FUNDAMENTAL GROUPS AND EMBEDDING PROBLEMS IN CHARACTERISTIC p

David Harbater

Abstract. Let X be a curve over an algebraically closed field k of arbitrary characteristic, and let S be a finite set of points of X. Let K be the function field of X, and let L_S be the maximal algebraic extension of K that is unramified over S. We prove that $\Pi_{K,S} = \mathrm{Gal}(L_S/K)$ is a free profinite group, of rank equal to the cardinality of k. Taking S empty, this implies the function field version of a conjecture of Shafarevich. The freeness of $\Pi_{K,S}$, which can be interpreted as a statement about fundamental groups, is proven as a consequence of showing that embedding problems over X can be solved with some control over ramification; and that result is proven using formal patching.

Section 1. Introduction

This paper considers fundamental groups of curves over an algebraically closed field k of arbitrary characteristic $p \geq 0$, in the local and birational situations. For affine curves X in characteristic 0, $\pi_1(X)$ is known by reduction to the case of $k = \mathbf{C}$ [Gr1, XIII, Cor. 2.12], where classical methods provide the answer. And in characteristic $p > 0$, if X is an affine curve then the set $\pi_A(X)$ of finite quotients of $\pi_1(X)$ is known, as a result of the recent proof ([Ra], [Ha3]) of Abhyankar's conjecture [Ab]. But in that case the fundamental group $\pi_1(X)$ itself is quite complicated and is far from being understood. Many finite groups are quotients of $\pi_1(X)$, but many embedding problems have obstructions, and so it is difficult even to formulate a conjecture as to the structure of the profinite group $\pi_1(X)$. The present paper shows that the situation is quite different in the local and birational cases.

Specifically, if X is a smooth projective curve over k, and S is a finite set of closed points of X, then we determine the fundamental group of the semi-localization X_S of X at S. In particular, if S is empty then this is the fundamental group of the generic point of X, i.e. the absolute Galois group of the function field K of X. And if S consists of a single closed point s, then this is the fundamental group of $\mathrm{Spec}(\mathcal{O}_{X,s})$. What we show is that every non-trivial finite embedding problem for X_S has many solutions (Theorem 4.1), and that $\pi_1(X_S)$ is a free profinite group, of rank equal to the cardinality of k (Theorem 4.4). We also prove a more precise

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14H30, 13B05; Secondary 12F12, 14D15.

Key words and phrases. fundamental group, embedding problem, Galois, cover.

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..

version of the theorem on embedding problems, which shows that although an embedding problem for a given affine curve cannot in general be solved (because π_1 is not free), a slight modification of the problem can be solved. That is, if $G \to H$ is a surjective group homomorphism, then any H-Galois cover of the curve can be lifted to a G-Galois cover having a few extra branch points (Theorem 3.6). This lifting theorem is shown using a formal patching result from [Ha3] together with Abhyankar's conjecture [Ha3, Theorem 6.2] (that G is in π_A of a given curve of genus g with $r > 0$ points deleted if and only if each prime-to-p quotient of G is generated by a set of at most $2g + r - 1$ elements).

Our results imply in particular the function field version of a conjecture of Shafarevich. Specifically, Shafarevich conjectured that the absolute Galois group of $\mathbf{Q}^{\mathrm{ab}}$ is a free profinite group of countable rank. (He discussed this conjecture in his talks at Obervolfach in 1964 on the class field tower problem, and it appeared later in [Be].) That conjecture would imply more generally that for any number field K, the absolute Galois group of the maximal cyclotomic extension K^{cycl} is free of countable rank. His conjecture has been further generalized to ask if this assertion about K^{cycl} holds for arbitrary global fields K. The function field case of this generalized conjecture is a special case of our Theorem 4.4, by taking our k to be the algebraic closure of $\mathbf{F}_p$, with S empty (cf. Corollary 4.2(b)). I have learned from F. Pop that he has independently found a proof of the function field case of Shafarevich's conjecture [Po3], using rigid analytic techniques and ideas from [Po2]. Meanwhile, the full Shafarevich conjecture has been generalized even further by Fried and Völklein [FV, introduction]; viz. they conjecture that if K is a countable Hilbertian field whose absolute Galois group G_K is projective, then G_K is free of countable rank.

Our results can also be interpreted from the perspective of Grothendieck's anabelian conjecture [Gr2]. According to that conjecture, if F is a field of finite type over its prime field, with separable closure F^{sep}, then affine F-curves ought to be determined by their fundamental groups, together with the induced actions of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on π_1. Special cases have been shown for affine curves over number fields [Na]. Also, the birational analog of this conjecture has been proven by Uchida [Uc], in the case that F is finite. That is, a smooth projective curve X over a finite field, with function field K, is determined by the absolute Galois group of K, together with the action of Frobenius on K. A generalization of this birational result has recently been proven by Pop [Po1], and an analog for number fields K (rather than for function fields K of F-curves) follows from previous work of Neukirch [Ne].

In the case of curves over *algebraically closed* fields k, the conjecture in [Gr2] does not apply, and is clearly false in characteristic 0. Indeed, in characteristic 0, if $g \geq 0$ and $r > 0$, then any two affine curves of the form (genus g) $-$ (r points) have isomorphic fundamental groups. Yet in characteristic $p > 0$, this last assertion is false, and even two curves of the form $\mathbf{P}^1 - (4 \text{ points})$ can have non-isomorphic π_1's [Ha4, Theorem 1.8], because different embedding problems have solutions. (This is despite the fact that two such curves must have the same π_A because of Abhyankar's conjecture.) Thus at least *some* pairs of affine curves over an algebraically closed field k of characteristic $p > 0$ can be distinguished by their fundamental groups, as well as by the embedding problems that can be solved. What the results of this paper show is that this is *never* the case in the birational and semi-local situations.

In particular, the fundamental groups of such k-curves X_S convey no information about the particular curve, but only about the cardinality of k.

The structure of this paper is as follows: Section 2 discusses the formal patching result that is needed in our construction, and section 3 then uses this to prove Theorem 3.6 on liftings of covers of affine curves. In section 4 this result is used to obtain the result about solutions to embedding problems in the birational and semi-local cases (Theorem 4.1), and that implies the freeness of fundamental groups and absolute Galois groups (Theorem 4.4).

Conventions:

For the remainder of the paper we fix an algebraically closed field k of characteristic $p \geq 0$, and we let $\Omega = k((t))$. Affine and projective spaces $\mathbf{A}^n$ and $\mathbf{P}^n$ will be over k unless otherwise specified.

If X is a scheme and ξ is a point of X such that the complete local ring $\hat{\mathcal{O}}_{X,\xi}$ is a domain, then we let $\hat{\mathcal{K}}_{X,\xi}$ be the fraction field of $\hat{\mathcal{O}}_{X,\xi}$. If X is integral, then a *cover* of X is a finite generically separable morphism $Y \to X$ of schemes (cf. [Ha3, sect. 1]). If G is a finite group then a *G-Galois* cover is a cover $Y \to X$ together with a homomorphism $\rho : G \to \mathrm{Aut}_X(Y)$ such that G acts simply transitively on a generic geometric fibre of the cover via ρ.

For any finite group G and any prime number p, we will write $p(G)$ for the *quasi-p-part* of G, i.e. the (normal) subgroup of G generated by the Sylow p-subgroups of G. Thus $G/p(G)$ is the maximal prime-to-p quotient of G. On the other hand if $p = 0$, then we let $p(G) = \{1\}$. A finite group G is a *quasi-p-group* if $p(G) = G$.

Section 2. Formal patching.

This section describes a formal patching result [Ha3, Proposition 2.3] that was used in the proof of Abhyankar's conjecture [Ha3, Theorem 6.2], and that will be needed in Section 3 of this paper. Roughly, the result says the following: Let G be a finite group generated by subgroups G_1 and G_2, and let $W_i \to X_i$ be connected G_i-Galois covers of k-curves for $i = 1, 2$. By taking a disjoint union of copies of W_i, indexed by the left cosets of G_i in G, we obtain induced disconnected G-Galois covers $\mathrm{Ind}_{G_i}^G W_i \to X_i$. Let T^* be a projective $k[[t]]$-curve whose closed fibre is a union of X_1 and X_2 meeting at a single point $\tau \in T^*$. Suppose that "patching data" is given for $\mathrm{Ind}_{G_1}^G W_1$ and $\mathrm{Ind}_{G_2}^G W_2$ over $\mathrm{Spec}(\hat{\mathcal{O}}_{T^*,\tau})$. Then there is a connected G-Galois cover $W^* \to T^*$ whose closed fibre is a union of $\mathrm{Ind}_{G_1}^G W_1$ and $\mathrm{Ind}_{G_2}^G W_2$ meeting over τ, and that agrees with the given patching data.

For technical reasons it is easier to prove this result under the extra condition that all the spaces are fibred over a smooth curve L. In practice this does not seem to be a significant restriction, but it does make the result more cumbersome. Also, the full result allows for the possibility that G is not generated by G_1 and G_2 alone, but rather is generated by those two groups together with the Galois group I of the patching data over $\hat{\mathcal{O}}_{T^*,\tau}$.

The precise situation is the following: Let T^* be an irreducible projective $k[[t]]$-scheme of relative dimension 1, whose closed fibre is a union of two smooth irreducible curves X_1, X_2 that meet at a single point $\tau \in T^*$. Assume also the technical condition that there is a smooth projective k-curve L together with a covering morphism $\phi : T^* \to L \times_k \mathrm{Spec}(k[[t]])$ over $k[[t]]$, and that ϕ is flat. (Here ϕ is automatically flat if T^* is normal.)

For $i = 1, 2$ let $X_i' = X_i - \{\tau\}$, so that X_i' is an affine curve, say $\mathrm{Spec}(R_i)$. Let $X_i'^* = \mathrm{Spec}(R_i[[t]])$; we regard this as a "thickening" of X_i'. Also, let $\hat{X}_i'^* = \mathrm{Spec}(\hat{\mathcal{K}}_{X_i,\tau}[[t]])$ and $\hat{T}^* = \mathrm{Spec}(\hat{\mathcal{O}}_{T^*,\tau})$.

Now consider a finite group G, together with subgroups G_1, G_2, I that generate G. For $i = 1, 2$ let $W_i'^* \to X_i'^*$ be an irreducible normal G_i-Galois cover, and let $\hat{W}_i'^*$ be an irreducible component of $W_i'^* \times_{X_i'^*} \hat{X}_i'^*$ such that $I_i = \mathrm{Gal}(\hat{W}_i'^*/\hat{X}_i'^*)$ is contained in I. Also, let $\hat{N}^* \to \hat{T}^*$ be an irreducible normal I-Galois cover, together with isomorphisms $\hat{N}^* \times_{\hat{T}^*} \hat{X}_i'^* \tilde{\to} \mathrm{Ind}_{I_i}^I \hat{W}_i'^*$ of I-Galois covers of $\hat{X}_i'^*$, for $i = 1, 2$.

Proposition 2.1. [Ha3, Proposition 2.3] *In the above situation, there is an irreducible normal G-Galois cover $V^* \to T^*$ such that $V^* \times_{T^*} X_i'^* \approx \mathrm{Ind}_{G_i}^G W_i'^*$ as G-Galois covers of $X_i'^*$ for $i = 1, 2$, and $V^* \times_{T^*} \hat{T}^* \approx \mathrm{Ind}_I^G \hat{N}^*$ as G-Galois covers of $\hat{T}^*$.*

This result relies on general formal patching results in [Ha2], which are proven by factoring matrices of power series. The significance of Proposition 2.1 is that it allows one to go from G_i-Galois covers of curves X_i to G-Galois covers. Note that the proposition yields a G-Galois cover of a $k[[t]]$-curve T^*, rather than of a k-curve. But by taking the generic fibre, we obtain an irreducible G-Galois cover of a curve over the field $\Omega = k((t))$. Then, since k is algebraically closed, the "Lefschetz principle" allows us to obtain such a cover of a k-curve.

The above strategy will be used in section 3 to prove the lifting result for covers, Theorem 3.6. A similar strategy was used in [Ha3] to prove the general case of Abhyankar's conjecture. Namely, Raynaud had previously shown [Ra] that that conjecture holds for the affine line, i.e. that every quasi-p-group is a Galois group over $\mathbf{A}^1$. In the case of the affine curve $\mathbf{P}^1 - \{0, \infty\}$, the conjecture says that every cyclic-by-quasi-p-group G must be a Galois group of an unramified cover. This is done [Ha3, Proposition 5.2] by using the above proposition to patch together a $p(G)$-Galois cover of the affine line (which exists by Raynaud's result) and an appropriate cyclic-by-p cover of the twice-punctured projective line. (In the construction, the latter is actually defined over Ω, and a model for it over $k[[t]]$ is in fact ramified along the fibre $(t = 0)$.) For a general affine curve U, if G is predicted by Abhyankar's conjecture to be a Galois group over U, then we can reduce to the case that G is generated by a prime-to-p-subgroup that occurs over U, together with a cyclic-by-quasi-p-subgroup (which occurs over $\mathbf{P}^1 - \{0, \infty\}$, by the previous case). Patching these together by the above proposition then yields the full conjecture [Ha3, Theorem 6.2]. (See also [Ha4, sect. 1] for a further discussion of this.)

Application 2.2. Proposition 2.1 can be used to prove a key step in Raynaud's proof of Abhyankar's conjecture for $\mathbf{A}^1$. Namely, let G be a quasi-p-group having a Sylow p-subgroup S, such that G is generated by quasi-p-subgroups $G_1, \dots, G_n$ that are each Galois groups over the affine line. Assume that each G_i has a Sylow p-subgroup S_i that is contained in S. Then G is a Galois group over the affine line [Ra, Thm. 2.2.1(2)].

We sketch a proof of this result of Raynaud using the above proposition. First, adjoining S to the set of G_i's, we are reduced by induction to the case that $n = 2$.

For $i = 1, 2$, take smooth irreducible G_i-Galois covers $W_i \to X_i = \mathbf{P}^1$ that are branched only over infinity. We may assume that the inertia groups over infinity are the Sylow p-subgroups of G_i, by [Ha2, Theorem 2 and Lemma to Theorem 4] or by [Ra, Cor. 2.2.6]. In particular one of the inertia groups of W_i over infinity is S_i. To prove the result, it suffices (by the Lefschetz principle) to patch the G_i-Galois covers W_i together to obtain an irreducible G-Galois cover of the line over $k[[t]]$. In order to do this using the above proposition, we can take X_1 to be the line $(y = x)$ in (x, y)-space $T = \mathbf{P}^1 \times \mathbf{P}^1$, and X_2 to be the line $(y = -x)$, where the origin $(x = y = 0)$ corresponds to the point at infinity on each line X_i. Setting $t = xy$, $X_1 \cup X_2$ is the fibre of T over $(t = 0)$. Take T^* to be the completion of T along this fibre. In order to apply the proposition in this situation, we need to find patching data over the complete local ring at the origin.

To do this, consider the restriction $\hat{W}_i \to \hat{X}$ of $W_i \to \mathbf{P}^1$ over $\hat{X} = \mathrm{Spec}(\hat{\mathcal{O}}_{\mathbf{P}^1,\infty})$. Then $\mathrm{Ind}_{S_i}^P \hat{W}_i \to \hat{X}$ is a P-Galois cover, where $P \subset S$ is the p-subgroup of G generated by S_1 and S_2. Let $X^o = \mathrm{Spec}(\hat{\mathcal{K}}_{\mathbf{P}^1,\infty})$, and let $W_i^o \to X^o$ be the restriction of $\hat{W}_i \to \hat{X}$ over X^o. By [Ha1, Thm. 1.2, Prop. 2.1], there is a fine moduli space M_P for P-Galois covers of X^o, viz. a certain direct limit of affine spaces $\mathbf{A}^n$. The points $\xi_i \in M_P$ corresponding to the covers $\mathrm{Ind}_{S_i}^P W_i^o \to X^o$ lie in some common $\mathbf{A}^n$ in this direct limit, and we may choose a morphism from the affine u-line $\mathbf{A}^1_k$ to this $\mathbf{A}^n$ such that the point $(u = 1)$ maps to ξ_1 and the point $(u = -1)$ maps to ξ_2. Pulling back by this map yields a P-Galois cover of the affine u-line over $\hat{X} = \mathrm{Spec}(k[[x]])$, and hence of $\mathrm{Spec}(k((x))[u])$. Setting $y = xu$, this latter space is isomorphic to $\mathrm{Spec}(k((x))[y])$, and the fibres over $(y = x)$ and $(y = -x)$ are respectively isomorphic to $\mathrm{Ind}_{S_i}^P W_i^o \to X^o$ for $i = 1, 2$. Hence we obtain a P-Galois cover $N^* \to \mathrm{Spec}(k[[x]][y])$ whose restriction $\hat{N}^* \to \hat{T}^* = \mathrm{Spec}(k[[x, y]])$ provides the desired patching data. Thus Proposition 2.1 applies, and as indicated above, Raynaud's result follows. □

Another application of Proposition 2.1 (i.e. of [Ha3, Proposition 2.3]) is to the problem of realizing finite groups as Galois groups of unramified covers of *projective* curves X over algebraically closed fields k of characteristic $p > 0$ (or equivalently, finding finite quotients of $\pi_1(X)$ for projective curves X). Such covers are constructed in the 1994 Ph. D. thesis of Katherine Stevenson [St], by using this patching result to paste together covers of curves of lower genus. As a consequence, she shows in particular that if G is a finite group having g generators, then G is the Galois group of an unramified cover of a generic projective curve of genus g. So by the Classification Theorem, each finite simple group can be realized as a Galois group of an unramified cover of a generic projective curve of genus 2.

Section 3. Lifting problems.

The main result of this section (Theorem 3.6) concerns lifting problems for affine curves. It says that if $U \to X$ is an H-Galois cover of curves that is unramified away from a given finite set $B \neq \emptyset$, and if $H = G/N$, then there is a G-Galois cover $Z \to X$ that is unramified over a given finite subset $S \subset X - B$, and such that $Z/N \approx U$ as H-Galois covers of X. Moreover, the number of additional branch points is at most $n+1$, where n is the number of generators of $N/p(N)$. In addition, if N is non-trivial, then there are infinitely many choices of Z; in fact, as many as the cardinality of k. The result also shows that we may allow B to be empty in the split case.

There are two reasons why the additional branch points are necessary in Theorem 3.6. The first, which applies even in characteristic 0, is that G may not be a quotient of $\pi_1(X - B)$, and hence there might not be any G-Galois covers $Z \to X$ branched only at B. The second reason, which presents difficulties in characteristic $p > 0$, is that even if G is a quotient of $\pi_1(X - B)$, it is possible that every such $Z \to X$ fails to dominate $U \to X$. These issues are discussed further in the remarks and question after Theorem 3.6.

Theorem 3.6 follows from Theorem 3.5, which shows that in the above situation we may choose one of the additional $n + 1$ branch points in advance. The proof of 3.5 uses formal patching (Proposition 2.1) to obtain an analogous lifting result (Lemma 3.2) over $k((t))$; this is then descended to a family of liftings parametrized by a k-variety E (3.3 and 3.4) which can afterwards be specialized to k.

We continue to work over a fixed algebraically closed field k of characteristic $p \geq 0$, and write $\Omega = k((t))$. Throughout this section, we consider the following hypotheses (3.1):

Hypotheses (3.1). Let

$$(*) \qquad 1 \to N \to G \to H \to 1$$

be an exact sequence of finite groups, with N non-trivial, and $N/p(N)$ generated by n elements ($n \geq 0$). Let $U \to X$ be a connected H-Galois cover of smooth projective k-curves, unramified away from some (possibly empty) finite set $B \subset X$.

Lemma 3.2. *Under Hypotheses (3.1), assume that the exact sequence (*) is split, and choose $\xi_0 \in X - B$. Let $U^o = U \times_k \Omega$, $X^o = X \times_k \Omega$, $B^o = B \times_k \Omega$, and $\xi_0^o = \xi_0 \times_k \Omega$. Then there is a projective $k[[t]]$-curve Σ^* with general fibre X^o; a G-Galois cover $V^* \to \Sigma^*$ whose general fibre $V^o = V^* \times_{k[[t]]} \Omega$ is a smooth connected Ω-curve; and a set of $k[[t]]$-points $B'^* = \{\eta_1^*, \ldots, \eta_n^*\}$ of Σ^* having pairwise disjoint support, such that*

- (i) *$V^o/N \approx U^o$ as H-Galois covers of X^o;*
- (ii) *the support of B'^* is disjoint from the closures of B^o and ξ_0^o in Σ^*, and $V^o \to X^o$ is étale away from $B^o \cup \{\xi_0^o\} \cup B'^o$ (where B'^o is the generic fibre of B'^*);*
- (iii) *the N-Galois cover $V^o \to U^o$ has non-trivial inertia groups over ξ_0^o, and also over some point of B'^o (provided, in the latter case, that $n > 0$);*
- (iv) *no point of B'^o is of the form $\xi \times_k \Omega$ for any $\xi \in X(k)$; and*
- (v) *V^* is irreducible and normal, and its closed fibre is connected and generically smooth.*

Proof. Write $B = \{\xi_1, \ldots, \xi_r\}$. Let $x \in \mathcal{O}_{X,\xi_0}$ be a local uniformizer of X at ξ_0. Let T be a copy of $\mathbf{P}^1_k$ with parameter t; let Σ be the blow-up of $X \times T$ at the point $(\xi_0, (t = 0))$; and let $\sigma \in \Sigma$ be the point at which the exceptional divisor meets the proper transform of $(t = 0) \subset X \times T$. Then Σ is a regular subvariety of $X \times T \times Y$, where Y is a copy of $\mathbf{P}^1_k$ with parameter y, and where Σ is given in a neighborhood of σ by $xy = t$. Thus $\sigma \in X \times T \times Y$ is the point $(\xi_0, (t = 0), \eta)$, where $\eta \in Y$ is the point $(y = 0)$.

The blow-up Σ contains a copy of X, viz. the proper transform of $(t = 0) \subset X \times T$. Also, Σ contains a copy of Y, viz. the exceptional locus of the blow-up map $\Sigma \to X \times T$. We will identify these copies with X and Y respectively. These curves intersect only at the point σ, which is identified with $\xi_0 \in X$ and with $\eta \in Y$.

Since $\Sigma \subset X \times T \times Y$, the rational functions x, t, y on Σ define morphisms $\Sigma \to \mathbf{P}^1$. Let $z = x + y$. Then we obtain a morphism $\Phi = (z, t) : \Sigma \to \mathbf{P}^1 \times \mathbf{P}^1$ to (z, t)-space. This morphism is finite and generically separable, and the fibre over $(t = 0)$ is the union of X and Y in Σ (under the identifications made in the previous paragraph), meeting at σ.

Let L be the projective z-line over k, let $\lambda \in L$ be the point $(z = 0)$, let L^* be the projective z-line over $k[[t]]$, let $L' = L - \{\lambda\} = \mathrm{Spec}(k[z^{-1}])$, and let $L'^* = \mathrm{Spec}(k[z^{-1}][[t]])$. Thus $L^* = L \times T^*$, where $T^* = \mathrm{Spec}(k[[t]])$. Let $\phi : \Sigma^* \to L^*$ be the pullback of $\Phi : \Sigma \to L \times T$ under $L^* \to L \times T$. Thus Σ^* is the completion of Σ along the locus of $(t = 0)$. Also, we may identify $\hat{\Sigma}^* = \mathrm{Spec}(\hat{\mathcal{O}}_{\Sigma^*,\sigma})$ with $\mathrm{Spec}(\hat{\mathcal{O}}_{\Sigma,\sigma})$, which is isomorphic to $\mathrm{Spec}(k[[x, y]])$. By construction, the closed fibre of ϕ is the union of X and Y, which meet only at σ.

Choose $n + 1$ distinct points $\eta_0, \ldots, \eta_n \in Y$, where η_0 is the point $(y = \infty)$, and where no η_j is the point $\eta \in Y$. For each j, let η_j^* be the inverse image of η_j under $y : \Sigma^* \to Y$ (i.e. under the composition of $\Sigma^* \to \Sigma$ with $y : \Sigma \to Y$). Thus $\eta_j^* \approx \eta_j \times_k T^*$ for all j. Also, for each i, let ξ_i^* be the proper transform of $\xi_i \times_k T^*$ under the blow-up map $\Sigma^* \to X \times T^*$. Thus $\xi_i^* \approx \xi_i \times_k T^*$ for $i \geq 1$, and $\xi_0^* = \eta_0^*$.

By the splitting assumption, we may regard H as a subgroup of G, such that H and N together generate G. By [Ha3, Thm.6.2] in the case that $p > 0$, and by [Gr1, XIII, Cor. 2.12] in the case that $p = 0$, we know that there is a smooth connected N-Galois cover $W \to Y$ that is étale except over $\{\eta_0, \ldots, \eta_n\}$.

We claim that $W \to Y$ may be chosen so that the inertia groups are non-trivial over η_0 and (if $n > 0$) over η_1. To see this, first consider the case that the order of N is prime to p. In this case, N has a set of n generators, and so there are non-trivial elements $a_0, \ldots, a_m \in N$ $(1 \leq m \leq n)$ that generate N and satisfy $a_0 \cdots a_m = 1$. By [Gr1, XIII, Cor. 2.12], $W \to Y$ may be chosen so that a_i generates an inertia group over η_i, for each $i \geq 0$ – proving the claim in this case. On the other hand, if p divides the order of N, then the Sylow p-subgroups of N are non-trivial. Applying [Ha2, Theorem 2] to the initial choice of W given by the previous paragraph, we obtain a new N-Galois cover of Y such that over the actual branch points of the original W the inertia is the same as before, but over the other η_i's the inertia groups are now the Sylow p-subgroups of N. So this new W has non-trivial inertia over every η_i, and thus is as desired. This proves the claim.

Let $X' = X - \{\xi_0\}$; let R_1 be the ring of functions on X'; let $X'^* = \mathrm{Spec}(R_1[[t]])$; and let $\hat{X}'^* = \mathrm{Spec}(\hat{\mathcal{K}}_{X,\xi_0}[[t]])$. Also, let $\mu \in U$ be a point over $\xi_0 \in X$; let U' be the inverse image of X' in U; let $U'^* = U' \times_{X'} X'^*$; and let $\hat{U}'^* = \mathrm{Spec}(\hat{\mathcal{K}}_{U,\mu}[[t]])$. Similarly, let $Y' = Y - \{\eta\} = \mathrm{Spec}(R_2)$, where $R_2 = k[y^{-1}]$; let $Y'^* = \mathrm{Spec}(R_2[[t]])$; and let $\hat{Y}'^* = \mathrm{Spec}(\hat{\mathcal{K}}_{Y,\eta}[[t]])$. Also, let W' be the inverse image of Y' in W; let $W'^* = W' \times_{Y'} Y'^*$; let $\omega \in W$ be a point over $\eta \in Y$; and let $\hat{W}'^* = \mathrm{Spec}(\hat{\mathcal{K}}_{W,\omega}[[t]])$.

Since $U \to X$ and $W \to Y$ are respectively unramified over the points ξ_0 and

η, we can apply Proposition 2.1, with Σ^* playing the role of the T^* of that result, and taking $G_1 = H$, $G_2 = N$, $I = I_1 = I_2 = \{1\}$, $v = t$, $X_1 = X$, $X_2 = Y$, $W_1'^* = U'^*$, $W_2'^* = W'^*$, and $\hat{N}^* = \hat{\Sigma}^*$. This yields an irreducible normal G-Galois cover $\psi : V^* \to \Sigma^*$ such that $V^* \times_{\Sigma^*} X'^* \approx \mathrm{Ind}_H^G U'^*$, $V^* \times_{\Sigma^*} Y'^* \approx \mathrm{Ind}_N^G W'^*$, and $V^* \times_{\Sigma^*} \hat{\Sigma}^*$ is trivial, as G-Galois covers of X'^*, Y'^*, and $\hat{\Sigma}^*$ respectively.

The branching of $\psi : V^* \to \Sigma^*$ is determined by that of its patches. On the patch over X'^*, it is branched only at $B^* = \{\xi_1^*, \ldots, \xi_r^*\}$. On the patch over Y'^*, there is ramification only over $B'^* = \{\eta_1^*, \ldots, \eta_n^*\}$ and over $\eta_0^* = \xi_0^*$, with constant non-trivial inertia over η_0^* and (if $n > 0$) over η_1^*. Finally, on the patch over $\hat{\Sigma}^*$, the cover is trivial and hence unramified. Since the closed fibre of Σ^* is generically smooth, and since the closed fibre of $V^* \to \Sigma^*$ is generically unramified, it follows that the closed fibre is generically smooth. By [Ha3, Lemma 2.4(b)], the closed fibre of V^* is connected.

Consider the intermediate H-Galois cover $V^*/N \to \Sigma^*$. Its pullback over X'^* agrees with U'^*, while the pullbacks over Y'^* and $\hat{N}^*$ are trivial. The same is true of the H-Galois cover $U \times_X \Sigma^*$ (where the pullback is with respect to the morphism $x : \Sigma^* \to X$). So by [Ha3, Cor. 2.2], there is an isomorphism $V^*/N \tilde{\to} U \times_X \Sigma^*$ as H-Galois covers. Also, since the trivial N-Galois cover $\mathrm{Ind}_H^G U'^* \to U'^*$ is unramified, and since $V^* \times_{\Sigma^*} X'^* \approx \mathrm{Ind}_H^G U'^*$, we have that $V^* \to V^*/N$ is unramified over the patch X'^*, and in particular at the locus over B^*.

Now by construction of Σ as a blow-up, the generic fibre Σ^{*o} of $\Sigma^* \to \mathrm{Spec}(k[[t]])$ is isomorphic to X^o. Identify Σ^{*o} with X^o, and let ξ_i^o and η_j^o denote the Ω-points of X^o corresponding to the generic points of the loci ξ_i^* and η_j^*. Thus $\xi_i^o = \xi_i \times_k \mathrm{Spec}(\Omega)$, $\eta_j^o = \eta_j \times_k \mathrm{Spec}(\Omega)$, and $\eta_0^o = \xi_0^o$. Let $B^o = \{\xi_1^o, \ldots, \xi_r^o\}$ and $B'^o = \{\eta_1^o, \ldots, \eta_n^o\}$. Then the restriction $\psi^o : V^{*o} \to X^o$ of the morphism $\psi : V^* \to \Sigma^*$ to the generic fibre is ramified only over $B^o \cup \{\xi_0^o\} \cup B'^o \subset X^o$. Here the closure of $B'^o \cup \{\xi_0^o\}$ in Σ^* consists of $\eta_0^*, \ldots, \eta_n^*$, and these $n+1$ loci are pairwise disjoint because they respectively meet the closed fibre at the $n+1$ distinct points $\eta_0, \ldots, \eta_n \in Y$, and nowhere else. Since $U \times_k \mathrm{Spec}(\Omega)$, $W \times_k \mathrm{Spec}(\Omega)$, and $\Sigma \times_{k[t]} \mathrm{Spec}(\Omega)$ are smooth over Ω, it follows that V^{*o} is also smooth over Ω. Also, V^{*o} is connected since V^* is irreducible. Moreover the inertia groups over the point $\eta_0^o = \xi_0^o$ (and over η_1^o if $n > 0$) are non-trivial because of the corresponding property for V^*. Thus the conditions of the lemma are satisfied. □

Remarks. (a) In the above lemma, we may replace condition (iii) above by

(iii)′ $V^o \to X^o$ is at most tamely ramified over B'^o.

Namely, this is automatic if $\mathrm{char}(k) = 0$; and if $\mathrm{char}(k) = p$ then the cover $W \to Y$ obtained in the above proof may be chosen to be at most tamely ramified except possibly over η_0, by [Ha3, Thm.6.2]. But in this case it is possible that the inertia groups over B'^o are all trivial, or that the inertia over ξ_0^o is trivial; so we cannot simultaneously insure that both (iii) and (iii)′ hold.

(b) The proof of the lemma shows that the result remains true if we add the additional condition:

(vi) The N-Galois cover $V^o \to U^o$ (cf. (i)) is unramified over B^o. □

Proposition 3.3. *Under Hypotheses (3.1), assume that either the exact sequence (*) is split or that B is non-empty. Let $\xi_0 \in X - B$. Then there exist a k-subalgebra*

$A \subset \Omega$ of finite type; an irreducible regular G-Galois cover $\pi_E : V_E \to X_E = X \times_k E$ (where $E = \mathrm{Spec}(A)$) such that V_E is smooth over E; and a set of E-points $B'_E = \{\eta_{1,E}, \ldots, \eta_{n,E}\}$ of X_E having pairwise-disjoint support, such that

(i) *$V_E/N \approx U \times_k E$ as H-Galois covers of X_E;*
(ii) *the support of B'_E is disjoint from those of $B_E = B \times_k E$ and $\xi_{0,E} = \xi_0 \times_k E$, and $V_E \to X_E$ is étale away from $B_E \cup \{\xi_{0,E}\} \cup B'_E$;*
(iii) *the N-Galois cover $V_E \to U \times_k E$ has non-trivial inertia groups over the generic point of $\xi_0 \times_k E$ and (if $n > 0$) over the generic point of some $\eta_{i,E}$ (where $0 < i \leq n$).*
(iv) *no $\eta_{j,E}$ (for $j > 0$) is of the form $\xi \times_k E$ for any $\xi \in X(k)$;*
(v) *for every closed point $e \in E$, the fibre V_e of $V_E \to X_E$ over e is irreducible, k-smooth, and non-empty.*

Proof. Case 1: The exact sequence (*) is split.

We proceed as in the proof of [Ha3, Prop. 2.6, case (ii)]. Namely, let $V^* \to \Sigma^*$, $V^o \to X^o$, and B'^o be as in the conclusion of Lemma 3.2. Since the connected normal G-Galois cover $V^* \to \Sigma^*$ is of finite presentation, it descends to a regular $k[t]$-algebra $R \subset k[[t]]$ of finite type over $k[t]$. That is, for some such algebra R, if we let $A = R[t^{-1}]$ and $E = \mathrm{Spec}(A)$, then the following exist:

(1) a connected normal projective R-scheme Σ_R such that $\Sigma_R \times_R E$ is isomorphic to $X_E = X \times_k E$;
(2) a set $B'_E = \{\eta_{1,E}, \ldots, \eta_{n,E}\}$ of n pairwise disjoint E-points of X_E that do not meet $(B \cup \{\xi_0\}) \times E$, and that satisfy $B'_E \times_E \Omega = B'^o$; and
(3) an irreducible normal projective R-scheme V_R together with a G-Galois covering morphism $V_R \to \Sigma_R$ that induces $V^* \to \Sigma^*$ over $k[[t]]$, and such that $V_E = V_R \times_R E$ is regular and satisfies (i) - (iv).

It remains to verify (v) of the Proposition. Since V_R induces V^*, part (v) of Lemma 3.2 implies that the fibre of V_R over $(t = 0)$ is connected and generically smooth. Moreover V^* is normal. Applying [Ha2,Proposition 5] to $V_R \to \mathrm{Spec}(R)$, and letting ε be the point $(t = 0)$, it follows that for all k-points e in a dense open subset E' of $\mathrm{Spec}(R)$, the fibre V_e is irreducible. We may assume that E' is a basic open subset $\mathrm{Spec}(A')$ of $E = \mathrm{Spec}(R) - (t = 0)$; thus $A' = A[f^{-1}]$ for some non-zero $f \in A$. Replacing A by A', and $V_E \to X_E$ by the pullback over E', we obtain condition (v) as well. (Alternatively, we could have used the Bertini-Noether Theorem [FJ, Propositions 8.8, 9.29] instead of [Ha2,Proposition 5].)

Case 2: B is non-empty.

Let $U_0 \to X - B$ be the restriction of $U \to X$ over $X - B$. This is an H-Galois unramified cover, and it corresponds to a surjective homomorphism $\alpha : \pi_1(X - B) \to H$. Since B is non-empty, the k-curve $X - B$ is affine and so has cohomological dimension 1 [Se, Prop.1]. Thus there is a lifting $\tilde{\alpha} : \pi_1(X - B) \to G$ of α, i.e. a (not necessarily surjective) homomorphism $\tilde{\alpha}$ such that $\nu \circ \tilde{\alpha} = \alpha$, where $\nu : G \to H = G/N$ is the quotient map. Let $J \subset G$ be the image of $\tilde{\alpha}$, and let $M = J \cap N$. Let $W_0 \to X - B$ be the J-Galois étale cover corresponding to the surjection $\tilde{\alpha} : \pi_1(X - B) \to J$, and let $W \to X$ be its completion to a J-Galois cover of smooth complete k-curves. Then $H = J/M$, and $W/M \approx U$ as H-Galois covers of X.

Let Γ be the semi-direct product $N \rtimes J$, where the action of J on N in Γ is taken to be the same as the conjugation action of J on N in G. Then there is a surjective homomorphism $\Gamma \to G$ given by taking $N \subset \Gamma$ to $N \subset G$ by the identity map, and taking $J \subset \Gamma$ to $J \subset G$ by the identity map. (This is a well-defined homomorphism because of the way that Γ was defined as a semi-direct product.) Let N_1 be the kernel of $\Gamma \to G$, and let N_2 be the kernel of $\Gamma \to H$. Thus $N_2/N_1 \approx N$.

Applying the result in Case 1, we obtain a connected Γ-Galois cover $\tilde{V}_E \to X$ of smooth k-curves, and a set B', such that conditions (i) - (v) of the proposition are satisfied with V_E replaced by $\tilde{V}_E$, U replaced by W, G replaced by Γ, and H replaced by J. Let $V_E = \tilde{V}_E/N_1$. Then the G-Galois cover $V_E \to X$, together with the set B'_E, will satisfy conditions (i) - (v) of the proposition. (Note in particular that condition (iii) is preserved when passing from Γ to G, because the quotient map $\Gamma \to G$ is injective on $N \subset \Gamma$.) $\square$

Remarks. (a) As in the remark after Lemma 3.2, we may, in the split case of Proposition 3.3, alter the statement of 3.3 by replacing condition (iii) by

(iii)′ for every closed point $e \in E$, the fibre $V_e \to X$ is at most tamely ramified over $B'_e = B'_E \cap (X \times \{e\})$.

Also in the split case, we may strengthen 3.3 by adding a condition

(vi) for every closed point $e \in E$, the N-Galois cover $V_e \to V_e/N \approx U$ (cf. (i)) is unramified at the points lying over B.

Namely, by the remarks after Lemma 3.2, the corresponding condition(s) can be made to hold in the split case for $V^o \to X^o$ over Ω, and in the passage to E we may demand the analogous condition $\text{(iii)}'_E$ [resp. (vi)_E]. The specialization to e will then satisfy (iii)′ [resp. (vi)] above.

(b) See also the remark after Theorem 4.1 concerning another variant of the above result and the three following, in terms of embedding problems. $\square$

Lemma 3.4. *In the situation of Proposition 3.3, let $i_1, \ldots, i_m$ be the values of $i > 0$ satisfying (iii) of Proposition 3.3. Let $\beta_i = \mathrm{pr}_X \circ \eta_{i,E} : E \to X$ for $i = 1, \ldots, n$, where $\mathrm{pr}_X : X_E = X \times_k E \to X$ is the projection onto the first factor. Let $\beta = (\beta_{i_1}, \ldots, \beta_{i_m}) : E \to X^{(m)}$, where $X^{(m)}$ is the mth symmetric power of X.*

(a) For every $e \in E$, the fibre $V_e \to X$ of $V_E \to X_E$ over e is a connected G-Galois cover of smooth k-curves satisfying

(i) *$V_e/N \approx U$ as H-Galois covers of X;*

(ii) *$V_e \to X$ is étale away from $B \cup \{\xi_0, \beta_{i_1}(e), \ldots, \beta_{i_m}(e)\}$, where the second set consists of $m+1$ distinct points, none of which lies in B; and*

(iii) *the inertia groups of $V_e \to X$ are non-trivial over ξ_0, and over $\beta_{i_j}(e)$ for all $j = 1, \ldots, m$.*

(b) Each β_{i_j} is a dominating morphism from E to X, and β is a dominating morphism from E to a subvariety $Y \subset X^{(m)}$, where $\dim(Y) \geq 1$ if $n > 0$.

(c) If $e, e' \in E$ satisfy $\beta(e) \neq \beta(e')$, then the covers $V_e \to X$ and $V'_e \to X$ are non-isomorphic.

Proof. (a) By Proposition 3.3(v), V_e is connected, smooth, and non-empty. Part (i) of (a) then follows from Proposition 3.3(i). Part (ii) follows from (ii) of Proposition

3.3 together with the fact that the E-points $\eta_{i,E}$ of Proposition 3.3 are disjoint. Part (iii) follows from 3.3(iii) and from the definition of the β_{i_j}'s, together with the fact that inertia groups either stay the same or become larger upon specialization.

(b) By Proposition 3.3(iv), each $\beta_{i_j} : E \to X$ is non-constant. But X is an irreducible curve; so β_{i_j} is a dominating morphism. Let $Y \subset X^{(m)}$ be the closure of the image of β. Thus $\beta : X^{(m)} \to Y$ is dominating. If $n > 0$ then Proposition 3.3(iii) implies that $m \geq 1$, and so in particular β_{i_1} exists. The dominating morphism $\beta_{i_1} : E \to X$ factors through β, and so $\dim(Y) \geq 1$.

(c) This is immediate from (ii) and (iii) of part (a), since covers with distinct branch loci are distinct. □

Theorem 3.5. *Under Hypotheses (3.1), assume either that the exact sequence (*) is split or that B is non-empty. Let S be a finite subset of $X - B$, and let $\xi_0 \in X - (B \cup S)$.*

(a) Then there is a smooth connected G-Galois cover $Z \to X$ such that $Z/N \approx U$ as H-Galois covers of X; such that $Z \to X$ is ramified only over $B \cup \{\xi_0\} \cup B'$, for some subset $B' \subset X - S$ consisting of at most n points; and such that the inertia groups over ξ_0 are non-trivial.

(b) If $n > 0$, then up to isomorphism there are exactly κ such covers $Z \to X$, where κ is the cardinality of k.

Proof. (a) Let E, β_i, β be as in Lemma 3.4. Since each $\beta_{i_j} : E \to X$ is dominating and since X is an irreducible curve, we have that $D_j = \beta_{i_j}^{-1}(B \cup \{\xi_0\} \cup S)$ is a proper closed subset of E. Hence so is $D = D_1 \cup \cdots \cup D_m$. By definition of D, each $\beta_{i_j}(E - D)$ is disjoint from $B \cup \{\xi_0\} \cup S$. The desired assertion now follows from part (a) of Lemma 3.4, by taking $Z = V_e$ for any $e \in E - D$, and using that $m \leq n$.

(b) Let Y be as in Lemma 3.4(b). Let $D \subset E$ be as in part (a), and let β' be the restriction of β to $E - D$. Now $\dim(Y) \geq 1$, and $\beta' : E - D \to Y$ is a dominating morphism. So the cardinality of the image of β' is κ, and there is a subset $\Sigma \subset (E - D)(k)$ of cardinality κ such that $\beta(e) \neq \beta(e')$ for $e \neq e'$ in Σ. (Namely, just pick one point in each non-empty fibre of β'.) By Lemma 3.4(c), distinct points in Σ yield distinct G-Galois covers $Z \to X$ as in (a) above. Thus there are at least κ non-isomorphic choices for $Z \to X$. But the opposite inequality holds by set theory, since there are at most κ non-isomorphic finite covers of X over k. □

Remarks. (a) Theorem 3.5 can be strengthened in the split case, because of Remark (a) after Proposition 3.3. Namely, using (vi) of that remark, we may require in 3.5(a) and (b) that $Z \to Z/N \approx U$ is unramified at the points lying over B. Also, using the replacement of (iii) by (iii)$'$ in that remark, we see that we may assert that $Z \to X$ is at most tamely ramified away from $B \cup \{\xi_0\}$, in Theorem 3.5(a). But by doing this we lose (iii) of 3.3, and hence also (b) of 3.4. Since 3.4(b) was used in the proof of 3.5(b), we cannot also assert this tameness in 3.5(b).

(b) The proof of 3.2, and hence that of 3.5, used the assertion of Abhyankar's conjecture [Ha3, Theorem 6.2]. Without relying on that result, it is nevertheless possible to prove a weaker version of Theorem 3.5, which would still be sufficient for use in Theorem 4.1 below (via a correspondingly weakened 3.6). Namely, if s is the number of Sylow p-subgroups of N, then we can show the assertion obtained by allowing B' to have at most $n+s$ points (rather than at most n points) in the statement of 3.5. This follows from the result obtained by allowing B'^* to have $n+s$ points in 3.2.

To show that latter variant without Abhyankar's conjecture, we need, in the proof of 3.2, to show that there is an N-Galois cover of the line branched at $s+n+1$ points (rather than $n+1$ points, as before). By [Gr1, XIII, Cor. 2.12], there is an $N/p(N)$-Galois cover of the line branched at $n+1$ points, and since the complement of those points has cohomological dimension 1 [Se, Prop.1], this lifts to an M-Galois cover of the line with the same branch locus, where $M \subset N$ is a subgroup such that N is generated by M and $p(N)$ (or equivalently, by M and the s Sylow p-subgroups of N). The result now follows by [Ha2, Theorem 2], which allows the addition of new p-inertia to covers at new branch points, and the corresponding enlargement of the Galois group. Namely, by adding s new branch points (corresponding to the Sylow p-subgroups of N) and enlarging the group from M to N, we can construct an N-Galois cover of the line having $s+n+1$ branch points. This gives the desired variant of 3.2 (and hence the variant of 3.5). $\square$

Theorem 3.5(b) required that $n > 0$. But if we do not insist on choosing in advance one of the extra branch points ξ_0, then (b) holds even if $n = 0$. Namely:

Theorem 3.6. *Under Hypotheses (3.1), assume either that the exact sequence (*) is split or that B is non-empty, and let S be a finite subset of $X - B$.*

(a) Then there is a smooth connected G-Galois cover $Z \to X$ such that $Z/N \approx U$ as H-Galois covers of X, and such that $Z \to X$ is ramified only over $B \cup B'$, for some subset $B' \subset X - S$ consisting of at most $n+1$ points.

(b) Up to isomorphism there are exactly κ such covers $Z \to X$, where κ is the cardinality of k.

Proof. Part (a) is immediate from 3.5(a), by including ξ_0 as an additional point in B'. To show part (b), let C be the set of isomorphism classes of such covers. By 3.5(a), for each $\xi \in X - (B \cup S)$ we may choose a cover $Z_\xi \to X$ satisfying the conclusion of 3.5(a) with $\xi_0 = \xi$. This cover is ramified non-trivially over ξ, and is otherwise unramified away from $B \cup B'_\xi \subset X$, where $B'_\xi \subset X - S$ is a set of at most n points. Thus if $\xi, \xi' \in X - (B \cup S)$ are distinct, then the covers $Z_\xi \to X$ and $Z_{\xi'} \to X$ cannot be isomorphic unless $\xi' \in B'_\xi$. So the map $X - (B \cup S) \to C$ given by $\xi \mapsto [Z_\xi \to X]$ is finite-to-one. Thus the cardinality of C is at least κ, and the opposite inequality follows as in 3.5(b). $\square$

Remarks. (a) In the case that (*) is split and B is empty, the $n+1$ in Theorem 3.6 is sharp. To see this, let G be a finite group such that the smallest generating set of $G/p(G)$ has n elements. Take $N = G$, so that (*) is split, H is trivial, $U = X$, and B is empty. Then the theorem asserts the existence of a G-Galois cover of X branched only at B'. By Abhyankar's conjecture [Ha3, Theorem 6.2], such a cover exists if and only if B' contains at least $n+1$ elements.

(b) We can also consider the weaker assertion obtained from 3.6 by dropping the condition that $Z/N \approx U$. If B is empty, then the $n+1$ in this weaker assertion is still sharp, by the example in Remark (a). But if B is non-empty, then the $n+1$ in this weaker statement may be replaced by n (which is then sharp). Namely, if B consists of $r > 0$ points, and X has genus g, then $H/p(H)$ is generated by $2g+r-1$ elements (since $H \in \pi_A(X-B)$). Hence $G/p(G)$ is generated by $2g+r+n-1$ elements (using the definition of n). Thus by Abhyankar's conjecture, $G \in \pi_A(X-B-B')$ for any subset $B' \subset X-B$ consisting of n elements (but not $n-1$ in general, since the smallest generating set of $G/p(G)$ may have exactly $2g+r+n-1$ elements).

Note that it is indeed possible for this weaker (existence) assertion to hold in a situation where the stronger (lifting) one fails. For example, suppose that (*) is split; that G is a quasi-p-group; that N is of the form $\mathbf{Z}/l^m$ for some prime l; and that $X = \mathbf{P}^1$ and $B = \{\infty\}$. Then by Abhyankar's conjecture for the affine line [Ra], there exists a G-Galois cover $Z \to X$ branched only at B, but not necessarily one such that $Z/N \approx U$. Cf. [Se, sect. 5,6], where a necessary and sufficient condition is given for this latter property. On the other hand, [Se, sect. 7] shows that such a lift Z *will* necessarily exist if $l = p$.

(c) Theorem 3.6 can be strengthened in the case that p does not divide the order of G (e.g. if k has characteristic 0), by

(i) dropping the requirement that B be non-empty if (*) is non-split;
(ii) replacing $n+1$ by n if B is non-empty; and
(iii) specifying in advance the points of B'.

Here (i) follows from (ii), since if $B = \emptyset$ then we may add a point to B and then use (ii). Parts (ii) and (iii) follow from the fact that the prime-to-p part $\pi_1^{p'}(X-A)$ is a free-pro-p'-group on $2g+s-1$ generators, if X is a projective curve of genus g and $A \subset X$ consists of $s > 0$ points [Gr1, XIII, Cor. 2.12].

(d) Theorem 3.6 leaves open the question of whether the conclusion is also true in the case that (*) is not split and B is empty – although it is true in characteristic 0, by Remark (c) above.

(e) The remarks after 3.5 also carry over to 3.6. $\square$

Remarks (a) - (c) above suggest the question of whether the $n+1$ in 3.6 is sharp when $B \neq \emptyset$ (for general G and p), or whether it may be replaced by n. As a special case, when $n = 0$, we obtain the following question (where $X_0 = X - B$ above):

Question 3.7. If $1 \to N \to G \to H \to 1$ is an exact sequence of finite groups with N a quasi-p-group, and if $U_0 \to X_0$ is a connected unramified H-Galois cover of smooth affine k-curves, is there a connected unramified G-Galois cover $Z_0 \to X_0$ such that $Z_0/N \approx U_0$?

In terms of fundamental groups, Question 3.7 can be rephrased as follows: Let X_0 be an affine k-curve, let G be a finite group, let N be a normal quasi-p-subgroup of G, and let $\gamma : \pi_1(X_0) \to G/N$ be a surjective group homomorphism. Then does γ lift to a surjective group homomorphism $\beta : \pi_1(X_0) \to G$? This is an "embedding problem," in the terminology of Section 4 below.

Section 4. Embedding and freeness

This section contains two related theorems: Theorem 4.1 asserts that in the birational and semi-local cases, the fundamental groups of curves have (many) solutions to every non-trivial finite embedding problem. Theorem 4.4 says that in these situations, the fundamental groups are free profinite groups, of rank equal to the cardinality of the coefficient field k.

As before, let k be an algebraically closed field of characteristic $p \geq 0$. Let X be a smooth projective k-curve with function field K, and let S be a finite subset of X (possibly empty). Let K^{sep} be the separable closure of K. We let $\Pi_{K,S}$ denote the Galois group $\text{Gal}(L_S/K)$, where L_S is the maximal algebraic extension of K (contained in K^{sep}) that is unramified over the places of K corresponding to the points of S. In the case that S is empty, we will also write $\Pi_{K,S} = \Pi_K$. In that case, Π_K is the absolute Galois group of K, i.e. the Galois group $\text{Gal}(K^{\text{sep}}/K)$.

The group $\Pi_{K,S}$ can be reinterpreted in terms of fundamental groups as follows. Let $\mathcal{O}_{X,S}$ be the semi-local ring of X at S; i.e.

$$\mathcal{O}_{X,S} = \{f \in K \mid f \text{ is regular at the points of } S\}.$$

Let $X_S = \text{Spec}(\mathcal{O}_{X,S})$, the "semi-localization of X at S." Then $\Pi_{K,S} = \pi_1(X_S)$ (taken with respect to the K^{sep}-valued base point of X_S corresponding to the inclusion of $\mathcal{O}_{X,S}$ into K^{sep}). In particular, if S is empty then we have $\Pi_K = \pi_1(\text{Spec}(K))$; and if $S = \{s\}$ is a single point, then $\mathcal{O}_{X,S} = \mathcal{O}_{X,s}$ (the usual local ring of X at the point s), and $\Pi_{K,S} = \pi_1(\text{Spec}(\mathcal{O}_{X,s}))$.

If Π is any profinite group, then an *embedding problem* for Π is a pair of surjective homomorphisms $(\gamma : \Pi \to H,\ \alpha : G \to H)$ of profinite groups. The embedding problem is *finite* if G is a finite group, and is *trivial* if α is an isomorphism. A *weak solution* [resp. *proper solution*] to the embedding problem is a homomorphism [resp. surjective homomorphism] $\beta : \Pi \to G$ such that $\alpha\beta = \gamma$.

Theorem 4.1. *Let S be a finite subset of a smooth projective k-curve X with function field K.*

(a) Every finite embedding problem for $\Pi_{K,S}$ has a proper solution.

(b) If such an embedding problem is non-trivial, then the cardinality of the set of proper solutions is equal to the cardinality of k.

Proof. (a) Let $\Pi = \Pi_{K,S}$, and let $(\gamma : \Pi \to H,\ \alpha : G \to H)$ be any finite embedding problem for Π. Letting $N = \ker(\alpha)$, we may identify H with G/N and α with the quotient map $G \to G/N$. The result is immediate if N is trivial, so we may assume that N is non-trivial. Choose a generating set Σ for $N/p(N)$, consisting of $n \geq 0$ generators. By Galois theory, $\gamma : \Pi \to H$ corresponds to an H-Galois field extension of K that is unramified over the places corresponding to S, or equivalently to a connected H-Galois cover $U \to X$ of smooth k-curves that is unramified over S. Let B be a non-empty finite subset of X that contains the branch locus of $U \to X$ and is disjoint from S. By Theorem 3.6(a), there is a smooth connected G-Galois cover $Z \to X$ such that $Z/N \approx U$ as H-Galois covers of X, and such that $Z \to X$ is ramified only over B and over at most $n+1$ other points, none of which lies in S. The G-Galois cover $Z \to X$ corresponds to a surjective homomorphism $\beta : \Pi \to G$ such that $\alpha\beta = \gamma$. Thus the embedding problem has a proper solution.

(b) By Theorem 3.6(b), there are $\text{card}(k)$ choices of $Z \to X$ in the proof of (a). Distinct choices correspond to distinct solutions to the embedding problem, and so the result follows. $\square$

Remark. By using the terminology of embedding problems, it is possible to reformulate the results in section 3, and their relationship to Theorem 4.1. First, note that the Hypotheses (3.1) yield an embedding problem $(\gamma : \pi_1(X-B) \to H, \alpha : G \to H)$. Next, observe that the proof of Proposition 3.3, Case 2, shows that we may replace the hypothesis of (*) being split or B non-empty by the assumption that the embedding problem has a weak solution (and by the same proof, this is in fact a weaker hypothesis). So the same carries over to 3.4, 3.5, and 3.6. Hence we obtain the following variation of 3.6:

Let $1 \to N \to G \to H \to 1$ be an exact sequence of finite groups, with N non-trivial, and $N/p(N)$ generated by n elements ($n \geq 0$). Let B, S be disjoint finite subsets of a smooth projective k-curve X. If an embedding problem $(\gamma : \pi_1(X-B) \to H, \alpha : G \to H)$ has a weak solution, then there is a subset $B' \subset X - S$ containing at most $n+1$ points, such that the induced embedding problem $(\tilde{\gamma} : \pi_1(X-(B \cup B')) \to H,\ \alpha : G \to H)$ has exactly $\mathrm{card}(k)$ *distinct proper solutions.*

The relationship to Theorem 4.1 can then be seen by observing that $\Pi_{K,S}$ is the inverse limit of the profinite groups $\pi_1(X-B)$, as B ranges over the non-empty finite subsets of $X - S$. $\square$

If Π is any profinite group, and I is a subset of Π, then I is called a *generating set* of Π if no proper closed subgroup of Π contains I. A generating set *converges to* 1 if each open subgroup of Π contains all but finitely many elements of I. The *rank* of a profinite group Π is the least cardinality of a generating set that converges to 1.

For any set I, let F_I be the free group on the generating set I. The *free profinite group* $\hat{F}_I$ on I is the inverse limit of the quotients F_I/N, where N ranges over the normal subgroups of finite index that contain all but finitely many elements of I. Thus I is a generating set of $\hat{F}_I$ converging to 1, and the rank of $\hat{F}_I$ is the cardinality of I. Since $\hat{F}_I$ depends, up to isomorphism, only on the cardinality of I, we also write $\hat{F}_\kappa$ if κ is the cardinality of I.

According to a result of Iwasawa ([Iw,p.567]; cf. also [FJ,Cor.24.2]), if Π is a profinite group of countably infinite rank, then Π is a free profinite group if and only if every finite embedding problem for Π has a proper solution. As a result, we obtain the following result, in which (b) is the function field version of Shafarevich's conjecture (cf. section 1):

Corollary 4.2. *Let k be the algebraic closure of $\mathbf{F}_p$, let X be a smooth connected projective k-curve, let K be the function field of X, and let S be a finite subset of X.*

(a) Then $\Pi_{K,S}$ is a free profinite group on countably many generators.

(b) In particular, the absolute Galois group Π_K of K is a free profinite group on countably many generators.

Proof. (a) Let $\Pi = \Pi_{K,S}$ and $r = \mathrm{rank}(\Pi)$. If r is finite, and G is any finite group of rank $> r$, then there is no surjective homomorphism $\Pi \to G$, and hence the embedding problem $(\Pi \to 1, G \to 1)$ cannot have a proper solution. This contradicts Theorem 4.1(a), and so actually r is infinite. But since k is countable, K has at most countably many finite extensions, and hence the rank of Π is at most countable. So the rank is countably infinite. The result now follows from 4.1(a) and Iwasawa's theorem cited above.

(b) This is just the special case that S is empty. □

Iwasawa's theorem fails for profinite groups of uncountable rank [Ja, Example 3.1]. That is, there are profinite groups of uncountable rank for which every finite embedding problem has a proper solution, yet which are not free. Nevertheless Corollary 4.2 does generalize to arbitrary algebraically closed fields k. Namely, if κ is the cardinality of k, then we show below that $\Pi_{K,S}$ is a free profinite group of rank κ. To see this, we need the following lemma:

Lemma 4.3. [Ja, Lemma 2.1] *Let κ be an infinite cardinal number, and let F be a profinite group of rank κ. Then F is isomorphic to $\hat{F}_\kappa$ if and only if each non-trivial finite embedding problem for F has exactly κ proper solutions.*

Using this, we obtain the desired freeness result, which generalizes Corollary 4.2:

Theorem 4.4. *Let k be an algebraically closed field of cardinality κ. Let X be a smooth connected projective k-curve, let K be the function field of X, and let S be a finite subset of X. Then $\Pi_{K,S}$ is a free profinite group on κ generators.*

Proof. Immediate from Theorem 4.1(b) and Lemma 4.3. □

References

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

[Be] G. V. Belyi, *On extensions of the maximal cyclotomic field having a given classical Galois group*, Journal für die reine und angewandte Mathematik **341** (1980), 147–158.

[FJ] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin-Heidelberg, 1986.

[FV] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC field*, Annals of Math. **135** (1992), 469–481.

[Gr1] A. Grothendieck, *Revêtements étales et groupe fondamental*, SGA 1, Lecture Notes in Math., vol. 224, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[Gr2] A. Grothendieck, *Esquisse d'un programme*, 1984 manuscript.

[Ha1] D. Harbater, *Moduli of p-covers of curves*, Communications in Algebra **8** (1980), 1095–1122.

[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*, Inventiones Math. **117** (1994), 1–25.

[Ha4] D. Harbater, *Galois groups with prescribed ramification*, 1993 manuscript, to appear in Arithmetic Geometry (N. Childress and J. Jones, eds.), Proceedings of a conference at Arizona State Univ.; AMS Contemporary Math. series.

[Iw] K. Iwasawa, *On solvable extensions of algebraic number fields*, Annals of Math. **58** (1953), 548–572.

[Ja] M. Jarden, *On free profinite groups of uncountable rank*, 1993 manuscript, this volume.

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

[Ne] J. Neukirch, *Kennzeichnung der p-adischen und endlichen algebraischen Zahlkörper*, Inventiones Math. **6** (1969), 269–314.

[Po1] F. Pop, *On Grothendieck's conjecture of birational anabelian geometry*, Annals of Math **138** (1994), 145–182.

[Po2] F. Pop, *Half Riemann existence theorem with Galois action*, 1992 manuscript, to appear in Algebra and Number Theory (G. Frey and J. Ritter, eds.), de Gruyter Proceedings in Mathematics, Berlin-New York.

[Po3] F. Pop, *The geometric case of a conjecture of Shafarevich*, 1993 manuscript, Heidelberg.

[Ra] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d' Abhyankar*, Inventiones Math. **116** (1994), 425–462.

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

[St] K. Stevenson, *Fundamental groups of projective curves in characteristic p*, Ph. D. thesis, University of Pennsylvania, 1994.

[Uc] K. Uchida, *Isomorphisms of Galois groups of algebraic function fields*, Annals of Math. **106** (1977), 589–598.

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

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