Generalized Hasse-Witt invariants and unramified Galois extensions of an algebraic function field

By Hidenori KATSURADA

(Received June 5, 1977)
(Revised April 10, 1978)

Introduction.

In this paper, we give a certain generalization of the Hasse-Witt theory (cf. [4]).

Let $K$ be an algebraic function field with an algebraically closed constant field $k$ of characteristic $p > 0$, and $g$ be its genus. Let $M$ be the maximum unramified Galois extension of $K$. Let $\Delta_g$ be the group generated by $2g$ elements $u_i, v_i$ ($i = 1, \ldots, g$) with the following fundamental relation:

$$(u_1 v_1 u_1^{-1} v_1^{-1}) \cdots (u_g v_g u_g^{-1} v_g^{-1}) = 1.$$ 

Let $\bar{\Delta}_g$ be the completion of $\Delta_g$ with respect to subgroups of finite index. Then, it is well known that there is a surjective homomorphism of $\bar{\Delta}_g$ onto $\text{Gal}(M/K)$, and that its kernel is contained in the intersection of kernels of continuous homomorphism from $\bar{\Delta}_g$ to finite groups with order prime to $p$. (cf. [3]).

It is obvious that the structure of $\text{Gal}(M/K)$ (as an abstract group) depends on $g$ and $p$. We note that for any finite group $G$ with order prime to $p$, the number of unramified Galois extensions of $K$ whose Galois group is isomorphic to $G$ is determined by $g$. Moreover, it is well-known that the structure of the Galois group of the maximal unramified abelian extension of $K$ is determined by $g$, $p$, and the invariant $\gamma_K$ that was introduced by Hasse-Witt (cf. [4]). Hence if $g = 1$, $\text{Gal}(M/K)$ is determined by $g$, $p$, and $\gamma_K$. But if $g \geq 2$, the structure of $\text{Gal}(M/K)$ is not determined only by $g$, $p$ and $\gamma_K$.

In §1, we define an unramified $D_{npm}$-extension of $K$ as an unramified Galois extension of $K$ whose Galois group is isomorphic to

$$D_{npm} = \langle \sigma, \tau | \sigma^p = \tau^n = 1, \tau \sigma \tau^{-1} = \sigma^i \rangle,$$

where $i$ is a primitive $n$-th root of unity in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. 

In §2, we construct a certain invariant of $K$ depending on $n$, and state our main theorem. Let $\mathcal{A}_n$ be the set of full representatives of divisor classes of degree 0 of $K$ whose orders are $n$. Then the invariant is the set \{${\gamma}_A$\}$_{A \in \mathcal{A}_n}$, where $\gamma_A$ is an integer which is determined by the class of $A$. Then, our main theorem gives the number of unramified $D_{n,p}$-extension of $K$ in terms of this invariant (cf. [4]).

In §3, we give some lemmas and in §4, we prove the main theorem and its corollaries.

In §5, we give some remarks which are mainly concerned with unramified $D_{n,p,m}$-extensions of $K$.

In §6, we give some examples. In particular, we give examples of algebraic function fields which have the same $g$, $p$, and $\gamma_K$ but have different numbers of unramified $D_{2,p}$-extensions. Hence, our invariant is essentially new.

The author wishes his hearty thanks to Professor Y. Ihara who suggested the author this problem. He wishes to express his hearty thanks to Professor Y. Morita and Dr. Takayuki Oda for encouragements and careful readings.

§ 1. Preliminaries and notations.

We shall use the following notations.

$\sharp(A)$: the cardinal of a set $A$.

$(a, b)$: the greatest common divisor of integers $a$ and $b$.

Let $k$ be an algebraically closed field of positive characteristic $p$. Let $K$ be an algebraic function field over $k$, and $g$ be its genus. We assume that $g \geq 2$. Let $L$ be a finite Galois extension of $K$. We denote by $[L: K]$ its degree over $K$, and by $\text{Gal}(L/K)$ the Galois group.

Let $\mathfrak{p}$ be a prime divisor of $K$, and $\nu_{\mathfrak{p}}$ be the corresponding normalized additive valuation of $K$. We denote by $K_{\mathfrak{p}}$ the completion of $K$ at $\mathfrak{p}$, and put

$$\mathcal{O}_{\mathfrak{p}} := \{a \in K_{\mathfrak{p}} \mid \nu_{\mathfrak{p}}(a) \geq 0\}.$$  

We denote by $K^*$ the multiplicative group $K - \{0\}$, and by $K^{*n}$ the subgroup of $K^*$ consisting of $n$-th powers of all elements of $K^*$. We denote by $K^p$ the image of $K$ under $p$-th power map. Finally, we denote by $F_p$ the field with $p$ elements.

Let $G$ be a group, $N$ be a subgroup of $G$, we put $C_G(N) = \{\sigma \in G \mid \sigma \tau = \tau \sigma \}$ for all $\tau \in N$, the centralizer of $N$ in $G$. We denote by

$$\langle u_1, u_2, \ldots, u_r \mid f_i(u_1, u_2, \ldots, u_r) = 1; i = 1, 2, \ldots, s \rangle$$

the group generated by $r$ elements $u_1, u_2, \ldots, u_r$ and with a fundamental relations $f_i(u_1, u_2, \ldots, u_r) = 1$. 


Let $L$ be an unramified abelian extension of $K$ of degree $n$. We put

$$\Delta_L = \{ \theta \in L^* \mid \theta^m \in K^* \text{ for some integer } m \geq 1 \}$$

and for each $\theta \in \Delta_L$, we define an element $\chi_\theta$ of $\text{Hom}(\text{Gal}(L/K), k^*)$ by

$$\chi_\theta : \text{Gal}(L/K) \ni \sigma \mapsto \theta^{-1} \theta^\sigma \in k^*.$$ 

Then it follows from the Kummer theory that the above homomorphism $\Delta_L \ni \theta \mapsto \chi_\theta$ gives an isomorphism of $\Delta_L/K^*$ onto $\text{Hom}(\text{Gal}(L/K), k^*)$. Let $\mathcal{D}_o$ be the group consisting of all divisors of $K$ of degree 0 and let $\mathcal{D}_H$ be the subgroup of all principal divisors. We denote $A \bmod \mathcal{D}_H$ by $\overline{A}$. For any element $\theta$ of $\Delta_L$, we associate an element $A_\theta$ of $\mathcal{D}_o$ such that $A_\theta = (\theta)$ in $L$. This correspondence induces an injective homomorphism of $\Delta_L/K^*$ into $\mathcal{D}_o/\mathcal{D}_H$. We denote its image by $\mathcal{C}(L,K)$, and call it the divisor class group corresponding to an extension $L$ over $K$.

We define the action of the operator $\varphi$ on a subset of an extension field of $K$ in the following manner:

$$\varphi(a) = a^p - a.$$ 

For any $\text{Gal}(L/K)$-submodule $A$ of $L$, we put $U_A = \bigcap_i (A \cap \mathcal{P}_L)$, and call an element of $U_A$ an unramified element of $A$. We note that, for any $\alpha \in L$, $L(\alpha/\mathcal{P})$ is unramified over $L$ if and only if $\alpha \in U_L$, where $\alpha/\mathcal{P}$ means a root of the equation $\varphi(X) = \alpha$ in the algebraic closure $\overline{L}$ of $L$. If we have $\mathcal{P}^p A \subset A$, we denote by $W_A$ a quotient of a group $U_A$ by a subgroup $\mathcal{P}A$.

Let $\Omega(K/k)$ be the space of $k$-differentials of $K$, and for any divisor $A$ of $K$, let

$$\Omega(A) = \{ \omega \in \Omega(K/k) \mid \nu_i(\omega) \geq \nu_i(A) \text{ for all primes } \mathfrak{p} \text{ of } K \}.$$ 

Now the Cartier operator $C$ of $\Omega(K/k)$ is defined as follows. Let $x$ be an element of $K$ which is not contained in $K^p$. Then, for any element $\omega$ of $\Omega(K/k)$, $\omega$ can be expressed uniquely as

$$\omega = \sum_{i=0}^{p-2} a_i^p x^i \, dx \quad (a_i \in K).$$ 

Then, $C\omega = a_{p-1}^p d x$.

This operator $C$ has the following properties:

- (1) $C(\omega_1 + \omega_2) = C(\omega_1) + C(\omega_2)$ for $\omega_1, \omega_2 \in \Omega(K/k)$
- (2) $C(x^p \omega) = x^p C(\omega)$ for $x \in K$ and $\omega \in \Omega(K/k)$
- (3) $C(dx) = 0$
- (4) $C(x^{-1} dx) = x^{-1} dx$
§ 2. Definition of invariants and the main theorem.

Let $A$ be an $n$-division point of $\mathfrak{D}_0 = \mathfrak{D}_0 / \mathfrak{D}_H$. Then, the dimension $l$ of $Q(A)$ is given by

$$l = \begin{cases} g & \text{if } A \in \mathfrak{D}_H \\ g - 1 & \text{if } A \notin \mathfrak{D}_H. \end{cases}$$

Now, we assume that $n$ divides $p - 1$. Let $\{\omega_i\}$ be a basis of $Q(A)$, and let $x$ be an element of $K$ such that $(x) = A$. Then, it follows from the basic properties of the Cartier operator that

$$C(A) \subset Q(A).$$

Since $\{x\omega_i\}$ is a basis of $Q(A^p)$, there is a matrix $C_A = (c_{ij})$ of $M_l(k)$ such that

$$C((x\omega_k)) = C_A(\omega_k),$$

that is, $C(x\omega_k) = \sum c_{ki} \omega_i$.

Let $\gamma_A$ be the rank of $C_A C_A^{(p)} \cdots C_A^{(p^{l-1})}$, where $C_A^{(p^{k})}$ is the matrix $(c_{ij}^{p^k})$.

We claim that this $\gamma_A$ does not depend on the choice of a basis of $Q(A)$ and a representative of a class of $A$. To see this, let $\{\eta_i\}$ be another basis of $Q(A)$, and $C_A$ be the matrix such that

$$C((x\eta_k)) = C_A((\eta_k)).$$

Then, there is a regular matrix $S$ of $GL_l(k)$ such that

$$(\eta_k) = S(\omega_k).$$

Then, we have

$$C(x\eta_k) = C(S(x\omega_k)).$$

It follows from the basic properties of Cartier operator (see § 1) that

$$C(S(x\omega_k)) = S^{(1/p)} C((x\omega_k)) = S^{(1/p)} C_A(\omega_k) = S^{(1/p)} C_A S^{-1}(\eta_k) = C'_A(\eta_k).$$

Hence, we have $C'_A = S^{(1/p)} C_A S^{-1}$. Therefore,

$$C'_A C_A^{(p)} \cdots C_A^{(p^{l-1})} = (S^{(1/p)} C_A S^{-1}) (S^{(1/p)} C_A S^{-1})^{(p)} \cdots (S^{(1/p)} C_A S^{-1})^{(p^{l-1})} = S^{(1/p)} C_A C_A^{(p)} \cdots C_A^{(p^{l-1})} S^{-1}.$$
Since $S$ is regular,
\[ \text{rank } C_A^p \cdots C_A^{p^{1-1}} = \text{rank } C_A^{(p)} \cdots C_A^{(p^{1-1})}. \]

Hence $\gamma_A$ does not depend on the choice of basis of $O(A)$.

Let $A_1$ be another representative of $A$. Then, there exists a function $y$ of $K$ such that $(y)A_1 = A$. Let $x_1$ be a function of $K$ such that $A_1^{p^{-1}} = (x_1)$. Then, $\{y\omega_1\}$ is a basis of $O(A_1)$ and $(x_1) = (y^{p^{-1}}x)$. Hence,
\[ C((x_1 y\omega_1)) = C((y^{p} x\omega_1)) = yC_A((\omega_1)) = C_{A_1}((y\omega_1)). \]

We have $C_A = C_{A_1}$, and $\gamma_A = \gamma_{A_1}$. Hence, $\gamma_A$ does not depend on the choice of representative of class $A$. Therefore, $\gamma_A$ is uniquely determined by $\bar{A}$. If we call $\bar{A}_n$ the set of all $n$-division points of $D_H$, the set $\{\gamma_A\}_{\bar{A} \in \bar{A}_n}$ is an invariant of $K$ (depending on $n$). Especially if $n = 1$, $\{\gamma_A\}_{\bar{A} \in \bar{A}_n}$ consists of one element $\gamma_K$, which was introduced by Hasse-Witt [4].

**Definition 1.** A group $G$ is said to be $(m, n)$ type if there exists abelian groups $A$ of order $m$ and $H$ of order $n$ such that $G$ is a semi-direct product of $H$ and $A$, with $H$ as its normal subgroup.

**Definition 2.** An unramified Galois extension of $K$ is said to be $(m, n)$ type if its Galois group is $(m, n)$ type. Especially, an unramified Galois extension of $K$ of $(n, p^m)$ type is said to be $D_{n p^m}$-type if its Galois group is isomorphic to
\[ D_{n p^m} = \langle \sigma, \tau | \sigma^{p^n} = \tau^n = 1, \tau \sigma \tau^{-1} = \sigma^i \rangle \text{ with } i \text{ a primitive } n\text{-th root of unity mod } p^m. \]

Then, we note that $n$ divides $p-1$ if $n$ is prime to $p$.

Now, the main results of this paper can be stated as:

**Theorem.** Let $K$ be an algebraic function field with an algebraically closed constant field of positive characteristic $p$, and let $g$ be its genus. We assume that $g \geq 2$. Let $n$ be a positive integer such that $n$ divides $p-1$. Then, the number of unramified $D_{n p^m}$-extensions of $K$ is equal to
\[ \sum_A \frac{(p^n A - 1)}{(p-1)}, \]

where $A$ runs over full representatives of divisor classes of $K$ of order $n$.

**Corollary 1.** Let $K$ be as in Theorem. Let $n$ be a positive integer prime to $p$. Then, the number of unramified Galois extensions of $K$ of $(n, p)$ type is determined by $\{\gamma_A\}$, where $\{A\}$ are full representatives of divisor classes of $K$ of degree 0 whose orders divide $p-1$ and $n$. 
COROLLARY 2. Let $K$ be as in Theorem. Let $L$ be an unramified abelian extension of $K$ of exponent $p-1$. Then, the Hasse-Witt invariant of $L$ is equal to
\[ \sum_A \gamma_A, \]
where $A$ runs full representatives of divisor classes of $K$ of degree 0 which correspond to $L$ over $K$.

COROLLARY 3. Let $K$ and $n$ be as in Theorem, and $m$ be a positive integer. Then, the number of unramified $D_{n,p^m}$-extensions of $K$ is equal to
\[ \sum_A \left( \frac{p^m \gamma_A - p^{(m-1)} \gamma_A}{p^m - p^{m-1}} \right), \]
where $\{A\}$ are as in Theorem.

§ 3. Some lemmas.

Let $K$ be an algebraic function field with an algebraically closed constant field of characteristic $p$, and $L$ be an unramified abelian extension of exponent $p-1$.

Let $W_L = \bigcap (\mathfrak{p} K \cap L)/\mathfrak{p} L = U_L/\mathfrak{p} L$. Since $n$ divides $p-1$, $\mathfrak{p}(\theta K) \subseteq \theta K$ for $\theta \in \Delta_L$. Hence we can define a sub-module $W_{\theta K}$ of $W_L$ by
\[ W_{\theta K} = U_{\theta K}/\mathfrak{p} \theta K \] (cf. § 1).

Let $A$ be a $Gal(L/K)$-module. Then we put for any element $\chi$ of $\text{Hom}(Gal(L/K), F_p^*)$,
\[ A^\chi = \{ u \in A | u^\sigma = \chi(\sigma) u \}. \]

LEMMA 1. Let $L$ be an abelian extension of $K$ of exponent $p-1$. Then,
\[ W_L = \bigoplus_{\theta \in \Delta_L/K^*} W_{\theta K} \]
and
\[ W_{\theta K} = W_{\chi^\theta} \]
where $\chi_\theta$ is an element of $\text{Hom}(Gal(L/K), F_p^*)$ corresponding to $\theta$ (cf. § 1).

PROOF. Let $u$ be an element of $U_L$. Since $L = \bigoplus_{\theta} \theta K = \bigoplus_{\theta} L^{2^\theta}$, $u$ can be expressed as
\[ u = \sum_{\theta} a_\theta, \]
where $a_\theta \in \theta K = L^{2^\theta}$ and the sum runs full representatives of $\Delta_L/K^*$. Then for
any element \( \sigma \) of \( \text{Gal}(L/K) \),

\[ u^\sigma = \sum_{\sigma \in \text{Gal}(L/K)} \chi_\theta(\sigma) a_\theta. \]

We note that

\[ \sum_{\sigma \in \text{Gal}(L/K)} \chi_\theta(\sigma) = \begin{cases} n & \text{if } \theta \in K^* \text{ where } n = \# \text{Gal}(L/K), \\ 0 & \text{if } \theta \in K^c. \end{cases} \]

Hence \( a_\theta \) can be expressed as

\[ a_\theta = \frac{1}{n} \sum_{\sigma \in \text{Gal}(L/K)} \chi_\theta(\sigma)^{-1} u^\sigma, \]

that is, \( a_\theta \in U_{\theta K} \).

Since \( L = \bigoplus_{\theta} \theta K \) and \( n \) divides \( p-1 \),

\[ U_L = \bigoplus_{\theta} U_{\theta K} \quad \text{and} \quad \mathfrak{m} L = \bigoplus_{\theta} \mathfrak{m} \theta K. \]

Hence,

\[ W_L = U_L / \mathfrak{m} L = (\bigoplus_{\theta} U_{\theta K}) / (\bigoplus_{\theta} \mathfrak{m} \theta K) \approx \bigoplus_{\theta} W_{\theta K}. \]

So the first assertion holds.

On the other hand, since \( n \) divides \( p-1 \), \( W_L \) can be expressed as

\[ W_L = \bigoplus_{\theta} W_{\theta K} \]

and \( W_{\theta K} \subset W_{\theta L} \). Then the second assertion holds from these facts and the first assertion.

**Lemma 2.** Let \( K, L \) be as in Lemma 1. Let \( M \) be an unramified Galois extension of \( K \) of \((n, p)\) type containing \( L \). (For the definition of \((n, p)\) type, see §2). Then there is an element \( \theta \) of \( \Delta_L \) and a subgroup \( \langle a \mod \mathfrak{m} \theta K \rangle \) of \( W_{\theta K} \) of order \( p \) such that \( M \) is generated over \( L \) by an element \( 1 / \mathfrak{m} (a) \). Moreover \( \theta \mod K^* \) and the subgroup \( \langle a \mod \mathfrak{m} \theta K \rangle \) is uniquely determined by \( M \). Conversely for a subgroup \( \langle a \mod \mathfrak{m} \theta K \rangle \) of \( W_{\theta K} \) of order \( p \), \( L(1 / \mathfrak{m} (a)) \) is an unramified Galois extension of \( K \) of \((n, p)\) type containing \( L \).

**Proof.** It follows from the Artin-Shreier theory that \( M \) is an unramified cyclic extension of \( L \) of degree \( p \) if and only if there exists a unique subgroup \( \langle a \mod \mathfrak{m} L \rangle \) of \( W_L \) of order \( p \) such that \( M = L(1 / \mathfrak{m} (a)) \). Moreover, \( M \) is a Galois extension of \( K \) if and only if for any \( \sigma \in \text{Gal}(L/K) \),

\[ L \left( \frac{1}{\mathfrak{m}} (a^\sigma) \right) = L \left( \frac{1}{\mathfrak{m}} (a) \right). \]

It holds if and only if \( \langle a^\sigma \mod \mathfrak{m} L \rangle = \langle a \mod \mathfrak{m} L \rangle \). That is, \( \langle a \mod \mathfrak{m} L \rangle \) is a \( \text{Gal}(L/K) \)-module. Hence there is an element \( \chi \) of \( \text{Hom}(\text{Gal}(L/K), F_p^* \) such
that \( \langle a \mod pL \rangle \subset W^L \). It follows from the Kummer theory and Lemma 1 that there exists an element \( \theta \) of \( \Delta_L \) such that \( W^L = W_{\theta K} \). Hence \( \langle a \mod pL \rangle \subset W_{\theta K} \).

Assume that \( \langle a \mod pL \rangle \subset W_{\theta K} \) for \( \theta' \) of \( \Delta_L \). Then, it follows from Lemma 1 that \( W_{\theta K} \cap W_{\theta' K} = 0 \) if \( \theta \equiv \theta' \mod K^* \). Hence \( \theta \equiv \theta' \mod K^* \).

Conversely, let \( \langle a \mod pL \rangle \) be a cyclic subgroup of \( W_{\theta K} \) of order \( p \). Then it is clearly a \( \text{Gal}(L/K) \)-module. Hence \( L(1/\langle a \rangle) \) is a Galois extension of \( K \) of \( (n, p) \) type containing \( L \). q.e.d.

**COROLLARY.** Let \( K, L \) be as in Lemma 2. Then there is a one-to-one correspondence between the set of unramified extensions of \( K \) of \( (n, p) \) type containing \( L \) and the set

\[
\bigcup_{\theta \in \Delta_L/K^*} \{ \text{subgroup of } W_{\theta K} \text{ of order } p \}.
\]

**PROOF.** We put

\[
U = \{ \text{unramified extensions of } (n, p) \text{ type containing } L \}
\]

and

\[
S = \bigcup_{\theta \in \Delta_L/K^*} \{ \text{subgroups of } W_{\theta K} \text{ of order } p \}.
\]

It follows from Lemma 2 that for any element \( M \) of \( U \), there is an element \( \langle a \mod pL \rangle \) of \( S \) such that \( M = L(1/\langle a \rangle) \), and that this \( \langle a \mod pL \rangle \) is uniquely determined by \( M \). Hence there is a mapping from \( U \) into \( S \). Conversely for any element \( \langle a \mod pL \rangle \) of \( S \), \( L(1/\langle a \rangle) \) is an unramified extension of \( (n, p) \) type, that is, an element of \( U \). Moreover if \( \langle a_1 \mod pL \rangle = \langle a_2 \mod pL \rangle \), \( L(1/\langle a_1 \rangle) = L(1/\langle a_2 \rangle) \). Hence the above correspondence is one-to-one.

q.e.d.

**REMARK 1.** Let \( K, L \) be as in Lemma 2. Let

\[
S_\theta = \{ \text{subgroups of } W_{\theta K} \text{ of order } p \}.
\]

It follows from Lemma 1 that \( S_\theta \cap S_{\theta'} = \emptyset \) if \( \theta \equiv \theta' \mod K^* \). Therefore it follows from the corollary to Lemma 2 that the number of unramified extensions of \( K \) of \( (n, p) \) type containing \( L \) is equal to

\[
\sum_{\theta \in \Delta_L/K^*} \#S_\theta.
\]

**REMARK 2.** Let \( L = K(\theta) \) be an unramified cyclic extension of \( K \) such that \([L : K]\) divides \( p - 1 \). We put \( n = [L : K] \). Then it follows from Lemma 2 that an unramified Galois extension of \( K \) of \( (n, p) \) type containing \( L \) is generated over by an element \( 1/p(\langle a \rangle) \), where \( \langle a \mod pL \rangle \) is an element of \( S_{\theta} \). Then, \( K(1/p(\langle a \rangle)) \) is an unramified \( D_{n_{\theta}} \)-extension of \( K \), where \( n_{\theta} = [K(\theta) : K] \).
In fact if we put \( v = 1/p(\alpha) \), the conjugates of \( v \) have the forms \( \zeta^i(v+i) \), with \( i \in F_p \) and \( \zeta \) a primitive \( n_0 \)-th root of unity. We define elements of \( \text{Gal}(K(v)/K) \) as follows:

\[ \tau(v) = \zeta v, \sigma(v) = v + 1. \]

Then \( \tau^n(v) = \sigma^n(v) = 1 \), and \( \tau \sigma^{-1}(v) = v + \zeta^{-1} \). Since \( \zeta \) is a primitive \( n_0 \)-th root of unity and contained in \( F_p \), \( \langle \sigma, \tau \rangle \cong D_{n_0p} \). On the other hand \( \# \text{Gal}(K(v)/K) = \#D_{n_0p} = n_0 p \). Hence \( \text{Gal}(K(v)/K) \cong D_{n_0p} \).

Therefore, \( K(v) \) is an unramified \( D_{n_0p} \)-extension of \( K \) if and only if \( \langle \alpha \mod \mathfrak{p} \rangle \) is an element of \( S_{n_0} \), with \( i \) an integer prime to \( n \). Therefore, the number of unramified \( D_{n_0p} \)-extensions of \( K \) containing \( L \) is equal to

\[ \sum_{\langle \alpha \rangle \in S_{n_0}} \#S_{n_0}. \]

§ 4. Proof of the Theorem.

Let \( L = K(\theta) (\theta^n \in K) \) be an unramified cyclic extension of \( K \) of degree \( n \). We assume that \( n \) divides \( p-1 \). Let \( A \) be a divisor of \( K \) which corresponds to \( \theta \) as in § 1. It follows from Remark 2 after Lemma 2 that there is one-to-one correspondence between the set of unramified \( D_{n_0p} \)-extensions of \( K \) containing \( L \) and the set \( \bigcup_{(i,n)=1} S(i) \), where \( S(i) \) is the set of subgroups of order \( p \) as defined in Remark 1 after Lemma 2. Therefore, the proof of Theorem can be reduced to the fact

\[ (\ast) \quad p^{\alpha} = \#W_A. \]

If \( A \in \mathfrak{D}_H \), this is nothing but the theory of Hasse-Witt [4]. Hence we assume that \( A \notin \mathfrak{D}_H \). In this case, we can prove \( (\ast) \) using the method shown in Hasse-Witt [4].

PROPOSITION 1. There are distinct primes \( \mathfrak{p}_1, \ldots, \mathfrak{p}_{g-1} \) of \( K \) such that

\[ \dim_k \Omega(A\mathfrak{p}_1 \cdots \mathfrak{p}_{g-1}) = 0, \text{ that is } l(A\mathfrak{p}_1 \cdots \mathfrak{p}_{g-1}) = 0. \]

PROOF. Since \( \dim_k \Omega(A) = g-1 > 0 \), there is a non-zero element \( \omega_i \) of \( \Omega(A) \).

The zeroes of \( \omega_i \) are finite, so there is a prime divisor of \( K \) such that \( \nu_{\mathfrak{p}_i}(\omega_i) < \nu_{\mathfrak{p}_i}(A\mathfrak{p}_i) \). Hence \( \Omega(A) \supset \Omega(A\mathfrak{p}_i) \), so \( \dim_k \Omega(A) - \dim_k \Omega(A\mathfrak{p}_i) > 0 \). On the other hand,

\[ \dim_k \Omega(A\mathfrak{p}_i) = g-2 + l(A\mathfrak{p}_i) \]

and

\[ \dim_k \Omega(A) = g-1. \]

Since \( l(A\mathfrak{p}_i) \geq 0 \), \( \dim_k \Omega(A) - \dim_k \Omega(A\mathfrak{p}_i) \leq 1 \). Hence \( \dim_k \Omega(A\mathfrak{p}_i) = g-2 \). Assume that there are distinct \( i \) primes \( \mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_t} \) of \( K \) such that \( \dim_k \Omega(A\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_t}) = g-1-i \). If \( i = g-1 \), the assertion holds. If \( \mathfrak{p}_{i_1} \), then using the above arguments, we can show that there is a prime divisor \( \mathfrak{p}_{i+1} \) such that \( \dim_k(A\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_t} \mathfrak{p}_{i+1}) = g-2-i \). By induction on \( i \), the assertion holds.
Let us take a prime divisor $G_i$ of $L$ which is an extension of $G_i$ and take a prime element $a_i$ with respect to $L_{a_i}$. Since any prime divisor of $K$ is completely decomposed in $L$, $K_{a_i}=L_{a_i}$. Hence, we can take an element of $K_{a_i}$ especially of $K$ as a prime element of $L_{a_i}$. Since $\theta$ is contained in $K_i$ for all prime divisors $i$ of $K$, there is an element $\xi$ of the adele ring $R_K$ of $K$ such that $(\xi)_i=\theta$, where $(\xi)_i$ is the $i$-th component of $\xi$. Hereafter, we shall denote $\xi$ simply denote by $\theta$. Let $r_i$ be an element of the adele ring $R_K$ such that

$$(r_i)_i=0 \quad \text{if } i \neq i$$

$$(r_i)_i=1/\pi_i \quad \text{if } i=i.$$}

**Proposition 2.** There exists a matrix $B_A$ of $M_{g-1}(k)$ such that

$$(r^p)_i=B_A(r_i) \pmod{\theta K+R_K(0)},$$

where $R_K(0)=\{r \in R_K \mid \nu_i((r)_i) \geq 0\}$.

**Proof.** Since $l(A\delta_1 \cdots \delta_{g-1})=\nu+(g-2)-g+1=\nu-1$, there is an element $v_{i,v}$ of $K$ such that $\nu_i(v_{i,v})=-\nu$, $\nu_{i'}(\theta v_{i,v}) \geq -1$ if $i \neq j$, and $\nu_{i'}(\theta v_{i,v}) \geq 0$ is $\mathcal{O}' \neq \mathcal{O}'_i$, $\mathcal{O}'_j$ for any integer $\nu \geq 2$. Since $L_{a_i}=k((\pi_i))$, we can express $\theta v_{i,v}$ as

$$\theta v_{i,v}=\sum_{i \neq j} c_i \pi_i^j$$

where $c_i$ is an element of $k$ and $c_{-\nu} \neq 0$. We can choose $\theta v_{i,v}$ so that $c_{\nu}=1$. Then,

$$\nu_{a_1}(\theta v_{i,v}-(1/\pi_i)^p-c_{-\nu}(\theta v_{i,v})) \geq -(p-2)$$

$$\nu_{a_j}(\theta v_{i,v}-c_{-\nu}(\theta v_{i,v})) \geq -1 \quad \text{if } i \neq j,$$

$$\nu_{a_i}(\theta v_{i,v}-c_{-\nu}(\theta v_{i,v})) \geq 0 \quad \text{if } \mathcal{O}' \neq \mathcal{O}'_i \text{ and } \mathcal{O}'_j.$$ 

Repeating this process, we can show that there are elements $v_i$ of $K$ and $b_{ij}$ of $k$ such that

$$\nu_{a_i}(1/\pi_i)^p-\sum_{j=1}^{g-1} b_{ij}(1/\pi_j)-\theta v_i \geq 0,$$

$$\nu_{a_i}(\theta v_i) \geq 0 \quad \text{if } \mathcal{O}' \neq \mathcal{O}'_i.$$ 

We put $B_A=(b_{ij})$. Then, it follows from the above formulas that

$$r^p=\sum_{j=1}^{g-1} b_{ij} r_j - \theta v_i \in R_K(0).$$

q.e.d.
Let \( \{\mathfrak{O}_i\}_i \) be a divisor system that is defined in Proposition 1. Then, we put
\[
L_L(\mathfrak{O}_p^i \cdots \mathfrak{O}_p^{i-1}) = \{x \in L \mid \nu_{\mathfrak{O}}(x) \geq -\nu_{\mathfrak{O}}(\mathfrak{O}_p^i \cdots \mathfrak{O}_p^{i-1}) \text{ for any prime } \mathfrak{O} \text{ of } L \}
\]
and
\[
V_{\theta_K} = \bigcap_{i=1}^{g-1} (\theta K \cap pK_{\mathfrak{O}_i} \cap L_L(\mathfrak{O}_p^i \cdots \mathfrak{O}_p^{i-1})).
\]
Then in the following proposition, we shall consider the relation between \( V_{\theta_K} \) and \( W_{\theta_K} = \bigcap_i (\theta K \cap pK_{\mathfrak{O}_i})/p\theta K \).

**Proposition 3.** \( W_{\theta_K} \subseteq V_{\theta_K} \).

**Proof.** Let \( u \) be an element of \( V_{\theta_K} \). If \( u \) is integral at a prime divisor \( \mathfrak{O}' \) of \( L \), it follows from Hensel’s lemma and the fact that \( k \) is algebraically closed that \( u \) is contained in \( p\mathfrak{O}_{\mathfrak{O}'} \). Hence \( u \) mod \( pK_{\mathfrak{O}'} \in W_{\theta_K} \). Conversely for any unramified element \( u \) of \( \theta K \), we are going to prove that there exists an element \( \theta u \) of \( V_{\theta_K} \) such that \( u \equiv \theta u \pmod{p K_{\mathfrak{O}'} / p \theta K} \).

First take a prime \( \mathfrak{O}' \) of \( L \) such that \( \mathfrak{O}' \neq \mathfrak{O}_i \). If \( \nu_{\mathfrak{O}}(u) \geq 0 \), \( u \) belongs to \( \mathfrak{O}_{\mathfrak{O}'} \). Assume that \( \nu_{\mathfrak{O}}(u) < 0 \). Then there exists an integer \( m \) such that \( \nu_{\mathfrak{O}}(u) = -pm \). Let \( \mathfrak{O} \) be the restriction of \( \mathfrak{O}' \) to \( K \). Since \( l(\mathfrak{O}_{\mathfrak{O}_i} \cdots \mathfrak{O}_{\mathfrak{O}_i} \mathfrak{O}^m) \geq 1 \), there is an element \( v' \) of \( K \) such that \( \nu_{\mathfrak{O}}(\theta v') = -m, \nu_{\mathfrak{O}}(\theta v') = -1 \), and \( \nu_{\mathfrak{O}}(\theta v') \geq 0 \) otherwise. Hence \( \theta v' \) can be expressed in \( K_{\mathfrak{O}} \) as
\[
\theta v' = \sum_{i=-m}^{\infty} a_i \pi^i,
\]
where \( \pi \) is a prime element of \( K_{\mathfrak{O}} \) and \( a_i \in k \). Similarly \( u \) can be expressed as
\[
u_{\mathfrak{O}}(u-p(\theta v')) \geq -p(m-1), \quad (m \geq 2), \quad \nu_{\mathfrak{O}}(u-p(\theta v')) \geq \min(0, \nu_{\mathfrak{O}}(u))
\]
if \( \mathfrak{O}' \) is a prime of \( L \) which is different from \( \mathfrak{O}_i \) and \( \mathfrak{O}_i' \). Repeating this process, we can show that there is an element \( v^* \) of \( K \) such that
\[
\nu_{\mathfrak{O}}(u-p(\theta v^*)) \geq 0
\]
for any prime divisor \( \mathfrak{O}' \) of \( L \) which is different from \( \mathfrak{O}_i \). Since \( u \in \bigcap_{i=1}^{g-1} (\theta K \cap pK_{\mathfrak{O}_i}) \), there is the set of integers \( k_i \) such that \( \nu_{\mathfrak{O}_i}(u) = -p k_i \). Let \( m \) be the largest number of \( k_i \). Then the assertion holds if we have \( m \leq 1 \). Assume that \( m > 1 \). Then since \( l(\mathfrak{O}_{\mathfrak{O}_i} \cdots \mathfrak{O}_{\mathfrak{O}_i} \mathfrak{O}^m) = k_i - 1 \), for any integer \( k_i \) such that \( k_i \geq 2 \), there is an element \( v_{h_i} \) of \( K \) such that
\[ \nu_{q_i}(\theta v_{k_i}) = -k_i \]
\[ \nu_{q_j}(\theta v_{k_j}) \geq -1 \text{ if } i \neq j \]
\[ \nu_{q}(\theta v_{k_i}) \geq 0 \text{ if } \mathcal{O}' \text{ is a prime divisor different from } \mathcal{O}_i \text{ and } \mathcal{O}_j. \]

We can express \( u \) and \( \theta v_{k_i} \) as
\[ u = \sum_{j \geq -p + k_i} b_j \pi^j, \quad \theta v_{k_i} = \sum_{j \geq -k_i} a_j \pi^j, \]
with \( \pi \) a prime element of \( K \). Then there is an element \( a \) of \( k \) such that \( a^p = b_{-k_i} \). We can take \( u \) as \( a_{-k_i} = a \). Then,
\[ \nu_{q}(u - \nu(\theta v_{k_i})) \geq -p + (m - 1) \quad \text{if } \mathcal{O}' = \mathcal{O}_i \]
\[ \geq \min(-p, \nu_{q}(u)) \quad \text{if } \mathcal{O}' \neq \mathcal{O}_i \quad (i \neq j) \]
\[ \geq \min(0, \nu_{q}(u)) \quad \text{if } \mathcal{O}' \neq \mathcal{O}_i, \mathcal{O}_j. \]

Repeating this process, we can show that there is an element \( v \) of \( K \) such that
\[ \nu_{q}(u - \nu(\theta v)) \geq -p \quad \text{if } \mathcal{O}' = \mathcal{O}_i, \]
\[ \geq 0 \quad \text{if } \mathcal{O}' \neq \mathcal{O}_i. \]

That is, \( u - \nu(\theta v) \in L_L(\mathcal{O}_i^p \cdots \mathcal{O}_g^p) \). Since \( \theta^{p-1} \in K \), there is an element \( w \) of \( K \) such that \( \theta w = u - \nu(\theta v) \). Then \( w \) satisfies the required conditions.

We note that this fact implies that the homomorphism \( f \) of \( V_{\theta K} = \bigcap_{i=1}^{g-1}(\theta K \cap pK_{a_i}) \cap L_L(\mathcal{O}_i^p \cdots \mathcal{O}_g^p) \) into \( W_{\theta K} = \bigcap_{\mathcal{O}}(\theta K \cap K_{a_i})/p\theta K \) defined by
\[ f : V_{\theta K} \longrightarrow W_{\theta K} \]
\[ u \quad u \mod p\theta K \]

is a surjective homomorphism.

Finally, let \( u \) be an element of \( V_{\theta K} \) such that \( u \equiv 0 \mod p\theta K \). Then \( u \) can be expressed as \( u = (\theta x)^p - \theta x \) with an element \( x \) of \( K \). Since \( u \in L_L(\mathcal{O}_i^p \cdots \mathcal{O}_g^p) \), \( \nu_{q_i}(\theta x) \geq -\nu_{q_i}(\theta x) \), that is \( \nu_{q_i}(x) \geq -\nu_{q_i}(A_{\mathcal{O}_i}) \) for any \( 1 \leq i \leq g-1 \) and \( \nu_{q}(x) \geq -\nu_{q}(A) \) for any prime divisor different from \( \mathcal{O}_i \). This implies \( x \in L_K(A_{\mathcal{O}_i} \cdots \mathcal{O}_{g-1}) \).

On the other hand, it follows from the choice of \( \mathcal{O}_i \) that \( \dim_K L_K(A_{\mathcal{O}_i} \cdots \mathcal{O}_{g-1}) = 0 \). Hence we have \( x = 0 \). This implies that \( f \) is injective.

We put
\[ R_A = \{ \langle c_i \rangle \} \in k^{g-1} \mid \langle c_i \rangle B_A = \langle c_i \rangle \} \]

This is an \( F_p \)-vector space of finite rank. Now we are going to calculate the rank of \( W_{\theta K} = \bigcap_{\mathcal{O}}(\theta K \cap K_{a_i})/p\theta K \) in terms of \( R_A \).
PROPOSITION 4. \( V_{\theta K} \cong R_A \).

PROOF. Let us take an element \( u \) of \( V_{\theta K} \). Then there is an element \( c_i \) of \( k \) such that
\[
\theta u = (c_i/\pi_i)^p - c_i/\pi_i \quad \text{(mod } \mathcal{O}_k)\text{),}
\]
that is, \( \theta u \equiv \langle \tau \rangle (c_i)(r_i) \quad \text{(mod } R_K(0)) \). \hspace{1cm} (1)

On the other hand, by Proposition 2,
\[
\langle \tau \rangle \equiv B_A(r_i) \quad \text{(mod } R_K(0)+\theta K)\text{).}
\]
That is, there is an element \( v_i \) of \( K \) such that
\[
\langle \theta v_i \rangle = \langle \tau \rangle - B_A(r_i) \quad \text{(mod } R_K(0)) \hspace{1cm} (2)
\]
Hence
\[
\langle \tau \rangle (\theta v_i) = \langle \tau \rangle (c_i)(r_i) - \langle \tau \rangle B_A(r_i) \quad \text{(mod } R_K(0)) \hspace{1cm} (3)
\]
It follows from (1) and (3) that
\[
\theta (u - \langle \tau \rangle (v_i)) = \langle \tau \rangle B_A(r_i) \hspace{1cm} (\text{mod } L_K(A\mathfrak{S}_1 \cdots \mathfrak{S}_{g-1}))\]
It follows from the choice of \( \mathfrak{S}_1, \cdots, \mathfrak{S}_{g-1} \) that
\[
u - \langle \tau \rangle (v_i) = 0.
\]
Hence \( \langle \tau \rangle (c_i)(r_i) - \langle \tau \rangle B_A(r_i) = 0 \). Hence \( \langle \tau \rangle (c_i)(r_i) B_A(r_i) = 0 \), that is, \( \langle \tau \rangle (c_i) \in R_A \). If \( u = 0 \), \( \langle \tau \rangle (v_i) = 0 \). Hence we have \( \langle \tau \rangle (\theta v_i) = 0 \). It follows from (2) that \( \{ \theta v_i \} \) is linearly independent over \( k \). Hence we have \( (c_i) = 0 \). Therefore we can define a homomorphism \( g \) of \( V_{\theta K} \) into \( R_A \) as follows:
\[
g : V_{\theta K} \rightarrow R_A
\]
\[
\theta u \rightarrow (c_i)
\]
such that \( u = \langle \tau \rangle (v_i) \).

We are going to show that this homomorphism is an isomorphism. Let \( \langle \tau \rangle (c_i) \) be an element of \( R_A \). Then,
\[
\langle \tau \rangle (\theta v_i) = \langle \tau \rangle (r_i) - \langle \tau \rangle B_A(r_i) \quad \text{(mod } R_K(0)) \hspace{1cm} (4)
\]
Hence \( \theta u = \sum \langle \tau \rangle \theta v_i \in V_{\theta K} \). This implies that \( g \) is surjective. Finally if \( (c_i) = 0 \), then we have \( u = 0 \). This implies that \( g \) is injective. Hence we have \( R_A \cong W_{\theta K} \).
\hspace{1cm} q. e. d.
It follows from Satz 10 of Hasse-Witt [4] that
\[ \text{rank}_{F_p} R_A = \delta_A, \]
where \( \delta_A \) is the rank of \( B_A B_A^{-1} \cdots B_A^{-(p-1)} \). Therefore the proof of Theorem is completed if we have the following proposition.

**Proposition 5.** \( \delta_A = \gamma_A. \)

**Proof.** We put
\[ R(A) = \{ r \in R_K | \nu_i((r)) \equiv -\nu_p(A) \text{ for any prime } \mathfrak{p} \text{ of } K \}. \]

Let \( r_i \) be elements of \( R_K \) that are defined in Proposition 2. Assume that
\[ \sum_{i=1}^{p-1} c_i r_i / \theta \equiv 0 \pmod{R(A)+K} \text{ with elements } c_i \text{ of } k. \]

Let \( v \) be an element of \( K \) such that
\[ \sum_{i=1}^{p-1} c_i r_i / \theta \equiv v(R(A)) \text{ for some } c_i \text{ of } k. \]

Then, \( \nu_{\mathfrak{p}}(\theta v) \equiv -1 \) for any prime divisor \( \mathfrak{p}_i \) that is defined in Proposition 1. Since \( l(A \mathfrak{p}_1 \cdots \mathfrak{p}_{g-1}) = 0 \), we have \( v = 0 \). That is,
\[ \sum_{i=1}^{p-1} c_i r_i \equiv 0 \pmod{R_K(0)}. \]

Therefore, we have \( c_i = 0 \) for all \( i \). This implies that \( \{ r_i / \theta \pmod{R(A)+K} \} \) is linearly independent over \( k \). On the other hand, \( \dim_k (R_K / (R(A)+K)) = \dim_k \Omega(A) = g-1 \). Hence
\[ \{ r_i / \theta \pmod{R(A)+K} \} \text{ forms a basis of } R_K / (R(A)+K). \]

Therefore, we can choose the dual basis \( \omega_1, \cdots, \omega_{g-1} \) of \( \Omega(A) \) such that
\[ (\omega_i, r_i / \theta) = \delta_{ij}, \]
where \( (\omega, \zeta) = \sum \text{Res}_w \omega \zeta \) for any \( \omega \in \Omega(K/k) \) and \( \zeta \in R_K \) (cf. [7]). Here the following formula holds for any \( \omega \in \Omega(K/k) \) and \( \zeta \in R_K ; \)
\[ (\omega, \zeta^p) = (C\omega, \zeta)^p \text{ (cf. Lang [6])}. \]

Let \( B_A = (b_{ij}) \) be as in Proposition 2. Then,
\[ b_{ji} = (\omega_i, \sum b_{jk} r_k / \theta) \text{ and } r_{ji}^p \equiv \sum b_{jk} r_k \pmod{R(A)+\theta K}. \]

Hence
\[ (\omega_i, \sum b_{jk} r_k / \theta) = (\omega_i, r_{ji}^p / \theta) = (\omega_i, \theta^{p-1}(r_{ji}/\theta)^p) \]
\[ = (\omega_i, x(r_{ji}/\theta)^p) = (x\omega_i, (r_{ji}/\theta)^p) = (C(x\omega_i), (r_{ji}/\theta))^p. \]
Generalized Hasse-Witt invariants

Let $C_A=(c_{ij})$ be as in § 2. Then, $c(x_\omega)=\sum c_{ij}\omega_i$. Hence

$$b_{ij}=\left(\sum c_{ij}\omega_i, r_j/\theta\right)^p=c_{ij}^p.$$

Hence $\lambda A=B_A$. Hence $\lambda A=q_A$.

**COROLLARY 1.** Let $n$ be prime to $p$. Let $K$ be an algebraic function field with an algebraically closed constant field $k$. Then the number of unramified Galois extensions of $K$ of $(n, p)$ type is determined by $\lambda A$, where $\lambda A$ is a complete set of representatives of divisor classes of degree 0 whose orders divide $p-1$ and $n$.

**PROOF.** Let $L$ be an unramified abelian extension of $K$ of degree $n$. Then it is sufficient to prove that the number of unramified Galois extensions of $K$ of $(n, p)$ type containing $L$ is determined by $\lambda A$.

Let $M$ be an unramified Galois extension of $K$ of $(n, p)$ type containing $L$. $G=\text{Gal}(M/K)=\text{Gal}(L/K)\cdot\text{Gal}(M/L)$ because $n$ is prime to $p$. We put $A=\text{Gal}(L/K)$ and $P=\text{Gal}(M/L)$. Then, $|A|=n$ and $|P|=p$, and $P\triangleleft\text{Gal}(M/K)$. Let $L_1$ be the subfield of $L$ which corresponds to the centralizer of $P$ in $G$. Then, $M$ is an abelian extension of $L_1$. Hence there is a unique cyclic extension $M_1$ of $L_1$ of degree $p$ such that $M=M_1\cdot L$. It is easy to say that $\text{Gal}(M/M_1)$ is a normal subgroup of $\text{Gal}(M/K)$. Since $\text{Gal}(L_1/K)\cong G/C_0(P)$ is isomorphic to a subgroup of $\text{Aut}(P)=P^\ast$, $L_1$ is an unramified cyclic extension of degree dividing $p-1$. We put $n_1=[L_1: K]$.

Now we are going to prove that $\text{Gal}(M/K)$ is isomorphic to

$$D_{n_1} = \angle \sigma, \tau | \sigma^p = \tau^* = 1 \text{ and } \tau \sigma \tau^{-1} = \sigma^i$$

with $i$ a primitive $n_1$-th root of unity mod $p$.

In fact, let $G_1=\text{Gal}(M_1/K)$, $P_1=\text{Gal}(M_1/L_1)$, and $A_1=\text{Gal}(L_1/K)$. It is sufficient to show that $C_{A_1}(P_1)$ is $P_1$. Since $G_1 = G/\text{Gal}(M/M_1)$, for any element $\tau$ of $C_{A_1}(P_1)$, $\tau$ mod $\text{Gal}(M/M_1)$ belongs to $C_{A_1}(P_1)$. Conversely, let $\tau$ be an element of $G$ such that $\tau$ mod $\text{Gal}(M/M_1)$ belongs to $C_{A_1}(P_1)$. Then, $\tau \sigma \tau^{-1} \sigma^{-1} \in \text{Gal}(M/M_1) \cap P=\{1\}$. Hence, $\tau$ is an element of $C_{A_1}(P_1)$. Hence, $C_{A_1}(P_1)=P_1$.

It follows from the above consideration that any unramified Galois extension of $K$ of $(n, p)$ type containing $L$ is a compositum of $L$ and an unramified $D_{n_1}$-extension of $K$. Conversely, let $L_1$ be the subfield of $L$ whose Galois group over $K$ is cyclic of order $n_1$ dividing $p-1$. Let $M_1$ be an unramified $D_{n_1}$-extension of $K$ containing $L_1$. Then, $M=M_1\cdot L$ is a Galois extension of $K$ of $(n, p)$ type containing $L$. Moreover $\text{Gal}(M/L_1)=C_0(P)$, where $P=\text{Gal}(M/L)$, $G=\text{Gal}(M/K)$. In fact, let $L_2$ be the subfield of $L$ corresponding to $C_0(P)$. We put $G_1=\text{Gal}(M_1/K)$ and $P_1=\text{Gal}(M_1/L_2)$. Since $\text{Gal}(M/L_1)$ is abelian and $\text{Gal}(M/L_1)$ is $C_0(P)$, $\text{Gal}(M/L_2)\triangleleft\text{Gal}(M/L_1)$. On the other hand, since $G_1=D_{n_1}$, $P_1=C_{A_1}(P_1)$. That is, $P_1=\text{Gal}(M_1/L_2)=\text{Gal}(M_1/L_2)$. Hence, $L_2=L_1$. 
It follows from the above considerations that the number of unramified Galois extensions of $K$ of $(n, p)$ type containing $L$ is determined by \{\gamma_A\} where \{A\} is the set of divisors which satisfies the conditions stated in Corollary 1.

Corollary 2. Let $K$ be as in Theorem and let $L$ be an unramified abelian extension of $K$ of exponent $p-1$. Then, the Hasse-Witt invariant $\gamma_L$ of $L$ is equal to $\sum A$, where $A$ runs full representatives of divisor classes of degree $0$ which correspond to $L$ over $K$.

Proof. It follows from Lemma 1 that

$$W_L = \bigcap_i (pK_i \cap L)/pL = \bigoplus \theta W_{\theta K}$$

where the sum runs full representatives of $\Delta_L/K^*$. On the other hand, it follows from the proof of Theorem that the $F_p$-rank of $W_{\theta K}$ is $\gamma_A$, where $A$ is a representative class of $K$ corresponding to $\theta$. Therefore

$$\gamma_L = \text{rank}_{F_p} W_L = \sum A.$$  

q. e. d.

§ 5. Remarks and generalizations.

Now, we shall consider unramified Galois extensions of $K$ of $(n, p^n)$ type. We assume that $n$ divides $p-1$ and mainly consider unramified $D_{np^n}$-extensions of $K$ (cf. Corollary 3 to Theorem).

First, we review the properties of Witt vectors. Let $R$ be a commutative ring of characteristic $p$. We denote by $W_m(R)$ the ring of Witt vectors of length $m$ with components in $R$ (cf. [8]). Let $a = (a_0, a_1, \ldots, a_{m-1})$, $b = (b_0, b_1, \ldots, b_{m-1})$ be elements of $W_m(R)$. Then, the $r$-th component of $a+b$ is expressed as

$$(a+b)_r = a_r + b_r + f_r(a_0, a_1, \ldots, a_{r-1}, b_0, b_1, \ldots, b_{r-1}),$$

where $f_r$ is an element of $F_p[X_0, X_1, \ldots, X_r, Y_0, Y_1, \ldots, Y_r]$, and $f_r(0, 0, \ldots, 0) = 0$. Similarly, the $r$-th component of $ab$ is also represented by such a form.

(a) Let $\overline{W}_m(R) = (a, 0, \ldots, 0)$ with $a \in R$.

Then this forms a multiplicative semigroup. Especially, if $R^*$ is a unit group of $R$, there is an isomorphism of $R^*$ onto $\overline{W}_m(R^*)$. We denote by $\bar{a}$ an element $(a, 0, \ldots, 0)$ of $\overline{W}_m(R)$. We note that, for any element $b$ of $W_m(R)$, $\bar{a}, b = (b_0, a, b_1, a^p, \ldots, b_{m-1}, a^{p^{m-1}})$. 

(b) We define the Frobenius endomorphism $F : W_m(R) \to W_m(R)$ by
$$F(a_0, a_1, \ldots, a_{m-1}) = (a_0^p, a_1^p, \ldots, a_{m-1}^p).$$
We define the $p$-operator by $\mathfrak{p}(a) = F(a) - a$. We note that the Frobenius endomorphism is $\mathbb{Z}/p^m\mathbb{Z}$-linear, and therefore the operator $\mathfrak{p}$ is also $\mathbb{Z}/p^m\mathbb{Z}$-linear.

(c) We define the shift $V : W_m(R) \to W_{m+1}(R)$ by
$$V(a_0, a_1, \ldots, a_{m-1}) = (0, a_0, a_1, \ldots, a_{m-1}).$$
This is an additive operator.

(d) We define the restriction $R : W_{m+1}(R) \to W_m(R)$ by
$$R(a_0, a_1, \ldots, a_{m-1}) = (a_0, a_1, \ldots, a_{m-1}).$$
This is a ring homomorphism, and commutes with the Frobenius endomorphism. Further, we have
$$RVF = FRV = RFV = p.$$  

The projective limit of the system $W_m(R)$ of rings with respect to the restriction is denoted by $W(R)$. It is a ring of characteristic zero on which the operators $F$ and $V$ are defined and satisfy the relation $FV = VF = p$. If $R = k$ is a perfect field of characteristic $p$, then, $W(k)$ is a complete valuation ring with the unique maximal ideal $pW(k)$. If $k = F_p$, this $W(k)$ is nothing but the ring of $p$-adic integers and $W(k)/p^mW(k) \cong \mathbb{Z}/p^m\mathbb{Z}$.

(e) We note that if $a_1, a_2, \ldots, a_r$ are elements of $R$ and if they are linearly independent over $F_p$, then, $\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_r$ are linearly independent over $\mathbb{Z}/p^m\mathbb{Z}$.

In fact, let $c_1, c_2, \ldots, c_r$ be elements of $\mathbb{Z}/p^m\mathbb{Z}$ such that $c = \sum c_i \tilde{a}_i = 0$. Then, the first component of $c$ has the form $\sum c_i^{(0)} a_i = 0$, with $c_i^{(0)} \in F_p$. Since $\{a_i\}$ are linearly independent over $F_p$, $c_i^{(0)} = 0$ for all $1 \leq i \leq r$. Assume that for all $1 \leq i \leq r$, and $1 \leq j \leq k-1$, the $j$-th components of the $i$-th component of $c$ are zero. Then, the $k$-th component of $c$ has the form
$$\sum_i c_i^{(k)} a_i^{(k)} + h_k(c_i^{(0)} a_1, c_i^{(0)} a_2, \ldots, c_i^{(0)} a_r, \ldots),$$
$$c_i^{(k+i)} a_i^{(k+i)} a_i^{(k-1)}, c_i^{(k+i)} a_i^{(k+i-1)}, \ldots, c_i^{(k+i)} a_i^{(k-1)}.$$  

Then, by the assumptions and the remark on the composition laws, $h_k(0, 0, \ldots, 0) = 0$, so $\sum c_i^{(k)} a_i^{(k)} = 0$. Since, $c_i^{(k)}$ are elements of $F_p$, we have $\sum c_i^{(k)} a_i = 0$. Since $\{a_i\}$ are linearly independent over $F_p$, we have $c_i^{(k)} = 0$ for all $1 \leq i \leq r$. By induction on $k$, $\{a_i\}$ are linearly independent over $\mathbb{Z}/p^m\mathbb{Z}$.

(f) Let $L$ be a field of characteristic $p$. Let $a = (a_0, a_1, \ldots, a_{m-1})$ be an element of $W_m(L)$. We denote by $1/p(a)$ a root of the equation $\mathfrak{p}(x) - a = 0$. 

---

**Generalized Hasse-Witt invariants** 117
Then, another root of the above equation is given by \( a + c \), where \( c \) is an element of \( W_m(F_p) = \mathbb{Z}/p^m\mathbb{Z} \). Especially, if \( a_0 \in \mathbb{P}L \), \( M = L(a_0, a_1, \ldots, a_r) \) is a cyclic extension of \( L \) of degree \( p^m \), where \( a_0, a_1, \ldots, a_{m-1} \) are the components of \( 1/p(a) \). Conversely, any cyclic extension of \( L \) of degree \( p^m \) is obtained as above.

Now, let \( L \) be an algebraic function field with an algebraically closed constant field \( k \), and \( L_i \) be the completion of \( L \) at \( \mathfrak{p} \). We put

\[
W_{m,L} = \bigcap_i \left( W_m(L) \cap p(W_m(L_i)) / pW_m(L) \right).
\]

If \( n = 1 \), \( W_{m,L} \) coincides with the set \( W_L \) defined in \( \S 1 \). It is well known that \( W_{m,L} \) is a \( \mathbb{Z}/p^m\mathbb{Z} \)-free module of rank \( \gamma_L \), where \( \gamma_L \) is the Hasse-Witt invariant of \( L \), and there is one to one correspondence between the set of unramified cyclic extensions of \( L \) of degree \( p^m \) and the set of cyclic sub-modules of \( W_{m,L} \) of order \( p^m \).

Let \( K \) be an algebraic function field with an algebraically closed constant field \( k \) and let \( g \) be its genus. Let \( L \) be an unramified cyclic extension of \( K \) of degree \( n \). We assume that \( n \) divides \( p-1 \), and \( L = K(\theta), \theta^m \in K \).

Then, we put

\[
W_m(\theta K) = \{ a = (a_0, a_1, \ldots, a_{m-1}) \in W_m(L), a_i \in \theta K \}.
\]

It follows from (a) that for any element \( (b_0, b_1, \ldots, b_{m-1}) \) of \( W_m(K) \), we have \( \theta b = (\theta b_0, \theta^p b_1, \ldots, \theta^{p^{m-1}} b_{m-1}) \). Since \( n \) divides \( p-1 \), we have \( \theta^{p^k-1} \in K \). Hence, we have \( \theta W_m(K) = W_m(\theta K) \). Therefore, \( W_m(\theta K) \) forms a subgroup of \( W_m(L) \). Moreover, we have \( F(W_m(\theta K)) \subset W_m(\theta K) \). Therefore, we can define a submodule \( W_{m,\theta K} \) of \( W_{m,L} \) by

\[
W_{m,\theta K} = \bigcap_i \left( W_m(\theta K) \cap pW(K_i) / W_m(\theta K) \right).
\]

We say an element \( a \) of \( \bigcap_i (W_m(A) \cap pW(K_i)) \) an unramified element of \( A \) for any submodule \( A \) of an unramified extension of \( K \).

**Lemma 3.** Let \( K, L \) be as above. Then, \( W_{m,\theta K} \) is a free \( \mathbb{Z}/p^m\mathbb{Z} \)-module of rank \( \gamma_{K,\theta} \), where \( \gamma_{K,\theta} \) is the integer defined in \( \S 2 \). Moreover, we have

\[
W_{m,L} = \bigoplus_{i=0}^{m-1} W_{m,\theta^i K}.
\]

**Proof.** If \( m = 1 \), this is nothing but Lemma 1. Assume that \( m > 1 \). It follows from the proof of Theorem that \( W_{\theta K} \) is an \( F_p \)-vector space of rank \( \gamma_{A,\theta} \). Hence, it follows from the above remark that \( W_{m,\theta K} \) contains a \( \mathbb{Z}/p^m\mathbb{Z} \)-free module of rank \( \gamma_{A,\theta} \).
In fact, let \( a^{i_0} \mod \theta^i K \) be a basis of \( W_{\theta^i K} \). Then,

\[
\{(a^{i_0}, 0, \ldots, 0) \mod \theta^i W_m(\theta^i K) \} \text{ are linearly independent over } Z/p^m Z.
\]

Using the same arguments, we can show that

\[
\{(a_{i^j}, 0, \ldots, 0) \mod \theta^i W_m(L) \} \text{ are linearly independent over } Z/p^m Z.
\]

Hence we have

\[
\sum_{i \in \hat{\kappa}} W_{m, \theta^i K} \cap W_{m, \theta^i K} = 0.
\]

On the other hand, it follows from Corollary 2 to Theorem that \( \gamma_L = \sum_{i=1}^{\frac{n-1}{m}} \gamma_{A^i} \).

Hence, \( W_{m, L} \cong \sum W_{m, \theta^i K} \), and \( W_{m, \theta^i K} \) is a free \( Z/p^m Z \) submodule of \( W_L \) of rank \( \gamma_{A^i} \).

**Lemma 4.** Let \( K, L \) be as above. Let \( M \) be an unramified \( D_{n, p^m} \)-extension of \( K \) containing \( L \). There exists an integer \( i \) prime to \( n \) and a cyclic subgroup \( \langle a \mod p W_m(\theta^i K) \rangle \) of \( W_{m, \theta^i K} \) of order \( p^m \) such that \( M \) is generated by the components of \( 1/\theta(a) \) over \( K \). This \( i \) and the subgroup is uniquely determined by \( M \). Conversely, for such an \( a \), a field generated by the components of \( 1/\theta(a) \) over \( K \) is a \( D_{n, p^m} \)-extension of \( K \) containing \( L \).

**Proof.** This is easily proved using the above lemma and the same arguments as in the proof of Lemma 2 and in Remark 2 after Lemma 2.

**Corollary to Theorem.** We assume that \( n \) divides \( p-1 \). Let \( K \) be as in Lemma 4. Then, the number of unramified \( D_{n, p^m} \)-extensions of \( K \) is

\[
\sum_{\hat{\kappa}} \frac{p^{m \gamma_{A^i}} - p^{(m-1)\gamma_{A^i}}}{p^n - p^{m-1}},
\]

where the sum runs full representatives of divisor classes of \( K \) of order \( n \).

**Proof.** It follows from Lemma 4 that the number of unramified \( D_{n, p^m} \)-extensions of \( K \) is equal to

\[
\sum_{\{i, m\} = 1} \# \text{subgroups of } W_{m, \theta^i K} \text{ of order } p^m.
\]

It follows from Lemma 3 that \( W_{m, \theta^i K} \) is a \( Z/p^m Z \) free module of rank \( \gamma_{A^i} \). Hence the assertion holds.

**Remark.** The above Lemmas 3 and 4 can be extended to the case when \( L \) is unramified abelian extension of \( K \) of exponent \( p-1 \). Moreover, using the same arguments as in the proof of Corollary 1 to Theorem, we can show that the number of unramified Galois extensions of \( (n, p^m) \) type is determined by
where \{A\} are full representatives of divisor classes of \( K \) of order dividing \( p-1 \) and \( n \).

Next, we study unramified \( D_{2p} \)-extensions of \( K \) with \( \text{ch}(k) \neq p \). Then, if \( \text{ch}(k) \neq 2 \), the number of unramified \( D_{2p} \)-extensions of \( K \) is determined by \( g \) and its characteristic. Here, we shall show that if \( \text{ch}(k)=2 \), the number of unramified \( D_{2p} \)-extensions of \( K \) is determined by \( g \) and the Hasse-Witt invariant \( T_K \).

**Proposition 6.** Let \( \text{ch}(k)=2 \). Then, the number of unramified \( D_{2p} \)-extensions of \( K \) is equal to

\[
\left(2^{g^2}-1\right) \frac{p^{2^g(g^2-1)}-1}{p-1}.
\]

For the proof of the above proposition, let \( L \) be an unramified quadratic extension of \( K \). Since the number of such extensions of \( K \) is equal to \( 2^{g^2}-1 \), it is sufficient to show that the number of unramified \( D_{2p} \)-extensions of \( K \) containing \( L \) is equal to \( \frac{p^{2^g(g^2-1)}-1}{p-1} \).

We denote \((L^* \cap K^*)/L^{*p}\) simply by \( V_L \). We note that \( V_L \) is an \( F_p \)-module of rank \( 2(2g-1) \) and that it can be regarded as a \( \text{Gal}(L/K) \) module by the natural action of \( \text{Gal}(L/K) \) on \( L \). Then, Proposition is proved if the following two propositions hold. They are easily to proved using the same method showed in Lemmas 1 and 2.

**Lemma 5.** Let \( K, L \) be as above. Then, \( V_L = V_K \oplus V_1 \), where \( V_1 = \{a \in V_L \mid \tilde{a} = a^{-1} \text{ for nontrivial automorphism } \tau \text{ of } L \text{ over } K\} \).

**Lemma 6.** Let \( K, L \) be as in Lemma 5. Then, let \( M \) be an unramified \( D_{2p} \)-extension of \( K \) containing \( L \). Then there exists a subgroup \( \langle \tilde{a} \rangle \) of \( V_1 \) of order \( p \) such that \( M \) is generated over \( K \) by \( \tilde{a} \). Conversely for such an element of \( V_1 \), \( K(\sqrt{a}) \) is an unramified \( D_{2p} \)-extension of \( K \) containing \( L \).

§ 6. Examples.

**Example 1.** Let \( K \) be an algebraic function field with an algebraically closed constant field \( k \) of genus 2. We shall consider the number of unramified \( D_{2p} \)-extensions of \( K \). We assume that the characteristic \( p=3 \). We often identify an algebraic function field \( K \) with the birational equivalent class of complete nonsingular model \( C_K \) of \( K \).

There exists six Weierstrass points \( \{P_i\} \) of \( K \). Then, \( K \) can be expressed as \( K=k(x, y) \) with \( y^3 = \prod_{i=1}^{3}(x-a_i) \). We may assume that \( a_0=0, a_5=1, a_i \neq a_j \).
if \( i \neq j \), and \((x-a_i) = \langle P_i/P_6 \rangle^i \) for \( i = 1, 2, \ldots, 5 \). The basis of \( \Omega_K \) of the space of differentials of the first kind is given by

\[ \{dx/y, x^{-1}dx/y\} \]

The full representatives of 2 division points of \( \mathfrak{G}_0/\mathfrak{G}_H \) are

\[ \langle P_i/P_6 \rangle_{i=1,\ldots,5}, \quad \langle P_iP_j/P_6 \rangle_{i,j} \]

and

\[ \Omega(P_i/P_6) = \{(x-a_i)dx/y\}, \quad \Omega(P_iP_j/P_6) = \{(x-a_i)(x-a_j)dx/y\} \]

Hence, the Hasse-Witt matrix of \( K \) is given by

\[
\begin{pmatrix}
-(a_1 a_2 a_3+a_1 a_2+a_2 a_3+a_3 a_1) & 1 \\
 a_1 a_2 a_3 & -(1+a_1+a_2+a_3)
\end{pmatrix}.
\]

Let \( C_A \) be the matrix defined in §2 for any 2-division point \( \bar{A} \). Then,

\[
C_{P_i/P_6}^{P_j/P_6} = \text{the coefficient of } X^2 \text{ in } \Pi_{k \neq i} (X-a_k)
\]

\[
C_{P_iP_j/P_6}^{P_iP_j/P_6} = \text{the coefficient of } X^2 \text{ in } \Pi_{k \neq i,j} (X-a_k).
\]

Let \( d \) be a function of \( k \) such that

\[ d(a) = \begin{cases} 
1 & \text{if } a \text{ is non zero}, \\
0 & \text{if } a \text{ is zero}.
\end{cases} \]

Let \( N_K \) be the number of unramified \( D_{2p} \)-extension of \( K \). Then,

\[ N_K = \sum_{i=1}^5 d(C_{P_i/P_6}) + \sum_{i \neq j} d(C_{P_iP_j/P_6}). \]

That is, the number of unramified \( S_3 \)-extensions of \( K \) is equal to

\[
\sum_{i=1}^5 d(a_i+1) + \sum_{i \neq j} d(1+a_i+a_j) + \sum_{i \neq j} d(a_i+a_j) + d(a_1+a_2+a_3) \\
+ \sum_{i \neq j} d(a_i a_j+a_i+a_j)+d(a_1 a_2+a_2 a_3+a_3 a_1) \\
+ d(a_1 a_2+a_2 a_3+a_3 a_1+a_1+a_2+a_3).
\]

Let

\[ \mathcal{M}_2 = \{ \text{birationally equivalent classes of algebraic curves with genus 2} \} \]
Then, \( \mathfrak{W}_2 \) has the structure of 3 dimensional algebraic variety.

We put
\[
N_i = \{ \text{equivalent classes of } C_K \text{ such that } N_K \leq 15 - i \}.
\]

We put
\[
v_1 = 1 + \sum_{i=1}^{3} a_i, \quad v_2 = \sum_{i<j<3} a_i a_j + \sum_{i=1}^{3} a_i,
\]
\[
v_3 = a_1 a_2 a_3 + \sum_{i=1}^{3} a_i, \quad v_4 = a_1 a_2 a_3.
\]

Moreover we put
\[
J_2 = -v_4 + v_1 v_3,
\]
\[
J_4 = -(v_1 - v_3 + v_3 - v_4 + v_2 v_3 v_4 - v_1 v_3 v_4 + v_1 v_2 v_4 - v_1 v_3 v_4 + v_1 v_2 v_3 v_4 - v_1 v_2 v_3 v_4 - v_2 v_3 v_4 + v_2 v_3 v_4 - v_2 v_3 v_4).
\]
\[
J_{10} = \prod_{i<j} (a_i - a_j)^3 \prod_{i=1}^{3} (a_i - 1)^2.
\]

Then it follows from the result of Igusa [5] that \( \mathfrak{W}_2 \) is a subvariety of \( A^8 \) and its coordinate ring is equal to
\[
k \left[ J_2 J_{10}^{3}, J_4 J_{10}^{3}, J_2 J_6 J_{10}, J_3 J_4 J_{10}, J_4 J_6 J_{10} \right].
\]

Then, it follows from the above fact that \( N_i \) is an algebraic set of \( \mathfrak{W}_2 \). Especially, \( N_1 \) consists of 7 algebraic surfaces. \( N_2 \) consists of 12 rational curves. \( N_3 \) consists of 4 points.

In the following we show the above varieties and their parameter types.

That is, in the following table, we denote by \((a_1, a_2, a_3)\) the variety consists of birationally equivalent classes of curves defined by \( y^2 = x(x-1)(x-a_1)(x-a_2)(x-a_3) \). That is, we obtain the coordinate ring of a subvariety of \((a_1, a_2, a_3)\) type by substituting \( a_1, a_2, a_3 \) in \( * \). In the following table \( \xi \) is a root of the following equation \( X^8 + X - 1 = 0 \). This is an 8-th root of unity.

Let \( C_K \) be the curve defined by \( y^2 = x(x^2-1)(x-a)(x-b) \). Then, the Hasse-Witt invariant of \( C_K \) is always 2, but \( N_K \) varies as \( a \) and \( b \) varies. This means that Grothendieck's fundamental group of \( C_K \) is not determined only by \( g, p, \) and \( \gamma_K \).
Table

<table>
<thead>
<tr>
<th>$N_1$</th>
<th>type of parameter</th>
<th>Hasse-Witt invariant</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>$-1, a, b$</td>
<td>2</td>
</tr>
<tr>
<td>$S_2$</td>
<td>$a, -1-a, b$</td>
<td>2</td>
</tr>
<tr>
<td>$S_3$</td>
<td>$a, -a, b$</td>
<td>2</td>
</tr>
<tr>
<td>$S_4$</td>
<td>$a, b, -a-b$</td>
<td>1, 2</td>
</tr>
<tr>
<td>$S_5$</td>
<td>$a, b, -b/(1+b)$</td>
<td>2</td>
</tr>
<tr>
<td>$S_6$</td>
<td>$a, b, (ab-a-b)/(1+a+b)$</td>
<td>2</td>
</tr>
<tr>
<td>$S_7$</td>
<td>$a, b, -ab/(a+b)$</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_2$</th>
<th>$S_{1} \cap S_{2}$</th>
<th>$-1, a, -1-a$</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_2$</td>
<td>$S_{1} \cap S_{3}$</td>
<td>$-1, a, -a$</td>
<td>2</td>
</tr>
<tr>
<td>$C_3$</td>
<td>$S_{1} \cap S_{4}$</td>
<td>$-1, a, -a+1$</td>
<td>2</td>
</tr>
<tr>
<td>$C_4$</td>
<td>$S_{1} \cap S_{5}$</td>
<td>$-1, a, -a/(1+a)$</td>
<td>2</td>
</tr>
<tr>
<td>$C_5$</td>
<td>$S_{1} \cap S_{6}$</td>
<td>$-1, a, 1/a$</td>
<td>2</td>
</tr>
<tr>
<td>$C_6$</td>
<td>$S_{1} \cap S_{7}$</td>
<td>$-1, a, a/(a-1)$</td>
<td>2</td>
</tr>
<tr>
<td>$C_7$</td>
<td>$S_{2} \cap S_{3}$</td>
<td>$a, -1-a, -a$</td>
<td>2</td>
</tr>
<tr>
<td>$C_8$</td>
<td>$S_{2} \cap S_{4}$</td>
<td>$a, -1-a, -a/(1+a)$</td>
<td>2</td>
</tr>
<tr>
<td>$C_9$</td>
<td>$S_{2} \cap S_{5}$</td>
<td>$a, -1-a, -a(1+a)$</td>
<td>2</td>
</tr>
<tr>
<td>$C_{10}$</td>
<td>$S_{2} \cap S_{6}$</td>
<td>$a, -a, a/(a-1)$</td>
<td>2</td>
</tr>
<tr>
<td>$C_{11}$</td>
<td>$S_{2} \cap S_{7}$</td>
<td>$a, -a, a^2$</td>
<td>2</td>
</tr>
<tr>
<td>$C_{12}$</td>
<td>$S_{3} \cap S_{4}$</td>
<td>$a, -a/(1+a), -a^2/(1+a)$</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$N_3$</th>
<th>$S_{1} \cap S_{2} \cap S_{7}$</th>
<th>$-1, \xi, -1-\xi$</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_{4}$</td>
<td>$S_{3} \cap S_{4} \cap S_{6}$</td>
<td>$-1, \xi^2, -\xi^2$</td>
<td>2</td>
</tr>
<tr>
<td>$S_{5}$</td>
<td>$S_{3} \cap S_{4} \cap S_{5}$</td>
<td>$-1, \xi-1, -\xi$</td>
<td>2</td>
</tr>
<tr>
<td>$S_{6}$</td>
<td>$S_{3} \cap S_{5} \cap S_{5}$</td>
<td>$\xi, -1+\xi, -\xi$</td>
<td>2</td>
</tr>
</tbody>
</table>

**Example 2.** We shall consider the relation between $\langle \gamma_{AI} \rangle$. Let $K$ be an algebraic function field with an algebraically closed constant field $k$ of characteristic $p$ and let $g$ be its genus. Let $\overline{A}$ be an $n$ division point of $\mathfrak{O}_k/\mathfrak{O}_H$. If $i$ is prime to $n$, $\langle \overline{A} \rangle = \langle \overline{A} \rangle$. Then, it is natural to ask whether $\gamma_{AI} = \gamma_A$ or not. We shall give some examples for this question.
First, let $K=k(x, y)$ such that $y^3 = x^5 - 1$. We assume $ch(k)=11$. Then, we have $g=4$ and there are prime divisors $P_0, P_{01}, P_{02}, P_1, P_2, P_3$ such that $(x) = P_0 P_{01} P_{02} P_3$ and $(y + \zeta) = P_3 / P_6$, where $\zeta$ is a primitive cubic root of unity. We put $\mathcal{A} = P_{03}/P$. Then, we have

$$\Omega(\mathcal{A}) = \{(y+1)dx/y^2, x dx/y^2, x^2 dx/y^2\}$$

$$\Omega(\mathcal{A}^3) = \{(y+1)dx/y^2, x^3 dx/y^2, (y+1)x dx/y^2\}$$

$$\Omega(\mathcal{A}^4) = \{(y+1)dx/y^2, x^2 dx/y^2, (y+1)x dx/y^2\}$$

Moreover, we have $(y+1)^{2k} = \mathcal{A}^{2k}$. Hence, we have

$$C \left( \begin{array}{ccc} (y+1)^2 dx/y^2 \\ (y+1)^2 x dx/y^2 \\ (y+1)^2 x^2 dx/y^2 \end{array} \right) = \left( \begin{array}{ccc} 3 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & -3 \end{array} \right) \left( \begin{array}{c} dx/y^2 \\ x dy/y^2 \end{array} \right) .$$

Hence we have $\gamma_A = 3$. Similarly, we have $\gamma_A = \gamma_A^4 = \gamma_A^4 = 3$.

Next, let $K=k(x, y)$ such that $y^3 = x(x^2 - 1)(x - i)$, where $i$ is a primitive 12-th root of unity and let $ch(k)=7$. Then, there are divisors $P_0, P_1, P_2, P_i, P_{i-1}$ such that $(y) = P_0 P_{1} P_{1-1} P_{i}/P^4$ and $(x-i) = P_{i}/P^3$. We put $\mathcal{A} = P_{i}/P$. Then, we have

$$\Omega(\mathcal{A}) = \{dx/y, (x-i)dx/y^3\}$$

$$\Omega(\mathcal{A}^2) = \{(x-i)dx/y^2, (x-i)^2 dx/y^2\}$$

and $(x-i)^3 = \mathcal{A}^6$.

Then,

$$C \left( \begin{array}{c} (x-i)^2 dx/y \\ (x-i)^2(x-i) dx/y^2 \end{array} \right) = \left( \begin{array}{cc} 0 & 0 \\ 0 & -4 \end{array} \right) \left( \begin{array}{c} dx/y \\ (x-i)dx/y^3 \end{array} \right) .$$

Hence, we have $\gamma_A = 1$. Similarly,

$$C \left( \begin{array}{c} (x-i)^2(x-i) dx/y^2 \\ (x-i)^2(x-i)^2 dx/y^2 \end{array} \right) = \left( \begin{array}{cc} -4 & 0 \\ i+4\sqrt{i} & 1 \end{array} \right) \left( \begin{array}{c} (x-i)dx/y^2 \\ (x-i)^2 dx/y^2 \end{array} \right) .$$

Hence, we have $\gamma_A^4 = 2$.

It follows from the above two examples that in general $\gamma_A \neq \gamma_A^4$. But we don't know which relation exists between them.


Generalized Hasse-Witt invariants

References


Hidenori KATSURADA
Department of Mathematics
Faculty of Science
Hokkaido University
Sapporo, Japan