ON THE FONTAINE-MAZUR CONJECTURE FOR NUMBER FIELDS AND AN ANALOGUE FOR FUNCTION FIELDS

JOSHUA BRANDON HOLDEN

Abstract. The Fontaine-Mazur Conjecture for number fields predicts that infinite ℓ-adic analytic groups cannot occur as the Galois groups of unramified ℓ-extensions of number fields. We investigate the analogous question for function fields of one variable over finite fields, and then prove some special cases of both the number field and function field questions using ideas from class field theory, ℓ-adic analytic groups, Lie algebras, arithmetic algebraic geometry, and Iwasawa theory.

1. Introduction

A conjecture of Fontaine and Mazur, in [11], says:

Conjecture 1 (Fontaine-Mazur)**.** *Let k be a number field and ℓ any prime. If M is an unramified ℓ-adic analytic ℓ-extension of k, then M is a finite extension of k.*

(See below for definitions.) It seems reasonable and straightforward to pose the same conjecture in the function field case. We immediately see that the naive version must be false, because the extension of a function field k over a finite field $\mathbf{F}$ given by constant field ℓ-extensions of $\mathbf{F}$ is already infinite and ℓ-adic analytic. The next logical question to ask would be something like the following:

Question 1. *Let k be a function field over a finite field $\mathbf{F}$ of characteristic p and order q, and ℓ a prime not equal to p. Let $K = k\mathbf{F}_{\ell^\infty}$ be obtained from k by taking the maximal ℓ-extension of the constant field. If M is an unramified ℓ-adic analytic ℓ-extension of k, and M does not contain K, must M be a finite extension of k?*

The answer is no; in fact Ihara has constructed examples (for example, see [18]) of function fields k which have, for all but finitely many ℓ not equal to p, a Galois extension M with no extension of the constant field, and with $\mathrm{Gal}(M/k)$ isomorphic to $\mathrm{PSL}_2(\mathbf{Z}_\ell)$. Frey, Kani, and Völklein, using another construction based on the one described in [12], have also achieved similar results.

Nevertheless, it is possible to prove that the answer is yes in some special cases. These cases are of interest not only independently, but also because the methods used to address them, which involve basic facts about abelian varieties over finite fields, can be adapted to number fields through the use of Iwasawa $\mathbf{Z}_\ell$-extensions and ℓ-adic L-functions, as we will show. (It is likely that they can also be used to address some cases of a conjecture recently made by de Jong, in [8], about unramified extensions of function fields. A future paper will address this issue.) These methods, which stem from work of Boston ([3, 4]) using group

Date: 21 August 1999.

1991 *Mathematics Subject Classification.* Primary 11R37; Secondary 11R58, 11R42, 20E18.

Accepted for publication in the Journal of Number Theory, as of August 25, 1999.

automorphisms, also introduce ℓ-adic Lie algebras in a crucial way, relating them to standard constructions of arithmetic algebraic geometry, such as the Tate module.

Conjecture 1 comes from two sources; one is a broad conjecture of Fontaine and Mazur about irreducible ℓ-adic representations of absolute Galois groups, positing necessary and sufficient local conditions for the representation to "come from algebraic geometry" in a certain specific sense. When combined with the Tate Conjecture about the subspace of étale cohomology generated by algebraic cycles, this broader conjecture yields the more narrow Conjecture 1. The other source is the Golod-Shafarevich proof that infinite class field towers exist; these give infinite unramified ℓ-extensions and the above conjecture says that such extensions cannot be analytic. (See [14] for more on the link with Golod-Shafarevich.)

For another formulation of Conjecture 1, consider the following definitions from [10]:

Definition 1.1. Let G be a pro-ℓ group. G is *powerful* if ℓ is odd and $G/\overline{G^\ell}$ is abelian, or if $\ell = 2$ and $G/\overline{G^4}$ is abelian. (G^n is the subgroup of G generated by the n-th powers of elements in G, and $\overline{G^n}$ is its closure.)

Definition 1.2. A pro-ℓ group is *uniformly powerful*, or just *uniform*, if (i) G is finitely generated, (ii) G is powerful, and (iii) for all i, $\left[\overline{G^{\ell^i}} : \overline{G^{\ell^{i+1}}}\right] = \left[G : \overline{G^\ell}\right]$.

(and for completeness)

Definition 1.3. Let G be a topological group. We call G an *ℓ-adic analytic group* (or *ℓ-adic Lie group*) if G has the structure of a ℓ-adic analytic manifold such that the function $g : G \times G \to G$ defined by $(x, y) \mapsto xy^{-1}$ is analytic.

(This is the same as the definition of a real Lie group over the real numbers. Such groups enter into the Fontaine-Mazur program as groups of ℓ-adic representations, so it may be convenient to think of such examples as $SL_n(\mathbf{Z}_\ell)$ and its subgroups.)

And the following important theorems:

Theorem 1.4 (4.8 of [10])**.** *A powerful finitely generated pro-ℓ group is uniform if and only if it is torsion-free.*

(All of the Galois groups we will be considering are, in fact, finitely generated.)

Theorem 1.5 (9.34 of [10]; Lazard, 1965)**.** *Let G be a topological group. Then G has the structure of an ℓ-adic analytic group if and only if G contains an open subgroup which is a uniformly powerful pro-ℓ group.*

Using these, we see that the Conjecture 1 is equivalent to:

Conjecture 2. *Let k, ℓ be as in Conjecture 1. If M is a uniformly powerful unramified ℓ-extension of k, then $M = k$.*

(Note that a finite uniformly powerful group must be trivial, by Theorem 1.4.)

Similarly, using the above and the fact that K/k is a $\mathbf{Z}_\ell$-extension, Question 1 is equivalent to:

Question 2. *Let k, $\mathbf{F}$, p, q, ℓ be as in Question 1. If M is a uniformly powerful unramified ℓ-extension of k with no constant field extension, must we have $M = k$?*

As special cases where the answer to Question 2 is yes, we have the following theorems. The first was originally proved by Boston for number fields in [4]; the same proof applies for function fields.

Theorem 1. *If a function field k has a subfield k_0 such that k/k_0 is cyclic of degree prime to ℓ and such that ℓ does not divide the class number $h(k_0)$, then any everywhere unramified* *powerful (*a fortiori *uniform) pro-ℓ extension of k, Galois over k_0, with no constant field extension, is finite.*

(This is true even if $\ell = p$, unlike the following theorems.)

The following two theorems will be proved in Sections 2 and 4, respectively.

Theorem 2. *Let k_0 be a function field over a finite field of characteristic p, and let k be a constant field extension. Let ℓ be a prime not equal to p. If ℓ does not divide the class number of k_0, then any everywhere unramified powerful (*a fortiori *uniform) pro-ℓ extension of k, Galois over k_0, with no constant field extension, is finite.*

(We will show how to prove Theorem 2 both independently and as a special case of Theorem 1.)

Theorem 3. *Let k_0 be a function field over a finite field $\mathbf{F}_0$, such that the Jacobian of its corresponding curve has a commutative endomorphism ring. For all but finitely many primes ℓ, given any constant field extension $k = k_0\mathbf{F}$, any everywhere unramified powerful (*a fortiori *uniform) pro-ℓ extension of k, Galois over k_0, with no constant field extension, is finite.*

Remark 1.6.
(a) The set of ℓ which need to be excluded can be calculated, and does not depend on the class number of k_0.
(b) This theorem is extendable to the case where the abelian variety has an endomorphism ring which is not quite abelian, with a slight enlargement of the set of excluded ℓ. (See Theorem 4.9 of Section 4.)

Furthermore, the idea behind Theorem 2 can be applied to number fields as well, using the Main Conjecture of Iwasawa theory as proved by Wiles. Let k_0 now be a totally real number field, and ℓ be an odd prime. Let $k_n = k_0(\zeta_{\ell^n})$ for $n > 1$ be a non-trivial extension of $k_1 = k_0(\zeta_\ell)$, where ζ_{ℓ^n} will denote a primitive ℓ^n-th root of unity. Let $K = \bigcup k_n$. Let $\Delta = \mathrm{Gal}(k_1/k_0)$, and let $\delta = |\Delta|$. Let ℓ^e be the largest power of ℓ such that $\zeta_{\ell^e} \in k_0(\zeta_\ell)$.

We need first a new definition.

Definition 1.7. Let ζ_{k_0} be the zeta function for k_0. We say that ℓ is *k_0-regular* if ℓ is relatively prime to $\zeta_{k_0}(1-m)$ for all even m such that $2 \le m \le \delta - 2$ and also ℓ is relatively prime to $\ell^e\zeta_{k_0}(1-\delta)$.

(It is known that these numbers are rational; we will prove that they are ℓ-integral also.)

Then in Section 6 we will prove, as a special case of Conjecture 2:

Theorem 4. *Suppose ℓ is k_0-regular. Then there are no unramified infinite powerful pro-ℓ extensions M of k_n, Galois over k_0, such that $K \cap M = k_n$ and* $\mathrm{Gal}(M_{el}/k_n) = \mathrm{Gal}(M_{el}/k_n)^-$ *according to the action of Δ, where M_{el} is the maximal elementary abelian subextension of M/k_n.*

A short outline of the paper is perhaps in order. Theorem 1 and Theorem 2 are discussed in Section 2, with some brief notes on how they may be proved. Section 3 describes a Lie algebra which we can associate to our uniform groups and some aspects of the relationship between this Lie algebra and the original group, and then Section 4 uses this Lie algebra to treat a situation which is related to those of Section 2, but which does not quite follow the the same plan of attack. We prove a lemma relating eigenspaces and ideals of Lie algebras, and then prove Theorem 3 and an extension thereof. Examples of fields to which the theorems discussed so far can be applied are given in Section 5.

After that, we turn back to number fields. Section 6 introduces the Main Conjecture and uses it to prove Theorem 4. Section 7 presents a theorem of Greenberg which also involves

k_0-regular primes and explores its connection to Theorem 4. Finally, we close with some numerical data on k_0-regular primes in Section 8.

2. Boston's theorem and some close relatives

The following theorem is from Boston [4]:

Theorem 2.1 (Boston, 1994)**.** *If a number field k has a (proper) subfield k_0 such that k/k_0 is cyclic of degree prime to ℓ and such that ℓ does not divide the class number $h(k_0)$, then any everywhere unramified powerful pro-ℓ extension of k, Galois over k_0, is finite.*

Theorem 2.1 is proved by using the Schur-Zassenhaus lemma to get a regular automorphism (i.e. one with no non-trivial fixed points) on the Galois group, and then using Shalev's theorem from [28] on the derived length of a group with few fixed points.

We have also an equivalent theorem for function fields, proved the same way:

Theorem 2.2. *If a function field k has a (proper) subfield k_0 such that k/k_0 is cyclic of degree prime to ℓ and such that ℓ does not divide the class number $h(k_0)$, then any everywhere unramified powerful pro-ℓ extension of k, Galois over k_0, with no constant field extension is finite.*

Remark 2.3. This holds also for $\ell = p$.

We now address the case where k is a non-trivial extension of some field k_0, such that k is obtained from k_0 by constant field extension. Let k_0 be a function field over a finite field $\mathbf{F}_0$ of characteristic p and order q_0, and let $k_n = k_0\mathbf{F}_n$ where $\mathbf{F}_n$ is the extension of $\mathbf{F}_0$ with degree $n > 1$ and order $q = (q_0)^n$.

Theorem 2.4. *If ℓ does not divide the class number of k_0, then there are no unramified infinite powerful pro-ℓ extensions of k_n, Galois over k_0, with no constant field extension.*

This theorem can be proved in much the same way as the previous ones. The important difference is that the regular automorphism now comes from a Frobenius action, rather than from the Schur-Zassenhaus lemma as in Boston's result.

Remark 2.5. Instead of proving Theorem 2.4 directly, we could also prove it using Theorem 2.2 as follows: Let $\ell^m n'$ be the degree of k_n/k_0, where n' is prime to ℓ. Let k_0' be the constant field extension of k_0 of degree ℓ^m; then k_n is a constant field extension of k_0' of degree n', and thus a cyclic extension of degree prime to ℓ. If ℓ does not divide the class number of k_0, then it can be proved that ℓ does not divide the class number of the constant field extension k_0', so we may apply Theorem 2.2 to the extension k_n/k_0'. Then there are no unramified infinite powerful pro-ℓ extensions of k_n, Galois over k_0', with no constant field extension, and *a forteriori* none Galois over k_0.

We will come back to this idea in Section 7 and compare it to the corresponding situation for number fields.

3. The Lie algebra associated to a uniform group

In this section we state some facts and theorems about finitely generated powerful groups and uniform groups. Many of these are taken from [10], perhaps the most definitive work on powerful and ℓ-adic analytic pro-ℓ groups to date. (My thanks to Dan Segal for sharing material from the upcoming second edition of [10].) Another vitally important source is Lazard's paper, [23], which laid the groundwork for the whole subject. Section 3.4 treats a somewhat anomalous situation which we will encounter; this material has not, as far as I know, appeared elsewhere.

3.1. **Definitions.** In addition to the definitions and theorems from the introduction, we also have a related definition from [10] which will be useful:

Definition 3.1. If G is a pro-ℓ group and N is an closed subgroup of G, we say N is *powerfully embedded* in G (also written N p.e. G) if ell is odd and $[N, G] \leq \overline{N^\ell}$, or $\ell = 2$ and $[N, G] \leq \overline{N^4}$.

Remark 3.2. Note that in particular such an N is a powerful group, and a normal subgroup of G.

We can also define analogous properties for Lie algebras. In the rest of this section a "$\mathbf{Z}_\ell$-Lie algebra", or simply a "Lie algebra", refers to a module over $\mathbf{Z}_\ell$ with a Lie bracket. A "$\mathbf{Z}_\ell$-Lie ideal" or "Lie ideal" refers to a $\mathbf{Z}_\ell$-subalgebra of a Lie algebra which is closed under bracket operations with elements of the algebra.

Definition 3.3. We say that a $\mathbf{Z}_\ell$-Lie algebra L is *powerful* if ℓ is odd and $(L, L) \subseteq \overline{\ell L}$, or $\ell = 2$ and $(L, L) \subseteq \overline{4L}$. It is *uniform* if it is powerful, finitely generated, and torsion-free. (In this case clearly $\overline{\ell L} = \ell L$, and so on.) We say that an closed $\mathbf{Z}_\ell$-Lie ideal I is *powerfully embedded* in L if ℓ is odd and $(I, L) \subseteq \overline{\ell I}$, or $\ell = 2$ and $(I, L) \subseteq \overline{4I}$.

Remark 3.4. (a) Note that if I is powerfully embedded as a Lie ideal, then it is powerful as a Lie algebra.
(b) Note that if L is any finitely generated Lie algebra, then it contains a characteristic open uniform Lie algebra. This is perhaps analogous to the fact that any pro-ℓ group of finite rank contains a uniform group as a characteristic open subgroup.

In the discussions that follow, I will assume ℓ is odd; unless otherwise noted everything is the same for $\ell = 2$ except where ℓ should be replaced by 4.

3.2. **The equivalence of categories.** Let G be a uniform pro-ℓ group.

The properties of uniform groups show that each element x of G^{ℓ^n} has a *unique* ℓ^n-th root in G, which we denote $x^{\ell^{-n}}$, following [10]. Then we can define a new group structure on G by transferring the group structures from successive G^{ℓ^n}'s, and take the limit.

Definition 3.5 (and Proposition)**.** For $x, y \in G$, define

$$x +_n y = (x^{\ell^n} y^{\ell^n})^{\ell^{-n}}.$$

(Note that $x^{\ell^n} y^{\ell^n}$ is an ℓ^n-th power with a unique ℓ^n-th root.) Then the limit

$$x + y = \lim_{n \to \infty} x +_n y$$

exists.

It may be verified that this gives G the structure of an abelian group, with the same identity element and inverses as before. It can also be shown that if $xy = yx$, then $x + y = xy$, so that powers of an element are also the same as before. This structure will be the group structure for our Lie algebra. We also need a Lie bracket, which will be defined similarly, as follows.

Definition 3.6 (and Proposition)**.** For $x, y \in G$, define

$$(x, y)_n = [x^{\ell^n}, y^{\ell^n}]^{\ell^{-2n}}.$$

(The brackets indicate commutators; note that $[G^{\ell^n}, G^{\ell^n}] \leq G^{\ell^{2n}}$ from properties of powerful groups. See, e.g., Propositions 1.16 and 3.6 of [10].) Then the limit

$$(x, y) = \lim_{n\to\infty} (x, y)_n$$

exists.

Thus the Lie bracket is derived from the commutators; it may be verified that these operations make the elements of G into a Lie algebra over $\mathbf{Z}_\ell$, which we will in the future denote $L(G)$.

It is also possible to define a group structure on the elements of a uniform Lie algebra. Section 10.5 of [10] and Section 4 of [19] give the essential ingredients. Let L be a uniform Lie algebra.

Definition 3.7. For $x, y \in L$, we define the group operation xy by

$$xy = \Phi(x, y) = x + y + \frac{1}{2}(x, y) + \cdots,$$

for $\Phi(X, Y)$ the Campbell-Hausdorff series in two non-commuting indeterminates (discussed in Chapter 7 of [10], and also in [22]).

A priori, this series only converges in $L \otimes \mathbf{Q}_\ell$, if at all. However, [10] shows that in fact the series converges, with sum in L. This map does give a group structure; the proof is essentially that of Lemma 10.13 of [10].

Now let $G = G(L)$ denote L with the group structure we have just defined. Since L is torsion free and finitely generated, it follows that G is, also.

Proposition 3.8 (see Lemma 4.1 of [19])**.** (a) *If G is a uniform group, then $L(G)$ is a uniform Lie algebra.*

(b) *If L is a uniform Lie algebra, then $G(L)$ is a uniform group.*

Finally, we should note that these operations define an equivalence of categories from the category of uniform groups with group homomorphisms to the category of uniform Lie algebras with Lie algebra homomorphisms. (See, for example, Section IV.3.2 of [23].) In particular, we will use the fact that a group automorphism of G induces a Lie algebra automorphism of $L(G)$.

3.3. **Substructures.**

Let G be a uniform group and L be the uniform Lie algebra $L(G)$.

Proposition 3.9 (see Lemma 4.1 of [19])**.** (a) *If B is a powerful $\mathbf{Z}_\ell$-subalgebra of L, then the elements of B form a subgroup of G.*

(b) *If I is a powerfully embedded $\mathbf{Z}_\ell$-Lie ideal of L, then the elements of I form a normal subgroup of G.*

Remark 3.10. It will be useful in the future to note that if $(B \otimes \mathbf{Q}_\ell) \cap L = B$ (i.e. B is "isolated"), then B is powerful: suppose $(B \otimes \mathbf{Q}_\ell) \cap L = B$, and let x be in (B, B). Clearly, $x \in (L, L)$, and by Proposition 3.8 we have $(L, L) \subseteq \ell L$. So $x \in \ell L$, implying $\ell^{-1}x \in L$. However, $\ell^{-1}x \in B \otimes \mathbf{Q}_\ell$ also, so it is in B. Thus $x \in \ell B$, as desired. Similarly, if I is an isolated ideal then I is powerfully embedded.

Conversely, we have:

Proposition 3.11 (see Lemma 4.1 of [19])**.** (a) *If H is a powerful closed subgroup of G, then the elements of H form a Lie subalgebra of L.*

(b) *If N is a powerfully embedded subgroup of G, then the elements of N form a Lie ideal of L.*

Although we will not use it in this paper, the reader may also be interested to note the fact that the equivalence of categories takes commutators of powerfully embedded subgroups to Lie brackets of powerfully embedded ideals, and vice versa. It thus preserves the derived series and the lower central series, and thus the properties of solvability and nilpotency.

3.4. **Quotients.** The quotient of uniform structures may have torsion, and so may not be uniform. Thus it is necessary to treat quotients of uniform structures as special objects in some cases.

Proposition 3.12. *Let I be a $\mathbf{Z}_\ell$-ideal of L which is also a normal subgroup of G, e.g. I is powerfully embedded. Then G/I has the same number of generators as L/I, and G/I is torsion free if and only if L/I is.*

Proof. The number of generators of G/I is the dimension of $(G/I)/\operatorname{Frat}(G/I)$ as a vector space over $\mathbf{Z}/\ell\mathbf{Z}$, where $\operatorname{Frat}(H)$ is the Frattini subgroup of H, namely $\overline{H^\ell[H,H]}$. Now $(G/I)/\operatorname{Frat}(G/I)$ is isomorphic to

$$\frac{G/I}{\operatorname{Frat}(G)I/I} \cong \frac{G}{\operatorname{Frat}(G)I} \cong \frac{G/\operatorname{Frat}(G)}{\operatorname{Frat}(G)I/\operatorname{Frat}(G)},$$

since $\operatorname{Frat}(H/N) = \operatorname{Frat}(H)N/N$ for normal subgroups N of H. But modulo $\operatorname{Frat}(G)$ (which equals ℓL since G is uniform), the structures of G and L are exactly the same, so this is isomorphic to

$$\frac{L/\ell L}{(\ell L + I)/\ell L} \cong \frac{L}{\ell L + I} \cong \frac{L/I}{(\ell L + I)/I} \cong \frac{L/I}{\ell(L/I)}$$

the dimension of which is the number of generators of L/I.

Powers in G are the same as powers in L, so $x^\lambda = 1 \in G/I$ if and only if $x^\lambda \in I \leq G$ if and only if $\lambda x \in I \leq L$ if and only if $\lambda x = 1 \in L/I$. So torsion is the same. □

Remark 3.13. If I is a $\mathbf{Z}_\ell$-ideal of L such that L/I is torsion free, then I is isolated in the sense of Remark 3.10: suppose $x \otimes q = y \otimes 1$ for $x \in I$, $q \in \mathbf{Q}_\ell$, and $y \in L$. Then by clearing the denominator of q, we get $rx \otimes 1 = sy \otimes 1$ for $r, s \in \mathbf{Z}_\ell$, and thus $rx = sy$. Now $sy \in I$, and L/I is torsion-free, so $y \in I$. Thus $(I \otimes \mathbf{Q}_\ell) \cap L = I$. Then by Remark 3.10 I is powerfully embedded, so I is a normal subgroup of G.

As a corollary of the proposition and the remark, we get:

Proposition 3.14. *If I is a $\mathbf{Z}_\ell$-ideal of L such that $L/I \cong \mathbf{Z}_\ell$, then I is a normal subgroup of G and $G/I \cong \mathbf{Z}_\ell$.*

Proposition 3.15. *Suppose φ is an automorphism of G, and thus also of L. Further suppose I is a $\mathbf{Z}_\ell$-ideal of L preserved by φ, such that φ acts trivially on L/I. If I is also a normal subgroup of G, then φ also acts trivially on G/I.*

Proof. We know that the elements of I form a normal subgroup of G preserved by φ, so φ acts on G/I. Suppose there exists $x \in G$ such that $\varphi(x) \not\equiv x$ modulo I, i.e. $\varphi(x)x^{-1} \notin I$. We can invoke our equivalence of categories, which implies:

$$\varphi(x) \cdot x^{-1} = \varphi(x) \cdot (-x) = \varphi(x) + (-x) + \frac{1}{2}(\varphi(x), -x)_L + \cdots.$$

But $(\varphi(x), \varphi(x))_L = (x, x)_L = 0$, and

$$(\varphi(x), -x)_L = (\varphi(x), \varphi(x) - x)_L + (\varphi(x), -\varphi(x))_L.$$

The first term of this is in the ideal I because $\varphi(x) - x \in I$, since φ acts trivially on L/I by hypothesis. The second term is 0, so $(\varphi(x), -x)_L \in I$. The other Lie bracket terms of $\varphi(x) \cdot x^{-1}$ are also in I, since they are Lie brackets of things with $(\varphi(x), -x)_L$. Also $\varphi(x) + (-x)$ is in I, but this contradicts $\varphi(x)x^{-1} \notin I$. So φ must act trivially on G/I. □

4. An ordinary theorem

The proof of the following theorem is somewhat different from the others in this paper, as it does not use Shalev's theorem. Instead, we allow a small space of fixed points on the Lie algebra, and use them to establish a $\mathbf{Z}_\ell$ extension of some function field, which we know is impossible.

First, however, we need a lemma about Lie algebras.

Lemma 4.1. *Suppose φ is an automorphism of a Lie algebra L, acting diagonalizably on the underlying vector space. Let $\lambda_1, \dots, \lambda_n$ be the* distinct *eigenvalues of φ, and suppose for all $i \neq j$, $\lambda_i\lambda_j \neq 1$. Suppose further that if any $\lambda_i = -1$, the eigenspace corresponding to λ_i has dimension* 1.

Let L_0 be the subalgebra of L consisting of the fixed points of φ. Then there is an ideal L_1 preserved by φ such that $L_0 \oplus L_1 = L$.

Proof. If 1 is not an eigenvalue then there are no fixed points, so we are done. Otherwise, let $\lambda_1 = 1$, and let $v_{i\alpha}$ be the eigenvectors in L corresponding to eigenvalue λ_i. Let L_1 be spanned by $\{v_{i\alpha}, i \neq 1\}$. Clearly $L = L_0 + L_1$.

Consider the Lie bracket of $v_{i\alpha}$ with $v_{j\beta}$. We have

$$\varphi([v_{i\alpha}, v_{j\beta}]) = [\varphi(v_{i\alpha}), \varphi(v_{j\beta})] = [\lambda_i v_{i\alpha}, \lambda_j v_{j\beta}] = \lambda_i\lambda_j[v_{i\alpha}, v_{j\beta}].$$

Thus $[v_{i\alpha}, v_{j\beta}]$ is an eigenvector (possibly 0), corresponding to the eigenvalue $\lambda_i\lambda_j$. But $\lambda_i\lambda_j$ is not 1 unless $i = j = 1$ or $i = j$ and $\lambda_i = -1$. If the latter, then $[v_{i\alpha}, v_{j\beta}] = [v_{i\alpha}, v_{i\alpha}] = 0$, since the eigenspace corresponding to λ_i has dimension 1. Therefore, either $[v_{i\alpha}, v_{j\beta}] = 0$, or $[v_{i\alpha}, v_{j\beta}]$ is some eigenvector in L_1 unless $i = j = 1$.

Let $a = \sum a_{i\alpha}v_{i\alpha} \in L$ and $b = \sum_{j\neq 1} b_{j\beta}v_{j\beta} \in L_1$. Then

$$[a, b] = [\sum a_{i\alpha}v_{i\alpha}, \sum_{j\neq 1} b_{j\beta}v_{j\beta}] = \sum_{j\neq 1} a_{i\alpha}b_{j\beta}[v_{i\alpha}, v_{j\beta}]$$

which is in L_1 by the above. Thus L_1 is an ideal. Finally, L_1 is generated by eigenvectors, so it is preserved by φ. □

Corollary 4.1.1. *Suppose φ is an automorphism of a $\mathbf{Z}_\ell$-Lie algebra L, acting semi-simply on the underlying vector space of $L \otimes \mathbf{Q}_\ell$. Let $\lambda_1, \dots, \lambda_n$ be the* distinct *roots in $\overline{\mathbf{Q}_\ell}$ of the characteristic polynomial of φ, and suppose for all $i \neq j$, $\lambda_i\lambda_j \neq 1$. Suppose further that if any $\lambda_i = -1$, λ_i is only a simple root of the characteristic polynomial.*

Then the conclusions of the lemma hold, i.e.: let L_0 be the subalgebra of L consisting of the fixed points of φ. Then there is an ideal L_1 preserved by φ such that $L_0 \oplus L_1 = L$.

Proof. Let $L' = L \otimes_{\mathbf{Z}_\ell} E$, where $E = \mathbf{Q}_\ell(\lambda_1, \dots, \lambda_n)$, so that φ acts diagonalizably on L', by extension of base ring. Then the λ are the eigenvalues for the action, and satisfy the hypotheses of the lemma, so we have $L' = L'_0 \oplus L'_1$. By extension of base ring, $L_0 = L'_0 \cap L$, and if we let $L_1 = L'_1 \cap L$ then L_1 is an ideal satisfying the desired properties. □

Let k_0 be a function field over a finite field $\mathbf{F}_0$ of characteristic p and order q_0, and let $k_n = k_0\mathbf{F}_n$ where $\mathbf{F}_n$ is the extension of $\mathbf{F}_0$ with degree $n > 1$ and order $q = (q_0)^n$. The fields k_n and k_0 have the same genus g, and correspond to some abelian variety A. Let ℓ be a prime not equal to p. Let $K = k_0\overline{\mathbf{F}_0}$ and let K^{urab} be the maximal abelian unramified ℓ-extension of K. We know that $\mathrm{Gal}(K/k_0)$ is generated by the Frobenius element φ, and we know $\mathrm{Gal}(K^{urab}/K) \cong T_\ell(A) \cong (\mathbf{Z}_\ell)^{2g}$. The Frobenius element has a semi-simple action on $T_\ell(A) \cong (\mathbf{Z}_\ell)^{2g}$ with characteristic polynomial $P(x)$ and minimal polynomial $m(x)$, each with integer coefficients. This $P(x)$ and this $m(x)$ are independent of ℓ. The discriminant of $m(x)$ is not zero because φ is semi-simple, so $m(x)$ is a product of distinct irreducibles.

Theorem 4.2. *Suppose that the roots of $m(x)$ modulo ℓ (possibly in some extension of $\mathbf{Z}/\ell\mathbf{Z}$) are all distinct, and consist of $\lambda_0, \lambda_1, \dots, \lambda_n$ such that for all $i \neq j$, $\lambda_i\lambda_j \neq 1$. If the variety A has a commutative endomorphism ring, then there are no unramified infinite powerful pro-ℓ extensions of k_n, Galois over k_0, with no constant field extension.*

The proof begins with a reduction step, which we isolate as a lemma so that we can use it in subsequent proofs.

Lemma 4.3 (see [4])**.** *Let M be an everywhere unramified pro-ℓ extension of k that is infinite and powerful. Then M contains a subextension N of k which is infinite and uniform. If k/k_0 is a Galois extension of fields, and M is Galois over k_0, then so is N.*

Proof. Let T denote the set of torsion elements of $\mathrm{Gal}(M/k)$. By Theorem 4.20 of [10], T is a finite characteristic subgroup, such that $\mathrm{Gal}(M/k)/T$ is uniform. Let N be the corresponding intermediate field. Then N is an infinite uniform unramified pro-ℓ extension. Finally, N is Galois over k_0 since T is a characteristic subgroup of $\mathrm{Gal}(M/k)$, which is normal in $\mathrm{Gal}(M/k_0)$. □

Proof of Theorem. If 1 is not a root of $m(x)$ then ℓ does not divide $m(1)$, which divides $P(1)$, so we may use Theorem 2.4. Thus we may assume $\lambda_0 = 1$.

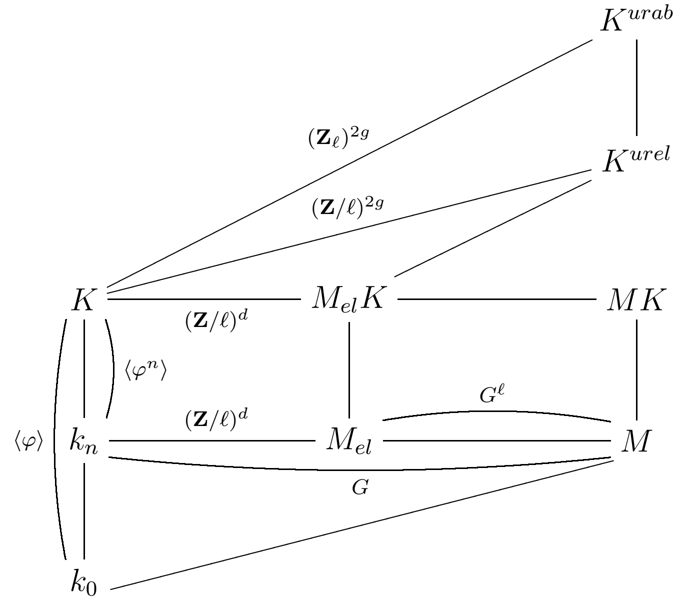
Let M be an unramified infinite powerful pro-ℓ extensions of k_n, Galois over k_0, with no constant field extension. By Lemma 4.3 we may assume M is a uniform extension of k_n. Let $G = \mathrm{Gal}(M/k_n)$, and let d be the dimension of G. Since M is Galois over k_0, φ acts on G.

Let K^{urel} be the maximal elementary abelian subextension of K^{urab}/K and let M_{el} be the maximal elementary abelian subextension of M/k_n. (See Figure 1.)

Since M has no constant field extension, $M \cap K = k_n$. Let $\mathrm{Frat}(G) = \overline{[G,G]G^\ell}$ be the Frattini subgroup of G, which is equal to G^ℓ since G is powerful and finitely generated. Then $G/\mathrm{Frat}(G) = G/G^\ell = \mathrm{Gal}(M_{el}/k_n) \cong \mathrm{Gal}(M_{el}K/K)$, which is a quotient of $\mathrm{Gal}(K^{urel}/K) \cong (\mathbf{Z}/\ell)^{2g}$ and is thus a vector space of dimension d over $\mathbf{Z}/\ell\mathbf{Z}$. Let R be the semi-simple $2g$ by $2g$ matrix, with $\mathbf{Z}_\ell$-coefficients, representing the action of φ on $\mathrm{Gal}(K^{urab}/K)$.

Since G is uniform, we have a $\mathbf{Z}_\ell$-Lie ring structure on G; let L denote G with this structure. By the equivalence of categories in Section 3.2, an automorphism of G induces an automorphism of L, so the action of φ on G gives an action on L also. The fact that A has a commutative endomorphism ring means that the degree of $m(x)$ is equal to $2g$, and thus it is also equal to the characteristic polynomial. Now φ acts on $\mathrm{Gal}(M_{el}/k_n) = L/\ell L$ according to some factor representation R' of the reduction of R modulo ℓ, and this action has characteristic polynomial equal to a factor of $m(x)$ modulo ℓ. The action of φ on L is

Figure 1. The relationships between the subfields of M and K in the function field case.



also represented by a matrix whose reduction modulo ℓ is equal to R'. Then our conditions on the roots of $m(x)$ modulo ℓ imply that the action of φ on L is as in the corollary (note *all* of the roots are simple, since the characteristic polynomial equals the minimal polynomial), so $L = L_0 \oplus L_1$ for L_1 an ideal as in the lemma. But all of the eigenvalues have multiplicity 1, so L_0, the eigenspace of L corresponding to eigenvalue 1, is one-dimensional. So L_1 is an ideal of codimension 1, and by the correspondence of G with L, specifically Proposition 3.14, we have a normal subgroup $N = L_1$ of G such that $G/N \cong \mathbf{Z}_\ell$. But this means there is an unramified infinite abelian extension of k_n with no constant field extension, which is impossible. □

Here is another way of looking at this result:

Theorem 4.4. *Let k_0 be a function field over a finite field $\mathbf{F}_0$, such that its corresponding abelian variety has a commutative endomorphism ring. For all but finitely many primes ℓ, given any constant field extension $k_n = k_0\mathbf{F}_n$, k has no unramified infinite powerful pro-ℓ extensions, Galois over k_0, with no constant field extension.*

Proof. As in the previous proof, the minimal polynomial $m(x)$ and the characteristic polynomial $P(x)$ are the same, and independent of ℓ. The discriminant Δ of $m(x)$ is not zero in $\mathbf{Z}$, so the roots are all distinct. Let λ_i be the roots, and set $\tau = \prod_{i<j}(\lambda_i\lambda_j - 1)$. We know for all i, $|\lambda_i| = \sqrt{q_0}$, so τ is not zero. However, $\tau \in \mathbf{Z}$ for the same reason Δ is.

Now we can say that the primes ℓ that need to be excluded are $\ell = p$ (of course), the primes dividing Δ, and the primes dividing τ. For every other ℓ, the hypotheses of the previous theorem are satisfied. □

Remark 4.5. A has a commutative endomorphism ring if, for example, it is the product of nonisogenous elementary abelian varieties which are ordinary.

In fact, Theorem 4.2 can be improved, using the following result about uniform groups.

Proposition 4.6 (Exercise 4.11.(i) of [10])**.** *Let G be a uniformly powerful pro-p group with 2 (topological) generators. Then G contains a unique normal procyclic subgroup H such that G/H is procyclic, and H has a complement in G.*

Theorem 4.7. *Suppose that the roots of $m(x)$ modulo ℓ (possibly in some extension of $\mathbf{Z}/\ell\mathbf{Z}$) are all distinct, and consist of $\lambda_0, \lambda_1, \ldots, \lambda_n$ such that for all $i \neq j$, $\lambda_i\lambda_j \neq 1$. Further, suppose that $\lambda_i \neq -1$ for all i. If the characteristic polynomial $P(x)$ associated to the variety A has only roots of multiplicity 2 or less, then there are no unramified infinite powerful pro-ℓ extensions of k_n, Galois over k_0, with no constant field extension.*

Remark 4.8. Let A be isogenous to $\prod_{i=1}^{t} A_i^{m_i}$ with the A_i nonisogenous elementary abelian varieties, as in the Poincaré-Weil Theorem. (See, for example, Part I of [32] for a summary of the classification of abelian varieties up to isogeny. We use a number of facts from that summary in this remark, especially from Sections 1 and 6.) Then the characteristic polynomial is $P(x) = \prod_{i=1}^{t} f_i(x)^{e_i m_i}$ for some e_i, with $f_i(x)$ irreducible. Clearly the minimal polynomial is $m(x) = \prod f_i(x)$. The codimension of the center of the endomorphism ring of $A_i^{m_i}$ is $e_i^2 m_i^2$, so if each $A_i^{m_i}$ has an endomorphism ring with center of codimension less than or equal to 4, the condition on the characteristic polynomial is true. More globally, the codimension of the center of the endomorphism ring of A is $\sum e_i^2 m_i^2$, so if A has an endomorphism ring with center of codimension less than or equal to 4 then the condition is true.

Proof (of Theorem). We keep the notation of the previous proofs. As before, we may assume $\lambda_0 = 1$.

As in the proof of Theorem 4.2, the action of φ on L has characteristic polynomial equal to a factor of $P(x)$ modulo ℓ. Then our conditions on the roots of $P(x)$ modulo ℓ imply that the action of φ on L is as in Corollary 4.1.1, so $L = L_0 \oplus L_1$ for L_1 an ideal as in the lemma. But all of the eigenvalues have multiplicity 1 or 2, so L_0, the eigenspace of L corresponding to eigenvalue 1, is one-dimensional or two-dimensional, and L_1 is an ideal of codimension 1 or 2. If the codimension is 1 then we conclude as in the proof of Theorem 4.2. If the codimension is 2, then by Proposition 3.12, we have a normal subgroup $N = L_1$ of G such that G/N is a torsion-free (and thus uniform) powerful group with 2 generators. Then Proposition 4.6 shows that G/N has a quotient group isomorphic to $\mathbf{Z}_\ell$. But again, this means there is an unramified infinite abelian extension of k_n with no constant field extension, which is impossible. □

Again, we can look at this result in terms of which ℓ it can be applied to:

Theorem 4.9. *Let k_0 be a function field over a finite field $\mathbf{F}_0$, such that its corresponding abelian variety is as described in the previous theorem. For all but finitely many primes ℓ, given any constant field extension $k_n = k_0\mathbf{F}_n$, k has no unramified infinite powerful pro-ℓ extensions, Galois over k_0, with no constant field extension.*

Proof. This time, the primes ℓ that need to be excluded are $\ell = p$ (of course), the primes dividing the discriminant Δ of the *minimal* polynomial, the primes dividing τ (also for the minimal polynomial), and the primes dividing $P(-1)$. □

Remark 4.10. In fact, we can squeeze even more out of Corollary 4.1.1 along these lines. For instance, only the multiplicities of the roots of $P(x)$ which are 1 or -1 modulo ℓ are relevant, so in a specific example we can look at only the irreducible factors of $P(x)$ containing these roots. If the total multiplicity of the roots which are 1 modulo ℓ is no more than 2, and the total multiplicity of the roots which are -1 modulo ℓ is no more than than 1, then there can be no extensions of the sort described. Also, only the discriminant of the minimal polynomial for the action modulo ℓ is relevant, and this may be smaller than the reduction modulo ℓ of $m(x)$. (It is the largest square-free polynomial over $\mathbf{Z}/\ell\mathbf{Z}$ dividing the reduction of $P(x)$ modulo ℓ.) Determining whether these looser conditions are satisfied, however, can be done only one ℓ at a time, and only if the polynomial $P(x)$ is known fairly explicitly.

5. Examples I

For varieties over finite fields given by equations of the form

$$a_1x_1^{m_1} + a_2x_2^{m_2} + \cdots + a_rx_r^{m_r} = c$$

$(a_i, c \neq 0)$, there is a relatively easy way to calculate the zeta function associated with the variety, as explained in Chapters 8 and 11 of [20]. In particular, we will use this method for curves of the form

$$ax^2 + by^m = c.$$

These correspond to quadratic extensions k of the function field $\mathbf{F}(t)$, and we will use their zeta functions to try to find examples of our theorems.

Define the zeta function for k, $\zeta_k(s)$, in the usual way, and let $Z_k(T)$ be the function such that $\zeta_k(s) = Z_k(q^{-s})$, where q is the number of elements of $\mathbf{F}$. Now if $C/\mathbf{F}$ is the curve associated to k, then we have an alternative expression

$$Z_k(T) = Z(C/\mathbf{F}, T) = \exp\left(\sum_{n=1}^{\infty} |C(\mathbf{F}_{q^n})| \frac{T^n}{n}\right),$$

where $\mathbf{F}_{q^n}$ is the finite field with q^n elements, and points are counted on a non-singular model of $C/\mathbf{F}$.

Let $Z(V/\mathbf{F}, T)$ be the zeta function of a variety V, defined analogously to that of a curve.

Proposition 5.1. *The zeta function $Z(V/\mathbf{F}, T)$ is equal to*

$$\frac{\prod_i (1 - \alpha_i T)}{\prod_j (1 - \beta_j T)}$$

if and only if there exist complex numbers $\{\alpha_i\}$ and $\{\beta_j\}$ such that for all $n \geq 1$,

$$|V(\mathbf{F}_{q^n})| = \sum_j \beta_j^n - \sum_i \alpha_i^n.$$

This is Proposition 11.1.1 of [20], and is proved by logarithmic differentiation.

We specialize to the curve $C/\mathbf{F}_q$, q odd, given by

$$ax^2 + by^m = c,$$

where $m > 2$ divides $q - 1$. (Since q is odd, 2 also divides $q - 1$.) Then it turns out that

$$\left|C(\mathbf{F}_{q^d})\right| = q^d + 1 + \sum_{i \neq m/2,\ i=1}^{m-1} (-1)^{d+1} \left(\rho\chi^i(c)\rho(a^{-1})\chi^i(b^{-1})J(\rho, \chi^i)\right)^d$$

where ρ is the quadratic character on $\mathbf{F}_q$, χ is a generator of the cyclic group of characters of order dividing m on $\mathbf{F}_q$, and $J(\rho, \chi^i)$ is their Jacobi sum. (See Chapter 8 of [20], for how to count the affine points, and Example II.2.5.1 and Exercise 2.14 of [30] for the projective points.)

Applying Proposition 5.1, we obtain a formula for the zeta function, namely:

$$\frac{\displaystyle\prod_{i\neq m/2,\ i=1}^{m-1} \left(1-\rho\chi^i(c)\rho(a^{-1})\chi^i(b^{-1})J(\rho,\chi^i)T\right)}{(1-T)(1-qT)}.$$

Finally, this gives us the polynomial $P(T)$ which we have been using in our theorems, namely

$$P(T) = \prod_{i\neq m/2,\ i=1}^{m-1} \left(T-\rho\chi^i(c)\rho(a^{-1})\chi^i(b^{-1})J(\rho,\chi^i)\right).$$

The following examples were calculated using the program PARI. (See [2].)

Example 5.2. $C = \{x^2 + y^5 = 1\}$; $\mathbf{F} = \mathbf{F}_{11}$. Then in terms of our theorems, $k_0 = \mathbf{F}_{11}(t, \sqrt{1-t^5})$.

$$P(T) = T^4 - 4T^3 + 6T^2 - 44T + 121,$$

$P(1) = 2^4 \cdot 5$, $\Delta = 2^{12} \cdot 5^3 \cdot 11^2$, and $\tau = 2^{12} \cdot 5^6 \cdot 211^2$. For every $\ell \neq p$ except 2 and 5, we can apply Theorem 2.4. For every $\ell \neq p$ except 2, 5, and 211, we can also apply Theorem 4.2.

Example 5.3. $C = \{x^2 + y^7 = 1\}$; $\mathbf{F} = \mathbf{F}_{29}$. Then $k_0 = \mathbf{F}_{29}(t, \sqrt{1-t^7})$.

$$P(T) = T^6 - 6T^5 - 13T^4 + 316T^3 - 377T^2 - 5046T + 24389,$$

$P(1) = 2^6 \cdot 7 \cdot 43$, $\Delta = -1 \cdot 2^{36} \cdot 7^5 \cdot 29^6$, and $\tau = 2^{36} \cdot 7^{10} \cdot 659^2 \cdot 2143^2 \cdot 1405153^2$. For every $\ell \neq p$ except 2, 7, and 43, we can apply Theorem 2.4. However, for $\ell = 43$, we can instead apply Theorem 4.2.

Example 5.4. $C = \{x^2 + y^9 = 1\}$; $\mathbf{F} = \mathbf{F}_{19}$. Then $k_0 = \mathbf{F}_{19}(t, \sqrt{1-t^9})$.

$$P(T) = (T^6 + 9T^4 + 64T^3 + 171T^2 + 6859)(T^2 - 8T + 19),$$

$P(1) = 2^8 \cdot 3^2 \cdot 37$, $\Delta = 2^{56} \cdot 3^{14} \cdot 17^2 \cdot 19^{12}$, and $\tau = 2^{56} \cdot 3^{28} \cdot 19^4 \cdot 163^2 \cdot 181^2 \cdot 379^2 \cdot 613^2 \cdot 13627^4$. For every $\ell \neq p$ except 2, 3, and 37, we can apply Theorem 2.4. However, for $\ell = 37$, we can instead apply Theorem 4.2.

There are many similar examples where Theorem 4.2 proves useful. Here is one where instead we can apply Theorem 4.7.

Example 5.5. $C = \{x^2 + (\alpha+2)y^6 = 1\}$, where $\alpha^2 + 3\alpha + 3 = 0$; $\mathbf{F} = \mathbf{F}_{25}$. Then $k_0 = \mathbf{F}_{25}(t, \sqrt{1-(\alpha+2)t^6})$.

$$P(T) = (T^2 - 5T + 25)^2,$$

$P(1) = 441 = 3^2 \cdot 7^2$, $P(-1) = 961 = 31^2$, $\Delta = -75 = -1 \cdot 3 \cdot 5^2$, and $\tau = 576 = 2^6 \cdot 3^2$. ($\Delta$ and τ are taken for the minimal polynomial.) Thus for $\ell = 7$, Theorem 4.7 may be applied, even though Theorem 2.4 cannot.

Remark 5.6. Note that for $m = 3$ and $m = 4$, C is an elliptic curve, i.e. has genus 1. Then by Abhyankar's Conjecture, proved by Harbater, $\mathrm{Gal}(K^{ur}/K)$ is a free pro-ℓ group with two generators. (See [15]). In this case, one of Theorem 2.4, Theorem 4.2, or Theorem 4.7 can always be applied, for all $\ell \neq p$.

6. Iwasawa theory and cyclotomic extensions

We now turn to number fields. Let ℓ be an odd prime, and let k_n be an extension of some totally real number field k_0, given by $k_n = k_0(\zeta_{\ell^n})$ for $n > 1$, where ζ_{ℓ^n} will denote a primitive ℓ^n-th root of unity. Let $k_1 = k_0(\zeta_\ell)$ be the subextension of degree prime to ℓ. Let $K = k_0(\zeta_{\ell^\infty}) = \bigcup_d k_0(\zeta_{\ell^d})$ and let K^{urab} be the maximal abelian unramified ℓ-extension of K. Then $\mathrm{Gal}(K/k_0) \cong \Delta \times \Gamma$, where $\Delta = \mathrm{Gal}(k_1/k_0)$ is a finite abelian group of order prime to ℓ, and $\Gamma = \mathrm{Gal}(K/k_1)$ is isomorphic to $\mathbf{Z}_\ell$ and is generated by some γ. Let $X = \mathrm{Gal}(K^{urab}/K)$, as in Chapter 13 of [31].

Then $\Delta \times \Gamma$ acts on X by conjugation, so Δ does. Since ℓ does not divide the order of Δ (which divides $\ell - 1$), and the values of the (one-dimensional) characters χ on $\Delta \hookrightarrow (\mathbf{Z}/\ell\mathbf{Z})^\times$ lie in $\mathbf{Z}_\ell$ (and not an extension), then as explained in Section 13.4 of [31], we can decompose X as

$$X = \bigoplus_\chi \epsilon_\chi X$$

according to the orthogonal idempotents ϵ_χ of the group ring $\mathbf{Z}_\ell[\Delta]$, where

$$\epsilon_\chi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \chi(\sigma)\sigma^{-1}.$$

We can also decompose

$$X = X^+ \oplus X^- = \epsilon_+ X \oplus \epsilon_- X$$

using the elements $\epsilon_\pm = (1 \pm J)/2$, where $J \in \Delta$ is complex conjugation. Then, we have

$$\frac{1+J}{2} = \sum_{\chi \text{ even}} \epsilon_\chi \qquad \text{and} \qquad \frac{1-J}{2} = \sum_{\chi \text{ odd}} \epsilon_\chi$$

so

$$X^+ = \bigoplus_{\chi \text{ even}} \epsilon_\chi X \qquad \text{and} \qquad X^- = \bigoplus_{\chi \text{ odd}} \epsilon_\chi X.$$

(See Section 6.3 of [31] for more details.)

Now, since k_1 is a CM field, by Proposition 13.28 of [31], X^- contains no finite Λ-submodules, where $\Lambda = \mathbf{Z}_\ell[[T]]$ and T corresponds to $\gamma - 1 \in \mathbf{Z}_\ell[\Gamma]$. Thus we have

$$X^- \hookrightarrow \bigoplus_i \Lambda/(\ell^{m_i}) \oplus \bigoplus_j \Lambda/(g_j(T))$$

with finite cokernel, and likewise

$$\epsilon_\chi X \hookrightarrow \bigoplus_i \Lambda/(\ell^{m_i^\chi}) \oplus \bigoplus_j \Lambda/(g_j^\chi(T))$$

with finite cokernel for all odd characters χ on Δ. (The polynomials g are distinguished polynomials in $\mathbf{Z}_\ell[T]$, meaning that $g_j^\chi(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ with ℓ dividing a_i for $0 \le i \le n-1$. As we have written the decomposition, they are not necessarily irreducible.) For all such χ, let $\mu_\chi = \sum m_i^\chi$, $\lambda_\chi = \sum \deg g_j^\chi$, and let

$$g^\chi(T) = \ell^{\mu_\chi} \prod g_j^\chi(T).$$

(This g^χ is not necessarily a distinguished polynomial, but $\prod g_j^\chi(T)$ is.) Let

$$\mu^- = \sum_{\chi \text{ odd}} \mu_\chi, \qquad \lambda^- = \sum_{\chi \text{ odd}} \lambda_\chi.$$

Barsky [1], Cassou-Noguès [5], and Deligne and Ribet [9] have each shown that one can construct an ℓ-adic L-function $L_\ell(s,\rho)$ for even characters ρ over a totally real field k_0. Furthermore, $L_\ell(s,\rho)$ is Iwasawa analytic if ρ is a non-trivial character on Δ, i.e. $L_\ell(s,\rho)$ can be expressed as a power series in $u^s - 1$, where u is an element of the principal units of $\mathbf{Z}_\ell$, defined by $\gamma\zeta_{\ell^n} = \zeta_{\ell^n}^u$ for $n \geq 1$. (For more information on Iwasawa analytic functions, see Section 4 of [27].) Let

$$\omega : \Delta = \mathrm{Gal}(k_1/k_0) \to \langle \zeta_{\ell-1} \rangle \subseteq \mathbf{Z}_\ell^\times$$

be the ℓ-adic Teichmüller character (which is odd), and let χ be an odd character on Δ. Then, more explicitly, it can be proved that there exists a power series $f_\chi \in \Lambda$ such that

$$L_\ell(1-s, \omega\chi^{-1}) = f_\chi(u^s - 1)/h_\chi(u^s - 1)$$

for $s \in \mathbf{Z}_\ell$, where $h_\chi(T) = T$ if $\chi = \omega$ and $h_\chi(T) = 1$ otherwise.

(This simple characterization of h_χ comes about because all of the characters ψ we consider are one-dimensional and of what Greenberg calls type S, i.e. $k_\psi \cap k_0\mathbf{B}_\infty = k_0$, where k_ψ is this extension of k_0 attached to ψ and $\mathbf{B}_\infty$ is the cyclotomic $\mathbf{Z}_\ell$-extension of $\mathbf{Q}$. For more general ℓ-valued Artin characters, we have $h_\chi(T) = \omega\chi^{-1}(\gamma)(1+T) - 1$ if $\omega\chi^{-1}$ is of what Greenberg calls type W, i.e. $k_\psi \subseteq k_0\mathbf{B}_\infty$, and $h_\chi(T) = 1$ otherwise.)

In order to relate these power series to X^-, we use the Main Conjecture of Iwasawa theory, which was proved by Mazur and Wiles for abelian extensions of $\mathbf{Q}$ in [24] and by Wiles for arbitrary totally real fields in [33]. Using notation from [33] and [31], the theorem says:

Theorem 6.1 (The Main Conjecture)**.** *For χ an odd character on Δ,*

$$f_\chi(u(1+T)^{-1} - 1) = g^\chi(T)U_\chi(T),$$

with $U_\chi(T)$ a unit in Λ.

(This is a combination of Theorems 1.2 and 1.4 of [33]. See also Section 13.6 of [31], or Section 5 of [6] for more on the Main Conjecture.)

Let $\delta = [k_1 : k_0] = |\Delta|$, and let ℓ^e be the largest power of ℓ such that $\zeta_{\ell^e} \in k_0(\zeta_\ell)$.

Definition 6.2. Let $L(s,\chi)$ be the L-function for characters associated to k_0. We say that ℓ is *k_0-regular* if ℓ is relatively prime to $L(1-m,1) = \zeta_{k_0}(1-m)$ for all even m such that $2 \leq m \leq \delta - 2$ and also ℓ is relatively prime to $\ell^e L(1-\delta,1) = \ell^e\zeta_{k_0}(1-\delta)$.

Remark 6.3. This new definition is analogous to ℓ being regular, since if $k_0 = \mathbf{Q}$ we have $\delta = \ell - 1$, $L(1-m,1) = -B_m/m$ for B_m the m-th Bernoulli number, $2 \leq m \leq \ell - 3$, and ℓ never divides $\ell^e L(2-\ell,1) = -\ell B_{\ell-1}/(\ell-1)$ by Von Staudt-Claussen's Theorem (Theorem 5.10 of [31]) or by the argument given in Section 2 of [26]. Also, k_0-regularity seems to share at least some of the properties of regularity. For example, by a proof analogous to one for the case over $\mathbf{Q}$, I have shown that there are infinitely many k_0-irregular primes for any given k_0. (See, e.g., Theorem 5.17 and Exercise 4.3.(a) of [31].)

Remark 6.4. We will show below that the numbers in these conditions are ℓ-integral. (It is well-known that they are rational numbers; see, e.g., [25].)

Theorem 6.5. *Suppose ℓ is k_0-regular. Then there are no unramified infinite powerful pro-ℓ extensions M of k_n, Galois over k_0, such that $K \cap M = k_n$ and $\mathrm{Gal}(M_{el}/k_n) = \mathrm{Gal}(M_{el}/k_n)^-$ according to the action of Δ, where M_{el} is the maximal elementary abelian subextension of M/k_n.*

Remark 6.6. The condition $K \cap M = k_n$ is equivalent to saying that k_n contains all the ℓ-th power roots of unity in M. Note that for sufficiently large n, K/k_n is totally ramified (see Lemma 13.3 of [31], e.g.). However, M/k_n is unramified by hypothesis, so for these n, $K \cap M = k_n$ always.

Remark 6.7. The action of Δ on $\mathrm{Gal}(M_{el}/k_n)$ comes from the action of $\mathrm{Gal}(k_n/k_0)$, which is by conjugation in $\mathrm{Gal}(M_{el}/k_0)$ by some representative. (Note that M_{el}/k_0 is Galois, because $\mathrm{Gal}(M/M_{el})$ is a characteristic subgroup of a normal subgroup of $\mathrm{Gal}(M/k_0)$, and the last extension is Galois by hypothesis. Furthermore, $\mathrm{Gal}(M_{el}/k_n)$ is a normal subgroup of $\mathrm{Gal}(M_{el}/k_0)$, so the action above is defined.) The action is independent of the choice of representative, since $\mathrm{Gal}(M_{el}/k_n)$ is abelian.

Proof (of Theorem). Let M be such an extension of k_n. As in previous theorems, we may assume by Lemma 4.3 that M is a uniform extension of k_n. Let $G = \mathrm{Gal}(M/k_n)$, and let d be the dimension of G. Since M is Galois over k_0, γ acts on G by conjugation in $\mathrm{Gal}(M/k_0)$ (equivalently in $\mathrm{Gal}(M/k_1)$) by some representative.

Let K^{urel} be the maximal elementary abelian subextension of K^{urab}/K and let M_{el} be the maximal elementary abelian subextension of M/k_n. Since Δ acts on X, and $\mathrm{Gal}(M_{el}/k_n) = \mathrm{Gal}(M_{el}/k_n)^-$, we can consider M_{el} as a subextension of $(K^{urab})^-$ and $(K^{urel})^-$. (See Figure 2.)

By hypothesis, $M \cap K = k_n$. Let $\mathrm{Frat}(G) = \overline{[G,G]G^\ell}$ be the Frattini subgroup of G, which is equal to G^ℓ since G is powerful and finitely generated. Then $G/\mathrm{Frat}(G) = G/G^\ell = \mathrm{Gal}(M_{el}/k_n) \cong \mathrm{Gal}(M_{el}K/K)$, which is a quotient of $\mathrm{Gal}((K^{urel})^-/K)$.

Since

$$X^- = \bigoplus_{\chi \text{ odd}} \epsilon_\chi X,$$

we can write

$$X^- \hookrightarrow \bigoplus_{\chi \text{ odd}} \left(\bigoplus_{i=1}^{s_\chi} \Lambda/(\ell^{m_i^\chi}) \oplus \bigoplus_{j=1}^{t_\chi} \Lambda/(g_j^\chi(T)) \right)$$

with finite cokernel. We want to know whether γ has any fixed points as an automorphism of $\mathrm{Gal}((K^{urel})^-/K) \cong X^-/\ell X^-$.

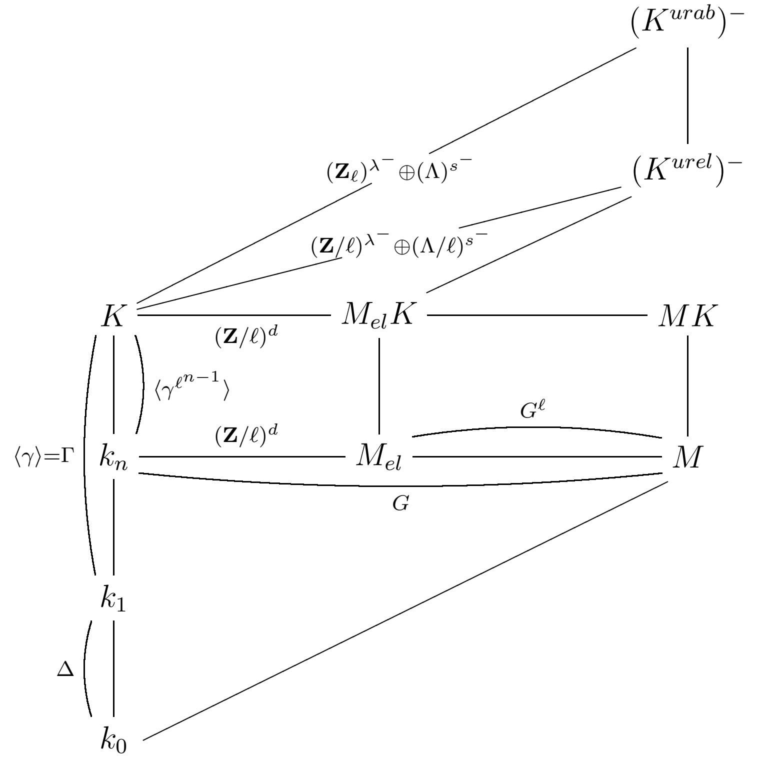
So far we can deduce that $X^-/\ell X^- \cong (\mathbf{Z}/\ell)^{\lambda^-} \oplus (\Lambda/\ell)^{s^-}$, where $s^- = \sum s_\chi$. We will next show that for all odd χ, $s_\chi = 0$ in the decomposition of X^-, so that in fact only the second group of terms exists, and $X^-/\ell X^- \cong (\mathbf{Z}/\ell)^{\lambda^-}$.

Claim 6.7.1. *Under the hypotheses of the theorem, ℓ is relatively prime to $f_\chi(u-1)$ for all odd χ.*

(We will defer the proof of this until later.)

By the Main Conjecture, $f_\chi(u-1) = f_\chi(u(1+0)^{-1}-1) = g^\chi(0)U_\chi(0)$. $U_\chi(T)$ is a unit power series, so it is well-known that $U_\chi(0)$ must be a unit in $\mathbf{Z}_\ell$. Thus if ℓ is relatively prime

FIGURE 2. The relationships between the subfields of M and K in the number field case.


$(K^{urab})^-$
$(\mathbf{Z}_\ell)^{\lambda^-}\oplus(\Lambda)^{s^-}$
$(K^{urel})^-$
$(\mathbf{Z}/\ell)^{\lambda^-}\oplus(\Lambda/\ell)^{s^-}$
K
$M_{el}K$
MK
$(\mathbf{Z}/\ell)^d$
$\langle\gamma^{\ell^{n-1}}\rangle$
G^ℓ
$\langle\gamma\rangle=\Gamma$
k_n
$(\mathbf{Z}/\ell)^d$
M_{el}
M
G
k_1
Δ
k_0

to $f_\chi(u-1)$ then it is also relatively prime to $g^\chi(0)$ in $\mathbf{Z}_\ell$. But $g^\chi(0) = \ell^{\mu_\chi}\prod g_j^\chi(0)$, so we must have $0=\mu_\chi=\sum m_i^\chi$, so $s_\chi = 0$. Thus

$$X^- \hookrightarrow \bigoplus_{\chi \text{ odd}} \bigoplus_{j=1}^{t_\chi} \Lambda/(g_j^\chi(T))$$

with finite cokernel.

Now let R be the λ^- by λ^- matrix, with $\mathbf{Z}_\ell$-coefficients, representing the action of γ on X^-, which is isomorphic to $\mathbf{Z}_\ell^{\lambda^-}$. Then γ acts on $X^-/\ell X^-$ according to the reduction of R modulo ℓ. If 1 is not an eigenvalue of R modulo ℓ, then this action has no non-trivial fixed points, i.e. is regular. Since $X^-\otimes\mathbf{Q}_\ell \cong \left(\bigoplus_{\chi\text{ odd}}\bigoplus_j \Lambda/(g_j^\chi(T))\right)\otimes\mathbf{Q}_\ell$, as $\mathbf{Q}_\ell[[T]]$-modules, their characteristic polynomials for γ are the same. Since T corresponds to $\gamma-1$, the characteristic polynomial of the right-hand side is $\prod_{\chi\text{ odd}} g^\chi(x-1) = \prod_{\chi\text{ odd}}\prod_j g_j^\chi(x-1)$, so this is the characteristic polynomial of R also.

Now the eigenvalues of R modulo ℓ are the roots of the various $g^\chi(x-1)$ modulo ℓ, so 1 is such an eigenvalue if and only if $g^\chi(0)\equiv 0$ modulo ℓ for some χ. Again, the Main Conjecture says this is only if $f_\chi(u-1)\equiv 0$ modulo ℓ, and we know from the claim that this does not happen. So 1 is not an eigenvalue for g^χ for any χ.

Thus, given the claim, the action of φ on $\mathrm{Gal}((K^{urel})^-/K)\cong X^-/\ell X^-$ is regular. We will now prove the claim.

Proof (of Claim). By the definition of f_χ, we have

$$f_\chi(u-1) = f_\chi(u^1-1) = L_\ell(0,\omega\chi^{-1})h_\chi(u-1). \tag{1}$$

Further, as in [33], we have by definition, for $n \geq 1$:

$$L_\ell(1-n,\rho) = L_S(1-n,\rho\omega^{-n}), \tag{2}$$

where

$$L_S(1-n,\rho\omega^{-n}) = L(1-n,\rho\omega^{-n}) \prod_{\mathfrak{l}\in S}(1-\rho\omega^{-n}((\mathfrak{l},k_1/k_0))(N\mathfrak{l})^{n-1}), \tag{3}$$

S is the set of primes of k_0 lying over ℓ, L is the complex Dirichlet L-function, N is the norm, and $(\mathfrak{l},k_1/k_0)$ is the Artin reciprocity symbol. (We use the convention that the product of characters is always primitive. This formula is a generalization of Theorem 5.11 of [31]; see also Section 4.1 of [6].) Furthermore, $L_\ell(1-s,\rho)h_\chi(u^s-1)$ is a power series in u^s-1 (i.e. Iwasawa analytic) so since $u^s-1 \equiv 0$ modulo $\ell\mathbf{Z}_\ell$ for all $s \in \mathbf{Z}_\ell$, we have that the expression

$$L_\ell(1-s,\rho)h_\chi(u^s-1) \tag{4}$$

has the same value modulo $\ell\mathbf{Z}_\ell$ for any $s \in \mathbf{Z}_\ell$.

We are looking at $f_\chi(u-1) = L_\ell(0,\omega\chi^{-1})h_\chi(u-1)$, where χ is an odd character on the Galois group Δ, and thus equal to ω^m for some odd m, $1 \leq m \leq \delta-1$. Since $f_\chi \in \Lambda$ and $u \in \mathbf{Z}_\ell$, we have $f_\chi(u-1) \in \mathbf{Z}_\ell$. Note that $\delta+1-m \equiv 1-m$ modulo δ, so $\omega^{1-m} = \omega^{\delta+1-m}$ and $2 \leq \delta+1-m \leq \delta$. Then we have

$$\begin{aligned}
&f_\chi(u-1)\\
&\quad= L_\ell(0,\omega\chi^{-1})h_\chi(u-1) \quad \text{from (1)}\\
&\quad= L_\ell(0,\omega^{\delta+1-m})h_\chi(u-1)\\
&\quad\equiv L_\ell(1-(\delta+1-m),\omega^{\delta+1-m})h_\chi(u^{\delta+1-m}-1) \pmod{\ell} \quad \text{from (4)}\\
&\quad= L_S(1-(\delta+1-m),\omega^{\delta+1-m})h_\chi(u^{\delta+1-m}-1) \quad \text{from (2)}\\
&\quad= L(1-(\delta+1-m),\omega^{\delta+1-m}\omega^{-(\delta+1-m)})\\
&\qquad\cdot\left(\prod_{\mathfrak{l}\in S}(1-\omega^{\delta+1-m}\omega^{-(\delta+1-m)}((\mathfrak{l},k_1/k_0))(N\mathfrak{l})^{\delta-m})\right) h_\chi(u^{\delta+1-m}-1)\\
&\qquad\text{from (3)}\\
&\quad= L(1-(\delta+1-m),1)\left(\prod_{\mathfrak{l}\in S}(1-(N\mathfrak{l})^{\delta-m})\right) h_\chi(u^{\delta+1-m}-1)
\end{aligned}$$

Now $(N\mathfrak{l})^{\delta-m}$ is a power of ℓ, since $m < \delta$. So this is congruent to

$$L(1-(\delta+1-m),1)h_\chi(u^{\delta+1-m}-1) \quad \text{modulo } \ell.$$

For $\chi \neq \omega$, we have $h_\chi(T) = 1$, and so this equals $L(1-(\delta+1-m),1)$, which is thus ℓ-integral since $f_\chi(u-1)$ is. Also, $\chi \neq \omega$ implies $m > 1$, so we actually have $2 \leq \delta+1-m \leq \delta-2$. If ℓ is k_0-regular then ℓ is relatively prime to $L(1-(\delta+1-m),1)$ for all of these $\delta+1-m$, so $f_\chi(u-1)$ is relatively prime to ℓ for any $\chi \neq \omega$. If $\chi = \omega$ then $h_\omega(T) = T$ so we have

$$\begin{aligned}
f_\omega(u-1) &\equiv L(1-(\delta+1-m),1)(u^{\delta+1-m}-1) \pmod{\ell}\\
&= L(1-\delta,1)(u^\delta-1),
\end{aligned}$$

since m must equal 1. Writing $u = 1 + t\ell^e$ for t a unit in $\mathbf{Z}_\ell$ and using the binomial theorem, we can see that $(u^\delta - 1)/\ell^e$ is a unit in $\mathbf{Z}_\ell$, in fact congruent to $\delta t = \delta(u-1)/\ell^e$ modulo ℓ. In particular, since $f_\omega(u-1)$ is in $\mathbf{Z}_\ell$, we must have $\ell^e L(1-\delta, 1)$ in $\mathbf{Z}_\ell$, since they differ by a unit in $\mathbf{Z}_\ell$. Further, ℓ divides $\ell^e L(1-\delta,1)$ if and only if it divides

$$f_\omega(u-1) \equiv L(1-\delta,1)(u^\delta - 1) = \ell^e L(1-\delta,1)\left(\frac{u^\delta - 1}{\ell^e}\right).$$

If ℓ is k_0-regular, then ℓ is relatively prime to $\ell^e L(1-\delta,1)$, and thus to $f_\omega(u-1)$. □

Now we know that the action of φ on $\mathrm{Gal}((K^{urel})^-/K)$, which can be regarded as a vector space over $\mathbf{Z}/\ell\mathbf{Z}$, is regular. We also know that φ acts on G, which induces an action on $G/G^\ell \cong \mathrm{Gal}(M_{el}K/K)$, since G^ℓ is characteristic. We can also regard G/G^ℓ as a vector space over $\mathbf{Z}/\ell\mathbf{Z}$, and then the action of φ is a quotient of the action on $\mathrm{Gal}((K^{urel})^-/K)$. Thus this action is regular, so the action on G can have no fixed points outside G^ℓ.

The rest of the proof follows as in [4].

□

7. Greenberg's criterion

The concept of k_0-regularity, though not the definition itself, has appeared earlier in work of Greenberg on a generalization of Kummer's criterion for the class number of k_1 to be divisible by ℓ. Greenberg's work ties into my own in a number of ways. The first is through k_0-regular primes. Another is that it allows us, in some cases, to restate Theorem 6.5 in a form rather more parallel to Theorem 2.4. This statement appears as Corollary 7.5.1 below. Furthermore, the techniques used in the previous section allow us to simplify the proofs and weaken the hypotheses in Greenberg's theorems, and we will explore some ways that this can be done. Finally, in some limited situations a proof of Corollary 7.5.1 can be given that parallels that of Remark 2.5, using the ideas of this section.

We keep the notation of the previous section, and also let k_1^+ denote the maximal real subfield of k_1, which is equal to $k_0(\zeta_\ell + \zeta_\ell^{-1})$. Let $h(k_1)$ denote the class number of k_1 and $h^+(k_1)$ denote the class number of k_1^+. By part (a) of Theorem 7.8 below, $h^+(k_1) \mid h(k_1)$; we let the relative class number $h^-(k_1)$ be the quotient.

In [13], Greenberg gave the following generalizations of Kummer's criterion:

Theorem 7.1 (Greenberg, 1973). *Assume that $\ell \nmid [k_0 : \mathbf{Q}]$ and that no prime of the field k_1^+ lying over ℓ splits in k_1. Then ℓ divides the class number of k_1 if and only if ℓ divides the numerator of*

$$\ell \prod_{i\ even, i=2}^{\delta} \zeta_k(1-i).$$

Theorem 7.2 (Greenberg, 1973). *Assume that $\ell \nmid [k_0 : \mathbf{Q}]$ and that no prime of the field k_1^+ lying over ℓ splits in k_1. Further, assume that k_0 is abelian over $\mathbf{Q}$. Then ℓ divides the class number of k_1 if and only if ℓ is not k_0-regular.*

Remark 7.3. Note that Greenberg uses ℓ in his definitions and theorems where we use ℓ^e; his hypothesis that $\ell \nmid [k_0 : \mathbf{Q}]$ implies that e must be equal to 1.

Greenberg also made a stronger conjecture. Let R and R^+ denote the regulators of k_1 and k_1^+ respectively, let w denote the number of roots of unity in k_1, and let

$$A = \lim_{s \to 0} \frac{\prod_{\mathfrak{l} \in S} (1 - (N\mathfrak{l})^{-s})}{\prod_{\mathfrak{l} \in S^+} (1 - (N\mathfrak{l})^{-s})}.$$

Then Greenberg conjectured that

$$Ah^-(k_1) \equiv \frac{w}{2(R/R^+)} \cdot \delta \cdot \prod_{i \text{ even}, i=1}^{\delta} \zeta_{k_0}(1-i) \pmod{\ell},$$

which implies Theorem 7.1.

Kudo, in [21], proved this conjecture in the case where k_0 is abelian over a real quadratic field with no restriction on the degree of k_0, using the ℓ-adic L-function constructed for these fields by Coates and Sinnott in [7]. Using the same construction, Kudo also proved Theorem 7.2 in the case where k_0 is abelian over a real quadratic field and $\ell \nmid [k_0 : \mathbf{Q}]$.

The general construction of the ℓ-adic L-function over any totally real number field and the congruences derived in the proof of the Claim from Theorem 6.5 allow us to prove this statement for any totally real k_0 whatsoever. This gives the following theorem:

Theorem 7.4. *Assume that no prime of the field k_1^+ lying over ℓ splits in k_1. Then ℓ divides $h^-(k_1)$ if and only if ℓ is not k_0-regular.*

Remark 7.5. Note that we no longer require a condition on the degree of k_0; this would only be necessary in order to replace the condition on $h^-(k_1)$ by one on $h(k_1)$ such as Greenberg used. (See Theorem 7.9 below.) Furthermore, as we observed earlier, the construction of the ℓ-adic L-function tells us that the numbers in the definition of k_0-regular are all ℓ-integral, allowing us to remove the distinction between Theorems 7.1 and 7.2.

As a corollary of Theorems 6.5 and 7.4, we get:

Corollary 7.5.1. *Assume that no prime of the field k_1^+ lying over ℓ splits in k_1, and that ℓ does not divide $h^-(k_1)$. Then there are no unramified infinite powerful pro-ℓ extensions M of k_n, Galois over k_0, such that $K \cap M = k_n$ and* $\mathrm{Gal}(M_{el}/k_n) = \mathrm{Gal}(M_{el}/k_n)^-$.

Remark 7.6. Note that if there *are* primes of k_1^+ which split in k_1, then ℓ divides A and so ℓ is *never* k_0-regular. Thus Theorem 6.5 can never be applied if this is true. Furthermore, Theorem 7.4 cannot be used to show ℓ divides $h^-(k_1)$ in this case. (See Greenberg's paper for more on this.)

Remark 7.7. If ℓ does not divide $h^-(k)$, then there are no unramified abelian ℓ-extensions M of k such that $\mathrm{Gal}(M_{el}/k) = \mathrm{Gal}(M_{el}/k)^-$ and thus trivially no powerful extensions. Remark 2.5 uses the corresponding idea to give a quick proof of Theorem 2.4; in certain circumstances we can do the same here.

Consider the following theorems on class groups (see, e.g., Chapter 10 of [31]):

Theorem 7.8. (a) *Suppose the extension of number fields F/F_1 contains no nontrivial unramified abelian subextensions. (This is true, e.g., if some prime is totally ramified.) Then $h(F_1)$ divides $h(F)$.*

(b) *Suppose the extension of number fields F/F_1 is an ℓ extension with at most one ramified prime. If ℓ divides $h(F)$ then ℓ divides $h(F_1)$.*

And finally, Greenberg in [13] gives the theorem (attributed to Leopoldt):

Theorem 7.9 (Leopoldt). *Let k_0 be a totally real finite extension of $\mathbf{Q}$ such that $\ell \nmid [k_0 : \mathbf{Q}]$. If $\ell | h^+(k_1)$ then $\ell | h^-(k_1)$.*

Now let k_0 be such an extension, and suppose as above that ℓ does not divide $h^-(k_1)$. Thus $\ell \nmid h^+(k_1)$ also, so $\ell \nmid h(k_1)$. Now if at most one prime of k_1 ramifies in k then ℓ cannot divide $h(k)$, by part (b) of Theorem 7.8. Thus ℓ certainly doesn't divide $h^-(k)$, so as we said there are trivially no powerful extensions. This gives us a trivial proof of Corollary 7.5.1 under the conditions supposed, but there is no reason to think that a similar proof will work outside these conditions. It is interesting to compare this to the cyclotomic case described in Remark 2.5.

Remark 7.10. Kudo also discusses some congruences modulo higher powers of ℓ which are similar to the one conjectured by Greenberg. It seems likely that under the proper conditions, these congruences would allow us to prove theorems in the number field case analogous to those proved for the function field case in Section 4.

8. Examples II

Having defined k_0-regular primes, it seems in order to give some analysis of how likely the situation is to occur for totally real fields k_0. I have therefore computed the numbers $\zeta_{k_0}(-1), \zeta_{k_0}(-3), \ldots, \zeta_{k_0}(3-\delta)$ and $\ell\zeta_{k_0}(1-\delta)$ for various real quadratic fields $k_0 = \mathbf{Q}(\sqrt{D})$. (For more about zeta functions for real quadratic fields, see [16].)

In the following tables, the discriminant D goes down the side and the prime ℓ goes across the top. The values shown are "numbers of irregularity" m such that ℓ divides $\zeta_{k_0}(1-m)$ or, if $m = \delta$, $\ell\zeta_{k_0}(1-\delta)$.

The tables were calculated using the program PARI (see [2]) using a formula of Siegel (see [29]). The algorithm is discussed further by the author in [17], which also includes some analysis of this raw data.

Table I covers $2 \leq D \leq 100$ and $3 \leq \ell \leq 50$, and Table II covers $2 \leq D \leq 100$ and $51 \leq \ell \leq 100$.

Acknowledgements

The author would like to thank Michael Rosen for his invaluable advice while this research was being done and for his unwavering support during the writing and publication of this paper. Hearty thanks are also due to Gerhard Frey, Ernst Kani, and Yasutaka Ihara for pointing out cases where Question 1 has a negative answer.

References

[1] D. Barsky, Fonctions zêta p-adiques d'une classes de rayon des corps de nombres totalement réels, in *Groupe d'Etude d'Analyse Ultramétrique*, 1977/1978, 5e année, Exp. no. 16, 23 pp.

[2] C. Batut, D. Bernardi, H. Cohen, and M. Olivier, User's Guide to PARI-GP, Laboratoire A2X, Université Bordeaux I, version 1.39 edn., January 14, 1995.

[3] N. Boston, Some cases of the Fontaine-Mazur conjecture, *J. Number Theory* **42** (1992) 285–291.

[4] N. Boston, Some cases of the Fontaine-Mazur conjecture, II, *J. Number Theory* (Submitted — Preliminary version).

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

[6] J. Coates, p-adic L-functions and Iwasawa's theory, in A. Fröhlich, editor, *Algebraic Number Fields (L-functions and Galois Properties)*, pages 269–353, Academic Press, 1977.

TABLE I. Numbers of irregularity for $2 \leq D \leq 100$ and $3 \leq \ell \leq 50$.

	3	5	7	11	13	17	19	23	29	31	37	41	43	47
5						14	8				32	18		
8				4	12		6			30	32 34			
12				8	8			4			30 32	6	16	20
13									4	20	32 34		12	16
17							8	10 16			32	4		20
21			4	4						14 24	16 32			
24	2		6					10	4		32			
28					10			14	18		32			
29	2			10		10	12			14	32			16
33	2								28	24	20 32 36			4
37		2	6							14	14		32	
40			2				4 8				32			
41			4			6	12		28		32		6	
44			2			12	14	8	14		16 32			
53		4	2							4 12	20 32			
56		2						8			24 32			
57			2				10			20 28	32	10		4
60	2						14	8			32			10 44
61				2	6 8	4					32	30		
65							12				32		6	
69	2	4		4		16	12 14	6			32			
73		4	4 6	2		8			10 16	14	32	40		
76							2	10	6		32	20		32
77	2			6							32			
85	2					6				22	32	38		
88				6				2			32		32 42	
89		4	6		2 8 10 12				14		4 32	10	12 14	14
92		2	6						8		32	4	24	
93	2				12				12	16	32			
97					10	2 4 16	12				32		12	

[7] J. Coates and W. Sinnott, On p-adic L-functions over real quadratic fields, *Invent. Math.* **25** (1974) 253–279.

[8] A. J. de Jong, A conjecture on arithmetic fundamental groups, Preprint available on the web.

[9] P. Deligne and K. Ribet, Values of abelian L-functions at negative integers over totally real fields, *Invent. Math.* **59** (1980) 227–286.

[10] J. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, Analytic Pro-p Groups, vol. 157 of *London Math. Soc. Lecture Note Series*, Cambridge University Press, Cambridge, 1991.

[11] J.-M. Fontaine and B. Mazur, Geometric Galois representations, in J. Coates and S. T. Yau, editors, *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, vol. 1 of *Series in Number Theory*, International Press, Cambridge, MA, 1995.

[12] G. Frey, E. Kani, and H. Völklein, Curves with infinite k-rational geometric fundamental group, Preprint available on the web.

[13] R. Greenberg, A generalization of Kummer's criterion, *Invent. Math.* **21** (1973) 247–254.

[14] F. Hajir, On the growth of p-class groups in p-class field towers, *J. Algebra* **188** (1997) 256–271.

[15] D. Harbater, Abhyankar's conjecture on Galois groups over curves, *Invent. Math.* **117** (1994) 1–25.

[16] D. Hayes, Brumer elements over a real quadratic base field, *Exposition. Math.* **8** (1990) 137–184.

[17] J. Holden, Irregularity of prime numbers over real quadratic fields, in *Algorithmic Number Theory: Third International Symposium; Proceedings*, no. 1423 in Springer Lecture Notes in Computer Science, pages 464–462, Springer-Verlag, 1998.

[18] Y. Ihara, On unramified extensions of function fields over finite fields, in *Galois Groups and Their Representations*, vol. 2 of *Adv. Studies in Pure Math.*, pages 89–97, North-Holland, 1983.

[19] I. Ilani, Analytic pro-p groups and their Lie algebras, *J. Algebra* **176** (1995) 34–58.

[20] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, vol. 84 of *Graduate Texts in Mathematics*, Springer-Verlag, second edn., 1990, second Corrected Printing.

TABLE II. Numbers of irregularity for $2 \leq D \leq 100$ and $51 \leq \ell \leq 100$.

	53	59	61	67	71	73	79	83	89	97
5		44	42	6 58		70				
8		34 36 44 50		58	68		16 30		32	
12		44	44	58 60				10		
13	16	32 44	48	58			24	46		32 72
17		44	32	32 50 58	46					36 54
21		12 14 44		58		42 64	16	52		
24		44	30	58	48	8		60 76		
28	46	44		58		24		52		44
29		44		26 58						
33	30	42 44	8	58			26			
37		44		58			50		56 66 88	
40	40 42	44	8	10 58	16 18 30	52	24 70	4		
41	20 52	44		58	34	60	24			46 78
44		18 26 44		58	34	12	14 60 74	22		
53		44		58	68	52	28	54		44
56	50	14 44	26	58	38 66		46			
57		44 58	4 10	26 50 58 64					52	
60		12 22 44	52	58	10 40	16		34		68
61		34 44		22 58				30 58 80		
65		32 44 48		58			16	50	18	
69	14 20	44		24 58			38	70	70	88
73		44 50	20	14 58	28			56	52 58	
76	22	44	38	58	16		8 74 78			
77		16 44		40 58			34 36			90
85		44 46	18	58			28			
88		36 44		58	16 26	56 72	50	40		
89		44 58		58	62	4		52		36
92		44		42 58				74	34 74	
93	26 50	44		58	54			46	34	
97		44		58	32	66	34		8	

[21] A. Kudo, On a generalization of a theorem of Kummer, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **29** (1975) 255–261.

[22] M. Lazard, Quelques calculs concernant la formule de Hausdorff, *Bull. Soc. Math. France* **91** (1963) 435–451.

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

[24] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbf{Q}$, *Invent. Math.* **76** (1984) 179–330.

[25] K. Ribet, Report on p-adic L-functions over totally real fields, *Astérisque* **61** (1979) 177–192.

[26] M. Rosen, Remarks on the history of Fermat's last theorem 1844 to 1984, in G. Cornell, J. H. Silverman, and G. Stevens, editors, *Modular Forms and Fermat's Last Theorem*, pages 505–525, Springer-Verlag, 1997.

[27] J.-P. Serre, Formes modulaires et fonctions zêta p-adiques, in *Modular Functions of One Variable, III (Antwerp 1972)*, vol. 350 of *Springer Lecture Notes in Mathematics*, pages 191–268, Springer-Verlag, 1973.

[28] A. Shalev, On almost fixed point free automorphisms, *J. Algebra* **157** (1993) 271–282.

[29] C. L. Siegel, Bernoullische Polynome und quadratische Zahlkörper, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* **2** (1968) 7–38.

[30] J. H. Silverman, The Arithmetic of Elliptic Curves, vol. 106 of *Graduate Texts in Mathematics*, Springer-Verlag, 1986.

[31] L. C. Washington, Introduction to Cyclotomic Fields, vol. 83 of *Graduate Texts in Mathematics*, Springer-Verlag, second edn., 1997.

[32] W. C. Waterhouse and J. S. Milne, Abelian varieties over finite fields, in D. J. Lewis, editor, *1969 Number Theory Institute (Proceedings of Symposia in Pure Mathematics, Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64, American Mathematical Society, Providence, R.I., 1971.

[33] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. of Math. (2)* **131** (1990) 493–540.

Department of Mathematics and Statistics, University of Massachusetts at Amherst, Amherst, MA 01003, USA
E-mail address: holden@math.umass.edu