TOKYO J. MATH.
VOL. 2, NO. 2, 1979

# Representation of Witt Vectors by Formal Power Series and its Applications

Kiyomi KANESAKA and Koji SEKIGUCHI

*Sophia University*

(Communicated by Y. Kawada)

## Introduction

In this paper we consider a representation of Witt vectors and its application to the Inaba theory of the construction of Galois extensions of a field of characteristic $p$ and to the explicit formula for the residue vectors in the formal power series field.

E. Artin and O. Schreier characterized any cyclic extension $L$ of order $p$ of a field $K$ of characteristic $p>0$ by a root $\alpha$ of the equation $x^p=x+\mu$: $L=K(\alpha)$. Thereafter E. Witt [10] has extended this method to any cyclic $p$-extension $L$ of $K$ by considering Witt vectors: $L=K(\alpha)$, $\alpha^p=\alpha+\mu$. On the other hand, E. Inaba [4, 5, 6] expressed any finite Galois extension $L$ of $K$ of characteristic $p$ by the matrix equation of the type $X^p=MX$, $M\in GL_m(K)$. We define in §1 an isomorphism $\mathfrak{f}_u$ of the additive group $W_\infty(K)$ of Witt vectors into the multiplicative 1-unit group of the formal power series ring $K[[t]]$: $\mathfrak{f}_u(\alpha+\alpha')=\mathfrak{f}_u(\alpha)\cdot\mathfrak{f}_u(\alpha')$.* As an application we consider in §2 the relation between the Witt theory and the Inaba theory.

Y. Kawada and I. Satake [7] applied the residue vectors defined in Witt [10] to the class formation theory over a formal power series field $K$ in one variable with a finite constant field. In §3 we calculate the residue vectors by the use of the mapping $\mathfrak{f}_u$ defined in §1. Using these results, we consider in §4 the orthogonal pairings and the duality defined by residue vectors. In §5 we consider the formal power series field $K$ in one variable with a finite constant field and the cyclic extension field $L$ of order $p^n$ over $K$. We calculate the ramification index and the conductor of $L$ over $K$.

The authors wish to express their thanks to Professor Yukiyosi

Received May 12, 1978
Revised July 1, 1979

* See also Dieudonné [1] and Whaples [8].

Kawada and Mr. Teluhiko Hilano.

## §1. Isomorphism of the additive group of Witt vectors into the multiplicative unit group of the formal power series ring.

**1.1.** Let $p$ be a prime number, $I_p$ the $p$-adic valuation ring of the rational numbers field $\boldsymbol{Q}$ and $\boldsymbol{Q}[[x]]$ the formal power series ring over $\boldsymbol{Q}$. Then we define

$$G(x)=\exp\left(\sum_{i=0}^{\infty}\frac{1}{p^i}x^{p^i}\right)\in\boldsymbol{Q}[[x]]\,. \tag{1.1}$$

LEMMA 1. *The coefficients $d_n(n\in\boldsymbol{Z})$ of $x^n$ of $G(x)$ satisfy the following recursive relations:*

$$\begin{cases} d_n=0 & (n<0) \\ d_0=1 & \\ d_n=\dfrac{1}{n}\displaystyle\sum_{i=0}^{\infty}d_{n-p^i} & (n>0)\,. \end{cases} \tag{1.2}$$

PROOF. Taking the formal derivation of (1.1), we have

$$G'(x)=\left(\sum_{i=0}^{\infty}\frac{1}{p^i}x^{p^i}\right)'G(x)\,.$$

Hence

$$\sum_{n=1}^{\infty}nd_nx^{n-1}=\left(\sum_{i=0}^{\infty}x^{p^i-1}\right)\left(\sum_{n=0}^{\infty}d_nx^n\right)\,. \tag{1.3}$$

Comparing the coefficients of $x^{n-1}$ in both sides of (1.3), we obtain

$$nd_n=d_{n-1}+d_{n-p}+d_{n-p^2}+\cdots\,. \qquad \text{Q.E.D.}$$

LEMMA 2. *All the coefficients of $G(x)$ are contained in $I_p$,* i.e., $G(x)\in I_p[[x]]$.*)

PROOF. We shall show $d_n\in I_p$ by induction on $n$. By (1.2), it is sufficient to show $d_n\in I_p$ for $n\geqq 1$ satisfying $p\,|\,n$. By (1.1), we have

$$G(x)^p=\exp\left(p\sum_{i=0}^{\infty}\frac{1}{p^i}x^{p^i}\right)\,.$$

Hence

$$G(x)^p=G(x^p)\exp(px)\,. \tag{1.4}$$

*) We owe Mr. T. Hilano for this proof.

Comparing the coefficients of $x^n$ in both sides of (1.4), we obtain

$$pd_n + p\cdot f(d_0, \cdots, d_{n-1}) + d_{n/p}^p = d_{n/p} + p \sum_{i+pj=n, i\geq 1} \frac{p^{i-1}}{i!} d_j ,$$

where $f(d_0, \cdots, d_{n-1})$ is a polynomial of $d_0, \cdots, d_{n-1}$ with integer coefficients. Hence

$$d_n = -f(d_0, \cdots, d_{n-1}) - \frac{1}{p}(d_{n/p}^p - d_{n/p}) + \sum_{\substack{i+pj=n \\ i\geq 0}} \frac{p^{i-1}}{i!} d_j .$$

Since $d_{n/p}^p - d_{n/p} \in pI_p$ and $p^{i-1}/i! \in I_p$, by our assumption we have $d_n \in I_p$.
Q.E.D.

Let $D$ be an integral domain containing $I_p$, $t$ an indeterminate element over $D$, $W_\infty(D)$ the ring of Witt vectors of infinite length over $D$ and $U^{(1)}(D[[t]])$ the 1-unit group of $D[[t]]$: $U^{(1)}(D[[t]]) = 1 + tD[[t]]$. For any element $u \in tD[[t]]$ and any Witt vector $X = (X_0, X_1, \cdots) \in W_\infty(D)$, we define

$$\mathfrak{F}_u(X) = \prod_{j=0}^{\infty} G(X_j u^{p^j}) . \tag{1.5}$$

$\mathfrak{F}_u(X)$ belongs to $U^{(1)}(D[[t]])$ by Lemma 2.

LEMMA 3.

$$\mathfrak{F}_u(X) = \exp\left(\sum_{i=0}^{\infty} \frac{X^{(i)}}{p^i} u^{p^i}\right) \tag{1.6}$$

*where $X^{(i)}$ is the i-th ghost component of $X$: $X^{(i)} = \sum_{j=0}^{i} p^j X_j^{p^{i-j}}$. (See Witt* [10].)

PROOF.

$$\begin{aligned}\mathfrak{F}_u(X) &= \prod_{j=0}^{\infty} G(X_j u^{p^j}) = \prod_{j=0}^{\infty} \exp\left(\sum_{i=0}^{\infty} \frac{1}{p^i}(X_j u^{p^j})^{p^i}\right) \\ &= \exp\left(\sum_{j=0}^{\infty} \sum_{i=j}^{\infty} p^{j-i} X_j^{p^{i-j}} u^{p^i}\right) \\ &= \exp\left(\sum_{i=0}^{\infty} \sum_{j=0}^{i} p^{j-i} X_j^{p^{i-j}} u^{p^i}\right) \\ &= \exp\left(\sum_{i=0}^{\infty} \frac{X^{(i)}}{p^i} u^{p^i}\right) .\end{aligned}$$

Q.E.D.

PROPOSITION 1. *The mapping $\mathfrak{F}_u$ $(u \neq 0)$ is an isomorphism of the additive group of $W_\infty(D)$ into the multiplicative group $U^{(1)}(D[[t]])$.*

PROOF. By (1.6), we have

$$\begin{aligned}\mathfrak{F}_u(X+X')&=\exp\left(\sum_{i=0}^{\infty}\frac{(X+X')^{(i)}}{p^i}u^{p^i}\right)\\&=\exp\left(\sum_{i=0}^{\infty}\frac{X^{(i)}+X'^{(i)}}{p^i}u^{p^i}\right)\\&=\mathfrak{F}_u(X)\mathfrak{F}_u(X')\qquad\text{for}\quad X,X'\in W_\infty(D)\,.\end{aligned}$$

If $\mathfrak{F}_u(X)=1$, then $\sum_{i=0}^{\infty}(X^{(i)}/p^i)u^{p^i}=0$. Hence we have $X=0$. Q.E.D.

Moreover, we have

$$\mathfrak{F}_u(VX)=\mathfrak{F}_{u^p}(X) \tag{1.7}$$

where $VX=(0, X_0, X_1, \cdots)$ for $X=(X_0, X_1, \cdots)\in W_\infty(D)$. For, we have

$$\begin{aligned}\mathfrak{F}_u(VX)&=\prod_{j=0}^{\infty}G((VX)_j u^{p^j})\\&=\prod_{j=1}^{\infty}G(X_{j-1}(u^p)^{p^{j-1}})\\&=\mathfrak{F}_{u^p}(X)\,.\end{aligned}$$

For any integer $i$, choose a positive integer $m$ such that $i<p^m$. Then for $X=(X_0, X_1, \cdots)\in W_\infty(D)$ we define

$$h_i(X)=\sum d_{i_0}\cdots d_{i_{m-1}}X_0^{i_0}\cdots X_{m-1}^{i_{m-1}} \tag{1.8}$$

where the summation is extended over all systems $\{i_0, \cdots, i_{m-1}\}$ of integers satisfying $i_0+i_1p+\cdots+i_{m-1}p^{m-1}=i$. Since $d_n=0$ for $n<0$, we can verify that $h_i$ is unchanged when we change $m$ under the condition $i<p^m$ for fixed $i$. Further $h_n(X)=0$ $(n<0)$, $h_0(X)=1$ and $h_1(X)=X_0$. Then we have obviously by (1.5)

$$\mathfrak{F}_u(X)=\sum_{i=0}^{\infty}h_i(X)u^i\,. \tag{1.9}$$

Hence we have

$$\mathfrak{F}_u(X)\equiv 1+X_0u \pmod{u^2}\,. \tag{1.10}$$

By Proposition 1 and (1.9) we can easily see that

$$h_i(X+X')=\sum_{j=0}^{i}h_j(X)h_{i-j}(X')\qquad\text{for}\quad X,X'\in W_\infty(D)\,. \tag{1.11}$$

LEMMA 4. *For $u\neq 0$ $m\geqq 1$ and $n\geqq 0$, the following two conditions are equivalent:*

(i) $m \leqq p^n \operatorname{ord} u$

(ii) $\mathfrak{F}_u(V^n W_\infty(D)) \subset U^{(m)}(D[[t]])$

*where* $U^{(m)}(D[[t]]) = 1 + t^m D[[t]]$.

PROOF. By (1.7) and (1.10), we have

$$\mathfrak{F}_u(V^n X) = \mathfrak{F}_{u^{p^n}}(X) = 1 + X_0 u^{p^n} + \cdots .$$

Hence (i) and (ii) are equivalent.

COROLLARY. *$\mathfrak{F}_u$ is a continuous mapping from $W_\infty(D)$ into $U^{(1)}(D[[t]])$.*

**1.2.** Let $K$ be a field of characteristic $p$, $\boldsymbol{F}_p$ the prime field of $K$ and $t$ an indeterminate element over $K$. We denote by $U^{(1)}(K[[t]])$ the 1-unit group of $K[[t]]$. For any element $u \in tK[[t]]$ and any Witt vector $\alpha = (\alpha_0, \alpha_1, \cdots) \in W_\infty(K)$, we define

$$(1.1)' \qquad \bar{G}(x) = \textstyle\sum_{n=0}^{\infty} \bar{d}_n x^n \in \boldsymbol{F}_p[[x]] \quad \text{for } \bar{d}_n = d_n (\mathrm{mod}\ p) \in \boldsymbol{F}_p$$

and

$$(1.5)' \qquad \mathfrak{f}_u(\alpha) = \textstyle\prod_{j=0}^{\infty} \bar{G}(\alpha_j u^{p^j}) \in U^{(1)}(K[[t]]).$$

PROPOSITION 1$'$. *The mapping $\mathfrak{f}_u$ $(u \neq 0)$ is an isomorphism of the additive group of $W_\infty(K)$ into the multiplicative group $U^{(1)}(K[[t]])$.*

PROOF. Let $D$ be an arbitrary integral domain containing $I_p$ such that there exists a ring homomorphism $\pi$ of $D$ onto $K$. For $X = (X_0, X_1, \cdots) \in W_\infty(D)$ we define $W_\infty(\pi)(X) = (\pi X_0, \pi X_1, \cdots) \in W_\infty(K)$, and for $Y = \sum_{i=0}^{\infty} Y_i t^i \in D[[t]]$ we define $\pi_t(Y) = \sum_{i=0}^{\infty} \pi(Y_i) t^i \in K[[t]]$. Then we have the following commutative diagram:

$$(1.12) \qquad \begin{array}{ccc} W_\infty(D) & \xrightarrow{\ \mathfrak{F}_u\ } & U^{(1)}(D[[t]]) \\ {\scriptstyle W_\infty(\pi)} \downarrow & \circlearrowright & \downarrow {\scriptstyle \pi_t} \\ W_\infty(K) & \xrightarrow[\ \mathfrak{f}_u\ ]{} & U^{(1)}(K[[t]]) \end{array} .$$

If $\mathfrak{f}_u(\alpha) = 1$, then $\pi_t \circ \mathfrak{F}_u(X) = 1$ for any Witt vector $X \in W_\infty(D)$ such that $W_\infty(\pi)(X) = \alpha$. By (1.9) we have $h_i(X) \in \operatorname{Ker} \pi$ for $i \geqq 1$ and so $X_j \in \operatorname{Ker} \pi$ for $j \geqq 0$. Therefore we obtain $\alpha = 0$. Hence $\mathfrak{f}_u$ is an into-isomorphism.

By (1.7), (1.9), (1.10), Lemma 4 , Corollary and (1.12) we have

$$(1.7)' \qquad \mathfrak{f}_u(V\alpha) = \mathfrak{f}_{u^p}(\alpha)$$

(1.9)′ $$\mathfrak{f}_u(\alpha)=\sum_{i=0}^{\infty}\bar{h}_i(\alpha)u^i$$

(1.10)′ $$\mathfrak{f}_u(\alpha)\equiv 1+\alpha_0 u \pmod{u^2}\ .$$

LEMMA 4′. *For $u\neq 0$, $m\geqq 1$ and $n\geqq 0$, the following two conditions are equivalent:*

(i) $m\leqq p^n \operatorname{ord} u$

(ii) $\mathfrak{f}_u(V^n W_\infty(K))\subset U^{(m)}(K[[t]])$.

COROLLARY′. *$\mathfrak{f}_u$ is a continuous mapping from $W_\infty(K)$ into $U^{(1)}(K[[t]])$.*

Moreover, we have

(1.13) $$\mathfrak{f}_u(a\alpha)=\mathfrak{f}_u(\alpha)^a \quad \text{for} \quad a\in W_\infty(F_p),\ \alpha\in W_\infty(K)\ .$$

Since $\mathfrak{f}_u(n\alpha)=\mathfrak{f}_u(\alpha)^n$ holds for $n\in \boldsymbol{Z}$, by Proposition 1′ and $\mathfrak{f}_u$ is continuous, we have (1.13).

## §2. Application to the Inaba theory on the construction of Galois extensions.

**2.1.** The isomorphic representation of the additive group of Witt vectors of length $n$ by matrices.

We denote by $W_n(K)$ the ring of Witt vectors of length $n$ over a field $K$ of characteristic $p>0$. Then we have the ring-isomorphism

(2.1) $$W_n(K)\cong W_\infty(K)/V^n W_\infty(K)$$

where $V\alpha=(0, \alpha_0, \alpha_1, \cdots)$ for $\alpha=(\alpha_0, \alpha_1, \cdots)\in W_\infty(K)$. For $m\geqq 2$ consider the set

$$B_m(K)=\left\{B\in M_m(K)\ \middle|\ B=\begin{pmatrix} 1 & b_1 & b_2 & \cdots & b_{m-1} \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & b_2 \\ & 0 & & \ddots & b_1 \\ & & & & 1 \end{pmatrix}\right\}.$$

Then $B_m(K)$ is a subgroup of $GL_m(K)$. We denote such a matrix $B\in B_m(K)$ by $B=[1, b_1, b_2, \cdots, b_{m-1}]$. Put

$$U^{(i)}=U^{(i)}(K[[t]])=1+t^i K[[t]] \quad \text{for} \quad i\geqq 1\ .$$

Then we have the group-isomorphism

(2.2) $$\varphi\colon B_m(K)\cong U^{(1)}/U^{(m)}$$

where $B=[1, b_1, b_2, \cdots, b_{m-1}] \in B_m(K)$ is mapped to the residue class containing $1+b_1t+b_2t^2+\cdots+b_{m-1}t^{m-1} \in U^{(1)}$ by $\varphi$.

LEMMA 5. *For* $u \in tK[[t]]$, $n \geqq 1$ *and* $m \geqq 1$ *satisfying* $(\mathrm{ord}\, u)p^{n-1}+1 \leqq m \leqq (\mathrm{ord}\, u)p^n$, *we can define the mapping* $\mathfrak{f}_u^{(n)}$ *satisfying the following commutative diagram:*

$$(2.3)\qquad \begin{array}{ccc} W_\infty(K) & \xrightarrow{\quad \mathfrak{f}_u \quad} & U^{(1)}(K[[t]]) \\ \text{canonical} \downarrow & \circlearrowright & \downarrow \text{canonical} \\ W_n(K) & \xrightarrow[\quad \mathfrak{f}_u^{(n)} \quad]{} & B_m(K) \end{array}$$

*where* $\mathfrak{f}_u$ *is the mapping defined by* (1.5)′ *in* §1. *Moreover, the mapping* $\mathfrak{f}_u^{(n)}$ *is injective. Hence the mapping* $\mathfrak{f}_u^{(n)}$ *is an isomorphism of the additive group of* $W_n(K)$ *into the multiplicative group* $B_m(K)$.

PROOF. By Lemma 4′, we have $\mathfrak{f}_u(V^n W_\infty(K)) \subset U^{(m)}$. Hence we can define the mapping $\mathfrak{f}_u^{(n)}$ with the above property. It is clear that $\mathfrak{f}_u^{(n)}$ is injective if $(\mathrm{ord}\, u)p^{n-1}+1 \leqq m$. Q.E.D.

**2.2.** Relation between the Witt theory and the Inaba theory.

In this section we shall consider the relation between the Witt theory [10] and the Inaba theory [4, 5, 6] by the use of the mapping $\mathfrak{f}_u^{(n)}$ defined by (2.3). In the Witt theory we have the following theorem:

THEOREM (*). *Let* $K$ *be a field of characteristic* $p>0$, $L \supset K$ *an abelian extension whose Galois group* $G=\mathrm{Gal}\,(L|K)$ *is cyclic of order* $p^n$ *and* $\chi$ *an isomorphic representation of* $G$ *onto* $W_n(F_p)$. *Then there exists a vector* $\alpha=(\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \in W_n(L)$ *such that* $\wp_w \alpha = P\alpha - \alpha = \mu \in W_n(K)$, $L=K(\alpha)$ *and* $\sigma\alpha = \alpha + \chi(\sigma)$ *for* $\sigma \in G$, *where* $\sigma\alpha = (\sigma\alpha_0, \sigma\alpha_1, \cdots, \sigma\alpha_{n-1})$, $P\alpha = (\alpha_0^p, \alpha_1^p, \cdots, \alpha_{n-1}^p)$ *and* $K(\alpha)=K(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$.

On the other hand, in the Inaba theory we have the following theorem:

THEOREM (**). *Let* $K$ *be a field of characteristic* $p>0$, $L \supset K$ *a finite Galois extension whose Galois group is* $G=\mathrm{Gal}\,(L|K)$ *and* $\Lambda$ *an isomorphic representation of* $G$ *into* $GL_m(F_p)$. *Then there exists a matrix* $A=(a_{ij}) \in GL_m(L)$ *such that* $\wp_I A = PA \cdot A^{-1} = M \in GL_m(K)$, $L=K(A)$ *and* $\sigma A = A \cdot \Lambda(\sigma)$ *for* $\sigma \in G$, *where* $\sigma A = (\sigma a_{ij})$, $PA=(a_{ij}^p)$, *and* $K(A)= K(a_{11}, \cdots, a_{ij}, \cdots, a_{mm})$.

When $L \supset K$ is a cyclic extension of order $p^n$ and the range of $\Lambda$ in

Theorem (**) is $B_m(F_p)$ where $p^{n-1}+1\leqq m\leqq p^n$, we shall consider the relation between Theorem (*) and Theorem (**).

Theorem (*) $\Rightarrow$ Theorem (**)

Let $L\supset K$ be a cyclic extension of order $p^n$ and $\Lambda$ an isomorphic representation of $G$ into $B_m(F_p)$. For a generator $\sigma_0$ of $G$, we put

$$\Lambda(\sigma_0)=[1, \lambda_1, \cdots, \lambda_{m-1}] \quad \text{and} \quad l=\min\{i\geqq 1 \mid \lambda_i\neq 0\} .$$

Since the order of $\Lambda(\sigma_0)$ is $p^n$, we have $l\cdot p^{n-1}<m$. We determine an isomorphic representation $\chi$ of the cyclic group of order $p^n$ such that $\chi(\sigma_0)=1\in W_n(F_p)$. Then by Theorem (*), there exists a vector $\alpha\in W_n(L)$ such that $\wp_w\alpha=\mu\in W_n(K)$, $L=K(\alpha)$ and $\sigma_0\alpha=\alpha+1$. On the other hand, the mapping $\bar{G}$ defined by (1.1)$'$ of $tF_p[[t]]$ to $U^{(1)}(F_p[[t]])$ is bijective. Hence there is an element $u\in tF_p[[t]]$ such that $\Lambda(\sigma_0)=\bar{G}(u) \bmod U^{(m)}=\mathfrak{f}_u^{(n)}(1)$. Since $\operatorname{ord} u=l$, by Lemma 5, the mapping $\mathfrak{f}_u^{(n)}$ is an isomorphism. If we put $\mathfrak{f}_u^{(n)}(\alpha)=A\in B_m(L)$ and $\mathfrak{f}_u^{(n)}(\mu)=M\in B_m(K)$, then $\wp_I A=M$, $L=K(A)$ and $\sigma A=A\cdot\Lambda(\sigma)$ for $\sigma\in G$. Q.E.D.

Theorem (**) $\Rightarrow$ Theorem (*)

Let $L\supset K$ be a cyclic extension of order $p^n$ and $\chi$ an isomorphic representation of $G$ onto $W_n(F_p)$. Then there exists a generator $\sigma_0$ of $G$ such that $\chi(\sigma_0)=1$. For $p^{n-1}+1\leqq m\leqq p^n$, we define the mapping $\Lambda=\mathfrak{f}_t^{(n)}\circ\chi$ of $G$ into $B_m(F_p)$. Then the mapping $\Lambda$ is an isomorphic representation of $G$ and $\Lambda(\sigma_0)=[1, \bar{d}_1, \bar{d}_2, \cdots, \bar{d}_{m-1}]$ where $d_1, d_2, \cdots$ are defined by (1.2) in §1 and $\bar{d}_n=d_n \pmod p)\in F_p$. By Theorem (**) there exists a matrix $A\in B_m(L)$ such that $\wp_I A=M\in B_m(K)$, $L=K(A)$ and $\sigma A=A\cdot\Lambda(\sigma)$ for $\sigma\in G$. Now if we put $A'=AC$ for $C\in B_m(K)$, then $\wp_I A'=M'\in B_m(K)$, $L=K(A')$ and $\sigma A'=A'\cdot\Lambda(\sigma)$ for $\sigma\in G$. On the other hand, in Galois cohomology theory we have the following lemma:

LEMMA (*). *Let $L\supset K$ be a finite Galois extension whose Galois group is $G=\mathrm{Gal}(L\mid K)$. Then the 1-cohomology group of $G$ over $W_n(L)$ is trivial:*

$$H^1(G, W_n(L))=0 \qquad (\textit{see Witt } [9]) .$$

Since $\chi$ is an isomorphism of $G$ onto $W_n(F_p)$, by Lemma (*), there exists a vector $\alpha\in W_n(L)$ such that $\chi(\alpha)=\sigma(\alpha)-\alpha$ for $\sigma\in G$. In particular, since $\chi(\sigma_0)=1$, $\sigma_0(\alpha)=\alpha+1$.

LEMMA 6. *For $1\leqq l\leqq m-1$ there exists a matrix $C(l)\in B_m(K)$ such that $A\cdot C(l)=[1, \bar{h}_1(\alpha), \bar{h}_2(\alpha), \cdots, \bar{h}_l(\alpha), a_l', \cdots]$ where $h_i$ is defined by* (1.8) *in* §1.

PROOF. We shall prove the existence of $C(l)$ by induction on $l$. In case $l=1$ by $\sigma_0 A = A\cdot\Lambda(\sigma_0)$, we have $\sigma(a_1-\bar{h}_1(\alpha))=a_1-\bar{h}_1(\alpha)$. Namely, there exists an element $c_1\in K$ such that $\bar{h}_1(\alpha)=a_1+c_1$. Hence put $C(1)=[1, c_1, 0, \cdots, 0]\in B_m(K)$, we have $A\cdot C(1)=[1, \bar{h}_1(\alpha), a_2', \cdots]$. Let us assume that this lemma is valid for $l-1$. Then there exists $C(l-1)\in B_m(K)$ such that $A\cdot C(l-1)=[1, \bar{h}_1(\alpha), \cdots, \bar{h}_{l-1}(\alpha), a_l', \cdots]$. Put $A'=A\cdot C(l-1)$. Since $\sigma_0 A'=A'\cdot\Lambda(\sigma_0)$ and $\bar{h}_l(\alpha+1)=\sum_{j=0}^{l}\bar{h}_j(\alpha)\bar{h}_{l-j}(1)$ by (1.11), we have $\sigma(a_l'-\bar{h}_l(\alpha))=a_l'-\bar{h}_l(\alpha)$. Hence there exists an element $c_l\in K$ such that $\bar{h}_l(\alpha)=a_l'+c_l$. Now if we put $C(l)=C(l-1)[\underbrace{1, 0, \cdots, 0}_{l}, c_l, 0, \cdots, 0]$, then we have $A\cdot C(l)=[1, \bar{h}_1(\alpha), \bar{h}_2(\alpha), \cdots, \bar{h}_l(\alpha), a_{l+1}'\cdots]$. In particular, if we put $C(m-1)=C$, then we have $AC=[1, \bar{h}_1(\alpha), \bar{h}_2(\alpha), \cdots, \bar{h}_{m-1}(\alpha)]=\mathfrak{f}_t^{(n)}(\alpha)$. Hence we have $\wp_w\alpha=\mu\in W_n(K)$, $L=K(\alpha)$ and $\sigma\alpha=\alpha+\chi(\sigma)$ for $\sigma\in G$.

Q.E.D.

SIMPLE EXAMPLES.

1. If $L\supset K$ is cyclic of order $p$ and $\Lambda(\sigma_0)=[1, 1, 1/2!, \cdots, 1/(p-1)!]\in B_p(F_p)$ where $\sigma_0$ is a generator of $G$, then we have

$$\begin{cases} M=\left[1, \mu_0, \dfrac{\mu_0^2}{2!}, \cdots, \dfrac{\mu_0^{p-1}}{(p-1)!}\right]\in B_p(K) \\ A=\left[1, \alpha_0, \dfrac{\alpha_0^2}{2!}, \cdots, \dfrac{\alpha_0^{p-1}}{(p-1)!}\right]\in B_p(L) \end{cases}$$

where $\alpha_0^p=\alpha_0+\mu_0$ and $\sigma_0\alpha_0=\alpha_0+1$.

2. If $L\supset K$ is cyclic of order $p^n$ and $\Lambda(\sigma_0)=[1, \bar{d}_1, \bar{d}_2, \cdots, \bar{d}_{m-1}]\in B_m(F_p)$ where $\sigma_0$ is a generator of $G$ and $p^{n-1}+1\leqq m\leqq p^n$, then we have

$$\begin{cases} M=[1, \bar{h}_1(\mu), \bar{h}_2(\mu), \cdots, \bar{h}_{m-1}(\mu)]\in B_m(K) \\ A=[1, \bar{h}_1(\alpha), \bar{h}_2(\alpha), \cdots, \bar{h}_{m-1}(\alpha)]\in B_m(L) \end{cases}$$

where $\wp_w\alpha=\mu$ and $\sigma_0\alpha=\alpha+1$.

REMARK. If $m=p^n$, then $\{1, \bar{h}_1(\alpha), \bar{h}_2(\alpha), \cdots, \bar{h}_{p^n-1}(\alpha)\}$ is a base of $L$ over $K$: $L=\bigoplus_{i=0}^{p^n-1}K\bar{h}_i(\alpha)$.

## §3. Calculation of the residue vectors.

Let $D$ be an integral domain of characteristic 0 and $t$ an indeterminate element over $D$. For $Y\in D((t))$, $Y\neq 0$ and $Z\in W_\infty(D((t)))$, the residue vector $(Y, Z)$ is defined as

$$(3.1)\qquad (Y, Z)^{(n)}=\mathrm{res}\left(\frac{dY}{Y}Z^{(n)}\right)\qquad (n\geqq 0)$$

where $Z^{(n)}$ and $(Y, Z)^{(n)}$ are $n$-th ghost components of $Z$ and $(Y, Z)$, respectively (see Witt [10]).

LEMMA 7. *Let $D$ contain $I_p$, $j\geqq 1$, $m\geqq 1$ and $(j, p)=(m, p)=1$. Let $Y=\mathfrak{F}_{t^j}(X)$ for $X\in W_\infty(D)$ where $\mathfrak{F}_{t^j}$ is defined by* (1.5) *and $Z=\{t^{-m}\}=(t^{-m}, 0, 0, \cdots)$. Then we have*

$$(Y, Z)=\begin{cases} jX & (m=j)\\ 0 & (m\neq j)\ .\end{cases}$$

PROOF. Using the formula (1.6) we have

$$\frac{d\mathfrak{F}_u(X)}{du}=\left(\sum_{i=0}^{\infty}X^{(i)}u^{p^i-1}\right)\cdot\mathfrak{F}_u(X)\ .$$

Therefore

$$\frac{1}{Y}\frac{dY}{dt}=\frac{1}{Y}\frac{dY}{dt^j}\frac{dt^j}{dt}=\left(\sum_{i=0}^{\infty}X^{(i)}(t^j)^{p^i-1}\right)\cdot jt^{j-1}=\sum_{i=0}^{\infty}jX^{(i)}t^{jp^i-1}$$

and $Z^{(n)}=t^{-mp^n}$. Hence we have

$$(Y, Z)^{(n)}=\mathrm{res}\left(Z^{(n)}\frac{dY}{Y}\right)=\mathrm{res}\left(\sum_{i=0}^{\infty}jX^{(i)}t^{jp^i-mp^n-1}dt\right)$$
$$=\begin{cases} jX^{(n)} & (m=j)\\ 0 & (m\neq j)\ .\end{cases}$$

This proves our result. Q.E.D.

Let $C$ be a field of characteristic $p$ and $K$ the formal power series field in one variable $t$ over the field $C$: $K=C((t))$. We denote by $K^\times$ the multiplicative group of $K$. For $\alpha\in K^\times$ and $\beta\in W_\infty(K)$ the residue vector $(\alpha, \beta)\in W_\infty(C)$ is defined and satisfies the following properties:
Let $\alpha, \alpha'\in K^\times$, $\beta, \beta'\in W_\infty(K)$. Then

(i) $(\alpha\alpha', \beta)=(\alpha, \beta)+(\alpha', \beta)$
(ii) $(\alpha, \beta+\beta')=(\alpha, \beta)+(\alpha, \beta')$
(iii) $(\alpha, c\beta)=c(\alpha, \beta)$ for $c\in W_\infty(C)$
(iv) $(\alpha, V\beta)=V(\alpha, \beta)$
(v) $(\alpha, P\beta)=P(\alpha, \beta)$

where $V\beta=(0, \beta_0, \beta_1, \cdots)$ and $P\beta=(\beta_0^p, \beta_1^p, \cdots)$ for $\beta=(\beta_0, \beta_1, \cdots)\in W_\infty(K)$ (see Witt [10]). Hence by the continuity of $(\alpha, \beta)$ and the properties (i), (ii), the multiplicative group $K^\times$ and the additive group of $W_\infty(K)$ are paired to $W_\infty(C)$. In order to calculate the residue vector $(\alpha, \beta)$ for any $\alpha \in K^\times$ and $\beta \in W_\infty(K)$, we consider the decomposition of $K^\times$ and $W_\infty(K)$ as follows.

PROPOSITION 2. *The multiplicative group $K^\times$ is decomposed as*

$$K^\times = C^\times \times t^Z \times \prod_{\substack{(j,p)=1 \\ j \geqq 1}} \mathfrak{f}_{tj}(W_\infty(C)) \tag{3.2}$$

*where $t^Z = \{t^l \mid l \in Z\}$ and the infinite product of $\mathfrak{f}_{tj}(W_\infty(C))$ $((j, p)=1, j \geqq 1)$ means the direct product as topological groups.*

PROOF. It is obvious that $K^\times = C^\times \times t^Z \times U^{(1)}$. By the relation (1.5)′ we have

$$\mathfrak{f}_{tj}(a(j)) = \prod_{\nu=0}^{\infty} \bar{G}(a(j)_\nu, t^{jp^\nu})$$

where $\bar{G}$ is defined by (1.1)′ in §1. Hence for any $\lambda \in U^{(1)}$, we can determine the components $a(j)_\nu \in C$ inductively such that

$$\lambda = \prod_{\substack{(j,p)=1 \\ j \geqq 1}} \mathfrak{f}_{tj}(a(j)) . \qquad \text{Q.E.D.}$$

PROPOSITION 3. *The additive group $W_\infty(K)$ is decomposed as*

$$\begin{aligned} W_\infty(K) = {} & W_\infty(tC[[t]]) \oplus W_\infty(C) \\ & \oplus \Big( \overline{\bigoplus_{e=0}^{\infty} \bigoplus_{\substack{(m,p)=1 \\ m \geqq 1}} W_\infty(C) P^e\{t^{-m}\}} \Big) \\ & \oplus \Big( \bigoplus_{i=1}^{\infty} V^i \Big( \overline{\bigoplus_{\substack{(m,p)=1 \\ m \geqq 1}} W_\infty(C)\{t^{-m}\}} \Big) \Big) \end{aligned} \tag{3.3}$$

*where $\bar{M}$ means the closure of the subset $M$ of the topological group $W_\infty(K)$, the sum $\oplus$ means the usual direct sum and the sum $\boldsymbol{\oplus}$ means the direct sum as topological groups.*

PROOF. It is clear that $W_\infty(K) = W_\infty(tC[[t]]) \oplus W_\infty(C[t^{-1}])$. Moreover,

$$W_\infty(C[t^{-1}]) = \sum_{i=0}^{\infty} \sum_{m=0}^{\infty} V^i(W_\infty(C)\{t^{-m}\}) .$$

Hence the additive group $W_\infty(K)$ is the sum of the additive groups of the right-hand side. We shall next show the uniqueness of the expression. $\overline{\bigoplus_{e=0}^{\infty} \bigoplus_{(m,p)=1, m \geqq 1} W_\infty(C) P^e\{t^{-m}\}} = \{\sum_{e=0}^{\infty} \sum_{m=1,(m,p)=1}^{\infty} b(e, m) P^e\{t^{-m}\} \mid b(e, m) \in W_\infty(C) \lim_{e\to\infty} b(e, m) = \lim_{m\to\infty} b(e, m) = 0\}$ and $\overline{\bigoplus_{m \geqq 1, (m,p)=1} W_\infty(C)\{t^{-m}\}} = \{\sum_{m=1,(m,p)=1}^{\infty} b(m)\{t^{-m}\} \mid b(m) \in W_\infty(C), \lim_{m\to\infty} b(m) = 0\}$. Put

$$b(0)+\sum_{e=0}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{\infty} b(e, m)P^e\{t^{-m}\}+\sum_{i=1}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{\infty} V^i(b'(i, m)\{t^{-m}\})=0$$

where $b(0)$, $b(e, m)$, $b'(i, m) \in W_\infty(C)$ and $\lim_{m\to\infty} b(e, m)=\lim_{e\to\infty} b(e, m)=\lim_{m\to\infty} b'(i, m)=0$. Comparing each component, we obtain that all components $b(0)$, $b(e, m)$, $b'(i, m)$ are 0. Q.E.D.

THEOREM 1. *Let $C$ be a field of characteristic $p>0$ and $K=C((t))$. Then we can calculate the residue vectors by using Propositions 2 and 3 as follows. Let $\alpha \in K^\times$ and $\beta \in W_\infty(K)$ be*

$$\begin{cases} \alpha=c\times t^l\times \prod_{\substack{(j,p)=1\\ j\geq 1}} \mathfrak{f}_{tj}(a(j)) \\ \beta=\gamma+b(0)+\sum_{e=0}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{\infty} b(e, m)P^e\{t^{-m}\}+\sum_{i=1}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{\infty} V^i(b'(i, m)\{t^{-m}\}) \end{cases}$$

*where $c \in C^\times$, $l \in \boldsymbol{Z}$, $a(j) \in W_\infty(C)$, $\gamma \in W_\infty(tC[[t]])$, $b(0)$, $b(e, m)$, $b'(i, m) \in W_\infty(C)$ and $\lim_{e\to\infty} b(e, m)=\lim_{m\to\infty} b(e, m)=\lim_{m\to\infty} b'(i, m)=0$. Then we have*

$$(\alpha, \beta)=lb(0)+\sum_{e=0}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{\infty} mb(e, m)P^e a(m)+\sum_{i=1}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{\infty} mV^i(a(m)\cdot b'(i, m)) .$$

PROOF. If $\alpha \in C^\times$, then we have $(\alpha, \beta)=0$ for any $\beta \in W_\infty(K)$. And if $\beta \in W_\infty(tC[[t]])$, then we have $(\alpha, \beta)=0$ for any $\alpha \in K^\times$. By the properties (i)~(v) of the residue vectors, it is sufficient to calculate four combinations:

$$(t, 1)\ , \quad (t, \{t^{-m}\})\ , \quad (\mathfrak{f}_{tj}(a), 1) \text{ and } (\mathfrak{f}_{tj}(a), \{t^{-m}\})$$

where $a \in W_\infty(C)$ and $(j, p)=(m, p)=1$. It is clear that $(t, 1)=1$, $(t, \{t^{-m}\})=0$ and $(\mathfrak{f}_{tj}(a), 1)=0$. Moreover, by Lemma 7 we have

$$(\mathfrak{f}_{tj}(a), \{t^{-m}\})=\begin{cases} ja & (m=j) \\ 0 & (m\neq j) . \end{cases}$$

Q.E.D.

We denote by $(\alpha, \beta)_n \in W_n(C)$ the residue vector of the length $n$ for $\alpha \in K^\times$ and $\beta \in W_n(K)$. Similarly we can calculate $(\alpha, \beta)_n$.

## §4. Orthogonal pairing and duality.

4.1. Let $C=\boldsymbol{F}_q$ ($q=p^f$, $f\geq 1$) be a finite field of characteristic $p$ with $q$ elements, $K$ the formal power series field with the coefficient field $\boldsymbol{F}_q$ and an indeterminate element $t$: $K=\boldsymbol{F}_q((t))$. Since $\boldsymbol{F}_q$ is a cyclic extension of degree $f$ over $\boldsymbol{F}_p$, the trace Tr from $W_\infty(\boldsymbol{F}_q)$ to $W_\infty(\boldsymbol{F}_p)$ is defined as

$$\text{(4.1)} \qquad \operatorname{Tr}(c)=\sum_{\sigma\in \mathrm{Gal}(\boldsymbol{F}_q|\boldsymbol{F}_p)}(\sigma c_0,\ \sigma c_1,\ \cdots)\in W_\infty(\boldsymbol{F}_p)$$

for $c=(c_0, c_1, \cdots)\in W_\infty(\boldsymbol{F}_q)$. We define

$$\text{(4.2)} \qquad \langle\alpha,\ \beta\rangle=\operatorname{Tr}(\alpha,\ \beta)\in W_\infty(\boldsymbol{F}_p)$$

for $\alpha\in K^\times$, $\beta\in W_\infty(K)$. Since the trace (4.1) is a continuous homomorphism of the additive group, the multiplicative group $K^\times$ and the additive group $W_\infty(K)$ are paired to $W_\infty(\boldsymbol{F}_p)$ by (4.2). Similarly the trace Tr from $W_n(\boldsymbol{F}_q)$ to $W_n(\boldsymbol{F}_p)$ is defined as

$$\text{(4.3)} \qquad \operatorname{Tr}(c)=\sum_{\sigma\in \mathrm{Gal}(\boldsymbol{F}_q|\boldsymbol{F}_p)}(\sigma c_0,\ \cdots,\ \sigma c_{n-1})\in W_n(\boldsymbol{F}_p)$$

for $c=(c_0, c_1, \cdots, c_{n-1})\in W_n(\boldsymbol{F}_q)$. And we define

$$\text{(4.4)} \qquad \langle\alpha,\ \beta\rangle_n=\operatorname{Tr}(\alpha,\ \beta)_n\in W_n(\boldsymbol{F}_p)$$

for $\alpha\in K^\times$, $\beta\in W_n(K)$. By (4.4), the multiplicative group $K^\times$ and the additive group $W_n(K)$ are paired to $W_n(\boldsymbol{F}_p)$. We shall calculate the residue vectors $\langle\alpha, \beta\rangle$ for any $\alpha\in K^\times$ and $\beta\in W_\infty(K)$. Since $\boldsymbol{F}_q$ is a cyclic extension of degree $f$ over $\boldsymbol{F}_p$, the additive group of $W_\infty(\boldsymbol{F}_q)$ is a free abelian group of rank $f$ over $W_\infty(\boldsymbol{F}_p)$. Let $\{\alpha(1), \alpha(2), \cdots, \alpha(f)\}$ be a base of $W_\infty(\boldsymbol{F}_q)$ over $W_\infty(\boldsymbol{F}_p)$ and $\{\beta(1), \beta(2), \cdots, \beta(f)\}$ the complementary base of $\{\alpha(1), \cdots, \alpha(f)\}$ such that

$$\text{(4.5)} \qquad \operatorname{Tr}(\alpha(k)\cdot\beta(h))=\delta_{kh} \qquad k,\ h=1,\ 2,\ \cdots,\ f$$

where Tr is defined by (4.1). In particular, we choose $\alpha(1)=1$ so that $\operatorname{Tr}\beta(1)=1$, $\operatorname{Tr}\beta(h)=0$ $(h=2, 3, \cdots, f)$ hold. Since the field of quotients $\boldsymbol{K}$ of $W_\infty(\boldsymbol{F}_q)$ is an unramified extension of degree $f$ over the field of quotients $\boldsymbol{Q}_p$ of $W_\infty(\boldsymbol{F}_p)$, $\{\beta(1), \cdots, \beta(f)\}$ is a base of $W_\infty(\boldsymbol{F}_q)$ over $W_\infty(\boldsymbol{F}_p)$. By Proposition 2, the multiplicative group $K^\times$ is decomposed as

$$\text{(4.6)} \qquad K^\times=\boldsymbol{F}_q^\times\times t^{\boldsymbol{Z}}\times\prod_{\substack{(j,p)=1\\ j\geq 1}}\prod_{k=1}^{f}\mathfrak{f}_{t^j}(W_\infty(\boldsymbol{F}_p)\alpha(k))\ .$$

And by Proposition 3, the additive group $W_\infty(K)$ is decomposed as

$$\text{(4.7)} \qquad \begin{aligned} W_\infty(K)= {} & W_\infty(t\boldsymbol{F}_q[[t]])\oplus\Big(\bigoplus_{h=1}^{f}W_\infty(\boldsymbol{F}_p)\beta(h)\Big)\\ & \oplus\Big(\overline{\bigoplus_{e=0}^{\infty}\bigoplus_{(m,p)=1}\bigoplus_{h=1}^{f}W_\infty(\boldsymbol{F}_p)P^e(\beta(h)\{t^{-m}\})}\Big)\\ & \oplus\Big(\bigoplus_{i=1}^{\infty}V^i\Big(\overline{\bigoplus_{\substack{(m,p)=1\\ m\geq 1}}\bigoplus_{h=1}^{f}W_\infty(\boldsymbol{F}_p)\beta(h)\{t^{-m}\}}\Big)\Big)\ .\end{aligned}$$

THEOREM 2. *Let $K$ be the formal power series field with the coefficient field $F_q$ and an indeterminate element $t$. Then we can calculate the residue vectors* (4.2) *by using* (4.6) *and* (4.7) *as follows. Let $\alpha \in K^{\times}$ and $\beta \in W_{\infty}(K)$ be*

$$\begin{cases} \alpha = c \cdot t^{l} \cdot \prod_{\substack{j=1 \\ (j,p)=1}}^{\infty} \prod_{k=1}^{f} \mathfrak{f}_{t^j}(a(j, k)\alpha(k)) \\ \beta = \gamma + \sum_{h=1}^{f} b(h)\beta(h) + \sum_{e=0}^{\infty} \sum_{\substack{m=1 \\ (m,p)=1}}^{\infty} \sum_{h=1}^{f} b(e, m, h)P^{e}(\beta(h)\{t^{-m}\}) \\ \qquad + \sum_{i=1}^{\infty} \sum_{\substack{m=1 \\ (m,p)=1}}^{\infty} \sum_{h=1}^{f} b'(i, m, h) V^{i}(\beta(h)\{t^{-m}\}) , \end{cases}$$

*where $c \in F_q^{\times}$, $l \in Z$, $a(j, k) \in W_{\infty}(F_p)$, $\gamma \in W_{\infty}(tF_q[[t]])$, $b(h)$, $b(e, m, h)$, $b'(i,m,h) \in W_{\infty}(F_p)$ and $\lim_{e\to\infty} b(e,m,h) = \lim_{m\to\infty} b(e,m,h) = \lim_{m\to\infty} b'(i,m,h) = 0$. Then we have*

$$\langle \alpha, \beta \rangle = lb(1) + \sum_{e=0}^{\infty} \sum_{\substack{m=1 \\ (m,p)=1}}^{\infty} \sum_{h=1}^{f} ma(m, h)b(e, m, h) + \sum_{i=1}^{\infty} \sum_{\substack{m=1 \\ (m,p)=1}}^{\infty} \sum_{h=1}^{f} mp^{i}a(m, h)b'(i, m, h) .$$

PROOF. By Theorem 1, we have

$$(\alpha, \beta) = l \cdot \sum_{h=1}^{f} b(h)\beta(h) + \sum_{e=0}^{\infty} \sum_{\substack{m=1 \\ (m,p)=1}}^{\infty} m \sum_{h=1}^{f} b(e, m, h)P^{e}\beta(h)P^{e}\left(\sum_{k=1}^{f} a(m, k)\alpha(k)\right) + \sum_{i=1}^{\infty} \sum_{\substack{m=1 \\ (m,p)=1}}^{\infty} mV^{i}\left(\sum_{k=1}^{f} a(m, k)\alpha(k) \cdot \sum_{h=1}^{f} b(i, m, h)\beta(h)\right) .$$

By (4.5) we have

$$\langle \alpha, \beta \rangle = \mathrm{Tr}\,(\alpha, \beta) = lb(1) + \sum_{e=0}^{\infty} \sum_{m=1}^{\infty} \sum_{h=1}^{f} ma(m, h)b(e, m, h) + \sum_{i=1}^{\infty} \sum_{m=1}^{\infty} \sum_{h=1}^{f} mp^{i}a(m, h)b'(i, m, h) . \qquad \text{Q.E.D.}$$

4.2. Let $K = F_q((t))$ be the formal power series field ($q = p^f$, $f \geqq 1$). We shall consider two pairings $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle_n$ defined by (4.2) and (4.4).

(I) On the pairing $\langle\ ,\ \rangle$ defined by (4.2).

We denote by $B$ the annihilator of the pairing $\langle\ ,\ \rangle$.

THEOREM 3.

(i) *The additive group $W_{\infty}(K)$ is decomposed as*

(4.8) $$W_\infty(K)=\wp W_\infty(K)\oplus W_\infty(\boldsymbol{F}_p)\beta(1)\oplus\Omega_\infty$$

*where* $\Omega_\infty$ *is the closure of* $\bigoplus_{(m,p)=1,m\geqq 1} W_\infty(\boldsymbol{F}_q)\{t^{-m}\}$ *in* $W_\infty(K)$, i.e., $\Omega_\infty=\{\beta=\sum_{m=1,(m,p)=1}^{\infty} b(m)\{t^{-m}\}\mid b(m)\in W_\infty(\boldsymbol{F}_q),\ \lim_{m\to\infty} b(m)=0\}$ *and* $\wp=P-1$.

(ii) $$\begin{cases}\boldsymbol{B}(W_\infty(K))=\boldsymbol{F}_q^\times\\ \boldsymbol{B}(K^\times)=\wp W_\infty(K)\end{cases}$$

*Hence we have an orthogonal pairing*

(4.9) $$\langle\ ,\ \rangle\colon (t^{\boldsymbol{Z}}\times U^{(1)})\times(W_\infty(\boldsymbol{F}_p)\beta(1)\oplus\Omega_\infty)\longrightarrow W_\infty(\boldsymbol{F}_p)\ .$$

(iii) *Let* $\alpha\in K^\times$ *and* $\beta\in W_\infty(K)$

$$\begin{cases}\alpha=c\cdot t^l\cdot\prod_j\prod_k \mathfrak{f}_{t^j}(a(j,k)\alpha(k))\\ \beta=\wp(\gamma)+b(0)\beta(1)+\sum_{m=1}^{\infty}\sum_{h=1}^{f} b(m,h)\beta(h)\{t^{-m}\}\end{cases}$$

*where* $c\in\boldsymbol{F}_q^\times$, $l\in\boldsymbol{Z}$, $a(j,k)\in W_\infty(\boldsymbol{F}_p)$, $\gamma\in W_\infty(K)$, $b(0)$, $b(m,h)\in W_\infty(\boldsymbol{F}_p)$ *and* $\lim_{m\to\infty} b(m,h)=0$.

*Then*

$$\langle\alpha,\beta\rangle=lb(0)+\sum_{\substack{m=1\\(m,p)=1}}^{\infty}\sum_{h=1}^{f} ma(m,h)b(m,h)\ .$$

PROOF. (i) It is obvious that

$$W_\infty(t\boldsymbol{F}_q[[t]])=\wp W_\infty(t\boldsymbol{F}_q[[t]])\quad\text{and}\quad W_\infty(\boldsymbol{F}_q)=\wp W_\infty(\boldsymbol{F}_q)\oplus W_\infty(\boldsymbol{F}_p)\beta(1)\ .$$

Hence it is sufficient to prove

$$W_\infty(t^{-1}\boldsymbol{F}_q[t^{-1}])=\wp W_\infty(t^{-1}\boldsymbol{F}_q[t^{-1}])\oplus\Omega_\infty\ .$$

Since $W_\infty(t^{-1}\boldsymbol{F}_q[t^{-1}])$ is closed in $W_\infty(K)$, $W_\infty(t^{-1}\boldsymbol{F}_q[t^{-1}])$ contains $\wp W_\infty(t^{-1}\boldsymbol{F}_q[t^{-1}])\oplus\Omega_\infty$. Conversely, for any $e\geqq 0$, $m\geqq 1$, $(m,p)=1$, $h=1,2,\cdots,f$, we have

$$P^e(\beta(h)\{t^{-m}\})=\wp\left(\sum_{i=0}^{e-1}P^i(\beta(h)\{t^{-m}\})\right)+\beta(h)\{t^{-m}\}\ .$$

Hence

$$\bigoplus_{e=0}^{\infty}\bigoplus_{\substack{(m,p)=1\\m\geqq 1}}\bigoplus_{h=1}^{f} W_\infty(\boldsymbol{F}_p)P^e(\beta(h)\{t^{-m}\})\subset\wp W_\infty(t^{-1}\boldsymbol{F}_q[t^{-1}])+\Omega_\infty\ .$$

For any

$$\beta\in\bigoplus_{i=1}^{\infty}\bigoplus_{m}\bigoplus_{h=1}^{f} W_\infty(\boldsymbol{F}_p)V^i(\beta(h)\{t^{-m}\})$$

such that

$$\beta=\sum_{i=1}^{\infty}\sum_{\substack{m=1\\(m,p)=1}}^{m_i}\sum_{h=1}^{f} b'(i, m, h) V^i(\beta(h)\{t^{-m}\}) ,$$

we put

$$\beta(i)=\sum_{m=1}^{m_i}\sum_{h=1}^{f} b'(i, m, h)\beta(h)\{t^{-m}\} \in \bigoplus_m W_\infty(F_q)\{t^{-m}\} .$$

Then we have $\beta=\sum_{i=1}^{\infty} V^i(\beta(i))$. Put $\beta'(i)=\beta(i)+P\beta(i)+\cdots+P^{i-1}\beta(i) \in W_\infty(t^{-1}F_q[t^{-1}])$ then $\wp(\beta(i))=P^i(\beta(i))-\beta(i)$. Hence

$$V^i(\beta(i))=V^iP^i(\beta(i))-V^i\wp(\beta'(i))=p^i\beta(i)-\wp(V^i\beta'(i)) .$$

Therefore we have

$$\begin{aligned}\beta=\sum_{i=1}^{\infty} V^i(\beta(i))&=\sum_{i=1}^{\infty} p^i\beta(i)-\sum_{i=1}^{\infty}\wp(V^i(\beta'(i)))\\&=\wp\Big(-\sum_{i=1}^{\infty} V^i(\beta'(i))\Big)+\sum_{i=1}^{\infty} p^i\beta(i)\\&\in \wp(W_\infty(t^{-1}F_q[t^{-1}]))\oplus\Omega_\infty .\end{aligned}$$

(ii) We shall prove that $B(W_\infty(K))=F_q^\times$. For $\alpha\in B(W_\infty(K))$ we can express $\alpha=c\cdot t^l\cdot\prod_j\prod_k \mathfrak{f}_{tj}(a(j, k)\alpha(k))$ by (4.6). Since $\langle\alpha, \beta(1)\rangle=l$ and $\langle\alpha, \beta(h)\{t^{-m}\}\rangle=ma(m, h)$ by Theorem 2, we have $l=0$ and $a(m, h)=0$. Hence $\alpha=c\in F_q^\times$. It is obvious that $B(W_\infty(K))$ contains $F_q^\times$. We shall prove that $B(K^\times)=\wp W_\infty(K)$. For $\beta\in\wp W_\infty(K)$ there exists $\gamma\in W_\infty(K)$ such that $\beta=\wp\gamma$. Since $\langle\alpha, \beta\rangle=\langle\alpha, \wp\gamma\rangle=\wp\langle\alpha, \gamma\rangle=0$ for all $\alpha\in K^\times$, we have $\beta\in B(K^\times)$. By Theorem 2 and (i), it is obvious that $B(K^\times)$ contains $\wp W_\infty(K)$.

(iii) The proof is clear by Theorem 2. Q.E.D.

(II) On the pairing $\langle\ ,\ \rangle_n$ defined by (4.4).

We denote by $B_n$ the annihilator of the pairing $\langle\ ,\ \rangle_n$.

THEOREM 4.

(i) *The additive group* $W_n(K)$ *is decomposed as*

$$W_n(K)=\wp W_n(K)\oplus W_n(F_p)\tilde{\beta}(1)\oplus\Omega_n \tag{4.10}$$

*where* $\Omega_n=\bigoplus_{(m,p)=1,m\geq 1} W_n(F_q)\{t^{-m}\}^\sim$ *and* $\tilde{\beta}=(\beta_0, \beta_1, \cdots, \beta_{n-1})\in W_n(K)$ *for* $\beta=(\beta_0, \beta_1, \cdots)\in W_\infty(K)$.

(ii) $\begin{cases}B_n(W_n(K))=(K^\times)^{p^n}\\ B_n(K^\times)=\wp W_n(K) .\end{cases}$

*Hence we have an orthogonal pairing*

(4.11) $\langle\ ,\ \rangle_n\colon K^\times/(K^\times)^{p^n}\times(W_n(F_p)\tilde{\beta}(1)\oplus\Omega_n)\longrightarrow W_n(F_p)$ .

(iii) *Let* $\alpha\in K^\times$ *and* $\beta\in W_n(K)$ *be*

$$\begin{cases}\alpha=c\cdot t^l\cdot\prod_j\prod_k \mathfrak{f}_{t^j}(a(j,k)\alpha(k))\\ \beta=\wp(\gamma)+b(0)\tilde{\beta}(1)+\sum_m\sum_h b(m,h)\tilde{\beta}(h)\{\tilde{t}^{-m}\}\end{cases}$$

*where* $c\in F_q^\times$, $l\in Z$, $a(j,k)\in W_\infty(F_p)$, $\gamma\in W_n(K)$, $b(0)$, $b(m,h)\in W_n(F_p)$. *Then*

$$\langle\alpha,\beta\rangle_n=lb(0)+\sum_m\sum_h m\tilde{a}(m,h)b(m,h)\ .$$

PROOF. (i) The proof is similar to that of Theorem 3 (i).

(ii) We shall prove that $B_n(W_n(K))=(K^\times)^{p^n}$. For $\alpha\in B_n(W_n(K))$ we can express

$$\alpha=c\cdot t^l\cdot\prod_j\prod_k \mathfrak{f}_{t^j}(a(j,k)\alpha(k))$$

by (4.6). Since $\langle\alpha,\tilde{\beta}(1)\rangle_n=l\cdot 1_n$ and $\langle\alpha,\tilde{\beta}(h)\{\tilde{t}^{-m}\}\rangle_n=m\tilde{a}(m,h)$ by Theorem 2, we have $p^n|l$ and $p^n|a(m,h)$. Hence

$$\alpha\in F_q^\times\times t^{p^nZ}\times\prod_j \mathfrak{f}_{t^j}(p^nW_\infty(F_q))=(K^\times)^{p^n}\ .$$

It is obvious that $B_n(W_n(K))$ contains $(K^\times)^{p^n}$. The proof of $B_n(K^\times)=\wp W_n(K)$ is similar to that of Theorem 3.

(iii) The proof is clear by Theorem 2. Q.E.D.

4.3. We shall consider the duality of two pairings $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle_n$ defined by (4.9) and (4.11) respectively.

ASSERTION (I). *On the orthogonal pairing* $\langle\ ,\ \rangle$ *defined by* (4.9).

(i) *For any continuous homomorphism* $\varphi\colon t^Z\times U^{(1)}\to W_\infty(F_p)$, *there exists an element* $\beta\in W_\infty(F_p)\beta(1)\oplus\Omega_\infty$ *such that* $\varphi(\alpha)=\langle\alpha,\beta\rangle$ *for* $\alpha\in t^Z\times U^{(1)}$.

(ii) *For any continuous homomorphism* $\psi\colon W_\infty(F_p)\beta(1)\oplus\Omega_\infty\to W_\infty(F_p)$ *with* $\psi(\beta(1))\in Z$, *there exists an element* $\alpha\in t^Z\times U^{(1)}$ *such that* $\psi(\beta)=\langle\alpha,\beta\rangle$ *for* $\beta\in W_\infty(F_p)\beta(1)\oplus\Omega_\infty$.

PROOF. (i) Put $b(m,h)=m^{-1}\varphi(\mathfrak{f}_{t^m}(\alpha(h)))$ and $b(m)=\sum_{h=1}^f b(m,h)\beta(h)$. Since $\varphi$ is a continuous mapping, $\lim_{m\to\infty,(m,p)=1}b(m)=0$. If we put $\beta=\varphi(t)\beta(1)+\sum_{m=1,(m,p)=1}^\infty b(m)\{t^{-m}\}$, then $\beta\in W_\infty(F_p)\beta(1)\oplus\Omega_\infty$ and $\varphi(\alpha)=\langle\alpha,\beta\rangle$ for all $\alpha\in t^Z\times U^{(1)}$.

(ii) We put

$$\alpha=t^l\cdot\prod_j\prod_k \mathfrak{f}_{t^j}(a(j,k)\alpha(k))$$

where $l=\psi(\beta(1))\in \boldsymbol{Z}$ and $a(j, k)=j^{-1}\psi(\beta(k)\{t^{-j}\})\in W_{\infty}(\boldsymbol{F}_p)$ for $j\geqq 1$, $(j, p)=1$, $k=1, 2, \cdots, f$. Then we have $\psi(\beta(1))=\langle\alpha, \beta(1)\rangle$ and $\psi(\beta(k)\{t^{-j}\})=\langle\alpha, \beta(k)\{t^{-j}\}\rangle$ by Theorem 2. Since $\psi$ is a continuous homomorphism, we have $\psi(\beta)=\langle\alpha, \beta\rangle$ for any $\beta\in W_{\infty}(\boldsymbol{F}_p)\beta(1)\oplus\Omega_{\infty}$. Q.E.D.

ASSERTION (II). *On the orthogonal pairing* $\langle\ ,\ \rangle_n$ *defined by* (4.11).

(i) *For any continuous homomorphism*

$$\varphi\colon K^{\times}/(K^{\times})^{p^n}\longrightarrow W_n(\boldsymbol{F}_p)$$

*there exists an element* $\beta\in W_n(\boldsymbol{F}_p)\tilde{\beta}(1)\oplus\Omega_n$ *such that* $\varphi(\hat{\alpha})=\langle\alpha, \beta\rangle_n$ *for* $\alpha\in K^{\times}$ *where* $\hat{\alpha}=\alpha \bmod (K^{\times})^{p^n}$.

(ii) *For any homomorphism* $\psi\colon W_n(\boldsymbol{F}_p)\tilde{\beta}(1)\oplus\Omega_n\rightarrow W_n(\boldsymbol{F}_p)$ *there exists an element* $\alpha\in K^{\times}$ *such that* $\psi(\beta)=\langle\alpha, \beta\rangle_n$ *for* $\beta\in W_n(\boldsymbol{F}_p)\tilde{\beta}(1)\oplus\Omega_n$. *Since* $K^{\times}/(K^{\times})^{p^n}$ *is compact,* $W_n(K)/\wp W_n(K)$ *is discrete and* $W_n(\boldsymbol{F}_p)$ *is contained in* $\boldsymbol{R}/\boldsymbol{Z}$, *this is a special case of the duality theorem of Pontrjagin.*

PROOF. (i) Since $\varphi$ is a continuous mapping, there exists $m_0\geqq 1$ such that $\varphi(\mathfrak{f}_{t^j}(W_{\infty}(\boldsymbol{F}_q)))=0$ for $j\geqq m_0$. We put

$$\beta=b(0)\tilde{\beta}(1)+\sum_{m=1}^{m_0}\sum_{h=1}^{f}b(m, h)\tilde{\beta}(h)\{\tilde{t}^{-m}\}$$

where $b(0)=\varphi(\hat{t})\in W_n(\boldsymbol{F}_p)$ and $b(m, h)=m^{-1}\varphi(\hat{\mathfrak{f}}_{t^m}(\alpha(h)))$ for $(m, p)=1$, $m\geqq 1$, $h=1, 2, \cdots, f$. Then we have $\varphi(\hat{t})=\langle t, \beta\rangle_n$ and $\varphi(\hat{\mathfrak{f}}_{t^m}(\alpha(h)))=\langle\mathfrak{f}_{t^m}(\alpha(h)), \beta\rangle_n$ by Theorem 4 (iii). Since $\varphi$ is a continuous homomorphism, we have $\varphi(\hat{\alpha})=\langle\alpha, \beta\rangle_n$ for any $\alpha\in K^{\times}$.

(ii) We put

$$\alpha=t^l\times\prod_j\prod_k\mathfrak{f}_{t^j}(a(j, k)\alpha(k))$$

where $l\cdot 1_n=\psi(\tilde{\beta}(1))\in W_n(\boldsymbol{F}_p)$ and $\tilde{a}(j, k)=j^{-1}\psi(\tilde{\beta}(k)\{\tilde{t}^{-j}\})$ for $(j, p)=1$, $j\geqq 1$, $k=1, 2, \cdots, f$. Then we have $\psi(\tilde{\beta}(1))=\langle\alpha, \beta(1)\rangle_n$ and $\psi(\tilde{\beta}(k)\{\tilde{t}^{-j}\})=\langle\alpha, \beta(k)\{t^{-j}\}\rangle_n$ by Theorem 4 (iii). Since $\psi$ is a homomorphism, we have $\psi(\beta)=\langle\alpha, \beta\rangle_n$ for any $\beta\in W_n(\boldsymbol{F}_p)\tilde{\beta}(1)\oplus\Omega_n$. Q.E.D.

## §5. Arithmetic of local fields of characteristic $p$.

Let $C=\boldsymbol{F}_q(q=p^f, f\geqq 1)$ be a finite field of characteristic $p$ with $q$ elements, $K$ the formal power series field with the coefficient field $\boldsymbol{F}_q$ and an indeterminate element $t$: $K=\boldsymbol{F}_q((t))$ and $L$ a cyclic extension of order $p^n$ over $K$. Then there exists a cyclic extension $\boldsymbol{F}_{q^d}$ $(d=p^s, s\geqq 0)$ over $\boldsymbol{F}_q$ and $T\in L$ such that $L=\boldsymbol{F}_{q^d}((T))$ and $(t)=(T)^{p^l}$ in $\boldsymbol{F}_{q^d}[[T]]$. Then $p^l$ is called the *ramification index* of $L$ over $K$ and $d=p^s=[\boldsymbol{F}_{q^d}\colon \boldsymbol{F}_q]$ is called the *relative degree* of $L$ over $K$. Moreover, let $r$ be the minimum positive integer $i$ such that $U^{(i)}\subset N_{L|K}(L^{\times})$. Then the ideal $(t)^r$ in $F_q[[t]]$ is called the *conductor* of $L$ over $K$. On the other hand there exists an element $\beta\in W_n(K)$ such that $L=K(\wp^{-1}\beta)$ by Theorem (*) in §2. Moreover, by Theorem 4 (i) we can choose

$$\beta\in W_n(F_p)\tilde{\beta}(1)\oplus\Omega_n \quad \text{where} \quad \Omega_n=\bigoplus_{(m,p)=1,m\geqq 1} W_n(F_q)\{\tilde{t}^{-m}\}$$

and we can express

$$\beta=b(0)\tilde{\beta}(1)+\sum_{\substack{m=1\\(m,p)=1}}^{m_0}\sum_{h=1}^{f} b(m,h)\tilde{\beta}(h)\{\tilde{t}^{-m}\}=b(0)\tilde{\beta}(1)+\sum_{m=1}^{m_0} b(m)\{\tilde{t}^{-m}\}\ ,$$

where $b(0)$, $b(m,h)\in W_n(F_p)$ and $b(m)=\sum_{h=1}^{f} b(m,h)\tilde{\beta}(h)\in W_n(F_q)$. For $m\geqq 1$, $(m,p)=1$ and $b(m)\neq 0$, take the non-negative integer $s_m$ such that $p^{s_m}\mid b(m)$ and $p^{s_m+1}\nmid b(m)$. If $b(m)=0$, then $s_m=n$. And we put

$$l_m=n-s_m\ . \tag{5.1}$$

By these constants $l_m (1\leqq m\leqq m_0,\ (m,p)=1)$ we shall calculate the ramification index and the conductor of $L$ over $K$.

THEOREM 5. *Let $F_q$ $(q=p^f,\ f\geqq 1)$ be a finite field of characteristic $p$ with $q$ elements, $K$ the formal power series field: $K=F_q((t))$ and $L$ a cyclic extension of order $p^n$ over $K$.*

(i) *If we put*

$$l=\max\{l_m \mid 1\leqq m\leqq m_0,\ (m,p)=1\}\ , \tag{5.2}$$

*where $l_m$ is given by* (5.1) *then $p^l$ is the ramification index of $L$ over $K$.*

(ii) *If we put*

$$r=\max\{mp^{l_m-1}+1 \mid 1\leqq m\leqq m_0,\ (m,p)=1,\ l_m\geqq 1\}\ , \tag{5.3}$$

*then $(t)^r$ is the conductor of $L$ over $K$.*

PROOF. (i) is easy to prove. We shall prove (ii). By Y. Kawada and I. Satake [7] (XII) p. 376, we have $N_{L|K}(L^{\times})=B_n(\beta)$ where $B_n(\beta)=\{\alpha\in K^{\times}\mid\langle\alpha,\beta\rangle_n=0\}$. Hence it is sufficient to prove that $U^{(r)}\subset B_n(\beta)$ and $U^{(r-1)}\not\subset B_n(\beta)$. For $r\geqq 1$, $j\geqq 1$ and $(j,p)=1$ we define $r_j=\min\{e\geqq 0\mid jp^e\geqq r\}$. Then we have

$$U^{(r)}=\prod_{\substack{(j,p)=1\\ j\geqq 1}} \mathfrak{f}_{t^j}(V^{r_j}(W_\infty(F_q)))\ .$$

Hence any element $\alpha \in U^{(r)}$ can be expressed as

$$\alpha = \prod_{\substack{(j,p)=1 \\ j \geqq 1}} \prod_{k=1}^{f} \mathfrak{f}_{tj}(a(j, k)\alpha(k))$$

where $a(j, k) \in V^{r_j}(W_\infty(F_p))$. On the other hand,

$$\beta = b(0)\tilde{\beta}(1) + \sum_{\substack{(m\ p)=1 \\ m=1}}^{m_0} \sum_{h=1}^{f} b(m, h)\tilde{\beta}(h)\{\tilde{t}^{-m}\}$$

where $b(m, h) \in V^{n-l_m}(W_n(F_p))$. Since

$$\langle \alpha, \beta \rangle_n = \sum_{m=1}^{m_0} \sum_{h=1}^{f} m\tilde{a}(m, h)b(m, h)$$

by Theorem 4 (iii), and $l_m \leqq r_m$, we have $\langle \alpha, \beta \rangle_n = 0$. Hence $U^{(r)} \subset \boldsymbol{B}_n(\beta)$. Next we shall show that $U^{(r-1)} \not\subset \boldsymbol{B}_n(\beta)$. Let $j$ be a positive integer such that $(j, p)=1$, $l_j \geqq 1$ and $r = jp^{l_j-1}+1$. Then $(r-1)_j = l_j - 1$. Since $b(m) = \sum_{h=1}^{f} b(m, h)\tilde{\beta}(h)$, there exists $k \in \{1, 2, \cdots, f\}$ such that $b(j, k) \notin V^{n-l_j+1}(W_n(F_p))$. If we put $\alpha = \mathfrak{f}_{tj}(p^{l_j-1}\alpha(k))$, then $\alpha \in U^{(r-1)}$ and $\langle \alpha, \beta \rangle_n = jp^{l_j-1}b(j, k) \neq 0$. Hence we have $\alpha \notin \boldsymbol{B}_n(\beta)$. Q.E.D.

For $\beta = (\beta_0, \beta_1, \cdots, \beta_{n-1}) \in W_n(K)$ we put

$$K_j = K(\wp^{-1}(\beta_0, \cdots, \beta_{j-1})) \qquad (j=1, 2, \cdots, n).$$

Then we have a sequence of fields $K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$, where $K_{j+1} \supset K_j$ $(j=0, 1, \cdots, n-1)$ is a cyclic extension of order $p$. We shall consider the conductor of $K_j$ over $K$. For $i=1, 2, \cdots, n$, we put

$$h_i = \max\{m \mid 1 \leqq m \leqq m_0,\ (m, p)=1,\ l_m = n-i+1\} \tag{5.4}$$

where $l_m$ is given by (5.1). If $\{m \mid 1 \leqq m \leqq m_0,\ (m, p)=1,\ l_m = n-i+1\} = \emptyset$, then we put

$$h_i = 0 . \tag{5.5}$$

By Theorem 5 the conductor $(t)^r$ of $L/K$ is determined by

$$r = 1 + \max\{h_1 p^{n-1}, h_2 p^{n-2}, \cdots, h_{n-1}p, h_n\} . \tag{5.6}$$

If $(t)^{F_j}$ is the conductor of $K_j$ over $K$, then we have similarly

$$\begin{aligned} F_j &= 1 + \max\{h_1 p^{j-1}, h_2 p^{j-2}, \cdots, h_{j-1}p, h_j\} \\ &= 1 + \max\{p(F_{j-1}-1), h_j\} . \end{aligned} \tag{5.7}$$

We can characterize the conductor of the intermediate fields.

THEOREM 6. *Let $(a_1, a_2, \cdots, a_n)$ be an n-tuple of positive integers $a_i$. In order that there exists a sequence of fields $K=K_0\subset K_1\subset\cdots\subset K_n=L$ such that $L\supset K$ is a totally ramified cyclic extension of order $p^n$ and $(t)^{a_i+1}$ is the conductor of $K_i$ over $K$ it is necessary and sufficient that $(a_1, a_2, \cdots, a_n)$ satisfies the following relations*:

$$\text{(5.8)}\qquad \begin{cases} \text{(i)} & (a_1, p)=1\ , \\ \text{(ii)} & \textit{either } a_i=pa_{i-1}, \textit{ or } a_i>pa_{i-1},\ (a_i, p)=1 \textit{ for } i=2, 3, \cdots, n\ . \end{cases}$$

PROOF. If we put $a_i=F_i-1$, then by (5.7) we have

$$\text{(5.9)}\qquad a_1=h_1 \quad\text{and}\quad a_i=\max\{pa_{i-1}, h_i\} \qquad (i=2, 3, \cdots, n)\ .$$

It is obvious that the relation (5.8) is a necessary condition by (5.9). Conversely, let $(a_1, a_2, \cdots, a_n)$ be an $n$-tuple with the properties (5.8). If we put $\beta=(t^{-a_1}, t^{-a_2}, \cdots, t^{-a_n})\in W_n(K)$, $L=K(\wp^{-1}\beta)$ and $K_j=K(\wp^{-1}(\beta_0, \beta_1, \cdots, \beta_{j-1}))$, $(j=1, 2, \cdots, n)$, then by the relation (5.8) the conductor of $K_j$ over $K$ is $(t)^{a_j+1}$. Q.E.D.

REMARK. If $L\supset K$ is not a totally ramified extension in Theorem 6, then we must change the relation (5.8) for the following relations: If the relative degree of $L$ over $K$ is $p^s$, then

$$\begin{cases} \text{(i)}' & a_1=a_2=\cdots=a_s=0,\ (a_{s+1}, p)=1 \\ \text{(ii)}' & \text{either } a_i=pa_{i-1}, \text{ or } a_i>pa_{i-1},\ (a_i, p)=1 \text{ for } i=s+2, s+3, \cdots, n\ . \end{cases}$$

By the above results, we can calculate the *ramification numbers* and the *discriminant ideal* of $L$ over $K$ by Hasse's formula (see Hasse [2]). Let $v_1, v_2, \cdots$ be the ramification numbers of $L/K$, then we have

$$\text{(5.10)}\qquad v_\nu=a_1+p(a_2-a_1)+p^2(a_3-a_2)+\cdots+p^{\nu-1}(a_\nu-a_{\nu-1}) \qquad (\nu=1, 2, \cdots)\ .$$

Moreover, if $\delta$ is the discriminant ideal of $L/K$, then we have

$$\text{(5.11)}\qquad \delta=(t)^{p^{n-l}[(p^l-1)+v_1(p^l-1)+(v_2-v_1)(p^{l-1}-1)+\cdots+(v_l-v_{l-1})(p-1)]}$$

where $p^l$ is the ramification index of $L$ over $K$.

## References


[1] J. DIEUDONNÉ, On the Artin-Hasse exponential series, Proc. Amer. Math. Soc., **8** (1957), 210-214.

[2] H. HASSE, Führer, Diskriminante und Verzweigungskörper relative-abelscher Zahlkörper, J. Reine Angew. Math., **162** (1930), 169-184.

[3] H. HASSE, Die Gruppe der $p^n$-primären Zahlen für einen Primteiler $\mathfrak{p}$ von $p$, J. Reine Angew. Math., **176** (1937), 174–183.
[4] E. INABA, On matrix equations for Galois extensions of fields with characteristic $p$, Natur. Sci. Rep. Ochanomizu Univ., **12** (1961), 26–36.
[5] E. INABA, On generalized Artin-Schreier equations, Natur. Sci. Rep. Ochanomizu Univ., **13** (1962), 1–13.
[6] E. INABA, Normal form of generalized Artin-Schreier equations, Natur. Sci. Rep. Ochanomizu Univ., **14** (1963), 1–15.
[7] Y. KAWADA and I. SATAKE, Class Formations II, J. Fac. Sci. Univ. Tokyo, Sect 1A Math., **7** (1956), 353–389.
[8] G. WHAPLES, Generalized local class field theory III, Second form of existence theorem, Structure of analytic groups, Duke Math. J., **21** (1954), 575–581.
[9] E. WITT, Der Existenzsatz für abelsche Funktionenkörper, J. Reine Angew. Math., **173** (1935), 43–51.
[10] E. WITT, Zyklische Körper und Algebren der Charakteristik $p$ vom Grad $p^n$, J. Reine Angew. Math., **176** (1936), 126–140.

*Present Address*:
DEPARTMENT OF MATHEMATICS
SOPHIA UNIVERSITY
KIOI-CHO, CHIYODA-KU, TOKYO 102