Bounding the symbol length in the Galois cohomology of function fields of $p$-adic curves

Venapally Suresh

Dedicated to my teacher Professor R. Parimala on her 60th birthday

Abstract. Let $K$ be a function field of a $p$-adic curve and $l$ a prime not equal to $p$. Assume that $K$ contains a primitive $l$th root of unity. We show that every element in the $l$-torsion subgroup of the Brauer group of $K$ is a tensor product of two cyclic algebras over $K$.

Mathematics Subject Classification (2000). Galois cohomology, central simple algebras, cyclic algebras, symbols.

Keywords. Primary 12G05; Secondary 11R58, 11R34.

Introduction

Let $k$ be a field and $l$ a prime number not equal to the characteristic of $k$. Let $\mu_l$ be the group of $l$th roots of unity and $\mu_l(m)$ the tensor product of $m$ copies of $\mu_l$. For $n \ge 0$, let $H^n(k, \mu_l)$ denote the $n$th Galois cohomology group with coefficients in $\mu_l$. Let $k^* = k \setminus \{0\}$. We have an isomorphism $k^*/k^*_l \to H^1(k, \mu_l)$. For $a \in k^*$, let $(a)$ denote its image in $H^1(k, \mu_l)$. For $a_1, \ldots, a_m \in k^*$, the cup product gives an element $(a_1) \cdot (a_2) \ldots (a_m) \in H^n(k, \mu_l(m))$, which we call a symbol.

Assume that $k$ contains a primitive $l$th root of unity. Fix a primitive $l$th root of unity $\zeta \in k$. Then we have isomorphisms $\mu_l \to \mu_l(m)$ of Galois groups. Hence we have isomorphisms $H^n(k, \mu_l(m)) \to H^n(k, \mu_l)$. A symbol in $H^n(k, \mu_l)$ is simply the image of a symbol under this map.

A classical theorem of Merkurjev ([M]) asserts that every element in $H^2(k, \mu_2)$ is a sum of symbols. A deep result of Merkurjev and Suslin ([MS]) says that every element in $H^2(k, \mu_l)$ is a sum of symbols. By a theorem of Voevodsky ([V]), every element in $H^n(k, \mu_2)$ is a sum of symbols. Suppose that $k$ is a $p$-adic field. Local class field theory tells us that every element in $H^2(k, \mu_l)$ is a symbol and $H^n(k, \mu_l) = 0$ for $n \ge 3$. If $k$ is a global field, then the global class field theory asserts that every element in $H^n(k, \mu_l)$ is a symbol.
**Question 1.** Do there exist integers $N_l(n)(k)$ such that every element in $H^n(k, \mu_l)$ is a sum of at most $N_l(n)(k)$ symbols?

Of course, the answer to the above question is negative in general. It can be shown that for $K = k(X_1, \ldots, X_n, \ldots)$, there is no such $N_l(n)(K)$ for $n \geq 2$. However we can restrict to some special fields. It is well-known that if $N_l(n)(k)$ exist for $k$, then $N_l(n)(k((t)))$ exist. We ask the following

**Question 2.** Suppose that $N_l(n)(k)$ exist for some field $k$. Do they exist for $k(t)$?

This is an open question. However we can restrict to fields of arithmetic interest. For example we consider the $p$-adic fields. The most important result in this direction is the following

**Theorem** (Saltman, [S1], (cf. [S2])). Let $k$ be a $p$-adic field and $K/k(t)$ be a finite extension. Suppose that $l \neq p$. If $A$ is a central simple algebra over $K$ representing an element in $H^2(K, \mu_1)$, then $\text{ind}(A)$ divides $l^2$.

Let $K$ be as in the above theorem. Suppose $p \neq 2$. Let $\alpha \in H^2(K, \mu_2)$ and $A$ a central simple algebra over $K$ representing $\alpha$. Then by the above theorem, we have $\text{ind}(A) = 1, 2, 4$. If $\text{ind}(A) = 1$, then $\alpha$ is a trivial element. If $\text{ind}(A) = 2$, then it is well known that $\alpha$ is a symbol. Assume that $\text{ind}(A) = 4$. By a classical theorem of Albert ([A]), $\alpha$ is a sum of two symbols. For $H^3(K, \mu_1)$, we have the following

**Theorem** ([PS2], 3.5, (cf. [PS1], 3.9)). Let $k$ be a $p$-adic field and $K/k(t)$ be a finite extension. Suppose that $l \neq p$. Every element in $H^3(K, \mu_1)$ is a symbol.

Let $k$ and $K$ be as above. The field $K$ is of cohomological dimension $3$ and $H^n(K, \mu_1) = 0$ for $n \geq 4$. By the above theorem, $N_l(3)(K) = 1$ and the only case where $N_l(n)(K)$ is to be determined is for $n = 2$. It is known that $N_l(2)(K) \geq 2$ (cf. [S1], Appendix). In this article we prove the following

**Theorem.** Let $k$ be a $p$-adic field and $K/k(t)$ be a finite extension. Suppose that $l \neq p$. Every element in $H^2(K, \mu_1)$ is a sum of at most two symbols; in other words, $N_l(2)(K) = 2$.

1. **Some preliminaries**

In this section we recall a few basic facts about Galois cohomology groups and divisors on arithmetic surfaces. We refer the reader to ([C]), ([Li1]), ([Li2]) and ([Se]).
Let $k$ be a field and $l$ a prime number not equal to the characteristic of $k$. Assume that $k$ contains a primitive $l^{th}$ root of unity. Let $\zeta \in k$ be a primitive $l^{th}$ root of unity. Let $\mu_l$ be the group of $l^{th}$ roots of unity. Since $k$ contains a primitive $l^{th}$ root of unity, the absolute Galois group of $k$ acts trivially on $\mu_l$. For $m \geq 1$, let $\mu_l(m)$ denote the tensor product of $m$ copies of $\mu_l$. By fixing a primitive $l^{th}$ root of unity $\zeta$ in $k$, we have isomorphisms of Galois modules $\mu_l(m) \to \mu_l$. Throughout this paper we fix a primitive $l^{th}$ root of unity and identify $\mu_l(m)$ with $\mu_l$.

Let $H^n(k, A)$ be the $n^{th}$ Galois cohomology group of the absolute Galois group $\Gamma$ of $k$ with values in a discrete $\Gamma$-module $A$. The identification of $\mu_l(m)$ with $\mu_l$ gives an identification of $H^n(k, \mu_l(m))$ with $H^n(k, \mu_l)$. In the rest of this paper we use this identification.

Let $k^* = k \setminus \{0\}$. For $a, b, c \in k^*$ we have the following relations in $H^2(k, \mu_l)$.

1. $(a) \cdot (bc) = (a) \cdot (b) + (a) \cdot (c)$;
2. $(a) \cdot (b) = -((b) \cdot (a))$;
3. $(a) \cdot (b^l) = 0$;
4. $(a) \cdot (-a) = 0$.

If $l \geq 3$, we have $(a) \cdot (a) = (a) \cdot ((-1)^l a) = (a) \cdot (-a) = 0$.

Let $K$ be a field and $l$ a prime number not equal to the characteristic of $K$. Let $v$ be a discrete valuation of $K$. The residue field of $v$ is denoted by $\kappa(v)$. Suppose $\text{char}(\kappa(v)) \neq l$. Then there is a residue homomorphism $\partial_v: H^n(K, \mu_l(m)) \to H^{n-1}(\kappa(v), \mu_l(m-1))$. Let $\alpha \in H^n(K, \mu_l(m))$. We say that $\alpha$ is unramified at $v$ if $\partial_v(\alpha) = 0$; otherwise it is said to be ramified at $v$.

Let $X$ be a regular integral scheme of dimension $d$, with function field $K$. Let $X^1$ be the set of points of $X$ of codimension 1. A point $x \in X^1$ gives rise to a discrete valuation $v_x$ on $K$. The residue field of this discrete valuation ring is denoted by $\kappa(x)$. The corresponding residue homomorphism is denoted by $\partial_x$. We say that an element $\zeta \in H^n(K, \mu_l(m))$ is unramified at $x$ if $\partial_x(\zeta) = 0$; otherwise it is said to be ramified at $x$. We define the ramification divisor $\text{ram}_X(\zeta) = \sum x$ as $x$ runs over points in $X^1$ where $\zeta$ is ramified. Suppose $C$ is an irreducible subscheme of $X$ of codimension 1. Then the generic point $x$ of $C$ belongs to $X^1$ and we set $\partial_C = \partial_x$. If $\alpha \in H^n(K, \mu_l(m))$ is unramified at $x$, then we say that $\alpha$ is unramified at $C$. We say that $\alpha$ is unramified on $X$ if it is unramified at every point of $X^1$.

Let $k$ be a $p$-adic field and $K$ the function field of a smooth projective geometrically integral curve $X$ over $k$. By the resolution of singularities for surfaces (cf. [Li1] and [Li2]), there exists a regular projective model $\mathcal{X}$ of $X$ over the ring of integers $\mathcal{O}_k$ of $k$. We call such an $\mathcal{X}$ a regular projective model of $K$. Since the generic fibre $X$ of $\mathcal{X}$ is geometrically integral, it follows that the special fibre $\mathcal{X}'$ is connected. Further if $D$ is a divisor on $\mathcal{X}$, there exists a proper birational morphism $\mathcal{X}' \to \mathcal{X}$ such that the total transform of $D$ on $\mathcal{X}'$ is a divisor with normal crossings (cf. [Sh], Theorem, p. 38 and Remark 2, p. 43). We use this result throughout this paper without further
We have the induced homomorphism

**Theorem 1.2** (Saltman [S1]). Let $K, \alpha, X, C$ and $E$ be as above and $P \in C \cup E$. Let $R$ be the local ring at $P$. Let $\pi, \delta \in R$ be local equations of $C$ and $E$ respectively at $P$.

1. If $P \in C \setminus E$ (or $E \setminus C$), then $\alpha = \alpha' + (\pi) \cdot (u)$ (or $\alpha = \alpha' + (\delta) \cdot (u)$) for some unit $u \in R$, $\alpha' \in H_2^1(K, \mu_1)$ unramified on $R$.
2. If $P \in C \cap E$, then either $\alpha = \alpha' + (\pi) \cdot (u) + (\delta) \cdot (v)$ or $\alpha = \alpha' + (\pi) \cdot (u\delta^i)$ for some units $u, v \in R$, $\alpha' \in H_2^1(K, \mu_1)$ unramified on $R$.

Let $P \in C \cap E$. Suppose that $\alpha = \alpha' + (\pi) \cdot (u) + (\delta) \cdot (v)$ for some units $u, v \in R$, $\alpha' \in H_2^1(K, \mu_1)$ unramified on $R$ and $\pi, \delta$ are local equations of $C$ and $E$ respectively. Then $u(P) = \partial_C(\alpha)(P)$ and $v(P) = \partial_E(\alpha)(P)$. Note that $u(P)$ and $v(P)$ are uniquely defined modulo $l^r$ powers. Following Saltman ([S3], §2), we say that $P$ is a hot point of $\alpha$ if $u(P)$ and $v(P)$ do not generate the same subgroup of $\kappa(P)^*/\kappa(P)^{ul}$.

We have the following

**Theorem 1.2** (Saltman ([S3], 5.2). Let $k, K, \alpha, X$ be as above. Then $\alpha$ is a symbol if and only if there are no hot points of $\alpha$.

### 2. The main theorem

Let $k$ be a $\mathfrak{p}$-adic field and $K/k(t)$ be a finite extension. Let $l \geq 3$ be a prime number not equal to $p$. Assume that $k$ contains a primitive $l^{th}$ root of unity. Let $\beta \in H_2^1(K, \mu_1)$ and $X$ a regular proper model of $K$. Let $\phi : X' \to X$ be a blow-up such that $X'$ is a regular proper model of $K$ and ram$_{X'}(\beta) = C' + E'$, where $C'$ and $E'$ are two regular curves with normal crossings (cf. §1 or [S1], Proof of 2.1). Let $Q \in C' \cap E'$. Let $C'_1 \subset C'$ and $E'_1 \subset E'$ be the irreducible curves containing $Q$. Let $R' = O_{X', Q}$ be the regular local ring at $Q$ and $m_Q$ its maximal ideal. We have $m_Q = (\pi', \delta')$, where $\pi'$ and $\delta'$ are local equations of $C'_1$ and $E'_1$ at $Q$ respectively. Let $v_{C'_1}$ and $v_{E'_1}$ be the discrete valuations on $K$ at $C'_1$ and $E'_1$ respectively.

Let $P = \phi(Q)$. Let $R$ be the regular local ring at $P$ and $m_P$ its maximal ideal. We have the induced homomorphism $\phi^* : R \to R'$ of local rings, which is injective. Let $\pi, \delta \in R$ be such that $m_P = (\pi, \delta)$. 


Lemma 2.1. Suppose that $\beta = \beta' + (f') \cdot (g')$ for some $f', g' \in K$ and $\beta'$ unramified on $R'$. Then $Q$ is not a hot point of $\beta$. 

Proof. Since $\beta'$ is unramified on $R'$, the ramification data of $\beta$ on $R'$ is same as that of $(f') \cdot (g')$. Since $(f') \cdot (g')$, being a symbol, has no hot points ([S3], cf. 1.2), $Q$ is not a hot point of $\beta$. □

Lemma 2.2. Suppose that $\beta = \beta' + (\delta) \cdot (gv) + (f) \cdot (g)$, where $\beta'$ is unramified on $R'$, $f \in R$ is not divisible by $\delta$ and $v, g \in R$ are units with $g(P) = v(P)$. Then $Q$ is not a hot point of $\beta$. 

Proof. We have $m_Q = (\pi', \delta')$ and $\beta$ has ramification on $R'$ only at $\pi'$ and $\delta'$. Since $R/m_P \hookrightarrow R'/m_Q$, we have $g(Q) = g(P) = v(P) = v(Q)$. If $C'_1$ (or $E'_1$) is the strict transform of a curve on $\mathcal{X}$, then either $\delta$ is a local equation of $C'_1$ or $v_{C'_1}(\delta) = 0$. In fact, if $C'_1$ is the strict transform of $C_1$ on $\mathcal{X}$, then $v_{C'_1}(\delta) = v_{C'_1}(\delta)$ and $\delta$ itself being a prime in $R$, the assertion follows.

Suppose that $C'_1$ and $E'_1$ are strict transforms of two irreducible curves on $\mathcal{X}$. If $\delta$ is not a local equation for either $C'_1$ or $E'_1$, we claim that $(\delta) \cdot (gv)$ is unramified on $R'$. In fact, since $g$ and $v$ are units in $R$, $(\delta) \cdot (gv)$ is unramified on $R$ except possibly at $\delta$. Since $f$ is not divisible by $\delta$, $(f) \cdot (g)$ is unramified at $\delta$. Since $\beta$ is ramified on $R'$ only at $\pi'$ and $\delta'$ and $\delta$ is not one of them, $(\delta) \cdot (gv)$ is unramified on $R'$. By (2.1), $Q$ is not a hot point of $\beta$. Assume that $\delta$ is a local equation for one of them, say $C'_1$. Since $\delta$ does not divide $f$, we have $\partial_{C'_1}(\beta) = \overline{gv}$ and $\partial_{E'_1}(\beta) = \tilde{g}^{\nu_{E'_1}(f)}$, where $\bar{g}$ denotes the image in the residue field of $C'_1$ and $\tilde{g}$ denotes the image in the residue field of $E'_1$. Since $\beta$ is ramified at $E'_1$, $\nu_{E'_1}(f)$ is not a multiple of $l$.

We have $\partial_{C'_1}(\beta)(Q) = v(Q)g(Q) = g(Q)^2$ and $\partial_{E'_1}(\beta)(Q) = g(Q)^{\nu_{E'_1}(f)}$. Since $\nu_{E'_1}(f)$ is not a multiple of $l$, $g(Q)^2$ and $g(Q)^{\nu_{E'_1}(f)}$ generate the same subgroup modulo $l$th powers. Hence $Q$ is not a hot point of $\beta$. 

Suppose that $C'_1$ is a strict transform of an irreducible curve on $\mathcal{X}$ and $E'_1$ is an exceptional curve on $\mathcal{X}'$. We have $\partial_{E'_1}(\beta) = (g^v)^{\nu_{E'_1}(\delta)} \cdot \tilde{g}^{\nu_{E'_1}(f)}$. Since $E'_1$ is an exceptional fibre in $\mathcal{X}'$, the residue field of $R$ is contained in the residue field at $E'_1$. Hence $\partial_{E'_1}(\beta) = (g(P)v(P))^{\nu_{E'_1}(\delta)} g(P)^{\nu_{E'_1}(f)} = g(P)^{2\nu_{E'_1}(\delta)+\nu_{E'_1}(f)}$. Since $\beta$ is ramified at $E'_1$, $2\nu_{E'_1}(\delta) + \nu_{E'_1}(f)$ is not a multiple of $l$. Suppose $\delta$ is a local equation of $C'_1$ at $Q$. Since $\delta$ does not divide $f$ and $v_{C'_1}(\delta) = 1$, we have $\partial_{C'_1}(\beta) = g^v$. Thus $\partial_{C'_1}(\beta)(Q) = g(P)v(P) = g(P)^2$. Since $l \neq 2$ and $2\nu_{E'_1}(\delta) + \nu_{E'_1}(f)$ is not a multiple of $l$, the subgroups generated by $g(Q)^2$ and $g(P)^{2\nu_{E'_1}(\delta)+\nu_{E'_1}(f)}$ are equal modulo $l$th powers. Hence $Q$ is not a hot point of $\beta$. Suppose $\delta$ is not a local equation of $C'_1$ at $Q$. We have $\partial_{C'_1}(\beta) = g^{\nu_{C'_1}(f)}$. Since $\beta$ is ramified at $C'_1$, $\nu_{C'_1}(f)$ is not a multiple of $l$. Thus as above $Q$ is not a hot point of $\beta$. 

Vol. 85 (2010) Bounding the symbol length 341
Theorem 2.4. Suppose that both $C'_1$ and $E'_1$ are exceptional curves in $X'$. Then as above we have
\[ \partial_{C'_1}(\beta) = g(P)^{2v_{C'_1}(\delta)+v_{C'_1}(f)} \quad \text{and} \quad \partial_{E'_1}(\beta) = g(P)^{2v_{E'_1}(\delta)+v_{E'_1}(f)}. \]
Since $\beta$ is ramified at $C'_1$ and $E'_1$, $2v_{C'_1}(\delta)+v_{C'_1}(f)$ and $2v_{E'_1}(\delta)+v_{E'_1}(f)$ are not multiples of $l$. In particular, the subgroups generated by $g(P)^{2v_{C'_1}(\delta)+v_{C'_1}(f)}$ and $g(P)^{2v_{E'_1}(\delta)+v_{E'_1}(f)}$ are equal modulo the $l$th powers. Thus $Q$ is not a hot point of $\beta$. \hfill \Box

Lemma 2.3. Suppose that $\beta = \beta' + (\pi) \cdot (u) + (\delta) \cdot (v)$, where $\beta'$ unramified on $R'$ and $u, v \in R$ units with $u(P) = v(P)$. Then $Q$ is not a hot point of $\beta$.

Proof. Since $\beta$ is ramified at $C'_1$, either $v_{C'_1}(\pi)$ or $v_{C'_1}(\delta)$ is not divisible by $l$. In particular their sum $v_{C'_1}(\pi \delta)$ is non-zero. We have
\[ \partial_{C'_1}(\beta)(Q) = u(P)^{v_{C'_1}(\pi)} v(P)^{v_{C'_1}(\delta)} = u(P)^{v_{C'_1}(\pi \delta)}. \]
Suppose that $v_{C'_1}(\pi \delta)$ is a multiple of $l$. Since $v_{C'_1}(\pi \delta)$ is non-zero, $C'_1$ is an exceptional curve. As in the proof of (2.2), we see that $\partial_{C'_1}(\beta) = u(P)^{v_{C'_1}(\pi \delta)} = 1$. Which is a contradiction, as $\beta$ is ramified at $C'_1$. Hence $v_{C'_1}(\pi \delta)$ is not a multiple of $l$. Similarly, we have $\partial_{E'_1}(\beta)(Q) = u(P)^{v_{E'_1}(\pi \delta)}$ and $v_{E'_1}(\pi \delta)$ is not a multiple of $l$. Hence $u(P)^{v_{C'_1}(\pi \delta)}$ and $u(P)^{v_{E'_1}(\pi \delta)}$ generate the same subgroup of $\kappa(P)^*$ modulo $\kappa(P)^{s^l}$ and $Q$ is not a hot point of $\beta$. \hfill \Box

Theorem 2.4. Let $k$ be a $p$-adic field and $K/k(t)$ be a finite extension. Let $l$ be a prime number not equal to $p$. Suppose that $k$ contains a primitive $l$th root of unity. Then every element in $H^2(K, \mu_l)$ is a sum of at most two symbols.

Proof. If $l = 2$, then, as we mentioned before, by $([A]), \alpha$ is a sum of at most two symbols. Assume that $l \geq 3$. Let $\alpha \in H^2(K, \mu_l)$. Let $X$ be a regular proper model of $K$ such that $\text{ram}_X(\alpha) = C + E$, where $C$ and $E$ are regular curves with normal crossings.

Let $P \in C \cup E$ be a closed point of $X$. Let $R_P$ be the regular local ring at $P$ on $X$ and $m_P$ be its maximal ideal.

Let $T$ be a finite set of closed points of $X$ containing $C \cap E$ and at least one closed point from each irreducible curve in $C$ and $E$. Let $A$ be the semi-local ring at $T$ on $X$. Let $\pi_1, \ldots, \pi_r, \delta_1, \ldots, \delta_s \in A$ be prime elements corresponding to irreducible curves in $C$ and $E$ respectively. Let $f_1 = \pi_1 \ldots \pi_r \delta_1 \ldots \delta_s \in A$. Let $P \in C \cap E$. Then $P \in C_i \cap E_j$ for unique irreducible curves $C_i$ in $C$ and $E_j$ in $E$. Then $\pi = \pi_i$ and $\delta = \delta_j$ are local equations of $C$ and $E$ at $P$. We have $\alpha = \alpha' + (\pi) \cdot (u_P) + (\delta) \cdot (v_P)$
or \( \alpha = \alpha' + (\pi) \cdot (u_P \delta^i) \) for some units, \( u_P, v_P \in R \) and \( \alpha' \) unramified on \( R \) ([S1], cf. 1.1). By the choice of \( f_1 \), we have \( f_1 = \pi \delta w_P \) for some \( w_P \in A \) which is a unit at \( P \). Let \( u \in A \) be such that \( u(P) = w_P(P)^{-1}u_P(P) \) for all \( P \in E \cap F \). Let \( f = f_1u \in A \). Then, we have \( (f) = C + E + F \), where \( F \) is a divisor on \( X \) which avoids \( C, E \) and all the points of \( C \cap E \). Further, for each \( P \in C_i \cap E_j \), we have \( f = \pi_i \delta_j w_{ij} \) for some \( w_{ij} \in A \) such that \( w_{ij}(P) = u_P(P) \).

By a similar argument, choose \( g \in K \) satisfying

1. \( (g) = C + G \), where \( G \) is a divisor on \( X \) which avoids \( C, E, F \) and also avoids the points of \( C \cap E, C \cap F, E \cap F \);
2. if \( P \in E \cap F \) and \( \alpha = \alpha' + (\delta) \cdot (v) \) for some unit \( v \in R_P \) and \( \alpha' \) is unramified at \( P \), then \( g(P) = v(P) \).

Since \( C \cap E \cap F = \emptyset \), such a \( g \) exists.

We claim that \( \beta = \alpha + (f) \cdot (g) \) is a symbol.

Let \( \phi : X' \to X \) be a blow up of \( X \) such that \( X' \) is a regular proper model of \( K \) and \( \text{ram}_{X'_{\phi}}(\beta) = C' + E' \), where \( C' \) and \( E' \) are regular curves with normal crossings.

To show that \( \beta \) is a symbol, it is enough to show that \( \beta \) has no hot points ([S3], cf. 1.2). Let \( Q \in C' \cap E' \). Let \( P = \phi(Q) \). Then \( P \) is a closed point of \( X \), \( R = \mathcal{O}_{X',P} \subset H_{X',Q} = R' \) and the maximal \( m_P \) of \( R \) is contained in the maximal ideal \( m_Q \) of \( R' \). Let \( m_Q = (\pi', \delta') \), with \( \pi' \) and \( \delta' \) be local equations of \( C' \) and \( E' \) at \( Q \) respectively.

Suppose that \( P \notin C \cup E \). Then \( \alpha \) is unramified at \( P \) and hence unramified at \( Q \).

By (2.1), \( Q \) is not a hot point of \( \beta \).

Assume that \( P \in C \cup E \).

Suppose that \( P \in C \cap E \). Let \( \pi \) and \( \delta \) be local equations of \( C \) and \( E \) at \( P \) respectively. Then \( m_P = (\pi, \delta) \). By the choice of \( f \) and \( g \), we have \( f = \pi \delta w_1 \) and \( g = \pi w_2 \) for some units \( w_1, w_2 \in R \). In particular, \( \beta \) is ramified on \( R \) only at \( \pi \) and \( \delta \). Suppose that \( \alpha = \alpha' + (\pi) \cdot (u) + (\delta) \cdot (v) \) for some units \( u, v \in R \) and \( \alpha' \) unramified on \( R \). We have

\[
\begin{align*}
\beta &= \alpha + (f) \cdot (g) \\
&= \alpha' + (\pi) \cdot (u) + (\delta) \cdot (v) + (\pi \delta w_1) \cdot (\pi w_2) \\
&= \alpha' + (\pi) \cdot (u) + (\delta w_1) \cdot (\pi + (w_1^{-1}) \cdot (v)) + (\pi w_2) + (\delta w_1) \cdot (\pi w_2) \\
&= \alpha' + (w_1^{-1}) \cdot (v) + (\pi) \cdot (u \pi w_2) + (\delta w_1) \cdot (\pi w_2 v) \\
&= \alpha' + (w_1^{-1}) \cdot (v) + (\pi) \cdot (uw_2) + (\delta w_1) \cdot (\pi w_2 v) \\
&= \alpha' + (w_1^{-1}) \cdot (v) + (\pi w_2 v) \cdot (uw_2) + (w_1^{-1} v^{-1}) \cdot (uw_2) + (\delta w_1) \cdot (\pi w_2 v) \\
&= \alpha' + (w_1^{-1}) \cdot (v) + (w_1^{-1} v^{-1}) \cdot (uw_2) + (\pi w_2 v) \cdot (uw_2 \delta^{-1} w_1^{-1}).
\end{align*}
\]

Since \( \alpha' + (w_1^{-1}) \cdot (v) + (w_1^{-1} v^{-1}) \cdot (uw_2) \) is unramified on \( R \), by (2.1), \( Q \) is not a hot point of \( \beta \).
Suppose that $\alpha = \alpha' + (\pi) \cdot (u\delta^i)$ for some units, $u, v \in R$ and $\alpha'$ unramified on $R$. Then we have

$$\beta = \alpha + (f) \cdot (g)$$

$$= \alpha' + (\pi) \cdot (u\delta^i) + (\pi w_1) \cdot (\pi w_2)$$

$$= \alpha' + (\pi) \cdot (u\delta^i) + (\delta w_1 w_2^{-1}) \cdot (\pi w_2)$$

$$= \alpha' + (\pi) \cdot (u\delta^i(\delta w_1 w_2^{-1})^{-1}) + (\delta w_1 w_2^{-1}) \cdot (w_2)$$

$$= \alpha' + (\pi) \cdot (\delta^{-1} u w_1^{-1} w_2) + (\delta w_1 w_2^{-1}) \cdot (w_2).$$

If $i = 1$, then $\beta = \alpha' + (\pi) \cdot (u w_1^{-1} w_2) + (\delta w_1 w_2^{-1}) \cdot (w_2)$. Since, by the choice of $f, u(P) = w_1 (P)$, by (2.3), $Q$ is not a hot point of $\beta$. Assume that $i > 1$. Then $1 \leq i - 1 < l - 1$. Let $i'$ be the inverse of $1 - i$ modulo $l$. We have

$$\beta = \alpha' + (\pi) \cdot (\delta^{-1} u w_1^{-1} w_2) + (\delta w_1 w_2^{-1}) \cdot (w_2)$$

$$= \alpha' + (\delta^{-1} w_1 w_2^{-1}) \cdot (\pi) + (\delta w_1 w_2^{-1}) \cdot (w_2)$$

$$= \alpha' + ((\delta(u^{-1} w_1 w_2^{-1})^{-i}) \cdot (w_2) + (\delta(u^{-1} w_1 w_2^{-1})^{-i}) \cdot (w_2)$$

$$+ ((u^{-1} w_1 w_2^{-1})^{-i}) \cdot (w_2) + (w_1 w_2^{-1}) \cdot (w_2)$$

$$= \alpha' + ((u^{-1} w_1 w_2^{-1})^{-i}) \cdot (w_2) + (w_1 w_2^{-1}) \cdot (w_2)$$

$$+ ((\delta(u^{-1} w_1 w_2^{-1})^{-i}) \cdot (w_2) + (\delta w_1 w_2^{-1}) \cdot (w_2).$$

Since $\alpha' + ((u^{-1} w_1 w_2^{-1})^{-i}) \cdot (w_2)$ is unramified on $R$, by (2.1), $Q$ is not a hot point of $\beta$.

Suppose that $P \in C \setminus E$. We have $\alpha = \alpha' + (\pi) \cdot (u)$ for some unit $u$ in $R$ and $\alpha'$ unramified on $R$. We also have $f = \pi f_1$ for some $f_1 \in R$ which is not divisible by $\pi$. We have

$$\beta = \alpha + (f) \cdot (g)$$

$$= \alpha' + (\pi) \cdot (u) + (\pi f_1) \cdot (g)$$

$$= \alpha' + (f_1^{-1}) \cdot (u) + (\pi f_1) \cdot (u) + (\pi f_1) \cdot (g)$$

$$= \alpha' + (f_1^{-1}) \cdot (u) + (\pi f_1) \cdot (g u).$$

If $f_1$ is a unit in $R$, then $\alpha' + (f_1^{-1}) \cdot (u)$ is unramified on $R$, by (2.1), $Q$ is not a hot point of $\beta$. Assume that $f_1$ is not a unit in $R$. Then $P \in C \cap F$ and $g = \pi g_1$ for some unit $g_1 \in R$. We have

$$\beta = \alpha + (f) \cdot (g)$$

$$= \alpha' + (\pi) \cdot (u) + (\pi f_1) \cdot (\pi g_1)$$

$$= \alpha' + (\pi g_1) \cdot (u) + (g_1^{-1}) \cdot (u) + (\pi f_1) \cdot (\pi g_1)$$

$$= \alpha' + (g_1^{-1}) \cdot (u) + (\pi g_1) \cdot (u(\pi f_1)^{-1}).$$
Since $\alpha' + (g_1^{-1}) \cdot (u)$ is unramified on $R$, by (2.1), $Q$ is not a hot point of $\beta$.

Suppose that $P \in E \setminus C$. Then $\alpha = \alpha' + (\delta) \cdot (v)$ for some unit $v \in R$ and $f = \delta f_1$ for some $f_1 \in R$ which is not divisible by $\delta$. Suppose that $f_1$ is a unit in $R$. Then, as above, $Q$ is not a hot point of $\beta$. Assume that $f_1$ is not a unit in $R$. Then $P \in E \cap F$ and $g$ is a unit in $R$. We have

\[
\beta = \alpha + (f) \cdot (g) = \alpha' + (\delta) \cdot (v) + (\delta f_1) \cdot (g) = \alpha' + (\delta) \cdot (vg) + (f_1) \cdot (g).
\]

Since $\alpha'$ is unramified on $R$ and by the choice of $g$, $g(P) = v(P)$, by (2.2), $Q$ is not a hot point of $\beta$.

By ([S3], cf. 1.2), $\beta$ is symbol. Thus $\alpha = (f) \cdot (g) - \beta$ is a sum of at most two symbols.

\[\square\]

Acknowledgments. We would like to thank for support from UGC (India) under the SAP program.

References


Received April 1, 2008

Venapally Suresh, Department of Mathematics and Statistics, University of Hyderabad, Gachibowli, Hyderabad - 500046, India

E-mail: vssm@uohyd.ernet.in