Stark's question and a refinement of Brumer's conjecture extrapolated to the function field case

Cristian D. Popescu

Abstract

We show that the extrapolation to the case of global fields of characteristic p of a question posed by Stark in 1980, regarding abelian L-functions of order of vanishing 2 at $s = 0$, has a negative answer. We provide links between various versions of Stark's question and a natural refinement of Brumer's conjecture, in the general context of global fields of arbitrary characteristic. As a consequence, we show that the refinement of Brumer's conjecture is, in general, false for characteristic p global fields.

Introduction

In [Sta71], Stark developed a remarkable conjecture, interpreting the lowest non-vanishing derivatives at $s = 0$ of the (imprimitive) Artin L-functions $L_{K/k,S}(s, \chi)$ associated to Galois extensions K/k of number fields in terms of values of a Galois-equivariant regulator, defined on a finite-dimensional $\mathbb{Q}$-vector space, constructed out of S-units in K, for any large enough set of primes S in k. In the 1970s and early 1980s, due to the work of Chinburg [Chi83, Chi85], Stark [Sta71] and Tate [Tat84], it became increasingly clear that, if one manages to replace the $\mathbb{Q}$-vector space in Stark's general conjecture by a Galois equivariant $\mathbb{Z}$-submodule (i.e. formulate a Stark conjecture 'over $\mathbb{Z}$'), the refined statement obtained this way would have far reaching applications to Hilbert's 12th problem and the theory of multiplicative Galois module structure. In the early 1990s, Rubin showed that a Stark conjecture 'over $\mathbb{Z}$' for abelian L-functions would provide a new source of Euler systems. In the last paper of [Sta71], Stark formulates a conjecture 'over $\mathbb{Z}$', covering the case of abelian L-functions of order of vanishing 1 at $s = 0$. As Tate shows in [Tat84, ch. IV, § 6], Brumer's conjecture can be viewed as a weak form of a particular case of this statement. During the same year, Stark studied the case of L-functions of order of vanishing 2 at $s = 0$. Presumably, due to a lack of compelling evidence, the refined statement at which he arrived in this case was formulated as a question rather than a conjecture (see [Sta80, San01]).

In this paper, we answer the extrapolation of Stark's question to the case of function fields and, as a consequence, we settle a natural refinement of Brumer's conjecture in this case. The paper is organized as follows. In §§ 1 and 2, we set the notations and state various forms of Stark's question. In § 3, we show that, in the case of function fields, a weak form of Stark's question (and consequently Stark's question itself) has a negative answer (see Theorem 3.3.2). In § 4, we state a refinement of Brumer's conjecture and provide links between this statement and various versions of Stark's question, for abelian extensions of global fields of arbitrary characteristic (see Propositions 4.2.1, 4.2.3 and 4.2.4). As a consequence, we show that the refinement of Brumer's conjecture is, in general, false in characteristic $p > 0$ (see Corollary 4.2.2).

This journal is © Foundation Compositio Mathematica 2004.

It is worth mentioning that, Rubin, the present author, and Burns and Flach have recently formulated versions 'over $\mathbb{Z}$' of Stark's general conjecture in the case of abelian L-functions of arbitrary order of vanishing at $s = 0$ (see Conjecture B in [Rub96], Conjecture C in [Pop02], and The Equivariant Tamagawa Number Conjecture in [Bur03], as well as the papers coauthored by Burns and Flach, cited in [Bur03].) The Equivariant Tamagawa Number Conjecture was also recently extended by Burns to non-abelian Artin L-functions (see [Bur97]).

1. Notation

Let K be a global field of arbitrary characteristic. Let μ_K be the group of roots of unity in K and $w_K := |\mu_K|$, the cardinality of μ_K. For a prime w of K, let K_w be the completion of K at w, and let $|\cdot|_w : K_w \longrightarrow \mathbb{R}^+ \cup \{0\}$ be the associated w-absolute value, normalized so that

$$|x|_w = \begin{cases} |x| \text{ (the Euclidian absolute value)}, & \text{if } K_w = \mathbb{R}, \\ x\bar{x}, & \text{if } K_w = \mathbb{C}, \\ (\mathbf{N}w)^{-\operatorname{ord}_w(x)}, & \text{if } K_w \text{ is non-archimedian.} \end{cases}$$

Here $\mathbf{N}w$ and $\operatorname{ord}_w(\cdot)$ denote, respectively, the cardinality of the residue field and the usual (discrete) valuation associated to the finite prime w.

Let us assume now that K/k is a finite Galois extension of global fields, with Galois group $G := \operatorname{Gal}(K/k)$. Let S be a non-empty finite set of primes in k, containing at least all the infinite primes and all the primes which ramify in K/k. Let S_K be the set of primes in K sitting above primes in S. We denote by $O_{K,S}$ the ring of S_K-integers in K (i.e. the set of elements in K with non-negative valuations at all primes outside S_K). $U_{K,S}$ and $A_{K,S}$ denote the group of units and the ideal-class group associated to the Dedekind domain $O_{K,S}$ respectively. Since the set S_K is closed under the natural action of G on primes in K, $O_{K,S}$, $U_{K,S}$, and $A_{K,S}$ are endowed with natural structures of left-modules over the integral group ring $\mathbb{Z}[G]$.

Assume now in addition that K/k is abelian. For every prime v of k, G_v denotes the decomposition group of w in K/k, for any prime w in K, sitting above v. If v is unramified in K/k, then G_v is cyclic, generated by the Frobenius automorphism associated to v in G, denoted by σ_v. Let $\widehat{G}$ denote the group of complex-valued irreducible characters of G. For every $\chi \in \widehat{G}$, let $e_\chi = 1/|G| \sum_{\sigma \in G} \chi(\sigma) \cdot \sigma^{-1}$ be the corresponding idempotent in the complex group ring $\mathbb{C}[G]$. To every $\chi \in \widehat{G}$, and every set S as above, one can associate the Artin L-function of complex variable s, with Euler factors at primes in S removed, denoted by $L_{K/k,S}(s,\chi)$. For a given χ and S, $L_{K/k,S}(s,\chi)$ is the (unique) meromorphic continuation to $\mathbb{C}$ of the infinite Euler product $\prod_{v \notin S}(1 - \mathbf{N}v^{-s} \cdot \chi(\sigma_v))^{-1}$, which is uniformly and absolutely convergent on compact subsets of the half-plane $\operatorname{Re}(s) > 1$. It is well known that if χ is different from the trivial character $\mathbf{1}_G$ of G, then $L_{K/k,S}(s,\chi)$ is holomorphic on the entire complex plane, whereas $L_{K/k,S}(s,\mathbf{1}_G)$ is holomorphic everywhere except for $s = 1$, where it has a pole of order 1. For fixed K/k, S and χ as above, let $\operatorname{ord}_{s=0} L_{K/k,S}(s,\chi)$ denote the order of vanishing of $L_{K/k,S}(s,\chi)$ at $s = 0$. As Tate shows in [Tat84, I], we have

$$\operatorname{ord}_{s=0} L_{K/k,S}(s,\chi) = \begin{cases} \operatorname{card}\{v \in S \mid \chi(G_v) = \{1\}\}, & \text{if } \chi \neq \mathbf{1}_G \\ \operatorname{card} S - 1, & \text{if } \chi = \mathbf{1}_G. \end{cases} \tag{1}$$

As in [Tat84], we combine the abelian Artin L-functions into what we call the Stickelberger function, defined by

$$\Theta_{K/k,S}(s) = \sum_{\chi \in \widehat{G}} L_{K/k,S}(s,\chi) \cdot e_{\chi^{-1}}.$$

632

$\Theta_{K/k,S}(s)$ is a meromorphic function in s, with values in the group ring $\mathbb{C}[G]$, holomorphic everywhere except for $s = 1$, where it has a pole of order 1.

2. Stark's question

Let K/k be an abelian extension of global fields and S a set of primes in k as in § 1. Let us assume that the set of data $(K/k, S)$ satisfies the following set of hypotheses.

HYPOTHESIS H.

   i) S contains all the infinite primes.

   ii) S contains all the primes which ramify in K/k.

   iii) S contains at least two primes which split completely in K/k.

   iv) $\operatorname{card} S \geqslant 3$.

Let us note that, according to (1), Hypothesis H implies that, for all $\chi \in \widehat{G}$, $\operatorname{ord}_{s=0} L_{K/k,S}(s, \chi) \geqslant 2$, and therefore

$$\Theta^{(2)}_{K/k,S}(0) := \lim_{s \to 0} s^{-2} \cdot \Theta_{K/k,S}(s)$$

makes sense if viewed inside $\mathbb{C}[G]$.

Let us choose a pair $V = (v_1, v_2)$ of distinct primes in S, which split completely in K/k, and let us fix $W = (w_1, w_2)$, where w_i is a prime in K sitting above v_i, for all $i = 1, 2$. For every $\mathbb{Z}[G]$-module M, let $\bigwedge^2_G M$ denote its second exterior power over $\mathbb{Z}[G]$. If R is a commutative ring, let $RM := R \otimes_{\mathbb{Z}} M$, viewed as an $R[G]$-module in the usual manner. As in [Pop02], one can define a $\mathbb{C}[G]$-equivariant regulator map $\mathbb{C} \bigwedge^2_G U_{K,S} \xrightarrow{R_W} \mathbb{C}[G]$, by letting

$$R_W(u_1 \wedge u_2) = \det_{1 \leqslant i,j \leqslant 2} \left(- \sum_{\sigma \in G} \log |u_j|_{w_i^\sigma} \cdot \sigma \right),$$

for $u_1, u_2 \in U_{K,S}$, and then extending to $\mathbb{C} \bigwedge^2_G U_{K,S}$ by $\mathbb{C}$-linearity.

Following Tangedal [Tan97], Grant [Gra99], and Sands [San01], we now state Stark's question for abelian L-functions of order of vanishing 2 at $s = 0$. We state Stark's Question in a Galois-equivariant form, in the spirit of the more general Conjectures B (see [Rub96]) and C (see [Pop02]), which deal with abelian L-functions of arbitrary order of vanishing at $s = 0$. We would like to emphasize that Stark only posed this question in the number field (characteristic 0) case. The extrapolation to characteristic p is natural and in line with the general philosophy of Stark's conjectures displayed in [Bur97, Bur03, Pop02, Rub96, Tat84] (see also Remark 2 below).

QUESTION A. *Assume that the set of data $(K/k, S)$ satisfies Hypothesis H. For V and W chosen as above, are there S-units u_1 and u_2 in $U_{K,S}$, such that the following conditions are simultaneously satisfied?*

   i) $\Theta^{(2)}_{K/k,S}(0) = (1/w_K)^2 \cdot R_W(u_1 \wedge u_2)$.

   ii) *The fields $K(u_1^{1/w_K})$ and $K(u_2^{1/w_K})$ are equal and are Galois, abelian extensions of k.*

Remark 1. The reader will notice that our formulation of Stark's question imposes fewer conditions on the S-units u_1 and u_2 than those appearing in [Gra99, San01, Tan97]. Namely, we are eliminating the following condition.

   iii) *For each $\sigma \in G$, the conjugate u_1^σ generates the same fractional ideal in K as u_1, and u_2^σ generates the same fractional ideal as u_2.*

We chose to eliminate this condition for three reasons. First, it was because this particular requirement on u_1 and u_2 has been subject to change over the years. Secondly it was because, as Sands noted in [San01], at least as it stands, it is too strong to be expected to be true in general. The third reasons is because in this paper we are only concerned with the most important condition i in the statement of Stark's question.

Remark 2. In [Sta80], Stark only formulates the above question in the particular case where k is a real quadratic number field and v_1 and v_2 are the two infinite primes in k. Later, Stark indicated that the original statement should be extended to the general situation described in this paper, at least in the characteristic 0 case (see [Gra99].)

Remark 3. The main theoretical evidence in support of an affirmative answer to Question A comes from the work of Tangedal [Tan97], who shows that units u_1 and u_2 satisfying conditions i–iii do indeed exist if k is a real quadratic field, v_1 and v_2 are the infinite primes of k, K/k is a quadratic extension, and card $S > 3$. A theoretical link between Question A and the more general Conjecture C was provided by Sands in [San01, Theorem 5.2]. Numerical evidence in support of an affirmative answer to Question A comes mainly from the work of Grant [Gra99] and Sands [San01].

One of the main goals of this paper is to show that, in the case of global function fields, the answer to a much weaker form of Question A, called Question B below, is in general negative. With notation as above, let $\bigwedge_G^2 \widetilde{U_{K,S}}$ be the image of $\bigwedge_G^2 U_{K,S}$ via the canonical (not necessarily injective) $\mathbb{Z}[G]$-morphism $\bigwedge_G^2 U_{K,S} \longrightarrow \mathbb{C} \bigwedge_G^2 U_{K,S}$.

QUESTION B. *Assume that the set of data $(K/k, S)$ satisfies Hypothesis H. For V and W chosen as above, is there an element ε_S in $(1/w_K)^2 \cdot \bigwedge_G^2 \widetilde{U_{K,S}}$, such that $\Theta_{K/k,S}^{(2)}(0) = R_W(\varepsilon_S)$?*

Obviously, for any u_1 and u_2 in $U_{K,S}$, we have $u_1 \wedge u_2 \in \bigwedge_G^2 \widetilde{U_{K,S}}$. However, in general, not every element in $\bigwedge_G^2 \widetilde{U_{K,S}}$ is of type $u_1 \wedge u_2$, with u_1 and u_2 in $U_{K,S}$. Therefore, if Question B is answered in the negative, then so is Question A.

For purposes which will become clear in § 4, we now state local versions of Questions A and B. Let ℓ be a prime number and let $\mathbb{Z}_{(\ell)} \subseteq \mathbb{Q}$ be the localization of $\mathbb{Z}$ at the prime ideal $\ell\mathbb{Z}$.

QUESTION $A_{(\ell)}$. *Let ℓ be a prime number. Assume that the set of data $(K/k, S)$ satisfies Hypothesis H. For V and W chosen as above, are there S-units $u_{1,\ell}$ and $u_{2,\ell}$ in $U_{K,S}$, and $n_\ell \in \mathbb{Z}_{(\ell)}$, such that the following conditions are simultaneously satisfied?*

i) $\Theta_{K/k,S}^{(2)}(0) = (n_\ell/w_K^2) \cdot R_W(u_{1,\ell} \wedge u_{2,\ell})$.

ii) *The fields $K(u_{1,\ell}^{1/w_K})$ and $K(u_{2,\ell}^{1/w_K})$ are equal and are Galois, abelian extensions of k.*

QUESTION $B_{(\ell)}$. *Let ℓ be a prime number. Assume that the set of data $(K/k, S)$ satisfies Hypothesis H. For V and W chosen as above, is there an element $\varepsilon_{S,\ell}$ in $(1/w_K)^2 \cdot \mathbb{Z}_{(\ell)} \bigwedge_G^2 \widetilde{U_{K,S}}$, such that $\Theta_{K/k,S}^{(2)}(0) = R_W(\varepsilon_{S,\ell})$?*

Obviously, if Question A (respectively Question B) is answered in the affirmative, then so is Question $A_{(\ell)}$ (respectively Question $B_{(\ell)}$), for all prime numbers ℓ.

3. Stark's question for function fields

In this section, we construct a class of examples of sets of data $(K/k, S)$, with char $k > 0$, satisfying Hypothesis H, and show that the answer to Question B (and therefore Question A) is negative in all these cases.

634

3.1 The extension K/k

Let p be a prime number, $q := p^\nu$, for some strictly positive integer ν and let $\mathbf{F}_q$ be the finite field of cardinality q. Let $k := \mathbf{F}_q(T)$ be the rational function field in one variable T of the exact field of constants $\mathbf{F}_q$. Let $\overline{k}_s$ be a fixed separable closure of k. For any prime v in k, we denote by $\mathbf{F}_q(v)$ the residue field corresponding to the discrete valuation associated to v. The index $[\mathbf{F}_q(v) : \mathbf{F}_q]$ is called the $\mathbf{F}_q$-residual degree of v. Let v_∞ be the prime of k corresponding to the discrete valuation on k of uniformiser T^{-1}. Let $P_0 \in \mathbf{F}_q[T]$ be an irreducible polynomial of degree p and let v_0 be the prime in k corresponding to the discrete valuation on k of uniformiser P_0. Obviously, the $\mathbf{F}_q$-residual degrees of v_∞ and v_0 are, respectively, 1 and p.

DEFINITION 3.1.1. Let K_1 be the unique degree p constant field extension of k inside $\overline{k}_s$ (i.e. $K_1 := \mathbf{F}_{q^p}(T)$, in this case). Let $G_1 := \mathrm{Gal}(K_1/k)$.

LEMMA 3.1.2. *The extension K_1/k defined above satisfies the following.*

i) $G_1 \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z}$.

ii) K_1/k *is unramified everywhere.*

iii) v_0 *splits completely in K_1/k.*

The proof is left to the reader.

DEFINITION 3.1.3. Let $\widetilde{K}_0$ be the maximal abelian extension of k inside $\overline{k}_s$ of the conductor dividing v_0^2, totally split at v_∞. Let $\widetilde{G}_0 := \mathrm{Gal}(\widetilde{K}_0/k)$.

LEMMA 3.1.4. *The field extension $\widetilde{K}_0/k$ defined above satisfies the following.*

i) *The p-rank of the p-Sylow subgroup of $\widetilde{G}_0$ is at least 2.*

ii) v_0 *is totally ramified in $\widetilde{K}_0/k$.*

Before we begin the proof of Lemma 3.1.4, we need some notation and to remind the reader of certain general facts on the arithmetic of function fields. For the moment, let us assume that k is a general function field of exact field of constants $\mathbf{F}_q$. Let $\mathrm{Pic}^0(k)$ denote the Picard group of k (i.e. the quotient of the group of degree zero divisors on k by the subgroup of principal divisors). Let J_k be the group of idèles associated with k. For any prime v of k, let U_v denote the group of units in the completion k_v of k with respect to the (normalized) discrete valuation ord_v associated to v. For all integers $i \geqslant 1$, let $U_v^{(i)}$ be the ith term of the canonical filtration of U_v with respect to ord_v, explicitly given by $U_v^{(i)} := \{x \in U_v \mid \mathrm{ord}_v(x-1) \geqslant i\}$. We have an exact sequence of abelian groups $1 \to J_k^0 \to J_k \xrightarrow{\deg_k} \mathbb{Z} \to 0$, where $\deg_k((x_v)_v) := \sum_v [\mathbf{F}_q(v) : \mathbf{F}_q] \cdot \mathrm{ord}_v(x_v)$, for all $(x_v)_v \in J_k$, and J_k^0 is defined to be the kernel of the map $\deg_k$. The group J_k^0 is linked to the Picard group by the exact sequence

$$1 \to k^\times \cdot \prod_v U_v \to J_k^0 \xrightarrow{\widehat{\mathrm{div}_k}} \mathrm{Pic}^0(k) \to 1,$$

where $\widehat{\mathrm{div}_k}((x_v)_v)$ is the class of $\mathrm{div}_k((x_v)_v) := \sum_v \mathrm{ord}_v(x_v) \cdot v$ in $\mathrm{Pic}^0(k)$, for all $(x_v)_v \in J_k^0$.

Proof of Lemma 3.1.4. i) Due to the fact that, in the particular case under discussion, $\mathrm{Pic}^0(k) = \{0\}$ (as k is a genus 0 function field) and $[\mathbf{F}_q(v_\infty) : \mathbf{F}_q] = 1$, the above exact sequences lead to the equality

$$J_k = k^\times \cdot \left[k_{v_\infty}^\times \times \prod_{v \neq v_\infty} U_v \right]. \tag{2}$$

635

Class field theory, combined with (2) and the definition of $\widetilde{K}_0$, shows that the global Artin map induces an exact sequence of groups

$$1 \to \mathbf{F}_q^\times \cdot U_{v_0}^{(2)} \to U_{v_0} \widetilde{G}_0 \to 1. \tag{3}$$

Consequently, the p-Sylow subgroup of $\widetilde{G}_0$ is isomorphic to $U_{v_0}^{(1)}/U_{v_0}^{(2)}$. Since $[\mathbf{F}_q(v_0) : \mathbf{F}_q] = q^p$, this group is isomorphic to the additive group $\mathbf{F}_{q^p}$ and, therefore, is an $\mathbf{F}_p$-vector space of dimension at least 2. This concludes the proof of part i.

ii) Since via the global Artin map U_{v_0} injects into the inertia group of a place of $\widetilde{K}_0$ over v_0, the exact sequence (3) shows that v_0 is totally ramified in $\widetilde{K}_0$. $\qquad \square$

Now, we finalize the construction of the field extension K/k. Lemma 3.1.4, part i implies that there exists at least a quotient G_0 of $\widetilde{G}_0$ such that $G_0 \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^2$. Let us fix a group G_0 with this property. Galois theory associates G_0 to a unique field K_0, such that $k \subseteq K_0 \subseteq \widetilde{K}_0$ and $\mathrm{Gal}(K_0/k) \xrightarrow{\sim} G_0$.

DEFINITION 3.1.5. Let K be the compositum $K_1 \cdot K_0$ inside $\overline{k}_s$, where K_1 and K_0 are the subfields of $\overline{k}_s$ constructed above. Let $G := \mathrm{Gal}(K/k)$.

The following lemma is an immediate consequence of the definitions.

LEMMA 3.1.6. *The field extension K/k defined above satisfies the following.*

i) *It is unramified away from v_0.*

ii) *One has a group isomorphism $G \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^3$.*

iii) *The decomposition group G_{v_0} of v_0 in K/k is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$.*

iv) *If F is an abelian p-extension of k containing K and unramified over K, with the property that every prime of K dividing v_0 splits completely in F, then $F = K$.*

Proof. We leave the (fairly elementary) proofs of statements i–iii to the reader. We sketch the proof of part iv. Let J be the inertia group in $\mathrm{Gal}(F/k)$ of a prime over v_0. Since F/K is unramified and consequently F/k is unramified outside v_0, J has order p^2 and F^J/k is an unramified abelian field extension. Since k is a rational function field, F^J must be a constant field extension. However, since the primes over v_0 split completely in F/K, the residue fields of all the primes over v_0 in F^J must be isomorphic to $\mathbf{F}_{q^p}$. This shows that $F^J = K_1$. Consequently, F has degree $\mathrm{card}(J) \cdot [K_1 : k] = p^3$ over k, implying that $F = K$. $\qquad \square$

3.2 The set S

For K/k defined in the previous section, we construct a special finite set of primes S in k, such that the set of data $(K/k, S)$ satisfies Hypothesis H. With the same notations as in § 3.1, let $S_0 := \{v_0\}$. The construction of S is based in an essential way on the following theorem, whose proof will be given in § 3.4.

THEOREM 3.2.1. *The p-Sylow subgroup $A_{K,S_0}^{(p)}$ of the S_0-ideal-class group A_{K,S_0} can be generated by two elements as a $\mathbb{Z}_p[G]$-module.*

Let ϖ_1 and ϖ_2 be ideal classes in $A_{K,S_0}^{(p)}$ which generate $A_{K,S_0}^{(p)}$ as a $\mathbb{Z}_p[G]$-module. Chebotarev's density theorem implies the existence of two primes w_1 and w_2 in K, satisfying the following properties.

i) $w_1 \in \varpi_1$ and $w_2 \in \varpi_2$.

ii) w_1 and w_2 do not lie above v_0 (i.e. $w_1, w_2 \notin S_{0,K}$.)

636

iii) If v_1 and v_2 are the primes in k below w_1 and w_2, respectively, then $v_1 \neq v_2$ and v_1 and v_2 split completely in K/k.

Let us fix two primes w_1 and w_2 in K which satisfy properties i–iii above, and let v_1 and v_2 be the primes in k sitting below w_1 and w_2, respectively.

DEFINITION 3.2.2. Let $S := \{v_0, v_1, v_2\}$, with v_1 and v_2 defined above and v_0 defined in as § 3.1.

Remark 4. The definition of S right away implies that the set of data $(K/k, S)$ satisfies Hypothesis H.

Remark 5. The p-Sylow subgroup $A_{K,S}^{(p)}$ of the S-ideal-class group $A_{K,S}$ is trivial. Indeed, $A_{K,S}^{(p)}$ is the quotient of $A_{K,S_0}^{(p)}$ by its $\mathbb{Z}_p[G]$-submodule generated by $\widehat{w_1}$ and $\widehat{w_2}$. However, by definition, $\widehat{w_1}$ and $\widehat{w_2}$ generate the full $A_{K,S_0}^{(p)}$ over $\mathbb{Z}_p[G]$.

3.3 Questions A and B for the set of data $(K/k, S)$

The main goal of this section is to show that, for the set of data $(K/k, S)$ constructed in the previous two sections, Question B and, consequently, Question A have negative answers.

In what follows, if Δ is a finite group and M is a $\mathbb{Z}[\Delta]$-module, then $\widehat{H}^i(\Delta, M)$ and $H_i(\Delta, M)$ denote the ith Tate-cohomology group and, respectively, the ith homology group of Δ with coefficients in M. For the moment, let us assume that K/k is an arbitrary, Galois extension of global fields (of arbitrary characteristic) of Galois group G (not necessarily abelian). Let Σ be a finite non-empty set of primes in k, containing at least all the infinite primes as well as those which ramify in K/k. Y_Σ denotes the free abelian group generated by the set Σ_K of all primes in K sitting above primes in Σ. Since Σ_K is stable under the natural Galois action on primes in K, Y_Σ is endowed with a natural $\mathbb{Z}[G]$-module structure. Let X_Σ be the $\mathbb{Z}[G]$-submodule of Y_Σ defined by the exact sequence

$$0 \to X_\Sigma \to Y_\Sigma \xrightarrow{J_\Sigma} \mathbb{Z} \to 0, \tag{4}$$

where J_Σ is the unique $\mathbb{Z}$-linear map sending every prime $w \in \Sigma_K$ to $1 \in \mathbb{Z}$. Since for every $v \in \Sigma$ and every $w \in \Sigma_K$ sitting above v, the G-stabilizer of w is the decomposition group $G_{w/v}$ of w in K/k, we clearly have $\mathbb{Z}[G]$-isomorphisms

$$Y_\Sigma \xrightarrow{\sim} \bigoplus_{v \in \Sigma} \mathbb{Z}[G/G_{w/v}] \xrightarrow{\sim} \bigoplus_{v \in \Sigma} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[G_{w/v}]} \mathbb{Z}). \tag{5}$$

For the second and third module involved in the isomorphism above, we choose a prime w above v, for each v in Σ. However, due to the fact that, for a given v, the groups $G_{w/v}$ are conjugate to one another, the $\mathbb{Z}[G]$-isomorphism class of the second and third module does not depend on this choice. For 'large' sets Σ, the link between the $\mathbb{Z}[G]$-module structure of X_Σ and that of the group of Σ-units $U_{K,\Sigma}$ is given by a result of Tate (see [Tat84, ch. II, § 5]), whose ℓ-adic version we state below.

THEOREM 3.3.1 (Tate). *Assume that K/k and Σ are as above, $G := \mathrm{Gal}(K/k)$, and ℓ is a prime number. Assume that $A_{K,\Sigma}^{(\ell)} = \{1\}$. Then, for all integers i, one has group isomorphisms*

$$\widehat{H}^i(G, U_{K,\Sigma} \otimes \mathbb{Z}_\ell) \xrightarrow{\sim} \widehat{H}^{i-2}(G, X_\Sigma \otimes \mathbb{Z}_\ell).$$

In the above statement, $\mathbb{Z}_\ell$ denotes the ring of ℓ-adic integers and $A_{K,\Sigma}^{(\ell)}$ denotes the ℓ-Sylow subgroup of the Σ-ideal-class group $A_{K,\Sigma}$ of K. Passing from Tate's original theorem 'over $\mathbb{Z}$' to the version 'over $\mathbb{Z}_\ell$' stated above can be done by tensoring all the exact sequences appearing in the proof of Tate's theorem with $\mathbb{Z}_\ell$ over $\mathbb{Z}$. We then use the fact that, since $\mathbb{Z}_\ell$ is a flat $\mathbb{Z}$-module, $* \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is an exact functor from the category of $\mathbb{Z}[G]$-modules to the category of $\mathbb{Z}_\ell[G]$-modules, which commutes with the Tate-cohomology functors $\widehat{H}^i(G, *)$.

THEOREM 3.3.2. *For the set of data $(K/k, S)$ constructed in §§ 3.1 and 3.2, Questions $B_{(p)}$ and, consequently, B and A, have negative answers.*

Proof. Let $V := (v_1, v_2)$, where v_1 and v_2 are the two totally split primes in S defined in § 3.2. Let $W = (w_1, w_2)$, for fixed primes w_1, w_2 in K, sitting above v_1 and v_2, respectively. Let us assume that Question $B_{(p)}$ has a positive answer. Let $\mathcal{U} = \{u_i^{(k)} \mid k = 1, \ldots, n; i = 1, 2\}$ be a subset of $U_{K,S}$ and $m \in \mathbb{Z}_{(p)}$, such that $\varepsilon_{S,p} := (m/w_K^2) \sum_{k=1}^{n} u_1^{(k)} \wedge u_2^{(k)}$ viewed as an element in $\mathbb{C} \bigwedge_G^2 U_{K,S}$ satisfies the regulator condition $\Theta_{K/k,S}^{(2)}(0) = R_W(\varepsilon_{S,p})$ in $\mathbb{C}[G]$. We project this equality on the direct summand $\mathbb{C}[G]e_{\mathbf{1}_G} = \mathbb{C}e_{\mathbf{1}_G}$ of $\mathbb{C}[G]$, where $e_{\mathbf{1}_G} := 1/|G| \sum_{\sigma \in G} \sigma := 1/|G| \cdot N_G$, and $N_G := \sum_{\sigma \in G} \sigma$ is the usual norm element in $\mathbb{C}[G]$. Since v_1 and v_2 are completely split in K/k, this projection leads to the following equality.

$$L_{K/k,S}^{(2)}(0, \mathbf{1}_G) \cdot e_{\mathbf{1}_G} = \left((m/w_K^2) \sum_{k=1}^{n} \det_{1 \leqslant i,j \leqslant 2} \left(-\log|N_G u_i^{(k)}|_{v_j} \right) \right) \cdot e_{\mathbf{1}_G}, \tag{6}$$

where $N_G u_i^{(k)}$ is the image of $u_i^{(k)}$ via the usual norm map $N_G : U_{K,S} \longrightarrow U_{k,S}$, for all i and k. However, equality (1) combined with the fact that card $S = 3$, shows that $\mathrm{ord}_{s=0} L_{K/k,S}(s, \mathbf{1}_G) = 2$ in this case. Therefore, the left-hand side of equality (6) is the leading Taylor coefficient at $s = 0$ of the ζ-function with S-Euler factors removed $\zeta_{k,S}(s)$, associated with k. The classical S-class-number formula gives

$$L_{K/k,S}^{(2)}(0, \mathbf{1}_G) = -\frac{1}{w_k} h_{k,S} \cdot R_{k,S},$$

where $h_{k,S}$ is the cardinality of $A_{k,S}$ and $R_{k,S}$ is the classical S-regulator of the free, rank two $\mathbb{Z}$-module $U_{k,S}/\mu_k$. For a subset M of $U_{k,S}$, let $R_{k,S}(M)$ denote the $\mathbb{Z}$-submodule of $\mathbb{C}$ generated by

$$\det \begin{bmatrix} \log|\epsilon_1|_{v_1} & \log|\epsilon_1|_{v_2} \\ \log|\epsilon_2|_{v_1} & \log|\epsilon_2|_{v_2} \end{bmatrix}, \quad \text{for all } \epsilon_1, \epsilon_2 \in M.$$

In particular, $R_{k,S}$ is the unique positive generator of $R_{k,S}(U_{k,S})$. The $\mathbb{Z}$-module $R_{k,S}(M)$ is always contained in $\mathbb{Z} \cdot R_{k,S}$, and it is non-zero if and only if the subgroup $\mathbb{Z}M$ of $U_{k,S}$ generated by M has finite index in $U_{k,S}$. Assuming that $\mathbb{Z}M$ has finite index in $U_{k,S}$, one has the following equality:

$$[\mathbb{Z} \cdot R_{k,S} : R_{k,S}(M)] = \frac{[U_{k,S} : \mathbb{Z}M]}{[\mu_k : \mu_k \cap \mathbb{Z}M]}.$$

For $\mathcal{U}$ defined above, let $N_G \mathcal{U} := \{N_G u \mid u \in \mathcal{U}\}$. Equality (6) divided by $R_{k,S}$ and combined with the S-class-number formula, implies firstly that $R_{k,S}(N_G \mathcal{U}) \neq \{0\}$, and secondly that

$$\mathbb{Z} \cdot \frac{w_K^2}{w_k} h_{k,S} \subseteq \mathbb{Z} \cdot \frac{m \cdot [U_{k,S} : \mathbb{Z}(N_G \mathcal{U})]}{[\mu_k : \mu_k \cap \mathbb{Z}(N_G \mathcal{U})]} \subseteq \mathbb{Z} \cdot \frac{m \cdot |\widehat{\mathrm{H}}^0(G, U_{K,S})|}{[\mu_k : \mu_k \cap \mathbb{Z}(N_G \mathcal{U})]}.$$

The second inclusion above is a direct consequence of the equality $\widehat{\mathrm{H}}^0(G, U_{K,S}) = U_{k,S}/N_G U_{K,S}$ and the inclusion $\mathbb{Z}(N_G \mathcal{U}) \subseteq N_G U_{K,S}$. Since char $K = p$, we have $\mu_K \otimes \mathbb{Z}_p = \{1\}$. Therefore, if we tensor the double inclusion above by the ring of p-adic integers $\mathbb{Z}_p$, and keep in mind that $m \in \mathbb{Z}_{(p)}$, we obtain

$$h_{k,S}^{(p)} \geqslant |\widehat{\mathrm{H}}^0(G, U_{K,S} \otimes \mathbb{Z}_p)|, \tag{7}$$

where $h_{k,S}^{(p)} := |A_{k,S}^{(p)}|$. The main idea of the proof of Theorem 3.3.2 is to show that, under our working hypotheses, inequality (7) does not hold true.

We first find an upper bound for $h_{k,S}^{(p)}$. Assume for the moment that k is any characteristic p global field, of the exact field of constants $\mathbf{F}_q$. Also, assume that $S_0 = \{v_0\}$ and S are finite sets of

primes in k, such that $S_0 \subseteq S$. Then, we have an exact sequence of groups

$$0 \to \mathrm{Pic}^0(k) \to A_{k,S_0} \xrightarrow{\deg_{v_0}} \mathbb{Z}/[\mathbf{F}_q(v_0) : \mathbf{F}_q] \cdot \mathbb{Z} \to 0,$$

where $\deg_{v_0}$ is the $\mathbb{Z}$-linear map which takes the S_0-ideal-class $\widehat{v}$ of a prime v into $[\mathbf{F}_q(v) : \mathbf{F}_q]$ mod $[\mathbf{F}_q(v_0) : \mathbf{F}_q]$ (see [Pop99], for example). The inclusion $S_0 \subseteq S$ also induces a natural surjective group-morphism $A_{k,S_0} \twoheadrightarrow A_{k,S}$. However, in our case, $\mathrm{Pic}^0(k) = \{0\}$. Also, $[\mathbf{F}_q(v_0) : \mathbf{F}_q] = p$ (see § 3.1). Therefore,

$$A_{k,S_0}^{(p)} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \quad \text{and} \quad h_{k,S}^{(p)} \leqslant p. \tag{8}$$

Next, we find a lower bound for $|\widehat{\mathrm{H}}^0(G, U_{K,S} \otimes \mathbb{Z}_p)|$. Remark 5 shows that, under our working hypotheses, Theorem 3.3.1 is applicable to $\Sigma := S$ and $\ell := p$. We therefore obtain group isomorphisms

$$\widehat{\mathrm{H}}^i(G, U_{K,S} \otimes \mathbb{Z}_p) \xrightarrow{\sim} \widehat{\mathrm{H}}^{i-2}(G, X_S \otimes \mathbb{Z}_p) \quad \text{for all integers } i.$$

In particular, for $i = 0$, we have

$$|\widehat{\mathrm{H}}^0(G, U_{K,S} \otimes \mathbb{Z}_p)| = |\widehat{\mathrm{H}}^{-2}(G, X_S \otimes \mathbb{Z}_p)| = |\mathrm{H}_1(G, X_S \otimes \mathbb{Z}_p)|, \tag{9}$$

where the second equality above is a consequence of the definition of Tate cohomology groups at negative levels. Let us now recall that $S = \{v_0, v_1, v_2\}$, with v_1 and v_2 completely split in K/k and, therefore, $G_{v_1} = G_{v_2} = \{1\}$. This shows that if we tensor the exact sequence (4) with $\mathbb{Z}_p$, for $\Sigma := S$, and use isomorphism (5), we obtain the following exact sequence of $\mathbb{Z}_p[G]$-modules:

$$0 \to X_S \otimes \mathbb{Z}_p \to (\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[G_{v_0}]} \mathbb{Z}_p) \oplus \mathbb{Z}_p[G]^2 \to \mathbb{Z}_p \to 0.$$

Next, we write the long exact sequence of homology groups corresponding to the above short exact sequence of G-modules. If we use Shapiro's lemma for computing the homology groups of the middle term, we obtain an exact sequence

$$\cdots \to \mathrm{H}_2(G_{v_0}, \mathbb{Z}_p) \to \mathrm{H}_2(G, \mathbb{Z}_p) \to \mathrm{H}_1(G, X_S \otimes \mathbb{Z}_p) \to \cdots.$$

Theorem 6.4(iii) of [Bro82] implies that, for any abelian group H, we have a canonical group isomorphism $\bigwedge_{\mathbb{Z}_p}^2 (H \otimes \mathbb{Z}_p) \xrightarrow{\sim} \mathrm{H}_2(H, \mathbb{Z}_p)$. This result, combined with Lemma 3.1.6, parts ii and iii, yields isomorphisms $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathrm{H}_2(G_{v_0}, \mathbb{Z}_p)$ and $(\mathbb{Z}/p\mathbb{Z})^3 \xrightarrow{\sim} \mathrm{H}_2(G, \mathbb{Z}_p)$, respectively. Therefore, the long exact sequence above becomes

$$\cdots \to \mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^3 \to \mathrm{H}_1(G, X_S \otimes \mathbb{Z}_p) \to \cdots.$$

This sequence, combined with equality (9), shows that

$$|\widehat{\mathrm{H}}^0(G, U_{K,S} \otimes \mathbb{Z}_p)| = |\mathrm{H}_1(G, X_S \otimes \mathbb{Z}_p)| \geqslant p^2. \tag{10}$$

Inequalities (10), (8), and (7) lead to a contradiction $(p \geqslant p^2)$. $\qquad\square$

3.4 Proof of Theorem 3.2.1

In this section, we provide a proof of Theorem 3.2.1. Let us assume for the moment that K/k is an arbitrary finite abelian extension of global fields (of arbitrary characteristic) of Galois group $G(K/k)$. Let Σ be a finite, non-empty set of primes in k, containing at least all the infinite primes and those which ramify in K/k. Let ℓ be a prime number. We denote by $K_\Sigma^{(\ell)}$ the maximal abelian extension of K of ℓ-power degree, unramified everywhere, and totally split at all the primes in Σ_K. The maximality of the field $K_\Sigma^{(\ell)}$ forces it to be a Galois extension of the base field k. This gives $G(K_\Sigma^{(\ell)}/K)$ a natural $\mathbb{Z}[G(K/k)]$-module structure, with $\sigma \in G(K/k)$ acting on $x \in G(K_\Sigma^{(\ell)}/K)$ by 'lift and conjugation' (i.e. $\sigma * x := \overline{\sigma} x \overline{\sigma}^{-1}$, where $\overline{\sigma}$ is an arbitrary lift of σ to $G(K_\Sigma^{(\ell)}/k)$). Class-field

theory shows that the usual Artin map (11) gives a group isomorphism

$$A_{K,\Sigma}^{(\ell)} \xrightarrow{\sim} G(K_\Sigma^{(\ell)}/K), \tag{11}$$

which is also a $\mathbb{Z}[G(K/k)]$-isomorphism. In the following, if H is a group and $x, y \in H$, then $[x, y] := xyx^{-1}y^{-1}$ denotes the usual commutator of x and y. Also, I_H denotes the usual augmentation ideal of $\mathbb{Z}[H]$.

Now, we return to the notation and definitions introduced in §§ 3.1 and 3.2. Since G is a p-group, $\mathbb{Z}_p[G]$ is a local ring whose maximal ideal is $M := I_G\mathbb{Z}_p[G] + p\mathbb{Z}_p[G]$. Consequently, Nakayama's lemma implies that $A_{K,S_0}^{(p)}$ can be generated by two elements as a $\mathbb{Z}_p[G]$-module if and only if the associated module of G-coinvariants

$$(A_{K,S_0}^{(p)})_G := A_{K,S_0}^{(p)}/I_G \cdot A_{K,S_0}^{(p)}$$

can be generated by two elements as an abelian group. By class field theory, the Artin reciprocity map (11) identifies $(A_{K,S_0}^{(p)})_G$ with the Galois group $\mathrm{Gal}(L/K)$ of a finite, unramified, abelian p-extension L of K, with the following properties. Each prime of K over v_0 splits completely in L, L is a Galois extension of k and $\mathrm{Gal}(L/K)$ is contained in the center of $\mathrm{Gal}(L/k)$. Let I be the inertia group in $\mathrm{Gal}(L/k)$ of a fixed prime w over v_0 in L. Since L/K_0 is unramified and K_0/k is totally ramified over v_0, we conclude that I maps isomorphically to $G_0 = \mathrm{Gal}(K_0/k) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^2$, under the natural restriction map $\mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(K_0/k)$. Let σ_1, σ_2 be generators for I as an abelian group. Since G_0 is a quotient of $G = \mathrm{Gal}(K/k) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^3$, we can find an element $\sigma \in \mathrm{Gal}(L/k)$, such that the images of σ_1, σ_2 and σ in G generate G. Since G is abelian, the commutators $c_1 := [\sigma, \sigma_1]$ and $c_2 := [\sigma, \sigma_2]$ lie in $\mathrm{Gal}(L/K)$. Since σ_1 and σ_2 lie in the abelian group I, we have $[\sigma_1, \sigma_2] = e$. Let H be the subgroup of $\mathrm{Gal}(L/K)$ generated by c_1 and c_2. We claim that the quotient $\mathrm{Gal}(L/k)/H$ is abelian. To show this, it will suffice to find a set X of generators of $\mathrm{Gal}(L/k)$, such that $[x, x'] \in H$, for all $x, x' \in X$. Let

$$X := \{\sigma, \sigma_1, \sigma_2\} \cup \mathrm{Gal}(L/K).$$

Since the images of σ, σ_1 and σ_2 in $G = \mathrm{Gal}(L/k) \xrightarrow{\sim} \mathrm{Gal}(L/k)/\mathrm{Gal}(L/K)$ generate G, X generates $\mathrm{Gal}(L/k)$. Also, since $\mathrm{Gal}(L/K)$ is contained in the center of $\mathrm{Gal}(L/k)$, we have $[x, x'] \in H$, for all $x, x' \in X$. Therefore, $\mathrm{Gal}(L/k)/H$ is indeed abelian. Consequently, the field $F := L^H$ (maximal, fixed by H) is an abelian p-extension of k, containing K, which is unramified over K, and which has the property that every prime of K over v_0 splits completely in F. Lemma 3.1.2, part iv implies that $F = K$. This proves that $\mathrm{Gal}(L/K) = H$ and, therefore, $\mathrm{Gal}(L/K)$ is generated as an abelian group by two elements c_1 and c_2. This implies that $(A_{K,S_0}^{(p)})_G$ is generated as an abelian group by two elements, which implies Theorem 3.2.1, as we have shown above.

4. A refinement of Brumer's conjecture

This section has two goals. First, we will provide links between Questions A and B and a natural refinement of Brumer's conjecture for arbitrary global fields. Secondly, as a consequence of the results proved in § 3, we will show that the refinement of Brumer's conjecture is, in general, false in characteristic $p > 0$.

4.1 The statement

Let K/k be an abelian extension of global fields of Galois group G. Let S_0 be a finite, non-empty set of primes in k, containing at least all the infinite primes, as well as all the primes which ramify in K/k. Let $\mathcal{A}(K/k) := \mathrm{Ann}_{\mathbb{Z}[G]}(\mu_K)$ be the annihilator of the $\mathbb{Z}[G]$-module μ_K of roots of unity in K. The following remarkable integrality result was proved independently by Deligne and Ribet [DR80]

and Barsky [Bar78] and Cassou-Nogues [Cas79] in the number field case, and Deligne (see [Tat84, V]) and Hayes [Hay85] in the function field case.

THEOREM 4.1.1. *If $\alpha \in \mathcal{A}(K/k)$, then $\alpha \cdot \Theta_{K/k,S_0}(0) \in \mathbb{Z}[G]$.*

We are now ready to state Brumer's conjecture, which is an attempt to generalize the classical theorem of Stickelberger.

CONJECTURE 4.1.2 (Brumer). *One has an inclusion of $\mathbb{Z}[G]$-ideals*

$$\mathcal{A}(K/k) \cdot \Theta_{K/k,S_0}(0) \subseteq \mathrm{Ann}_{\mathbb{Z}[G]}(A_{K,S_0}).$$

Equivalently, for all primes ℓ, one has an inclusion of $\mathbb{Z}_{(\ell)}[G]$-ideals

$$\mathbb{Z}_{(\ell)}\mathcal{A}(K/k) \cdot \Theta_{K/k,S_0}(0) \subseteq \mathrm{Ann}_{\mathbb{Z}_{(\ell)}[G]}(A_{K,S_0}^{(\ell)}).$$

In the case of function fields, Brumer's conjecture was proved independently and with different methods by Deligne [Tat84, V] and Hayes [Hay85]. In the case of number fields, this conjecture is far from being proved. The statement has been known to hold true for a long time if $k = \mathbb{Q}$, as a result of the classical theorem of Stickelberger (see [Was96]). Wiles developed a series of results and techniques in [Wil90], which lead to a proof of the conjecture above in the case where K is a CM-field, k is totally real, $\ell \nmid |G|$ and S_0 satisfies extra hypotheses. Finally, by using the techniques developed in [Wil90], Greither proves the conjecture above, for a very special class of CM extensions K of totally real fields k, under the assumption that $\ell \neq 2$ (see [Gre00]).

If R is a Noetherian commutative ring and M is a finitely generated R-module, we denote by $\mathrm{Fitt}_R(M)$ the R-Fitting ideal of M. For the definition and properties of Fitting ideals used in this paper, we refer the reader to [Pop99]. We will only recall here the fact that we always have an inclusion $\mathrm{Fitt}_R(M) \subseteq \mathrm{Ann}_R(M)$, and the equality is very rare. (Equality happens if, for instance, M is a cyclic R-module.) We are now ready to state the refinement (or strong form) of Brumer's conjecture.

STATEMENT SBr. *The following inclusion of $\mathbb{Z}[G]$-ideals holds true:*

$$\mathcal{A}(K/k) \cdot \Theta_{K/k,S_0}(0) \subseteq \mathrm{Fitt}_{\mathbb{Z}[G]}(A_{K,S_0}).$$

For any prime ℓ, we can formulate the following ℓ-adic version of Statement SBr.

STATEMENT SBr$_{(\ell)}$. *The following inclusion of $\mathbb{Z}_{(\ell)}[G]$-ideals holds true:*

$$\mathbb{Z}_{(\ell)}\mathcal{A}(K/k) \cdot \Theta_{K/k,S_0}(0) \subseteq \mathrm{Fitt}_{\mathbb{Z}_{(\ell)}[G]}(A_{K,S_0}^{(\ell)}).$$

Since the Fitting ideal behaves nicely with respect to extensions of scalars and direct sums (see [Pop99]), and since $A_{K,S_0} = \bigoplus_\ell A_{K,S_0}^{(\ell)}$, Statement SBr is true if and only if Statement SBr$_{(\ell)}$ is true, for all prime numbers ℓ.

Remark 6. We would like to emphasize that Brumer himself never conjectured that Statement SBr is true. However, the motivation for introducing the refinement Statement SBr of Brumer's conjecture is threefold. First, evidence in support of Statement SBr has been found by various researchers over the years. In the case of function fields, we proved that a statement even stronger than Statement SBr holds true for constant field extensions (see Theorem 4.2.9 in [Pop99]). We also showed that Statement SBr$_{(\ell)}$ holds true for general function field extensions K/k, provided that $\ell \nmid |G|$ (see Theorem 3.1.1 in [Pop99]). In the case of CM-extensions K of totally real number fields k, Greither [Gre00] showed that the 'minus part' of Statement SBr$_{(\ell)}$ holds true, provided that $\ell \neq 2$ and K/k satisfies extra properties of cohomological type. Also, our close analysis of [Wil90] revealed that

Wiles's techniques lead to a proof of Statement $\mathrm{SBr}_{(\ell)}$, for CM-extensions K of totally real fields k under his extra hypotheses on S_0 for primes $\ell \nmid |G|$.

Secondly, Statement SBr has very interesting links to the versions 'over $\mathbb{Z}$' of Stark's conjecture for abelian L-functions of arbitrary order of vanishing at $s = 0$, formulated by Rubin in [Rub96] and the present author in [Pop02]. We show in [Pop99, § 2] that, in the case of function fields for example, a slightly stronger version of Statement SBr implies Rubin's Conjecture B. A similar argument can be used to show that the same strong version of Statement SBr also implies our Conjecture C. Also, as the interested reader will see in § 4.2 below, Statement SBr has connections to Questions A and B, formulated in § 2 above.

Thirdly, the methods employed so far by various researchers in their attempts to prove Brumer's conjecture seem to lead more naturally to Fitting ideals than annihilators of ideal-class groups. More precisely, the main techniques employed in [Wil90] and [Gre00] rely in an essential way on the Main Conjecture in Iwasawa theory. The Main Conjecture is a statement linking values of L-functions to the Fitting ideal of a certain Λ-module, obtained as a projective limit of ideal-class groups, where Λ is the Iwasawa algebra associated with the cyclotomic $\mathbb{Z}_p$-extension. Wiles [Wil90] and Greither [Gre00] 'project' the Main Conjecture to finite levels of the $\mathbb{Z}_p$-extension and obtain statements about Fitting ideals of ideal-class groups, in the spirit of Statement SBr. Finally, in the case of function fields, in [Pop99] we use the Weil–Grothendieck interpretations of global L-functions in terms of characteristic polynomials of the action of a Frobenius morphism on various ℓ-adic étale and crystalline cohomology groups, to prove statements of the type of Statement $\mathrm{SBr}_{(\ell)}$, in the cases mentioned above. Once again, the use of characteristic polynomials (and therefore determinants) leads naturally to Fitting ideals rather than annihilators.

4.2 Links between Questions A and B and Statement SBr

In this section, we provide links between Statement $\mathrm{SBr}_{(\ell)}$ and Questions $\mathrm{B}_{(\ell)}$ and $\mathrm{A}_{(\ell)}$, for a given prime ℓ. As a consequence, we show that Statement $\mathrm{SBr}_{(p)}$ and, consequently, SBr are in general false in characteristic p. We are still working under the hypotheses and notation of § 4.1. In particular, our global fields are of arbitrary characteristic.

PROPOSITION 4.2.1. *Let ℓ be a prime number. Let $S = S_0 \cup \{v_1, v_2\}$, with v_1, v_2 distinct primes in k, split in K/k and not belonging to S_0. Assume the following.*

i) *$A_{K,S}^{(\ell)}$ is trivial.*

ii) *Statement $\mathrm{SBr}_{(\ell)}$ is true.*

Then, Question $\mathrm{B}_{(\ell)}$ has an affirmative answer.

Proof. Let $W = (w_1, w_2)$, with w_1 and w_2 primes in K, sitting above v_1 and v_2, respectively. For $i = 1, 2$, let $\widehat{w_i}^{(\ell)}$ be the projection of the class $\widehat{w_i}$ of w_i in A_{K,S_0}, onto the ℓ-Sylow component $A_{K,S_0}^{(\ell)}$ of A_{K,S_0}. Assumption i above shows that $\widehat{w_1}^{(\ell)}$ and $\widehat{w_2}^{(\ell)}$ generate the $\mathbb{Z}_{(\ell)}[G]$-module $A_{K,S_0}^{(\ell)}$ (see also Remark 5). Therefore, assumption ii above, combined with the definition of the Fitting ideal, shows that there exist 2×2 matrices $A_k = (a_{ij}^k)_{1 \leqslant i,j \leqslant 2}$, for $k = 1, \ldots, n$, with entries a_{ij}^k in $\mathbb{Z}_{(\ell)}[G]$, such that the following hold true.

i) $a_{i1}^k \cdot \widehat{w_1}^{(\ell)} + a_{i2}^k \cdot \widehat{w_2}^{(\ell)} = 0$ in $A_{K,S_0}^{(\ell)}$, for all $k = 1, \ldots, n$, and $i = 1, 2$.

ii) $w_K \cdot \Theta_{K/k,S_0}(0) = \sum_{k=1}^n \det(A_k)$.

It is easy to see that, since A_{K,S_0} is finite, part i above implies that one can find $\beta \in \mathbb{Z}$, such that $\mathrm{ord}_\ell(\beta) = 0$ (i.e. $\beta^{-1} \in \mathbb{Z}_{(\ell)}$), $\beta \cdot a_{ij}^k \in \mathbb{Z}[G]$, for all i, j, k, and:

i') $\beta a_{i1}^k \cdot \widehat{w_1} + \beta a_{i2}^k \cdot \widehat{w_2} = 0$ in A_{K,S_0}, for all $k = 1, \ldots, n$, and $i = 1, 2$.

Let us fix β satisfying the above properties. Then part i' implies the existence of S-units $u_1^{(k)}, u_2^{(k)} \in U_{K,S}$, for $k = 1, \ldots, n$, such that the following hold true:

$$\sum_{\sigma \in G} \mathrm{ord}_{w_j^\sigma}(u_i^{(k)}) \cdot \sigma = \beta \cdot a_{ij}^k, \text{ for all } i, j, \text{ and } k. \tag{12}$$

Since v_1 and v_2 are finite primes, completely split in K/k, we have $\Theta_{K/k,S}^{(2)}(s) = (1 - \mathrm{N}v_1^{-s})(1 - \mathrm{N}v_2^{-s})\Theta_{K/k,S_0}(s)$. Therefore, $\Theta_{K/k,S}^{(2)}(0) = \log(\mathrm{N}v_1)\log(\mathrm{N}v_2)\Theta_{K/k,S_0}(0)$. If we combine this equality with (12), part ii above, and the definition of the regulator R_W, we obtain

$$\Theta_{K/k,S}^{(2)}(0) = R_W(\varepsilon_{S,\ell}),$$

where $\varepsilon_{S,\ell} := (\beta^{-1}/w_K)\sum_{k=1}^n u_1^{(k)} \wedge u_2^{(k)}$ is clearly in $(1/w_K)^2 \cdot \mathbb{Z}_{(\ell)}\bigwedge_G^2 \widetilde{U_{K,S}}$. This shows that Question $\mathrm{B}_{(\ell)}$ indeed has an affirmative answer. $\qquad\square$

COROLLARY 4.2.2. *Let K/k be the extension of global fields of characteristic p and S_0 the set of primes in k constructed in §§ 3.1 and 3.2. Then, Statements $\mathrm{SB}_{(p)}$ and (consequently) Statement $\mathrm{SBr}_{(\ell)}$ are false.*

Proof. It is obviously sufficient to show that Statement $\mathrm{SB}_{(p)}$ is false. Let $S = S_0 \cup \{v_1, v_2\}$ be the set of primes in k defined in Definition 3.2.2. Then Remark 5, shows that the hypotheses in Proposition 4.2.1 are satisfied by K/k, S and the prime $\ell := p$. On the other hand, Theorem 3.3.2 shows that Question $\mathrm{B}_{(p)}$ has a negative answer. Therefore, Proposition 4.2.1 implies that Statement $\mathrm{SB}_{(p)}$ is false. $\qquad\square$

Remark 7. At Victor Kolyvagin's suggestion, we also searched for counter-examples for the ℓ-part of the refinement of Brumer's conjecture Statement $\mathrm{SBr}_{(\ell)}$, in the case where $\mathrm{char}(k) = p > 0$ and $\ell \neq p$. We would like to report here that we have found an infinite class of such counter-examples. As the techniques involved in dealing with such counter-examples are quite different from those developed in this paper, the detailed constructions will appear elsewhere.

Obviously, a proof almost identical to that of Proposition 4.2.1 leads to the following 'global' link between Question B and Statement SBr.

PROPOSITION 4.2.3. *Let $S := S_0 \cup \{v_1, v_2\}$, with v_1, v_2 distinct primes in k, split in K/k, and not belonging to S_0. Assume the following.*

  i) *$A_{K,S}$ is trivial.*
  ii) *Statement SBr is true.*

Then, Question B has an affirmative answer.

The proof is similar to the proof of Proposition 4.2.1 and is left to the reader.

Next, we establish links between Question A and Statement SBr. We remind the reader that, if G is a finite group and M is a $\mathbb{Z}[G]$-module, we say that M is G-cohomologically trivial if $\widehat{\mathrm{H}}^i(H, M) = 0$, for all subgroups H of G and all $i \in \mathbb{Z}$.

PROPOSITION 4.2.4. *Let ℓ be a prime number. Let $S = S_0 \cup \{v_1, v_2\}$, with v_1, v_2 distinct primes in k, split in K/k and not belonging to S_0. Assume the following.*

  i) *$A_{K,S}^{(\ell)}$ is trivial.*
  ii) *$A_{K,S_0}^{(\ell)}$ is G-cohomologically trivial.*
  iii) *Statement $\mathrm{SBr}_{(\ell)}$ is true.*

Then, Question $\mathrm{A}_{(\ell)}$ has an affirmative answer.

We will need two lemmas of purely algebraic nature.

LEMMA 4.2.5. *Let R be a commutative, semi-local Noetherian ring and let P be a finitely generated, projective R-module. Assume that the local ranks $\mathrm{rk}_{R_{\mathfrak{m}}}(P_{\mathfrak{m}})$ are independent of the maximal ideal $\mathfrak{m}$ of R. Then, P is a free R-module of rank equal to the local ranks.*

For a proof, see exercise 4.13* of [Eis94].

LEMMA 4.2.6 (compare with Proposition 4 in [CG98]). *Let R denote a commutative, semi-local Noetherian ring, and let $Q(R)$ be its total ring of fractions. Let M be a finitely generated R-module, such that $M \otimes_R Q(R) = 0$. Assume that the projective dimension of M over R is at most 1. Then, the following hold true.*

i) $\mathrm{Fitt}_R(M)$ *is a principal ideal, generated by a non-zero divisor of R.*

ii) *Let $X = \{x_1, \ldots, x_n\} \subseteq M$ be a fixed set of generators for the R-module M. Then, we can choose a generator for $\mathrm{Fitt}_R(M)$ of the form $\det(A)$, where $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ is an $n \times n$ matrix with entries in R, such that $\sum_{j=1}^n a_{ij} \cdot x_j = 0$ in M, for all $i = 1, \ldots, n$.*

Proof. We start by noting that, since R is Noetherian (and therefore the ideal (0) admits a primary decomposition in R), $Q(R)$ can be written as a direct sum of local Artin rings $Q(R) = \bigoplus_{\mathfrak{p}} R_{\mathfrak{p}}$. Here $R_{\mathfrak{p}}$ denotes the localization of R at the prime ideal $\mathfrak{p}$, and $\mathfrak{p}$ runs through the (finite) set of minimal prime ideals of R. This observation also shows that the condition $M \bigotimes_R Q(R) = 0$ is equivalent to $M_{\mathfrak{p}} = 0$ or, equivalently, $\mathrm{Ann}_R(M) \not\subseteq \mathfrak{p}$ for all minimal prime ideals $\mathfrak{p}$ of R.

We will now prove parts i and ii simultaneously. For the fixed set of generators X of M, we have an exact sequence of R-modules

$$0 \to K \xrightarrow{i} R^n \xrightarrow{\pi} M \to 0,$$

where π sends the elements of an ordered canonical basis $\mathcal{E} := (e_1, \ldots, e_n)$ of R^n into $x_1, x_2, \ldots, x_n$, respectively, $K := \ker(\pi)$, and i is the inclusion map. Since $\mathrm{pd}_R(M) \leqslant 1$, K is a projective R-module and, therefore, locally free (see [Mil71, Lemma 1.2]). Let $\mathfrak{m}$ be a maximal ideal of R and $\alpha_{\mathfrak{m}} := \mathrm{rk}_{R_{\mathfrak{m}}}(K_{\mathfrak{m}})$. If we localize the exact sequence above at $\mathfrak{m}$, we obtain the following exact sequence of $R_{\mathfrak{m}}$-modules:

$$0 \to R_{\mathfrak{m}}^{\alpha_{\mathfrak{m}}} \to R_{\mathfrak{m}}^n \xrightarrow{\pi_{\mathfrak{m}}} M_{\mathfrak{m}} \to 0.$$

However, there always exists a minimal prime ideal $\mathfrak{p}$ of R, such that $\mathfrak{p} \subseteq \mathfrak{m}$. If we localize the above exact sequence even further, at $\mathfrak{p}$, and take into account that $M_{\mathfrak{p}} = 0$, we obtain an isomorphism of $R_{\mathfrak{p}}$-modules $R_{\mathfrak{p}}^{\alpha_{\mathfrak{m}}} \xrightarrow{\sim} R_{\mathfrak{p}}^n$. This shows that $\alpha_{\mathfrak{m}} = n$ (see [Eis94, Corollary 4.4(b)]). We now apply Lemma 4.2.5 to the R-module K to conclude that K is a free R-module of rank n. Let us fix an ordered R-basis $\mathcal{K} := (k_1, \cdots, k_n)$ for K, and let $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ be the matrix representation of the R-morphism i with respect to bases $\mathcal{K}$ and $\mathcal{E}$. Since i is injective, $\det(A)$ is a non-zero divisor in R. On the other hand, since $K \xrightarrow{\sim} R^n$, the definition of the Fitting ideal shows that $\mathrm{Fitt}_R(M) = \det(A)R$. $\square$

Proof of Proposition 4.2.4. Let w_1, w_2, W, $\widehat{w_i}$, and $\widehat{w_i}^{(\ell)}$, for $i = 1, 2$, be as in the proof of Proposition 4.2.1. We will apply Lemma 4.2.6 to the semi-local ring $R := \mathbb{Z}_{(\ell)}[G]$, the finitely generated R-module $M := A_{K,S_0}^{(\ell)}$ and its set of R-generators $X := \{\widehat{w_1}^{(\ell)}, \widehat{w_2}^{(\ell)}\}$. Since M is finite and $Q(R) = \mathbb{Q}[G]$, we clearly have $M \otimes_R Q(R) = 0$. Also, since M is G-cohomologically trivial, we have $\mathrm{pd}_R(M) \leqslant 1$ (see [CF67, IV.9, Theorem 9]). According to Lemma 4.2.6, we can choose a matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant 2}$ with entries in R, such that $\mathrm{Fitt}_R(M) = \det(A) \cdot R$, $\det(A)$ is a non-zero divisor in R, and $\sum_{j=1}^2 a_{ij} \cdot \widehat{w_j}^{(\ell)} = 0$ in M for all $i = 1, 2$. Moreover, if we multiply the entries of A by a suitably chosen $\beta \in \mathbb{Z}_{(\ell)}^{\times}$, as in the proof of Proposition 4.2.1, we can further assume that

A in fact has entries in $\mathbb{Z}[G]$, and $\sum_{j=1}^{2} a_{ij} \cdot \widehat{w_j} = 0$ in A_{K,S_0}, for all $i = 1, 2$. As in the proof of Proposition 4.2.1, these equalities imply the existence of two S-units $u_1', u_2' \in U_{K,S}$, such that

$$R_W(u_1' \wedge u_2') = \log(\mathrm{N}v_1)\log(\mathrm{N}v_2)\det(A). \tag{13}$$

Now, hypothesis iii in Proposition 4.2.4, combined with the fact that $\det(A)$ is a non-zero divisor, shows, for a suitably chosen $\beta' \in \mathbb{Z}_{(\ell)}^{\times}$, that there exists a set $\{\xi_\alpha | \alpha \in \mathcal{A}(K/k)\} \subseteq \mathbb{Z}[G]$, satisfying

$$\beta' \cdot \alpha \cdot \Theta_{K/k,S_0}(0) = \xi_\alpha \cdot \det(A) \quad \text{and} \quad \xi_\alpha = (\alpha/w_K) \cdot \xi_{w_K}, \quad \text{for all } \alpha \in \mathcal{A}(K/k). \tag{14}$$

For a unit $u \in U_{K,S}$, let $\tilde{u}$ denote its image in $\mathbb{Q}U_{K,S}$ via the canonical $\mathbb{Z}[G]$-morphism $U_{K,S} \longrightarrow \mathbb{Q}U_{K,S}$. Let $\varepsilon := \widetilde{u_1'}^{(\xi_{w_K}/w_K)} \in \mathbb{Q}U_{K,S}$. Let $\varepsilon_\alpha := u_1'^{\xi_\alpha} \in U_{K,S}$, for all $\alpha \in \mathbb{Z}[G]$. Equalities (14) imply that the following hold true.

 i) $\varepsilon^\alpha = \widetilde{\varepsilon_\alpha}$, for all $\alpha \in \mathcal{A}(K/k)$.

 ii) $\varepsilon_\alpha^\gamma = \varepsilon_\gamma^\alpha$, for all $\alpha, \gamma \in \mathcal{A}(K/k)$.

We combine the last equalities with Proposition 1.2 in [Pop02] to conclude that there exists a unit $u_1 \in U_{K,S}$, such that $\varepsilon = \widetilde{u_1}^{1/w_K}$ in $\mathbb{Q}U_{K,S}$, and $K(u_1^{1/w_K})/k$ is a Galois abelian extension. Let $u_2 := u_2'^{w_K} \cdot u_1 \in U_{K,S}$. Then, we clearly have an equality of fields $K(u_1^{1/w_K}) = K(u_2^{1/w_K})$. Moreover, (13) and (14) show that

$$\Theta_{K/k,S}^{(2)} = \log(\mathrm{N}v_1)\log(\mathrm{N}v_2)\Theta_{K/k,S_0}(0) = (\beta'^{-1}/w_K^2)R_W(u_1 \wedge u_2).$$

This shows that, indeed, Question $\mathrm{A}_{(\ell)}$ has an affirmative answer. $\qquad\square$

REFERENCES

Bar78   D. Barsky, *Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels*, Groupe d'Etude d'Analyse Ultramétrique, Exp. No. 16 (1977/78), eds Y. Amice, D. Barsky and P. Robba (Secretariat Mathématique, Paris, 1978).

Bro82   K. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87 (Springer, Berlin, 1982).

Bur97   D. Burns, *Iwasawa theory and p-adic Hodge theory over non-commutative algebras I, II*, Preprints (1997).

Bur03   D. Burns, *Equivariant Tamagawa numbers and refined abelian Stark conjectures*, J. Math. Sci. Univ. Tokyo **10** (2003), 225–259.

CF67   J. W. S. Cassels and A. Fröhlich, *Algebraic number theory* (Academic Press, New York, 1967).

Cas79   P. Cassou-Nogues, *Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques*, Invent. Math. **51** (1979), 29–59.

Chi83   T. Chinburg, *On the Galois structure of algebraic integers and S-units*, Invent. Math. **74** (1983), 321–349.

Chi85   T. Chinburg, *Exact sequences and Galois module structure*, Ann. of Math. (2) **121** (1985), 351–376.

CG98   P. Cornacchia and C. Greither, *Fitting ideals of class groups of real fields with prime power conductor*, J. Number Theory **73** (1998), 459–471.

DR80   P. Deligne and K. Ribet, *Values of L-functions at negative integers over totally real fields*, Invent. Math. **159** (1980), 227–286.

Eis94   D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150 (Springer, Berlin, 1994).

Gra99   D. Grant, *Units from 5-torsion of the Jacobian of $y^2 = x^5 + 1/4$ and the conjectures of Stark and Rubin*, J. Number Theory **77** (1999), 227–251.

Gre00   C. Greither, *Some cases of Brumer's conjecture*, Math. Z. **233** (2000), 515–534.

Hay85   D. Hayes, *Stickelberger elements in function fields*, Compositio Math. **55** (1985), 209–239.

Mil71   J. Milnor, *Introduction to Algebraic K-Theory* (Princeton University Press, NJ, and Tokyo University Press, 1971).

Pop99   C. D. Popescu, *On a refined Stark Conjecture for function fields*, Compositio Math. **116** (1999), 321–367.

Pop02   C. D. Popescu, *Base change for Stark-type conjectures 'over $\mathbb{Z}$'*, J. Reine Angew Math. **542** (2002), 85–111.

Rub96   K. Rubin, *A Stark conjecture 'over $\mathbb{Z}$' for abelian L-functions with multiple zeros*, Ann. Inst. Fourier **46** (1996), 33–62.

San01   J. W. Sands, *Stark's Question and Popescu's Conjecture for abelian L-functions*, in *Number theory, Proc. Turku symposium on number theory in memory of Kustaa Inkeri*, eds M. Jutila and T. Metänkylä (Walter de Gruyter, 2001), 305–316.

Sta71   H. Stark, *L-functions at $s = 1$, I*, Adv. Math. **7** (1971), 301–343; *L-functions at $s = 1$, II*, Adv. Math. **17** (1975), 60–92; *L-functions at $s = 1$, III*, Adv. Math. **22** (1976), 64–84; *L-functions at $s = 1$, IV*, Adv. Math. **35** (1980), 197–235.

Sta80   H. Stark, *Derivatives of L-series at $s = 0$*, Abstracts Amer. Math. Soc. **1** (1980), 28.

Tat84   J. Tate, *Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$*, Progress in Mathematics, vol. 47 (Birkhäuser, Basel, 1984).

Tan97   B. Tangedal, *A question of Stark*, Pacific J. Math. **180** (1997), 187–199.

Was96   L. Washington, *Introduction to cyclotomic fields*, second edition, Graduate Texts in Mathematics, vol. 83 (Springer, Berlin, 1996).

Wil90   A. Wiles, *On a conjecture of Brumer*, Ann. of Math. (2) **131** (1990), 555–565.

Cristian D. Popescu   cpopescu@math.ucsd.edu

University of California, San Diego, Department of Mathematics, 9500 Gilman Drive, La Jolla, CA 92093-0112, USA