ON UNRAMIFIED SEPARABLE ABELIAN p-EXTENSIONS OF FUNCTION FIELDS I

HISASI MORIKAWA

1. Let k be an algebraically closed field of characteristic $p>0$. Let K/k be a function field of one variable and L/K be an unramified separable abelian extension of degree p^r over K. The galois automorphisms $\varepsilon_1, \ldots, \varepsilon_{p^r}$ of L/K are naturally extended to automorphisms $\eta(\varepsilon_1), \ldots, \eta(\varepsilon_{p^r})$[1] of the jacobian variety J_L of L/k. If we take a svstem of p-adic coordinates on J_L, we get a representation $\{M_p(\eta(\varepsilon_\nu))\}$ of the galois group $G(L/K)$ of L/K over p-adic integers.

The aim the present note is to determine the p-adic integral representation $\{M_p(\eta(\varepsilon_\nu))\}$ for cyclic L/K (as a representation over p-adic integers). Use will be made of the results in our previous paper [2].

2. Let $\{H_0, H_1, \ldots, H_s\}$ be the set of all the subgroup of $G(L/K)$ such that $G(L/K)/H_i$ $(i=0, 1, \ldots, s)$ are cyclic, where H_0 means $G(L/K)$. We denote by L_{H_i} the subfield of L corresponding to H_i.

We use the following notations:

p^{ν_i}: the degree of L_{H_i} over K,

J_{L_H}: the jacobian variety of L_H/k,

$\pi_{L'/L''}$: the trace mapping of $J_{L'}$ onto $J_{L''}$, where $L'\supset L''$,[2]

$B_{L'/L''}$: the irreducible component of $\pi_{L'/L''}^{-1}(0)$ containing $\{0\}$,

$\bar{A}_{L'/L''}$: the quotient abelian variety of $J_{L'}$ by $B_{L'/L''}$,

$\alpha_{L'/L''}$: the natural homomorphism of $J_{L'}$ onto $\bar{A}_{L'/L''}$,

$\bar{\pi}_{L'/L''}$: the homomorphism of $\bar{A}_{L'/L''}$ onto $J_{L''}$ such that $\bar{\pi}_{L'/L''}\alpha_{L'/L''}=\pi_{L'/L''}$,

$\rho_{L'/L''}$: the cotrace mapping of $J_{L''}$ into $J_{L'}$,

$\bar{B}_{L'/L''}$: the quotient abelian variety of $J_{L'}$ by $\rho_{L'/L''}(J_{L''})$,

$A(n)$: the group consisting of all points t on A such that $nt=0$, where A is an abelian variety.

Received May 8, 1958.

1) 2) See 1.2 in [2].

3. When the order of $A(p)$ is p^r, we say, for the sake of simplicity, that the p-dimension of A is r. We denote by $\gamma(A)$ the p-dimension of A.

The next Šafarevič's lemma is fundamental for our study:

LEMMA 1 (*Šafarevič*).[3] *Let K be a function field of one variable over an algebraically closed field k and K' be a separable normal extension of p-power degree over K, where p is the characteristic of k. Let γ_K and $\gamma_{K'}$ be respectively the number of independent unramified separable cyclic extensions of degree p over K and K'. Then we have*

$$\gamma_{K'} = [K':\ K]\ (\gamma_K - 1) + 1.$$

On the other hand, the number of independent unramified separable cyclic extensions of degree p over K equals to the p-dimension $\gamma(J_K)$ of J_K([2]). Therefore we get:

LEMMA 2. *If $L \supset L_{H_i} \supset L_{H_j} \supset K$, we have*

$$(1)\quad \begin{aligned} \gamma(J_L) &= [L:\ L_{H_i}]\ (\gamma(J_{L_{H_i}}) - 1) + 1 = p^{r-\nu_i}(\gamma(J_{H_i}) - 1) + 1, \\ \gamma(J_{H_i}) &= [L_{H_i}:\ L_{H_j}]\ (\gamma(J_{H_j}) - 1) + 1 = p^{\nu_i - \nu_j}(\gamma(J_{H_j}) - 1) + 1. \end{aligned}$$

If x is a generic point of J_{H_i} over k, then $(\delta_{J_{H_i}} - \eta(\bar{\varepsilon}_{H_i}))x$ is a generic point of $B_{L_{H_i}}/K$ over k, where $\delta_{J_{H_i}}$ is the identity automorphism of $J_{L_{H_i}}$ and $\eta(\bar{\varepsilon}_{H_i})$ is the extension of a generator $\bar{\varepsilon}_{H_i}$ of the galois group $G(L_{H_i}/K)$ of L_{H_i}/K. Therefore we may denote

$$B_{L_{H_i}}/K = (\delta_{J_{L_{H_i}}} - \eta(\bar{\varepsilon}_{H_i}))\ (J_{L_{H_i}}).$$

LEMMA 3. $\gamma(B_{L_{H_i}}/K) = (\gamma(J_K) - 1)\ ([L_{H_i}:\ K] - 1)$
$= (\gamma(J_K) - 1)\ (p^{\nu_i} - 1)$

Proof. $\rho_{L_{H_i}/K}(J_K)$ and $B_{L_{H_i}/K}$ generate $J_{L_{H_i}}$ and $\rho_{L_{H_i}/K}(J_K) \cap B_{L_{H_i}/K}$ is a finite group. Hence we have

$$\begin{aligned} \gamma(B_{L_{H_i}/K}) &= \gamma(J_{L_{H_i}}/\rho_{L_{H_i}/K}(J_K)) = \gamma(J_{L_{H_i}}) - \gamma(\rho_{L_{H_i}/K}(J_K)) \\ &= ([L_{H_i}:\ K]\ (\gamma(J_K) - 1) + 1) - \gamma(J_K) \\ &= (\gamma(J_K) - 1)\ ([L_{H_i}:\ K] - 1) = (\gamma(J_K) - 1)\ (p^{\nu_i} - 1). \end{aligned}$$

4. First we shall show that $\rho_{L/L_{H_i}}$ and $\rho_{L_{H_i}/K}$ are purely inseparable.

[3] See § 3 in [3].

LEMMA 4. $\rho_{L/L_{H_i}}(\rho_{L_{H_i}/K})$ *is purely inseparable.*

Proof. Assume that $\rho_{L/L_{H_i}}^{-1}(0)$ $(\rho_{L_{H_i}/K}^{-1}(0))$ constains a $L_{H_i}(K)$, non-zero element t. Then there exists an element f in $L(L_{H_i})$, not in such that $f^{p^{r-\nu_i}}(f^{p^{\nu_i}})$ is contained in $L_{H_i}(K)$. This contradics with the separability of $L/L_{H_i}(L_{H_i}/K)$.

LEMMA 4. *If $G(L/K)$ is cyclic, the p-addic representation $M_p(\eta(\varepsilon_\nu))$ is equivalent to the direct sum of $(\gamma(J_K)-1)$ times of the regular representation and the identical representation as a representation over p-addic numbers.*

Proof. We shall prove the proposition by the induction on the degree p^r of L/K. If $r=0$, the proposition is clearly true. We assume that the proposition is true for the subfield L_H such that L/L_H is of degree p. Let ε be a generator of $G(L/K)$. Then the subgroup H corresponding to L_H is $(\varepsilon^{p^{r-1}})$. Since $\eta(\varepsilon)$ $(\rho_{L/L_H}(J_{L_H})) = \rho_{L/L_H}(J_{L_H})$, $\eta(\varepsilon)$ induces an automorphism $\eta^*(\varepsilon)$ on $J_L/\rho_{L/L_H}(J_{L_H})$. On the other hand $B_{L/L_H} = (\delta_{J_L} - \eta(\varepsilon^{p^{r-1}}))$ (J_L) and $J_L/\rho_{L/L_H}(J_{L_H})$ is isogeneous with B_{L/L_H}, hence $\eta^*(\varepsilon^{p^{r-1}}) \neq \delta_{J_L/\rho_{L/L_H}(J_{L_H})}$. By virtue of lemma 3 the p-dimension of B_{L/L_H} is $(p-1)(\gamma(J_{L_H})-1) = (p-1)p^{r-1}(\gamma(J_K)-1)$. Therefore, since $B_{L/L_H} = (\delta_{J_L} - \eta(\varepsilon^{p^{r-1}}))(J_L)$, we observe that the p-adic representation $\{M_p(\eta^*(\varepsilon^\nu))\}$ of $\{\eta^*(\varepsilon^\nu)\}$ is equivalent to $(\gamma(J_K)-1)$-times of the faithful irreducible representation of $G(L/K)$ over p-adic integers as a representation over p-adic numbers. This shows that $\{M_p(\eta(\varepsilon^\nu))\}$ is equivalent to the direct sum of $(\gamma(J_K)-1)$-times of the regular representation and the identical representation as a representation over p-adic numbers.

PROPOSITION 1. *The p-adic representation $\{M_p(\eta(\varepsilon_\nu))\}$ of $G(L/K)$ is equivalent to the direct sum of $(\gamma(J_K)-1)$-times of the regular representation and the identical representation as a representation over p-adic numbers.*

Proof. Since $G(L/K)$ is abelian, $\{M_p(\eta(\varepsilon_\nu))\}$ is equivalent to a direct sum of p-adic irreducible representations of cyclic factor groups of $G(L/K)$. By virtue of lemma 4, $\{M_p(\eta(\varepsilon_\nu))\}$ contains at least $(\gamma(J_K)-1)$-times of the p-adic irreducible faithful representation of any non-trivial cyclic factor group of $G(L/K)$. On the other hand the degree $p^r(\gamma(J_K)-1)+1$ of $\{M_p(\eta(\varepsilon_\nu))\}$ is equal to that of the direct sum of $(\gamma(J_K)-1)$-times of the regular representation and the identical representation. Moreover the latter sum contains exactly $(\gamma(J_K)-1)$-times of p-adic irreducible faithful representation of any non-trivial cyclic factor group of $G(L/K)$ and $\gamma(J_K)$-times of the identical representation. This shows that $\{M_p(\eta(\varepsilon_\nu))\}$ is equivalent to the sum of $(\gamma(J_K)-1)$-times of regular representation and the identical representation as a representation over p-adic numbers.

PROPOSITION 2. $\rho_{L_{H_i}/K}(J_K)\cap B_{L_{H_i}/K}=\rho_{L_{H_i}/K}\pi_{L_{H_i}/K}(J_{L_{H_i}}(p^{\nu_i}))$
$$=(\delta_{J_{B_{L_{H_i}/K}}}-\eta_{B_{L_{H_i}/K}}(\bar{\varepsilon}_{H_i}))^{-1}(0),$$
where $\eta_{B_{L_{H_i}/K}}(\bar{\varepsilon}_{H_i})$ *is the restriction of* $\eta(\bar{\varepsilon}_{H_i})$ *on* $B_{L_{H_i}/H}$.

Proof. Since $\pi_{L_{H_i}/K}\rho_{L_{H_i}/K}=\bar{\pi}_{L_{H_i}/K}\alpha_{L_{H_i}/K}\rho_{L_{H_i}/K}=p^{\nu_i}\delta_{J_K}$, we have $\rho_{L_{H_i}/K}\bar{\pi}_{L_{H_i}/K}(\bar{A}_{L_{H_i}/K}(p^{\nu_i}))=\alpha^{-1}_{L_{H_i}/K}(0)\cap\rho_{L_{H_i}/K}(J_K)=B_{L_{H_i}/K}\cap\rho_{L_{H_i}/K}(J_K)$. On the other hand $\pi_{L_{H_i}/K}(J_{L_{H_i}}(p^{\nu_i})=\bar{\pi}_{L_{H_i}/K}(\bar{A}_{L_{H_i}/K}(p^{\nu_i}))$, hence we have $\rho_{L_{H_i}/K}(J_K)\cap B_{L_{H_i}/K}=\rho_{L_{H_i}/K}\pi_{L_{H_i}/K}(J_{L_{H_i}}(p^{\nu_i}))$.

From $(\delta_{J_{L_{H_i}}}-\eta(\bar{\varepsilon}_{H_i}))\rho_{L_{H_i}/K}(J_K)=0$, we observe that $\rho_{L_{H_i}/K}(J_K)\cap B_{L_{H_i}/K}\subset(\delta_{B_{L_{H_i}/K}}-\eta_{B_{L_{H_i}/K}}(\bar{\varepsilon}_{H_i}))^{-1}(0)$. Therefore it is sufficient to prove that the order of $\rho_{L_{H_i}/K}(J_K)\cap B_{L_H/K}$ equals to that of $(\varepsilon_{B_{L_{H_i}/K}}-\eta_{B_{L_{H_i}/K}}(\bar{\varepsilon}_{H_i}))^{-1}(0)$. Since $J_K(p^{\nu_i})/\rho_{L_{H_i}/K}J_{L_{H_i}}(p^{\nu_i})\cong G(L_{H_i}/K)$ and $\rho_{L_{H_i}/K}$ is purely inseparable, the order of $\rho_{L_{H_i}/K}(J_K)\cap B_{L_{H_i}/K}$ is $p^{(\gamma(J_K)-1)\nu_i}$. On the other hand, by virtue of proposition 1, the p-adic representation $\{M_p(\eta_{B_{L_{H_i}/K}}(\bar{\mathfrak{z}}_{H_i\nu}))\}$ of $G(L_{H_i}/K)$ is equivalent to $(\gamma(J_K)-1)$-times of the sum of all the non-trivial irreducible p-adic representations of $G(L_{H_i}/K)$ as a representation over p-adic numbers. This shows that the order of $(\delta_{J_{B_{L_{H_i}/K}}}-\eta_{B_{L_{H_i}/K}}(\bar{\varepsilon}_{H_i}))^{-1}(0)$ is $p^{\nu_i(\gamma(J_K)-1)}$. We have proved proposition 2.

5. Using proposition 2, we shall determine the structure of J_L.

PROPOSITION 3. *Let* H_j *be the subgroup of* H_i *such that* H_i/H_j *is a cyclic group of order* p. *Then* $\rho_{L/L_j}(B_{L_j/L_i})$ *is the invariant abelian subvariety for* $\{\eta(\varepsilon_\nu)\}$ *on* J_L *such that the* p*-adic representation* $\{M_p^*(\eta(\varepsilon_\nu))\}$ *of* $\{\eta(\varepsilon_\nu)\}$ *on* $\rho_{L/L_{H_j}}(B_{L_{H_j}/L_{H_i}})$ *is equivalent to* $(\gamma(J_K)-1)$*-times of the* p*-adic irreducible representation* $\{M_p^{H_i}(\eta(\varepsilon_\nu))\}$ *of* $G(L/K)$ *whose kernel is* H_j, *as a representation over* p*-adic numbers.*

Proof. By virtue of proposition 1, the multiplicity of $\{M_p^{H_i}(\eta(\varepsilon_\nu))\}$ in

$\rho_{L/L_{H_j}}(J_{L_{H_j}})$ is $(\gamma(J_K)-1)$ and that in $\rho_{L/L_{H_i}}(J_{L_{H_i}})$ is zero. This proves the proposition.

We denote by B_{H_j} the above $\rho_{L/L_{H_j}}(B_{L_{H_j}/L_{H_i}})$. Namely B_{H_j} means the invariant subabelian variety on J_L for $\{\eta(\varepsilon^\nu)\}$ such that the p-adic representation of $\{\eta(\varepsilon_\nu)\}$ on B_{H_j} is equivalent to $(\gamma(J_K)-1)$-times of the p-adic irreducible representation of $G(L/K)$ whose kernel is H_j, as a representation over p-adic numbers. Then we get

THEOREM 1. *J_L is isogeneous with $B_{H_1}+\ldots+B_{H_s}+\rho_{L/K}(J_K)$ and the subvarieties $B_{H_1},\ldots,B_{H_s}$ and $\rho_{L/K}(J_K)$ satisfy the following conditions:*

(1) $$\rho_{L/K}(J_K)\cap B_{H_i}=\rho_{L/K}\pi_{L_{H_i}/K}(J_{H_i}(p)),$$

(2) $$\text{if } L_{H_i}\cap L_{H_j}=L_{H_l},$$

then

$$B_{H_i}\cap B_{H_j}=\rho_{L/L_{H_l}}(\pi_{L_{H_i}/L_{H_l}}(J_{L_{H_i}}(p))\cap\pi_{L_{H_j}/L_{H_l}}(J_{L_{H_j}}(p))$$
$$=\rho_{L/L_{H_l}}(J_{L_{H_l}})\cap B_{H_i}\cap B_{H_j}.$$

Proof. The first assertion has been proved in proposition 1. Let H_i' be the subgroup of $G(L/K)$ such that H_i'/H_i is a cyclic group of order p. Then, by virtue of theorem 2 in [2], we observe that $J_K(p^{\nu_i-1})/\pi_{L_{H_i'}/K}(J_{L_{H_i'}}(p^{\nu_i-1}))\cong G(L/K)/H_i'$ and $J_K(p^{\nu_i})/\pi_{L_{H_i}/K}(J_{L_{H_i}}(p^{\nu_i}))\cong G(L/K)/H_i$, hence $J_K(p)/\pi_{L_{H_i'}/K}(J_{L_{H_i'}}(p))$ and $J_K(p)/\pi_{L_{H_i}/K}(J_{L_{H_i}}(p))$ are isomorphic. On the other hand $\pi_{L_{H_i'}/K}(J_{L_{H_i}}(p))\subseteq\pi_{L_{H_i'}/K}(J_{L_{H_i'}}(p))$, therefore we have $\pi_{L_{H_i'}/K}J_{L_{H_i'}}(p)=\pi_{L_{H_i}/K}(J_{L_{H_i}}(p))$ for $L_{H_i'}\neq K$. Moreover, since $[J_{L_{H_i'}}(p):\ \pi_{L_{H_i}/L_{H_i}}(J_{L_{H_i}}(p))]=p$ and $\rho_{L_{H_i'}/K}\pi_{L_{H_i}/K}(J_{L_{H_i}}(p))\subseteq\rho_{L_{H_i'}/K}(J_K(p))$, we have $\rho_{L_{H_i'}/K}\pi_{L_{H_i'}/K}(J_{L_{H_i'}}(p))=\rho_{L_{H_i'}/K}\pi_{L_{H_i}/K}(J_{L_{H_i}}(p))=\rho_{L_{H_i}/K}(J_K)\cap\pi_{L_{H_i}/L_{H_i'}}(J_{L_{H_i}}(p))$.

On the other hand, by virtue of proposition 2 and the pure inseparability of $\rho_{L/K}$, we have

$$\rho_{L/K}(J_K)\cap B_{H_i}=\rho_{L/K}(J_K)\cap\rho_{L/L_{H_i}}(B_{L_{H_i}/L_{H_i'}})$$
$$=\rho_{L/L_{H_i}}(\rho_{L_{H_i}/K}(J_K)\cap(\rho_{L_{H_i}/L_{H_i'}}(J_{L_{H_i}})\cap B_{L_{H_i}/L_{H_i'}}))$$
$$=\rho_{L/L_{H_i}}(\rho_{L_{H_i}/K}(J_K)\cap\rho_{L_{H_i}/L_{H_i'}}\pi_{L_{H_i}/L_{H_i'}}(J_{L_{H_i}}(p))$$
$$=\rho_{L/L_{H_i'}}(\rho_{L_{H_i}/K}(J_K)\cap\pi_{L_{H_i}/L_{H_i'}}(J_{L_{H_i}}(p))),$$

https://doi.org/10.1017/S0027763000005869 Published online by Cambridge University Press

This proves (1).

By virtue of (1) we have

$$\rho_{L/LH_i}(J_{LH_i}) \cap B_{H_j} = \rho_{L/LH_i}\pi_{LH_i\frown H_j/LH_i}(J_{LH_i\frown H_j}(p))$$

and

$$\rho_{L/LH_j}(J_{LH_j}) \cap B_{H_i} = \rho_{L/LH_j}\pi_{LH_i\frown H_j/LH_j}(J_{LH_i\frown H_j}(p)).$$

On the other hand $\rho_{L/LH_i}(J_{LH_i}) \cap \rho_{L/LH_j}(J_{LH_j}) \subset \rho_{L/LH_i\frown LH_j}(J_{LH_i\frown LH_j})$ hence

$$B_{H_i} \cap B_{H_j} = \rho_{L/LH_i}\pi_{LH_i\frown H_j/LH_i}(J_{LH_i\frown H_j}(p))$$
$$\cap \rho_{L/LH_j}\pi_{LH_i\frown H_j/LH_j}(J_{LH_i\frown H_j}(p)) \subset \rho_{L/LH_i\frown LH_j}(J_{LH_i\frown LH_j}).$$

This shows that

$$B_{H_i} \cap B_{H_j} = B_{H_i} \cap B_{H_j} \cap \rho_{L/LH_i\frown LH_j}(J_{LH_i\frown LH_j}(p)).$$

Therefore, if $L_{H_i} \cap L_{H_j} = L_{H_l}$, we have

$$B_{H_i} \cap B_{H_j} = (\rho_{L/LH_l}(J_{LH_l}) \cap B_{H_i}) \cap (\rho_{L/LH_l}(J_{LH_l}) \cap B_{H_j})$$
$$= \rho_{L/LH_l}(\pi_{LH_i/LH_l}(J_{LH_i}(p)) \cap \rho_{LH_j/LH_l}(J_{LH_j}(p))).$$

6. In this section we shall study some p-adic integral representations of cyclic groups.

LEMMA 5. *Let $\{R(\varepsilon^\nu)\}$ be a regular representation and $\{M(\varepsilon^\nu)\}$ be any representation of a cyclic group (ε). Then a p-adic integral representation*

$$\left\{\begin{pmatrix} M(\varepsilon^\nu) & 0 \\ A(\varepsilon^\nu) & R(\varepsilon^\nu) \end{pmatrix}\right\}$$

is equivalent to

$$\left\{\begin{pmatrix} M(\varepsilon^\nu) & 0 \\ 0 & R(\varepsilon^\nu) \end{pmatrix}\right\}$$

as a p-adic integral representation.

Since the group ring $Z_p[G]$ over p-adic integers is projective as a left G-module, this lemma is clearly time.

LEMMA 6. *Let $G=(\varepsilon)$ be a cyclic group of order p^r and G_{r-1} be the subgroup $(\varepsilon^{p^{r-1}})$. Let $\{N(\varepsilon^{p^{r-1}})^\nu\}$ be the non-trivial irreducible p integral representation of G_{r-1}. Let $\{\hat{M}(\varepsilon)^\nu\}$ be the representation of G induced by*

https://doi.org/10.1017/S0027763000005869 Published online by Cambridge University Press

$\{N(\varepsilon^{p^{r-1}})^{\nu}\}$ and $\{R_{r-1}(\bar{\varepsilon})^{\nu}\}$ be the regular representation of G/G_{r-1}. Then any p-adic integral representation of the following type

$$\left\{\begin{pmatrix} E_n\times\hat{M}(\varepsilon) & 0 \\ A(\varepsilon) & E_n\times R_{r-1}(\bar{\varepsilon})\end{pmatrix}^{\nu}\right\}$$

is equivalent to

$$\left\{\begin{pmatrix} E_n\times\hat{M}(\varepsilon) & & 0 \\ \mathfrak{a} & 0 & E_n\times R_{r-1}(\bar{\varepsilon})\end{pmatrix}^{\nu}\right\}$$

as a representation over p-adic integers, where $\bar{\varepsilon}$ is the class of ε in G/G_{r-1} and $\mathfrak{a}$ is a p-adic integral $(np^{r-1},\ n(p-1))$-matrix.

Proof. Since $\{\hat{M}(\varepsilon)^{\nu}\}$ is the induced representation of G by $\{N(\varepsilon^{p^{r-1}})^{\nu}\}$, we have

$$E_n\times\hat{M}(\varepsilon)=\begin{pmatrix} 0 & E_{n(p-1)} & 0\ldots 0 & \\ 0 & \bigcirc & E_{n(p-1)} & \\ 0 & & & E_{n(p-1)} \\ E_n\times N & \bigcirc & \ldots\ldots & 0\end{pmatrix},$$

where $N=N(\varepsilon^{p^{r-1}})$. We put

$$\begin{pmatrix} E_n\times\hat{M}(\varepsilon) & \\ A(\varepsilon) & E_n\times R(\bar{\varepsilon})\end{pmatrix}=\left(\begin{array}{ccc|cccc} 0 & E_{n(p-1)} & 0\cdots 0 & & & & \\ \vdots & & \ddots\ \vdots & & & & \\ E_n\times N & & E_{n(p-1)} & & & & \\ & & 0 & & & & \\ \hline A_{00} & \cdots\cdots & A_{0,\,p^{r-1}-1} & 0 & E_n & & \\ \vdots & & & \vdots & & \ddots & \\ \vdots & & & \vdots & & & E_n \\ A_{p^{r-1}-1,\,0} & \cdots & A_{p^{r-1}-1,\,p^{r-1}-1} & E_n & & & 0\end{array}\right).$$

We choose p-adic integral matrices X_{ij} such that

$$X_{i,0}=0,\ X_{i+1,1}=A_{i,1},\ X_{i+1,j}=A_{i,j}-X_{i,j-1}$$

$(i=0,1,\ldots,p^{r-1}-1;\ j=1,2,\ldots,p^{r-1}-1)$, where $X_{p^{r-1},j}=X_{0,j}$ and $X_{i,-1}=X_{i,p^{r-1}-1}$. Then we have

$$\begin{pmatrix} E_{np^{r-1}(p-1)} & \\ X_{01}\cdots\cdots X_{0,\,p^{r-1}-1} & \\ \vdots & E_{np^{r-1}} \\ X_{p^{r-1}-1,\,0}\cdots X_{p^{r-1}-1,\,p^{r-1}-1} & \end{pmatrix}^{-1}\begin{pmatrix} E_n\times\hat{M}(\varepsilon) & \\ A(\varepsilon) & E_n\times R_{r-1}(\bar{\varepsilon})\end{pmatrix}$$

https://doi.org/10.1017/S0027763000005869 Published online by Cambridge University Press

$$\times \begin{pmatrix} \multicolumn{2}{c}{E_{np^{r-1}(p-1)}} & \\ X_{01} \cdots\cdots X_{0p^{r-1}-1} & & \\ \vdots & & E_{np^{r-1}} \\ X_{p^{r-1}-1,0} \cdots X_{p^{r-1}-1,p^{r-1}-1} & & \end{pmatrix} = \begin{pmatrix} E_n \times \hat{M}(\varepsilon) & \\ \mathfrak{a}_0 & \\ \mathfrak{a}_1 & \\ \vdots & \\ \mathfrak{a}_{p^{r-1}-1} & 0 \quad E_n \times R_{r-1}(\bar{\varepsilon}) \end{pmatrix},$$

where

$$\mathfrak{a}_i = A_{i,0} + X_{i+1,0}(E_n \times N - E_{n(p-1)}).$$

This proves the lemma.

LEMMA 7. *In the notations in lemma 6, let*

$$(*) \qquad \left\{ \begin{pmatrix} E_n \times \hat{M}(\varepsilon) & \\ A'(\varepsilon) & R_{r-1}(\bar{\varepsilon}) \end{pmatrix}^{\nu} \right\}$$

and

$$(**) \qquad \left\{ \begin{pmatrix} E_n \times \hat{M}(\varepsilon) & \\ A''(\varepsilon) & E_n \times R_{r-1}(\bar{\varepsilon}) \end{pmatrix}^{\nu} \right\}$$

be p-adic integral representations of (ε) whose restrictions on the subgroup $(\varepsilon^{p^{r-1}})$ are equivalent (as p-adic integral representation). Then the representations $(*)$ and $(**)$ are equivalent (as p-adic integral representations).

Proof. By virtue of lemma 6, we may assume that

$$A'(\varepsilon) = (\mathfrak{a}', 0) \text{ and } A''(\varepsilon) = (\mathfrak{a}'', 0)$$

with p-adic integral $(np^{r-1}, n(p-1))$-matrices $\mathfrak{a}'$ and $\mathfrak{a}''$. From the assumption of the lemma, we have

$$A''(\varepsilon^{p^{r-1}}) = A'(\varepsilon^{p^{r-1}}) + E_n \times R_{r-1}(\bar{\varepsilon}^{p^{r-1}})X - X \cdot E_n \times \hat{M}(\varepsilon^{p^{r-1}})$$

$$= A'(\varepsilon^{p^{r-1}}) + X - X \begin{pmatrix} E_n \times N(\varepsilon^{p^{r-1}}) & & \\ & \ddots & \\ & & E_n \times N(\varepsilon^{p^{r-1}}) \end{pmatrix},$$

with a p-adic integral matrix X.

On the other hand we observe that

$$E_n \times \hat{M}(\varepsilon) = \begin{pmatrix} 0 & E_{n(p-1)} & 0 \cdots 0 \\ \vdots & \ddots & \vdots \\ 0 & & E_{n(p-1)} \\ E_n \times N(\varepsilon^{p^{r-1}}) & & 0 \end{pmatrix}$$

https://doi.org/10.1017/S0027763000005869 Published online by Cambridge University Press

and

$$\begin{aligned} &A''(\varepsilon^{p^{r-1}}) - A'(\varepsilon^{p^{r-1}}) \\ &\quad = \sum_{\nu=0}^{p^{r-1}-1} E_n \times R_{r-1}(\bar{\varepsilon})^{p^{r-1}-1-\nu}(A''(\varepsilon) - A'(\varepsilon))E_n \times \hat{M}(\varepsilon)^{\nu}. \end{aligned}$$

Therefore, putting

$$A''(\varepsilon^{p^{r-1}}) - A'(\varepsilon^{p^{r-1}}) = (\overbrace{P,}^{n(p-1)} \overbrace{\quad Q \quad}^{n(p^{r-1}-1)(p-1)}),$$

we have

$$P = E_n \times R(\bar{\varepsilon})^{p^{r-1}-1}(\mathfrak{a}'' - \mathfrak{a}').$$

On the other hand, if we put

$$X = (\overbrace{Y,}^{n(p-1)} \overbrace{\quad Z \quad}^{n(p^{r-1}-1)(p-1)}),$$

we have

$$P = Y(E_{n(p-1)} - E_n \times N(\varepsilon^{p^{r-1}})).$$

This shows that

$$\begin{aligned} \mathfrak{a}'' - \mathfrak{a}' &= E_n \times R_{r-1}(\bar{\varepsilon})^{1-p^{r-1}} Y(E_{n(p-1)} - E_n \times N(\varepsilon^{p^{r-1}})) \\ &= E_n \times R_{r-1}(\bar{\varepsilon}) Y(E_{n(p-1)} - E_n \times N(\varepsilon^{p^{r-1}})) \end{aligned}$$

Hence, putting $Y_1 = E_n \times R_{r-1}(\bar{\varepsilon})Y$, we have

$$\begin{aligned} \begin{pmatrix} E_n \times \hat{M}(\varepsilon) & \\ A''(\varepsilon) & E_n \times R_{r-1}(\bar{\varepsilon}) \end{pmatrix} &= \begin{pmatrix} E_{n(p-1)p^{r-1}} & \\ Y_1 \;\; 0 & E_{np^{r-1}} \end{pmatrix}^{-1} \\ &\times \begin{pmatrix} E_n \times \hat{M}(\varepsilon) & \\ A'(\varepsilon) & E_n \times R_{r-1}(\bar{\varepsilon}) \end{pmatrix} \begin{pmatrix} E_{n(p-1)p^{r-1}} & \\ Y_1 \;\; 0 & E_{np^{r-1}} \end{pmatrix}. \end{aligned}$$

7. In this section, using proposition 2 and lemma 7, we shall prove the main theorem.

LEMMA 8. *If $G(L/K)$ is a cyclic group of order p, the p-adic representation $\{M_p(\eta(\varepsilon^{\nu}))\}$ of the galois group is equivalent to the direct sum of $(\gamma(J_K)-1)$-times of the regular representation and the identical representation as a representation over p-adic integers.*

Proof. First we notice that there exist only two inequivalent p-adic integral representations of $G(L/K)$

$$\left\{\begin{pmatrix} 1 & \\ \hline 1 & \\ 0 & \\ \cdot & N(\varepsilon) \\ \cdot & \\ \cdot & \\ 0 & \end{pmatrix}^{\nu}\right\} \quad \text{and} \quad \left\{\begin{pmatrix} 1 & \\ & N(\varepsilon)\end{pmatrix}^{\nu}\right\}$$

which have the same irreducible components 1 and $\{N(\varepsilon)^{\nu}\}$, where $\{N(\varepsilon)^{\nu}\}$ is the non-trivial irreducible representation.[4]

By virtue of proposition 2, we observe that

$$\rho_{L/K}(J_K)\cap B_{L/K} = (\delta_{B_{L/K}} - \eta(\varepsilon)_{B_{L/K}})^{-1}(0).$$

This shows that $\{M_p(\eta(\varepsilon))^{\nu}\}$ contains no

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & N(\varepsilon)\end{pmatrix}^{\nu}\right\}$$

as a component. Namely there exists a system of p-adic coordinates on J_L such that

$$M_p(\eta(\varepsilon)) = \begin{pmatrix} \left.\begin{matrix} R_1(\varepsilon) & & & \\ & \cdot & & \\ & & \cdot & \\ & * & & R_1(\varepsilon) \end{matrix}\right\} \gamma(J_K)-1 & \\ & 1 \end{pmatrix},$$

where $\{R_1(\varepsilon)^{\nu}\}$ is the regular representation of $G(L/K)$. By virtue of lemma 5, there exists a system of p-adic coordinates on J_L such that

$$M_p(\eta(\varepsilon)) = \begin{pmatrix} \left.\begin{matrix} R_1(\varepsilon) & & & \\ & \cdot & & \\ & & \cdot & \\ & & & R_1(\varepsilon) \end{matrix}\right\} \gamma(J_K)-1 & \\ & 1 \end{pmatrix}$$

---

[4] [5] Since $[Q_p(\sqrt[p^r]{1}): Q_p] = p^{r-1}(p-1)$ and the class number of $Q_p(\sqrt[p^r]{1})$ is one, there exists only one faithful p-adic integral irreducible representation. Moreover $G=(\varepsilon)$ is cyclic, hence a p-adic integral representation

$$\left\{\begin{pmatrix} \hat{M}(\varepsilon) & \\ \Delta(\varepsilon) & \hat{M}(\varepsilon)\end{pmatrix}^{\nu}\right\}$$

with an irreducible representation $\{\hat{M}(\varepsilon)^{\nu}\}$ is equivalent to

$$\left\{\begin{pmatrix} \hat{M}(\varepsilon) & \\ & \hat{M}(\varepsilon)\end{pmatrix}^{\nu}\right\}$$

as a representation over p-adic integers. See § 4, 6 in [1].

https://doi.org/10.1017/S0027763000005869 Published online by Cambridge University Press

THEOREM 2. *If $G(L/K)$ is cyclic, the p-adic representation $\{M_p(\eta(\varepsilon^{\vee}))\}$ of the galois group $G(L/K)$ is equivalent to the direct sum of $(\gamma(J_K)-1)$-times of the regular representation and the identical representation as a representation over p-adic integers.*

Proof. Let ε be a generator of $G(L/K)$ and H_i be the subgroup (ε^{p^i}) $(i=1,2,\ldots,r)$. We shall prove the theorem by the induction on $G(L/K)/H_i$. If $i=1$, by virtue of lemma 8, the theorem is true. We assume the theorem on $G(L/L_{H_{r-1}})$. Then, since G has only one faithful irreducible p-adic integral representation $\{\hat{M}(\varepsilon)^{\vee}\}$ and any p-adic integral representation of the following type

$$\left\{\begin{pmatrix}\hat{M}(\varepsilon) & 0\\ A(\varepsilon) & \hat{M}(\varepsilon)\end{pmatrix}^{\vee}\right\}$$

is equivalent to

$$\left\{\begin{pmatrix}\hat{M}(\varepsilon) & \\ & \hat{M}(\varepsilon)\end{pmatrix}^{\vee}\right\},^{5)}$$

there exists a system of p-adic coordinates on J_L such that

$$M_p(\eta(\varepsilon))=\begin{pmatrix}E_{\gamma(K)-1}\times\hat{M}(\varepsilon) & & \\ A(\varepsilon) & E_{\gamma(K)-1}\times R_{r-1}(\bar{\varepsilon}) & \\ \mathfrak{b}(\varepsilon) & & 1\end{pmatrix}$$

where $\{\hat{M}(\varepsilon)^{\vee}\}$ is the representation of $G(L/K)$ induced by the non-trivial irreducible representation $N(\varepsilon^{p^{r-1}})$ of $(\varepsilon^{p^{r-1}})$ and $\{R_{r-1}(\bar{\varepsilon})^{\vee}\}$ is the regular representation of $G(L/K)/H_{r-1}$.

On the other hand, by virtue of lemma 8,

$$(*)\qquad \{M_p(\eta(\varepsilon^{p^{r-1}})^{\vee})\}$$

is equivalent to the direct sum of $(\gamma(J_K)-1)p^{r-1}$-times of the regular representation of $(\varepsilon^{p^{r-1}})$ and the identical representation. The latter representation is equivalent to the restriction on $(\varepsilon^{p^{r-1}})$ of the direct sum of $(\gamma(J_K)-1)$-times of the regular representation of $G(L/K)$ and the identical representation. Therefor, by virtue of lemma 5, 7, we have a system of p-adic coordinates on J_L such that

$$M_p(\eta(\varepsilon)) = \begin{pmatrix} \left.\begin{matrix} R_r(\varepsilon) & & \\ & \ddots & \\ & & R_r(\varepsilon) \end{matrix}\right\} \gamma(J_K)-1 & \\ & 1 \end{pmatrix},$$

where $\{R_r(\varepsilon)^\nu\}$ is the regular representation of $G(L/K)$.

References

[1] Diederichsen, Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz, Abh. Math. Hamb. Sem. Bd. **13** (1940).

[2] H. Morikawa, Generalized jacobian varieties and separable abelian extensions of function fields, Nagoya Math. Jour. vol. **12** (1957).

[3] Šafarević, On p-extensions, Math. Sbornik N.S. **20** (62), (1947).