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 Ω be an intermediate field of K/k such that Ω/k is cyclic. Then each ambigous ideal in Ω 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 $S_1, \cdots, S_m$ representatives of generators of the abelian group H/G', with orders mod G' $e_1, \cdots, e_m$, respectively. We shall assume also that $S_1, \cdots, S_m$ 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 $A = S_{i_1}^{\alpha_1} \cdots S_{i_n}^{\alpha_n}$ of H satisfies $SAS^{-1}A^{-1} \in H'$, then*

$$V_{H \to G'}(A) = \prod_{j=1}^{n} V_{H \to G'}(S_{i_j})^{\alpha_j} = 1.$$

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;

$$S_i : z' = t_i z + a_i \qquad (i = 0, 1, \cdots, m)$$

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

$$\bar{S}_{i_1}^{\alpha_1} \cdots \bar{S}_{i_n}^{\alpha_n} : z' = Tz + A = t_{i_1}^{\alpha_1} \cdots t_{i_n}^{\alpha_n} z + A,$$

1) F. TERADA, On a generalization of the principal ideal theorem, this, journal, 2nd Ser., Vol. 1(1949).

2) T. TANNAKA, An alternative proof of a generalized principal ideal theorem, Proc. Japan Academy, vol. 25(1949).

3) W. MAGNUS, Ueber den Beweis des Hauptidealsatzes, Crelle's Journal 170(1934).

where A is a linear form of a_i with rational functions of t_i as coefficients.[4] More precisely, expanding $1-T$ as

(1) $\quad 1-T=1-t_{i_1}^{\alpha_1}+t_{i_1}^{\alpha_1}(1-t_{i_2}^{\alpha_2})+\cdots\cdots=\delta_1\Delta_{i_1}+\cdots\cdots+\delta_n\Delta_{i_n},$

where $\Delta_i=1-t_i$[5], we have an identity[6]

(2) $\quad A=\delta_1 a_{i_1}+\cdots\cdots+\delta_n a_{i_n}$ and $\delta_i(1)=\alpha_i.$

Moreover following relations are also verified easily.

(3) $\quad \bar{S}_i\bar{S}_k\bar{S}_i^{-1}\bar{S}_k^{-1}: z'=z+(\Delta_k a_i-\Delta_i a_k)$

(4) $\quad \bar{S}: z'=Tz+A, \qquad \bar{S}': z'=z+C \longrightarrow \bar{S}\bar{S}'\bar{S}^{-1}: z=z+TC$

(5) $\quad \bar{S}: z'=z+C, \qquad \bar{S}': z'=z+C' \longrightarrow \bar{S}\bar{S}': z'=z+C+C'$

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

(6) $\quad \bar{S}_i^{e_i}: z'=z+(1+t_i+\cdots\cdots+t_i^{e_i-1})a_i=z+f_i a_i \quad (i=1,\cdots\cdots,m),$

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

The elements $S_i^{e_i}$ $(i=1,\cdots\cdots,m)$ of G are contained in G', and there is m relations between these elements and commutators. These will be written as

(7) $\quad S_i^{e_i}=\prod [S_k,S_l]^{P_{kl}^{(i)}} \qquad (i=1,\cdots\cdots,m),$

where the sign $[x,y]$ means the commutator $xyx^{-1}y^{-1}$ and $P_{kl}^{(i)}$ 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 $P_{kl}^{(i)}$, we have a function which will be denoted by the same symbol $P_{kl}^{(i)}$. Now, let us introduce the relation (7) into the group $\mathfrak{G}$ and denote the group obtained by $\bar{\mathfrak{G}}$. These relations may be denoted additively as

4) The denominator of this coefficient is a monomial of t_0, t_1, ...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_{kl}, 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 δ_j is just the derivation $\frac{\partial T}{\partial t_{i_j}}$ which is defined in the free group generated by t_0, ..., 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, ..., t_m in the following.

(7*) $$f_i a_i = \sum_{k>l}^{0,\dots,m} P_{kl}^{(i)}(\Delta_l a_k - \Delta_k a_l) \qquad (i = 1, \cdots, m)$$

The subgroup of $\mathfrak{G}$ corresponding to $\mathfrak{G}_0$ will be denoted by $\bar{\mathfrak{G}}_0$. Then the correspondence $\bar{S}_i \to S_i$ defines a homomorphism ψ of $\mathfrak{G}$ onto G (c. f. 4).

3. **Proof of the theorem.** An inverse image $S_{i_1}^{\alpha_1} \cdots S_{i_n}^{\alpha_n}$ in our Theorem by the homomorphism ψ is expressed as

$$z' = Tz + A, T = t_{i_1}^{\alpha_1} \cdots t_{i_n}^{\alpha_n}, A = \delta_1 a_{i_1} + \cdots + \delta_n a_{i_n}.$$

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

$$(1-T)a_0 - \Delta_0 A = \delta_1(\Delta_{i_1} a_0 - \Delta_0 a_{i_1}) + \cdots + \delta_n(\Delta_{i_n} a_0 - \Delta_0 a_{i_n}), \delta_j(1) = \alpha_j,$$

and this will be rewritten as $\sum_{i=1}^{m} \gamma_i (\Delta_0 a_i - \Delta_i a_0)$. But also, an inverse image of $V_{H\to G'}(S_{i_j})^{\alpha_j} = (\prod_x S_1^{x_1} \cdots S_m^{x_m} S_{i_j}^{e_{ij}} S_1^{-x_1} \cdots S_m^{-x_m})^{\alpha_j}$ is $f_1 \cdots f_m \alpha_j a_{i_j} = f_1 \cdots f_m \delta_j a_{i_j}$; and therefore, $f_1 \cdots f_m \sum \gamma_i a_i$ is an inverse image of $V_{H\to G'}(A)$. Now let us prove the following

PROPOSITION. *If there is a relation*

(8) $$\sum_{i=1}^{m} \gamma_i(\Delta_i a_0 - \Delta_0 a_i) = \sum_{i>j}^{1,\dots,m} f_{ij}(\Delta_i a_j - \Delta_j a_i) + C$$

in the group $\mathfrak{G}_0$, then there is a rational function D of $t_0, \cdots, t_m$ such that

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

Each element of H' has an inverse image of the form $\sum f_{ij}(\Delta_i a_j - \Delta_j a_i)$, and the relation (8) is a general form of the inverse image of the assumption $SAS^{-1}A^{-1} \in H'$ of our theorem, where C satisfies the relation $\psi(C) = 1$. From this proposition, we have $V_{H\to G'}(A) = \psi(f_1 \cdots f_m \sum \gamma_i a_i) = \psi(DC)$, 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[8]. From (7*) we have

$$f_i a_i - \sum_{k>l}^{1,\dots,m} P_{kl}^{(i)} (\Delta_l a_k - \Delta_k a_l) - \sum_{k=1}^{m} P_{k0}^{(i)} \Delta_0 a_k = -\sum_{k=1}^{m} P_{k0}^{(i)} \Delta_k a_0.$$

Rewriting $-\sum P_{kl}^{(i)}(\Delta_l a_k - \Delta_k a_l) - \sum P_{k0}^{(i)} \Delta_0 a_k = \sum_{k=1}^{m} Q_{ik} a_k, \quad -\sum P_{k0}^{(i)} \Delta_k = R_i,$

we have

8) It can be assumed that the functions $\gamma_i, f_{ij}, P_{kl}^{(i)}, \ldots\ldots$ in this proof are polynomials of t_i, although it is not necessary for our purpose.

$$f_i a_i + \sum_{k=1}^{m} Q_{ik} a_k = R_i a_0. \qquad (i = 1, \cdots, m) \tag{9}$$

By the Cramer's formula concerning linear equations, we have

$$\begin{vmatrix} f_1 + Q_{11} \cdots Q_{1m} \\ \cdots\cdots\cdots\cdots \\ Q_{m1} \cdots\cdots f_m + Q_{mm} \end{vmatrix} a_k = \begin{vmatrix} f_1 + Q_{11} \cdots R_1 \cdots Q_{1m} \\ \cdots\cdots\cdots\cdots\cdots \\ Q_{m1} \cdots\cdots R_m \cdots f_m + Q_{mm} \end{vmatrix} a_0 \tag{10}$$

L t us denote these determinants by D_0 and D_k respectively. Then we have

$$D_l a_k = D_k a_l \qquad (k, l = 0, 1, \cdots, m). \tag{11}$$

For $l = 0$, this is the identity (10) itself: and 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 $R_i a_0$ in the right-hand side to the left (i. e, exchanging the term of a_j and $R_i a_0$ with negative sign), we have (11) by a similar method.

As the above equality $-\sum P_{kl}^{(i)} (a_k \Delta_l - a_l \Delta_k) - \sum P_{k0}^{(i)} \Delta_0 a_k = \sum Q_{ik} a_k$ is an identity, we may put Δ_k into a_k, and we have $\sum Q_{ik} \Delta_k = -\sum P_{k0}^{(i)} \Delta_0 \Delta_k = R_i \Delta_0$. Also, by the definition, $\Delta_i f_i = 0$. Therefore, after multiplying the first row of the determinant D_0 by $\Delta_1, \cdots$, the last row of D_0 by Δ_m, we have the following identities by adding them to the k-th row:

$$\Delta_i D_0 = \begin{vmatrix} f_1 + Q_{11} \cdots\cdots \sum Q_{1k} \Delta_k \cdots Q_{1m} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ Q_{m1} \cdots\cdots\cdots \sum Q_{mk} \Delta_k \cdots f_m + Q_{mm} \end{vmatrix} = \Delta_0 D_i. \quad (i = 1, \cdots, m).$$

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

$$D_i = \Delta_i D \qquad (i = 1, \cdots, m) \tag{12}$$

and $\Delta_i D' = 0$ by comparing the t_0-degree of the both side of the identity. Moreover, the last formula $\Delta_i D' = 0$ shows that D' is divisible by each f_i $(i = 1, \cdots, m)$, and D' is expressed as $D' = f_1 \cdots f_m D''$ where D'' is a function of $t_1, \cdots, t_m$ and therefore it may be considered as a constant because $t_i f_1 \cdots f_m = f_1 \cdots f_m$ $(i = 1, \cdots, m)$. Thus we have $D_0 = \Delta_0 D + f_1 \cdots f_m D''$, and putting 1 into all t_i $(i = 0, \cdots, m)$ of this identity, we have $D_0(1) = e_1 \cdots e_m D''$. It is shown easily from the definition of D_0, $D_0(1) = e_1 \cdots e_m$, and this shows $D'' = 1$. Therefore we have

$$D_0 = \Delta_0 D + f_1 \cdots f_m. \tag{13}$$

Finally, let us compute $f_1 \cdots f_m \sum \gamma_i a_i$. It is performed by (8) and (11)~(12).

$f_1 \cdots f_m \sum \gamma_i a_i = \sum \gamma_i (D_0 - \Delta_0 D) a_i = \sum \gamma_i D a_0 - \sum D \Delta_0 \gamma_i a_i$, by (13) and (11),

$= \sum \gamma_i \Delta_i D a_0 - \sum \gamma_i \Delta_0 D a_i = D \sum \gamma_i (\Delta_i a_0 - \Delta_0 a_i)$, by (11),

$= D \sum f_{ij} (\Delta_i a_j - \Delta_j a_i) + DC = \sum f_{ij} (D_i a_j - D_j a_i) + DC$, by (8) and (11),

$= DC$, by (11),

which is our proposition. q. e. d.

4. Remarks. *a*) We shall prove that ψ is a homomorphism of the group $\mathfrak{G}$ onto the group G. Let us consider a free group $\mathfrak{F}$ generated by $m+1$ elements $F_0, \cdots, F_m$, and prove that the correspondence φ: $F_i \to \overline{S_i}$ defines an isomorphism φ of the group $\mathfrak{F}/\{F_1^{e_1}, \cdots, F_m^{e_m}, \mathfrak{F}'\}'$ onto the group $\mathfrak{G}$. It is easy to see that our purpose follows from this immediately. Moreover, it is enough to prove that if there is a relation

$$\varphi(F) = \overline{S}_{i_1}^{\alpha_1} \cdots \cdot S_{i_n}^{\alpha_n} = 1 \text{ in } \mathfrak{G}, \tag{14}$$

we have

$$F = F_{i_1}^{\alpha_1}, \cdots \cdot F_{i_n}^{\alpha_n} \equiv 1 \bmod \mathfrak{F}_0 = \{F_1^{e_1}, \cdots, F_m^{e_m}, \mathfrak{F}'\}'. \tag{15}$$

Firstly, rewriting F as $F \equiv F_0^{\beta_0} \cdots \cdot F_m^{\beta_m} (\bmod\ \mathfrak{F}')$, we have $\varphi(F) = \overline{S}_0^{\beta_0} \cdots \cdot \overline{S}_m^{\beta_m} \equiv 1 \bmod \mathfrak{G}'$, and this shows $t_0^{\beta_0} \cdots \cdot t_m^{\beta_m} = 1$, and it follows $\beta_0 = 0$, $\beta_i \equiv 0 \bmod e_i$ for $i \geqq 1$. Therefore F is expressed as

$$F = F_1^{e_1\gamma_1} \cdots \cdot F_m^{e_m\gamma_m} \prod_{k>l}^{0,\ldots,m} [F_k, F_l]^{g_{kl}} \bmod \mathfrak{F}_0, \tag{16}$$

where the powers mean the symbolic power. In this expression, we may assume that g_{kl} is polynomial of $F_0, \cdots, F_m$, and especially such that

1) the F_i-degree of g_{kl} is less than e_i for all $i \geqq 1$,
2) the F_k-and F_l-degree of g_{kl} is less than $e_k - 1$ and $e_l - 1$ for $k, l \geqq 1$,
3) the F_j-degree of g_{kl} is zero for $j < l < k$,
4) the F_i-degree of γ_i is zero for all $i \geqq 1$.

For, 1) follows from $[F_i^{e_i}, \mathfrak{F}'] \subset \mathfrak{F}_0$, 2) follows from $[F_k, F_l]^{F_k^{e_k-1}+\cdots+1} = F_k^{e_k(1-F_l)}$, which is combined with $F_k^{e_k\gamma_k}$ into a factor, 3) follows from $[F_k, F_l]^{1-F_j} = [F_l, F_j]^{F_k-1}[F_k, F_j]^{1-F_l}$, which are combined with $[F_l, F_j]^{g_{lj}}$ and $[F_k, F_j]^{g_{kj}}$, and finally 4) follows from $F_i^{e_i(1-F_i)} = 1$. Now we have from (14) and (16)

$$\varphi(F) = \overline{S}_1^{e_1\gamma_1} \cdots \cdot \overline{S}_m^{e_m\gamma_m} \prod_{k<l}^{,\ldots,m} [\overline{S}_k, S_l]^{g_{kl}} = 1,$$

where γ_i and g_{kl} are polynomials of t_i obtained from γ_i and g_{kl} 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

$$\gamma_i f_i + \Delta_{i+1} g_{i+1,i} + \cdots + \Delta_m g_{m_i} - \Delta_0 g_{i0} - \cdots - \Delta_{i-1} g_{i,i-1} = 0 \ (i = 1, \cdots, m).$$

Comparing the t_i-degree, we have $\gamma_i = 0$ from the normality of γ and g. Moreover, comparing the t_0-degree, we have $g_{i0} = 0$, and so on. Thus we have $\gamma_i(t) = 0$, $g_{kl}(t) = 0$, and this shows $\gamma_i(F) = 0$, $g_{kl}(F) = 0$; that is $F \equiv 1 \bmod \mathfrak{F}_0$, as it was desired.

b) In our group $\overline{\mathfrak{G}}$ of linear transformations, let us denote $\overline{\mathfrak{H}}$ an invariant subgroup generated by $\overline{S}_1, \cdots, \overline{S}_m$ and $\overline{\mathfrak{G}}_0 (= \mathfrak{G}')$. Then the factor group $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$

is a cyclic group with generator $\overline{S_0}$, and $\mathfrak{H}/\overline{\mathfrak{G}'}$ is an abelian group of the type $(e_1, \cdots, e_m)$. It will be shown easily that we have our main theorem concerning the group $\overline{\mathfrak{G}}$, which is an infinite group. But also, we have the inverse of this theorem concerning this group $\overline{\mathfrak{G}}$; that is, we have

THEOREM 2. *A necessary and sufficient condition for an element $A \in \overline{\mathfrak{H}}$ to satisfy $V_{\overline{\mathfrak{H}}\to\overline{\mathfrak{G}'}}(A) = 1$ is that A is an ambigous element, that is, A satisfies $SAS^{-1}A^{-1} \in \overline{\mathfrak{H}}'$.*

PROOF. The commutator subgroup $\overline{\mathfrak{H}}'$ is generated by the following elements with symbolic power

$$\Delta_i a_j - \Delta_j a_i, \quad \Delta_i(\Delta_j a_0 - \Delta_0 a_j) \qquad (i, j = 1, \cdots, m),$$

and the group $\overline{\mathfrak{G}}_0 = \overline{\mathfrak{G}}'$ is generated by these elements and $\Delta_j a_0 - \Delta_0 a_j$ ($j = 1, \cdots, m$). As it was shown in §3, $V_{\overline{\mathfrak{H}}\to\overline{\mathfrak{G}'}}(A)$ and $SAS^{-1}A^{-1}$ are expressed as $f_1 \cdots f_m \sum_{i=1}^{m} \gamma_i a_i$ and $\sum_{i=1}^{m} \gamma_i(\Delta_i a_0 - \Delta_0 a_i)$, respectively. Let us denote the element $\sum \gamma_i(\Delta_i a_0 - \Delta_0 a_i)$ in $\overline{\mathfrak{G}}'$ as

$$\sum_{i=1}^{m} \gamma_i(\Delta_i a_0 - \Delta_0 a_i)$$

$$= \sum_{i=1}^{m} \lambda_i(\Delta_i a_0 - \Delta_0 a_i) + \sum_{i>j}^{1,\ldots,m} \mu_{ij}(\Delta_i a_j - \Delta_j a_i) + \sum_{i,j}^{1,\ldots,m} \nu_{ij}\Delta_i(\Delta_j a_0 - \Delta_0 a_j),$$

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

$$f_1, \cdots, f_m \sum \gamma_i a_i = D \sum \gamma_i(\Delta_i a_0 - \Delta_0 a_i)$$

$$= \sum D\lambda_i(\Delta_i a_0 - \Delta_0 a_i) + \sum D\mu_{ij}(\Delta_i a_j - \Delta_j a_i) + \sum D\nu_{ij}\Delta_i(\Delta_j a_0 - \Delta_0 a_j).$$

As it was shown in the mentioned proposition, it holds $D(\Delta_i a_j - \Delta_j a_i) = 0$ for $i > j \geqq 1$. Also, $D\Delta_i(\Delta_j a_0 - \Delta_0 a_j) = D_j\Delta_i a_0 - D_0\Delta_i a_j + \Delta_i f_1 \cdots f_m a_j$ by (12) and (13), and $= \Delta_i D_j a_0 - \Delta_i D_j a_0$ by (11), and hence $= 0$. Finally $D(\Delta_i a_0 - \Delta_0 a_i) = D_i a_0 - D_0 a_i + f_1 \cdots f_m a_i = f_1 \cdots f_m a_i$. Thus we have

$$f_1 \cdots f_m \sum \gamma_i a_i = f_1 \cdots f_m \sum \lambda_i a_i$$

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

This theorem suggests us that the condition $SAS^{-1}A^{-1} \in H'$ 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, TÔHOKU UNIVERSITY