39. *On the General Principal Ideal Theorem*

By Katsuya MIYAKE
Department of Mathematics, College of General Education,
University of Nagoya

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1980)

By means of the theory of the module of genus, S. Iyanaga and Herbrand established the general principal ideal theorem in [4], [5] and [6]. In this paper, we prove the theorem in an improved form by an investigation of the structure of the idele groups [8].

1. Let k be an algebraic number field, $\mathfrak{m}$ a divisor of k, *which may contain Archimedian primes*, and K the ray class field modulo $\mathfrak{m}$ of k. Denote the conductor, the different and the module of genus of K over k by $\mathfrak{f}_{K/k}$, $\mathfrak{D}_{K/k}$ and $\mathfrak{F}_{K/k}$ respectively. Then as divisors of K, we have

$$\mathfrak{f}_{K/k}=\mathfrak{D}_{K/k}\cdot\mathfrak{F}_{K/k}.$$

For a prime ideal $\mathfrak{P}$ of K, let $e(\mathfrak{P})=e(\mathfrak{P}/k)$ be the order of ramification of $\mathfrak{P}$ over k, i.e.

$$\mathfrak{P}^{e(\mathfrak{P})}\,|\,(\mathfrak{P}\cap k)\cdot O_K, \quad \text{and} \quad \mathfrak{P}^{e(\mathfrak{P})+1}\nmid(\mathfrak{P}\cap k)\cdot O_K,$$

and put

$$\mathfrak{M}_{K/k}=\mathfrak{m}\cdot\mathfrak{D}_{K/k}^{-1}\cdot\prod_{\mathfrak{P}}\mathfrak{P}^{e(\mathfrak{P})-1}=\mathfrak{F}_{K/k}\cdot(\mathfrak{m}\cdot\mathfrak{f}_{K/k}^{-1})\cdot\prod_{\mathfrak{P}}\mathfrak{P}^{e(\mathfrak{P})-1}.$$

Our improved form of the general principal ideal theorem is

Theorem 1. *The extension of an ideal $\mathfrak{a}$ of k into K belongs to the principal ray class modulo $\mathfrak{M}_{K/k}$ if $\mathfrak{a}$ is relatively prime to $\mathfrak{m}$. In other words,*

$$\mathfrak{a}\cdot O_K=A\cdot O_K$$

with $A\in K^\times$ such that

$$A\equiv 1 \qquad \mathrm{mod}\,\mathfrak{M}_{K/k}.$$

Here O_K is the maximal order of K.

In [4] and [6], the general principal ideal theorem was proved for $\mathfrak{F}_{K/k}$ in place of $\mathfrak{M}_{K/k}$ of Theorem 1. Note that $\mathfrak{f}_{K/k}$ divides $\mathfrak{m}$.

2. Let $k_A^\times$ and $K_A^\times$ be the idele groups of k and K respectively, and, $k_\infty^\times$ and $K_\infty^\times$ the Archimedian parts of $k_A^\times$ and $K_A^\times$ respectively. Let $k_{\infty+}^\times$ be the connected component of the unity of $k_\infty^\times$, and $k^\#$ the closure of $k^\times\cdot k_{\infty+}^\times$ in $k_A^\times$. For a prime ideal $\mathfrak{p}$ of k, we denote the $\mathfrak{p}$-adic completion of k by $k_\mathfrak{p}$, the closure of the maximal order O_k in $k_\mathfrak{p}$ by $O_\mathfrak{p}$, and the unit group of $O_\mathfrak{p}$ by $O_\mathfrak{p}^\times$. For an Archimedian prime $\mathfrak{p}_\infty$, the completion of k at $\mathfrak{p}_\infty$ is denoted by $k_{\mathfrak{p}_\infty}$, and the connected component of the unity of $k_{\mathfrak{p}_\infty}^\times$ by $k_{\mathfrak{p}_\infty+}^\times$. For K, for a prime ideal $\mathfrak{P}$ of K, and for an Archimedian prime $\mathfrak{P}_\infty$ of K, we define $K_{\infty+}^\times$, $K^\#$, $K_\mathfrak{P}$, $O_\mathfrak{P}$, $O_\mathfrak{P}^\times$, $K_{\mathfrak{P}_\infty}$ and

$K^{\times}_{\mathfrak{P}_\infty +}$ in the same manner.

For a non-Archimedian prime factor $\mathfrak{p}$ of $\mathfrak{m}$, let $w=w(\mathfrak{p})$ be the exponent of $\mathfrak{p}$ in $\mathfrak{m}$, i.e.

$$\mathfrak{p}^w \mid \mathfrak{m}, \quad \text{and} \quad \mathfrak{p}^{w+1} \nmid \mathfrak{m}.$$

Similarly, for a non-Archimedian prime factor $\mathfrak{p}$ of the conductor $\mathfrak{f}_{K/k}$, let $u=u(\mathfrak{p})$ be the exponent of $\mathfrak{p}$ in $\mathfrak{f}_{K/k}$. Then

$$u(\mathfrak{p}) \leqq w(\mathfrak{p}).$$

Take a prime ideal $\mathfrak{P}$ of K lying over $\mathfrak{p}$, and denote by $N_{\mathfrak{P}}$ the norm map of $K_{\mathfrak{P}}$ over $k_{\mathfrak{p}}$. As is well known,

$u=u(\mathfrak{p})$ is the smallest integer such that

$$N_{\mathfrak{P}}(K^{\times}_{\mathfrak{P}}) \supset 1+\mathfrak{p}^u \cdot O_{\mathfrak{p}}.$$

Since K is the ray class field modulo $\mathfrak{m}$ of k, we have

$$(1) \qquad k^{\#} \cdot N_{K/k}(K^{\times}_A) = k^{\times} \times \prod_{\mathfrak{p}_\infty \nmid \mathfrak{m}} k^{\times}_{\mathfrak{p}_\infty} \times \prod_{\mathfrak{p}_\infty \mid \mathfrak{m}} k^{\times}_{\mathfrak{p}_\infty +} \times \prod_{\substack{\mathfrak{p} \nmid \mathfrak{m} \\ \text{non-Arch}}} O^{\times}_{\mathfrak{p}} \times \prod_{\substack{\mathfrak{p} \mid \mathfrak{m} \\ \text{non-Arch}}} (1+\mathfrak{p}^{w(\mathfrak{p})} \cdot O_{\mathfrak{p}}).$$

Here $N_{K/k}$ is the norm map of K over k. (See, for example, [7, Ch. 4, 7–3].)

3. For a non-Archimedian prime divisor $\mathfrak{P}$ of the module of genus $\mathfrak{F}_{K/k}$, let $v=v(\mathfrak{P})$ be the exponent of $\mathfrak{P}$ in $\mathfrak{F}_{K/k}$.

Proposition 1. *Let $\mathfrak{p}$ be a non-Archimedian prime divisor of $\mathfrak{f}_{K/k}$. Then every prime ideal $\mathfrak{P}$ of K lying over $\mathfrak{p}$ divides both of $\mathfrak{D}_{K/k}$ and $\mathfrak{F}_{K/k}$. Moreover, for each i ($v(\mathfrak{P}) \leqq i \leqq v(\mathfrak{P})+e(\mathfrak{P})-1$),*

$$N_{\mathfrak{P}}(1+\mathfrak{P}^i \cdot O_{\mathfrak{P}}) = 1+\mathfrak{p}^{u(\mathfrak{p})} \cdot O_{\mathfrak{p}}.$$

One can easily derive this proposition from [7, Ch. 5, Th. 2.1, Th. 2.2 and Ch. 2, Th. 7.3].

Remark. For $j=v(\mathfrak{P})+e(\mathfrak{P})$,

$$N_{\mathfrak{P}}(1+\mathfrak{P}^j \cdot O_{\mathfrak{P}}) = 1+\mathfrak{p}^{u(\mathfrak{p})+1} \cdot O_{\mathfrak{p}}.$$

Therefore this proposition characterizes $v(\mathfrak{P})+e(\mathfrak{P})-1$ as the maximal i such that

$$N_{\mathfrak{P}}(1+\mathfrak{P}^i \cdot O_{\mathfrak{P}}) = 1+\mathfrak{p}^{u(\mathfrak{p})} \cdot O_{\mathfrak{p}}.$$

The integer $v(\mathfrak{P})$ is the smallest among those v for which the higher ramification group $\mathfrak{g}_{V(v)}$ becomes trivial.

Proposition 2. *Let $\mathfrak{p}$ be a non-Archimedian prime divisor of $\mathfrak{m}$, and $\mathfrak{P}$ a prime ideal of K lying over $\mathfrak{p}$.*

(i) *If $\mathfrak{p} \mid \mathfrak{f}_{K/k}$, then $u(\mathfrak{p}) \leqq w(\mathfrak{p})$, and*

$$N_{\mathfrak{P}}(1+\mathfrak{P}^i \cdot O_{\mathfrak{P}}) = 1+\mathfrak{p}^{w(\mathfrak{p})} \cdot O_{\mathfrak{p}}$$

for every i such that

$$v(\mathfrak{P})+e(\mathfrak{P}) \cdot (w(\mathfrak{p})-u(\mathfrak{p})) \leqq i \leqq v(\mathfrak{P})+e(\mathfrak{P}) \cdot (w(\mathfrak{p})-u(\mathfrak{p})+1)-1.$$

(ii) *If $\mathfrak{p} \nmid \mathfrak{f}_{K/k}$, then $e(\mathfrak{P})=1$, and for any i,*

$$N_{\mathfrak{P}}(1+\mathfrak{P}^i \cdot O_{\mathfrak{P}}) = 1+\mathfrak{p}^i \cdot O_{\mathfrak{p}}.$$

As for (i), one can derive it from [7, Ch. 5, Th. 2.1] immediately. If $\mathfrak{p} \nmid \mathfrak{f}_{K/k}$, then $\mathfrak{p}$ is unramified in K over k. Therefore, (ii) is clear.

4. For a prime ideal $\mathfrak{P}$ of K, let $\mathfrak{p}=\mathfrak{P}\cap k$, and put

$$x(\mathfrak{P})=v(\mathfrak{P})+e(\mathfrak{P})\cdot(w(\mathfrak{p})-u(\mathfrak{p})+1)-1.$$

Then $\mathfrak{M}_0=\prod_{\mathfrak{P}}\mathfrak{P}^{x(\mathfrak{P})}$ is the non-Archimedian part of $\mathfrak{M}_{K/k}$ defined in § 1. Let $\mathfrak{M}_\infty$ be the Archimedian part of $\mathfrak{M}_{K/k}$.

Theorem 2. *Let the notation and the assumptions be as above. Then naturally considered as a subgroup of $K_A^\times$, the idele group $k_A^\times$ is contained in*

$$(*)\qquad K^\times\times\prod_{\mathfrak{P}_\infty\nmid\mathfrak{M}_\infty}K_\infty^\times\times\prod_{\mathfrak{P}_\infty\mid\mathfrak{M}_\infty}K_{\infty+}^\times\times\prod_{\mathfrak{P}\nmid\mathfrak{M}_0}O_{\mathfrak{P}}^\times\times\prod_{\mathfrak{P}\mid\mathfrak{M}_0}(1+\mathfrak{P}^{x(\mathfrak{P})}\cdot O_{\mathfrak{P}}).$$

This is just the adelic version of Theorem 1. Therefore it is sufficient to prove this theorem.

Proof. Let U be the subgroup of $K_A^\times$ defined by (*). It follows from (1) in § 2 and Proposition 2 that

$$k^\#\cdot N_{K/k}(K_A^\times)=k^\#\cdot N_{K/k}(U).$$

Therefore we have

$$K_A^\times=N_{K/k}^{-1}(k^\#)\cdot U.$$

Because U is an open subgroup of finite index of $K_A^\times$, we also have $U\supset K^\#$. We see easily from the definition that

$$U^\sigma=U\qquad\text{for any }\sigma\in\mathrm{Gal}\,(K/k).$$

The theorem now follows from the next proposition, which is proved in [8] as Theorem 2 by the results of E. Artin [1] and Furtwängler [3].

Proposition 3. *Let k be an algebraic number field and K a finite Galois extension of k. If an open subgroup U of $K_A^\times$ satisfies*

(i) $U\supset K^\#$,

(ii) $U^\sigma=U$ *for any* $\sigma\in\mathrm{Gal}\,(K/k)$,

(iii) $U\cdot N_{K/k}^{-1}(k^\#)=K_A^\times$,

then we have $U\supset k_A^\times$.

5. **Remark.** For the ray class field K modulo $\mathfrak{m}$ of k, fix a non-Archimedian prime factor $\mathfrak{p}$ of $\mathfrak{m}$, and put $w=w(\mathfrak{p})$. Let $\mathfrak{P}$ be a prime ideal of K lying over $\mathfrak{p}$. Then

$$O_{\mathfrak{p}}^\times\cap k^\#\cdot N_{K/k}(K_A^\times)=N_{\mathfrak{P}}(O_{\mathfrak{P}}^\times)$$

is the subgroup of $O_{\mathfrak{p}}^\times$ generated by the elements of $1+\mathfrak{p}^w\cdot O_{\mathfrak{p}}$ and all those (global) units ε of k which satisfies

$$\varepsilon\equiv1\qquad\mathrm{mod}\ \mathfrak{p}^{-w}\cdot\mathfrak{m}.$$

Therefore if $\mathfrak{p}^{-w}\cdot\mathfrak{m}$ is suitably chosen for the fixed $\mathfrak{p}^w$, then

$$N_{\mathfrak{P}}(O_{\mathfrak{P}}^\times)=1+\mathfrak{p}^w\cdot O_{\mathfrak{p}}.$$

(See Chevalley [2].) If this is the case, then $u(\mathfrak{p})=w(\mathfrak{p})=w$, and we have

$$e(\mathfrak{P})=e(\mathfrak{P}/k)=[O_{\mathfrak{p}}^\times:1+\mathfrak{p}^w\cdot O_{\mathfrak{p}}]=(q-1)\cdot q^{w-1},$$
$$v(\mathfrak{P})=e(\mathfrak{P})\cdot(q-1)^{-1}=q^{w-1},$$
$$v(\mathfrak{P})+e(\mathfrak{P})-1=q^w-1,$$

where $q=\#(O_{\mathfrak{p}}/\mathfrak{p}\cdot O_{\mathfrak{p}})$. (See [7, Ch. 5, Th. 2.1 and Ch. 2, Th. 7.3], or Weil [9, XII–4, Cor. of Prop. 13].)

References

[1] E. Artin: Idealklassen in Oberkörpern und allgemeine Reziprozitätsgesetze. Abh. Math. Sem. Hamburg, **7** (1930).

[2] C. Chevalley: Deux théorèmes d'arithmétique. J. Math. Soc. Japan, **3** (1951).

[3] Ph. Furtwängler: Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper. Abh. Math. Sem. Hamburg, **7** (1930).

[4] J. Herbrand: Sur les théorèmes du genre principal et des ideaux principaux. Ibid., **9** (1933).

[5] S. Iyanaga: Über den allgemeinen Hauptidealsatz. Jap. J. Math., **7** (1930).

[6] ——: Zur Theorie der Geschlechtermoduln. J. reine angew. Math., **177** (1934).

[7] —— (ed.): The Theory of Numbers. North-Holland (1975).

[8] K. Miyake: On the structure of the idele group of an algebraic number field (to appear in Nagoya Math. J., **80** (1980)).

[9] A. Weil: Basic Number Theory. Springer Verlag (1967).