THE FUNDAMENTAL GROUP OF AFFINE CURVES IN POSITIVE CHARACTERISTIC

MANISH KUMAR

Abstract. It is shown that the commutator subgroup of the fundamental group of a smooth irreducible affine curve over an uncountable algebraically closed field k of positive characteristic is a profinite free group of rank equal to the cardinality of k.

1. Introduction

The algebraic (étale) fundamental group of an affine curve over an algebraically closed field k of positive characteristic has a complicated structure. It is an infinitely generated profinite group, in fact the rank of this group is same as the cardinality of k. The situation when k is of characteristic zero is simpler to understand. The fundamental group of a smooth curve over an algebraically closed field of characteristic zero is just the profinite completion of the topological fundamental group ([SGA1, XIII, Corollary 2.12, page 392]). In positive characteristic as well, Grothendieck gave a description of the prime-to-p quotient of the fundamental group of a smooth curve which is in fact analogous to the characteristic zero case. From now on, we shall assume that the characteristic of the base field k is $p > 0$. Consider the following exact sequence for the fundamental group of a smooth affine curve C.

$$1 \to \pi_1^c(C) \to \pi_1(C) \to \pi_1^{ab}(C) \to 1$$

where $\pi_1^c(C)$ and $\pi_1^{ab}(C)$ are the commutator subgroup and the abelianization of the fundamental group $\pi_1(C)$ of C respectively. In [Ku2], a description of $\pi_1^{ab}(C)$ was given [Ku2, Corollary 3.5] and it was also shown that $\pi_1^c(C)$ is a free profinite group of countable rank if k is countable [Ku2, Theorem 1.2]. In fact some more exact sequences with free profinite kernel like the above were also observed [Ku2, Theorem 7.1]. Later using somewhat similar ideas and some profinite group theory Pacheco, Stevenson and Zalesskii claim to find a condition for a closed normal subgroup of $\pi_1(C)$ to be profinite free of countable rank [PSZ] but unfortunately there seems to be a gap in their argument as Example 3.16 suggests.

A consequence of the main result of this paper generalizes [Ku2, Theorem 1.2] to uncountable fields.

Theorem 1.1. *Let C be a smooth affine curve over an algebraically closed field k (possibly uncountable) of characteristic p then $\pi_1^c(C)$ is a free profinite group of rank* $\mathrm{card}(k)$.

This answers a question of Harbater and Zalesskii who had asked the author in an email communication if the above is true or at least whether there exist a closed subgroup of $\pi_1(C)$ which is free of rank same as $\mathrm{card}(k)$. Let $P_g(C)$ be the intersection of all index p normal subgroups of $\pi_1(C)$ corresponding to étale covers of C of genus at least g (see Definition 3.4). In the main theorem (Theorem 3.6) it is shown that if Π is a closed normal subgroup of $\pi_1(C)$ of rank card(k) such that $\pi_1(C)/\Pi$ is abelian, $\Pi \subset P_g(C)$ for some $g \geq 0$ and for every finite simple group S there exist a surjection from Π to card(k) copies of S then Π is profinite free.

As a consequence we get the following result.

Corollary 1.2. *Let Π be a closed normal subgroup of $P_g(C)$ for some $g \geq 0$. If rank of $P_g(C)/\Pi$ is strictly less than* card(k) *then Π is profinite free of rank* card(k).

Proof. Note that $P_g(C)$ is a profinite free group of rank card(k) by Corollary 3.15. So the corollary follows from Melnikov's result on freeness of a normal subgroup of a profinite free group ([RZ, Theorem 8.9.4]). □

The existence of wildly ramified covers is the primary reason why so little is known about fundamental groups of affine curves. More precisely, there is a positive dimensional configuration space of p-cyclic Artin-Schreier covers of the affine line (see [Pri]), and while this family is relatively well understood, the structure of $\pi_1(\mathbb{A}^1)$ remains elusive. This is because we do not know how the various wildly ramified covers fit in with the tamely ramified covers in the tower of covers over $\mathbb{A}^1$. This also suggests that the fundamental group of an affine curve in positive characteristic contains much more information about the curve than in characteristic zero case. In fact Harbater and Tamagawa have conjectured that the fundamental group of a smooth affine curve over an algebraically closed field of characteristic p should determine the curve completely (as a scheme) and in particular one should be able to recover the base field. Harbater and Tamagawa have shown some positive results supporting the conjecture. See [Ku1, Section 3.4], [Ha5], [Ta1] and [Ta2] for more details.

The above theorem on the commutator subgroup can also be interpreted as an analogue of the Shafarevich's conjecture for global fields. The Shafarevich conjecture says that the commutator subgroup of the absolute Galois group of the rational numbers $\mathbb{Q}$ is a profinite free group of countable rank. David Harbater [Ha3], Florian Pop [Pop] and later Dan Haran and Moshe Jarden [HJ] have shown, using different patching methods, that the absolute Galois group of the function field of a curve over an algebraically closed field is profinite free of the rank same as the cardinality of the base field. See [Ha4] for more details on these kind of results and questions.

Though the profinite group structure of the fundamental group of a smooth affine curve is not well understood, a 1994 proof of Abhyankar's 1957 conjecture provides a characterization for a finite group to be a quotient of the fundamental group of a smooth affine curve. For a finite group G, let $p(G)$ denote the subgroup of G generated by all the Sylow-p subgroups of G. The conjecture was proved by Raynaud for the affine line [Ray] and by Harbater in general [Ha1].

Theorem 1.3. *(Harbater, Raynaud) Let C be a smooth affine curve of genus g over an algebraically closed field of characteristic p. Let D be the smooth compactification of C and* card$(D \setminus C) = n + 1$. *Then a finite group G is a quotient of $\pi_1(C)$ if and only if $G/p(G)$ is generated by $2g + n$ elements.*

Section 2 consists of definitions and results on profinite groups. This section also reduces Theorem 1.1 to solving certain embedding problems. The last section consists of solutions to these embedding problems.

Acknowledgments

Thanks are due to David Harbater for some useful discussions regarding the uncountable case. Hilaf Hasson pointed out some typographical errors in a preliminary version. I am also grateful to an anonymous referee of an earlier version of this manuscript for pointing out a critical gap and various suggestion. Thanks are also due to the current referee for some suggestions to improve the presentation of the paper. Lior Bary-Soroker encouraged me to include Corollary 1.2 for which I am thankful to him. A part of this work was done when the author was at Universität Duisburg-Essen where the author was supported by SFB/TR45 grant.

2. Profinite group theory

Notation and contents of this section are inspired from [RZ] and [FJ]. For a finite group G and a prime number p, let $p(G)$ denote the subgroup of G generated by all the p-Sylow subgroups of G. The subgroup $p(G)$ is called the *quasi-p* subgroup of G. If $G = p(G)$ then G is called a quasi-p group.

A family of finite groups $\mathcal{C}$ is said to be *almost full* if it satisfies the following conditions:

(1) A nontrivial group is in $\mathcal{C}$.
(2) If G is in $\mathcal{C}$ then every subgroup of G is in $\mathcal{C}$.
(3) If G is in $\mathcal{C}$ then every homomorphic image of G is in $\mathcal{C}$.
(4) If $G_1, G_2, \ldots, G_n$ are in $\mathcal{C}$ then the product $G_1 \times G_2 \times \ldots \times G_n$ is in $\mathcal{C}$.

Moreover $\mathcal{C}$ is called a *full* family if it is closed under extensions, i.e., if G_1 and G_3 are in $\mathcal{C}$ and there is a short exact sequence

$$1 \to G_1 \to G_2 \to G_3 \to 1$$

then G_2 is in $\mathcal{C}$.

Example. The family of all finite groups is full. For a prime number p, the family of all p-groups is full.

Let $\mathcal{C}$ be an almost full family of finite groups. A *pro-$\mathcal{C}$* group is a profinite group whose finite quotients lie in $\mathcal{C}$. Equivalently, it is an inverse limit of an inverse system of groups contained in $\mathcal{C}$. If $\mathcal{C}$ is the family of all p-groups then pro-$\mathcal{C}$ groups are also called pro-p groups.

Let m be an infinite cardinal or a positive integer. A subset I of a profinite group Π is called a *generating set* if the smallest closed subgroup of Π containing I is Π itself. A generating set I is said to be converging to 1 if every open normal subgroup of Π contains all but finitely many elements of I. The *rank* of Π is the infimum of the cardinalities of all the generating sets of Π converging to 1.

Let m be an infinite cardinal, I be a set of cardinality m and F_I be the free group over I. A profinite group Π is called a *free* pro-$\mathcal{C}$ group of rank m if Π is isomorphic to the inverse limit $\hat{F}_I$ of the inverse system obtained by taking quotients of F_I by finite index normal subgroups K which contain all but finitely many elements of I and $F_I/K \in \mathcal{C}$. The image of I under the natural map $F_I \to \hat{F}_I \cong \Pi$ is a generating set converging to 1. When $\mathcal{C}$ is the family of all finite groups then free pro-$\mathcal{C}$ groups are same as free profinite groups.

For a group Π and a finite group S, let $R_S(\Pi)$ denote the maximal cardinal m such that there exist a surjection from Π to S^m. The intersection of all the proper normal maximal subgroups of Π is denoted by $M(\Pi)$.

An *embedding problem* consists of surjections $\phi\colon \Pi \twoheadrightarrow G$ and $\alpha\colon \Gamma \twoheadrightarrow G$

$$\begin{tikzcd} & & & \Pi \arrow[d, "\phi"] \arrow[dl, dashed, "\psi"'] & \\ 1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r, "\alpha"'] & G \arrow[r] \arrow[d] & 1 \\ & & & 1 & \end{tikzcd}$$

where G, Γ and Π are groups and $H = \ker(\alpha)$. It is also sometimes called an embedding problem for Π. It is said to have a *weak solution* if there exists a group homomorphism ψ which makes the diagram commutative, i.e., $\alpha\circ\psi = \phi$. Moreover, if ψ is an epimorphism then it is said to have a *proper solution* (or a *solution*). It is said to be a finite embedding problem if Γ is finite. An embedding problem is said to be a *split* if there exists a group homomorphism from G to Γ which is a right inverse of α. Two proper solutions ψ_1 and ψ_2 are said to be distinct if $\ker(\psi_1) \neq \ker(\psi_2)$.

Let $\mathcal{C}$ be an almost full family and Π a profinite group of rank m. If every embedding problem for Π

$$\begin{tikzcd} & & & \Pi \arrow[d] \arrow[dl, dashed] & \\ 1 \arrow[r] & \tilde{H} \arrow[r] & \tilde{\Gamma} \arrow[r] & \tilde{G} \arrow[r] \arrow[d] & 1 \\ & & & 1 & \end{tikzcd}$$

with $\tilde{\Gamma}$ a pro-$\mathcal{C}$ group of rank less than or equal to m, $\tilde{G}$ a pro-$\mathcal{C}$ group of rank strictly less than m, $\tilde{H} \in \mathcal{C}$ a minimal normal subgroup of $\tilde{\Gamma}$ and $\tilde{H}$ contained in $M(\tilde{\Gamma})$ has a solution then Π is called *$\mathcal{C}$-homogeneous*. Moreover, if $\mathcal{C}$ is the class of all finite groups then Π is called *homogeneous*.

Note. In view of [RZ, Lemma 3.5.4], the above definition of homogeneous is equivalent to the definitions given in [RZ] and [FJ].

Let m denote an infinite cardinal and $\mathcal{C}$ be an almost full family. The following is an easy generalization of [FJ, Lemma 25.1.5]. The proof is exactly the same but is reproduced here for the sake of completion.

Lemma 2.1. *Let Π be a profinite group such that every nontrivial finite embedding problem $\phi : \Pi \twoheadrightarrow G, \alpha : \Gamma \twoheadrightarrow G$ with Γ in $\mathcal{C}$ and $H = \ker(\alpha)$ a minimal normal subgroup of Γ has m solutions. Let $\tilde{\Gamma}$ be a pro-$\mathcal{C}$ groups with $\mathrm{rank}(\tilde{\Gamma}) \leq m$. Let $\tilde{H} \in \mathcal{C}$ be a minimal normal subgroup of $\tilde{\Gamma}$ such that the quotient $\tilde{G} = \tilde{\Gamma}/\tilde{H}$ has* *rank strictly less than m. Then the following embedding problem has a solution.*

(2.1)
$$\begin{tikzcd}
 & & & \Pi \arrow[dl, dashed] \arrow[d] & \\
1 \arrow[r] & \tilde{H} \arrow[r] & \tilde{\Gamma} \arrow[r, "\tilde{\alpha}"'] & \tilde{G} \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

Moreover, if the existence of solutions to only those embedding problems with $\tilde{H} \subset M(\tilde{\Gamma})$ is desired then the hypothesis can be weakened to the existence of m solutions to finite embedding problems in which $H = \ker(\alpha)$ is contained in $M(\Gamma)$.

Proof. Consider the embedding problem (2.1). Since $\tilde{H} \in \mathcal{C}$, it is finite. So there exist an open normal subgroup N of $\tilde{\Gamma}$ such that $N \cap \tilde{H} = \{1\}$. Taking quotient by N, we get a finite embedding problem

$$\begin{tikzcd}
 & & & \Pi \arrow[dl, dashed] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r, "\alpha"'] & G \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

where $\Gamma = \tilde{\Gamma}/N$, $G = \tilde{G}/\tilde{\alpha}(N)$, the subgroup H of Γ is isomorphic to $\tilde{H}$ and Γ is in $\mathcal{C}$. If we assume that $\tilde{H} \subset M(\tilde{\Gamma})$ then $H \subset M(\Gamma)$ since every maximal normal subgroup of Γ is a quotient of a maximal normal subgroup of $\tilde{\Gamma}$ containing N. The rest of the proof is same as that of [FJ, Lemma 25.1.5]. We have the following scenario:

$$\begin{tikzcd}
\Pi \arrow[drr, "\phi"] \arrow[ddr, dashed] & & \\
\tilde{H} \arrow[r, hook] \arrow[d, equal] & \tilde{\Gamma} \arrow[r, two heads, "\tilde{\alpha}"'] \arrow[d, two heads] & \tilde{G} \arrow[d, two heads] \\
H \arrow[r, hook] & \Gamma \arrow[r, two heads, "\alpha"'] & G
\end{tikzcd}$$

By assumption there exist $\beta : \Pi \twoheadrightarrow \Gamma$ which makes the above diagram commutative. In fact there are m choices for β. If $\ker(\phi) \subset \ker(\beta)$ then β factors through $\tilde{G}$. By [FJ, Lemma 25.1.1], there are at most $\mathrm{rank}(\tilde{G}) < m$ surjections from $\tilde{G}$ to Γ. Hence we can choose β so that $\ker\beta$ does not contain $\ker\phi$. Since $\tilde{\Gamma}$ is the fiber product of $\tilde{G}$ and Γ over G, the maps β and ϕ induce a map $\gamma : \Pi \to \tilde{\Gamma}$ so that the following diagram commutes:

$$\begin{tikzcd}
\Pi \arrow[dr, "\gamma"] \arrow[drr, bend left, "\phi"] \arrow[ddr, bend right, "\beta"'] & & \\
& \tilde{\Gamma} \arrow[r, two heads, "\tilde{\alpha}"'] \arrow[d] & \tilde{G} \arrow[d] \\
& \Gamma \arrow[r, two heads, "\alpha"'] & G
\end{tikzcd}$$

By [FJ, Lemma 24.4.1] there exist a group G' which fits in the following diagram:

$$\begin{tikzcd}
\mathrm{Im}(\gamma) \arrow[r, two heads, "\tilde{\alpha}"] \arrow[d] & \tilde{G} \arrow[d, "\zeta'"'] \arrow[ddr, bend left, two heads] & \\
\Gamma \arrow[r, two heads, "\alpha'"] \arrow[drr, bend right, two heads, "\alpha"'] & G' \arrow[dr, two heads, "\theta"] & \\
& & G
\end{tikzcd}$$

the maps from $\mathrm{Im}(\gamma)$ are the restriction of maps from $\tilde{\Gamma}$ and $\mathrm{Im}(\gamma)$ is the fiber product of $\tilde{G}$ and Γ over G'. Since $H = \ker(\alpha)$ is a minimal normal subgroup of Γ, one of θ or α' is an isomorphism. If α' where an isomorphism then $\beta = \alpha'^{-1} \circ \zeta' \circ \phi$ contradicting $\ker(\phi)$ is not a subset of $\ker(\beta)$. Hence θ is an isomorphism. So again by [FJ, Lemma 24.4.1], $\mathrm{Im}(\gamma) = \tilde{\Gamma}$ solves the embedding problem (2.1). $\square$

The following proposition may be attributed to Melnikov and Chatzidakis (cf. [HS, Remark 2.2]) and a variant of it appeared in [HS, Theorem 2.1]

Theorem 2.2. *Let Π be a profinite group of rank m. Suppose:*

(1) *Π is projective.*
(2) *Every nontrivial finite embedding problem*

$$\begin{tikzcd}
& & & \Pi \arrow[dl, dashed] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r] & G \arrow[r] \arrow[d] & 1 \\
& & & 1 &
\end{tikzcd} \tag{2.2}$$

with H a quasi-p group, minimal normal subgroup of Γ and $H \subset M(\Gamma)$ has m solutions.

(3) *Every nontrivial finite split embedding problem* (2.2) *with H prime-to-p group and minimal normal subgroup of Γ has m solutions.*

Then Π is homogeneous. Moreover, if $R_S(\Pi) = m$ for every finite simple group S then Π is a profinite free group.

Proof. First of all, let us observe that (1), (2) and (3) allow us to assume that every finite nontrivial (not necessarily split) embedding problem (2.2) with $H \subset M(\Gamma)$ has m solutions. The proof is via induction on $|H|$.

Note that $p(H)$ is a normal subgroup of Γ. Since H is a minimal normal subgroup of Γ, either $p(H) = H$ or $p(H)$ is trivial. If $p(H) = H$ then (2) guarantees m solutions to the embedding problem (2.2)

If $p(H)$ is trivial then H is a prime-to-p group. The embedding problem (2.2) has a weak solution ϕ since Π is projective. Let $G' \leq \Gamma$ be the image of ϕ. The subgroup G' acts on H via conjugation so we can define $\Gamma' = H \rtimes G'$ and get the following embedding problem:

(2.3)
$$\begin{tikzcd}
 & & & \Pi \arrow[dl, dashed] \arrow[d, "\phi"] & \\
1 \arrow[r] & H \arrow[r] & \Gamma' \arrow[r] & G' \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

Also Γ' surjects onto Γ under the homomorphism sending $(h, g) \mapsto hg$. So it is enough to find m solutions to the embedding problem (2.3). Now if H is not a minimal normal subgroup of Γ' then there exist H' proper nontrivial subgroup of H and normal in Γ'. Quotienting by H' we get the following embedding problem:

$$\begin{tikzcd}
 & & & \Pi \arrow[dl, dashed] \arrow[d, "\phi"] & \\
1 \arrow[r] & H/H' \arrow[r] & \Gamma'/H' \arrow[r] & G' \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

which has m solutions by induction hypothesis (since $|H/H'| < |H|$). For each solution θ' to the above, the following embedding problem:

$$\begin{tikzcd}
 & & & \Pi \arrow[dl, dashed] \arrow[d, "\theta'"] & \\
1 \arrow[r] & H' \arrow[r] & \Gamma' \arrow[r] & \Gamma'/H' \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

also has m solutions by induction hypothesis as $|H'| < |H|$. Let θ be solution to this embedding problem then it is in fact a solution to (2.3) as well. Note that distinct solutions for (2.3) induce distinct solutions for (2.2) by [HS, Lemma 2.4]. Finally if H is a minimal normal subgroup of Γ' then hypothesis (3) guarantees m solutions to (2.3). Lemma 2.1 yields Π is homogeneous. The rest of the statement follows from [RZ, Theorem 8.5.2] and [RZ, Lemma 3.5.4]. $\square$

Let Γ be a finite group, H a normal subgroup of Γ contained in $M(\Gamma)$, $G = \Gamma/H$ and $\alpha : \Gamma \to G$ be the quotient map. Let Π be a closed normal subgroup of a profinite group Θ.

Lemma 2.3. *Suppose we have a surjection ψ from $\Theta \to G$ which restricted to Π is also a surjection.*

$$
\begin{tikzcd}
 & 0 \arrow[r] & \Pi \arrow[r] \arrow[dr] & \Theta \arrow[d, "\psi"] \arrow[dl] & \\
0 \arrow[r] & H \arrow[r] & \Gamma \arrow[r, "\alpha"'] & G \arrow[r] & 0
\end{tikzcd}
$$

Let ϕ be a surjection of Θ onto Γ such that $\psi = \alpha \circ \phi$. Then the restriction of ϕ to Π is a surjection onto Γ.

Proof. Let us first note that $\phi(\Pi)$ is a normal subgroup of Γ and $\alpha(\phi(\Pi)) = G$. Suppose $\phi(\Pi)$ is a proper normal subgroup of Γ, then there exists a maximal normal proper subgroup Γ' of Γ containing $\phi(\Pi)$. Since H is contained in $M(\Gamma)$, $H \subset \Gamma'$. Also $\alpha(\Gamma') = G$, so $\Gamma' = \Gamma$ contradicting that Γ' is a proper subgroup of Γ. Hence $\phi(\Pi) = \Gamma$. $\square$

3. Solutions to embedding problems

A morphism of schemes, $\Phi \colon X \to Y$, is said to be a *cover* if Φ is finite, surjective and generically separable. For a finite group G, Φ is said to be a G*-cover* (or a G-Galois cover) if in addition there exists a group monomorphism $G \to \mathrm{Aut}_Y(X)$ which acts transitively on the geometric generic fibers of Φ. Let $k_0 \subset k$ be fields. For a k_0-scheme X, $X \times_{\mathrm{Spec}(k_0)} \mathrm{Spec}(k)$ will also be denoted by $X \otimes_{k_0} k$. For an integral k_0-scheme X, $k(X)$ will denote the function field of $X \otimes_{k_0} k$. We begin with a few results on Galois theory.

Lemma 3.1. *Let A be a field. All the algebraic extensions of A will be considered in some fixed algebraic closure of A. Let B/A be a Galois extension. Let L/A be a finite Galois extension such that $B \cap L = A$. Let M/L be a finite Galois extension with Galois group H. If $M \subset BL$ then there exists a finite H-Galois extension E/A such that $EL = M$ and $E \cap L = A$.*

Proof. First we shall reduce to the case when B/A is a finite Galois extension. Since M/L is a finite extension, $M \subset BL$ and a vector space basis of B over A generates BL over L, there exists a finite extension B'/A with $B' \subset B$ such that $M \subset B'L$. Also Galois closure B'' of B'/A is a subfield of B since B/A is Galois. So replacing B by B'' we may assume B/A is a finite Galois extension.

Now we shall reduce to the case where M/A is a Galois extension. Let M' be the Galois closure of M/A. Also note that BL/A is a Galois extension. So $M \subset BL$ implies $M' \subset BL$. Suppose we know the conclusion of the lemma holds for M', i.e., suppose there exists a finite Galois extension E'/A such that $\mathrm{Gal}(E'/A) = \mathrm{Gal}(M'/L)(= H'$ say), $E'L = M'$ and $E' \cap L = A$. We will find a subfield E of E' such that E/A is an H-extension and $EL = M$. Since M/L is a sub-Galois extension of M'/L, H is a quotient of H' by some normal subgroup N of H' and M is the subfield of M' fixed by N. Let E be the subfield of E' fixed by N. Then $\mathrm{Gal}(E/A) = H'/N = H$. Also the field L is fixed by the action of H' and hence by the action of the subgroup N. So EL is a subfield of M' fixed by the action of N which means $EL \subset M = {M'}^N$. But $E' \cap L = A$ implies $E \cap L = A$. The linear disjointness of E and L over A implies that $[EL : L] = [E : A] = |H| = [M : L]$. So $EL = M$. Hence we are reduced to showing the case where M/A is a Galois extension.

Let $G_1 = \mathrm{Gal}(B/A)$ and $G_2 = \mathrm{Gal}(L/A)$, so $\mathrm{Gal}(BL/A) = G_1 \times G_2$. The inclusions $A \subset M \subset BL$ implies that there is an epimorphism $a : G_1 \times G_2 \to \mathrm{Gal}(M/A)$. Hence there is a group homomorphism $b : G_2 \to \mathrm{Gal}(M/A)$ given by $b(g) = a(e_{G_1}, g)$, where e_{G_1} is the identity of G_1. This gives an action of G_2 on the field M whose restriction to the subfield L agrees with the action of $\mathrm{Gal}(L/A) = G_2$ on L. This is because for $c \in L$, $b(g) \cdot c = a(e_{G_1}, g) \cdot c = (e_{G_1}, g) \cdot c = g \cdot c$. So b is injective and G_2 can be viewed as a subgroup of $\mathrm{Gal}(M/A)$. We have the following split short exact sequence of groups.

$$1 \to H = \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/A) \to G_2 = \mathrm{Gal}(L/A) \to 1$$

Let $E = M^{b(G_2)}$ be the fixed subfield of M then $[E : A] = |H|$. Also $E = M^{b(G_2)} \subset BL^{\{e_{G_1}\} \times G_2} = B$. Hence $E \cap L = A$ and $E \subset B \cap M$. Also we have

$$\begin{aligned}[B \cap M : A] &\le [(B \cap M)L : L] \\ &\le [M : L] \text{ as } (B \cap M)L \subset M \\ &= |H| = [E : A]\end{aligned}$$

Hence $E = B \cap M$. But B/A and M/A are Galois extensions, so E/A is also Galois extension. Moreover $E^H = (M^{b(G_2)})^H = M^{\mathrm{Gal}(M/A)} = A$. Hence $\mathrm{Gal}(E/A) = H$. □

Lemma 3.2. *Let H be a minimal normal subgroup of Γ with $G = \Gamma/H$ and let B/A be a G-Galois extension. Suppose D_1/A, D_2/A be two distinct Γ-Galois extensions containing B. Then $D_1 \cap D_2 = B$.*

Proof. First note that $\mathrm{Gal}(D_1/B) = H$. Let $E = D_1 \cap D_2$. Then E/A is a Galois extension and we have $D_1 \supsetneq E \supset B \supset A$. So $\mathrm{Gal}(D_1/E)$ is a nontrivial normal subgroup of Γ and $\mathrm{Gal}(D_1/E) \le H = \mathrm{Gal}(D_1/B)$. Since H is a minimal normal subgroup of Γ, we must have $\mathrm{Gal}(D_1/E) = \mathrm{Gal}(D_1/B)$. This implies $E = B$. □

Lemma 3.3. *Let k_0 be an algebraically closed field of characteristic $p > 0$. Let k be an algebraically closed field with $k_0 \subsetneq k$. Let X be a k_0-curve. All fields considered will be subfields of a fixed algebraic closure of $k(X)$. Let $f \in k(X)$ be such that the polynomial $g(z) = z^p - z - f$ is irreducible over $k(X)$ and $f - h^p + h \notin k_0(X)$ for any $h \in k(X)$. Let $L/k(X)$ be the $\mathbb{Z}/p\mathbb{Z}$-extension given by adjoining roots of $g(z)$ to $k(X)$. Let M_0 be an algebraic extension of $k_0(X)$. Then L is not contained in the compositum kM_0.*

Proof. Suppose $L \subset kM_0$, we will obtain a contradiction. Since $L/k(X)$ is finite and a $k_0(X)$-vector space basis of M_0 generates $k(X)M_0 = kM_0$ as vector space over $k(X)$, there exists a finite extension $M_0'/k_0(X)$ such that $L \subset kM_0'$. So replacing M_0 by M_0' we may assume $M_0/k_0(X)$ is finite. Further passing to the Galois closure of $M_0/k_0(X)$, we may assume $M_0/k_0(X)$ is a finite Galois extension.

Also note that $M_0 \cap k(X) = k_0(X)$ and $k(X)M_0 = kM_0$. So $\mathrm{Gal}(M_0/k_0(X)) = \mathrm{Gal}(kM_0/k(X))$. Let N be the Galois group of kM_0/L and $L_0 = M_0^N$ be the fixed subfield. Since $L/k(X)$ is a $\mathbb{Z}/p\mathbb{Z}$-Galois extension, N is a normal subgroup of $\mathrm{Gal}(kM_0/k(X))$ with $\mathrm{Gal}(kM_0/k(X))/N \cong \mathbb{Z}/p\mathbb{Z}$. So L_0 is a $\mathbb{Z}/p\mathbb{Z}$-extension of $k_0(X)$. Moreover, since $k(X) \subsetneq kL_0 \subset (kM_0)^N = L$, $L = kL_0$. By Artin-Schreier theory L_0 is obtained by adjoining roots of the polynomial $z^p - z - f_0$ to $k_0(X)$ for some $f_0 \in k_0(X)$. So the Artin-Schreier extensions of $k(X)$ given by polynomials $z^p - z - f_0$ and $z^p - z - f$ are same. But this implies $f = cf_0 + h^p - h$ for some $h \in k(X)$ and nonzero $c \in \mathbb{F}_p$. This contradicts the hypothesis of the lemma. □

Let k be an algebraically closed field of characteristic p and cardinality m. Let C be a smooth affine k-curve. Let K^{un} denote the compositum (in a fixed algebraic closure Ω of $k(C)$) of the function fields of all Galois étale covers of C. In these notations $\pi_1(C) = \mathrm{Gal}(K^{un}/k(C))$.

Definition 3.4. For each $g \geq 0$, let

$$P_g(C) = \cap\{\pi_1(Z) : Z \to C \text{ is an étale } \mathbb{Z}/p\mathbb{Z}\text{-cover and genus of } Z \geq g\}$$

be an increasing sequence of closed normal subgroups of $\pi_1(C)$.

Remark 3.5. Let K_g be the fixed subfield of K^{un} under the action of $P_g(C)$. The definition of $P_g(C)$ implies that the étale pro-cover of C corresponding to K_g dominates all p-cyclic étale covers of C of genus at least g. The profinite subgroups of $\pi_1(C)$ we shall consider will be subgroups of $P_g(C)$, so the pro-cover associated to such a subgroup will also dominate a all p-cyclic étale covers of C of genus at least g.

The main objective of this section is to prove the following.

Theorem 3.6. *Let Π be a closed normal subgroup of $\pi_1(C)$ of rank m such that $\pi_1(C)/\Pi$ is an abelian group and Π is a subset of $P_g(C)$ for some $g \geq 0$. Then Π is a homogeneous profinite group. Moreover if $R_S(\Pi) = m$ for every finite simple group S then Π is a free profinite group of rank m.*

More precisely, in view of Theorem 2.2, it will be shown that the finite embedding problem

$$\begin{tikzcd}
 & & & \Pi \arrow[dl, dashed] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r] & G \arrow[r] \arrow[d] & 1 \\
 & & & 1 &
\end{tikzcd}$$

has m solutions in the following situations:

(1) The kernel H is a quasi-p minimal normal subgroup of Γ contained in $M(\Gamma)$ (Theorem 3.12).
(2) The embedding problem is split and H is a prime-to-p minimal normal subgroup of Γ (Theorem 3.9).

Let K^b be the fixed subfield of K^{un} under the action of Π. So by Galois theory $\mathrm{Gal}(K^{un}/K^b) = \Pi$ and $\mathrm{Gal}(K^b/k(C)) = \pi_1(C)/\Pi$ is abelian. Note that the surjection from Π to G corresponds to a Galois extension $M \subset K^{un}$ of K^b with Galois group G. Since K^b is an algebraic extension of $k(C)$ and M is a finite extension of K^b, we can find a finite extension $L \subset K^b$ of $k(C)$ and $L' \subset K^{un}$ a G-Galois extension of L so that $M = K^b L'$. Let $\pi_1^L = \mathrm{Gal}(K^{un}/L)$.

Let D be the smooth completion of C, X be the normalization of D in L and $\Phi'_X : X \to D$ be the normalization morphism. Then X is an abelian cover of D étale over C and its function field $k(X)$ is L. Let W_X be the normalization of X in L' and Ψ_X be the corresponding normalization morphism. Then Ψ_X is étale away from the points lying above $D \setminus C$ and $k(W_X) = L'$. The following figure provides a summary.

$$
\begin{tikzcd}
K^{un} & & & \\
& M \arrow[ul] \arrow[rr, equal] & & L'K^b \arrow[ulll] \\
& K^b \arrow[uul, "\Pi"] \arrow[u] \arrow[urr, "G"'] & & L' = k(W_X) \arrow[u] \\
& L = k(X) \arrow[uuul, bend left, "\pi_1^L"] \arrow[u] \arrow[urr, "G"'] & & \\
& k(C) \arrow[u] & &
\end{tikzcd}
$$

FIGURE 1

Since k is an algebraically closed field, $k(C)/k$ has a separating transcendence basis. By a stronger version of Noether normalization (for instance, see [Eis, Corollary 16.18]), there exist a finite generically separable surjective k-morphism from C to $\mathbb{A}^1_x$, where x denotes the local coordinate of the affine line. The branch locus of such a morphism is codimension 1, hence this morphism is étale away from finitely many points. By translation we may assume none of these points maps to $x = 0$. This morphism extends to a finite surjective morphism $\Theta : D \to \mathbb{P}^1_x$. Let $\Phi_X : X \to \mathbb{P}^1_x$ be the composition $\Theta \circ \Phi'_X$. Let $\{r_1, \ldots, r_N\} = \Phi_X^{-1}(\{x = 0\})$, then Φ_X is étale at $r_1, \ldots, r_N$. Also note that $\Theta^{-1}(\{x = \infty\}) = D \setminus C$.

Let k_0 be a countable algebraically closed subfield of k such that X and W_X are defined over k_0 and the morphisms Φ_X and Ψ_X are base change of k_0-morphisms to k. We shall denote the corresponding k_0-curves and k_0-morphisms as well by X, W_X, Φ_X and Ψ_X to simplify notation.

3.1. **Prime-to-p group.** Let Γ be a finite group, H a prime-to-p nontrivial normal subgroup of Γ and G a subgroup of Γ such that $\Gamma = H \rtimes G$. Let $\Phi_Y : Y \to \mathbb{P}^1_y$ be the smooth $\mathbb{Z}/p\mathbb{Z}$-cover ramified only at $y = 0$ given by $z^p - z - y^{-r}$ where r is coprime to p and can be chosen to ensure that the genus of Y is as large as desired. Recall that $\Pi \subset P_g(C)$ for some $g \geq 0$. The r above is chosen so that the genus of Y is at least g and greater than the number of generators for H. Let F be the locus of $t - xy = 0$ in $\mathbb{P}^1_x \times_k \mathbb{P}^1_y \times_k \times_k \mathrm{Spec}(k[[t]])$. Let $Y_F = Y \times_{\mathbb{P}^1_y} F$, where the morphism from $F \to \mathbb{P}^1_y$ is given by the composition of morphisms $F \hookrightarrow \mathbb{P}^1_x \times_k \mathbb{P}^1_y \times_k \mathrm{Spec}(k[[t]]) \to \mathbb{P}^1_y$. Similarly define $X_F = X \times_{\mathbb{P}^1_x} F$. Let T be the normalization of an irreducible dominating component of the fiber product $X_F \times_F Y_F$. The situation so far can be described by the following picture:

$$\begin{tikzcd}
 & & T \arrow[dl] \arrow[dr] & & \\
 & X_F \arrow[dl] \arrow[dr] & & Y_F \arrow[dl] \arrow[dr] & \\
X \arrow[dr] & & F \arrow[dl] \arrow[dr] & & Y \arrow[dl] \\
 & \mathbb{P}^1_x & & \mathbb{P}^1_y &
\end{tikzcd}$$

Lemma 3.7. *In the above setup, let $L_1 = k((t))(X)$ and L_2 be the p-cyclic extension of $k((t))(D)$ given by $z^p - z - (x/t)^r$ where r is as in the definition of Y above. Let Z be the normalization of $D \otimes_k k((t))$ in L_2. Then the function field $k(T) = L_1L_2$. In particular $k(T)$ is an abelian extension of $k((t))(D)$, a p-cyclic extension of $k((t))(X)$ and the genus of Z is at least the genus of Y.*

Proof. By construction of T, we observe that the function field of T is the compositum of $k(X) \otimes_k k((t)) = k((t))(X) = L_1$ and the function field of a dominating irreducible component of $(Y \otimes_k k((t))) \times_{\mathbb{P}^1_y \otimes_k k((t))} (D \otimes_k k((t)))$. Here the morphism $D \otimes_k k((t)) \to \mathbb{P}^1_y \otimes_k k((t))$ is the composition of $D \otimes_k k((t)) \to \mathbb{P}^1_x \otimes_k k((t))$ with $\mathbb{P}^1_x \otimes_k k((t)) \to \mathbb{P}^1_y \otimes_k k((t))$ where the later morphism is defined in local co-ordinates by sending y to t/x. Now using the defining equation of Y, we get that this function field is $k((t))(D)[z]/(z^p - z - (x/t)^r)$. Hence $k(T) = L_1L_2 = k((t))(X)[z]/(z^p - z - (x/t)^r)$.

Note that $L_1 \cap L_2 = k((t))(D)$. Also $k(X)/k(D)$ is an abelian extension, so $\mathrm{Gal}(L_1L_2/k((t))(D)) = \mathrm{Gal}(L_1/k((t))(D)) \times \mathrm{Gal}(L_2/k((t))(D)$ is also abelian. The morphism $Z \to D \otimes_k k((t)) \to \mathbb{P}^1_y \otimes k((t))$ factors through $Y \otimes_k k((t))$. So the genus of Z is greater than the genus of Y. □

Let $\Psi_Y : W_Y \to Y$ be an étale H-cover of Y. Note that this is possible because H is a prime-to-p group and the genus of Y is greater than the number of generators of H (Grothendieck's lifting [SGA1, XIII, Corollary 2.12, page 392]). Let T_X and T_Y be the open subschemes of T given by $x \neq 0$ and $y \neq 0$ respectively. Let W_{XF} and W_{XT} be the normalized pullback of $W_X \to X$ to X_F and T_X respectively. Similarly define W_{YF} and W_{YT} to be the normalized pullback of $W_Y \to Y$. The following result (Proposition 3.8) assumes the above setup and uses the above construction of F, T, W_{XT}, W_{YT} etc explicitly. Note that the construction of these objects depend on the given curve X and the choice of the curve Y. This is also the basic setup of [Ku2, Proposition 6.4] which is used in the proof of Proposition 3.8.

Note that every set of ordinals is a well-ordered set, so there exist an ordinal I of infinite cardinality m such that for any $\beta \in I$, $I_\beta = \{\alpha \in I | \alpha \leq \beta\}$ has cardinality strictly less than m. Such an I is called the *initial ordinal* of cardinality m.

Proposition 3.8. *Let I be the initial ordinal of cardinality m. Let the groups G, Γ and H be as in the setup of this subsection. There exists a set $\mathcal{F}$ of algebraically closed subfields k_α, $k_0 \subset k_\alpha \subset k$ indexed by I such that the* $\mathrm{card}(k_\alpha) \leq \max(\mathrm{card}(I_\alpha), \mathrm{card}(\mathbb{N}))$, *for $\alpha < \beta \in I$, $k_\alpha \subset k_\beta \in \mathcal{F}$ and for each $k_\alpha \in \mathcal{F}$ there exists an irreducible Γ-cover $W_\alpha \to T_\alpha$ of k_α-curves with the following properties:*

(1) *T_α is a $\mathbb{Z}/p\mathbb{Z}$-cover of X unramified over the preimage of C in X, the composition $W_\alpha \to T_\alpha \to D$ is unramified over C and the G-cover $W_\alpha/H \to T_\alpha$ is isomorphic to the cover $W_X \times_X T_\alpha \to T_\alpha$.*
(2) *T_α is an abelian cover of D with $\Pi \subset \mathrm{Gal}(K^{un}/k(T_\alpha))$, i.e., $k(T_\alpha) \subset K^b$.*
(3) *Let $H' \neq \{e\}$ be a quotient of H. If $V \to W_X$ is an H'-cover étale over the preimage of C in W_X then $k(V)k(T_\alpha)$ and $k(W_\alpha)$ are linearly disjoint over $k(W_X)k(T_\alpha)$.*
(4) *Let $\alpha < \beta \in I$ and $M_\alpha/k_\alpha(X)$ be an algebraic extension. Then $k(T_\beta)$ and the compositum kM_α are linearly disjoint over $k(X)$.*

Proof. The above setup mentioned in this subsection will be used in this proof. In particular we shall use the construction of T above for various choices of Y. First we shall show that for any algebraically closed field k_α, $k_0 \subset k_\alpha \subset k$, there are "many" choices for $W_\alpha \to T_\alpha$ which satisfy (1), (2) and (3) of the proposition. The existence of $W_\alpha \to T_\alpha$ satisfying (1) and (2) relies on [Ku2, Proposition 6.4] and [Ku2, Proposition 6.9]. For it to satisfy (3) as well one tweaks the argument slightly to get linear disjointness. Finally using transfinite induction, we will construct $\mathcal{F}$ and for each $k_\alpha \in \mathcal{F}$, we will choose a $W_\alpha \to T_\alpha$ which satisfy property (4) as well This uses a bit of set theory and Galois theory.

By [Ku2, Proposition 6.4] there exist an irreducible normal Γ-cover $W \to T$ of $k[[t]]$-schemes such that over the generic point $\mathrm{Spec}(k((t)))$, $W^g \to T^g$ is ramified only over the points of T^g lying above $x = \infty$. This cover can be specialized to k_α to obtain $W_\alpha \to T_\alpha$ satisfying (1) and (2). But we shall apply this argument in a slightly modified setup to obtain the morphism $W_\alpha \to T_\alpha$ which satisfy (3) as well.

Since H is a prime-to-p group, so is any quotient H' of H. By Grothendieck's lifting there are only finitely many H'-covers of W_X which are étale over the preimage of C. So there are only finitely many subcovers of these H'-covers of W_X. Also, since H is a finite group, it has only finitely many quotients. We fix l to be greater than the total number of all the subcovers of H'-covers of W_X étale over the preimage of C, for all the quotients H' of H.

Let $\Gamma^{(l)} = H^l \rtimes G$, where the action of G on H^l is given by the component-wise action of G on each copy of H. Increasing r in the definition of Y to increase the genus of Y, we may assume that there exists an étale H^l-cover $W'_Y \to Y$. Since H^l is still a prime-to-p group and $\Gamma^{(l)} = H^l \rtimes G$, we can apply [Ku2, Proposition 6.4] to obtain an irreducible normal $\Gamma^{(l)}$-cover $W' \to T$ of $k[[t]]$-schemes such that $W'^g \to T^g$ is ramified only over the points of T^g lying above $x = \infty$.

Now this cover can be specialized to obtain covers of k_α-curves using [Ku2, Proposition 6.9]. In fact in the proof of [Ku2, Proposition 6.9] it was shown that there exists an open subset S of the spectrum of a $k[t, t^{-1}]$-algebra such that the coverings $W'^g \to W^g_{XT} \to T^g \to X \otimes_k k((t))$ descend to covers of S-schemes $W'_S \to W_{XT,S} \to T_S \to X \times_k S$. Moreover, the fiber over every closed point in S leads to covers of smooth k-curves with the desired ramification properties and Galois groups same as that over the generic point $\mathrm{Spec}(k((t)))$.

In view of Lemma 3.7, the fiber over a k_α-point of S provides a $\mathbb{Z}/p\mathbb{Z}$-cover $T_\alpha \to X$ of k_α-curves and $T_\alpha \to D$ is an abelian cover. Let Z be as in Lemma 3.7. Since T_α is a specialization of T to k at a k_α-point and $k(T) = k(Z)k((t))(X)$, $k(T_\alpha)$ is the compositum of $k(X)$ and $k(Z_\alpha)$ where Z_α is the corresponding specialization of Z to k at that k_α-point. Since the genus of Z is greater than the genus of Y which in turn is at least g, the genus of Z_α is at least g. Also $Z_\alpha \to D$ is unramified over C because

T_α dominates Z_α. The extension $k(Z)/k((t))(D)$ is p-cyclic. So the same is true for $k(Z_\alpha)/k(D)$. So we obtain that the Galois group $\mathrm{Gal}(K^{un}/k(Z_\alpha)) \supset P_g(C)$. Hence $\Pi \subset \mathrm{Gal}(K^{un}/k(Z_\alpha))$. Also Π is clearly contained in $\pi_1^L = \mathrm{Gal}(K^{un}/k(X))$ (see Figure 1). So $\Pi \subset \mathrm{Gal}(K^{un}/k(X)k(Z_\alpha)) = \mathrm{Gal}(K^{un}/k(T_\alpha))$.

The fiber over any k_α-point of S provides a $\Gamma^{(l)}$-cover $W'_\alpha \to T_\alpha$ of k_α-curves. Moreover, let $H_i = H \times \ldots H \times \hat{H} \times H \times \ldots H$ be the subgroup of $\Gamma^{(l)}$ where the i^{th} factor of H is replaced by the trivial group. Then the quotients $W'_\alpha/H_i \to T_\alpha$ are Γ-covers satisfying (1) and (2). Let $W^i_\alpha = W'_\alpha/H_i$. Note that for each i, $k(W^i_\alpha)$ is linearly disjoint with the compositum $\prod_{j\neq i} k(W^j_\alpha)$ over $k(W_X)k(T_\alpha)$.

We claim that at least one of these W^i_α satisfy (3) as well. Suppose not, then for each i there exists an $H' \neq \{e\}$ a quotient of H and an H'-cover $V^i \to W_X$ étale over the preimage of C such that $k(V^i)k(T_\alpha)$ and $k(W^i_\alpha)$ are not linearly disjoint over $k(T_\alpha)k(W_X)$. We already saw $k(T_\alpha) \subset K^b$, $\mathrm{Gal}(k(T_\alpha)/k(X)) = \mathbb{Z}/p\mathbb{Z}$ and K^b and $k(W_X)$ are linearly disjoint over $k(X)$. So $\mathrm{Gal}(k(T_\alpha)k(W_X)/k(W_X)) = \mathbb{Z}/p\mathbb{Z}$. Since $k(V^i)/k(W_X)$ is a prime-to-p extension, $k(T_\alpha)k(W_X)$ and $k(V^i)$ are linearly disjoint over $k(W_X)$. We have the following picture:

$$\begin{tikzcd}
 & & k(V^i)k(W^i_\alpha) & \\
 & k(V^i)k(T_\alpha) \arrow[ur] & & k(W^i_\alpha) \arrow[ul] \\
k(V^i) \arrow[ur, "\mathbb{Z}/p\mathbb{Z}"] & & k(T_\alpha)k(W_X) \arrow[ul, "H'"'] \arrow[ur] & \\
 & k(W_X) \arrow[ul, "H'"] \arrow[ur, "\mathbb{Z}/p\mathbb{Z}"'] & &
\end{tikzcd}$$

If $k(V^i)k(T_\alpha)$ and $k(W^i_\alpha)$ are not linearly disjoint over $k(T_\alpha)k(W_X)$ then $k(V^i)$ and $k(W^i_\alpha)$ are not linearly disjoint over $k(W_X)$. Hence $M_i := k(V^i) \cap k(W^i_\alpha) \supsetneq k(W_X)$. Note that M_i defines a nontrivial subcover of the H'-cover $V^i \to W_X$ and $k(W_X)k(T_\alpha) \subsetneq M_ik(T_\alpha) \subset k(W^i_\alpha)$. But linear disjointness of $k(W^i_\alpha)$ with the compositum $\prod_{j\neq i} k(W^j_\alpha)$ over $k(W_X)k(T_\alpha)$ tells us that $M_i \neq M_j$ for $i \neq j$. So we have produced l distinct covers of W_X such that each one is a subcover of some H'-cover of W_X étale over the preimage of C where H' is a quotient of H. This contradicts the choice of l. Hence for some $1 \le i \le l$, W^i_α satisfy (3) as well. We let W_α to be this W^i_α.

Now to construct $\mathcal{F}$ along with the choice of $W_\alpha \to T_\alpha$ for every $k_\alpha \in \mathcal{F}$ satisfying (1), (2), (3) and (4), we use transfinite induction. Let $\gamma \in I$ and suppose for all $\alpha \in I$, $\alpha < \gamma$, we have constructed algebraically closed fields k_α, $k_0 \subset k_\alpha \subset k$, with $\mathrm{card}(k_\alpha) \le \max(\mathrm{card}(I_\alpha), \mathrm{card}(\mathbb{N}))$ and chosen $W_\alpha \to T_\alpha$ satisfying (1), (2) and (3). Moreover for $\beta \in I$, with $\alpha < \beta < \gamma$, (4) is also satisfied.

Let $k' = \cup_{\alpha<\gamma} k_\alpha$, we claim that $\mathrm{card}(k') \le \max(\mathrm{card}(I_\gamma), \mathrm{card}(\mathbb{N}))$. If I_γ is a finite set then k' is a finite union of countable fields and hence itself is countable. Now assume I_γ is an infinite set. Note that for $\alpha < \gamma$, we have $\mathrm{card}(k_\alpha) \le \max(\mathrm{card}(I_\alpha), \mathrm{card}(\mathbb{N})) \le \mathrm{card}(I_\gamma)$. But $k' = \cup_{\alpha \in I_\gamma \setminus \{\gamma\}} k_\alpha$, so $\mathrm{card}(k') \le \mathrm{card}(I_\gamma)$.

We shall construct an algebraically closed subfield k_γ of k and choose $W_\gamma \to T_\gamma$ such that $\mathrm{card}(k_\gamma) \le \max(\mathrm{card}(I_\gamma), \mathrm{card}(\mathbb{N}))$, $k' \subset k_\gamma$ and the set $\{k_\alpha \in \mathcal{F} : \alpha \le \gamma\}$ along with the choices $W_\alpha \to T_\alpha$ for $\alpha \le \gamma$ satisfies (1), (2), (3) and (4). More precisely, we shall show that there exists an irreducible smooth Γ-cover $W_\gamma \to T_\gamma$ of k_γ-curves satisfying (1), (2) and (3). Moreover, for any $\alpha < \gamma$ and $M_\alpha/k_\alpha(X)$ algebraic extension, $k(T_\gamma)$ and kM_α are linearly disjoint over $k(X)$.

Note that the function field of T is an Artin-Schreier extension of $k((t))(X)$ given by the polynomial $z^p - z - (x/t)^r$. Recall that S is an open subset of the spectrum of a $k[t, t^{-1}]$-algebra such that the fibers over any point of S of the covers $W_S \to T_S \to X \times_k S$ lead to covers of k-curves satisfying (1), (2) and (3). Since k has a transcendence basis of cardinality m over k_0, there exists $B = \{a_i | i \in I\} \subset k$ of cardinality m such that B is a part of a transcendence basis of k/k_0 and $t = a$ defines a point P_a of S for all $a \in B$. Let $W_a \to T_a$ be the fiber over the point P_a of $W_S \to T_S \to X \times_k S$ for $a \in B$. Then $k(T_a) = k(X)[z]/(z^p - z - (x/a)^r)$. Note that for $a \neq c \in B$, $k(T_a)$ and $k(T_c)$ are distinct subfields of K^b.

Claim. There exists $a \in B$ such that given any algebraic extension $M'/k'(X)$, $k(T_a)$ is not contained in kM'.

Proof of the claim: Suppose not, then by Lemma 3.3, for each $a \in B$ there exists $h_a \in k(X)$ such that $f_a = (x/a)^r - h_a^p + h_a \in k'(X)$. Let u_a in Ω, the fixed algebraic closure of $k(C)$, be such that $u_a^p - u_a = f_a$. Since $k(X)[u_a]$ and $k(T_a)$ are both $\mathbb{Z}/p\mathbb{Z}$-extensions of $k(X)$ and $(u_a + h_a)^p - (u_a + h_a) = (x/a)^r$, $k(X)[u_a] = k(T_a)$. Note that if $a \neq c \in B$ then $k(T_a) \neq k(T_c)$ and hence $f_a \neq f_b \in k'(X)$. So there is an injective set map from B to $k'(X)$. The cardinality of B is m but $\mathrm{card}(k'(X)) = \mathrm{card}(k') \le max(\mathrm{card}(I_\gamma), \mathrm{card}(\mathbb{N}))$. Since I is the first ordinal of cardinality m, $\mathrm{card}(I_\gamma) < m$ which provides a contradiction. □

We let k_γ to be the algebraic closure of $k'(a)$ in k and $W_\gamma \to T_\gamma$ be the morphism $W_a \to T_a$. Then $W_\gamma \to T_\gamma$ satisfies (1), (2) and (3). Let $\alpha \in I$ be such that $\alpha < \gamma$ then $k_\alpha \subset k'$. Let $M_\alpha/k_\alpha(X)$ be an algebraic extension then $k'M_\alpha/k'(X)$ is also an algebraic extension. So by the above claim $k(T_\gamma)$ is not contained in $kk'M_\alpha = kM_\alpha$. Since $k(T_\gamma)/k(X)$ is of degree p, we get that $k(T_\gamma) \cap kM_\alpha = k(X)$. Also $\mathrm{card}(k_\gamma) = \mathrm{card}(k') \le \max(\mathrm{card}(I_\gamma), \mathrm{card}(\mathbb{N}))$. This completes the proof. □

Theorem 3.9. *Let Π be a closed normal subgroup of $\pi_1(C)$ of rank m such that $\pi_1(C)/\Pi$ is abelian and $\Pi \subset P_g(C)$ for some $g \ge 0$. The following finite split embedding problem has* $\mathrm{card}(k) = m$ *proper solutions*

$$\begin{tikzcd} & & & \Pi \arrow[dl, dashed] \arrow[d] & \\ 1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r] & G \arrow[r] \arrow[d] & 1 \\ & & & 1 & \end{tikzcd}$$

Here H is a nontrivial prime-to-p group and a minimal normal subgroup of Γ.

Proof. First we note that translating the problem to Galois theory using Figure 1, our objective is to find m distinct Γ-extensions of K^b, contained in K^{un} and containing M (or equivalently $k(W_X)$). By Proposition 3.8, we have a collection of fields $\mathcal{F}$ indexed by a set I of cardinality m, such that for each $k_\alpha \in \mathcal{F}$, there exist W_α and T_α with $\mathrm{Gal}(k(W_\alpha)/k(T_\alpha)) = \Gamma$. Also $k(W_X)$ and K^b are linearly disjoint over $k(X)$ and by Proposition 3.8(2) $k(T_\alpha) \subset K^b$. So $\mathrm{Gal}(k(W_X)k(T_\alpha)/k(T_\alpha)) = \mathrm{Gal}(k(W_X)/k(X)) = G$ and $\mathrm{Gal}(k(W_\alpha)/k(W_X)k(T_\alpha)) = H$.

Claim. For every $k_\alpha \in \mathcal{F}$, the fields $K^b k(W_X)$ and $k(W_\alpha)$ are linearly disjoint over $k(W_X)k(T_\alpha)$ and $\mathrm{Gal}(K^b k(W_\alpha)/K^b) = \Gamma$.

Proof of the claim. Let $A = K^b k(W_X) \cap k(W_\alpha)$ then $A/k(T_\alpha)k(W_X)$ is an H'-extension where H' is a quotient of H. Since $K^b k(W_X)/k(W_X)$ is an abelian extension, so is $A/k(W_X)$. Also $k(T_\alpha)/k(X)$ is a $\mathbb{Z}/p\mathbb{Z}$-extension by Proposition 3.8(1), so $\mathrm{Gal}(k(T_\alpha)k(W_X)/k(W_X)) = \mathbb{Z}/p\mathbb{Z}$. Since H' is a prime-to-p group, $\mathrm{Gal}(A/k(W_X)) = H' \times \mathbb{Z}/p\mathbb{Z}$. So there exists an H'-cover $V \to W_X$ étale over the preimage of C such that $k(V) \subset A$. Hence $k(W_X)k(T_\alpha) \subset k(V)k(T_\alpha) \subset k(W_\alpha)$. But Proposition 3.8(3) forces H' to be $\{e\}$. Hence $K^b k(W_X)$ and $k(W_\alpha)$ are linearly disjoint over $k(W_X)k(T_\alpha)$. But this implies $\mathrm{Gal}(K^b k(W_\alpha)/K^b k(W_X)) = \mathrm{Gal}(k(W_\alpha)/k(T_\alpha)k(W_X)) = H$. Also $\mathrm{Gal}(K^b k(W_X)/K^b) = G$, so $[K^b k(W_\alpha) : K^b] = |\Gamma|$. Hence comparing degrees, we get that $k(W_\alpha)$ and K^b are linearly disjoint over $k(T_\alpha)$ and $\mathrm{Gal}(K^b k(W_\alpha)/K^b) = \Gamma$. □

To complete the proof, it is enough to show that for $k_\alpha \subsetneq k_\beta \in \mathcal{F}$, $k(W_\alpha)K^b \neq k(W_\beta)K^b$ as subfields of K^{un}. Let $L_0 = k(T_\alpha)k(T_\beta)$. Note that $k(X) \subset L_0 \subset K^b$, so by the above claim $\mathrm{Gal}(k(W_\alpha)L_0/L_0) = \Gamma$. We will first show the following:

Claim. The fields $k(W_\alpha)L_0$ and $k(W_\beta)L_0$ are linearly disjoint over $k(W_X)L_0$.

Proof of the claim. Let M_α be the Galois closure of $k_\alpha(W_\alpha)$ over $k_\alpha(W_X)$. By Proposition 3.8(4), $k(T_\beta)$ and kM_α are linearly disjoint over $k(X)$. So $k(T_\beta)k(W_X)$ and kM_α are linearly disjoint over $k(W_X)$. Suppose $k(W_\beta)L_0 = k(W_\alpha)L_0$. Then $k(W_\beta) \subset k_\alpha(W_\alpha)k(T_\beta) \subset M_\alpha k(T_\beta)$. So applying Lemma 3.1, with A, B, L and M of the lemma as $k(W_X)$, kM_α, $k(T_\beta)k(W_X)$ and $k(W_\beta)$ respectively, we obtain an H-extension $E/k(W_X)$ such that $Ek(T_\beta) = k(W_\beta)$. But this contradicts Proposition 3.8(3). So $k(W_\beta)L_0 \neq k(W_\alpha)L_0$. Since H is a minimal normal subgroup of Γ by Lemma 3.2 we obtain the claim. □

Let K_p^b be the compositum of all $\mathbb{Z}/p\mathbb{Z}$-extension of $k(X)$ contained in K^b.

Claim. The fields $k(W_\alpha)K_p^b$ and $k(W_\beta)K_p^b$ are linearly disjoint over $k(W_X)K_p^b$.

Proof of the claim. Since $K_p^b/k(X)$ is a pro-p extension, so is $k(W_X)K_p^b/k(W_X)L_0$. By the above claim $\mathrm{Gal}(k(W_\alpha)k(W_\beta)/k(W_X)L_0) = H \times H$, which is a prime-to-$p$ group. Hence $k(W_\alpha)k(W_\beta)$ and $k(W_X)K_p^b$ are linearly disjoint over $k(W_X)L_0$. So $\mathrm{Gal}(k(W_\alpha)k(W_\beta)K_p^b/k(W_X)K_p^b) = H \times H$. Also $\mathrm{Gal}(k(W_\alpha)K_p^b/k(W_X)K_p^b) = H = \mathrm{Gal}(k(W_\beta)K_p^b/k(W_X)K_p^b)$, since $k(W_X)K_p^b \subset k(W_X)K^b$. So $k(W_\alpha)K_p^b$ and $k(W_\beta)K_p^b$ are linearly disjoint over $k(W_X)K_p^b$. □

Finally we will show that there exists a subset of I of cardinality m such that for any $\gamma \neq \delta$ in this subset, $k(W_\gamma)K^b \neq k(W_\delta)K^b$.

Since H is a prime-to-p group, by Grothendieck's lifting there are only finitely many H-extensions of $k(X)$ contained in K^{un}. Let L_H denote their compositum. Then $L_H/k(X)$ is a finite extension. For $\alpha, \beta \in I$, we say $\alpha \sim \beta$ if $k(W_\alpha)K_p^b L_H = k(W_\beta)K_p^b L_H$. Clearly, $\sim$ is an equivalence relation on I. Moreover, each equivalence class is finite because $k(W_\alpha)K_p^bL_H/K_p^b$ is a finite extension and if $\alpha \sim \beta$ then $K_p^b \subset k(W_\beta)K_p^b \subset k(W_\alpha)K_p^bL_H$, so only finitely many $k(W_\beta)K_p^b$ is contained in $k(W_\alpha)K_p^bL_H$. So there are m different equivalence classes.

Finally to complete the proof, it is enough to show that if α and β are in different equivalence class then $k(W_\alpha)K^b \neq k(W_\beta)K^b$. Suppose $k(W_\alpha)K^b = k(W_\beta)K^b$. Let $L_1 = k(W_\alpha)k(W_\beta) \cap K^b$. Then $\mathrm{Gal}(k(W_\alpha)k(W_\beta)/L_1) = \mathrm{Gal}(k(W_\alpha)k(W_\beta)K^b/K^b)$. But $k(W_\alpha)k(W_\beta)K^b = k(W_\alpha)K^b$, hence $\mathrm{Gal}(k(W_\alpha)k(W_\beta)/L_1) = \Gamma$. Also note that $[k(W_\alpha)k(W_\beta) : L_0] = |G||H|^2$ because $[k(W_X)L_0 : L_0] = |G|$ and, $k(W_\alpha)L_0$ and $k(W_\beta)L_0$ are linearly disjoint H-extensions of $k(W_X)L_0$. We have the following tower of fields where the labels of the arrow denote the degree:

$$\begin{tikzcd}
 & & k(W_\alpha)K^b = k(W_\beta)K^b & & \\
K^b \arrow[urr, "|G||H|"] & & & & k(W_\alpha)k(W_\beta) \arrow[ull] \\
 & & L_1 \arrow[ull] \arrow[urr, "|G||H|"'] & & \\
 & & L_0 = k(T_\alpha)k(T_\beta) \arrow[u, "|H|"] \arrow[uurr, bend right, "|G||H|^2"'] & & \\
 & & k(X) \arrow[u, "p^2"] & &
\end{tikzcd}$$

From the above figure we also conclude that $[L_1 : L_0] = |H|$. Also observe that $[L_0 : k(T_\alpha)] = p$, so $[L_1 : k(T_\alpha)] = p|H|$. Since $L_1 \subset K^b$, L_1 and $k(W_\alpha)$ are linearly disjoint over $k(T_\alpha)$. So we have $[k(W_\alpha)L_1 : k(T_\alpha)] = p|G||H|^2$. Moreover $[k(W_\alpha)k(W_\beta) : k(T_\alpha)] = p|G||H|^2$ since $[L_0 : k(T_\alpha)] = p$. So the inclusion $k(W_\alpha)L_1 \subset k(W_\alpha)k(W_\beta)$ is in fact the equality $k(W_\alpha)L_1 = k(W_\alpha)k(W_\beta)$. Similarly $k(W_\beta)L_1 = k(W_\alpha)k(W_\beta)$.

Note that $L_1 \subset K^b$ and $K^b/k(X)$ is an abelian extension, so $L_1/k(X)$ is also abelian. Since $L_0/k(X)$ is $(\mathbb{Z}/p\mathbb{Z})^2$-extension and $(|H|, p) = 1$, there exists a prime-to-p Galois extension $L_2/k(X)$ such that $L_1 = L_2L_0$ and L_2, L_0 are linearly disjoint over $k(X)$. Now using various linear disjointness we get that

$$\begin{aligned}
\mathrm{Gal}(L_2/k(X)) &= \mathrm{Gal}(L_1/L_0) \\
&= \mathrm{Gal}(L_1k(W_\alpha)/L_0k(W_\alpha)) \text{ (since } L_0k(W_\alpha) \cap L_1 = L_0) \\
&= \mathrm{Gal}(k(W_\alpha)k(W_\beta)/k(W_\alpha)L_0) \text{ (since } L_1k(W_\alpha) = k(W_\alpha)k(W_\beta)) \\
&= \mathrm{Gal}(k(W_\beta)L_0/k(W_X)L_0) \ (\because k(W_\alpha)L_0 \cap k(W_\beta)L_0 = k(W_X)L_0) \\
&= H
\end{aligned}$$

Hence $L_2 \subset L_H$. Since $L_0 \subset K_p^b$, we have $L_1 \subset K_p^bL_H$. Since $k(W_\alpha)L_1 = k(W_\beta)L_1$, $k(W_\alpha)K_p^bL_H = k(W_\beta)K_p^bL_H$. Hence $\alpha \sim \beta$. $\square$

Remark 3.10. Note that the assumption $\Pi \subset P_g(C)$ for some g means that the étale pro-cover of C corresponding to the field K^b dominates all p-cyclic covers of C of genus at least g. If we relax the above assumption on Π by asking that the pro-cover corresponding to K^b dominates all but a “small set” of p-cyclic covers of C of genus at least g then also Theorem 3.9 holds with slight modifications in the proof. Here a “small set” means a set of cardinality strictly less than m.

3.2. **Quasi-p group.** Now the embedding problem with quasi-p kernel contained in the $M(\Gamma)$ will be shown to have m distinct solutions.

Proposition 3.11. *Let Π be a closed normal subgroup of $\pi_1(C)$ of rank m such that $\pi_1(C)/\Pi$ is abelian then $R_S(\Pi) = m$ for all finite p-groups S.*

Proof. We observe that the pro-p quotient of $\pi_1(C)$ is isomorphic to the pro-p free group of rank m by [Ha2, Theorem 5.3.4], Lemma 2.1 and [RZ, Theorem 8.5.2]. So the pro-p quotient of Π is also pro-p free of rank m by [RZ, Corollary 8.9.3]. Hence $R_S(\Pi) = m$ for every finite p-group S. □

Theorem 3.12. *Suppose Π is closed normal subgroup of $\pi_1(C)$ of rank m such that $\pi_1(C)/\Pi$ is abelian. Then the following finite embedding problem has* $\mathrm{card}(k) = m$ *proper solutions*

$$\begin{tikzcd}
& & & \Pi \arrow[dl, dashed] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r] & G \arrow[r] \arrow[d] & 1 \\
& & & 1 &
\end{tikzcd} \tag{3.1}$$

Here H is a quasi-p group, a minimal normal subgroup of Γ and it is contained in $M(\Gamma)$.

Proof. Let us recall Figure 1 and the setup just before subsection 3.1. In the notation of Figure 1, let X^0 be the normalization of C in L, i.e., X^0 is the open subset of X lying above C. Hence $\pi_1(X^0)$ contains Π and the surjection $\Pi \to G$ extends to $\pi_1(X^0)$. Also note that $\pi_1(X^0)$ is a subgroup of $\pi_1(C)$. By a result ([Pop],[Ha2, Theorem 5.3.4]) first proved by F. Pop, the following embedding problem has m distinct solutions

$$\begin{tikzcd}
& & & \pi_1(X^0) \arrow[dl, dashed] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & \Gamma \arrow[r] & G \arrow[r] \arrow[d] & 1 \\
& & & 1 &
\end{tikzcd}$$

Let I be an indexing set of cardinality m and $\tilde{\theta}_i, i \in I$ denote the m distinct solutions to the above embedding problem. Let θ_i be the restriction of $\tilde{\theta}_i$ to the normal subgroup Π. By Lemma 2.3 we know that every θ_i is a solution to the embedding problem (3.1).

Now we shall show that the embedding problem (3.1) has m distinct solutions. For each solution $\tilde{\theta}_i$ of the above embedding problem for $\pi_1(X^0)$, let L_i be the fixed subfield of K^{un} by the group $\ker \tilde{\theta}_i$. Note that $\mathrm{Gal}(L_i/L) = \Gamma$. Moreover, since θ_i

is a solution to the embedding problem (3.1), we have $\mathrm{Gal}(L_iK^b/K^b) = \Gamma$. Let us summarize the situation in the following diagram.

$$\begin{tikzcd}
K & & & L_iK^b \arrow[lll] \\
& M \arrow[ul] \arrow[r, equal] & L'K^b \arrow[ull] \arrow[ur, "H"] & \\
& K^b \arrow[u] \arrow[uul, "\Pi"] \arrow[ur, "G"'] & & L_i \arrow[uu] \\
& & k(W_X) = L' \arrow[uu] \arrow[ur, "H"] & \\
& k(X) = L \arrow[uu] \arrow[ur, "G"'] \arrow[uuuul, bend left, "\Theta"] \arrow[uurr, bend right, "\Gamma"'] & &
\end{tikzcd}$$

Note that L_i and $L'K^b$ are linearly disjoint over L' for all $i \in I$. Let i and j be two distinct elements of I. Since L_i and L_j are distinct Γ-extensions of L containing L' and H is a minimal normal subgroup of Γ, we must have $L_i \cap L_j = L'$ by Lemma 3.2. In particular, $\mathrm{Gal}(L_iL_j/L') = H \times H$ and $\mathrm{Gal}(L_iL_j/L) = \Gamma \times_G \Gamma = \{(\gamma_1, \gamma_2) | \gamma_1, \gamma_2 \in \Gamma \text{ and } \bar{\gamma}_1 = \bar{\gamma}_2 \in G\}$. Since H is a minimal normal subgroup of Γ, $H = \mathbb{S} \times \mathbb{S} \times \ldots \mathbb{S}$ for some simple group $\mathbb{S}$.

If $\mathbb{S}$ is not abelian then H and hence $H \times H$ is perfect (i.e. it has no non-trivial quotient group that is abelian). But $L'K^b/L'$ is an abelian extension since K^b/L is an abelian extension. Hence $L'K^b$ and L_iL_j are linearly disjoint over L'. Therefore $[L_iL_jK^b/K^b] = |G||H|^2$. In particular, $L_iK^b \neq L_jK^b$ and hence θ_i for $i \in I$ are all distinct.

Now suppose $\mathbb{S}$ is abelian. Since H is a quasi-p group $S = \mathbb{Z}/p\mathbb{Z}$. Hence H is a p-group. If $L_iK^b \neq L_jK^b$ for every $i, j \in I$, $i \neq j$ then clearly θ_i for $i \in I$ are all distinct solutions to the embedding problem (3.1) and we are done again.

So we may assume there exist $i, j \in I$, $i \neq j$, $L_iK^b = L_jK^b$. In this case as well we shall construct m distinct solutions. Let $L_1 = K^b \cap L_iL_j$. Since L_1 is the intersection of Galois extensions of L, L_1/L is a Galois extension. Note that K^b and L_iL_j are linearly disjoint over L_1 so $[L_iL_j : L_1] = [L_iK^b : K^b] = |\Gamma| = |G||H|$. Also $[L_iL_j : L] = |\Gamma \times_G \Gamma| = |G||H|^2$. Hence $[L_1 : L] = |H|$. The following summarizes the situation.

$$\begin{tikzcd}
& L_iK^b = L_jK^b & \\
K^b \arrow[ur, "|G||H|"] & & L_iL_j \arrow[ul] \\
& L_1 \arrow[ul] \arrow[ur, "|G||H|"'] & \\
& L \arrow[u, "|H|"] \arrow[uur, bend right, "|G||H|^2"'] &
\end{tikzcd}$$

We have already observed that L_i and K^b are linearly disjoint over L and $L_1 \subset K^b$, hence L_i and L_1 are linearly disjoint over L. So $[L_iL_1 : L] = |G||H|^2 = [L_iL_j : L]$. Hence the inclusion $L_iL_1 \subset L_iL_j$ is in fact the equality $L_iL_1 = L_iL_j$. Linear disjointness of L_i and L_1 also tells us that $\mathrm{Gal}(L_iL_1/L) = \Gamma \oplus H_1$ where $H_1 = \mathrm{Gal}(L_1/L)$. So we have $\Gamma \oplus H_1 = \mathrm{Gal}(L_iL_1/L) = \mathrm{Gal}(L_iL_j/L) \cong \Gamma \times_G \Gamma$. Also note that $|H_1| = |H|$ hence H_1 is a p-group.

Fix an $i \in I$. Since L_iK^b/K^b is a finite extension, there are only finitely many intermediate field extensions. We choose l to be greater than this number. Let I' be another indexing set of cardinality m. Using Proposition 3.11 we have $R_{H_1^l}(\Pi) = m$. So there are m H_1^l-extensions M'_α of K^b indexed by $\alpha \in I'$ such that $M'_\alpha \subset K^{un}$ and M'_α is linearly disjoint with $\prod_{\beta \in I' \setminus \{\alpha\}} M'_\beta$ over K^b. Taking fixed subfields of M'_α by various copies of H_1^{l-1}, we get l distinct H_1-extensions of K^b contained in M'_α such that any one of them is linearly disjoint with the compositum of the remaining ones over K^b. By choice of l, one of these extensions must be linearly disjoint with L_iK^b over K^b. We will denote this field by M_α. So for each $\alpha \in I'$ there exist $M_\alpha \subset M'_\alpha$ such that L_iK^b and M_α are linearly disjoint over K^b and $\mathrm{Gal}(M_\alpha/K^b) = H_1$. In particular, $\mathrm{Gal}(M_\alpha L_i/K^b) = \Gamma \oplus H_1 \cong \Gamma \times_G \Gamma$. Moreover, every $\alpha \in I'$, M_α and $\prod_{\beta \in I' \setminus \{\alpha\}} M_\beta$ are linearly disjoint over K^b.

Let $L^\alpha \subset M_\alpha L_i$ be a Γ-extension of K^b different from L_i and containing $L'K^b$. Then L^α provides a solution to the embedding problem (3.1). Again using the fact that H is a minimal normal subgroup of Γ, by Lemma 3.2 we observe that L_iK^b and L_α are linearly disjoint over $L'K^b$. Therefore, $[L^\alpha L_i : K^b] = |G||H|^2 = [M_\alpha L_i : K^b]$ and hence $L^\alpha L_i = M_\alpha L_i$.

For $\alpha, \beta \in I'$, we say $\alpha \sim \beta$, if $M_\alpha L_i = M_\beta L_i$. This is clearly an equivalence relation. Since $M_\alpha L_i/K^b$ is a finite extension, there can be only finitely many intermediate fields. So only finitely many M_β's are contained in $M_\alpha L_i$. Hence each equivalence class is finite. Finally if α and β are in two different equivalence classes then $L^\alpha L_i$ and $L^\beta L_i$ are distinct, which implies L^α and L^β are distinct. Since there are m distinct equivalence classes, we obtain m distinct solutions to the embedding problem (3.1). □

Remark 3.13. Note that the hypothesis $\Pi \subset P_g(C)$ is not necessary in the above result.

Proof. **(of theorem 3.6)** The étale fundamental group $\pi_1(C)$ is projective so Π, being a closed subgroup of $\pi_1(C)$, is also projective ([FJ, Proposition 22.4.7]). The result now follows from Theorem 2.2, Theorem 3.9 and Theorem 3.12. □

Let C be a smooth affine curve as above. Recall that $\pi_1^c(C)$ is the commutator subgroup of $\pi_1(C)$.

Proposition 3.14. *Let S be a finite simple group. Then $R_S(\pi_1^c(C)) = m$ and $R_S(P_g(C)) = m$ for all $g \geq 0$.*

Proof. Note that $\pi_1^c(C)$ and $P_g(C)$ for all $g \geq 0$ are closed normal subgroups of $\pi_1(C)$ of rank m and $\pi_1^c(C)$ is contained in $P_0(C)$. Moreover, $\pi_1(C)/\pi_1^c(C)$ and $\pi_1(C)/P_g(C)$ are abelian groups. Let S be a finite simple group. If S is a prime-to-p group then the result follows from Theorem 3.9 by taking $H = \Gamma = S$. If p divides $|S|$ then S is a quasi-p simple group. Moreover if S is also non-abelian group then the result follows from [Ku2, Theorem 5.3]. Finally if S is an abelian simple quasi-p group then $S \cong \mathbb{Z}/p\mathbb{Z}$. Since $\pi_1(C)/\pi_1^c(C)$ and $\pi_1(C)/P_g(C)$ are abelian groups, the result follows from Proposition 3.11. □

Corollary 3.15. *The commutator subgroup $\pi_1^c(C)$ of $\pi_1(C)$ is a profinite free group of rank m for any smooth affine curve C over an algebraically closed field k of characteristic p and cardinality m. The subgroups $P_g(C)$ of $\pi_1(C)$ are also free profinite group of rank m for all $g \geq 0$.*

Proof. As observed earlier, $\pi_1^c(C)$ is a closed normal subgroup of $\pi_1(C)$ of rank m contained in $P_0(C)$. Also $\pi_1(C)/\pi_1^c(C)$ and $\pi_1(C)/P_g(C)$ are abelian groups. So the result follows from Theorem 3.6 and Proposition 3.14. □

The restriction that $\Pi \subset P_g(C)$ for some g can not be dropped completely as the following example suggests. Though it could be somewhat relaxed (see Remark 3.10).

Example 3.16. Let C be the affine line and $\Pi = \cap\{\pi_1(Z)|Z \to C$ an étale cover and Z is again the affine line$\}$. Clearly Π is a closed normal subgroup of $\pi_1(C)$ and $\pi_1(C)/\Pi$ is an infinite abelian pro-p subgroup. But Π has no non-trivial prime-to-p quotients. To see this, assume there is one. Then there exists a prime-to-p finite field extension M/K^b with $M \subset K^{un}$. Using finiteness of this field extension, one could get a prime-to-p extension of L where $L \subset K^b$ is a finite extension of $k(C)$. But the normalization of C in L is also an affine line, so it can not have a prime-to-p étale cover by Theorem 1.3.

Let K_{p^n} denote the intersection of all open normal subgroups of $\pi_1(C)$ so that the quotient is an abelian group of exponent at most p^n. Let $G_{p^n} = \pi_1(C)/K_{p^n}$ then $G_{p^n} = \varprojlim \mathrm{Gal}(k(Z)/k(C))$ where $Z \to C$ is a Galois étale cover of C with Galois group $(\mathbb{Z}/p^n\mathbb{Z})^l$ for some $l \geq 1$. The group G_{p^n} has a description in terms of Witt rings of the coordinate ring of C. In fact $G_{p^n} \cong \mathrm{Hom}(W_n(\mathcal{O}_C)/P(W_n(\mathcal{O}_C)), \mathbb{Z}/p^n\mathbb{Z})$ by [Ku2, Lemma 3.3]. Here $W_n(\mathcal{O}_C)$ is the ring of Witt vectors of length n and P is a group homomorphism from $W_n(\mathcal{O}_C)$ to itself given by "Frobenius - Identity" (see Section 2 of [Ku2] for details). Hence for any $n \geq 1$, we get the following exact sequence:

$$1 \to K_{p^n} \to \pi_1(C) \to \mathrm{Hom}(W_n(\mathcal{O}_C)/P(W_n(\mathcal{O}_C)), \mathbb{Z}/p^n\mathbb{Z}) \to 1$$

Corollary 3.17. *K_{p^n} is a profinite free group of rank m*

Proof. Note that K_{p^n} is a closed normal subgroup of $\pi_1(C)$ and it is contained in $P_0(C)$. The quotient $\pi_1(C)/K_{p^n}$ is clearly an abelian group. Proposition 3.14 is also true when $\pi_1^c(C)$ is replaced by K_{p^n} and the proof is the same. Hence K_{p^n} is also profinite free of rank m in view of Theorem 3.6. □

References

[Eis] Eisenbud, David *Commutative Algebra* with a view towards algebraic geometry, Springer-Verlag, New York, 1995. xvi+785 pp.

[FJ] Fried, Michael and Jarden, Moshe *Field Arithmetic.* Third edition. Revised by Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 2008. xxiv+792 pp.

[HJ] Haran, Dan and Jarden, Moshe *The Absolute Galois Group of C(x).* Pacific Journal of Mathematics 196, pages 445-459, 2000.

[Ha1] Harbater, David *Abhyankar's conjecture on Galois groups over curves.* Invent. Math., 117, pages 1-25, 1994.

[Ha2] Harbater, David *Patching and Galois theory.* Galois groups and fundamental groups, 313-424, Math. Sci. Res. Inst. Publ., 41, Cambridge Univ. Press, Cambridge, 2003.

[Ha3] Harbater, David *Fundamental groups and embedding problems in characteristic p.* In "Recent Developments in the Inverse Galois Problem" (M. Fried, et al, eds.), AMS Contemporary Mathematics Series, vol. 186, 1995, pages 353-369.

[Ha4] Harbater, David *On function fields with free absolute Galois groups.* Crelle's Journal, vol. 632 (2009), 85-103.

[Ha5] Harbater, David *Galois groups with prescribed ramification.* Airthemetic, 1993 manuscript.

[HS] Harbater, David and Stevenson, Kate *Local Galois theory in dimension two.* Adv. Math. 198 (2005), no. 2, 623–653.

[Iwa] Iwasawa, Kenkichi *On solvable extensions of algebraic number fields.* Annals of Math. 58 (1953), 548-572.

[Ku1] Kumar, Manish *Fundamental group in positive characteristic.* PhD thesis, Purdue University, 2007, http://www.math.msu.edu/∼mkumar/Publication/thesis.pdf.

[Ku2] Kumar, Manish *Fundamental group in positive characteristic.* J. Algebra 319 (2008), no. 12, 5178–5207.

[PSZ] Pacheco, Amílcar and Stevenson, Katherine F. and Zalesskii, Pavel *Normal subgroups of the algebraic fundamental group of affine curves in positive characteristic* Math. Ann. 343 (2009), no. 2, 463–486.

[Pop] Pop, Florian *Etale Galois covers of affine smooth curves.* Invent. Math., 120(1995), 555-578.

[Pri] Pries, Rachel *Families of wildly ramified covers of curves* Amer. J. Math. 124 (2002), 737-768.

[Ray] Raynaud, Michel *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar.* Invent. Math., 116, pages 425-462, 1994.

[RZ] Luis Ribes and Pavel Zalesskii *Profinite groups* Ergebn. der Mathematik, Vol. 40, Springer-Verlag, Berlin 2000.

[SGA1] Grothendieck, Alexander *Revêtements étales et groupe fondamental (SGA 1)* Lecture Notes in Math., vol 224, Springer-Verlag, New York, 1971.

[Ta1] Tamagawa, Akio *Fundamental groups and geometry of curves in positive characteristic.* Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., 70, Amer. Math. Soc., Providence, RI, pages 297-333, 2002.

[Ta2] Tamagawa, Akio *Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups.* J. Algebraic Geom. 13, no. 4, pages 675-724, 2004.

Mathematics and Statistics Unit, Indian Statistical Institute, Bangalore, India-560059

E-mail address: manish@isibang.ac.in