International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 10 No. 3 (2021), pp. 103-124.

http://ijgt.ui.ac.ir/
www.ui.ac.ir

MAXIMAL ABELIAN SUBGROUPS OF THE FINITE SYMMETRIC GROUP

JANUSZ KONIECZNY

Communicated by Attila Maroti

Abstract. Let G be a group. For an element $a \in G$, denote by $C^2(a)$ the second centralizer of a in G, which is the set of all elements $b \in G$ such that $bx = xb$ for every $x \in G$ that commutes with a. Let M be any maximal abelian subgroup of G. Then $C^2(a) \subseteq M$ for every $a \in M$. The *abelian rank* (*a-rank*) of M is the minimum cardinality of a set $A \subseteq M$ such that $\bigcup_{a \in A} C^2(a)$ generates M. Denote by S_n the symmetric group of permutations on the set $X = \{1, \ldots, n\}$. The aim of this paper is to determine the maximal abelian subgroups of S_n of a-rank 1 and describe a class of maximal abelian subgroups of S_n of a-rank at most 2.

1. Introduction

Much effort has been devoted to the study of maximal subgroups of the symmetric group S_n (see, for example, [4, 7, 8]). In this paper, we will be interested in maximal *abelian* subgroups of S_n, that is, abelian subgroups of S_n that are not properly included in any abelian subgroup of S_n. Of the latter subgroups relatively little is known: the abelian subgroups of S_n of maximum order were classified in [1, 2]; lower and upper bounds for the number of maximal abelian subgroups of S_n were found in [3]; and it was proved in [9] that maximal elementary abelian subgroups of S_n are maximal abelian subgroups of S_n if and only if they have at most one fixed point.

Manuscript Type: Research Paper
MSC(2010): Primary: 20B35; Secondary: 20K01.
Keywords: Symmetric groups, maximal abelian subgroups, second centralizers, abelian rank.
Received: 07 March 2020, Accepted: 25 April 2020.
http://dx.doi.org/10.22108/ijgt.2020.122036.1603

.

In this paper, we describe a method of constructing some maximal abelian subgroups of S_n. Our approach, which uses the notion of the abelian rank of a maximal abelian subgroup (see Definition 1.1), may perhaps be helpful in finding some maximal abelian subgroups of other groups as well.

Let G be a group. For $a \in G$, the sets $C(a) = \{x \in G : ax = xa\}$ and $C^2(a) = \{b \in G : bx = xb \text{ for every } x \in C(a)\}$ are called, respectively, the (first) *centralizer* and *second centralizer* of a in G. It is easy to see that $C^2(a) \subseteq C(a)$, $C(a)$ is a subgroup of G, and $C^2(a)$ is an abelian subgroup of G. Note that $C^2(a)$ is equal to $Z(C(a))$, the center of $C(a)$.

Let K be a non-empty subset of a group G. We denote by $C(K)$ the centralizer of K in G, that is, $C(K) = \bigcap_{a\in K} C(a)$. Then

$$K \text{ is a maximal abelian subgroup of } G \Leftrightarrow K = C(K). \tag{1.1}$$

Let M be a maximal abelian subgroup of G. Then $C^2(a) \subseteq M$ for every $a \in M$ [6]. Indeed, let $a \in M$. Since M is abelian, $M \subseteq C(a)$. Thus, by (1.1), $M = C(M) \supseteq C(C(a)) = C^2(a)$. This fact motivates the following definition.

Definition 1.1. Let M be a maximal abelian subgroup of a non-abelian group G. We define the *abelian rank* of M (*a-rank* for short) as the minimum cardinality of a set $A \subseteq M$ such that $\bigcup_{a\in A} C^2(a)$ generates M.

Our approach will depend on the following basic facts about the centralizers. For non-empty subsets $A_1, A_2, \dots, A_m$ of a group G,

$$A_1A_2\cdots A_m = \{x_1x_2\cdots x_m : x_1 \in A_1, x_2 \in A_2, \dots, x_m \in A_m\}.$$

Proposition 1.2. *Let A be a non-empty subset of a group G such that the elements of A pairwise commute, and let $M = \langle \bigcup_{a\in A} C^2(a)\rangle$. Then:*

1. *M is an abelian subgroup of $C(A)$;*
2. *M is a maximal abelian subgroup of $G \Leftrightarrow M = C(A)$;*
3. *if $A = \{a_1, a_2, \dots, a_m\}$ is finite, then $M = C^2(a_1)C^2(a_2)\cdots C^2(a_m)$.*

Proof. Let $a_1, a_2 \in A$, $x_1 \in C^2(a_1)$, and $x_2 \in C^2(a_2)$. For every $a \in A$, we have $a_1a = aa_1$, so $x_1 \in C^2(a_1)$ implies $x_1a = ax_1$, that is, $x_1 \in C(a)$. It follows that $\bigcup_{a\in A} C^2(a)$ is a subset of $\bigcap_{a\in A} C(a)$. Further, since $a_1a_2 = a_2a_1$ and $x_1 \in C^2(a_1)$, we have $x_1a_2 = a_2x_1$. Thus, since $x_2 \in C^2(a_2)$, we have $x_1x_2 = x_2x_1$. Hence the elements of $\bigcup_{a\in A} C^2(a)$ pairwise commute, and (1) follows.

To prove (2), we claim that $C(M) = C(A)$. We have $C(M) \subseteq C(A)$ since $A \subseteq M$. If $x \in C(A)$ and $b \in C^2(a)$, where $a \in A$, then x and b commute, so $x \in C(\bigcup_{a\in A} C^2(a))$. Since M is generated by $\bigcup_{a\in A} C^2(a)$, we have $C(\bigcup_{a\in A} C^2(a)) = C(M)$, which implies $C(A) \subseteq C(M)$.

To prove (3), suppose $A = \{a_1, a_2, \dots, a_m\}$, and let $x_i \in C^2(a_i)$ for $i \in \{1, 2, \dots, m\}$. By (1), $x_ix_j = x_jx_i$ for all i, j. Hence any product of elements of $C^2(a_1) \cup \cdots \cup C^2(a_m)$ can be written as a product of elements of $C^2(a_1)$, followed by a product of elements of $C^2(a_2)$, …, followed by a product of elements of $C^2(a_m)$. The result follows since each $C^2(a_i)$ is a subgroup of G. □

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

By Proposition 1.2, if M is any maximal abelian subgroup of G of a-rank m, then $M = C^2(a_1)\cdots C^2(a_m)$ for some commuting elements $a_1,\ldots,a_m$ of G. This fact suggests the following method of finding maximal abelian subgroups of G of a-rank 1 and 2.

(a) Describe the elements of $C(a)$ and $C^2(a)$ for an arbitrary $a \in G$.

(b) Characterize the elements $a \in G$ such that $C^2(a) = C(a)$. Such elements a will determine all maximal abelian subgroups of G of a-rank 1, namely the second centralizers $C^2(a)$.

(c) Select any $a \in G$ such that $C^2(a) \neq C(a)$ and any $b \in C(a) \setminus C^2(a)$ such that $C^2(a)C^2(b) = C(a) \cap C(b)$. Any such pair (a, b) will determine a maximal abelian subgroup of G of a-rank at most 2, namely $C^2(a)C^2(b)$.

(d) For every pair (a, b) as in (c), go through the elements $x \in C^2(a)C^2(b)$ checking if $C(x) = C^2(x)$. The groups $C^2(a)C^2(b)$ for which no such x exists are the maximal abelian groups of a-rank 2.

Regarding (c), we select $b \notin C^2(a)$ since otherwise $C(a) \subseteq C(b)$, and so $C^2(a)C^2(b) = C(a) \cap C(b)$ is equivalent to $C^2(a) = C(a)$, which contradicts the choice of a. Thus to obtain a maximal abelian subgroup of G of a-rank 2, we must select $b \notin C^2(a)$. However, even with such a b, we cannot claim that $C^2(a)C^2(b)$ that is equal to $C(a) \cap C(b)$ has a-rank exactly 2. The reason is that there may exist $x \in C^2(a)C^2(b)$ such that $C^2(x) = C(x)$. Hence, to obtain the maximal abelian subgroups of a-rank exactly 2, (d) must be performed.

The purpose of this paper is to use the approach described above to construct all maximal abelian subgroups of S_n of a-rank 1, and a class of maximal abelian subgroups of S_n of a-rank at most 2. In Section 2, we present a known descriptions of the first and second centralizers of the elements of S_n, and fix a notation that will be used throughout the paper. In Section 3, we describe all maximal abelian subgroups of S_n of a-rank 1 (Theorem 3.1). Our description follows easily from Proposition 1.2 and the work done in [6]. In Section 4, we construct a class of maximal abelian subgroups of S_n of a-rank at most 2 (Theorem 4.11). The construction is in terms of selecting $\alpha \in S_n$ such that $C^2(\alpha) \neq C(\alpha)$, and $\beta \in C(\alpha)\setminus C^2(\alpha)$ such that β satisfies three conditions (A), (B), and (C) (stated before Theorem 4.11) that are sufficient for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n. We apply Theorems 3.1 and 4.11 to constructing all maximal abelian subgroups of S_6 up to conjugation (Example 4.13). We also prove that two of the sufficient condition, (A) and (B), are also necessary for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n (Propositions 4.15, 4.16, and 4.17). The proof of Theorem 4.11, which is quite technical, is presented in Section 5.

2. First and second centralizers of S_n

The first and second centralizers in S_n were described in [10] and [6], respectively. These descriptions are in terms of the decomposition of $\alpha \in S_n$ into cycles.

Definition 2.1. Let $2 \le k \le n$, and $x_0, x_1, \ldots, x_{k-1}$ be pairwise distinct elements of $X = \{1,\ldots,n\}$. As usual, $(x_0\, x_1, \ldots\, x_{k-1})$ will denote $\delta \in S_n$ such that $x_i\delta = x_{i+1}$ for all $i \in \{0, 1, \ldots, k-2\}$,

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

$x_{k-1}\delta = x_0$, and $x\delta = x$ for all other $x \in X$. Any such element is called a *cycle* of length k (or a k-cycle). For $x \in X$, (x) will denote the set $\{x\}$. Any such subset will be called a 1-cycle.

For the remainder of the paper we will fix the following notation.

Notation 2.2. For $\alpha \in S_n$ and $2 \le k \le n$, we denote by Δ_α^k the set of k-cycles in the cycle decomposition of α. In addition, we denote by Δ_α^1 the set $\{(x) : x \in X \text{ and } x\alpha = x\}$, and include these 1-cycles (viewed each as the identity on X) in the cycle decomposition of α. We will denote by Δ_α the union $\bigcup_{k=1}^n \Delta_\alpha^k$.

Finally, given $\alpha \in S_n$, we split the set X into the following pairwise disjoint subsets:

$$X_1^\alpha = \{x \in X : x\alpha = x\},$$
$$X_k^\alpha = \{x \in X : x\delta \ne x \text{ for some } \delta \in \Delta_\alpha^k\}, \text{ where } 2 \le k \le n.$$

In other words, X_1^α is the set of fixed points of α and, for each $k \ge 2$, X_k^α consists of all elements of X that lie on some k-cycle in α.

The following two lemmas describe the first and second centralizers in S_n.

Lemma 2.3. ([10, p. 295]) *Let $\alpha, \beta \in S_n$. Then $\beta \in C(\alpha)$ if and only if for all $k \ge 1$ and $\delta = (x_0\, x_1 \dots x_{k-1}) \in \Delta_\alpha^k$, $\beta^{-1}\delta\beta = (x_0\beta\, x_1\beta \cdots x_{k-1}\beta) \in \Delta_\alpha^k$.*

Lemma 2.3 is an elementary and well-known result in group theory. In fact, more is known. If $\alpha \in S_n$ has r-cycles, with m_i cycles of length k_i $(1 \le i \le r)$, then $C(\alpha) \cong (\mathbb{Z}_{k_1} \wr S_{m_1}) \times \cdots \times (\mathbb{Z}_{k_r} \wr S_{m_r})$, where $\mathbb{Z}_{k_i}$ is the cyclic group with k_i elements and $\mathbb{Z}_{k_i} \wr S_{m_i}$ is the wreath product of $\mathbb{Z}_{k_i}$ and S_{m_i} [10, p. 296].

For a set A, id_A will denote the identity map on A.

Lemma 2.4. ([6, Theorem 3.5]) *Let $\alpha, \beta \in S_n$, and let X_1^α and X_k^α, where $k \ge 2$, be the sets defined in* Notation 2.2. *Then $\beta \in C^2(\alpha)$ if and only if:*

1. *for each integer k with $2 \le k \le n$, there exists an integer w_k such that $0 \le w_k < k$ and $\beta|_{X_k^\alpha} = \alpha^{w_k}|_{X_k^\alpha}$;*
2. *if $|X_1^\alpha| \ne 2$, then $\beta|_{X_1^\alpha} = \mathrm{id}_{X_1^\alpha}$;*
3. *if $X_1^\alpha = \{x_1, x_2\}$ with $x_1 \ne x_2$, then $\beta|_{X_1^\alpha} = \mathrm{id}_{X_1^\alpha}$ or $\beta|_{X_1^\alpha} = (x_1\, x_2)$.*

Lemma 2.5. ([6, Theorem 5.2]) *Let $\alpha \in S_n$. Then $C^2(\alpha) = C(\alpha)$ if and only if $|\Delta_\alpha^1| \le 2$ and $|\Delta_\alpha^k| \le 1$ for all $k \ge 2$.*

3. Maximal abelian subgroups of S_n of a-rank 1

Using Proposition 1.2 and Lemmas 2.4 and 2.5, we can construct all maximal abelian subgroups of S_n of a-rank 1.

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Theorem 3.1. *Select $\alpha \in S_n$ such that α has at most two fixed points and at most one k-cycle for every $k \in \{2, 3, \dots, n\}$. Then $C^2(\alpha)$ is a maximal abelian subgroup of S_n of abelian rank 1. Moreover, every maximal abelian subgroup of S_n of abelian rank 1 can be constructed this way.*

Proof. Suppose $\alpha \in S_n$ such that $|\Delta^1_\alpha| \le 2$ and $|\Delta^k_\alpha| \le 1$ for all $k \ge 2$. Then $C^2(\alpha) = C(\alpha)$ by Lemma 2.5, and so $C^2(\alpha)$ is a maximal abelian subgroup of S_n of a-rank 1 by Proposition 1.2 and Definition 1.1.

Suppose M is a maximal abelian subgroup of S_n of a-rank 1. Then, by Definition 1.1, there is $\alpha \in M$ such that $M = \langle C^2(\alpha)\rangle = C^2(\alpha)$. Thus, by Proposition 1.2, $C^2(\alpha) = C(\alpha)$, and so α has the desired properties by Lemma 2.5. $\square$

Example 3.2. Consider $\alpha_1 = (1\,2)(3\,4\,5)$ and $\alpha_2 = (1\,2)(3\,4\,5\,6)$ in S_6. By Theorem 3.1, $C^2(\alpha_1)$ and $C^2(\alpha_2)$ are maximal abelian subgroups of S_6 of a-rank 1. Moreover, by Lemma 2.4,

$$C^2(\alpha_1) = \{(1\,2)^k(3\,4\,5)^m : 0 \le k \le 1, 0 \le m \le 2\} = \{(1), (3\,4\,5), (3\,5\,4), (1\,2), (1\,2)(3\,4\,5), (1\,2)(3\,5\,4)\},$$

$$\begin{aligned} C^2(\alpha_2) &= \{(1\,2)^k(3\,4\,5\,6)^m : 0 \le k \le 1, 0 \le m \le 3\} \\ &= \{(1), (3\,4\,5\,6), (3\,5)(4\,6), (3\,6\,5\,4), (1\,2), (1\,2)(3\,4\,5\,6), (1\,2)(3\,5)(4\,6), (1\,2)(3\,6\,5\,4)\}. \end{aligned}$$

Note that $C^2(\alpha_1)$ is cyclic, but $C^2(\alpha_2)$ is not.

We can easily find the structure of any maximal abelian subgroup of S_n if a-rank 1. Let $\alpha \in S_n$ be as in Theorem 3.1. Let p be the number of fixed points of α and $\{k_1, \dots, k_r\}$ be the set of lengths of cycles in α, where each $k_i \ge 2$. Then $p \le 2$ and α has exactly one cycle of length k_i. Thus, by Lemma 2.4,

$$C^2(\alpha) \cong \mathbb{Z}_p \times \mathbb{Z}_{k_1} \times \dots \times \mathbb{Z}_{k_r},$$

where, since p can be 0, we define $\mathbb{Z}_0$ to be the trivial group. For example, if $\alpha_1 = (1\,2)(3\,4\,5)$ and $\alpha_2 = (3\,4\,5)$ are permutations in S_5, then $C(\alpha_1) \cong C(\alpha_2) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

4. Maximal abelian subgroups of S_n of a-rank at most 2

In this section, we construct a class of maximal abelian subgroups of S_n of a-rank at most 2 (see Theorem 4.11). Any such subgroup must be of the form $C^2(\alpha)C^2(\beta)$ for some (carefully selected) $\alpha, \beta \in S_n$ (see Definition 1.1 and Proposition 1.2). We formulate sufficient conditions for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n (see (A), (B), and (C) before Theorem 4.11), state Theorem 4.11 in terms of these conditions, and prove that (A) and (B) are also necessary. The proof of Theorem 4.11, which is quite technical, is presented in Section 5. To understand (A)–(C), we need some definitions and results.

Definition 4.1. Let $\alpha \in S_n$. By Lemma 2.3, $C(\alpha)$ acts on Δ_α (and Δ^k_α) by conjugation. For $\beta \in C(\alpha)$, denote by β_α the permutation of Δ_α induced by β. That is, if $\delta = (x_0\, x_1 \dots x_{k-1}) \in \Delta_\alpha$, then $\delta\beta_\alpha = \beta^{-1}\delta\beta = (x_0\beta\, x_1\beta \dots x_{k-1}\beta)$.

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

For any set A, we denote by $\mathrm{Sym}(A)$ the symmetric group of permutations of A. With this notation, β_α from Definition 4.1 is an element of $\mathrm{Sym}(\Delta_\alpha)$. Note that if θ is a cycle in β_α, then $\theta = (\delta_0\,\delta_1 \ldots \delta_{m-1})$, where the δ_i are k-cycles in α for some fixed $k \geq 1$.

Definition 4.2. Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$. Suppose $\theta = (\delta_0\,\delta_2, \ldots \delta_{m-1})$ is a cycle in β_α. The *content* of θ is defined as the following subset of X:

$$\mathrm{cont}(\theta) = \{x \in X : x \text{ lies on some } \delta_i\}. \tag{4.1}$$

Example 4.3. Let $X = \{1, \ldots, 8\}$ and consider $\alpha = (1\,2)(3\,4)(5\,6)(7)(8) \in S_8$. Let $\beta = (1\,3\,2\,4)(7\,8)$. Then $\beta \in C(\alpha)$ and $\beta_\alpha = \theta_1\theta_2\theta_3$, where $\theta_1 = ((1\,2)\,(3\,4))$, $\theta_2 = ((5\,6))$, and $\theta_3 = ((7)\,(8))$, with $\mathrm{cont}(\theta_1) = \{1, 2, 3, 4\}$, $\mathrm{cont}(\theta_2) = \{5, 6\}$, and $\mathrm{cont}(\theta_3) = \{7, 8\}$.

The following lemma is obvious by Definition 4.1.

Lemma 4.4. *Let $\alpha, \beta, \gamma \in S_n$ with $\beta, \gamma \in C(\alpha)$. If $\beta\gamma = \gamma\beta$, then $\beta_\alpha\gamma_\alpha = \gamma_\alpha\beta_\alpha$.*

For an integer $k \geq 1$, we denote by $\mathbb{Z}_k$ the cyclic group of integers modulo k.

Lemma 4.5. *Let $k \geq 1$ be an integer, $a \in \{0, 1, \ldots, k-1\}$, $d = \gcd(a, k)$, and $e = \frac{k}{d}$. Then, there is a unique $s \in \{0, 1, \ldots, e-1\}$ such that $sa = d \pmod{k}$.*

Proof. In $\mathbb{Z}_k$, we have $\langle a \rangle = \langle d \rangle$ and $|\langle d \rangle| = e$. The result follows. □

Definition 4.6. Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$. Suppose $\theta = (\delta_0\,\delta_1 \ldots \delta_{m-1})$ is a cycle in β_α consisting of k-cycles in α with $\delta_0 = (x_0\,x_1 \ldots x_{k-1})$. We denote by $a(\theta)$, $d(\theta)$, $l(\theta)$, and $c(\theta)$ the following integers:

(1) $a(\theta)$ is the unique integer $a \in \{0, 1, \ldots, k-1\}$ such that $x_0\beta^m = x_a$;
(2) $d(\theta) = \gcd(a, k)$, where $a = a(\theta)$;
(3) $l(\theta) = m\frac{k}{d}$, where $d = d(\theta)$;
(4) $c(\theta) = ms$, where $a = a(\theta)$, $d = d(\theta)$, $e = \frac{k}{d}$, and $s \in \{0, 1, \ldots, e-1\}$ is such that $sa = d \pmod{k}$ (see Lemma 4.5).

Remark 4.7. By Lemma 2.3, the integers $a(\theta)$, $d(\theta)$, $l(\theta)$, and $c(\theta)$ from Definition 4.6 do not depend on the cyclical order of $\delta_0, \delta_1, \ldots, \delta_{m-1}$ in the cycle θ or the cyclical order of points within each cycle δ_i.

The following lemma clarifies the meaning of the integers $d(\theta)$, $l(\theta)$, and $c(\theta)$ from Definition 4.6.

Lemma 4.8. *Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$. Suppose $\theta = (\delta_0\,\delta_1 \ldots \delta_{m-1})$ is a cycle in β_α with $\delta_i = (x_0^i\,x_1^i \ldots x_{k-1}^i)$. Let $a = a(\theta)$, $d = d(\theta)$, $e = \frac{k}{d}$, $l = l(\theta) = me$, and $c = c(\theta)$. Then:*

(1) *β contains d disjoint l-cycles, $\sigma_0, \sigma_1, \ldots, \sigma_{d-1}$, with $\sigma_j = (y_0^j\,y_1^j \ldots y_{l-1}^j)$ and $y_0^j = x_j^0$ $(0 \leq j < d)$;*
(2) *α_β contains the cycle $(\sigma_0\,\sigma_1 \ldots \sigma_{d-1})$ and $y_0^0\alpha^d = y_c^0$;*
(3) *$\mathrm{cont}(\theta) = \mathrm{cont}((\sigma_0\,\sigma_1, \ldots \sigma_{d-1}))$.*

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Proof. Let $j \in \{0, 1, \ldots, d-1\}$. Since $x_0^0\beta^m = x_a^0$ and $\alpha\beta^m = \beta^m\alpha$, we have $x_j^0\beta^m = x_{j+a}^0$ by Lemma 2.3. Since the cyclic subgroup $\langle a \rangle$ of $\mathbb{Z}_k$ has e elements: $0, a, \ldots, (e-1)a$, the transformation β^m contains the e-cycle $(x_j^0\, x_{j+a}^0, \ldots\, x_{j+(e-1)a}^0)$, where the subscripts are calculated modulo k. Thus β itself contains

$$(x_j^0\, x_j^0\beta \ldots x_j^0\beta^{m-1}\, x_{j+a}^0\, x_{j+a}^0\beta\, \ldots x_{j+a}^0\beta^{m-1} \ldots x_{j+(e-1)a}^0\, x_{j+(e-1)a}^0\beta \ldots x_{j+(e-1)a}^0\beta^{m-1}),$$

which is our desired l-cycle $\sigma_j = (y_0^j\, y_1^j\, \ldots\, y_{l-1}^j)$ with $y_0^j = x_j^0$. It remains to show that the σ_j are pairwise disjoint. Let $j_1, j_2 \in \{0, 1, \ldots, d-1\}$ with $j_1 \le j_2$. Suppose that $x_{j_2}^0$ lies on σ_{j_1}, that is, $x_{j_2}^0 = x_{j_1+va}^0$ for some $v \in \{0, 1, \ldots, e-1\}$. Then $j_2 - j_1 = va \pmod{k}$. Since d divides both k and a in $\mathbb{Z}$, we obtain $j_2 - j_1 = va = 0 \pmod{d}$, and so $j_2 - j_1 = 0$ since $j_2 - j_1 \in \{0, 1, \ldots, d-1\}$. We have proved (1).

If $j < d-1$, then $y_0^j\alpha = x_j^0\alpha = x_{j+1}^0 = y_0^{j+1}$, so $\sigma_j\alpha_\beta = \sigma_{j+1}$. Further, $y_0^{d-1}\alpha = x_{d-1}^0\alpha = x_d^0 = x_{sa}^0$, where $s \in \{0, 1, \ldots, e-1\}$ (see Lemma 4.5). Thus, since x_{sa}^0 lies on the cycle σ_0, we have $\sigma_{d-1}\alpha_\beta = \sigma_0$. Hence $(\sigma_0\, \sigma_1\, \ldots\, \sigma_{d-1})$ is a cycle in α_β. Consider the cycle

$$\sigma_0 = (x_0^0\, x_0^0\beta \ldots x_0^0\beta^{m-1}\, x_a^0\, x_a^0\beta\, \ldots x_a^0\beta^{m-1} \ldots x_{(e-1)a}^0\, x_{(e-1)a}^0\beta \ldots x_{(e-1)a}^0\beta^{m-1}). \tag{4.2}$$

We have $y_0^0\alpha^d = x_0^0\alpha^d = x_d^0 = x_{sa}^0$, where s is as in Lemma 4.5. The number of elements in the cycle (4.2) to the left of x_{sa}^0 is ms. Thus the index of $y_0^0\alpha^d$ in $\sigma_0 = (y_0^0\, y_1^0\, \ldots, y_{l-1}^0)$ is $ms = c$ (see Definition 4.6). We have proved (2).

Finally, (3) is true since $\operatorname{cont}((\sigma_0\, \sigma_1, \ldots\, \sigma_{d-1})) \subseteq \operatorname{cont}(\theta)$ and $|\operatorname{cont}((\sigma_0\, \sigma_1, \ldots\, \sigma_{d-1}))| = dl = mk = |\operatorname{cont}(\theta)|$. ∎

Our description of α and β in Theorem 4.11 such that $C^2(\alpha)C^2(\beta)$ is a maximal abelian subgroup of S_n is in terms of relations between the cycles in β_α. The latter may contain one or more of four special cycles that are not involved in these relations. These cycles have to do with (3) of Lemma 2.4. Recall that for $\alpha \in S_n$, X_1^α is the set of fixed points of α.

Definition 4.9. Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$. Any cycle θ in β_α such that $\operatorname{cont}(\theta) \subseteq X_1^\alpha$ and $X_1^\alpha = \{x_1, x_2\}$, or $\operatorname{cont}(\theta) \subseteq X_1^\beta$ and $X_1^\beta = \{y_1, y_2\}$, where $x_1 \ne x_2$ and $y_1 \ne y_2$, will be called a *special cycle* in β_α.

Lemma 4.10. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$. Suppose $X_1^\alpha = \{x_1, x_2\}$ or $X_1^\beta = \{y_1, y_2\}$, where $x_1 \ne x_2$ and $y_1 \ne y_2$. Then:*

(1) *exactly one of the following holds:*
  (a) *$|X_1^\alpha| = 2$, $|X_1^\beta| = 2$, and either $X_1^\alpha = X_1^\beta$ or $X_1^\alpha \cap X_1^\beta = \emptyset$,*
  (b) *$|X_1^\alpha| = 2$ and $|X_1^\beta| \ne 1, 2$, or $|X_1^\beta| = 2$ and $|X_1^\alpha| \ne 1, 2$;*

(2) *the special cycles in β_α are:*
  (i) *$((x_1))$ and $((x_2))$ (if ($X_1^\alpha = X_1^\beta = \{x_1, x_2\}$),*
  (ii) *$((x_1)\,(x_2))$ and $((y_1\, y_2))$ (if $X_1^\alpha = \{x_1, x_2\}$, $X_1^\beta = \{y_1, y_2\}$, and $X_1^\alpha \cap X_1^\beta = \emptyset$),*
  (iii) *$((x_1)\,(x_2))$ or $((x_1))$ and $((x_2))$ (if $X_1^\alpha = \{x_1, x_2\}$ and $|X_1^\beta| \ne 1, 2$),*
  (iv) *$((y_1\, y_2))$ or $((y_1))$ and $((y_2))$ (if $X_1^\beta = \{y_1\, y_2\}$ and $|X_1^\alpha| \ne 1, 2$).*

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Proof. Suppose $X_1^\alpha = \{x_1, x_2\}$, where $x_1 \neq x_2$. Since $\beta \in C(\alpha)$, $x_1\beta = x_2$ and $x_2\beta = x_1$, or $x_1\beta = x_1$ and $x_2\beta = x_2$. In the latter case, $\{x_1, x_2\} \subseteq X_1^\beta$, and either (a) holds (if $X_1^\beta = \{x_1, x_2\}$) or (b) holds (if $X_1^\beta \neq \{x_1, x_2\}$). Suppose $x_1\beta = x_2$ and $x_2\beta = x_1$ and $|X_1^\beta| \geq 1$, and let y_1 be a fixed point of β. The point y_1 must lie on some cycle $(y_1 \cdots)$ in α. Since $\beta \in C(\alpha)$, every point on this cycle is fixed by β. Thus $(y_1 \ldots) = (y_1\, y_2\, \ldots)$ has length ≥ 2 since otherwise α would have the third fixed point. Hence, either $X_1^\beta = \{y_1, y_2\}$ and $X_1^\alpha \cap X_1^\beta = \emptyset$, or $|X_1^\beta \geq 3$. It follows by the foregoing argument (and the symmetrical one for β) that then (a) or (b) holds. We have proved (1). Statement (2) follows immediately from (1) and the fact that $\alpha\beta = \beta\alpha$. □

Let $\alpha \in S_n$ with $C^2(\alpha) \neq C(\alpha)$, and $\beta \in C(\alpha) \setminus C^2(\alpha)$. We can now state the sufficient conditions for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n.

- (A) If θ_1 and θ_2 are distinct non-special cycles in β_α of length m_1 and m_2, respectively, both consisting of k-cycles in α, $a_1 = a(\theta_1)$, and $a_2 = a(\theta_2)$, then:
  - (i) $\gcd(a_1, a_2)$ is a unit in $\mathbb{Z}_k$;
  - (ii) if $l(\theta_1) = l(\theta_2)$, then $k \geq 3$, $m_1 = m_2 = 1$, and a_1, a_2, and $a_1 - a_2$ are units in $\mathbb{Z}_k$.
- (B) If θ_1 and θ_2 are distinct non-special cycles in β_α such that $l(\theta_1) = l(\theta_2)$ $(= l)$, $c_1 = c(\theta_1)$, and $c_2 = c(\theta_2)$, then $\gcd(c_1, c_2)$ is a unit in $\mathbb{Z}_l$.
- (C) There do not exist pairwise distinct non-special cycles θ_1, θ_2, and θ_3 in β_α such that θ_1 and θ_2 consist of k-cycles in α, and $l(\theta_2) = l(\theta_3)$.

If $k = 1$ in (A), then $a_1 = a_2 = 0$. We agree that $\gcd(0, 0) = 0$. Note that 0 is a unit in $\mathbb{Z}_1 = \{0\}$. The same remark applies to the case when $l = 1$ in (B).

Here is the main theorem of the paper.

Theorem 4.11. *Select $\alpha \in S_n$ with $C^2(\alpha) \neq C(\alpha)$. Then select $\beta \in C(\alpha) \setminus C^2(\alpha)$ that satisfies conditions* (A)*,* (B)*, and* (C)*. Then $C^2(\alpha)C^2(\beta)$ is a maximal abelian subgroup of S_n of a-rank at most* 2*.*

The labels (A), (B), and (C) will be unique in this paper. The reader should remember that the conditions labeled by these symbols appear before Theorem 4.11.

In the remainder of this section, we give some examples and prove that (A) and (B) are necessary for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n. We will prove Theorem 4.11 in Section 5.

Example 4.12. Consider $\alpha = (1\,2\,3\,4)(5\,6\,7\,8)$ and $\beta = (1\,5\,3\,7)(2\,6\,4\,8)$ in S_8. Then $\beta \in C(\alpha) \setminus C^2(\alpha)$ and $\beta_\alpha = ((1\,2\,3\,4)\,(5\,6\,7\,8))$ is a 2-cycle. Thus β satisfies (A)–(C), and so $C^2(\alpha)C^2(\beta)$ is a maximal abelian subgroup of S_8. By Lemma 2.4,

$$C^2(\alpha)C^2(\beta) = \{(1), (1\,2\,3\,4)(5\,6\,7\,8), (1\,3)(2\,4)(5\,7)(6\,8), (1\,4\,3\,2)(5\,8\,7\,6), (1\,5\,3\,7)(2\,6\,4\,8),$$
$$(1\,7\,3\,5)(2\,8\,4\,6), (1\,6)(2\,7)(3\,8)(4\,5), (1\,8)(2\,5)(3\,6)(4\,7)\}.$$

This subgroup has a-rank 2, order 8, and is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

Recall that subgroups H_1 and H_2 of a group G are conjugate if $H_2 = a^{-1}H_1a$ for some $a \in G$.

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Example 4.13. In this example, we will apply Theorems 3.1 and 4.11 to constructing all maximal abelian subgroups of S_6 up to conjugation. By Theorem 3.1, S_6 has (up to conjugation) four maximal abelian subgroups of a-rank 1:

$$\begin{aligned}
M_1 &= C^2((1\,2\,3\,4\,5\,6)) = \langle(1\,2\,3\,4\,5\,6)\rangle,\\
M_2 &= C^2((1\,2\,3\,4\,5)) = \langle(1\,2\,3\,4\,5)\rangle,\\
M_3 &= C^2((1\,2\,3)(4\,5)) = \langle(1\,2\,3)(4\,5)\rangle,\\
M_4 &= C^2((1\,2\,3\,4)(5\,6)) = C^2((1\,2\,3\,4)).
\end{aligned}$$

The subgroups M_1, M_2, and M_3 are cyclic, while M_4 is not cyclic. The latter is conjugate to $C^2(\alpha_2)$ from Example 3.2, and isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

To construct maximal abelian subgroups of S_6 of a-rank 2, we select commuting $\alpha, \beta \in S_6$ such for all $x, y \in \{\alpha, \beta\}$ with $x \neq y$, $C^2(x) \neq C(x)$ and $y \notin C^2(x)$. Moreover, we can ignore such α, β if they already appear in a maximal abelian subgroup of S_6 already constructed. Further, note that for every $\alpha \in S_6$ that contains a k-cycle with $k \geq 4$, we have $C(\alpha) = C^2(\alpha)$, that is, a maximal abelian subgroup of S_6 of a-rank 1.

It turns out that S_6 has (up to conjugation) three maximal abelian subgroups of a-rank 2, and no maximal abelian subgroup of a-rank ≥ 3.

Suppose $\alpha = (1\,2\,3)(4\,5\,6)$ and $\beta = (1\,2\,3)(4\,6\,5)$. Then

$$\beta_\alpha = \theta_1\theta_2 = ((1\,2\,3))((4\,5\,6)).$$

The 1-cycles θ_1 and θ_2 in β_α consist of 3-cycles in α. We have (see Definition 4.6, and also Lemma 4.8): $a(\theta_1) = 1$, $l(\theta_1) = 3$, $c(\theta_1) = 1$, $a(\theta_2) = 2$, $l(\theta_2) = 3$, and $c(\theta_2) = 2$. Thus β satisfies (A)–(C), and so $M_5 = C^2(\alpha)C^2(\beta)$ is a maximal abelian group of S_6. By Lemma 2.4,

$$\begin{aligned}
M_5 = C^2((1\,2\,3)(4\,5\,6))C^2((1\,2\,3)(4\,6\,5)) = \{&(1), (1\,2\,3)(4\,5\,6), (1\,3\,2)(4\,6\,5), (1\,2\,3)(4\,6\,5), (1\,3\,2)(4\,5\,6),\\
&(1\,3\,2), (4\,6\,5), (4\,5\,6), (1\,2\,3)\}.
\end{aligned}$$

The subgroup M_5 has a-rank 2, and is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. It is an abelian subgroup of S_6 of maximum order (see [2, Thm. 1]).

Suppose $\alpha = (1\,2)(3\,4)(5\,6)$ and $\beta = (1\,3)(2\,4)(5)(6)$. Then

$$\beta_\alpha = \theta_1\theta_2 = ((1\,2)\,(3\,4))((5\,6)).$$

Since the cycle θ_2 is special, β satisfies (A)–(C), and so $M_6 = C^2(\alpha)C^2(\beta)$ is a maximal abelian group of S_6. By Lemma 2.4,

$$\begin{aligned}
M_6 = C^2((1\,2)(3\,4)(5\,6))C^2((1\,3)(2\,4)) = \{&(1), (1\,2)(3\,4)(5\,6), (1\,3)(2\,4), (5\,6), (1\,3)(2\,4)(5\,6),\\
&(1\,4)(2\,3)(5\,6), (1\,2)(3\,4), (1\,4)(2\,3)\}.
\end{aligned}$$

The subgroup M_6 has a-rank 2, and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Suppose $\alpha = (1\,2)(3\,4)(5)(6)$ and $\beta = (1\,2)(5\,6)(3)(4)$. Then

$$\beta_\alpha = \theta_1\theta_2\theta_3 = ((1\,2))((3\,4))((5)\,(6)).$$

Since the cycles θ_2 and θ_3 are special, β satisfies (A)–(C), and so $M_7 = C^2(\alpha)C^2(\beta)$ is a maximal abelian group of S_6. By Lemma 2.4,

$$M_7 = C^2((1\,2)(3\,4))C^2((1\,2)(5\,6)) = \{(1),(1\,2)(3\,4),(5\,6),(1\,2)(3\,4)(5\,6),(1\,2)(5\,6),(3\,4),(3\,4)(5\,6),(1\,2)\}.$$

The subgroup M_7 has a-rank 2, and is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

For the remaining choices of α and β, we find that (up to conjugation) they lie in one of the subgroups already constructed. For example, $\alpha = (1\,2\,3)(4\,5\,6)$, $\beta = (1\,4)(2\,5)(3\,6)$ lie in the conjugate $\langle(1\,5\,3\,4\,2\,6)\rangle$ of M_1; $\alpha = (1\,2\,3)$, $\beta = (4\,5)$ lie in M_3; and $\alpha = (1\,2)$, $\beta = (3\,4)$ lie in M_7.

Since the maximum order of an abelian subgroup of S_6 is 9 [2, Thm. 1], S_6 does not have a maximal abelian subgroup of a-rank ≥ 4. Suppose $M = C^2(\alpha)C^2(\beta)C^2(\gamma)$ is a maximal abelian subgroup of S_6 of a-rank 3. Since $|M| \leq 9$, it follows that α, β, γ have order 2. Moreover, since M has a-rank 3, for all $x, y \in \{\alpha, \beta, \gamma\}$, with $x \neq y$, $C^2(x) \neq C(x)$ and $y \notin C^2(x)$. Analyzing (up to conjugation), the possibilities for such α, β, and γ, we find that they all lie in M_6 or in M_7. It follows that S_6 does not have a maximal abelian subgroup of a-rank 3.

Therefore, we have constructed all maximal abelian subgroups of S_6. There are seven such subgroups up to conjugation: M_1–M_7. Four of these have a-rank 1: M_1–M_4 (of which only M_4 is not cyclic), and three have a-rank 2: M_5–M_7. Up to isomorphism, S_6 has five maximal abelian subgroups: $\mathbb{Z}_6$, $\mathbb{Z}_5$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_3 \times \mathbb{Z}_3$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The first three have a-rank 1, and the last two a-rank 2.

We will now prove that conditions (A) and (B) are necessary for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n. The following lemma will be crucial.

Lemma 4.14. *Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$, $\gamma \in C^2(\alpha)C^2(\beta)$, and $x, y \in X$ such that neither x nor y is an element of* $\operatorname{cont}(\theta)$*, where θ is a special cycle in β_α. Then:*

1. *$x\gamma = x(\alpha^g\beta^s)$ and $y\gamma = y(\alpha^h\beta^t)$ for some $g, s, h, t \geq 0$;*
2. *if x and y lie on cycles in α of the same length, then g and h from* (1) *can be selected so that $g = h$;*
3. *if x and y lie on cycles in β of the same length, then s and t from* (1) *can be selected so that $s = t$.*

Proof. We have $\gamma = \gamma_1\gamma_2$, where $\gamma_1 \in C^2(\alpha)$ and $\gamma_2 \in C^2(\beta)$. By the hypothesis about x, it is not the case that $X_1^\alpha = \{x, z\}$ for some $z \neq x$. Thus, by Lemma 2.4, $x\gamma_1 = x\alpha^g$ for some $g \geq 0$. Suppose $x\alpha^g \in X_1^\beta$. Then, since x and $x\alpha^g$ lie on the same cycle of α, we have $x \in X_1^\beta$ by Lemma 2.4. Thus, by the hypothesis about x again, it is not the case that $X_1^\beta = \{x\alpha^g, z\}$ for some $z \neq x\alpha^g$. Hence $(x\alpha^g)\gamma_2 = (x\alpha^g)\beta^s$ for some $s \geq 0$. By the same argument $y\gamma = (x\alpha^h)\beta^t$ for some $h, t \geq 0$. This proves (1). Statement (2) follows by Lemma 2.4. Finally, suppose x and y lie on cycles in β of the same length. Then, since $\alpha\beta = \beta\alpha$, $x\alpha^g$ and $y\alpha^h$ also lie on cycles in β of the same length, and so (3) follows by Lemma 2.4. □

The following proposition shows that condition (A)(i) is necessary.

Proposition 4.15. *Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$. Suppose $\theta_1 = (\delta_0\, \delta_1\, \ldots\, \delta_{m_1-1})$ and $\theta_2 = (\tau_0\, \tau_1\, \ldots\, \tau_{m_2-1})$ are distinct non-special cycles in β_α both consisting of k-cycles in α, $a_1 = a(\theta_1)$ and $a_2 = a(\theta_2)$. If $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$, then $\gcd(a_1, a_2)$ is a unit in $\mathbb{Z}_k$.*

Proof. Suppose $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$. Let $\gamma = \tau_0\tau_1 \cdots \tau_{m_2-1} \in S_n$. Then $\gamma \in C(\alpha) \cap C(\beta)$, and so $\gamma \in C^2(\alpha)C^2(\beta)$. Let $\delta_0 = (x_0\, x_1\, \ldots\, x_{k-1})$ and $\tau_0 = (y_0\, y_1\, \ldots\, y_{k-1})$. By Lemma 4.14, $x_0\gamma = x_0(\alpha^g\beta^s)$ and $y_0\gamma = y_0(\alpha^g\beta^t)$ for some $g, s, t \geq 0$. Since $(x_0\alpha^g)\beta^s = x_0\gamma = x_0$ and $x_0\alpha^g$ both lie on δ_0, s must be a multiple of m_1, say $s = um_1$ for some $u \geq 0$. Similarly, since $(y_0\alpha^g)\beta^t = y_0\gamma = y_1$ and $y_0\alpha^g$ both lie on τ_0, $t = vm_2$ for some $v \geq 0$. Since $a_1 = a(\theta_1)$ and $a_2 = a(\theta_2)$, we have $x_0\beta^{m_1} = x_{a_1}$ and $y_0\beta^{m_2} = y_{a_2}$ (see Definition 4.6). Thus, $x_0 = (x_0\alpha^g)\beta^{um_1} = x_g\beta^{um_1} = x_{g+ua_1}$ and $y_1 = (y_0\alpha^g)\beta^{vm_2} = y_g\beta^{vm_2} = y_{g+va_2}$, and so $g + ua_1 = 0 \pmod{k}$ and $g + va_2 = 1 \pmod{k}$. Hence $(-u)a_1 + va_2 = 1 \pmod{k}$, which implies that $\gcd(a_1, a_2)$ is a unit in $\mathbb{Z}_k$. □

The following proposition shows that condition (A)(ii) is necessary.

Proposition 4.16. *Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$. Suppose $\theta_1 = (\delta_0\, \delta_1\, \ldots\, \delta_{m_1-1})$ and $\theta_2 = (\tau_0\, \tau_1\, \ldots\, \tau_{m_2-1})$ are distinct non-special cycles in β_α both consisting of k-cycles in α, $a_1 = a(\theta_1)$, $a_2 = a(\theta_2)$, and $l(\theta_1) = l(\theta_2)$. If $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$, then $k \geq 3$, $m_1 = m_2$, and a_1, a_2, and $a_1 - a_2$ are units in $\mathbb{Z}_k$.*

Proof. Suppose $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$. Let $l = l(\theta_1) = l(\theta_2)$. Let $\gamma = \tau_0\tau_1 \cdots \tau_{m_2-1} \in S_n$. Then $\gamma \in C(\alpha) \cap C(\beta)$, and so $\gamma \in C^2(\alpha)C^2(\beta)$. Let $\delta_0 = (x_0\, x_1\, \ldots\, x_{k-1})$ and $\tau_0 = (y_0\, y_1\, \ldots\, y_{k-1})$. By Lemma 4.8, x_0 and y_0 both lie on k-cycles in α and l-cycles in β. Thus, by Lemma 4.14, $x_0\gamma = x_0(\alpha^g\beta^t)$ and $y_0\gamma = y_0(\alpha^g\beta^t)$ for some $g, t \geq 0$. As in the proof of Proposition 4.15, we obtain some $u, v \geq 0$ such that $t = um_1$, $t = vm_2$, $g + ua_1 = 0 \pmod{k}$, and $g + va_2 = 1 \pmod{k}$.

Let $e_1 = \frac{k}{\gcd(a_1,k)}$ and $e_2 = \frac{k}{\gcd(a_2,k)}$. Note that $e_1m_1 = l$ and $e_2m_2 = l$ (see Definition 4.6), and that $e_1a_1 = 0 \pmod{k}$ and $e_2a_2 = 0 \pmod{k}$. Since $um_1 = vm_2 = t$ and $e_1m_1 = e_2m_2 = l$, we obtain $ve_1m_2 = e_1vm_2 = e_1um_1 = ue_1m_1 = ue_2m_2$, and so $ve_1 = ue_2$. Now, we have

$$\begin{aligned} g + va_2 &= 1 \pmod{k}, \\ e_1g + e_1va_2 &= e_1 \pmod{k}, \\ e_1g + e_2ua_2 &= e_1 \pmod{k}, \\ e_1g + u0 &= e_1 \pmod{k}, \\ e_1g &= e_1 \pmod{k}. \end{aligned}$$

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

On the other hand,

$$\begin{aligned} g + ua_1 &= 0 \pmod{k}, \\ e_1 g + e_1 u a_1 &= 0 \pmod{k}, \\ e_1 g + u0 &= 0 \pmod{k}, \\ e_1 g &= 0 \pmod{k}. \end{aligned}$$

Thus $e_1 = e_1 g = 0 \pmod{k}$. Similarly, $e_2 = 0 \pmod{k}$. Thus $e_1 = e_2 = k$, and so $\gcd(a_1, k) = \gcd(a_2, k) = 1$, that is, a_1 and a_2 are units in $\mathbb{Z}_k$. Now, we have $e_1 = e_2 = k$, $ve_1 = ue_2$, and $e_1 m_1 = e_2 m_2$. Hence $u = v$ and $m_1 = m_2$. From $u = v$, we obtain $g + ua_1 = 0 \pmod{k}$, and $g + ua_2 = 1 \pmod{k}$, which implies $u(a_2 - a_1) = 1 \pmod{k}$. Thus $a_1 - a_2$ is a unit in $\mathbb{Z}_k$.

Let $m = m_1 = m_2$. We will show that $m = 1$. Suppose to the contrary that $m \geq 2$. Recall that $x_0\gamma = x_0(\alpha^g\beta^t)$ and $y_0\gamma = y_0(\alpha^g\beta^t)$. Since $(x_0\alpha^g)\beta^t = x_0\gamma = x_0$ and $x_0\alpha^g$ both lie on the cycle δ_0, t must be a multiple of m. On the other hand, $(y_0\alpha^g)\beta^t = y_0\gamma = y_0\beta$ lies on τ_1 and $y_0\alpha^g$ lies on τ_0. Since $m \geq 2$, we have $\tau_0 \neq \tau_1$, which implies that t cannot be a multiple of m. This is a contradiction. Hence $m_1 = m_2 = 1$.

It remains to show that $k \geq 3$. First, $k \neq 2$ since otherwise a_1, a_2, and $a_1 - a_2$ would not be all units. Suppose to the contrary that $k = 1$. Then $\theta_1 = ((x_0))$ and $\theta_2 = ((y_0))$. Define $\eta = (x_0\, y_0) \in S_n$. Then $\eta \in C(\alpha) \cap C(\beta)$, and so $\eta \in C^2(\alpha)C^2(\beta)$. By Lemma 4.14, $x_0\eta = x_0(\alpha^h\beta^s)$ for some $h, s \geq 0$. This is a contradiction since $x_0\eta = y_0$ and $x_0(\alpha^h\beta^s) = x_0$. Hence $k \geq 3$. □

Finally, the following proposition shows that condition (B) is necessary.

Proposition 4.17. *Let $\alpha, \beta \in S_n$ with $\alpha\beta = \beta\alpha$. Suppose θ_1 and θ_2 are distinct non-special cycles in β_α consisting of k_1- and k_2-cycles in α, respectively, such that $l(\theta_1) = l(\theta_2)$ $(= l)$, $c_1 = c(\theta_1)$, and $c_2 = c(\theta_2)$. If $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$, then $\gcd(c_1, c_2)$ is a unit in $\mathbb{Z}_l$.*

Proof. Suppose $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$. By Lemma 4.8, α_β has distinct non-special cycles $\phi_1 = (\sigma_0\, \sigma_1\, \ldots\, \sigma_{d_1-1})$ and $\phi_2 = (\rho_0\, \rho_1\, \ldots\, \rho_{d_2-1})$, both consisting of l-cycles in β. Let $\sigma_0 = (y_0, \ldots\, y_{l-1})$ and $\rho_0 = (z_0, \ldots\, z_{l-1})$. Again by Lemma 4.8, $y_0\alpha^{d_1} = y_{c_1}$ and $z_0\alpha^{d_2} = z_{c_2}$. Thus $\gcd(c_1, c_2)$ is a unit in $\mathbb{Z}_l$ by Proposition 4.15 applied to α and β with their roles reversed. □

We point out that condition (C) is not necessary for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n. Indeed, consider $\alpha = (1\,2)(3)(4)(5)$ and $\beta = (1)(2)(3\,4)(5)$ in S_5. Then $\beta_\alpha = \theta_1\theta_2\theta_3 = ((1\,2))((3)\,(4))((5))$. The cycles θ_2 and θ_3 consist of 1-cycles in α, with $l(\theta_2) = 2$ and $l(\theta_3) = 1$. The cycle θ_1 consists of 2-cycles in α, with $l(\theta_1) = 1$. Thus β does not satisfy (C). However, $C^2(\alpha)C^2(\beta) = \{(1), (1\,2), (3\,4), (1\,2)(3\,4)\}$ is a maximal abelian subgroup of S_5 since $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$.

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

5. Proof of the main theorem

In this section, we will prove Theorem 4.11. Recall that, by Proposition 1.2, if G is a group and $a, b \in G$ with $ab = ba$, then

$$C^2(a)C^2(b) \text{ is a maximal abelian subgroup of } G \Leftrightarrow C^2(a)C^2(b) = C(a) \cap C(b). \tag{5.1}$$

To prove that conditions (A)–(C) are sufficient for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n, we will use Lemma 2.4 and (5.1). The first step is to show that if $\gamma \in C(\alpha) \cap C(\beta)$ and θ is a non-special cycle in β_α, then there are integers $g, t \geq 0$ such that $x\gamma = x(\alpha^g\beta^t)$ for all $x \in \mathrm{cont}(\theta)$. This first step is proved in the next three lemmas. We note that the first time we will need condition (C) is in Lemma 5.10.

Lemma 5.1. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)*. Suppose $\gamma \in C(\alpha) \cap C(\beta)$. Then, for any non-special cycle θ in β_α, $\theta^{-1}\gamma_\alpha\theta = \theta$.*

Proof. Suppose $\theta = (\delta_0\, \delta_1\, \dots\, \delta_{m-1})$ is a non-special m-cycle in β_α consisting of k-cycles in α. We have $\beta_\alpha\gamma_\alpha = \gamma_\alpha\beta_\alpha$ by Lemma 4.4. Thus, by Lemma 2.3 applied to β_α and γ_α, $\theta_1 = \theta^{-1}\gamma_\alpha\theta = (\delta_0\gamma_\alpha\, \delta_1\gamma_\alpha, \dots\, \delta_{m-1}\gamma_\alpha)$ is also an m-cycle consisting of k-cycles in α. Note that $\mathrm{cont}(\theta) = \{x\gamma^{-1} : x \in \mathrm{cont}(\theta_1)\}$. Since $\gamma^{-1} \in C(\alpha) \cap C(\beta)$, it follows by Definition 4.9 and Lemma 4.10 that θ_1 is not a special cycle in β_α. Suppose to the contrary that $\theta_1 \neq \theta$. Let $\delta_0 = (x_0\, x_1\, \dots\, x_{k-1})$. Then $\delta_0\gamma_\alpha = (y_0\, y_1\, \dots\, y_{k-1})$, where $y_i = x_i\gamma$. Let $a = a(\theta)$ and $a_1 = a(\theta_1)$. Then, $x_0(\beta^m\gamma) = x_a\gamma = y_a$ and $x_0(\gamma\beta^m) = y_0\beta^m = y_{a_1}$. Since γ and β^m commute, we obtain $a = a_1 \pmod k$. Thus, $l(\theta) = m\frac{k}{\gcd(a,k)} = m\frac{k}{\gcd(a_1,k)} = l(\theta_1)$ (see Definition 4.6). Hence, by (A)(ii), $k \geq 3$ and $a - a_1$ is a unit in $\mathbb{Z}_k$. This is a contradiction since $a - a_1 = a - a = 0 \pmod k$. Hence $\theta_1 = \theta$. □

Lemma 5.2. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)*. Suppose $\gamma, \lambda \in C(\alpha) \cap C(\beta)$. Let $\theta = (\delta_0\, \delta_1\, \dots\, \delta_{m-1})$ be a non-special cycle in β_α and let $x \in \mathrm{cont}(\theta)$. If $x\gamma = x\lambda$, then $y\gamma = y\lambda$ for every $y \in \mathrm{cont}(\theta)$.*

Proof. For $0 \leq i < m$, let $\delta_i = (x^i_0\, x^i_1\, \dots\, x^i_{k-1})$. We may assume that $x = x^0_0$. By Lemma 5.1, $\delta_0\gamma_\alpha = \delta_w$ for some w. Since $x^0_0\gamma = x^0_0\lambda$, we also have $\delta_0\lambda_\alpha = \delta_w$. Since $\gamma_\alpha, \lambda_\alpha \in C(\beta_\alpha)$, it follows that $\delta_i\gamma_\alpha = \delta_i\lambda_\alpha = \delta_{i+w}$ for every i.

Let s_i, t_i, and p_i be such that $x^i_0\gamma = x^{i+w}_{s_i}$, $x^i_0\lambda = x^{i+w}_{t_i}$, and $x^i_0\beta = x^{i+1}_{p_i}$. Since $\beta, \gamma \in C(\alpha)$, we have

$$x^i_0(\beta\gamma) = x^{i+1}_{p_i}\gamma = x^{i+1+w}_{p_i+s_{i+1}} \quad \text{and} \quad x^i_0(\gamma\beta) = x^{i+w}_{s_i}\beta = x^{i+w+1}_{s_i+p_{i+w}}$$

by Lemma 2.3. Since $\beta\gamma = \gamma\beta$, it follows that $p_i + s_{i+1} = s_i + p_{i+w} \pmod k$, and so $s_{i+1} - s_i = p_{i+w} - p_i \pmod k$. Similarly, $t_{i+1} - t_i = p_{i+w} - p_i \pmod k$, and so $s_{i+1} - s_i = t_{i+1} - t_i \pmod k$.

Next, we have $x^0_0\gamma = x^w_{s_0}$ and $x^0_0\lambda = x^w_{t_0}$. Thus $x^w_{s_0} = x^w_{t_0}$, and so $s_0 = t_0 \pmod k$. The latter, combined with $s_{i+1} - s_i = t_{i+1} - t_i \pmod k$ for all i, gives $s_i = t_i \pmod k$ for all i. Thus, for all i and j, $x^i_j\gamma = x^{i+w}_{j+s_i} = x^{i+w}_{j+t_i} = x^i_j\lambda$. □

Lemma 5.3. *Let $\alpha,\beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A). *Suppose $\gamma \in C(\alpha)\cap C(\beta)$. Let $\theta = (\delta_0\,\delta_1\,\dots\,\delta_{m-1})$ be a non-special cycle in β_α. Then there are integers $g,t \geq 0$ such that for every $x \in \operatorname{cont}(\theta)$, $x\gamma = x(\alpha^g\beta^t)$.*

Proof. Let $\delta_0 = (x_0\,x_1\,\dots\,x_{k-1})$. Then, by Lemma 5.1, $x_0\gamma$ lies on $\delta_t = (y_0\,y_1\,\dots\,y_{k-1})$ for some $t \in \{0,1,\dots,m-1\}$. Let $y_i = x_0\gamma$ and $y_j = x_0\beta^t$. Then

$$x_0\gamma = y_i = y_j\alpha^{k-j+i} = (x_0\beta^t)\alpha^{k-j+i} = x_0(\alpha^g\beta^t),$$

where $g = k-j+i$. Thus, by Lemma 5.2, $x\gamma = x(\alpha^g\beta^t)$ for every x that lies on any δ_i. □

Let $\alpha,\beta,\gamma,\theta$ and g,t be as in Lemma 5.3. Let k be the length of each cycle in θ, $l = l(\theta)$, and $x \in \operatorname{cont}(\theta)$. Then x lies on a k-cycle in α and on an l-cycle in β (by Lemma 4.8), and $x\gamma = x(\alpha^g\beta^t)$. To prove that $\gamma \in C^2(\alpha)C^2(\beta)$, we need to show that the same g can be selected for all non-special cycles θ_1 in β_α that consist of of k-cycles in α, and that the same t can be selected for all non-special cycles θ_2 in β_α such that $l(\theta_2) = l$ (see Lemma 2.4).

Lemma 5.4. *Let $k \geq 1$, a_1, and a_2 be integers such that $a_1 - a_2$ is a unit in $\mathbb{Z}_k$. Then, for all integers b_1 and b_2, the system of congruences*

$$x + a_1y = b_1 \pmod{k}$$
$$x + a_2y = b_2 \pmod{k}$$

with variables x and y, has a solution.

Proof. Let b_1 and b_2 be integers. For a unit c in $\mathbb{Z}_k$, let c^{-1} be the inverse of c in $\mathbb{Z}_k$. Consider $x = (a_1-a_2)^{-1}(a_1b_2 - a_2b_1)$ and $y = (a_1-a_2)^{-1}(b_1-b_2)$. Then

$$x + a_1y = (a_1-a_2)^{-1}(a_1b_2 - a_2b_1) + a_1(a_1-a_2)^{-1}(b_1-b_2) = b_1 \pmod{k},$$
$$x + a_2y = (a_1-a_2)^{-1}(a_1b_2 - a_2b_1) + a_2(a_1-a_2)^{-1}(b_1-b_2) = b_2 \pmod{k}.$$

Thus a solution exists. □

Lemma 5.5. *Let $\alpha,\beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A). *Suppose $\gamma \in C(\alpha)\cap C(\beta)$. Let θ_1 and θ_2 be distinct non-special cycles in β_α consisting of k-cycles in α with $l(\theta_1) = l(\theta_2)$. Then there are integers $g,t \geq 0$ such that for every $x \in \operatorname{cont}(\theta_1)\cup\operatorname{cont}(\theta_2)$, $x\gamma = x(\alpha^g\beta^t)$.*

Proof. Let $a_1 = a(\theta_1)$ and $a_2 = a(\theta_2)$. By (A)(i), θ_1 and θ_2 are 1-cycles and $a_1 - a_2$ is a unit in $\mathbb{Z}_k$. Let $\theta_1 = (\delta_1)$ and $\theta_2 = (\delta_2)$ with $\delta_1 = (x_0\,x_1\,\dots\,x_{k-1})$ and $\delta_2 = (y_0\,y_1\,\dots\,y_{k-1})$. We have $x_0\beta = x_{a_1}$ and $y_0\beta = y_{a_2}$. By Lemma 5.1, $x_0\gamma = x_{b_1}$ and $y_0\gamma = y_{b_2}$ for some b_1 and b_2. By Lemma 5.4, there are $g,t \in \{0,1,\dots,k-1\}$ such that $g + a_1t = b_1$ and $g + a_2t = b_2$. Then

$$x_0(\alpha^g\beta^t) = (x_0\beta^t)\alpha^g = x_{ta_1}\alpha^g = x_{ta_1+g} = x_{g+a_1t} = x_{b_1} = x_0\gamma.$$

Similarly $y_0(\alpha^g\beta^t) = y_{g+a_2t} = y_{b_2} = y_0\gamma$. Hence, by Lemma 5.2, $x\gamma = x(\alpha^g\beta^t)$ for every $x \in \operatorname{cont}(\theta_1)\cup\operatorname{cont}(\theta_2)$. □

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Lemma 5.6. *Let $k \geq 1$ be an integer. Suppose $a_1, a_2, \ldots, a_p$, $p \geq 1$, are integers such that $\gcd(a_i, a_j)$ is a unit in $\mathbb{Z}_k$ if $i \neq j$. Then, for all integers $b_1, b_2, \ldots, b_p$, the system of congruences*

$$x + a_1 x_1 = b_1 \pmod{k}$$
$$x + a_2 x_2 = b_2 \pmod{k}$$
$$\vdots$$
$$x + a_p x_p = b_p \pmod{k},$$

with variables $x, x_1, x_2, \ldots, x_p$, has a solution.

Proof. Let $i \in \{1, 2, \ldots, p\}$. If $a_i \neq 0$, write a_i as $a_i = s_i r_i$, where s_i is the largest factor of a_i such that $\gcd(s_i, k) = 1$; if $a_i = 0$, set $s_i = 1$ and $r_i = k$. Let $i, j \in \{1, 2, \ldots, p\}$ with $i \neq j$. Then $\gcd(r_i, r_j) = 1$ (since $\gcd(a_i, a_j)$ is a unit in $\mathbb{Z}_k$). Let $b_1, b_2, \ldots, b_p$ be any integers. By the Chinese Remainder Theorem, the system of congruences

$$x = b_1 \pmod{r_1}$$
$$x = b_2 \pmod{r_2}$$
$$\vdots$$
$$x = b_p \pmod{r_p},$$

has a solution, say $x = g$. Let $i \in \{1, 2, \ldots, p\}$. If $a_i \neq 0$, set $h_i = \frac{s_i b_i - s_i g}{a_i}$ and note that h_i is an integer (since r_i divides $b_i - g$ in $\mathbb{Z}$); if $a_i = 0$, set $h_i = 1$. Suppose $a_i \neq 0$. Then

$$s_i g + a_i h_i = s_i g + a_i \frac{s_i b_i - s_i g}{a_i} = s_i b_i.$$

Since $\gcd(s_i, k) = 1$, s_i has the inverse s_i^{-1} in $\mathbb{Z}_k$, and so $s_i g + a_i h_i = s_i b_i$ implies $g + a_i(s_i^{-1} h_i) = b_i \pmod{k}$. Note that $g + a_i(s_i^{-1} h_i) = b_i \pmod{k}$ is also true if $a_i = 0$. Hence $x = g$, $x_1 = s_1^{-1} h_1$, $x_2 = s_2^{-1} h_2, \ldots, x_p = s_p^{-1} h_p$ is a desired solution. □

Lemma 5.7. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A). *Suppose $\gamma \in C(\alpha) \cap C(\beta)$. Let $\theta_1, \theta_2, \ldots, \theta_p$ be pairwise distinct non-special cycles in β_α, each consisting of k-cycles in α. Then there is an integer $g \geq 0$ such that for every $j \in \{1, \ldots, p\}$, there is an integer $t_j \geq 0$ such that for every $x \in \mathrm{cont}(\theta_j)$, $x\gamma = x(\alpha^g \beta^{t_j})$.*

Proof. Let $j \in \{1, \ldots, p\}$. Let $\theta_j = (\delta_0^{(j)}\, \delta_1^{(j)}, \ldots\, \delta_{m_j-1}^{(j)})$, with $\delta_i^{(j)} = (x_0^{i,j}\, x_1^{i,j} \ldots x_{k-1}^{i,j})$. By Lemma 5.1, $x_0^{0,j}\gamma \in \mathrm{cont}(\theta_j)$. Let $x_0^{0,j}\gamma = x_{s_j}^{w_j,j}$, $x_0^{0,j}\beta^{w_j} = x_{q_j}^{w_j,j}$, $a_j = a(\theta_j)$ (so $x_0^{0,j}\beta^{m_j} = x_{a_j}^{0,j}$), and $b_j = s_j - q_j \pmod{k}$ with $b_j \in \{0, 1, \ldots, k-1\}$. By A(i), for all distinct $j_1, j_2 \in \{1, \ldots, p\}$, $\gcd(a_{j_1}, a_{j_2})$ is a unit in $\mathbb{Z}_k$. Thus, by Lemma 5.6, there is $g \in \{0, 1, \ldots, k-1\}$ such that for every $j \in \{1, \ldots, p\}$, there is $v_j \in \{0, 1, \ldots, k-1\}$ such that $g + a_j v_j = b_j \pmod{k}$. Let $j \in \{1, \ldots, p\}$ and set $t_j = w_j + v_j m_j \geq 0$.

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Then

$$x_0^{0,j}(\alpha^g\beta^{t_j}) = (x_0^{0,j}\beta^{w_j+v_jm_j})\alpha^g = (x_0^{0,j}\beta^{v_jm_j})(\beta^{w_j}\alpha^g) = x_{v_ja_j}^{0,j}(\beta^{w_j}\alpha^g)$$
$$= x_{v_ja_j+q_j+g}^{w_j,j} = x_{b_j+q_j}^{w_j,j} = x_{s_j-q_j+q_j}^{w_j,j} = x_{s_j}^{w_j,j} = x_0^{0,j}\gamma.$$

Hence, by Lemma 5.2, $x\gamma = x(\alpha^g\beta^{t_j})$ for every $x \in \mathrm{cont}(\theta_j)$. □

Lemma 5.8. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A) *and* (B). *Suppose $\gamma \in C(\alpha)\cap C(\beta)$. Let $l \geq 1$ and let $\theta_1, \theta_2, \ldots, \theta_p$ be pairwise distinct non-special cycles in β_α such that for every $j \in \{1, \ldots, p\}$, θ_j consists of k_j-cycles in α and $l(\theta_j) = l$. Then there is an integer $t \geq 0$ such that for every $j \in \{1, \ldots, p\}$, there is an integer $h_j \geq 0$ such that for every $x \in \mathrm{cont}(\theta_j)$, $x\gamma = x(\alpha^{h_j}\beta^t)$.*

Proof. Let $j \in \{1, \ldots, p\}$. Let $\theta_j = (\delta_0^{(j)}\,\delta_1^{(j)}\ldots\delta_{m_j-1}^{(j)})$, with $\delta_i^{(j)} = (x_0^{i,j}\,x_1^{i,j}\ldots x_{k_j-1}^{i,j})$. By Lemma 4.8, α_β contains a cycle $\mu_j = (\sigma_0^{(j)}\,\sigma_1^{(j)}\ldots\sigma_{d_j-1}^{(j)})$ with $\mathrm{cont}(\mu_j) = \mathrm{cont}(\theta_j)$, $\sigma_i^{(j)} = (y_0^{i,j}\,y_1^{i,j}\ldots y_{l-1}^{i,j})$, $y_0^{0,j} = x_0^{0,j}$, and $y_0^{0,j}\alpha^{d_j} = y_{c_j}^{0,j}$, where $c_j = c(\theta_j)$. Since $\mathrm{cont}(\mu_j) = \mathrm{cont}(\theta_j)$, $y_0^{0,j}\gamma = x_0^{0,j}\gamma \in \mathrm{cont}(\mu_j)$ by Lemma 5.1. Let $y_0^{0,j}\gamma = y_{s_j}^{w_j,j}$, $y_0^{0,j}\alpha^{w_j} = y_{q_j}^{w_j,j}$, and $b_j = s_j - q_j \pmod{l}$ with $b_j \in \{0, 1, \ldots, l-1\}$. By (B), for all distinct $j_1, j_2 \in \{1, \ldots, p\}$, $\gcd(c_{j_1}, c_{j_2})$ is a unit in $\mathbb{Z}_l$. Thus, by Lemma 5.6, there is $t \in \{0, 1, \ldots, l-1\}$ such that for every $j \in \{1, \ldots, p\}$, there is $v_j \in \{0, 1, \ldots, l-1\}$ such that $t + c_jv_j = b_j \pmod{l}$. Let $j \in \{1, \ldots, p\}$ and set $h_j = w_j + v_jd_j \geq 0$. Then

$$y_0^{0,j}(\alpha^{h_j}\beta^t) = (y_0^{0,j}\alpha^{w_j+v_jd_j})\beta^t = (y_0^{0,j}\alpha^{v_jd_j})(\alpha^{w_j}\beta^t) = y_{v_jc_j}^{0,j}(\alpha^{w_j}\beta^t)$$
$$= y_{v_jc_j+q_j+t}^{w_j,j} = y_{b_j+q_j}^{w_j,j} = y_{s_j-q_j+q_j}^{w_j,j} = y_{s_j}^{w_j,j} = y_0^{0,j}\gamma.$$

Recall that $y_0^{0,j} = x_0^{0,j} \in \mathrm{cont}(\theta_j)$. Hence, by Lemma 5.2, $x\gamma = x(\alpha^{h_j}\beta^t)$ for every $x \in \mathrm{cont}(\theta_j)$. □

Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies (A)–(C). Suppose $\gamma \in C(\alpha)\cap C(\beta)$. Lemmas 5.1–5.8 will enable us to prove that $\gamma = \gamma_1\gamma_2$ for some $\gamma_1 \in C^2(\alpha)$ and $\gamma_2 \in C^2(\beta)$. To define suitable γ_1 and γ_2, we will need the following preliminary definitions and accompanying lemmas.

Definition 5.9. Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$. For every integer $k \geq 1$, let $\mathcal{D}_k$ be the set of all non-special cycles θ in β_α such that θ consists of k-cycles in α and there exists a non-special cycle $\theta' \neq \theta$ in β_α such that θ' consists of k-cycles in α and $l(\theta') = l(\theta)$.

Lemma 5.10. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)–(C), *and let $\gamma \in C(\alpha)\cap C(\beta)$. Suppose $\mathcal{D}_k \neq \emptyset$. Then $k \geq 3$ and $|\mathcal{D}_k| = 2$. Moreover, if $\mathcal{D}_k = \{\phi_1^{(k)}, \phi_2^{(k)}\}$, then each $\phi_i^{(k)}$ is a 1-cycle in β_α, and there are integers $u_k, v_k \geq 0$ such that $x\gamma = x(\alpha^{u_k}\beta^{v_k})$ for every $x \in \mathrm{cont}(\phi_1^{(k)})\cup\mathrm{cont}(\phi_2^{(k)})$.*

Proof. We have $k \geq 3$ by (A)(ii), and $|\mathcal{D}_k| = 2$ by (C). Suppose $\mathcal{D}_k = \{\phi_1^{(k)}, \phi_2^{(k)}\}$. Then each $\phi_i^{(k)}$ is a 1-cycle in β_α by (A)(ii), and the desired $u_k, v_k \geq 0$ exist by Lemma 5.5. □

Definition 5.11. Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$. For every integer $k \geq 1$, let $\mathcal{A}_k$ be the set of all non-special cycles θ in β_α such that θ consists of k-cycles in α, $\theta \notin \mathcal{D}_k$, and exactly one of the following conditions is satisfied:

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

(a) there exists a non-special cycle $\theta' \neq \theta$ in β_α such that θ' consists of k-cycles in α; or

(b) θ is the only non-special cycle in β_α of length k, and there does not exist a non-special cycle $\theta' \neq \theta$ in β_α such that $l(\theta') = l(\theta)$.

We will write $\mathcal{A}_k$ as $\mathcal{A}_k = \{\theta_1^{(k)}, \theta_2^{(k)}, \ldots, \theta_{m_k}^{(k)}\}$. Note that if (b) holds, then $m_k = 1$.

The following result follows immediately from Lemma 5.7.

Lemma 5.12. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A) *and* (B)*, and let $\gamma \in C(\alpha) \cap C(\beta)$. Suppose $k \geq 1$ is such that $\mathcal{A}_k = \{\theta_1^{(k)}, \theta_2^{(k)}, \ldots, \theta_{m_k}^{(k)}\} \neq \emptyset$. Then there are non-negative integers g_k and $t_1^k, t_2^k, \ldots, t_{m_k}^k$ such that $x\gamma = x(\alpha^{g_k}\beta^{t_i^k})$ for all $i \in \{1, 2, \ldots, m_k\}$ and $x \in \operatorname{cont}(\theta_i^{(k)})$.*

Definition 5.13. Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$. For every integer $l \geq 1$, let $\mathcal{B}_l$ be the set of all non-special cycles μ in β_α such that $l(\mu) = l$ and $\mu \notin \bigcup_{k\geq 1}(\mathcal{D}_k \cup \mathcal{A}_k)$. We will write $\mathcal{B}_l$ as $\mathcal{B}_l = \{\mu_1^{(l)}, \mu_2^{(l)}, \ldots, \mu_{n_l}^{(l)}\}$.

The following result follows immediately from Lemma 5.8.

Lemma 5.14. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A) *and* (B)*, and let $\gamma \in C(\alpha) \cap C(\beta)$. Suppose $l \geq 1$ is such that $\mathcal{B}_l = \{\mu_1^{(l)}, \mu_2^{(l)}, \ldots, \mu_{n_l}^{(l)}\} \neq \emptyset$. Then there are non-negative integers s_l and $h_1^l, h_2^l, \ldots, h_{n_l}^l$ such that $x\gamma = x(\alpha^{h_j^l}\beta^{s_l})$ for all $j \in \{1, 2, \ldots, n_l\}$ and $x \in \operatorname{cont}(\mu_j^{(l)})$.*

Finally, we denote by $\mathcal{E}$ the set of special cycles in β_α (see Definition 4.9 and Lemma 4.10).

Lemma 5.15. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)–(C)*. Then:*

(1) *the sets $\bigcup_{k\geq 1}\mathcal{D}_k$, $\bigcup_{k\geq 1}\mathcal{A}_k$, $\bigcup_{l\geq 1}\mathcal{B}_l$, and $\mathcal{E}$ are pairwise disjoint, and every θ in β_α is in one of these sets;*

(2) *for all $k, l \geq 1$, if $\mathcal{A}_k \neq \emptyset$, then $\mathcal{D}_k = \emptyset$ and $\mathcal{B}_l$ does not contain any elements consisting of k-cycles in α;*

(3) *for all $k, l \geq 1$, if $\mathcal{D}_k \neq \emptyset$, then $\mathcal{B}_l$ does not contain any elements consisting of k-cycles in α;*

(4) *for all $k \geq 1$, $\bigcup_{l\geq 1}\mathcal{B}_l$ contains at most one element consisting of k-cycles in α;*

(5) *for all $l \geq 1$, if θ_1 and θ_2 are distinct non-special cycles in β_α with $l = l(\theta_1) = l(\theta_2)$, then either $\theta_1, \theta_2 \in \mathcal{B}_l$ or $\theta_1, \theta_2 \in \mathcal{D}_l$.*

Proof. The sets are pairwise disjoint by their definitions. Let θ be a non-special cycle in β_α consisting of k-cycles in α with $l = l(\theta)$. If there is a non-special cycle $\theta' \neq \theta$ in β_α such that θ' consists of k-cycles in α and $l(\theta') = l$, then $\theta \in \mathcal{D}_k$. Otherwise, either $\theta \in \mathcal{A}_k$ or $\theta \in \mathcal{B}_l$. We have proved (1).

Let $k, l \geq 1$. If $\mathcal{A}_k \neq \emptyset$, then $\mathcal{D}_k = \emptyset$ by (C), and $\mathcal{B}_l$ does not contain any element consisting of k-cycles in α by Definitions 5.11 and 5.13. If $\mathcal{D}_k \neq \emptyset$, then $\mathcal{B}_l$ does not contain any element consisting of k-cycles in α by (C). We have proved (2) and (3).

Suppose to the contrary that there is $k \geq 1$ such that $\bigcup_{l\geq 1}\mathcal{B}_l$ contains distinct θ and θ' consisting of k-cycles in α. By (3), $\mathcal{D}_k = \emptyset$, so $\theta, \theta' \notin \mathcal{D}_k$. Thus, by the definition of $\mathcal{A}_k$, $\theta \in \mathcal{A}_k$, which contradicts (2). We have proved (4).

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

Let $l \geq 1$ and let θ_1 and θ_2 be distinct non-special cycles in β_α consisting of cycles in α of length k_1 and k_2, respectively, with $l = l(\theta_1) = l(\theta_2)$. If $\theta_1, \theta_2 \in \mathcal{D}_l$, then the conclusion of (5) is true. Suppose $\theta_i \notin \mathcal{D}_l$ for some $i \in \{1, 2\}$. We may assume that $\theta_1 \notin \mathcal{D}_l$. Suppose to the contrary that $\theta_2 \in \mathcal{D}_l$. By Definition 5.9, there exists $\theta_3 \in \mathcal{D}_l$ with $\theta_3 \neq \theta_2$. But then the existence of θ_2, θ_3, and θ_1 contradicts (C). Hence $\theta_2 \notin \mathcal{D}_l$.

We now have $\theta_1, \theta_2 \notin \mathcal{D}_l$. Suppose to the contrary that $\theta_1 \in \mathcal{A}_{k_1}$. By (2), $\mathcal{D}_{k_1} = \emptyset$, so $k_1 \neq k_2$ (since otherwise θ_1 and θ_2 would be in $\mathcal{D}_{k_1}$). Since $l(\theta_2) = l(\theta_1)$, θ_1 does not satisfy (b) of Definition 5.11. Thus, there is $\theta_3 \in \mathcal{A}_{k_1}$ such that $\theta_3 \neq \theta_1$. But then the existence of θ_3, θ_1, and θ_2 contradicts (C). Hence $\theta_1 \in \mathcal{B}_l$. Similarly, $\theta_2 \in \mathcal{B}_l$. We have proved (5). □

We can now define γ_1 and γ_2 (see the paragraph before Definition 5.9).

Definition 5.16. Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies (A)–(C) of Theorem 4.11, and let $\gamma \in C(\alpha) \cap C(\beta)$. To define γ_1 and γ_2, in addition to the integers $u_k, v_k, g_k, t_i^k, s_l, h_j^l$ from Lemmas 5.10, 5.12, and 5.14, we will use two additional integers p and q.

Recall from Definitions 5.11 and 5.13 that we write $\mathcal{A}_k = \{\theta_1^{(k)}, \theta_2^{(k)}, \ldots, \theta_{m_k}^{(k)}\}$ and $\mathcal{B}_l = \{\mu_1^{(l)}, \mu_2^{(l)}, \ldots, \mu_{n_l}^{(l)}\}$. By Lemma 5.15(4), $\bigcup_{l\geq 1} \mathcal{B}_l$ contains at most one element consisting of 2-cycles in α. We will denote this element (if it exists) by $\mu_{j(2)}^{(l(2))}$. By Lemma 5.15(1)(5), $\bigcup_{k\geq 1} \mathcal{A}_k$ contains at most one element θ with $l(\theta) = 2$. We will denote this element (if it exists) by $\theta_{i(2)}^{(k(2))}$.

We now define integers $p, q \geq 0$ by:

$$p = \begin{cases} g_2 & \text{if } \mathcal{A}_2 \neq \emptyset, \\ h_{j(2)}^{l(2)} & \text{if } \bigcup_{l\geq 1} \mathcal{B}_l \text{ contains an element consisting of 2-cycles in } \alpha, \\ 0 & \text{otherwise;} \end{cases}$$

$$q = \begin{cases} s_2 & \text{if } \mathcal{B}_2 \neq \emptyset, \\ t_{i(2)}^{(k(2))} & \text{if } \bigcup_{k\geq 1} \mathcal{A}_k \text{ contains an element } \theta \text{ with } l(\theta) = 2, \\ 0 & \text{otherwise.} \end{cases}$$

The integers p and q are well defined by Lemma 5.15. Define $\gamma_1, \gamma_2 : X \to X$ by:

$$x\gamma_1 = \begin{cases} x\alpha^{u_k} & \text{if } x \in \text{cont}(\phi_1^{(k)}) \cup \text{cont}(\phi_2^{(k)}) \text{ for some } k \geq 3, \\ x\alpha^{g_k} & \text{if } x \in \text{cont}(\theta_i^{(k)}) \text{ for some } k \geq 1 \text{ and } i \in \{1, 2, \ldots, m_k\}, \\ x\alpha^{h_j^l} & \text{if } x \in \text{cont}(\mu_j^{(l)}) \text{ for some } l \geq 1 \text{ and } j \in \{1, 2, \ldots, n_l\}, \\ x\alpha^{p} & \text{if } x \in \text{cont}((y_1\, y_2)) \in \mathcal{E}, \\ x(\gamma\beta^{-q}) & \text{if } x \in \text{cont}(((x_1)\,(x_2))) \in \mathcal{E}, \\ x\gamma & \text{if } x \in \text{cont}(((x_1))) \in \mathcal{E} \text{ and } X_1^\alpha = \{x_1, x_2\}, \\ x & \text{if } x \in \text{cont}(((y_1))) \in \mathcal{E} \text{ and } |X_1^\alpha| \neq 2; \end{cases}$$

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

$$x\gamma_2 = \begin{cases} x\beta^{v_k} & \text{if } x \in \mathrm{cont}(\phi_1^{(k)}) \cup \mathrm{cont}(\phi_2^{(k)}) \text{ for some } k \geq 3, \\ x\beta^{t_i^k} & \text{if } x \in \mathrm{cont}(\theta_i^{(k)}) \text{ for some } k \geq 1 \text{ and } i \in \{1, 2, \dots, m_k\}, \\ x\beta^{s_l} & \text{if } x \in \mathrm{cont}(\mu_j^{(l)}) \text{ for some } l \geq 1 \text{ and } j \in \{1, 2, \dots, n_l\}, \\ x(\alpha^{-p}\gamma) & \text{if } x \in \mathrm{cont}((y_1\, y_2)) \in \mathcal{E}, \\ x\beta^q & \text{if } x \in \mathrm{cont}(((x_1)\,(x_2))) \in \mathcal{E}, \\ x & \text{if } x \in \mathrm{cont}(((x_1))) \in \mathcal{E} \text{ and } X_1^\alpha = \{x_1, x_2\}, \\ x\gamma & \text{if } x \in \mathrm{cont}(((y_1))) \in \mathcal{E} \text{ and } |X_1^\alpha| \neq 2. \end{cases}$$

By Lemmas 5.15 and 5.10, γ_1 and γ_2 are well defined functions from X to X.

Lemma 5.17. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)–(C)*, let $\gamma \in C(\alpha) \cap C(\beta)$. Let γ_1 and γ_2 be the functions from* Definition 5.16*. Then $\gamma = \gamma_1\gamma_2$ and $\gamma_1, \gamma_2 \in S_n$.*

Proof. Let $x \in X$. Suppose $x \in \mathrm{cont}(\theta_i^{(k)})$ for some $k \geq 1$ and $i \in \{1, 2, \dots, m_k\}$. Then $x\alpha^{g_k} \in \mathrm{cont}(\theta_i^{(k)})$, and so $x(\gamma_1\gamma_2) = (x\gamma_1)\gamma_2 = (x\alpha^{g_k})\gamma_2 = (x\alpha^{g_k})\beta^{t_i^k} = x(\alpha^{g_k}\beta^{t_i^k})$. On the other hand, by Lemma 5.12, $x\gamma = x(\alpha^{g_k}\beta^{t_i^k})$. Thus $x\gamma = x(\gamma_1\gamma_2)$. By similar arguments, $x\gamma = x(\gamma_1\gamma_2)$ for $x \in \mathrm{cont}(\phi_1^{(k)}) \cup \mathrm{cont}(\phi_2^{(k)})$ ($k \geq 3$), and for $x \in \mathrm{cont}(\mu_j^{(l)})$ ($l \geq 1$ and $j \in \{1, 2, \dots, n_l\}$). If $x \in \mathrm{cont}((y_1\, y_2)) \in \mathcal{E}$, then $x\gamma = x(\gamma_1\gamma_2)$ by the definitions of γ_1 and γ_2. Suppose $x \in \mathrm{cont}(((x_1)\,(x_2))) \in \mathcal{E}$. Then $X_1^\alpha = \{x_1, x_2\}$ (by Lemma 4.10), and so $x(\gamma\beta^{-q}) \in \mathrm{cont}(((x_1)\,(x_2)))$ since $\beta, \gamma \in C(\alpha)$. Thus $x(\gamma_1\gamma_2) = x(\gamma\beta^{-q}\beta^q) = x\gamma$. Similarly, $x\gamma = x(\gamma_1\gamma_2)$ if $x \in \mathrm{cont}(((x_1))) \in \mathcal{E}$ and $X_1^\alpha = \{x_1, x_2\}$. Finally, if $x \in \mathrm{cont}(((y_1))) \in \mathcal{E}$ and $|X_1^\alpha| \neq 2$, then $x(\gamma_1\gamma_2) = x\gamma_2 = x\gamma$. Hence $\gamma = \gamma_1\gamma_2$.

Since γ is a bijection from X to X and $\gamma = \gamma_1\gamma_2$, γ_1 is injective and γ_2 is surjective. Thus γ_1 and γ_2 are bijections since X is finite. That is, $\gamma_1, \gamma_2 \in S_n$. ☐

The next two lemmas show that $\gamma_1 \in C^2(\alpha)$ (see Lemma 2.4).

Lemma 5.18. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)–(C)*, let $\gamma \in C(\alpha) \cap C(\beta)$. Let γ_1 be the function from* Definition 5.16*. Then for every integer $k \geq 2$, there is an integer $w_k \geq 0$ such that $x\gamma_1 = x\alpha^{w_k}$ for every $x \in X_k^\alpha$.*

Proof. Let $k \geq 2$. We my assume that $X_k^\alpha \neq \emptyset$. Consider four possible cases.

Case 1. $\mathcal{A}_k \neq \emptyset$.

By Lemma 5.15(2), $\mathcal{D}_k = \emptyset$ and $\bigcup_{l\geq 1}\mathcal{B}_l$ does not contain any element that consists of k-cycles in α. Thus $X_k^\alpha = \bigcup_{i=1}^{m_k} \mathrm{cont}(\theta_i^{(k)})$, or $k = 2$ and $X_k^\alpha = \bigcup_{i=1}^{m_k} \mathrm{cont}(\theta_i^{(k)}) \cup \{y_1, y_2\}$, where $((y_1\, y_2)) \in \mathcal{E}$. In either case, by the definition of p, $x\gamma_1 = \alpha^{g_k}$ for every $x \in X_k^\alpha$.

Case 2. $\mathcal{D}_k \neq \emptyset$.

By Lemma 5.15(2)(3), $\mathcal{A}_k = \emptyset$ and $\bigcup_{l\geq 1}\mathcal{B}_l$ does not contain any element that consists of k-cycles in α. By Lemma 5.10, $k \geq 3$. Thus $X_k^\alpha = \mathrm{cont}(\phi_1^{(k)}) \cup \mathrm{cont}(\phi_2^{(k)})$, and so $x\gamma_1 = \alpha^{u_k}$ for every $x \in X_k^\alpha$.

Case 3. $\mathcal{A}_k \cup \mathcal{D}_k = \emptyset$ and $\bigcup_{l\geq 1}\mathcal{B}_l$ contains an element that consists of k-cycles in α.

By Lemma 5.15(4), $\bigcup_{l\geq 1}\mathcal{B}_l$ contains a unique element that consists of k-cycles in α, say $\mu_j^{(l)}$. Thus $X_k^\alpha = \mathrm{cont}(\mu_j^{(l)})$, or $k=2$ and $X_k^\alpha = \mathrm{cont}(\mu_j^{(l)})\cup\{y_1,y_2\}$, where $((y_1\, y_2))\in\mathcal{E}$. Note that if $k=2$, then $\mu_j^{(l)} = \mu_{j(2)}^{(l(2))}$. Thus, in either case, by the definition of p, $x\gamma_1 = \alpha^{h_j^l}$ for every $x\in X_k^\alpha$.

Case 4. $\mathcal{A}_k\cup\mathcal{D}_k=\emptyset$ and $\bigcup_{l\geq 1}\mathcal{B}_l$ does not contain any element that consists of k-cycles in α.

Then $X_k^\alpha=\{y_1,y_2\}$, where $((y_1\, y_2))\in\mathcal{E}$, and so $x\gamma_1 = x\alpha^p = x\alpha^0$ for every $x\in X_k^\alpha$. □

Lemma 5.19. *Let $\alpha,\beta\in S_n$ such that $\alpha\beta=\beta\alpha$ and β satisfies* (A)–(C)*, let $\gamma\in C(\alpha)\cap C(\beta)$. Let γ_1 be the function from* Definition 5.16*. Then:*

(1) *if $|X_1^\alpha|\neq 2$ and $x\in X_1^\alpha$, then $x\gamma_1=x$;*
(2) *if $X_1^\alpha=\{x_1,x_2\}$ with $x_1\neq x_2$, then either $x_i\gamma_1=x_i$ for $i=1,2$, or $x_1\gamma_1=x_2$ and $x_2\gamma_1=x_1$.*

Proof. Suppose $|X_1^\alpha|\neq 2$ and $x\in X_1^\alpha$. By the definition of γ_1, $x\gamma_1=x\alpha^t$, where $t\in\{u_k,g_k,h_j^l,p\}$, or $x\gamma_1=x$. Thus (1) is true since α fixes x. To prove (2), suppose $X_1^\alpha=\{x_1,x_2\}$ with $x_1\neq x_2$. Then, by Lemma 4.10, β_α has a special 2-cycle $((x_1)\,(x_2))$ or two special 1-cycles $((x_1))$ and $((x_2))$. Since $\gamma\in C(\alpha)$, in either case, γ maps $\{x_1,x_2\}$ onto $\{x_1,x_2\}$. The same statement is true for β. Hence, γ_1 maps $\{x_1,x_2\}$ onto $\{x_1,x_2\}$ by Definition 5.16. □

The next two lemmas show that $\gamma_2\in C^2(\beta)$ (see Lemma 2.4).

Lemma 5.20. *Let $\alpha,\beta\in S_n$ such that $\alpha\beta=\beta\alpha$ and β satisfies* (A)–(C)*, let $\gamma\in C(\alpha)\cap C(\beta)$. Let γ_2 be the function from* Definition 5.16*. Then for every integer $l\geq 2$, there is an integer $w_l\geq 0$ such that $x\gamma_2=x\beta^{w_l}$ for every $x\in X_l^\beta$.*

Proof. Let $l\geq 2$. We my assume that $X_l^\beta\neq\emptyset$. By Lemma 4.8, for every $x\in X$, $x\in X_l^\beta$ if and only if $x\in\mathrm{cont}(\theta)$, where θ is a cycle in β_α with $l(\theta)=l$. Consider four possible cases.

Case 1. $\mathcal{B}_l\neq\emptyset$.

Let $x\in X_l^\beta$. Then $x\in\mathrm{cont}(\theta)$ for some θ in β_α consisting of k-cycles in α such that $l(\theta)=l$. By Lemma 5.15(2)(3), $\mathcal{A}_k$ and $\mathcal{D}_k$ are empty. Thus, if θ is not special, then $\theta=\mu_j^{(l)}$ for some j. If θ is special, then, since β moves x, $\theta=((x_1)\,(x_2))\in\mathcal{E}$. It follows that $X_l^\beta=\bigcup_{j=1}^{n_l}\mathrm{cont}(\mu_j^{(l)})$, or $l=2$ and $X_l^\beta=\bigcup_{j=1}^{n_l}\mathrm{cont}(\mu_j^{(l)})\cup\{x_1,x_2\}$, where $((x_1)\,(x_2))\in\mathcal{E}$. In either case, by the definition of q, $x\gamma_2=\beta^{s_l}$ for every $x\in X_l^\beta$.

Case 2. $\mathcal{B}_l=\emptyset$ and $\bigcup_{k\geq 1}\mathcal{A}_k$ contains a cycle θ with $l(\theta)=l$.

By Lemma 5.15(1)(5), θ is a unique element in $\bigcup_{k\geq 1}\mathcal{A}_k$ such that $l(\theta)=l$, say $\theta=\theta_i^{(k)}$, and $\bigcup_{k\geq 1}\mathcal{D}_k$ does not contain any cycle θ' with $l(\theta')=l$. Thus $X_l^\beta=\mathrm{cont}(\theta_i^{(k)})$, or $l=2$ and $X_l^\beta=\mathrm{cont}(\theta_i^{(k)})\cup\{x_1,x_2\}$, where $((x_1)\,(x_2))\in\mathcal{E}$. Note that if $l=2$, then $\theta_i^{(k)}=\theta_{i(2)}^{(k(2))}$. Thus, in either case, by the definition of q, $x\gamma_2=\beta^{t_i^k}$ for every $x\in X_l^\beta$.

Case 3. $\mathcal{B}_l=\emptyset$ and $\bigcup_{k\geq 1}\mathcal{D}_k$ contains a cycle θ with $l(\theta)=l$.

Let k be such that $\theta \in \mathcal{D}_k$. By Definition 5.9 and Lemma 5.10, $k \geq 3$, $\mathcal{D}_k = \{\phi_1^{(k)}, \phi_2^{(k)}\}$, and $l(\phi_1^{(k)}) = l(\phi_2^{(k)}) = l$. By Lemma 5.15(1)(5), $k = l$ and $\bigcup_{k\geq 1} \mathcal{A}_k$ does not contain any cycle θ' with $l(\theta') = l$. It follows that $X_l^\beta = \mathrm{cont}(\phi_1^{(l)}) \cup \mathrm{cont}(\phi_2^{(l)})$, and so $x\gamma_2 = x\beta^{v_l}$ for every $x \in X_l^\beta$.

Case 4. $\mathcal{B}_l = \emptyset$ and $\bigcup_{k\geq 1} \mathcal{D}_k \cup \bigcup_{k\geq 1} \mathcal{A}_k$ does not contain a cycle θ with $l(\theta) = l$.

Then $X_l^\beta = \{x_1, x_2\}$, where $((x_1)\,(x_2)) \in \mathcal{E}$, and so $x\gamma_2 = x\beta^q = \beta^0$ for all $x \in X_l^\beta$. □

Lemma 5.21. *Let $\alpha, \beta \in S_n$ such that $\alpha\beta = \beta\alpha$ and β satisfies* (A)–(C) *of* Theorem 4.11*, and let $\gamma \in C(\alpha) \cap C(\beta)$. Let γ_2 be the transformation from* Definition 5.16*. Then:*

(1) *if $|X_1^\beta| \neq 2$ and $x \in X_1^\beta$, then $x\gamma_2 = x$;*
(2) *if $X_1^\beta = \{y_1, y_2\}$ with $y_1 \neq y_2$, then either $y_i\gamma_2 = y_i$ for $i = 1, 2$, or $y_1\gamma_2 = y_2$ and $y_2\gamma_2 = y_1$.*

Proof. Suppose $|X_1^\beta| \neq 2$ and $x \in X_1^\beta$. By the definition of γ_2, $x\gamma_2 = x\beta^s$, where $s \in \{v_k, t_i^k, s_l, q\}$, or $x\gamma_2 = x$. Thus (1) is true since β fixes x. To prove (2), suppose $X_1^\beta = \{y_1, y_2\}$ with $y_1 \neq y_2$. Then, by Lemma 4.10, β_α has a special 1-cycle $((y_1\,y_2))$ or two special 1-cycles $((y_1))$ and $((y_2))$. In the latter case, $y_1\gamma_2 = y_1$ and $y_2\gamma_2 = y_2$ by Definition 5.16. Suppose β_α has a special 1-cycle $((y_1\,y_2))$. Since $\gamma \in C(\beta)$ and y_1, y_2 are the only fixed points of β, γ maps $\{y_1, y_2\}$ onto $\{y_1, y_2\}$. Since $(y_1\,y_2)$ is a 2-cycle in α, $y_1\alpha = y_2$ and $y_2\alpha = y_1$. Hence $\alpha^{-p}\gamma$ maps $\{y_1, y_2\}$ onto $\{y_1, y_2\}$, and so does γ_2 by Definition 5.16. □

We can now complete the proof of our main theorem.

Proof of **Theorem 4.11**. We will show that $C^2(\alpha)C^2(\beta) = C(\alpha) \cap C(\beta)$. By Proposition 1.2, $C^2(\alpha)C^2(\beta) \subseteq C(\alpha) \cap C(\beta)$. To prove the reversed inclusion, let $\gamma \in C(\alpha) \cap C(\beta)$. By Lemma 5.17, $\gamma = \gamma_1\gamma_2$, where γ_1 and γ_2 are the functions from Definition 5.16. By Lemmas 5.18, 5.19, and Lemma 2.4, $\gamma_1 \in C^2(\alpha)$. By Lemmas 5.20, 5.21, and Lemma 2.4, $\gamma_2 \in C^2(\beta)$. Thus $\gamma \in C^2(\alpha)C^2(\beta)$, and so $C(\alpha) \cap C(\beta) \subseteq C^2(\alpha)C^2(\beta)$. Hence, by (5.1), $C^2(\alpha)C^2(\beta)$ is a maximal abelian subgroup of S_n. □

We conclude the paper with the following problem.

Problem. Let $\alpha, \beta \in S_n$ such that $C^2(\alpha) \neq C(\alpha)$ and $\beta \in C(\alpha) \setminus C^2(\alpha)$. Find sufficient and necessary conditions for $C^2(\alpha)C^2(\beta)$ to be a maximal abelian subgroup of S_n.

References

[1] R. Bercov and L. Moser, On Abelian permutation groups, *Canad. Math. Bull.*, **8** (1965) 627–630.

[2] J. M. Burns and B. Goldsmith, Maximal order abelian subgroups of symmetric groups, *Bull. London Math. Soc.*, **21** (1989) 70–72.

[3] J. D. Dixon, Maximal abelian subgroups of the symmetric groups, *Canad. J. Math.*, **23** (1971) 426–438.

[4] L. A. Kalužnin and M. H. Klin, Certain maximal subgroups of symmetric and alternating groups (Russian), *Mat. Sb. (N.S.)*, **87** (1972) 91–121.

[5] J. Konieczny, Centralizers in the semigroup of injective transformations on an infinite set, *Bull. Aust. Math. Soc.*, **82** (2010) 305–321.

DOI: http://dx.doi.org/10.22108/ijgt.2020.122036.1603

[6] J. Konieczny, Second centralizers in the semigroup of injective transformations, *Asian-Eur. J. Math.*, **3** (2020) 11 pp.

[7] M. W. Liebeck, C. E. Praeger and J. Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra*, **111** (1987) 365–383.

[8] B. Newton and B. Benesh, A classification of certain maximal subgroups of symmetric groups, *J. Algebra*, **304** (2006) 1108–1113.

[9] B. K. Sahoo and B. Sahu, Maximal elementary abelian subgroups of the symmetric group, *J. Appl. Algebra Discrete Struct.*, **4** (2006) 47–56.

[10] M. Suzuki, *Group Theory I*, Springer-Verlag, New York, 1982.

Janusz Konieczny

Department of Mathematics, University of Mary Washington, Fredericksburg, Virginia, USA

Email: jkoniecz@umw.edu