(\overline{C}_g) = \overline{C}_x$ for some x in G ([2], [3], [6]). Thus, $\mathcal{N}\mathcal{A}(G)$ acts as a permutation group on the class sums of G. Further, let $\mathcal{C}\mathcal{P}(G)$ denote the kernel of this permutation representation. It follows that

$$\mathcal{C}\mathcal{P}(G) = \{\tau_u | u \text{ is a unit in } Q(G) \text{ normalizing } Z(G)\}$$

by first extending every element of $\mathcal{C}\mathcal{P}(G)$ to $Q(G)$, and then, since every element of $\mathcal{C}\mathcal{P}(G)$ will fix the simple components of $Q(G)$, by applying the Noether-Skolem Theorem.

We will make use of the following two additional results.

LEMMA 2.1. *Let $f \in \mathcal{N}\mathcal{A}(G)$ and x, y, u, v be elements of G such that*

Received by the editors August 8, 1975.

AMS (MOS) subject classifications (1970). Primary 20C05, 16A26; Secondary 20B05, 20D45.

Key words and phrases. Integral group ring, symmetric group, normalized automorphism, group automorphism, augmentation, class sum.

© American Mathematical Society 1976

$f(\overline{C}_x) = \overline{C}_u$ and $f(\overline{C}_y) = \overline{C}_v$. Then, for some $g \in G$,

$$f\left(\overline{C}_{xy}\right) = \overline{C}_{uv^g}.$$

PROOF. Note that $f(\overline{C}_{xy})$ appears as a summand when $f(\overline{C}_x\overline{C}_y)$ is written as a linear combination of class sums. Also, $f(\overline{C}_x\overline{C}_y)$ is a linear combination of class sums comprised of elements of the form $u^w v^z$ where $w, z \in G$. Therefore, for some w and z in G, $f(\overline{C}_{xy}) = \overline{C}_{u^w v^z}$ and we are done with $g = zw^{-1}$.

The second lemma is due to Brown [2].

LEMMA 2.2. *Let $f \in \mathfrak{N}\mathfrak{A}(G)$ and suppose that $f(\overline{C}_g) = \overline{C}_x$ where g and x are elements of G. Then for every integer n, $f(\overline{C}_{g^n}) = \overline{C}_{x^n}$. Also, it follows that $|g| = |x|$.*

3. **Symmetric groups.** We will now show that S_n is an $\mathfrak{S}.\mathfrak{R}$. group. In fact, we will actually see that $\mathfrak{N}\mathfrak{A}(S_n) = \mathcal{C}\mathcal{P}(S_n)$ for $n \neq 6$ which would have to hold since every group automorphism of S_n is inner when $n \neq 6$ ([5], Theorem 11.4.8).

We first record two results about S_n. The first result is Exercise 11.4.11(a) of [5]. The second is a well-known result about the order of conjugacy classes of S_n and can be found, for instance, in [1].

LEMMA 3.1. *Let $n > 2$, $n \neq 6$. Then an element x of S_n is a 2-cycle if and only if $|x| = 2$ and $\max|xx^y| = 3$ where y ranges over the elements of S_n.*

LEMMA 3.2. *Let $g \in S_n$ and suppose that g is a product of disjoint k_1 1-cycles, k_2 2-cycles, $\ldots$, k_n n-cycles. Then the order of C_g, C_g the conjugacy class of g, is given by*

$$|C_g| = n!/\left(k_1!1^{k_1}k_2!2^{k_2}\ldots k_n!n^{k_n}\right).$$

We next show

LEMMA 3.3. *Let f be a normalized automorphism of $Z(S_n)$ and suppose that $n > 2$, $n \neq 6$. Let g in S_n be a product of disjoint transpositions. Then $f(\overline{C}_g) = \overline{C}_g$.*

PROOF. Let t denote the number of transpositions appearing in G. We may assume that g has the form $g = (1, 2)(3, 4)\ldots(2t-1, 2t)$. Let $f(\overline{C}_g) = \overline{C}_x$, $x \in G$. To show $\overline{C}_x = \overline{C}_g$ we proceed by induction on t.

If $t = 1$, let $u \in S_n$. By Lemma 2.1, we can find v in S_n such that $f(\overline{C}_{gg^u}) = \overline{C}_{xx^v}$. Conversely, given v in S_n we can also find u in S_n satisfying the above equation. Thus by Lemma 2.2, $\max|xx^v| = 3$ as v runs over S_n. Thus x is a transposition by Lemma 3.1 since $|x| = 2$ by Lemma 2.2.

In the general case we have

$$f\left(\overline{C}_{(1,2)(3,4)\ldots(2t-3,2t-2)}\right) = \overline{C}_{(1,2)(3,4)\ldots(2t-3,2t-2)}$$

and $f(\overline{C}_{(2t-1,2t)}) = \overline{C}_{(2t-1,2t)}$. Hence by Lemma 2.1,

$$f\left(\overline{C}_g\right) = \overline{C}_{(1,2)(3,4)\ldots(2t-3,2t-2)(2t-1,2t)^y}$$

for some $y \in S_n$.

If we can show that $(2t-1, 2t)^y$ is disjoint from $(1, 2)(3, 4)\ldots(2t-3, 2t-2)$, we will be done, so suppose this is not the case. If $(2t-1, 2t)^y$ has one letter in common with $(1, 2) \ldots (2t-3, 2t-2)$, it follows that $(1, 2) \ldots (2t-3, 2t-2)(2t-1, 2t)^y$ is a product of disjoint cycles which are transpositions and a 3-cycle. But then 3 divides $|x|$ which is impossible.

Next, suppose $(2t-1, 2t)^y$ has two letters in common with one transposition of $(1, 2) \ldots (2t-3, 2t-2)$. Then x is a product of disjoint transpositions and has fewer transpositions than g does. Thus f fixes $\overline{C}_x$ and so $f(\overline{C}_g) \neq \overline{C}_x$.

The final possibility would be for $(2t-1, 2t)^y$ to have one letter in common with two different transpositions of $(1, 2) \ldots (2t-3, 2t-2)$. But then $(1, 2) \ldots (2t-3, 2t-2)(2t-1, 2t)^y$ is a product of disjoint cycles which are transpositions and a 4-cycle. Hence 4 divides $|x|$, again a contradiction.

We now come to

THEOREM 3.4. *S_n is an $\mathfrak{S}.\mathfrak{R}.$ group for every positive integer n. Moreover, $\mathcal{N}\mathcal{Q}(S_n) = \mathcal{C}\mathcal{P}(S_n)$ for every $n \neq 6$.*

PROOF. By the results of [2], we may assume $n > 2$ and $n \neq 6$. Let $f \in \mathcal{N}\mathcal{Q}(G)$ and note that it suffices to show that $f \in \mathcal{C}\mathcal{P}(G)$. To accomplish this, we set

$$N = \left\{ g \in S_n | f\left(\overline{C}_g\right) \neq \overline{C}_g \right\}$$

and show that N is the empty set.

Suppose N is nonempty. We pick a "minimal element" g of N satisfying the following properties:

(1) Suppose g has its largest cycle of smallest length among the elements of N. Let h denote the length of its largest cycle.

(2) Suppose that g has the fewest number of cycles of length h among the elements of N satisfying (1).

Note that we have $h \geqslant 3$ by Lemma 3.3.

Write $g = \beta_1 \beta_2 \ldots \beta_r$ where the β_i are disjoint cycles and $2 \leqslant |\beta_i| \leqslant |\beta_{i+1}|$. Also, assume that $\beta_r = (1, 2, \ldots, h)$. Let $\gamma_r = (1, 2, \ldots, h-1)$, then $g = \beta_1 \ldots \beta_{r-1}\gamma_r(1, h)$. Also, by the minimality of g,

$$f\left(\overline{C}_{\beta_1 \ldots \beta_{r-1}\gamma_r}\right) = \overline{C}_{\beta_1 \ldots \beta_{r-1}\gamma_r}$$

and by Lemma 3.3, $f(\overline{C}_{(1,h)}) = \overline{C}_{(1,h)}$. Thus by Lemma 2.1

$$f\left(\overline{C}_g\right) = \overline{C}_{\beta_1 \ldots \beta_{r-1}\gamma_r\alpha}$$

where $\alpha = (1, h)^x$ for some $x \in S_n$. Let $y = \beta_1 \ldots \beta_{r-1}\gamma_r\alpha$. We will obtain a contradiction by showing $\overline{C}_g = \overline{C}_y$. The proof of this is broken into the following cases:

Case 1. If $(1, h)^x$ is disjoint from $\beta_1 \ldots \beta_{r-1}\gamma_r$.

In this case, f must fix $\overline{C}_y$ by the minimality of g since y has fewer cycles of length h than g with its largest cycle of length less than or equal to h. But then $f(\overline{C}_g) \neq f(\overline{C}_y) = \overline{C}_y$ and so this case cannot occur.

Case 2. If $(1, h)^x$ has one letter in common with $\beta_1 \ldots \beta_{r-1}\gamma_r$.

Suppose $(n_1, n_2, \ldots, n_t)$ is the cycle of $\beta_1 \ldots \beta_{r-1}\gamma_r$ where the common letter occurs. Then $(1, h)^x = (n_j, a)$ where a does not appear in $\beta_1 \ldots \beta_{r-1}\gamma_r$.

Also, note that

$$(n_1, \ldots, n_t)(n_j, a) = (n_1, \ldots, n_{j-1}, a, n_j, \ldots, n_t).$$

If $t < h - 1$, y would have fewer cycles of length h with its largest cycle of length less than or equal to h. Thus by the minimality of g, $\overline{C}_y$ is fixed by f and so $f(\overline{C}_g) \neq \overline{C}_y$.

If $t > h - 1$, then $t = h$. But then, y has one more cycle of length $h - 1$ than g does. Thus y^h has one more cycle of length $h - 1$ than g^h does. Therefore, by the minimality of g,

$$f\left(\overline{C}_{g^h}\right) = \overline{C}_{g^h} = \overline{C}_{y^h}$$

which is impossible.

Thus we have $t = h - 1$. But then y has the same cycle structure as g, and hence $\overline{C}_g = \overline{C}_y$.

Case 3. If $(1, h)^x$ has two letters in common with $\beta_1 \ldots \beta_{r-1}\gamma_r$.

First, suppose that $(1, h)^x$ has two letters in common with one cycle of $\beta_1 \ldots \beta_{r-1}\gamma_r$. Let $(n_1, \ldots, n_t)$ denote this cycle and suppose $(1, h)^x = (n_j, n_s)$ where $j < s$. Then

$$\begin{aligned}(n_1, \ldots, n_t)&(n_j, n_s)\\ &= (n_1, \ldots, n_{j-1}, n_s, n_{s+1}, \ldots, n_t)(n_j, n_{j+1}, \ldots, n_{s-1})\end{aligned}$$

where the first cycle on the right side of the above equation is taken to be the identity when $j = 1$ and $s = t$. Hence, y has fewer cycles of length h with its largest cycle of length less than or equal to h. By the minimality of g, f fixes $\overline{C}_y$ so that $f(\overline{C}_g) \neq \overline{C}_y$.

Thus, $(1, h)^x$ must have its letters in common with two cycles of $\beta_1 \ldots \beta_{r-1}\gamma_r$. Let $(n_1, \ldots, n_t)$ and $(n'_1, \ldots, n'_s)$ denote these cycles where $t \leqslant s$. Then $(1, h)^x$ has the form (n_i, n'_j) and

$$\begin{aligned}(n_1, \ldots, n_t)&(n'_1, \ldots, n'_s)(n_i, n'_j)\\ &= (n_1, \ldots, n_{i-1}, n'_j, n'_{j+1}, \ldots, n'_s, n'_1, \ldots, n'_j, n_i, \ldots, n_t).\end{aligned}$$

If neither s nor t is $h - 1$, then y has one more cycle of length $h - 1$ than g does. Thus, y^h has one more cycle of length $h - 1$ than g^h does. But then, by the minimality of g, $f(\overline{C}_{g^h}) = \overline{C}_{g^h} \neq \overline{C}_{y^h}$. Hence, either s or t is $h - 1$ and $s + t > h$.

Suppose that g has k_1 1-cycles, k_2 2-cycles, $\ldots$, k_h h-cycles. By Lemma 3.2,

$$|C_g| = n!/k_1!k_2!2^{k_2} \ldots k_h!h^{k_h}.$$

If $s = h - 1$ and $t < s$, then

$$\begin{aligned}|C_y| = n!/\big(&k_1!k_2!2^{k_2} \ldots k_{t-1}!\,(t-1)^{k_{t-1}}(k_t - 1)!\,t^{k_t - 1}\\ &\cdot k_{t+1}!\,(t+1)^{k_{t+1}} \ldots k_{h-1}!\,(h-1)^{k_{h-1}}(k_h - 1)!\,h^{k_h - 1}(s + t)\big).\end{aligned}$$

Since $|C_g| = |C_y|$, $s + t = k_t t k_h h$. But this is impossible since $th > s + t$.

If $t = h - 1$ and $s = h - 1$,

$$|C_y| = n!/\big(k_1!k_2!2^{k_2} \ldots (k_{h-1} - 1)!\,(h-1)^{k_{h-1}-1}(k_h - 1)!\,h^{k_h - 1}(s + t)\big).$$

Thus $|C_g| = |C_y|$ implies $s + t = k_{h-1}(h - 1)k_h h$. But this is also impossible since $(h - 1)h > s + t$.

Finally, if $t = h - 1$ and $s = h$,

$$|C_y| = n!/\left(k_1!k_2!2^{k_2}\ldots k_{h-1}!\,(h-1)^{k_{h-1}}(k_h - 2)!h^{k_h-2}(s+t)\right).$$

Again, since $|C_g| = |C_y|$, $s + t = (k_h - 1)k_h h^2$. Once more, this is impossible since $h^2 > s + t$ and hence Case 3 cannot occur.

Thus, since only Case 2 occurs and since $\overline{C}_g = \overline{C}_y$ in this case, N is the empty set and $f \in \mathcal{C}\mathcal{P}(G)$.

ACKNOWLEDGEMENT. This paper is taken from Chapter V of the author's doctoral thesis written under the supervision of Professor J. E. Adney whom I wish to thank for his encouragement and guidance.

REFERENCES

1. H. Boerner, *Representations of groups*, 2nd English ed., North-Holland, Amsterdam; American Elsevier, New York, 1970. MR **42** #7792.

2. C. F. Brown, *Automorphisms of integral group rings*, Ph. D. Thesis, Michigan State University, 1971.

3. G. L. Peterson, *Automorphisms of integral group rings*. I Arch. Math. (to appear).

4. ———, *Automorphisms of integral group rings*. II (to appear).

5. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N. J., 1964. MR **29** #4785.

6. S. K. Sehgal, *On the isomorphism of integral group rings*. I, Canad. J. Math. **21** (1969), 410–413. MR **41** #366.

DEPARTMENT OF MATHEMATICS, MICHIGAN STATE UNIVERSITY, EAST LANSING, MICHIGAN 48824

DEPARTMENT OF MATHEMATICS, SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, ILLINOIS 62901 (Current address)