AN EXPLICIT REPRESENTATION OF THE GENERALIZED PRINCIPAL IDEAL THEOREM FOR THE RATIONAL GROUND FIELD

SHŌICHI TAKAHASHI

(Received March 1, 1964)

In the following lines the author wants to give an explicit representation for generalized principal ideal theorems of S.Iyanaga [1] and T.Tannaka [2] for the case of rational ground field.

Let K be the "Strahlklassenkörper" over k, with "Geschlechtermodul" $\mathfrak{F} = \mathfrak{F}(K/k)$, then every ideal $\mathfrak{a}$ of k which is unramified in K, becomes principal ideal belonging to the principal class modulo $\mathfrak{F}$ (Iyanaga [1]).

Tannaka [2] obtained, suggested by a conjecture of Prof. Deuring, a more precise form of the principal ideal theorem, he gave namely those bases $\theta(\mathfrak{a})$ of $\mathfrak{a}$ (unramified ideals in k), for which the units

$$\varepsilon(\mathfrak{a}, \mathfrak{b}) = \frac{\theta(\mathfrak{a})\ \theta(\mathfrak{b})^{\sigma(\mathfrak{a})}}{\theta(\mathfrak{a}\mathfrak{b})}$$

lie in the ground field. There $\sigma(\mathfrak{a}) = (K/k, \mathfrak{a})$ means the Artin-automorphism of $\mathfrak{a}$.

Let now n,m be two natural numbers which are relatively prime to each other, $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$ and $\mathfrak{F}_n$ the "Geschlechtermodul" of $Q(\zeta_n)/Q$ (Q: rational number field), then we can find a unit $\boldsymbol{E}(m)$ in $Q(\zeta_n)$ explicitly, for which

$$m \equiv \boldsymbol{E}(m) \pmod{\mathfrak{F}_n}$$

and

$$\frac{\boldsymbol{E}(m)(\boldsymbol{E}(m'))^{\sigma(m)}}{\boldsymbol{E}(mm')} = 1$$

hold.

1. Calculation of the "Geschlechtermodul". Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} = n_1 n_2 \cdots n_t$ be a natural number, where $p_1, p_2, \cdots, p_t$ are different prime numbers and $p_1 = 2$, $e_1 = 0$ or $e_1 = 2$, and $\mathfrak{F}_n$ the "Geschlechtermodul" of $Q(\zeta_n)/Q$. We have then

$$(p_i)=(1-\zeta_{n_i})^{\varphi(n_i)}=(1-\zeta_{p_i})^{p_i-1}, \tag{1}$$

in $Q(\zeta_{n_i})$ and $Q(\zeta_{p_i})$, where $\mathfrak{p}_{n_i}=(1-\zeta_{n_i})$ and $\mathfrak{p}_{p_i}=(1-\zeta_{p_i})$ are prime ideals in $Q(\zeta_{n_i})$ and $Q(\zeta_{p_i})$ respectively, and $\varphi(\quad)$ means Euler's function. We can see also easily that $\mathfrak{p}_{n_i}$ is unramified in $Q(\zeta_n)/Q(\zeta_{n_i})$ for each i.

We now introduce the following notations:

G: Galois group of $Q(\zeta_n)/Q$.
g: Subgroup of G corresponding to $Q(\zeta_{n_i})$ in the sense of Galois theory.
G_j: Hilbert's ramification groups of order $(G_j)=N_j$ for a prime ideal $\mathfrak{p}$ in $Q(\zeta_n)$, which divides $\mathfrak{p}_{n_i}$, that is G_j consists of all Galois substitutions with

$$A^\sigma \equiv A (\text{mod } \mathfrak{p}^j) \qquad (A \text{ in } Q(\zeta_n)).$$

We put also $g_j=G_j \cap g$ and denote its order (g_j) by n_j.

LEMMA. *$\mathfrak{p}$-component of $\mathfrak{F}_n$ is equal to that of $\mathfrak{F}_{n_i}$.*

PROOF. According to a formula in [4] (See the formula (4. 4) in [4]), $\mathfrak{p}$-exponents of $\mathfrak{F}_n$ and $\mathfrak{F}_{n_i}$ are

$$\sum 1 \qquad (\text{number of } G_j \text{ which are } \neq 1) \tag{2}$$

and

$$\sum (g_j) \quad (G_j \not\subset g) \tag{3}$$

respectively. But, as $\mathfrak{p}$ is unramified in $Q(\zeta_n)/Q(\zeta_{n_i})$, $g_j=G_j\cap g=\{1\}$, accordingly (2) and (3) are identical. q.e.d.

From the above lemma, we have

$$\mathfrak{F}_n=\mathfrak{F}_{n_1}\mathfrak{F}_{n_2}\cdots\mathfrak{F}_{n_t},$$

so that we have only to decide $\mathfrak{F}_{n_i}$.

Now we apply the formula (2) to the case $n=p^e$. Then the $\mathfrak{p}$-exponent of $\mathfrak{F}_{p^e}$ is the maximum number l, for which there exists a Galois automorphism τ $(\neq 1)$ of $Q(\zeta_{p^e})/Q$, which satisfies

$$\zeta^{\tau} \equiv \zeta (\bmod\ \mathfrak{p}^{l},) \tag{4}$$

where ζ means ζ_{p^e} and

$$\mathfrak{p} = (1-\zeta).$$

But ζ^{τ} can be expressed as

$$\zeta^{k} \qquad ((k, p) = 1),$$

the condition (4) turns out

$$\zeta^{k} \equiv \zeta \qquad (\bmod\ \mathfrak{p}^{l}), \tag{5}$$

with additional condition

$$k \not\equiv 1 \qquad (\bmod\ p^{e}). \tag{6}$$

It is well known that if

$$k \equiv 1 \qquad (\bmod\ p^{a}),$$

then

$$\zeta^{k} \equiv \zeta \qquad (\bmod\ \mathfrak{p}^{pa}),$$

hence maximum number of l is p^{e-1} and

$$\mathfrak{F}_{p^e} = \mathfrak{p}^{p^{e-1}} = \mathfrak{p}_p = \mathfrak{F}_p,$$

from which we have the following theorem:

THEOREM. *If* $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} = n_1 n_2 \cdots n_t$, *we have*

$$\mathfrak{F}_n = \mathfrak{F}_{n_1}\mathfrak{F}_{n_2} \cdots \mathfrak{F}_{n_t} = \mathfrak{F}_{p_1}\mathfrak{F}_{p_2} \cdots \mathfrak{F}_{p_t}.$$

2. Explicit representation for the case of Iyanaga's principal ideal theorem. We first assume that

$$n = p_1^{e_1}\ p_2^{e_2} \cdots p_t^{e_t} \qquad (p_1 = 2,\ e_1 \geqq 2) \tag{7}$$

and set

$$n' = 4p_2p_3\cdots p_t,$$

then we have by §1, $\mathfrak{F}_n = \mathfrak{F}_{n'}$, accordingly it is enough to give an explicit representation for the case $Q(\zeta_{n'})$.

Let m be a natural number relatively prime to n and put

$$E_i = 1 + \zeta_{p_i} + \zeta_{p_i}^2 + \cdots + \zeta_{p_i}^{m-1}, \qquad (i = 1, 2, \cdots, t)$$

$$E_{ij} = 1 + \zeta_{p_i}\zeta_{p_j} + (\zeta_{p_i}\zeta_{p_j})^2 + \cdots + (\zeta_{p_i}\zeta_{p_j})^{m-1} \qquad (i \neq j,\ i,j = 1, 2, \cdots, t)$$

$$E_{ij\cdots l} = 1 + \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l} + (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^2 + \cdots + (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^{m-1}$$

($i, j, \cdots, l$ are k different numbers from $1, 2, \cdots, t$)

$$E_{12\cdots t} = 1 + \zeta_{p_1}\zeta_{p_2}\cdots\zeta_{p_t} + (\zeta_{p_1}\zeta_{p_2}\cdots\zeta_{p_t})^2 + \cdots + (\zeta_{p_1}\zeta_{p_2}\cdots\zeta_{p_t})^{m-1},$$

$$\cdots\cdots\cdots$$

$$\boldsymbol{E}_1 = \prod_i E_i$$

$$\boldsymbol{E}_2 = \prod_{(i,j)} E_{ij}$$

$$\boldsymbol{E}_k = \prod_{(i,j,\ldots,l)} E_{i,j,\ldots,l}$$

($(i,j,\cdots,l)$: all combinations of k different numbers from $1,2,\cdots,t$)

$$\boldsymbol{E}_t = E_{12\cdots t}.$$

Then E_i, $E_{ij}, \cdots$, $E_{12\cdots t}$, $\boldsymbol{E}_1, \boldsymbol{E}_2, \cdots, \boldsymbol{E}_t$ are units in $Q(\zeta_{n'})$.

For fixed $i = 1, 2, \cdots, t$ we define $E_k^{(i)}, \bar{E}_k^{(i)}$ as follows

$$\boldsymbol{E}_1 = E_1^{(i)}\ \bar{E}_1^{(i)}, \quad E_1^{(i)} = E_i$$

$$\boldsymbol{E}_2 = E_2^{(i)}\ \bar{E}_2^{(i)}, \quad E_2^{(i)} = \prod E_{ij}$$

$$\cdots\cdots\cdots$$

$$\boldsymbol{E}_k = E_k^{(i)}\bar{E}_k^{(i)}, \quad E_k^{(i)} = \prod_{(j,\dots,l)} E_{ij\dots l}$$

$$\boldsymbol{E}_t = E_{12\dots t} = E_t^{(i)}.$$

Since we have

$$\zeta_{p_i} \equiv 1 \qquad (\text{mod } \mathfrak{F}_{p_i})$$

it holds

$$E_1^{(i)} \equiv m \qquad (\text{mod } \mathfrak{F}_{p_i}), \tag{8}$$

$$E_k^{(i)} \equiv \bar{E}_{k-1}^{(i)} \quad (\text{mod } \mathfrak{F}_{p_i}), \tag{9}$$

$$(k = 2, 3,\cdots, t).$$

If $t = 2s$, we have

$$\begin{aligned} A &= m\boldsymbol{E}_2\boldsymbol{E}_4\cdots\boldsymbol{E}_{2s} - \boldsymbol{E}_1\boldsymbol{E}_3\cdots\boldsymbol{E}_{2s-1} \\ &= mE_2^{(i)}\ \bar{E}_2^{(i)}\ E_4^{(i)}\bar{E}_4^{(i)}\cdots\ E_{2s-2}^{(i)}\bar{E}_{2s-2}^{(i)}E_{2s}^{(i)} \\ &- E_1^{(i)}\bar{E}_1^{(i)}E_3^{(i)}\bar{E}_3^{(i)}\cdots E_{2s-1}^{(i)}\bar{E}_{2s-1}^{(i)} \\ &\equiv 0 \qquad (\text{mod } \mathfrak{F}_{p_i}) \\ &\qquad\qquad (i = 1, 2,\cdots, t), \end{aligned}$$

hence

$$m \equiv \frac{\boldsymbol{E}_1\boldsymbol{E}_3\cdots\boldsymbol{E}_{2s-1}}{\boldsymbol{E}_2\boldsymbol{E}_4\cdots\boldsymbol{E}_{2s}} \qquad (\text{mod } \mathfrak{F}).$$

In this case we put the right-hand side by $\boldsymbol{E}(m)$, we have namely

$$m \equiv \boldsymbol{E}(m) \ (\text{mod } \mathfrak{F}) \tag{10}$$

If $t = 2s + 1$ an odd number, we have likewise

$$\begin{aligned} A &= m\boldsymbol{E}_2\boldsymbol{E}_4\cdots\boldsymbol{E}_{2s} - \boldsymbol{E}_1\boldsymbol{E}_3\cdots\boldsymbol{E}_{2s-1}\boldsymbol{E}_{2s+1} \\ &= mE_2^{(i)}\bar{E}_2^{(i)}E_4^{(i)}\bar{E}_4^{(i)}\cdots E_{2s}^{(i)}\bar{E}_{2s}^{(i)} \\ &- E_1^{(i)}\bar{E}_1^{(i)}\cdots E_{2s-1}^{(i)}\ \bar{E}_{2s-1}^{(i)}\ E_{2s+1}^{(i)} \end{aligned}$$

$$\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{F}_{p_i}),$$

$$i = 1,2,\cdots, t,$$

hence we have (10), by putting

$$\boldsymbol{E}(m) = \frac{\boldsymbol{E}_1\boldsymbol{E}_3\cdots\boldsymbol{E}_{2s+1}}{\boldsymbol{E}_2\boldsymbol{E}_4\cdots\boldsymbol{E}_{2s}}.$$

Thus we have proved Iyanaga's principal ideal theorem for cyclotomic field, under the assumption (7).

The case $e_1 = 0$ can be treated similarly.

3. Explicit representation for the case of Deuring-Tannaka's principal ideal theorem. Let m, m' be two natural numbers relatively prime to n,and $\sigma(m)$ be Artin-symbol corresponding to m in $Q(\zeta_n)/Q$. Then it holds

$$\frac{\boldsymbol{E}(m)\boldsymbol{E}(m')^{\sigma(m)}}{\boldsymbol{E}(mm')} = 1 \tag{11}$$

We have in fact

$$E^{(m)}_{ij\ldots l} = 1 + \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l} + (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^2 + \cdots + (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^{m-1}$$

$$(\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^{\sigma(m)} = (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^m,$$

$$(E^{(m')}_{ij\ldots l})^{\sigma(m)} = 1 + (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^m + (\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^{2m}$$

$$+\cdots+(\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^{(m'-1)m},$$

$$E^{(m)}_{ij\ldots l}\,(E^{(m')}_{ij\ldots l})^{\sigma(m)}$$

$$= \frac{1-(\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^m}{1-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}\,\frac{1-(\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^{mm'}}{1-(\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l})^m} = E_{ij\ldots l}^{(mm')}$$

hence by the definition of $\boldsymbol{E}(m)$ we have (11), which proves Deuring-Tannaka's form of principal ideal theorem.

REFERENCES

[1] S. IYANAGA, Über den allgemeinen Hauptidealsatz, Japanese. Journ., 7(1931).
[2] T. TANNAKA, A generalized principal ideal theorem and a proof of a conjecture of Deuring, Ann. of Math., 67(1958).
[3] F. TERADA, On a generalization of the principal ideal theorem, Tôhoku Math. Journ., (2) 1(1949).

[4] T. TANNAKA, Some remarks concerning principal ideal theorem, Tôhoku Math. Journ., (2) 1(1949).
[5] T. TANNAKA, An alternative proof of a generalized principal ideal theorem, Proc. Japan Acad., 25(1949).

FACULTY OF ARTS AND SCIENCES,
IBARAGI UNIVERSITY.