# Galois cohomology of Witt vectors of algebraic integers

By Lars Hesselholt[†]
*Massachusetts Institute of Technology, Cambridge, Massachusetts*
*email*: larsh@math.mit.edu

(*Received* )

## *Introduction*

Let $K$ be a complete discrete valuation field of characteristic zero with residue field $k_K$ of characteristic $p > 0$. Let $L/K$ be a finite Galois extension with Galois group $G = G_{L/K}$ and suppose that the induced extension of residue fields $k_L/k_K$ is separable. By the normal basis theorem, $L$ is always a projective $K[G]$-module. But the ring of integers $\mathcal{O}_L$ is a projective $\mathcal{O}_K[G]$-module if and only $L/K$ is tamely ramified. For wildly ramified extensions, the structure of $\mathcal{O}_L$ as an $\mathcal{O}_K[G]$-module is very complicated and quite far from understood. We propose that the ring of Witt vectors $W.(\mathcal{O}_L)$ is a more well-behaved object. Indeed, we show that for a large class of extensions $L/K$, the pro-abelian group $H^1(G, W.(\mathcal{O}_L))$ is zero. We conjecture that this is true in general.

We recall that 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. 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. Hence, it suffices to show that $H^1(G, W.(\mathcal{O}_L))$ is zero, if $L/K$ is a totally ramified cyclic extension of order $p$. Let $\sigma$ be a generator of the Galois group, and let $t$ be the integer given by $v_L(\sigma(\pi_L) - \pi_L) = t + 1$. Then $1 \leq t \leq pe_K/(p-1)$.

*Theorem. Let $L/K$ be a totally ramified cyclic extension of order $p$ and suppose that $t > e_K/(p-1)$. Then 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 conjecture 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 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 conjecture that was the original motivation

[†] Supported in part by a grant from the National Science Foundation

for proving it. To explain this, let $K_v = K(\mu_{p^v})$. It follows from [**2**, theorem 5.12] and from [**4**, 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 [**3**, §3].) The theorem of this paper establishes the case $q = 0$, for instance, if $K$ is absolutely unramified.

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.

## *Proof of the theorem*

### 1. *A preliminary reduction*

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. *Let $m \geq 1$ be an integer and suppose that the map*

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

*is equal to zero, for $n = 1$. Then the same is true, for all $n \geq 1$.*

*Proof.* Suppose that for some $m = m_0 \geq 1$, the map

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

is equal to zero. Then the same is true, for all $m \geq m_0$. The long-exact sequence of cohomology groups shows that for all $m \geq m_0$, 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 that for all $m \geq m_0$ 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 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 $a \in M$, $\mathrm{tr}(a)$ is the sum of the Galois conjugates of $a$. In the case at hand, we have a canonical isomorphism

$$H^1(G, W_m(\mathcal{O}_L)) \approx W_m(\mathcal{O}_L)^{\mathrm{tr}=0}/(\sigma-1)W_m(\mathcal{O}_L).$$

In the following we shall often identify the cohomology group on the left with the group on the right.

## 2. *The main argument*

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

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

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

Lemma 2.1. *For all $a \in \mathcal{O}_L$, $v_K(\mathrm{tr}(a)) \geq (v_L(a) + t(p-1))/p$.*

*Proof.* This follows from the following formula from [**6**, chap. V, §3].

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

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

Lemma 2.2. *For all $x \in \mathcal{O}_L$, $v_K(\mathrm{tr}(x^p) - \mathrm{tr}(x)^p) = e_K + v_L(x)$.*

*Proof.* To prove the statement, we now use that, by the multinomial formula,

$$\mathrm{tr}(x)^p - \mathrm{tr}(x^p) = \sum_I \frac{p!}{i_0! \dots i_{p-1}!} x^{i_0} \sigma(x)^{i_1} \dots \sigma^{p-1}(x)^{i_{p-1}},$$

where the sum runs over tuples $(i_0, \dots, i_{p-1})$ of integers $0 \leq i_0, \dots, i_{p-1} < p$ with sum $i_0 + \dots i_{p-1} = p$. The summand $I = (1, \dots, 1)$ has valuation

$$v_K(p! \cdot x\sigma(x) \dots \sigma^{p-1}(x)) = e_K + v_L(x),$$

so it suffices to show that the sum of the remaining summands has strictly greater valuation. The cyclic group of order $p$ acts on the set of tuples $I \neq (1, \dots, 1)$ by cyclically permuting the coordinates, and the action is free. The partial sum of the summands with indices belonging to the orbit through $(i_0, \dots, i_{p-1})$ is equal to

$$\frac{p!}{i_0! \dots i_{p-1}!} \mathrm{tr}(x^{i_0} \sigma(x)^{i_1} \dots \sigma^{p-1}(x)^{i_{p-1}}).$$

It follows from lemma 2.1 that the valuation of this element is greater than or equal to $e_K + v_L(x) + 1$. This proves the lemma. □

COROLLARY 2.3. *Suppose that $t > e_K/(p-1)$. Then for all $x \in \mathcal{O}_L$,*

$$v_K(\mathrm{tr}(x^p)) = e_K + v_L(x).$$

*Proof.* We have from lemma 2.1 that

$$v_K(\mathrm{tr}(x)^p) = pv_K(\mathrm{tr}(x)) \geq t(p-1) + v_L(x) > e_K + v_L(x).$$

The statement thus follows from lemma 2.2. □

Comparing the statements of lemma 2.1 and corollary 2.3, we obtain the following well-known inequality [**6**, chap. IV, §2, exer. 3(c)].

$$1 \leq t \leq pe_K/(p-1).$$

We next recall the structure of $H^1(G, \mathcal{O}_L)$ from [**5**, theorem 2]. We let $\pi_L \in \mathcal{O}_L$ be a uniformizer, let $1 \leq \mu \leq p-1$ be an integer, and define

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

Then $v_L(x_\mu) = \mu$, and hence the elements $x_\mu$, $1 \leq \mu \leq p-1$, and the unit 1 form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. We define

$$\begin{aligned} y_\mu &= (\sigma - 1)x_\mu, \\ y'_\mu &= y_\mu/\pi_K^{(\mu)}, \end{aligned}$$

where $(\mu)$ is the greatest integer less than or equal to $(\mu + t)/p$. One can show that $v_L(y_\mu) = \mu + t$ and $v_L(y'_\mu) = \mu + t - p(\mu)$. It follows that the elements $y_\mu$ and $y'_\mu$, where $1 \leq \mu \leq p-1$, form an $\mathcal{O}_K$-basis of $(\sigma-1)\mathcal{O}_L$ and $\mathcal{O}_L^{\mathrm{tr}=0} = \mathcal{O}_L \cap (\sigma-1)L$, respectively. Hence, as an $\mathcal{O}_K$-module,

$$H^1(G, \mathcal{O}_L) \approx \bigoplus_{\mu=1}^{p-1} \mathcal{O}_K/\mathfrak{m}_K^{(\mu)} \cdot y'_\mu.$$

Since $t \leq pe_K/(p-1)$, we have $(\mu) \leq e_K/(p-1)$. In particular, $H^1(G, \mathcal{O}_L)$ is annihilated by $p$. Let $k$ be the residue field of $\mathcal{O}_K$, 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 $1 \leq \mu \leq p-1$ and $0 \leq i < (\mu)$.

LEMMA 2.4. *Suppose that $x \in \mathcal{O}_L^{\mathrm{tr}=0}$ represents a non-zero class in $H^1(G, \mathcal{O}_L)$. Then $v_L(x) \leq t-1$.*

*Proof.* We can write every $x \in \mathcal{O}_L^{\mathrm{tr}=0}$ uniquely as a sum

$$x = \sum_{\mu=1}^{p-1}(\sum_{i=0}^{(\mu)-1} \alpha_{\mu,i}\,\pi_K^i y'_\mu + \sum_{i=(\mu)}^{e_K-1} \beta_{\mu,i}\,\pi_K^i y'_\mu),$$

where $\alpha_{\mu,i}, \beta_{\mu,i} \in W$. Moreover, the class in $H^1(G, \mathcal{O}_L)$ represented by $x$ is zero if and only if $\alpha_{\mu,i} \in pW$, for all $1 \leq \mu \leq p-1$ and $0 \leq i \leq (\mu) - 1$.

We first note that the elements $\pi_K^i y'_\mu$, with $1 \leq \mu \leq p-1$ and $0 \leq i \leq (\mu)-1$, have valuation at most $t-1$. Indeed, if we write $t = pt' + \epsilon$ with $0 < \epsilon \leq p$, then

$$(\mu) = [(\mu+t)/p] = t' + [(\mu+\epsilon)/p],$$

which is less than or equal to $t'$ and $t'+1$, respectively, as $\mu+\epsilon < p$ and $\mu+\epsilon \geq p$. Hence $v_L(\pi_K^i y'_\mu)$ is less than or equal to $t-2$ and $t-1$, respectively.

Let $x \in \mathcal{O}_L^{\mathrm{tr}=0}$ be a general element. The summands $\alpha_{\mu,i}\,\pi_K^i y'_\mu$, with $\alpha_{\mu,i}$ not divisible by $p$, all have distinct valuations less than or equal to $t-1$. The summands $\alpha_{\mu,i}\,\pi_K^i y'_\mu$, with $\alpha_{\mu,i}$ divisible by $p$, have valuation greater than or equal to $e_L$, and

$$e_L = pe_K \geq pe_K/(p-1) \geq t > t-1.$$

Finally, the summands $\beta_{\mu,i}\,\pi_K^i y'_\mu$ have valuation greater than or equal to $t+1$. It follows that if $x$ represents a non-zero class in $H^1(G, \mathcal{O}_L)$, then the valuation of $x$ is at most $t-1$. □

Proposition 2.5. *Suppose that $t > e_K/(p-1)$. Then the map*

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

*is equal to zero, provided that $p^m > t$.*

*Proof.* Let $a = (a_0, \dots, a_m) \in W_{m+1}(\mathcal{O}_L)^{\mathrm{tr}=0}$ represent a class in the domain of the map of the statement. Then $a_0 \in \mathcal{O}_L^{\mathrm{tr}=0}$ represents the image of that class by the map of the statement. Suppose that the latter class is non-zero. Then, by lemma 2.4, $v_L(a_0) \leq t-1$. To prove the proposition, we show that

$$v_L(a_s) \leq t - p^s,$$

for all $0 \leq s \leq m$, and that

$$v_L(a_s) = v_K(\mathrm{tr}(a_{s+1})),$$

for all $0 \leq s < m$. The proof is by induction. So assume the inductive hypothesis for $m-1$. In the proof of induction step we use that the following equation holds.

$$\mathrm{tr}(a_0^{p^m}) + p\,\mathrm{tr}(a_1^{p^{m-1}}) + \dots + p^{m-1}\,\mathrm{tr}(a_{m-1}^p) + p^m\,\mathrm{tr}(a_m) = 0.$$

Inductively, we can estimate the valuation of all but the last summands on the left. If $0 \leq s \leq m-1$, then induction and corollary 2.3 show that

$$v_K(p^s\,\mathrm{tr}(a_s^{p^{m-s}})) = (s+1)e_K + p^{m-1-s}v_L(a_s),$$

and if $0 \leq s < m-1$, we have

$$\begin{aligned} v_K(p^s\,\mathrm{tr}(a_s^{p^{m-s}})) &= (s+1)e_K + p^{m-1-s}v_L(a_s) \\ &= (s+1)e_K + p^{m-1-s}v_K(\mathrm{tr}(a_{s+1})) \\ &\geq (s+1)e_K + p^{m-1-(s+1)}(v_L(a_{s+1}) + t(p-1)). \end{aligned}$$

Since $t(p-1) > e_K$, it follows that for $0 \leq s < m-1$,

$$v_K(p^s\,\mathrm{tr}(a_s^{p^{m-s}})) > v_K(p^{s+1}\,\mathrm{tr}(a_{s+1}^{p^{m-(s+1)}})),$$

and hence, the equation above shows that

$$v_K(p^{m-1}\,\mathrm{tr}(a_{m-1}^p)) = v_K(p^m\,\mathrm{tr}(a_m)).$$

On the one hand, we have, by induction and by corollary 2.3, that

$$v_K(p^{m-1}\operatorname{tr}(a_{m-1}^p)) = me_K + v_L(a_{m-1}) \leq me_K + t - p^{m-1},$$

and on the other hand, we have from lemma 2.1 that

$$v_K(p^m \operatorname{tr}(a_m)) = me_K + v_K(\operatorname{tr}(a_m)) \geq me_K + (v_L(a_m) + t(p-1))/p.$$

This proves the induction step. □

*Proof of the theorem* The theorem of the introduction follows immediately from proposition 2.5 and lemma 1.1. □

*Remark* 2.6. We end with a few comments on $H^2(G_{L/K}, W.(\mathcal{O}_L))$. In general, this is a module over the pro-ring $W.(\mathcal{O}_K)$. But if the residue field $k$ is perfect, there exists a canonical ring homomorphism

$$\rho\colon W(k) \to W.(\mathcal{O}_K),$$

which allows us to view $H^2(G, W.(\mathcal{O}_L))$ as a $W(k)$-module. The ring homomorphism $\rho$ is defined as the composite $W(f) \circ \lambda$, where $f\colon W(k) \to \mathcal{O}_K$ is the unique ring homomorphism such that the induced map of residue fields is the identity, and where $\lambda\colon W(k) \to W(W(k))$ is the unique ring homomorphism such that $w_n\lambda = F^n$, for all $n \geq 0$. Here $w_n\colon W(A) \to A$ is the $n$th ghost component, and $F\colon W(k) \to W(k)$ is the Frobenius.

Let $L/K$ be a totally ramified cyclic extension of order $p$. Suppose in addition that $p$ divides $t$, or equivalently, that $t = pe_K/(p-1)$. Then, if $k$ is perfect,

$$\operatorname{length}_{W(k)} H^2(G, W.(\mathcal{O}_L)) = pe_K/(p-1).$$

For the proof of proposition 2.5 identifies the left hand side with the sum over all integers $s \geq 0$ of the cardinality of the set of integers $v$ prime to $p$ such that

$$(1-p^{-s})e_K/(1-p^{-1}) \leq v < e_K/(1-p^{-1}) = pe_K/(p-1).$$

But the function which to $v$ associates $a = p^s v - (p^{s-1} + \cdots + p + 1)pe_K$ gives a bijection between this set and the set of integers $0 \leq a < pe_K/(p-1)$ which satisfy that $v_p(a - pe_K/(p-1)) = s$.

## 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**] L. Hesselholt and I. Madsen, *On the K-theory of local fields*, Ann. of Math. **158** (2003), 1–113.

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

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

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