

Let  $F_n$  be a free group of degree  $n$ ; let  $A_n$  be its automorphism group and let  $Fix(\alpha)$  be the subgroup of the fixed points of the automorphism  $\alpha$ .

In Sec. 1 of this paper we indicate an effective algorithm solving the conjugacy problem for automorphisms of prime order of the group  $A_n$ . In Sec. 2 we indicate an algorithm for the determination of a basis of the subgroup of fixed points of an automorphism for  $A_2$ . With the use of this algorithm, in Sec. 3 we solve the conjugacy problem in the group  $A_2$  (Theorem 3). The formulation of Theorem 3 is contained also in [8].

1. Problem of Conjugacy for Automorphisms of Prime Order

Let  $\alpha$  be an automorphism of a group  $F_n$  of order  $\rho$ , where  $\rho$  is a prime number. In view of [1], the group  $F_n$  can be decomposed into a free product of  $\alpha$ -invariant subgroups:

$$F_n = Fix(\alpha) * (*_{i \in M} X_i) * (*_{j \in K} Y_j), \tag{1}$$

where  $M = \{1, \dots, m\}$ ,  $K = \{1, \dots, k\}$  and

1)  $X_i$ ,  $i \in M$ , has a basis  $x_{i,1}, \dots, x_{i,\rho}$  such that  $\alpha(x_{i,\nu}) = x_{i,\nu+1}$ ,  $1 \leq \nu \leq \rho$  (the second indices are taken modulo  $\rho$ );

2)  $Y_j$ ,  $j \in K$ , has a basis  $y_{j,1}, \dots, y_{j,\rho-1}, z_{j,1}, \dots, z_{j,t_j}$  such that

$$\alpha(y_{j,i}) = y_{j,i+1}, \quad i = 1, \dots, \rho-2;$$

$$\alpha(y_{j,\rho-1}) = (y_{j,1} \dots y_{j,\rho-1})^{-1};$$

$$\alpha(z_{j,\ell}) = y_{j,1}^{-1} z_{j,\ell} y_{j,1}, \quad \ell = 1, \dots, t_j.$$

Assume that the degree of the free group  $Fix(\alpha)$  is equal to  $r$ ;  $t_1 \leq \dots \leq t_k$ .

**THEOREM 1.** The problem of the conjugacy of automorphisms of prime order of a free group of finite degree, defined by the action on a basis, is algorithmically solvable: The conjugacy class is determined by a collection of numbers  $r, m, k, t_1, \dots, t_k$ , which can be found effectively.

**Proof.** We assume that the automorphism  $\alpha$  is defined on a fixed basis  $b_1, \dots, b_n$  of the group  $F_n$ . Assume that to the automorphism  $\alpha$  there corresponds a decomposition of the form (1) with some parameters  $r, m, k, t_1, \dots, t_k$  and let  $d_1, \dots, d_r$  be a basis of the group  $Fix(\alpha)$ , being the union of the above indicated bases of the groups  $X_i$ ,  $i \in M$ ,  $Y_j$ ,  $j \in K$ , and of some

basis of the group  $\text{Fix}(\alpha)$ . For an element  $X$  of some group, we denote by  $\bar{X}$  the image of  $X$  in the quotient with respect to the commutator.

Since  $b_1, \dots, b_n$  and  $d_1, \dots, d_n$  are bases of the group  $F_n$ , we have

$$\{\alpha(w) \cdot w^{-1}; w \in F_n\}^{F_n} = \{\alpha(b_i) b_i^{-1}; i=1, \dots, n\}^{F_n} = \{\alpha(d_i) d_i^{-1}; i=1, \dots, n\}^{F_n}$$

We introduce the notations:

$$H = \text{gr} (b_1, \dots, b_n) / \{\alpha(b_i) b_i^{-1}; i=1, \dots, n\}^{F_n},$$

$$T = \text{gr} (d_1, \dots, d_n) / \{\alpha(d_i) d_i^{-1}; i=1, \dots, n\}^{F_n}.$$

We have

$$H \simeq T \simeq F_{z+m} * (\mathbb{Z}_p \times F_{t_1}) * \dots * (\mathbb{Z}_p \times F_{t_k}). \quad (2)$$

Let  $f_1, \dots, f_{z+m}, e_1, h_1, \dots, h_t, \dots, e_k, h_{t_1+\dots+t_{k-1}+1}, h_{t_1+\dots+t_k}$  be a sequence of elements from  $T$ , consisting of the bases of the corresponding subgroups. Let  $G = H / H_3(H)^\rho$ ,  $S = T / T_3(T)^\rho$ ,  $\Delta = z+m+t_1+\dots+t_k$ . We have  $T/T' = \text{gr}(\bar{e}_1, \dots, \bar{e}_k) \oplus \text{gr}(f_1, \dots, f_{z+m}, h_1, \dots, h_{t_1+\dots+t_k}) \simeq \mathbb{Z}_p^k \oplus \mathbb{Z}^\Delta$ . Therefore, in  $H$  one can find effectively the elements  $a_1, \dots, a_k, a_{k+1}, \dots, a_{k+\Delta}$  such that

$$H/H' \simeq \text{gr}(\bar{a}_1, \dots, \bar{a}_k) \oplus \text{gr}(\bar{a}_{k+1}, \dots, \bar{a}_{k+\Delta}) \simeq \mathbb{Z}_p^k \oplus \mathbb{Z}^\Delta,$$

and, thus, one can find  $k$  and  $\Delta$ . From (1) there follows that  $n = z + \rho m + (\rho-1)k + (t_1 + \dots + t_k) = (\rho-1)(m+k) + \Delta$ . From here  $m = \frac{n-\Delta}{\rho-1} - k$ . From (2) there follows that  $G' \simeq S' \simeq \mathbb{Z}_p^l$  where  $l = \frac{C_{z+m+t_1+\dots+t_k+k} - (t_1+\dots+t_k)}{(\Delta+k)(\Delta+k-1)} - \Delta + (z+m)$ . From here  $z = l + \Delta - m - \frac{2}{(\Delta+k)(\Delta+k-1)}$ .

Taking into account that  $G$  is a finitely generated, finitely presented nilpotent group of level  $\leq 2$ , one can effectively find a basis of the group  $G'$  and the numbers  $l$  and  $z$ . It remains to determine  $t_1, \dots, t_k$ .

We have  $C_S(\bar{e}_1) / S^\rho S' \simeq \mathbb{Z}_p^{t_1+1}, \dots, C_S(\bar{e}_k) / S^\rho S' \simeq \mathbb{Z}_p^{t_k+1}$ . The notation  $C_S(\bar{e}_i)$  makes sense since the centralizers of the elements, differing by an element from  $S'$ , coincide. We note that

$$C_S(\bar{e}_i^{\delta_i} \dots \bar{e}_k^{\delta_k}) / S^\rho S' \simeq \mathbb{Z}_p,$$

if for some  $i, j, t \leq i < j \leq k$ , we have  $\delta_i \neq 0, \delta_j \neq 0$  modulo  $\rho$ . Thus, the basis  $\bar{e}_1, \dots, \bar{e}_k$  of the periodic component of the group  $T/T'$  is distinguished among all the bases (to within a permutation and the raising to powers of the basis elements) by the property that for it the sum

$$|C_S(\bar{e}_1) / S^\rho S'| + \dots + |C_S(\bar{e}_k) / S^\rho S'|$$

is maximal.

Thus, in order to find  $t_1, \dots, t_k$  we have:

1) to fix a basis  $\bar{a}_{k+1}, \dots, \bar{a}_{k+\Delta}$  not the periodic part in some decomposition of the group  $H/H' \simeq \mathbb{Z}_p^k \oplus \mathbb{Z}^\Delta$ ;

2) to enumerate all the bases of the periodic component of the group  $H/H'$ . There are at most  $|GL_k(\mathbb{Z}_p)|$ ;

3) for each such basis  $\bar{a}_1, \dots, \bar{a}_k$  compute  $|C_G(\bar{a}_i)/G^p G'|$ ,  $1 \leq i \leq k$ . This can be done by going through all the elements of the form

$$c_{j_1, \dots, j_{k+\Delta}} = \bar{a}_1^{j_1} \dots \bar{a}_{k+\Delta}^{j_{k+\Delta}}, \quad 0 \leq j_1, \dots, j_{k+\Delta} < p,$$

and verifying the validity of the equalities  $[c_{j_1, \dots, j_{k+\Delta}}, \bar{a}_i] = 1$  in the group  $G$ . The latter is possible in view of the fact that the equality problem in a finitely generated, finitely presented nilpotent group of level  $\leq 2$  is solvable;

4) to find a basis  $\bar{a}_1, \dots, \bar{a}_k$  for which the sum

$$\sum_{i=1}^k |C_G(\bar{a}_i)/G^p G'|$$

is maximal. Performing a permutation, we can assume that  $|C_G(\bar{a}_1)/G^p G'| \leq \dots \leq |C_G(\bar{a}_k)/G^p G'|$ . Then  $t_i = \log_p |C_G(\bar{a}_i)/G^p G'| - 1$ .

## 2. Basis of $Fix(\alpha)$

Let  $F_n$  be a free group with basis  $x_1, \dots, x_n$ ; let  $|x|$  be the length of the element  $x$  in this basis, and let  $A_n = Aut F_n$ . For  $\alpha \in A_n$  we set  $\|\alpha\| = \max |x_i^\alpha|$ ,  $i=1, \dots, n$ . By  $\deg F$  we denote the free group  $F$ .

**LEMMA 1.** Let  $F_n$  be a free group with basis  $x_1, \dots, x_n$ ;  $u_1, \dots, u_m \in F_n$ ;  $\alpha_1, \dots, \alpha_k \in A_n$ ,  $A = \text{gr}(\alpha_1, \dots, \alpha_k)$  and assume that it is known that the degree of the subgroup  $H = \text{gr}(u_1, \dots, u_m)^A$  does not exceed  $\nu$ . Then there exists an algorithm which allows us to find in a finite number of steps a basis of the subgroup  $H$ .

**Proof.** Assume that  $|u_1| \leq \dots \leq |u_m|$ ;  $|\alpha_1| \leq \dots \leq |\alpha_k|$ ;  $M = |u_m|$ ,  $K = \|\alpha_k\|$ ;  $\sigma_1, \dots, \sigma_\nu$  is an  $N$ -reduced basis of the group  $H$  (see [2]),  $t \leq \nu$ ,  $|\sigma_1| \leq \dots \leq |\sigma_t|$ . We have  $|\sigma_1| \leq |u_1| \leq M$ . We prove that

$$|\sigma_t| \leq (2(M+K))^2. \quad (3)$$

We assume the opposite. Then there exists  $\ell$ ,  $1 \leq \ell < t$ , such that

$$|\sigma_{\ell+1}| > 2(M+K)|\sigma_\ell|. \quad (4)$$

We prove that  $\text{gr}(\sigma_1, \dots, \sigma_\ell)$  is an invariant group with respect to  $\alpha_1, \dots, \alpha_k$ . We assume the opposite. Then for some  $\sigma_\rho$  and  $\alpha_j$ ,  $1 \leq \rho \leq \ell$ ,  $1 \leq j \leq k$ , there exists at least one basis element  $\sigma_s$ ,  $s > \ell$ , which occurs in the irreducible notation of the element  $\sigma_\rho \alpha_j$  in the form of the product of the basis elements  $\sigma_1, \dots, \sigma_t$  of the group  $H$ . Let  $\sigma_\rho \alpha_j = \sigma_{i_1}^{\pm 1} \dots \sigma_{i_q}^{\pm 1} \sigma_s^{\pm 1} \dots \sigma^{\pm 1}$  be this notation;  $i_1, \dots, i_q \leq \ell$ ,  $s > \ell$ .

By virtue of the  $N$ -reducibility of the basis  $\sigma_1, \dots, \sigma_t$  and formula (4), we have

$$|\sigma_\rho \alpha_j| \geq \frac{|\sigma_s|}{2} - \frac{|\sigma_{i_q}|}{2} \geq \frac{|\sigma_{\ell+1}| - |\sigma_\ell|}{2} > (M+K - \frac{1}{2})|\sigma_\ell| > K|\sigma_\rho|.$$

We obtain a contradiction with the fact that  $|\mathcal{U}_\rho \alpha_j| \leq \|\alpha_j\| \cdot |\mathcal{U}_\rho| \leq K |\mathcal{U}_\rho|$ .

Thus, the group  $\text{gr}(\mathcal{U}_1, \dots, \mathcal{U}_\rho)$  is  $A$ -admissible. In a similar way one proves that  $\mathcal{U}_1, \dots, \mathcal{U}_m \in \text{gr}(\mathcal{U}_1, \dots, \mathcal{U}_\rho)$ . From here it follows that  $H \leq \text{gr}(\mathcal{U}_1, \dots, \mathcal{U}_\rho) < \text{gr}(\mathcal{U}_1, \dots, \mathcal{U}_\rho) = H$  is a contradiction. Therefore, formula (3) holds.

One can effectively enumerate all the collections of  $t$  elements,  $t \leq \mathcal{U}$ , ordered according to increasing length, for which formula (3) is valid. Let  $H_1, \dots, H_d$  be their corresponding subgroups. We select from them  $A$ -admissible subgroups  $H_{i_1}, \dots, H_{i_c}$  containing the elements  $\mathcal{U}_1, \dots, \mathcal{U}_m$ . This is possible by virtue of the fact that the problem of the occurrence of an element of a free group in a subgroup of finite degree is effectively solvable. We have

$$H = \bigcap_{j=1}^c H_{i_j},$$

and the basis  $H$  is effectively sought in terms of the bases of the groups  $H_{i_1}, \dots, H_{i_c}$  (see [3]).

**LEMMA 2.** Let  $F_n$  be a free group with basis  $X = \{x_1, \dots, x_n\}$ ,  $\alpha \in A_n$ . Then  $\text{deg. Fix}(\alpha) \leq 1 + (2n-1)n\|\alpha\|$ .

The proof follows from [6] with slight modifications in the notations. Let  $G$  be a graph, let  $G^0$  be the set of its vertices, and let  $G^1$  be the set of its edges. For a vertex  $\sigma$ , by  $St(\sigma)$  we denote the set of the edges incident to  $\sigma$ , together with the vertex  $\sigma$ .

In [6] one constructs a graph  $\Gamma$ , whose vertices are the elements of the group  $F_n$ . The vertices  $u$  and  $v$  are joined by an edge with label  $(u, x, v)$  if  $x \in X$ ,  $v = \alpha(x)^{-1}ux$ . Let  $\Gamma_1$  be the connected component of the graph  $\Gamma$ , containing 1. It is easy to see that  $\text{Fix}(\alpha) \simeq \pi(\Gamma_1)$ . Then a finite set  $V$  of vertices of the graph  $\Gamma_1$  is selected and the graph  $\Gamma_2 = \Gamma_1 \setminus (\bigcup_{\sigma \in V} St(\sigma))$  is oriented in such a manner that at most one edge starts from each of its vertices. The set  $V$  consists of all initial segments of the words  $\alpha(x)$ ,  $x \in X$ , lying in  $\Gamma_1^0$ . By  $E$  we denote the set of the edges in the set

$$\bigcup_{\sigma \in V} St(\sigma).$$

Obviously,  $|V| \leq n\|\alpha\|$ ,  $|E| \leq 2n|V|$ . The graph  $\Gamma_2$  is oriented in the following manner. Let  $e \in \Gamma_2^1$  be an edge with label  $(u, x, v)$  and  $u \neq v$ . Then in the product  $\alpha(x)^{-1}u$  at least the letter of the word  $u$  is not cancelled. If this letter is cancelled in the product  $ux$ , then we direct the edge  $e$  from  $u$  to  $v$ ; otherwise, from  $v$  to  $u$ . In the case  $u=v$  we say that  $u$  is the origin and the end of the edge  $e$ .

Let  $G_1, \dots, G_m$  be the connected components of the graph  $\Gamma_2$ . In [6] one proves, with the use of the indicated orientation property, that  $\text{deg. } \pi(G_i) \leq 1$ ,  $1 \leq i \leq m$ . Let  $K_1, \dots, K_m$  be finite subgraphs of the graphs  $G_1, \dots, G_m$  such that  $\pi(K_i) \simeq \pi(G_i)$  and the graph

$$K = \left( \bigcup_{i=1}^m K_i \right) \cup \left( \bigcup_{\sigma \in V} St(\sigma) \right)$$

is connected. Then  $\pi(\Gamma_1) \simeq \pi(K)$  and

$$\begin{aligned} \text{deg. } \mathcal{N}(K) &= |K'| - |K^0| + 1 = \sum_{i=1}^m (|K'_i| - |K_i^0|) + |E| - |V| + 1 = \\ &= \sum_{i=1}^m (\text{deg. } \mathcal{N}(G_i) - 1) + |E| - |V| + 1 \leq |E| - |V| + 1 \leq 1 + (2n-1)n|\alpha|. \end{aligned}$$

Let  $F_2$  be a free group with basis  $x_1, x_2$ . There exists a unique homomorphism from  $A_2$  onto  $GL_2(\mathbb{Z})$  with kernel  $F_2$ . We denote by  $A_2^+$  the subgroup of those automorphisms which are mapped in  $SL_2(\mathbb{Z})$ . For  $\alpha \in A_2$ ,  $G \in A_2$ , we denote by  $\tilde{\alpha}$  and  $\tilde{G}$  the images of  $\alpha$  and  $G$  in  $GL_2(\mathbb{Z})$ .

**THEOREM 2.** There exists an algorithm which allows us to find in a finite number of steps a basis of the subgroup of the fixed points of an automorphism for  $A_2$ . For an automorphism from  $A_2^+$ , the number of steps in this algorithm can be estimated from above.

**Proof.** It is known [4, pp. 341, 351] that  $A_2^+ \simeq B_4 / Z(B_4)$  where  $B_4 \simeq (\sigma_1, \sigma_2, \sigma_3 \mid \sigma_1 \sigma_3 = \sigma_3 \sigma_1, \sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2, \sigma_2 \sigma_3 \sigma_2 = \sigma_3 \sigma_2 \sigma_3)$  is the braid group,  $Z(B_4) = \text{gr}(\sigma_1 \sigma_2 \sigma_3)$  is its center, isomorphic to the infinite cyclic group. The generators  $\sigma_1, \sigma_2, \sigma_3$  can be selected in the following manner:

$$\sigma_1: \begin{cases} x_1 \rightarrow x_1 x_2^{-1} \\ x_2 \rightarrow x_2 \end{cases}, \quad \sigma_2: \begin{cases} x_1 \rightarrow x_1 \\ x_2 \rightarrow x_2 x_1 \end{cases}, \quad \sigma_3: \begin{cases} x_1 \rightarrow x_2^{-1} x_1 \\ x_2 \rightarrow x_2 \end{cases}.$$

Assume first that  $\alpha \in A_2^+$ ;  $C(\alpha)$  is the centralizer of  $\alpha$  in the group  $A_2^+$ . We have  $\text{Fix}(\alpha) = F_2 \cap C(\alpha)$ . We show that

$$C(\alpha) = N(\alpha) / Z(B_4), \quad (5)$$

where  $N(\alpha)$  is the centralizer of some preimage of the element  $\alpha$  in the group  $B_4$ . Let  $C \in C(\alpha)$ ,  $C$  and  $\alpha$  being written in the generators  $\sigma_1, \sigma_2, \sigma_3$ . Then in the group  $B_4$  we have  $C^{-1} \alpha C = \alpha z$  for some  $z \in Z(B_4)$ . Mapping the generators  $\sigma_1, \sigma_2, \sigma_3$  of the group  $B_4$  onto the generator  $Q$  of the infinite cyclic group  $\text{gr}(Q)$  and extending this mapping to a homomorphism from  $B_4$  onto  $\text{gr}(Q)$ , we can see that  $z = 1$  and formula (5) holds.

Makanin's algorithm [5] allows us to find effectively a finite set of elements, generating  $N(\alpha)$  and, therefore, also  $C(\alpha)$ . Let  $C(\alpha) = \text{gr}(C_1, \dots, C_k)$ .

Since  $SL_2(\mathbb{Z}) \simeq \mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$  is an almost free group, one can effectively obtain the representation of each of its finitely generated subgroups, including also that of the group  $\widetilde{C(\alpha)}$ , with a given generating set. Indeed, assume that the cyclic groups  $\mathbb{Z}_4$  and  $\mathbb{Z}_6$  are generated by the elements  $a$  and  $b$ , respectively. There exists a homomorphism from the group  $\mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$  into the group  $\mathbb{Z}_{12}$ , under which the factors  $\mathbb{Z}_4$  and  $\mathbb{Z}_6$  are imbedded in the group  $\mathbb{Z}_{12}$ . In view of the description of the subgroups of a free product with the union, the kernel  $H$  of this homomorphism is a free group. It is easy to see that the elements  $g_1 = [a, b]$  and  $g_2 = [a, b^2]$  form a basis of the group  $H$ . The group  $\widetilde{C(\alpha)}$  is a finite cyclic extension of the free group  $\widetilde{C(\alpha)} \cap H$  and in order to find its representation with the generating set  $\{\tilde{c}_1, \dots, \tilde{c}_k\}$  it is necessary to find a basis of the group  $\widetilde{C(\alpha)} \cap H$  in the form of words of  $\tilde{c}_1, \dots, \tilde{c}_k$ . Making use of Schreier's method, first we find the generating elements of the group  $\widetilde{C(\alpha)} \cap H$

in the form of words of  $\tilde{c}_1, \dots, \tilde{c}_k$ . Then we express these words in terms of  $g_1, g_2$  and we apply Nielsen transformations in order to find a basis of the group  $\widetilde{C(\alpha)} \cap H$  in the form of words of  $g_1, g_2$ . Knowing the used Nielsen transformations, one can find this basis in the form of words of  $\tilde{c}_1, \dots, \tilde{c}_k$ .

Let  $\widetilde{C(\alpha)} = (\tilde{c}_1, \dots, \tilde{c}_k \mid \omega_1(\tilde{c}_1, \dots, \tilde{c}_k) = 1, \dots, \omega_m(\tilde{c}_1, \dots, \tilde{c}_k) = 1)$ , where  $\omega_1, \dots, \omega_m$  are some words, in which the letters  $\tilde{c}_1, \dots, \tilde{c}_k$  have been substituted;  $N$  is the normal closure in  $C(\alpha)$  of the set  $\{\omega_1(c_1, \dots, c_k), \dots, \omega_m(c_1, \dots, c_k)\} \subseteq F_2$ . Then  $Fix(\alpha) = C(\alpha) \cap F_2 = N$ . In view of Lemmas 1 and 2, we can find effectively a basis of the group  $Fix(\alpha)$ .

Assume now that  $\alpha \in A_2$ . Then  $\alpha^2 \in A_2^+$  and one can find a basis of  $Fix(\alpha^2)$ . If  $\alpha$  acts as the identity on  $Fix(\alpha^2)$  then  $Fix(\alpha) = Fix(\alpha^2)$ . Otherwise,  $\alpha$  is an automorphism of the second order on the group  $Fix(\alpha^2)$  and there exists for it a suitable basis of the group  $Fix(\alpha^2)$  whose initial piece is a basis of the group  $Fix(\alpha)$  (see Sec. 1). Knowing one basis of the group  $Fix(\alpha^2)$  one can enumerate all the bases. At some step we encounter a suitable basis for  $\alpha$  and we find a basis of the group  $Fix(\alpha)$ .

### 3. Conjugacy Problem in $A_2$

**THEOREM 3.** The conjugacy problem in the group  $A_2$  is solvable.

**Proof.** First we prove that the conjugacy problem (CP) in the group  $A_2$  is solvable for the elements from  $A_2^+$ . It is sufficient to prove the solvability of the CP for the elements from  $A_2^+$  in the group  $A_2^+$  itself. Let  $\beta, \gamma \in A_2^+$ . We fix the notation of  $\beta$  and  $\gamma$  in the generators  $\sigma_1, \sigma_2, \sigma_3$  (see Sec. 2). The elements  $\beta$  and  $\gamma$  are conjugate in  $A_2^+ \simeq B_4 / Z(B_4)$  if and only if there exists  $\delta \in B_4$  such that  $\delta^{-1}\beta\delta = \gamma z$  in the group  $B_4$  for some  $z \in Z(B_4)$ . The element  $z$  is defined uniquely by  $\beta$  and  $\gamma$  from the condition of the equality of the sums of the exponents of the elements  $\beta$  and  $\gamma z$ . Therefore, the CP for the elements  $\beta$  and  $\gamma$  in  $A_2^+$  reduces to the CP for the elements  $\beta$  and  $\gamma z$  in  $B_4$ . The CP in  $B_4$  is solvable [7].

Let  $\beta, \gamma \in A_2$ . A necessary condition for the conjugacy of the elements  $\gamma$  and  $\beta$  in the group  $A_2$  is the conjugacy of the elements  $\tilde{\gamma}$  and  $\tilde{\beta}$  in  $GL_2(\mathbb{Z})$ . Let  $\tilde{\gamma}^{-1}\tilde{\gamma}\tilde{\delta} = \tilde{\beta}$  for some  $\delta \in A_2$ . We find  $y \in F_2$  such that  $\delta^{-1}\gamma\delta = \beta y$ .

From here it follows that the CP for  $\gamma$  and  $\beta$  is equivalent to the CP for  $\beta y$  and  $\beta$ . We assume that  $\beta y$  and  $\beta$  are conjugate:  $c^{-1}\beta c = \beta y$  for some  $c \in A_2$ . Then  $\tilde{c} \in C(\tilde{\beta})$ . We describe the centralizer  $C(\tilde{\beta})$ , assuming that  $\tilde{\beta} \neq \pm E$  (the case when  $\beta \in A_2^+$  has been considered above). One can find an element  $\tilde{\beta}_1 \in GL_2(\mathbb{Z})$  and a number  $\kappa$  such that  $\tilde{\beta} = \tilde{\beta}_1^\kappa$  or  $\tilde{\beta} = -\tilde{\beta}_1^\kappa$  and  $\kappa$  is maximal. Making use of the decomposition  $GL_2(\mathbb{Z}) \simeq D_4 *_{D_2} D_6$  if  $\tilde{\beta}$  is an element of

infinite order and of matrix computations if  $\tilde{\beta}$  is an element of finite order, we can prove that  $C(\tilde{\beta}) = \langle \pm \tilde{\beta}_1^j \rangle$ . Let  $\tilde{c} = \pm \tilde{\beta}_1^j$ ,  $j = q\kappa + r$ ,  $0 \leq r < \kappa$ . Replacing  $c$  by  $\beta^{-r}c$ , we can assume that  $\tilde{c} = \pm \tilde{\beta}_1^r$ . Let  $x_1, x_2$  be a basis of  $F_2$ ,  $\sigma \in A_2$ ,  $\sigma(x_1) = x_1^{-1}$ ,  $\sigma(x_2) = x_2^{-1}$ . Then  $c = \sigma^\varepsilon \beta_1^r f$  for some  $f \in F_2$ ,  $0 \leq r < \kappa$ ,  $\varepsilon \in \{0, 1\}$ . Thus,  $\beta$  and  $\beta y$  are conjugate if and only if, for some  $r$  and  $\varepsilon$ ,  $0 \leq r < \kappa$ ,  $\varepsilon \in \{0, 1\}$ , the elements  $\beta_1^r \sigma^{-\varepsilon} \beta \sigma^\varepsilon \beta_1^r$  and  $\beta y$  are conjugate to an element of  $F_2$ . By virtue of the fact that  $(\beta_1^{-r} \sigma^{-\varepsilon} \beta \sigma^\varepsilon \beta_1^r)(\beta y)^{-1} \in F_2$  it is sufficient to answer the follow-

ing question. For given  $\alpha \in A_2$ ,  $x \in F_2$  is there an  $f \in F_2$  such that  $f^{-1}\alpha f = \alpha x$ ? A necessary condition for the existence of  $f$  is the existence of  $f \in F_2$  with the property

$$f^{-1}\alpha^2 f = (\alpha x)^2. \quad (6)$$

The elements  $\alpha^2$  and  $(\alpha x)^2$  belong to  $A_2^+$  and for them the CP is solvable in the group  $A_2^+$ . We find an element  $g_0 \in A_2^+$  (if it exists) such that  $g_0^{-1}\alpha^2 g_0 = (\alpha x)^2$ . The element  $g_0$  need not belong to  $F_2$ . The set of all the solutions of the equation  $g^{-1}\alpha^2 g = (\alpha x)^2$ ,  $g \in A_2^+$  coincides with the right coset  $C(\alpha^2)g_0$  where  $C(\alpha^2)$  is the centralizer of  $\alpha^2$  in the group  $A_2^+$ . Therefore, the solution of Eq. (6) in the group  $F_2$  exists if and only if  $\tilde{g}_0^{-1} \in \widetilde{C(\alpha^2)}$ . The group  $\widetilde{C(\alpha^2)}$  is a finitely generated subgroup (see Sec. 2) of the almost free group  $SL_2(\mathbb{Z}) \simeq \mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$ . Therefore, the problem of the occurrence in the group  $\widetilde{C(\alpha^2)}$  is solvable.

We assume that  $\tilde{g}_0^{-1} \in \widetilde{C(\alpha^2)}$  i.e.,  $\tilde{g}_0^{-1} = \tilde{c}$  for some  $c \in C(\alpha^2)$ . Setting  $f_0 = c g_0$  we find that  $f_0$  is a solution of Eq. (6), lying in  $F_2$ .

Thus, assume that there exists a solution  $f_0$  of Eq. (6), lying in  $F_2$ . The remaining solutions of Eq. (6), lying in  $F_2$ , have the form  $h f_0$ , where  $h \in \text{Fix}(\alpha^2)$ . Therefore, all the solutions (if they exist) of the equation  $f^{-1}\alpha f = \alpha x$ ,  $f \in F_2$  have the form  $h f_0$  for some  $h \in \text{Fix}(\alpha^2)$ .

Thus, the CP reduces to the question of the existence of an element  $h \in \text{Fix}(\alpha^2)$  such that  $f_0^{-1} h^{-1} \alpha h f_0 = \alpha x$ . We set  $z = f_0 x^{-1} \alpha^{-1} f_0^{-1} \alpha$ . Then one has to answer the following question: Is there an element  $h \in \text{Fix}(\alpha^2)$  such that  $h^\alpha = h z$ ?

If  $z \notin \text{Fix}(\alpha^2)$  then solutions do not exist. Let  $z \in \text{Fix}(\alpha^2)$ . We find a basis of the group  $\text{Fix}(\alpha^2)$  (see Sec. 2). If  $\alpha$  is the identity automorphism on  $\text{Fix}(\alpha^2)$  then a solution exists only in the case  $z=1$  (then one can take, for example,  $h=1$ ). If  $\alpha$  is an automorphism of the second order on  $\text{Fix}(\alpha^2)$  then we find a basis of the group  $\text{Fix}(\alpha^2)$  suitable for  $\alpha$ . For each element  $x$  from  $\text{Fix}(\alpha^2)$  by  $|x|$  we denote its length in this basis. Let  $L = \{h \mid h^\alpha = h z, h \in \text{Fix}(\alpha^2)\}$ .

We prove that if  $L \neq \emptyset$  then there exists  $h \in L$  such that  $|h| \leq |z|$ . We assume the opposite:  $L \neq \emptyset$ ,  $h$  is a solution of minimal length, and  $|h| \geq |z| + 1$ . Then the irreducible notation of the element  $h$  cannot start with a basis element of the group  $\text{Fix}(\alpha)$ . Since in the products  $h z$  at least the first letter of the word  $h$  does not cancel, it follows that  $h$  cannot start with other basis elements. Contradiction.

Thus, it is sufficient to verify only those  $h$  whose lengths do not exceed the length of the word  $z$  in a suitable basis.

#### LITERATURE CITED

1. J. L. Dyer and J. P. Scott, "Periodic automorphisms of free groups," *Commun. Algebra*, 3, No. 3, 195-201 (1975).
2. R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer, Berlin (1977).
3. J. R. Stallings, "Topology of finite graphs," *Invent. Math.*, 71, No. 3, 551-565 (1983).
4. A. Karrass, A. Pietrowski, and D. Solitar, "Some remarks on braid groups," in: *Contributions to Group Theory, Contemp. Math.*, Vol. 33, Am. Math. Soc., Providence, R.I. (1984), pp. 341-352.

5. G. S. Makanin, "On the normalizers of the braid group," Mat. Sb., 86 (128), No. 2, 171-179 (1971).
6. R. Z. Goldstein and E. C. Turner, "Fixed subgroups of homomorphisms of free groups," Bull. London Math. Soc., 18, No. 5, 468-470 (1986).
7. G. S. Makanin, "Separable closed braids," Mat. Sb., 132 (1974), No. 4, 531-540 (1987).
8. G. T. Kozlov, "The structure of the group  $\text{Aut } F_2$  and the conjugacy problem," in: 8th All-Union Conference on Mathematical Logic (Moscow, September 16-18, 1986) [in Russian], Mosk. Gos. Pedagog. Inst., Moscow (1986), p. 85.