# Galois cohomology of Witt vectors of algebraic integers

Lars Hesselholt*

## Introduction

Let $K$ be a complete discrete valuation field, and let $L/K$ be a finite Galois extension with Galois group $G = G_{L/K}$. By the normal basis theorem, $L$ is always a projective $K[G]$-module, and by a classical theorem of Noether, the ring of integers $\mathcal{O}_L$ is a projective $\mathcal{O}_K[G]$-module, provided that $L/K$ is tamely ramified. But for wildly ramified extensions, the structure of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module is extremely complicated and quite far from understood. In this paper, we show that the ring of Witt vectors $W.(\mathcal{O}_L)$ is a more well-behaved object. We assume that $K$ has characteristic 0 and that the residue field $k$ has characteristic $p > 2$, but we do not assume that $k$ is perfect. Then for every finite Galois extension $L/K$ we show:

THEOREM. *The pro-abelian group $H^1(G_{L/K}, W.(\mathcal{O}_L))$ is zero.*

In general, the higher groups $H^i(G_{L/K}, W.(\mathcal{O}_L))$, $i > 1$, are non-zero. Hence, the theorem may be viewed as an additive version of Hilbert's theorem 90.

The theorem is equivalent to the statement that the canonical inclusion

$$W.(\mathcal{O}_K)/p^v W.(\mathcal{O}_K) \xrightarrow{\sim} \big(W.(\mathcal{O}_L)/p^v W.(\mathcal{O}_L)\big)^G$$

is an isomorphism of pro-abelian groups, for all $v \geq 1$. Indeed, the cokernel of this map is isomorphic to the subgroup of $H^1(G, W.(\mathcal{O}_L))$ of elements killed by $p^v$. But by [**6**, theorem 3], this subgroup is equal to the whole group, if $v$ is greater than or equal to the $p$-adic valuation of $[L : K]$.

It was this equivalent statement of the theorem that was the original motivation for proving it. To explain this, let $K_v = K(\mu_{p^v})$. It follows from [**2**, theorem 5.12] and [**5**, théorème 1(1)] that for all $v \geq 1$, the inclusion of Milnor $K$-groups

$$K_q^M(K)/p^v \xrightarrow{\sim} (K_q^M(K_v)/p^v)^G$$

is an isomorphism. By analogy, we conjecture that for all $v \geq 1$, the canonical inclusion of de Rham-Witt groups

$$W.\,\Omega^q_{(\mathcal{O}_K, M_K)}/p^v \to \big(W.\,\Omega^q_{(\mathcal{O}_{K_v}, M_{K_v})}/p^v\big)^G$$

is an isomorphism of pro-abelian groups. (The definition of the de Rham-Witt groups is given in [**4**, §3].) The theorem of this paper establishes the case $q = 0$.

---

* Supported in part by a grant from the National Science Foundation.

We shall always normalize the valuation $v_L$ on $L$ such that the valuation of a uniformizer $\pi_L \in \mathcal{O}_L$ is equal to 1.

This paper was written while the author was visiting the Issac Newton Institute for Mathematical Sciences in Cambridge, England. It is a pleasure to thank the institute for its hospitality and support and for the excellent working conditions it provided. Finally, I wish to thank Spencer Bloch and Vic Snaith for much help and encouragement.

## 1. Proof of the theorem

**1.1.** Let $L/K$ be a finite Galois extension with Galois group $G$. Then for all $m, n \geq 1$, we have a short-exact sequence of $G$-modules

$$0 \to W_m(\mathcal{O}_L) \xrightarrow{V^n} W_{m+n}(\mathcal{O}_L) \xrightarrow{R^m} W_n(\mathcal{O}_L) \to 0.$$

The induced sequence of $G$-fixed sets again is exact. For as a set, $W_s(\mathcal{O}_L)$ is equal to the $s$-fold product of copies of $\mathcal{O}_L$, and $\mathcal{O}_L^G = \mathcal{O}_K$. Hence, we have an exact sequence of cohomology groups

$$\begin{aligned} 0 \to H^1(G, W_m(\mathcal{O}_L)) &\xrightarrow{V^n_*} H^1(G, W_{m+n}(\mathcal{O}_L)) \xrightarrow{R^m_*} H^1(G, W_n(\mathcal{O}_L)) \\ \xrightarrow{\partial} H^2(G, W_m(\mathcal{O}_L)) &\xrightarrow{V^n_*} H^2(G, W_{m+n}(\mathcal{O}_L)) \longrightarrow \dots . \end{aligned}$$

Lemma 1.1.1. *Let $N \geq 1$ be an integer. Then the following are equivalent.*

(i) *For all $m \geq N$ and all $n \geq 1$, the map induced by the restriction*

$$R^m_* \colon H^1(G, W_{m+n}(\mathcal{O}_L)) \to H^1(G, W_n(\mathcal{O}_L))$$

*is equal to zero.*

(ii) *For all $m \geq N$, the map induced by the restriction*

$$R^m_* \colon H^1(G, W_{m+1}(\mathcal{O}_L)) \to H^1(G, \mathcal{O}_L)$$

*is equal to zero.*

(iii) *For all $m \geq N$, the boundary map*

$$\partial = \partial_{m,1} \colon H^1(G, \mathcal{O}_L) \to H^2(G, W_m(\mathcal{O}_L))$$

*is injective.*

Proof. The statements (ii) and (iii) are clearly equivalent, and statement (ii) is a special case of statement (i). Suppose that statement (ii) holds. Then for all $m \geq N$, the map

$$V_* \colon H^1(G, W_m(\mathcal{O}_L)) \xrightarrow{\sim} H^1(G, W_{m+1}(\mathcal{O}_L))$$

is an isomorphism. It follows for all $m \geq N$ and all $n \geq 1$, the iterated map

$$V^n_* \colon H^1(G, W_m(\mathcal{O}_L)) \xrightarrow{\sim} H^1(G, W_{m+n}(\mathcal{O}_L))$$

is an isomorphism, and this, in turn, implies statement (i) of the lemma. □

Suppose that $L/K$ is a cyclic extension, and let $\sigma$ be a generator of the Galois group. We recall that for every $G$-module $M$, the cohomology group $H^i(G, M)$ is canonically isomorphic to the $i$th cohomology group of the complex

$$M \xrightarrow{1-\sigma} M \xrightarrow{\mathrm{tr}} M \xrightarrow{1-\sigma} M \xrightarrow{\mathrm{tr}} M \to \dots,$$

where for $a \in M$, $\operatorname{tr}(a)$ is the sum of the Galois conjugates of $a$. In the case at hand, we have canonical isomorphisms

$$\begin{aligned} H^1(G, \mathcal{O}_L) &\approx (\mathcal{O}_L \cap (\sigma - 1)L)/(\sigma - 1)\mathcal{O}_L, \\ H^2(G, W_m(\mathcal{O}_L)) &\approx W_m(\mathcal{O}_K)/\operatorname{tr}(W_m(\mathcal{O}_L)). \end{aligned} \tag{1.1.2}$$

In the following we shall often identify the cohomology groups on the left with the corresponding groups on the right. We also recall the ghost map

$$w \colon W_m(A) \to A^m$$

is the ring homomorphism, which to a Witt vector $(a_0, \dots, a_{m-1})$ associates the $m$-tuple $(w_0, \dots, w_{m-1})$, where for $0 \le s < m$,

$$w_s = a_0^{p^s} + p a_1^{p^{s-1}} + \dots + p^{s-1} a_{s-1}^p + p^s a_s.$$

It is injective, if $p$ is a non-zero-divisor in $A$. This is the case for $A = \mathcal{O}_K$, as we assume that $K$ has characteristic zero. Hence, lemma 1.1.1 (iii) is equivalent to the statement that for $m \ge N$, the composite map

$$H^1(G, \mathcal{O}_L) \xrightarrow{\partial} H^2(G, W_m(\mathcal{O}_L)) \xrightarrow{w} \mathcal{O}_K^N / w(\operatorname{tr}(W_m(\mathcal{O}_L))) \tag{1.1.3}$$

is injective. We remark that this is a map of $W_{m+1}(\mathcal{O}_K)$-modules. It is not a map of $\mathcal{O}_K$-modules unless $\mathcal{O}_K$ is absolutely unramified with perfect residue field.

LEMMA 1.1.4. *The composite map (1.1.3) is given by*

$$\operatorname{class}(x) \mapsto \operatorname{class}((\frac{\operatorname{tr}(x^p)}{p}, \dots, \frac{\operatorname{tr}(x^{p^m})}{p})).$$

PROOF. Since the ghost map is natural and additive, we have

$$w(\operatorname{tr}(a)) = \operatorname{tr}(w(a)),$$

for all $a \in W_m(\mathcal{O}_L)$. To prove the lemma, one applies this to the Teichmüller representative $[x] = (x, 0, \dots, 0) \in W_{m+1}(\mathcal{O}_L)$ of $x \in \mathcal{O}_L$ with $\operatorname{tr}(x) = 0$. □

**1.2.** Let $L/K$ be a totally ramified cyclic extension of order $p$, and let $\sigma$ be a generator of $G = G_{L/K}$. Then the filtration by ramification groups takes the form

$$G = G_1 = \dots = G_t \supset G_{t+1} = \{0\},$$

where $t$ is the integer given by $v_p((\sigma - 1)\pi_L) = t + 1$.

LEMMA 1.2.1. *If $v_L(a) = ps - (p-1)t$, then $v_K(\operatorname{tr}(a)) = s$.*

PROOF. We must show that the trace induces an isomorphism

$$\mathfrak{m}_L^{ps-(p-1)t} / \mathfrak{m}_L^{ps-(p-1)t+1} \xrightarrow{\sim} \mathfrak{m}_K^s / \mathfrak{m}_K^{s+1}.$$

But this follows from the formula [**7**, chap. V, §3]

$$\operatorname{tr}(\mathfrak{m}_L^n) = \mathfrak{m}_K^r,$$

where $r = [(d+n)/p]$ and $d = (t+1)(p-1)$. □

We wish to evaluate the valuation of the trace of $p$th powers. The lemma shows that this is possible, if $p$ divides $t$. We now assume this to be the case.

COROLLARY 1.2.2. *Suppose that $p$ divides $t$. Then for all $s \ge 1$,*

$$v_K(\operatorname{tr}(a^{p^s})) = e_K + p^{s-1} v_L(a).$$

Proof. We write $t = pt'$. Then $v_L(a) = ps'$ implies $v_K(\mathrm{tr}(a)) = s' + (p-1)t'$, and hence, $v_K(\mathrm{tr}(a^{p^s})) = p^{s-1}v_L(a) + (p-1)t'$, for all $s \geq 1$. If $a = 1$, we get $v_K(\mathrm{tr}(1)) = (p-1)t'$. But $\mathrm{tr}(1) = p$ and $v_K(p) = e_K$. □

Lemma 1.2.3. *Suppose that $p$ divides $t$. Then every non-zero class in $H^1(G, \mathcal{O}_L)$ is represented by an element $x \in \mathcal{O}_L$ such that $1 \leq v_L(x) < pe_K/(p-1)$ and such that $p$ does not divide $v_L(x)$.*

Proof. We recall the $\mathcal{O}_K$-basis of $\mathcal{O}_L^{\mathrm{tr}=0} = \mathcal{O}_L \cap (\sigma - 1)L$ exhibited in the proof of [**6**, theorem 2]. Let $\sigma$ be a generator of $G$. Then for $\mu \geq 1$, we let

$$x_\mu = \prod_{0 \leq i < \mu} \sigma^i(\pi_L),$$

where $\pi_L \in \mathcal{O}_L$ is a uniformizer. Since $v_L(x_\mu) = \mu$, the elements $x_\mu$, $1 \leq \mu \leq p-1$, and 1 form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. We let $y_\mu = (\sigma - 1)(x_\mu)$ and $y'_\mu = y_\mu/\pi_K^{t'}$. Then $v_L(y_\mu) = \mu + t$ and $v_L(y'_\mu) = \mu$. It follows that the elements $y_\mu$, $1 \leq \mu \leq p-1$, form an $\mathcal{O}_K$-basis of $(\sigma - 1)\mathcal{O}_L$, and that the elements $y'_\mu$, $1 \leq \mu \leq p-1$, form an $\mathcal{O}_K$-basis of $\mathcal{O}_L \cap (\sigma - 1)L$. Hence, as an $\mathcal{O}_K$-module,

$$H^1(G, \mathcal{O}_L) \approx \bigoplus_{\mu=1}^{p-1} \mathcal{O}_K/\mathfrak{m}_K^{t'} \cdot y'_\mu.$$

Let $k$ be the residue field of $K$, and let $W$ be a complete discrete valuation ring such that $W/pW$ is isomorphic to $k$. Such a ring $W$ always exists [**1**, proposition 1.1.7]. In addition, there exists a ring homomorphism $f \colon W \to \mathcal{O}_K$ such that the induced map of residue fields is the identity. It follows that, if $\pi_K \in \mathcal{O}_K$ is a uniformizer, then $f$ induces an isomorphism $W[\pi_K]/(\phi_K(\pi_K)) \xrightarrow{\sim} \mathcal{O}_K$, where $\phi_K(X) \in W[X]$ is an Eisenstein polynomial of degree $e_K$. Hence, as a $W$-module, $H^1(G, \mathcal{O}_L)$ is a $k$-vector space with a basis given by the classes of $\pi_K^i y'_\mu$, where $0 \leq i < t'$ and $1 \leq \mu \leq p-1$. The valuation $v_L(\pi_K^i y'_\mu) = pi + \mu$ is not divisible by $p$ and satisfies

$$1 \leq pi + \mu \leq p(t'-1) + p - 1 = pe_K/(p-1) - 1.$$

Let $x \in \mathcal{O}_L^{\mathrm{tr}=0}$ be a general element and write $x$ as a linear combination

$$x = \sum_{i=0}^{t'-1} \sum_{\mu=1}^{p-1} \alpha_{i,\mu} \pi_K^i y'_\mu,$$

where $\alpha_{i,\mu} \in W$. We associate to $x$ the element

$$x' = \sum_{i=0}^{t'-1} \sum_{\mu=1}^{p-1} \alpha'_{i,\mu} \pi_K^i y'_\mu,$$

where $\alpha'_{i,\mu}$ is equal to $\alpha_{i,\mu}$, if $p$ does not divide $\alpha_{i,\mu}$, and zero, otherwise. Then $x$ and $x'$ represents the same class in $H^1(G, \mathcal{O}_L)$. Moreover, this class is non-zero if and only if $x'$ is non-zero. If this is the case, then $p$ does not divide $v_L(x')$ and $1 \leq v_L(x') < pe_K/(p-1)$. □

Proposition 1.2.4. *Suppose that $p$ divides $t$. Then the boundary map*

$$\partial = \partial_{N,1} \colon H^1(G, \mathcal{O}_L) \to H^2(G, W_N(\mathcal{O}_L))$$

*is injective, provided that $p^N > pe_K/(p-1) = t$.*

Proof. It suffices, by lemma 1.2.3, to show that for every $x \in \mathcal{O}_L^{\mathrm{tr}=0}$ such that $1 \leq v_L(x) < pe_K/(p-1)$, the image of the class represented by $x$ under the following map is non-zero.

$$H^1(G,\mathcal{O}_L) \xrightarrow{\partial_{N,1}} H^2(G,W_N(\mathcal{O}_L)) \xrightarrow{w} \mathcal{O}_K^N/w(\mathrm{tr}(W_N(\mathcal{O}_L))).$$

This, by lemma 1.1.4, is equivalently to showing that there cannot exist $a_0,\dots,a_{N-1} \in \mathcal{O}_L$ such that for all $0 \leq s < N$,

$$\mathrm{tr}(a_0^{p^s}) + p\,\mathrm{tr}(a_1^{p^{s-1}}) + \cdots + p^{s-1}\,\mathrm{tr}(a_{s-1}) = p^{-1}\,\mathrm{tr}(x^{p^{s+1}}). \tag{1.2.5}$$

To prove this, we assume the opposite and establish a system of inequalities on the valuations of the elements $a_0,\dots,a_{N-1}$. We then observe that these inequalities cannot be satisfied simultaneously, if $t' < p^N$. The basic observation needed to establish the inequalities is that for all $a \in \mathcal{O}_L$,

$$v_L(a) \leq p(v_K(\mathrm{tr}(a)) - e_K).$$

To see this, we write $a = \alpha_0 \cdot 1 + \alpha_1 y_1' + \cdots + \alpha_{p-1} y_{p-1}'$ with $\alpha_0,\dots,\alpha_{p-1} \in \mathcal{O}_K$. Then $\mathrm{tr}(a) = p\alpha_0$, and hence, $v_K(\mathrm{tr}(a)) = e_K + p^{-1}v_L(\alpha_0)$. But $v_L(a) \leq v_L(\alpha_0)$.

We first consider the equation (1.2.5) for $s = 0$. By comparing the valuation of the two sides, we see that the equation has no solutions, if $v_L(x) < e_K$. Hence, in this case, the image by $\partial_{1,1}$ of the class of $x$ is non-trivial. We may therefore assume that $v_L(x) \geq e_K$. In this case, a solution $a_0 \in \mathcal{O}_L$ will satisfy that

$$v_L(a_0) - e_K \leq pv_L(x) - (p+1)e_K.$$

We next show, inductively, that if the equations (1.2.5) with $s = 0,1,\dots,n$ have a solution, then

$$v_L(x) \geq (1 + p^{-1} + \cdots + p^{-n})e_K$$

and any such solution will satisfy

$$\begin{aligned} 0 \leq v_L(a_s) - e_K &\leq p^{s+1}v_L(x) - (p^{s+1} + \cdots + p + 1)e_K, \qquad 0 \leq s < n, \\ v_L(a_n) - e_K &\leq p^{n+1}v_L(x) - (p^{n+1} + \cdots + p + 1)e_K. \end{aligned}$$

We now assume that the equations (1.2.5) with $s = 0,1,\dots,n-1$ have a solution and consider the equation for $s = n$. The right hand side of the equation has valuation $p^n v_L(x)$ and, inductively, the valuation of the terms on the left hand side with $0 \leq i \leq n-2$ satisfy

$$p^{n-1-i}e_K \leq v_K(p^i\,\mathrm{tr}(a_i^{p^{n-i}})) - (i+1)e_K \leq p^{n-i}(p^i v_L(x) - (p^i + \cdots + 1)e_K),$$

and for the term $i = n-1$, we have

$$v_K(p^{n-1}\,\mathrm{tr}(a_{n-1}^p)) - ne_K \leq p(p^{n-1}v_L(x) - (p^{n-1} + \cdots + p + 1)e_K).$$

The last term $i = n$ on the left is our new variable. We claim that the valuation of the term $i = n-1$ on the left is strictly smaller than the valuation of the terms $i = 0,1,\dots,n-2$ and also strictly smaller than the valuation of the right hand side. The proof will be given below. Assuming the claim, we see that if a solution exists, we necessarily must have

$$v_K(p^n\,\mathrm{tr}(a_n)) = v_K(p^{n-1}\,\mathrm{tr}(a_{n-1}^p))$$

and this implies the inequality

$$0 \leq v_K(\mathrm{tr}(a_n)) - e_K = v_L(a_{n-1}) - e_K \leq p^n v_L(x) - (p^n + \cdots + p + 1)e_K.$$

There are no solutions, if the integer on the right is negative. And if this number is non-negative, a solution will satisfy

$$v_L(a_n) - e_K \le p^{n+1} v_L(x) - (p^{n+1} + \cdots + p + 1)e_K.$$

This completes the proof of the induction step. The proposition follows, since

$$p^{N-1} v_L(x) - (p^{N-1} + \cdots + p + 1)e_K < 0.$$

Indeed, we have $v_L(x) \le pe_K/(p-1) - 1$, so we must show that

$$p^{N-1}(pe_K/(p-1) - 1) < (p^N - 1)e_K/(p-1),$$

which holds if and only if $p^{N-1} > e_K/(p-1)$.

It remains to prove the claim. We first note that for all $0 \le i \le n-2$, the valuation of the $i$th term is greater than or equal to the valuation of the $n-2$nd term. Indeed, this is the statement that

$$p^{n-1-i} e_K + (i+1)e_K \ge pe_K + (n-1)e_K,$$

or equivalently, $p^{n-1-i} \ge n-1-i$, which is certainly true. So it suffices to show that the valuation of the $n-2$nd term is strictly greater than the valuation of the $n-1$st term. This is the statement that

$$pe_K + (n-1)e_K > p^n v_L(x) - (p^n + \cdots + p + 1)e_K,$$

and since $v_L(x) < pe_K/(p-1)$, it suffices to show that

$$p + (n-1) \ge 1/(p-1) + (n+1).$$

But this is equivalent to the statement that $(p-2)(p-1) \ge 1$, which is true, if and only if $p > 2$. This completes the proof. □

COROLLARY 1.2.6. *Let $L/K$ be a totally ramified cyclic extension of order $p$ and let $\sigma$ be a generator of $G = G_{L/K}$. Suppose that $v_L(\sigma(\pi_L) - \pi_L)$ is congruent to 1 modulo $p$, and let $N$ be the smallest integer such that $p^N > pe_K/(p-1)$. Then*

$$R_*^N : H^1(G, W_{N+n}(\mathcal{O}_L)) \to H^1(G, W_n(\mathcal{O}_L))$$

*is equal to zero, for all $n \ge 1$.*

PROOF. This follows from proposition 1.2.4 in view of lemma 1.1.1. □

**1.3.** We next consider the case of a general cyclic extension $L/K$ of order $p$.

LEMMA 1.3.1. *Let $L/K$ be a cyclic extension of order $p$, let $K'/K$ be a finite tamely ramified extension, and let $L'$ be the composition of $L$ and $K'$. Then for all integers $i \ge 0$ and $n \ge 1$, there is a canonical isomorphism*

$$H^i(G_{L/K}, W_n(\mathcal{O}_L)) \xrightarrow{\sim} H^i(G_{L'/K'}, W_n(\mathcal{O}_{L'}))^{G_{K'/K}}.$$

PROOF. The extension $L'/L$ is again tamely ramified, and therefore, by a theorem of Noether [**3**, chap. I §3, theorem 3], $\mathcal{O}_{L'}$ is a projective $\mathcal{O}_L[G_{L'/L}]$-module. It follows that the Hochschild-Serre spectral sequence

$$E_2^{s,t} = H^s(G_{L/K}, H^t(G_{L'/L}, W_n(\mathcal{O}_{L'}))) \Rightarrow H^{s+t}(G_{L'/K}, W_n(\mathcal{O}_{L'}))$$

collapses, such that the edge homomorphism

$$H^s(G_{L/K}, W_n(\mathcal{O}_L)) \xrightarrow{\sim} H^s(G_{L'/K}, W_n(\mathcal{O}_{L'}))$$

is an isomorphism. Similarly, since $K'/K$ is tamely ramified, the spectral sequence

$$E_2^{s,t}(G_{K'/K}, H^t(G_{L'/K'}, W_n(\mathcal{O}_{L'}))) \Rightarrow H^{s+t}(G_{L'/K}, W_n(\mathcal{O}_{L'}))$$

collapses, and the edge homomorphism

$$H^t(G_{L'/K}, W_n(\mathcal{O}_{L'})) \xrightarrow{\sim} H^t(G_{L'/K'}, W_n(\mathcal{O}_{L'}))^{G_{K'/K}}$$

is an isomorphism. The composition of these two isomorphisms gives the isomorphism of the statement. □

LEMMA 1.3.2. *Let $L/K$ be a totally ramified cyclic extension of order $p$. Then there exists a finite tamely ramified extension $K'/K$ such that if $L'$ is the composition of $L$ and $K'$, then $v_{L'}(\sigma(\pi_{L'}) - \pi_{L'})$ is congruent to 1 modulo $p$.*

PROOF. Let $L_1$ be the composition of $L$ and $K_1 = K(\mu_p)$. Then, by Kummer theory, $L_1 = K_1(x^{1/p})$, for some $x \in K_1$. Moreover, if we write $x = u\pi_{K_1}^i$ with $u \in K_1^*$, we can assume that $p$ does not divide $i$. Let $L'$ be the composition of $L_1$ and $K' = K_1(u^{1/i})$. Then

$$L' = K'((\pi_{K'}^i)^{1/p}) = K'(\pi_{K'}^{1/p}),$$

where $\pi_{K'} \in \mathcal{O}_{K'}$ is a uniformizer. If $\pi_{L'} \in \mathcal{O}_{L'}$ is a $p$th root of $\pi_{K'}$, then $\pi_{L'}$ is a uniformizer. Moreover, if $\sigma \in G_{L'/K'}$ is a generator, then $\sigma(\pi_{L'}) = \zeta_p \cdot \pi_{L'}$, so

$$\sigma(\pi_{L'}) - \pi_{L'} = (\zeta_p - 1)\pi_{L'}.$$

This shows that

$$v_{L'}(\sigma(\pi_{L'}) - \pi_{L'}) = v_{L'}(\zeta_p - 1) + 1 = pv_{K'}(\zeta_p - 1) + 1.$$

Finally, $K'/K$ is tamely ramified. □

COROLLARY 1.3.3. *Let $L/K$ be a totally ramified cyclic extension of order $p$. Then there exists $N \geq 1$ such that the map*

$$R_*^N : H^1(G, W_{N+n}(\mathcal{O}_L)) \to H^1(G, W_n(\mathcal{O}_L))$$

*is equal to zero, for all $n \geq 1$.*

PROOF. If we choose a tamely ramified extension $K'/K$ as in lemma 1.3.2, then the statement follows from lemma 1.3.1 and corollary 1.2.6. The smallest integer such that $p^{N-1}(p-1) > e_{K'} = e_{K'/K}e_K$ will do. □

**1.4.** We now prove the theorem of the introduction. Let $L/K$ be a finite Galois extension with Galois group $G$. The ramification groups define a finite filtration

$$G = G_{-1} \supset G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{v-1} \supset G_v = \{1\}$$

of $G$ by normal subgroups. We recall the following facts about the quotients $G_i/G_{i+1}$ from [**7**, chap. IV, §2]. The quotient $G/G_0$ is canonically isomorphic to the Galois group of the extension $k_L/k_K$ of residue fields, the quotient $G_0/G_1$ is cyclic of order prime to $p$, and the quotients $G_i/G_{i+1}$, $i \geq 1$, are elementary abelian $p$-groups. Let $K' = L^{G_1}$. Then $K'/K$ is a tamely ramified extension, and the extension $L/K'$ is the composition of a sequence of extensions

$$K' = M_1 \subset M_2 \subset \cdots \subset M_n = L$$

each of which is cyclic of order $p$. The theorem follows from corollary 1.3.3 by iterated use of the Hochschild-Serre spectral sequence.

## References

[1] P. Berthelot and W. Messing, *Théorie de Dieudonné cristalline. III. Théorèmes d'équivalence et de pleine fidélité*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser, Boston, MA, 1990, pp. 173–247.

[2] S. Bloch and K. Kato, *p-adic etale cohomology*, Publ. Math. IHES **63** (1986), 107–152.

[3] A. Fröhlich, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 1, Springer-Verlag, 1983.

[4] L. Hesselholt and I. Madsen, *On the $K$-theory of local fields*, Ann. Math. (to appear).

[5] B. Kahn, *Deux théorèmes de comparaison en cohomologie étale: applications*, Duke Math. J. **69** (1993), 137–165.

[6] S. Sen, *On automorphisms of local fields*, Ann. Math. **90** (1969), 33–46.

[7] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, 1979.

Massachusetts Institute of Technology, Cambridge, Massachusetts

*E-mail address*: `larsh@math.mit.edu`