Journal of the Mathematical Society of Japan Vol. 7, Supplement, December, 1955

A generalization of the principal ideal theorem

By Fumiyuki TERADA

(Received Nov. 25, 1955)

The purpose of this paper is to give a cohomology-theoretical description of a generalized principal ideal theorem. The definitions and the notations in this paper are borrowed from C. Chevalley's lecture notes at Nagoya University [1].

1. Let G be a finite group, and S be an automorphism of the group G. The image of an element $\sigma\in G$ by S will be denoted by $S(\sigma)$. Let H be the invariant subgroup of G, which is generated by all the elements $S(\sigma)\sigma^{-1}, \sigma\tau\sigma^{-1}\tau^{-1}(\sigma, \tau G)$. Then H is an S-invariant subgroup of G, and G/H is abelian.

Let A be a G-module. We shall denote a submodule of A which is generated by all the elements $(1-\sigma)a$ $(\sigma\in G, a\in A)$ by $I_{G}A$. Especially, if A is the group ring $Z(G)$ over the integral domain Z of all rational integers, the submodule $I_{G}Z(G)$ will be denoted by I_{G}. We shall use analogous symbols concerning subgroups of G.

2. We shall consider, in this section, certain mappings of the cohomology groups of G.

Let $x, y\in I_{G}$, and $n\in Z$. Then, $x\otimes y\otimes n\rightarrow x\otimes ny$ defines an isomorphism $\psi_{G}: H^{-2}(G, Z)\rightarrow H^{-1}(G, I_{G})$. We have also an isomorphism $\psi_{H}: H^{-2}(H, Z)\rightarrow H^{-1}(H, I_{H})$.

Let A be a G-module, and $\tau\in G, a(\tau)\in A$ such that $\sum a(\tau)=0$. Then, $\sum\tau\otimes a(\tau)\rightarrow a(e)$, where e is the unit element of G, induces an isomorphism $H^{-1}(G, A)\rightarrow A^{G\rightarrow 0}/I_{G}A$. Especially, if $A=I_{G}$, we have an isomorphism $\varphi_{G}: H^{-1}(G, I_{G})\rightarrow I_{G}/I_{G}I_{G}$, and also, $\varphi_{H}: H^{-1}(H, I_{G})\rightarrow I_{G}^{H\rightarrow 0}/I_{H}I_{G}$.

We have also an isomorphism $\Phi: H^{-1}(H, I_{H})\rightarrow H^{-1}(H, I_{G})$ (cf. [1] Theorem 7.1).

Let j_{-r} be the injection mapping $H^{-r}(H, I_{G})\rightarrow H^{-r}(G, I_{G})$, $r=1,2$. Then, $\varphi_{G}j_{-1}\varphi_{H}^{-1}$ maps $I_{G}^{H\rightarrow 0}/I_{H}I_{G}$ into $I_{G}/I_{G}I_{G}$, and the kernel is the subgroup $(I_{G'}, I_{H}I_{G})/I_{H}I_{G}$ of the group $I_{G}^{H\rightarrow 0}/I_{H}I_{G}$, where G' is the commutatorsubgroup of G.

The ideal I_{G} of $Z(G)$ is generated by all the elements $1-\sigma, \sigma\in G$, and each element of I_{G} is described as $\sum a(\sigma)(1-\sigma)$, where $a(\sigma)\in Z$.

Then, $\sum a(\sigma)(1-\sigma)\to\sum a(\sigma)(1-\sigma^{-1}S(\sigma))$ defines a homomorphism S^* of the module I_G into I_H. And when we consider the ideal I_H modulo $(I_{G'}, I_H I_G)$, S^* induces a G-homomorphism of the G-module I_G into $I_H/(I_{G'}, I_H I_G)$. The kernel of this homomorphism contains $I_G I_G$. Thus we have a G-homomorphism $S_1^*: I_G/I_G I_G\to I_G^{H\to 0}/(I_H I_G, I_{G'})$, and combining with ψ, φ, we may define a homomorphism $S_2^*: H^{-2}(G, Z)\to H^{-2}(H, Z)/$ (kernel of j_{-2}). More precisely, $S_2^*=\psi_H^{-1}\cdot\Phi^{-1}\cdot\varphi_H^{-1}S_1^*\varphi_G\psi_G$, and if $\sum\sigma\otimes a(\sigma)\in(I_G\otimes I_G)^G$, $a(\sigma)\in I_G$, $\sum a(\sigma)=0$, then S_2^* maps $\sum_{\sigma\in G}\sigma\otimes a(\sigma)$ to $\sum_{h\in G} h\otimes hS^*(a(e))\in(I_H\otimes I_H)^H$.

Moreover, we shall consider the restriction mapping. We shall describe it in details (cf. [1], Chap. 7). Let $\sigma_1=1, \sigma_2,\cdots,\sigma_m$ be representatives of the quotient group G/H, and X be a submodule of the module I_G which is generated by σ_i-1 $(i=1,\cdots,m)$. Then $I_G=I_H+U$ (direct), where $U=\sum_{h\in H} hX$. Let α be the mapping of I_G onto I_H which maps U upon 0 and maps I_H identically. Then the mapping $\alpha\otimes\alpha: I_G\otimes I_G\to I_H\otimes I_H$ defines the restriction mapping $r_2: H^{-2}(G, Z)\to H^{-2}(H, Z)$. Also, $\alpha\otimes 1: I_G\otimes I_G\to I_H\otimes I_G$ defines the restriction mapping $r_1: H^{-1}(G, I_G)\to H^{-1}(H, I_G)$, and we have a commutativity relation $r_1\cdot\psi_G=\Phi\cdot\psi_H\cdot r_2$. Moreover, $r=\varphi_H r_1\varphi_G^{-1}$ is a mapping $I_G/I_G I_G\to I_G^{H\to 0}/I_H I_G$ and by the definition of α, r is a mapping which maps $x\in I_G$ to $\sum_{i=1}^{m}\sigma_i x\in I_G^{H\to 0}$.

Finally, we shall describe these mappings in the following diagrams, which are commutative.

$$\begin{array}{ccccccc}
H^{-2}(G, Z) & & \xrightarrow{\quad\psi_G\quad} & & H^{-1}(G, I_G) & \xrightarrow{\varphi_G} & I_G/I_G I_G \\
\downarrow r_2 & & & & \downarrow r_1 & & \downarrow r \\
H^{-2}(H, Z) & \xrightarrow{\psi_H} & H^{-1}(H, I_H) & \xrightarrow{\Phi} & H^{-1}(H, I_G) & \longrightarrow & I_G^{H\to 0}/I_H I_G
\end{array}$$

$$\begin{array}{ccccccc}
H^{-2}(G, Z) & & \xrightarrow{\qquad\psi_G\qquad} & & H^{-1}(G, I_G) & \xrightarrow{\varphi_G} & I_G/I_G I_G \\
\downarrow S_2^* & & & & & & \downarrow S_1^* \\
H^{-2}(H, Z)/(\textit{kernel of } j_{-2}) & \xrightarrow{\psi_H} & H^{-1}(H, I_H)/* & \xrightarrow{\Phi} & H^{-1}(H, I_G)/* & \xrightarrow{\varphi_G} & I_G^{H\to 0}/(I_H I_G, I_{G'})
\end{array}$$

3. In this section, we shall prove the following proposition.

PROPOSITION. *Kernel of* $S_1^* \subset$ *kernel of* r.

Let $\tau_1, \cdots, \tau_m$ be representatives of generators of the abelian group G/H, where we may assume that these elements generate the group G. This is accomplished by adding to them certain elements of H. Let $e_1, \cdots, e_m$ be the order of $\tau_1, \cdots, \tau_m$ mod H. Then, $a_i = 1 - \tau_i (i = 1, \cdots, m)$ form an ideal base of I_G.

Let M be the direct sum $\sum_{i=0}^{l-1} Z(G)\bar{S}^i$, where $\bar{S}$ is a symbol such that $\bar{S}^l = 1$ and l is the order of the automorphism S. If we define $\bar{S}(\sigma \bar{S}^i) = S^{-1}(\sigma)\bar{S}^{i+1}$, then M will have the structure of a ring. Let I_M be the ideal of M generated by all the elements $1-\xi, \xi \in M$. Then $a_0 = 1 - \bar{S}$ and a_i $(i = 1, \cdots, m)$ form an ideal base of I_M.

Let $\bar{I}_G = MI_G, \bar{I}_H = MI_H$, and $\bar{I}_{G'} = MI_{G'}$. In this section, we shall consider the module $\bar{I}_G$ modulo $\bar{I}_H I_M$, where $\bar{I}_H I_M$ is an ideal of M generated by all the elements $(1-h)(1-m), h \in H, m \in M$. Then, $\bar{I}_H I_M \subset \bar{I}_H$, and $\bar{I}_H$ is generated by the following elements (1), (2) modulo $\bar{I}_H I_M$.

$$(1-\tau_i)a_j - (1-\tau_j)a_i \qquad (i, j = 1, \cdots, m) \tag{1}$$

$$(1-\bar{S})a_i - (1-\tau_i)a_0 \qquad (i = 1, \cdots, m) \tag{2}$$

And $(\bar{I}_{G'}, \bar{I}_H I_M)$ is generated by elements (1) modulo $\bar{I}_H I_M$. It is shown easily that $xya_j \equiv yxa_j$ mod $\bar{I}_H I_M$, $(j = 0, 1, \cdots, m)$, where $x, y \in G$ or $x = \bar{S}$ or $y = \bar{S}$. In other words, we can calculate coefficients of a_i commutatively, when we consider in $\bar{I}_G$ modulo $\bar{I}_H I_M$. And it is shown that

$$\bar{I}_H I_M \cap I_G^{H\to 0} \subset I_H I_G \tag{3}$$

Now let $a = \sum_{i=1}^{m} \gamma_i a_i \in I_G$. Then

$$\begin{aligned} S^*a = S^* \sum \gamma_i a_i \equiv \sum \gamma_i \cdot S^* a_i = \sum \gamma_i (1 - \tau_i^{-1} \bar{S}^{-1} \tau_i \bar{S}) \\ = \sum \gamma_i \tau_i^{-1} \bar{S}^{-1}((1-\bar{S})a_i - (1-\tau_i)a_0) \qquad \text{mod } (I_{G'}, I_H I_G). \end{aligned}$$

On the other hand $ra = \sum_{\sigma_i \in G/H} \sigma_i \cdot \sum_{i=1}^{m} \gamma_i a_i$. Let $f_i = 1 + \tau_i + \cdots + \tau_i^{e_i - 1}$. Then, $\tau_i^{-1} f_1 \cdots f_m a_i \equiv f_1 \cdots f_m a_i \pmod{I_H \cdot I_G}$, and

$$\bar{S}^{-1}(r \cdot a) = \bar{S}^{-1} f_1 \cdots f_m \sum \gamma_i a_i \equiv \bar{S}^{-1} \sum \gamma_i f_1 \cdots f_m a_i$$

$$\equiv \sum \gamma_i \tau_i^{-1} \bar{S}^{-1} f_1 \cdots f_m a_i .$$

Let $\eta_i = \gamma_i \tau_i^{-1} \bar{S}^{-1}$, then our proposition is reduced to the following:

"If $\sum \eta_i ((1 - \bar{S}) a_i - (1 - \tau_i) a_0) \in (\bar{I}_{G'}, \bar{I}_H I_M)$, then

$$\sum \eta_i f_1 \cdots f_m a_i \in \bar{I}_H I_M \text{''} . \qquad \text{(cf. (3))}$$

PROOF OF THE PROPOSITION. As $\tau_i^{e_i} \in H, 1 - \tau_i^{e_i} \in I_H$ is expressed by (1), (2) as follows.

$$1 - \tau_i^{e_i} = \sum_{k > l}^{1, \cdots, m} P_{kl}^{(i)} ((1 - \tau_l) a_k - (1 - \tau_k) a_l) + \sum_{k=1}^{m} P_{k0}^{(i)} ((1 - S) a_k - (1 - \tau_k) a_0) .$$

In this formula, $1 - \tau_i^{e_i} = f_i a_i$; and if we rewrite

$$-\sum P_{kl}^{(i)} ((1 - \tau_l) a_k - (1 - \tau_k) a_l) - \sum P_{k0}^{(i)} (1 - \bar{S}) a_k = \sum Q_k^{(i)} a_k \tag{4}$$

$$-\sum P_{k0}^{(i)} (1 - \tau_k) a_0 = R_i a_0 , \tag{5}$$

we have

$$f_i a_i + \sum_{k=1}^{m} Q_k^{(i)} a_k = R_i a_0 \qquad (i = 1, \cdots, m)$$

By the elimination formula, we have

$$D_l a_k = D_k a_l \qquad (k, l = 0, 1, \cdots, m) \tag{6}$$

where

$$D_0 = \begin{vmatrix} f_1 + Q_1^{(1)} \cdots\cdots & Q_m^{(1)} \\ \vdots & \vdots \\ Q_1^{(m)} \cdots\cdots & f_m + Q_m^{(m)} \end{vmatrix} , \qquad D_k = \begin{vmatrix} f_1 + Q_1^{(1)} \cdots & \overset{(k)}{R_1} \cdots\cdots & Q_m^{(1)} \\ \vdots & \vdots & \vdots \\ Q_1^{(m)} \cdots\cdots & R_m \cdots & f_m + Q_m^{(m)} \end{vmatrix}$$

Since we can calculate the coefficients of a_k commutatively, we have from (4),

$$\sum Q_k^{(i)}(1-\tau_k)a_l = -\sum P_{k0}^{(i)}(1-\bar{S})\,(1-\tau_k)a_l = (1-\bar{S})R_i a_0\,.$$

Also we have $(1-\tau_k)f_k a_l = 0$. Therefore, after multiplying the first row of D_0 by $1-\tau_1,\cdots,$ the last row of D_0 by $1-\tau_m$, we have the following formula by adding each row to the k-th row:

$$(1-\tau_k)D_0 a_l = (1-\bar{S})D_k a_l \qquad (l=0,1,\cdots,m;\quad k=1,\cdots,m) \tag{7}$$

Thus we get elements D_k of M, which satisfy (6) and (7). Since $(1-\bar{S})\,(1+\bar{S}+\cdots+\bar{S}^{l-1})=0$, we may assume that the $\bar{S}$-degree of D_k ($k=1,\cdots,m$; that is, except D_0) is at most $l-2$.

Since M is the direct sum of $Z(G)$ and $M(1-\bar{S})$, D_0 can be described as $D_0 = D' + D(1-\bar{S})$, where $D' \in Z(G)$ and the $\bar{S}$-degree of D is at most $l-2$. Therefore, we have from (7)

$$(1-\tau_k)D' a_l = (1-\bar{S})\,(D_k - (1-\tau_k)D)a_l$$

Since the left-hand side of this equality is an element of $Z(G)$, and the $\bar{S}$-degree of $D_k - (1-\tau_k)D$ is at most $l-2$, we have the following two relations.

$$D_k a_l = (1-\tau_k)D a_l \qquad (l=0,1,\cdots,m;\ k=1,\cdots,m) \tag{8}$$

$$(1-\tau_k)D' a_l = 0$$

From the second formula, we have $D' a_l = f_1\cdots f_m D'' a_l$, and then

$$D_0 a_l = D(1-\bar{S})a_l - f_1\cdots f_m D'' a_l \qquad (l=1,\cdots,m)$$

When we consider this relation modulo $I_M I_M$, we have $e_1\cdots e_m a_l = e_1\cdots e_m D''(1)a_l$, and this implies $D''(1)=1$. Since $D'' \in Z(G)$, $D''(1)=1$ means $f_1\cdots f_m D'' a_l = f_1\cdots f_m a_l$. Therefore, we get the following relation

$$D_0 a_l = D(1-\bar{S})a_l - f_1\cdots f_m a_l \qquad (l=1,\cdots,m) \tag{9}$$

Thus we have an element D which satisfies (8) and (9).

Now let us compute $\sum \eta_i f_1\cdots f_m a_i$. It is performed by (6)$\sim$(9).

Let $\sum_{i=1}^{m}\eta_i a_i$ be an element of I_G, which satisfies

$$\sum\eta_i((1-\bar{S})a_i-(1-\tau_i)a_0)=\sum_{i,j=1}^{m}f_{ij}((1-\tau_i)a_j-(1-\tau_j)a_i)\,.$$

Then

$$\begin{aligned}\sum\eta_i f_1\cdots f_m a_i&=\sum\eta_i(D_0a_i-D(1-\bar{S})a_i)\,, && \text{by (9)}\\ &=\sum\eta_i(D(1-\tau_i)a_0-D(1-\bar{S})a_i)\,, && \text{by (6) and (8)}\\ &=D\cdot\sum f_{ij}((1-\tau_j)a_i-(1-\tau_i)a_j)\,, && \text{by the assumption}\\ &=0 && \text{by (6),}\end{aligned}$$

which proves our proposition.

Since ψ and φ are isomorphisms, our proposition implies that the kernel of S_2^* is contained in the kernel of r_2.

4. Let $\bar{\Omega}/\Omega$ be a finite normal extention of an algebraic number field Ω, G be the Galois group of $\bar{\Omega}/\Omega$, and S be an automorphism of the group G.

Let H be the invariant subgroup of G which is considered in 1., K be the corresponding intermediate field of $\bar{\Omega}/\Omega$.

Let $C_{\bar{\Omega}}, C_K$, and C_Ω be the idele class groups of $\bar{\Omega}, K$, and Ω, respectively. Let ξ be the canonical class of $H^2(G, C_{\bar{\Omega}})$. Then $\zeta\rightarrow\xi\otimes\zeta$ ($\zeta\in H^{-2}(G,Z)$) induces an isomorphism of $H^{-2}(G,Z)$ with $H^0(G, C_{\bar{\Omega}})$. And, combining with this isomorphism, S_2^* induces a homomorphism S_0^* of $H^0(G,C_{\bar{\Omega}})$ into $H^0(H,C_{\bar{\Omega}})$/(kernel of j_0). Then, $j_0S_0^*=S^*$ defines an endomorphism of the class group $C_\Omega/N_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$.

On the other hand, the restriction mapping r_0 of the group $H^0(G,C_{\bar{\Omega}})$ into $H^0(H,C_{\bar{\Omega}})$ induces the injection mapping of $C_\Omega/N_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$ into $C_K/N_{\bar{\Omega}/K}C_{\bar{\Omega}}$. Therefore, we have the following theorem from the preceding proposition.

THEOREM. *The kernel of the endomorphism $j_0S_0^*$ of the group $C_\Omega/N_{\bar{\Omega}/\Omega}C_{\bar{\Omega}}$ is contained in $N_{\bar{\Omega}/K}C_{\bar{\Omega}}$, when it is considered in C_K.*

A special case of this theorem is the generalised principal ideal theorem which was obtained by Prof. Tannaka and the author. Now, let k be a finite algebraic number field and K be the absolute class field (generally a ray class field) over k. Let Ω/k be a cyclic intermediate field of K/k, and S be a generator of the (cyclic) Galois group of Ω/k. Let $\bar{\Omega}/K$ be the absolute class field of K, and G be the Galois group of $\bar{\Omega}/\Omega$. Then S induces an automorphism of the group G, and K is just the intermediate field of $\bar{\Omega}/\Omega$ which is considered in the preceding theorem. It is easy to see that the homomorphism $j_0 S_0^*$ in the theorem is the endomorphism such that $c \rightarrow c^{1-s}$, where $c \in C_\Omega$ and c^s means the image of c by the element S of the Galois group of Ω/k. Thus we have the following theorem.

THEOREM. *Let k be an algebraic number field, K the absolute class field over k, and Ω/k a cyclic intermediate field of K/k. Let S be a generator of the Galois group of the cyclic extension Ω/k. Then all ambigous classes in Ω (i.e. idele class c such that $c^{1-s}=1$) are contained in $N_{\bar{\Omega}/K} C_{\bar{\Omega}}$, when considered in K.*

By the usual correspondence which exists between ideles and ideals we have an analogous result which was obtained in [2] and [3]. The description of our theorem by an automorphism is due to a suggestion by K. Masuda.

Tōhoku University

References

[1] C. Chevalley, Class field theory, Nagoya University, 1953-1954.
[2] T. Tannaka, Some remarks concerning principal ideal theorem, Tōhoku Math. Journal, second series, vol. 1 (1951).
[3] F. Terada, On generalized principal ideal theorem, Tohoku Math. Journal, second series, vol. 6 (1954), 95-100.