GALOIS GROUPS WITH PRESCRIBED RAMIFICATION

David Harbater

Abstract. The paper studies Galois groups with a given set of ramified places, in both the function field and number field cases. In the geometric case, it is shown in characteristic p that the fundamental group of a curve of genus g with $r > 0$ points deleted depends upon the choice of curve and points, and not just on g and r (unlike in characteristic 0). In the arithmetic case, certain groups are shown to occur over $\mathbf{Q}$ with given ramification, or are shown not to occur, particularly when the only ramified prime is 2.

Introduction

This paper concerns the problem of finding which groups occur as Galois groups with prescribed ramification. The problem can appear both in arithmetic and in geometric settings, and can be interpreted as a problem of finding fundamental groups. Specifically, given a Dedekind domain D and a finite set S of primes, we may consider the fundamental group $\pi_1(\mathrm{Spec}(D) - S)$, and the related set $\pi_A(\mathrm{Spec}(D) - S)$ of finite quotients of π_1. Here π_A consists of the finite groups that can occur as Galois groups over (the fraction field of) D with ramification only at S. We then wish to understand π_A and, if possible, π_1, as well as obtaining information about which subgroups of a given group $G \in \pi_A$ can occur as inertia groups. In this paper, we consider these four situations (which are in turn less and less well understood):

(i) complex affine curves;
(ii) affine curves over an algebraically closed field of characteristic p;
(iii) affine curves over a finite field;
(iv) open subsets $U_n = \mathrm{Spec}(\mathbf{Z}[1/n])$ of $\mathrm{Spec}(\mathbf{Z})$.

Section 1 considers (i) - (iii). Situation (i) is the most classical, of course, and in particular π_1 is known, by Riemann's Existence Theorem. But even there, there is no known *explicit* version of Riemann's Existence Theorem, and as a result one can rarely write down algebraically an extension of $\mathbf{C}(x)$ with given group and ramification. Situation (ii) was until recently wide open, but the recent proof [Ra], [Ha3] of Abhyankar's Conjecture [Ab1] has answered the question of what π_A is. In particular, it is now known that π_A of an affine curve U of the form (genus g) $-$ (r points) depends only on the numbers g and r. But the profinite

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R32, 14H30; Secondary 13B05, 12F10.

Key words and phrases. Galois, ramification, cover, fundamental group.

The author was supported in part by NSA grant # MDA 904-92-H-3024.

This paper is in final form, and no version of it will be submitted for publication elsewhere..

group π_1 is still very much unknown, and in section 1 we show that $\pi_1(U)$ does *not* just depend on g and r (Theorem 1.8). This raises the question of to what extent $\pi_1(U)$ determines the curve U. In section 1 we give some results concerning this question, and pose some open problems, as well as deriving other consequences of Abhyankar's Conjecture. We also discuss situation (iii), about which less is known.

Section 2 concerns situation (iv), which is the most wide-open of the four. While much is known about the realization of groups as Galois groups over $\mathbf{Q}$ ("inverse Galois theory"), and about *abelian* groups as Galois groups with prescribed ramification (class field theory), much less is known about which general finite groups occur as Galois groups over $\mathbf{Q}$ with prescribed ramification. While a full solution is of course far off in the future, we present some results of the sort that are currently being sought in connection with situation (iii). Motivated by the analogy with the geometric situation, we make a conjecture on how the tame fundamental group of $U_n = \mathrm{Spec}(\mathbf{Z}[1/n])$ grows with n (Conjecture 2.1), and give some evidence for this (Theorem 2.6). Concerning the opposite part of π_1, viz. the p-part of $\pi_1(U_p)$, after showing that this is cyclic for odd p (Theorem 2.11) we study the more involved case of $p = 2$ (where, e.g., the dihedral group D_4 is in $\pi_A(U_2)$ but not the quaternion group; cf. 2.12(b), 2.14). We also show (cf. Corollary 2.7) that all groups in $\pi_A(U_2)$ are quasi-2 groups (which is analogous to the result for situations (ii) and (iii) in the case of the affine line), but that there are also further restrictions, such as the fact that a non-2 Galois extension ramified only at 2 must have a high index of wild ramification (Theorem 2.23). In fact, we show that all small groups in $\pi_A(U_2)$ are 2-groups, and we find the smallest non-2-group in $\pi_A(U_2)$ (of order 272). In particular, we show that the four smallest non-abelian simple groups do not lie in $\pi_A(U_2)$ (Example 2.21); this relates to Serre's Conjecture. In connection with these results, we also state some open questions and speculations.

I would like to thank Robert Coleman for posing to me the problem of how $\pi_1(U_n)$ grows with n; Hendrik Lenstra for a number of discussions concerning techniques that can be used in studying $\pi_1(U_n)$; and J.-P. Serre for his comments on an earlier version of this paper. I would also like to thank Ram Abhyankar, Michael Larsen, Karl Rubin, Alice Silverberg, John Tate, Jaap Top, and Larry Washington for useful comments and suggestions.

Section 1. Geometric Galois groups

Let k be a field, and consider smooth connected affine curves U over k. Each such U is of the form $X - S$, where X is a smooth projective k-curve of some genus g, and $S \neq \emptyset$ consists of finitely many closed points of X. For each U, we wish to understand $\pi_1(U)$ and $\pi_A(U)$. In particular, we may ask how π_1 and π_A vary as U changes – viz. as the choice of S changes, or as the projective curve X varies in moduli.

The most classical case is that of $k = \mathbf{C}$. In this case, we know by Riemann's Existence Theorem (e.g. [Gr, XIII, Cor.2.12]) that $\pi_A(U)$ is the set of finite quotients of the topological fundamental group $\pi_1^{\mathrm{top}}(U)$, and that $\pi_1(U)$ is the profinite completion of $\pi_1^{\mathrm{top}}(U)$. Thus if S consists of n points (so $n > 0$), then $\pi_1^{\mathrm{top}}(U)$ is the group generated by elements $a_1, \ldots, a_g, b_1, \ldots, b_g, c_1, \ldots, c_n$ subject only to the relation that $\prod_{j=1}^{g}[a_j, b_j] \prod_{i=1}^{n} c_i = 1$, where $[a, b]$ denotes the commutator $aba^{-1}b^{-1}$.

This is isomorphic to the free group on $2g+n-1$ generators; so $\pi_A(U)$ consists of the finite groups having $2g+n-1$ generators, and the algebraic fundamental group $\pi_1(U)$ is isomorphic to the free profinite group on $2g+n-1$ generators.

If X is fixed and the n points of S are allowed to vary, then the above fundamental groups do not change, up to isomorphism. (But there is no canonical isomorphism between the π_1's of the old and new U's, since an isomorphism depends on a choice of homotopy basis.) More generally, consider the moduli space $\mathcal{M}_{g,n}$ of projective curves of genus g and n marked points. For each point $[(X,S)]$ of $\mathcal{M}_{g,n}$, we may consider $\pi_1(U)$ and $\pi_A(U)$, where $U = X - S$. Again, these do not depend on the point of $\mathcal{M}_{g,n}$, up to isomorphism.

Similarly, one may consider the case where k is a general algebraically closed field of characteristic 0. For such k, Grothendieck used the technique of specialization to show [Gr, XIII, Cor.2.12] that the fundamental group of $U = X - S$ is given by the same expression as in the case of ground field $\mathbf{C}$. So again $\pi_1(U)$ depends only on the genus of the curve X and the number of points in S – not on the specific choice of curve X or position of the points S, and not on the field k.

For the rest of this section we consider the situation in characteristic $p > 0$. For now, assume that the field k is algebraically closed. Then π_1 behaves differently than over $\mathbf{C}$. In particular, the affine line is no longer simply connected, since there are Artin-Schreier covers. For example, for each non-zero $c \in k$, there is a $\mathbf{Z}/p$-Galois cover of the affine x-line given by $y^p - y = cx$. Moreover, these covers are non-isomorphic (as $\mathbf{Z}/p$-Galois covers of the x-line) for distinct values of $c \in k$. This points out another difference between characteristics 0 and p: In characteristic p, coverings have "moduli"; and as a result, the group π_1 depends on the choice of algebraically closed ground field k. Indeed, if one enlarges k, then π_1 also becomes enlarged, in characteristic p.

More generally, by taking towers of $\mathbf{Z}/p$-covers, it is possible to realize every finite p-group as a Galois group over any affine k-curve. Many other finite groups also occur in π_A, as the following result states. (For a finite group G, the notation $p(G)$ denotes the (normal) subgroup of G generated by the subgroups of p-power order.)

Theorem 1.1. *Let X be a smooth connected projective curve over k, and let $S \subset X$ consist of n points ($n > 0$). Then $\pi_A(U) = \{G \mid G/p(G)$ has $2g+n-1$ generators$\}$.*

This result was originally conjectured in 1957 by Abhyankar [Ab1]. Equivalently, he conjectured that a finite group G occurs over U if and only if every prime-to-p quotient of G occurs over an analogous curve over $\mathbf{C}$ (i.e. a curve of the same genus with the same number of punctures). After partial results by Nori [Ka], Abhyankar [Ab2], and Serre [Se2], the theorem was proven by Raynaud [Ra] in the case that U is the affine line. In this case, the result asserts that π_A consists of all the finite *quasi-p groups*, i.e. the finite groups G such that $G = p(G)$. The more general case of the theorem was proven by the present author in [Ha3]. Moreover that paper proved even more, viz. that for a given G that is predicted to lie in π_A, the cover may be chosen so that its smooth completion is wildly ramified only over one particular point of S. Both [Ra] and [Ha3] rely on patching techniques (rigid or formal analysis) to construct covers with desired Galois groups.

Remark. While a full description of the proof of Theorem 1.1 is beyond the scope of this paper, here is a brief outline. Raynaud's proof of the case $U = \mathbf{A}^1$ [Ra] proceeds by induction, and considers three cases:

(i) G has a non-trivial normal p-subgroup N. Then $G/N \in \pi_A$ by induction, and then $G \in \pi_A$ by Serre's result [Se2].

(ii) A Sylow p-subgroup P of G has the property that G is generated by the set S of proper quasi-p subgroups of G having a Sylow p-subgroup contained in P. Then the groups in S are in π_A by induction, and a patching argument allows the corresponding covers to be pasted together to form a G-Galois cover of $\mathbf{A}^1$.

(iii) Both (i) and (ii) fail. Then an argument involving semi-stable reduction is used to construct a G-cover of $\mathbf{A}^1$.

The proof in the general case [Ha3] proceeds in two steps:

(a) Using [Ra], the result is shown for $\mathbf{P}^1 - \{0, \infty\}$. This is done by patching a $p(G)$-Galois cover of $\mathbf{A}^1$ (which exists by [Ra]) to a cyclic-by-p cover of $\mathbf{P}^1 - \{0, \infty\}$ (which is essentially constructed explicitly).

(b) For a more general affine curve U, an appropriate Galois cover of $\mathbf{P}^1 - \{0, \infty\}$ (given by step (a)) is pasted to a prime-to-p cover of U, to yield a G-Galois cover of U. □

Corollary 1.2. *Let X be a smooth connected projective k-curve of genus g and let S be a non-empty finite subset of X, say having n points. Let $U = X - S$. Then $\pi_A(U)$ depends only on g and n, and not on the choices of X or S. In fact, $\pi_A(U)$ depends only on the value of $2g + n$.*

Proof. Immediate from Theorem 1.1. □

Corollary 1.3. *Fix $g \geq 0$ and $n > 0$. Then π_A of a k-curve of genus g with n points deleted strictly contains π_A of a $\mathbf{C}$-curve of genus g with n points deleted.*

Proof. Denote these two affine curves by U_k and $U_{\mathbf{C}}$. If G is in $\pi_A(U_{\mathbf{C}})$, then G and hence $G/p(G)$ has $2g + n - 1$ generators; so G is in $\pi_A(U_k)$ by 1.1. This shows containment. For strict containment, choose $N > 2g + n - 1$, and let $G = (\mathbf{Z}/p)^N$. Then G is in $\pi_A(U_k)$ by 1.1, since $G/p(G)$ is trivial; but G is not in $\pi_A(U_{\mathbf{C}})$. □

Remarks. (a) Corollary 1.3 is somewhat surprising, for the following reason: A $\mathbf{Z}/3$-Galois cover $E \to \mathbf{P}^1_{\mathbf{C}}$ branched at $\{0, 1, \infty\}$ is an elliptic curve, and its maximal unramified elementary abelian p-cover $F \to E$ satisfies $\mathrm{Gal}(F/E) = (\mathbf{Z}/p)^2$. The composition $F \to \mathbf{P}^1_{\mathbf{C}}$ is Galois, with three-fold ramification over each of its branch points $\{0, 1, \infty\}$, and its Galois group G is a semi-direct product of $(\mathbf{Z}/p)^2$ with $\mathbf{Z}/3$. But there is no such cover of the projective k-line (i.e. no cover with the same group, branch locus, and inertia groups), since any such cover would yield a $(\mathbf{Z}/p)^2$-Galois unramified cover of an elliptic curve in characteristic p. But by Corollary 1.3, there must be some *other* G-Galois cover of $\mathbf{P}^1_k$ branched at $\{0, 1, \infty\}$. Note that such a cover must be wildly ramified somewhere.

(b) Theorem 1.1 and its corollaries do not carry over to the case of *projective* curves (i.e. where we allow $n = 0$). For example, 1.1 and 1.3 fail to hold for genus 1 curves, since $(\mathbf{Z}/p)^2$ is not in π_A of any elliptic curve over k. Similarly, 1.2 fails since $\mathbf{Z}/p$ fails to lie in π_A of a supersingular elliptic curve, although it is in π_A

of an ordinary elliptic curve. A further discussion of the projective analog of these questions will appear in the forthcoming Ph.D. thesis of Katherine Stevenson. □

In addition to knowing which groups can occur as Galois groups of unramified covers of an affine curve $U = X - S$ (and hence as Galois groups of branched covers of X unramified away from S), it would be desirable to know what types of ramification can occur over each of the points of S. While the strong form of Theorem 1.1 in [Ha3] provides some information of this sort, the situation is unknown in general. (Cf. also Remark (a) above.) In the simplest situation, that of the affine line, it is easy to see that there is a necessary condition for a group to occur as inertia over infinity:

Proposition 1.4. *Let G be a quasi-p group, let $Y \to \mathbf{P}^1$ be a G-Galois connected branched cover ramified only over infinity, and let $I \subset G$ be an inertia group over infinity. Then I is a semi-direct product $P \rtimes C$, where C is a cyclic group of order prime to p and where P is a p-group whose conjugacy class generates G.*

Proof. Since k is algebraically closed of characteristic p, every inertia group is cyclic-by-p. Now for $I = P \rtimes C$ an inertia group over infinity, let $N \subset G$ be the subgroup generated by the conjugacy class of P. Then N is a normal subgroup, and $Y/N \to \mathbf{P}^1$ is a G/N-Galois connected branched cover, unramified away from infinity. But since N contains P and its conjugates, this cover is at most tamely ramified over infinity. But over any algebraically closed field, the projective line has no non-trivial connected covers that are unramified away from infinity and tamely ramified over infinity. So G/N is trivial, and thus $N = G$. □

Abhyankar has recently suggested that the converse of Proposition 1.4 may be true; i.e. that the conditions on I in the conclusion of 1.4 may imply that I is an inertia group over infinity of some G-Galois unramified cover of $\mathbf{A}^1$ (i.e. of a branched cover of $\mathbf{P}^1$ ramified over infinity). Some evidence for this is the following:

(i) For many quasi-p matrix groups, Abhyankar has shown that the cyclic group of order p occurs as an inertia group over infinity of some unramified cover of $\mathbf{A}^1$.

(ii) By [Ha2, Theorem 2], if $I \subset G$ is a p-subgroup occuring as an inertia group over infinity of a G-Galois cover of $\mathbf{A}^1$, and if $I' \subset G$ is a p-subgroup containing I, then I' also occurs (for some other cover).

(iii) By (ii) and [Ha2, Lemma to Theorem 4], or by [Ra, Cor. 2.2.6], every Sylow p-subgroup of a quasi-p group G is an inertia group over infinity of some G-Galois cover of $\mathbf{A}^1$.

A related problem is to describe the set $\pi_A^{p'\mathrm{ram}}(U)$ of Galois groups of unramified Galois covers of $U = X - S$ whose completion has the property that all of its inertia groups (over the points of S) are of order prime to p. (In characteristic p, $\pi_A^{p'\mathrm{ram}}(U) = \pi_A^{\mathrm{t}}(U)$, the set of Galois groups of tamely ramified covers; these groups may have order divisible by p.) With $\pi_A^{p'\mathrm{ram}}(U)$ replacing $\pi_A(U)$, the statement of Theorem 1.1 becomes false because every group in $\pi_A^{p'\mathrm{ram}}(U)$ has $2g + n - 1$ generators [Gr, XIII, Cor.2.12], unlike $\pi_A(U)$; the correct replacement for the assertion is unknown. Remark (a) after Corollary 1.3 shows that the analog of 1.3 for $\pi_A^{p'\mathrm{ram}}$

fails. And the analog of Corollary 1.2 for $\pi_A^{p'\mathrm{ram}}$ also fails, as the following example shows:

Example 1.5. Assume $p \neq 2$ and let $\lambda \in \mathbf{P}^1$. Let $E \to \mathbf{P}^1_k$ be the branched cover having degree 2 and branched precisely at $\{0, 1, \infty, \lambda\}$. Thus E is an elliptic curve, and if λ is chosen so that E is ordinary then there is a unique unramified Galois covering morphism $E^* \to E$ of degree p, where E^* is connected. Thus $E^* \to \mathbf{P}^1$ is Galois, and its Galois group G is a semi-direct product of $\mathbf{Z}/p$ with $\mathbf{Z}/2$. Thus $G \in \pi_A^{\mathrm{t}}(U)$, where $U = \mathbf{P}^1 - \{0, 1, \infty, \lambda\}$. But if now another value of λ is chosen (say λ') yielding a supersingular elliptic curve $E' \to \mathbf{P}^1_k$, then G cannot lie in $\pi_A^{\mathrm{t}}(U')$, where $U' = \mathbf{P}^1 - \{0, 1, \infty, \lambda'\}$. For otherwise, there is a Galois branched cover $E'^* \to \mathbf{P}^1$ with group G, having only tame ramification. By the structure of G, this cover dominates a degree two cover $E'' \to \mathbf{P}^1$ that is unbranched away from $\{0, 1, \infty, \lambda'\}$. Since the characteristic of k is not 2, such a cover has genus at most 1, with equality if and only if $E'' \cong E'$ (in which case E'' is supersingular). Thus E'' has no connected unramified covers of degree p, and so the $\mathbf{Z}/p$-Galois cover $E'^* \to E''$ is totally ramified somewhere. But $E'^* \to E''$ is at most tamely ramified, since $E'^* \to \mathbf{P}^1$ is. This is a contradiction, showing that $G \notin \pi_A^{\mathrm{t}}(U')$, although $G \in \pi_A^{\mathrm{t}}(U)$. $\square$

The above results concerned π_A, the set of finite quotients of the algebraic fundamental group π_1. The profinite group π_1 contains more information than the set π_A, and it would be desirable to have analogs for π_1. But while negative results are known – e.g. that π_1 is not free – there is no reasonable conjecture describing what π_1 is isomorphic to, even in the case of the affine line. And the analog of the last part of Corollary 1.2 is false for π_1; i.e. the fundamental group of a curve of genus g with n points deleted does not just depend on $2g + n$ in characteristic p:

Proposition 1.6. *Let $U = \mathbf{P}^1 - S$, where S is a set of $n + 2$ points ($n \geq 0$), and let $U' = E - S'$, where E is an ordinary elliptic curve and S' is a set of n points. Then $\pi_1(U)$ is not isomorphic to $\pi_1(U')$.*

Proof. Let $f' : E^* \to E$ be an unramified connected $\mathbf{Z}/p$-Galois cover of elliptic curves, which exists since E is ordinary, and let $U'^* = f'^{-1}(U') \subset E^*$. Let $N' \subset \pi_1(U')$ be the normal subgroup of index p corresponding to the unramified Galois cover $U'^* \to U'$. Thus N' may be identified with $\pi_1(U'^*)$. Note that $E^* - U'^* = f'^{-1}(S')$ consists of np points, since there are p points of E^* over each point of E. Since E^* has genus 1, it follows that the prime-to-p part of N' is free on $2 \cdot 1 + np - 1 = np + 1$ generators.

Now suppose that there is an isomorphism $\phi : \pi_1(U) \to \pi_1(U')$. Let $N = \phi^{-1}(N')$. Thus N is a normal subgroup of index p in $\pi_1(U)$, corresponding to a connected unramified $\mathbf{Z}/p$-Galois cover $U^* \to U$. So N may be identified with $\pi_1(U^*)$. Let P^* be the smooth completion of the affine curve U^*. Thus there is a $\mathbf{Z}/p$-Galois branched cover $f : P^* \to \mathbf{P}^1$, whose branch locus in contained in S. Let i be the number of points of S that are actually ramified; each of these i points is then totally ramified, since p is prime. Here $i > 0$, since there are no connected unramified covers of $\mathbf{P}^1$ of degree greater than 1. Now $f^{-1}(S) = P^* - U^*$ consists of exactly $i + (n + 2 - i)p$ points. Also, if g is the genus of P^*, then by the Riemann-

Hurwitz formula in the wild case we get $2g-2 \geq -2p+ip$, i.e. $2g \geq 2+(i-2)p$. So the prime-to p part of N is free on at least $(2+(i-2)p)+(i+(n+2-i)p)-1 = np+i+1$ generators. But since $N = \phi^{-1}(N')$ and ϕ is an isomorphism, and since $i > 0$, this contradicts the fact that the prime-to-p part of N' is free on only $2\cdot 1+np-1 = np+1$ generators. $\square$

Moreover, the analog for π_1 of the first part of 1.2 also fails. That is, for a fixed choice of $g \geq 0$ and a positive integer n, two distinct affine curves of the form (genus g) $-$ (n points) can have non-isomorphic fundamental groups, as the following result shows:

Proposition 1.7. *Let E be an ordinary elliptic curve, let E' be a supersingular elliptic curve, and let $n > 0$. Let U and U' be affine curves obtained by deleting n points from E and E' respectively. Then $\pi_1(U)$ and $\pi_1(U')$ are non-isomorphic.*

Proof. Since E is ordinary there is a connected $\mathbf{Z}/p$-Galois unramified cover $f : E^* \to E$. Let $U^* = f^{-1}(U)$, and let N be the normal subgroup of index p in $\pi_1(U)$ corresponding to f. Thus N may be identified with $\pi_1(U^*)$. Since $U^* = E^* - f^{-1}(S)$ and $f^{-1}(S)$ consists of np points, the prime-to-p part of N is free on $2 \cdot 1 + np - 1 = np + 1$ generators.

Now assume that there is an isomorphism $\phi : \pi_1(U) \to \pi_1(U')$, and let $N' = \phi(N)$. Also, let $U'^* \to U'$ be the $\mathbf{Z}/p$-Galois connected unramified cover corresponding to N'; thus N' may be indentified with $\pi_1(U'^*)$. Let E'^* be the smooth completion of U'^*, and let $f' : E'^* \to E'$ be the corresponding branched cover. Let i be the number of branch points of f'. Thus $i \leq n$, and also $i > 0$ since the supersingular elliptic curve E' has no degree p connected unramified covers. Now $E'^* - U'^* = f'^{-1}(E' - U')$ consists of exactly $i + (n-i)p$ points. And by the Riemann-Hurwitz formula in the wild case, we find that $g = \text{genus}(E'^*)$ satisfies $2g - 2 \geq ip$, i.e. $2g \geq ip + 2$. So the prime-to-p part of N' is free on at least $(ip+2)+(i+(n-i)p)-1 = np+i-1$ generators. Since $i > 0$ and N' is isomorphic to N, this is a contradiction. $\square$

Finally, even two affine open subsets of the same projective curve, with the same number of points deleted, can fail to have isomorphic fundamental groups. In particular, this can occur for the projective line with four points deleted:

Theorem 1.8. *Assume that $p \neq 2$. Let $\lambda, \lambda' \in \mathbf{P}^1 - \{0, 1, \infty\}$ be points which respectively have ordinary and supersingular j-invariants. Let $U = \mathbf{P}^1 - \{0, 1, \infty, \lambda\}$ and $U' = \mathbf{P}^1 - \{0, 1, \infty, \lambda'\}$. Then $\pi_1(U)$ and $\pi_1(U')$ are non-isomorphic.*

Proof. Let $f : P^* \to \mathbf{P}^1$ be the two-fold cover that is totally ramified over the points $0, 1, \infty, \lambda$, let $U^* = P^* - f^{-1}(\{0, 1, \infty, \lambda\})$, and let N be the normal subgroup of index 2 in $\pi_1(U)$ corresponding to the unramified cover $U^* \to U$. Thus P^* is an ordinary elliptic curve, $P^* - U^*$ consists of the four ramification points of f, and N may be identified with $\pi_1(U^*)$. Assume that there is an isomorphism $\phi : \pi_1(U) \to \pi_1(U')$, and let $N' = \phi(N)$. Thus N' is a normal subgroup of index 2 in $\pi_1(U')$, corresponding to a two-fold unramified cover $U'^* \to U'$, and isomorphic to $\pi_1(U'^*)$. Let P'^* be the smooth completion of U'^*, and let $f' : P'^* \to \mathbf{P}^1$ be the corresponding branched cover. Since f' is a two-fold cover of the projective line having at most four branch points, and since $p \neq 2$, the Hurwitz formula implies

that the number of branch points of f' is either 2 or 4. In the former case P'^* has genus 0, and U'^* is isomorphic to $\mathbf{P}^1 - (6 \text{ points})$. And in the latter case, P'^* is a supersingular elliptic curve, and U'^* is isomorphic to $P'^* - (4 \text{ points})$. But ϕ restricts to an isomorphism $\pi_1(U^*) \to \pi_1(U'^*)$. So in the first case this contradicts Proposition 1.6, and in the second case this contradicts Proposition 1.7. □

Remark. The proofs of 1.6-1.8 actually show more. Namely, for any group G, let G' denote the commutator subgroup $[G, G]$. Then under the hypotheses of 1.6 and 1.7, the quotients π_1/π_1'' are non-isomorphic; and under the hypotheses of 1.8, the quotients π_1/π_1''' are non-isomorphic. □

The above theorem suggests the following question:

Question 1.9. For U an affine k-curve, to what extent does the profinite group $\pi_1(U)$ determine U?

A very weak form of Question 1.9, which is nevertheless not known, is this: Consider two affine curves $U_i = X_i - S_i$ $(i = 1, 2)$, where X_i is a smooth projective k-curve of genus g_i and S_i has n_i elements. If $\pi_1(U_1) \cong \pi_1(U_2)$, then must $g_1 = g_2$ and $n_1 = n_2$? In light of Proposition 1.6, the first case to consider is that of $X_1 = \mathbf{P}^1$, $n_1 = 3$, $X_2 =$ a supersingular elliptic curve, $n_2 = 1$; we would then wish to show that the π_1's are not isomorphic.

Alternatively, if we instead fix values for g and n, then the first case to consider is that of $U = \mathbf{P}^1 - S$, where S consists of four points. By the triple transitivity of $\mathrm{Aut}(\mathbf{P}^1)$, we may assume that S is of the form $\{0, 1, \infty, \lambda\}$, and the question is then to what extent $\pi_1(U)$ determines $j(\lambda)$. The following result shows two cases in which different values of j can correspond to isomorphic π_1's:

Proposition 1.10. *Let $\lambda, \lambda' \in \mathbf{P}^1 - \{0, 1, \infty\}$, and let $j, j' \in k$ be the corresponding j-invariants. Also, let $U = \mathbf{P}^1 - \{0, 1, \infty, \lambda\}$ and $U' = \mathbf{P}^1 - \{0, 1, \infty, \lambda'\}$. Then $\pi_1(U) \cong \pi_1(U')$ provided that either:*

(a) *j, j' are algebraic over $\mathbf{F}_p$ and lie in the same orbit under Frobenius; or*
(b) *j, j' are both transendental over $\mathbf{F}_p$.*

Proof. In each case, it suffices to show that there is an $\mathbf{F}_p$-isomorphism $U \to U'$, since this would pull back the tower of covers of U' to the tower of covers of U. Now the k-isomorphism classes of U and U' are determined by j and j', and any field automorphism of k induces an $\mathbf{F}_p$-automorphism of $\mathbf{P}^1$. So it suffices to show that there is a field automorphism of k taking j to j'.

In (a), we have that $j, j' \in \overline{\mathbf{F}}_p$. We are supposing that $F^i(j) = j'$, for some i, where $F : \overline{\mathbf{F}}_p \to \overline{\mathbf{F}}_p$ is the Frobenius automorphism. Since k is algebraically closed, there is an extension of F^i to an automorphism of k, also taking j to j'.

In (b) there is a field isomorphism $\overline{\mathbf{F}}_p(j) \to \overline{\mathbf{F}}_p(j')$ taking j to j'. Again this extends to an automorphism of k, taking j to j'. □

This proposition suggests the following more precise form of Question 1.9:

Question 1.11. (a) Does the converse of 1.10 hold? That is, if U and U' are as in 1.10 and if $\pi_1(U) \cong \pi_1(U')$ holds, must (a) or (b) hold?

(b) If $k = \overline{\mathbf{F}}_p$, then more generally for any two affine k-curves U and U', does $\pi_1(U) \cong \pi_1(U')$ imply that U and U' are $\mathbf{F}_p$-isomorphic?

Next, we turn to the case in which k is taken to be a *finite* field of characteristic p, and we consider fundamental groups of geometrically connected affine curves U over k. That is, we consider $\pi_1(U)$ and $\pi_A(U)$, arising from connected unramified Galois covers of U. Since U is geometrically connected, the $\overline{k}$-scheme $\overline{U} = U \times_k \overline{k}$ is connected, and there is a split exact sequence

$$1 \to \pi_1(\overline{U}) \to \pi_1(U) \to \mathrm{Gal}(\overline{k}/k) \to 1.$$

Since $\mathrm{Gal}(\overline{k}/k)$ is a cyclic profinite group generated by the Frobenius automorphism F, to give a splitting is to give the image of F. And once this lifting of F to $\pi_1(U)$ is given, there is an action of F on $\pi_1(\overline{U})$. This action thus determines the group $\pi_1(U)$ as an extension of $\mathrm{Gal}(\overline{k}/k)$ by $\pi_1(\overline{U})$, and hence it determines $\pi_A(U)$. But this action of Frobenius is not currently understood. The previous discussion in the algebraically closed case, however, suggests the following

Question 1.12. Let U, U' be geometrically connected affine k-curves. Let $\phi : \pi_1(U) \to \mathrm{Gal}(\overline{k}/k)$ and $\phi' : \pi_1(U') \to \mathrm{Gal}(\overline{k}/k)$ be as in the exact sequence above. If there is an isomorphism $\alpha : \pi_1(U) \to \pi_1(U')$ such that $\alpha \circ \phi' = \phi$, must $U \cong U'$ as k-schemes?

The analog of this for affine open subsets of the projective line over a *number field* was proven by Nakamura, in [Na].

Another issue in this situation is that connected covers of U need not be geometrically connected. Indeed, a Galois cover $U^* \to U$ will be geometrically connected if and only if it is *regular*; i.e. if and only if k is algebraically closed in the function field of U^*. Thus there is a subset $\pi_A^{\mathrm{reg}}(U) \subset \pi_A(U)$ corresponding to Galois groups of regular covers. We would like to understand $\pi_A^{\mathrm{reg}}(U)$.

If U is a geometrically connected affine k-curve and $U^* \to U$ is a G-Galois unramified cover, then we may extend constants to the algebraic closure $\overline{k}$ of k, and obtain a G-Galois cover $\overline{U}^* \to \overline{U}$ of connected k-curves. Thus $\pi_A^{\mathrm{reg}}(U) \subset \pi_A(\overline{U})$, and the latter set is understood by the algebraically closed case. Now given a connected G-Galois cover $\overline{U}^* \to \overline{U}$, Frobenius acts on the cover, in the sense of inducing a G-Galois cover $\overline{U}^{*F} \to \overline{U}$ by letting F act on the coefficients of the equations defining $\overline{U}^*$ as a cover and also on the Galois automorphisms. By [De], the G-Galois cover $\overline{U}^* \to \overline{U}$ is induced by a G-Galois cover $U^* \to U$ if and only if $\overline{U}^{*F} \to \overline{U}$ is isomorphic, as a G-Galois cover, to $\overline{U}^* \to \overline{U}$. (The corresponding fact is false in the case of covers over number fields, because the field of moduli of a G-Galois cover need not in general be a field of definition; cf. [CH, Example 2.6].) And so a finite group G lies in $\pi_A^{\mathrm{reg}}(U)$ if and only if some G-Galois cover $\overline{U}^* \to \overline{U}$ satisfies the above property. But again, the difficulty in using this criterion to find $\pi_A^{\mathrm{reg}}(U)$ explicitly is that the action of Frobenius on $\pi_1(\overline{U})$ is not understood.

Recently, Abhyankar has obtained many quasi-p groups as Galois groups of explicit unramified covers of the affine line over $\mathbf{F}_p$. Motivated by this, he has asked the following

Question 1.13. If p is a prime and G is a finite quasi-p group, must G lie in $\pi_A(\mathbf{A}^1_{\mathbf{F}_p})$?

But the patching methods used in [Ra] and [Ha3] to prove Abhyankar's conjecture over algebraically closed fields do not seem applicable to this situation, due to difficulties involved with specialization.

Section 2. Arithmetic Galois groups

This section considers the problem of finding π_1 and π_A in the unequal characteristic case – specifically, for a "curve" of the form $U_n = \mathrm{Spec}(\mathbf{Z}[\frac{1}{n}])$, where n is a square-free positive integer. It was suggested by I.R. Shafarevich [Sh, sect. 3] that $\pi_1(U_n)$ is topologically finitely generated for each n, and R. Coleman has asked how π_A and π_1 grow with n. Presumably every finite group lies in $\pi_A(U_n)$ for some sufficiently large n.

By the analogy between number fields and function fields, we might expect $\pi_A(U_n)$ to behave similarly to $\pi_A(U)$, where U is an open subset of the affine line over $\mathbf{F}_p$. In that situation, a square-free polynomial f of degree d has norm p^d and defines a set of d geometric points. For such an f, if $U \subset \mathbf{A}^1_{\mathbf{F}_p}$ is the set where $f \neq 0$, then the tame part of $\pi_A^{\mathrm{reg}}(U)$ is contained in $\pi_A^{\mathrm{t}}(\overline{U})$, whose elements are each generated by d elements. In the arithmetic situation, $U_n \subset \mathrm{Spec}(\mathbf{Z})$ is the non-vanishing set of a square-free positive integer n, of norm n. So we make the following conjecture:

Conjecture 2.1. *There is a constant C such that for every positive square-free integer n, every group in $\pi_A^{\mathrm{t}}(U_n)$ has a generating set with at most $\log n + C$ elements.*

That is, if K is a Galois extension of $\mathbf{Q}$ having Galois group G and only tame ramification, and if n is the product of the distinct primes dividing the discriminant, then the number of generators of G is conjectured to be at most $\log n + \mathcal{O}(1)$. More groups would thus be allowed as n increases. This conjecture is consistent with the expectation, suggested at this conference by B. Birch, that every finite group is the Galois group of a tamely ramified extension of $\mathbf{Q}$.

In this section we particularly consider the case where $n = p$ is prime. If G is the Galois group of an extension K of $\mathbf{Q}$ ramified only over p, and if $N \subset G$ is the (normal) subgroup generated by the Sylow p-subgroups of the inertia groups, then N is a quasi-p group, and $L = K^N$ is a tamely ramified Galois extension of $\mathbf{Q}$ with group G/N ramified only over p. Since $N \subset p(G)$ (where, as in section 1, $p(G)$ denotes the quasi-p part of G), we obtain

Proposition 2.2. *If Conjecture 2.1 holds, and if $G \in \pi_A(U_p)$ for some prime number p, then $G/p(G)$ is generated by at most $\log p + C$ elements (where C is as in 2.1).*

We begin with two examples of Galois extensions K of $\mathbf{Q}$ that are ramified only at a single prime:

Examples 2.3. (a) If a prime number p is chosen so that the class number $h(\mathbf{Q}(\zeta_p)) > 1$ then the Hilbert class field K of $\mathbf{Q}(\zeta_p)$ is ramified only at p. For example we may take p to be 23, with class number 3, showing that the non-trivial semi-direct product $\mathbf{Z}/3 \rtimes (\mathbf{Z}/23)^*$ is in $\pi_A(U_{23})$.

(b) (following ideas of Ken Ribet in his talk at this conference) Let N be a prime such that the genus of $J = J_0(N)$ is at least 1, and take p to be a prime not dividing the numerator of $\frac{N-1}{12}$. The action of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the torsion points of J yields a representation $\rho : G_{\mathbf{Q}} \to GL(2,k)$ for some finite field k of characteristic p, and the image A of ρ is $\{g \in GL(2,k) \mid \det(g) \in \mathbf{F}_p^*\}$. So A is a quotient of $G_{\mathbf{Q}}$, and taking $p = N$ we get a corresponding Galois extension of $\mathbf{Q}$ with Galois group A. This extension is unramified away from p, since ρ is (because J has good reduction outside p). □

Note that in these examples the prime p must be sufficiently large, and this may reflect the fact that according to 2.1 and 2.2 there should be "more" extensions ramified only over a fixed large prime than there are ramified only over a fixed small prime.

For any group G, let G' be the commutator subgroup of G; let $G^{\mathrm{ab}} = G/G'$ be the abelianization of G; and let G^{solv} be the maximal solvable quotient of G.

By class field theory, the abelianized fundamental group of U_n is given by $\pi_1(U_n)^{\mathrm{ab}} \cong \prod_{p|n} \mathbf{Z}_p^* \cong \prod_{p|n}[(\mathbf{Z}/p)^* \times \mathbf{Z}_p]$. Similarly, the abelianized tame fundamental group is given by $\pi_1^{\mathrm{t}}(U_n)^{\mathrm{ab}} = \prod_{p|n}(\mathbf{Z}/p)^*$, and hence the number of generators of this group is equal to the number of distinct odd primes dividing n.

Remark. In the geometric situation, Theorem 1.8 produced two affine curves of the form $\mathbf{P}^1 - (4 \text{ points})$ whose π_1's were non-isomorphic, even modulo π_1''' (cf. the remark after that result). In the arithmetic situation, much more is true: by the comments above, a square-free positive integer n is determined by $\pi_1(U_n)^{\mathrm{ab}} = \pi_1(U_n)/\pi_1(U_n)'$. But this is less surprising, since no two n's can have the same norm, and so intuitively different U_n's have different numbers of "missing points."

A key difference between the arithmetic and geometric cases concerns the relationship between the discriminant Δ and the index of ramification e. In the geometric case, fixing the degree N and bounding the values of e does not bound $|\Delta|$, when there is wild ramification. Thus, in characteristic p, there are branched covers of $\mathbf{P}^1_k$ of degree p, unramified except at a single point, having arbitrarily large discriminant and hence arbitrarily large genus (e.g. the covers $y^p - y = x^{-n}$, with n prime to p). But in the arithmetic case, for a given degree N, knowing the values of e bounds the discriminant. By combining this upper bound on $|\Delta|$ with a lower bound (e.g. Odlyzko's bounds), it is often possible to show that G is not in $\pi_A(U_n)$.

Specifically, if $K \subset L$ is a totally ramified extension of p-adic fields having ramification index e, and if $\mathbf{p}$ is the prime of $\mathcal{O}_K$ over p, then

$$v_{\mathbf{p}}(\Delta_{L/K}) \leq e - 1 + e v_{\mathbf{p}}(e).$$

(This can be seen by writing $\mathcal{O}_L = \mathcal{O}_K[x]/(f(x))$ and then evaluating $v_{\mathbf{q}}(f'(\pi_L))$, where $\mathbf{q}$ is the prime of $\mathcal{O}_L$ over p and π_L is the uniformizer of $\mathcal{O}_L$. See [Se1, p. 568,

Proposition 3].) So for a global finite extension $\mathbf{Q} \subset L$, with ramification indices e_i and residue degrees f_i over p, we have

$$(*) \qquad v_p(\Delta_{L/\mathbf{Q}}) \leq \sum_i f_i\big(e_i - 1 + e_i v_p(e_i)\big).$$

In particular, if L is ramified only over a single prime p and $[L : \mathbf{Q}] = n$, then $|\Delta_{L/\mathbf{Q}}|^{\frac{1}{n}} \leq p^{1+\frac{1}{n}\sum(e_i f_i v_p(e_i) - f_i)}$; so if L is Galois over $\mathbf{Q}$ with ramification indices equal to e then

$$(**) \qquad |\Delta_{L/\mathbf{Q}}|^{\frac{1}{n}} \leq p^{1+v_p(e)-\frac{1}{e}}.$$

(Compare [Se1, p. 570, Proposition 6].)

Using this, we obtain evidence for Conjecture 2.1 (Theorem 2.6 below). First we need two lemmas:

Lemma 2.4. *Let p be prime.*

(a) If the class number $h_p = h(\mathbf{Q}(\zeta_p))$ is equal to 1, then $\pi_1^{\mathrm{t}}(U_p)^{\mathrm{solv}}$ is cyclic of order $p-1$.

(b) If $h_p > 1$, then $\pi_1^{\mathrm{t}}(U_p)^{\mathrm{solv}}$ is not cyclic.

Proof. (a) Let $G \in \pi_A^{\mathrm{t}}(U_p)^{\mathrm{solv}}$ and let K be a G-Galois extension of $\mathbf{Q}$ that is unramified except at p, where it is tamely ramified. We wish to show that $K \subset \mathbf{Q}(\zeta_p)$. The fixed field $K^{G'}$ under the commutator subgroup G' is an abelian extension of $\mathbf{Q}$ ramified only at p, where it is tamely ramified; so $K^{G'} \subset \mathbf{Q}(\zeta_p)$.

Now any non-trivial unramified abelian extension L of $K^{G'}$ is linearly disjoint from $\mathbf{Q}(\zeta_p)$ over $K^{G'}$, since the latter extension is totally ramified. Thus $L(\zeta_p)$ is a non-trivial abelian unramified extension of $\mathbf{Q}(\zeta_p)$; a contradiction, showing that $h(K^{G'}) = 1$. So the abelian extension $K^{G'} \subset K^{G''}$ has no unramified subextensions, and hence is totally ramified. Thus the G/G''-Galois extension $\mathbf{Q} \subset K^{G''}$ is totally, and tamely, ramified over p. So its inertia group, viz. G/G'', is cyclic, and in particular abelian. Thus G'' contains G', and hence $G'' = G'$. But G' is solvable; so G' is trivial and $K = K^{G'} \subset \mathbf{Q}(\zeta_p)$.

(b) Let K be the Hilbert class field of $\mathbf{Q}(\zeta_p)$. Thus K is Galois over $\mathbf{Q}$; let G be the Galois group. If G is cyclic, then $\mathbf{Q} \subset K$ is an abelian extension ramified only at p, where it is tamely ramified. Thus $K \subset \mathbf{Q}(\zeta_p)$, and hence $K = \mathbf{Q}(\zeta_p)$. This contradicts the assumption that $h_p = 1$, showing that G is non-cyclic. Hence the group $\pi_1^{\mathrm{t}}(U_p)^{\mathrm{solv}}$ is also non-cyclic. □

Lemma 2.5. *Let G be a non-solvable group of order ≤ 500, such that every proper quotient of G is abelian. Let $g \in G$ and let e be the order of g. Then one of the following holds:*

(i) $G \cong A_5$, $e \leq 5$;
(ii) $G \cong S_5$, $e \leq 6$;
(iii) $G \cong \mathrm{PSL}(2,7)$, $e \leq 7$;
(iv) $1 \to \mathrm{PSL}(2,7) \to G \to \mathbf{Z}/2 \to 1$ *is exact*, $e \leq 14$;
(v) $G \cong A_6$, $e \leq 5$.

Proof. Let N be a minimal non-trivial normal subgroup of G. Thus N is of the form H^ν, for some simple group H and some integer $\nu \geq 1$. Let $\overline{G} = G/N$. So $\overline{G}$ is abelian. Since G is not solvable and $\overline{G}$ is solvable, it follows that N and hence H is non-abelian. Thus $|H| \geq 60$. Since $|G| \leq 500$, we have that $\nu = 1$ and so $N = H$.

Since $n \leq 500$, we have that $|H| \leq 500$, and therefore H is isomorphic either to the alternating group A_5 of order 60; to the simple group $\mathrm{SL}(3,2) \cong \mathrm{PSL}(2,7)$ of order 168; or to the alternating group A_6 of order 360. The maximal order of an element in A_5 and A_6 is 5 (corresponding to a five-cycle), and in $\mathrm{PSL}(2,7)$ it is 7 (corresponding to the upper triangular matrix with entries on and above the diagonal equal to 1). Since $|G| \leq 500$, we have that $|\overline{G}| = 1$ if $H \cong A_6$, and $|\overline{G}| \leq 2$ if $H \cong \mathrm{PSL}(2,7)$. If $G \cong S_5$ then the maximal order of an element is 6 (the product of a two-cycle and a three-cycle). And if $H \cong \mathrm{PSL}(2,7)$ and $\overline{G} \cong \mathbf{Z}/2$, then any $g \in G$ satisfies $g^2 \in H$ and so $g^{14} = 1$. So it remains to show that if $H \cong A_5$ and $\overline{G}$ is non-trivial, then $G \cong S_5$.

So take $H = A_5$ and assume $\overline{G} = G/H$ is non-trivial, and let $\rho : \overline{G} \to \mathrm{Out}(A_5) \cong \mathbf{Z}/2$ be the homomorphism induced by the given extension. We claim that ρ is an isomorphism. If not, then since $\overline{G}$ is non-trivial, we have that $\ker(\rho)$ is non-trivial. Let $\overline{g} \neq 1$ be in $\ker(\rho)$, and let $g \in G$ lie over $\overline{g}$. Also, let $\overline{E} \subset \overline{G}$ be the subgroup generated by $\overline{g}$, and let $E \subset G$ be the inverse image of $\overline{E}$. Thus $g \in E$, and E is generated by g and H. Since $\overline{G}$ is abelian, $\overline{E}$ is normal in $\overline{G}$, and hence E is normal in G. By the choice of $\overline{g}$, conjugation of H by g is an inner automorphism of H, say by $h \in H$. Thus $gh^{-1} \in G$ acts trivially on H by conjugation, i.e. gh^{-1} commutes with the elements of H, and in particular with h. Thus g commutes with h, and so gh^{-1} commutes with g. Since E is generated by g and H, we have that gh^{-1} lies in the center Z of E. But $gh^{-1} \neq 1$ (because its image in $\overline{G}$ is $\overline{g} \neq 1$), and so $Z \neq 1$. Since Z is a characteristic subgroup of N, and since N is normal in G, it follows that Z is a non-trivial normal subgroup of G. But Z is abelian, and so G/Z is (like G) non-solvable and hence non-abelian. This contradicts the hypothesis on G, proving the claim that ρ is an isomorphism.

Thus $\rho : \overline{G} \to \mathrm{Out}(A_5) \cong \mathbf{Z}/2$ is an isomorphism. Let $\overline{g}$ be the involution in $\overline{G}$ and let $g \in G$ lie over $\overline{g}$. Thus the conjugation action of g on $H = A_5$ is not an inner automorphism. But $\mathrm{Aut}(A_5) = S_5$, and so this conjugation action agrees with conjugation on A_5 by some odd permutation τ in S_5. Here $\tau = \sigma h$, where $\sigma \in S_5$ is a transposition and $h \in H = A_5$. Replacing the lift g of $\overline{g}$ by gh^{-1}, we are reduced to the case that g has order 2 and it acts on A_5 the same way as the transposition σ. So there is an isomorphism $G \to S_5$ which is the identity on A_5 and takes g to σ. $\square$

Theorem 2.6. *(a) If $p < 23$ is prime, then $\pi_1^{\mathrm{t}}(U_p)$ is cyclic of order $p-1$.*
(b) The group $\pi_1^{\mathrm{t}}(U_{23})$ is not cyclic.

Proof. (a) Since $p \leq 19$, the class number $h(\mathbf{Q}(\zeta_p)) = 1$. So if 2.6 fails, then 2.4(a) implies that there is a non-solvable finite quotient of $\pi_1^{\mathrm{t}}(U_p)$. Let G be such a quotient of smallest possible order n, and let K be a corresponding G-Galois extension of $\mathbf{Q}$ ramified only over p, where it is tamely ramified of index e. For any non-trivial normal subgroup of $N \subset G$, the minimality of G implies that G/N

is solvable. So by 2.4(a), G/N is cyclic of order r dividing $p-1$. This shows that every proper quotient of G is abelian.

In particular, let $N_0 \subset G$ be minimal among the non-trivial normal subgroups of G. The minimality of N_0 implies that N_0 is of the form H^ν, for some simple group H and some integer $\nu \geq 1$. Here H is non-abelian since G is not solvable. Write $\Delta = \Delta_{K/\mathbf{Q}}$.

We claim that $n = |G| < 500$. Namely, since K is tamely ramified over p with ramification index $e < n$, and unramified elsewhere, by the inequality (**) above we have that $|\Delta|^{\frac{1}{n}} < 19^{1-\frac{1}{n}}$. But by [Od, p. 380, 1.11], $|\Delta|^{\frac{1}{n}} \geq 21.8 \cdot e^{-70/n}$. So $21.8 \cdot e^{-70/n} < 19^{1-\frac{1}{n}}$, and so

$$n < \frac{70 - \log(19)}{\log(21.8/19)} < 500.$$

Since the ramification is tame, the ramification index e is equal to the order of some element in G. Since $n = |G| < 500$, and since every proper quotient of G is abelian, by Lemma 2.5 we are in one of the following five cases:

(i) $n = 60$, $e \leq 5$;
(ii) $n = 120$, $e \leq 10$;
(iii) $n = 168$, $e \leq 7$;
(iv) $n = 2 \cdot 168 = 336$, $e \leq 14$;
(v) $n = 360$, $e \leq 5$.

In each case, inequality (**) shows that $|\Delta|^{\frac{1}{n}} \leq 19^{1-\frac{1}{e}}$, and [Od, Table 1, pp. 400-401] provides a lower bound for $|\Delta|^{\frac{1}{n}}$. These upper and lower bounds (rounding up, in the case of the upper bounds) are respectively 10.55 and 12.23; 14.16 and 14.38; 12.48 and 15.12; 15.40 and 17.51; 10.55 and 17.94. In each case this is a contradiction.

(b) Since the class number of $\mathbf{Q}(\zeta_{23})$ is 3, by 2.4(b) we have that $\pi_1^{\mathrm{t}}(U_{23})^{\mathrm{solv}}$ is not cyclic. Hence $\pi_1^{\mathrm{t}}(U_{23})$ is also not cyclic. □

As in section 1, for any finite group G and any prime p, we denote by $p(G)$ the subgroup of G generated by the p-subgroups of G, and we say that G is a *quasi-p group* if $p(G) = G$.

Corollary 2.7. *If $p < 23$ is prime, and G is in $\pi_A(U_p)$, then $G/p(G)$ is cyclic of order dividing $p-1$.*

Proof. Let K be a G-Galois extension of $\mathbf{Q}$ ramified only at p. Then the subfield $K^{p(G)}$ is a $G/p(G)$-Galois extension of $\mathbf{Q}$ ramified only at p, and it is tamely ramified over p since $|G/p(G)|$ is prime to p. So we are done by 2.6(a). □

In particular, every group in $\pi_A(U_2)$ is a quasi-2 group.

Remark. J.-P. Serre has observed to the author that $\pi_1(U_{11})$ is not solvable. In particular, it has a quotient isomorphic to $\mathrm{GL}(2,11)$, provided by the 11-division points of the elliptic curve of conductor 11 (or equivalently, by the Ramanujan function representation modulo 11). Moreover, the same argument using the Ramanujan function shows that $\pi_1(U_p)$ is not solvable for larger primes p (using modular forms other than delta for $p = 23$ and $p = 691$).

Proposition 2.8. *Let p and q be (possibly equal) prime numbers, let G be a p-group, and let $\mathbf{Q} \subset K$ be a G-Galois extension ramified only at q.*

(a) *The extension $\mathbf{Q} \subset K$ is totally ramified over q.*
(b) *The class number of K is prime to p.*

Proof. (a) If not, let I be an inertia group over q. Then I is a proper subgroup of G. But any proper subgroup of a p-group is contained in a proper normal subgroup. So I lies in a proper normal subgroup $N \subset G$. Thus the fixed field K^N is unramifed over $\mathbf{Q}$ with group $G/N \neq 1$, and this is impossible.

(b) Let C be the class group of K, let $C' = C/N$ be the maximal quotient of C of p-power order, let L be the Hilbert class field of K, and let $L' = L^N$. Then the extension $\mathbf{Q} \subset L'$ is a Galois extension of p-power order, and thus by (a) it is totally ramified over q. Hence so is $K \subset L'$. But $K \subset L'$ is a subextension of $K \subset L$, and so is unramified. Hence the extension $K \subset L'$ is trivial, and so its Galois group C' is also trivial. Thus $N = C$. So the class number of K, which is equal to $|C|$, is prime to p. □

Proposition 2.9. *Under the hypotheses of 2.8, suppose additionally that every proper subfield K' of K that is Galois over $\mathbf{Q}$ has class number 1. Assume that the class group C of K is non-trivial.*

(a) There is an injective group homomorphism $\rho : G \to \mathrm{Aut}(C)$, arising from the action of G on $C = \mathrm{Gal}(L/K)$, where L is the Hilbert class field of K.

(b) If G is non-abelian, then C is not cyclic.

Proof. (a) Let $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$. Thus we have the exact sequence $1 \to C \to \Gamma \to G \to 1$, and by 2.8(b) the kernel and cokernel have relatively prime order. Thus this sequence splits and we may regard $G \subset \Gamma$. Let $\rho : G \to \mathrm{Aut}(C)$ correspond to the induced conjugation action of G on C, and let $N = \ker(\rho) \subset G \subset \Gamma$. We wish to show that N is trivial.

So assume not. Then N is a non-trivial normal subgroup of G, and the elements of N commute with all the elements of C. So N is normal in Γ. Let $G' = G/N$, $\Gamma' = \Gamma/N$, $K' = K^N$ and $L' = L^N$. Then the extension $\mathbf{Q} \subset K'$ is G'-Galois, and $\mathbf{Q} \subset L'$ is Γ'-Galois. Hence the extension $K' \subset L'$ is C-Galois. Since $N \neq 1$, the field K' is strictly contained in K; so by hypothesis, the class number of K' is 1. Thus the abelian extension $K' \subset L'$ is totally ramified. Also, $K' \subset K$ is totally ramified over q since $\mathbf{Q} \subset K$ is, by 2.8(a). Now the degree of the Galois extension $K' \subset K$ is a power of p, whereas $[L' : K'] = |C|$ is prime to p by 2.8(b). So the fields K and L' are linearly disjoint over K', and thus the compositum $KL' = L$ is totally ramified over K. But L is unramified over K. So $L = K$ and C is trivial, a contradiction.

(b) If C is cyclic, then $\mathrm{Aut}(C)$ is abelian. Since G is non-abelian, this contradicts the conclusion of (a). □

Corollary 2.10. *Under the hypotheses of 2.9, if $p = 2$ and G is non-abelian, then the class number of K is at least 9.*

Proof. Let C be the class group of K. Then $|C|$ is odd by 2.8(b), and C is non-cyclic by 2.9(b). Thus the abelian group C is a product of at least two cyclic groups, each of order at least 3. So $|C| \geq 9$. □

If p is an odd prime, and $\mathbf{Q} \subset K$ is a G-Galois extension ramified only at p, with G an abelian p-group, then $G = \mathbf{Z}/p^{n-1}$ for some n. For the prime 2, the corresponding assertion holds provided one restricts attention to totally real fields. In fact, these assertions remain true even without assuming that G is abelian. Namely, if we write $\pi_1^{\mathrm{tr}}(U_2)$ for the quotient of $\pi_1(U_2)$ corresponding to totally real extensions, and write $\pi_1^p(U_p)$ [resp. $(\pi_1^{\mathrm{tr}})^p(U_2)$] for the maximal p-quotient of $\pi_1(U_p)$ [resp. of $\pi_1^{\mathrm{tr}}(U_2)$], we have the following easy result:

Theorem 2.11. *(a) If p is an odd prime, then $\pi_1^p(U_p) \cong \mathbf{Z}_p$. Equivalently, a finite p-group G is in $\pi_A(U_p)$ if and only if G is cyclic.*

(b) $(\pi_1^{\mathrm{tr}})^2(U_2) \cong \mathbf{Z}_2$. Equivalently, a finite 2-group G is in $\pi_A^{\mathrm{tr}}(U_2)$ if and only if G is cyclic.

Proof. Let $\Pi = \pi_A(U_p)$ if p is odd, and let $\Pi = \pi_A^{\mathrm{tr}}(U_2)$ if $p = 2$. It suffices to show that if $G \in \Pi$ then G is cyclic. Now for $G \in \Pi$, the abelianization G^{ab} is also in Π. So by the comment before the theorem, G^{ab} is cyclic of p-power order. But $G^{\mathrm{ab}} = G/G'$, where G' is the commutator, and G' is contained in the Frattini subgroup F of G. So G/F is cyclic. By the Burnside Basis Theorem, so is G. □

From now on we restrict attention to the case of U_2, and study the set $\pi_A(U_2)$. While 2.11(b) does not determine precisely which 2-groups are in $\pi_A(U_2)$, it does provide a necessary condition for a 2-group to lie in $\pi_A(U_2)$:

Proposition 2.12. *Let G be a non-trivial 2-group in $\pi_A(U_2)$.*

(a) Then G contains an involution i such that the normal subgroup $N \subset G$ generated by i has the property that G/N is cyclic.

(b) The normal subgroup H of G generated by the involutions of G has the property that G/H is cyclic.

Proof. Part (b) is immediate from (a). For (a), assume that $G \in \pi_A(U_2)$, and let $\mathbf{Q} \subset K$ be a corresponding G-Galois extension ramified only over 2. Let $g \in G$ be the image of complex conjugation, under $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q}) = G$. If g is trivial, then K is a real Galois extension of $\mathbf{Q}$, and hence is totally real; so G is cyclic by Proposition 2.11(b), and we may choose i to be the unique involution in G. So now assume that g is non-trivial, take $i = g$, and let N be the normal subgroup generated by i (i.e. the subgroup of G generated by i and its conjugates). Thus K^N is totally real, and so is cyclic over $\mathbf{Q}$ with group G/N. □

Question 2.13. Is condition (a) of Proposition 2.12 necessary and sufficient for a finite 2-group G to lie in $\pi_A(U_2)$?

Using 2.12, various 2-groups can be shown not to lie in $\pi_A(U_2)$. For example, the quaternion group Q of order 8 is not in $\pi_A(U_2)$, since the only involution is -1, and so it does not satisfy (b) of Proposition 2.12. On the other hand, we have:

Example 2.14. The dihedral group $D_4 = \langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle$ is in $\pi_A(U_2)$. Namely, writing $u = 1 - \sqrt{2}$ for the fundamental unit in $\mathbf{Q}(\zeta_8)$, we have that $D_4 = \mathrm{Gal}(K_\nu/\mathbf{Q})$, $\nu = 1, 2$, where $K_1 = \mathbf{Q}\big(\zeta_8, \sqrt{u}\big)$ and $K_2 = \mathbf{Q}\big(\zeta_8, \sqrt{\zeta_8 u}\big) = \mathbf{Q}\big(\zeta_8, \sqrt[4]{2}\big)$. The discriminants of these fields satisfy $|\Delta|^{1/8} \leq 8$. Moreover these

are the only two D_4-Galois extensions of $\mathbf{Q}$ ramified only at 2, and each has class number 1.

To see this, one notes that any D_4-Galois extension of $\mathbf{Q}$ ramified only at 2 must be a degree 2 Kummer extension of $\mathbf{Q}(\zeta_8)$, ramified only at the prime over 2. Hence such an extension is of the form $\mathbf{Q}(\zeta_8, \sqrt{\alpha})$, where $\alpha = \zeta_8^i u^j \pi^k$, where $\pi = 1 - \zeta_8$ generates the prime of $\mathbf{Q}(\zeta_8)$ over 2, and where i, j, k each equal 0 or 1. Examining the possibilities and ruling out the non-Galois extensions and the abelian extensions of $\mathbf{Q}$, one obtains precisely the above two fields, each of which has Galois group D_4.

To see that the class number h_ν of K_ν is 1, note that otherwise Corollary 2.10 implies that $h_\nu \geq 9$. So K_ν has an unramified abelian extension L of degree ≥ 9, which is Galois over $\mathbf{Q}$. Now since K_ν is obtained by adjoining the square root of a unit to $\mathbf{Q}(\zeta_8)$, we have that the discriminant $\Delta_{K_\nu} = \Delta_{K_\nu/\mathbf{Q}}$ satisfies $|\Delta|^{1/8} \leq 8$. Hence the discriminant Δ_L of L over $\mathbf{Q}$ satisfies $|\Delta_L|^{1/[L:\mathbf{Q}]} \leq 8$. But $[L : \mathbf{Q}] \geq 8 \cdot 9 = 72$, and for extensions of degree $N \geq 72$, Odlyzko's lower bound on $|\Delta|^{1/N}$ [Od, p. 401, Table 1] is 12.84. This is a contradiction. □

By the above, we obtain

Proposition 2.15. *The 2-groups of order ≤ 8 in $\pi_A(U_2)$ are precisely the groups 1, $\mathbf{Z}/2$, $\mathbf{Z}/2 \times \mathbf{Z}/2$, $\mathbf{Z}/4$, $\mathbf{Z}/8$, $\mathbf{Z}/4 \times \mathbf{Z}/2$, and the dihedral group D_4. Moreover, all of the corresponding field extensions of $\mathbf{Q}$ have class number 1.*

Proof. By Example 2.14, the dihedral group D_4 is in $\pi_A(U_2)$, and the two corresponding field extensions K_1 and K_2 each have class number 1. Also, as noted after Proposition 2.12, the quaternion group Q does not occur in $\pi_A(U_2)$. Since the abelian groups in $\pi_A(U_2)$ are precisely the groups of the form $\mathbf{Z}/2^n$ or $\mathbf{Z}/2^n \times \mathbf{Z}/2$ for $n \geq 0$, corresponding the the quotients of $\mathrm{Gal}\big(\mathbf{Q}(\zeta_{2^{n+1}})/\mathbf{Q}\big)$, the abelian groups that occur are those listed. Each of the corresponding fields is thus a subfield of $\mathbf{Q}(\zeta_{32})$, which has class number 1. If a subfield $K \subset \mathbf{Q}(\zeta_{32})$ has a class number bigger than 1, then by 2.8(b) there is a non-trivial unramified Galois extension $K \subset L$ having odd degree. Thus L and $\mathbf{Q}(\zeta_{32})$ are linearly disjoint over K, and so the compositum $L(\zeta_{32})$ is a non-trivial unramified extension of $\mathbf{Q}(\zeta_{32})$. This is a contradiction. □

In degree 16, a more delicate use of Odlyzko's bounds is required, as in the following example (which is needed in Theorem 2.25 below):

Example 2.16. There are precisely two groups of order 16 lying in $\pi_A(U_2)$ that have D_4 as a quotient, viz. D_8 and the group $E = \langle s, t \mid s^8 = 1, t^2 = 1, tst^{-1} = s^3 \rangle$. Moreover each of these groups corresponds to exactly two non-isomorphic extensions of $\mathbf{Q}$ ramified only at 2, one of which dominates K_1 and the other of which dominates K_2 (where the fields K_ν are as in Example 2.14). These four fields L satisfy $|\Delta_L|^{1/16} \leq 16$, and they have class number 1.

To see this, we begin as in Example 2.14. Namely, any such field L is a degree 4 Kummer extension of $\mathbf{Q}(\zeta_8)$, ramified only at the prime over 2. Hence it is of the form $\mathbf{Q}(\zeta_8, \sqrt[4]{\alpha})$, with $\alpha = \zeta_8^i u^j \pi^k$, where $u = 1 - \sqrt{2}$, $\pi = 1 - \zeta_8$ and $0 \leq i, j, k \leq 3$. Ruling out the non-Galois extensions, one is left with the

fields $L_1 = \mathbf{Q}\big(\zeta_8, \sqrt[4]{u}\big) = K_1(\sqrt{u_1})$, where $u_1 = \sqrt{u} \in K_1$, and having Galois group E over $\mathbf{Q}$; $L_2 = \mathbf{Q}\big(\zeta_8, \sqrt[4]{iu}\big) = K_1(\sqrt{\zeta_8 u_1})$, with group D_8 over $\mathbf{Q}$; $L_3 = \mathbf{Q}\big(\zeta_8, \sqrt[4]{\zeta_8 u\pi^2}\big) = \mathbf{Q}(\zeta_8, \sqrt[8]{2})$ containing K_2, with group E over $\mathbf{Q}$; and $L_4 = \mathbf{Q}\big(\zeta_8, \sqrt[4]{\zeta_8^{-1} u\pi^2}\big)$ containing K_2, with group D_8 over $\mathbf{Q}$.

Now L_1 and L_2 are each obtained from K_1 by adjoining the square root of a unit. Also, letting $v = \pi/\omega^2 \in K_2$, where $\omega = 1 - \sqrt{\zeta_8 u} \in K_2$ generates the prime of K_2 over 2, we have that v is a unit. Writing $u_2 = \sqrt{\zeta_8 u} \in K_2$, we have that $L_3 = K_2(\sqrt{u_2 v})$ and $L_4 = K_2(\sqrt{\zeta_8^{-1} u_2 v})$, each of which is obtained from K_2 by adjoining the square root of a unit. So for $1 \leq \nu \leq 4$, the discriminant Δ_{L_ν} over $\mathbf{Q}$ satisfies $|\Delta_{L_\nu}|^{1/16} \leq 16$, and any unramified extension H of L_ν with $n = [H : \mathbf{Q}]$ satisfies $|\Delta_H|^{1/n} \leq 16$.

Now if the class number $h(L_\nu)$ is greater than 1, then the class group C of L_ν is non-cyclic, by Proposition 2.9 (using Proposition 2.15 to verify the hypotheses of 2.9) and odd (by 2.8). So either $C \cong (\mathbf{Z}/3)^2$ or else $|C| \geq 25$. In the latter case, L_ν has an abelian unramified extension that is Galois over $\mathbf{Q}$ with degree at least $16 \cdot 25 = 400$. But Odlyzko's lower bound for extensions $\mathbf{Q} \subset H$ of degree $n \geq 240$ [Od, Table 1, p.401] is $|\Delta_H|^{1/n} \geq 16.28$. This is a contradiction. Thus $C \cong (\mathbf{Z}/3)^2$.

Let H be the Hilbert class field of L_ν. Thus H is Galois over $\mathbf{Q}$, say with group Γ. Writing $G = \mathrm{Gal}(K_\nu/\mathbf{Q})$, there is an exact sequence $1 \to C \to \Gamma \to G \to 1$, which splits since C is odd and G is a 2-group. By 2.9(a), the induced map $\rho : G \to \mathrm{Aut}(C)$ is injective. But $\mathrm{Aut}(C) \cong \mathrm{GL}(2,3)$, and the highest power of 2 dividing $|\mathrm{GL}(2,3)|$ is 16, so ρ must be an isomorphism from G to a Sylow 2-subgroup of $\mathrm{GL}(2,3)$. Now there is an injection $\rho : E \to \mathrm{GL}(2,3)$, given by

$$s \mapsto \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},\ t \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

and this is an isomorphism onto a Sylow 2-subgroup S of $\mathrm{GL}(2,3)$. So there is no embedding of D_8 into $\mathrm{GL}(2,3)$, and thus L_2 and L_4 have class number 1.

It remains to show that L_ν has class number 1 for $\nu = 1, 3$. So assume otherwise. Then by the above, Γ must be isomorphic to the semidirect product of $N = (\mathbf{Z}/3)^2$ with E, where E acts on $(\mathbf{Z}/3)^2$ via the above injection. Thus $n = |\Gamma| = 144$.

Let $\wp$ be the unique prime of L_ν over 2. We claim that $\wp$ splits completely in H, into nine primes of norm 2. To see this, let $\mathcal{P}$ be a prime of H over $\wp$, let D be the decomposition group at $\mathcal{P}$, and let I be the inertia group at $\mathcal{P}$. Then I is a Sylow 2-subgroup of Γ, and after altering the choice of $\mathcal{P}$ we may assume that $I = E$ (which we regard as a subgroup of Γ, with conjugation action given via the isomorphism $E \tilde{\to} S$). Now I is normal in D, and to prove the claim it suffices to show that $D = I$, or equivalently that $D \cap N = 1$. So let $d \in D \cap N$. Since $s \in E$, the normality of $I = E$ in D implies that $dsd^{-1} \in E$; so the commutator $[d, s] \in E$. But $[d, s] = d(sd^{-1}s^{-1}) \in N$ since $d \in N$ and N is normal in Γ. Since $E \cap N = 1$ in Γ, we have that $[d, s] = 1$. But conjugation by s (i.e. multiplication by the matrix $\rho(s)$) cyclically permutes the non-identity elements of N. Thus $d = 1$. This proves the claim.

According to Odlyzko's lower bound [Wa, p.221], if real numbers $\sigma, \tilde{\sigma} > 1$ are chosen subject to two inequalities, and $H/\mathbf{Q}$ is any totally complex Galois extension

of degree n, then

$$\log(|\Delta_H|) \geq n(\log(2\pi) - \psi(\sigma)) + \frac{n}{2}(2\sigma - 1)\psi'(\tilde{\sigma}) + 2Z(\sigma) + (2\sigma - 1)Z_1(\tilde{\sigma}) - \frac{2}{\sigma} - \frac{2}{\sigma - 1} - \frac{2\sigma - 1}{\tilde{\sigma}^2} - \frac{2\sigma - 1}{(\tilde{\sigma} - 1)^2}.$$

Here $\psi(s) = \Gamma'(s)/\Gamma(s)$, $Z(s) = -\zeta_H'(s)/\zeta_H(s)$, and $Z_1(s) = -Z'(s)$. Thus for real $s > 1$,

$$Z(s) = \sum_{\mathcal{P}} \frac{\log N\mathcal{P}}{N\mathcal{P}^s - 1}, \quad Z_1(s) = \sum_{\mathcal{P}} \frac{(\log N\mathcal{P})^2 N\mathcal{P}^s}{(N\mathcal{P}^s - 1)^2}.$$

Since all of the terms in the two above summations are positive, the inequality remains true if only those primes over 2 are included. In our situation, there are nine such primes, each of norm 2. So we have that $Z(\sigma) \geq 9(\log 2)/(2^\sigma - 1)$ and $Z_1(\tilde{\sigma}) \geq 9(\log 2)^2 \cdot 2^{\tilde{\sigma}}/(2^{\tilde{\sigma}} - 1)^2$. Taking $\sigma = 1.145$ and $\tilde{\sigma} = \frac{5}{6} + \frac{1}{6}\sqrt{12\sigma^2 - 5}$ (which satisfy the two required inequalities), we thus obtain that $\log|\Delta_H| \geq 404.53$ and so $|\Delta_H|^{1/144} \geq 16.59$. But $|\Delta_H|^{1/144} \leq 16$. This is a contradiction, proving that indeed the class number of L_ν is 1. □

Remarks. (a) If one is willing to assume the Generalized Riemann Hypothesis, then the computations of the above example can be significantly shortened. Namely, by Corollary 2.10 and Proposition 2.15, if the class number of L_ν is greater than 1, then it is at least 9. In that case, L_ν has an abelian unramified extension H that is Galois over $\mathbf{Q}$ with degree $n \geq 16 \cdot 9 = 144$. As before, $|\Delta_H|^{1/n} \leq 16$. But under GRH, Odlyzko's lower bound for extensions $\mathbf{Q} \subset H$ of degree $n \geq 140$ (even without any information about splittings of primes) is $|\Delta_H|^{1/n} \geq 16.67$. This is a contradiction.

(b) J.-P. Serre observed that Odlyzko's method can be systematized and improved by use of Weil's "explicit formulas." This yields better lower bounds for the discriminant, either with or without assuming GRH. For example, the bound 16.28 in the above example can be replaced by 18.81. See [Se1, pp. 240-243 and p. 710] for further details and references.

By Corollary 2.7, every group in $\pi_A(U_2)$ is a quasi-2 group. This can also be seen more directly. Namely, if $G \in \pi_A(U_2)$, then $G/p(G)$ is of odd order, and so is solvable. Thus if $G/p(G)$ is non-trivial, then it has a non-trivial abelian odd quotient, corresponding to a non-trivial abelian odd extension of $\mathbf{Q}$ ramified only at 2. This is impossible, since such an extension would have to lie in some $\mathbf{Q}(\zeta_{2^n})$. So actually $G/p(G)$ is trivial, and thus G is a quasi-2-group.

Strengthening this argument, we obtain the following result (where $K_0 = \mathbf{Q}$ is the case just considered):

Proposition 2.17. *Let K be a Galois extension of $\mathbf{Q}$ ramified only over 2, and let $\mathbf{Q} \subset K_0$ be an intermediate Galois extension whose degree is a power of 2. Then either*

(i) $\mathrm{Gal}(K/K_0)$ *is a quasi-2-group; or*
(ii) *there is a non-trivial abelian unramified extension $K_0 \subset L$ of odd degree such that $L \subset K$ and L is Galois over $\mathbf{Q}$.*

Proof. Let $G = \mathrm{Gal}(K/\mathbf{Q})$ and let $N = \mathrm{Gal}(K/K_0)$. The quasi-2 part $p(N)$ of N is normal in G, since it is characteristic in the normal subgroup $N \subset G$. Replacing G and N by $G/p(N)$ and $N/p(N)$ respectively, we may assume that N has odd order, and hence is solvable. In this situation, it suffices to prove that if $K_0 \neq K$ (i.e. if (i) fails) then the extension $K_0 \subset K$ is not totally ramified. For then (ii) holds, with L taken to be the maximal abelian unramified subextension of $K_0 \subset K$.

So assume otherwise, i.e. that $K_0 \subset K$ is non-trivial, and is totally ramified. Now the extension $\mathbf{Q} \subset K_0$ is unramified away from 2 and is Galois of 2-power degree; hence it is totally ramified over 2. Thus $\mathbf{Q} \subset K$ is totally ramified over 2, with inertia group G. But then $G = P \rtimes C$, where the normal subgroup P is a 2-group and C is cyclic of order prime to 2. Here C is non-trivial, since G is not a 2-group (because $|N| = [K : K_0]$ is odd and greater than 1). So the field of invariants K^P is a non-trivial C-Galois extension of $\mathbf{Q}$ ramified only over 2, which is impossible since C is abelian and odd. □

As a consequence of 2.17, various quasi-2-groups can be shown not to lie in $\pi_A(U_2)$. In particular, we have:

Example 2.18. For any positive integer n, let G be the dihedral group D_n of order $2n$. Then G is a quasi-2 group, and $G^{\mathrm{ab}} \cong \mathbf{Z}/2$ or $(\mathbf{Z}/2)^2$, but G is not in $\pi_A(U_2)$ unless n is a power of 2. Namely, if D_n is the Galois group of a Galois extension $\mathbf{Q} \subset K$ ramified only at the prime 2, then let $N \subset G$ be a cyclic normal subgroup of order n, and let L be the fixed field of N. Then L is either $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{2})$, or $\mathbf{Q}(\sqrt{-2})$, since these are the only 2-cyclic extensions of $\mathbf{Q}$ ramified only at 2. Each of these has class number 1, so 2.17 implies that the cyclic group $N = \mathrm{Gal}(K/L)$ is a quasi-2-group. Thus n is a 2-power. □

In the solvable case, 2.17 yields:

Lemma 2.19. *Under the hypotheses of Lemma 2.17, if $G = \mathrm{Gal}(K/\mathbf{Q})$ is solvable, and K_0 is the maximal 2-power subextension of K, then we may replace (i) of 2.17 by the condition that $K = K_0$ (i.e. G is a 2-group).*

Proof. Let $N = \mathrm{Gal}(K/K_0)$. Then N is the minimal normal subgroup of G whose index is a power of 2. If $K \neq K_0$, then $N \neq 1$. Since G is solvable, G has a normal subgroup $N_1 \subset N$ such that N/N_1 is of the form $(\mathbf{Z}/p)^n$ for some prime p and some $n \geq 1$. By the minimality of N, the index $(G : N_1)$ is not a power of 2, and so p is odd. Thus every 2-subgroup of N is contained in the proper subgroup N_1, and so $N = \mathrm{Gal}(K/K_0)$ is not a quasi-2-group. So (i) of 2.17 fails, and thus (ii) holds. □

As a result, we obtain:

Theorem 2.20. *Let G be a solvable group in $\pi_A(U_2)$. Then either G is a 2-group of order < 16, or G has a quotient of order 16.*

Proof. The result is clear if G is a 2-group, so assume not. Let K be a G-Galois extension of $\mathbf{Q}$ ramified only at 2, let K_0 be as in Lemma 2.19, and let $N = \mathrm{Gal}(K/K_0)$. Since G is not a 2-group, $N \neq 1$. So by 2.19, K_0 has class number > 1. Since K_0 is Galois over $\mathbf{Q}$ of 2-power degree, it follows by 2.15 that $|G/N| = [K_0 : \mathbf{Q}] \geq 16$. □

In the non-solvable case, there are the following examples of groups that are not in $\pi_A(U_2)$:

Example 2.21. (a) J. Top [To, Lemma 4.8.2] has shown that the alternating groups A_5 and A_6, and the symmetric groups S_5 and S_6, do not lie in $\pi_A(U_2)$. This follows from showing that there is no extension of $\mathbf{Q}$ of degree 5 or 6 that is ramified only at 2, even without a Galois hypothesis. This was shown by observing that the upper bound (*) given above shows that $v_2(\Delta) \leq 11$ for degree 5, and $v_2(\Delta) \leq 14$ for degree 6; and by inspecting lists of all fields of degree 5 and 6 with small discriminant. (In the case of A_5, Lenstra and Brumer have each observed that one can instead apply the upper bound (**) to the Galois extension itself, and this contradicts Odlyzko's lower bound.)

(b) The simple group $\mathrm{SL}(2,8)$ is not in $\pi_A(U_2)$. To see this, assume not and apply (**) to such an extension. Since the largest power of 2 dividing $|\mathrm{SL}(2,8)| = 504$ is 8, we have that $v_2(e) \leq 3$ (dropping the last term in the exponent), and so $|\Delta|^{\frac{1}{n}} \leq 2^4 = 16$. But according to [Od, p. 380, 1.11], for any extension of $\mathbf{Q}$ of degree n we have the inequality $|\Delta| \geq (21.8)^n e^{-70}$ (where in *this* formula $e = 2.718\ldots$). So in our situation, $|\Delta|^{\frac{1}{n}} \geq 21.8 \cdot e^{-70/504} = 18.973... > 16$. This is a contradiction.

(c) The simple group $G = \mathrm{SL}(3,2)$ of order 168 does not lie in $\pi_A(U_2)$. For this, we again proceed by contradiction and apply (**). But now in order to get a contradiction we must proceed more carefully, and need to analyze the possible ramification indices. Since the largest power of 2 dividing $|G| = 168$ is 8, we have that $v_2(e) \leq 3$. If $v_2(e) < 3$, then (**) gives $|\Delta|^{\frac{1}{n}} \leq 2^3 = 8$. On the other hand if $v_2 = 3$, then each of the Sylow 2-subgroups of G lies in some inertia group as a normal subgroup. But the upper triangular matrices in G form a Sylow 2-subgroup P of G, and the normalizer $N_G(P)$ is equal to P (this being true for the subgroup of upper triangular matrices in $\mathrm{SL}(m,k)$ for any m and any field k). Thus the inertia group containing P is P itself, showing that $e = 8$. Hence in this case (i.e. when $v_2 = 3$), (**) gives that $|\Delta|^{\frac{1}{n}} \leq 2^{1+3-\frac{1}{8}} = 14.672\ldots$. So in both cases, $|\Delta|^{\frac{1}{n}} \leq 15$. But by [Od, Table 1, p.401], for any Galois extension of degree ≥ 160, $|\Delta|^{\frac{1}{n}} \geq 15.12$. This is a contradiction. □

Remarks. (a) Example 2.21 shows that the four smallest simple groups (viz. A_5, $\mathrm{SL}(3,2)$, A_6, and $\mathrm{SL}(2,8)$) do not lie in $\pi_A(U_2)$. This raises the question of whether there are any simple groups in $\pi_A(U_2)$. It seems probable (to the author) that such groups do exist, but it may be difficult to find them.

(b) Example 2.21 provides instances of Serre's Conjecture. Namely, that conjecture implies that no group G of the form $\mathrm{SL}(2,2^m)$ can lie in $\pi_A(U_2)$. For $m = 1$ we get $G = S_3$, which by Theorem 2.20 (or by Example 2.18) does not lie in $\pi_A(U_2)$. For $m = 2$ we get $G = A_5$, and for $m = 3$ we get $G = \mathrm{SL}(2,8)$; by Example 2.21 these also do not lie in $\pi_A(U_2)$. But in fact, in a 1973 letter to Serre, J. Tate gave a proof of Serre's conjecture in the case of the prime 2. Specifically, he showed that if $G \subset \mathrm{SL}(2,2^m)$ is the Galois group of an extension $K/\mathbf{Q}$ that is ramified only at 2, then $K \subset \mathbf{Q}(\sqrt{-1}, \sqrt{2})$ and G is contained in the matrices of trace 0. His argument used the fact that a Sylow 2-subgroup of G is elementary abelian, along with class field theory and the Minkowski bound on the discriminant. Serre has observed that

a similar argument shows that no $\mathrm{SL}(2,3^m)$ lies in $\pi_A(U_3)$. See [Se1, p.710, note 2 to p.229] for further comments on Tate's argument.

By 2.6(a), there is no non-trivial Galois extension of $\mathbf{Q}$ that is tamely ramified over 2 and unramified elsewhere. In fact more is true, as Theorem 2.23 below shows. First we prove

Lemma 2.22. *If $G \in \pi_A(U_2)$ and $|G| \leq 300$ then G is solvable.*

Proof. Proceeding by induction on $|G|$, we assume the result holds for all strictly smaller groups. If N is any non-trivial normal subgroup in G, then G/N is also in $\pi_A(U_2)$, but it is smaller than G. So G/N is a solvable.

If G is not solvable, then any N as above is also non-solvable (since G/N is solvable), and so N has order ≥ 60. Since $|G| \leq 300$, we have that G/N has order ≤ 5 and so is abelian. Thus G satisfies the hypotheses of Lemma 2.5. Since $|G| \leq 300$, we have that G is isomorphic either to A_5, to S_5, or to $\mathrm{PSL}(2,7) \cong \mathrm{SL}(3,2)$. But these groups do not lie in $\pi_A(U_2)$, by Example 2.21, and this is a contradiction. □

Theorem 2.23. *Let $\mathbf{Q} \subset K$ be a Galois extension ramified only over 2, with Galois group G and ramification index e. Then 16 divides e unless G is a 2-group of order < 16 (in which case the extension is totally ramified).*

Proof. We have already observed that if G is a 2-group then the extension is totally ramified. And by Theorem 2.20, if G is not a 2-group of order < 16 and G is solvable, then G has a quotient H of order 16. In this case the corresponding H-Galois subextension of K is totally ramified, and so 16 divides e. So it remains to consider the case that G is not solvable. Now by Lemma 2.22, $|G| > 300$. But for a Galois field extension $\mathbf{Q} \subset K$ of degree $n \geq 240$, [Od, Table 1, p.401] says that $|\Delta|^{\frac{1}{n}} \geq 16.28$. So by (**), we have that $16.28 < 2^{1+v_2(e)}$ and so $v_2(e) > 3$. Since $v_2(e)$ is an integer, it is at least 4, and so 16 divides e. □

The number 16 in Theorem 2.23 cannot be replaced by a higher power of 2, as the following example shows:

Example 2.24. Let Γ be the semi-direct product $\mathbf{Z}/17 \rtimes (\mathbf{Z}/17)^*$, where the conjugation action of $(\mathbf{Z}/17)^*$ on $\mathbf{Z}/17$ is given by multiplication. Then $\Gamma \in \pi_A(U_2)$, corresponding to the Hilbert class field H of $\mathbf{Q}(i(\zeta_{64} + {\zeta_{64}}^{-1}))$. Namely, the class number of $F = \mathbf{Q}(\zeta_{64})$ is 17, and so the maximal abelian unramified extension L of F is Galois over F with group $\mathbf{Z}/17$. Now $\mathrm{Gal}(F/\mathbf{Q}) \cong \mathbf{Z}/16 \times \mathbf{Z}/2$, which has a unique subgroup V of the form $(\mathbf{Z}/2)^2$. The three subgroups of order 2 correspond to the intermediate fields $F_1 = \mathbf{Q}(\zeta_{64})^+$, $F_2 = \mathbf{Q}(\zeta_{32})$, and $F_0 = \mathbf{Q}(i(\zeta_{64} + {\zeta_{64}}^{-1}))$. For $i = 0, 1, 2$ let a_i be the involution in $V_i = \mathrm{Gal}(F/F_i)$. Thus $a_1 a_2 = a_0$. For $i = 1, 2$, F_i has class number 1, and so the unramified $\mathbf{Z}/17$-Galois extension $F \subset L$ does not descend to a $\mathbf{Z}/17$-Galois extension of F_i (which, if it existed, would have to be unramified; a contradiction). Now for $i = 1, 2$, $\mathrm{Gal}(L/F_i)$ is a semidirect product of the form $\mathbf{Z}/17 \rtimes \mathbf{Z}/2$, and since $F \subset L$ does not descend to F_i, this cannot be a direct product. Thus in the semi-direct product, the involution a_i acts on $\mathrm{Gal}(L/F) \cong \mathbf{Z}/17$ non-trivially, and hence as multiplication by -1 (for $i = 1, 2$).

Thus $a_0 = a_1 a_2$ acts trivially on $\mathrm{Gal}(L/F)$. So $\mathrm{Gal}(L/F_0) \cong \mathbf{Z}/17 \times \mathbf{Z}/2$, and the subfield L_0 of L corresponding to the subgroup $\mathbf{Z}/2$ is then a $\mathbf{Z}/17$-Galois unramified extension of F_0. In fact, it is the maximal abelian unramified extension of F_0, and so it is Galois over $\mathbf{Q}$, with group $\mathbf{Z}/17 \rtimes \mathrm{Gal}(F_0/\mathbf{Q})$. The conjugation action of this semi-direct product is given by a homomorphism $\alpha : \mathrm{Gal}(F_0/\mathbf{Q}) \to \mathrm{Aut}(\mathbf{Z}/17)$, and the kernel of α is trivial since the $\mathbf{Z}/17$-Galois extension $F_0 \subset L_0$ does not descend further (by Theorem 2.23). Thus α is an isomorphism, showing that the extension is as asserted. □

In fact, the Γ-Galois extension $\mathbf{Q} \subset H$ of Example 2.24 is the smallest non-2-group extension of $\mathbf{Q}$ with ramification only at 2:

Theorem 2.25. *The group $\Gamma = \mathbf{Z}/17 \rtimes (\mathbf{Z}/17)^*$, of order 272, is the smallest non-2-group in $\pi_A(U_2)$, and there is a unique extension of $\mathbf{Q}$ with this degree that is ramified only at 2.*

Proof. By 2.24, the group Γ is in $\pi_A(U_2)$, corresponding to the Hilbert class field H of $\mathbf{Q}(i(\zeta_{64} + \zeta_{64}{}^{-1}))$. Let G be the smallest non-2-group in $\pi_A(U_2)$, corresponding to a field extension $\mathbf{Q} \subset L$. We wish to show that $G \cong \Gamma$, and that $L = H$.

Since G is smallest, we have that $|G| \leq 272$, and so G is solvable by Lemma 2.22. Let N be the minimal normal subgroup of 2-power index in G. Thus $N \neq 1$, since $|G|$ is not a power of 2. By minimality of G, the subgroup N is minimal among all the non-trivial normal subgroups of G; hence N is an elementary abelian p-group $(\mathbf{Z}/p)^\nu$, for some odd prime p. By Theorem 2.20, $\overline{G} = G/N$ has order ≥ 16. Let $K = L^N$. Thus $\mathbf{Q} \subset K$ is $\overline{G}$-Galois and is ramified only over 2. Since $|G| \leq 16 \cdot 17$, we have that $|N| \leq 17$.

We claim that the extension $K \subset L$ is unramified. For if not, let $K \subset L_0$ be the maximal unramified intermediate extension. This extension is Galois, say with group G/N_0, where $N_0 \neq 1$. If N_0 is strictly contained in N, then the index $(G : N_0)$ is not a power of 2 (by definition of N), and so G/N_0 is a non-2-group in $\pi_A(U_2)$ which is strictly smaller than G (since $N_0 \neq 1$). This is a contradiction, proving that $N_0 = N$. Thus the extension $K \subset L$ is totally ramified, with inertia group N. Since N has no non-trivial 2-power quotients (by definition of N), this inertia group must be tame, and hence cyclic of odd order. This contradicts Proposition 2.17, proving the claim.

Next, we show that the homomorphism $\rho : \overline{G} \to \mathrm{Out}(N) = \mathrm{Aut}(N)$, induced by the exact sequence $1 \to N \to G \to \overline{G} \to 1$, is injective. Let I be an inertia group of $L/\mathbf{Q}$ over 2. Since $K \subset L$ is unramified, and since $\mathbf{Q} \subset K$ is totally ramified over 2 by 2.8(a), it follows that the homomorphism $G \to \overline{G}$ maps I isomorphically onto G. This induces a splitting of the exact sequence, and allows us to regard $\overline{G} \subset G$. Let $N_1 = \ker(\rho) \subset \overline{G} \subset G$. Then the elements of N_1 commute with those of N, and N_1 is normal in $\overline{G}$; so N_1 is normal in G, of 2-power order. Thus G/N_1 is a non-2-group in $\pi_A(U_2)$. The minimality of G implies that $N_1 = 1$, as desired.

In order to prove that $G \cong \Gamma$, it suffices to show that $\nu = 1$. For if this is shown, then N is cyclic of order p, so that $\mathrm{Out}(N) = \mathrm{Aut}(N) \cong (\mathbf{Z}/p)^*$ has $p-1$ elements. But $\rho : \overline{G} \to \mathrm{Out}(N)$ is injective, and so $p - 1 \geq 16$; i.e. $|N| = p \geq 17$. But $|N| \leq 17$, and so $p = 17$ and ρ is an isomorphism. Thus $G \cong \Gamma$, as desired.

As shown above, the Galois extension $K \subset L$ is unramified, and has group N. If $\nu > 1$, then $17 \geq |N| \geq p^2$, and so $p = 3$ and $\nu = 2$. Thus $N \cong (\mathbf{Z}/3)^2$, and so

$\mathrm{Out}(N) = \mathrm{Aut}(N) \cong \mathrm{GL}(2,3)$, a group of order $48 = 16 \cdot 3$. Since $\rho : \overline{G} \to \mathrm{Out}(N)$ is injective, and since $\overline{G}$ is a 2-group of order ≥ 16, it follows that $|\overline{G}| = 16$ and ρ defines an isomorphism between $\overline{G}$ and a Sylow 2-subgroup of $\mathrm{GL}(2,3)$. That is, $\overline{G}$ is isomorphic to the group $E = \langle s, t \mid s^8 = 1, t^2 = 1, tst^{-1} = s^3 \rangle$ (cf. Example 2.16). Since K is E-Galois over $\mathbf{Q}$ with ramification only over 2, Example 2.16 says that K has class number 1. But L is an unramified Galois extension of K with group $(\mathbf{Z}/3)^2$. This is a contradiction, and so indeed $\nu = 1$.

Thus $G \cong \Gamma$. As above, L is a 17-cyclic unramified extension of K, which is a 16-cyclic extension of $\mathbf{Q}$ ramified only at 2. But the only such degree 16 extensions of $\mathbf{Q}$ are $\mathbf{Q}(i(\zeta_{64} + \zeta_{64}{}^{-1}))$ and $\mathbf{Q}(\zeta_{64})^+$. The former has class number 17 and the latter has class number 1. So L must be the Hilbert class field of the former. This proves uniqueness. $\square$

We conclude by returning to the problem of studying $\pi_1^{\mathrm{tr}}(U_2)$ (cf. Theorem 2.11(b)).

Remark. In terms of the parallel between the arithmetic and geometric situations, $\pi_1^{\mathrm{tr}}(U_2)$ may be regarded as an analog of $\pi_1(\mathbf{P}^1 - \{\xi\})$, where ξ is a single point, since 2 is the rational prime of minimal possible degree, and since number theorists traditionally regard totally real number fields as being the ones that are unramified over the prime at infinity. On the other hand, this standard interpretation of totally real fields is a bit arbitrary, since the extension of local fields at infinity could instead be viewed as arising from "an extension of residue fields," rather than from ramification. Indeed, there are reasons for this alternative interpretation [Ha1, section 2, esp. remark after Proposition 2.5]. Under this view, totally real fields ramified only over 2 correspond to Galois covers of $\mathbf{P}^1_k$ that are ramified only over $(x = 0)$, and have a k-rational point over the base point $(x = \infty)$.

Proposition 2.26. *Let G be a non-cyclic solvable group in $\pi_A^{\mathrm{tr}}(U_2)$, corresponding to a totally real field K. Let K_0 be the maximal subfield of K of the form $\mathbf{Q}(\zeta_{2^n})^+$. Then K contains a subfield L which is unramified over K_0 of odd degree > 1.*

Proof. By 2.11(b), the fields of the form $\mathbf{Q}(\zeta_{2^m})^+$ are the only totally real 2-power Galois extensions of $\mathbf{Q}$ ramified only at 2. So K_0 is the maximal subfield of K that is Galois over $\mathbf{Q}$ and whose Galois group over $\mathbf{Q}$ is a 2-group. Also, $K \neq K_0$ since G is not cyclic. So the result follows from 2.19. $\square$

Corollary 2.27. *Let G be a non-cyclic solvable group in $\pi_A^{\mathrm{tr}}(U_2)$. Then G has a cyclic quotient of order 32 (or 64, assuming the Generalized Riemann Hypothesis).*

Proof. Let K and K_0 be as in Proposition 2.26. Then the class number of $\mathbf{Q}(\zeta_{2^n})^+$ is greater than 1. But the class number of $\mathbf{Q}(\zeta_{2^n})^+$ is known to be 1 for $n \leq 6$ (or even $n \leq 7$, assuming GRH). So in K_0, $n > 6$ (resp. $n > 7$), and the conclusion follows. $\square$

Actually, there is no value of n for which $\mathbf{Q}(\zeta_{2^n})^+$ is known to have class number greater than 1. And as H.W. Lenstra and L. Washington have speculated to the author, the ideas of [CL] suggest the possibility that all of these fields might have class number 1. Also, no non-abelian simple groups are known to lie in $\pi_A^{\mathrm{tr}}(U_2)$ (or, for that matter, in $\pi_A(U_2)$; cf. the comment after Example 2.21). Indeed, the only groups known to lie in $\pi_A^{\mathrm{tr}}(U_2)$ are the cyclic 2-groups. So we ask the following

Question 2.28. (a) Is every $h(\mathbf{Q}(\zeta_{2^n})^+) = 1$? Equivalently (by Prop. 2.26), is $(\pi_1^{\mathrm{tr}})^{\mathrm{solv}}(U_2) = \mathbf{Z}_2$?

(b) Is $\pi_1^{\mathrm{tr}}(U_2) = \mathbf{Z}_2$?

Addendum (added April 25, 1994). G. Malle has pointed out to me that an affirmative answer to Question 2.13 follows from a result of H. Markscheitis [Ma]. In fact, [Ma] showed that $\pi_1^2(U^2)$ is the pro-2-group on two generators a, b subject only to the relation $b^2 = 1$. So by the Burnside Basis Theorem, a finite 2-group G is in $\pi_A(U^2)$ if and only if G/F has two generators, one of them of order ≤ 2. (Here F is the Frattini subgroup of G.) Since G/F is abelian, this condition will be satisfied if G is generated by an element g together with the conjugates of an involution i. Hence the condition in 2.12(a) indeed implies that $G \in \pi_A(U^2)$. Cf. also [Ko].

References

[Ab1] S. Abhyankar, *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825–856.

[Ab2] S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. Amer. Math. Soc. (New Ser.) **27** (1992), 68–133.

[CL] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, Number Theory: Noordwijkerhout 1983 (H. Jager, eds.), Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin-Heidelberg-New York, pp. 33–62.

[CH] K. Coombes and D. Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), 821–839.

[De] E. Dew, *Fields of definition of arithmetic Galois covers.*, Ph.D. thesis, University of Pennsylvania, 1991.

[Gr] A. Grothendieck, *Revêtements étales et groupe fondamental*, SGA 1, Lecture Notes in Math., vol. 224, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[Ha1] D. Harbater, *Arithmetic discriminants and horizontal intersections*, Math. Annalen **291** (1991), 705–724.

[Ha2] D. Harbater, *Formal patching and adding branch points*, Amer. J. Math. **115** (1993), 487–508.

[Ha3] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, 1993 preprint, Inventiones Math. (to appear).

[Ka] T. Kambayashi, *Nori's construction of Galois coverings in positive characteristics*, Algebraic and Topological Theories, Tokyo, 1985, pp. 640–647.

[Ko] H. Koch., *l-Erweiterungen mit vorgegebenen Verzweigungsstellen.*, J. reine angew. Math. **219** (1965), 30–61.

[Ma] H. Markscheitis., *On p-extensions with one critical prime.*, Izvestija Akad. Nauk SSSR, Ser. Mat. **27** (1963), 463–466 (Russian).

[Na] H. Nakamura., *Galois rigidity of the étale fundamental groups of punctured projective lines.*, J. reine angew. Math. **411** (1990), 205–216.

[Od] A.M. Odlyzko., *On conductors and discriminants*, Algebraic Number Fields (A. Fröhlich, eds.), Durham Symposium, 1975, Academic Press, London, 1977, pp. 377–407.

[Ra] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d' Abhyankar*, 1992 preprint, Inventiones Math. (to appear).

[Se1] J.-P. Serre, *Oeuvres: Collected Papers, Volume III*, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1986.

[Se2] J.-P. Serre, *Construction de revêtements étales de la droite affine en caractéristique p*, Comptes Rendus **311** (1990), 341–346.

[Sh] I.R. Shafarevich, *Algebraic number fields*, Proc. Intl. Congr. Math., Stockholm, 1962, Inst. Mittag-Leffler, Djursholm, 1963, pp. 163–176 (also in I.R. Shafarevich, Collected Mathematical Papers, Springer-Verlag, Berlin-Heidelberg-New York, 1989, pp. 283–294).

[To] J. Top, *Hecke L-series related with algebraic cycles or with Siegel modular forms*, Ph.D. thesis, Utrecht, 1989.

[Wa] L. Washington, *Introduction to Cyclotomic Fields*, GTM, vol. 83, Springer-Verlag, New York, 1982.

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395

E-mail: harbater@rademacher.math.upenn.edu