ON TANNAKA-TERADA'S PRINCIPAL IDEAL THEOREM FOR RATIONAL GROUND FIELD

SHÔICHI TAKAHASHI

Let n be a natural number $2\nmid n$ or $4|n$ and m be one more natural number which have no quadratic factor and satisfy the relation $Q(\zeta_n)\supset Q(\sqrt{m})$ (Q: the rational number field, $\zeta_n=\exp(2\pi i/n)$), then the author wants to give an explicit representation for Tannaka-Terada's principal ideal theorem for the case of $Q(\zeta_n)\supset Q(\sqrt{m})\supset Q$. In **1** we express the calculation of Geschlechtermodul $\mathfrak{F}_n$ of $Q(\zeta_n)/Q$ and $\mathfrak{M}=\mathfrak{f}(Q(\zeta_n)/Q(\sqrt{m})/Q)$ according to the definition and notation of T. Tannaka [1], S. Takahashi [5]. In **2** we show that the ideals in each ambigous ideal class mod. $\mathfrak{M}$ which are prime to n (i.e. $\mathfrak{A}$ an ambigous ideal in $Q(\sqrt{m})$ prime to n satisfying the relation $\mathfrak{A}^{\sigma-1}=(\alpha)$, $\alpha\in Q(\sqrt{m})$, $\alpha\equiv 1$ (mod. $\mathfrak{M}$) there σ means a generator of the Galois group of $Q(\sqrt{m})/Q$)), are only principal $\mathfrak{A}=(A)$ ideals in $Q(\sqrt{m})$, and decide their form explicitly. In **3** it is shown that we can find a unit $E(A)$ in $Q(\zeta_n)$ explicitly, for which

$$A\equiv E(A)\quad (\text{mod. } \mathfrak{F}_n)$$

so that

$$\mathfrak{A}\sim 1\quad (\text{mod. } \mathfrak{F}_n)\ \text{in}\ Q(\zeta_n)$$

holds.

1. Calculation of $\mathfrak{F}_n$, $\mathfrak{M}$. Let $n=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ be a natural number, where $p_1, p_2, \cdots, p_t$ are different prime numbers and $p_1=2$, $e_1=0$ or $e_1\geqq 2$, and $\mathfrak{F}_n$ the "Geschlechtermodul" of $Q(\zeta_n)/Q$. We have then from S. Takahashi [5]

$$\mathfrak{F}_n=\mathfrak{F}_{p_1}\mathfrak{F}_{p_2}\cdots\mathfrak{F}_{p_t},\quad \mathfrak{F}_{p_i}=(1-\zeta_{p_i}),\quad i=1,2,\cdots,t. \tag{1}$$

Subsequently, let $\mathfrak{f}(Q(\zeta_n)/Q)$ and $\mathfrak{f}(Q(\sqrt{m})/Q)$ be "Fühlers" of $Q(\zeta_n)/Q$ and $Q(\sqrt{m})/Q$ respectively, then

$$\mathfrak{f}(Q(\zeta_n)/Q)=np_\infty$$

$$\mathfrak{f}(Q(\sqrt{m})/Q)=d\,p_\infty{}^e=\begin{cases} mp_\infty{}^e & (m\equiv 1\ (\text{mod. } 4))\\ 4mp_\infty{}^e & (m\equiv 2,3\ (\text{mod. } 4))\end{cases}$$

(provided that $e=0$ for $m>0$, $e=1$ for $m<0$) hold.

Now from $Q(\zeta_n)\supset Q(\sqrt{m})$ we have $|d|\,|n$, and set $n=|d|n'$. Therefore, according to the definitions and notations of T. Tannaka [1], we get

$$\mathfrak{M}=\mathfrak{f}(Q(\zeta_n)/Q(\sqrt{m})/Q)=\mathfrak{D}(Q(\zeta_n)/Q(\sqrt{m}))\cdot\mathfrak{F}(Q(\zeta_n)/Q)\,.$$

On the other hand

$$\mathfrak{D}(Q(\zeta_n)/Q(\sqrt{m}))\,\mathfrak{D}(Q(\sqrt{m})/Q)=\mathfrak{D}(Q(\zeta_n)/Q)$$

hence

$$\begin{aligned}\mathfrak{M}&=\mathfrak{D}(Q(\zeta_n)/Q)\,\mathfrak{F}(Q(\zeta_n)/Q)/\mathfrak{D}(Q(\sqrt{m})/Q)\\&=\mathfrak{f}(Q(\zeta_n)/Q)/\mathfrak{D}(Q(\sqrt{m})/Q)\\&=n\,p_\infty/\sqrt{d}\;p_\infty{}^e\\&=n'\sqrt{d}\;p_\infty^{e'}\end{aligned}$$

(provided that $e'=0$ for $m<0$ and $e'=1$ for $m>0$).

From the above, we get the following proposition.

PROPOSITION 1. *Let m, n be as above and $Q(\zeta_n)\supset Q(\sqrt{m})\supset Q$, then*

$$\begin{aligned}\mathfrak{F}_n&=\mathfrak{F}(Q(\zeta_n)/Q)=\mathfrak{F}_{p_1}\mathfrak{F}_{p_2}\cdots\mathfrak{F}_{p_t}\,,\quad \mathfrak{F}_{p_t}=(1-\zeta_{p_t})\,,\\ \mathfrak{M}&=\mathfrak{f}(Q(\zeta_n)/Q(\sqrt{m})/Q)=n\,p_\infty/\sqrt{d}\;p_\infty^e\\&\qquad\qquad\qquad\qquad\quad=n'\sqrt{d}\;p_\infty^{e'}\,,\end{aligned}$$

provided that

$$d=\begin{cases}m & (m\equiv 1\ (\mathrm{mod.}\ 4))\\ 4m & (m\equiv 2,3\ (\mathrm{mod.}\ 4))\end{cases}$$

$$n'=n/|d|,\quad e'=\begin{cases}1, & \textit{for}\quad m>0\\ 0, & \textit{for}\quad m<0.\end{cases}$$

2. A decision of ambigous ideals mod $\mathfrak{M}$. Let σ be the generator of the Galois group of $Q(\zeta_n)/Q$ such that $\sqrt{m}^\sigma=-\sqrt{m}$, and $\mathfrak{A}$ an ambigous ideal mod. $\mathfrak{M}$ prime to n, then

$$\mathfrak{A}^{\sigma-1}=(\alpha),\quad \mathfrak{A}^\sigma=(\alpha)\mathfrak{A},\quad \alpha\in Q(\sqrt{m}),\quad \alpha\equiv 1\ (\mathrm{mod.}\ \mathfrak{M})\,.$$

Here we set

$$\alpha=\frac{\lambda}{\mu}\quad \lambda,\mu \text{ are integers of } Q(\sqrt{m}) \text{ prime to } n.$$

Now from $\alpha\equiv 1 \pmod{\mathfrak{M}}$

$$\lambda-\mu\equiv 0 \pmod{\mathfrak{M}} \tag{2}$$

$$\frac{\alpha+1}{2}-1=\frac{\alpha-1}{2}=\frac{\lambda-\mu}{2\mu} \tag{3}$$

hold. On the other hand, from $\mathfrak{A}^{\sigma-1}=(\alpha)$ we get

$$N\alpha=\pm 1 \quad (N\text{: the norm } Q(\sqrt{m})\to Q)$$

here

$$\text{if } m<0, \qquad N\alpha>0$$

$$\text{if } m>0, \text{ from } \alpha\equiv 1 \ (\text{mod. } p_\infty) \quad N(\alpha)>0$$

hold. Therefore, for any cases we can set

$$N\alpha=1,\quad \alpha^\sigma=1/\alpha.$$

Now from

$$\left(\frac{\alpha+1}{2}\mathfrak{A}\right)^\sigma=\frac{\alpha^\sigma+1}{2}\mathfrak{A}^\sigma=\frac{1/\alpha+1}{2}\cdot\alpha\mathfrak{A}=\frac{\alpha+1}{2}\mathfrak{A}$$

$\frac{\alpha+1}{2}\mathfrak{A}$ is an σ-invariant ideal of $Q(\sqrt{m})$ which is not always prime to n. Therefore, if we set all prime numbers in d, $p_1, p_2, \cdots, p_t$ and $p_i=\mathfrak{p}_i^2$ in $Q(\sqrt{m})$, then we get

$$\frac{\alpha+1}{2}\mathfrak{A}=(a)\,\mathfrak{p}_1^{\lambda_1}\mathfrak{p}_2^{\lambda_2}\cdots\mathfrak{p}_t^{\lambda_t} \tag{4}$$

(provided that a is a rational number, where $\lambda_i=0$ or 1).

In the following lines we decide $\mathfrak{A}$ for each case of m (mod. 4).

I. $m\equiv 1$ (mod. 4)

In this case, $d=m$ is prime to 2, and n is prime to 2 or $4|n$. Therefore from **1**, proposition 1 we get

$\mathfrak{M}$ is prime to 2 or $4|\mathfrak{M}$ and
$\mathfrak{F}_n$ is prime to 2 or $2\|\mathfrak{M}$.

If n is prime to 2, then so is $\mathfrak{M}$. Hence from (2), (3) we get

$$\frac{\alpha+1}{2} \equiv 1 \pmod{\mathfrak{M}}$$

and from $\mathfrak{F}_n | \mathfrak{M}$,

$$\frac{\alpha+1}{2} \equiv 1 \pmod{\mathfrak{F}_n}$$

holds.

If $4|n$, then $4|\mathfrak{M}$, $2\|\mathfrak{F}_n$. Let $\mathfrak{M}'$ be the maximal part of $\mathfrak{M}$ relatively prime to n, then as above

$$\frac{\alpha+1}{2} \equiv 1 \pmod{\mathfrak{M}'}$$

holds.

Furthermore, from $2\|2\mu$, $\lambda-\mu\equiv 0 \pmod 4$ and (3), we get

$$\frac{\alpha+1}{2} \equiv 1 \pmod 2,$$

therefore from $\mathfrak{F}_n | (2)\mathfrak{M}'$

$$\frac{\alpha+1}{2} \equiv 1 \pmod{\mathfrak{F}_n}.$$

Thus we have the following proposition.

PROPOSITION 2. *Let m be $m\equiv 1 \pmod 4$ and $\mathfrak{A}$ an ideal of an ambigous ideal class* mod. $\mathfrak{M}$ *in* $Q(\sqrt{m})/Q$, i.e.

$$\mathfrak{A}^{\sigma-1} = (\alpha),\ \alpha \in Q(\sqrt{m}),\ \alpha \equiv 1 \pmod{\mathfrak{M}}$$

then

$$\frac{\alpha+1}{2} \equiv 1 \pmod{\mathfrak{F}_n}$$

and $\frac{\alpha+1}{2}$, $\mathfrak{A}$ *are both prime to n and d, now from* (4) *we have*

$$\frac{\alpha+1}{2}\mathfrak{A} = (a), \quad a \text{ is a rational number prime to } n$$

and
$$\mathfrak{A} = \left(\frac{a}{\frac{\alpha+1}{2}}\right) \text{ is principal in } Q(\sqrt{m})$$

$$\frac{a}{\frac{\alpha+1}{2}} \equiv a \pmod{\mathfrak{F}_n}$$

II. $m\equiv 3$ **(mod. 4)**

In this case, $d=4mp_\infty^e$, $4|n$, $2|\mathfrak{M}$. For the maximal part $\mathfrak{M}'$ of $\mathfrak{M}$ which is prime to n, as by the case of **I**, we get

$$\frac{\alpha+1}{2}\equiv 1 \pmod{\mathfrak{M}'}.$$

For mod. 2, we set $(2)=\mathfrak{p}^2$ in $Q(\sqrt{m})$, $\mathfrak{p}=(2,\ 1+\sqrt{m})$ and investigate it corresponding to the following cases.

i) $\mathfrak{p}^{2k}\,\|\,\dfrac{\alpha+1}{2}$, $k=0,1,2,\cdots$

Then $\dfrac{\alpha+1}{2^{k+1}}$ is prime to 2 and from

$$\left(\frac{\alpha+1}{2^{k+1}}\right)^{\sigma}\mathfrak{A}^{\sigma}=\frac{\alpha+1}{2^{k+1}}\mathfrak{A}$$

$\dfrac{\alpha+1}{2^{k+1}}\mathfrak{A}$ is prime to n especially to d. Therefore $\left(\dfrac{\alpha+1}{2^{k+1}}\right)\mathfrak{A}$ is a σ-invariant ideal prime to d. Now from (4), we have

$$\frac{\alpha+1}{2^{k+1}}\mathfrak{A}=(a),\quad a \text{ is a rational number prime to } n$$

and

$$\mathfrak{A}=\left(\frac{a}{\dfrac{\alpha+1}{2^{k+1}}}\right) \quad \text{is principal in } Q(\sqrt{m}).$$

ii) $\mathfrak{p}^{2k+1}\,\|\,\dfrac{\alpha+1}{2}$

Then $\mathfrak{p}\,\|\,\dfrac{\alpha+1}{2^{k+1}}$ holds. And we can set

$$\beta=\frac{\alpha+1}{2^{k+1}}=\frac{\beta_0}{b}$$

$$\beta_0=x+y\sqrt{m}$$

provided that x, y, b are rational integers, b is prime to n, and β_0 is an integer in $Q(\sqrt{m})$ satisfying the condition $\mathfrak{p}\,\|\,\beta_0$.

Now from $\mathfrak{p}=(2,\ 1+\sqrt{m})$, $\mathfrak{p}\,\|\,\beta_0$, x, y must be both odd numbers, because if x, y are both even then $2|\beta_0$, if x is odd, and y is even i.e. $x=2s+1$ $y=2t$ (s, t are rational integers), then from

$$\beta_0 = 2s + 1 + 2t\sqrt{m} = 2(s + t\sqrt{m}) + 1, \ \mathfrak{p} \nmid \beta_0$$

and if x is even, y is odd, i.e. $x=2s$, $y=2t+1$ (s, t are rational integers) then from

$$\begin{aligned} \beta_0 &= 2s + (2t+1)\sqrt{m} \\ &= 2(s + t\sqrt{m}) + \sqrt{m}, \quad \mathfrak{p} \nmid \beta_0 . \end{aligned}$$

We have then

$$\beta_0^{1-\sigma} = (\alpha+1)^{1-\sigma} = \alpha \equiv 1 \pmod{\mathfrak{M}}$$

especially

$$\beta_0^{1-\sigma} \equiv 1 \pmod{2} .$$

On the other hand we have

$$\beta_0^{1-\sigma} - 1 = \frac{2y\sqrt{m}}{x-y\sqrt{m}}$$

$$\mathfrak{p}^2 \| 2y\sqrt{m}, \ \mathfrak{p} \| x-y\sqrt{m},$$

$$\beta_0^{1-\sigma} \not\equiv 1 \pmod{2}.$$

Therefore the case ii) does not happen. As was stated above, we have the following proposition.

PROPOSITION 2′. *Let m be $m \equiv 3 \pmod{4}$ and $\mathfrak{A}$ an ambigous ideal of an ambigous ideal class* mod. $\mathfrak{M}$ *in $Q(\sqrt{m})/Q$ i.e. $\mathfrak{A}^{\sigma-1}=(\alpha)$, $\alpha \in Q(\sqrt{m})$, $\alpha \equiv 1 \pmod{\mathfrak{M}}$. Then, the exponential index of $\mathfrak{p}$ for $\frac{\alpha+1}{2}$ is even, hence we can set $\mathfrak{p}^{2k} \| \frac{\alpha+1}{2}$ ($k=0, 1, 2, \cdots$).* And *$\frac{\alpha+1}{2^{k+1}}\mathfrak{A}$ is a σ-invariant ideal of $Q(\sqrt{m})$ prime to n. Therefore again from* (4), *we get*

$$\frac{\alpha+1}{2^{k+1}}\mathfrak{A} = (a), \qquad \mathfrak{A} = \left(\frac{a}{\frac{\alpha+1}{2^{k+1}}}\right) \ \textit{is principal in } Q(\sqrt{m})$$

a is a rational number prime to n.

III. $m \equiv 2 \pmod{4}$

In this case, we have $d = 4mp_\infty^e$, $n = 2^t \cdot n_0$ ($t \geqq 3$, n_0 odd). And if we set $2 = \mathfrak{p}^2$ in $Q(\sqrt{m})$, then

$$\mathfrak{p} = (2, \sqrt{m})$$

$$\mathfrak{p}^6 \mid n, \quad \mathfrak{p}^3 \parallel \sqrt{d}\,, \quad \mathfrak{p}^3 \mid \mathfrak{M}\,.$$

Now we set

$$\beta = \frac{\alpha+1}{2} = \frac{\lambda+\mu}{2\mu} = \frac{\lambda-\mu+2\mu}{2\mu}$$

then from $\mathfrak{M} \mid \lambda-\mu$, $\mathfrak{p}^3 \mid \lambda-\mu$ and $\mathfrak{p}^2 \parallel 2\mu$

$$\mathfrak{p}^2 \parallel \lambda - \mu + 2\mu$$

holds. Therefore β is prime to $\mathfrak{p}$, and for the maximal part $\mathfrak{M}'$ of $\mathfrak{M}$ which is prime to 2, we have as above

$$\frac{\alpha+1}{2} \equiv 1 \pmod{\mathfrak{M}'}\,.$$

Hence β is prime to n, and especially prime to d. And $(\beta)\mathfrak{A}$ is a σ-invariant ideal of $Q(\sqrt{m})$ prime to d, therefore

$$\beta\mathfrak{A} = (a), \quad a \text{ is a rational number prime to } n$$

holds. Consequently, we have the following proposition:

PROPOSITION 2″. *Let m be $m \equiv 2$ (mod. 4), $\mathfrak{A}$ an ideal of an ambigous ideal class mod. $\mathfrak{M}$ of $Q(\sqrt{m})$,* i.e.

$$\mathfrak{A}^{\sigma-1} = (\alpha), \quad \alpha \in Q(\sqrt{m}), \ \alpha \equiv 1 \pmod{\mathfrak{M}}$$

then

$$\frac{\alpha+1}{2}\mathfrak{A} = (a), \quad a \textit{ is a rational number prime to } n$$

and

$$\mathfrak{A} = \left(\frac{a}{\frac{\alpha+1}{2}}\right) \textit{ is principal in } (Q\sqrt{m}).$$

Now in consideration of the premises, for any cases we have that $\mathfrak{A}$ is principal in $Q(\sqrt{m})$.

3. An explicit representation for Tannaka-Terada's principal ideal therem. In the following we consider according to three cases of **2**.

2. I. From the proposition 2 we get

$$\mathfrak{A} = \left(\frac{a}{\frac{\alpha+1}{2}} \right), \qquad \frac{a}{\frac{\alpha+1}{2}} \equiv a \quad (\text{mod. } \mathfrak{F}_n)$$

and, a is a rational number prime to n.

Now from S. Takahashi [5], there is an explicit form of an unit which satisfy

$$a \equiv E(a) \quad (\text{mod. } \mathfrak{F}_n).$$

Therefore

$$\frac{a}{\frac{\alpha+1}{2}} \equiv a \equiv E(a) \quad (\text{mod. } \mathfrak{F}_n)$$

and

$$\mathfrak{A} \sim 1 \quad (\text{mod. } \mathfrak{F}_n).$$

2. II. From the proposition 2′ we get

$$\mathfrak{A} = \left(\frac{a}{\frac{\alpha+1}{2^{k+1}}} \right)$$

and if we set $\beta = \dfrac{a}{\frac{\alpha+1}{2^{k+1}}}$, then β is an integer of $Q(\sqrt{m})$ prime to n. Now

$$\beta^{\sigma-1} = (\alpha+1)^{1-\sigma} = \frac{\alpha+1}{\alpha^{\sigma}+1} = \alpha \equiv 1 \quad (\text{mod. } \mathfrak{M}).$$

And if we set $\beta = x+y\sqrt{m}$ (x, y are rational integers), then from

$$\beta^{\sigma-1} \equiv 1 \quad (\text{mod. } \mathfrak{M}),$$

$$2y\sqrt{m} \equiv 0 \quad (\text{mod. } \mathfrak{M})$$

holds. Furthermore, from $\mathfrak{F}_n | \mathfrak{M}$, $2 \| \mathfrak{F}_n$

$$y\sqrt{m} \equiv 0 \quad (\text{mod. } \mathfrak{F}_n/(2))$$

holds. On the other hand we have

$$x \not\equiv y \quad (\text{mod. } 2), \text{ because } \beta \text{ is prime to } \mathfrak{p} = (2, 1+\sqrt{m}).$$

If x, y are both even, then $2|\beta$, and if x, y are both odd i.e. $x = 2s+1$, $y=2t+1$ (s, t are rational integers) then

$$\beta = 2s+1+(2t+1)\sqrt{m} = 2(s+t\sqrt{m})+(1+\sqrt{m}), \ \mathfrak{p}|\beta .$$

In the following we consider according to the cases where x, y are even or odd respectively.

i) x: odd, y: even

In this case $y\sqrt{m} \equiv 0$ (mod. 2) holds, so $y\sqrt{m} \equiv 0$ (mod. $\mathfrak{F}_n$) and $\beta = x+y\sqrt{m}$ are prime to n especially prime to $\mathfrak{F}_n$, so that x is prime to $\mathfrak{F}_n$ and n. Therefore

$$\beta \equiv x \quad (\text{mod. } \mathfrak{F}_n) .$$

Now from S. Takahashi [5], there is a unit satisfying the congruence equation

$$x \equiv E(x) \quad (\text{mod. } \mathfrak{F}_n) .$$

For this unit we get

$$\beta \equiv E(x) \quad (\text{mod. } \mathfrak{F}_n)$$

and

$$\mathfrak{A} \sim 1 \quad (\text{mod. } \mathfrak{F}_n) \quad \text{in } Q(\zeta_n) .$$

ii) x: even, y: odd

It we set $n = 2^{t'} \cdot n_0$ (n_0: odd), so x is prime to n, because $\beta=x+y\sqrt{m}$ is prime to n and $y\sqrt{m} \equiv 0$ (mod. $\mathfrak{F}_n/(2)$). Therefore the following linear congruence equations have the solution k, and k relatively prime to n

$$\begin{cases} kx \equiv 1 \quad (\text{mod. } n_0) \\ ky \equiv 1 \quad (\text{mod. } 2) . \end{cases}$$

For this k

$$\begin{cases} k\beta = kx + ky\sqrt{m} \equiv 1 \quad (\text{mod. } \mathfrak{F}_n/(2)) \\ k\beta = kx + ky\sqrt{m} \equiv \sqrt{m} \ (\text{mod. } 2) \end{cases} \tag{5}$$

hold. Furthermore, from $4|n$

$$i = \sqrt{-1} \in Q(\zeta_n),$$

and

$$\sqrt{m} - i = \frac{1}{i}(\pm\sqrt{-m}+1)$$

holds.

On the other hand $\pm\sqrt{-m}+1/2$ is an integer, because $-m\equiv 1$ (mod. 4), hence $\sqrt{m}\equiv i$ (mod. 2) holds. So we have from (5) the following congruences,

$$\begin{cases} k\beta \equiv 1 \pmod{\mathfrak{F}_n/(2)} \\ k\beta \equiv i \pmod{2}\,. \end{cases} \tag{6}$$

Let $n=2^{t'}\cdot n_0=2^{t'}\cdot p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ be, where p_i are all odd prime numbers and $e_i\neq 0$. Then we have

$$\mathfrak{F}_n = 2\,\mathfrak{F}_{p_1}\mathfrak{F}_{p_2}\cdots\mathfrak{F}_{p_t}\,,\quad \mathfrak{F}_{p_i}=(1-\zeta_{p_i})\,.$$

Now we put

$$E_1=\prod_{i=1}^{t}(1-\zeta_4\zeta_{p_i})\,,\qquad F_1=\prod_{i=1}^{t}(\zeta_{p_i}-\zeta_4)$$

$$E_2=\prod_{(i,j)}(1-\zeta_4\zeta_{p_i}\zeta_{p_j})\,,\quad F_2=\prod_{(i,j)}(\zeta_{p_i}\zeta_{p_j}-\zeta_4) \tag{7}$$

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

. . . .

$$E_k=\prod_{(i,j,\cdots,l)}(1-\zeta_4\zeta_{p_i}\cdots\zeta_{p_l})\,,\quad F_k=\prod_{(i,j,\cdots,l)}(\zeta_{p_i}\cdots\zeta_{p_l}-\zeta_4)$$

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

. . . .

$$E_t=1-\zeta_4\zeta_{p_1}\cdots\zeta_{p_t}\,,\quad F_t=\zeta_{p_1}\zeta_{p_2}\cdots\zeta_{p_t}-\zeta_4$$

Then, $E_1,E_2,\cdots,E_t$, $F_1,F_2,\cdots,F_t$ are units in $Q(\zeta_n)$.

Generally it is well known that if m is a natural number which contains two or more prime numbers, and ζ is a primitive root of unity, then $1-\zeta$ is a unit. Therefore

$$1-\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}\,,$$

$$\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}-\zeta_4=\zeta_4(\zeta_4^3\zeta_{p_i}\cdots\zeta_{p_l}-1)$$

$$(k=1,2,\cdots,t)$$

are all units. And furthermore, we set

$$E=\begin{cases}\dfrac{E_1F_2E_3F_4\cdots E_{t-1}F_t}{F_1E_2F_3E_4\cdots F_{t-1}E_t} & \text{(if } t \text{ is even)}\\[2ex] \dfrac{E_1F_2E_3\cdots F_{t-1}E_t}{F_1E_2F_3\cdots E_{t-1}F_t} & \text{(if } t \text{ is odd)}\end{cases} \tag{8}$$

Then E too is a unit in $Q(\zeta_n)$. Now we put for fixed i from $1, 2, \cdots, t$ as follows

$$\begin{aligned}
&E_1 = E_1^{(i)}\bar{E}_1^{(i)}, \qquad E_1^{(i)} = 1-\zeta_4\zeta_{p_i}\\
&F_1 = F_1^{(i)}\bar{F}_1^{(i)}, \qquad F_1^{(i)} = \zeta_{p_i}-\zeta_4\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&E_k = E_k^{(i)}\bar{E}_k^{(i)}, \qquad E_k^{(i)} = \prod_{(j,\cdots,l)}(1-\zeta_4\zeta_i\cdots\zeta_l)\\
&F_k = F_k^{(i)}\bar{F}_k^{(i)}, \qquad F_k^{(i)} = \prod_{(j,\cdots,l)}(\zeta_i\zeta_j\cdots\zeta_l-\zeta_4)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&E_t = E_t^{(i)}\\
&F_t = F_t^{(i)}. \qquad (\bar{E}_t^{(i)} = \bar{F}_t^{(i)} = 1)
\end{aligned} \tag{9}$$

Then from $\zeta_{p_i} \equiv 1 \pmod{\mathfrak{F}_{p_i}}$

$$\begin{aligned}
&E_1^{(i)} \equiv F_1^{(i)} \pmod{\mathfrak{F}_{p_i}}\\
&E_k^{(i)} \equiv \bar{E}_{k-1}^{(i)} \pmod{\mathfrak{F}_{p_i}}\\
&F_k^{(i)} \equiv \bar{F}_{k-1}^{(i)} \pmod{\mathfrak{F}_{p_i}}
\end{aligned} \qquad k = 2, 3, \cdots, t \tag{10}$$

hold. Therefore, from (8), (9), (10)

$$E = \frac{E_1^{(i)}\bar{E}_1^{(i)}F_2^{(i)}\bar{F}_2^{(i)}\cdots}{F_1^{(i)}\bar{F}_1^{(i)}E_2^{(i)}\bar{E}_2^{(i)}\cdots} \equiv 1 \pmod{\mathfrak{F}_{p_i}},$$

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

$$E \equiv 1 \pmod{\mathfrak{F}_n/(2)}.$$

In the next we show that $E \equiv i \pmod{2}$. It holds

$$\begin{cases} \dfrac{1-\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}}{\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}-\zeta_4} \equiv \zeta_4 \pmod{2} \\ 1/\zeta_4 = -\zeta_4 \equiv \zeta_4 \pmod{2}. \end{cases} \tag{11}$$

Therefore

$$\frac{E_k}{F_k} \equiv \frac{F_k}{E_k} \equiv \zeta_4^{{}_tC_k} \pmod{2}.$$

And from (8) it holds

$$E \equiv \zeta_4^{\sum_{k=}^{t} {}_tC_k} = \zeta_4^{(1+1)^t-1} \equiv \zeta_4 \pmod{2}. \tag{12}$$

Therefore from (11), (12)

$$\begin{cases} E \equiv 1 \pmod{\mathfrak{F}_n/(2)} \\ E \equiv i \pmod{2}. \end{cases} \tag{13}$$

And from (6) we have

$$k\beta \equiv E \pmod{\mathfrak{F}_n}.$$

Now again take the unit $E(k)$ in $Q(\zeta_n)$ satisfying $k \equiv E(k) \pmod{\mathfrak{F}_n}$ according to S. Takahashi [5]. Then

$$\mathfrak{A} = (\beta) = \left(\frac{k\beta}{k}\right)$$

$$\frac{k\beta}{k} \equiv \frac{E}{E(k)} \pmod{\mathfrak{F}_n}$$

$$\mathfrak{A} \sim 1 \pmod{\mathfrak{F}_n} \text{ in } Q(\zeta_n).$$

2. III From the proposition 2″ we have

$$\mathfrak{A} = \left(\frac{a}{\frac{\alpha+1}{2}}\right)$$

and put

$$\beta = \frac{a}{\frac{\alpha+1}{2}}$$

β is an integer of $Q(\sqrt{m})$ which is prime to n, and

$$\beta^{\sigma-1} = (\alpha+1)^{1-\sigma} = \alpha \equiv 1 \pmod{\mathfrak{M}}.$$

Therefore if we put

$$\beta = x + y\sqrt{m} \quad (x, y \text{ are rational integers})$$

then

$$\beta^{\sigma-1} = \frac{x-y\sqrt{m}}{x+y\sqrt{m}} - 1 = \frac{-2y\sqrt{m}}{x+y\sqrt{m}} \equiv 0 \pmod{\mathfrak{M}}.$$

So

$$2y\sqrt{m} \equiv 0 \pmod{\mathfrak{M}}$$

and x is prime to n

$$y\sqrt{m} \equiv 0 \pmod{\mathfrak{F}_n/(2)}. \tag{14}$$

In the following we consider according to the cases where y is even or odd respectively.

i) y: even

In this case it holds from (14),

$$y\sqrt{m} \equiv 0 \pmod{\mathfrak{F}_n},$$

so

$$\beta \equiv x \pmod{\mathfrak{F}_n}$$

and x is prime to n. Therefore take again a unit in $Q(\zeta_n)$ satisfying $x \equiv E(x)$ (mod. $\mathfrak{F}_n$). Then

$$\mathfrak{A} = (\beta),\ \beta \equiv x \equiv E(x) \pmod{\mathfrak{F}_n}$$

so it holds

$$\mathfrak{A} \sim 1 \pmod{\mathfrak{F}_n} \text{ in } Q(\zeta_n).$$

ii) y: odd

Write $n = 2^t \cdot n_0$, n_0 being odd. Then the following linear congruence equations have the solution k which is prime to n

$$\begin{cases} kx \equiv 1 \pmod{n_0} \\ k \equiv 1 \pmod{2} \end{cases}$$

so, for $\beta = x+y\sqrt{m}$

$$\begin{cases} k\beta = kx+ky\sqrt{m} \equiv 1+\sqrt{m} \pmod{2} \\ k\beta = kx+ky\sqrt{m} \equiv 1 \pmod{\mathfrak{F}_n/(2)} \end{cases} \tag{15}$$

hold. (phr. $\mathfrak{F}_n/(2) \mid n_0$, $y\sqrt{m} \equiv 0 \pmod{\mathfrak{F}_n/(2)}$).

Now we write $m = 2m'$ (m' is odd). Here, if $m' \equiv 1 \pmod{4}$ holds

$$\sqrt{m} - \sqrt{2} = \sqrt{2}\,(\sqrt{m'} - 1) \text{ in } Q(\zeta_n)$$

and $\sqrt{m'}-1/2$ is an integer in $Q(\sqrt{m'}) \subset Q(\zeta_n)$

so $$\sqrt{m} \equiv \sqrt{2} \pmod{2}.$$

And if $m' \equiv 3 \pmod{4}$ holds

$$\sqrt{m} - \sqrt{2}\,i = \sqrt{2}\,(\sqrt{m'} - i)$$

and $\sqrt{m'} - i/2 = \dfrac{1}{2i} \cdot (\pm\sqrt{-m'} + 1)$ is an integer, because $-m' \equiv 1 \pmod{4}$

so $$\sqrt{m} \equiv \sqrt{2}\,i \pmod{2}.$$

On the other hand take

$$\zeta_8 = \frac{1+i}{\sqrt{2}} \in Q(\zeta_8)$$

then

$$\begin{aligned} \zeta_8 + \zeta_8^{-1} &= \frac{1+i}{\sqrt{2}} + \frac{\sqrt{2}}{1+i} \\ &= \frac{\sqrt{2}\,(1+i)}{2} + \frac{\sqrt{2}\,(1-i)}{2} \\ &= \sqrt{2}\,. \end{aligned}$$

Therefore

$$\begin{aligned} \sqrt{2} - \sqrt{2}\,i = \sqrt{2}\,(1-i) &= (\zeta_8+\zeta_8^{-1})(1-\zeta_8^2) \\ &= \zeta_8 + \zeta_8^{-1} - \zeta_8^3 - \zeta_8 \\ &= \zeta_8^{-1}(1-\zeta_8^4) = 2\zeta_8^{-1} \equiv 0 \pmod{2}. \end{aligned}$$

From the above we have for any cases

$$1 + \sqrt{m} \equiv 1 + \sqrt{2} \pmod{2}.$$

Now $1+\sqrt{2}$ is a unit in $Q(\zeta_n)$, and has the following representasion.

$$1+\sqrt{2}=1+\zeta_8+\zeta_8^{-1},\quad \zeta_8^4=-1,\quad \zeta_8^3=-\zeta_8^{-1}$$
$$=1+\zeta_8-\zeta_8^3.$$

On the other hand

$$(1+\zeta_8-\zeta_8^3)(1-\zeta_8)=1+\zeta_8-\zeta_8^3-\zeta_8-\zeta_8^2+\zeta_8^4$$
$$=-\zeta_8^3-\zeta_8^2,$$

hence

$$1+\zeta_8-\zeta_8^3=\frac{\zeta_8^3+\zeta_8^2}{\zeta_8-1}=\frac{\zeta_8^3+\zeta_4}{\zeta_8-1}.$$

In the following we write

$$E_0=1+\sqrt{2}=\frac{\zeta_8^3+\zeta_4}{\zeta_8-1},$$

so from (15)

$$\begin{cases} k\beta\equiv E_0 \pmod{2} \\ k\beta\equiv 1 \pmod{\mathfrak{F}_n/(2)}. \end{cases} \tag{16}$$

Now let all prime numbers contained in n_0 be $p_1, p_2, \cdots, p_t$, and we put

$$E_1=\prod_{i=1}^{t}\frac{\zeta_8-\zeta_{p_i}}{\zeta_8^3+\zeta_4\zeta_{p_i}}\cdot\frac{\zeta_4\zeta_{p_i}-1}{\zeta_4-\zeta_{p_i}}$$

$$E_2=\prod_{(i,j)}\frac{\zeta_8-\zeta_{p_i}\zeta_{p_j}}{\zeta_8^3+\zeta_4\zeta_{p_i}\zeta_{p_j}}\cdot\frac{\zeta_4\zeta_{p_i}\zeta_{p_j}-1}{\zeta_4-\zeta_{p_i}\zeta_{p_j}}$$

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

. . . .

$$E_k=\prod_{(i,j,\cdots,l)}\frac{\zeta_8-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}{\zeta_8^3+\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}}\cdot\frac{\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}-1}{\zeta_4-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}$$

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

. . . .

$$E_t=\frac{\zeta_8-\zeta_{p_1}\zeta_{p_2}\cdots\zeta_{p_t}}{\zeta_8^3+\zeta_4\zeta_{p_1}\cdots\zeta_{p_t}}\cdot\frac{\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}-1}{\zeta_4-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}.$$

Now

$$\zeta_8 - \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l} = \zeta_8(1 - \zeta_8^7\zeta_{p_i}\cdots\zeta_{p_l})$$

$$\zeta_8^3 + \zeta_4\zeta_{p_i}\cdots\zeta_{p_l} = \zeta_8^3(1 - \zeta_8^3\zeta_{p_i}\cdots\zeta_{p_l})$$

$$\zeta_4\zeta_{p_i}\cdots\zeta_{p_l} - 1$$

$$\zeta_4 - \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l} = \zeta_4(1 - \zeta_4^3\zeta_{p_i}\cdots\zeta_{p_l})$$

are all units. Therefore $E_1, E_2, \cdots, E_t$ are all units in $Q(\zeta_n)$. Now, for fixed i from $1, 2, \cdots, t$ we put

$$E_1 = E_1^{(i)}\bar{E}_1^{(i)}, \quad E_1^{(i)} = \frac{\zeta_8-\zeta_{p_i}}{\zeta_8^3+\zeta_4\zeta_{p_i}}\cdot\frac{\zeta_4\zeta_{p_i}-1}{\zeta_4-\zeta_{p_i}}$$

$$E_2 = E_2^{(i)}\bar{E}_2^{(i)}, \quad E_2^{(i)} = \prod_j \frac{\zeta_8-\zeta_{p_i}\zeta_{p_j}}{\zeta_8^3+\zeta_4\zeta_{p_i}\zeta_{p_j}}\cdot\frac{\zeta_4\zeta_{p_i}\zeta_{p_j}-1}{\zeta_4-\zeta_{p_i}\zeta_{p_j}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$E_k = E_k^{(i)}\bar{E}_k^{(i)}, \quad E_k^{(i)} = \prod_{(j,\cdots,l)} \frac{\zeta_8-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}{\zeta_8^3+\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}}\cdot\frac{\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}-1}{\zeta_4-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$E_t = E_t^{(i)}.$$

Then

$$\begin{aligned} E_0E_1^{(i)} &= \frac{\zeta_8^3+\zeta_4}{\zeta_8-1}\cdot\frac{\zeta_8-\zeta_{p_i}}{\zeta_8^3+\zeta_4\zeta_{p_i}}\cdot\frac{\zeta_4\zeta_{p_i}-1}{\zeta_4-\zeta_{p_i}} \\ &\equiv \frac{\zeta_8^3+\zeta_4}{\zeta_8-1}\cdot\frac{\zeta_8-1}{\zeta_8^3+\zeta_4}\cdot\frac{\zeta_4-1}{\zeta_4-1} \\ &= 1 \pmod{\mathfrak{P}_{p_i}} \end{aligned}$$

and for $k = 2, 3, \cdots, t$

$$\begin{aligned} E_k^{(i)} &= \prod_{(j\cdots l)} \frac{\zeta_8-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}{\zeta_8^3+\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}}\cdot\frac{\zeta_4\zeta_{p_i}\cdots\zeta_{p_l}-1}{\zeta_4-\zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}} \\ &\equiv \prod_{(j\cdots l)} \frac{\zeta_8-\zeta_{p_j}\cdots\zeta_{p_l}}{\zeta_8^3+\zeta_4\zeta_{p_j}\cdots\zeta_{p_l}}\cdot\frac{\zeta_4\zeta_{p_j}\cdots\zeta_{p_l}-1}{\zeta_4-\zeta_{p_j}\cdots\zeta_{p_l}} \\ &= \bar{E}_{k-1}^{(i)} \pmod{\mathfrak{P}_{p_i}} \end{aligned}$$

holds. Therefore we have the following congruence equations

$$\left\{\begin{array}{l} E_0E_1^{(i)} \equiv 1 \quad (\mathrm{mod.}\mathfrak{F}_{p_i}) \\ E_k^{(i)} \equiv \bar{E}_{k-1}^{(i)} \ (\mathrm{mod.}\ \mathfrak{F}_{p_i}) \\ (k = 2, 3, \cdots, t)\,. \end{array}\right. \tag{17}$$

Now if t is even we put

$$E = \frac{E_0E_1E_3\cdots E_{t-1}}{E_2E_4\cdots E_t}$$

$$= \frac{E_0E_1^{(i)}\bar{E}_1^{(i)}\cdots E_{t-1}^{(i)}\bar{E}_{t-1}^{(i)}}{E_2^{(i)}\bar{E}_2^{(i)}E_4^{(i)}\bar{E}_4^{(i)}\cdots E_t^{(i)}}\,.$$

So from (17)

$$E \equiv 1 \quad (\mathrm{mod.}\ \mathfrak{F}_{p_i})\,.$$

If t is odd we put

$$E = \frac{E_0E_1E_3\cdots E_t}{E_2E_4\cdots E_{t-1}}$$

$$= \frac{E_0E_1^{(i)}\bar{E}_1^{(i)}\cdots E_t^{(i)}}{E_2^{(i)}\bar{E}_2^{(i)}\cdots E_{t-1}^{(i)}\bar{E}_{t-1}^{(i)}}\,.$$

So from (17) we have

$$E \equiv 1 \quad (\mathrm{mod.}\ \mathfrak{F}_{p_i})\,.$$

As the above we have for any cases

$$E \equiv 1 \quad (\mathrm{mod.}\ \mathfrak{F}_{p_i})\ i = 1, 2, \cdots, t\,,$$

accordingly

$$E \equiv 1 \quad (\mathrm{mod.}\ \mathfrak{F}_n/(2))\,. \tag{18}$$

On the other hand we can show that $E \equiv E_0$ (mod. 2).
Put for brevity as the following

$$B = \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}$$

$$A = \frac{\zeta_8 - \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}{\zeta_8^3 + \zeta_4\zeta_{p_i}\cdots\zeta_{p_l}}\cdot\frac{\zeta_4\zeta_{p_i}\cdots\zeta_{p_l} - 1}{\zeta_4 - \zeta_{p_i}\zeta_{p_j}\cdots\zeta_{p_l}}\,.$$

Then

$$A-1 = \frac{\zeta_8 - B}{\zeta_8^3 + \zeta_4 B} \cdot \frac{\zeta_4 B - 1}{\zeta_4 - B} - 1$$

$$= \frac{(\zeta_8 - B)(\zeta_4 B - 1) - (\zeta_8^3 + \zeta_4 B)(\zeta_4 - B)}{(\zeta_8^3 + \zeta_4 B)(\zeta_4 - B)}$$

$$= \frac{\zeta_8\zeta_4 B - \zeta_8 - \zeta_4 B^2 + B - \zeta_8^3\zeta_4 + \zeta_8^3 B - \zeta_4^2 B + \zeta_4 B^2}{(\zeta_8^3 + \zeta_4 B)(\zeta_4 - B)}$$

$$= \frac{2B(1+\zeta_8^3)}{(\zeta_8^3 + \zeta_4 B)(\zeta_4 - B)} \equiv 0 \pmod{2}.$$

Namely

$$A \equiv 1 \pmod{2}$$

and so

$$\begin{cases} E_1 \equiv E_2 \equiv \cdots \equiv E_t \equiv 1 \pmod{2} \\ E \equiv E_0 \pmod{2}. \end{cases} \tag{19}$$

From the above formulas (16), (18), (19)

$$k\beta \equiv E \pmod{\mathfrak{F}_n}.$$

Now take once again according to S. Takahashi [5] a unit $E(k)$ in $Q(\zeta_n)$ satisfying the congruence equation $k \equiv E(k) \pmod{\mathfrak{F}_n}$, then we have the following congruence which is the desired result:

$$\beta = \frac{k\beta}{k} \equiv \frac{E}{E(k)} \pmod{\mathfrak{F}_n}$$

$$\mathfrak{A} \sim 1 \pmod{\mathfrak{F}_n} \text{ in } Q(\zeta_n).$$

REFERENCES

[1] T. TANNAKA, A generalised principal ideal theorem and a proof of a conjecture of Deuring, Ann. of Math., 67 (1958).

[2] F. TERADA, On a generalization of the principal ideal theorem, Tôhoku Math. Journ., (2) 1 (1949).

[3] T. TANNAKA, An alternative proof of a generalized principal ideal theorem, Proc. Japan Acad., 25 (1949).

[4] ————, On the generalized principal ideal theorem, Proc. of the international symposium on algebraic number theory, Tokyo-Nikoo, 1955.

[5] S. TAKAHASHI, An explicit representation of the generalized principal ideal theorem for the rational ground field, Tôhoku Math. Journ., 16, 2 (1964).

MATH. INSTITUTE
IWATE UNIVERSITY.