ON FAITHFUL REPRESENTATIONS OF FREE GROUPS

By Tsuyoshi HAYASHIDA.

That the fundamental group of a Riemannian surface has no relation other than

$$(1) \qquad A_1 B_1 A_1^{-1} B_1^{-1} \cdots A_s B_s A_s^{-1} B_s^{-1} = E$$

is recognized from the algebraic function theory. But in general it is hard to see whether or not certain given matrices considered as a multiplicative group have any relation such as (1). And when we represent a group by matrices, above all in the case of free groups, we must be careful about the existence of the intrinsic matrices-relations (for non-singular matrices) like

$$(2) \qquad \underbrace{A^{\alpha_1} B^{\beta_1} \cdots A^{\alpha_i} \cdots L^{\lambda_j} \cdots}_{\text{finite}} = E$$

In fact in the case of characteristic p, there are such identities as (2). I shall prove that there are no such identities in the case of characteristic 0 or infinite field, or if "length" is short in the case of finite field. I shall show in a similar manner that a free group which is generated by countable elements, is contained in the unimodular group of order two whose components are integers.

Theorem. Let $A, B, \cdots, L$ be matrix-variables of order n and let their components run through the field k having infinitely many elements. Then there is no system of a finite number of non-zero integers $\alpha_1, \beta_1, \cdots, \alpha_i, \cdots, \lambda_j \cdots$, such that $A^{\alpha_1} B^{\beta_1} \cdots A^{\alpha_i} \cdots L^{\lambda_j} \cdots = E$ is an identity for non-singular matrices.

Proof. When a system of integers $(\alpha_1, \beta_1, \cdots, \alpha_i, \cdots, \lambda_j, \cdots)$ is given, we can find matrices $A_0, B_0, \cdots, L_0$, whose components are elements of k and $A_0^{\alpha_1} B_0^{\beta_1} \cdots A_0^{\alpha_i} \cdots L_0^{\lambda_j} \cdots \neq E$. It is sufficient to show this in the case $n=2$, for if $n>2$ we can choose $a_{ii}=1$ $(i>2)$, $a_{ij}=0$ $(i$ or $j>2)$ *etc*. Put $A=B^x C^y$ and let $x \neq 0$, $y \neq 0$, $x+\beta_i \neq 0$, $y+\gamma_j \neq 0$. Then, if A is substituted by $B^x C^y$ we find $A^{\alpha_1} B^{\beta_1} \cdots A^{\alpha_i} \cdots L^{\lambda_j} \cdots = E$ is not reduced to the trivial case: $E = E$. Proceeding in this manner, the proposition will be reduced to the case when the number of matrix-variables is two.

Now we have to show that there are no identity like

$$(3) \qquad A^{\alpha_1} B^{\beta_1} \cdots A^{\alpha_m} B^{\beta_m} = E.$$

Suppose there exist such one. Put $A_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B_0 = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ in (3). Then we obtain:

$$A_0^{\alpha_1} B_0^{\beta_1} \cdots A_0^{\alpha_m} B_0^{\beta_m} = \begin{pmatrix} 1+\alpha_1\beta_1\lambda & \alpha_1 \\ \beta_1\lambda & 1 \end{pmatrix} \cdots \begin{pmatrix} 1+\alpha_m\beta_m\lambda & \alpha_m \\ \beta_m\lambda & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_1\beta_1 \cdots \alpha_m\beta_m \lambda^m + \cdots & * \\ * & * \end{pmatrix},$$

$$\alpha_1\beta_1 \cdots \alpha_m\beta_m \neq 0.$$

The polynomial $\alpha_1\beta_1 \cdots \alpha_m\beta_m \lambda^m + \cdots$ must be 1 for all values of λ in k. But if $m \geqq 1$ and k contains infinitely many elements, this is impossible.

Remark. In the case of Galois field k', if the order p^s of k is greater than the "length" m, the above proof is applicable.

When we take $H = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ any element M of the unimodular group can be expressed uniquely in the form $M = \pm H^{\alpha_0} T H^{\alpha_1} T \cdots T H^{\alpha_{m-1}} T H^{\alpha_m}$, in which we must take $\alpha_i = +1$ or -1, but α_0 and α_m are possibly zero [Takagi: Shotô Seisuron Kôgi]. This is easily verified when we notice that

$$TH = -\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad TH^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

If we represent M by $\pm(\alpha_0, \alpha_1, \cdots, \alpha_{m-1}, \alpha_m)$, then as an example, countable elements $(1, -1, 1), (1, 1, -1, 1, 1), \cdots, (\underbrace{1, 1, \cdots, 1}_{k}, -1, \underbrace{1, 1, \cdots, 1}_{k}), \cdots$ generate a free group.

(*) Received March 7, 1949.

Tokyo Institute of Technology.