THE AUTOMORPHISM GROUP OF THE FREE GROUP WITH TWO GENERATORS

Bomshik Chang

Let F be the free group generated by a and b, and let F' denote the derived group [F, F] of F. The main purpose of this note is to prove

THEOREM 1. *An automorphism* G *of* F *is an inner automorphism if* $G(a) \equiv a$, $G(b) \equiv b \pmod{F'}$.

As an immediate consequence of Theorem 1, we have

THEOREM 2. *Let* A *and* I *be the automorphism group and the inner automorphism group of* F, *respectively. Then the group* A/I *is isomorphic to the group of two-by-two matrices with integer coefficients and with determinants* ± 1.

Proof of Theorem 1. It is known [2], [3] that A is generated by the three automorphisms

$$P: a \to b,\ b \to a, \qquad Q: a \to a^{-1},\ b \to b, \qquad U: a \to ab,\ b \to b.$$

Let V be the automorphism $V: a \to a,\ b \to ba$; then we have

$$PU = VP, \qquad PU^{-1} = V^{-1}P, \tag{1}$$

$$QU \equiv U^{-1}Q \pmod{I}. \tag{2}$$

(The symbol $G_1 G_2$ denotes the automorphism G_1 followed by G_2. Thus

$$G_1 G_2: a \to G_2(G_1(a)),\ b \to G_2(G_1(b)).)$$

Using the above relations, we may write an automorphism

$$G = P^{\delta_1} Q^{\varepsilon_1} U^{\lambda_1} \cdots P^{\delta_k} Q^{\varepsilon_k} U^{\lambda_k},$$

where $\delta_1, \varepsilon_1, \cdots, \delta_k, \varepsilon_k$ are 0 or 1 and $\lambda_1, \cdots, \lambda_k$ are integers, as

$$G \equiv U^{\mu_1} V^{\nu_1} \cdots U^{\mu_j} V^{\nu_j} W \pmod{I},$$

where $\mu_1, \nu_1, \cdots, \mu_j, \nu_j$ are integers and W is a word in P and Q.

Let

$$R: a \to a^{-1},\ b \to b^{-1}, \qquad S: a \to b,\ b \to a^{-1}, \qquad T: a \to b^{-1},\ b \to ba.$$

We have

$$S^2 = R, \tag{3}$$

Received November 25, 1959.

This research was done while the author was a fellow of the Summer Research Institute of the Canadian Mathematical Congress during the summer of 1959.

(4) $$T^3 \equiv R \pmod{I},$$

(5) $$U \equiv ST \pmod{I},$$

(6) $$V \equiv ST^2 \pmod{I},$$

(7) $$PQ = S,$$

(8) $$R^2 = \text{the identity of } A,$$

and, for any $H \in A$,

(9) $$RH \equiv HR \pmod{I}.$$

Using (5) and (6), we may write the word $U^{\mu_1}V^{\nu_1} \cdots U^{\mu_j}V^{\nu_j}$ in U and V as a word in S and T (mod I), and applying (3), (4), (8) and (9), we have

$$G \equiv S^{\alpha_1} T^{\beta_1} ST^{\beta_2} \cdots ST^{\beta_i} S^{\alpha_2} R^{\gamma_1} W \pmod{I},$$

where $\alpha_1, \alpha_2, \gamma_1$ are 0 or 1 and $\beta_1, \beta_2, \cdots, \beta_i$ are 1 or 2. Using (7), we can reduce the word W in P and Q to the form $S^{\alpha_3} R^{\gamma_2} P^{\delta} Q^{\varepsilon}$, where $\alpha_3, \gamma_2, \delta, \varepsilon$ are 0 or 1 and $(\delta, \varepsilon) \neq (1, 1)$. Finally, we obtain,

$$G \equiv S^{\alpha_1} T^{\beta_1} ST^{\beta_2} \cdots ST^{\beta_i} S^{\alpha_4} R^{\gamma} P^{\delta} Q^{\varepsilon} \pmod{I}.$$

We consider the automorphism of F/F' induced by G. Note that if G_1, G_2 are automorphisms of F such that

$$G_1\colon a \to a^{i_1} b^{j_1} c_1, \quad b \to a^{h_1} b^{k_1} d_1,$$

$$G_2\colon a \to a^{i_2} b^{j_2} c_2, \quad b \to a^{h_2} b^{k_2} d_2,$$

where $c_1, d_1, c_2, d_2 \in F'$, then

$$G_1 G_2\colon a \to a^{i_3} b^{j_3} c_3, \quad b \to a^{h_3} b^{k_3} d_3,$$

where $c_3, d_3 \in F'$, and $\begin{pmatrix} i_3 & j_3 \\ h_3 & k_3 \end{pmatrix} = \begin{pmatrix} i_1 & j_1 \\ h_1 & k_1 \end{pmatrix} \begin{pmatrix} i_2 & j_2 \\ h_2 & k_2 \end{pmatrix}$.

Suppose G is an automorphism of F such that $G\colon a \to ac$, $b \to bd$, with $c, d \in F'$, that is, the automorphism of F/F' induced by G is the identity automorphism; then

$$s^{\alpha_1} t^{\beta_1} st^{\beta_2} \cdots st^{\beta_i} s^{\alpha_4} r^{\gamma} p^{\delta} q^{\varepsilon} = e,$$

where

$$s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad r = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad p = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad q = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

By comparing the determinants of both sides, we have $\delta = \varepsilon = 0$. We recall a well-known theorem [1, p. 261]: the unimodular group is the free product of the cyclic group $\{s\}$ of order 2 and the cyclic group $\{t\}$ of order 3. This theorem shows that $s^{\alpha_1} t^{\beta_1} st^{\beta_2} \cdots st^{\beta_i} s^{\alpha_4}$ cannot be r or e unless it is a trivial word, that is, unless $i = 0$ and $\alpha_1 + \alpha_4$ is 0 or 2. If $\alpha_1 + \alpha_4 = 0$, then $\gamma = 0$; and if $\alpha_1 + \alpha_4 = 2$, then $\gamma = 1$.

Thus we have shown that

$$G \equiv \text{identity} \pmod{I},$$

or G is an inner automorphism.

REFERENCES

1. A. G. Kurosh, *The theory of groups*, Vol. II (English translation by K. A. Hirsch, Chelsea, New York, 1955).

2. B. Neuman, *Die Automorphismengruppe der freien Gruppen*, Math. Ann. 107 (1933), 367-386.

3. J. Nielsen, *Die Isomorphismengruppe der freien Gruppen*, Math. Ann. 91 (1924), 169-209.

The University of British Columbia