Absolute Galois groups viewed from small quotients and the Bloch–Kato conjecture

SUNIL K CHEBOLU
JÁN MINÁČ

In this survey we concentrate on the relations between the structure of small Galois groups, arithmetic of fields, Bloch–Kato conjecture, and Galois groups of maximal pro–p–quotients of absolute Galois groups.

20C20, 20J06; 55P42

Dedicated to Professor Paulo Ribenboim with admiration, respect and friendship on the occasion of his 80th birthday

1 Introduction

The second author fondly remembers how a number of years ago Paulo Ribenboim helped him to escape to the West and immediately upon his arrival welcomed him with beautiful lectures on the Galois group of the Pythagorean closure of $\mathbb{Q}$. Ribenboim's lectures, writings, and research have influenced us strongly, and in particular this paper reflects his influence on the choice of topics and our way of thinking about them. The paper is a selective survey of results on small quotients of absolute Galois groups and their relations with the Bloch–Kato conjecture. It is by no means a comprehensive historical survey. Instead, it focuses only on some selective topics from the work of the authors and their collaborators.

The main idea of our paper, and a key point we want to illustrate, is that already relatively small quotients of absolute Galois groups encode substantial information about them. Absolute Galois groups of fields play a central role in arithmetic, geometry, and topology. Yet these profinite groups are mysterious and not much is known about the fundamental problem of characterizing absolute Galois groups among all profinite groups. Therefore, it is natural to investigate the maximal pro–p–quotients of absolute Galois groups for a fixed prime p which are in general much simpler than the absolute Galois groups. But even these pro–p–quotients are quite mysterious and one would like to find more manageable, yet interesting, quotients of maximal pro–p–quotients of absolute Galois groups. One extremely interesting family of such quotients are the

Published: 16 June 2009 DOI: 10.2140/gtm.2009.16.31

W–groups defined in Section 6. These are pro–p–groups of nilpotent class at most 2 and they have exponent dividing p^2. So they are rather simple groups in comparison with the maximal pro–p–quotients of absolute Galois groups. Nevertheless, when the primitive pth root of unity is contained in the base field, these groups carry complete information about the entire Galois cohomology with $\mathbb{F}_p$–coefficients of the absolute Galois groups. This is a consequence of the Bloch–Kato conjecture which was proved recently by Rost and Voevodsky with C. Weibel's patch; see Voevodsky [33; 32] for an overview of the proof, and other references (Haeasemeyer and Weibel [11]; Mazza, Voevodsky and Weibel [19]; Rost [27; 28]; Suslin and Joukhovitski [30]; Voevodsky [34]; and Weibel [35; 36; 37]), for the foundation and completion of the proof, and some further exposition. Therefore, it is clear that the W–groups of fields are good candidates for thorough investigation.

The plan of this survey paper is as follows. We begin with Šafarevič's early work as a motivation for studying the Galois module structure of p–power classes of fields. This is interesting even in the case when we consider just cyclic extensions of degree p. We show that the answer in this case already leads to a description of relatively small pro–p–quotients of absolute Galois groups called T–groups. We then describe some recent results on the Galois module structure of Galois cohomology. After that we give a description of W–groups, their relationship with Witt rings of quadratic forms, Galois cohomology, valuations, and the structure of maximal pro–p–extensions. Here the Bloch–Kato conjecture plays a very important role, especially in the case $n = 2$ which was established by Merkurjev and Suslin almost 30 years ago. At the conclusion of the paper we touch upon our recent work with D. Benson and J. Swallow in progress whose goal is to provide a refinement of the Bloch–Kato conjecture with group cohomology, combinatorics, and Galois theoretic consequences.

2 Some work of Šafarevič

Šafarevič initiated the very interesting program of studying Galois groups of maximal p–extensions. Let F be a field and F_{sep} the separable closure of F. Given a prime number p, let $F(p)$ be the maximal p–extension over F. Thus $F(p)$ is the compositum in F_{sep} of all Galois extensions K/F which have degree a power of p. Let $G_F(p) := \text{Gal}(F(p)/F)$ be the Galois group of the maximal p–extension. In 1947 Šafarevič showed that if $\mathbb{Q}_p \subseteq F$, $[F : \mathbb{Q}_p] < \infty$, and if F does not contain a primitive pth root of unity, then $G_F(p)$ is a free pro–p–group on $[F : \mathbb{Q}_p] + 1$ generators. The key part of Šafarevič's argument was the determination of the number $d(H)$ of minimal generators for all open subgroups H of $G_F(p)$. This number $d(H)$ is equal to $\dim_{\mathbb{F}_p} H/\Phi(H)$, where $\Phi(H) = H^p[H, H]$ is the Frattini subgroup of H. By local

class field theory it follows that $d(H) = \dim_{\mathbb{F}_p} K^*/K^{*p}$ where K is the fixed field of H and $K^* = K\backslash\{0\}$ is the multiplicative group of K. We can calculate $d(H)$ explicitly in terms of invariants of the extension K/F. It turns out that

$$\dim_{\mathbb{F}_p} K^*/K^{*p} - 1 = [K : F](\dim_{\mathbb{F}_p} F^*/F^{*p} - 1).$$

Thus

$$d(H) - 1 = (d(G_F(p)) - 1)[K : F]$$

and therefore the number of generators $d(H)$, for each H open subgroup of $G_F(p)$, grow in the same way as if $G_F(p)$ were a free pro–p–group. It was the insight of Šafarevič that in fact this property is enough to prove that $G_F(p)$ is a free pro–p–group. Šafarevič did not use the convenient language of profinite groups as this terminology was not available at that time. Similarly, the language of Galois cohomology appeared much later, and all became wide-spread only after the appearance of Serre's lecture notes in 1964; see [29] for the latest edition of Serre's book. In particular, now we can rewrite the above equation as

$$\dim_{\mathbb{F}_p} H^1(H, \mathbb{F}_p) - 1 = (\dim_{\mathbb{F}_p} H^1(G_F(p), \mathbb{F}_p) - 1)[G_F(p) : H].$$

Let G be a pro–p–group with $\dim_{\mathbb{F}_p} H^r(G, \mathbb{F}_p) < \infty$ for $1 \leq r \leq n$. Following H. Koch we can set the nth partial Euler–Poincaré characteristic $\chi_n(G)$ as

$$\chi_n(G) = \sum_{r=0}^{n} (-1)^r \dim_{\mathbb{F}_p} H^r(G, \mathbb{F}_p).$$

Koch proved that if W is a system of open subgroups of G which form a neighbourhood basis at 1 and $\chi_n(U) = [G : U]\chi_n(G)$ for all U in W, then the cohomological dimension $cd(G)$ of G is at most n. Because $cd(G) = 1$ if and only if G is a free pro–p–group, we see that Koch's criterion for $cd(G) \leq n$ generalises Šafarevič's criterion for $G_F(p)$ being a free pro–p–group.

3 The Bloch–Kato conjecture

We briefly recall the Bloch–Kato conjecture for the novice. This conjecture will be used in this article at various places. Let F be a field that has a primitive pth root ζ_p of unity. Consider the Kummer sequence

$$1 \longrightarrow \mu_p \longrightarrow F^*_{\text{sep}} \overset{x \to x^p}{\longrightarrow} F^*_{\text{sep}} \longrightarrow 1$$

of modules over the absolute Galois group G_F, where μ_p denotes the group of pth roots of unity. The boundary map

$$H^0(G_F, F^*_{\text{sep}}) = F^* \to H^1(G_F, \mathbb{F}_p)$$

in the induced long exact sequence in Galois cohomology extends naturally to a map

$$T(F^*) \to H^*(G_F, \mathbb{F}_p),$$

where $T(F^*)$ is the tensor algebra on F^* and $H^*(G_F, \mathbb{F}_p)$ is the Galois cohomology ring of G_F. Bass and Tate verified that the Steinberg relations $(a) \cup (1-a) = 0$ for $a \neq 0, 1$ hold in $H^*(G_F, \mathbb{F}_p)$. Milnor K–theory $K_*(F)$ is a graded ring obtained by taking the quotient of $T(F^*)$ by the graded two-sided ideal generated by the elements $a \otimes (1-a)$, $a \in F^* \backslash \{1\}$. Thus we get a map, known as the norm-residue map,

$$\eta\colon K_*(F)/pK_*(F) \longrightarrow H^*(F, \mathbb{F}_p)$$

from the reduced Milnor K–theory to the Galois cohomology of F. The Bloch–Kato conjecture claims that the norm-residue map η is an isomorphism. The case $p = 2$ was implicitly conjectured by J. Milnor in 1970; see [21]. The Milnor conjecture was eventually proved by Voevodsky [33; 32]. For this spectacular work Voevodsky was awarded a Fields medal in 2002. His work used some sophisticated machinery such as motivic cohomology operations and the development of $\mathbb{A}^1$–stable homotopy theory. The proof of the Bloch–Kato conjecture is even more subtle. Although Voevodsky announced a proof of the Bloch–Kato conjecture in 2003, not until September 2007 were all of the details for the Rost–Voevodsky proof made available by Voevodsky, Rost and Weibel; see [27; 28; 30; 34; 35; 36; 37]. The work on the proof of the Bloch–Kato conjecture and the resulting theorem has already had tremendous impact on contemporary mathematics and is expected to have an even broader impact in the coming years. Note that the Bloch–Kato conjecture gives a presentation of the rather mysterious Galois cohomology $H^*(F, \mathbb{F}_p)$ by generators and relations. In particular, it tells us that $H^*(F, \mathbb{F}_p)$ is generated by one dimensional classes.

4 Classical Hilbert 90 and absolute Galois groups

Šafarevič's approach to $G_F(p)$ made clear that the pth power class group F^*/F^{*p} is a very useful and fundamental object to study. In 1960 Faddeev began to study the Galois module structure of pth power classes of cyclic extensions of local fields, and during the mid 1960s he and Borevič established the Galois module structure of pth power class groups of local fields using basic arithmetic invariants attached to these extensions. (See Faddeev [10] and Borevič [5]).

In the theory of quadratic forms, the exact sequence of square class groups associated with the quadratic extension $K = F(\sqrt{a})$, $a \in F^*\setminus F^{*2}$, $\mathrm{char}(F) \neq 2$ has been playing an important role. This sequence is

$$1 \to \{F^{*2}, aF^{*2}\} \to F^*/F^{*2} \xrightarrow{i_{F/K}} K^*/K^{*2} \xrightarrow{N_{K/F}} F^*/F^{*2} \xrightarrow{\epsilon} B(F),$$

where $i_{F/K}$ is induced by the inclusion map $F \to K$ and $N_{K/F}\colon K^*/K^{*2} \to F^*/F^{*2}$ is the map induced by the norm map $K^* \to F^*$, and ϵ is the homomorphism from F^*/F^{*2} to the Brauer group $B(F)$ defined by $bF^{*2} \to \left[\left(\frac{a,b}{F}\right)\right]$ in $B(F)$, where $\left[\left(\frac{a,b}{F}\right)\right]$ is the class of the quaternion algebra

$$\left(\frac{a,b}{F}\right) = \{f_0 + f_1 i + f_2 j + f_3 ij \mid f_l \in F,\ i^2 = j^2 = -1,\ ij = -ji\}$$

in the Brauer group of F. (See Lam [15, Theorem 3.2, p. 200].) Observe that this sequence completely determines the size of K^*/K^{*2} provided we know the size $N_{K/F}(K^*)/F^{*2}$. In fact, this sequence determines the structure of K^*/K^{*2} as an $\mathbb{F}_2[\mathrm{Gal}(K/F)]$–module provided we know $N_{K/F}(K^*)/F^{*2}$ and of course also F^*/F^{*2}. Therefore it is desirable to extend the work of Borevič and Faddeev from the case of local fields to general fields. Borevič, Faddeev and Šafarevič used local class field theory to establish their results in the case of local fields. However, in Mináč and Swallow [26] it was observed that it is possible to determine the structure of the $\mathbb{F}_p[\mathrm{Gal}(K/F)]$–module K^*/K^{*p} in the case when a primitive pth root of unity is contained in F using just Hilbert 90 in place of local class field theory. In Mináč, Schultz and Swallow [22], the work of [26] was extended to all cyclic extensions K/F of degree p^n with no restriction on the base field. The remarkable feature of the final result is that K^*/K^{*p} can be written as a sum of cyclic modules over $\mathbb{F}_p[\mathrm{Gal}(K/F)]$ of dimensions over $\mathbb{F}_p$ all powers of p with the possible single cyclic module exception of dimension $p^m + 1$, $0 \leq m \leq n-1$.

As an example we formulate here the main result of [22] when the exceptional summand does not occur. For the more complicated case when the exceptional summand does occur, we refer the reader to [22]. Let F be any field. Consider a cyclic Galois extension K/F with Galois group $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$, a cyclic group of order p^n. We set $J = K^*/K^{*p}$. Then J has the obvious $\mathbb{F}_p G$–module structure.

Theorem 4.1 *Assume that F does not contain any primitive pth root of unity. Then the $\mathbb{F}_p G$–module J decomposes as*

$$J \cong Y_0 \oplus Y_1 \oplus \cdots \oplus Y_n,$$

where Y_i is a direct sum of cyclic $\mathbb{F}_p G$–modules of dimension p^i.

Moreover, the multiplicity of cyclic summands of dimension p^i in Y_i is completely determined by the filtration of F^*K^{*p} by norm groups

$$K^{*p} \subset K^{*p}N_{K/F}(K^*) \subset K^{*p}N_{K_{n-1}/F}(K_{n-1}^*) \subset \cdots \subset F^*K^{*p}$$

where, for each $i = 0, 1, \ldots n$, K_i is the unique subfield of K which has dimension p^i over F. Indeed if

$$Y_i = \bigoplus_I C_{p^i}$$

where C_{p^i} is the cyclic $\mathbb{F}_pG$–module of dimension p^i, then the cardinality of I is just

$$\dim_{\mathbb{F}_p}\big(N_{K_i/F}(K_i^*)K^{*p}\big)\big/\big(N_{K_{i+1}/F}(K_{i+1}^*)\big)K^{*p},$$

where we set $N_{K_{n+1}/F}(K_{n+1}^*)$ to be $\{1\}$. Further set $[K_i^*] = K_iK^{*p}/K^{*p}$ and set $H_i = \mathrm{Gal}(K/K_i)$. Then we have Galois descent in the sense that $[K_i^*] = J^{H_i}$ — the fixed elements of J under the action of H_i.

The results in the case when F contains a primitive pth root of unity are similar, but technically more challenging due to the occurrence of the exceptional module mentioned earlier.

These results are remarkable because of the absence of summands of dimensions not equal to a power of p. (Except in the case of exceptional summands which have dimension $p^m + 1$.) These results severely restrict possible small quotients of absolute Galois groups. We shall illustrate this by describing a result from a recent paper by Benson, Lemire and Swallow [3].

We call a pro–p–group R elementary abelian if it has the form $R = \prod_I C_p$, where C_p is a cyclic group of order p, and I is some possibly infinite index set. We say that a pro–p–group G is a T–group if G contains a maximal closed subgroup N, $N \neq G$, of exponent dividing p. Then N is a normal subgroup of G and the factor group G/N acts naturally on N via conjugation. Furthermore, the subgroup N is uniquely determined by G provided that G is neither an elementary abelian group of order greater than p nor the direct product of an elementary abelian group and a nonabelian group of order p^3 of exponent p if $p > 2$, and the dihedral group of order 8 if $p = 2$. Given any profinite group A with a closed normal subgroup B of index p, the factor group $A/B^p[B, B]$ is a T–group. Now suppose that E/F is a cyclic field extension of degree p. We define the T–group of E/F to be $T_{E/F} := G_F/G_E^p[G_E, G_E]$, where G_F and G_E are absolute Galois groups of F and E respectively. (For the benefit of topologists, in order to avoid a possible confusion, we remark that the name "T-group" is not motivated by Kazhdan's property (T), and in fact we do not know of any connection between T-groups and groups with property (T) in Kazhdan's sense.) We

shall now classify those T–groups which are realisable as $T_{E/F}$ for fields containing a primitive pth root of unity.

In order to illustrate the restrictions on those T–groups which are realisable as $T_{E/F}$ for fields which contain a primitive pth root of unity we shall introduce a simple set of invariants which determine T–groups up to isomorphism. We shall then see that for $p > 2$ we obtain restrictions on possible invariants of T–groups which are $T_{E/F}$ for suitable E/F. On the other hand there are no restrictions in the case $p = 2$. The proof of these statements can be found in [3].

For a pro–p–group A, denote $Z(A)$ its center and $Z(A)[p]$ the elements of $Z(A)$ of order dividing p. Let $A_{(n)}$ be the nth group in the central series of A. Thus $A_{(1)} = A$, and $A_{(n+1)} = [A_{(n)}, A]$. Here we always consider closed subgroups of A. Hence $A_{(n+1)}$ is the closed subgroup of A generated by commutators $[x, y]$, $x \in A_{(n)}$, $y \in A$. For a T–group A we define:

$$t_1 = \dim_{\mathbb{F}_p} H^1\left(\frac{Z(A)[p]}{Z(A) \cap A_{(2)}}, \mathbb{F}_p\right)$$

$$t_i = \dim_{\mathbb{F}_p} H^1\left(\frac{Z(A)[p] \cap A_{(i)}}{Z(A) \cap A_{(i+1)}}, \mathbb{F}_p\right) \quad 2 \le i \le p$$

$$\mu = \max\{i : 1 \le i \le p,\ A^p \subset A_{(i)}\}$$

These invariants are convenient for describing the $\mathbb{F}_p[A/N]$–module N associated with our T–group A; see [3, Section 1]. We have

Proposition 4.2 *For arbitrary cardinalities t_i, $i = 1, 2, \dots, p$, and μ with $1 \le \mu \le p$, the following are equivalent:*

(1) *The t_i and μ are invariants of some T–group.*
(2) (a) *If $\mu < p$, then $t_\mu \ge 1$, and*
    (b) *If $\mu = p$ and $t_i = 0$ for all $2 \le i \le p$, then $t_1 \ge 1$.*

Moreover, T–groups are uniquely determined up to isomorphism by these invariants.

Theorem 4.3 *For p an odd prime, the following are equivalent.*

(1) *A is a T–group with invariants t_i and μ satisfying*
    (a) $\mu \in \{1, 2\}$
    (b) $t_2 = \mu - 1$, *and*
    (c) $t_i = 0$ *for* $3 \le i < p$.

(2) $A \cong T_{E/F}$ *for some cyclic extension* E/F *of degree* p *such that* F *contains a primitive* p*th root of unity.*

Now suppose $p = 2$*. Then each* T*–group is isomorphic to* $T_{E/F}$ *for some cyclic extension of degree* 2*.*

It is interesting to note that these strong restrictions on possible T–groups occurring as $T_{E/F}$ are consequences of the classical Hilbert 90 theorem which can now be viewed as the Bloch–Kato conjecture in degree 1, as it just involves basic Kummer theory which depends on Hilbert 90. For the realisation of given T–groups with invariants described in our theorem one uses constructions of cyclic extensions E/F of degree p with prescribed groups F^*/F^{*p} and $N_{E/F}(E^*)/F^{*p}$ developed in Mináč, Schultz and Swallow [22], which in turn uses results in Efrat and Haran [7] realising certain semidirect products and free pro–p–products as absolute Galois groups. This theorem provides restrictions on possible relations in $G_F(p)$; see [3].

5 Higher Galois cohomology and the Bloch–Kato conjecture

In [22] it was shown that the classical theorem Hilbert 90 is the key for determining the $\mathbb{F}_p[\mathrm{Gal}(E/F)]$–module structure of E^*/E^{*p} in the case of cyclic extensions of degree p^n. But E^*/E^{*p} is also $K_1(E)/pK_1(E)$. On the other hand Merkurjev and Suslin established in [20] an analogue of the Hilbert 90 theorem for Milnor K–theory in degree 2. Further it turned out that the analogue of Hilbert 90 for higher Milnor K–theory is essentially equivalent to the Bloch–Kato conjecture. This follows from the work of Merkurjev, Suslin, Rost and Voevodsky. Therefore it was a natural idea to extend results on Galois module structure of p–power classes to Galois module structure of $K_n(E)/pK_n(E)$ for any positive integer n. This was achieved in Lemire et al [17] in the case when E/F is a cyclic extension of prime degree p and the primitive pth root of unity ξ_p is in F. (An extension of this work for the case of cyclic extension of degree p^n is work in progress.) Some of the main results are explained in this section on the language of Galois cohomology as we freely use the Bloch–Kato conjecture.

Let G be the Galois group of E/F. Write $E = F(\sqrt[p]{a}), a \in F^\times$ and let $(a).(\xi_p) \in H^2(F, \mathbb{F}_p)$ denote the cup product of $(a), (\xi_p) \in H^1(F, \mathbb{F}_p)$. For each $n \in \mathbb{N}$ set also:

$$\Upsilon_1 \colon \dim_{\mathbb{F}_p}\big(\mathrm{ann}_{H^{n-1}(F,\mathbb{F}_p)}(a).(\xi_p)/\mathrm{ann}(a)\big)$$

and

$$\Upsilon_2 \colon \dim_{\mathbb{F}_p} H^{n-1}(F, \mathbb{F}_p)/\mathrm{ann}_{H^{n-1}(F,\mathbb{F}_p)}(a).(\xi_p).$$

Here $H^i(F,\mathbb{F}_p) = H^i(G_F,\mathbb{F}_p)$ is the ith Galois cohomology, G_F is the absolute Galois group of F and ann is an abbreviation for the annihilator. Thus for example $\operatorname{ann}_{H^{n-1}(F,\mathbb{F}_p)}(a).(\xi_p)$ is the kernel of the cup product

$$(a).(\xi_p).-\colon H^{n-1}(F,\mathbb{F}_p) \to H^{n+1}(F,\mathbb{F}_p).$$

Set U to be the absolute Galois group of E and consider $H^n(U,\mathbb{F}_p) = H^n(E,\mathbb{F}_p)$ as an $\mathbb{F}_p[G]$–module. In [17] we prove the following theorem. Our symbol cor below denotes the corestriction map $H^n(E,\mathbb{F}_p) \to H^n(F,\mathbb{F}_p)$ and res means the restriction map res: $H^n(F,\mathbb{F}_p) \to H^n(E,\mathbb{F}_p)$.

Theorem 5.1 *If $p > 2$ and $n \in \mathbb{N}$ then*

$$H^n(E,\mathbb{F}_p) \cong X_1 \oplus X_2 \oplus Y \oplus Z,$$

where

(1) *X_1 is a trivial $\mathbb{F}_p[G]$–module of dimension Υ_1, and*

$$X_1 \cap \operatorname{res} H^n(F,\mathbb{F}_p) = \{0\}.$$

(2) *X_2 is a direct sum of Υ_2 cyclic $\mathbb{F}_p[G]$–modules of dimension 2.*

(3) *Y is a free $\mathbb{F}_p[G]$–module of rank*

$$\dim_{\mathbb{F}_p} \operatorname{Im}\big(\text{cor: } H^n(E,\mathbb{F}_p) \to H^n(F,\mathbb{F}_p)\big)/(a).H^{n-1}(F,\mathbb{F}_p).$$

(4) *Z is a trivial $\mathbb{F}_p[G]$–module of dimension*

$$z = \dim_{\mathbb{F}_p} H^n(F,\mathbb{F}_p)/((\xi_p)H^{n-1}(F,\mathbb{F}_p) + \operatorname{cor} H^n(E,\mathbb{F}_p)) \quad \text{and}$$
$$Z \subset \operatorname{res}(H^n(F,\mathbb{F}_p)).$$

We see in particular that there is no cyclic summand of dimension larger than 2 but smaller than p.

A similar, but different theorem is valid in the case when $p = 2$. (See [17, Theorem 2].) Our decomposition of G–modules $H^n(F,\mathbb{F}_p)$ are not canonical but they allow a canonical equivalent reformulation. Let I be the augmentation ideal of $\mathbb{F}_p[G]$. Then from the analysis of the proof in Theorem 5.1, one sees that our theorem is equivalent to the statements below. (Here we abbreviate $H^n(E,\mathbb{F}_p)$ as $H^n(E)$.)

(1) For each $3 \le i \le p$, $I^{i-1}H^n(E) \cap H^n(E)^G = I^{p-1}H^n(E)$.

(2) $IH^m(E) \cap H^m(E)^G = \operatorname{res}(\xi_p).H^{m-1}(F) + \operatorname{res}\operatorname{cor} H^m(E)$.

(3) $0 \to \operatorname{ann}(a) \to H^{n-1}(E) \xrightarrow{(a).-} H^m(F) \xrightarrow{\text{res}} H^m(E)^G \xrightarrow{\text{cor}} (a).\operatorname{ann}(a,\xi_p) \to 0$.

As we mentioned earlier this work uses in an essential way the key ingredients of the proof of the Bloch–Kato conjecture, namely Hilbert 90 and the exact sequence in Milnor K–theory. However, in the case of $n = 2$, we do not need the recent proof but we can use instead results from the mid-1980s: the seminal results of Merkurjev and Suslin [20].

In the case when characteristic of F is p and $G = \mathrm{Gal}(E/F) = \mathbb{Z}/p^n\mathbb{Z}$ is a cyclic group of prime power order all Galois modules K_mE/p^sK_mE, $s = 1, 2, \ldots$ over $\mathbb{Z}/p^s\mathbb{Z}[G]$ were classified; see Bhandari et al [4] and Mináč, Schultz and Swallow [23].

These results and ideas were applied to the development of an analog of Schreier's formulas for the growth of the dimension of Galois cohomology over $\mathbb{F}_p$ in Labute et al [14]. In Labute et al [13] applications to the characterization of Galois Demuškin groups via Galois modules were obtained. (Demuškin groups are Poincaré groups of cohomological dimension two, and Galois Demuškin groups are Poincaré groups which are also Galois groups of maximal p–extensions.)

Recall now that for a pro–p–group G with finite cohomology groups $H^i(G, \mathbb{F}_p)$ for $0 \leq i \leq n$, the nth partial Euler–Poincaré characteristic $\chi_n(G)$ is defined as

$$\chi_n(G) = \sum_{i=0}^{n} (-1)^i h_i(G).$$

Suppose now that $G = G(p)$ for a field F containing a primitive pth root of unity, and suppose G has finite rank. Having determined $\chi_n(G)$, we have obtained a strengthening of a result of Koch [12, Theorem 5.5]:

Theorem 5.2 [16, Corollary 2] *Suppose that $\xi_p \in F$, and let $n \in \mathbb{N}$. The following are equivalent:*

(1) *$cd(G) \leq n$.*

(2) *$\chi_n(N) = p\chi_n(G)$ for all open subgroups N of G of index p.*

(3) *$\chi_n(V) = p\chi_n(U)$ for all open subgroups U of G and all open subgroups V of U of index p.*

6 Galois theoretic connections

We will explain the role played by certain Galois groups called W–groups in arithmetic. To set the stage, we begin with our notation.

Let F be a field of characteristic not equal to 2. We shall introduce several subextensions of F_{sep}.

- $F^{(2)}$ = compositum of all quadratic extensions of F.
- $F^{(3)}$ = compositum of all quadratic extensions of $F^{(2)}$ that are Galois over F.
- F_q = compositum of all Galois extensions K/F such that $[K : F] = 2^n$, for some positive integer n.

All of these subextensions are Galois and they fit in a tower

$$F \subset F^{(2)} \subset F^{(3)} \subset F_q \subset F_{\text{sep}}.$$

We denote their Galois groups (over F) as

$$G_F \longrightarrow G_q \longrightarrow G_F^{[3]} (= \mathcal{G}_F) \longrightarrow G_F^{[2]} \longrightarrow 1.$$

Observe that $G_F^{[2]}$ is just $\prod_{i \in I} C_2$, where I is the dimension of F^*/F^{*2} over $\mathbb{F}_2$. G_F is the absolute Galois group of F. Although the quotients G_q are much simpler than G_F we are far from understanding their structure in general. $F^{[3]}$ and its Galois group over F are considerably much simpler and yet they already contain substantial arithmetic information of the absolute Galois group. The groups $G_F^{[3]} (= \mathcal{G}_F)$ are called W–groups.

To illustrate this point, consider WF the Witt ring of quadratic forms; see [15] for the definition. Then we have the following theorem.

Theorem 6.1 [25] *Let F and L be two fields of characteristic not 2. Then $WF \cong WL$ (as rings) implies that $\mathcal{G}_F \cong \mathcal{G}_L$ as pro–2–groups. Further if we assume additionally in the case when each element of F is a sum of two squares that $\sqrt{-1} \in F$ if and only if $\sqrt{-1} \in L$, then $\mathcal{G}_F \cong \mathcal{G}_L$ implies $WF \cong WL$.*

Thus we see that $\mathcal{G}_F$ essentially controls the Witt ring WF and in fact, $\mathcal{G}_F$ can be viewed as a Galois theoretic analogue of WF. In particular, $\mathcal{G}_F$ detects orderings of fields. (Recall that P is an ordering of F if P is an additively closed subgroup of index 2 in F^*.) More precisely, we have:

Theorem 6.2 [24] *There is a one-to-one correspondence between the orderings of a field F and cosets $\{\sigma\Phi(\mathcal{G}_F) \mid \sigma \in \mathcal{G}_F \backslash \Phi(\mathcal{G}_F) \text{and } \sigma^2 = 1\}$. Here $\Phi(\mathcal{G}_F)$ is the Frattini subgroup of $\mathcal{G}_F$, which is just the closed subgroup of $\mathcal{G}_F$ generated by all squares in $\mathcal{G}_F$. The correspondence is as follows:*

$$\sigma\Phi(\mathcal{G}_F) \longrightarrow P_\sigma = \{f \in F^* \mid \sigma(\sqrt{f}) = \sqrt{f}\}.$$

This theorem was generalised considerably for detecting additive properties of multiplicative subgroups of F^* in Mahé, Mináč and Smith [18]. In this paper (see [18, Section 8]) it was shown that $\mathcal{G}_F$ can be used also for detecting valuations on F. The work on extending these ideas is in progress; see Chebolu, Efrat and Mináč [6] and forthcoming papers.

Also in [1, Corollary 3.9] it is shown that $\mathcal{G}_F \cong \mathcal{G}_L$ if and only if $k_*(F) \cong k_*(L)$. Here $k_*(A)$ denotes the Milnor K–theory (mod 2) of a field A. In particular, in [1, Theorem 3.14] it is shown that if R is the subring of $H^*(\mathcal{G}_F, \mathbb{F}_2)$ generated by one dimensional classes, then R is isomorphic to the Galois cohomology $H^*(G_F, \mathbb{F}_2)$ of F. Thus we see that $\mathcal{G}_F$ also controls Galois cohomology and in fact $H^*(\mathcal{G}_F, \mathbb{F}_2)$ contains some further substantial information about F which $H^*(G_F, \mathbb{F}_2)$ does not contain. These results can be extended to the case when $p > 2$ and F contains a primitive pth root of unity; see [6; 2; 3]. In summary, $\mathcal{G}_F$ is a very interesting object. On the one hand $\mathcal{G}_F$ is much simpler than G_F or G_q, yet it contains substantial information about the arithmetic of F. In fact, consider the case when $p > 2$ and F contains a primitive pth root of unity. Then let $G = G_F$ be the absolute Galois group of F. The descending p–central series of G is defined inductively by $G^{(1)} = G$, and $G^{(i+1)} = (G^{(i)})^p[G^{(i)}, G]$, for $i \geq 1$. Thus $G^{(i+1)}$ is the closed subgroup of G generated by all powers h^p and all commutators $[h, g] = h^{-1}g^{-1}hg$, where $h \in G^{(i)}$ and $g \in G$. Then the fixed fields $F^{(i)}$ of $G^{(i)}$ are precisely analogue of fields

$$F = F^{(1)} \subset F^{(2)} \subset F^{(3)} \subset \cdots \subset F^{(i)} \subset \cdots$$

introduced above in the case $p = 2$ and $i = 1, 2$ and 3.

The special case of the main theorem in Efrat and Mináč [8] then states:

Theorem 6.3 *For $p > 2$ and for $G = G_F$ as above, $G^{(3)}$ is the intersection of all normal subgroups N of G such that G/N is isomorphic to one of $\{1\}$, C_{p^2}, and M_{p^3} (the modular group of order p^3 which is the unique nonabelian group of order p^3 and exponent p^2).*

The analogous result in the case $p = 2$ was discovered by Villegas [31] in a different formalism. In [25, Corollary 2.18] this result was reformulated and reproved using the descending 2–central sequence of G_F. Namely, then $G^{(3)} = G_F^{(3)}$ is the intersection of all open normal subgroups N of G such that G/N is isomorphic to $\{1\}, C_2, C_4$, or to the dihedral group of order 8. The main ingredients in the proofs of the above results is the Bloch–Kato conjecture in degree 2 which was proved in [20]. The case $p = 2$ was the first breakthrough in the case of general fields made by Merkurjev who used some K–theoretic calculations due to Suslin. For this particular case there is now an

elementary proof available due to Merkurjev; see Elman, Karpenko and Merkurjev [9]. If $p > 2$, in the cohomology group $H^2(C_{p^2}, \mathbb{F}_p)$ we have elements not expressible as sums of products of elements in $H^1(C_{p^2}, \mathbb{F}_p)$. To handle these elements, in [8] there is a detailed consideration of the Bockstein homomorphism

$$B_G\colon H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p).$$

In fact, in [8] not the full strength of Merkurjev–Suslin theorem was used. The essential tool was the injectivity of the map

$$K_2(F)/p\,K_2(F) \to H^2(F, \mathbb{F}_p).$$

In [6], the surjectivity of this map is used to obtain restrictions on presentation of groups $G_F(p)$ via generators and relations.

Let $1 \to R \to S \to G \to 1$, where $G = G_F(p)$ with F as above, S a free pro–p–group with minimal number of generators (see [12, Chapter 4]), and R is the subgroup of S of relations in G. Then we have:

Theorem 6.4 ([6] for any p, [25] for $p = 2$.) *Let $S \supset S^{(2)} \supset S^{(3)} \supset \cdots$ be the p–descending series of S. Then we have*

$$R^p[R, S] = R \cap S^{(3)}.$$

Observe that for any minimal presentation of any pro–p–group G as above, we have $R^p[R, S] \subset R \bigcap S^{(3)}$, as $R \subset S^{(2)}$. The equality in the case when $G = G_F(p)$ is the consequence of the surjectivity of the norm residue map

$$K_2(F)/p\,K_2(F) \to H^2(G_F(p), \mathbb{F}_p).$$

which follows from the Merkurjev–Suslin theorem.

From the above theorem, one can deduce that if G is any pro–p–group such that $R \subset S^{(3)}$, and $G = G_F(p)$, then G is a free pro–p–group.

Example 6.5 Let G be a pro–p–group on n generators $a_1, a_2, \ldots, a_n$ for $n \geq 2$ subject to relations $[[a_i, a_j], a_r] = 1$ for all $1 \leq i < j \leq n$ and $1 \leq r \leq n$. Then G is not $G_F(p)$ for any field F containing a primitive pth root of unity.

Chebolu, Efrat and Mináč, in [6] and forthcoming papers, consider further restrictions on possible groups $G_F(p)$ by exploring its quotients $G_F^{[3]} = G_F(p)/G_F(p)^{(3)}$ and close connections between properties of $G_F^{[3]}$ and the existence of nontrivial valuations on F.

We now outline a joint project with Benson and Swallow in which our goal is to obtain a refinement of the Bloch–Kato conjecture. Associated to the field F, we have a natural tower of subfields $F^{(n)}$ of the separable closure F_{sep} defined as follows: $F^{(1)} = F$, $F^{(2)}$ is the compositum of all cyclic extensions of degree p over F, and for $n \geq 3$, $F^{(n)}$ is the compositum of all cyclic extensions of degree p over $F^{(n-1)}$ which are Galois over F. We call this tower the *filtration tower* associated to F. We define (in agreement with the notation we used above) the Galois groups

$$G_F^{[n]} := \text{Gal}(F^{(n)}/F) \quad \text{and} \quad G_F^{(n)} := \text{Gal}(F_{\text{sep}}/F^{(n)}),$$

which fit in a sequence $1 \to G_F^{(n)} \to G_F \to G_F^{[n]} \to 1$, where G_F is the absolute Galois group $\text{Gal}(F_{\text{sep}}/F)$. In [6] (see also [2]), we have shown that the decomposable part of $H^*(G_F^{[3]}, \mathbb{F}_p)$ — that is, the subalgebra of $H^*(G_F^{[3]}, \mathbb{F}_p)$ generated by degree-one elements over $\mathbb{F}_p$ — is isomorphic to $H^*(F, \mathbb{F}_p)$ under the inflation map. The important question therefore is to determine how an indecomposable class in $H^*(G_F^{[3]}, \mathbb{F}_p)$ decomposes under the various inflation maps along the filtration tower. By the Bloch–Kato conjecture, we know that it decomposes completely into one-dimensional classes when it goes all the way up to the separable closure. But what happens in between? A precise knowledge of this gives a refinement of the Bloch–Kato conjecture. We have shown (using the Bloch–Kato conjecture in degree 2!) that every indecomposable class in $H^2(G_F^{[n]}, \mathbb{F}_p)$ decomposes into one-dimensional classes when it goes to the next level

$$H^2(G_F^{[n+1]}, \mathbb{F}_p)$$

under the inflation map. Thus we have obtained a second cohomology refinement of the Bloch–Kato conjecture. The goal of our joint project with Benson and Swallow is to understand this refinement of the Bloch–Kato conjecture for higher cohomology. This is work in progress.

Acknowledgements

We are very grateful to our collaborators and friends especially to Dave Benson, Ido Efrat, John Labute, Andy Schultz, and John Swallow for working with us on these fascinating topics and sharing with us their unique insight. We would like also to thank the referee, whose valuable suggestions helped us to improve our exposition.

Ján Mináč was supported in part by Natural Sciences and Engineering Research Council of Canada grant R3276A01.

References

[1] **A Adem**, **D B Karagueuzian**, **J Mináč**, *On the cohomology of Galois groups determined by Witt rings*, Adv. Math. 148 (1999) 105–160 MR1736643

[2] **D J Benson**, **S K Chebolu**, **J Mináč**, **J Swallow**, *Bloch–Kato pro–p–groups and a refinement of the Bloch–Kato conjecture*, preprint (2007)

[3] **D Benson**, **N Lemire**, **J Mináč**, **J Swallow**, *Detecting pro–p–groups that are not absolute Galois groups*, J. Reine Angew. Math. 613 (2007) 175–191 MR2377134

[4] **G Bhandari**, **N Lemire**, **J Mináč**, **J Swallow**, *Galois module structure of Milnor K-theory in characteristic p*, New York J. Math. 14 (2008) 215–224 MR2413220

[5] **Z I Borevič**, *The multiplicative group of cyclic p-extensions of a local field*, Trudy Mat. Inst. Steklov 80 (1965) 16–29 MR0205976 In Russian: translated in *Proc. Steklov Inst. Math.*, 80 (1965), 15–30

[6] **S K Chebolu**, **I Efrat**, **J Mináč**, *Quotients of absolute Galois groups which determine the entire Galois cohomology* `arXiv:0905.1364`

[7] **I Efrat**, **D Haran**, *On Galois groups over Pythagorean and semi-real closed fields*, Israel J. Math. 85 (1994) 57–78 MR1264339

[8] **I Efrat**, **J Mináč**, *On the descending central sequence of absolute Galois groups* `arXiv:0809.21669`

[9] **R Elman**, **N Karpenko**, **A Merkurjev**, *The algebraic and geometric theory of quadratic forms*, American Mathematical Society Colloquium Publications 56, American Mathematical Society (2008) MR2427530

[10] **D K Faddeev**, *On the structure of the reduced multiplicative group of a cyclic extension of a local field*, Izv. Akad. Nauk SSSR Ser. Mat. 24 (1960) 145–152 MR0152518

[11] **C Haesemeyer**, **C W Weibel**, *Norm varieties and the chain lemma (after Markus Rost)*, preprint (2008) to appear in Proc. Abel Symposium 4 (2009)

[12] **H Koch**, *Galois theory of p-extensions*, Springer Monographs in Mathematics (2002) MR1930372 With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, with a postscript by the author and Lemmermeyer

[13] **J Labute**, **N Lemire**, **J Mináč**, **J Swallow**, *Demuškin groups, Galois modules, and the elementary type conjecture*, J. Algebra 304 (2006) 1130–1146 MR2265509

[14] **J Labute**, **N Lemire**, **J Mináč**, **J Swallow**, *Cohomological dimension and Schreier's formula in Galois cohomology*, Canad. Math. Bull. 50 (2007) 588–593 MR2364207

[15] **T Y Lam**, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics 67, American Mathematical Society (2005) MR2104929

[16] **N Lemire**, **J Mináč**, **J Swallow**, *When is Galois cohomology free or trivial?*, New York J. Math. 11 (2005) 291–302 MR2154357

[17] **N Lemire**, **J Mináč**, **J Swallow**, *Galois module structure of Galois cohomology and partial Euler–Poincaré characteristics*, J. Reine Angew. Math. 613 (2007) 147–173 MR2377133

[18] **L Mahé**, **J Mináč**, **T L Smith**, *Additive structure of multiplicative subgroups of fields and Galois theory*, Doc. Math. 9 (2004) 301–355 MR2117418

[19] **C Mazza**, **V Voevodsky**, **C Weibel**, *Lecture notes on motivic cohomology*, Clay Mathematics Monographs 2, American Mathematical Society (2006) MR2242284

[20] **A S Merkurjev**, **A A Suslin**, *K–cohomology of Severi–Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982) 1011–1046, 1135–1136 MR675529

[21] **J Milnor**, *Algebraic K-theory and quadratic forms*, Invent. Math. 9 (1969/1970) 318–344 MR0260844

[22] **J Mináč**, **A Schultz**, **J Swallow**, *Galois module structure of pth-power classes of cyclic extensions of degree p^n*, Proc. London Math. Soc. (3) 92 (2006) 307–341 MR2205719

[23] **J Mináč**, **A Schultz**, **J Swallow**, *Galois module structure of Milnor K-theory mod p^s in characteristic p*, New York J. Math. 14 (2008) 225–233 MR2413221

[24] **J Mináč**, **M Spira**, *Formally real fields, Pythagorean fields, C-fields and W-groups*, Math. Z. 205 (1990) 519–530 MR1082872

[25] **J Mináč**, **M Spira**, *Witt rings and Galois groups*, Ann. of Math. (2) 144 (1996) 35–60 MR1405942

[26] **J Mináč**, **J Swallow**, *Galois module structure of pth-power classes of extensions of degree p*, Israel J. Math. 138 (2003) 29–42 MR2031948

[27] **M Rost**, *Chain lemma for splitting fields of symbols*, preprint (1998) Available at `http://www.math.uni-bielefeld.de/~rost/chain-lemma.html`

[28] **M Rost**, *On the basic correspondence of a splitting variety*, preprint (2006) Available at `http://www.math.uni-bielefeld.de/~rost/basic-corr.html`

[29] **J-P Serre**, *Galois cohomology*, Springer Monographs in Mathematics, Springer (2002) MR1867431

[30] **A Suslin**, **S Joukhovitski**, *Norm varieties*, J. Pure Appl. Algebra 206 (2006) 245–276 MR2220090

[31] **F R Villegas**, *Relations between quadratic forms and certain Galois extensions, a manuscript*, preprint, Ohio State University (1998) Available at `http://www.math.utexas.edu/users/villegas/osu.pdf`

[32] **V Voevodsky**, *Voevodsky's Seattle lectures: K-theory and motivic cohomology*, from: "Algebraic K-theory (Seattle, WA, 1997)", Proc. Sympos. Pure Math. 67, Amer. Math. Soc. (1999) 283–303 MR1743245

[33] **V Voevodsky**, *Motivic cohomology with* $\mathbf{Z}/2$*-coefficients*, Publ. Math. Inst. Hautes Études Sci. (2003) 59–104 MR2031199

[34] **V Voevodsky**, *Motivic Eilenberg–MacLane spaces*, preprint (2007) Available at `http://www.math.uiuc.edu/K-theory/0864/`

[35] **C W Weibel**, *The norm residue isomorphism theorem*, preprint (2007) Available at `http://www.math.rutgers.edu/~weibel/papers.html`

[36] **C W Weibel**, *Axioms for the norm residue isomorphism*, from: "K-theory and Noncommutative Geometry", European Math. Soc. Pub. House (2008) 427–435

[37] **C W Weibel**, *The proof of the Bloch–Kato Conjecture*, ICTP Lecture Notes Series 23 (2008)

Department of Mathematics, Illinois State University
Normal, IL 61790, USA

Department of Mathematics, University of Western Ontario
London, ON N6A 5B7, Canada

`schebol@ilstu.edu, minac@uwo.ca`

Received: 14 November 2008