COLLOQUIUM MATHEMATICUM

VOL. 150 2017 NO. 2

ON GENERATION OF THE SYMMETRIC OR THE ALTERNATING GROUP BY TWO CYCLES

BY

CZESŁAW BAGIŃSKI (Białystok) and GRZEGORZ GROMADZKI (Gdańsk)

Abstract. We study the question which pairs of cycles generate the alternating or the symmetric group. We give some sufficient conditions for that, which are also frequently necessary. Furthermore, we also characterize a certain class of involutive automorphisms of such groups. The paper has a combinatorial character but the problems are motivated by geometry.

1. Introduction. It is well known that every finite simple group can be generated by two elements. A particular role in this context is played by symmetric groups due to their universality in the sense of Cayley's classical embedding theorem. In an old paper [15], G. A. Miller determined all possible orders of two cycles generating symmetric or alternating groups. Therefore, in particular, one can probably attribute to Miller the well known fact that the symmetric group S_n and the alternating group A_n on n symbols, say $\{1,\dots,n\}$, can be generated by two cycles. In [12] it is proved that for every nontrivial $\alpha \in \mathrm{S}_n$, $n \neq 4$, there exists $\beta \in \mathrm{S}_n$ such that $\langle \alpha, \beta \rangle = \mathrm{S}_n$. In [11] necessary and sufficient conditions are given for a permutation $\alpha \in \mathrm{S}_k$ to generate S_n or A_n together with $\beta = (1,\dots,n)$, where $n \geq 2k-1$. There are other results concerning 2-generation of S_n or A_n (see for instance [15]), but it seems to the present authors that there is no general result concerning necessary and sufficient conditions for two permutations to generate S_n or A_n, although [8] gives a classification of all isomorphism classes of groups which (viewed as subgroups of S_n) can be generated by two cycles of a prime length p. It follows from this classification that if two such cycles act nontrivially on at least $p+3$ elements then they generate A_n.

In this paper we not only study the pairs of positive integers which can be the orders of two generating cycles for S_n or A_n, but also we give some

2010 *Mathematics Subject Classification*: Primary 20B30; Secondary 20B25, 20B35.
Key words and phrases: symmetric group, alternating group, permutation group, transitive group, cycle, finite group actions on closed surfaces, birational actions on complex algebraic curves (defined over algebraic numbers).
Received 16 September 2016; revised 19 October 2016.
Published online 30 June 2017.

DOI: 10.4064/cm7090-10-2016 © Instytut Matematyczny PAN, 2017

sufficient and, in certain situations also necessary, conditions for given two cycles to generate these groups. Furthermore, for two generators a and b of S_n or A_n we give a necessary and sufficient condition for the map $a \mapsto a^{-1}$, $b \mapsto b^{-1}$ to extend to an automorphism.

We hope that the reader will find these problems of sufficient interest in themselves. However, the main motivation for this study came from low-dimensional algebraic geometry where these problems arise in connection with certain important objects. For example, it is well known that each finite group G can be realized as the group of birational automorphisms of a complex algebraic curve $\mathcal{C}$. Furthermore, due to the seminal theorem of Belyi [3], such a $\mathcal{C}$ can be defined over the algebraic numbers when G can be generated by two elements a, b, and so in the case of alternating and symmetric groups it is natural hope that restriction to pairs of cycles may make the study of such curves more efficient and effective, similarly to our earlier papers [7] and [2]. The point is however that the orders of a, b, even together with the order of their product, only determine the genus of such a curve and not its birational type. There is no shortage of such phenomena (see e.g. [14] or [6]) but the simplest example is two birationally different curves of genus 3 corresponding to the generating pairs (x, x) and (x, x^2) of $\mathbb{Z}_7$ (see e.g. [4]). So we need more information on the generating pair than in Miller's result of existential type, and hence this paper.

Also the second combinatorial thread considered in our paper has remarkable connections with geometry. Namely, it follows from an old theorem of Singerman [16] that a curve as above can be defined over the reals if and only if for the above generators, the map $a \mapsto a^{-1}, b \mapsto b^{-1}$ or $a \mapsto b^{-1}, b \mapsto a^{-1}$ extends to an automorphism of G. But what adds an extra value to these two facts is the recent result of Köck and Singerman [13] which guarantees that such a $\mathcal{C}$ can enjoy these two properties simultaneously, i.e. $\mathcal{C}$ can be defined over the real algebraic numbers, which is a remarkable fact in the modern study of Grothendieck's dessins d'enfants and inverse Galois problem [9]. Finally, the last motivation is provided by [10], where the second author has developed an algebraic method to describe the topological type of all real forms for such curves and which was successfully applied in [2] and [7] for certain particular pairs of generating cycles for the symmetric and alternating groups respectively.

So, from this geometric point of view, our results can be seen as an ample source of algebraic curves $\mathcal{C}$ defined over the real algebraic numbers on which alternating or symmetric groups act as the full groups of birational automorphisms. Their importance is enhanced by the above-mentioned Cayley theorem, which allows the same conclusion for an arbitrary finite group G provided we do not require G to be the *full* group of automorphisms of $\mathcal{C}$.

2. Preliminaries and known results. We use standard notation. Recall only that for a permutation α of a set X, by $\mathrm{supp}(\alpha)$ we mean $\{x \in X : \alpha(x) \neq x\}$. We begin with some well known and easy observations.

LEMMA 2.1. *The alternating group* A_n *is generated by all cycles of length* 3.

LEMMA 2.2. *Let* n *be a positive integer.*

(i) *If* $n > 2$, *then* $\langle (1,2), (1,\dots,n)\rangle = \langle (1,2), (2,\dots,n)\rangle = \mathrm{S}_n$.

(ii) *If* $n > 3$, *then*

$$\langle (1,2,3), (1,\dots,n)\rangle = \langle (1,2,3), (3,\dots,n)\rangle = \begin{cases} \mathrm{A}_n & \text{if } n \text{ is odd,} \\ \mathrm{S}_n & \text{if } n \text{ is even.} \end{cases}$$

(iii) *If* $n > 4$, $n \neq 6$, *then*

$$\langle (1,2)(3,4), (1,\dots,n)\rangle = \begin{cases} \mathrm{A}_n & \text{if } n \text{ is odd,} \\ \mathrm{S}_n & \text{if } n \text{ is even.} \end{cases}$$

LEMMA 2.3. *Let* $1 < k < m$, $\alpha = (1,\dots,k)$, $\beta = (1,\dots,m)$. *Then*

$$\langle \alpha, \beta\rangle = \begin{cases} \mathrm{A}_n & \text{if } km \text{ is odd,} \\ \mathrm{S}_n & \text{if } km \text{ is even.} \end{cases}$$

Proof. In view of Lemma 2.2 we assume $k > 3$. Now set $\gamma = \alpha\beta\alpha^{-1}\beta^{-1} = (1,2,k+1)$. Then $\alpha^{k-2}\gamma\alpha^{-k+2} = (k-1,k,k+1)$ and $\beta^{-k+2}(k-1,k,k+1)\beta^{k-2} = (1,2,3)$. By Lemma 2.2(ii) we get $\mathrm{A}_m \leq \langle \alpha, \beta\rangle$. Therefore, if at least one of k, m is even, then $\langle \alpha, \beta\rangle = \mathrm{S}_m$. ∎

Note that Lemma 2.3 is proved in [12, Theorem B].

3. Main results. Given $1 < k, m < n$ such that $k + m > n$, G. A. Miller [15] has proved the existence of two cycles of orders k and m generating A_n if both k, m are odd, and generating S_n otherwise. However, going a bit deeper into details of Miller's paper, one realizes that he actually proved more than he declared. Namely the following theorem can be deduced from [15]; here we reprove it giving an alternative, direct and elementary proof.

THEOREM 3.1. *Let* k, l, m *be integers such that* $k \geq 3$, $0 < l < k \leq m$, $n = k + m$, *and let*

$$\xi = (1,\dots,k-l+1,\dots,k), \qquad \eta = (k-l+1,\dots,k+m).$$

Then

$$\langle \xi, \eta\rangle = \begin{cases} \mathrm{A}_n & \text{if } k(m+l) \text{ is odd,} \\ \mathrm{S}_n & \text{if } k(m+l) \text{ is even.} \end{cases}$$

Proof. We begin with the case $l = 1$. Let $\xi = (1, \dots, k)$, $\eta = (k, \dots, k+m)$ and $\gamma = \xi\eta\xi^{-1}\eta^{-1}$. Then $\gamma = (1, k+1, k)$ and

$$\begin{aligned}(\xi^3\eta^{-1}\xi^{-2})\gamma(\xi^2\eta\xi^{-3}) &= (\xi^3\eta^{-1}\xi^{-2})(1, k+1, k)(\xi^2\eta\xi^{-3}) \\ &= (\xi^3\eta^{-1})(k-2, k-1, k+1)(\eta\xi^{-3}) \\ &= \xi^3(k-2, k-1, k)\xi^{-3} = (1, 2, 3),\end{aligned}$$

and the conclusion follows from Lemma 2.2(ii).

For $l = 2$ we consider two cases for the smallest value of k. For $k = 3$ set $\xi = (1, 2, 3)$, $\eta = (2, \dots, m+3)$ and $\gamma = \xi\eta\xi^{-1}\eta^{-1}$. Then $\gamma = (1, 4)(2, 3)$, and so $\langle \xi, \gamma \rangle$ is the group of all even permutations of $\{1, 2, 3, 4\}$. It contains an element $(2, 3, 4)$, which together with η generates a subgroup G containing all even permutations of $\{2, \dots, m+3\}$, by Lemma 2.2(ii). Now $\langle G, \xi \rangle$ is the group we need.

If $k = 4$, we set $\xi = (1, 2, 3, 4)$, $\eta = (3, \dots, m+4)$ and $\gamma = \xi\eta\xi^{-1}\eta^{-1}$. Then $\gamma = (1, 5)(3, 4)$, and for $\sigma = \eta^{-2}\xi^{-2}\eta^{-1}\xi^2\eta^2\xi^{-1}$ we obtain $\sigma\gamma\sigma^{-1} = (\sigma(1), \sigma(5))(\sigma(3), \sigma(4)) = (1, 2)(3, 4)$.

Now $T = \langle \gamma, \gamma_1 \rangle$ is a Sylow 2-subgroup of S_4 acting on $\{1, 2, 3, 4\}$. Let $\delta = \xi\gamma_1\xi^{-1}\gamma_1^{-1} = (1, 2, 5, 4, 3)$. Then $\langle T, \delta \rangle$ has at least 40 elements, and so it is equal to S_5 acting on $\{1, 2, 3, 4, 5\}$. Since it contains the cycles $(1, 2)$ and $(1, 2, 3)$ and $(1, 2, 3)\eta = (1, \dots, m+4)$, the conclusion follows from Lemma 2.2(i).

Before we consider the general case, let us analyse one more case: $k = 5$, $l = 3$. Take $\xi = (1, 2, 3, 4, 5)$ and $\eta = (3, \dots, m+5)$. It follows from Example 4.5 below that the subgroups $A = \langle \xi, \eta\xi\eta^{-1} \rangle = \langle (1, 2, 3, 4, 5), (1, 2, 4, 5, 6) \rangle$ and

$$B = \langle \eta\xi\eta^{-1}, \eta^2\xi\eta^{-2} \rangle = \langle (1, 2, 4, 5, 6), (1, 2, 5, 6, 7) \rangle$$

are isomorphic to A_5. Since $(1, 2, 4, 5, 6) \in A \cap B$, we have $|A \cap B| \leq 10$ and the product AB has at least 360 elements, as $360 \geq |A|\,|B|/|A \cap B|$. But this product of subgroups contains an element of order 7, for instance $(1, 2, 3, 4, 5) \cdot (1, 2, 5, 6, 7) = (1, 3, 4, 5, 6, 7, 2)$. Thus $\langle A, B \rangle = \mathrm{A}_7$. Now conjugates of the subgroups A and B by consecutive powers of η generate the whole group A_{m+5}. This ends the proof in this case.

Let us now consider the general case $k > 4$. Suppose first $l = 2$, that is, $\xi = (1, \dots, k)$ and $\eta = (k-1, \dots, k+m)$. We have $\eta^2\xi\eta^2 = (1, \dots, k-2, k+1, k+2)$ and we set

$$\xi_1^{-1} = (k+2, k+1, k-2, \dots, 1)(1, \dots, k) = (k-2, k-1, k, k+2, k+1).$$

By the case $k = 5$, $l = 3$ the elements $\xi_1 = (k+1, k+2, k, k-1, k-2)$ and $\eta_1 = \xi^{-1} = (k, k-1, \dots, 1)$ generate a subgroup containing all even permutations or all permutations of $\{1, \dots, k+2\}$, depending on whether k is odd or even respectively. In particular, it contains the cycles $(1, \dots, k-1)$

if k is even and $(2,\dots,k-1)$ if k is odd. Now, by the case $l=1$ we know that $\langle(1,\dots,k-1),\eta\rangle$ contains A_{n+k} and $\langle(2,\dots,k-1),\eta\rangle$ contains all even permutations of $\{2,\dots,k+m\}$. If we add ξ we obtain either S_n or A_n.

We may assume that $l\geq 3$. Notice that we may also assume $l\leq (k+1)/2$. In fact, if $l>(k+1)/2$, then $k-l+1<k-(k+1)/2+1=(k+1)/2$, and we can replace η by the cycle

$$\eta^{-1}\xi=(k,1,2,\dots,k-l,k+m,k+m-1,\dots,k+1)$$

whose first $k-l+1$ elements are the same as the last consecutive elements of ξ, if we write it in the form

$$\xi=(k-l+1,k-l+2,\dots,k-1,k,1,2,\dots,k-l).$$

In view of this and of the special cases considered, we may assume that $l>1$ and $k-l\geq 3$. So set

$$\begin{aligned}\xi&=(1,\dots,k-l+1,\dots,k),\\ \eta&=(k-l+1,k-l+2,\dots,k+m),\\ \gamma&=\xi\eta\xi^{-1}\eta^{-1}=(1,k+1)(k-l+1,k-l+2).\end{aligned}$$

Notice that $l-1<k-l+1$ as otherwise we would have $l>(k+1)/2$. Finally, it is easy to check that conjugating $(1,k+1)(k-l+1,k-l+2)$ by

$$\sigma=\xi^{-k+l+2}\eta^2\xi^{-1}\eta^{-l-2}\xi^{k-2l+1}\eta^2\xi^{l-2}$$

we get $(1,2)(3,4)$. Hence the conclusion follows from Lemma 2.2(iii). ∎

The following result can be proved by an easy induction.

COROLLARY 3.2. *Let $\alpha_1,\dots,\alpha_k$ $(k>1)$ be cycles of lengths $m_1,\dots,m_k$ respectively such that $\operatorname{supp}(\alpha_i)\cap\operatorname{supp}(\alpha_{i+1})=\{a_{i1},\dots,a_{is_i}\}$ for $i=1,\dots,k-1$, $s_i\geq 1$. Suppose also $\alpha_i(a_{ij})=a_{i,j+1}=\alpha_{i+1}(a_{ij})$ for $i=1,\dots,k-1$ and $j=1,\dots,s_i-1$. Then*

$$\langle\alpha_1,\dots,\alpha_k\rangle\cong\begin{cases}\mathrm{A}_n & \text{if } m_1\cdots m_k \text{ is odd,}\\ \mathrm{S}_n & \text{if } m_1\cdots m_k \text{ is even,}\end{cases}$$

where $n=|\operatorname{supp}(\alpha_1)\cup\cdots\cup\operatorname{supp}(\alpha_k)|$. ∎

In particular we have

COROLLARY 3.3. *Let $\alpha_1,\dots,\alpha_k$ $(k>1)$ be cycles of lengths $m_1,\dots,m_k$ respectively such that $|\operatorname{supp}(\alpha_i)\cap\operatorname{supp}(\alpha_{i+1})|=1$ for $i=1,\dots,k-1$. Then*

$$\langle\alpha_1,\dots,\alpha_k\rangle\cong\begin{cases}\mathrm{A}_n & \text{if } m_1\cdots m_k \text{ is odd,}\\ \mathrm{S}_n & \text{if } m_1\cdots m_k \text{ is even,}\end{cases}$$

where $n=|\operatorname{supp}(\alpha_1)\cup\cdots\cup\operatorname{supp}(\alpha_k)|$. ∎

As a consequence, one can easily derive the main result of [1] (Theorem 3.1).

COROLLARY 3.4. *Let n and k be positive integers with $n \geq k \geq 2$ such that $(n,k) \neq (2,2)$ and $(n,k) \neq (3,3)$. If k is odd (respectively even), then the minimum number of k-cycles needed to generate A_n (respectively S_n) is* $\max\{2, \lceil (n-1)/(k-1) \rceil\}$. ∎

Let ξ be a cycle of length n, let m be an integer dividing n and let $k = n/m$. By a *natural decomposition* of ξ^m we mean $\xi^m = \xi_1 \cdots \xi_m$ where ξ_i, $i = 1, \ldots, m$, are k-cycles with disjoint supports contained in $\mathrm{supp}(\xi)$.

LEMMA 3.5. *Let $n > 1$ be an integer. Let β be a cycle of length n and let $\beta^m = \beta_1 \cdots \beta_m$ be a natural decomposition, where m is an integer dividing n, $n/m = k \geq 3$. Let α be a nontrivial permutation with* $\mathrm{supp}(\alpha) \subset \mathrm{supp}(\beta_1)$.

(i) *If $\langle \alpha, \beta_1 \rangle \cong \mathrm{A}_k$ then $\langle \alpha, \beta \rangle \cong \mathrm{A}_k \wr \mathrm{C}_m$.*
(ii) *If α is odd and $\langle \alpha, \beta_1 \rangle \cong \mathrm{S}_k$ then $\langle \alpha, \beta \rangle \cong \mathrm{S}_k \wr \mathrm{C}_m$.*
(iii) *If α is even and $\langle \alpha, \beta_1 \rangle \cong \mathrm{S}_k$ then $\langle \alpha, \beta \rangle$ contains a subgroup of order $2m(k!/2)^m$ isomorphic to a subgroup of $\mathrm{S}_k \wr \mathrm{C}_m$.*

Proof. Let $\beta = (1, a_{21}, \ldots, a_{m1}, 2, a_{22}, \ldots, a_{m2}, 2, \ldots, k, a_{2k}, \ldots, a_{mk})$. Then

$$\beta^m = (1, \ldots, k)(a_{21}, \ldots, a_{2k}) \cdots (a_{m1}, \ldots, a_{mk})$$

and we may assume that $\beta_1 = (1, \ldots, k)$. It can be seen that the element

$$\gamma = \beta_1^{-1}\beta = (1, a_{21}, \ldots, a_{m1})(2, a_{22}, \ldots, a_{m2}) \cdots (k, a_{2k}, \ldots, a_{mk})$$

is of order m.

Now, the subgroup $\langle \alpha, \beta^m \rangle$ can be epimorphically mapped onto $\langle \alpha, \beta_1 \rangle$, which, by the assumptions, is either symmetric or alternating on $\mathrm{supp}(\beta_1)$. The commutator subgroup of $\langle \alpha, \beta^m \rangle$ is equal to the commutator subgroup of $\langle \alpha, \beta_1 \rangle$. Hence, if $\langle \alpha, \beta_1 \rangle \cong \mathrm{S}_k$ or $k > 5$, the alternating group H acting on $\mathrm{supp}(\beta_1)$ is a subgroup of $\langle \alpha, \beta \rangle$.

(i) If $\langle \alpha, \beta_1 \rangle \cong \mathrm{A}_k$ (in this case k is odd), then $k > 4$ or $k = 3$. In both cases, $\langle \alpha, \beta_1 \rangle = H$ is a subgroup of $\langle \alpha, \beta \rangle = \langle \alpha, \beta_1, \gamma \rangle$ by the previous paragraph. Let $H_i = \gamma^i H \gamma^{-i}$, $i = 0, 1, \ldots, m-1$. Then $\langle H_i : 0 \leq i \leq m-1 \rangle$ is the direct product of the H_i, which is normalized by γ. Hence, by the construction of the wreath product, $\langle \alpha, \beta \rangle = \langle H, \gamma \rangle \cong \mathrm{A}_k \wr \mathrm{C}_m$.

(ii) In this case the commutator subgroup of $\langle \alpha, \beta_1 \rangle$ together with α generate a subgroup isomorphic to S_k. Now the proof is analogous to the previous one.

(iii) The subgroup $K_0 = \langle \alpha, \beta^m \rangle$ is isomorphic to S_k and contains a subgroup H_0 isomorphic to A_k. Its conjugate $K_j = K_0^{\beta^{j-1}}$ for $j = 1, \ldots, m$ acts on $\{a_{j1}, \ldots, a_{jk}\}$ (here $j = a_{1j}$). So, as in the previous case, the subgroup generated by all the H_j is their direct product. It is easily seen that $\langle \beta \rangle$ acts on this direct product by cyclically moving its factors H_j. Moreover, for

all j, β^m normalizes H_j and $\langle H_j, \beta^m\rangle \cong \mathrm{S}_k$. Thus it is clear that $|\langle\alpha,\beta\rangle| = 2m\cdot(k!/2)^m$, and obviously $\langle\alpha,\beta\rangle$ is isomorphic to a subgroup of $\mathrm{S}_k \wr \mathrm{C}_m$. ∎

If α is a cycle of length 2 or 3, we can omit the assumption that $\langle\alpha,\beta_1\rangle$ is isomorphic to A_k or S_k because this follows from other assumptions. In fact, for $\alpha = (i,j)$ with $1 \le i < j \le k$ a suitable power of β_1 with exponent prime to k has the form $(i, j, a_3, \dots, a_k)$. Now it follows from Lemma 2.1(i) that α together with this last k-cycle generate S_k.

Suppose now that α is a 3-cycle. We may assume that $\alpha = (1,2,3)$ and

$$\beta_1 = (1, 2, b_2, \dots, b_s, 3, c_2, \dots, c_t),$$

where $s \le t$ ($s + t + 1 = k$). Now, it is a direct observation that the 3-cycles

$$\alpha,\ \alpha^{\beta_1},\ \alpha^{\beta_1^2},\ \dots,\ \alpha^{\beta_1^{t-1}}$$

have supports covering $\mathrm{supp}(\beta_1)$ and satisfy the assumptions of Corollary 3.2, so they generate A_k.

In [11] a necessary and sufficient condition is given for a permutation $\alpha \in \mathrm{S}_k$ and the cycle $(1,\dots,n)$, $n \ge 2k-1$, to generate A_n or S_n. The following theorem answers the question when two cycles having exactly two or three common elements in their supports generate the symmetric or the alternating group.

THEOREM 3.6. *Let α and β be cycles of lengths m an n respectively with $m, n > 2$. Let $|\mathrm{supp}(\alpha)\cap\mathrm{supp}(\beta)| = l \in \{2,3\}$ and $k = |\mathrm{supp}(\alpha)\cup\mathrm{supp}(\beta)|$. Then $\langle\alpha,\beta\rangle \cong \mathrm{A}_k$ or $\langle\alpha,\beta\rangle \cong \mathrm{S}_k$ if and only if $\mathrm{supp}(\alpha)\cap\mathrm{supp}(\beta)$ is not a common block under the action of α and β.*

Proof. Suppose first that $\mathrm{supp}(\alpha)\cap\mathrm{supp}(\beta)$ is a common block for both α and β. Then $m = lm_1$, $n = ln_1$, $\alpha^{m_1} = \alpha_1\cdots\alpha_{m_1}$ and $\beta^{n_1} = \beta_1\cdots\beta_{n_1}$ are products of independent l-cycles with, say, $\mathrm{supp}(\alpha_1) = \mathrm{supp}(\beta_1)$ and all other l-cycles independent. Let $K = \langle\alpha,\beta\rangle$. The conjugates of H by powers of α and β generate a direct product H of $k = m_1 + n_1 - 1$ copies of K, which is normalized by both α and β. Moreover for $L = \langle\alpha,\beta\rangle\cap H$, the factor group $\langle\alpha,\beta\rangle/L$ can be interpreted as the group of permutations generated by two cycles of length m_1 and n_1 with exactly one common element in their supports, so by Theorem 3.1 it is isomorphic to S_k. It follows from the construction of the wreath product that $\langle\alpha,\beta\rangle$ is isomorphic to a subgroup of $K \wr \mathrm{S}_k$.

Now we assume that $\mathrm{supp}(\alpha)\cap\mathrm{supp}(\beta)$ is not a block under the action of β. We consider the cases $l = 2$ and $l = 3$ separately. So let $l = 2$ and suppose that

$$\begin{aligned}\alpha^{m_1} &= (1,2)(a_{21},a_{22})\cdots(a_{s1},a_{s2}),\\ \beta^{n_1} &= (1,2,b_{13},\dots,b_{1t})(b_{21},\dots,b_{2,t})\cdots(b_{u1},\dots,b_{ut})\end{aligned}$$

with $u \geq 1$, $s \geq 2$ and $t \geq 3$. The subgroup $\langle \alpha^{m_1}, \beta^{n_1} \rangle$ contains a subgroup H_1 which can be epimorphically mapped onto the group of all permutations of $\{1, 2, b_{13}, \ldots, b_{1t}\}$, by Lemma 2.2(i). Its commutator subgroup A_1 is the alternating group on this set, so contains a 3-cycle $\gamma_1 = (1, 2, b_{13})$. Its conjugates $A_1^{\alpha^{i-1}}$, $i = 2, \ldots, s$, contain the 3-cycles $\gamma_i = (a_{i1}, a_{i2}, b_{13})$. Hence, by Corollary 3.2, $\langle \gamma_1, \ldots, \gamma_s \rangle$ is the alternating group A on $\mathrm{supp}(\alpha) \cup \{b_{13}\}$. Take the 3-cycle $(1, 2, a_{21}) \in A$. Conjugating it by suitable powers of β we can produce a sequence of 3-cycles such that any two neighbors have one or two common elements and the union of their supports is $\mathrm{supp}(\beta) \cup \{a_1 2\}$. By Corollary 3.3 they generate a group B which is alternating on this set.

Now, one can easily choose two cycles of odd lengths, one from A and the other from B, satisfying the assumptions of Theorem 3.1, as ξ and η generate the alternating group on $\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)$. This ends the proof of this case.

The general case for $l = 2$, in which

$$\alpha^{m_1} = (1, 2, a_{13}, \ldots, a_{1r})(a_{21}, \ldots, a_{2r}) \cdots (a_{s1}, \ldots, a_{sr}), \quad r, s \geq 2,$$

can proved by repeating the arguments from the above special case.

For $l = 3$ we need first to consider some special situations. Let

$$\alpha = (1, 2, 3, b_4, \ldots, b_m), \quad \beta = (1, 2, c_2, \ldots, c_t, 3, d_2, \ldots, d_u),$$

with $m \geq 4$, and let $\gamma = \alpha\beta\alpha^{-1}\beta^{-1}$. Then $\gamma = (1, 2)(3, 4, d_2, c_2)$, and easy GAP calculations show that

$$\langle \gamma, \alpha\gamma\alpha^{-1} \rangle \cong \begin{cases} \mathrm{A}_6 & \text{if } m = 4, \\ \mathrm{A}_7 & \text{if } m > 4. \end{cases}$$

In both cases we have $(1, 2, 3) \in \langle \alpha, \beta \rangle$, so using arguments as just after the proof of Lemma 3.5, we deduce that $\langle \alpha, \beta \rangle$ is either symmetric or alternating on $\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)$.

Suppose now that

$$\alpha = (1, 2, a_2, \ldots, a_r, 3, b_2, \ldots, b_s), \quad \beta = (1, 2, c_2, \ldots, c_t, 3, d_2, \ldots, d_u).$$

Hence $\gamma = \alpha\beta\alpha^{-1}\beta^{-1} = (1, 2)(3, b_2, d_2)(a_2, c_2)$ and so $(3, b_2, d_2) \in \langle \alpha, \beta \rangle$, which again as in the previous case implies that $\langle \alpha, \beta \rangle$ is either symmetric or alternating on $\mathrm{supp}(\alpha) \cup \mathrm{supp}(\beta)$.

Let us now consider the general case of $l = 3$. For suitable m_1 and n_1 we can write natural decompositions $\alpha^{m_1} = \alpha_1 \cdots \alpha_l$ and $\beta^{n_1} = \beta_1 \cdots \beta_k$ such that α_1 and β_1 are as α and β in the previous two paragraphs. The final part of the proof now repeats the arguments from the proof for $l = 2$. ∎

It is clear that under the assumptions of Theorem 3.6, there is a group isomorphism

$$\langle \alpha, \beta \rangle \cong \begin{cases} \mathrm{A}_k & \text{if } mn \text{ is odd}, \\ \mathrm{S}_k & \text{if } mn \text{ is even}. \end{cases}$$

COROLLARY 3.7. *If cycles α and β satisfy the assumptions of Theorem* 3.6 *and $l \nmid mn$ then $\langle \alpha, \beta \rangle$ is alternating or symmetric on* $\operatorname{supp}(\alpha) \cup \operatorname{supp}(\beta)$. ∎

In particular the conclusion of Theorem 3.6 is true when $m, n > 3$ are primes and

$$1 \leq |\operatorname{supp}(\alpha) \cap \operatorname{supp}(\beta)| \leq 3.$$

It would be interesting to establish when the analogous condition for two cycles with an arbitrary intersection of supports is necessary and sufficient for generation of the symmetric or alternating group. Example 3.10 below shows that an analogous result is not true in general, even in the case when $|\operatorname{supp}(\alpha) \cap \operatorname{supp}(\beta)| = 4$. However, the situation of Example 3.10 is very special. Note that [8] describes all (thirteen) classes of groups which can be generated by two p-cycles when p is a prime.

We finish this section with the following result.

THEOREM 3.8. *Let $A = \{a_1, \ldots, a_k\}$, $B = \{b_1, \ldots, b_m\}$ and $C = \{c_1, \ldots, c_l\}$ be nonempty disjoint sets, and let $X = A \cup B \cup C$. Let also γ be an arbitrary permutation of C. If*

$$\alpha = (a_1, \ldots, a_k, c_1, \ldots, c_l),$$
$$\beta = (\gamma(c_1), \ldots, \gamma(c_l), b_1, \ldots, b_m)$$

are cycles in the group of all permutations of X then $\langle \alpha, \beta \rangle$ is a $t{+}1$-transitive group of permutations of X, where $t = \max\{k, m\}$.

Proof. It is enough to show that for every sequence $(x_1, \ldots, x_{k+1})$ of different elements of $A \cup B \cup C$ there exists $\gamma \in \langle \alpha, \beta \rangle$ such that $\gamma(x_i) = a_i$ $(i = 1, \ldots, k)$ and $\gamma(x_{k+1}) = c_1$.

Let $(x_1, \ldots, x_n)$ be a sequence of different elements of $A \cup B \cup C$, where $n \leq k$. We first show by induction that there exists $\gamma \in \langle \alpha, \beta \rangle$ such that $\gamma(x_i) = a_i$ for $i = 1, \ldots, n$.

For $n = 1$ this is obvious. Suppose that it is true for some $n < k$, and consider a sequence $(x_1, \ldots, x_n, x_{n+1})$ of different elements of $A \cup B \cup C$. By induction there exists $\delta \in \langle \alpha, \beta \rangle$ such that $\delta(x_1) = a_1, \ldots, \delta(x_n) = a_n$. Let $y = \delta(x_{n+1})$. If $y \in B$, then $\beta^s(y) = c_1$ for some s with $0 \leq s \leq l + m$ and we can take $\gamma = \alpha^{-(k-n)} \delta \alpha^{k-n}$. Assume that $y \in A \cup C$ and let i be the smallest nonnegative integer such that $\alpha^i(y) \in C$. It is clear that $\alpha^i(a_1), \ldots, \alpha^i(a_n) \in A$. Let s, t be such that $\beta^s(\alpha^i(y)) = b_1$ and $\beta^t(b_1) = c_1$. Set

$$\gamma = \alpha^{-(k-n)} \beta^t \alpha^{k-n-i} \beta^s \alpha^i \delta.$$

Then $\gamma(x_i) = a_i$ for $i = 1, \ldots, n+1$, proving the induction step.

Now, if $(x_1, \ldots, x_{k+1})$ is a sequence of different elements and γ_1 is such that $\gamma_1(x_i) = a_i$ for $i = 1, \ldots, k$, then $\gamma_1(x_{k+1}) \notin A$. So for some integer s, $\beta^s(\gamma_1(x_{k+1})) = c_1$ and we can set $\gamma = \beta^s \gamma_1$ to finish the proof. ∎

REMARK 3.9. It follows from the classification of finite simple groups that if $n > 4$ or $k > 4$ then the group generated by cycles α and β satisfying the assumptions of Theorem 3.8 is either symmetric or alternating (see for instance [5, Theorem 4.11]).

EXAMPLE 3.10. It is well known that S_5 contains a subgroup of index 6, which means in particular that S_5 has a transitive permutation representation on the set of six elements. For instance, any two cycles from among the following ones have four elements in common and generate the same subgroup isomorphic to S_5 acting transitively on $\{1, 2, 3, 4, 5, 6\}$:

$$(1,2,3,4,5), \quad (1,2,6,3,4), \quad (1,2,5,6,3),$$
$$(1,2,4,5,6), \quad (1,3,4,6,5), \quad (2,5,4,6,3).$$

According to Theorem 3.8 this action is 2-transitive. As is well known, $A_5 \cong \mathrm{PSL}_2(5)$. More generally, for a prime $p > 3$ the group $\mathrm{PSL}_2(p)$ is simple and acts 2-transitively on the projective space consisting of $p + 1$ elements. By Theorem 3.8 any two elements of order p having different fixed points (treated as permutations of the projective space) generate $\mathrm{PSL}_2(p)$.

EXAMPLE 3.11. It is shown in [8] that if p is a Mersenne prime then in S_{p+2} there exist two p-cycles as in Theorem 3.8 with $p - 2$ symbols in common generating $\mathrm{PSL}_2(p + 1)$. In particular, for $p = 7$ we can find two 7-cycles having five symbols in common which do not generate S_9. By Theorem 3.8 the group generated by these cycles is 3-transitive.

These examples also show that Theorem 3.6 cannot be strengthened in a direct way for cycles α, β such that $|\mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta)| > 3$.

4. On involutive automorphisms of A_n and S_n. By the Belyi theorem [3], a group G generated by two elements a, b can be assumed to be a group of birational automorphisms of a complex algebraic curve $\mathcal{C}$ which can be defined over the algebraic numbers. The study of pairs of generating cycles for alternating and symmetric groups was the subject of the previous part of the paper. In turn, the fact that for these generators the correspondence

$$\alpha \mapsto \alpha^{-1}, \quad \beta \mapsto \beta^{-1} \tag{4.1}$$

can be extended to an automorphism of G means, by a theorem of Singerman [16], that $\mathcal{C}$ can be assumed to be defined over the reals. A recent result of Köck and Singerman [13] ensures that the fact that (4.1) extends to an automorphism, which is the subject of our interest for alternating and symmetric groups in this section, implies that $\mathcal{C}$ can enjoy these two properties simultaneously; i.e., G can be assumed to be a group of automorphisms of a complex algebraic curve defined over a real algebraic number field.

Let us consider the question of existence of such an automorphism when α and β are permutations generating A_n or S_n. It is clear that if such an automorphism exists then it is unique and it is conjugation by an involution from S_n because each automorphism of A_n and S_n is conjugation by an element from S_n. Let $A = \mathrm{supp}(\alpha)$, $B = \mathrm{supp}(\beta)$ and $C = A \cap B$, and $|A| = m$, $|B| = n$, $|C| = k$.

LEMMA 4.1. *If $\xi \in S_n$ is an involution such that $\xi\alpha\xi = \alpha^{-1}$ and $\xi\beta\xi = \beta^{-1}$ and $\mathrm{supp}(\xi) \subseteq A \cup B$, then $\xi(C) = C$.*

Proof. Let $x \in C$ and suppose $\xi(x) \notin C$. Then $\xi(x) \in (A-C)\cup(B-C)$. Suppose that $\xi(x) \in A - B$. Hence $\xi(x) \notin B$ and then $\beta(\xi(x)) = \xi(x)$ Therefore $\xi(\beta(\xi(x))) = \xi(\xi(x)) = x$ and by assumption $\beta^{-1}(x) = (\xi\beta\xi)(x) = x$. But $x \in \mathrm{supp}(\beta) = \mathrm{supp}(\beta^{-1})$, a contradiction. ∎

It is well known how to determine all involutions σ such that $\mathrm{supp}(\sigma) \subseteq A$ and $\sigma\alpha\sigma = \alpha^{-1}$ with support contained in A. Their number depends on the decomposition of α into a product of independent cycles. For instance, for $\alpha = (1, \ldots, n)$ we have n such involutions:

$$\sigma_i = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & n \\ i & i-1 & \ldots & 1 & n & \ldots & i+1 \end{pmatrix}, \qquad i = 1, \ldots, n.$$

Let $S = \{\xi \in S_n : \mathrm{supp}(\xi) \subseteq A,\ \xi\alpha\xi = \alpha^{-1},\ \xi(C) = C\}$ and $T = \{\eta \in S_n : \mathrm{supp}(\eta) \subseteq B,\ \eta\beta\eta = \beta^{-1},\ \eta(C) = C\}$. Let also S_1 and T_1 be the sets of involutions of C obtained as restrictions to C of involutions from S and T respectively.

THEOREM 4.2. *For permutations α, β generating A_n or S_n there exists an automorphism ξ obeying* (4.1) *if and only if $|S_1 \cap T_1| = 1$.*

Proof. If an involution σ as above exists then its restriction ξ to A inverts α and its restriction η to B inverts β. It is clear that $\sigma_{|C} = \xi_{|C} = \eta_{|C}$. It is also clear that if for permutations α, β we have $|S_1 \cap T_1| > 1$ then $\langle\alpha, \beta\rangle \neq A_n$ and $\langle\alpha, \beta\rangle \neq S_n$.

Let σ be an involution which is a restriction to C of an involution σ_1 inverting α, with $\mathrm{supp}(\sigma_1) \subseteq A$, and let τ be the restriction of an involution τ_1 inverting β with $\mathrm{supp}(\tau_1) \subseteq B$. If $\sigma = \tau$, then, treating this permutation as an element of S_n with support contained in C, we conclude that $\xi = \sigma_1\sigma\tau_1$ inverts the permutations α and β. ∎

COROLLARY 4.3. *Let α and β be as in Theorem* 3.1. *Then conjugation by the involution*

$$\xi = \begin{pmatrix} 1 & \ldots & k-l & k-l+1 & \ldots & k & k+1 & \ldots & m \\ k-l & \ldots & 1 & k & \ldots & k-l+1 & m & \ldots & k+1 \end{pmatrix}$$

inverts α and β.

The following corollary and example concern the cycles studied in Theorem 3.6.

COROLLARY 4.4. *Let α and β be such that $1 \le |A \cap B| \le 2$. Then there exists $\xi \in \mathrm{S}_n$ satisfying*

$$\xi\alpha\xi = \alpha^{-1}, \quad \xi\beta\xi = \beta^{-1}. \tag{4.2}$$

Proof. The case $|A \cap B| = 1$ is already considered in the previous corollary. Let $\alpha = (1, \dots, m)$ and $\beta = (1, m+1, \dots, m+l, k, m+l+1, \dots, n)$. Then the involution

$$\xi = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & m & m+1 & \cdots \\ k & k-1 & \cdots & 1 & m & \cdots & 1 & m+l & \cdots \end{pmatrix}$$

$$\begin{pmatrix} m+l & m+l+1 & \cdots & n \\ m+1 & n & \cdots & m+l+1 \end{pmatrix}$$

satisfies (4.2). ∎

EXAMPLE 4.5. Let $\alpha = (1,2,3,4,5)$ and $\beta = (1,2,6,3,7)$. Then the only involution ξ such that $\xi\alpha\xi = \alpha^{-1}$ and $\xi(\{1,2,3\}) = \{1,2,3\}$ is $(1,3)(4,5)$. On the other hand, the only involution η such that $\eta\beta\eta = \beta^{-1}$ and $\eta(\{1,2,3\}) = \{1,2,3\}$ is $(1,2)(6,7)$. Hence no involution inverts both cycles. Obviously the elements $\alpha = (1, \dots, k)$, $\beta = (1, 2, k+1, 3, k+2, \dots, k+m)$ with $k \ge 5$ and $m \ge 2$ have similar properties.

COROLLARY 4.6. *Let α and β be as in Theorem* 3.6. *Then there exists an involution inverting α and β if and only if*

$$\begin{pmatrix} c_1 & c_2 & \dots & c_k \\ c_l & c_{l-1} & \dots & c_1 \end{pmatrix} = \begin{pmatrix} \gamma(c_1) & \gamma(c_2) & \dots & \gamma(c_l) \\ \gamma(c_l) & \gamma(c_{k-1}) & \dots & \gamma(c_1) \end{pmatrix}.$$

Proof. If this condition is satisfied then the involution

$$\xi = \begin{pmatrix} a_1 & a_2 & \cdots & a_k & c_1 & c_2 & \dots & c_l & b_1 & b_2 & \cdots & b_m \\ a_k & a_{k-1} & \cdots & a_1 & c_l & c_{l-1} & \dots & c_1 & b_m & b_{m-1} & \cdots & b_1 \end{pmatrix}$$

inverts α and β.

Conversely, if such an involution exists then by Lemma 4.1 it must preserve C. The unique involution with support contained in $\mathrm{supp}(\alpha)$ inverting α and preserving C is equal to

$$\xi = \begin{pmatrix} a_1 & a_2 & \cdots & a_k & c_1 & c_2 & \dots & c_l \\ a_k & a_{k-1} & \cdots & a_1 & c_l & c_{l-1} & \dots & c_1 \end{pmatrix}.$$

Similarly the unique involution with support contained in $\mathrm{supp}(\beta)$ inverting

β and preserving C is equal to

$$\eta = \begin{pmatrix} \gamma(c_1) & \gamma(c_2) & \dots & \gamma(c_l) & b_1 & b_2 & \cdots & b_m \\ \gamma(c_l) & \gamma(c_{l-1}) & \dots & \gamma(c_1) & b_m & b_{m-1} & \cdots & b_1 \end{pmatrix}.$$

Since $\xi_{|C} = \eta_{|C}$, the desired condition follows. ∎

Acknowledgements. The authors are grateful to the referee for bringing the paper of Miller to their attention and for other useful remarks. The authors are also grateful to the editors of Colloquium Mathematicum for their vigilant reading of the preprint and valuable comments and suggestions.

Both authors were supported by the Research Grant of the Polish National Center of Sciences NCN 2012/05/B/ST1/02171.

REFERENCES

[1] S. Annin and J. Maglione, *Economical generating sets for the symmetric and alternating groups consisting of cycles of a fixed length*, J. Algebra Appl. 11 (2012), 1250110, 8 pp.

[2] C. Bagiński, J. J. Etayo, G. Gromadzki and E. Martínez, *Real forms for Belyi actions of alternating groups*, Albanian J. Math. 10 (2016), 3–10.

[3] G. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. 14 (1980), 247–256.

[4] E. Bujalance and M. Conder, *On cyclic groups of automorphisms of Riemann surfaces*, J. London Math. Soc. (2) 59 (1999), 573–584.

[5] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts 45, Cambridge Univ. Press, Cambridge, 1999.

[6] M. Conder and P. Dobcsányi, *Determination of all regular maps of small genus*, J. Combin. Theory Ser. B 81 (2001), 224–242.

[7] J. J. Etayo, G. Gromadzki and E. Martínez, *On real forms of Belyi surfaces with symmetric groups of automorphisms*, Mediterr. J. Math. 9 (2012), 669–675.

[8] K. R. Fawcett and G. L. Walls, *Groups generated by two p-cycles*, Arch. Math. (Basel) 50 (1988), 391–393.

[9] E. Girondo and G. González-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, London Math. Soc. Student Texts 79, Cambridge Univ. Press, Cambridge, 2012.

[10] G. Gromadzki, *On Singerman symmetries of a class of Belyi Riemann surfaces*, J. Pure Appl. Algebra 213 (2009), 1905–1910.

[11] D. Heath, I. M. Isaacs, J. Kiltinen and J. Sklar, *Symmetric and alternating groups generated by a full cycle and another element*, Amer. Math. Monthly 116 (2009), 447–451.

[12] I. M. Isaacs and T. Zieschang, *Generating symmetric groups*, Amer. Math. Monthly 102 (1995), 734–739.

[13] B. Köck and D. Singerman, *Real Belyi theory*, Quart. J. Math. 58 (2007), 463–478.

[14] A. M. Macbeath, *Generators of the linear fractional groups*, in: Number Theory (Houston, TX, 1967), Proc. Sympos. Pure Math. 12, Amer. Math. Soc., Providence, RI, 1969, 14–32.

[15] G. A. Miller, *Possible orders of two generators of the alternating and of the symmetric group*, Trans. Amer. Math. Soc. 30 (1928), 24–32.
[16] D. Singerman, *Symmetries of Riemann surfaces with large automorphism group*, Math. Ann. 210 (1974), 17–32.

Czesław Bagiński
Faculty of Computer Science
Białystok University of Technology
15-351 Białystok, Poland
E-mail: c.baginski@pb.edu.pl

Grzegorz Gromadzki
Institute of Mathematics
University of Gdańsk
80-952 Gdańsk, Poland
E-mail: grom@mat.ug.edu.pl