119. On Unramified Extensions of Algebraic Function Fields.

By Tuneo TAMAGAWA.

(Comm. by Z. SUETUNA, M.J.A., Nov. 12, 1951.)

Let K be an algebraic function field over an algebraically closed constant field k, with an arbitrary characteristic p. We can take a suitable element x of K such that K is separably algebraic over $k(x)$. The set $\mathfrak{L}_K$ of all differentials of the first kind of K forms a linear set over k whose dimension g is equal to the genus of K. Let L be a normal extension of K of degree n, $\mathfrak{G}$ the Galois group of this normal extension; let, further, $\mathfrak{L}_L$ be the linear set of all differentials of the first kind of L, whose dimension G is equal to the genus of L, d the degree of the different of L/K, then we have the well known formula of Hurwitz:

$$2G-2 = n(2g-2)+d. \tag{1}$$

L is clearly separably algebraic over $k(x)$, and every differential ω of L is expressed uniquely as $ydx\,(y\in L)$. ω is a differential of K if and only if $y\in K$. Let σ be an arbitrary element of $\mathfrak{G}$, then σ transforms ω to $\omega^\sigma = y^\sigma dx$. ω^σ depends only on ω and σ and not on the choice of a "separating element" x of K. Therefore σ induces a linear transformation of $\mathfrak{L}_L$, and if we choose a basis $\omega_1, \ldots, \omega_G$ of $\mathfrak{L}_L$, we have a matric representation $\sigma \to \mathbf{A}(\sigma)$ of $\mathfrak{G}$ such as

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_G \end{pmatrix} = \mathbf{A}(\sigma) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_G \end{pmatrix}. \tag{2}$$

We shall study the structure of this representation in the following lines. When the characteristic p of k is 0, this problem was solved completely by C. Chevalley and A. Weil.[1]

If p is a prime number, Weil's proof may be extended to the case $(p, n) = 1$, but if p divides n, our problem is more difficult, and has not yet been solved in general. This difficulty arises from the fact that the representation (2) is not completely reducible. In this paper, we shall deal with a special case: L is unramified over K and $\mathfrak{G}$ is a cyclic group. In this case, the different of L/K is the unit divisor, and the genus G of L is equal to $n(g-1)+1$. Let σ be a generator of $\mathfrak{G}$, fixed once for all. We shall first solve our problem in two spacial cases.

1) C. Chevalley—A. Weil, Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers. Abh. Math. Sem. Hamburg 10 (1934).

Case I. $(p, n) = 1$. Let ζ be an n-th root of unity, then we can select from L an element z_ζ such that $z_\zeta^\sigma = \zeta z_\zeta$. The principal divisor (z_ζ) is invariant by σ and since L is unramified over K, $(z_\zeta) = \mathfrak{a}_\zeta$ may be regarded as a divisor of K. If $\mathfrak{b}$ is an arbitrary divisor of K, we denote the dimension of the linear set of all elements of K whose denominators divide $\mathfrak{b}$, by $\dim\{\mathfrak{b}\}$. If $\zeta \neq 1$, $\mathfrak{a}_\zeta$ is not a principal divisor of K and $\dim\{\mathfrak{a}_\zeta^{-1}\} = 0$. Then from Riemann-Roch's theorem, we have $\dim\{(dx)\mathfrak{a}_\zeta\} = g-1$, and we have $g-1$ elements $y_1, \ldots, y_{g-1}$ which are linearly independent over k and whose denominators divide $(dx)\mathfrak{a}_\zeta$. Hence $g-1$ differentials of L, $\omega_{i,\zeta} = y_i z_\zeta dx$, $(1 \leq i \leq g-1)$, are linearly independent over k and are of the first kind, and we have $\omega_{i,\zeta}^\sigma = \zeta \omega_{i,\zeta}$. If $\zeta = 1$, we may take as $\omega_{i,1}$ $(1 \leq i \leq g)$ arbitrary g linearly independent differentials of the first kind of K. If $\zeta_1, \ldots, \zeta_n$ are all n-th roots of unity, $n(g-1)+1$ differentials of the first kind of L defined above are clearly linearly independent over k and form a basis of $\mathfrak{Q}_L$. Therefore the representation (2) is the direct sum of one identity representation of degree 1 and $g-1$ regular representations of $\mathfrak{G}$.

Case II. $n = p^\nu$. We introduce first the notion of additive differentials, which will be useful in the sequel. If $\omega \in \mathfrak{Q}_L$ is transformed by σ to $\omega + \omega'$, where ω' is in $\mathfrak{Q}_K$, then we shall call ω an *additive differential* of L. The set A_L of all additive differentials of L is obviously a linear sub-set of $\mathfrak{Q}_L$ containing $\mathfrak{Q}_K$. To each $\omega \in A_L$ corresponds $\omega' = \varphi(\omega) \in \mathfrak{Q}_K$ such that $\omega^\sigma = \omega + \omega'$, and we have a linear mapping φ from A_L into $\mathfrak{Q}_K$.

Lemma. $\varphi(A_L)$ *is at most* $(g-1)$*-dimensional over* k.

Proof. We shall prove this first in the case $\nu = 1$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ be prime divisors of k different with each other such that

$$\dim\{\mathfrak{p}_1 \ldots \mathfrak{p}_g\} = 1 ;$$

then we can take an element y of L satisfying following conditions[2]:

$$L = K(y), \quad y^p - y = v, \quad v \in K,$$

$$(v) = \frac{\mathfrak{h}}{\mathfrak{p}_1^p \ldots \mathfrak{p}_g^p}, \qquad y^\sigma = y + 1,$$

where $\mathfrak{h}$ is an integral divisor of K. If we consider $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ as divisors of L, it is obvious that

$$(y) = \frac{\mathfrak{H}}{\mathfrak{p}_1 \ldots \mathfrak{p}_g},$$

2) H. Hasse—E. Witt, Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p. Monatsh. f. Math. u. Phy. 43 (1936).

where $\mathfrak{P}$ is an integral divisor of L. We may assume without loss of generality, that $\mathfrak{p}_1$ is really contained in the denominator of v. from $\dim(\mathfrak{p}_1 \ldots \mathfrak{p}_g) = 1$ follows

$$\dim\{(dx)\mathfrak{p}_2^{-1}\ldots\mathfrak{p}_g^{-1}\} = 1, \quad \dim\{(dx)\mathfrak{p}_1^{-1}\ldots\mathfrak{p}_g^{-1}\} = 0,$$

so we have a differential ω_1 of the first kind of K such that $\omega_1 \neq 0$ and $\mathfrak{p}_2 \ldots \mathfrak{p}_g$ divides (ω_1). Then ω_1 is not contained in $\varphi(A_L)$. In fact, if $\omega_1 \in \varphi(A_L)$, we might take $A_L \ni \omega$ such that $\omega^\sigma = \omega + \omega_1$, then $\omega - y\omega_1 = \omega'$ should be invariant by σ, hence ω' should be a differential of K. Here ω' should not be contained in $\mathfrak{L}_K$, for if $\omega' \in \mathfrak{L}_K$, $y\omega_1$ must be of the first kind, and, on the other hand, L is an unramified extension of K and $\mathfrak{p}_1$ does not divide (ω_1), so $y\omega_1$ can not be of the first kind. Hence $y\omega_1$ should be a differential of K whose denominator contains only $\mathfrak{p}_1$ with exponent 1, and this contradicts the "residue theorem" of Hasse. So $\varphi(A_L)$ does not contain ω_1, and the dimension of $\varphi(A_L)$ is at most equal to $g-1$.

In the general case $\nu > 1$, L contains one and only one extension L_1 of K of degree p, and if $\omega \in A_L$, $\omega^\sigma = \omega + p\varphi(\omega) = \omega$, so ω is invariant by σ^p. Hence we have $\omega \in A_{L_1}$. As our assertion is already proved on L_1, our lemma is thereby proved in the general case.

Now we define $\mathbf{A} = \mathbf{A}(\sigma)$ by (2). Since $A^{p^\nu} = E$, the eigen-values of $\mathbf{A}$ are all equal to 1. We decompose $\mathfrak{L}_L$ in indecomposable subspace $\mathfrak{L}_1, \ldots, \mathfrak{L}_g$, with $\mathfrak{L}_L$ as a $\mathfrak{G}$-representation space, and take a suitable basis $\omega_{i,1}, \ldots, \omega_{i,\nu_i}$ of $\mathfrak{L}_i$ such that

$$\begin{pmatrix} \omega_{i,1} \\ \vdots \\ \omega_{i,\nu_i} \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 1 & \cdot & 1 \\ & \ddots & \\ 0 & \cdot & 1 \end{pmatrix} \begin{pmatrix} \omega_{i,1} \\ \vdots \\ \omega_{i,\nu_i} \end{pmatrix}.$$

Then we have $\omega_{1,1}^\sigma = \omega_{1,1}, \ldots, \omega_{g',1}^\sigma = \omega_{g',1}$. Therefore $\omega_{i,1}$ $(1 \leq i \leq g')$ are contained in $\mathfrak{L}_K$, for L is unramified over K and a differential ω of K is contained in $\mathfrak{L}_L$ if and only if ω is contained in $\mathfrak{L}_K$. So we have $g' \leq g$.

Next, let $\mathfrak{L}_{i_1}, \ldots, \mathfrak{L}_{i_h}$ be the set of all $\mathfrak{L}_i$'s such that $\nu_i \geq 2$. Then $\omega_{i_k,2}^\sigma = \omega_{i_k,2} + \omega_{i_k,1}$, hence $\omega_{i_1,2}, \ldots, \omega_{i_h,2}$ are additive differentials of L and $\varphi(\omega_{i_1,2}), \ldots, \varphi(\omega_{i_h,2})$ are linearly independent over k. Then we have $h \leq g-1$ from the above proved lemma. Furthermore from $\mathbf{A}^{p^\nu} = E$, we have $\nu_i \leq p^\nu$. The genus G of L is equal to $p^\nu(g-1)-1$, so we have $g' = g$, $h = g-1$, $\nu_{i_k} = p^\nu$ $(1 \leq k \leq g-1)$. We may assume $\nu_1 = 1$. Put $\eta_i = \omega_{i,p^\nu}$ $(2 \leq i \leq g)$. Then it is easily proved that

$$S_{pL/K}(\eta_i) = \omega_{i,1} \tag{3}$$

and the conjugates of η_i are linear combinations of $\omega_{i,1}, \ldots, \omega_{i,p^\nu}$.

As of course $\omega_{i,1} \neq 0$, it follows easily from (3) that p^ν conjugates of η_i are linearly independent over K. Then we may take $\omega_{i,1}$, and the conjugates of $\eta_i (2 \leq i \leq g)$ as a basis of A_L. Therefore the representation (2) is the direct sum of one identity representation of degree 1 and $(g-1)$ regular representations of $\mathfrak{G}$.

Finally, we study our problem in the general case $n = p^\nu n'$, $\nu \geq 1$, $n' > 1$, $(n', p) = 1$. L contains uniquely determined subfields L' and L'', which have degrees n' and p^ν over K respectively.

We decompose $\mathfrak{L}_L$ in indecomposable subspaces $\mathfrak{L}_1, \ldots, \mathfrak{L}_{g'}$ with $\mathfrak{L}_L$ as a $\mathfrak{G}$-representation space, σ introduces a linear transformation of $\mathfrak{L}_i$ whose eigen-values are all equal to some n'-th root of unity ζ. $\sigma^{n'} = \sigma''$ is a generator of the Galois group of the unramified cyclic extension L/L''. So we have from II, $g' = n'(g-1)-1$ and some $\mathfrak{L}_i$ is of dimension 1 and the other $\mathfrak{L}_i$'s are of dimension p^ν. We may assume that the dimension of $\mathfrak{L}_1$ is equal to 1. On the other hand, $\sigma^{p^\nu} = \sigma'$ is a generator of the Galois group of the extension on L/L', and the eigen-values of $A = A(\sigma)$ are as follows:

$$\underbrace{1, \ldots, 1}_{p^\nu(g-1)+1}, \quad \underbrace{\zeta_2, \ldots, \zeta_2}_{p^\nu(g-1)}, \quad \ldots, \underbrace{\zeta_{n'}, \ldots, \zeta_{n'}}_{p^\nu(g-1)},$$

where $1 = \zeta_1, \zeta_2, \ldots, \zeta_g$ are all the n-th roots of unity. Then $\mathfrak{L}_1$ induces the identity representation of degree 1, and the representation (2) is the direct sum of one identity representations of degree 1 and $g-1$ regular representations of $\mathfrak{G}$. We have thereby proved the following.

Theorem. If L is an unramified cyclic extension of K, then the representation (2) is the direct sum of one identity representation of degree 1 and $g-1$ regular representations of $\mathfrak{G}$.

Remark. If $(n, p) = 1$, the assumption "L is cyclic over K" in the above theorem is not necessary. When $(p, n) = p$ and L is not cyclic over K, I have not yet proved this theorem, but it seems to me very probable that the theorem is true in general.