THE BLOCH-KATO CONJECTURE AND GALOIS THEORY

DIKRAN KARAGUEUZIAN, JOHN LABUTE, AND JÁN MINÁČ

To Paulo Ribenboim who showed us the Galois road

Abstract. We investigate the relations in Galois groups of maximal p-extensions of fields, the structure of their natural filtrations, and their relationship with the Bloch-Kato conjecture proved by Rost and Voevodsky with Weibel's patch. Our main focus is on the third degree, but we provide examples for all degrees.

1. Introduction

Let p be a fixed prime number and let F be a field such that F contains a primitive p-th root of unity ζ_p. Let F_s be the separable closure of F and $\mathrm{Gal}(F_s/F)$ be the absolute Galois group of F. Let $H^*(F) = H^*(\mathrm{Gal}(F_s/F), \mathbb{Z}/p\mathbb{Z})$ be the Galois cohomology of F in coefficients $\mathbb{Z}/p\mathbb{Z}$. (From now on we shall omit the coefficients of our cohomology groups as they will always be $\mathbb{Z}/p\mathbb{Z}$.) In [Mi], Milnor defined the group K_nF by generators and relations for any $n \in \mathbb{N} \cup \{0\}$. The generators are n-tuples $\{a_1, \ldots, a_n\}$ of elements of F^*, and the defining relations are the multiplicativity in each component and the Steinberg relation $\{a_1, \ldots, a_n\} = 0$ if $a_i + a_j = 1$ for some $i \neq j$. Set $k_nF = K_nF/pK_nF$ and $k_*F = \bigoplus_{n\geq 0} k_nF$. Thus k_*F is the Milnor K-theory of F modulo p. In the same paper Milnor defined a graded homomorphism $h_* : k_*F \to H^*(F)$ and implicitly conjectured that it is an isomorphism when $p = 2$. Because of the later important work of Bloch and Kato for any prime p, the general case is now known as the Bloch-Kato conjecture.

Let $F(p)$ be the maximal p-extension of F. This means that $F(p)$ is a union of Galois extensions K/F, such that $\mathrm{Gal}(K/F)$ is a p-group, in a fixed F_s of F. Let G be the Galois group of $F(p)/F$. Observe that $\inf : H^1(G) \to H^1(F)$ is an isomorphism and the Steinberg

Date: October 11, 2009.

The second and third authors are partially supported by NSERC grants.

relations hold in $H^2(G)$. Then $h_* : k_*F \to H^*(F)$ factors through $h_* : k_*F \to H^*(G)$. A simple application of the Hochschild-Serre spectral sequence shows that if $h_n : k_nF \to H^n(F)$ is isomorphic for all fields F then $h_n : k_nF \to H^n(G)$ is an isomorphism for all fields F. Also see [G-M, page 97, for the case $p = 2$]. In the paper [M-S], Merkurjev and Suslin proved that h_2 is an isomorphism. Recently Rost and Voevodsky, with Weibel's patch, proved that h_n is an isomorphism for all $n \in \mathbb{N}$. (See [Ha-W], [Ro1], [Ro2], [Voe1], [Voe2], [Voe3], and [Wei1], [Wei2].) The cohomology of Galois groups of maximal pro-p-extensions of fields reflects some properties that the class of these groups share. The relationship between the structure of groups and their cohomology groups is in general nontrivial and it is quite mysterious. We are interested in the group theoretic meaning of the Bloch-Kato conjecture.

We investigate some strong, and at the same time simple conditions on the relations of $\mathrm{Gal}(F(p)/F)$ for any field F which is closely related to the Bloch-Kato conjecture. These conditions say that all relations of $G = \mathrm{Gal}(F(p)/F)$ are generated by relations of small weight. This will be made more precise in section 4. For related work on the structure of $\mathrm{Gal}(F(p)/F)$ and its relations with cohomology, see [A-K-M], [J-W], [Ko1], [Ko2], [Mi-Sp1] and [N-S-W].

Let $\{\sigma_i\}_{i\in I}$ be a minimal set of generators of G. (See [Ko1, Chapter 4].) We assume that I is well ordered. Let S be a free pro-p-group with a minimal set of generators $\{s_i\}_{i\in I}$. By sending s_i to σ_i we obtain a continuous homomorphism $\pi : S \to G$. We set $R = Ker(\pi)$.

For a pro-p-group G, we define $G^{(n+1)} = (G^{(n)})^p[G^{(n)}, G]$ and $G^{(1)} = G$. Then $G^{(n)}$ is a closed normal subgroup of G. We denote the quotient by $G^{[n]}$. We set $R^{(1,S)} = R$ and $R^{(n+1,S)} = (R^{(n,S)})^p[R^{(n,S)}, S]$ for $n \geq 1$. Since S and G have the same cardinality of the minimal set of generators, then $R \subset S^{(2)}$. In general, we see by induction on n that $R^{(n,S)} \subset R \cap S^{(n+1)}$. Lemma 3.2 says that if h_2 is surjective, then $R^{(2,S)} = R \cap S^{(3)}$.

Example A. The equality $R^{(2,S)} = R \cap S^{(3)}$ implies that every $\sigma \in G = \mathrm{Gal}(F(p)/F)$ of finite order $\neq 1$ has order p as follows. Suppose that σ has order $\geq p^2$. The subgroup of G generated by σ is a closed subgroup of G and if L is its fixed field, we have $L(p) = F(p)$ and $\mathrm{Gal}(L(p)/L) = \langle\sigma\rangle$. Hence we may assume that $F = L$ and $G = \langle\sigma\rangle$. Moreover by taking a suitable power of σ we may assume that σ has an order p^2. Then $\sigma^{p^2} \in R \cap S^{(3)}$ but $\sigma^{p^2} \notin R^{(2,S)}$ as σ^{p^2} generates R as a normal subgroup of S. Hence the order of σ is p. This fact also

follows from the work of Becker [Be] where he also shows that $p = 2$ and that two elements of G order 2 cannot commute. In fact the only non-trivial finite subgroup of G is the cyclic group of order 2.

Example B. (See [Ch-E-M, Section 9] for more examples.) One can also deduce from the equality $R^{(2,S)} = R \cap S^{(3)}$ that a minimal se of relations among the σ_i cannot contain a relation of the form $[[\sigma_1, \sigma_2], \sigma_3]$ with $\sigma_1, \sigma_2, \sigma_3$ distinct. Indeed, such a relator would be in $R \cap S^{(3)}$ but not in $R^p[R, S] = R^{(2,S)}$.

Our first result is

Theorem 1.1. *Assume that G is $G_F(p)$ for some field F containing a primitive pth-root of 1. Then $R^{(3,S)} = R \cap S^{(4)}$.*

Theorem 1.1 is proved in section 3. It is natural to ask the following question.

Question 1.2. *Let G be isomorphic to a Galois group of a maximal p-extension of a field. Under which condition is $R^{(n,S)} = R \cap S^{(n+1)}$ for all $n \geq 1$?*

More generally we ask:

Question 1.3. *Let G be isomorphic to the Galois group of the maximal p-extension of a field. Describe the quotients $R \cap S^{(n+1)}/R^{(n,S)}$ for all $n \geq 1$.*

In the first two sections we show that $R^{(n,S)} = R \cap S^{(n+1)}$ for $n \leq 3$. In section 4, we give an equivalent description of Question 1.2 in the language of Lie algebras. We prove that, for quadratically defined pro-2-groups as well as for $G = \mathrm{Gal}(F(2)/F)$ when F is a totally imaginary number field, the relation $R^{(n,S)} = R \cap S^{(n+1)}$ is valid for each $n \geq 1$. For all odd primes p we show the same holds for $G = \mathrm{Gal}(F(p)/F)$ where F is any local or global field.

2. Preliminaries

We use the following usual notation: $[a]$ means both an element of F^*/F^{*p} and its corresponding element (a) in $H^1(F)$ or more generally in $H^1(\mathrm{Gal}(T/F))$ where T/F is any Galois extension of F which contains $F^{(2)}$: $=$ compositum of all cyclic extensions of degree p of F, and

is a subfield of $F(p)$. Observe that by Kummer theory we have the canonical isomorphism $F^*/F^{*p} \to H^1(\mathrm{Gal}(T/F))$, which justifies our identification mentioned above.

We will work in the category of pro-p-groups and make the usual conventions that by "subgroup" we mean "closed subgroup", by "generated" we mean "topologically generated" and by "morphism" we mean "continuous morphism". We shall always work with $\mod p$ cohomology except when we explicitly mention other coefficients. For the standard facts for Galois cohomology we refer to [Se2] and [N-S-W].

For an extension $1 \to A \to B \to C \to 1$ of profinite groups and a discrete B-module M we have the corresponding Lyndon-Hochschild-Serre (LHS, for short) spectral sequences $\{E_r^{p,q}, d_r^{p,q}\}$ where $E_2^{p,q} = H^p(C, H^q(A, M))$ ([H-S] and [N-S-W]). Using LHS we also have the five-term exact sequence

$$0 \to H^1(C, M^A) \xrightarrow{\inf} H^1(B, M) \xrightarrow{\mathrm{res}} H^1(A, M)^C \xrightarrow{d_2^{0,1}} H^2(C, M^A) \xrightarrow{\inf} H^2(B, M)$$

where inf is the inflation map and res is the restriction map.

Observe that k_nF is isomorphic to the factor group of

$$F^*/F^{*p} \otimes \cdots \otimes F^*/F^{*p}$$

by the subgroup generated by $[a_1] \otimes \cdots \otimes [a_n]$ where a_1 is a norm in the extension $F(\sqrt[p]{a_j})/F$ of degree p, for some $j = 2, \ldots, n$. (If $F(\sqrt[p]{a_j})/F$ is not an extension of degree p, then $[a_j] = [1]$ and $[a_1] \otimes \cdots \otimes [a_n] = 0$.)

Indeed let l_nF be this factor group. Because all relations in l_nF are valid in k_nF, we see that k_nF is a naturally homomorphic image of l_nF. (See [F-V, page 303, Exercise 6].) In order to show that this homomorphism is actually an isomorphism, it is enough to show that the Steinberg relations which generate the relations in k_nF are valid in l_nF also. Let $a_1, \ldots, a_n \in F^*$. We denote as $\langle a_1, \ldots, a_n \rangle$ the image of $[a_1] \otimes \cdots \otimes [a_n], [a_i] \in F^*/F^{*p}$ in l_nF.

We want to show that if $1 = a_i + a_j, 1 \leq i < j \leq n$, then

$$\langle a_1, \ldots, a_n \rangle = 0 \text{ in } l_nF.$$

Because this is trivially true if $a_j \in F^{*p}$ we shall assume that $a_j \notin F^{*p}$. If $i = 1$ then this is true by our definition of the relations in l_nF as

$$\begin{aligned} 1 - a_j &= \prod_{i=0}^{p-1}(1 - \zeta_p^i \sqrt[p]{a_j}) \\ &= N_{F(\sqrt[p]{a_j})/F}(1 - \sqrt[p]{a_j}). \end{aligned}$$

Hence it is enough to show that if

$$1 < i < j \leq n$$

then

$$\langle a_1, \dots, a_i, \dots, a_j, \dots, a_n\rangle = -\langle a_i, \dots, a_1, \dots, a_j, \dots, a_n\rangle.$$

However using the equation

$$-a = (1 - a)/(1 - a^{-1}) \text{ for } a \neq 1,$$

we see that

$$\langle a, \dots, -a, \dots\rangle = 0 \text{ in } l_nF \text{ for all } a \in F^*.$$

Hence

$$\begin{aligned} 0 &= \langle a_1a_i, \dots, -a_1a_i, \dots a_n\rangle \\ &= \langle a_1, \dots, -a_1, \dots\rangle + \langle a_1, \dots, a_i, \dots\rangle + \\ &\langle a_i, \dots, a_1, \dots\rangle + \langle a_i, \dots, -a_i, \dots\rangle \\ &= \langle a_1, \dots, a_i, \dots\rangle + \langle a_i, \dots, a_1, \dots\rangle, \end{aligned}$$

as required.

Hence $l_nF = k_nF$.

3. The proof of Theorem 1.1

We divide our proof into several lemmas. Lemma 3.5 shows that it is enough to prove that $\inf : H^2(S^{[3]}) \to H^2(S/R^{(2,S)})$ is surjective. This is proved by considering certain spectral sequences below.

Lemma 3.1. $R^{(n,S)} \subset R \cap S^{(n+1)}$.

Proof. Our inclusion is true if $n = 1$. Assume that it is true for $k \leq n$. Then $R^{(n+1,S)} = (R^{(n,S)})^p[R^{(n,S)}, S] \subset (S^{(n+1)})^p[S^{(n+1)}, S] = S^{(n+2)}$. So $R^{(n+1,S)} \subset R \cap S^{(n+2)}$. □

Lemma 3.2 below was observed in [Wür, page 102] under an additional hypothesis, and in [Mi-Sp2, page 57] for the case $p = 2$. This lemma was also generalized in [G-M, page 207] in the case $p = 2$ and in [Ch-E-M] for all p.

Lemma 3.2. *If h_2 is surjective then $R^p[R, S] = R^{(2,S)} = R \cap S^{(3)}$.*

We consider the following pair of extensions

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R^{(2,S)} & \longrightarrow & S & \longrightarrow & S/R^{(2,S)} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & S^{(3)} & \longrightarrow & S & \longrightarrow & S^{[3]} & \longrightarrow & 1\,. \end{array} \tag{3.3}$$

By applying the five-term exact sequence to (3.3), we obtain a commutative diagram

$$\begin{array}{ccc} H^1(R^{(2,S)})^{S/R^{(2,S)}} & \xrightarrow{\cong} & H^2(S/R^{(2,S)}) \\ \uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{inf}} \\ H^1(S^{(3)})^{S^{[3]}} & \xrightarrow{\cong} & H^2(S^{[3]})\,. \end{array} \tag{3.4}$$

The surjectivities of both isomorphisms follow from the fact that $H^2(S) = 0$, because S is a free pro-p-group. The injectivities follow from the fact that $H^1(S/R^{(2,S)}) \cong H^1(S)$ and $H^1(S^{[3]}) \cong H^1(S)$, since both $R^{(2,S)}$ and $S^{(3)}$ are normal subgroups of $S^{(2)}$.

Observe that $H^1(S^{(3)}/S^{(4)}) \cong H^1(S^{(3)})^{S^{[3]}}$ and $H^1(R^{(2,S)}/R^{(3,S)}) \cong H^1(R^{(2,S)})^{S/R^{(2,S)}}$. The restriction $H^1(S^{(3)}/S^{(4)}) \to H^1(R^{(2,S)}/R^{(3,S)})$ is given by the composite

$$H^1(S^{(3)}/S^{(4)}) \xrightarrow{\mathrm{res}} H^1(R^{(2,S)}S^{(4)}/S^{(4)}) \xrightarrow{\cong} H^1(R^{(2,S)}/R^{(2,S)} \cap S^{(4)})$$
$$\xrightarrow{\mathrm{inf}} H^1(R^{(2,S)}/R^{(3,S)})\,.$$

The restriction $H^1(S^{(3)}/S^{(4)}) \to H^1(R^{(2,S)}S^{(4)}/S^{(4)})$ is surjective. If $R^{(2,S)} = R \cap S^{(3)}$, then $R^{(2,S)} \cap S^{(4)} = (R \cap S^{(4)}) = R \cap S^{(4)}$. Then $R^{(3,S)} = R \cap S^{(4)}$ iff $R^{(3,S)} = R^{(2,S)} \cap S^{(4)}$. Also the last inflation map is surjective iff $R^{(2,S)} \cap S^{(4)} = R^{(3,S)}$. Thus the last map inf : $H^1(R^{(2,S)}/R^{(2,S)} \cap S^{(4)} \to H^1(R^{(2,S)}/R^{(3,S)})$ is surjective iff $R^{(3,S)} = R \cap S^{(4)}$. Therefore we obtain

Lemma 3.5. *Assume that $R^{(2,S)} = R \cap S^{(3)}$. The following are equivalent*

(1) $R^{(3,S)} = R \cap S^{(4)}$.
(2) $R^{(3,S)} = R^{(2,S)} \cap S^{(4)}$.
(3) $\inf : H^1(R^{(2,S)}/R^{(2,S)} \cap S^{(4)}) \to H^1(R^{(2,S)}/R^{(3,S)})$ *is surjective.*
(4) $\mathrm{res} : H^1(S^{(3)}/S^{(4)}) \to H^1(R^{(2,S)}/R^{(3,S)})$ *is surjective.*
(5) $\inf : H^2(S^{[3]}) \to H^2(S/R^{(2,S)})$ *is surjective.*

We have a pair of extensions

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R/R^{(2,S)} & \longrightarrow & S/R^{(2,S)} & \longrightarrow & S/R = G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & S^{(2)}/S^{(3)} & \longrightarrow & S^{[3]} & \longrightarrow & S^{[2]} & \longrightarrow & 1\,. \end{array} \tag{3.6}$$

To prove (5) in Lemma 3.5 we can compare the LHS spectral sequences corresponding to (3.6). We set $E_r^{p,q}(S^{[3]})$ (or $E_r^{p,q}(S/R^{(2,S)})$) the $E_r^{p,q}-$term corresponding to the bottom extension (or the top extension).

Observe that $H^1(R/R^{(2,S)}) \cong H^1(R)^G$ and $H^1(R)^G \cong H^2(G)$, the last isomorphism follows from the five-term exact sequence corresponding to the extension $1 \to R \to S \to G \to 1$. Then $H^1(R/R^{(2,S)})^G = H^1(R/R^{(2,S)}) \cong H^2(G)$. Similarly we have $H^1(S^{(2)}/S^{(3)}) \cong H^2(S^{[2]})$. Therefore the transgression maps $d_2^{0,1}$ in both spectral sequences are surjective. Thus we obtain

Lemma 3.7. $E_\infty^{2,0}(S^{[3]}) = E_\infty^{2,0}(S/R^{(2,S)}) = 0$.

To prove the surjectivity of $\inf : H^2(S^{[3]}) \to H^2(S/R^{(2,S)})$, it is enough to show the surjectivities of the homomorphism corresponding to $E_\infty^{1,1}$-terms and the homomorphism corresponding to $E_\infty^{0,2}$-terms.

Assume that $R^{(2,S)} = R \cap S^{(3)}$. Observe that

$$H^1(R/R^{(2,S)}) = H^1(R/R \cap S^{(3)}) \cong H^1(RS^{(3)}/S^{(3)})\,.$$

Thus we obtain

Lemma 3.8. $\mathrm{res}\colon H^1(S^{(2)}/S^{(3)}) \to H^1(R/R^{(2,S)})$ *is surjective.*

Since both extensions in 3.6 are central extensions, then $E_2^{0,2}(S^{[3]}) \cong H^2(S^{(2)}/S^{(3)})$ and $E_2^{0,2}(S/R^{(2,S)}) \cong H^2(R/R^{(2,S)})$. Let $\{z_c\}_{c\in C}$ be a basis for $H^1(R/R^{(2,S)})$ and $\{w_d\}_{d\in D}$ be a basis for $H^1(S^{(2)}/S^{(3)})$. Let βw_d and βz_c be Bocksteins of w_d and z_c in $H^2(R/R^{(2,S)}) = E_3^{0,2}(S/R^{(2,S)})$ and $H^2(S^{(2)}/S^{(3)}) = E_3^{0,2}(S^{[3]})$ respectively. Then $\{\beta w_d\}_{d\in D}$ and $\{\beta z_c\}_{c\in C}$ generate $E_3^{0,2}(S/R^{(2,S)})$ and $E_3^{0,2}(S^{[3]})$ respectively. This follows from

a standard argument exploiting the fact that d_2 is a derivation with respect to the multiplicative structure of $E_2^{p,q}$ and the fact that $d_2^{0,1}$ is injective. However using the fact that $d_2^{1,1}$ is surjective, we see that $d_3^{0,2}(S^{[3]}) = 0$. Hence $E_3^{0,2}(S^{[3]}) = E_\infty^{0,2}(S^{[3]})$. In Lemma 3.9 we denote the natural map $E_3^{0,2}(S^{[3]}) \to E_3^{0,2}(S/R^{(2,S)})$ as res because it is induced by the restriction map $S^{(2)}/S^{(3)} \longrightarrow R/R^{(2,S)}$. By Lemma 3.8, and our discussion above, we obtain

Lemma 3.9. res: $E_3^{0,2}(S^{[3]}) \to E_3^{0,2}(S/R^{(2,S)})$ *is surjective and* $E_3^{0,2}(S^{[3]}) = E_\infty^{0,2}(S^{[3]})$.

We have a commutative diagram

$$\begin{array}{ccc} E_\infty^{0,2}(S/R^{(2,S)}) & \longrightarrow & E_3^{0,2}(S/R^{(2,S)}) \\ \uparrow & & \uparrow \\ E_\infty^{0,2}(S^{[3]}) & = & E_3^{0,2}(S^{[3]}) \, . \end{array}$$

Using Lemma 3.9 we deduce the following corollaries.

Corollary 3.10. res : $E_\infty^{0,2}(S^{[3]}) \to E_\infty^{0,2}(S/R^{(2,S)})$ *is surjective.*

Corollary 3.11. $E_\infty^{0,2}(S/R^{(2,S)}) = E_3^{0,2}(S/R^{(2,S)})$.

Since both extensions in the above are central, then

$$d_2^{1,1} : H^1(G, H^1(R/R^{(2,S)})) \to H^3(G)$$

is the composite $H^1(G, H^1(R/R^{(2,S)})) \xrightarrow[\cong]{(1,d_2^{0,1})} H^1(G) \otimes H^2(G) \xrightarrow{\cup} H^3(G)$.
Also $d_2^{1,1} : H^1(S^{[2]}, H^1(S^{(2)}/S^{(3)})) \to H^3(S^{[3]})$ is the composite

$$H^1(S^{[2]}, H^1(S^{(2)}/S^{(3)})) \xrightarrow[\cong]{(1,d_2^{0,1})} H^1(S^{[2]}) \otimes H^2(S^{[2]}) \xrightarrow{\cup} H^3(S^{[2]}) \, .$$

We may abuse notation by setting

$$E_\infty^{1,1}(S/R^{(2,S)}) = \mathrm{Ker}(\cup : H^1(G) \otimes H^2(G) \to H^3(G))$$

and $E_\infty^{1,1}(S^{[3]}) = \mathrm{Ker}(\cup : H^2(S^{[2]}) \otimes H^2(S^{[2]}) \to H^3(S^{[2]}))$. We have a commutative diagram

(3.12)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_\infty^{1,1}(S/R^{(2,S)}) & \longrightarrow & H^1(G) \otimes H^2(G) & \xrightarrow{\cup} & H^3(G) & \longrightarrow & 0 \\ & & \uparrow u & & \uparrow v & & \uparrow inf & & \\ 0 & \longrightarrow & E_\infty^{1,1}(S^{[3]}) & \longrightarrow & H^1(S^{[2]}) \otimes H^2(S^{[2]}) & \xrightarrow{\cup} & H^3(S^{[2]}) & \longrightarrow & 0. \end{array}$$

Here u and v are natural maps induced by inflation maps. Recall that $S^{[2]} \cong G^{[2]}$ under our projection map $S \to G$. In the next lemma we use both the injectivity of h_3 and the surjectivity of h_2.

Lemma 3.13. *The map* $u\colon E_\infty^{1,1}(S^{[3]}) \longrightarrow E_\infty^{1,1}(S/R^{(2,S)})$ *is surjective.*

Proof. We consider $E_\infty^{1,1}(S/R^{(2,S)})$ as a subgroup of $H^1(G) \otimes H^2(G)$. Using the surjectivity of h_2, we see that each element in $H^1(G) \otimes H^2(G)$ can be written as a sum of elements of the form $\alpha \otimes (\beta \cup \gamma)$ where $\alpha, \beta, \gamma \in H^1(G)$. As we remarked at the end of Section 2, the injectivity of h_3 implies that $E_\infty^{1,1}(S/R^{(2,S)})$ is generated by the elements $z_1 \otimes (z_2 \cup z_3)$ such that $z_1 \cup z_2 = 0$ in $H^2(G)$. (Since h_2 is the isomorphism, we can work in $H^1(G)$ rather than in k_2F.) Because the map $\inf\colon H^1(S^{[2]}) \longrightarrow H^1(G)$ is an isomorphism, we see that for the element $z_1 \otimes (z_2 \cup z_3)$ as above we can find $y_i \in H^1(S^{[2]}), i = 1, 2, 3$ such that $\inf(y_i) = z_i$. Using our assumption that $z_1 \cup z_2 = 0$ in $H^2(G)$ we see that

$$u((y_1 \otimes (y_2 \cup y_3) - y_3 \otimes (y_1 \cup y_2)) = z_1 \otimes (z_2 \cup z_3).$$

Therefore we see that our map u is surjective. □

4. Graded Lie Algebras

Here we give an equivalent description of Question 1.2 in Lie algebra language. A convenient reference is Lazard's paper [Laz1]. As usual, we consider a minimal presentation of G.

$$1 \longrightarrow R \longrightarrow S \longrightarrow G \xrightarrow{\pi} 1\ . \tag{4.1}$$

Let S and G admit the usual filtrations

$$S^{(1)} = S, \ldots, S^{(n+1)} = (S^{(n)})^p[S^{(n)}, S], \ldots$$
$$G^{(1)} = G, \ldots, G^{(n+1)} = (G^{(n)})^p[G^{(n)}, G], \ldots\ .$$

The formulae $G^{(n+1)} \subset G^{(n)}, [G^{(n)}, G^{(m)}] \subset G^{(n+m)}$ imply that $\mathrm{gr}_n(G) = G^{(n)}/G^{(n+1)}$ (denoted additively) is an vector space over $\mathbb{F}_p$ and that the graded algebra $\mathrm{gr}(G) = \sum \mathrm{gr}_n(G)$ is an algebra over $\mathbb{F}_p$ where multiplication of homogenous elements of $\mathrm{gr}(G)$ is induced by the commutator operation. This operation satisfies the Jacobi identity and hence is a

Lie bracket. The p-th power map in G induces an operator P on $\mathrm{gr}(G)$ making it a Lie algebra over $\mathbb{F}_p[\pi]$ if $p \neq 2$ and a mixed Lie algebra if $p = 2$ (cf. [Laz1]). Similarly, the induced filtration $\{R \cap S^{(n)}\}$ yields the graded Lie algebra $\mathrm{gr}(R)_{ind}$. The extension 4.1 induces an exact sequence of (mixed) Lie algebras

$$0 \to \mathrm{gr}(R)_{ind} \to \mathrm{gr}(S) \xrightarrow{\phi} \mathrm{gr}(G) \longrightarrow 0.$$

Since the filtration of G is discrete the map ϕ is surjective. (See pages 428-430 in [Laz1] for details.)

On the other hand, the filtration $\{R^{(n,S)}\}$ yields another Lie algebra $\mathrm{gr}(R, S)$. The inclusion $R^{(n,S)} \subset R \cap S^{(n+1)}$ (see Lemma 3.1 induces the homomorphism $\iota_n : \mathrm{gr}_n(R, S) \to \mathrm{gr}_{n+1}(R)_{ind}$ and therefore a Lie algebra homomorphism $\iota : \mathrm{gr}(R, S) \to \mathrm{gr}(R)_{ind}$. Let U be the enveloping algebra of $\mathrm{gr}(S)$. Then U is the free associative $\mathbb{F}_p[\pi]$-algebra on the free generators of S. There is a canonical embedding of $\mathrm{gr}(S)$ into U with $P(x) = \pi x$ if $p \neq 2$. If $p = 2$ we have $P(x) = x^2 + \pi x$ if x is of degree 1 and $P(x) = \pi x$ if x is of degree > 1. Note that $\mathrm{gr}(R, S)$ and $\mathrm{gr}(R)_{ind}$ are U-modules via the adjoint representation and that ι is a homomorphism of U-modules.

Theorem 4.2. *The following are equivalent*

(A) *We have* $R^{(n,S)} = R \cap S^{(n+1)}$ *for* $n \geq 1$.
(B) *The homomorphism* ι *is injective.*
(C) *The homomorphism* ι *is surjective.*

Proof. Note that (A) holds for $n = 1$ since $R \subset S^{(2)}$.

Assume that ι is injective and that (A) holds for some $n \geq 1$. Let $x \in R \cap S^{(n+2)}$. Then $x \in R \cap S^{(n+1)} = R^{(n,S)}$. If ξ is the image of x in $\mathrm{gr}_n(R, S)$ we have $\iota_n(\xi) = 0$ which implies $x \in R^{(n+1,S)}$. Hence (A) holds for $n + 1$ and by induction for all n.

Assume that ι is surjective and let $x \in R \cap S^{(n+1)}$. Then there exists $y_0 \in R^{(n,S)}$ such that $x_1 = y_0^{-1}x \in R \cap S^{(n+2)}$. In the same way we define inductively y_i such that $y_i \in R^{(n+i,S)}$ and $x_{i+1} = y_i^{-1}x_i \in R \cap S^{(n+2+i)}$ for $i \geq 0$ with $x_0 = x$. Then $x = \prod y_i \in R^{(n,S)}$. □

Corollary 4.3. *Let* $G = S/R$ *be a minimal presentation of* G *of finite type. Then* i *is surjective if* $\iota(\mathrm{gr}_1(R, S))$ *generates* $\mathrm{gr}(R)_{ind}$ *as an ideal of* $\mathrm{gr}(S)$.

The elements of $i(\mathrm{gr}_1(R,S)) \subset \mathrm{gr}_2(S)$ are images of elements r of R under the canonical mapping of $S^{(2)}$ onto $\mathrm{gr}_2(S)$. These images are called initial forms of the elements r. If ι is bijective and $R \neq 1$ then R has a minimal generating set whose initial forms are of degree 2. In this case the presentation $G = S/R$ is called **quadratic**. If $G = F/R$ is of finite type we say it is **quadratically defined** if it is quadratic and the set of initial forms of a minimal generating set for R generate $\mathrm{gr}(R)_{ind}$ as an ideal of $\mathrm{gr}(S)$. The latter is true if the set of initial forms is strongly free, cf. [LM], [Lab2]. The group G is said to be quadratically defined if it has a minimal presentation which is quadratically defined.

Theorem 4.4. *Let $G = S/R$ be a minimal presentation of G of finite type. Then i is bijective iff $R = 1$ or $G = S/R$ is quadratically defined.*

Proof. If $G = S/R$ is quadratically defined then $i(\mathrm{gr}_1(R,S))$ is a generating set for $\mathrm{gr}(R)_{ind}$ as an ideal of $\mathrm{gr}(S)$. Then i is surjective since it is a U-module homomorphism and hence bijective by Theorem 4.2.

Conversely, suppose that i is bijective and identify $\mathrm{gr}(R,S)$ with its image in $\mathrm{gr}(S)$. To prove that $G = S/R$ is quadratically defined it suffices to prove that $\mathrm{gr}_1(R,S)$ generates $\mathrm{gr}(R,S)$ as a U-module. Let M be the U-submodule of $\mathrm{gr}(R,S)$ generated by $\mathrm{gr}_1(R,S)$. We have $M_1 = \mathrm{gr}_1(R,S)$. Suppose that $M_n = \mathrm{gr}_n(R,S)$ and let $\xi \in \mathrm{gr}_{n+1}(R,S)$, $\xi \neq 0$. If $x \in R^{(n+1,S)}$ is a representative of ξ then x is a product of elements of the form u^p, $[u,v]$ with $u \in R^{(n,S)}$, $v \in S$. Since i is injective these elements lie in $\mathrm{gr}_{n+1}(S)$ unless the degree of u is n and the degree of v is 1. It follows that ξ is a linear combination of elements of the form $\pi\eta$, $[\eta,\zeta]$ with $\eta \in M_n$, $\zeta \in U_1$ and hence that $\xi \in M_{n+1}$. □

Question 4.5. Let G be isomorphic to the Galois group of a maximal p-extension of a field, and let i be a natural graded Lie algebra homomorphism $i : \mathrm{gr}(R,S) \to \mathrm{gr}(R)_{ind}$. When is i an isomorphism?

If F is a global field of characteristic $\neq p$ which is totally imaginary if F is a number field and $p = 2$, then by the results of [LM] and [Sch], $G = \mathrm{Gal}(F(p)/F)$ is a projective limit of quadratically defined presentations. More precisely, the group G has a presentation S/R where $S = \cup S_i$ $i \geq 1$ with $S_i \subset S_{i+1}$ finitely generated and, if R_i is the image of R under the canonical projection of S onto S_i, we have S_i/R_i quadratically defined for all i. By Theorem 4.2 this means that $R_i^{(n,S_i)} = R_i \cap S_i^{(n+1)}$ for all i,n which implies $R^{(n,S)} = R \cap S^{(n+1)}$ for all n since S is the projective limit of the S_i. Hence, by Theorem 4.2, the map ι is an isomorphism. The same is true if F is a local field with

ζ_p in F since then $G = \mathrm{Gal}(F(p)/F)$ is a Demushkin group which is quadratically defined by [LM], [Lab2]. We thus obtain the following result.

Theorem 4.6. *Let F be a field containing a primitive p-th root of unity. If F is a global field, which is totally imaginary if F is a number field and $p = 2$, or a local field containing a primitive p-th root of unity then F is quadratically defined.*

Question 4.7. Is $\mathrm{Gal}(\mathbb{Q}(2)/\mathbb{Q})$ quadratically defined?

5. Acknowledgements

We are very grateful to Alejandro Adem and Wenfeng Gao, who made important contributions towards this work in its early stages. Alejandro Adem's continuous interest, and discussions, have been a considerable encouragement for our work.

References

[A-K-M] A. Adem, D. Karagueuzian and J. Mináč, *On the cohomology of Galois groups determined by Witt rings,* Advances in Math. **148** (1999), 105–160.

[Be] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern,* J. reine angew. Math. **268/269** (1974), 41–52.

[Ch-E-M] S. Chebolu, I. Efrat and J. Mináč. Quotients of absolute Galois groups which determine the entire Galois cohomology. (http://arxiv.org/PS_cache/arxiv/pdf/0905/0905.1364v2.pdf.)

[F-V] I. B. Fesenko and S. V. Vostokov. Local Fields and Their Extensions. Second Edition, AMS Translations of Mathematical Monographs **121**, 2002.

[G-M] W. Gao and J. Mináč, *Milnor conjecture and Galois theory I*, Fields Institute Communications, AMS **16** (1997), 95–110.

[Ha-W] C. Haesemeyer and Ch. Weibel. Norm varieties and the chain lemma (after Markus Rost). *Proc. Abel Symposium*, to appear.

[H-S] G. Hochschild and J-P. Serre, *Cohomology of group extensions,* Trans. AMS **74** (1953), 110–134.

[J-W] B. Jacob and R. Ware, *A recursive description of the maximal pro-2-group via Witt rings*, Math. Zeit. **200** (1989) 379–396.

[Ko1] H. Koch, *Galoische theorie der p-Erweiterungen,* Grundlehren der mathematische Wissenchaften, Springer-Verlag, 1970.

[Ko2] ———, *On p-extensions with given ramification,* Appendix 1 in K. Haberland, VEB Deutscher Verlag Der Wissenchaften, Springer-Verlag, 1978.

[Lab1] J. Labute, *Algèbres de Lie et pro-p-groupes definis par une seule relation,* Invent. Math. **4** (1967), 142–158.

[Lab2] ———, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. Reine Angew. Math. 596 (2006), 115-130.

[LM] J. Labute and J. Mináč, *Mild Pro-2-Groups and 2-Extensions of* $\mathbb{Q}$ *with Restricted Ramification*, preprint.

[Laz1] M. Lazard, *Groupes analytiques p-adiques,* Publ. Math. Inst. Hautes Etud. **26** (1965), 389–603.

[M-S] A. S. Merkurjev and A. A. Suslin. K-cohomology and Brauer-Severi varieties and the norm residue homomorphism. *Math. USSR. Izv.* **21** (1983), 307–340.

[Mi] J. Milnor, *Algebraic K-theory and quadratic forms,* Invent. Math. **9** (1970), 318–344.

[Mi-Sp1] J. Mináč and M. Spira, *Formally real fields, pythagorean fields, C-fields and W-groups,* Math. Z. **205** (1990), 519–530.

[Mi-Sp2] ———, *Witt rings and Galois groups,* Annals of Mathematics **144** (1996), 35–60.

[N-S-W] J. Neukirch, A. Schmidt and K. Winberg, *Cohomology of Number Fields,* Springer-Verlag, vol. **323** (2000).

[Ro1] M. Rost, *Chain lemma for symbols.* (Available at www.math.uni-bielefeld.de/ rost/chain-lemma.html.)

[Ro2] ———, *On the basic correspondence of a splitting variety.* (Available at: www.math.uni-bielefeld.de/ rost/chain-lemma.html.)

[Se1] J.-P. Serre, *Lie algebra and Lie groups,* Lectures given at Harvard University, Reading, Mass., 1964.

[Se2] ———, *Cohomologie Galoisienne,* Fifth Edition, Lecture Notes in Mathematics, Vol. 5, Springer Verlag, 1995.

[Sch] A. Schmidt, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, to appear in J. Reine Angew. Math., Engl. Transl.:arXiv:0806.1863[math.NT].

[S-J] A. A. Suslin and S. Joukhovitski. Norm varieties. *J. Pure Appl. Algebra* **206** (2006), 235–276.

[Voe1] V. Voevodsky. Motivic cohomology with $\mathbb{Z}/2$-coefficients. *Publ. Inst. Hautes Etudes Sci.* **98** (2003) 59–104.

[Voe2] V. Voevodsky. On Motivic cohomology with $\mathbb{Z}/l$-coefficients. K-theory preprint archive no. 639. (Available: www.math.uiuc.edu/K-theory/0639.)

[Voe3] V. Voevodsky. Motivic Eilenberg-MacLane spaces. K-theory preprint 2007.

[Wei1] Ch. Weibel. The norm residue isomorphism theorem. *J. Topology* **2** (2009) 346–372.

[Wei2] Ch. Weibel. The proof of the Bloch-Kato Conjecture. *ICTP Lecture Notes Series* **23** (2008) 1–28.

[Wür] T. Würfel, *On a class of pro-p-groups occuring in Galois theory,* Journal of Pure and Applied Algebra **36** (1985), 95–103.

SUNY at Binghamton, Department of Mathematical Sciences, P. O. Box 6000, Binghamton, NY 13902-6000

E-mail address: dikran@math.binghamton.edu

McGill University, Department of Mathematics and Statistics, 805 Sherbrooke Street West, Montreal, Quebec, Canada H3A 2K6

E-mail address: labute@math.mcgill.ca

The University of Western Ontario, Department of Mathematics, Middlesex College, London, Ontario, Canada N6A 5B7

E-mail address: minac@uwo.ca