Near-final version. November 2002. Comments appreciated
http://www.math.uiuc.edu/K-theory/0589/

GALOIS COHOMOLOGY OF CERTAIN FIELD EXTENSIONS AND THE DIVISIBLE CASE OF MILNOR–KATO CONJECTURE

LEONID POSITSELSKI

Let F be a field and $m \geqslant 2$ be an integer not divisible by the characteristic of F. Consider the absolute Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$, where $\overline{F}$ denotes the (separable) algebraic closure of F. The famous *Milnor–Kato conjecture* [6, 5] claims that the natural homomorphism of graded rings

$$K_n^{\mathrm{M}}(F) \otimes \mathbb{Z}/m \longrightarrow H^n(G_F, \mu_m^{\otimes n})$$

from the Milnor K-theory of the field F modulo m to the Galois cohomology of F with cyclotomic coefficients is an isomorphism (here, as usually, μ_m denotes the group of m-roots of unity in $\overline{F}$). One can see that it suffices to verify this conjecture in the case when m is a prime number.

Several years ago V. Voevodsky outlined his approach to the Milnor–Kato conjecture in the preprint [10]. The first step of his argument dealt with a prime number ℓ, a field F having no finite extensions of degree prime to ℓ, and an integer $n \geqslant 1$ such that the group $K_{n+1}^{\mathrm{M}}(F)$ is ℓ-divisible. Assuming that the conjecture holds in degree less or equal to n for $m = \ell$ and any field containing F, Voevodsky was proving that $H^{n+1}(G_F, \mathbb{Z}/\ell) = 0$. The main goal of this paper is to give a simplified elementary version of Voevodsky's proof of this step. In particular, we do not need to consider fields transcendental over F and we make no use of motivic cohomology at all. Our main result is formulated as follows.

Theorem 1. *Let ℓ be a prime number, $n \geqslant 1$ be an integer, and F be a field of characteristic not equal to ℓ, having no finite extensions of degree prime to ℓ. Suppose that the homomorphism $K_n^{\mathrm{M}}(L)/\ell K_n^{\mathrm{M}}(L) \longrightarrow H^n(G_L, \mathbb{Z}/\ell)$ is an isomorphism for any finite extension L of the field F. Furthermore, assume that $K_{n+1}^{\mathrm{M}}(F) = \ell K_{n+1}^{\mathrm{M}}(F)$. Then one has $H^{n+1}(G_F, \mathbb{Z}/\ell) = 0$.*

We deduce the above theorem from two results, one related to the Milnor K-theory of fields and the other to the cohomology of Galois groups. The first one is but a version of a lemma of Suslin [9], which was also used in [10]. We only rewrote it for the Milnor K-theory groups modulo ℓ. The second statement is essentially the "relative conjecture" of Bloch and Kato [3]. It is obvious for $\ell = 2$ (when it holds for any pro-finite group). For odd primes ℓ we show that the desired cohomological sequence is exact provided that certain Bockstein homomorphisms vanish. This is the key point of this paper.

Proposition 2. *Let $m \geqslant 2$ be an integer, G be a pro-finite group, and $H \subset G$ be a normal subgroup such that $\Sigma = G/H$ is a cyclic group of order m. Let T_{m^2} be a free module over $\mathbb{Z}/m^2$ endowed with an action of G, and let $T_m = mT_{m^2} = T_{m^2}/mT_{m^2}$ be the corresponding G-module over $\mathbb{Z}/m$. Assume that for a certain $n \geqslant 0$ both Bockstein homomorphisms*

$$H^n(G, T_m) \longrightarrow H^{n+1}(G, T_m) \quad \text{and} \quad H^n(H, T_m) \longrightarrow H^{n+1}(H, T_m)$$

vanish. Then the following sequence of cohomology groups is exact

$$H^n(G, T_m) \xrightarrow{\text{res}} H^n(H, T_m)_\Sigma \xrightarrow{\text{cor}} H^n(G, T_m)$$
$$\xrightarrow{u\cup} H^{n+1}(G, T_m) \xrightarrow{\text{res}} H^{n+1}(H, T_m)^\Sigma \xrightarrow{\text{cor}} H^{n+1}(G, T_m),$$

where $u \in H^1(G, \mathbb{Z}/m)$ is the class corresponding to the character $G \longrightarrow \Sigma \simeq \mathbb{Z}/m$. (The letter Σ in the upper or lower index denotes the invariants or the coinvariants with respect to a natural action of the group Σ.)

In sections 3 and 5 of this paper we apply the same techniques to obtain further exact sequences of Galois cohomology for cyclic, biquadratic, and dihedral field extensions. In particular, our method proves the biquadratic exact sequences conjectured by Merkurjev–Tignol [7] and Kahn [4].

I would like to express my gratitude to Vladimir Voevodsky for posing the problem and for very helpful conversations and explanations. He also always urged me to write down this proof. I am grateful to Alexander Vishik for numerous very helpful discussions. Most of this work was done during my stay at the Institute for Advanced Study in Princeton and the rest at the Institute des Hautes Etudes Scientifiques in Paris, Max-Planck-Intitut für Mathematik in Bonn and the Independent University of Moscow. I wish to thank all these four institutions.

1. Suslin's Lemma for Milnor K-theory modulo ℓ

The goal of this section is to deduce Theorem 1 from Proposition 2. This is the least elementary part of this paper, to the extent that the proof of Corollary 4 is based on existence of transfer homomorphisms on the Milnor K-theory groups. We will only use the transfer maps for extensions of degree ℓ of fields having no extensions of degree prime to ℓ. The existence of transfers for such field extensions was established in [1]; their basic properties are the base change and the projection formula.

Let us fix a prime number ℓ, a number $n \geqslant 1$, and a field F with $\operatorname{char} F \neq \ell$, having no finite extensions of degree prime to ℓ. Introduce the notation $k_m(K) = K_m^{\mathrm{M}}(K)/\ell$ for the Milnor K-theory groups modulo ℓ of a field K. For a field extension $K \subset L$ we will denote by

$$i_{L/K} \colon k_m(K) \longrightarrow k_m(L) \quad \text{and} \quad tr_{L/K} \colon k_m(L) \longrightarrow k_m(K)$$

the inclusion and transfer homomorphisms.

Lemma 3. *Assume that for any finite field extensions $F \subset K \subset L$ with $[L:K] = \ell$ the sequence of Milnor K-theory groups*

$$k_n(K) \xrightarrow{\ i\ } k_n(L)_\Sigma \xrightarrow{\ tr\ } k_n(K), \qquad \Sigma = \mathrm{Gal}(L/K)$$

is exact. Further assume that $[E:F] = \ell$ and the map $tr_{E/F}\colon k_n(E) \longrightarrow k_n(F)$ is surjective. Then the sequence

$$k_{n+1}(F) \xrightarrow{\ i\ } k_{n+1}(E)_\Sigma \xrightarrow{\ tr\ } k_{n+1}(F), \qquad \Sigma = \mathrm{Gal}(E/F)$$

is also exact.

Proof. In order to prove that the map $tr_{E/F}\colon k_{n+1}(E)_\Sigma / i_{E/F} k_{n+1}(F) \longrightarrow k_{n+1}(F)$ is injective, we will construct a surjective homomorphism

$$\phi\colon k_{n+1}(F) \longrightarrow k_{n+1}(E)_\Sigma / i_{E/F}(k_{n+1}(F))$$

for which $tr_{E/F} \circ \phi = \mathrm{id}$. This is done as follows.

By our assumptions, the map $tr_{E/F}\colon k_n(E)_\Sigma / i_{E/F} k_n(F) \longrightarrow k_n(F)$ is an isomorphism. Therefore, we can define a homomorphism

$$\Phi\colon k_1(F) \otimes k_n(F) \longrightarrow k_{n+1}(E)_\Sigma / i_{E/F}(k_{n+1}(F))$$

by the rule $\Phi(b \otimes \alpha) = \overline{b\beta}$, where $\beta \in k_n(E)$ is such that $tr_{E/F}\,\beta = \alpha$. Let us verify that Φ can be factorized through $k_{n+1}(F)$. It suffices to show that $\Phi((1-a)\otimes\alpha) = 0$ whenever $\alpha \in k_n(F)$ is divisible by the class $(a) \in k_1(F)$ of an element $a \in F \setminus \{0,1\}$.

Let us first assume that a is not an ℓ-th power in E. Consider the field $K = F(\sqrt[\ell]{a})$; let $L = EK$ be the field generated by E and K over F. Then we have $tr_{L/K}\, i_{L/E}\beta = i_{K/F}\, tr_{E/F}\,\beta = 0$, since $tr_{E/F}\,\beta = \alpha$ is divisible by (a). By assumption, it follows that $i_{L/E}\beta \in i_{L/K} k_n(K) + (1-\sigma)k_n(L)$, where σ is a generator of the group $\mathrm{Gal}(L/K) = \mathrm{Gal}(E/F)$. Now we have

$$\begin{aligned}(1-a)\cdot\beta = {} & tr_{L/E}((1-\sqrt[\ell]{a}))\cdot\beta = tr_{L/E}((1-\sqrt[\ell]{a})\cdot i_{L/E}\beta) \\ & \subset tr_{L/E}(i_{L/K}k_{n+1}(K) + (1-\sigma)k_{n+1}(L)) \subset i_{E/F}k_{n+1}(F) + (1-\sigma)k_{n+1}(E),\end{aligned}$$

hence $\Phi((1-a)\otimes\alpha) = 0$.

It remains to consider the case $\sqrt[\ell]{a} \in E$. In this case we have $\sum_{s=1}^{\ell} \sigma^s(\beta) = i_{E/F}\, tr_{E/F}\,\beta = i_{E/F}\alpha = 0$ and therefore

$$(1-a)\cdot\beta = \textstyle\sum_{s=1}^{\ell} \sigma^s(1-\sqrt[\ell]{a})\cdot\beta = \sum_{s=1}^{\ell}(1-\sqrt[\ell]{a})\cdot\sigma^{-s}(\beta) = 0$$

modulo $(1-\sigma)k_{n+1}(E)$.

Thus we have constructed the desired map ϕ. Since the field F has no finite extensions of degree less than ℓ, we have $k_{n+1}(E) = k_1(F)\cdot k_n(E)$ (see [1] and section 4); hence the map ϕ is surjective. It is obvious that $tr_{E/F}\circ\phi = \mathrm{id}$. $\square$

Corollary 4. *Assume that for any finite field extensions $F \subset K \subset L$ with $[L:K] = \ell$ the following sequence of Milnor K-theory groups is exact*

$$k_n(K) \xrightarrow{\ i\ } k_n(L)_\Sigma \xrightarrow{\ tr\ } k_n(K) \xrightarrow{\ u\cdot\ } k_{n+1}(K),$$

where $u \in k_1(K)$ is the element corresponding to the cyclic extension $K \subset L$ and $\Sigma = \mathrm{Gal}(L/K)$. Further assume that $k_{n+1}(F) = 0$. Then one has $k_{n+1}(E) = 0$ for any finite field extension $F \subset E$.

Proof. Proceeding by induction, we only have to consider the case when $[E:F] = \ell$. Since $k_{n+1}(F) = 0$, it follows from our exact sequence that the transfer homomorphism $tr_{E/F}\colon k_n(E) \longrightarrow k_n(F)$ is surjective. Therefore, the conditions of Lemma 3 are satisfied and we can conclude that $k_{n+1}(E)_\Sigma = 0$. Thus $k_{n+1}(E) = (1-\sigma)k_{n+1}(E) = (1-\sigma)^\ell k_{n+1}(E) = 0$. $\square$

Proof of Theorem 1. Let $F \subset K \subset L$ be finite field extensions with $[L:K] = \ell$. We will apply Proposition 2 for $m = \ell$, the pro-finite group $G = G_K$, the subgroup $H = G_L$, the modules $T_{\ell^2} = \mu_{\ell^2}^{\otimes n}$ and $T_\ell \simeq \mathbb{Z}/\ell$ over G, and the degree n. It follows from the assumptions of Theorem 1 that the required Bockstein homomorphisms vanish. From Proposition 2 we conclude that the conditions of Corollary 4 are satisfied for the field F. Thus we have $k_{n+1}(E) = 0$ for any field E finite over F.

Now assume that α is a nonzero element of $H^{n+1}(G_F, \mathbb{Z}/\ell)$. It is clear that there exist finite field extensions $F \subset K \subset L$ such that $\mathrm{res}_{K/F}\,\alpha \neq 0$, but $\mathrm{res}_{L/F}(\alpha) = 0$ and $[L:K] = \ell$. Using Proposition 2 again, we see that $\mathrm{res}_{K/F}\,\alpha = u_{L/K} \cup \beta$ for some $\beta \in H^n(G_K, \mathbb{Z}/\ell)$. Since $k_n(K) \simeq H^n(G_K, \mathbb{Z}/\ell)$ and $k_{n+1}(K) = 0$, it follows that $\mathrm{res}_{K/F}\,\alpha = 0$. This contradiction proves that $H^{n+1}(G_F, \mathbb{Z}/\ell) = 0$. $\square$

2. The Six-Term Cohomological Exact Sequence

In this section we develop a rather general setting for exact sequences of cohomology under the assumptions of vanishing of Bockstein homomorphisms. The results below are actually valid for an arbitrary cohomological functor on an abelian category endowed with a central element with zero square, etc. We restrict ourselves to the cohomology of a pro-finite group for the sake of simplicity of exposition only.

Let us fix a pro-finite group G and a number $m \geqslant 2$. We will use the following notation: A_2, B_2, etc. will denote free modules over $\mathbb{Z}/m^2$ endowed with a discrete action of G and A_1, B_1, etc. will be the corresponding G-modules over $\mathbb{Z}/m$, defined as $A_1 = mA_2 = A_2/mA_2$. For a G-module M, we will simply write $H^n(M) = H^n(G, M)$. The Bockstein homomorphisms corresponding to exact triples

$$0 \longrightarrow M_1 \xrightarrow{\ \tau\ } M_2 \xrightarrow{\ \pi\ } M_1 \longrightarrow 0, \qquad \tau\pi = m$$

will be denoted by $\beta_M^n\colon H^n(M_1) \longrightarrow H^{n+1}(M_1)$.

Lemma 5. *Let $0 \to X_2 \xrightarrow{i} Y_2 \xrightarrow{p} Z_2 \to 0$ be an exact triple of G-modules over $\mathbb{Z}/m^2$, $0 \to X_1 \longrightarrow Y_1 \longrightarrow Z_1 \to 0$ be the corresponding exact triple of G-modules over $\mathbb{Z}/m$, and $\partial_{XZ}\colon H^n(Z_1) \longrightarrow H^{n+1}(X_1)$ be the induced homomorphism of pro-finite group cohomology.*

Let h be a homotopy map on the complex $X_2 \longrightarrow Y_2 \longrightarrow Z_2$ such that $dh + hd = m \cdot \mathrm{id}$, where $d = (i, p)$. Then the induced map h_1 is an endomorphism of degree -1 of the complex $X_1 \longrightarrow Y_1 \longrightarrow Z_1$. It follows that there is a map $h_{XZ}\colon Z_1 \longrightarrow X_1$ such that $h_{XZ} \circ p_1 = h_1\colon Y_1 \longrightarrow X_1$ and $i_1 \circ h_{XZ} = -h_1\colon Z_1 \longrightarrow Y_1$.

Then the following equality holds: $\partial_{XZ} = \beta_X \circ H(h_{XZ}) - H(h_{XZ}) \circ \beta_Z$.

Proof. The desired equality of homomorphisms of cohomology is to be understood as the corollary to an identity in the G-module extension group $\mathrm{Ext}^1_{\mathbb{Z}/m^2[G]}(Z_1, X_1)$, where ∂_{XZ} and the betas represent certain extension classes and h_{XZ} is just a map of modules. This identity in the group of extension classes is verified as follows.

The composition of the Bockstein extension $X_1 \longrightarrow X_2 \longrightarrow X_1$ with $h_{XZ}\colon Z_1 \longrightarrow X_1$ is an extension of the form $X_1 \longrightarrow X_2 \sqcap_{X_1} Z_1 \longrightarrow Z_1$, while the composition of $Z_1 \longrightarrow Z_2 \longrightarrow Z_1$ with h_{XZ} is $X_1 \longrightarrow X_1 \sqcup_{Z_1} Z_2 \longrightarrow Z_1$ (where $\sqcap$ and $\sqcup$ denote the relative product and coproduct, respectively). We have to check that the difference of these extensions is isomorphic to $X_1 \longrightarrow Y_1 \longrightarrow Z_1$. The middle term of the desired difference can be defined as the homology module of the sequence $X_1 \xrightarrow{(1,1)} (X_2 \sqcap_{X_1} Z_1) \oplus (X_1 \sqcup_{Z_1} Z_2) \xrightarrow{(1,-1)} Z_1$.

Let us construct an isomorphism f from Y_1 to this homology module. Given an element $y_1 \in Y_1$, we choose its preimage $y_2 \in Y_2$ and set $f(y_1) = (h(y_2), p_1(y_1)) \oplus (h_1(y_1), p(y_2))$. The rest is a straightforward computation. ☐

Theorem 6. *Let G be a pro-finite group, $m \geqslant 2$ and $n \geqslant 0$ be some integers, and*

$$0 \longrightarrow A_2 \longrightarrow B_2 \longrightarrow C_2 \longrightarrow D_2 \longrightarrow 0$$

be a 4-term exact sequence of free $\mathbb{Z}/m^2$-modules with a discrete action of G in it. Suppose that we are given a homotopy map h in this exact sequence such that $dh + hd = m$. Assume that the Bockstein maps

$$\beta^n_X\colon H^n(G, X_1) \longrightarrow H^{n+1}(G, X_1), \qquad X_1 = mX_2 = X_2/m$$

vanish for all $X = A$, B, C, or D and the given n. Then there is a 6-term exact sequence of the form

$$H^n(B_1 \oplus D_1) \xrightarrow{(d_1, h_1)} H^n(C_1) \xrightarrow{d_1} H^n(D_1)$$
$$\xrightarrow{\nu} H^{n+1}(A_1) \xrightarrow{d_1} H^{n+1}(B_1) \xrightarrow{(h_1, d_1)} H^{n+1}(A_1 \oplus C_1).$$

The middle arrow ν comes from a certain extension

$$0 \longrightarrow A_1 \longrightarrow N \longrightarrow D_1 \longrightarrow 0$$

of discrete G-modules over $\mathbb{Z}/m$, whose compositions with the morphisms $A_1 \longrightarrow B_1$ and $C_1 \longrightarrow D_1$ are trivial. If the group G acts on the original exact quadruple of modules through its finite quotient group Γ, then N is a $\mathbb{Z}/m[\Gamma]$-module.

Proof. Let L_2 denote the image of the differential $B_2 \longrightarrow C_2$. It is clear that L_2 is a free module over $\mathbb{Z}/m^2$. Now our 4-term exact sequence of G-modules consists of two exact triples: $A_2 \longrightarrow B_2 \longrightarrow L_2$ and $L_2 \longrightarrow C_2 \longrightarrow D_2$. Reducing modulo m, we see that the map $h_1 \colon C_1 \longrightarrow B_1$ defines a homomorphism from the exact triple $L_1 \longrightarrow C_1 \longrightarrow D_1$ to $A_1 \longrightarrow B_1 \longrightarrow L_1$. The corresponding "intermediate" induced extension provides the desired exact triple $A_1 \longrightarrow N \longrightarrow D_1$.

Now the 6-term sequence is constructed; it remains to check that it's exact. Let us introduce notation for maps $p \colon B_2 \longrightarrow L_2$ and $i \colon L_2 \longrightarrow C_2$; the same maps reduced modulo m will be be denoted by p_1 and i_1. It is easy to see that the homotopy map h induces analogous homotopies on the exact triples $A_2 \longrightarrow B_2 \longrightarrow L_2$ and $L_2 \longrightarrow C_2 \longrightarrow D_2$. Therefore, both triples satisfy the conditions of Lemma 5. We have connecting maps $\partial_{AL} \colon H^n(L_1) \longrightarrow H^{n+1}(A_1)$ and $\partial_{LD} \colon H^n(D_1) \longrightarrow H^{n+1}(L_1)$ in the pro-finite group cohomology; the cohomology maps induced by the module maps $h_{AL} \colon L_1 \longrightarrow A_1$ and $h_{LD} \colon D_1 \longrightarrow L_1$ will be denoted simply by h_{AL} and h_{LD}. According to Lemma 5, there are two identities: $\partial_{LD} = \beta_L \circ h_{LD} - h_{LD} \circ \beta_D$ and $\partial_{AL} = \beta_A \circ h_{AL} - h_{AL} \circ \beta_L$. We also know that $\nu = \partial_{AL} \circ h_{LD} = -h_{AL} \circ \partial_{LD}$.

Assume that $x \in H^n(D_1)$ and $\nu(x) = 0$. Let us prove that $x \in d_1 H^n(C_1)$. We have $\partial_{AL} h_{LD}(x) = 0$, hence $h_{LD}(x) = p_1(z)$ for some $z \in H^n(B_1)$. Since p_1 is induced by a map of modules over $\mathbb{Z}/m^2$, it commutes with betas. So it follows from our assumptions about vanishing of Bockstein homomorphisms that $0 = p_1\beta_B(z) = \beta_L p_1(z) = \beta_L h_{LD}(x) = \beta_L h_{LD}(x) - h_{LD}\beta_D(x) = \partial_{LD}(x)$. Thus $x \in d_1 H^n(C_1)$.

Next assume that $w \in H^{n+1}(A_1)$ and $d_1(w) = 0$. Then $w = \partial_{AL}(u)$ for some $u \in H^n(L_1)$, hence $w = \beta_A h_{AL}(u) - h_{AL}\beta_L(u) = h_{AL}\beta_L(u)$. The map i_1 commutes with betas for the same reason as above, so according to our assumption about Bockstein maps we have $i_1\beta_L(u) = \beta_C i_1(u) = 0$. It follows that $\beta_L(u) = \partial_{LD}(x)$ for some $x \in H^n(D_1)$. Thus $w = h_{AL}\beta_L(u) = h_{AL}\partial_{LD}(x) = \nu(-x)$.

Now assume that $y \in H^n(C_1)$ and $d_1(y) = 0$. Let us prove that $y \in d_1 H^n(B_1) + h_1 H^n(D_1)$. Since $d_1(y) = 0$, we have $y = i_1(u)$ with $u \in H^n(L_1)$. Then $i_1\beta_L(u) = \beta_C i_1(u) = 0$, hence $\beta_L(u) = \partial_{LD}(x)$ for some $x \in H^n(D_1)$. Therefore, $\partial_{AL}(u) = \beta_A h_{AL}(u) - h_{AL}\beta_L(u) = -h_{AL}\beta_L(u) = -h_{AL}\partial_{LD}(x) = \partial_{AL} h_{LD}(x)$. It follows that $\partial_{AL}(u - h_{LD}(x)) = 0$ and $u - h_{LD}(x) = p_1(z)$ for some $z \in H^n(B_1)$. Applying i_1, we obtain $y = i_1 p_1(z) + i_1 h_{LD}(x) = d_1(z) - h_1(x)$.

Finally, assume that $t \in H^{n+1}(B_1)$ is such that $d_1(t) = 0$ and $h_1(t) = 0$. Then $i_1 p_1(t) = d_1(t) = 0$, hence $p_1(t) = \partial_{LD}(x)$ for some $x \in H^n(D_1)$. We have $\partial_{AL} h_{LD}(x) = -h_{AL}\partial_{LD}(x) = -h_{AL} p_1(t) = -h_1(t) = 0$, so $h_{LD}(x) = p_1(z)$ with $z \in H^n(B_1)$. It follows that $p_1(t) = \partial_{LD}(x) = \beta_L h_{LD}(x) - h_{LD}\beta_D(x) = \beta_L h_{LD}(x) = \beta_L p_1(z) = p_1\beta_B(z) = 0$ and therefore $t \in d_1 H^{n+1}(A_1)$. $\square$

Remark. The middle arrow ν does not depend on the choice of a homotopy map h, provided that h satisfies the conditions of Theorem 6. Indeed, let us consider another homotopy map $h' = h + t$, where $dt + td = 0$. Then the induced maps t_{AL} and t_{LD} commute with Bockstein homomorphisms, and according to the above computations we have $\nu' - \nu = t_{AL} \circ \partial_{LD} = t_{AL} \circ \beta_L \circ h_{LD} - t_{AL} \circ h_{LD} \circ \beta_D = \beta_A \circ t_{AL} \circ h_{LD} - t_{AL} \circ h_{LD} \circ \beta_D = 0$ on $H^n(D_1)$. If A_1 and D_1 are permutational modules (as in all applications below), then $t_{AL} \circ h_{LD}$ can be lifted to a map $D_2 \longrightarrow A_2$ and it follows that the extension $A_1 \longrightarrow N \longrightarrow D_1$ does not depend on h either.

3. The Relative Conjecture of Bloch and Kato

In this section we will prove two theorems providing exact sequences for Galois cohomology of cyclic field extensions, both of them generalizations of Proposition 2. The first one will be essentially the "relative conjecture" of Bloch and Kato [3, Conjecture 3.1]. In particular, the proof of Theorem 1 will be completed.

Throughout this section, we will use the following notation: $m \geqslant 2$ is an integer, G is a pro-finite group, T_{m^2} is a free module over $\mathbb{Z}/m^2$ endowed with an action of G, and $T_m = mT_{m^2} = T_{m^2}/mT_{m^2}$ is the corresponding G-module over $\mathbb{Z}/m$. Furthermore, $n \geqslant 0$ is another integer, and it is assumed that the Bockstein homomorphisms

$$H^n(H, T_m) \longrightarrow H^{n+1}(H, T_m), \qquad H \subset G$$

vanish for all relevant open subgroups H in G, including G itself. In applications to Galois cohomology it will be always meant that $G = G_F$ is the absolute Galois group of a field F and $T_{m^2} = \mu_{m^2}^{\otimes n}$ is the cyclotomic module.

Proposition 7. *Let $H \subset G$ be a normal subgroup such that $\Sigma = G/H$ is a cyclic group of an order k dividing m. Then the following sequence of cohomology groups is exact*

$$H^n(G, T_m) \xrightarrow{m/k\cdot\mathrm{res}} H^n(H, T_m)_\Sigma \xrightarrow{\mathrm{cor}} H^n(G, T_m)$$
$$\xrightarrow{u\,\cup} H^{n+1}(G, T_m) \xrightarrow{\mathrm{res}} H^{n+1}(H, T_m)^\Sigma \xrightarrow{m/k\cdot\mathrm{cor}} H^{n+1}(G, T_m),$$

where $u \in H^1(G, \mathbb{Z}/m)$ is the class corresponding to the character $G \longrightarrow \Sigma \hookrightarrow \mathbb{Z}/m$.

Proof. Consider the following very well known 4-term exact sequence of modules over the cyclic group Σ:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{1+\cdots+\sigma^{k-1}} \mathbb{Z}[\Sigma] \xrightarrow{1-\sigma} \mathbb{Z}[\Sigma] \xrightarrow{\sigma^i \longmapsto 1} \mathbb{Z} \longrightarrow 0,$$

where σ is a generator of Σ. Let us construct a homotopy map h_k such that $dh_k + h_k d = k$. Set $f(x)$ to be the polynomial for which $k - (1 + \cdots + x^{k-1}) = (1 - x)f(x)$. The leftmost component of h_k sends σ^i to 1 for all i, the middle part is given by the multiplication with $f(\sigma)$ in the group ring $\mathbb{Z}[\Sigma]$, and the rightmost component sends 1 to $1+\cdots+\sigma^{k-1}$. For the purposes of our proof it suffices to put $h = m/k \cdot h_k$, tensor the above exact quadruple with T_{m^2}, and apply Theorem 6. $\square$

The proof of Theorem 1 is now finished.

Proposition 8. *Let $H \subset G$ be a normal subgroup such that $\Sigma = G/H$ is a cyclic group of an order k divisible by m. Let $\Pi \subset \Sigma$ be the cyclic subgroup of order m and $K \subset G$ be kernel of the projection $G \longrightarrow \Sigma/\Pi$. Then the following sequences of cohomology groups are exact*

$$H^n(H)_\Sigma \xrightarrow{\mathrm{cor}} H^n(K)_{\Sigma/\Pi} \xrightarrow{\mathrm{cor}\circ u\cup} H^{n+1}(G) \xrightarrow{\mathrm{res}} H^{n+1}(H)^\Sigma \xrightarrow{\mathrm{cor}} H^{n+1}(K)^{\Sigma/\Pi}$$

and

$$H^n(K)_{\Sigma/\Pi} \xrightarrow{\mathrm{res}} H^n(H)_\Sigma \xrightarrow{\mathrm{cor}} H^n(G) \xrightarrow{u\cup\,\circ\,\mathrm{res}} H^{n+1}(K)^{\Sigma/\Pi} \xrightarrow{\mathrm{res}} H^{n+1}(H)^\Sigma,$$

where we write $H^i(I) = H^i(I, T_m)$ for any subgroup $I \subset G$, and $u \in H^1(K, \mathbb{Z}/m)$ is the cohomology class corresponding to the character $K \longrightarrow \Pi \simeq \mathbb{Z}/m$.

Proof. The first of the desired exact sequences holds due to the following exact quadruple Q_Σ of permutational Σ-modules

$$\mathbb{Z} \longrightarrow \mathbb{Z}[\Sigma] \oplus \mathbb{Z} \longrightarrow \mathbb{Z}[\Sigma] \oplus \mathbb{Z}[\Sigma/\Pi] \longrightarrow \mathbb{Z}[\Sigma/\Pi],$$

where the first map is $(1+\cdots+\sigma^{k-1}, -m)$, the third map is $(\mathrm{pr}_\Pi, -1+\bar\sigma)$, and the middle arrow is given by the matrix U with components $U_{11} = 1-\sigma$, $U_{12} = 0$, $U_{21} = \mathrm{pr}_\Pi$, and $U_{22} = 1+\cdots+\bar\sigma^{k/m-1}$. Here σ is a generator of Σ, by $\bar\sigma$ we denote its image in Σ/Π, and pr_Π is the projection map $\mathbb{Z}[\Sigma] \longrightarrow \mathbb{Z}[\Sigma/\Pi]$. It is not difficult to construct a homotopy map h with $dh + hd = m$. Using this exact quadruple, one argues as in the proof of Proposition 7 above. To obtain the second exact sequence of cohomology, one has to use the dual exact quadruple of Σ-modules $\mathrm{Hom}_\mathbb{Z}(Q_\Sigma, \mathbb{Z})$. $\square$

4. The Bass–Tate Lemma and Applications to Annihilator Ideals

The next theorem provides a more sophisticated version of the classical technique known as the “Bass–Tate lemma” [1].

Theorem 9. *Let E/F be a separable extension of fields of degree k. Assume that the field F has no nontrivial finite extensions of degrees less or equal to $k/2$. Then $K^{\mathrm{M}}_{\geqslant 1}(E) = \bigoplus_{i=1}^{\infty} K^{\mathrm{M}}_n(E)$ is a quadratic module over the ring $K^{\mathrm{M}}_*(F)$, i. e., a graded module generated in degree 1 with relations in degree 2.*

Lemma 10. *Let $E = F[t]$ be a finite extension of fields of degree k, where $t \in E$ is a generator. Then any element of the field E can be represented as a fraction of polynomials $f(t)/g(t)$, where f and g are two polynomials of degree $\leqslant k/2$ each.*

Proof. Let $V \subset E$ be the vector subspace of all elements of the form $f(t)$, where $\deg f \leqslant k/2$. Then $2\dim V \geqslant k+1$, thus for any element $e \in E$ one has $V \cap eV \neq 0$. This simple argument was communicated to the author by Alexander Vishik. $\square$

Proof of Theorem 9. Consider the field of rational functions $F(x)$ in a transcendental variable x. Let $D \subset F(x)^*$ be the multiplicative subgroup generated by polynomials of degree $\leqslant 1$. Let $R_* = \bigoplus_{n=0}^{\infty} R_n$ be the graded anti-commutative ring generated by $R_1 = D$ with relations $\{f, 1-f\} = 0$ for all $f,\ 1-f \in D$ and $\{f, -f\} = 0$ for all $f \in D$. Arguing as in [1, Theorem I.5.1], it is not hard to show that R_* is a free $K_*^{\mathrm{M}}(F)$-module with a basis consisting of 1 and $\{x-a\}$ for all $a \in F$. Hence the $K_*^{\mathrm{M}}(F)$-module $R_{\geqslant 1}$ is the direct sum of $K_{\geqslant 1}^{\mathrm{M}}(F)$ and a free module, so it is quadratic.

Now let us choose an element $t \in E$ such that $E = F[t]$. Let $\pi(x) \in F[x]$ be the irreducible equation of the element t. Obviously, there is a homomorphism $p_\pi\colon R_* \longrightarrow K_*^{\mathrm{M}}(E)$ assigning $\{f \bmod \pi\}$ to $\{f\}$ for any $f \in D$. According to Lemma 10, this homomorphism is surjective. Moreover, the ideal $J_* = \ker p_\pi \subset R_*$ is generated by its first-degree component J_1. This follows from the fact that for any $e \in E \setminus \{0,1\}$ one can find $f \in D \subset F(x)^*$ such that $1-f \in D$ and $\pi(f) = e$. Since R_* is anti-commutative, we have

$$J_* = R_* \cdot J_1 = (K_*^{\mathrm{M}}(F) + K_*^{\mathrm{M}}(F) \cdot R_1) \cdot J_1 = K_*^{\mathrm{M}}(F) \cdot (J_1 + R_1 J_1).$$

Therefore, the $K_*^{\mathrm{M}}(F)$-module J_* is generated by J_1 and J_2, while the module $R_{\geqslant 1}$ is quadratic. Thus the quotient module $K_{\geqslant 1}^{\mathrm{M}}(E) = R_{\geqslant 1}/J_*$ is also quadratic. $\square$

For reader's convenience, the statement of Bass–Tate lemma proper is formulated here, together with an improvement by Karim Becher [2].

Proposition 11. *Let E/F be a separable field extension of degree $k = \ell^s$, where ℓ is a prime number. Assume that either (a) $\ell = 2$, or (b) the field F has no finite extensions of degree different from powers of ℓ and less or equal to $k/2$, or (c) E/F is a tower of extensions of degree ℓ such that the largest proper subfield of E in this tower has no nontrivial finite extensions of degree $\leqslant \ell/2$. Then the Milnor ring $K_*^{\mathrm{M}}(E)$ is generated in degree $\leqslant s$ as a module over $K_*^{\mathrm{M}}(F)$.*

Proof. The case (a) is covered by the result of [2]. The case (b) follows from Lemma 10 and [1, Lemma I.5.2]. In the case (c) one argues by induction in s, applying (b) to extensions of degree ℓ. $\square$

From now on and for the rest of this section we will assume that the Milnor–Kato conjecture holds for all relevant fields, primes, and degrees. Under this assumption we will deduce corollaries from Proposition 7, Proposition 8, and Theorem 9.

Corollary 12. *Let ℓ be a prime number, m be a power of ℓ, and F be a field containing a primitive root of unity of degree m. Consider the ring $H^*(G_F, \mathbb{Z}/m)$. Let $u \in H^1(G_F, Z/m)$ be an element of additive order $k = \ell^s$. Assume that the* *maximal proper subfield of E over F has no nontrivial finite extensions of degree $\leqslant \ell/2$. Then the ideal $\mathrm{Ann}(u)$ in the ring $H^*(G_F, \mathbb{Z}/m)$ is generated by elements of degree less or equal to s. In particular, if $m = \ell$ is a prime and F has no nontrivial extensions of degree $\leqslant \ell/2$, then $\mathrm{Ann}(u)$ is generated in degree 1.*

Proof. Let E/F be the cyclic extension of degree k corresponding to the element u. According to Proposition 7, we have an exact sequence of $H^*(G_F, \mathbb{Z}/m)$-modules

$$H^*(G_E, \mathbb{Z}/m) \xrightarrow{\mathrm{cor}} H^*(G_F, \mathbb{Z}/m) \xrightarrow{u\,\cup} H^*(G_F, \mathbb{Z}/m).$$

But $H^*(G_E, \mathbb{Z}/m)$ is generated in degree $\leqslant s$ as a module over $H^*(G_F, \mathbb{Z}/m)$; this follows from the Milnor–Kato conjecture and Proposition 11. ☐

Corollary 13. *Let ℓ be a prime number, m and k be powers of ℓ, and F be a field containing a primitive root of unity of degree m. Let L/F be a cyclic extention of degree k. Consider the kernel J of the ring homomorphism $H^*(G_F, \mathbb{Z}/m) \longrightarrow H^*(G_L, \mathbb{Z}/m)$. Assume that the maximal proper subfield of E over F has no nontrivial finite extensions of degree $\leqslant \ell/2$. Then the ideal J in the ring $H^*(G_F, \mathbb{Z}/m)$ is generated by elements of degree less or equal to $s+1$, where $k/m = \ell^s$ if k is divisible by m and $s = 0$ if m is divisible by k.*

Proof. The case when k is divisible by m follows from Proposition 8 in the way analogous to the proof of Corollary 12. Namely, one has to use the exact sequence

$$H^n(G_E, \mathbb{Z}/m) \xrightarrow{\mathrm{cor}\,\circ\, u\,\cup} H^{n+1}(G_F, \mathbb{Z}/m) \xrightarrow{\mathrm{res}} H^{n+1}(G_L, \mathbb{Z}/m),$$

where $F \subset E \subset L$ is the intermediate extension of degree k/m over F and $u \in H^1(G_E, \mathbb{Z}/m)$ is the class of the extension L/E. The case when m is divisible by k follows directly from Proposition 7. ☐

The next corollary is the main result of this section.

Corollary 14. *Let ℓ be a prime number and F be a field containing a primitive root of unity of degree ℓ. Assume that F has no nontrivial finite extensions of degree $\leqslant \ell/2$ (note that for $\ell = 2$ or $\ell = 3$ this always holds). Then for any element $u \in H^1(G_F, \mathbb{Z}/\ell)$ the ideal $\mathrm{Ann}(u)$ in the cohomology ring $H^*(G_F, \mathbb{Z}/\ell)$ is a quadratic module over the this ring, i. e., it is isomorphic to a graded module with generators and relations, where generators are in degree 1 and relations in degree 2.*

Proof. Let E/F be the cyclic extension of degree ℓ corresponding to the class u and Σ be its Galois group. Consider the spectral sequence related to the maximal (ℓ-term) filtration of the G_F-module $\mathbb{Z}/\ell[\Sigma]$. It follows from the exact sequence

$$H^n(G_E, \mathbb{Z}/\ell) \xrightarrow{\mathrm{cor}} H^n(G_F, \mathbb{Z}/\ell) \xrightarrow{u\,\cup} H^{n+1}(G_F, \mathbb{Z}/\ell) \xrightarrow{\mathrm{res}} H^{n+1}(G_E, \mathbb{Z}/\ell)$$

that this spectral sequence degenerates at the term $E_2^{*,*}$. In other words, there is a filtration $V^1 \supset \cdots \supset V^\ell$ on the $H^*(G_F, \mathbb{Z}/\ell)$-module $H^*(G_E, \mathbb{Z}/\ell)$ with associated quotient modules of the form $V^1/V^2 \simeq \ker(u\cup)$, $V^i/V^{i+1} \simeq \ker(u\cup)/\operatorname{im}(u\cup)$ for $i = 2, \ldots, \ell-1$, and $V^\ell \simeq \operatorname{coker}(u\cup)$. From this filtration it follows that the $H^*(G_F, \mathbb{Z}/\ell)$-modules $H^{\geqslant 1}(G_E, \mathbb{Z}/\ell)$ and $\operatorname{Ann}(u)$ are quadratic simultaneously. (They are also simultaneously Koszul, see [8].) Now it remains to apply Theorem 9. Alternatively, one can argue as in the proof of Corollary 19 below. $\square$

Conjecture 15. *Let ℓ be a prime number and F be a field containing a primitive root of unity of degree ℓ. Then for any element $u \in H^1(G_F, \mathbb{Z}/\ell)$ the $H^*(G_F, \mathbb{Z}/\ell)$-module $\operatorname{Ann}(u) \subset H^*(G_F, \mathbb{Z}/\ell)$ is Koszul. For any cyclic extension E/F of degree ℓ, the $H^*(G_F, \mathbb{Z}/\ell)$-module $H^{\geqslant 1}(G_E, \mathbb{Z}/\ell)$ is Koszul (see [8] for the definition).*

5. Biquadratic and Dihedral Field Extensions

Using Theorem 6 and assuming the Milnor–Kato conjecture, one can construct some exact sequences of Galois cohomology for any finite field extension whose Galois group admits a "nontrivial enough" exact quadruple of permutational representations over it. Unfortunately, examples of finite groups with such exact quadruples of representations that I am aware of are very few. Almost all of them are dihedral groups and their subgroups. The latter include cyclic groups and the biquadratic group $\mathbb{Z}/2 \times \mathbb{Z}/2$. The goal of this section is to construct those exact quadruples and deduce some corollaries, including the conjectures of Merkurjev–Tignol [7] and Kahn [4] about biquadratic field extensions. Throughout this section we will assume that the Milnor–Kato conjecture holds for $\ell = 2$ and the characteristic of our fields is not equal to 2. We will sometimes use the notation $H^i(F) = H^i(G_F, \mathbb{Z}/2)$.

Let $\Delta = \Delta_k$ be a dihedron of order k, i. e., a regular polygon with k vertices and k edges. We will denote by Δ' the set of all vertices of Δ and by Δ'' the set of all its edges. Let $\Gamma = \Gamma_k$ be the group of all automorphisms (symmetries) of Δ and $\Sigma \subset \Gamma$ be the subgroup of orientation-preserving automorphisms (rotations). Then Σ is a cyclic group of order k and a normal subgroup of order 2 in Γ.

Assume that k is divisible by 4. Let Π be the (only) subgroup of order 2 in Σ. Then the following quadruple of permutational representations of Γ is exact

$$(Q_\Gamma) \qquad \mathbb{Z} \longrightarrow \mathbb{Z}[\Delta'] \oplus \mathbb{Z} \longrightarrow \mathbb{Z}[\Delta''] \oplus \mathbb{Z}[\Delta'/\Pi] \longrightarrow \mathbb{Z}[\Delta''/\Pi],$$

where the arrows are defined by the formulas below. Choose an arbitrary generator $\sigma \in \Sigma$; let $\bar\sigma$ be its image in Σ/Π. Further, let $\sigma^{\pm 1/2}$ and $\bar\sigma^{\pm 1/2}$ be the uniquely defined maps $\Delta' \longrightarrow \Delta'' \longrightarrow \Delta'$ and $\Delta'/\Pi \longrightarrow \Delta''/\Pi \longrightarrow \Delta'/\Pi$ whose squares are $\sigma^{\pm 1}$ and $\bar\sigma^{\pm 1}$, respectively. Denote by pr_Π the projection maps modulo Π and by $\#X$ the sum of all elements of a set X. Then the first map in this sequence is $(\#\Delta', -2)$, the third one is $(\mathrm{pr}_\Pi,\ -\bar\sigma^{-1/2}-\bar\sigma^{1/2})$, and the middle arrow is given by the matrix U with components $U_{11}=\sigma^{-1/2}+\sigma^{1/2}$, $U_{12}=\#\Delta''$, $U_{21}=\mathrm{pr}_\Pi$, and $U_{22}=\#\Delta'/\Pi$.

Moreover, there exists a chain homotopy h such that $dh+hd=2$. Of the three maps constituting h, the leftmost one is given by the pair $(\mathrm{pr}_1,\ -k/2-1)$, where $\mathrm{pr}_1\colon \mathbb{Z}[X]\to\mathbb{Z}$ sends every $x\in X$ to 1. To define the remaining two maps, one needs some preparatory work. Let $f(x)$ be a Laurent polynomial solving the equation $(x^{-1/2}+x^{1/2})^2 f(x)=1+\sum_{i=-k/2+1}^{k/2-1}x^i$. Set $\psi=(\sigma^{-1/2}+\sigma^{1/2})f(\sigma)\in\sigma^{1/2}\mathbb{Z}[\Sigma]$ and $\bar\psi=\psi \bmod \Pi\in\bar\sigma^{1/2}\mathbb{Z}[\Sigma/\Pi]$. The rightmost piece of h is equal to $(1+\pi,\ \bar\sigma^{1/2}\#\Sigma/\Pi-\bar\psi)$, where π is the only nontrivial element of Π. The middle arrow is given by the matrix H with components $H_{11}=\psi$, $H_{12}=1+\pi$, $H_{21}=\mathrm{pr}_1$, and $H_{22}=0$.

Further useful exact quadruples can be obtained by restricting Q_Γ to a dihedral subgroup of index 2. The group $\Gamma_{k/2}$ can be embedded into Γ_k in two ways; namely, under the first embedding the action of $\Gamma_{k/2}$ on Δ_k' is transitive, while under the second embedding the action of $G_{k/2}$ on Δ_k'' is. These embeddings correspond to the two essentially different ways of defining a regular polygon with $k/2$ vertices in terms of the given polygon Δ_k: one can make edges of the new polygon out of every second edge of the original one, or one can take every second vertice of the original polygon to be the new polygon's vertices. Taking the restriction of Q_Γ with respect to the first of these emdeddings, we obtain an exact quadruple of $\Gamma_{k/2}$-modules

$$(Q_\Gamma^+)\quad \mathbb{Z}\longrightarrow\mathbb{Z}[\Delta^+]\oplus\mathbb{Z}\longrightarrow\mathbb{Z}[\Delta'']\oplus\mathbb{Z}[\Delta'']\oplus[\Delta^+/\Pi]\longrightarrow\mathbb{Z}[\Delta'/\Pi]\oplus\mathbb{Z}[\Delta''/\Pi],$$

where Δ' and Δ'' denote the sets of all vertices and edges of the regular polygon $\Delta_{k/2}$, while Δ^+ denotes the principal homogeneous space for the dihedral group $\Gamma_{k/2}$ which is defined as the set of all pairs (an edge of $\Delta_{k/2}$; one of its two vertices).

Now let M/F be an extension of fields with a dihedral Galois group Γ. Then the category of intermediate field extensions K/F embeddable into M is equivalent to the category of sets endowed with a transitive action of Γ. Let L' and L'' be the intermediate fields corresponding to the Γ-sets Δ' and Δ'', let K' and K'' be the fields corresponding to Δ'/Π and Δ''/Π, and $E\supset F$ be the normal extension of F corresponding to the subgroup $\Pi\subset\Gamma$.

Proposition 16. *For any dihedral field extension M/F of degree $[M\colon F]$ divisible by 8, there is an exact sequence of Galois cohomology of the form*

$$H^n(L'')\oplus H^n(K')\xrightarrow{(\mathrm{cor}_{L''/K''},\ \mathrm{cor}_{E/K''}\circ\mathrm{res}_{E/K'})}H^n(K'')\xrightarrow{\mathrm{cor}_{K''/F}\circ\, u_{L''/K''}\cup}H^{n+1}(F)$$
$$\xrightarrow{\mathrm{res}_{L'/F}}H^{n+1}(L')\xrightarrow{(\mathrm{cor}_{M/L''}\circ\mathrm{res}_{M/L'},\ \mathrm{cor}_{L'/K'})}H^{n+1}(L'')\oplus H^{n+1}(K').$$

For any dihedral extension M/F of degree divisible by 4, there is an exact sequence

$$H^n(L')\oplus H^n(L'')\oplus H^n(E) \xrightarrow{\operatorname{cor}^4} H^n(K')\oplus H^n(K'') \xrightarrow{\operatorname{cor}_{K(i)/F}\circ\, u_{L(i)/K(i)}\cup} H^{n+1}(F)$$
$$\xrightarrow{\operatorname{res}} H^{n+1}(M) \xrightarrow{\operatorname{cor}^3} H^{n+1}(L')\oplus H^{n+1}(L'')\oplus H^{n+1}(E).$$

Proof. The proposition follows from Theorem 6 applied to the above exact quadruples Q_Γ and Q_Γ^+, respectively. There are also dual exact sequences of cohomology, corresponding to the dual exact quadruples $\operatorname{Hom}_{\mathbb{Z}}(Q_\Gamma, \mathbb{Z})$ and $\operatorname{Hom}_{\mathbb{Z}}(Q_\Gamma^+, \mathbb{Z})$, but we will not write them down here. $\square$

Remark. There is yet another exact quadruple of permutational representations of a dihedral group Γ, whose restrictions to the subgroup of rotations and dihedral subgroups of index 2 are also of some interest. Let Δ_k be the dihedron of an arbitrary order k and $\Pi\subset\Sigma\subset\Gamma_k$ be a cyclic subgroup of order m. Then there is a self-dual exact quadruple of the form

$$\mathbb{Z}[\Delta'/\Pi] \longrightarrow \mathbb{Z}[\Delta']\oplus\mathbb{Z} \longrightarrow \mathbb{Z}[\Delta'']\oplus\mathbb{Z} \longrightarrow \mathbb{Z}[\Delta''/\Pi]$$

if k/m is even (and one should replace Δ'' with Δ' if k/m is odd). The first map in this sequence is $(\#\Pi, -\operatorname{pr}_1)$, the third map is $(\operatorname{pr}_\Pi,\ -\#\Delta''/\Pi)$, and the middle arrow is given by the matrix U with components $U_{11}=\sigma^{-(k/m-1)/2}+\dots+\sigma^{(k/m-1)/2}$, $U_{12}=\#\Delta''$, $U_{21}=\operatorname{pr}_1$, and $U_{22}=m$ in the above notation. It is not difficult to find a homotopy map h with $dh+hd=m$.

Let $\Theta=\{1,a,b,c\}$ denote an abelian group isomorphic to $\mathbb{Z}/2\times\mathbb{Z}/2$. The group Θ can be embedded into Γ_4 in two ways: as above, under the first embedding the action of Θ on Δ' is transitive, while under the second embedding the action of Θ on Δ'' is. Taking the restrictions on Θ of the exact quadruple Q_Γ for $\Gamma=\Gamma_4$, we obtain (after one simple cancellation in the second case) two exact quadruples of permutational representations of Θ. They have the form

$$(Q_\Theta)\qquad \mathbb{Z} \longrightarrow \mathbb{Z}[\Theta]\oplus\mathbb{Z} \longrightarrow \mathbb{Z}[\Theta/a]\oplus\mathbb{Z}[\Theta/b]\oplus\mathbb{Z}[\Theta/c] \longrightarrow \mathbb{Z}^{\oplus 3}/\mathbb{Z}$$

and

$$\mathbb{Z} \longrightarrow \mathbb{Z}[\Theta/a]\oplus\mathbb{Z}[\Theta/b] \longrightarrow \mathbb{Z}[\Theta]\oplus\mathbb{Z} \longrightarrow \mathbb{Z}[\Theta/c],$$

where we denote for simplicity by a the subgroup $\{1,a\}$ etc. All maps in these sequences can be defined directly in the rather obvious way.

We are interested in the exact sequence of cohomology corresponding to the first of these quadruples. Let L/F be a biquadratic field extension with Galois group Θ. We will consider Θ as a two-dimensional vector space over the field $\mathbb{Z}/2$. Notice that there is a canonical isomorphism between Θ and the dual vector space Θ^*, given by the only bilinear form on Θ with the property that $(\theta,\theta)=0$ for all $\theta\in\Theta$. The three intermediate fields $F\subset K_\theta\subset L$ bijectively correspond to nonzero elements a, b, c

of the group Θ in a natural way. The six-term exact sequence of Galois cohomology corresponding to the exact quadruple Q_Θ has the form

$$H^n(L)\oplus H^n(F)^{\oplus 3} \xrightarrow{(\mathrm{cor},\,\mathrm{res}^3)} \bigoplus\nolimits_{\theta=a,b,c} H^n(K_\theta) \xrightarrow{\mathrm{cor}^3} \Theta\otimes_{\mathbb{Z}/2} H^n(F)$$
$$\xrightarrow{\cup} H^{n+1}(F) \xrightarrow{\mathrm{res}} H^{n+1}(L) \xrightarrow{\mathrm{cor}^3} \bigoplus\nolimits_{\theta=a,b,c} H^{n+1}(K_\theta),$$

where the middle arrow $\Theta\otimes H^n(F)\longrightarrow H^{n+1}(F)$ is defined in terms of the embedding $\Theta\simeq \mathrm{Hom}(\Theta,\mathbb{Z}/2)\longrightarrow \mathrm{Hom}(G_F,\mathbb{Z}/2)\simeq H^1(F)$. This 6-term exact sequence is a part of one of the 7-term exact sequences of Merkurjev–Tignol and one of the 8-term exact sequences of Kahn [7, 4] for a biquadratic extension of fields.

Corollary 17. *Both 8-term sequences of Bruno Kahn* [4] *for Galois cohomology in a biquadratic field extension L/F are exact, provided that the first Bockstein homomorphism $H^n(E,\mathbb{Z}/2)\longrightarrow H^{n+1}(E,\mathbb{Z}/2)$ vanishes in the relevant degree n for the five fields E between F and L (namely, F, L, and all three intermediate fields).*

Proof. The middle 6-term part of the first of Kahn's 8-term sequences is written down right above; its exactness follows from Theorem 6 applied to the exact quadruple Q_Θ tensored with $\mu_4^{\otimes n}$. The middle part of the second sequence can be obtained from the dual exact quadruple $\mathrm{Hom}_{\mathbb{Z}}(Q_\Theta,\mathbb{Z})$. Exactness at the remaining terms follows from exactness at the middle terms due to Merkurjev–Tignol and Kahn's results. ☐

Corollary 18. *Let L/F be a field extension of degree 4 and M/F be its Galois closure. Suppose that the degree $[M:F]$ is a power of 2. Then the kernel J of the restriction map $H^*(G_F,\mathbb{Z}/2)\longrightarrow H^*(G_L,\mathbb{Z}/2)$ is generated in degrees 1 and 2 as an ideal in $H^*(G_F,\mathbb{Z}/2)$. Moreover, the kernel of the restriction map $H^*(G_F,\mathbb{Z}/2)\longrightarrow H^*(G_M,\mathbb{Z}/2)$ is also generated in degrees 1 and 2.*

Proof. There are only three cases: either L/F is a cyclic extension, or a biquadratic one, or it has the form L'/F for a dihedral extension M/F with Galois group Γ_4. The first case follows from Corollary 13, the second from Corollary 17, and the third from Proposition 16 (both statements). Note that in the biquadratic case the ideal J is actually generated by a two-dimensional subspace in $H^1(G_F,\mathbb{Z}/2)$. ☐

Corollary 19. *For any field F and any two-dimensional subspace $\Theta\subset H^1(G_F,\mathbb{Z}/2)$ the kernel of the multiplication map $\Theta\otimes H^*(G_F,\mathbb{Z}/2)\longrightarrow H^{*+1}(G_F,\mathbb{Z}/2)$ is a quadratic module over the algebra $H^*(G_F,\mathbb{Z}/2)$.*

Proof. Clearly, any two-dimensional subspace in $H^1(F)$ corresponds to a biquadratic field extension L/F, so we can apply the 6-term exact sequence of Corollary 17. The kernel in question is isomorphic to the quotient module of $\bigoplus_\theta H^{\geqslant 1}(K_\theta)$ by the image of the module $H^{\geqslant 1}(L)\oplus H^{\geqslant 1}(F)^{\oplus 3}$. Since the first module is quadratic (by

Theorem 9) and the second module is generated in degree 1 and 2 (by Proposition 11), the quotient module is quadratic. □

Conjecture 20. *For any field F, the ideal generated by any two-dimensional subspace $\Theta \subset H^1(G_F, \mathbb{Z}/2)$ in the cohomology algebra $H^*(G_F, \mathbb{Z}/2)$ is a Koszul module (see* [8]*) over that algebra.*

Remark. It is possible to extend the first statement of Corollary 18 to arbitrary field extensions of degree 4 using the following exact quadruple of permutational representations of the symmetric group $\mathbb{S}_4$

$$\mathbb{Z} \longrightarrow \mathbb{Z}[X_4] \oplus \mathbb{Z} \longrightarrow \mathbb{Z}[X_6] \oplus \mathbb{Z} \longrightarrow \mathbb{Z}[X_3],$$

where X_4 is a four-element set on which $\mathbb{S}_4$ acts in the standard way, X_6 is the set of all two-element subsets of X_4, and X_3 is the quotient of X_6 modulo the involution $*$ sending a subset to its complement. The first map in this sequence is $(\#X_4, -2)$, the third one sends a two-element subset to its class modulo $*$ and 1 to $-\#X_3$, and the middle arrow is given by the matrix U with component maps $U_{11}\colon \mathbb{Z}[X_4] \longrightarrow \mathbb{Z}[X_6]$ sending each element of X_4 to the sum of three two-element subsets containing it, $U_{12} = \mathrm{pr}_1$, $U_{21} = \#X_6$, and $U_{22} = 2$. It is easy to construct a homotopy map h with $dh + hd = 2$. In fact, one can generalize the 6-term biquadratic exact sequences to arbitrary field extensions of degree 4 using this exact quadruple!

References

[1] H. Bass, J. Tate. The Milnor ring of a global field. In *K-theory II*, *Lecture Notes in Math.* **342**, p. 349–446, 1973.

[2] K. J. Becher. Milnor K-groups and finite field extensions. Preprint, July 2002.

[3] S. Bloch, K. Kato. P-adic étale cohomology. *Publ. Math. IHÉS* **63**, p. 107–152, 1986.

[4] B. Kahn. On the cohomology of biquadratic extensions. *Comment. Math. Helvetici* **69**, p. 120–136, 1994.

[5] K. Kato. Galois cohomology of complete discrete valuation fields. In *Algebraic K-theory, Part II (Oberwolfach, 1980)*, *Lecture Notes in Math.* **967**, p. 215–238, 1982.

[6] J. Milnor. Algebraic K-theory and quadratic forms. *Inventiones Math.* **9**, p. 318–344, 1970.

[7] A. S. Merkurjev, J.-P. Tignol. Galois cohomology of biquadratic extensions. *Comment. Math. Helvetici* **68**, p. 138-169, 1993.

[8] L. Positselski. Koszul property and Bogomolov's conjecture. Preprint, *K-theory electronic preprint archives*, http://www.math.uiuc.edu/K-theory/0296 , August 1998.

[9] A. Suslin. Algebraic K-theory and the norm residue homomorphism. *Journ. Soviet Math.* **30**, p. 2556–2611, 1985.

[10] V. Voevodsky. The Milnor conjecture. Preprint, December 1996.

Independent University of Moscow and MPI für Mathematik, Bonn
E-mail address: posic@mccme.ru, posic@mpim-bonn.mpg.de