ACTA ARITHMETICA
158.2 (2013)

An equicharacteristic analogue of Hesselholt's conjecture on cohomology of Witt vectors

by

Amit Hogadi and Supriya Pisolkar (Mumbai)

1. Introduction. Let K be a complete discrete valued field with residue field of characteristic $p > 0$, and L/K be a finite Galois extension with Galois group G. Suppose that k_L/k_K is separable. When K is of characteristic zero, Hesselholt conjectured in [4] that the proabelian group $\{H^1(G, W_n(\mathcal{O}_L))\}_{n\in\mathbb{N}}$ vanishes, where $W_n(\mathcal{O}_L)$ is the ring of Witt vectors of length n with coefficients in $\mathcal{O}_L$ (with respect to to the prime p). As explained in [4], this can be viewed as an analogue of Hilbert's Theorem 90 for the Witt ring $W(\mathcal{O}_L)$. This conjecture was proved in some cases in [4] and in general in [5].

In this paper we show that a similar vanishing holds when K is of characteristic p. The main result of this paper is as follows.

Theorem 1.1. *Let L/K be a finite Galois extension of complete discrete valued equicharacteristic fields with Galois group G. Assume that the induced residue field extension is separable. Then the proabelian group $\{H^1(G, W_n(\mathcal{O}_L))\}$ is zero.*

In order to prove this result one easily reduces it to the case where L/K is a totally ramified Galois extension of degree p (see [5, Lemma 3.1]). We make the argument in [5] work in the equicharacteristic case using an explicit description of the Galois cohomology of $\mathcal{O}_L$ when L/K is an Artin–Schreier extension (see Proposition 2.4).

We recall that a *proabelian group* indexed by $\mathbb{N}$ is an inverse system of abelian groups $\{A_n\}_{n\in\mathbb{N}}$ whose vanishing means that for every $n \in \mathbb{N}$, there exists an integer $m > n$ such that the map $A_m \to A_n$ is zero (see [6, Section 1]). This clearly implies the vanishing of $\varprojlim_n H^1(G, W_n(\mathcal{O}_L))$. It also implies the vanishing of $H^1(G, W(\mathcal{O}_L))$ (with $W(\mathcal{O}_L)$ being considered as a discrete G-module) by [5, Corollary 1.2].

2010 *Mathematics Subject Classification*: Primary 11S25.
Key words and phrases: Galois cohomology, Witt vectors.

DOI: 10.4064/aa158-2-4

Remark 1.2. One may also consider an analogue of Theorem 1.1 when K is of equicharacteristic zero. However, in this case, all extensions L/K are tamely ramified and the vanishing

$$H^1(\mathrm{Gal}(L/K), W_n(\mathcal{O}_L)) = 0 \quad \forall n \geq 0$$

can be easily deduced from the fact that $\mathcal{O}_L$ is a projective $\mathcal{O}_K[G]$-module (see [2, I, Theorem (3)]).

2. Cohomology of integers in Artin–Schreier extensions. Let K be a complete discrete valued field of characteristic p as before. Let $\mathcal{O}_K$ and k denote the discrete valuation ring and residue field of K respectively. Let L/K be a Galois extension of degree p. Recall that the *ramification break* (or *lower ramification jump*) of this extension, to be denoted by $s = s(L/K)$, is the smallest non-negative integer such that the induced action of $\mathrm{Gal}(L/K)$ on $\mathcal{O}_L/m_L^{s+1}$ is faithful, where m_L is the maximal ideal of $\mathcal{O}_L$ ([1, II, 4.5]). Thus unramified extensions are precisely the extensions with ramification break zero. We recall the following well known result.

Proposition 2.1 (see [3] or [7, Proposition 2.1]). *Let L/K be a Galois extension of degree p of complete discrete valued fields of characteristic p. There exists an element $f \in K$ such that L is obtained from K by adjoining a root of the polynomial*

$$X^p - X - f = 0.$$

Further one can choose f such that $v_K(f)$ is coprime to p. In this case

$$v_K(f) = -s$$

where s is the ramification break of $\mathrm{Gal}(L/K)$.

We now fix an $f \in K$ given by the above proposition. Clearly, if $v_K(f) > 0$ then by Hensel's lemma $X^p - X - f$ already has a root in K. If $v_K(f) = 0$ then the extension given by adjoining the root of this polynomial is an unramified extension.

Proposition 2.2. *Let L/K and $f \in K$ be as above. Assume L/K is totally ramified. Let λ be a root of $X^p - X - f$ in L. Let s be the ramification break of* $\mathrm{Gal}(L/K)$. *Then the discrete valuation ring $\mathcal{O}_L$ is the subset of L given by*

$$\mathcal{O}_L = \Big\{ \sum_{i=0}^{p-1} a_i \lambda^i \;\Big|\; a_i \in \mathcal{O}_K \text{ with } v_K(a_i) \geq is/p \Big\}.$$

Proof. Clearly the set $\{1, \lambda, \ldots, \lambda^{p-1}\}$ is a K-basis of L. Thus each $x \in L$ can be uniquely written in the form

$$x = \sum_{i=0}^{p-1} a_i \lambda^i.$$

Note that $v_L(\lambda) = v_K(f) = -s$ is coprime to p by the choice of f. Since L/K is ramified, s is non-zero. Moreover $v_L(a_i) = pv_K(a_i)$ is divisible by p. We thus conclude that for each $0 \le i \le p-1$, the values of $v_L(a_i\lambda^i)$ are all distinct modulo p, and hence distinct.

Thus

$$v_L\Big(\sum_{i=0}^{p-1} a_i\lambda^i\Big) \ge 0 \quad \text{if and only if} \quad v_L(a_i\lambda^i) \ge 0 \text{ for all } 0 \le i < p.$$

But $v_L(a_i\lambda^i) = pv_K(a_i) - is$. This proves the claim. ∎

LEMMA 2.3. *Let p be a prime number as before. Let*

$$S_k = \sum_{n=0}^{p-1} n^k.$$

Then

(1) $S_k \equiv 0 \bmod p$ *if* $0 \le k \le p-2$,
(2) $S_{p-1} \equiv -1 \bmod p$.

Proof. The first congruence follows from the recursive formula (see [8, (4)])

$$S_k = \frac{1}{k+1}\Big(p^{k+1} - p^k - \sum_{j=0}^{k-2} \binom{k}{j} S_{j+1}\Big)$$

and the fact that $k+1$ is invertible modulo p when $k \le p-2$. (2) follows from Fermat's little theorem. ∎

We now state an explicit description of $H^1(G, \mathcal{O}_L)$.

PROPOSITION 2.4. *With notation as in Proposition* 2.1, *let σ be a generator of* $\mathrm{Gal}(L/K)$. *Let $\mathcal{O}_L^{\mathrm{tr}=0}$ denote the set of all trace zero elements in $\mathcal{O}_L$, and*

$$(\sigma - 1)\mathcal{O}_L = \{\sigma(x) - x \mid x \in \mathcal{O}_L\}.$$

Then

(1) $\mathcal{O}_L^{\mathrm{tr}=0} = \Big\{\sum_{i=0}^{p-2} a_i\lambda^i \;\Big|\; v_K(a_i) \ge is/p\Big\}$,

(2) $(\sigma - 1)\mathcal{O}_L = \Big\{\sum_{i=0}^{p-2} a_i\lambda^i \;\Big|\; v_K(a_i) \ge (i+1)s/p\Big\}$.

Proof. Since the sets $\mathcal{O}_L^{\mathrm{tr}=0}$ and $(\sigma-1)\mathcal{O}_L$ are independent of the choice of σ, we may assume that $\sigma(\lambda) = \lambda + 1$.

(1) Let $x = \sum_{i=1}^{p-1} a_i\lambda^i$. Let S_k be as in Lemma 2.3. We have

$$\operatorname{tr}(x) = \sum_{j=0}^{p-1} \sigma^j(x) = \sum_{j=0}^{p-1}\sum_{i=0}^{p-1} a_i(\lambda+j)^i = \sum_{i=0}^{p-1} a_i\Big(\sum_{j=0}^{p-1}(\lambda+j)^i\Big).$$

By binomially expanding and collecting coefficients of λ^i, we get

$$\begin{aligned}\operatorname{tr}(x) &= \sum_{i=0}^{p-1} a_i\left(p\lambda^i + \sum_{j=1}^{i}\binom{i}{j}S_j\lambda^{i-j}\right)\\ &= -a_{p-1} \quad \text{(by Lemma 2.3).}\end{aligned}$$

This together with Proposition 2.2 proves (1).

(2) Suppose $x = \sum_{i=1}^{p-1} a_i\lambda^i \in (\sigma-1)\mathcal{O}_L$. Then

$$\sum_{i=1}^{p-1} a_i\lambda^i = (\sigma-1)\sum_{i=1}^{p-1} b_i\lambda^i,$$

where $v_K(b_i) \geq is/p$ by Proposition 2.2. This gives us the following system of p equations:

$$\begin{aligned}a_0 &= b_1 + \cdots + b_{p-1},\\ a_1 &= \tbinom{2}{1}b_2 + \tbinom{3}{2}b_3 + \cdots + \tbinom{p-1}{p-2}b_{p-1}, \quad \ldots,\\ a_i &= \tbinom{i+1}{i}b_{i+1} + \cdots + \tbinom{p-1}{p-(i+1)}b_{p-1}, \quad \ldots,\\ a_{p-2} &= (p-1)b_{p-1},\\ a_{p-1} &= 0.\end{aligned}$$

Since $v_K(b_{i+1}) \geq (i+1)s/p$, we get $v_K(a_i) \geq (i+1)s/p$. Thus

$$(\sigma-1)\mathcal{O}_L \subset \Big\{\sum_{i=0}^{p-2} a_i\lambda^i \;\Big|\; v_K(a_i) \geq (i+1)s/p\Big\}.$$

Conversely, assume

$$\sum_{i=1}^{p-1} a_i\lambda^i \in \Big\{\sum_{i=0}^{p-2} a_i\lambda^i \;\Big|\; v_K(a_i) \geq (i+1)s/p\Big\}.$$

Since $H^1(G,L) = 0$, there exists $\sum b_i\lambda^i \in L$ such that

$$\sum_{i=1}^{p-1} a_i\lambda^i = (\sigma-1)\sum_{i=1}^{p-1} b_i\lambda^i.$$

The b_i's satisfy the above system of p equations. Using $v_K(a_i) \geq (i+1)s/p$, it is straightforward to prove by induction that $v_K(b_i) \geq is/p$. Hence $\sum_{i=1}^{p-1} b_i\lambda^i \in \mathcal{O}_L$. ■

The following corollary is the equicharacteristic analogue of [4, Lemma 2.4].

COROLLARY 2.5. *Let L/K be as in Proposition 2.1. Let $x \in \mathcal{O}_L^{\mathrm{tr}=0}$ define a non-zero class in $H^1(G, \mathcal{O}_L)$. Then $v_L(x) \le s-1$.*

Proof. We will show that for any $x \in \mathcal{O}_L^{\mathrm{tr}=0}$, if $v_L(x) \ge s$, then the class of x in $H^1(G, \mathcal{O}_L)$ is zero. By (2.4), we may write

$$x = \sum_{i=1}^{p-2} a_i \lambda^i \quad \text{with} \quad v_L(a_i) \ge is.$$

Since for all i, $v_L(a_i\lambda^i)$ are distinct (see proof of Proposition 2.2), we have

$$v_L(x) = \inf\{v_L(a_i\lambda^i)\}.$$

Thus $v_L(x) \ge s$ implies

$$v_L(a_i\lambda^i) = v_L(a_i) - is \ge s \quad \forall i.$$

This shows that $v_L(a_i) \ge (i+1)s$, which by Proposition 2.4 implies $x \in (\sigma-1)\mathcal{O}_L$, and hence defines a trivial class in $H^1(G, \mathcal{O}_L)$. ∎

3. Proof of the main theorem. Following [5, Lemma 3.1], the proof of the main theorem reduces to the case when L/K is a totally ramified Galois extension of degree p. So throughout this section we fix an extension L/K of this type. We also fix a generator $\sigma \in \mathrm{Gal}(L/K)$. We first define a polynomial $G \in \mathbb{Z}[X_1, \ldots, X_p]$ in p variables by

$$G(X_1, \ldots, X_p) = \frac{1}{p}\Big(\Big(\sum_{i=1}^{p} X_i\Big)^p - \sum_{i=1}^{p} X_i^p\Big).$$

Note that despite the occurrence of $1/p$, G is a polynomial with integral coefficients.

Now for $x \in L$ define

$$F(x) = G(x, \sigma(x), \ldots, \sigma^i(x), \ldots, \sigma^{p-1}(x)).$$

The expression $F(x)$ is formally equal to $(\mathrm{tr}(x)^p - \mathrm{tr}(x^p))/p$ and makes sense in characteristic p since G has integral coefficients. Moreover, since for any $x \in L$, $F(x)$ is invariant under the action of $\mathrm{Gal}(L/K)$, we have $F(x) \in K$. We now observe that [4, Lemma 2.2] holds in characteristic p in the following form:

LEMMA 3.1 ([4, Lemma 2.2]). *For all $x \in \mathcal{O}_L$, $v_K(F(x)) = v_L(x)$.*

Proof of Theorem 1.1. The proof follows [5, proof of 1.4] verbatim, with Corollary 2.5 and Lemma 3.1 replacing [5, Lemma 3.2] and [5, Lemma 3.4] respectively. We briefly recall the idea of the proof for the convenience of the reader. By [4, Lemma 1.1], it is enough to show that for large n, the map

$$H^1(G, W_n(\mathcal{O}_L)) \to H^1(G, \mathcal{O}_L)$$

is zero. By Corollary 2.5, it is enough to show that for large n,

$$(x_0, \ldots, x_{n-1}) \in W_n(\mathcal{O}_L)^{\mathrm{tr}=0} \;\Rightarrow\; v_L(x_0) \geq s.$$

The condition $(x_0, \ldots, x_{n-1}) \in W_n(\mathcal{O}_L)^{\mathrm{tr}=0}$ can be rewritten as

$$\sum_{i=0}^{p-1} (\sigma^i(x_0), \ldots, \sigma^i(x_{n-1})) = 0.$$

Using the formula for addition of Witt vectors, one analyses the above equation and obtains (see [5, Lemma 3.5])

$$\mathrm{tr}(x_\ell) = F(x_{\ell-1}) - C\,\mathrm{tr}(x_{\ell-1})^p + h_{\ell-2}, \quad 1 \leq \ell \leq n-1, \tag{1}$$

where C is a fixed integer and $h_{\ell-2}$ is a polynomial in $x_0, \ldots, x_{\ell-2}$ and its conjugates such that each monomial appearing in $h_{\ell-2}$ is of degree $\geq p^2$. Using the above equation, Lemma 3.1 and [4, Lemma 2.1] one proves the theorem in the following three steps, for the details of which we refer the reader to [5, proof of 1.4].

Step 1. We claim that for $0 \leq \ell \leq n-2$,

$$v_L(x_\ell) \geq \frac{s(p-1)}{p}.$$

One proves this claim by induction on ℓ. Since $h_{-1} = \mathrm{tr}(x_0) = 0$, equation (1) gives

$$-\mathrm{tr}(x_1) = F(x_0).$$

This, together with [4, Lemma 2.1], proves the claim for $\ell = 0$. The rest of the induction argument is straightforward. This claim, together with equation (1), is then used to show that $v_K(h_\ell) \geq s(p-1)$ for all ℓ.

Step 2. We show that for $2 \leq i \leq n-1$,

$$v_L(x_{n-i}) \geq \frac{s(p-1)}{p}\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{i-2}}\right).$$

This is proved by induction on i, using (1) and the estimates

$$v_L(x_\ell) \geq s(p-1)/p, \qquad v_L(h_\ell) \geq s(p-1)$$

obtained in Step 1.

Step 3. Since v_L is a discrete valuation, for an integer M such that

$$\frac{s(p-1)}{p}\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{M-2}}\right) > s-1,$$

we have $v_L(x_0) \geq s$. ∎

Acknowledgements. We thank the referee for several useful comments and suggestions.

References

[1] I. B. Fesenko and S. V. Vostokov, *Local Fields and their Extensions*, 2nd ed., Transl. Math. Monogr. 121, Amer. Math. Soc., 2002.
[2] A. Fröhlich, *Galois Module Structure of Algebraic Integers*, Springer, Berlin, 1983.
[3] H. Hasse, *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. 172 (1934), 37–54.
[4] L. Hesselholt, *Galois cohomology of Witt vectors of algebraic integers*, Math. Proc. Cambridge Philos. Soc. 137 (2004), 551–557.
[5] A. Hogadi and S. Pisolkar, *On the cohomology of Witt vectors of p-adic integers and a conjecture of Hesselholt*, J. Number Theory 131 (2011), 1797–1807.
[6] U. Jannsen, *Continuous étale cohomology*, Math. Ann. 280 (1988), 207–245.
[7] L. Thomas, *Ramification groups in Artin–Schreier–Witt extensions*, J. Théor. Nombres Bordeaux 17 (2005), 689–720.
[8] B. Turner, *Sums of powers of integers via the binomial theorem*, Math. Mag. 53 (1980), 92–96.

Amit Hogadi, Supriya Pisolkar
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Colaba, Mumbai 400005, India
E-mail: amit@math.tifr.res.in
supriya@math.tifr.res.in

Received on 23.2.2012
and in revised form on 15.10.2012 (6984)