ON A GENERALIZED PRINCIPAL IDEAL THEOREM

FUMIYUKI TERADA

(Received May 27, 1954)

1. Introduction. The author proved several years ago following theorem\(^1\), which is a generalization of the Hilbert's principal ideal theorem.

**Theorem.** Let \( K \) be the absolute class field of a number field \( k \), and \( \Omega \) be an intermediate field of \( K/k \) such that \( \Omega/k \) is cyclic. Then each ambiguous ideal in \( \Omega \) is principal when it is considered in \( K \).

By the Artin's law of reciprocity, this theorem can be translated into a group theoretical one. Let \( G \) be a finite group whose commutator subgroup \( G' \) is abelian. Let \( H \) be an invariant subgroup with cyclic factor group \( G/H \).

Let us denote \( S (=S_0) \) a representative of a generator of the cyclic group \( G/H \), and also denote \( S_1, \ldots, S_m \) representatives of generators of the abelian group \( H/G' \), with orders mod \( G'/e_i, \ldots, e_m \), respectively. We shall assume also that \( S_1, \ldots, S_m \) generate the group \( H \); this is accomplished by adding to them, if necessary, certain elements in \( G \) with \( e_i = 1 \). Now the theorem is translated into the following

**Theorem 1.** If an element \( A = S_1^{e_1} \cdots S_m^{e_m} \) of \( H \) satisfies \( SAS'^{-1}A'^{-1} \in H' \), then

\[
V_{H' \circ A}(A) = \prod_{j=1}^n V_{H' \circ x}(S_i)^{e_j} = 1.
\]

Author's proof of this theorem was rather complicated, and an alternative simplified proof was given by Prof. T. Tannaka\(^2\). The aim of this note is to give another proof transforming it into a problem concerning a group of linear transformations as it was done by Magnus\(^3\), and we avoided the computations concerning determinants as much as possible.

2. A group of linear transformations. Let us consider a group generated by the following \( m + 1 \) linear transformations:

\[
S_i: z' = t_i z + a_i \quad (i = 0, 1, \ldots, m)
\]

where \( m \) is the number of \( S_i \) in §1, and \( t_i, a_i \) are supposed to be algebraically independent with respect to the rational integral domain \( Z \). We can show easily that

\[
S_i^{e_1} \cdots S_i^{e_m}: z' = t_2z + A = t_1^{e_1} \cdots t_2^{e_2} + A,
\]

where $A$ is a linear form of $a_i$ with rational functions of $t_i$ as coefficients.  

More precisely, expanding $1 - T$ as

\[
1 - T = 1 - t_1^{a_1} + t_2^{a_2}(1 - t_2^{a_2}) + \cdots = \delta_1\Delta_1 + \cdots + \delta_m\Delta_m,
\]

where $\Delta_i = 1 - t_i(a_i)$, we have an identity\(^6\)

\[
A = \delta_1a_1 + \cdots + \delta_ma_m
\]

Moreover following relations are also verified easily.

\[
S_i: S'_i = Tz + A, \quad S'_i: z' = z + C 
\]

We now introduce $m$ relations $t_i^r = 1$ $(i = 1, \ldots, m)$\(^7\) into the coefficients of the above transformations, $e_i$ being the order of $S$ mod $G$. Let us denote by $\mathcal{G}$ the group obtained by this manner, and also denote $\mathcal{G}_0$ the subgroup of $\mathcal{G}$ consisting of the elements of the form $S_i z' = z + C$ (i.e. $T = 1$). Then $S'_i(i = 1, \ldots, m)$ is contained in $\mathcal{G}_0$ as it follows from the relation

\[
S'_i: z' = z + (1 + t_i + \cdots + t_i^{r-1})a_i = z + f_i a_i \quad (i = 1, \ldots, m),
\]

where $f_i = 1 + t_i + \cdots + t_i^{r-1}$. It follows from (3)~(5) that $G_0$ is an abelian normal subgroup of $\mathcal{G}$ with abelian factor group $\mathcal{G}/\mathcal{G}_0$. To avoid confusion, we shall describe an element $S: z' = z + C$ of $\mathcal{G}_0$ simply by $C$, and the group operation will be denoted additively.

The elements $S'_i(i = 1, \ldots, m)$ of $G$ are contained in $\mathcal{G}_0$, and there is $m$ relations between these elements and commutators. These will be written as

\[
S'_i = \prod [S_j, S_j]^{\delta_j} \quad (i = 1, \ldots, m),
\]

where the sign $[x, y]$ means the commutator $xyx^{-1}y^{-1}$ and $P^{\delta_i}_{ki}$ is an element of the group ring $[G/G]$ and the powers mean the usual symbolic power. In the following we shall confine ourself with a fixed representation (7) among the possible representations. Replacing all $S_j$ by $t_j$ in $P^{\delta_i}_{ki}$, we have a function which will be denoted by the same symbol $P^{\delta_i}_{ki}$. Now, let us introduce the relation (7) into the group $\mathcal{G}$ and denote the group obtained by $\mathcal{G}_0$. These relations may be denoted additively as

\[
S'_i = \prod [S_j, S_j]^{\delta_j} \quad (i = 1, \ldots, m),
\]

where $\delta_j$ is just the derivation which is defined in the free group generated by $t_0, \ldots, t_m$. All the rational functions of $t_i$ which will be appear in the followings are of this type, and we shall denote $h_i, g_i, P_{ki}$, etc., without notice there. We shall call the $t_i$-degree of a function the $t_i$-degree of the numerator of this function in its incommensurable form.

\(4\) The denominator of this coefficient is a monomial of $t_0, t_1, \ldots, t_m$. All the rational functions of $t_i$ which will be appear in the followings are of this type, and we shall denote $h_i, g_i, P_{ki}$, etc., without notice there. We shall call the $t_i$-degree of a function the $t_i$-degree of the numerator of this function in its incommensurable form.

\(5\) This symbol will be used till the end of this paper.

\(6\) The coefficient $\delta_j$ is just the derivation $\frac{\partial T}{\partial t_j}$ which is defined in the free group generated by $t_0, \ldots, t_m$. Cf. R. H. Fox, Differential calculus in free groups, Ann. of Math., vol. 57(1953).

\(7\) Notice that we introduce no relations for $t_0$, which is corresponded to $S = S_0$ in $G$, and is treated distinctively from the other elements $t_1, \ldots, t_m$ in the following.
The subgroup of $\mathcal{G}$ corresponding to $0_0$ will be denoted by $0_0^\prime$. Then the correspondence $S_i \to S_i^*$ defines a homomorphism $\psi$ of $\mathcal{G}$ onto $G$ (c. f. 4).

3. Proof of the theorem. An inverse image $S_i^* \ldots S_n^*$ in our Theorem by the homomorphism $\psi$ is expressed as

$$z' = Tz + A, T = t_1^*, \ldots, t_n^*, A = \delta_1a_1 + \cdots + \delta_na_n.$$ 

Then an inverse image of $SAS^{-1}A^{-1}$ is an element of $0_0^\prime$ expressed, from (2), as

$$\psi = (1 - T)a_0 = \sum_{i=1}^{m} \gamma_i (\Delta_0a_i - \Delta_0a_i),$$

and this will be rewritten as $\sum_{i=1}^{m} \gamma_i (\Delta_0a_i - \Delta_0a_i) = \delta_i(\Delta_0a_0 - \Delta_0a_i) + \cdots + \delta_m(\Delta_0a_m - \Delta_0a_m), \delta_i(1) = \alpha_i,$

and this will be rewritten as $\sum_{i=1}^{m} \gamma_i (\Delta_0a_i - \Delta_0a_i) = \delta_i(\Delta_0a_0 - \Delta_0a_i).$ But also, an inverse image of $V_{H^0}(A) = (\prod S_i S_i^* \ldots S_m S_m^*)$ is $f_1 \cdot \cdots \cdot f_m \cdot \alpha_i a_i = f_1 \cdot \cdots \cdot f_m \cdot \delta_i a_i$; and therefore, $f_1 \cdot \cdots \cdot f_m \sum \gamma_i a_i$ is an inverse image of $V_{H^0}(A)$. Now let us prove the following

**Proposition.** If there is a relation

$$\sum_{i=1}^{m} \gamma_i (\Delta_0a_i - \Delta_0a_i) = \sum_{i=1}^{m} f_i (\Delta_0a_i - \Delta_0a_i) + C$$

in the group $0_0^\prime$, then there is a rational function $D$ of $t_0, \ldots, t_m$ such that

$$f_1 \cdot \cdots \cdot f_m \sum \gamma_i a_i = DC.$$

Each element of $H^0$ has an inverse image of the form $\sum f_i (\Delta_0a_i - \Delta_0a_i)$, and the relation (8) is a general form of the inverse image of the assumption $SAS^{-1}A^{-1} \in H^0$ of our theorem, where $C$ satisfies the relation $\psi(C) = 1.$

From this proposition, we have $V_{H^0}(A) = \psi(f_1 \cdot \cdots \cdot f_m \sum \gamma_i a_i) = \psi(DC)$, and it follows from (4) that $\psi(DC)$ is a conjugate of $\psi(C) = 1$, and this shows our main theorem.

**Proof of the Proposition.** From (7*) we have

$$f_i a_i = \sum_{k=1}^{m} P^{(i)}_{k}(\Delta a_k - \Delta_0 a_k) - \sum_{k=1}^{m} P^{(i)}_{k} \Delta_0 a_k = - \sum_{k=1}^{m} P^{(i)}_{k} \Delta_0 a_k.$$

Rewriting $- \sum_{k=1}^{m} P^{(i)}_{k} \Delta_0 a_k = \sum_{k=1}^{m} Q_{ik} a_k,$ we have

$$- \sum_{k=1}^{m} P^{(i)}_{k} \Delta_0 a_k = R_0.$$
By the Cramer's formula concerning linear equations, we have

\[
\begin{vmatrix}
f_1 + Q_{11} \cdots Q_{1m} \\
\vdots \\
Q_{m1} \cdots f_m + Q_{mm}
\end{vmatrix}
= \begin{vmatrix}
a_1 \\
\vdots \\
a_m
\end{vmatrix}
\begin{vmatrix}
f_1 + Q_{11} \cdots Q_{1m} \\
\vdots \\
Q_{m1} \cdots f_m + Q_{mm}
\end{vmatrix}
\]

Let us denote these determinants by \(D_0\) and \(D_k\) respectively. Then we have

(11)  \[D_0 = \Delta_0 D_0 = D_0 \delta_k, \quad (k, l = 0, 1, \ldots, m).\]

For \(l = 0\), this is the identity (10) itself. For \(k \neq 0, l \neq 0\), after transposing, in the equality (9), the term of \(a_l\) in the left-hand side to the right and also the term \(Ra_l\) in the right-hand side to the left (i.e., exchanging the term of \(a_j\) and \(Ra_l\) with negative sign), we have (11) by a similar method.

As the above equality \(- \sum \Delta_i \Delta_k \Delta_m \sum Q_{i1} \Delta_k \sum Q_{im} = \sum \Delta_i \Delta_k \Delta_m = R \Delta_0\). Also, by the definition, \(\Delta_i \Delta_0 = 0\). Therefore, after multiplying the first row of the determinant \(D_0\) by \(\Delta_0\) in the left-hand side to the right, the last row of \(D_0\) by \(\Delta_m\), we have the following identities by adding them to the \(k\)-th row:

\[\Delta_k D_0 = \begin{vmatrix}
f_1 + Q_{11} \cdots \sum Q_{i1} \Delta_k \cdots Q_{1m} \\
\vdots \\
Q_{m1} \cdots \sum Q_{i1} \Delta_k \cdots f_m + Q_{mm}
\end{vmatrix} = \Delta_0 D_l, \quad (i = 1, \ldots, m).\]

Denoting \(D_0(1, t_1, \ldots, t_m)\) by \(D'\), then there is a rational function \(D\) such that \(D_0 = \Delta_0 D + D'\). Then the above formula shows \(\Delta_0 (D_0 - \Delta_0 D) = \Delta_0 D'\), and this shows

(12)  \[D_0 = \Delta_0 D, \quad (i = 1, \ldots, m)\]

and \(\Delta_0 D' = 0\) by comparing the \(t_i\)-degree of the both side of the identity. Moreover, the last formula \(\Delta_0 D' = 0\) shows that \(D'\) is divisible by each \(f_i\) \((i = 1, \ldots, m)\), and \(D'\) is expressed as \(D' = f_i \cdots f_m D'\) where \(D'\) is a function of \(t_1, \ldots, t_m\) and therefore it may be considered as a constant because \(t_i \cdots f_m = f_i \cdots f_m \quad (i = 1, \ldots, m)\). Thus we have \(D_0 = \Delta_0 D + f_i \cdots f_m D'\), and putting 1 into all \(t_i\) \((i = 0, \ldots, m)\) of this identity, we have \(D_0(1) = e_i \cdots e_m\) \(D'\). It is shown easily from the definition of \(D_0\), \(D_0(1) = e_i \cdots e_m\), and this shows \(D' = 1\). Therefore we have

(13)  \[D_0 = \Delta_0 D + f_i \cdots f_m.\]

Finally, let us compute \(f_i \cdots f_m \sum \gamma_i a_i\). It is performed by (8) and (11)~(12).

\[f_i \cdots f_m \sum \gamma_i a_i = \sum \gamma_i (D_0 - \Delta_0 D) a_i = \sum \gamma_i D a_i - \sum D \Delta_0 \gamma_i a_i,\]

by (13) and (11),

\[= \sum \gamma_i \Delta_i D a_i - \sum \gamma_i \Delta_i D a_i = D \sum \gamma_i (\Delta_0 a_i - \Delta_0 a_i), \quad \text{by (11),}
\]

\[= D \sum f_i (\Delta_0 a_i - \Delta_0 a_i) + DC = \sum f_i D (a_i - a_i) + DC, \quad \text{by (8) and (11),}
\]

\[= DC, \quad \text{by (11),}
\]
4. Remarks. a) We shall prove that \( \psi \) is a homomorphism of the group \( G \) onto the group \( \mathcal{G} \). Let us consider a free group \( \mathcal{G} \) generated by \( m + 1 \) elements \( F_0, \ldots, F_m \), and prove that the correspondence \( \phi: F_i \mapsto S_i \) defines an isomorphism \( \phi \) of the group \( \mathcal{G}/\langle F_1^2, \ldots, F_m^2, \mathcal{G}^2 \rangle \) onto the group \( \mathcal{G} \). It is easy to see that our purpose follows from this immediately. Moreover, it is enough to prove that if there is a relation

\[
S_{\sum_{i=1}^{m} i}^{l_1} \cdots S_{\sum_{i=1}^{m} i}^{l_m} = 1 \quad \text{in} \quad \mathcal{G},
\]

we have

\[
F = F_1^{l_1} \cdots F_m^{l_m} \equiv 1 \quad \text{mod} \quad \mathcal{G},
\]

Firstly, rewriting \( F \) as \( F = F_1^{l_1} \cdots F_m^{l_m} \) (mod \( \mathcal{G} \)), we have \( \phi(F) = S_0^{l_0} \cdots S_m^{l_m} \equiv 1 \mod \mathcal{G} \), and this shows that the group is expressed as

\[
F = F_1^{l_1} \cdots F_m^{l_m} \prod_{k > 1} [F_k, F_i]^{\gamma_k} \mod \mathcal{G},
\]

where the powers mean the symbolic power. In this expression, we may assume that \( g_{l_0} \) is polynomial of \( F_0, \ldots, F_m \), and especially such that

1) the \( F_i \)-degree of \( g_{l_0} \) is less than \( e_i \) for all \( i \geq 1 \),
2) the \( F_k \)- and \( F_i \)-degree of \( g_{l_0} \) is less than \( e_k - 1 \) and \( e_i - 1 \) for \( k, i \geq 1 \),
3) the \( F_j \)-degree of \( g_{l_0} \) is zero for \( j < i < k \),
4) the \( F_i \)-degree of \( \gamma_i \) is zero for all \( i \geq 1 \).

For 1), follows from \( [F_k, F_i] \subseteq \mathcal{G} \), 2) follows from \( [F_k, F_i]^{l_k+1} \cdots [F_1, F_i]^{l_1+1} = F_k^{l_k+1} \cdots F_i^{l_i+1} \) which is combined with \( F_k^{l_k+1} \) into a factor, 3) follows from \( [F_k, F_i] \cdot \mathcal{G} = [F_k, F_i]^{\gamma_k} - [F_k, F_i]^{\gamma_k-1} \), which are combined with \( [F_k, F_i]^{\gamma_k} \) and \( [F_k, F_i]^{\gamma_k+1} \), and finally 4) follows from \( F_i^{l_i} \cdot l_i = 1 \). Now we have from (14) and (16)

\[
\phi(F) = S_0^{l_0} \cdots S_m^{l_m} \prod_{k < i} [S_k, S]^{\gamma_i} = 1,
\]

where \( \gamma_i \) and \( g_{l_0} \) are polynomials of \( t_i \) obtained from \( \gamma_i \) and \( g_{l_0} \) in (16) by replacing all \( F_i \) by \( t_i \). Expressing this condition by means of \( a_i \), and recalling the algebraic independence of \( a_i \), we have

\[
\gamma_i t_i + \Delta_{i+1} g_{i+1} t_i + \cdots + \Delta_{i+m} g_{i+m} t_i - \Delta_0 g_{l_0} t_i - \cdots - \Delta_{i-1} g_{i-1} t_i = 0 \quad (i = 1, \ldots, m).
\]

Comparing the \( t_i \)-degree, we have \( \gamma_i = 0 \) from the normality of \( \gamma \) and \( g \). Moreover, comparing the \( F_i \)-degree, we have \( g_{l_0} = 0 \), and so on. Thus we have \( \gamma_i(t) = 0, g_{l_0}(t) = 0 \), and this shows that \( \gamma_i(F) = 0, g_{l_0}(F) = 0 \); that is \( F = 1 \) mod \( \mathcal{G} \), as it was desired.

b) In our group \( \mathcal{G} \) of linear transformations, let us denote \( \mathcal{D} \) an invariant subgroup generated by \( S_i, \ldots, S_m \) and \( \mathcal{G} \) (\( = \mathcal{G} \)). Then the factor group \( \mathcal{G} / \mathcal{D} \)
is a cyclic group with generator $S_0$, and $\bar{G}/\bar{G}'$ is an abelian group of the type $(e, \ldots, e_m)$. It will be shown easily that we have our main theorem concerning the group $\bar{G}$, which is an infinite group. But also, we have the inverse of this theorem concerning this group $\bar{G}'$; that is, we have

**Theorem 2.** A necessary and sufficient condition for an element $A \in \bar{G}$ to satisfy $V_{\bar{G} - \bar{G}'}(A) = 1$ is that $A$ is an ambiguous element, that is, $A$ satisfies $\text{SAS}^{-1}A^{-1} \in \bar{G}'$.

**Proof.** The commutator subgroup $\bar{G}'$ is generated by the following elements with symbolic power

$$\Delta a_i - \Delta a_i, \Delta (\Delta a_0 - \Delta a_i)$$

and the group $\bar{G}_0 = \bar{G}'$ is generated by these elements and $\Delta a_0 - \Delta a_j (j = 1, \ldots, m)$. As it was shown in §3, $V_{\bar{G} - \bar{G}'}(A)$ and $\text{SAS}^{-1}A^{-1}$ are expressed as $f_1 \cdots f_m \sum_{i=1}^m \gamma_i a_i$ and $\sum_{i=1}^m \gamma_i (\Delta a_0 - \Delta a_i)$, respectively. Let us denote the element $\sum_{i=1}^m \gamma_i (\Delta a_0 - \Delta a_i)$ in $\bar{G}'$ as

$$= \sum_{i=1}^m \lambda_i (\Delta a_0 - \Delta a_i) + \sum_{i \neq j} \mu_{ij} (\Delta a_j - \Delta a_i) + \sum_{i} \nu_i \Delta (\Delta a_0 - \Delta a_j),$$

where $\lambda_i$ has no terms of $t_1, \ldots, t_m$. Then, as it was proved in the preceding proposition,

$$f_1 \cdots f_m \sum_{i=1}^m \gamma_i a_i = D \sum_{i=1}^m \gamma_i (\Delta a_0 - \Delta a_i) = \sum_{i=1}^m D \lambda_i (\Delta a_0 - \Delta a_i) + \sum_{i \neq j} D \mu_{ij} (\Delta a_j - \Delta a_i) + \sum_{i} D \nu_i \Delta (\Delta a_0 - \Delta a_j).$$

As it was shown in the mentioned proposition, it holds $D (\Delta a_i - \Delta a_i) = 0$ for $i \neq j, i \geq 1$. Also, $D \Delta a_0 = \Delta a_0$ and $D \Delta a_i = \Delta a_i$ by (12) and (13), and $\Delta D a_0 = \Delta D a_0$ by (11), and hence $\Delta a_0 = 0$. Finally $D (\Delta a_0 - \Delta a_i) = D a_0 - D a_i + f_1 \cdots f_m a_i$. Thus we have

$$f_1 \cdots f_m \sum_{i=1}^m \gamma_i a_i = f_1 \cdots f_m \sum_{i=1}^m \lambda_i a_i$$

But $\lambda_i$ has no terms of $t_1, \ldots, t_m$ and therefore, a necessary and sufficient condition for $f_1 \cdots f_m \sum_{i=1}^m \gamma_i a_i = 0$ is $\lambda_i = 0 (i = 1, \ldots, m)$, that is, $\text{SAS}^{-1}A^{-1}$ is contained in $\bar{G}'$.

This theorem suggests us that the condition $\text{SAS}^{-1}A^{-1} \in \bar{G}'$ will be necessary in general for the validity of the main theorem, though for individual groups some special condition will guarantee a generation.

**Mathematical Institute, Tohoku University**