J. Math. Soc. Japan
Vol. 31, No. 1, 1979

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 Δ_g be the group generated by $2g$ elements u_i, v_i $(i=1, \cdots, g)$ 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 Δ_g with respect to subgroups of finite index. Then, it is well known that there is a surjective homomorphism of $\bar{\Delta}_g$ onto $Gal(M/K)$, 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 $Gal(M/K)$ (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 γ_K that was introduced by Hasse-Witt (cf. [4]). Hence if $g=1$, $Gal(M/K)$ is determined by g, p, and γ_K. But if $g\geqq 2$, the structure of $Gal(M/K)$ is not determined only by g, p and γ_K.

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

$$D_{np^m}=\langle \sigma, \tau \mid \sigma^{p^m}=\tau^n=1,\ \tau\sigma\tau^{-1}=\sigma^i, \text{ where } i \text{ is a primitive } n\text{-th root of unity in } (\boldsymbol{Z}/p^m\boldsymbol{Z})^{\times}\rangle.$$

In §2, we construct a certain invariant of K depending on n, and state our main theorem. Let $\mathfrak{A}_n$ be the set of full representatives of divisor classes of degree 0 of K whose orders are n. Then the invariant is the set $\{\gamma_A\}_{A\in\mathfrak{A}_n}$, where γ_A is an integer which is determined by the class of A. Then, our main theorem gives the number of unramified D_{np}-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_{np^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 γ_K but have different numbers of unramified D_{2p}-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 $g\geqq 2$. Let L be a finite Galois extension of K. We denote by $[L:K]$ its degree over K, and by $Gal(L/K)$ the Galois group.

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

$$\mathfrak{O}_{\mathfrak{z}}=\{a\in K_{\mathfrak{z}}\,|\,\nu_{\mathfrak{z}}(a)\geqq 0\}.$$

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 $C_G(N)=\{\sigma\in G\,|\,\sigma\tau=\tau\sigma$ for all $\tau\in N\}$, the centralizer of N in G. We denote by

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

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

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

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

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

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

Then it follows from the Kummer theory that the above homomorphism $\Delta_L\ni\theta\to\chi_\theta$ gives an isomorphism of Δ_L/K^* onto $\mathrm{Hom}(Gal(L/K), k^*)$. Let $\mathfrak{D}_0$ be the group consisting of all divisors of K of degree 0 and let $\mathfrak{D}_H$ be the subgroup of all principal divisors. We denote $A \bmod \mathfrak{D}_H$ by $\bar{A}$. For any element θ of Δ_L, we associate an element A_θ of $\mathfrak{D}_0$ such that $A_\theta=(\theta)$ in L. This correspondence induces an injective homomorphism of Δ_L/K^* into $\mathfrak{D}_0/\mathfrak{D}_H$. We denote its image by $cl_{L/K}$, and call it the divisor class group corresponding to an extension L over K.

We define the action of the operator $\mathfrak{p}$ on a subset of an extension field of K in the following manner:

$$\mathfrak{p}(a)=a^p-a.$$

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

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

$$\Omega(A)=\{\omega\in\Omega(K/k)\,;\,\nu_{\mathfrak{z}}(\omega)\geqq\nu_{\mathfrak{z}}(A) \text{ for all primes } \mathfrak{z} \text{ of } K\}.$$

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 ω of $\Omega(K/k)$, ω can be expressed uniquely as

$$\omega=\sum_{i=0}^{p-1}a_i^p x^i dx \quad (a_i\in K).$$

Then, $C\omega=a_{p-1}dx$.

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) $C(x^p\omega)=xC(\omega)$ for $x\in K$ and $\omega\in\Omega(K/k)$

(3) $C(dx)=0$

(4) $C(x^{-1}dx)=x^{-1}dx$

(5) $\nu_{\mathfrak{z}}(C(\omega))>\nu_{\mathfrak{z}}(\omega)/p-1$ (cf. Cartier [1], [2]).

We denote by $L_K(A)$ the subspace of K such that $\nu_{\mathfrak{z}}(x)\geqq-\nu_{\mathfrak{z}}(A)$ for all prime divisors $\mathfrak{z}$ of K, and put $l(A)=\dim_k L_K(A)$.

§ 2. Definition of invariants and the main theorem.

Let A be an n-division point of $\overline{\mathfrak{D}_0}=\mathfrak{D}_0/\mathfrak{D}_H$. Then, the dimension l of $\Omega(A)$ 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 $\Omega(A)$, and let x be an element of K such that $(x)=A^{p-1}$. Then, it follows from the basic properties of the Cartier operator that

$$C\Omega(A^p)\subset\Omega(A).$$

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

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

Let γ_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 γ_A does not depend on the choice of a basis of $\Omega(A)$ and a representative of a class of A. To see this, let $\{\eta_i\}$ be another basis of $\Omega(A)$, 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

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

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

$$\begin{aligned} C'_A C'^{(p)}_A\cdots C'^{(p^{l-1})}_A &=(S^{(1/p)}C_A S^{-1})(S^{(1/p)}C_A S^{-1})^{(p)}\cdots(S^{(1/p)}C_A S^{-1})^{(p^{l-1})} \\ &=S^{(1/p)}C_A C_A{}^{(p)}\cdots C_A{}^{(p^{l-1})}(S^{-1})^{(p^{l-1})}. \end{aligned}$$

Since S is regular,

$$\operatorname{rank} C'_A C'^{(p)}_A \cdots C'^{(p^{l-1})}_A = \operatorname{rank} C_A C_A^{(p)} \cdots C_A^{(p^{l-1})}.$$

Hence γ_A does not depend on the choice of basis of $\Omega(A)$.

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, $\{y\omega_i\}$ is a basis of $\Omega(A_1)$ and $(x_1)=(y^{p-1}x)$. Hence,

$$\mathcal{C}((x_1 y\omega_k))=\mathcal{C}((y^p x\omega_k))=yC_A((\omega_k))=C_{A_1}((y\omega_k)).$$

We have $C_A=C_{A_1}$, and $\gamma_A=\gamma_{A_1}$. Hence, γ_A does not depend on the choice of representative of class A. Terefore, γ_A is uniquely determined by $\bar{A}$. If we call $\mathfrak{A}_n$ the set of all n-division points of $\mathfrak{D}_0/\mathfrak{D}_H$, the set $\{\gamma_A\}_{\bar{A}\in\bar{\mathfrak{A}}_n}$ is an invariant of K (depending on n). Especially if $n=1$, $\{\gamma_A\}_{\bar{A}\in\bar{\mathfrak{A}}_n}$ consists of one element γ_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_{np^m}-type if its Galois group is isomorphic to

$$D_{np^m}=\langle\sigma, \tau \mid \sigma^{p^m}=\tau^n=1,\ \tau\sigma\tau^{-1}=\sigma^i \text{ with } i \text{ a primitive } n\text{-th root of unity} \mod p^m\rangle.$$

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 $g\geqq 2$. Let n be a positive integer such that n divides $p-1$. Then, the number of unramified D_{np}-extensions of K is equal to*

$$\sum_A (p^{\gamma_A}-1)/(p-1),$$

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_{np^m}-extensions of K is equal to*

$$\sum_{A} \frac{p^{m\gamma_A}-p^{(m-1)\gamma_A}}{p^m-p^{m-1}},$$

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 $W_L=\bigcap_{\mathfrak{s}}(\mathfrak{p}K_{\mathfrak{s}}\cap L)/\mathfrak{p}L=U_L/\mathfrak{p}L$. Since n divides $p-1$, $\mathfrak{p}(\theta K)\in\theta K$ for $\theta\in\Delta_L$. Hence we can define a sub-module $W_{\theta K}$ of W_L by

$$W_{\theta K}=U_{\theta K}/\mathfrak{p}\theta K \qquad (\text{cf. } \S 1).$$

Let A be a $Gal(L/K)$-module. Then we put for any element χ of $\mathrm{Hom}(Gal(L/K), F_p^*)$,

$$A^{\chi}=\{u\in A \mid u^{\sigma}=\chi(\sigma)u\}.$$

LEMMA 1. *Let L be an abelian extension of K of exponent $p-1$. Then,*

$$W_L\cong\bigoplus_{\bar{\theta}\in\Delta_L/K^*} W_{\theta K}$$

and

$$W_{\theta K}=W_L^{\chi_\theta}$$

where χ_θ is an element of $\mathrm{Hom}(Gal(L/K), F_p^*)$ *corresponding to θ* (cf. § 1).

PROOF. Let u be an element of U_L. Since $L=\bigoplus_{\theta}\theta K=\bigoplus_{\theta} L^{\chi_\theta}$, u can be expressed as

$$u=\sum_{\theta} a_\theta,$$

where $a_\theta\in\theta K=L^{\chi_\theta}$ and the sum runs full representatives of Δ_L/K^*. Then for any element σ of $Gal(L/K)$,

$$u^{\sigma}=\sum_{\theta}\chi_{\theta}(\sigma)a_{\theta}.$$

We note that

$$\sum_{\sigma\in Gal(L/K)}\chi_{\theta}(\sigma)\begin{array}{ll} =n & \text{if } \theta\in K^* \text{ where } n=\#Gal(L/K), \\ =0 & \text{if } \theta\notin K^*. \end{array}$$

Hence a_{θ} can be expressed as

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

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

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

$$U_L=\bigoplus_{\theta}U_{\theta K} \quad\text{and}\quad \mathfrak{p}L=\bigoplus_{\theta}\mathfrak{p}\vartheta K. \quad\text{Hence,}$$

$$W_L=U_L/\mathfrak{p}L=(\bigoplus_{\theta}U_{\theta K})/(\bigoplus_{\theta}\mathfrak{p}\theta K)\cong\bigoplus_{\theta}W_{\theta K}.$$

So the first assertion holds.

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

$$W_L=\bigoplus_{\theta}W_L^{\chi_{\theta}}$$

and $W_{\theta K}\hookrightarrow W_L^{\chi_{\theta}}$. Then the second assertion holds from these facts and the first assertion. q. e. d.

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 θ of Δ_L and a subgroup $\langle a \bmod \mathfrak{p}\theta K\rangle$ of $W_{\theta K}$ of order p such that M is generated over L by an element $1/\mathfrak{p}(a)$. Moreover $\theta \bmod K^*$ and the subgroup $\langle a \bmod \mathfrak{p}\theta K\rangle$ is uniquely determined by M. Conversely for a subgroup $\langle a \bmod \mathfrak{p}\theta K\rangle$ of $W_{\theta K}$ of order p, $L(1/\mathfrak{p}(a))$ 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 $\langle a \bmod \mathfrak{p}L\rangle$ of W_L of order p such that $M=L(1/\mathfrak{p}(a))$. Moreover, M is a Galois extension of K if and only if for any $\sigma\in Gal(L/K)$,

$$L\Big(\frac{1}{\mathfrak{p}}(a^{\sigma})\Big)=L\Big(\frac{1}{\mathfrak{p}}(a)\Big).$$

It holds if and only if $\langle a^{\sigma} \bmod \mathfrak{p}L\rangle=\langle a \bmod \mathfrak{p}L\rangle$. That is, $\langle a \bmod \mathfrak{p}L\rangle$ is a $Gal(L/K)$-module. Hence there is an element χ of $\mathrm{Hom}(Gal(L/K), F_p^*)$ such that $\langle a \bmod \mathfrak{p}L\rangle \subset W_L^\chi$. It follows from the Kummer theory and Lemma 1 that there exists an element θ of Δ_L such that $W_L^\chi = W_{\theta K}$. Hence $\langle a \bmod \mathfrak{p}L\rangle \subset W_{\theta K}$.

Assume that $\langle a \bmod \mathfrak{p}L\rangle \subset W_{\theta' K}$ for θ' of Δ_L. Then, it follows from Lemma 1 that $W_{\theta K} \cap W_{\theta' K} = 0$ if $\theta \not\equiv \theta' \bmod K^*$. Hence $\theta \equiv \theta' \bmod K^*$.

Conversely, let $\langle a \bmod \mathfrak{p}L\rangle$ be a cyclic subgroup of $W_{\theta K}$ of order p. Then it is clearly a $Gal(L/K)$-module. Hence $L(1/\mathfrak{p}(a))$ 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*

$$\bigcup_{\bar{\theta} \in \Delta_L/K^*} \{\textit{subgroup of } W_{\theta K} \textit{ of order } p\}.$$

PROOF. We put

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

and

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

It follows from Lemma 2 that for any element M of U, there is an element $\langle a \bmod \mathfrak{p}L\rangle$ of S such that $M = L(1/\mathfrak{p}(a))$, and that this $\langle a \bmod \mathfrak{p}L\rangle$ is uniquely determined by M. Hence there is a mapping from U into S. Conversely for any element $\langle a \bmod \mathfrak{p}L\rangle$ of S, $L(1/\mathfrak{p}(a))$ is an unramified extension of (n, p) type, that is, an element of U. Moreover if $\langle a_1 \bmod \mathfrak{p}L\rangle = \langle a_2 \bmod \mathfrak{p}L\rangle$, $L(1/\mathfrak{p}(a_1)) = L(1/\mathfrak{p}(a_2))$. 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 $\theta \not\equiv \theta' \bmod K^*$. 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

$$\sum_{\bar{\theta} \in \Delta_L/K^*} \sharp S_\theta .$$

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 $1/\mathfrak{p}(a)$, where $\langle a \bmod \mathfrak{p}L\rangle$ is an element of $S_{\theta i}$. Then, $K(1/\mathfrak{p}(a))$ is an unramified $D_{n_0 p}$-extension of K, where $n_0 = [K(\theta^i) : K]$.

In fact if we put $v=1/\mathfrak{p}(a)$, the conjugates of v have the forms $\zeta^{j}(v+i)$, with $i\in F_{p}$ and ζ a primitive n_{0}-th root of unity. We define elements of $Gal(K(v)/K)$ as follows:

$$\tau(v)=\zeta v, \quad \sigma(v)=v+1.$$

Then $\tau^{n}(v)=\sigma^{p}(v)=1$, and $\tau\sigma\tau^{-1}(v)=v+\zeta^{-1}$. Since ζ is a primitive n_{0}-th root of unity and contained in F_{p}, $\langle\sigma, \tau\rangle\cong D_{n_{0}p}$. On the other hand $\sharp Gal(K(v)/K)=\sharp D_{n_{0}p}=n_{0}p$. Hence $Gal(K(v)/K)\cong D_{n_{0}p}$.

Therefore, $K(v)$ is an unramified $D_{n_{0}p}$-extension of K if and only if $\langle a \bmod \mathfrak{p}L\rangle$ is an element of $S_{\theta i}$, with i an integer prime to n. Therefore, the number of unramified D_{np}-extensions of K containing L is equal to

$$\sum_{(i,n)=1}\sharp S_{\theta i}.$$

§ 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 θ as in § 1. It follows from Remark 2 after Lemma 2 that there is one-to-one correspondence between the set of unramified D_{np}-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

$$p^{r_{A}}=\sharp W_{\theta K}. \tag{*}$$

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 (*) using the method shown in Hasse-Witt [**4**].

PROPOSITION 1. *There are distinct primes* $\mathfrak{G}_{1}, \cdots, \mathfrak{G}_{g-1}$ *of* K *such that* $\dim_{k}\Omega(A\mathfrak{G}_{1}\cdots\mathfrak{G}_{g-1})=0$, *that is* $l(A\mathfrak{G}_{1}\cdots\mathfrak{G}_{g-1})=0$.

PROOF. Since $\dim_{k}\Omega(A)=g-1>0$, there is a non-zero element ω_{1} of $\Omega(A)$. The zeroes of ω_{1} is finite, so there is a prime divisor of K such that $\nu_{\mathfrak{G}_{1}}(\omega_{1})<\nu_{\mathfrak{G}_{1}}(A\mathfrak{G}_{1})$. Hence $\Omega(A)\supsetneqq\Omega(A\mathfrak{G}_{1})$, so $\dim_{k}\Omega(A)-\dim_{k}\Omega(A\mathfrak{G}_{1})>0$. On the other hand,

$$\dim_{k}\Omega(A\mathfrak{G}_{1})=g-2+l(A\mathfrak{G}_{1})$$

and

$$\dim_{k}\Omega(A)=g-1.$$

Since $l(A\mathfrak{G}_{1})\geqq 0$, $\dim_{k}\Omega(A)-\dim_{k}\Omega(A\mathfrak{G}_{1})\leqq 1$. Hence $\dim_{k}\Omega(A\mathfrak{G}_{1})=g-2$. Assume that there are distinct i primes $\mathfrak{G}_{1}, \cdots, \mathfrak{G}_{i}$ of K such that $\dim_{k}\Omega(A\mathfrak{G}_{1}\cdots\mathfrak{G}_{i})=g-1-i$. If $i=g-1$, the assertion holds. If $i<g-1$, then using the above arguments, we can show that there is a prime divisor $\mathfrak{G}_{i+1}$ such that $\dim_{k}(A\mathfrak{G}_{1}\cdots\mathfrak{G}_{i}\mathfrak{G}_{i+1})=g-2-i$. By induction on i, the assertion holds.

Let us take a prime divisor $\mathfrak{G}'_i$ of L which is an extension of $\mathfrak{G}_i$ and take a prime element π_i with respect to $L_{\mathfrak{G}'_i}$. Since any prime divisor of K is completely decomposed in L, $K_{\mathfrak{G}_i}=L_{\mathfrak{G}'_i}$. Hence, we can take an element of $K_{\mathfrak{G}_i}$ (especially of K) as a prime element of $L_{\mathfrak{G}'_i}$. Since θ is contained in $K_{\mathfrak{z}}$ for all prime divisors $\mathfrak{z}$ of K, there is an element ξ of the adele ring R_K of K such that $(\xi)_{\mathfrak{z}}=\theta$, where $(\xi)_{\mathfrak{z}}$ is the $\mathfrak{z}$-th component of ξ. Hereafter, we shall denote ξ simply denote by θ. Let r_i be an element of the adele ring R_K such that

$$(r_i)_{\mathfrak{z}}=0 \qquad \text{if } \mathfrak{z}\neq\mathfrak{G}_i$$

$$(r_i)_{\mathfrak{z}}=1/\pi_i \qquad \text{if } \mathfrak{z}=\mathfrak{G}_i.$$

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

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

where $R_K(0)=\{r\in R_K \mid \nu_{\mathfrak{z}}((r)_{\mathfrak{z}})\geqq 0\}$.

PROOF. Since $l(A\mathfrak{G}_1\cdots\mathfrak{G}_i^{\nu}\cdots\mathfrak{G}_{g-1})=\nu+(g-2)-g+1=\nu-1$, there is an element $v_{i,\nu}$ of K such that $\nu_{\mathfrak{G}'_i}(\theta v_{i,\nu})=-\nu$, $\nu_{\mathfrak{G}'_j}(\theta v_{i,\nu})\geqq -1$ if $i\neq j$, and $\nu_{\mathfrak{G}'}(\theta v_{i,\nu})\geqq 0$ is $\mathfrak{G}'\neq\mathfrak{G}'_i$, $\mathfrak{G}'_j$ for any integer $\nu\geqq 2$. Since $L_{\mathfrak{G}'_i}=k((\pi_i))$, we can express $\theta v_{i,\nu}$ as

$$\theta \nu_{i,\nu}=\sum_{l\geqq -\nu} c_l \pi_i^l$$

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

$$\nu_{\mathfrak{G}'_i}(\theta v_{i,p}-(1/\pi_i)^p-c_{-(p-1)}\theta v_{i,p-1})\geqq -(p-2)$$

$$\nu_{\mathfrak{G}'_j}(\theta v_{i,p}-c_{-(P-1)}\theta v_{i,p-1})\geqq -1 \qquad \text{if } i\neq j,$$

$$\nu_{\mathfrak{G}'}(\theta v_{i,p}-c_{-(p-1)}\theta v_{i,p-1})\geqq 0 \qquad \text{if } \mathfrak{G}'\neq\mathfrak{G}'_i \text{ and } \mathfrak{G}'_j.$$

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

$$\nu_{\mathfrak{G}'_i}((1/\pi_i)^p-\sum_{j=1}^{g-1} b_{ij}(1/\pi_j)-\theta v_i)\geqq 0,$$

$$\nu_{\mathfrak{G}'}(\theta v_i)\geqq 0 \qquad \text{if } \mathfrak{G}\neq\mathfrak{G}'_i.$$

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

$$r_i^p-\sum_{j=1}^{g-1} b_{ij} r_j-\theta v_i\in R_K(0). \qquad \text{q. e. d.}$$

Let $\{\mathfrak{G}_i\}_i$ be a divisor system that is defined in Proposition 1. Then, we put

$L_L(\mathfrak{G}_1^p \cdots \mathfrak{G}_{g-1}^p)=\{x\in L \mid \nu_{\mathfrak{G}}(x)\geqq -\nu_{\mathfrak{G}}(\mathfrak{G}_1^p \cdots \mathfrak{G}_{g-1}^p)$ for any prime $\mathfrak{G}\}$ of L

and

$$V_{\theta K}=\bigcap_{j=1}^{g-1}(\theta K \cap \mathfrak{p}K_{\mathfrak{G}_i} \cap L_L(\mathfrak{G}_1^p \cdots \mathfrak{G}_{g-1}^p)).$$

Then in the following proposition, we shall consider the relation between $V_{\theta K}$ and $W_{\theta K}=\bigcap_{\mathfrak{s}}(\theta K \cap \mathfrak{p}K_{\mathfrak{s}})/\mathfrak{p}\theta K$.

PROPOSITION 3. $W_{\theta K}\cong V_{\theta K}$.

PROOF. Let u be an element of $V_{\theta K}$. If u is integral at a prime divisor $\mathfrak{G}'$ of L, it follows from Hensel's lemma and the fact that k is algebraically closed that u is contained in $\mathfrak{p}\mathfrak{O}_{\mathfrak{G}'}$. Hence $u \bmod \mathfrak{p}K \in W_{\theta K}$. Conversely for any unramified element u of θK, we are going to prove that there exists an element θw of $V_{\theta K}$ such that $u\equiv\theta w \pmod{\mathfrak{p}\theta K}$.

First take a prime $\mathfrak{G}'$ of L such that $\mathfrak{G}'\neq\mathfrak{G}_i'$. If $\nu_{\mathfrak{G}}(u)\geqq 0$, u belongs to $\mathfrak{O}_{\mathfrak{G}'}=\mathfrak{p}\mathfrak{O}_{\mathfrak{G}'}$. Assume that $\nu_{\mathfrak{G}'}(u)<0$. Then there exists an integer m such that $\nu_{\mathfrak{G}'}(u)=-pm$. Let $\mathfrak{G}$ be the restriction of $\mathfrak{G}'$ to K. Since $l(A\mathfrak{G}_1\cdots\mathfrak{G}_{g-1}\mathfrak{G}^m)\geqq 1$, there is an element v' of K such that $\nu_{\mathfrak{G}'}(\theta v')=-m$, $\nu_{\mathfrak{G}_i'}(\theta v')\geqq -1$, and $\nu_{\mathfrak{G}'}(\theta v')\geqq 0$ otherwise. Hence $\theta v'$ can be expressed in $K_{\mathfrak{G}}$ as

$$\theta v'=\sum_{i\geqq -m} a_i\pi^i,$$

where π is a prime element of $K_{\mathfrak{G}}$ and $a_i\in k$. Similarly u can be expressed as $u=\sum_{i\geqq -pm} b_i\pi^i$, with $b_i\in k$. Since k is perfect field, there is an element a of k such that $a^p=b_{-pm}$. We can choose v' so that $a_{-m}=a$. Then

$$\nu_{\mathfrak{G}'}(u-\mathfrak{p}(\theta v'))\geqq -p(m-1),\quad (m\geqq 2),\quad \nu_{\mathfrak{G}''}(u-\mathfrak{p}(\theta v'))\geqq \min(0,\nu_{\mathfrak{G}''}(u))$$

if $\mathfrak{G}''$ is a prime of L which is different from $\mathfrak{G}'$ and $\mathfrak{G}_i'$. Repeating this process, we can show that there is an element v'' of K such that

$$\nu_{\mathfrak{G}'}(u-\mathfrak{p}(\theta v''))\geqq 0$$

for any prime divisor $\mathfrak{G}'$ of L which is different from $\mathfrak{G}_i'$. Since $u\in\bigcap_{i=1}^{g-1}(\theta K\cap \mathfrak{p}K_{\mathfrak{G}_i})$, there is the set of integers k_i such that $\nu_{\mathfrak{G}_i'}(u)=-pk_i$. Let m be the largest number of k_i. Then the assertion holds if we have $m\leqq 1$. Assume that $m>1$. Then since $l(A\mathfrak{G}_1\cdots\mathfrak{G}_i^{k_i}\cdots\mathfrak{G}_{g-1})=k_i-1$, for any integer k_i such that $k_i\geqq 2$, there is an element v_{k_i} of K such that

$\nu_{\mathfrak{G}_i'}(\theta v_{k_i})=-k_i$

$\nu_{\mathfrak{G}_j'}(\theta v_{k_i})\geqq -1$ if $i\neq j$

$\nu_{\mathfrak{G}'}(\theta v_{k_i})\geqq 0$ if $\mathfrak{G}'$ is a prime divisor different from $\mathfrak{G}_i'$ and $\mathfrak{G}_j'$.

We can express u and θv_{k_i} as

$$u=\sum_{j\geq -pk_i} b_j\pi^j,\ \theta v_{k_i}=\sum_{j\geq -k_j} a_j\pi^j,$$

with π a prime element of K. Then there is an element a of k such that $a^p=b_{-pk_i}$. We can take u as $a_{-k_i}=a$. Then,

$$\begin{aligned}\nu_{\mathfrak{G}'}(u-\mathfrak{p}(\theta v_{k_i}))&\geqq -p(m-1) && \text{if } \mathfrak{G}'=\mathfrak{G}_i'\\ &\geqq \min(-p,\ \nu_{\mathfrak{G}'}(u)) && \text{if } \mathfrak{G}'\neq\mathfrak{G}_j'\ \ (i\neq j)\\ &\geqq \min(0,\ \nu_{\mathfrak{G}'}(u)) && \text{if } \mathfrak{G}'\neq\mathfrak{G}_i',\ \mathfrak{G}_j'.\end{aligned}$$

Repeating this process, we can show that there is an element v of K such that

$$\begin{aligned}\nu_{\mathfrak{G}'}(u-\mathfrak{p}(\theta v))&\geqq -p && \text{if } \mathfrak{G}'=\mathfrak{G}_i,\\ &\geqq 0 && \text{if } \mathfrak{G}'\neq\mathfrak{G}_i.\end{aligned}$$

That is, $u-\mathfrak{p}(\theta v)\in L_L(\mathfrak{G}_1^p\cdots\mathfrak{G}_{g-1}^p)$. Since $\theta^{p-1}\in K$, there is an element w of K such that $\theta w=u-\mathfrak{p}(\theta v)$. Then w satisfies the required conditions.

We note that this fact implies that the homomorphism f of $V_{\theta K}=\bigcap_{i=1}^{g-1}(\theta K\cap \mathfrak{p}K_{\mathfrak{G}_i})\cap L_L(\mathfrak{G}_1^p\cdots\mathfrak{G}_{g-1}^p)$ into $W_{\theta K}=\bigcap_{\mathfrak{G}}(\theta K\cap K_{\mathfrak{G}})/\mathfrak{p}\theta K$ defined by

$$\begin{array}{rccc} f: & V_{\theta K} & \longrightarrow & W_{\theta K}\\ & \Uparrow & & \Uparrow\\ & u & \longrightarrow & u \bmod \mathfrak{p}\theta K\end{array}$$

is a surjective homomorphism.

Finally, let u be an element of $V_{\theta K}$ such that $u\equiv 0 (\bmod\, \mathfrak{p}\theta K)$. Then u can be expressed as $u=(\theta x)^p-\theta x$ with an element x of K. Since $u\in L_L(\mathfrak{G}_1^p\cdots\mathfrak{G}_{g-1}^p)$, $\nu_{\mathfrak{G}_i'}(\theta x)\geqq -\nu_{\mathfrak{G}_i'}(\mathfrak{G}_i)$, that is $\nu_{\mathfrak{G}_i}(x)\geqq -\nu_{\mathfrak{G}_i}(A\mathfrak{G}_i)$ for any $1\leqq i\leqq g-1$ and $\nu_{\mathfrak{G}}(x)\geqq -\nu_{\mathfrak{G}}(A)$ for any prime divisor different from $\mathfrak{G}_i$. This implies $x\in L_K(A\mathfrak{G}_1\cdots\mathfrak{G}_{g-1})$.

On the other hand, it follows from the choice of $\mathfrak{G}_i$ that $\dim_k L_K(A\mathfrak{G}_1\cdots\mathfrak{G}_{g-1})=0$. Hence we have $x=0$. This implies that f is injective. q. e. d.

We put

$$R_A=\{(c_i)\in k^{g-1}\mid {}^t(c_i^p)B_A={}^t(c_i)\}.$$

This is an F_p-vector space of finite rank. Now we are going to calculate the rank of $W_{\theta K}=\bigcap_{\mathfrak{s}}(\mathfrak{p}K_{\mathfrak{s}}\cap\theta K)/\mathfrak{p}\theta K$ 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

$$\theta u = (c_i/\pi_i)^p - c_i/\pi_i \qquad (\bmod\ \mathfrak{O}_{\mathfrak{G}_i}),$$

that is,

$$\theta u \equiv {}^t(c_i^p)(r_i^p) - {}^t(c_i)(r_i) \qquad (\bmod\ R_K(0)). \tag{1}$$

On the other hand, by Proposition 2,

$$(r_i^p) \equiv B_A(r_i) \qquad (\bmod\ R_K(0) + \theta K).$$

That is, there is an element v_i of K such that

$$(\theta v_i) = (r_i^p) - B_A(r_i) \qquad (\bmod\ R_K(0)). \tag{2}$$

Hence

$${}^t(c_i^p)(\theta v_i) = {}^t(c_i^p)(r_i^p) - {}^t(c_i^p) B_A(r_i) \qquad (\bmod\ R_K(0)). \tag{3}$$

It follows from (1) and (3) that

$$\theta(u - {}^t(c_i^p)(v_i)) = {}^t(c_i^p) B_A(r_i) - {}^t(c_i)(r_i) \in L_K(A \mathfrak{G}_1 \cdots \mathfrak{G}_{g-1}).$$

It follows from the choice of $\mathfrak{G}_1, \cdots, \mathfrak{G}_{g-1}$ that

$$u - {}^t(c_i^p)(v_i) = 0.$$

Hence ${}^t(c_i)(r_i) - {}^t(c_i^p) B_A(r_i) = 0$. Hence ${}^t(c_i) - {}^t(c_i^p) B_A = 0$, that is, ${}^t(c_i) \in R_A$. If $u=0$, ${}^t(c_i^p)(v_i)=0$. Hence we have ${}^t(c_i^p)(\theta v_i)=0$. 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:

$$\begin{array}{cccc} g: & V_{\theta K} & \longrightarrow & R_A \\ & \Cup & & \Cup \\ & \theta u & \longrightarrow & (c_i) \end{array}$$

such that $u = (c_i^p)(v_i)$.

We are going to show that this homomorphism is an isomorphism. Let ${}^t(c_i)$ be an element of R_A. Then,

$$\begin{aligned} {}^t(c_i^p)(\theta v_i) &= {}^t(c_i^p)(r_i^p) - {}^t(c_i^p) B_A(r_i) && (\bmod\ R_K(0)) \\ &= {}^t(c_i^p)(r_i^p) - {}^t(c_i)(r_i) && (\bmod\ R_K(0)). \end{aligned}$$

Hence $\theta u = \sum c_i^p \theta v_i \in V_{\theta K}$. 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 $R_A \cong W_{\theta K}$.

q. e. d.

It follows from Satz 10 of Hasse-Witt [4] that

$$\mathrm{rank}_{F_p} R_A=\delta_A,$$

where δ_A is the rank of $B_A B_A^{(p)} \cdots B_A^{(p^{l-1})}$. Therefore the proof of Theorem is completed if we have the following proposition.

PROPOSITION 5. $\delta_A=\gamma_A$.

PROOF. We put

$$R(A)=\{r\in R_K \mid \nu_{\mathfrak{z}}((r)_{\mathfrak{z}})\geqq -\nu_{\mathfrak{p}}(A) \text{ for any prime } \mathfrak{z} \text{ of } K\}.$$

Let r_i be elements of R_K that are defined in Proposition 2. Assume that

$$\sum_{i=1}^{g-1} c_i r_i/\theta\equiv 0 \pmod{R(A)+K} \quad \text{with elements } c_i \text{ of } k.$$

Let v be an element of K such that

$$\sum_{i=1}^{g-1} c_i r_i/\theta\equiv v(R(A)) \quad \text{for some } c_i \text{ of } k.$$

Then, $\nu_{\mathfrak{G}_i}(\theta v)\geqq -1$ for any prime divisor $\mathfrak{G}_i$ that is defined in Proposition 1. Since $l(A\mathfrak{G}_1\cdots\mathfrak{G}_{g-1})=0$, we have $v=0$. That is,

$$\sum_{i=1}^{g-1} c_i r_i=0 \pmod{R_K(0)}.$$

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

$$\{r_i/\theta \bmod R(A)+K\} \quad \text{forms a basis of } R_K/(R(A)+K).$$

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 $(\omega, \zeta)=\sum_{\mathfrak{z}} \mathrm{Res}\,\omega\zeta_{\mathfrak{z}}$ 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 $\zeta\in R_K$;

$$(\omega, \zeta^p)=(C\omega, \zeta)^p \quad \text{(cf. Lang [6])}.$$

Let $B_A=(b_{ij})$ be as in Proposition 2. Then,

$$b_{ji}=(\omega_i, \textstyle\sum b_{jk} r_k/\theta) \quad \text{and} \quad r_j^p\equiv \textstyle\sum b_{jk} r_k \pmod{R(A)+\theta K}.$$

Hence

$$\begin{aligned}(\omega_i, \textstyle\sum b_{jk} r_k/\theta)&=(\omega_i, r_j^p/\theta)=(\omega_i, \theta^{p-1}(r_j/\theta)^p)\\ &=(\omega_i, x(r_j/\theta)^p)=(x\omega_i, (r_j/\theta)^p)=(C(x\omega_i), (r_j/\theta))^p.\end{aligned}$$

Let $C_A=(c_{il})$ be as in §2. Then, $C(x\omega_i)=\sum c_{il}\omega_l$. Hence

$$b_{ji}=(\sum c_{il}\omega_l,\ r_j/\theta)^p=c_{ij}^p.$$

Hence ${}^tC_A^{(p)}=B_A$. Hence $\delta_A=\gamma_A$. q. e. d.

COROLLARY 1. *Let n is 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 $\{\gamma_A\}_A$, where $\{A\}$ 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 $\{\gamma_A\}_A$.

Let M be an unramified Galois extension of K of (n, p) type containing L. $G=Gal(M/K)=Gal(L/K)\cdot Gal(M/L)$ because n is prime to p. We put $A=Gal(L/K)$ and $P=Gal(M/L)$. Then, $\#A=n$ and $\#P=p$, and $P\lhd Gal(M/K)$. 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 $Gal(M/M_1)$ is a normal subgroup of $Gal(M/K)$. Since $Gal(L_1/K)\cong G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)=F_p^*$, 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 $Gal(M_1/K)$ is isomorphic to

$$D_{n_1p}=\langle\sigma_1,\tau\,|\,\sigma_1{}^p=\tau_1{}^{n_1}=1 \text{ and } \tau_1\sigma_1\tau_1{}^{-1}=\sigma_1{}^i \text{ with } i \text{ a primitive } n_1\text{-th root of unity mod } p\rangle.$$

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

It follows from the above consideration that any unramified Galois extension of K of (n, p) type containing L is a compositumn of L and an unramified D_{np}-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_1p}-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 $Gal(M/L_1)=C_G(P)$, where $P=Gal(M/L)$, $G=Gal(M/K)$. In fact, let L_2 be the subfield of L corresponding to $C_G(P)$. We put $G_1=Gal(M_1/K)$ and $P_1=Gal(M_1/L_1)$. Since $Gal(M/L_1)$ is abelian and $Gal(M/L_2)$ is $C_G(P)$, $Gal(M/L_2)\supset Gal(M/L_1)$. On the other hand, since $G_1=D_{np}$, $P_1=C_{G_1}(P_1)$. That is, $P_1=Gal(M_1/L_1)=Gal(M_1/L_2)$. 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.

q. e. d.

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 γ_L of L is equal to $\sum_A \gamma_A$, where A runs full representatives of divisor classes of degree* 0 *which correspond to L over K.*

PROOF. It follows from Lemma 1 that

$$W_L = \bigcap_{\mathfrak{z}} (\mathfrak{p}K_{\mathfrak{z}} \cap L)/\mathfrak{p}L = \bigoplus_{\theta} W_{\theta K},$$

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

$$\gamma_L = \mathrm{rank}_{F_p} W_L = \sum_A \gamma_A. \qquad \text{q. e. d.}$$

§ 5. Remarks and generalizations.

Now, we shall consider unramified Galois extensions of K of (n, p^m) type. We assume that n divides $p-1$ and mainly consider unramified D_{np^m}-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 $a=(a_0, a_1, \cdots, a_{m-1})$, $b=(b_0, b_1, \cdots, b_{m-1})$ be elements of $W_m(R)$. Then, the r-th component of $a+b$ is expressed as

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

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

(a) Let $\widetilde{W}_m(R) = (a, 0, \cdots, 0)$ 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 $\widetilde{W}_m(R^*)$. We denote by $\tilde{a}$ an element $(a, 0, \cdots, 0)$ of $\widetilde{W}_m(R)$. We note that, for any element b of $W_m(R)$, $\tilde{a}.b = (b_0 a, b_1 a^p, \cdots, b_{m-1} a^{p^{m-1}})$.

(b) We define the Frobenius endomorphism $F: W_m(R) \to W_m(R)$ by

$$F(a_0, a_1, \cdots, a_{m-1}) = (a_0^p, a_1^p, \cdots, a_{m-1}^p).$$

We define $\mathfrak{p}$-operator by $\mathfrak{p}(a) = F(a) - a$. We note that the Frobenius endomorphism is $\boldsymbol{Z}/p^m\boldsymbol{Z}$-linear, and therefore the operator $\mathfrak{p}$ is also $\boldsymbol{Z}/p^m\boldsymbol{Z}$-linear.

(c) We define the shift $V: W_m(R) \to W_{m+1}(R)$ by

$$V(a_0, a_1, \cdots, a_{m-1}) = (0, a_0, a_1, \cdots, a_{m-1}).$$

This is an additive operator.

(d) We define the restriction $R: W_{m+1}(R) \to W_m(R)$ by

$$R(a_0, a_1, \cdots, a_{m-1}) = (a_0, a_1, \cdots, a_{m-1}).$$

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 $W(k)/p^m W(k) \cong \boldsymbol{Z}/p^m\boldsymbol{Z}$.

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

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

$$\sum_i c_i^{(k)} a_1^{p^k} + h_k(c_1^{(0)} a_1, c_2^{(0)} a_2, \cdots, c_r^{(0)} a_r, \cdots,$$
$$c_1^{(k-1)} a_1^{p^{k-1}}, c_2^{(k-1)} a_2^{p^{k-1}}, \cdots, c^{(k-1)} a_r^{p^{k-1}}).$$

Then, by the assumptions and the remark on the composition laws, $h_r(0, 0, \cdots, 0) = 0$, so $\sum c_i^{(k)} a_i^{p^k} = 0$. 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 $1 \leqq i \leqq r$. By induction on k, $\{\tilde{a}_i\}$ are linearly independent over $\boldsymbol{Z}/p^m\boldsymbol{Z}$.

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

$$\mathfrak{p}(x) - a = 0.$$

Then, another root of the above equation is given by $a+c$, where c is an element of $W_m(F_p)=\boldsymbol{Z}/p^m\boldsymbol{Z}$. Especially, if $a_0 \notin \mathfrak{p}L$, $M=L(b_0, b_1, \cdots, b_r)$ is a cyclic extension of L of degree p^m, where $b_0, b_1, \cdots, b_{m-1}$ are the components of $1/\mathfrak{p}(a)$. 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 $L_{\mathfrak{z}}$ be the completion of L at $\mathfrak{z}$. We put

$$W_{m,L}=\bigcap_{\mathfrak{z}}(W_m(L)\cap\mathfrak{p}(W_m(L_{\mathfrak{z}})))/\mathfrak{p}W_m(L).$$

If $n=1$, $W_{m,L}$ coincides with the set W_L defined in §1. It is well known that $W_{m,L}$ is a $\boldsymbol{Z}/p^m\boldsymbol{Z}$-free module of rank γ_L, where γ_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 $L=K(\theta)$, $\theta^n\in K$.
Then, we put

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

It follows from (a) that for any element $(b_0, b_1, \cdots, b_{m-1})$ of $W_m(K)$, we have $\tilde{\theta}b=(\theta b_0, \theta^p b_1, \cdots, \theta^{p^{m-1}}b_{m-1})$. Since n divides $p-1$, we have $\theta^{p^{k-1}}\in K$. Hence, we have $\tilde{\theta}W_m(K)=W_m(\theta K)$. 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

$$W_{m,\theta K}=\bigcap_{\mathfrak{z}}(W_m(\theta K)\cap\mathfrak{p}W(K_{\mathfrak{z}}))/W_m(\theta K).$$

We say an element a of $\bigcap_{\mathfrak{z}}(W_m(A)\cap\mathfrak{p}W(K_{\mathfrak{z}}))$ an unramified element of A for any submodule A of an unramified extension of K.

LEMMA 3. *Let K, L be as above. Then, $W_{m,\theta^i K}$ is a free $\boldsymbol{Z}/p^m\boldsymbol{Z}$-module of* rank γ_{Ai}, *where γ_{Ai} is the integer defined in* §2. *Moreover, we have*

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

PROOF. If $m=1$, this is nothing but Lemma 1. Assume that $m>1$. It follows from the proof of Theorem that $W_{\theta^i K}$ is an F_p-vector space of rank γ_{Ai}. Hence, it follows from the above remark that $W_{m,\theta^i K}$ contains a $\boldsymbol{Z}/p^m\boldsymbol{Z}$-free module of rank γ_{Ai}.

In fact, let $a_j^{(i)} \bmod \mathfrak{p}\theta^i K$ be a basis of $W_{\theta^i K}$. Then,

$\{(a^{(i)}, 0, \cdots, 0) \bmod \mathfrak{p} W_m(\theta^i K)_{1 \leq i \leq r}\}$ are linearly independent over $\boldsymbol{Z}/p^m\boldsymbol{Z}$.

Using the same arguments, we can show that

$\{(a^{(i)}{}_j, 0, \cdots, 0) \bmod \mathfrak{p} W_m(L)_{1 \leq j \leq r, 0 \leq i \leq n-1}\}$ are linearly independent over $\boldsymbol{Z}/p^m\boldsymbol{Z}$.

Hence we have

$$\sum_{i \neq k} W_{m,\theta^k K} \cap W_{m,\theta^i K} = 0 .$$

On the other hand, it follows from Corollary 2 to Theorem that $\gamma_L = \sum_{i=1}^{n-1} \gamma_{A^i}$. Hence, $W_{m,L} \cong \sum W_{m,\theta^i K}$, and $W_{m,\theta^i K}$ is a free $\boldsymbol{Z}/p^m\boldsymbol{Z}$ submodule of W_L of rank γ_{A^i}. q. e. d.

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

COROLLARY TO THEOREM. *We assume that n divides $p-1$. Let K be as in Lemma 4. Then, the number of unramified D_{np^m}-extensions of K is*

$$\sum_{A} \frac{p^{m\gamma_A} - p^{(m-1)\gamma_A}}{p^m - p^{m-1}} ,$$

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_{np^m}-extensions of K is equal to

$$\sum_{(i,m) \neq 1} \# \{\text{subgroups of } W_{m,\theta^i K} \text{ of order } p^m\}.$$

It follows from Lemma 3 that $W_{m,\theta^i K}$ is a $\boldsymbol{Z}/p^m\boldsymbol{Z}$ free module of rank γ_{A^i}. Hence the assersion 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

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

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

$$(2^{\gamma_k}-1)\cdot\frac{p^{2(g-1)}-1}{p-1}.$$

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 $2^{\gamma_k}-1$, it is sufficient to show that the number of unramified D_{2p}-extensions of K containing L is equal to $\frac{p^{(g-1)}-1}{p-1}$.

We denote $(L^*\cap K_{\mathfrak{s}}^{p})/L^{*p}$ 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 $Gal(L/K)$ module by the natural action of $Gal(L/K)$ 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 $V_1=\{\bar{a}\in V_L \mid \bar{a}^{\tau}=\bar{a}^{-1}$ for nontrivial automorphism τ of L 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 $\langle\bar{a}\rangle$ of V_1 of order p such that M is generated over K by $\sqrt[p]{a}$. Conversely for such an element of V_1, $K(\sqrt[p]{a})$ 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 $y^2=\prod_{i=1}^{5}(x-a_i)$. We may assume that $a_4=0$, $a_5=1$, $a_i\neq a_j$

if $i \neq j$, and $(x-a_i)=(P_i/P_6)^2$ for $i=1, 2, \cdots, 5$. The basis of Ω_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

$$\{P_i/P_6\ {}_{i=1,\cdots,5},\ P_iP_j/P_6^2\ {}_{i\neq j}\}$$

and

$$\Omega(P_i/P_6)=\{(x-a_i)\,dx/y\},\quad \Omega(P_iP_j/P_6^2)=\{(x-a_i)(x-a_j)\,dx/y\}.$$

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

$$\begin{bmatrix} -(a_1a_2a_3+a_1a_2+a_2a_3+a_3a_1), & 1 \\ a_1a_2a_3 \qquad , & -(1+a_1+a_2+a_3) \end{bmatrix}.$$

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

$$C^{(p)}_{P_i/P_6} = \text{the coefficient of } X^2 \text{ in } \prod_{k\neq i}(X-a_k)$$
$$C^{(p)}_{P_iP_j/P_6^2} = \text{the coefficient of } X^2 \text{ in } \prod_{k\neq i,j}(X-a_k).$$

Let d be a function of k such that

$$d(a)=1 \quad \text{if } a \text{ is non zero,}$$
$$d(a)=0 \quad \text{if } a \text{ is zero.}$$

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

$$N_K=\sum_{i=1}^{5} d(C_{P_i/P_6})+\sum_{i\neq 1} d(C_{P_iP_j/P_6^2}).$$

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

$$\sum_{i=1}^{3} d(a_i+1)+\sum_{i\neq j\leqq 3} d(1+a_i+a_j)+\sum_{i\neq j\leqq 3} d(a_i+a_j)+d(a_1+a_2+a_3)$$
$$+\sum_{i\neq j\leqq 3} d(a_ia_j+a_i+a_j)+d(a_1a_2+a_2a_3+a_3a_1)$$
$$+d(a_1a_2+a_2a_3+a_3a_1+a_1+a_2+a_3).$$

Let

$$\mathfrak{M}_2=\left\{\begin{matrix}\text{birationally equivalent classes of algebraic} \\ \text{curves with genus 2}\end{matrix}\right\}.$$

Then, $\mathfrak{M}_2$ has the structure of 3 dimensional algebraic variety.

We put

$$N_i=\{\text{equivalent classes of } C_K \text{ such that } N_K \leqq 15-i\}.$$

We put

$$v_1=1+\sum_{i=1}^{3} a_i, \qquad v_2=\sum_{i \neq j \leqq 3} a_i a_j+\sum_{i=1}^{3} a_i,$$

$$v_3=a_1 a_2 a_3+\sum_{i=1}^{3} a_i, \qquad v_4=a_1 a_2 a_3.$$

Moreover we put

$$J_2=-v_4+v_1 v_3,$$

$$J_4=-v_1 v_3 v_4-v_2^2 v_4-v_1^2 v_2 v_4-v_1^2 v_3^2+v_1 v_2^2 v_3,$$

$$J_6=-(-v_4^3-v_1 v_3 v_4^2+v_2^2 v_4^2+v_2 v_3^2 v_4-v_3^4+v_1^2 v_2 v_4^2+v_1^2 v_3^2 v_4+v_1 v_2^2 v_3 v_4$$
$$+v_1^3 v_2 v_3 v_4-v_1^2 v_2^3 v_4+v_1 v_2 v_3^3-v_1^2 v_2^2 v_3^2-v_1 v_2^4 v_3-v_2^6-v_2^4 v_4-v_2^3 v_3^2-v_1^4 v_4^2),$$

$$J_{10}=\prod_{i \neq j}(a_i-a_j)^2 \prod_{i=1}^{3}(a_i-1)^2.$$

Then it follows from the result of Igusa [5] that $\mathfrak{M}_2$ is a subvariety of A^8 and its coordinate ring is equal to

$$k\left[\begin{matrix} J_2^5 J_{10}^{-1},\ J_2^3 J_4 J_{10}^{-1},\ J_2^2 J_4 J_{10}^{-1},\ J_2^2 J_6 J_{10}^{-1} \\ J_4 J_6 J_{10}^{-1},\ J_2 J_6^3 J_{10}^{-2},\ J_4^5 J_{10}^{-2},\ J_6^5 J_{10}^{-3} \end{matrix}\right].$$

Then, it follows from the above fact that N_i is an algebraic set of $\mathfrak{M}_2$. 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 ξ is a root of the following equation $X^2+X-1=0$. 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 γ_K.

Table

	type of parameter	Hasse-Witt invariant
N_1		
S_1	$-1, a, b$	2
S_2	$a, -1-a, b$	2
S_3	$a, -a, b$	2
S_4	$a, b, -a-b$	1, 2
S_5	$a, b, -b/(1+b)$	
S_6	$a, b, (-ab-a-b)/(1+a+b)$	2
S_7	$a, b, -ab/(a+b)$	
N_2		
$C_1=S_1 \cap S_2$	$-1, a, -1-a$	2
$C_2=S_1 \cap S_3$	$-1, a, -a$	2
$C_3=S_1 \cap S_4$	$-1, a, -a+1$	2
$C_4=S_1 \cap S_5$	$-1, a, -a/(1+a)$	2
$C_5=S_1 \cap S_6$	$-1, a, 1/a$	2
$C_6=S_1 \cap S_7$	$-1, a, a/(a-1)$	2
$C_7=S_2 \cap S_3$	$a, -1-a, -a$	2
$C_8=S_2 \cap S_5$	$a, -1-a, -a/(1+a)$	2
$C_9=S_2 \cap S_7$	$a, -1-a, -a(1+a)$	2
$C_{10}=S_3 \cap S_5$	$a, -a, a/(a-1)$	2
$C_{11}=S_3 \cap S_6$	$a, -a, a^2$	2
$C_{12}=S_4 \cap S_5$	$a, -a/(1+a), -a^2/(1+a)$	2
N_3		
$S_1 \cap S_2 \cap S_7$	$-1, \xi, -1-\xi$	2
$S_1 \cap S_3 \cap S_6$	$-1, \xi^2, -\xi^2$	2
$S_1 \cap S_4 \cap S_5$	$-1, \xi-1, -\xi$	2
$S_2 \cap S_3 \cap S_5$	$\xi, -1+\xi, -\xi$	2

EXAMPLE 2. We shall consider the relation between $\{\gamma_{A^i}\}$. Let K be an algebraic function field with an algebraically closed constant field k of characteristic p and let g be its genus. Let $\bar{A}$ be an n division point of $\mathfrak{G}_0/\mathfrak{G}_H$. If i is prime to n, $\langle\bar{A}^i\rangle=\langle\bar{A}\rangle$. Then, it is natural to ask whether $\gamma_{A^i}=\gamma_A$ 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 $P_{01}, P_{02}, P_{03}, P$ such that $(x)=P_{01}P_{02}P_{03}/P^3$ and $(y+\zeta^i)=P_{0i}^5/P^5$, where ζ is a primitive cubic root of unity. We put $A=P_{03}/P$. Then, we have

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

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

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

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

Moreover, we have $((y+1)^{2k})=A^{10k}$. Hence, we have

$$C\begin{pmatrix}(y+1)^2(y+1)dx/y^2\\ (y+1)^2xdx/y^2\\ (y+1)^2x^2dx/y^2\end{pmatrix}=\begin{pmatrix}3&0&0\\0&4&0\\0&0&-3\end{pmatrix}\begin{pmatrix}(y+1)dx/y^2\\ xdx/y^2\\ x^2dy/y^2\end{pmatrix}.$$

Hence we have $\gamma_A=3$. Similarly, we have $\gamma_{A^2}=\gamma_{A^3}=\gamma_{A^4}=3$.

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_{-1}, P_i such that $(y)=P_0P_1P_{-1}P_i/P^4$ and $(x-i)=P_i^3/P^3$. We put $A=P_i/P$. Then, we have

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

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

and $((x-i)^2)=A^6$.

Then,

$$C\begin{pmatrix}(x-i)^2dx/y\\ (x-i)^2(x-i)dx/y^2\end{pmatrix}=\begin{pmatrix}0&0\\0&-4\end{pmatrix}\begin{pmatrix}dx/y\\ (x-i)dx/y^2\end{pmatrix}.$$

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

$$C\begin{pmatrix}(x-i)^2(x-i)dx/y^2\\ (x-i)^2(x-i)^2dx/y^2\end{pmatrix}=\begin{pmatrix}-4&0\\ i+4\sqrt[7]{i}&1\end{pmatrix}\begin{pmatrix}(x-i)dx/y^2\\ (x-i)^2dx/y^2\end{pmatrix}.$$

Hence, we have $\gamma_{A^2}=2$.

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

References

[1] M. P. Cartier, Une nouvell opération sur les formes différentielles, C. R. Acad. Sci. Paris, **244** (1957), 426-428.

[2] M. P. Cartier, Questions de rationalités des diviseures en géométrie algébrique, Bull. Soc. Math. France, **86** (1958), 177-251.

[3] A. Grothendieck, S. G. A., 1960-61, Exposé X.

[4] H. Hasse and E. Witt, Zyklische unverzweigte Erweiterungskörper von Primzahl Grade p über einem algebraischen Funktionenkörpern der Charakteristik p, Monatsh. Math. Phys., **43** (1936), 477-492.

[5] J. Igusa, Arithmetic variety of moduli for genus two, Ann. of Math., **72** (1960), 612-649.

[6] S. Lang, Elliptic functions, Addison-Wesly.

[7] J.-P. Serre, Groupe algébrique et corps de classes, Hermann, Paris.

[8] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grade p^m, J. Reine Angew. Math., **176** (1936), 126-140.

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