ACTA ARITHMETICA
108.2 (2003)

On the vanishing of Iwasawa invariants of geometric cyclotomic $\mathbb{Z}_p$-extensions

by

Akira Aiba (Ibaraki)

0. Introduction. Several authors have studied Iwasawa invariants of cyclotomic $\mathbb{Z}_p$-extensions of a number field. The constant $\mathbb{Z}_p$-extension of an algebraic function field K over a finite field of characteristic $p > 0$ has often provided a useful analogy for the study of cyclotomic $\mathbb{Z}_p$-extensions of number fields. But little is known about the corresponding results for geometric $\mathbb{Z}_p$-extensions of K (cf. [4]). In this paper, we first define a geometric cyclotomic $\mathbb{Z}_p$-extension of K (Section 1). Our aim is the determination of all abelian p-extension fields of a rational function field k such that the Iwasawa invariants of a geometric cyclotomic $\mathbb{Z}_p$-extension are zero. The main result is stated in Section 2. This is an analogue of G. Yamamoto's theorem ([7]). The proof is based on the central class field and genus field theory. The function field analogue that we need is essentially shown by Bae and Jung [1]. Following them, we determine in Section 3 all elementary abelian p-extensions of k whose class number is prime to p. Using this, we conclude the proof of our main theorem in Section 4.

1. Geometric cyclotomic $\mathbb{Z}_p$-extension. Let p be a prime and $\mathbb{Z}_p$ the ring of p-adic integers. Let q be a power of p and $\mathbb{F}_q$ the finite field of q elements. We set $k = \mathbb{F}_q(T)$, the rational function field over the finite field $\mathbb{F}_q$, and $O = O_k = \mathbb{F}_q[T]$. We write $k_{1/T}$ for the completion of k at the place corresponding to $1/T$ and choose a uniformizer π of $k_{1/T}$. Denote by C the field $k_{1/T}(\sqrt[q-1]{-\pi})$. In the following, by an *extension* of k we mean a separable extension of k for which any embedding into an algebraic closure $k^{\mathrm{ac}}_{1/T}$ lies in C viewed as a subfield of $k^{\mathrm{ac}}_{1/T}$. Let K be a finite abelian extension of k. Let O_K be the integral closure of O_k in K. Let I_K be the group of non-zero fractional ideals of O_K and P_K the group of non-zero principal ideals of O_K. We set $\mathrm{Pic}(O_K) = I_K/P_K$, the ideal class group of O_K. Let H_K be

2000 *Mathematics Subject Classification*: 11R23, 11R60.

the Hilbert class field of K, i.e. the maximal unramified geometric abelian extension of K. We set $h_K = \sharp\,\mathrm{Pic}(O_K)$. It is known that $\mathrm{Gal}(H_K/K) \simeq \mathrm{Pic}(O_K)$.

Let K_∞/K be a geometric $\mathbb{Z}_p$-extension (i.e. K_∞/K is a Galois extension with $\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ and for all n, the nth layer K_n has constant field $\mathbb{F}_q$). Let $A(K_n)$ be the p-Sylow subgroup of $\mathrm{Pic}(O_{K_n})$. Let $X_\infty = \varprojlim A(K_n)$ be the inverse limit of the groups $A(K_n)$ with respect to the norm map. Let Λ denote the complete group ring $\mathbb{Z}_p[[\Gamma]]$, so that $\Lambda \simeq \mathbb{Z}_p[[T]]$.

The proof of the next proposition is the same as that of Theorem 2 in [4].

PROPOSITION 1. *If there are only a finite number of primes* (*of* K) *ramified in* K_∞/K *then* X_∞ *is a noetherian torsion* Λ*-module. If there are infinitely many ramified primes then* X_∞ *is not a noetherian* Λ*-module.*

COROLLARY 1. *Let* K_∞/K *be a geometric* $\mathbb{Z}_p$*-extension with only a finite number of ramified primes. Then there exist integers* $\lambda = \lambda(K_\infty/K) \geq 0$, $\mu = \mu(K_\infty/K) \geq 0$, $\nu = \nu(K_\infty/K)$ *and* $n_0 \geq 0$ *such that*

$$\sharp A(K_n) = p^{\lambda n + \mu p^n + \nu} \quad \text{for all } n \geq n_0.$$

We denote by K_G the genus field of K. So K_G is the maximal geometric unramified abelian extension of K such that K_G/k is an abelian extension. As in the number field case it has been shown that (cf. [1, Lemma 1.1])

$$(*) \qquad [K_G : K] = \frac{\prod_v e_v}{[K : k]},$$

where e_v is the ramification index of a place v of k in K. We use this result to prove the next proposition.

PROPOSITION 2. *Let* k_∞/k *be a geometric* $\mathbb{Z}_p$*-extension over* $k = \mathbb{F}_q(T)$ *with only a finite number of ramified primes.*

(1) *If there is only one prime of* k *ramified in* k_∞/k *then* $\lambda(k_\infty/k) = \mu(k_\infty/k) = \nu(k_\infty/k) = 0$.

(2) *If there are more than two primes of* k *ramified in* k_∞/k *then* $\lambda(k_\infty/k) > 0$ *or* $\mu(k_\infty/k) > 0$.

Proof. (1) See [4, p. 156].

(2) Let k_∞/k be a geometric $\mathbb{Z}_p$-extension which ramifies at $P_1, \ldots, P_m$ ($m > 1$). There exists $n_0 \geq 0$ such that every prime which ramifies in k_∞/k_{n_0} is totally ramified. By $(*)$,

$$p^{sm - n_0 - s} \mid [(k_{n_0+s})_G : k_{n_0+s}]\sharp A(k_{n_0+s})$$

and

$$\log_p \sharp A(k_{n_0+s}) \geq (m-1)(s + n_0) - n_0 m.$$

Therefore $\mu(k_\infty/k) > 0$ or $\lambda(k_\infty/k) \geq m - 1$. ∎

Recall that the rational number field $\mathbb{Q}$ has a unique $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ ($\lambda(\mathbb{Q}_\infty/\mathbb{Q}) = \mu(\mathbb{Q}_\infty/\mathbb{Q}) = \nu(\mathbb{Q}_\infty/\mathbb{Q}) = 0$) and for a number field K, we call the $\mathbb{Z}_p$-extension $K \cdot \mathbb{Q}_\infty/K$ a *cyclotomic $\mathbb{Z}_p$-extension* of K. By Proposition 2, it is natural to make the following:

DEFINITION. Let k_∞/k be a geometric $\mathbb{Z}_p$-extension unramified outside one prime over a rational function field $k = \mathbb{F}_q(T)$. Let K be a finite extension of k. We set $K_\infty = Kk_\infty$. We call the $\mathbb{Z}_p$-extension K_∞/K a *geometric cyclotomic $\mathbb{Z}_p$-extension*.

2. Main theorem. First, we define some notations and recall some properties of Artin–Schreier extensions. For details, see [5], [6].

Let F be a field of characteristic $p > 0$. If L is an abelian extension of degree p of F (an *Artin–Schreier extension* of F), then L can be written as $L = F(y_A)$, where y_A satisfies the equation

$$y_A^p - y_A = A \quad \text{with } A \in F.$$

(1) *Local case*. Let $F = \mathbb{F}_q((t))$ be the power series field over a finite field $\mathbb{F}_q$. We let o be the valuation ring, $\mathfrak{p}$ its maximal ideal and $v_\mathfrak{p}$ the valuation with respect to $\mathfrak{p}$. We put $L = F(y_A)$. Then L/F is unramified if and only if $A \in o + \mathcal{P}F$, where $\mathcal{P}F = \{x^p - x : x \in F\}$. In this case, let $\left(\frac{L/F}{\mathfrak{p}}\right)$ be the Frobenius automorphism and set $\left(\frac{A}{\mathfrak{p}}\right) = \left(\frac{L/F}{\mathfrak{p}}\right)y_A - y_A$.

For $a \in F^*, x \in F$, let $x\frac{da}{dt} = \sum_i c_i t^i$. It is known that $\operatorname{Res} x da = c_{-1}$ (the residue of a differential form xda) is independent of the choice of a uniformizer t. We set

$$\left(\frac{a, x}{\mathfrak{p}}\right) = \operatorname{Tr}\left(\operatorname{Res} x\frac{da}{a}\right),$$

where $\operatorname{Tr} = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$. If $F(y_A)/F$ is unramified, then $\left(\frac{a,A}{\mathfrak{p}}\right) = v_\mathfrak{p}(a)\left(\frac{A}{\mathfrak{p}}\right) \in \mathbb{F}_p$.

(2) *Global case.* We set $k = \mathbb{F}_q(T)$. Let $K = k(y_A)$ be an Artin–Schreier extension of k. One may assume that A is in *standard form*, that is,

$$A = \frac{B}{\prod P_i^{e_i}},$$

where

(a) $P_i \in O_k$ are irreducible polynomials,
(b) e_i are positive integers relatively prime to p,
(c) $B \in O_k$ is relatively prime to the denominator, and
(d) $\deg A = \deg B - \deg(\prod P_i^{e_i})$ is negative.

The primes of k that ramify in $k(y_A)$ are exactly the P_i. From now on, when we consider an Artin–Schreier extension $k(y_{B/\prod P_i^{e_i}})$ of a global field, we assume that $B/\prod P_i^{e_i}$ is in standard form.

For $P \in O_k$ an irreducible polynomial of degree d, we let i_P be the natural embedding

$$i_P : k \hookrightarrow k_P \simeq \mathbb{F}_{q^d}((t)),$$

where k_P is the completion of k at P. For $a \in k^*, x \in k$, we define $\mathrm{Res}_P\, x da = \mathrm{Res}\, i_P(x) d i_P(a)$. We can show the reciprocity law in this case as follows:

Proposition 3 ([6, Chapter 4, §5]). *For $a \in k^*, x \in k$,*

$$\sum_P \left(\frac{i_P(a), i_P(x)}{P} \right) = 0,$$

where the sum runs over the irreducible polynomials of O_k.

Corollary 2. *Let $P \neq Q$ be irreducible polynomials in O_k and $A = B/P^e$. Then*

$$\left(\frac{A}{Q}\right) = -\,\mathrm{Tr}\left(\mathrm{Res}_P\, A \frac{dQ}{Q}\right).$$

Proof. By the definition and Proposition 3,

$$0 = \sum_L \left(\frac{i_L(Q), i_L(A)}{L} \right) = \left(\frac{i_P(Q), i_P(A)}{P} \right) + \left(\frac{i_Q(Q), i_Q(A)}{Q} \right)$$
$$= \mathrm{Tr}\left(\mathrm{Res}_P\, A \frac{dQ}{Q}\right) + \left(\frac{A}{Q}\right). \quad \blacksquare$$

We now state our main result.

Theorem. *Let k_∞/k be a geometric cyclotomic $\mathbb{Z}_p$-extension which ramifies only at P_0. Let the first layer be $k_1 = k(y_{B_0/P_0^{e_0}})$. Let K be an abelian p-extension of k, and $P_1, \ldots, P_t$ be distinct prime factors different from P_0 of its conductor f_K. Let $\widetilde{K}$ be the maximal elementary p-subextension of K and $K_\infty = K k_\infty$. If*

$$\lambda(K_\infty/K) = \mu(K_\infty/K) = \nu(K_\infty/K) = 0, \tag{1}$$

then $t \leq 2$. Conversely, in each case of $t = 0, 1$ or 2, the following are necessary and sufficient conditions for (1):

In case $t=0$, (1) *always holds.*

In case $t=1$, (1) *holds if and only if $K_1 = K_{1,G}$ and $\widetilde{K} = k(y_{C_1}, \ldots, y_{C_s}) \not\supset k(y_{B_0/P_0^{e_0}})$, where either*

(1.1)
$$C_i = t_{i0} B_0/P_0^{e_0} + \sum_{j=1}^{s} t_{ij} B_j / P_1^{e_j} \quad \textit{for } t_{ij} \in \mathbb{F}_p \ (1 \leq j \leq s),$$
$$\mathrm{Tr}\left(\mathrm{Res}_{P_0} \frac{B_0 dP_1}{P_0^e P_1}\right) \neq 0$$

or

$$(1.2)\qquad \begin{aligned} &C_i=\sum_{j=0}^{s-1} t_{ij}B_i/P_0^{e_j}+t_{is}B_s/P_1^{e_s} \quad \textit{for } t_{ij}\in\mathbb{F}_p\ (1\le j\le s),\\ &\operatorname{Tr}\left(\operatorname{Res}_{P_1}\frac{B_s dP_0}{P_1^{e_s}P_0}\right)\neq 0. \end{aligned}$$

In case $t=2$, (1) *holds if and only if* $K_1=K_{1,G}$ *and* $\widetilde{K}=k(y_{C_1},y_{C_2})\not\supset k(y_{B_0/P_0^{e_0}})$, *where* $C_i=\sum_{j=0}^{2} t_{ij}B_j/P_j^{e_j}$ *for* $t_{ij}\in\mathbb{F}_p$, $\operatorname{rank}(t_{ij})=2$ *and*

$$\begin{aligned} &\operatorname{Tr}\left(\operatorname{Res}_{P_0}\frac{B_0 dP_1}{P_0^{e_0}P_1}\right)\operatorname{Tr}\left(\operatorname{Res}_{P_1}\frac{B_1 dP_2}{P_1^{e_1}P_2}\right)\operatorname{Tr}\left(\operatorname{Res}_{P_2}\frac{B_2 dP_0}{P_2^{e_2}P_0}\right)\\ &\qquad\neq \operatorname{Tr}\left(\operatorname{Res}_{P_0}\frac{B_0 dP_2}{P_0^{e_0}P_2}\right)\operatorname{Tr}\left(\operatorname{Res}_{P_1}\frac{B_1 dP_0}{P_1^{e_1}P_0}\right)\operatorname{Tr}\left(\operatorname{Res}_{P_2}\frac{B_2 dP_1}{P_2^{e_2}P_1}\right). \end{aligned}$$

3. Review of the genus theory. Suppose that p is a prime and $\operatorname{Gal}(K/k)$ is an abelian p-group. Then the genus field K_G of K is also an abelian p-extension as is easily seen from $(*)$. If p does not divide the class number of K, then K does not have any non-trivial geometric unramified abelian p-extension by class field theory, hence $K_G=K$. In the following we will assume $K_G=K$. Further, we consider the central p-class field K_C of K, that is, K_C is the maximal p-extension of K such that K_C/K is geometric, abelian and unramified, K_C/k is Galois and $\operatorname{Gal}(K_C/K)$ is in the center of $\operatorname{Gal}(K_C/k)$. Since a p-group must have a lower central series that terminates in the identity, one sees that $p\nmid h_K$ if and only if $K_C=K$. So we are interested in when $K_C=K$. This can be reduced to the case when $\operatorname{Gal}(K/k)$ is an elementary abelian p-group by the following result:

Lemma 1 ([2, Theorem 1], [7, Lemma 3]). *Let K/k be an abelian p-extension with $K_G=K$. Let $\widetilde{K}$ be the maximal intermediate extension between k and K such that* $\operatorname{Gal}(\widetilde{K}/k)$ *is an elementary p-group. Then the p-rank of* $\operatorname{Gal}(K_C/K)$ *is equal to the p-rank of* $\operatorname{Gal}((\widetilde{K})_C/\widetilde{K})$.

Now let K/k be a finite elementary abelian p-extension. Let $G=\operatorname{Gal}(K/k)$ and X_G be the group of characters of G. Let $\bigwedge^2(G)$ denote the exterior product of G. If $[K:k]=p^r$, we may view G and $\bigwedge^2(G)$ as $\mathbb{F}_p$-vector spaces of dimension r and $r(r-1)/2$, respectively. Let $\{\chi_1,\dots,\chi_r\}$ be a basis of X_G over $\mathbb{F}_p$. Let S be the set of all primes of k which ramify on K. For each prime $P\in S$, let $\{\mathfrak{g}_1,\dots,\mathfrak{g}_s\}$ be a basis of the decomposition group G_P over $\mathbb{F}_p$. Let $[\delta_{tu,\alpha\beta}]_{\mathfrak{p}}$ be the matrix over $\mathbb{F}_p$ with $s(s-1)/2$ rows and $r(r-1)/2$ columns whose entry $\delta_{tu,\alpha\beta}$ in the tu row and $\alpha\beta$ column is defined by the relation

$$(\chi_\alpha\wedge\chi_\beta)(\mathfrak{g}_t\wedge\mathfrak{g}_u)=\zeta_p^{\delta_{tu,\alpha\beta}},$$

where ζ_p is a fixed primitive pth root of unity and $\wedge$ is the exterior product. Let $\Delta(K/k)$ be the matrix over $\mathbb{F}_p$ whose rows are all the rows of the matrices $[\delta_{tu,\alpha\beta}]_{\mathfrak{p}}$ as $\mathfrak{p}$ runs over all elements of S.

PROPOSITION 4 ([3, Theorem 3], [1, Proposition 2.2]). *Let K/k be a finite elementary abelian p-extension. Then the following are equivalent*:

(1) $\mathrm{Gal}(K_C/K)$ *has trivial p-rank.*
(2) $\Delta(K/k)$ *has rank $r(r-1)/2$, where r is the p-rank of* $\mathrm{Gal}(K/k)$.

Now we use this criterion to determine all elementary abelian p-extensions of k whose class number is prime to p.

Let $P_1, \dots, P_z$ be distinct monic irreducible polynomials and let $d_i = \deg P_i$ for each i. Let K be a finite elementary abelian p-extension of k whose conductor has prime factors $P_1, \dots, P_z$. Let T_{P_i} be the inertia group of P_i and r_i be the p-rank of T_{P_i}.

If $z = 1$, then P_1 is the only prime of k which ramifies in K. So the decomposition group G_{P_1} of P_1 is G and p does not divide h_K.

If $z \geq 4$, then $z < z(z-1)/2$. The p-rank of $\bigwedge^2(G_{P_i})$ is at most $r_i(r_i+1)/2$. Since $\operatorname{rank} G = \sum \operatorname{rank} T_{P_i}$ (cf. [1, Section 1]), the p-rank of $\bigwedge^2(G)$ is $\sum r_i(\sum r_i - 1)/2$. We have

$$\frac{\sum r_i(\sum r_i - 1)}{2} - \sum_i \frac{r_i(r_i+1)}{2} = \sum_{i<j} r_i r_j - \sum_i r_i$$
$$= \sum_{i=1}^{z-1} r_i(r_{i+1}-1) + r_z(r_1-1) + \sum_{\substack{i+1<j \\ (i,j)\neq(1,z)}} r_i r_j > 0.$$

So $\mathrm{Gal}(K_C/K)$ has non-trivial p-rank and p divides h_K. It remains to consider the cases: $z=2$ and $z=3$.

LEMMA 2. *Suppose $z = 2$. Then $p \nmid h_K$ if and only if, by changing the order of P_1 and P_2 if necessary, $K = k(y_{A_{1,1}}, y_{A_{2,1}}, \dots, y_{A_{2,s}})$ $(A_{i,j} = B_{i,j}/P_k^{e_{ij}})$ and*

$$\mathrm{Tr}\left(\mathrm{Res}_{P_1} A_{1,1} \frac{dP_2}{P_2}\right) \neq 0.$$

Proof. Since $K_G = K$, the p-rank of G is $r = r_1 + r_2$. Since G_{P_i}/T_{P_i} is a cyclic group, the p-rank of G_{P_i} is r_i or $r_i + 1$. Hence in order that $\Delta(K/k)$ has rank $r(r-1)/2$, we must have

$$\binom{r}{2} \leq \sum_{i=1}^{2} \binom{r_i+1}{2}.$$

Hence $p \nmid h_K$ only if $r_1 r_2 - (r_1 + r_2) \leq 0$. This inequality holds if and only if either $r_1 = r_2 = 2$ (in this case, the p-rank of G_{P_i} is $r_i + 1$ for $i = 1, 2$) or $r_i = 1$ for some i.

When $r_1 = r_2 = 2$, let

$$K = k(y_{A_{1,1}}, y_{A_{1,2}}, y_{A_{2,1}}, y_{A_{2,2}}),$$
$$T_{P_i} = \mathrm{Gal}(K/k(y_{A_{j,1}}, y_{A_{j,2}})) \quad (i = 1, 2,\ j \neq i).$$

Let $\{\chi_{i,1}, \chi_{i,2}\}$ be a basis of the dual group of T_{P_i} over $\mathbb{F}_p$ defined by $\chi_{i,k}(\sigma) = \zeta_p^{(\sigma-1)y_{A_{i,k}}}$ for $\sigma \in T_{P_i}$. Then with respect to the basis $\{\chi_{1,1}\wedge\chi_{1,2}, \ldots, \chi_{2,1}\wedge\chi_{2,2}\}$, by choosing suitable bases of G_{P_i}'s, the matrix $\Delta(K/k)$ is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \left(\frac{A_{2,1}}{P_1}\right) & \left(\frac{A_{2,2}}{P_1}\right) & 0 & 0 & 0 \\ 0 & 0 & 0 & \left(\frac{A_{2,1}}{P_1}\right) & \left(\frac{A_{2,2}}{P_1}\right) & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & -\left(\frac{A_{1,1}}{P_2}\right) & 0 & -\left(\frac{A_{1,2}}{P_2}\right) & 0 & 0 \\ 0 & 0 & -\left(\frac{A_{1,1}}{P_2}\right) & 0 & -\left(\frac{A_{1,2}}{P_2}\right) & 0 \end{pmatrix}.$$

Since

$$\begin{aligned}\det(\Delta(K/k)) &= -\left(\frac{A_{2,1}}{P_1}\right)\left(\frac{A_{2,2}}{P_1}\right)\left(\frac{A_{1,1}}{P_2}\right)\left(\frac{A_{1,2}}{P_2}\right) + \left(\frac{A_{2,2}}{P_1}\right)\left(\frac{A_{2,1}}{P_1}\right)\left(\frac{A_{1,1}}{P_2}\right)\left(\frac{A_{1,2}}{P_2}\right) \\ &= 0,\end{aligned}$$

p divides h_K.

When $r_i = 1$ and $r_j \geq 1$ arbitrary, we may assume that $i = 1$, $j = 2$. Let $K = k(y_{A_{1,1}}, y_{A_{2,1}}, \ldots, y_{A_{2,r_j}})$, $T_{P_1} = \mathrm{Gal}(K/k(y_{A_{2,1}}, \ldots, y_{A_{2,r_2}}))$ and $T_{P_2} = \mathrm{Gal}(K/k(y_{A_{1,1}}))$. Let χ_1 be a multiplicative character on the inertia group T_{P_1} defined by $\chi_1(\sigma) = \zeta_p^{(\sigma-1)y_{A_{1,1}}}$ for $\sigma \in T_{P_1}$ and $\{\chi_{2,1}, \chi_{2,2}, \ldots, \chi_{2,r_2}\}$ be a basis of the dual group of T_{P_2} defined by $\chi_{2,k}(\tau) = \zeta_p^{(\tau-1)y_{A_{2k}}}$ for $\tau \in T_{P_2}$. With respect to the basis $\{\chi_1 \wedge \chi_{2,1}, \chi_1 \wedge \chi_{2,2}, \ldots, \chi_{2,r_2-1} \wedge \chi_{2,r_2}\}$, again by choosing suitable bases for G_{P_1}'s, the matrix $\Delta(K/k)$ is

$$\begin{pmatrix} \left(\frac{A_{2,1}}{P_1}\right) & \left(\frac{A_{2,2}}{P_1}\right) & \ldots & \left(\frac{A_{2,r_2}}{P_1}\right) & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 1 \\ -\left(\frac{A_{1,1}}{P_2}\right) & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & -\left(\frac{A_{1,1}}{P_2}\right) & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & -\left(\frac{A_{1,1}}{P_2}\right) & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

So we see that $\Delta(K/k)$ has rank $r(r-1)/2$, where $r = r_2 + 1$, if and only if $\left(\frac{A_{1,1}}{P_2}\right) \neq 0$. By Corollary 2, this condition is equivalent to

$$\mathrm{Tr}\left(\mathrm{Res}_{P_1} A_{1,1} \frac{dP_2}{P_2}\right) \neq 0. \blacksquare$$

LEMMA 3. *Suppose $z=3$. Then $p \nmid h_K$ if and only if $K = k(y_{A_1}, y_{A_2}, y_{A_3})$ ($A_i = B_i/P_i^{e_i}$) and*

$$\mathrm{Tr}\left(\mathrm{Res}_{P_1} A_1 \frac{dP_2}{P_2}\right) \mathrm{Tr}\left(\mathrm{Res}_{P_2} A_2 \frac{dP_3}{P_3}\right) \mathrm{Tr}\left(\mathrm{Res}_{P_3} A_3 \frac{dP_1}{P_1}\right) \neq \mathrm{Tr}\left(\mathrm{Res}_{P_1} A_1 \frac{dP_3}{P_3}\right) \mathrm{Tr}\left(\mathrm{Res}_{P_2} A_2 \frac{dP_1}{P_1}\right) \mathrm{Tr}\left(\mathrm{Res}_{P_3} A_3 \frac{dP_2}{P_2}\right).$$

Proof. Let T_{P_i} be the inertia group of P_i in $G = \mathrm{Gal}(K/k)$. Then the p-rank of G is $r_1 + r_2 + r_3$. Since G_{P_i}/T_{P_i} is a cyclic group, the p-rank of G_{P_i} is either r_i or $r_i + 1$. Hence the p-rank of $\bigwedge G_{P_i}$ is either $\binom{r_i}{2}$ or $\binom{r_i+1}{2}$ and

$$\binom{r}{2} \leq \sum_{i=1}^{3} \binom{r_i + 1}{2}.$$

Thus $p \nmid h_K$ only if $(r_1 r_2 + r_1 r_3 + r_2 r_3) - (r_1 + r_2 + r_3) \leq 0$. This inequality holds if and only if $r_1 = r_2 = r_3 = 1$. (In this case, the p-rank of G_{P_i} is $r_i + 1$ for $i = 1, 2, 3$.) Let $K = k(y_{A_1}, y_{A_2}, y_{A_3})$ and $T_{P_i} = \mathrm{Gal}(K/k(y_{A_j}, y_{A_k}))$, where $\{i, j, k\} = \{1, 2, 3\}$. Let χ_i be a multiplicative character on the inertia group T_{P_i} defined by $\chi_i(\sigma) = \zeta_p^{(\sigma-1)y_{A_i}}$ for $\sigma \in T_{P_i}$. With respect to the basis $\{\chi_1 \wedge \chi_2, \chi_1 \wedge \chi_3, \chi_2 \wedge \chi_3\}$ the matrix $\Delta(K/k)$ is given by

$$\begin{pmatrix} \left(\frac{A_2}{P_1}\right) & \left(\frac{A_3}{P_1}\right) & 0 \\ -\left(\frac{A_1}{P_2}\right) & 0 & \left(\frac{A_3}{P_2}\right) \\ 0 & -\left(\frac{A_1}{P_3}\right) & -\left(\frac{A_2}{P_3}\right) \end{pmatrix}.$$

So $\Delta(K/k)$ has rank 3 if and only if

$$\left(\frac{A_2}{P_1}\right)\left(\frac{A_3}{P_2}\right)\left(\frac{A_1}{P_3}\right) \neq \left(\frac{A_3}{P_1}\right)\left(\frac{A_1}{P_2}\right)\left(\frac{A_2}{P_3}\right).$$

By Corollary 2, this completes the proof. $\blacksquare$

EXAMPLE. Let $p = q > 2$. For $a, b \in \mathbb{F}_p$, and natural numbers e, f, g, we set $A_1 = 1/T^e$, $A_2 = 1/(T+a)^f$ and $A_3 = 1/(T+b)^g$. Let $K = k(y_{A_1}, y_{A_2}, y_{A_3})$. Then p is prime to h_K if and only if

$$(-1)^{e+f+g} a^{e-f} b^{g-e} (a-b)^{f-g} \neq 1, 0.$$

4. Proof of the Theorem. Suppose that $\lambda(K_\infty/K) = \mu(K_\infty/K) = \nu(K_\infty/K) = 0$. This condition is equivalent to $A(K_n) = 0$ for any sufficiently large n. This is equivalent to $K_n = K_{n,G} = K_{n,C}$. By Lemma 1, $\widetilde{K}$ must be an elementary abelian p-extension of k such that

$$\widetilde{K}k_1 = \widetilde{K}_n = (\widetilde{K}_n)_C = (\widetilde{K}k_1)_C.$$

By the argument of Section 3, when $t = 0$, K always satisfies this condition, and when $t \geq 3$, it does not.

In the case of $t = 1$, by Lemma 2,

$$\widetilde{K}k_1 = k(y_{A_0}, y_{A_1}, \ldots, y_{A_s}),$$

where either

$$A_0 = B_0/P_0^{e_0}, \quad A_i = B_i/P_1^{e_i} \quad (1 \leq i \leq s), \quad \mathrm{Tr}\left(\mathrm{Res}_{P_0} A_0 \frac{dP_1}{P_1}\right) \neq 0$$

or

$$A_i = B_i/P_0^{e_i} \quad (0 \leq i \leq s-1), \quad A_s = B_s/P_1^{e_s}, \quad \mathrm{Tr}\left(\mathrm{Res}_{P_1} A_0 \frac{dP_0}{P_0}\right) \neq 0.$$

It will suffice to find conditions for their subfields of index p to be different from k_1. But these conditions are (1.1) and (1.2).

In the case of $t = 2$, we use Lemma 3 and the statement can be obtained in the same way.

Conversely, assume that K satisfies the conditions of the Theorem. Then $K_n = K_1k_n = (K_n)_G$ and $(\widetilde{\widetilde{K}k_n})_C = (\widetilde{K}k_1)_C = \widetilde{K}k_1 = \widetilde{\widetilde{K}k_n}$ for all $n \geq 1$. This completes the proof.

Acknowledgements. The author is grateful to the referee for his very careful reading of the manuscript and for his comments that improved the presentation.

References

[1] S. Bae and H. Jung, *Central extensions and Hasse norm principle over function fields*, Tokyo J. Math. 24 (2001), 93–106.

[2] G. Cornell and M. Rosen, *The class group of an absolutely abelian l-extension*, Illinois J. Math. 32 (1988), 453–461.

[3] F. Gerth, *The Hasse norm principle for abelian extensions of number fields*, Bull. Amer. Math. Soc. 83 (1977), 264–266.

[4] R. Gold and H. Kisilevsky, *On geometric $\mathbb{Z}_p$-extensions of function fields*, Manuscripta Math. 62 (1988), 145–161.

[5] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. 172 (1934), 37–54.

[6] S. Iyanaga (ed.), *Suuron* [Number Theory], Iwanami Shoten, Tokyo, 1969 (in Japanese).

[7] G. Yamamoto, *On the vanishing of Iwasawa invariants of absolutely abelian p-extensions*, Acta Arith. 94 (2000), 365–371.

Department of Mathematical Sciences
Ibaraki University
Mito, Ibaraki 310-8512, Japan
E-mail: aiba@mx.ibaraki.ac.jp

Received on 19.2.2001
and in revised form on 9.8.2002 (3976)