Embedding problems for the étale fundamental group of curves

Poulami Mandal

Indian Statistical Institute

August 2024

Indian Statistical Institute

Doctoral Thesis

Embedding problems for the étale fundamental group of curves

Author:
Poulami Mandal

Supervisor:
Manish Kumar

A thesis submitted to the Indian Statistical Institute
in partial fulfilment of the requirements for
the degree of
Doctor of Philosophy (in Mathematics)

Theoretical Statistics & Mathematics Unit

Indian Statistical Institute, Bangalore Centre

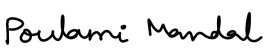
August 2024

Dedicated to my Parents

Acknowledgements

Above all, I express my gratitude to Prof. Manish Kumar, my Ph.D. advisor, for his invaluable guidance and motivation. I extend special thanks to our primary school teacher, the late Manju Didimoni, and my tutor, Nilkontho Mastermoshai, who sparked my interest in mathematics. Appreciation is also due to my seniors for helpful discussions. I am thankful to my friends Aritra, Deepak, and Susmita for their enduring support and enthusiasm. Finally, I am grateful to our institution, the Indian Statistical Institute Bangalore, for creating a conducive research environment.

Poulami Mandal
January 2024



Contents

Chapter 1

Introduction

Let X be a smooth integral projective curve over an algebraically closed field k, S be a finite set of r closed points of X, U be the complement of S in X and g be the genus of X. Let $\bar{u} \to U$ be a geometric point. We are interested in the structure of the étale fundamental group of U (see Definition 3.15) and solving embedding problems (see Definition 4.6) for U. We briefly discuss some of the properties of the étale fundamental group (for details see Chapter 4). When k is the field of complex numbers $\mathbb{C}$, Riemann's existence theorem ensures that the étale fundamental group $\pi_1^{\text{ét}}(U, \bar{u})$ is the profinite completion of the surface group $\Pi_{g,r}$, the free group generated by $2g + r - 1$ elements. In general, when $\text{char}(k) = p \geq 0$, Grothendieck proved that the maximal prime-to-p quotient of the étale fundamental group, $\pi_1^{(p')}(U)$ is isomorphic to the "prime-to-p" part of the profinite completion of $\Pi_{g,r}$. It is also known that when $\text{char}(k) = p > 0$, the maximal pro-p quotient $\pi_1^{(p)}(U)$ is the projective limit of the pro-p quotient of a free group. Even though the structures of the prime-to-p and the pro-p parts of the étale fundamental group are known, these fail to give the complete structure of $\pi_1^{\text{ét}}(U, \bar{u})$.

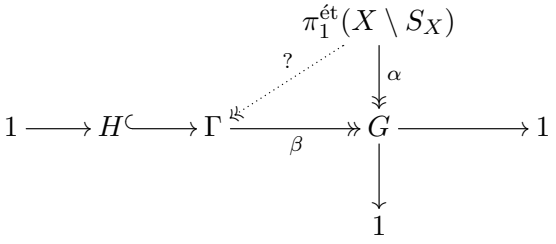
Note that the étale fundamental group is the projective limit of automorphism groups of Galois étale covers of U. Hence an effective approach to understanding it is to describe its finite quotients. Abhyankar's conjecture on affine curves (now a theorem, proved by Serre, Raynaud, and Harbater) states that these finite quotients are essentially finite groups whose maximal prime-to-p quotient is generated by at most $2g + r - 1$ elements. However, this result does not explicitly describe the relations between these finite quotients, especially how they fit in the inverse system of finite quotients. Some of these questions can be can be formally presented as embedding problems $(\Gamma \twoheadrightarrow G, \pi_1^{\text{ét}}(U) \twoheadrightarrow G)$ for finite groups Γ and G (see Section 4.2.1 for details). Solutions to such embedding problems "enlarge" a G-Galois étale cover of U to a "bigger" Γ-Galois étale cover of U that dominates the former cover.

When $\ker(\Gamma \to G)$ is a quasi-p subgroup, it was proven by Pop ([31, Theorem B]) and Harbater ([15, Corollary 4.6]) that there are proper solutions to the embedding problem

(see Proposition 4.9). Since an embedding problem can be split into a quasi-p and a prime-to-p embedding problems (Remark 4.8), we are interested in embedding problems when this kernel has order prime to p.

Now we present the main result of this thesis. Let k be an algebraically closed field of positive characteristic p, G be a finite group, $\psi : V \longrightarrow X$ be a G-Galois cover of smooth integral projective k-curves étale away from S_X and $S_V = \psi^{-1}(S_X)$. Let $r_X = |S_X|$, $r_V = |S_V|$ and g_X (resp., g_V) be the genus of X (resp., V). Let $m > 1$ be a positive integer prime to p. Here $P_m(V \setminus S_V)$ (see Definition 3.21) is a generalization of $\mathrm{Pic}(V)[m]$. In fact, it is a (right) G-module (see Subsection 5.2.1).

Theorem 1.1. *Let H be a free $\mathbb{Z}/m\mathbb{Z}$-submodule of $P_m = P_m(V \setminus S_V)$. Then the following embedding problem*



has a solution for some Γ and β if H is a G-submodule of P_m. Here α corresponds to the G-Galois cover $V \longrightarrow X$. Conversely, given a solution $\gamma : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow \Gamma$ to the above embedding problem with H a free $\mathbb{Z}/m\mathbb{Z}$-module, then the H-Galois étale cover of $V \setminus S_V$ induced from γ comes from a G-stable subgroup of P_m isomorphic to H as G-modules.

Moreover, two solutions to the embedding problem lead to the same G-submodule of $P_m(V \setminus S_V)$ iff they are equivalent.

Given H and G as above, this theorem gives us tools to form Γ-covers of U for each extension group Γ of G by H, by examining the structures of $P_m(V \setminus S_V)$ as G-modules.

We consequently get some sufficient conditions for an index-p subgroup of $\pi_1^{\text{ét}}(U)$ to be effective for some embedding problem (e.g., Corollary 5.12).

When G is a cyclic p-group, we also discuss in section 5.4 some sufficient and necessary conditions on n (Theorem 4.12, Corollaries 5.29 and 5.31) for the existence of a proper solution of an embedding problem for some extension $\Gamma = H \rtimes_\theta G$ of G by H. We describe a method of counting the minimal genus of Γ-covers corresponding to a given embedding problem (Corollaries 5.21 and 5.22). Here we also count (Theorem 4.13) the number of proper solutions for all embedding problems $\{(H \rtimes_\theta G \twoheadrightarrow G, \pi_1^{\text{ét}}(U) \twoheadrightarrow G) : \theta \text{ is any homomorphism } G \to \mathrm{Aut}(H)\}$.

We begin the thesis by declaring general notations and conventions in Chapter 2.

In Chapter 3 we recall basic definitions of the ramification theory of Dedekind domains and discuss some relevant theorems. Then we discuss briefly the definition and properties of étale fundamental groups. We also revisit the representation theory of cyclic groups over finite rings $\mathbb{Z}/m\mathbb{Z}$. Finally, we state some results on the extension of groups by an abelian group.

In Chapter 4 we discuss some classical theorems on étale fundamental groups of k-curves and some known results on embedding problems. Then we state the motivating problems and our approach towards them.

We prove some preliminary results (Lemmas 3.33, 3.37 and Propositions 3.24, 5.1) before giving a proof of Theorem 1.1 in the last chapter. Consequently, we prove certain results on effective subgroups of the étale fundamental group in Section 5.3. When H (as in the hypothesis of Theorem 1.1) is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^n$ and G is a cyclic p-group, we give a characterization of n for the existence of solutions of the above embedding problems and count the number of solutions in section 5.4. We also discuss the method of finding a cover with genus minimum among the genera of covers corresponding to the proper solutions of the above embedding problem.

Chapter 2

Notations and Conventions

All rings are commutative with unity 1, except (possibly) group rings.

Unless otherwise stated, k will denote an algebraically closed field of characteristic p.

For a set S, both $|S|$ and $\#(S)$ denote the cardinality of S.

For a scheme X, $\mathcal{O}_X$ will denote the structure sheaf of X. When X is integral, $k(X)$ will denote the function field of X.

Field extension $K \hookrightarrow L$ will be denoted by $L|K$. Similarly, extensions $A \hookrightarrow B$ of (Dedekind) domains will be denoted by $A|B$. For prime ideal Q in B and $P = A \cap Q$, we write $Q|P$. For morphism of schemes $Y \to X$, mapping $y \mapsto x$, we write $y|x$.

For a scheme X, a geometric point $\bar{x} \to X$ is a morphism $\mathrm{Spec}(K) \to X$ for a separably closed field K and $x \in X$ is the image of $\mathrm{Spec}(K) \to X$.

Covers are by definition finite generically étale morphisms of reduced schemes. Unless otherwise mentioned, covers of schemes will be smooth, and connected.

For Galois covers $Y \to X$, $\mathrm{Gal}(Y|X)$ will denote the automorphism group $\mathrm{Aut}(Y|X)$.

For a finite group H, $p(H)$ will denote the characteristic subgroup of H generated by all Sylow p-subgroups, $H/p(H)$ is the maximal prime-to-p quotient of H. When $H = p(H)$, H is called a *quasi-p* group. When $p(H)$ is trivial, H is called a *prime-to-p* group.

For a scheme U and a geometric point $\bar{u}$, $\pi_1(U, u)$ denotes the (topological) fundamental group, $\pi_1^{\text{ét}}(U, \bar{u})$ denotes the étale fundamental group.

EP is the abbreviated form of embedding problem.

The ceiling function $\lceil \cdot \rceil : \mathbb{R} \to \mathbb{Z}$ maps x to the lowest integer $\lceil x \rceil$ greater than or equal to x.

Chapter 3

Preliminaries

3.1 Ramification groups

Here, we briefly recall the notion and basic definitions related to the ramification theory (See [35], [27] for details). Let A be a Dedekind domain, K be its fraction field, L be a finite extension of K, and B be the integral closure of A in L. Then we know that B is also a Dedekind domain. For a non-zero prime ideal P in A, there are only a finite number of distinct prime ideals Q_i, $1 \leq i \leq r$, in B lying over P. In fact, there is a primary decomposition $PB = \Pi_{i=1}^{r} Q_i^{e_i}$ for unique positive integers e_i. Let f_i denote the index of the finite extension of residue fields B/Q_i over A/P, $f_i = [B/Q_i : A/P]$.

Definition 3.1. The integer $e(Q_i|P) := e_i$ is called the *ramification index* Q_i over P, $f(Q_i|P) := f_i$ is called the *inertia degree* of Q_i over P.

Let $L|K$ be a finite separable extension. Then the degree of extension $n = [L : K]$ satisfies the equation $n = \sum_{i=1}^{r} e_i f_i$. The prime ideal Q_i is *unramified* over P if $e(Q_i|P)$ is 1 and the extension of residue fields $B/Q_i|A/P$ is separable. If not, $Q_i|P$ is *ramified*. We say P is *unramified* or *unbranched* in L if all such Q_i are unramified over P. The field extension $L|K$ itself is *unramified* if every prime ideal P in K is unramified. Note that almost all prime ideals in K are unramified.

Now assume that $L|K$ is a finite Galois extension, the Galois group is $\mathrm{Gal}(L|K)$.

Proposition 3.2 ([27, Proposition 9.1])**.** *For any non-zero prime ideal P in A, $\mathrm{Gal}(L|K)$ acts transitively on the set $\{Q_i | a \leq i \leq r\}$ of prime ideals in B lying over P.*

Hence, for a fixed non-zero prime ideal P, e_i's are all equal to, say, e and f_i's are equal to, say, f. In fact, $n = [L : K]$ satisfies $n = efr$ for any non-zero prime ideal P in A.

Definition 3.3. Let Q be a prime ideal in B such that $P = Q \cap A$. The *decomposition group* of Q over P, denoted by $D(Q|P)$, is the stabilizer of Q in $\mathrm{Gal}(L|K)$, i.e.,

$$D(Q|P) = \{\sigma \in \mathrm{Gal}(L|K) : \sigma(Q) = Q\}.$$

Note that any σ in $D(Q|P)$ naturally induces an automorphism of the residue field B/Q, fixing A/P pointwise. This induces a natural homomorphism

$$D(Q|P) \to \mathrm{Gal}(B/Q|A/P).$$

Definition 3.4. The kernel of the homomorphism $D(Q|P) \to \mathrm{Gal}(B/Q|A/P)$ is called the *inertia group* of Q over P and is denoted by $I(Q|P)$.

Note that $\#(D(Q|P)) = e(Q|P)f(Q|P)$ and $\#(I(Q|P)) = e(Q|P)$.

Field extension and completion: Let $L|K$ be a finite extension, v be a discrete valuation of K, A be the valuation ring, $\mathfrak{m} = \{a \in A : v(a) \geq 1\}$ be the maximal ideal of A, B be the integral closure of A in L. Let $w_i, 1 \leq i \leq r$, be the different prolongations of v in L corresponding to maximal ideals $\mathfrak{M}_i$ lying over $\mathfrak{m}$, respectively. Let e_i and f_i be respectively the ramification index and inertia degree of $\mathfrak{M}_i|\mathfrak{m}$. Let $\hat{K}$ ($\hat{L}_i$) be the completion of K for v (respectively, of L for w_i). Then the extension $\hat{L}_i|\hat{K}$ of local fields is finite of degree $e_i f_i$. If $\hat{v}$ is the valuation of $\hat{K}$, then $\hat{w}_i$ is the unique prolongation of $\hat{v}$ in $\hat{L}_i$ and $e_i = e(\mathfrak{M}_i\hat{L}_i|\mathfrak{m}\hat{K})$, $f_i = f(\mathfrak{M}_i\hat{L}_i|\mathfrak{m}\hat{K})$.

Proposition 3.5 ([35, II §3. Corollary 4])**.** *If $L|K$ is a Galois extension, then so is $\hat{L}_i|\hat{K}$ with the Galois group $\mathrm{Gal}(\hat{L}_i|\hat{K})$ equal to the decomposition group $D(\mathfrak{M}_i|\mathfrak{m})$ in $G(L|K)$.*

3.1.1 Ramification Groups and Upper jump

Let K be a complete field with a discrete valuation v, A, $\mathfrak{m}$ be as before. Let κ denote the residue field $A/\mathfrak{m}$ and U_K denote the multiplicative group $A \setminus \mathfrak{m}$.

Let $L|K$ be a finite Galois extension and B be as above. Then L is a complete local ring. Let w be the prolongation of v in L, $\mathfrak{M}$ be the maximal ideal of B, λ denote $B/\mathfrak{M}$, U_L denote $B \setminus \mathfrak{M}$, $e = e(\mathfrak{M}|\mathfrak{m})$ and $f = f(\mathfrak{M}|\mathfrak{m})$. Let x be in B that generates B as an A-algebra.

Definition 3.6. For each integer $i \geq -1$, Let G_i denote the set

$$\begin{aligned} G_i &= \{\sigma \in \mathrm{Gal}(L|K) : w(\sigma(x) - x) \geq i + 1\} \\ &= \{\sigma \in \mathrm{Gal}(L|K) : w(\sigma(b) - b) \geq i + 1 \forall b \in B\}. \end{aligned}$$

Then the $\{G_i\}_{i\geq -1}$ form a decreasing sequence of normal subgroups of G. The group G_i is called the *i-th ramification group* of G. They define a filtration of G, called the *ramification filtration*.

Note that $G_{-1} = G$, G_0 is the inertia subgroup $I(\mathfrak{M}|\mathfrak{m})$, $G/G_0 = \mathrm{Gal}(\lambda|\kappa)$, and G_i is the trivial subgroup for large i.

Define $i_{L|K} : G \to \mathbb{Z} \cup \{\infty\}$ by $i_{L|K}(\sigma) = w(\sigma(x) - x)$. Note that $i_{L|K}(1_G) = \infty$ and $i_{L|K}(\sigma)$ is non-negative when $\sigma \neq 1_G$.

For $-1 \leq t \leq 0$, let $[G_0 : G_{\lceil t \rceil}] := [G_{-1} : G_0]^{-1}$. Define $\phi_{L|K}$ or simply $\phi : [-1, \infty) \to [-1, \infty)$ by

$$\phi(u) = \int_0^u \frac{dt}{[G_0 : G_{\lceil t \rceil}]}.$$

Then $\phi(u) = u$ when $-1 \leq u \leq 0$. For $0 < m \leq u \leq m + 1$ for a positive integer m, we have the explicit formula

$$\phi(u) = \frac{g_1 + \cdots + g_m + (u - m)g_{m+1}}{g_0}, \text{ where } g_i := \#(G_i).$$

Clearly, ϕ is a homeomorphism on $[-1, \infty)$. Let ψ be the inverse of ϕ. Then both ϕ and ψ are continuous, piecewise linear, increasing and $\phi(0) = \psi^{-1}(0) = 0$. If s is an integer, so is $\psi(s)$.

Definition 3.7. The *upper numbering* of ramification groups is defined as follows: $G^s := G_{\lceil \psi(s) \rceil}$. The *upper jumps* of the $L|K$ are the numbers s in $[-1, \infty\}$ where $G^s \neq G^{s+\epsilon}$ for all $\epsilon \geq 0$.

Note that $G^{-1} = G$, $G^0 = G_0$, and G^s is the trivial subgroup for large s.

3.2 Covers of schemes and the étale fundamental group

Let k be a field. We will assume the following convention. An *affine variety* over k is the affine scheme associated with a finitely generated algebra over k. An *algebraic variety* over k is a scheme over k such that there is a covering by a finite number of affine varieties over k. A *curve* over k is an algebraic variety over k whose irreducible components are of dimension 1.

Definition 3.8. A morphism $\pi : Y \to X$ of reduced schemes is called *generically étale* if for each generic point ζ in X and each $\eta \in \pi^{-1}(\zeta)$, π is étale at η.

Definition 3.9. Let X be a reduced scheme (respectively, a reduced k-algebra). A *cover* of X is defined to be a finite generically étale surjective morphism $\pi : Y \to X$ of reduced schemes (respectively, reduced k-algebras). We say that the cover is *connected*

(respectively, *normal*, *smooth*) if both X and Y are connected (respectively, normal, smooth).

A morphism $\pi : Y \longrightarrow X$ between smooth reduced curves is called a *cover* if it is finite and generically smooth (separable).

The cover is étale if the morphism π is étale. If S is a finite subset such that π is étale at every x in $X \setminus S$, then we say that π is *étale away from* S. Let us denote by $\mathrm{Aut}(Y|X)$ the group of automorphisms $\{\sigma : \sigma \text{ is an automorphism of } Y, \pi \circ \sigma = \pi\}$.

Definition 3.10. If G is a finite group, then a *G-Galois cover* is a cover $Y \to X$ of schemes together with a monomorphism $G \to \mathrm{Aut}(Y|X)$ via which G acts simply transitively on all the generic geometric fibres.

Notation. If H is a subgroup of G, and if $V \longrightarrow X$ is an H-Galois cover, then there is an *induced G-Galois cover* $\mathrm{Ind}_H^G(V) \longrightarrow X$, which consists of a disjoint union of $[G : H]$ copies of V, indexed by the cosets of H in G. More precisely, $\mathrm{Ind}_H^G(V) = (G \times V)/\sim$ where $(g, v) \sim (gh, h^{-1}v)$ for $g \in G$, $h \in H$ and $v \in V$.

Let the equivalence class of (g, v) in $(G \times V)/\sim$ be $[g, v]$. For g' in G, the action of g' is given by $g'([g, v]) := [g'g, v]$.

Note that when X is an integral scheme, $G \to \mathrm{Aut}(Y|X)$ becomes an isomorphism.

Unless otherwise mentioned, we will assume that a cover is connected.

Definition 3.11. We say that the reduced and irreducible covers $X_1 \longrightarrow Y, \ldots, X_n \longrightarrow Y$ are *mutually linearly disjoint* if the fibre product $X_1 \times_Y X_2 \times \ldots \times_Y X_n$ is an integral scheme.

Now let k be an algebraically closed field of positive characteristic p and X be a smooth projective integral (connected) curve over k. Let $\pi : Y \to X$ be a cover of smooth integral (connected) projective curves over k. Clearly, the extension $k(Y)|k(X)$ of function fields is a finite separable extension. Note that any open set $U \subset X$ is affine and $\mathcal{O}_X(U)$ is a Dedekind domain. Let x be a closed point in X and y be in $\pi^{-1}(x)$. Let $\hat{\mathcal{O}}_{X,x}$ (resp. $\hat{\mathcal{O}}_{Y,y}$) be the completion of the DVR $\mathcal{O}_{X,x}$ (resp. $\mathcal{O}_{Y,y}$), $\hat{K}$ (resp. $\hat{L}$) denote the fraction field of $\hat{\mathcal{O}}_{X,x}$ (resp. $\hat{\mathcal{O}}_{Y,y}$), $\mathfrak{m}$ (resp. $\mathfrak{M}$) be the maximal ideal of $\hat{\mathcal{O}}_{X,x}$ (resp. $\hat{\mathcal{O}}_{Y,y}$). As discussed in the previous section, $\hat{\mathcal{O}}_{Y,y}$ is the integral closure of $\hat{\mathcal{O}}_{X,x}$ in $\hat{L}$. The ramification index and inertia degree of y over x are respectively $e(y|x) = e(\mathfrak{M}|\mathfrak{m})$ and $f(y|x) = f(\mathfrak{M}|\mathfrak{m})$. Similarly, decomposition and inertia groups are defined.

As k is algebraically closed, $f(y|x)$ is 1. Hence $D(y|x) = I(y|x)$ and y is ramified over x if and only if $e(y|x) > 1$. Note that $\deg(\pi) = \sum_{y \in \pi^{-1}(x)} e(y|x) = [k(Y) : k(X)]$.

Definition 3.12. When $e(y|x) > 1$ for some x in X and some y in $\pi^{-1}(x)$, we say that x is a *branch point*. The finite subset of branch points of X is called the *branched locus* of the cover π.

The following result (see [38, Lemma 5.7.11]) shows that ramification kills ramification

Lemma 3.13 (Abhyankar)**.** *Let A be a discrete valuation ring with maximal ideal $\mathfrak{m}$, fraction field K, and perfect residue field κ. Let $K_i|K$, $i = 1, 2$, be two finite Galois extensions. Denote by A_i the integral closure of A in K_i, and fix maximal ideals $\mathfrak{M}_i$ lying above $\mathfrak{m}$ for $i = 1, 2$. Assume that $e(\mathfrak{M}_i|\mathfrak{m})$ are prime to the characteristic of κ, and that moreover $e(\mathfrak{M}_1|\mathfrak{m})$ divides $e(\mathfrak{M}_2|\mathfrak{m})$. Then the finite morphism $\mathrm{Spec}(C) \to \mathrm{Spec}(A_2)$ is étale, where C denotes the integral closure of A in the composite field K_1K_2.*

The following formula (see Riemann-Hurwitz formula [19, Theorem 7.27] and Hilbert different formula [19, Theorem 11.70]) helps calculate the genus of a cover of a curve.

Theorem 3.14 ([19, Theorem 11.72])**.** *Let $\pi : Y \to X$ be a G-Galois (connected) cover of smooth projective curves over an algebraically closed field k, for a finite group G. Let g_Y (resp. g_X) denote the genus of Y (resp. X). Let $G_{y,i}$ denote the i-th ramification group at $y \in Y$. Then we have the following equality*

$$2g_Y - 2 = |G|(2g_X - 2) + \sum_{y \in Y} \sum_{i \geq 0} (|G_{y,i}| - 1).$$

Note that when the above cover is tamely ramified at $\pi(y)$, $G_{y,i}$ is trivial for $i \geq 1$ and $|G_{y,0}| = e(y|\pi(y))$.

3.2.1 Étale fundamental group

Here we discuss the definition and some properties of the étale fundamental group (see [11], [24] and [38]). Let S be a locally connected, locally simply connected topological space and s be a point in S. Then the (topological) fundamental group $\pi_1(S, s)$ can be shown to be isomorphic to the automorphism group of the universal covering space of S. The motivation for the definition of the algebraic (étale) fundamental group of a scheme comes from this property of the topological fundamental group.

Let X be a connected scheme, $\bar{x} \to X$ be a geometric point of X and $\mathbf{FEt}\,/X$ denote the category of X-schemes which are finite and étale over X. For an object Y in $\mathbf{FEt}\,/X$, let $\mathrm{Fib}_{\bar{x}}(Y)$ denote the underlying set of the geometric fibre $Y \times_X \bar{x}$ of Y. A morphism $Y \to Z$ in $\mathbf{FEt}\,/X$ induces a morphism of the geometric fibres $Y \times_X \bar{x} \to Z \times_X \bar{x}$ and hence a set theoretic map $\mathrm{Fib}_{\bar{x}}(Y) \to \mathrm{Fib}_{\bar{x}}(Z)$. Thus $\mathrm{Fib}_{\bar{x}}$ becomes a functor from $\mathbf{FEt}\,/X$ to the category of sets.

Definition 3.15. The *étale fundamental group* $\pi_1^{\text{ét}}(X, \bar{x})$ is the automorphism group of the functor $\mathrm{Fib}_{\bar{x}}$ on the category $\mathbf{FEt}\,/X$.

Let F be a functor from $\mathbf{FEt}/X$ to the category of sets defined by $F(Y) = \mathrm{Hom}_X(\bar{x}, Y)$. An element of $F(Y)$ is a point $y \in Y$ lying over x with a $k(x)$-homomorphism $k(y) \to k(\bar{x})$. For Y in $\mathbf{FEt}/X$, $\mathrm{Aut}(Y|X)$ acts on $F(Y)$ by composition on the right and this action is faithful if Y is connected. When Y is connected and $\mathrm{Aut}(Y|X)$ acts transitively on $F(Y)$, $Y|X$ becomes a Galois étale cover.

The functor F is strictly pro-representable, i.e., there exists a directed set I, a projective system $\tilde{X} = (X_i, \phi_{ij})_{i\in I}$ where $X_i|X$ is Galois, $\phi_{ij} : X_j \to X_i (i \leq j)$ are epimorphisms and elements $f_i \in F(X_i)$ such that $f_i = \phi_{ij} \circ f_j$ and for any Z in $\mathbf{FEt}/X$, f_i induces an isomorphism $\varinjlim \mathrm{Hom}(X_i, Z) \to F(Z)$. When $j \geq i$, define a map $\Phi_{ij} : \mathrm{Aut}(X_j|X) \to \mathrm{Aut}(X_i|X)$ satisfying $\Phi_{ij}(\sigma)f_i = \phi_{ij} \circ \sigma \circ f_j$ for all σ in $\mathrm{Aut}(X_j|X)$. The following proposition gives us a useful alternative definition of the étale fundamental group.

Proposition 3.16 ([38, Corollary 5.4.8])**.** *The étale fundamental group $\pi_1^{\text{ét}}(X, \bar{x})$ is isomorphic to $\varprojlim \mathrm{Aut}(X_j|X)$ as profinite groups.*

In [2] Abhyankar studied this inverse system of Galois groups of U, the complement of curves C in the projective plane over a field of positive characteristic. Abhyankar also considered ([2, Section]) the system $\pi'(U)$ of Galois groups of (finite) étale covers of U that are only tamely ramified over C. In particular, generalizing a result of Zariski, he showed in [2, Section 13] that the groups in $\pi'(U)$ are abelian if C is a divisor with strict normal crossings, i.e., a union of smooth curves that intersect transversally.

Proposition 3.17. *Let X be a connected scheme. For any two geometric points $\bar{x} \to X$ and $\bar{x'} \to X$, there exists a continuous isomorphism of profinite groups $\pi_1^{\text{ét}}(X, \bar{x}) \cong \pi_1^{\text{ét}}(X, \bar{x'})$.*

Hence, for a connected scheme X, we will simply write $\pi_1^{\text{ét}}(X)$ to denote the étale fundamental group. Let us define some quotients of the étale fundamental group.

Definition 3.18. Let U be a smooth connected affine curve over an algebraically closed field k of characteristic $p > 0$. Let X be its smooth completion and S be the finite set of closed points $X \setminus U$. The *tame fundamental group* is denoted by $\pi_1^t(U)$ and is defined to be the inverse limit $\pi_1^t(U) = \varprojlim \mathrm{Aut}(Y|X)$ where $Y \to X$ varies over all connected Galois covers of X which are étale away from S and are tamely ramified over S.

The *prime-to-p* (resp., *pro-p*) *fundamental group* is denoted by $\pi_1^{(p')}(U)$ (resp., $\pi_1^{(p)}(U)$) and is defined to be the inverse limit $\varprojlim \mathrm{Aut}(Y|X)$ where $Y \to X$ varies over all connected Galois covers of X étale over U whose Galois group has order prime-to-p (resp., Galois group is a p-group).

Note that $\pi_1^{(p')}(U)$ (resp., $\pi_1^{(p)}(U)$) is the maximal prime-to-p (resp., maximal pro-p) quotient of the étale fundamental group.

3.2.2 Cyclic covers

In this section, we discuss m-cyclic covers of curves, for an integer m prime to p. Let Y be a smooth connected projective curve of genus g over an algebraically closed field k of characteristic $p > 0$. Let $m > 1$ be an integer coprime to p. Let S be a finite set in Y with r closed elements. The following definitions, notations and results can be found in [10, Chapter 3] and [40, Section 3].

We are interested in the structure of the étale cohomology group $H^1_{\text{ét}}(Y \setminus S, \mu_{\mathbf{m}}) \cong \text{Hom}(\pi_1^{\text{ét}}(Y \setminus S), \mathbb{Z}/m\mathbb{Z})$, where $\mu_{\mathbf{m}}$ is the group scheme: $\mu_{\mathbf{m}} = \text{Spec}\,\mathbb{Z}[T]/(T^m - 1)$, $\gcd(m, p) = 1$.

We denote by $\text{Pic}(Y)$ the Picard group of Y, by $\text{Div}(Y)$ the Cartier divisors of Y, by $\mathbb{Z}[S]$ the subgroup of divisors whose supports are contained in S, which can be identified with the free $\mathbb{Z}$-module with basis S. $\text{Div}_{\mathbb{Q}}(Y) := \text{Div}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $(\mathbb{Z}/m\mathbb{Z})[S] := \mathbb{Z}[S] \otimes_{\mathbb{Z}} (\mathbb{Z}/m\mathbb{Z})$, the free module over $\mathbb{Z}/m\mathbb{Z}$ with basis S.

Let $\Delta = \sum_{i=1}^n q_i D_i \in \text{Div}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$, where $q_i \in \mathbb{Q}$, D_i is a prime divisor and $n \in \mathbb{Z}_{\geq 0}$. Then let $[\Delta]$ denote $\sum_{i=1}^n [q_i] D_i \in \text{Div}(Y)$, where $[q_i]$ = the integral part of q_i. For $L \in \text{Pic}(Y)$, $m \geq 1$ and an effective Cartier divisor D such that $L^{\otimes m} \cong \mathcal{O}(-D)$ where $\mathcal{O}$ is the structure sheaf on Y. Define $L^{(i,D)} := L^{\otimes i} \otimes \mathcal{O}([\frac{i}{m} D])$.

We fix an isomorphism $L^{\otimes m} \cong \mathcal{O}(-D)$. This isomorphism allows one to define an $\mathcal{O}$-algebra structure on $\mathcal{O} \oplus L^{(1,D)} \oplus \cdots \oplus L^{(m-1,D)}$.

Proposition 3.19. *Let V be the scheme $\text{Spec}_{\mathcal{O}}(\oplus_{i=0}^{m-1} L^{(i,D)})$. Then $\pi : V \to Y$ is the normalization of the finite morphism $\text{Spec}_{\mathcal{O}}(\oplus_{i=0}^{m-1} L^i) \to Y$.*

Let G be a cyclic group of order m and σ be a generator. Let μ be a fixed primitive m-th root of unity in k. Then G acts on $\oplus_{i=0}^{m-1} L^{(i,D)}$ by $\mathcal{O}$-algebra homomorphism defined by

$$\sigma(l) = \mu^i \sigma(l)$$

for any local section l of $L^{(i,D)} \subset \oplus_{i=0}^{m-1} L^{(i,D)}$ (see [10, Section 3.9]).

Corollary 3.20. *The cyclic group G acts on V and $\pi_* O_V$. One has $V/G = Y$ and the decomposition $\pi_* O_V = \oplus_{i=0}^{m-1} L^{(i,D)}$ is the decomposition in eigenspaces.*

Hence, $V = \text{Spec}_{\mathcal{O}}(\oplus_{i=0}^{m-1} L^{(i,D)}) \longrightarrow Y$ is a G-Galois (possibly disconnected) cover of smooth curves, étale away from $D_{red} \subset S$. Let us assume that V is connected. Since $L^{\otimes m} \otimes \mathcal{O}_Y(D) = \text{div}(s) \cong \mathcal{O}_Y$ for some s in $k(Y)$, $k(V) = k(Y)(t)$ for some $t \in k(V)$ such that $t^m = s$ and $\sigma(t) = \mu t$. Let $D = \sum_{j=1}^r a_j y_j$, for positive integers a_j and points y_j in S. Then this cover is (tamely) ramified at y_j iff $\gcd(m, a_j) < m$ and the ramification index is $\frac{m}{\gcd(m, a_j)}$.

Definition 3.21. We define

$$P_m(Y \setminus S) = \frac{\{([L], D) \in \mathrm{Pic}(Y) \oplus \mathbb{Z}[S] | L^{\otimes m} \cong \mathcal{O}(-D)\}}{\{(\mathcal{O}(-D), mD) | D \in \mathbb{Z}[S]\}} \tag{3.2.1}$$

as an m-torsion abelian group.

For simplicity, we also write elements of P_m as $([L], D)$. We may assume that D is an effective Cartier divisor with support in S since the multiplicity at each point in S can be chosen from $\{0, 1, \ldots, m-1\}$.

When $S = \emptyset$ then $P_m(Y)$ is the m-torsion subgroup $\mathrm{Pic}(Y)[m]$ of the Picard group $\mathrm{Pic}(Y)$ and is isomorphic to $\mathbb{Z}/m\mathbb{Z}^{\oplus 2g}$. In general, $P_m(Y \setminus S)$ is an extension of a subgroup of $\mathbb{Z}/m\mathbb{Z}[S]$ by $P_m(Y)$. We have the following exact sequence (see [40, Equation 3.4]):

$$0 \longrightarrow \mathrm{Pic}^0(Y)[m] \hookrightarrow P_m(Y \setminus S) \xrightarrow{f} \mathbb{Z}/m\mathbb{Z}[S] \xrightarrow{\overline{\deg}} \mathbb{Z}/m\mathbb{Z} \tag{3.2.2}$$

Here the inclusion map is $[L] \mapsto ([L], 0)$, $f(([L], D)) = D \mod m$ and $\overline{\deg}(D \mod m) = \deg(D) \mod m$.

Exactness at $P_m(Y \setminus S)$ comes from the definition. To see the equation is exact at $\mathbb{Z}/m\mathbb{Z}[S]$, choose any $([L], D)$ in $P_m(Y \setminus S)$ and let C be a cartier divisor such that $L = \mathcal{O}(C)$. Then $mC + D \sim 0$ and so $m \deg(C) + \deg(D) = \deg(mC + D) = 0$. Then $\deg(D) \equiv 0 \mod m$. Hence $f(P_m(Y \setminus S)) \subset \ker(\overline{\deg})$. Conversely, suppose $D \in \mathbb{Z}[S]$ such that its image is in $\ker(\deg)$. Then $\deg(\mathcal{O}(D)) = mi$ for some integer i. Choose any L of degree i from the Picard group. Since the multiplication operator $[m]_Y : \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(Y)$ is surjective and $[L^{-m} \otimes \mathcal{O}(D)] \in \mathrm{Pic}^0(Y)$, choose $[M] \in \mathrm{Pic}^0(Y)$ such that $[M]^m = [m]_Y([M]) = [L_1^{-m} \otimes \mathcal{O}(D)]$. Then $([M \otimes L_1], D) \in P_m(Y \setminus S)$ and $f(([M \otimes L_1], D)) = D \mod m$. Hence, $f(P_m(Y \setminus S)) \supset \ker(\overline{\deg})$.

The above corollary and Equation 3.2.2 gives rise to the following proposition (see [40, Proposition 3.5]).

Proposition 3.22. *There is a bijection between the elements of $P_m(Y \setminus S)$ and $\mathbb{Z}/m\mathbb{Z}$-Galois (possibly disconnected) smooth covers of Y, étale away from S. In fact, we have isomorphisms of groups:*

$$P_m(Y \setminus S) \cong H^1_{\text{ét}}(Y \setminus S, \mu_{\mathbf{m}}) \cong \mathrm{Hom}(\pi_1^{\text{ét}}(Y \setminus S), \mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^{\oplus 2g+r-1+b^{(2)}},$$

where $b^{(2)} = 1$ if $r = 0$, $b^{(2)} = 0$ otherwise.

Definition 3.23. We say a subset B of a finite group is of *type T1* if subgroups generated by the elements in any two disjoint sets of B intersect trivially. We say that the reduced and irreducible covers $X_1 \longrightarrow Y, \ldots, X_n \longrightarrow Y$ are *mutually linearly disjoint* if the fibre product $X_1 \times_Y X_2 \times \ldots \times_Y X_n$ is an integral scheme.

Let us describe some useful properties of $P_m(Y \setminus S)$ (see Definition 3.21). The proofs are included here for the sake of completeness.

Proposition 3.24. *For Y and $P_m = P_m(Y \setminus S)$ as above:*

(i) An element of order m in P_m corresponds to a connected m-cyclic cover.

(ii) Let $B \subset P_m$ be such that every element of B is of order m and for $\lambda \in B$ let $V_\lambda \longrightarrow Y$ be the m-cyclic cover corresponding to λ. Then B is of type T1 iff the set of covers $\{V_\lambda \longrightarrow Y : \lambda \in B\}$ are mutually linearly disjoint.

(iii) Let B be as above of type T1. Let ζ be an element in the subgroup generated by B. Each connected component of the cover $V_\zeta \longrightarrow Y$ is dominated by the normalization of the fibre product of the covers $V_\lambda \longrightarrow Y$ for $\lambda \in B$.

(iv) Let B be as above of type T1 and μ be a primitive m-th root of unity in k. The subgroup generated by B acts on the normalization of the cover $\times_{\lambda \in B} V_\lambda \longrightarrow Y$ naturally which extends the automorphism defined by $\lambda = ([L], D) \in B$ of the cover $\mathrm{Spec}_{\mathcal{O}}(\oplus_{i=0}^{m-1} L^{(i,D)}) = V_\lambda \longrightarrow Y$ given by the multiplication of μ^i on sections of $L^{(i,D)}$.

Proof. Let $\psi : W \longrightarrow Y$ be a smooth disconnected cover of Y, étale over $Y \setminus S$ with an m-cyclic group action. Then all connected components of W are isomorphic and a connected component W_1 of W is an n-cyclic cover of Y and $nl = m$ where l is the number of connected components of W. Then $\exists([N], F) \in P_n$ corresponding to $W_1 \longrightarrow Y$. Then W corresponds to $([N], lF) \in P_m$ and the order of $([N], lF)$ in P_m is n.

Conversely, any element of order $n < m$ in P_m is of the form $([L^{\otimes a}], aD)$, for some $([L], D)$ of order m in P_m and $n = \frac{m}{\gcd(a,m)}$. The cover W corresponding to $([L^{\otimes a}], aD)$ is a disjoint union of $\frac{m}{n}$ number of isomorphic n-cyclic covers, each given by the normalization of $\mathrm{Spec}_{\mathcal{O}}(\oplus_{i=0}^{n-1} L^{\otimes ai})$.

For (ii) we use induction on $|B|$. Suppose $([L], D)$ and $([M], E)$ are in B and for some a and b let $([L^{\otimes a}], aD) = ([M^{\otimes b}], bE)$ be order $n > 1$. Let W, W', W'' be the m-cyclic covers corresponding to $([L], D), ([M], E), ([L^{\otimes a}], aD)$, respectively. Let $N = L^{\otimes a}$. Then a connected component V of W'' corresponds to $([N], a'D) \in P_n$ for some a'. Moreover W and W' dominate V (the $\mathcal{O}$-algebra defining V is a subalgebra of $\mathcal{O}$-algebra defining W and W').

Conversely suppose W_1 and W_2 are covers of Y corresponding to $([L], D)$ and $([M], E)$. If they are not linearly disjoint then they both dominate a connected cover $V \longrightarrow Y$ of degree $n > 1$. Let $([N], F) \in P_n$ be the element corresponding to V. Then $L^{\otimes a} = N = M^{\otimes b}$ and the cover associated to $([L^{\otimes a}], aD)$ is $\mathrm{Ind}_{\frac{m}{n}\mathbb{Z}/m\mathbb{Z}}^{\mathbb{Z}/m\mathbb{Z}}(V) = \mathrm{Ind}_{\mathbb{Z}/n\mathbb{Z}}^{\mathbb{Z}/m\mathbb{Z}}(V)$. Hence $\{([L], D), ([M], E)\}$ is not of type T1.

When $|B| = t+1 > 2$ the same argument works. Consider the connected covers $W_1 \longrightarrow Y, \ldots, W_t \longrightarrow Y$ for any t elements $\lambda_1, \ldots, \lambda_t$ of B. Then by induction hypothesis, these are mutually linearly disjoint and their normalized fibre product W is a connected cover of Y. Let $W_0 \longrightarrow Y$ be the cover corresponding to the remaining element λ_0. By looking at the algebra associated with these covers, if $W \longrightarrow Y$ and $W_0 \longrightarrow Y$ are not linearly disjoint then the common cover will correspond to a connected component of the cover associated with $a\lambda_0 = a_1\lambda_1 + \ldots a_n\lambda_t$ for some $0 < a < m$ and some $0 \leq a_i \leq m-1$.

For (iii), we again use induction on $|B|$. Let W_1 and W_2 be covers of Y corresponding to $([L], D)$ and $([M], E)$ and W be the normalization of $W_1 \times_Y W_2$. Then W is the normalization of $\mathrm{Spec}(\oplus_{i=0}^{m-1} \oplus_{j=0}^{m-1} L^{(i,D)} \otimes M^{(j,E)})$. From Lemma 3.25, we see that the $\mathcal{O}$-algebra associated to the connected component W_3 of the cover associated to $([L^{\otimes a} \otimes M^{\otimes b}], aD + bE)$ is a subalgebra of $\oplus_{i=0}^{m-1} \oplus_{j=0}^{m-1} L^{(i,D)} \otimes M^{(j,E)}$. This induces a dominating map from $W \longrightarrow W_3$.

Now, let $|B| = t+1$ be greater than 2. As before, assume that $W_i \to Y$ is the connected cover corresponding to λ_i in B, for $0 \leq i \leq t$, and W denotes the (connected) normalized fibre product of $W_1, \ldots, W_t$. Clearly W is the normalization of $\mathrm{Spec}(\oplus_{j_1=0}^{m-1} \ldots \oplus_{j_t=0}^{m-1} \left(\otimes_{i=1}^{t} L_i^{(j_i,D_i)}\right))$. By Lemma 3.25, the $\mathcal{O}$-algebra defining the normalization of $W_0 \times_Y W$ contains the $\mathcal{O}$-algebra defining the cover corresponding to an element of the subgroup generated by B.

To prove (iv), we fix μ, a primitive m-th root of unity in k. For $\lambda_j = ([L_j], D_j) \in B$, let $\mathrm{Spec}_{\mathcal{O}}(\oplus_{i=0}^{m-1} L_j^{(i,D_j)}) = V_j \longrightarrow Y$ be the smooth irreducible cover. The $\mathcal{O}$-algebra homomorphism defined by $h_j(l) = \mu^i l$ for any local section l in $L_j^{(i,D_j)}$ defines an element $h_j \in \mathrm{Aut}(V_j|Y)$ (see Corollary 3.20). Fix an isomorphism from $< \lambda_j >$ to $< h_j >$ by mapping λ_j to h_j to identify $< \lambda_j >$ with $\mathrm{Aut}(V_j|Y)$.

Now if $B = \{\lambda_1, \ldots, \lambda_t\}$, the m-cyclic covers $V_1, \ldots, V_t$ of Y are linearly disjoint. The abelian group $< B >=< \lambda_1 > \times \ldots \times < \lambda_t >$ acts component-wise on the normalised fibre product of these covers. □

Lemma 3.25. *Let $B = \{([L_i], D_i) : 1 \leq i \leq t\}$, $0 \leq a_i < m$ for each i. Then the $\mathcal{O}$-algebra associated to the connected component of the cover associated to $\sum_{i=1}^{t} a_i([L_i], D_i)$ is a subalgebra of $\oplus_{j_1=0}^{m-1} \ldots \oplus_{j_t=0}^{m-1} \left(\otimes_{i=1}^{t} L_i^{(j_i,D_i)}\right)$.*

Proof. First note that $\sum_{i=0}^{t} [x_i] \leq [\sum_{i=0}^{t} x_i]$ for non-negative rational numbers x_i and so $[\sum_{i=0}^{t} x_i D_i] - \sum_{i=0}^{t} [x_i D_i]$ is effective for effective cartier divisors D_i with support in S. Also, a cartier divisor $D - D'$ is effective $\Leftrightarrow \mathcal{O}(D - D') \subset \mathcal{O} \Leftrightarrow \mathcal{O}(D) \subset \mathcal{O}(D')$.

Given $([L], D) \in P_m(Y \backslash S)$ and positive integers a, j, d such that $md = aj$, $(L^a)^{(j,aD)} = L^{aj} \otimes \mathcal{O}([\frac{aj}{m} D]) \cong \mathcal{O}(-dD) \otimes \mathcal{O}(dD) = \mathcal{O}$.

Let ι be the least positive integer $< m$ such that $md_i = a_i\iota$ for positive integers d_i, $1 \leq i \leq t$. For $0 \leq j < m$, let $a_ij \equiv s_{ij}$ modulo m for $0 \leq s_{ij} < m$. Note that $s_{ij} \neq s_{ij'}$ if $j \neq j'$. Clearly, $a_ij \geq s_{ij}$. Then the $\mathcal{O}$ algebra associated to the cover for $\sum_{i=1}^{t} a_i([L_i], D_i)$ is

$$\oplus_{j=0}^{m-1}(\otimes_{i=1}^{t} L_i^{a_i})^{(j,\sum_i a_iD_i)} = \oplus_{j=0}^{m-1}(\otimes_{i=1}^{t} L_i^{a_ij}) \otimes \mathcal{O}([\frac{\sum_{i=1}^{t} a_ij}{m} D_i]).$$

The $\mathcal{O}$ algebra associated to the connected component is

$$\mathcal{A} = \oplus_{j=0}^{\iota-1} (\otimes_{i=1}^{t} L_i^{a_ij}) \otimes \mathcal{O}([\frac{\sum_{i=1}^{t} a_ij}{m} D_i]).$$

Note that $\otimes_{i=1}^{t} L_i^{a_ij} \hookrightarrow \otimes_{i=1}^{t} L_i^{s_{ij}}$. Since $[\frac{\sum_{i=1}^{t} a_ij}{m} D_i] - \sum_{i=1}^{t} [\frac{s_{ij}}{m} D_i]$ is effective (as $a_ij \geq s_{ij}$), $\mathcal{O}([\frac{\sum_{i=1}^{t} a_ij}{m} D_i]) \subset \mathcal{O}(\sum_{i=1}^{t} [\frac{s_{ij}}{m} D_i])$. Then

$$\begin{aligned}\mathcal{A} = \oplus_{j=0}^{\iota-1}(\otimes_{i=1}^{t} L_i^{a_ij}) \otimes \mathcal{O}([\frac{\sum_{i=1}^{t} a_ij}{m} D_i]) &\hookrightarrow \oplus_{j=0}^{\iota-1}(\otimes_{i=1}^{t} L_i^{s_{ij}}) \otimes \mathcal{O}(\sum_{i=1}^{t} [\frac{s_{ij}}{m} D_i]) \\ &= \oplus_{j=0}^{\iota-1} \otimes_{i=1}^{t} L_i^{(s_{ij}, D_i)} \\ &\hookrightarrow \oplus_{j_1=0}^{m-1} \cdots \oplus_{j_t=0}^{m-1} \left(\otimes_{i=1}^{t} L_i^{(j_i, D_i)}\right).\end{aligned}$$

□

3.3 Representation of cyclic groups over finite rings

In this section, we discuss basic representation theory (see [33], [34]). We are interested in the representation of finite cyclic groups over finite rings such that the characteristic of the ring is coprime to the order of the group.

Let R be a commutative ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be any finite multiplicative group. The group ring $R[G]$ is the set of all formal sums $\sum_{i=1}^{n} a_ig_i$, for $a_i \in R$, $1 \leq i \leq n$. Note that $1g_i$ and $0g_i$ are simply written respectively as g_i and 0. For $a_i, b_i \in R$, addition and multiplication are defined as follows:

$$(\sum_{i=1}^{n} a_ig_i) + (\sum_{i=1}^{n} b_ig_i) = \sum_{i=1}^{n} (a_i + b_i)g_i$$

and

$$(\sum_{i=1}^{n} a_ig_i)(\sum_{j=1}^{n} b_jg_j) = \sum_{k=1}^{n} (\sum_{g_ig_j=g_k} a_ib_j)g_k.$$

These operations make $R[G]$ into a ring and it is commutative if G is abelian.

An $R[G]$-module M is a R-module together with a R-linear homomorphism $\rho : R[G] \to \mathrm{End}_R(M)$, where $\mathrm{End}_R(M)$ consists of R-linear endomorphisms of M. For $g \in G$ and $m \in M$, $\rho(g)(m)$ is simply written as gm. We also say ρ or M is a *representation* of G over R or a *G-module over R*.

Definition 3.26. Two $R[G]$-modules (or representations of G over R) are called *isomorphic* if there is an isomorphism as R-modules that preserves the action of $R[G]$.

Definition 3.27. A representation given by $\rho : R[G] \to \mathrm{End}_R(M)$ is *irreducible* if M is nontrivial and it does not have a proper nontrivial submodule that is invariant under $\rho(g)$ for every $g \in G$.

Definition 3.28. A *subrepresentation* or *G-stable submodule* of M is a submodule N of M over R such that gm is in N for all m in N. A *G-stable decomposition* of M is expressing M as a direct sum of G-stable submodules. A non-empty $R[G]$-module is *indecomposable* if any G-stable decomposition of M consists of only one non-empty summand.

Proposition 3.29 (Maschke's theorem, [33, Theorem 3.4])**.** *Let $\mathbb{F}$ be a field of characteristics not dividing the order of G and M be a finitely generated $\mathbb{F}[G]$-module. Let N be a vector subspace of M stable under G. Then there exists a complement N' of N in M which is stable under G.*

A useful consequence of this theorem is the following corollary.

Corollary 3.30. *Every representation of a finite group G over a field $\mathbb{F}$ with characteristics not dividing the order of G is a direct sum of irreducible representations of G over $\mathbb{F}$.*

Definition 3.31. Let $\mathbb{F}$ be a field of characteristics not dividing the order of G and M be a representation of G over $\mathbb{F}$. By the corollary above, $M \cong \oplus_{i=1}^{n} N_i^{\alpha_i}$ (as $\mathbb{F}[G]$-modules) for irreducible non-isomorphic $\mathbb{F}[G]$-modules N_i and non-negative integers α_i. We call α_i the *multiplicity* of N_i in M.

Let l and p be two distinct prime numbers and q be a positive integer. Let us recall the following lemma about q-th cyclotomic polynomial $\Phi_q(x) = \prod_{\substack{1 \le k \le q \\ \gcd(k,q)=1}} \left(x - e^{2i\pi\frac{k}{q}}\right)$.

Lemma 3.32 ([22, Theorem 2.47])**.** *Φ_q is irreducible over $\mathbb{Q}$ and $\deg(Q_q)$ is $\phi(q)$. If $\gcd(l, q) = 1$, then $\Phi_q(x)$ factors into $\frac{\phi(q)}{d}$ distinct monic irreducible polynomials in $\mathbb{F}_l[x]$, each of the same degree d. Here d is equal to the least positive integer such that $l^d \equiv 1$ mod q.*

Let G be a cyclic group of order p^a and consider the group ring $\mathbb{F}_l[G]$. For $b \ge 1$, d_b will denote the order of l in $(\mathbb{Z}/p^b\mathbb{Z})^*$. Now we can describe irreducible representations of G over $\mathbb{F}_l$.

Lemma 3.33. *Every nontrivial irreducible $\mathbb{F}_l$-representation of the group $\mathbb{Z}/p^a\mathbb{Z}$ is of dimension d_b for some $b \leq a$.*

Proof. Let G be the cyclic group of order p^a and σ be its generator. Clearly $\sigma^{p^a} = 1_G$ implies that the minimal polynomial of σ divides $x^{p^a} - 1$. Now,

$$x^{p^a} - 1 = (x-1)\prod_{b=1}^{a} \Phi_{p^b}(x) = (x-1)\prod_{b=1}^{a} \prod_{i=1}^{\frac{p^{b-1}(p-1)}{d_b}} P_{bi}(x),$$

where $\Phi_{p^b}(x)$ is the p^b-th cyclotomic polynomial, $P_{bi}(x)$ are irreducible factors (over $\mathbb{F}_l$) of $\Phi_{p^b}(x)$ (by the lemma above) of degree d_b. Let M be a nontrivial irreducible G-representation. Then M is a simple $\mathbb{F}_l[x]$-module where multiplication by x is the nontrivial action by σ. Hence $M \cong \mathbb{F}_l[x]/P_{bi}(x)$ for some $i \in \{1, \ldots, \frac{p^{b-1}(p-1)}{d_b}\}, b \in \{1, \ldots, a\}$, by structure theorem for modules over PID. Since M is a nontrivial representation $\mathbb{F}_l[x]/(x-1)$ is ruled out. Hence the dimension of M is $d_b = \deg(P_{bi})$. □

Note. Every nontrivial irreducible $\mathbb{F}_l$-representation of $\mathbb{Z}/p^a\mathbb{Z}$ is isomorphic to $\mathbb{F}_l[x]/P_{bi}(x)$ for some $1 \leq b \leq a$ and $1 \leq i \leq p^{b-1}(p-1)/d_b$.

Now, let us assume that σ is a generator of the cyclic group G of order p^a and consider the group ring $(\mathbb{Z}/l^c\mathbb{Z})[G]$ for a positive integer c. Let us fix ζ_{p^b}, a primitive p^b-th root of unity in $\mathbb{C}$, for $1 \leq b \leq a$. Then Φ_{p^b} is the minimal polynomial of ζ_{p^b} over $\mathbb{Q}$.

Let us recall an important result for prime decomposition in number rings.

Proposition 3.34. *If m is a positive integer, ζ_m is a primitive m-th root of unity in $\mathbb{C}$ and l does not divide m, then $l\mathbb{Z}[\zeta_m]$ splits into $\frac{\phi(m)}{f}$ distinct prime ideals in $\mathbb{Z}[\zeta_m]$, where f is the order of l mod m.*

Let $r_b = \frac{p^{b-1}(p-1)}{d_b}$ for $b \geq 1$. Then, by the above proposition, $l\mathbb{Z}[\zeta_{p^b}]$ splits into r_b distinct prime ideals, say, $Q_{b1}, \ldots, Q_{br_b}$ in $l\mathbb{Z}[\zeta_{p^b}]$. Using the Chinese Remainder Theorem, $(\mathbb{Z}/l^c\mathbb{Z})[G]$ can be shown to have the following G-stable decomposition:

$$\begin{aligned}(\mathbb{Z}/l^c\mathbb{Z})[G] \cong \frac{\mathbb{Z}[x]}{(l^c, x^{p^a}-1)} &= \frac{\mathbb{Z}[x]/(x-1) \oplus (\oplus_{b=1}^{a}(\mathbb{Z}[x]/(\Phi_{p^b}(x))))}{(\overline{l^c})} \\ &= \frac{(\mathbb{Z}/l^c\mathbb{Z})[x]}{(x-1)} \oplus \frac{\mathbb{Z}[\zeta_p]}{(l^c)} \oplus \ldots \oplus \frac{\mathbb{Z}[\zeta_{p^a}]}{(l^c)} \\ &= \frac{(\mathbb{Z}/l^c\mathbb{Z})[x]}{(x-1)} \oplus (\oplus_{b=1}^{a}(\oplus_{i=1}^{r_b} \frac{\mathbb{Z}[\zeta_{p^b}]}{Q_{bi}^c})).\end{aligned}$$

Here σ acts on $\frac{\mathbb{Z}[x]}{(l^c, x^{p^a}-1)}$ by multiplication by x on the left. Similarly, the action of σ on $\frac{\mathbb{Z}[\zeta_{p^b}]}{Q_{bi}^c}$ is given by multiplication by ζ_{p^b} on the left.

Let M be a finitely generated $(\mathbb{Z}/l^c\mathbb{Z})[G]$-module. Then M admits a G-stable decomposition as above (some of the summands may be trivial):

$$M \cong \ker(\sigma - \mathbf{I}) \oplus (\oplus_{b=1}^{a}(\oplus_{j=1}^{r_b}\frac{M}{Q_{bj}^c M})). \tag{3.3.1}$$

To describe the decomposition of $M/Q_{bj}^c M$, we need the structure theorem for finitely generated torsion modules over a Dedekind domain (see [20, Theorems 9 and 10]).

Proposition 3.35. *Let R be a Dedekind domain and T be a finitely generated torsion module over R. Then*

$$T \cong R/P_1^{a_1} \oplus \ldots \oplus R/P_n^{a_n}$$

for uniquely determined prime ideals P_i of R and non-negative integers a_i.

Let us describe the structure further. Let $J = \{r \in R | rT = 0\}$ be the annihilator of T. Let $J = P_1^{s_1} \ldots P_n^{s_n}$ be its prime factorization in R. Then

$$R/J \cong R/P_1^{s_1} \oplus \ldots \oplus R/P_n^{s_n}.$$

Then T, as an R/J module, decomposes into

$$T \cong T/P_1^{s_1}T \oplus \ldots \oplus T/P_n^{s_n}T,$$

where each $T/P_i^{s_i}T$ can be identified with the submodule $\{m \in T | P^{s_i}T = 0\}$. To describe the structure of each summand above is the same as describing the structure of a finitely generated module over an Artinian quotient ring $R/P^s \cong R_P/P^s R_P$ for any prime ideal P. This is given by the following result.

Proposition 3.36. *Let T be a finitely generated module over a quotient ring $S/(t^s)$, where S is a DVR and t is a generator of the maximal ideal. Then T is isomorphic to a direct sum of modules $S/(t^j)$, where $1 \leq j \leq s$. Let f_i be the dimension of the vector space $t^iT/t^{i+1}T$ over $R/(t)$. Then the number of summands of type $S/(t^j)$ appearing in the decomposition of T is $f_{j-1} - f_j$.*

Note. When $S = R_P$ in the above proposition, and $(t) = PR_P$, $S/(t^j)$ is isomorphic to R/P^j.

Now we go back to Equation (3.3.1) and apply the above results on $M/Q_{bj}^c M$.

Lemma 3.37. *Let the hypothesis be as before Equation (3.3.1). Then M can be expressed as a direct sum of indecomposable G-submodules isomorphic to $\mathbb{Z}/l^i\mathbb{Z}$, $\mathbb{Z}[\zeta_{p^b}]/Q_{bj}^i, 1 \leq i \leq c$, $1 \leq b \leq a$. The number of direct summands isomorphic to $\mathbb{Z}/l^i\mathbb{Z}$ is $f'_{i-1} - f'_i$ where $f'_i = \dim_{(\mathbb{Z}_l/l\mathbb{Z}_l)}(\frac{l^i M^G}{l^{i+1}M^G})$. The number of summands isomorphic to $\mathbb{Z}[\zeta_{p^b}]/Q_{bj}^i$ is $f_{b,i-1,j} - f_{bij}$ where $f_{bij} = \dim_{(\mathbb{Z}[\zeta_{p^b}]/Q_{bj})}(\frac{Q_{bj}^i N_{bj}}{Q_{bj}^{i+1}N_{bj}})$ and $N_{bj} = M/Q_{bj}^c M$.*

Proof. Let $R = \mathbb{Z}[\zeta_{p^b}]$. As N_{bj} is a R/Q_{bj}^c-module and $R/Q_{bj}^c \cong R_{Q_{bj}}/Q_{bj}^c R_{Q_{bj}}$, N_{bj} is a torsion module over $R_{Q_{bj}}$. By the propositions above, we have the following decomposition as G-modules:

$$N_{bj} \cong \oplus_{i=1}^{c}(R_{Q_{bj}}/(Q_{bj}^i))^{f_{b,i-1,j}-f_{bij}} \cong \oplus_{i=1}^{c}(R/Q_{bj}^i)^{f_{b,i-1,j}-f_{bij}}.$$

Note that $\ker(\sigma - \mathrm{Id})$ is a $\mathbb{Z}/l^c\mathbb{Z}$-module with trivial G-action. Then again, $M^G = \ker(\sigma - \mathrm{Id}) \cong \oplus_{i=1}^{c} \oplus^{f'_{i-1}-f'_i} (\mathbb{Z}/l^i\mathbb{Z})$. Then we get the G-stable decomposition into indecomposable (or zero) G-submodules:

$$M \cong (\oplus_{i=1}^{c}(\mathbb{Z}/l^i\mathbb{Z})^{f'_{i-1}-f'_i}) \oplus (\oplus_{b=1}^{a} \oplus_{j=1}^{r_b} \oplus_{i=1}^{c}(\mathbb{Z}[\zeta_{p^b}]/Q_{bj}^i)^{f_{b,i-1,j}-f_{bij}}). \tag{3.3.2}$$

□

3.4 Group cohomology and group extension

We briefly discuss some basic definitions and results in the theory of group cohomology (see [44]).

Definition 3.38. Let A be an object of an abelian category $\mathcal{A}$. A *projective resolution* of A is a complex $P.$ with $P_i = 0$ for $i < 0$, together with an augmentation map $\epsilon : A \leftarrow P_0$ so that each P_i is projective and the augmented complex

$$0 \longleftarrow A \xleftarrow{\epsilon} P_0 \xleftarrow{d} P_1 \longleftarrow P_2 \longleftarrow \cdots$$

is exact.

Lemma 3.39. *If an abelian category $\mathcal{A}$ has enough projectives, then every object A in $\mathcal{A}$ has a projective resolution.*

Let $F : \mathcal{B} \to \mathcal{A}$ be a left exact contravariant functor between abelian categories such that $\mathcal{B}$ has enough projectives. For an object B in $\mathcal{B}$ choose a projective resolution $B \leftarrow P.$. The *right derived functor* $R^iF(B)$ is defined by $R^iF(B) = H^i(F(P))$. Note that $R^*F(B)$ is independent of the choice of projective resolution.

Proposition 3.40. *The derived functors R^*F form a universal cohomological δ-functor.*

Definition 3.41. Let G be a group. A *(right) G-module* is an abelian group A on which G acts on the right.

For g in G and a in A we simply write $a \cdot g$ or ag for the (right) action of g on a. For another G-module B, let $\mathrm{Hom}_G(B, A)$ denote the G-set maps from B to A. Then we obtain a category **mod**-G of (right) G-modules. This category can be identified with the category of $\mathbb{Z}[G]$-modules, with G acting on the right.

Note that **mod**-G is an abelian category with enough projectives.

Definition 3.42. A *trivial G-module* is an abelian group A with trivial G-action, i.e. $a \cdot g = a$ for all a in A and g in G.

Notation. Let us denote a free G-module on a set S of symbols by $< S >_G$. Note that $< S >_G \cong \oplus_{s \in S} \mathbb{Z}[G]$.

Now we describe two free (hence projective) resolutions of the trivial G-module $\mathbb{Z}$ in **mod**-G. They are called the normalized and unnormalized bar resolutions, respectively.

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\epsilon} B_0 \xleftarrow{d} B_1 \xleftarrow{d} B_2 \qquad \cdots, \tag{3.4.1}$$

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\epsilon} B_0^u \xleftarrow{d} B_1^u \xleftarrow{d} B_2^u \qquad \cdots. \tag{3.4.2}$$

Here $B_0 = B_0^u = \mathbb{Z}[G]$ with G-action on the right.

For $n \geq 1$, consider the set of symbols $S_n^u = \{[g_1 \otimes \cdots \otimes g_n] : g_i \in G \text{ for } 1 \leq i \leq n\}$. Then we get the G-module $B_n^u =< S_n^u >_G$. Denote by B_n a quotient of B_n^u, $B_n := B_n^u / B_n'$, where $B_n' =< \{[g_1 \otimes \cdots \otimes g_n] : g_i = 1_G \text{ for some } 1 \leq i \leq n\} >_G$. B_n is the free G-module over the set of symbols $\{[g_1 | \cdots | g_n] : \text{ where } g_i \in G \setminus \{1_G\} \text{ for} 1 \leq i \leq n\}$.

Let $[\cdot]$ denote 1_G in $\mathbb{Z}[G]$. The map $\epsilon : B_0 \to \mathbb{Z}$ (or $\epsilon : B_0^u \to \mathbb{Z}$) sends $[\cdot]$ to 1. For $n \geq 1$ the differential $d : B_n^u \to B_{n-1}^u$ is defined by $d = \sum_{i=0}^{n} (-1)^i d_i$, where:

$$\begin{aligned}
&d_0([g_1 \otimes \cdots \otimes g_n]) = [g_1 \otimes \cdots \otimes g_{n-1}] g_n; \\
&d_i([g_1 \otimes \cdots \otimes g_n]) = [g_1 \otimes \cdots \otimes g_{n-i} g_{n-i+1} \otimes \cdots \otimes g_n], 0 < i < n; \\
&d_n([g_1 \otimes \cdots \otimes g_n]) = [g_2 \otimes \cdots \otimes g_n].
\end{aligned}$$

Similarly, for the complex $B.$ the differentials are defined as above, except for $0 < i < n$,

$$d_i([g_1 \otimes \cdots \otimes g_n]) = \begin{cases} [g_1 | \cdots | g_{n-i} g_{n-i+1} | \cdots | g_n] & \text{when } g_{n-i} g_{n-i+1} \neq 1_G, \\ 0 & \text{when } g_{n-i} g_{n-i+1} = 1_G. \end{cases}$$

Since $d_i \circ d_j = d_{j-1} \circ d_i$ when $i \leq j-1$, we have $d \circ d = 0$. Hence $B_\bullet^u$ is a chain complex. Since $d(B_n') \subset B_{n-1}'$, $B_\bullet$ is a quotient chain complex.

Proposition 3.43. *The sequences* (3.4.1) *and* (3.4.2) *are exact. Thus both $B_\bullet$ and $B_\bullet^u$ are free resolutions of $\mathbb{Z}$ in* ***mod***-G.

Proof. Consider the group homomorphisms s_n defined by

$$\begin{aligned}
&s_1 : \mathbb{Z} \to B_0^u, 1 \mapsto [\cdot]; \\
&s_n : B_n^u \to B_{n+1}^u, [g_1 \otimes \cdots \otimes g_n] g_{n+1} \mapsto [g_1 \otimes \cdots \otimes g_{n+1}], \text{ for } n \geq 0.
\end{aligned}$$

It is easy to see that $\epsilon s_1 = \mathrm{Id}_{\mathbb{Z}}$, $ds_0 + s_{-1}\epsilon = id_{B_0^u}$ and $(ds_n + s_{n-1}d)([g_1 \otimes \cdots \otimes g_n]g_{n+1}) = [g_1 \otimes \cdots \otimes g_n]g_{n+1}$. Hence, $\{s_n\}$ forms a chain contraction of (3.4.2). Thus (3.4.2) is split exact as a chain complex of abelian groups. Similar proof works for (3.4.1). □

Let A be an object of **mod**-G. Note that $\mathrm{Hom}_G(-, A)$ is a left exact contravariant functor on **mod**-G. $\mathrm{Hom}_G(B_n^u, A)$ consists of n-cochains, i.e., set maps $\phi : G^n \to A$ that extend bilinearly on B_n^u as $\mathbb{Z}[G]$-module. Similarly, $\mathrm{Hom}_G(B_n, A)$ consists of normalized n-cochains, i.e., n-cochains ϕ such that $\phi(g_1, \cdots, g_n)$ becomes 0 whenever some g_i is 1_G. The differential $d : \mathrm{Hom}_G(B_n^u, A) \to \mathrm{Hom}_G(B_{n+1}^u, A)$ is defined by $\phi \mapsto d\phi$,

$$(d\phi)(g_0, \cdots, g_n) = (\phi(g_0, \cdots, g_{n-1})) \cdot g_n + \sum_{i=1}^{n} (-1)^i \phi(\cdots, g_{n-i}g_{n-i+1}, \cdots) + (-1)^{n+1}\phi(g_1, \cdots, g_n).$$

Similarly, the differential d is defined on $\mathrm{Hom}_G(B_n, A)$. We denote by $Z^n(G; A)$ the n-cocycles, i.e., the n-cochains ϕ such that $d\phi = 0$. $B^n(G; A)$ denotes the set of n-coboundaries, the image of $n-1$-cocycles.

Notation. $H^*(G; A) := H^*(\mathrm{Hom}_G(\mathbb{Z}, A))$, the cohomology of either $\mathrm{Hom}_G(B_n^u, A)$ or $\mathrm{Hom}_G(B_n, A)$. Thus $H^n(G; A) = Z^n(G; A)/B^n(G; A)$.

We are interested in $H^2(G; A)$. Note that $Z^2(G; A)$ consists of all 2-cochains $\phi : G \times G \to A$ such that

$$\phi(1_G, g) = \phi(g, 1_G) \text{ and}$$
$$0 = (d\phi)(f, g, h) = \phi(f, g) \cdot h - \phi(f, gh) + \phi(fg, h) - \phi(g, h), \text{ for } f, g, h \in G.$$

$B^2(G; A)$ is the set of 2-cochains $\phi : G \times G \to A$ such that for every $f, g \in G$ and some 1-cochain ψ

$$\phi(1_G, g) = \phi(g, 1_G) \text{ and } \phi(f, g) = (d\psi)(f, g) = (\psi(f)) \cdot g - \psi(fg) + \psi(g).$$

3.4.1 Group extension by an abelian kernel

Definition 3.44. Let $(G, \cdot)$ be a (multiplicative) group and $(A, +)$ be an (additive) abelian group. A *group extension of G by A* is a short exact sequence

$$0 \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

of groups. The extension *splits* if π has a section $\sigma : G \to E$.

Note that $(A, +)$ is a subgroup of $(E, \cdot)$, $+$ and $\cdot$ denote the same group operation in E. The notation $+$ is used in between elements specifically in A as they commute.

Given a group extension E of G by A, G acts on the right on A by conjugation in E. For a in A and g in G, $a \mapsto a^g := \tilde{g}^{-1} a \tilde{g}$ for any $\tilde{g}$ in E such that $\pi(\tilde{g}) = g$. This action makes A a (right) G-module.

Note that an extension $0 \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$ splits if and only if E is isomorphic to the semidirect product $A \rtimes_\theta G$ for the homomorphism $\theta : G \to \mathrm{Aut}(A)$ given by $\theta(a) = a^g$.

Definition 3.45. Two extensions $0 \longrightarrow A \longrightarrow E_i \xrightarrow{\pi} G \longrightarrow 1$, $i = 1, 2$, are *equivalent* if there exists an isomorphism $\phi : E_1 \cong E_2$ so that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E_1 & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \cong \downarrow \phi & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E_2 & \xrightarrow{\pi} & G & \longrightarrow & 1. \end{array}$$

Given a G-module A, how many extensions (up to equivalence) of G by A are there such that the induced G-action on A is the same as the G-module structure of A, i.e., $a^g = a \cdot g$?

Given an extension $0 \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$, choose a lift Φ_g in E for every g in G such that $\pi(\Phi_g) = g$ and $\Phi_{1_G} = 1_E$. Define a set map $[\cdot, \cdot] : G \times G \to A$,

$$[f, g] = \Phi_{fg}^{-1} \Phi_f \Phi_g.$$

Note that $\pi(\Phi_{fg}^{-1} \Phi_f \Phi_g) = (\pi(\Phi_{fg}))^{-1} \pi(\Phi_f) \pi(\Phi_g) = (fg)^{-1} fg = \mathrm{Id}_G$. Hence $[g, h] \in \ker \pi = A$. We call such a set map a *factor set*.

Proposition 3.46. *Let A be an object of **mod**-G. A set function $[\cdot, \cdot] : G^2 \to A$ is a factor set if and only if $[\cdot, \cdot] \in Z^2(G; A)$.*

Proof. If $[\cdot, \cdot]$ is a factor set, then for any $f, g, h \in G$, we have $[1_G, g] = \Phi_g^{-1} \Phi_g = \mathrm{Id} = [g, 1_G]$ and

$$\begin{aligned} &[f, g] \cdot h - [f, gh] + [fg, h] - [g, h] \\ &\quad = \Phi_h^{-1} \Phi_{fg}^{-1} \Phi_f \Phi_g \Phi_h - \Phi_{fgh}^{-1} \Phi_f \Phi_{gh} + \Phi_{fgh}^{-1} \Phi_{fg} \Phi_h - \Phi_{gh}^{-1} \Phi_g \Phi_h \\ &\quad = (\Phi_{fgh}^{-1} \Phi_{fg} \Phi_h + \Phi_h^{-1} \Phi_{fg}^{-1} \Phi_f \Phi_g \Phi_h) - (\Phi_{fgh}^{-1} \Phi_f \Phi_{gh} + \Phi_{gh}^{-1} \Phi_g \Phi_h) \\ &\quad = \Phi_{fgh}^{-1} \Phi_f \Phi_g \Phi_h - \Phi_{fgh}^{-1} \Phi_f \Phi_g \Phi_h = 0. \end{aligned}$$

Hence $[\cdot, \cdot]$ is an element of $\mathbb{Z}^2(G; A)$.

Conversely, suppose $[\cdot,\cdot]$ is a normalized 2-cocycle. Let $E := G \times A$ as a set. Define an operation on E by:

$$(f,a)\cdot(g,b) = (fg, a\cdot g + [f,g] + b).$$

It can be shown that the above operation is associative, $(1_G, 0)$ is the identity element and the inverse of (f,a) is $(f^{-1}, -a\cdot f^{-1} - [f,f^{-1}]) = (f^{-1}, -a\cdot f^{-1} - [f^{-1},f]\cdot f^{-1})$. Then E is a group, A is isomorphic to $\{1_G\}\times A$, and G is isomorphic to the quotient of E by $\{1_G\}\times A$. Thus E is a group extension of G by A and the factor set arising from this is the 2-cocycle we began with. □

Theorem 3.47 (Classification Theorem)**.** *The equivalence classes of extensions of a group G by an abelian group A are in bijective correspondence with $H^2(G;A)$.*

In fact, given an extension $0 \to A \to E \to G \to 1$, any choice of factor set $[\cdot,\cdot] : G\times G \to A$ modulo $B^2(Z;A)$ determines the extension (up to equivalence) uniquely.

3.4.1.1 Group Extension by a non-abelian kernel

We quickly discuss the theory of group extensions of G by a (possibly non-abelian) group H. Let $1 \to H \to \Gamma \to G \to 1$ be an extension and $\Phi_\sigma \in \Gamma$ be a lift of $\sigma \in G$, $\Phi_{1_G} = 1_\Gamma$. Let $\alpha : G \longrightarrow \mathrm{Aut}(H)$ be defined by $\alpha(\sigma)(h) := \Phi_\sigma^{-1}\circ h \circ \Phi_\sigma$, for every h in H; $\alpha(1) := \mathrm{Id}_H$. Let $\theta : G \longrightarrow \mathrm{Aut}(H)/\mathrm{Inn}(H)$ be the group homomorphism defined by $\theta(\sigma) := [\alpha(\sigma)]$. Then (H,θ) is a *G-kernel with centre $Z(H)$*. This θ induces a group homomorphism $\theta_0 : G \longrightarrow Z(H)$. Each G-kernel determines in invariant fashion a cohomology class of 3-cocycle. Let $f_3 \in Z^3(G, Z(H))$ be such a cocycle determined by (H,θ) and $F_3(H,\theta) = [f_3]$ be the cohomology class in $H^3(G;Z(H))$. Here Γ is a group extension of G by the *kernel* (H,θ). So, (H,θ) is extendible. Then $F_3(H,\theta) = 1$. Then (H,θ) can be realised as a kernel of an extension group E of G (see [9], the proof of the converse part of the theorem 8.1). Note that this construction of E depends only on G, H and α.

Theorem 3.48 ([9, Theorem 11.1])**.** *If (H,θ) is an extendible kernel, then the classes of (G,H)-equivalent extensions (E_1,ϕ_1) of G may be put into one-one correspondence with $H^2(G,Z(H))$ and hence into one-one correspondence with the classes of $(G,Z(H))$-equivalent extensions of G by the center $Z(H)$ of H (with given operators of G on $Z(H)$).*

The following is an example of when a group extension can only be a semidirect product.

Theorem 3.49 (Schur-Zassenhaus)**.** *If G and H are groups of relatively prime orders, any extension of G by H is split.*

Chapter 4

Motivation and main problems

Here we discuss some of the known results about the structure of the étale fundamental group of smooth connected curves and Abhyankar's conjectures (see [38], [18]).

4.1 The fundamental group of complex curves

Let X be a compact Riemann surface (equivalently, a smooth projective complex curve) of genus g, $U = X \setminus \{x_1, \cdots, x_n\}$ be an open subset of X obtained by removing n points from X. We know that the fundamental group of U has the following presentation:

$$\Pi_{g,n} := \pi_1(X \setminus \{x_1, \cdots, x_n\}) =< a_1, \cdots a_g, b_1, \cdots, b_g, c_1, \cdots, c_n \\ : a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1} c_1 \cdots c_n = 1 > .$$

Riemann's existence theorem translates the results of the topological fundamental group, which can be obtained via loops into the results about the étale covers and étale fundamental group.

Theorem 4.1 (Explicit form of Riemann's existence theorem [16, Corollary 2.1.2])**.** *Let U be $\mathbb{P}^1_{\mathbb{C}} \setminus \{x_1, \cdots, x_n\}$ for a non-negative integer n. Let G be a finite group and $\mathcal{C}$ be the set of equivalence classes $\{\underline{g} = (g_1, \cdots, g_n) \in G^n :< g_1, \cdots, g_n >= G\}/\sim$ where $\underline{g} \sim \underline{g'}$ if $\exists h \in G$ such that $g'_i = h g_i h^{-1}$ for $1 \leq i \leq n$. Then there is a bijection between the G-Galois connected étale covers of U and elements of $\mathcal{C}$. Moreover, this correspondence is functorial under the operation of taking quotients of G, and also under the operation of deleting more points from $\mathbb{P}^1_{\mathbb{C}}$.*

Note that, giving a homomorphism $\pi_1(U) \twoheadrightarrow G$ is the same as giving a G-Galois (topological) connected covering space of U, and these are naturally in bijection with $\mathcal{C}$, and this is naturally bijective to G-Galois connected étale covers of U by Riemann's

Existence Theorem. In fact $\pi_1^{\text{ét}}(U)$ is continuously isomorphic to the profinite completion of $\pi_1(U) = \Pi_{g,n}$.

4.2 Étale fundamental group of k-curves

Let k be an algebraically closed field of characteristic $p \geq 0$.

Grothendieck's result (see [11, XIII, Corollaire 2.12]) generalizes Riemann's existence theorem for an n-punctured curve over an algebraically closed field:

Theorem 4.2. *Let X be an integral proper normal k-curve of genus g, $p \geq 0$, S be a finite (possibly empty) subset of closed points of X, U be the open curve $X \setminus S$ and $\#(S) = n \geq 0$. Then $\pi_1^{(p')}(U)$ is isomorphic to $\widehat{\Pi}_{g,n}^{(p')}$, the profinite prime-to-p completion of $\Pi_{g,n}$.*

Clearly, when $p > 0$, the étale fundamental group is much bigger than $\widehat{\Pi}_{g,n}^{(p')}$. The following theorem describes the structure of the pro-p part of $\pi_1^{\text{ét}}(U)$.

Theorem 4.3 ([5, Chapitre 17, Propositions 2.1, 2.2])**.** *Let U be an integral normal k-curve, $p > 0$. Then $\pi_1^{(p)}(U)$ is the maximal pro-p-quotient of the profinite completion of a free group of rank r. This r is finite (equal to the p-rank of the Jacobian variety of U) when U is a proper k-curve, r is infinite (equal to the cardinality of k) if U is affine.*

The pro-p and prime-to-p parts of $\pi_1^{\text{ét}}(U)$ do not describe the full structure of the étale fundamental group. Since this is a profinite group, one way would be to describe its finite quotients (or, equivalently, the finite Galois étale covers of U). When N is a positive integer, X is an integral proper normal curve over k and $p > 0$, there are only finitely many Galois étale covers of X of degree N (see [23, Théorème 4]). Abhyankar's conjecture ([1, Conjecture 1]) gives a sufficient and necessary condition for a finite group to be a quotient of the étale fundamental group of an affine curve. The "if" (sufficient) part comes from Theorem 4.2 . The proof of the "only if" (necessary) part involves contributions from Serre ([36]), Raynaud ([32, Théorème 2.2.1]) and Harbater ([14, Theorem 6.2] and [15, Corollary 4.7]).

Theorem 4.4 (Abhyankar's conjecture on affine curves)**.** *Let U be a smooth affine k-curve, $p > 0$, X be the smooth completion of U, the genus of X be g and $S = X \setminus U$ be of cardinality r. Then a finite group G is the Galois group of an unramified cover of U if and only if $G/p(G)$ has a generating set of size at most $2g + r - 1$.*

Abhyankar gave many examples (see [3]) of Galois étale covers of $\mathbb{A}_k^1$, for the Galois group equal to various permutation groups, alternating groups, projective special linear groups.

Nori ([18, Theorem 3.5]) showed that for any semisimple, simply connected algebraic group G over $\mathbb{F}_q$, where q is a power of p, $G(\mathbb{F}_q)$ is a Galois group of a Galois étale cover of $\mathbb{A}^1_k$.

Abhyankar's affine arithmetical conjecture ([4, Section 16]) states that for a finite group G, $\pi_1^{\text{ét}}(\mathbb{A}^1_{\mathbb{F}_p}) \twoheadrightarrow G$ iff $\pi_1^{\text{ét}}(\mathbb{A}^1_k) \twoheadrightarrow G$. The "only if" part of this conjecture is still open. Abhyankar extended this conjecture to the total arithmetical conjecture: every finite group is a finite quotient of the absolute Galois group of $\mathbb{F}_p(X)$.

An interesting way to understand the relationship of the fundamental group $\pi_1^{\text{ét}}(U)$ with U is via anabelian geometry, first introduced by Grothendieck ([12]). Here, it was conjectured that the curve U, as a scheme, should be determined (up to isomorphism of schemes) by the profinite group $\pi_1^{\text{ét}}(U)$. In characteristic 0, Theorem 4.2 implies that the étale fundamental group of a proper normal curve is completely determined by the genus of the Riemann surface associated with the curve. But, in higher characteristic cases, the result is very interesting. In fact, the anabelian conjecture by Grothendieck was proved for hyperbolic curves over finite fields by Tamagawa ([39]) and Mochizuki ([25]). Over the algebraic closure of a finite field, the consequence is very different:

Theorem 4.5 (Tamagawa ([41]))**.** *Let* Π *be a profinite group. There are only finitely many proper normal curves of genus* $g \geq 2$ *over* $\bar{\mathbb{F}}_p$ *with étale fundamental group isomorphic to* Π*.*

More works on Grothendieck's anabelian conjecture can be found in [43], [37].

There have been different attempts to understand $\pi_1^{\text{ét}}(U)$ in various ways ([6, Theorem 1.1], [7], [28], [29]). In [30], Pop described certain results (analogous to the Riemann existence theorem) on $\pi_1^{\text{ét}}(\mathbb{P}^1_K \setminus S)$ for a henselian field K of rank 1 and and a specific closed subset S, with the action of $\text{Gal}(K^{sep}|K)$. For discussions on patching methods, formal and rigid geometry, and semistable reduction see [16], [5].

To study G-covers of a curve X, branched at S, for a fixed Galois group G, one needs to examine the ramification groups at the branch points. Since the ramification groups contribute to the degree of the ramification divisor and consequently the genus of the cover, the existence of G-covers with "small" ramification at particular points can be understood by finding G-covers with "small" genus. Some A_p-Galois étale covers of $\mathbb{A}^1_k$ with a given ramification group at infinity were constructed in [26, Theorem 4.6] and it was shown to be of minimal genus over all A_p-Galois étale covers of $\mathbb{A}^1_k$. Similar result for A_d-covers ($p+2 \leq d < 2p$) can be found in [26, Theorem 4.9] and [8, Corollary 2.2]. In [13], for a prime number l other than p, $(\mathbb{Z}/l\mathbb{Z})^{\oplus n} \rtimes \mathbb{Z}/p\mathbb{Z}$-Galois covers of $\mathbb{P}^1_k$ ramified only at infinity with minimal genus were constructed.

Another approach to describe the étale fundamental group and its finite quotients is to consider embedding problems.

4.2.1 Embedding problems

Definition 4.6. For finite groups Γ, G, H, an *embedding problem* (EP) for a profinite group Π is a pair of epimorphisms $(\beta : \Gamma \twoheadrightarrow G, \alpha : \Pi \twoheadrightarrow G)$, with $H = \ker(\beta)$.

$$\begin{array}{ccccccccc} & & & & & & \Pi & & \\ & & & & & \overset{?}{\nearrow} & \downarrow{\scriptstyle \alpha} & & \\ 1 & \longrightarrow & H & \hookrightarrow & \Gamma & \xrightarrow[\beta]{} & G & \longrightarrow & 1 \\ & & & & & & \downarrow & & \\ & & & & & & 1 & & \end{array} \tag{4.2.1}$$

A *proper solution* to the EP is an epimorphism $\gamma : \Pi \twoheadrightarrow \Gamma$ so that the above diagram commutes.

Let U be a smooth integral k-curve, k is an algebraically closed field of characteristic $p > 0$. Consider the embedding problem $(\mathcal{E})$ for the étale fundamental group $\pi_1^{\text{ét}}(U)$, $(\beta : \Gamma \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(U) \twoheadrightarrow G)$.

$$\mathcal{E} = (\beta : \Gamma \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(U) \twoheadrightarrow G) \tag{$\mathcal{E}$}$$

Let X be the smooth completion of U, S be the complement of U in X, α correspond to the G-Galois cover $\pi : Y \to X$, étale away from S. Then, giving a proper solution to the above EP $(\mathcal{E})$ means giving a Γ-Galois connected cover $\psi : W \to X$, étale away from S such that W dominates Y, and we get an embedding of $k(Y)$ in $k(W)$ as H-Galois $k(X)$-algebras (Note that G-action on $k(Y)$ is the same as the action induced by restricting the action of Γ on the image of $k(Y)$ in $k(W)$).

By considering an EP, one can study not only the finite quotients of the profinite group $\pi_1^{\text{ét}}(U)$ but also how they fit in the inverse system of quotients of the fundamental group.

Definition 4.7. The embedding problem (4.2.1) is said to be *prime-to-p* (resp. *quasi-p*) if H is a prime-to-p (resp. quasi-p) group; it is *non-trivial* if H is non-trivial; it is *split* if β has a section.

Remark 4.8. From the EP (4.2.1), we obtain a prime-to-p EP $\mathcal{E}' = (\beta' : \Gamma/p(H) \twoheadrightarrow G, \alpha)$ with $\ker(\beta') = H/p(H)$. Let γ' be a proper solution to the EP $\mathcal{E}'$.

$$\begin{array}{ccccccc} p(H) & = & p(H) & & & & \Pi \\ \downarrow & & \downarrow & & \overset{?}{\nearrow} & & \downarrow{\scriptstyle \alpha} \\ H & \hookrightarrow & \Gamma & \xrightarrow{\beta} & & \twoheadrightarrow & G \\ \downarrow & & \downarrow{\scriptstyle \beta''} & & \overset{\gamma'}{\nearrow} & & \| \\ H/p(H) & \hookrightarrow & \Gamma/p(H) & & \xrightarrow{\beta'} & & G \end{array}$$

Then we have a quasi-p EP $\mathcal{E}^{(p)} = (\beta'' : \Gamma \twoheadrightarrow \Gamma/p(H), \gamma')$, where $\beta' \circ \beta'' = \beta$ and $\ker(\beta'') = p(H)$. The EP (4.2.1) splits into the prime-to-p EP $\mathcal{E}'$ and the quasi-p EP $\mathcal{E}^{(p)}$.

Proposition 4.9. *All (finite) quasi-p embedding problems over smooth connected affine k-curves ($p > 0$) can be solved properly and in $\#(k)$ non-isomorphic ways if the embedding problem is non-trivial.*

This was proven by Pop [31, Theorem B] (also see the proof by Harbater [15, Corollary 4.6]).

The result below by Harbater and Stevenson is about EP restricted to open subgroups of the étale fundamental group.

Theorem 4.10 ([17, Theorem 6])**.** *Let X be a smooth connected projective k-curve, $p > 0$, $S \subset X$ be a non-empty set of closed points in X, and let $U = X \setminus S$. Then the above EP ($\mathcal{E}$) satisfies the following: there exists an open subgroup $\Pi \subset \pi_1^{\text{ét}}(U)$ such that $\alpha|_\Pi(\Pi) = G$ and such that the induced embedding problem $(\alpha|_\Gamma, \beta)$ has a proper solution.*

In [6], [21], it was shown that one can find an index-p open subgroup Π of $\pi_1^{\text{ét}}(U)$ which satisfies the conclusion of the above theorem.

Notation. Let $NS(\mathcal{E})$ denote the number of equivalence classes of proper solutions to $\mathcal{E}$. Here we consider two solutions γ_1 and γ_2 of $\mathcal{E}$ to be equivalent if $\ker(\gamma_1) = \ker(\gamma_2)$. In other words, $NS(\mathcal{E})$ counts the number of distinct H-covers of Y which become Γ covers of X, étale over U.

As we have discussed earlier, if $\mathcal{E}$ is a nontrivial quasi-p EP then $NS(\mathcal{E})$ is infinite (Proposition 4.9). Since there are only finitely many H-Galois étale covers of X when H is a prime-to-p group (Theorem 4.2), we have the following proposition.

Proposition 4.11. *If the embedding problem ($\mathcal{E}$) is a prime-to-p EP then $NS(\mathcal{E})$ is a finite number.*

Also note that if G is trivial then $NS(\mathcal{E})$ is simply the number of surjective group homomorphism $\pi_1^{\text{ét}}(U) \longrightarrow H$ divided by $|\operatorname{Aut}(H)|$.

4.2.2 Main problems

Let the hypothesis be as in the previous section, k is an algebraically closed field, and $p = \operatorname{char}(k) > 0$. Since any embedding problem splits into a prime-to-p EP and a quasi-p EP (Remark 4.8), and quasi-p EPs over smooth connected k-affine curves have proper solutions (Proposition 4.9), we are interested in embedding problems with prime-to-p kernel. Let H be a finite abelian group of order prime to p. We are interested in the following problems:

1. How do we find a proper solution of the prime-to-p EP ($\mathcal{E}$), and in general, a Γ-Galois étale cover of U, where Γ can be any extension of G by H?
2. Given an prime-to-p EP ($\mathcal{E}$), what is the value of $NS(\mathcal{E})$?
3. What is the minimal genus of covers corresponding to the proper solutions of a given EP?

When $H \cong (\mathbb{Z}/m\mathbb{Z})^n$ for some positive integer m prime to p, we translate the first problem of finding a proper solution to the EP into finding G-submodule of $P_m(U)$ (G acts on $P_m(U)$ on the right, see Subsection 5.2.1). This is Theorem 1.1.

Let X be a smooth connected projective curve and S_X be a finite set of closed points of X. Let $\psi : V \longrightarrow X$ be a connected G-Galois cover étale away from S_X for a finite cyclic p-group group G, g_V be the genus of V, $S_V = \psi^{-1}(S_X)$ and $\alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G$ be the homomorphism corresponding to ψ. Let l be a prime number other than p. For $b \geq 1$, d_b will denote the order of l in $(\mathbb{Z}/p^b\mathbb{Z})^*$. $\Phi_{p^b}(x)$ denotes the p^b-th cyclotomic polynomial, $P_{bi}(x)$ are irreducible factors (over $\mathbb{F}_l$) of $\Phi_{p^b}(x)$.

Theorem 4.12. *Let G be a cyclic group of order p^a, σ be a generator of G, l be a prime number other than p, $H = (\mathbb{Z}/l\mathbb{Z})^n$, n_0 (resp. n_b, $1 \leq b \leq a$) be the dimension of $P_l(V \setminus S_V)^G$ (resp. $\ker(\Phi_{p^b}(\sigma)) \subset P_l(V \setminus S_V)$) over $\mathbb{F}_l$. Then n can be expressed as*

$$n = u + \Sigma_{b=1}^{a} v_b d_b$$

for non-negative integers $u \leq n_0$, $v_b \leq n_b/d_b, \forall b \leq a$ if and only if the embedding problem $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G)$ has a proper solution for some group homomorphism $\theta : G \longrightarrow \text{Aut}(H)$.

This result can be generalized partially for any finite abelian group H of order coprime to p (see Corollaries 5.29, 5.31).

For the second problem, we count the number of equivalence classes of solutions for the embedding problems in Theorem 4.12. See Equation 5.1.2 for the notation $NSExt(\theta, \alpha)$.

Theorem 4.13. *Let G be a cyclic group of order p^a, and l be a prime number different from p. Let $H = (\mathbb{Z}/l\mathbb{Z})^{\oplus n}$ be a G-module, $\theta : G \longrightarrow \text{Aut}(H)$ be the G-action, $\alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G$ be an epimorphism. Let γ_{bi} (resp. γ'_{bi}) be the multiplicity of $\mathbb{F}_l[x]/P_{bi}(x)$ in the G-module $P_l(V \setminus S_V)$ (resp. H). Let n_0 (resp. u) be the dimension of $P_l(V \setminus S_V)^G$ (resp. H^G). Then*

$$NSExt(\theta, \alpha) = NS(H \rtimes_\theta G \twoheadrightarrow G, \alpha) = [\Pi_{b=1}^{a} \Pi_{i=1}^{p^{b-1}(p-1)/d_b}(n_{bi}/n'_{bi})]\bar{n}/\overline{n'},$$

where $n_{bi} = \Pi_{r=o}^{\gamma'_{bi}-1}(\sum_{s=r}^{\gamma_{bi}-1} l^{d_b s})$, $n'_{bi} = \Pi_{r=o}^{\gamma'_{bi}-1}(\sum_{s=r}^{\gamma'_{bi}-1} l^{d_b s})$, $\bar{n} = \Pi_{r=o}^{u-1}(\sum_{s=r}^{n_0-1} l^s)$ and $\overline{n'} = \Pi_{r=o}^{u-1}(\sum_{s=r}^{u-1} l^s)$.

Given an embedding problem $((\mathbb{Z}/l\mathbb{Z})^n \rtimes_\theta (\mathbb{Z}/p^a\mathbb{Z}) \twoheadrightarrow \mathbb{Z}/p^a\mathbb{Z}, \alpha : \pi_1^{\text{ét}}(X \setminus S_X \twoheadrightarrow \mathbb{Z}/p^a\mathbb{Z})$, the third problem of finding the minimum of genera of covers corresponding to the proper solutions of the EP is addressed in Corollaries 5.21 and 5.22.

Chapter 5

Proofs of the main results

Throughout this chapter k denotes an algebraically closed field of characteristic $p > 0$.

5.1 Pullback of Galois covers

Let Z be a normal variety over k. Let G be a finite group and $\pi : V \longrightarrow Z$ be a smooth G-Galois cover of Z, étale over a non-empty open subset U of Z. Let H be a finite group and $\psi : W \longrightarrow V$ be a smooth H-Galois cover of V, étale over $\pi^{-1}(U)$. Let $\sigma \in \mathrm{Aut}(V|Z) = G$. Consider the pullback W_σ of W:

$$\begin{array}{ccc} W_\sigma := V \times_V W & \xrightarrow{\tilde{\sigma}} & W \\ \downarrow{\scriptstyle \psi_\sigma} & & \downarrow{\scriptstyle \psi} \\ V & \xrightarrow{\sigma} & V \end{array}$$

Then $\psi_\sigma : W_\sigma \longrightarrow V$ is also an H-Galois cover, étale over $\pi^{-1}(U)$ and $\tilde{\sigma}$ is an isomorphism of schemes over k.

Proposition 5.1. *The H-covers $W_\sigma \longrightarrow V$ are isomorphic to $W \longrightarrow V$, $\forall \sigma \in \mathrm{Aut}(V|Z)$ if and only if the composition $W \xrightarrow{\psi} V \xrightarrow{\pi} Z$ is also Galois.*

Proof. First we assume that for $\sigma \in \mathrm{Aut}(V|Z)$, $\phi_\sigma : W \longrightarrow W_\sigma$ is an isomorphism of H-covers of V. We need to show that the field extension $k(W)|k(Z)$ induced by $k(Z) \hookrightarrow k(V) \hookrightarrow k(W)$ is Galois. Let $\tau : k(W) \longrightarrow \overline{k(W)}$ be any field embedding in the algebraic closure $\overline{k(W)}$ that fixes $k(Z)$. It is enough to prove that $\tau(k(W)) = k(W)$. Since $k(V)|k(Z)$ is Galois $\tau(k(V)) = k(V) \subset \tau(k(W))$. Let $\sigma = \tau|_{k(V)}$ and it defines an element of $\mathrm{Aut}(V|Z)$. Let $\psi' : W' \longrightarrow V$ be the normalization of V in $\tau(k(W))$. Also,

τ induces an isomorphism $W' \longrightarrow W$ and the following diagram is cartesian.

$$\begin{array}{ccc} W' & \xrightarrow{\tau} & W \\ {\scriptstyle \psi'}\downarrow & & \downarrow{\scriptstyle \psi} \\ V & \xrightarrow{\sigma} & V \end{array}$$

Hence $W' = W_\sigma$, $\psi' = \psi_\sigma$ and by hypothesis $\phi_\sigma : W \longrightarrow W'$ is an isomorphism of H-covers of V. Hence $k(W) = k(W') = \tau(k(W))$.

Conversely, suppose the composition $W \xrightarrow{\psi} V \xrightarrow{\pi} Z$ is Galois. Let $\sigma \in \mathrm{Aut}(V|Z)$ be non-identity and W_σ be the corresponding pullback of W. We want to define an isomorphism $\phi_\sigma : W \longrightarrow W_\sigma$ such that $\psi_\sigma \circ \phi_\sigma = \psi$. Let $k(W)$ be the splitting field of a polynomial $f \in k(V)[x]$. Then $k(W_\sigma)$ is the splitting field of $\sigma(f) \in k(V)[x]$. Every root of $\sigma(f)$ is $k(Z)$-conjugate of a root of f and since $k(W)|k(Z)$ is Galois, $\sigma(f)$ splits in $k(W)$. Hence by comparing degrees $k(W)$ is also the splitting field of $\sigma(f)$. Hence there is an isomorphism $\phi_\sigma : k(W_\sigma) \longrightarrow k(W)$ fixing $k(V)$. This induces the isomorphism $\phi_\sigma : W \longrightarrow W_\sigma$ of V-schemes. □

Let $\phi_\sigma : W \longrightarrow W_\sigma$ be an isomorphism of covers over V, for all $\sigma \in \mathrm{Aut}(V|Z)$. Then by the proposition above, the composition $\pi \circ \psi : W \xrightarrow{\psi} V \xrightarrow{\pi} Z$ is Galois. For $\sigma \in \mathrm{Aut}(V|Z)$, we get the following commuting diagram:

$$\begin{array}{ccccc} & & \overset{\tilde\sigma\circ\phi_\sigma}{\frown} & & \\ W & \xrightarrow{\phi_\sigma} & W_\sigma & \xrightarrow{\tilde\sigma} & W \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi_\sigma} & & \downarrow{\scriptstyle\psi} \\ V & = & V & \xrightarrow{\sigma} & V \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ Z & = & Z & = & Z \end{array}$$

Let $\Phi_\sigma := \tilde\sigma \circ \phi_\sigma : W \longrightarrow W$. Clearly, Φ_σ is an automorphism of W and $\psi \circ \Phi_\sigma = \sigma \circ \psi$, $(\pi \circ \psi) \circ \Phi_\sigma = \pi \circ \psi$. Hence $\Phi_\sigma \in \mathrm{Aut}(W|Z)$ and it is a lift of σ. When $\sigma = \mathrm{Id}_V \in \mathrm{Aut}(V|Z)$, we choose its lift to be Id_W.

5.1.1 The G-action on H:

For all $\sigma \in G = \mathrm{Aut}(V|Z)$ we fix a lift Φ_σ as above. When H is abelian, the right action of G on H is given by (see Section 3.4.1):

$$h \cdot \sigma := \Phi_\sigma^{-1} \circ h \circ \Phi_\sigma, \forall \sigma \in G \text{ and } h \in H \tag{5.1.1}$$

Remark 5.2. When H is abelian with the G-action as above, H becomes an object of **mod**-G. Then the equivalence classes of extensions of G by H are in one-to-one

correspondence with the cohomology group $H^2(G;H)$ (Theorem 3.47). The factor set $[\cdot,\cdot] : G \times G \longrightarrow H$ given by $[\sigma,\tau] := \Phi_{\sigma\tau}^{-1}\Phi_\sigma\Phi_\tau$ is a 2-cocycle (Proposition 3.46) and its image in $H^2(G;H) = Z^2(G,H)/B^2(G,H)$ corresponds to the Galois group Γ of $W \longrightarrow Z$. For general H, using the bijective correspondence between the classes of (G,H)-equivalent extensions of G with $H^2(G,Z(H))$ (Theorem 3.48) one can similarly find the cohomology class corresponding to Γ.

Let C be a smooth connected curve, $\alpha : \pi_1^{\text{ét}}(C) \longrightarrow G$ be an epimorphism and H be a finite abelian group. Let $a : G \longrightarrow \mathrm{Aut}(H)$ be a fixed action of G on H.

Notation. Let $NSExt(a,\alpha)$ denote the sum of the number of solutions to embedding problems (β,α) where β runs over all extensions of G by H given by a.

Since $H^2(G,H)$ classifies all such extensions, we have the following formula. For $e \in H^2(G,H)$, let Γ_e denote the extension and $\beta_e : \Gamma_e \longrightarrow G$ denote the epimorphism. Then

$$NSExt(a,\alpha) = \sum_{e\in H^2(G,H)} NS(\beta_e,\alpha). \tag{5.1.2}$$

5.2 Galois action on cyclic covers

5.2.1 G-action on P_m

Let X be a smooth connected projective curve and S_X be a finite set of closed points of X. Let $\psi : V \longrightarrow X$ be a connected G-Galois cover for a finite group G and $S_V = \psi^{-1}(S_X)$. Let $r_X = |S_X|$, $r_V = |S_V|$ and g_X (resp., g_V) be the genus of X (resp., V).

For $\sigma \in G$ and any $D = \sum_{v\in S_V} a_v v \in \mathbb{Z}[S_V]$, $\sigma^* D = \sum_{v\in S_V} a_v \sigma^{-1} v \in \mathbb{Z}[S_V]$ as $\sigma(S_V) = S_V$. So G acts on $P_m = P_m(V \setminus S_V)$ on the right by

$$([L],D)\cdot\sigma = ([\sigma^* L],\sigma^* D).$$

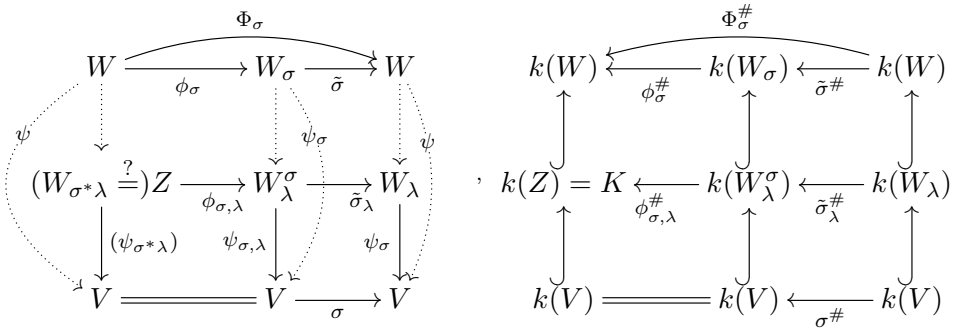
It is easy to see that this action preserves the group operation of P_m. Hence P_m is a right G-module. Note that P_m is naturally a $\mathbb{Z}/m\mathbb{Z}$-module with compatible G-action.

Remark 5.3. We choose a generating set $A = \{a_1,\ldots,a_N\}$ of type T1 of $P_m(V \setminus S_V)$ such that each a_i is of order m. We also fix μ, a primitive m-th root of unity in k. Using Proposition 3.24(iv), we fix an isomorphism from P_m to the Galois group of the normalization of the cover $\times_{i=1}^N W_i \longrightarrow V$, where $W_i \longrightarrow Y$ is the cover corresponding to a_i.

Now we prove the main result: Theorem 1.1 from the introduction.

Proof of Theorem 1.1. Let $B \subset P_m = P_m(V \setminus S_V)$ be of type T1 consisting of elements of order m and $H =< B >$. Suppose H is a G-submodule of P_m. For $\lambda \in B$, let $W_\lambda \longrightarrow V$ be the m-cyclic cover corresponding to λ. Let $W \longrightarrow V$ be the normalized fibre product of these covers. Then by Proposition 3.24, $W \longrightarrow V$ is an H-Galois connected cover étale over $V \setminus S_V$. Since H is a G-module for any $\sigma \in G$ and $\lambda \in B$, $\sigma^*\lambda \in H$. Hence $W \longrightarrow V$ dominates the m-cyclic covers $W_{\sigma^*\lambda} \longrightarrow V$ corresponding to $\sigma^*\lambda$ for every $\lambda \in B$. Moreover, $\sigma(B)$ consists of elements of order m and is of type T1. Hence by Proposition 3.24 the normalized fibre product W^*_σ of the covers $W_{\sigma^*\lambda} \longrightarrow V$ is dominated by $W \longrightarrow V$. Comparing degrees we obtain that the covers $W^*_\sigma \longrightarrow V$ and $W \longrightarrow V$ are isomorphic. Since this is true for all $\sigma \in G$, by Proposition 5.1 $W \longrightarrow X$ is a Galois cover. Let Γ be the Galois group. Then Γ is an extension of G by H.

Since $W \longrightarrow X$ is Galois, for any $\sigma \in G$, we choose a lift $\Phi_\sigma = \tilde{\sigma} \circ \phi_\sigma$ from the Galois group $\Gamma = \mathrm{Aut}(W|X)$. Let $h \in \mathrm{Gal}(W|V)$ be the image of $\lambda \in < B >$ (by Proposition 3.24) and h^σ be the pullback of h under σ. Let W_σ and W^σ_λ be the pullbacks (by σ) of W and W_λ respectively. For a morphism f of varieties over k, we let $f^\#$ denote the map of rational functions. Let $K = \Phi^\#_\sigma(k(W_\lambda)) \subset k(W)$, Z be the normalization of V in K. We will show that $Z = W_{\sigma^*\lambda}$.



From the diagram above, note that Φ_σ induces the isomorphism $\sigma : V \to V$ and consequently induces an automorphism of $P_m(V \setminus S_V)$. If $\lambda = ([L], D)$, its pull back under σ is $\sigma^*\lambda = ([\sigma^*L], \sigma^*D)$. Then (by Corollary 3.20 and the discussion after the corollary) $L^m \otimes \mathcal{O}_V(D) = \mathrm{div}(s) \sim 0$ for some s in $k(V)$ and $k(W_\lambda)$ is $k(V)(t)$ for some $t \in k(W^\sigma_\lambda) \subset k(W)$ such that $t^m = s$. Similarly, $\sigma^*L^m \otimes \mathcal{O}_V(\sigma^*(D)) = \mathrm{div}(\sigma^\#(s))$ and $k(W_{\sigma^*\lambda}) = k(V)(t')$ for some $t' \in k(W_{\sigma^*\lambda}) \subset k(W)$ such that $(t')^m = \sigma^\#(s)$. Note that $k(W^\sigma_\lambda) = k(V)_\sigma \otimes k(W_\lambda) = k(V)_\sigma \otimes k(V)[t]$, where $a'(a \otimes b) = (a\sigma^\#(a')) \otimes b = a \otimes a'b$ for $a, a' \in k(V)$, $b \in k(W_\lambda)$. Clearly, $\tilde{\sigma}^\#_\lambda$ is given by $b \mapsto 1 \otimes b$, $a \mapsto 1 \otimes a = \sigma^\#(a) \otimes 1$. Since $k(V) \hookrightarrow k(W^\sigma_\lambda)$ implies $a \mapsto a \otimes 1$ and $\phi^\#_{\sigma,\lambda}|_{k(V)} = \mathrm{Id}$, $\phi^\#_{\sigma,\lambda}(a \otimes 1) = a$. Now,

$$\begin{aligned} 0 = \Phi^\#_\sigma|_{k(W_\lambda)}(t^m - s) = \phi^\#_{\sigma,\lambda} \circ \tilde{\sigma}^\#_\lambda(t^m - s) \\ = (\phi^\#_{\sigma,\lambda}(1 \otimes t))^m - \phi^\#_{\sigma,\lambda}(\sigma^\#(s) \otimes 1) = (\Phi^\#_\sigma(t))^m - \sigma^\#(s). \end{aligned}$$

Hence $K|k(V)$ dominates the m-cyclic extension $k(W_{\sigma^*\lambda})|k(V)$ (corresponding to the equation $x^m - \sigma^\#(s) = 0$). By comparing degrees of extensions, $k(Z) = K = k(W_{\sigma^*\lambda})$

and hence Φ_σ^{-1} induces $\phi_{\sigma,\lambda}^{-1} \circ \tilde{\sigma}_\lambda^{-1} : W_\lambda \longrightarrow W_{\sigma^*\lambda}$, the m-cyclic cover of V corresponding to $\sigma^*\lambda$.

$$\begin{array}{ccccc} W & \xrightarrow{\phi_\sigma} & W_\sigma & \xrightarrow{\tilde{\sigma}} & W \\ \downarrow{\scriptstyle \sigma^*h} & & \downarrow{\scriptstyle h^\sigma} & & \downarrow{\scriptstyle h} \\ W & \xrightarrow{\phi_\sigma} & W_\sigma & \xrightarrow{\tilde{\sigma}} & W \end{array}$$

From the commuting diagram above, h induces σ^*h, the image of $\sigma^*\lambda$ in $\mathrm{Gal}(W_{\sigma^*\lambda}|V)$.

Let $B = \{\lambda_1, \ldots, \lambda_n\}$, $\lambda_i = ([L_i], D_i)$, W_i be the corresponding cover and h_i be the image of λ_i in $\mathrm{Gal}(W_i|V)$. Again, (by Corollary 3.20 and the discussion after the corollary) we have $L_i^m \otimes \mathcal{O}_V(D_i) = \mathrm{div}(s_i)$ for some s_i in $k(V)$ and $k(W_i)$ is $k(V)(t_i)$ for some $t_i \in k(W)$ such that $t_i^m = s_i$ and $h_i^\#(t_j) = \mu^{\delta_{ij}} t_j$ where $\delta_{ij} = 0$ if $i \neq j$, $\delta_{ij} = 1$ if $i = j$.

Note that $k(W_{\sigma^*\lambda_j}) = k(V)(\Phi_\sigma^\#(t_j))$ such that $(\Phi_\sigma^\#(t_j))^m = \sigma^\#(s_j)$. Clearly, $k(W) = k(V)(\Phi_\sigma^\#(t_1), \ldots, \Phi_\sigma^\#(t_n))$ and $(\sigma^*h_i)^\#(\Phi_\sigma^\#(t_j)) = \mu^{\delta_{ij}}(\Phi_\sigma^\#(t_j))$.

Note that

$$\begin{aligned}(\Phi_\sigma^{-1} h_i \Phi_\sigma)^\#(\Phi_\sigma^\#(t_j)) &= \Phi_\sigma^\# h_i^\# (\Phi_\sigma^\#)^{-1}(\Phi_\sigma^\#(t_j)) \\ &= \Phi_\sigma^\#(\mu^{\delta_{ij}} t_j) = \mu^{\delta_{ij}}(\Phi_\sigma^\#(t_j)) = (\sigma^* h_i)^\#(\Phi_\sigma^\#(t_j)).\end{aligned}$$

We have $\Phi_\sigma^{-1} \circ h_i \circ \Phi_\sigma = \sigma^* h_i$. So, by Equation 5.1.1, we obtain $h \cdot \sigma = \Phi_\sigma^{-1} \circ h \circ \Phi_\sigma = \sigma^* h$, for any $h \in \mathrm{Gal}(W|V)$. Hence, the group action of G on $H \cong \mathrm{Gal}(W|V)$ is the same as the action of G on H as a G-submodule of P_m and $W \longrightarrow X$ provides a solution to the embedding problem.

For the converse, we choose a basis $B = \{h_1, \ldots, h_r\}$ of the free $\mathbb{Z}/m\mathbb{Z}$-module H. The solution γ to the EP corresponds to the Γ-cover $W \to X$ which leads to the H-cover $W \longrightarrow V$. Let $W_i \longrightarrow V$ be the $\mathbb{Z}/m\mathbb{Z}$-cover W/H_i where $H_i =< h_j : 1 \leq j \leq r, j \neq i >$. Note that W is the normalization of fibre product of W_i's. Since $W_i \longrightarrow V$ is a $\mathbb{Z}/m\mathbb{Z}$-cover, it corresponds to some $([L_i], D_i)$ in P_m. So the subgroup of P_m generated by $\{([L_i], D_i) : 1 \leq i \leq r\}$ is isomorphic to H. Note that this subgroup does not depend on the choice of the basis (by Proposition 3.24(iii)). By Proposition 5.1, this subgroup of P_m is G-stable under the G-action on P_m. Moreover, exactly like in the previous paragraph, the G-action on this subgroup of P_m is the same as the G-action on H induced from the EP. Hence H is isomorphic to this subgroup $< \{([L_i], D_i) : 1 \leq i \leq r\} >$ of P_m as G-modules.

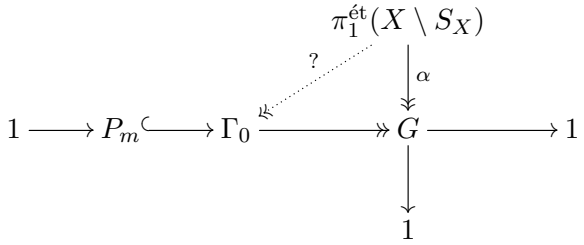
Furthermore, for the last part of the theorem, observe that two solutions for the embedding problem are equivalent iff they induce the same H-cover $W \longrightarrow V$. Finally, the H-cover $W \longrightarrow V$ determines the subgroup of P_m isomorphic to H by the above. □

Corollary 5.4. *Let α be as above, $H = (\mathbb{Z}/m\mathbb{Z})^r$ be a G-module and $a : G \longrightarrow \mathrm{Aut}(H)$ be the associated action. Then $NSExt(a, \alpha)$ is the number of distinct G-submodules of $P_m(V \setminus S_V)$ isomorphic to H.*

Proof. By Theorem 1.1, there is a bijection between G-submodules H of $P_m = P_m(V \setminus S_V)$ and equivalence classes of solutions to the embedding problems (β, α) where $\beta : \Gamma \longrightarrow G$ is an epimorphism and Γ is any extension of G by H. □

Note that $P_m = P_m(V \setminus S_V) \cong (\mathbb{Z}/m\mathbb{Z})^N$ for $N = 2g_V + r_V - 1 + b^{(2)}$ (by Proposition 3.22. An immediate consequence of Corollary 5.4 is the following corollary.

Corollary 5.5. *There exists a unique extension Γ_0 of G by P_m such that the following embedding problem has a unique equivalence class of solutions.*



When $a : G \to \mathrm{Aut}((\mathbb{Z}/m\mathbb{Z})^N)$ is equal to the action given in Subsection 5.2.1, $NSExt(a, \alpha) = NS(\Gamma_0 \twoheadrightarrow G, \alpha) = 1$, $NSExt(a, \alpha) = 0$ otherwise.

Proof. Taking $H = P_m$ in the Corollary 5.4, we obtain a unique equivalence class of solutions to the embedding problem.

Let $W_0 \longrightarrow X$ be the Γ_0 cover corresponding to the unique solution of the above EP. Since any $(\mathbb{Z}/m\mathbb{Z})^N$-Galois cover of V, étale away from S_V, is dominated by W_0, from Equation (5.1.2) we obtain the last part of the corollary. □

We are interested in finding G-submodules H of P_m as these give rise to the solutions to embedding problems for $\alpha : \pi_1^{\text{ét}}(X \setminus S_X) \longrightarrow G$ with some extension Γ of G by H.

Note that S_V is a G-set. Let S be a (possibly empty) G-stable subset of S_V.

Proposition 5.6. *The group $P_m(V \setminus S)$ is a G-submodule of $P_m(V \setminus S_V)$. In particular, there is an extension Γ of G by $P_m(V \setminus S)$ such that the embedding problem $(\beta : \Gamma \longrightarrow G, \alpha)$ has a solution.*

Proof. By definition of P_m there is a natural inclusion of $H = P_m(V \setminus S)$ in $P_m(V \setminus S_V)$. Since S is a G-set H is stable under the action of G on $P_m(V \setminus S_V)$ defined in 5.2.1. Hence H is a G-submodule of $P_m(V \setminus S_V)$. The rest follows from Theorem 1.1. □

Let us apply the above proposition to the following example.

Example 5.7. Let $X = \mathbb{P}^1_k = \operatorname{Spec} k[x] \cup \operatorname{Spec} k[\frac{1}{x}]$, $S_X = \{(x=0), (x=1), \infty := (\frac{1}{x} = 0)\}$, V be the smooth completion of the affine curve $\operatorname{Spec} \frac{k[x, \frac{1}{x-1}, y]}{\left(y^p - y - \frac{x^\iota + \varsigma}{(x-1)^\varsigma}\right)}$, where ι, ς are positive integers coprime to p, $G = \operatorname{Aut}(V|X) \cong \mathbb{Z}/p\mathbb{Z}$, $\psi : V \longrightarrow X$ be the Galois cover corresponding to $\alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G$.

- Let $n_1 = (\varsigma + \iota)(p-1), n_2 = n_1 + 1, n_3 = n_1 + p - 1, n_4 = n_1 + p$. Then the EP

$$\mathcal{E}_i = ((\mathbb{Z}/m\mathbb{Z})^{n_i} \rtimes_{\theta_i} G \twoheadrightarrow G, \alpha)$$

has a proper solution for some $\theta_i : G \to \operatorname{Aut}((\mathbb{Z}/m\mathbb{Z})^{n_i})$, $1 \le i \le 4$.

Note that $\psi : V \longrightarrow X$ is a p-cyclic (Galois) cover, branched (totally ramified) at $(x=1)$ and ∞ (since $\frac{x^\iota + \varsigma}{(x-1)^\varsigma}$ has poles at $(x=1), \infty$ of orders ς, ι, respectively). For $i = 0, \ldots, p-1$, let $O_i \in V$ corresponds to $(x = 0, y = (p-i))$. Let $\tilde{I}$ (respectively, $\tilde{\infty}$) in V be the point above $(x=1)$ (respectively, ∞) in S_X. Note that $\psi^{-1}((x=0)) = \{O_0, \ldots, O_{p-1}\}$. Then $S_V = \psi^{-1}(S_X) = \{O_0, \ldots, O_{p-1}\} \sqcup \{\tilde{I}\} \sqcup \{\tilde{\infty}\}$, a disjoint union of G-subsets and ψ is étale over $X \setminus S_X$. By Theorem 3.14, the genus of V, $g_V = \frac{2+p(0-2)+(\varsigma+1)(p-1)+(\iota+1)(p-1)}{2} = \frac{(\varsigma+\iota)(p-1)}{2} = \frac{n_1}{2}$. Clearly, $(\mathbb{Z}/m\mathbb{Z})^{n_i} \rtimes_{\theta_i} G$ is the unique extension of G by $(\mathbb{Z}/m\mathbb{Z})^{n_i}$ w.r.to θ_i (by Theorem 3.49).

($\mathcal{E}_1$) If $S_1 = \phi, \{\tilde{I}\}$ or $\{\tilde{\infty}\}$, by the above proposition, we have a G-submodule $P_m(V \setminus S_1) = \{([L], D) \in P_m(V \setminus S_V) : L^m \cong \mathcal{O}_V(D) \cong \mathcal{O}_V\} \cong \operatorname{Pic}^0(V)[m] \cong (\mathbb{Z}/m\mathbb{Z})^{n_1}$ (by Proposition 3.22). Let $\theta_1 : G \to \operatorname{Aut}((\mathbb{Z}/m\mathbb{Z})^{n_1})$ be the restriction of the canonical G action on $P_m(V \setminus S_V)$. By the above proposition, there is a proper solution for the EP $\mathcal{E}_1$.

($\mathcal{E}_2$) When $S_2 = \{\tilde{I}, \tilde{\infty}\}$, $P_m(V \setminus S_2) \cong (\mathbb{Z}/m\mathbb{Z})^{n_2}$ (Proposition 3.22) is a G-submodule by the proposition above with the canonical G-action θ_2 and the EP $\mathcal{E}_2$ has a proper solution.

($\mathcal{E}_3$) When $S_3 = \{O_0, \ldots, O_{p-1}\}$, by Proposition 3.22 and the proposition above, $P_m(V \setminus S_3) \cong (\mathbb{Z}/m\mathbb{Z})^{n_3}$. Let θ_3 be the G-action on this submodule $(\mathbb{Z}/m\mathbb{Z})^{n_3} \hookrightarrow P_m(V \setminus S_V)$. Then the EP $\mathcal{E}_3$ has a proper solution.

($\mathcal{E}_4$) When $S_4 = \{O_0, \ldots, O_{p-1}\} \cup \{\tilde{I}\}$ or $\{O_0, \ldots, O_{p-1}\} \cup \{\tilde{\infty}\}$, $P_m(V \setminus S_V) \cong (\mathbb{Z}/m\mathbb{Z})^{n_4}$ (by Proposition 3.22) with G-action θ_4. By the proposition above, there are at least two (non-equivalent) proper solutions for the embedding problem $\mathcal{E}_4$.

Suppose $G_1 \trianglelefteq G$ and let $f_1 : X_1 \longrightarrow X$ be the normalization of X in $k(V)^{G_1}$. Then the cover $V \longrightarrow X$ factors through $X_1 \longrightarrow X$, $\operatorname{Aut}(X_1|X) = G/G_1$ and $\operatorname{Aut}(V|X_1) = G_1$.

Proposition 5.8. *Let S_1 be a subset of $f_1^{-1}(S_X)$ stable under the action of G/G_1. There is a natural G-equivariant homomorphism $P_m(X_1 \setminus S_1) \longrightarrow P_m(V \setminus S_V)$. Moreover if*

$(|G_1^{ab}|, m) = 1$ *then this homomorphism is injective. In particular there is an extension* Γ *of* G *by* $P_m(X_1 \setminus S_1)$ *such that the embedding problem* $(\beta : \Gamma \longrightarrow G, \alpha)$ *has a solution.*

Proof. By definition of P_m there is a natural inclusion of $P_m(X_1 \setminus S_1)$ in $P_m(X_1 \setminus f_1^{-1}(S_X))$. Since S_1 is a G/G_1-set $P_m(X_1 \setminus S_1)$ is stable under the action of G/G_1 on $P_m(X_1 \setminus f_1^{-1}(S_X))$ defined in 5.2.1. Hence $P_m(X_1 \setminus S_1)$ is a G-submodule of $P_m(X_1 \setminus f_1^{-1}(S_X))$.

Let $h : V \longrightarrow X_1$ be the cover which composed with $X_1 \longrightarrow X$ is $V \longrightarrow X$. Then for $([\mathcal{L}], D) \in P_m(X_1 \setminus f_1^{-1}(S_X))$, $([h^*\mathcal{L}], h^*D)$ is in $P_m(V \setminus S_V)$. This defines a G-equivariant map $h^* : P_m(X_1 \setminus f_1^{-1}(S_X)) \longrightarrow P_m(V \setminus S_V)$. Since the cover of $W \longrightarrow X_1$ defined by elements of $P_m(X_1 \setminus f_1^{-1}(S_X))$ are Galois with abelian Galois group of order some power of m and G_1^{ab} is of order prime to m, $W \longrightarrow X_1$ and $V \longrightarrow X_1$ are linearly disjoint. Hence h^* is injective. The remaining statement follows from Theorem 1.1. □

Let us explain the above proposition further in the following example.

Example 5.9. Let $X = \mathbb{P}^1_k = \operatorname{Spec} k[x] \cup \operatorname{Spec} k[\frac{1}{x}]$ and $S_X = \{(x = 1), (x = c), \infty := (\frac{1}{x} = 0)\}$ for some $c \in k \setminus \{0, 1\}$. Let V be the normalization of X in

$$\frac{k(x)[y, z]}{\left(y^p - y - \frac{x^{\iota+\varsigma}}{(x-1)^\varsigma}, z^p - z - \frac{x^{\delta+\varepsilon}}{(x-c)^\varepsilon}\right)}; \iota, \varsigma, \delta, \varepsilon \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}.$$

Clearly $G = \operatorname{Gal}(V|X) =< \sigma, \tau : \sigma^p = \tau^p = \mathrm{Id}_G, \sigma\tau = \tau\sigma >\cong (\mathbb{Z}/p\mathbb{Z})^2$, where σ, τ are defined by $\sigma(y) = y + 1, \sigma(z) = z$; $\tau(y) = y, \tau(z) = z + 1$. Let $G_1 =< \tau >$ and $\psi : V \longrightarrow \mathbb{P}^1_k$ be the G-cover corresponding to α.

- For $1 \leq i \leq 4$, let n_i be as in Example 5.7. Then the EP

$$\mathcal{E}'_i = ((\mathbb{Z}/m\mathbb{Z})^{n_i} \rtimes_{\rho_i} G \twoheadrightarrow G, \alpha)$$

has a proper solution for some $\rho_i : G \to \operatorname{Aut}((\mathbb{Z}/m\mathbb{Z})^{n_i})$, $1 \leq i \leq 4$.

Here X_1 is the smooth completion of $\operatorname{Spec} \frac{k[x, \frac{1}{x-1}, y]}{\left(y^p - y - \frac{x^{\iota+\varsigma}}{(x-1)^\varsigma}\right)}$ and $\operatorname{Gal}(X_1|X) = G/G_1 =< \bar{\sigma} >$. Let $\alpha_1 : \pi_1^{\text{ét}}(X) \twoheadrightarrow G/G_1$ corresponds to $f_1 : X_1 \longrightarrow X$. This cover is branched only at $(x = 1)$ and ∞, and unramified at $(x = c)$. Let $\tilde{I}, \tilde{\infty}$ be the points in X_1 over $(x = 1), \infty$, respectively; and $\bar{C}_i, 0 \leq i \leq p - 1$, be the points in X_1 above $(x = c)$. Since $h : V \longrightarrow X_1$ branched at $\tilde{\infty}$ and each $\bar{C}_i$ and unramified at $\tilde{I}$, let $h^{-1}(\tilde{\infty}) = \hat{\infty}$, $h^{-1}(\tilde{I}) = \{I_0, \ldots, I_{p-1}\}$ and $h^{-1}(\bar{C}_i) = C_i$. Then

$$S_V = \{I_0, \ldots, I_{p-1}, C_0, \ldots, C_{p-1}, \hat{\infty}\}, f_1^{-1}(S_X) = \{\tilde{I}, \bar{C}_0, \ldots, \bar{C}_{p-1}, \tilde{\infty}\}.$$

Then $h^* : P_m(X_1 \setminus f_1^{-1}(S_X)) \to P_m(V \setminus S_V)$ is defined by

$$h^*\left(\left([\mathcal{L}], a\tilde{I} + \sum_{i=0}^{p-1} b_i\bar{C}_i + d\tilde{\infty}\right)\right) = \left([h^*\mathcal{L}], a(\sum_{i=0}^{p-1} I_i) + \sum_{i=0}^{p-1} pb_iC_i) + pd\hat{\infty}\right),$$

for $a, b_i, d \in \mathbb{Z}, a+\sum_{i=0}^{p-1} b_i+d \equiv 0(\mod m)$. By the above proposition (since $\gcd(|G_1^{ab}|, m) = \gcd(p, m) = 1$), it is a natural G-equivariant injective homomorphism.

Let $S_i, 1 \leq i \leq 4$, be as in Example 5.7 (substitute V, G, α, O_j by $X_1, G/G_1, \alpha_1, \bar{C}_j, 0 \leq j \leq p-1$, respectively). Then $(\mathbb{Z}/m\mathbb{Z})^{n_i} = h^*(P_m(X_1 \setminus S_i))$ is a G-stable free $\mathbb{Z}/m\mathbb{Z}$-submodule of $P_m(V \setminus S_V)$ (by Proposition 3.22 and the proposition above). Let ρ_i be the corresponding G-action. Clearly, $(\mathbb{Z}/m\mathbb{Z})^{n_i} \rtimes_{\rho_i} G$ is the unique extension of $(\mathbb{Z}/m\mathbb{Z})^{n_i}$ by G w.r.to ρ_i (by Theorem 3.49). By the proposition above, there is a $((\mathbb{Z}/m\mathbb{Z})^{n_i} \rtimes_{\rho_i} G)$-Galois cover $W_i \longrightarrow X$ (resp. a $(P_m(X_1 \setminus S_i) \rtimes_{\theta_i} (G/G_1))$-Galois cover $Y_i \longrightarrow X$) corresponding to the proper solution of the EP $\mathcal{E}_i'$ (resp. the EP $\mathcal{E}_i$). Then W_i is the normalization of $Y_i \times_{X_1} V$.

5.3 Some results on effective subgroups

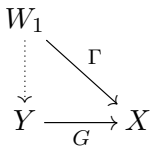
Definition 5.10. Let H be a subgroup of a finite group Γ. A subset $B \subset H$ will be called a *relative generating set* for H in Γ if for every subset $T \subset \Gamma$ such that $H \cup T$ generates Γ, the subset $B \cup T$ also generates Γ. The *relative rank* of H in Γ is the smallest non-negative integer $\rho := \text{rank}_\Gamma(H)$ such that there is a relative generating set for H in Γ consisting of ρ elements.

Let X^o be a smooth connected affine curve, X be its smooth completion and $S_X = X \setminus X^o$. Let G, H and Γ be finite groups. Let $\alpha : \pi_1^{\text{ét}}(X^o) \longrightarrow G$ be an epimorphism. Let $Y \longrightarrow X$ be the G-Galois connected cover corresponding to α.

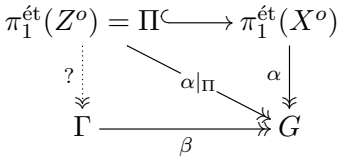
Definition 5.11. Given a finite index subgroup $\Pi \subset \pi_1^{\text{ét}}(X^o)$, we say the EP $(\beta : \Gamma \twoheadrightarrow G, \alpha)$ *restricts to* Π if $\alpha(\Pi) = G$. If the restricted EP $(\beta, \alpha|_\Pi)$ has a proper solution then we say Π is an *effective subgroup* for the EP (β, α).

Let $Z \to X$ be the normalization of X in the fixed field of Π and Z^o be the inverse image of X^o in Z. Then $\Pi = \pi_1^{\text{ét}}(Z^o)$. Let V be the normalization of $Y \times_X Z$. Then $V \longrightarrow Z$ is an $\alpha(\Pi)$-Galois cover. Note that the embedding problem restricts to Π if and only if the covers $Z \to X$ and $Y \to X$ are linearly disjoint. Recall that a proper solution to the EP $(\beta : \Gamma \twoheadrightarrow G, \alpha)$ translates to finding a dominating cover $W_1 \longrightarrow X$

so that the following diagram commutes.

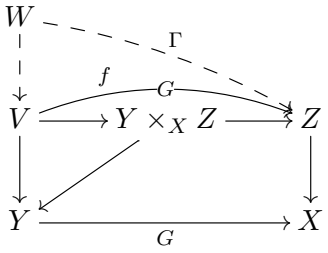


A proper solution to the restricted EP $(\beta, \alpha|_\Pi)$ gives a Γ-Galois cover W of Z étale over Z^o that dominates the normalization V of $Y \times_X Z \to Z$.



(5.3.1)

A proper solution to the above EP translates to the problem of finding a Γ-cover $W \longrightarrow Z$ dominating $V \longrightarrow Z$.



(5.3.2)

When there exists a Γ-Galois cover $W \longrightarrow Z$ so that the above diagram commutes, Π becomes an effective subgroup for the EP (β, α).

For ramification filtration and upper jump, see Section 3.1.1. The following is an immediate consequence of Proposition 5.1.

Corollary 5.12. *Let $Z \longrightarrow X$ be a cover étale over X^o such that the normalization $f : V \longrightarrow X$ of the fibre product $Y \times_X Z$ is connected. Also assume that there exists an H-cover W^o of $V^o = f^{-1}(X^o)$ whose pullback by all $\sigma \in G$ is again the same H-cover $W^o \longrightarrow V^o$. Then there exist an extension $\beta : \Gamma \longrightarrow G$ of G by H such that $\pi_1^{\text{ét}}(Z^o)$ is an effective subgroup of $\pi_1^{\text{ét}}(X^o)$ for the EP (β, α).*

Hypothesis **(H)**: Let H be a finite group, G, Γ be finite quasi-p groups. Put $X^o = \mathbb{A}^1 = \operatorname{Spec} k[x]$ and $X = \mathbb{P}^1$ in the Diagrams (5.3.1) and (5.3.2)respectively. Let $Y^o \longrightarrow \mathbb{A}^1$ be an étale G-Galois cover associated with $\alpha : \pi_1^{\text{ét}}(\mathbb{A}^1) \twoheadrightarrow G$. Let $Z^o \longrightarrow \mathbb{A}^1$ be a p-cyclic étale cover, g_Y and g_Z be the genera of the smooth completions Y and Z of Y^o and Z^o respectively. Let $f : V \longrightarrow Z$ be the normalization of the fibre product $Y \times_{\mathbb{P}^1} Z$, $V^o = f^{-1}(Z^o)$ and g_V be the genus of V . Let $\mathcal{E}_1 = (\beta : \Gamma \twoheadrightarrow G, \alpha)$ be an EP and $H = \ker(\beta)$.

Recall that $\Pi_g = \Pi_{g,0}$ is the surface group (see Chapter 4). Let us state the following theorem that gives us a sufficient condition so that an index-p-subgroup of $\pi_1^{\text{ét}}(\mathbb{A}^1)$ can be an effective subgroup for the EP $\mathcal{E}_1$.

Theorem ([21, Proposition 15])**.** Consider the Hypothesis **(H)**. Let $\mathfrak{g}$ be such that there is a homomorphism $\pi : \Pi_{\mathfrak{g}} \to H/p(H)$ and the image of π is a relative generating set for $H/p(H)$ in $\Gamma/p(H)$. Let g_Z be at least $\mathfrak{g}$. Suppose that the genus of the normalization of $Z' \times_{\mathbb{P}^1} Y$ is same as g_V for all but finitely many p-cyclic covers $Z' \to \mathbb{P}^1$ branched only at $x = \infty$ with the genus $g(Z') = g_Z$. Then $\pi_1^{\text{ét}}(Z^o)$ is an effective subgroup for the above EP $\mathcal{E}_1$.

The example below shows that the sufficient condition mentioned in the above theorem is not necessary.

Example 5.13. Let $Y^o \to \mathbb{A}^1$ and $Z^o \to \mathbb{A}^1$ in the Hypothesis **(H)** be such that $g_Y > g_Z|G|$ and $k(Z) \cap k(Y) = k(x)$. Here m is coprime to p, $H = P_m = P_m(V^o)$ and the G-action a on $H = P_m$ is the same as in 5.2.1. Let $B \subset P_m$ be of cardinality at most $2g_Z$. Let $\Gamma = P_m \rtimes_a G$. By Theorem 1.1, the EP $(\beta, \alpha|_{\pi_1^{\text{ét}}(Z^o)})$ has a proper solution and so $\pi_1^{\text{ét}}(Z^o)$ is an effective subgroup of $\pi_1^{\text{ét}}(\mathbb{A}^1)$ for the EP $\mathcal{E}_1$.

Remark 5.14. The condition "$g_Z \geq \mathfrak{g}$ *and the image of* $\Pi_{\mathfrak{g}} \to H/p(H)$ *is a relative generating set for* $H/p(H)$ *in* $\Gamma/p(H)$" in the theorem above is not necessary in the given example. Note that $g_V > g_Z|G|$ (since $g_V \geq g_Y > g_Z|G|$) and hence $|P_m| > m^{2g_Z|G|}$ (Since $P_m \supset \text{Pic}^0(V)[m] \cong (\mathbb{Z}/m\mathbb{Z})^{2g_V}$). Put $\mathfrak{g} = g_Z$ in the hypothesis of the theorem above. Since $p(H) = p(P_m)$ is trivial, $g_Z = \mathfrak{g} < \frac{1}{2}\,\text{rank}_\Gamma(H)$. By Corollary 5.5, we are in the set-up of the above theorem. Clearly, the G-submodule of P_m generated by B has cardinality at most $m^{2g_Z|G|}$ and hence is not the whole of P_m. This implies B is not a relative generating set of H in Γ. In fact, no image of Π_{g_Z} in H can be a relative generating set of H in Γ. Then the sufficient condition mentioned in the theorem above is far from necessary.

Let us recall a corollary to the above theorem from [21].

Corollary 5.15 ([21, Corollary 17])**.** *Consider the the Hypothesis* ***(H)****. Let* g_Z *is at least* $\text{rank}_\Gamma(H)$ *and the upper jump of the cover* $Z \longrightarrow \mathbb{P}^1$ *at* ∞ *is different from all the upper jumps of* $Y \longrightarrow \mathbb{P}^1$ *at* ∞*. Then* $\pi_1^{\text{ét}}(Z^o)$ *is an effective subgroup of* $\pi_1^{\text{ét}}(\mathbb{A}^1)$ *for the given EP* $\mathcal{E}_1$*.*

Note that the condition "$g_Z \geq \text{rank}_\Gamma(H)$" in the above corollary can be relaxed: "$g_Z \geq \frac{1}{2}\,\text{rank}_\Gamma(H)$ when H is abelian" as we can define a homomorphism $\pi : \Pi_{g_Z} \to H$ such that $\pi(\Pi_{g_Z})$ is a relative generating set for $H/p(H)$ in $\Gamma/p(H)$.

Theorem 5.16. *Let* m *be prime to* p*,* $a : G \longrightarrow \text{Aut}(H)$ *be a representation over* $\mathbb{Z}/m\mathbb{Z}$ *and* r *be the size of the smallest generating set of* H *as a* G*-module. Consider the hypothesis* ***(H)****. If* $g_Z \geq r/2$ *and all the upper jumps of* $Y^o \longrightarrow \mathbb{A}^1$ *at* ∞ *are different from* $1 + 2g_Z/(p-1)$ *then* $a : G \longrightarrow \text{Aut}(H)$ *is a subrepresentation of* $P_m(V^o)$*.*

Proof. Note that the upper jump of $Z \longrightarrow \mathbb{P}^1$ over ∞ is $1 + 2g_Z/(p-1)$ (see [21, Remark 18]). Also $f : V \longrightarrow Z$ is a connected G-Galois cover étale over Z^o. Let $\alpha : \pi_1^{\text{ét}}(Z^o) \longrightarrow G$ be corresponding epimorphism and $\beta : \Gamma \longrightarrow G$ be any extension of G by H with respect to the action a. Note that $p(H)$ is the (proper) trivial subgroup and $\text{rank}_\Gamma(H) \leq r$. By the corollary above the EP $\mathcal{E}_1$ has a proper solution. Hence by Theorem 1.1, H is a G-submodule of $P_m(V^o)$. □

5.4 The case when G is a cyclic p-group

Let X be a smooth connected projective curve and S_X be a finite set of closed points of X. Let $\psi : V \longrightarrow X$ be a connected G-Galois cover étale away from S_X for a finite cyclic p-group G of order p^a generated by σ, g_V and g_X be the genera of V and X; $S_V = \psi^{-1}(S_X)$ and $\alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G$ be the homomorphism corresponding to ψ. Let l be a prime number other than p, $H = (\mathbb{Z}/l\mathbb{Z})^n$ be a module over $\mathbb{Z}/l\mathbb{Z} \cong \mathbb{F}_l$. For $b \geq 1$, d_b will denote the order of l in $(\mathbb{Z}/p^b\mathbb{Z})^*$. $\Phi_{p^b}(x)$ denotes the p^b-th cyclotomic polynomial, $P_{bi}(x)$ are irreducible factors (over $\mathbb{F}_l$) of $\Phi_{p^b}(x)$.

Note that $\deg(P_{bi}(x)) = d_b$ (see the proof of Lemma 3.33).

Since $\gcd(|G|, l) = 1$, by Theorem 3.49, $H^2(G; (\mathbb{Z}/l\mathbb{Z})^n)$ is trivial. Hence any extension of G by $(\mathbb{Z}/l\mathbb{Z})^n$ must be a semidirect product.

Now we prove Theorem 4.12.

Proof of Theorem 4.12. By Lemma 3.33, we have an isomorphism of $\mathbb{F}_l[G]$-modules

$$P_l(V \setminus S_V) \cong (\mathbb{F}_l)^{n_0} \oplus (\oplus_{b=1}^{a} \oplus_{i=1}^{p^{b-1}(p-1)/d_b} (\mathbb{F}_l[x]/P_{bi}(x))^{\gamma_{bi}}),$$

where the non-negative integers γ_{bi} satisfy $\Sigma_{i=1}^{p^{b-1}(p-1)/d_b} \gamma_{bi} d_b = n_b$. As mentioned before, since $\gcd(|H|, |G|) = \gcd(l, p) = 1$, any extension of G by H with respect to some G-action θ must be equivalent to $H \rtimes_\theta G$. Note that any basis of H over $\mathbb{F}_l$ is of type T1 consisting of elements of order l.

If n satisfies the expression given in Theorem 4.12, then H is identified with a G-stable subspace $(\mathbb{F}_l)^u \oplus (\oplus_{b=1}^{a} \oplus_{i=1}^{p^{b-1}(p-1)/d_b} (\mathbb{F}_l[x]/P_{bi}(x))^{\gamma'_{bi}})$ of $P_l(V \setminus S_V)$ where

$$\Sigma_{i=1}^{p^{b-1}(p-1)/d_b} \gamma'_{bi} = v_b$$

and the embedding problem $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G)$ has a proper solution by Theorem 1.1 where θ depends on the choice of identification of H.

Conversely, if an embedding problem $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G)$ has a proper solution, then $H = \ker(\beta)$ must be a $\mathbb{F}_l[G]$-submodule of $P_l(V \setminus S_V)$ (Theorem

1.1). So

$$H \cong (\mathbb{F}_l)^u \oplus (\oplus_{b=1}^{a} \oplus_{i=1}^{p^{b-1}(p-1)/d_b} (\mathbb{F}_l[x]/P_{bi}(x))^{\gamma'_{bi}})$$

where $0 \leq u \leq n_0$, $0 \leq \gamma'_{bi} \leq \gamma_{bi}$. Put $v_b = \Sigma_{i=1}^{p^{b-1}(p-1)/d_b} \gamma'_{bi}$. Then $v_b \leq n_b/d_b$ and $n = u + \Sigma_{b=1}^{a} \Sigma_{i=1}^{p^{b-1}(p-1)/d_b} \gamma'_{bi} d_b = u + \Sigma_{b=1}^{a} v_b d_b$. □

Lemma 5.17. *Let that hypothesis be as in Theorem 4.12. For each $x \in S_X$, $\psi^{-1}(\{x\}) = \{v_1, \ldots, v_r\}$ is a G-subset of S_V. Moreover, r divides p^a and v_i's can be rearranged so that $\sigma^{-1}(v_i) = v_{i+1}$ for $i < r$, $\sigma^{-1}(v_r) = v_1$.*

Proof. Since $\psi(v_1) = x$, and the Galois group $G =< \sigma >$ acts transitively on the fibre, $\psi^{-1}(x)$ is the orbit of v_1 in S_V and $v_i = \sigma^{s_i}(v_1)$ for some integer s_i, $1 \leq i \leq r$. Hence $\psi^{-1}(x)$ is a G-set and r divides $\#(G) = p^a$. Since σ^{p^a} is identity, $\exists s \leq r$ such that $\sigma^s(v_1) = v_1$ and so $\{v_1, \sigma^{-1}(v_1), \ldots, \sigma^{-(s-1)}(v_1)\}$ is a G-subset. For each $1 \leq i \leq r$, $v_i = \sigma^{s_i}(v_1)$ must be in $\{v_1, \sigma^{-1}(v_1), \ldots, \sigma^{-(s-1)}(v_1)\}$. Then $r = s$. □

Lemma 5.18. *Let the hypothesis be as in Theorem 4.12 and S_X be nonempty. Let $r_X = \#(S_X)$, $r_j = \#(\{x \in S_X | \#(\psi^{-1}(\{x\})) = p^j\})$ for $0 \leq j \leq a$. There is a G-module isomorphism*

$$P_l(V \setminus S_V) \cong \mathrm{Pic}^0(V)[l] \oplus \mathbb{F}_l^{r_X - 1} \oplus (\oplus_{i=1}^{a} \oplus_{t=1}^{p^{i-1}(p-1)/d_i} (\mathbb{F}_l[x]/P_{it}(x))^{\sum_{j=i}^{a} r_j}).$$

Proof. Recall the exact sequence (Equation 3.2.2) of abelian groups:

$$0 \longrightarrow \mathrm{Pic}^0(V)[l] \hookrightarrow P_l(V \setminus S_V) \xrightarrow{f} \mathbb{Z}/l\mathbb{Z}[S_V] \xrightarrow{\overline{\deg}} \mathbb{Z}/l\mathbb{Z},$$

where the inclusion map is $[L] \mapsto ([L], 0)$, $f(([L], D)) = D \mod l$ and $\overline{\deg}(D \mod l) = \deg(D) \mod l$. Clearly, $[\sigma^* L] \mapsto ([\sigma^* L], 0) = ([L], 0) \cdot \sigma$. Also, $(f(([L], D))) \cdot \sigma = \sigma^* D \mod l = f(([\sigma^* L], \sigma^* D)) = f(([L], D) \cdot \sigma)$. Since σ is an automorphism of V, $\deg(D) = \deg(\sigma^* D)$ for any cartier divisor D. Hence the inclusion map, f and $\overline{\deg}$ are all G-module homomorphisms. From this exact equation of G-modules and Proposition 3.29, we have a G-module isomorphism

$$\begin{aligned} P_l(V \setminus S_V) &\cong \mathrm{Pic}^0(V)[l] \oplus P_l(V \setminus S_V)/\mathrm{Pic}^0(V)[l] \cong \mathrm{Pic}^0(V)[l] \oplus f(P_l(V \setminus S_V)) \\ &\cong \mathrm{Pic}^0(V)[l] \oplus \ker(\overline{\deg}) \\ &\cong \mathrm{Pic}^0(V)[l] \oplus \{\Sigma_{v \in S_V} a_v v | a_v \in \mathbb{Z}/l\mathbb{Z}, \Sigma_{v \in S_V} a_v = 0\} \\ &\cong \mathrm{Pic}^0(V)[l] \oplus P_{\mathrm{ram}}(S_V, l), \end{aligned}$$

where $P_{\mathrm{ram}} = P_{\mathrm{ram}}(S_V, l)$ denotes the G-module $\{\Sigma_{v \in S_V} a_v v | a_v \in \mathbb{Z}/l\mathbb{Z}, \Sigma_{v \in S_V} a_v = 0\}$. We fix a section $\imath : P_{\mathrm{ram}} \hookrightarrow P_l(V \setminus S_V)$ of f. As an abelian group, P_{ram} has dimension $\#(S_V) - 1$ over $\mathbb{F}_l$. Clearly, the l-cyclic cover of V corresponding to $[L] \in \mathrm{Pic}^0(V)[l]$ is étale over V. If $\imath(\Sigma_{v \in S_V} a_v v) = ([L], \Sigma_{v \in S_V} a_v v)$ (for simplicity, we choose the coefficients a_v to denote element of both $\mathbb{Z}/l\mathbb{Z}$ and $\mathbb{Z}$), the corresponding l-cyclic cover of V is

(tamely) ramified at $v \in S_V$ iff $a_v \not\equiv 0 \mod l$, ramification index at v is l (see the discussion after Corollary 3.20). The G action on P_{ram} is given by

$$(\Sigma_{v\in S_V} a_v v)\cdot\sigma = \Sigma_{v\in S_V} a_v(\sigma^{-1}v).$$

Let $C_i^X := \{x \in S_X | \#(\psi^{-1}(\{x\})) = p^i\} = \{x_{i1},\dots,x_{i,r_i}\}$, $0 \le i \le a$. C_i^X can be empty. Then r_i is the cardinality of C_i^X, $S_X = \sqcup_i C_i^X$ (by Lemma 5.17), $r_X = \sum r_i$ and $\#(S_V) = \sum_{i=0}^a r_i p^i$. Let $\psi^{-1}(\{x_{ij}\}) = \{v_{ij1},\dots,v_{ijp^i}\}$, rearranged as in Lemma 5.17.

WLOG, we may assume that C_I^X is non-empty for some $I \in \{0,1,\dots,a\}$. For $0 \le i,j \le a$, note that $\lceil p^{j-i}\rceil = 1$ if $j \le i$, $\lceil p^{j-i}\rceil = p^{j-i}$ if $j > i$. Since $\lceil p^{I-i}\rceil p^i - \lceil p^{i-I}\rceil p^I = 0$ and G acts trivially on $\lceil p^{I-i}\rceil \sum_{k=1}^{p^i} v_{ijk} - \lceil p^{i-I}\rceil \sum_{k=1}^{p^I} v_{I1k}$, this element of P_{ram} corresponds to the l-cyclic cover $V_{ij} \longrightarrow V$, where V_{ij} is the normalization of $V'_{ij} \times_X V$ and $V'_{ij} \longrightarrow X$ is the l-cyclic cover corresponding to $x_{ij} - x_{I1}$, an element of $P_{\text{ram}}(S_X,l) = \{\Sigma_{x\in S_X} a_x x | \Sigma_{x\in S_X} a_x = 0 \mod l\} \hookrightarrow P_l(X \setminus S_X)$. Then $B_0 = \{\lceil p^{I-i}\rceil \sum_{k=1}^{p^i} v_{ijk} - \lceil p^{i-I}\rceil \sum_{k=1}^{p^I} v_{I1k} : 0 \le i \le a, 1 \le j \le r_i, (i,j) \ne (I,1)\}$ is linearly independent and each element generates a trivial submodule of P_{ram}. Hence the number of trivial components of P_{ram} is at least $\#(B_0) = r_X - 1$.

Let W_{ij} be the subspace of P_{ram} generated by the basis $B_{ij} = \{v_{ij1} - v_{ij2}, v_{ij2} - v_{ij3}, \dots, v_{i,j,p^i-1} - v_{ijp^i}\}$ when $i > 0$. Then $\dim(W_{ij}) = p^i - 1$, $W_{ij} \cap (\cup_{(i,j)\ne(i',j')} W_{i'j'}) = \{0\}$. Since the basis is a G-set, each W_{ij} is G-stable. Since B_0 and B_{ij}'s are disjoint and there union is linearly independent, $P_{\text{ram}} \cong \mathbb{F}_l^{r_X-1} \oplus (\oplus_{i=1}^a \oplus_{j=1}^{r_i} W_{ij})$ is a G-stable decomposition (since, equating dimensions on both sides, $\#(S_V) - 1 = r_X - 1 + \sum_{i=1}^a r_i(p^i - 1)$).

Since $(v_{ijk} - v_{i,j,k+1})\cdot\sigma = v_{i,j,k+1} - v_{i,j,k+2}$ (here $k+2 = 1$ when $k = p^i - 1$), the characteristic polynomial of σ is $(x^{p^i} - 1)/(x-1) = \prod_{b=1}^i \prod_{t=1}^{\phi(p^b)/d_b} P_{bt}(x)$, a product of irreducible polynomials, each of multiplicity 1. Thus, we have the G-module decomposition: $W_{ij} \cong \oplus_{b=1}^i \oplus_{t=1}^{\phi(p^b)/d_b} (\mathbb{F}_l[x]/(P_{bt}(x))$. Hence,

$$\begin{aligned} P_{\text{ram}}(S_V,l) &\cong \mathbb{F}_l^{r_X-1} \oplus (\oplus_{i=1}^a \oplus_{j=1}^{r_i} \oplus_{b=1}^i \oplus_{t=1}^{\phi(p^b)/d_b} (\mathbb{F}_l[x]/P_{bt}(x))) \\ &\cong \mathbb{F}_l^{r_X-1} \oplus (\oplus_{i=1}^a \oplus_{t=1}^{p^{i-1}(p-1)/d_i} (\mathbb{F}_l[x]/P_{it}(x))^{\sum_{j=i}^a r_j}). \end{aligned}$$

□

Lemma 5.19. *The $\mathbb{Z}/l\mathbb{Z}$-cover $V_{ij} \longrightarrow V$ in the proof of Lemma 5.18 is ramified at each v_{I1k}, $1 \le k \le p^I$, and each v_{ijk}, $1 \le k \le p^i$, and étale elsewhere.*

For $i > 0$ and any irreducible G-submodule M of W_{ij}, the corresponding M-cover of V will be ramified at each point in $\psi^{-1}(x_{ij}) = \{v_{ij1},\dots,v_{ijp^i}\}$ and étale elsewhere.

Proof. Once we have fixed an index $I \in \{0,\dots,a\}$, V_{ij} corresponds to $([L],D) \in \imath(P_{\text{ram}})$, where $f(([L],D)) = D \mod l = \lceil p^{I-i}\rceil \sum_{k=1}^{p^i} v_{ijk} - \lceil p^{i-I}\rceil \sum_{k=1}^{p^I} v_{I1k} \in P_{\text{ram}}$. Since

$(\lceil p^{I-i}\rceil, -\lceil p^{i-I}\rceil)$ is either $(p^{I-i}, -1)$ or $(1, -p^{i-I})$, coefficient of each $vijk$ and v_{I1k} is nonzero in $\mathbb{Z}/l\mathbb{Z}$. The result follows from the discussion after Corollary 3.20.

Let w be a nonzero element of $M \subset W_{ij} =< B_{ij} >$. Then $w = \sum_{k=1}^{p^i} a_{ijk}v_{ijk}$ for $a_{ijk} \in \mathbb{Z}/l\mathbb{Z}$. Then at least one coefficient, say $a_{ij\kappa}$ is nonzero. For $1 \leq t \leq p^i$, let $1 \leq \overline{\kappa+t} \leq p^i$ such that $\kappa + t \equiv \overline{\kappa+t} \mod p^i$. Then $a_{ij\kappa}v_{ij\overline{\kappa+t}}$ is present in the expression of $w \cdot \sigma^t$ and $\{\overline{\kappa+t} : 1 \leq i \leq p^i\} = \{1, \ldots, p^i\}$. The the cover corresponding to $\imath(w \cdot \sigma^t)$ is ramified at $v_{ij\overline{\kappa+t}}$. Since G acts transitively on $\psi^{-1}(x_{ij})$, M is G-stable and the M-cover of V dominates the connected component of the cover corresponding to every element in M, the M-cover is ramified at each point in $\psi^{-1}(x_{ij})$. □

Proposition 5.20. *Let the hypothesis and notations be as in the Theorem 4.12 and Lemma 5.18. Let $\Psi : W \longrightarrow V$ be an H-Galois cover corresponding to a proper solution of an EP $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G)$. Let $B_j^W := \{x \in C_j^X :$ points in W over some $v \in \psi^{-1}(\{x\})$ is ramified$\}$, possibly empty. Then the genus of W is*

$$g_W = \frac{2 + |H|(2g_V - 2) + l^{n-1}(l-1)(\sum_{j=0}^{a} |B_j^W|p^j)}{2}.$$

Proof. Note that for any $x \in B_j^W$ and for every $w \in (\psi \circ \Psi)^{-1}(\{x\})$ and $e(w|\Psi(w)) = l$, $\#(\Psi^{-1}(\Psi(w))) = |H|/l = l^{n-1}$ (by Lemma 3.13). Since there are p^j points in S_V over each $x \in B_j^W$ and l^{n-1} points in W over each $v \in \psi^{-1}(\{x\})$, by Theorem 3.14, $2g_W - 2 = |H|(2g_V - 2) + l^{n-1}(\sum_{j=0}^{a} |B_j^W|p^j)(l-1)$. □

Now we can calculate the minimal genus of $H \rtimes_\theta G$-covers of X dominating $\psi : V \to X$ in specific cases.

Corollary 5.21. *Let the hypothesis and the notations be as in the Theorem 4.12, Lemma 5.18 and Proposition 5.20. Let $P_l(V \setminus S_V) = \text{Pic}^0(V)[l] \oplus P_{\text{ram}} \cong (\oplus_i W_i^{\beta_i'}) \oplus (\oplus_i W_i^{\beta_i''})$ be a G-stable decomposition into non-isomorphic irreducible submodules W_i, β_i and β_i' are non-negative integers. Let W_0 be the trivial representation. Let $\theta : G \to \text{Aut}(H)$, $H \cong \oplus W_i^{\gamma_i}$ as G-modules for non-negative integers γ_i. Assume that $\gamma_i \leq \beta_i' + \beta_i''$. Let $H' = \oplus_i W_i^{\min\{\beta_i', \gamma_i\}}$ and $H'' = \oplus_i W_i^{\alpha_i}$, where $\alpha_i = 0$ if $\beta_i' \geq \gamma_i$, $\alpha_i = \gamma_i - \beta_i'$ if $\beta_i' < \gamma_i$. Then $H = H' \oplus H''$. Let $g_{\min}$ be the minimum of genera of H-covers of V corresponding to the proper solutions of the EP $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha)$.*

1. *Let S_X contain r_0 elements and each v in S_V be totally ramified. Then*

$$g_{\min} = \frac{2 + |H|(2g_V - 2) + l^{n-1}(l-1)(\alpha_0 + 1)}{2}.$$

2. *Let there be r_1 elements in S_X and for each $x \in S_X$, let there be p elements in $\psi^{-1}(x)$. Let $\alpha_0 \neq 0$. Then*

$$g_{\min} = \frac{2 + |H|(2g_V - 2) + l^{n-1}(l-1)p\max\{\alpha_0 + 1, \alpha_1, \alpha_2 \ldots\}}{2}.$$

3. *Let $S_X = C_0^X \sqcup C_1^X$ such that for each $x \in C_i^X$ there are p^i elements in $\psi^{-1}(\{x\})$, $i = 0, 1$. Let there be r_i elements in C_i^X. Then $g_{\min} = \frac{2+|H|(2g_V-2)+l^{n-1}(l-1)B}{2}$ where B is as follows:*

   (a) *If $\alpha_i = 0$ for all $i > 0$*

      i. *if $\alpha_0 \leq r_0 - 1$, then $B = (\alpha_0 + 1)$,*

      ii. *if $r_0 \leq \alpha_0 \leq r_0 + r_1 - 1$, then $B = [(\alpha_0 + 1 - r_0)p + r_0]$.*

   (b) *If $\alpha_i \neq 0$ for some $i > 0$*

      i. *if $\alpha_0 + 1 \leq \max_{i>0}\{\alpha_i\}$, then $B = (\max_{i>0}\{\alpha_i\})p$,*

      ii. *if $\max_{i>0}\{\alpha_i\} < \alpha_0 + 1 \leq \max_{i>0}\{\alpha_i\} + r_0$, then $B = [(\max_{i>0}\{\alpha_i\})p + (\alpha_0 + 1 - \max_{i>0}\{\alpha_i\})]$,*

      iii. *if $\max_{i>0}\{\alpha_i\} + r_0 < \alpha_0 + 1 \leq r_0 + r_1$, then $B = [(\alpha_0 + 1 - r_0)p + r_0]$.*

Proof. Let $\Psi : W \longrightarrow V$ be an H-Galois cover such that the composition $\psi \circ \Psi : W \longrightarrow X$ is a $H \rtimes_\theta G$-Galois cover of X, étale away from S_X. The genus of W is determined by the number of ramification points of the H-cover $W \longrightarrow V$. If W is of minimum genus among all such curves, then the corresponding inclusion map $H \hookrightarrow P_l(V \setminus S_V)$ (by Theorem 1.1) must satisfy $H \cap \mathrm{Pic}^0(V)[l] = H'$ (this is because the elements in $\mathrm{Pic}^0(V)[l]$ correspond to étale covers of V). We have to choose $H'' \hookrightarrow P_{\mathrm{ram}}$, such that for the corresponding H-cover $W \longrightarrow V$, $B_j^W \subset C_j^X$ as in Proposition 5.20 and that the number of ramification points $\sum_{j=0}^{a} |B_j^W| p^j$ is minimum.

1. Here $S_X = C_0^X = \{x_1, \ldots, x_{r_0}\}$, $P_{\mathrm{ram}} \cong \mathbb{F}_l^{r_0-1}$ and $H'' \cong W_0^{\alpha_0} \cong \mathbb{F}_l^{\alpha_0}$. Note that $\alpha_0 + 1 \leq r_0$. Put $H'' \cong < x_2 - x_1, \ldots, x_{\alpha_0+1} - x_1 >$ so that for the resultant $H' \oplus H''$-cover $W \longrightarrow V$, $B_0^W = \{x_1, \ldots, x_{\alpha_0+1}\}$. Then the H-cover $W \longrightarrow V$ has the required genus. For any other H-cover $W' \longrightarrow V$ satisfying the given conditions, $|B_j^{W'}| \geq \dim(H'') + 1 = \alpha_0 + 1$. Therefore, the genus of W above is minimal.

2. Here $S_X = C_1^X = \{x_1, \ldots x_{r_1}\}, r_X = r_1, \#(S_V) = pr_1$, and

$$H'' \cong \mathbb{F}_l^{\alpha_0} \oplus [\oplus_{i=1}^{(p-1)/d_1} (\mathbb{F}_l[x]/P_{1i}(x))^{\alpha_i}].$$

   Let $A = \max\{\alpha_0 + 1, \alpha_1, \alpha_2, \ldots\}$. Choose $< x_2 - x_1, \ldots, x_{\alpha_0+1} - x_1 > \cong \mathbb{F}_l^{\alpha_0}$. For $1 \leq j \leq \alpha_i$, choose the irreducible submodule isomorphic to $\mathbb{F}_l[x]/(P_{1i}(x))$ from a fixed decomposition of $W_{1j} \cong \oplus_{t=1}^{(p-1)/d_1} \mathbb{F}_l[x]/P_{1t}(x)$ (as in the proof of the lemma above). These will give G-stable submodule isomorphic to $\mathbb{F}_l[x]/(P_{1i}(x))^{\alpha_i}$. From these and the $H' \hookrightarrow \mathrm{Pic}^0(V)[l]$, we form an H-cover W of V, and $B_1^W = \{x_1, \ldots, x_A\}$. Then the genus of W is $g_{\min}$.

   Let W' be another $H \rtimes_\theta G$-cover of X dominating V, étale away from S_X. Then $B_1^{W'} \subset S_X$. We may assume that w.r.to the H-cover $W' \to V$, $H \cap \mathrm{Pic}^0(V)[l] = H'$. Then its genus is $g_{W'} = \frac{2+|H|(2g_V-2)+l^{n-1}(l-1)(|A_1^{W'}|p)}{2}$. Note that $\mathbb{F}_l^{\alpha_0}$ ensures that

there are at least α_0+1 points in $B_1^{W'}$. Also, by comparing dimension, $\#(B_1^{W'}) \geq \alpha_i$. Therefore $g_{W'} \geq g_{\min}$.

3. Assume that $C_0^X = \{x_{01}, \ldots x_{0r_0}\}$ and $C_1^X = \{x_{11}, \ldots x_{1r_1}\}$.

   (a) Here $H'' \cong W_0^{\alpha_0}$.

      i. Since $a_0 + 1 \leq r_0$, we choose the isomorphism: $H'' \cong < \{v_{0j1} - v_{011} : 0 \leq j \leq \alpha_0 + 1\} >$. For the corresponding H-cover $W \longrightarrow V$, B_0^W is $\{x_{01}, \ldots, x_{0,\alpha_0+1}\}$. Clearly, this gives us the minimal genus curve.

      ii. If $r_0 < \alpha_0+1 \leq r_0+r_1$, then identify H'' with the vector space generated by $\{v_{0i1} - v_{011} : 1 \leq i \leq \alpha_0+1\} \sqcup \{\sum_{k=1}^p v_{ijk} - p \cdot v_{011} | 1 \leq j \leq t\}$ which gives us the cover $W \longrightarrow V$ with $B_0^W = C_0^X$, $B_1^W = \{x_{11}, \ldots, x_{1t}\}$ for $t = \alpha_0 - (r_0 - 1)$. Clearly, W has the minimal genus mentioned above.

   (b) Here $H'' \cong \mathbb{F}_l^{\alpha_0} \oplus [\oplus_{i=1}^{(p-1)/d_1} (\mathbb{F}_l[x]/P_{1i}(x))^{\alpha_i}]$. We begin by embedding the nontrivial part of H'' in P_{ram} as those can only be generated by elements in C_1^X. As in the first part of the proof above, we get $B_1^{(1)} \subset C_1^X$ ($B_1^{(1)}$ here is the set B_1^W in part 2 when $\alpha_0 = 0$). Assume that $B_1^{(1)} = \{x_{11}, \ldots, x_{1A}\}$, $A = \max_{i>0}\{\alpha_i\}$.

      i. When $\alpha_0+1 \leq A$, $< \sum_{k=1}^p v_{1jk} - \sum_{k=1}^p v_{11k} | 2 \leq j \leq \alpha_0+1 > \cong (\frac{\mathbb{F}_l[x]}{(x-1)})^{\alpha_0}$ and no additional point gets ramified. $B_0^W = \phi$ and B_1^W has $\max_{i>0}\{\alpha_i\}$ points. Now apply Proposition 5.20.

      ii. When $A < \alpha_0 + 1 \leq A + r_0$, $< \{\sum_{k=1}^p v_{1jk} - \sum_{k=1}^p v_{11k} | 1 < j \leq A\} \sqcup \{p \cdot v_{0j1} - \sum_{k=1}^p v_{11k} | 1 \leq j \leq \alpha_0 + 1 - A > \cong (\frac{\mathbb{F}_l[x]}{(x-1)})^{\alpha_0}$, $B_0^W = \{x_{0i} | 1 \leq i \leq \alpha_0 + 1 - A\}$, $B_1^W = B_1^{(1)}$. Apply Proposition 5.20.

      iii. When $A + r_0 < \alpha_0 + 1 \leq r_0 + r_1$, we have to choose extra $\alpha_0 + 1 - A - r_0$ elements from $\psi^{-1}(C_1^X \setminus B_1^{(1)})$. $\{\sum_{k=1}^p v_{1jk} - \sum_{k=1}^p v_{11k} : A+1 \leq j \leq A + (\alpha_0 + 1 - A - r_0)\}$ should be taken with the basis above to generate a vector space isomorphic to $\mathbb{F}_l^{\alpha_0}$. Then $B_0^W = C_0^X$, $B_1^W = B_1^{(1)} \sqcup \{x_{1j} | A + 1 \leq j \leq \alpha_0 + 1 - r_0\}$, $\#(B_1^W) = \alpha_0 + 1 - r_0$. Again apply Proposition 5.20.

□

Notation. Let M_{it} denote the irreducible G-module $\mathbb{F}_l[x]/P_{it}(x)$ for $i \leq i \leq a$, $1 \leq t \leq p^{i-1}(p-1)/d_i$ (σ acts by multiplication by x). For $1 \leq j \leq r_i$, the multiplicity of M_{it} in W_{sj} is 1 if $s \geq i$, the multiplicity is zero if $s < i$.

Let the hypothesis and the notations be as in the Theorem 4.12, the Lemma 5.18 and the Proposition 5.20. Let the G-modules H, H', H'' be as in the Corollary 5.21.

Corollary 5.22. *Consider the G-stable decomposition $H'' \cong \mathbb{F}_l^{\alpha_0} \oplus (\oplus_{i=1}^a \oplus_{t=1}^{p^{i-1}(p-1)/d_i} M_{it}^{\alpha_{it}})$ for non-negative integers α_0, α_{it}. In general, a method of finding an $H \rtimes_\theta G$-cover of X of genus $\mathfrak{g}$, minimum among the genera of all the covers corresponding to the*

proper solutions of the EP $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha)$ *is given by the following integer linear programming problem with bounded variables.*

Minimize

$$\sum_{i=0}^{a} p^i y_i$$

subject to : $\sum_{s=i}^{a} y_s \geq \max_t\{\alpha_{it}\}$, *for* $i > 0$ *and* $\sum_{i=0}^{a} y_i \geq \alpha_0 + 1$; *with* $0 \leq y_i \leq r_i$ *and* $y_i \in \mathbb{Z}$, $0 \leq i \leq a$.

If $c_{\min}$ *is the minimum value of* $\sum_{i=0}^{a} p^i y_i$, *then the minimum genus is*

$$\mathfrak{g} = \frac{2 + l^n(2g_V - 2) + l^{n-1}(l-1)c_{\min}}{2}.$$

Proof. Let $\Psi : W \longrightarrow V$ be an H-cover corresponding to a proper solution for the given EP. WLOG, we may assume that the corresponding G-module monomorphism $H \hookrightarrow P_l(V \setminus S_V)$ (by Theorem1.1) satisfies $H' \hookrightarrow \mathrm{Pic}^0(V)[l]$ and $H'' \hookrightarrow P_{\mathrm{ram}}$ (since the direct summand of H embedded into $\mathrm{Pic}^0(V)[l]$ does not contribute to the degree of the ramification divisor of Ψ). By Proposition 5.20 the genus of W depends on the cardinality $\sum_0^a p^i |B_i^W|$ of the (tamely) ramified points of Ψ in V, for all proper solutions of the EP. By Lemma 5.19, the non-trivial part $\oplus_{i>0} \oplus_t M_{it}^{\alpha_{it}}$ of H'' is embedded into $\oplus_{x_{sj} \in \sqcup_{s=1}^a B_s^W} W_{sj}$. Also, for $i > 0$, $M_{it}^{\alpha_{it}} \subset \ker(\Phi_{p^i}(\sigma|_{H''}))$ is embedded into $\ker(\Phi_{p^i}(\sigma|_{P_{\mathrm{ram}}})) = \oplus_{s=i}^a \oplus_{j=1}^{r_s} W_{sj}$. Hence the image of $M_{it}^{\alpha_{it}} \subset H''$ must be in

$$(\oplus_{x_{sj} \in \sqcup_{s=1}^a B_s^W} W_{sj}) \cap (\oplus_{s=i}^a \oplus_{j=1}^{r_s} W_{sj}) = \oplus_{x_{sj} \in \sqcup_{s=i}^a B_s^W} W_{sj}.$$

Note that the multiplicity of M_{it} in $\oplus_{x_{sj} \in \sqcup_{s=i}^a B_s^W} W_{sj}$ is $\sum_{s=i}^a |B_s^W|$. Hence $\sum_{s=i}^a |B_s^W| \geq \alpha_{it}$, the multiplicity of M_{it} in H'', for each $t \in \{1, \ldots, \frac{p^{i-1}(p-1)}{d_i}\}$. Clearly, if $\alpha_0 > 0$, then $\mathbb{F}_l^{\alpha_0} \hookrightarrow P_{\mathrm{ram}}(S_V, l)$ factors through $\mathbb{F}_l^{\alpha_0} \hookrightarrow P_{\mathrm{ram}}(S_X, l)$ and the corresponding $\mathbb{F}_l^{\alpha_0}$-cover of X (dominated by $W \longrightarrow X$) is ramified over at least $\alpha_0 + 1$ points in $\sqcup_0^a B_i^W$. Hence, $\sum_{s=0}^a |B_s^W| \geq \alpha_0 + 1$. Since $B_i^W \subset C_i^X$, $|B_i^W| \leq r_i$. Put $y_i = |B_i^W|$. Then we have to minimize $\sum_0^a p^i y_i$ subject to the given conditions for integer values of y_i in the given range.

Suppose the minimum value $c_{\min}$ is attained at $y_i = \lambda_i$. For $i \geq 0$, we choose subsets Λ_i of cardinality λ_i in C_i^X. For $i \geq 1$, we can define $M_{it}^{\alpha_{it}} \hookrightarrow \oplus_{x_{sj} \in \sqcup_{s=i}^a \Lambda_s} W_{sj}$ (since the multiplicity of M_{it} in the later is $\sum_i^a \lambda_s \geq \max_t \alpha_{it}$). For $\mathbb{F}_l^{\alpha_0} \hookrightarrow P_{\mathrm{ram}}(S_X, l)$ $(\subset P_{\mathrm{ram}}(S_V, l))$ we choose $\alpha_0 + 1$ points $\{u_0, \ldots, u_{\alpha_0}\}$ in $\sqcup_{s=0}^a \Lambda_s$ and define $\mathbb{F}_l^{\alpha_0+1} \xrightarrow{\cong} < u_s - u_0 | 1 \leq s \leq \alpha_0 >$. Choose $H' \hookrightarrow \mathrm{Pic}^0(V)[l]$ and this will give us an H-cover $\Psi' : W' \longrightarrow V$ (by Theorem 1.1) and the image of its branch locus in X will be contained in $\sqcup_{s=0}^a \Lambda_s$ (by Lemma 5.19). In fact, the image is exactly $\sqcup_{s=0}^a \Lambda_s$ as $\sum_0^a p^i \lambda_i$ is minimum. Clearly, the genus of W' is $\mathfrak{g}$ and it is minimum. □

Example 5.23. Let X be $\mathbb{P}^1_k = \operatorname{Spec} k[x] \cup \operatorname{Spec} k[\frac{1}{x}]$, $p = 5$, $l = 11$, $a = 2$, $G =< \sigma >\cong \mathbb{Z}/25\mathbb{Z}$, $S_X = \sqcup_0^2 C_i^X$, $C_i^X = \{x_{i1}, x_{i2}, x_{i3}\}$, where $x_{ij} := (x = \varepsilon_{ij}) \in \mathbb{P}^1_k$ for $\{\varepsilon_{ij} : i = 0, 1, 2; j = 1, 2, 3; \varepsilon_{ij} \neq \varepsilon_{i'j'} \text{ if } (i, j) \neq (i', j')\} \subset k$.

Let $\psi : V \longrightarrow \mathbb{P}^1_k$ corresponding to $\alpha : \pi_1^{\text{ét}}(\mathbb{P}^1_k \setminus S_X) \twoheadrightarrow G$ be given by the witt vector

$$(f_1, f_2) = \left(\frac{1}{(x-\varepsilon_{01})^2(x-\varepsilon_{02})^2(x-\varepsilon_{03})^2}, \frac{1}{(x-\varepsilon_{11})^2(x-\varepsilon_{12})^2(x-\varepsilon_{13})^2} \right) \in W_2(k).$$

Then $k(V) = k(x)[x_1, x_2]/I$ where the ideal I is generated by

$$\begin{aligned} x_1^5 - x_1 &= f_1, \\ x_2^5 - x_2 + x_1^{21} - 2x_1^{17} + 2x_1^{13} - x_1^9 &= f_2. \end{aligned}$$

• Let $H = \left(\frac{\mathbb{Z}}{25\mathbb{Z}}\right)^n \cong \operatorname{Pic}^0(V)[11] \oplus (\mathbb{F}_{11})^3 \oplus \left(\frac{\mathbb{F}_{11}[T]}{(T-3)}\right)^4 \oplus \left(\frac{\mathbb{F}_{11}[T]}{(T-4)}\right)^3 \oplus \left(\frac{\mathbb{F}_{11}[T]}{(T^5-9)}\right)^2 \oplus \left(\frac{\mathbb{F}_{11}[T]}{(T^5-5)}\right)$ as a G-module for $n = 2g_V + 25$ and θ be the corresponding G-action (σ acts on the nontrivial summands by multiplication by T). We want to calculate the minimum $g_{\min}$ of genera of H-covers of V corresponding to the proper solutions of the EP

$$((\mathbb{Z}/11\mathbb{Z})^{2g_V+25} \rtimes_\theta \mathbb{Z}/25\mathbb{Z} \twoheadrightarrow (\mathbb{Z}/25\mathbb{Z}), \alpha : \pi_1^{\text{ét}}(\mathbb{P}^1_k \setminus S_X) \twoheadrightarrow \mathbb{Z}/25\mathbb{Z}).$$

Note that $r_0 = r_1 = r_2 = 3$ and $r_X = \sum_i r_i = 9$. Let $X_1 \longrightarrow \mathbb{P}^1_k$ be the ($\mathbb{Z}/5\mathbb{Z}$-Galois) intermediate cover given by the normalization of $\mathbb{P}^1_k$ in $k(x, x_1)$ ($\subset k(V)$). It is totally ramified over C_0^X as f_1 has poles of order 2 only at those points. Since $x_1 \in k(X_1)$ has poles (of order 2) only at those ramified points and f_2 does not, $V \longrightarrow \mathbb{P}^1_k$ is totally ramified at points over C_0^X. Since $f_2 - (x_1^{21} - 2x_1^{17} + 2x_1^{13} - x_1^9)$ has poles (of order coprime to 5) only at points in X_1 over $C_0^X \sqcup C_1^X$, $V \longrightarrow X_1$ is totally ramified at these points, i.e., $V \longrightarrow \mathbb{P}^1_k$ is ramified at points in C_1^X, with ramification index 5. In fact, the order of the pole of $f_2 - (x_1^{21} - 2x_1^{17} + 2x_1^{13} - x_1^9)$ at the unique point in X_1 over x_{0j} (respectively, at each of the 5 points in X_1 over x_{1j}) is 42 (respectively 2), Let $S_V = \psi^{-1}(S_X)$. Now we are in the setup of the above corollary.

Note that $d_1 = 1$, $d_2 = 5$ and we have the following factorization in $\mathbb{F}_{11}[T]$ into irreducible factors:

$$T^{25} - 1 = (T-1)(\prod_{t=1}^{4}(T - 3^t))(\prod_{t=1}^{4}(T^5 - 3^t)).$$

Here $3^2 = 9, 3^3 = 5, 3^4 = 4$ in $\mathbb{F}_{11}$. Then we have a G-module decomposition:

$$P_{11}(V \setminus S_V) \cong \operatorname{Pic}^0(V)[11] \oplus (\mathbb{F}_{11})^8 \oplus \left(\oplus_{t=1}^4 (\mathbb{F}_{11}[T]/(T - 3^t))^6\right) \oplus \left(\oplus_{t=1}^4 (\mathbb{F}_{11}[T]/(T^5 - 3^t))^3\right).$$

We have $H = H' \oplus H''$, where $H' = \mathrm{Pic}^0(V)[11]$. We want to define an injective homomorphism $H'' \hookrightarrow P_{\mathrm{ram}}(S_V, l)$. Here $\max_t \alpha_{2t} = 2$,, $\max_t \alpha_{1t} = 4$, $\alpha_0 + 1 = 4$. We have to minimize $y_0 + 5y_1 + 25y_2$ subject to $y_2 \geq 2$, $y_1 + y_2 \geq 4$, $y_0 + y_1 + y_2 \geq 4$, $0 \leq y_i \leq 3$, $y_i \in \mathbb{Z}$.

Clearly the minimum value is attained at $y_2 = 2$, $y_1 = 2$, $y_0 = 0$ and $c_{\min} = 0 + 5 \times 2 + 25 \times 2 = 60$.

Choose $\Lambda_2 = \{x_{21}, x_{22}\}$ and simultaneously an embedding $\left(\frac{\mathbb{F}_{11}[T]}{(T^5-9)}\right)^2 \oplus \left(\frac{\mathbb{F}_{11}[T]}{(T^5-5)}\right) \hookrightarrow W_{21} \oplus W_{22}$.

Choose $\Lambda_1 = \{x_{11}, x_{12}\}$ and a G-module monomorphism $\left(\frac{\mathbb{F}_{11}[T]}{(T-3)}\right)^4 \oplus \left(\frac{\mathbb{F}_{11}[T]}{(T-4)}\right)^3 \hookrightarrow W_{11} \oplus W_{12} \oplus W_{21} \oplus W_{22}$.

Clearly Λ_0 is empty. We define an injective map from $\mathbb{F}_l^3$ to the subspace $< \sum_{s=1}^{p} v_{12s} - \sum_{s=1}^{p} v_{11s}, \sum_{s=1}^{25} v_{21s} - 5\sum_{s=1}^{5} v_{11s}, \sum_{s=1}^{25} v_{22s} - 5\sum_{s=1}^{5} v_{11s} >$ of P_{ram}.

If g_1 is the genus of X_1, then (apply Theorem 3.14 on $X_1 \longrightarrow \mathbb{P}^1_k$ and $V \longrightarrow X_1$)

$$2g_1 - 2 = 5(0-2) + 3 \times (2+1)(5-1) \implies g_1 = 14.$$

$$2g_V - 2 = 5(28-2) + 3 \times (42+1)(5-1) + 3 \times 5 \times (2+1)(5-1) \implies g_V = 414.$$

Note that $|H| = 11^{828+3+(4+3)\times 1+(2+1)\times 5} = 11^{853}$. Then the minimal genus is given by

$$g_{\min} = \frac{2 + 11^{853}(828-2) + 11^{853-1}(11-1)(c_{\min})}{2} = 1 + 11^{852} \times 4843.$$

Now we count the number of equivalence classes of solutions for the EPs in Theorem 4.12 for a fixed G action θ on $H = (\mathbb{Z}/l\mathbb{Z})^n$.

Proof of Theorem 4.13. Since $\gcd(|G|, l) = 1$, by Theorem 3.49, $H^2(G; (\mathbb{Z}/l\mathbb{Z})^n)$ is trivial. Hence any extension of G by $(\mathbb{Z}/l\mathbb{Z})^n$ must be a semidirect product. Hence $NSExt(\theta, \alpha) = NS(H \rtimes_\theta G \twoheadrightarrow G, \alpha)$.

Let $P_l(V \setminus S_V) \cong (\mathbb{F}_l)^{n_0} \oplus (\oplus_{b=1}^{a} \oplus_{i=1}^{p^{b-1}(p-1)/d_b} (\mathbb{F}_l[x]/P_{bi}(x))^{\gamma_{bi}})$ and fix an isomorphism $H \cong (\mathbb{F}_l)^u \oplus (\oplus_{b=1}^{a} \oplus_{i=1}^{p^{b-1}(p-1)/d_b} (\mathbb{F}_l[x]/P_{bi}(x))^{\gamma'_{bi}})$ (by Lemma 3.33). Let σ be a generator of G. For $v \in \ker(P_{bi}(\sigma)) \setminus \{0\} \subset P_l(V \setminus S_V)$, $\{v, \sigma v, \ldots, \sigma^{d_b-1} v\}$ is linearly independent and $\{\sum_{j=0}^{d_b-1} \alpha_j \sigma^j v | \alpha_j \in \mathbb{F}_l\}$ is a G-stable irreducible subspace of $\ker P_{bi}(\sigma)$. Note that each nonzero element of $\ker(P_{bi}(\sigma))$ generates a G-submodule as above containing $l^{d_b} - 1$ nonzero elements and $\#(\ker(P_{bi}(\sigma)) = l^{d_b \gamma_{bi}}$. Hence the number of d_b-dimensional G-stable subspaces of $\ker(P_{bi}(\sigma))$ is

$$a_{bi} = \frac{l^{d_b \gamma_{bi}} - 1}{l^{d_b} - 1} = (l^{d_b(\gamma_{bi}-1)} + l^{d_b(\gamma_{bi}-2)} + \ldots + l^{d_b} + 1)$$

and the same for $\ker_H(P_{bi}(\sigma))$ is $a'_{bi} = \frac{l^{d_b\gamma'_{bi}}-1}{l^{d_b}-1}$. Since these distinct subspaces are irreducible, the intersection of any two of them is trivial. So we can choose first two in $a_{bi}(a_{bi}-1)$ ways. After we have chosen first $t \geq 2$ so that their sum is a direct sum, again note that this direct sum contains $\frac{l^{td_b}-1}{l^{d_b}-1}$ irreducible subspaces. Hence, we can choose the $(t+1)$-th component in $(a_{bi} - \frac{l^{td_b}-1}{l^{d_b}-1})$ ways.

The number of ways to choose first γ'_{bi} components up to G-module automorphism

$$= \frac{a_{bi}(a_{bi}-1)(a_{bi}-\frac{l^{2d_b}-1}{l^{d_b}-1})(a_{bi}-\frac{l^{3d_b}-1}{l^{d_b}-1})\dots(a_{bi}-\frac{l^{(\gamma'_{bi}-1)d_b}-1}{l^{d_b}-1})}{a'_{bi}(a'_{bi}-1)(a'_{bi}-\frac{l^{2d_b}-1}{l^{d_b}-1})(a'_{bi}-\frac{l^{3d_b}-1}{l^{d_b}-1})\dots(a'_{bi}-\frac{l^{(\gamma'_{bi}-1)d_b}-1}{l^{d_b}-1})} = \frac{n_{bi}}{n'_{bi}}.$$

Similarly, the number of ways to choose first u components of $P_l(V \setminus S_V)^G$ up to G-module isomorphism is $\bar{n}/\overline{n'}$. Then we get $[\Pi_{b=1}^{a}\Pi_{i=1}^{p^{b-1}(p-1)/d_b}(n_{bi}/n'_{bi})]\bar{n}/\overline{n'}$ distinct G-submodules of $P_l(V \setminus S_V)$ isomorphic to H. Now apply Corollary 5.4. □

The following result (a consequence of Proposition 5.8) holds for any finite group G and any positive integer m coprime to p.

Lemma 5.24. *Let $K \trianglelefteq G$, $\gcd(m, |K|) = 1$ and $Y = V/K$. Then $\mathrm{Pic}^0(V)[m]^K = \mathrm{Pic}^0(Y)[m]$.*

Proof. Let ψ factor through $h : V \xrightarrow{K} Y$ and $f : Y \xrightarrow{G/K} X$. By Proposition 5.8, we identify $\mathrm{Pic}^0(Y)[m]$ with $h^*(\mathrm{Pic}^0(Y)[m]) \subset \mathrm{Pic}^0(V)[m]^K$. Let $\lambda \in \mathrm{Pic}^0(V)[m]^K$. Then $< \lambda >$ is K-stable (in fact, $\lambda \cdot g = \lambda \ \forall g \in K$). If $W_\lambda \longrightarrow V$ is the corresponding m-cyclic cover with Galois group $< \lambda >$ then the composition $W_\lambda \longrightarrow V \longrightarrow X$ is also Galois (by Proposition 5.1). Since $\gcd(m, |K|) = 1$, $H^2(< \lambda >; K) = \{0\}$ and hence $\mathrm{Aut}(W_\lambda|X) =< \lambda > \rtimes K$. But the K-action on $< \lambda >$ is trivial. Hence $\mathrm{Aut}(W_\lambda|X) =< \lambda > \times K$. Then $W_\lambda/K \xrightarrow{<\lambda>} Y$ is a Galois cover. In other words, $\lambda \in h^*(\mathrm{Pic}^0(Y)[m]) = \mathrm{Pic}^0(Y)[m]$. □

Lemma 5.25. *Let the hypothesis be as in Theorem 4.12. Let σ_o be the linear transformation on the $\mathbb{F}_l$-vector space $\mathrm{Pic}^0(V)[l]$ induced by σ. Then $\dim_{\mathbb{F}_l}(\ker(\Phi_{p^b}(\sigma_o))) = 2g_b - 2g_{b-1}$ for $0 \leq b \leq a$, where $g_{-1} := 0$, and g_b is the genus of $V/ < \sigma^{p^{a-b}} >$ for $0 \leq b \leq a$.*

Proof. Let $\tau = \sigma^{p^{a-1}}$, τ_o be the linear transformation induced by τ on $\mathrm{Pic}^0(V)[l]$ and consider the intermediate p-cyclic cover $V \longrightarrow V/ < \tau >= X_{a-1}$. Since $\ker(\tau_o - \mathrm{Id}) = \mathrm{Pic}^0(X_{a-1})[l]$ by the lemma above and the minimal polynomial of τ_o divides $x^p - 1 = (x-1)\Phi_p(x)$, we have $\mathrm{Pic}^0(V)[l] = \mathrm{Pic}^0(X_{a-1})[l] \oplus \ker(\Phi_p(\tau_o))$. Since $\Phi_{p^a}(x) = \frac{(x^{p^{a-1}})^p-1}{x^{p^{a-1}}-1} = \Phi_p(x^{p^{a-1}})$, $\ker(\Phi_p(\tau_o)) = \ker(\Phi_{p^a}(\sigma_o))$ and it has dimension $2g_a - 2g_{a-1} = 2g_V - 2g_{a-1}$.

Let $\overline{\sigma}$ be the image of σ in the quotient group $\mathrm{Aut}(X_{a-1}|X)$, a p^{a-1}-cyclic group generated by $\overline{\sigma}$. Let $\overline{\sigma_o}$ be the linear transformation on $\mathrm{Pic}^0(X_{a-1})[l]$ induced by $\overline{\sigma}$. As before, we see that the dimension of $\ker(\Phi_{p^{a-1}}(\overline{\sigma_o}))$ is $2g_{a-1} - 2g_{a-2}$. But as operators on $\mathrm{Pic}^0(X_{a-1})[l]$, $\overline{\sigma_o} = \sigma_o$. Hence $\ker(\Phi_{p^{a-1}}(\sigma_o))$ has dimension $2g_{a-1} - 2g_{a-2}$. Now the result follows from induction. □

The result below follows directly from Lemma 5.18 and the lemma above.

Corollary 5.26. *Let g_b be the genus of $V/ < \sigma^{p^{a-b}} >$, $0 \leq b \leq a$. The dimension of $\ker(\Phi_{p^b}(\sigma)) \subset P_l(V \setminus S_V)$ (in Theorem 4.12) is given by $n_b = 2g_b - 2g_{b-1} + p^{b-1}(p-1)\sum_{i=b}^{a} r_i$ for $1 \leq b \leq a$. The dimension of $P_l(V \setminus S_V)^G$ is $n_0 = 2g_X + r_X - 1$.*

Remark 5.27. From Corollary 5.26, it is obvious that the dimensions n_b, $0 \leq b \leq a$, are independent of the prime number l.

Example 5.28. Let X be $\mathbb{P}^1_k = \mathrm{Spec}\, k[x] \cup \mathrm{Spec}\, k[\frac{1}{x}]$, $p = 3$, $l = 2$, $a = 2$, $G =< \sigma >\cong \mathbb{Z}/9\mathbb{Z}$, $S_X = \infty$. Let $\psi : V \longrightarrow \mathbb{P}^1_k$ corresponding to $\alpha : \pi_1^{\text{ét}}(\mathbb{A}^1_k) \twoheadrightarrow G$ be given by a witt vector (f_1, f_2) for polynomials f_1 of degree 2, f_2 of degree 4 in k[x]. Then $k(V) = k(x)[x_1, x_2]/I$ where the ideal I is generated by

$$x_1^3 - x_1 = f_1,$$
$$x_2^3 - x_2 + x_1^7 - x_1^5 = f_2$$

and $f_1 \neq g_1^3 - g_1$ for any $g_1 \in k(x)$, $x_1^7 - x_1^5 - f_2 \neq g_2^3 - g_2$ for any $g_2 \in k(x, x_1)$.

• We will show that the EP $\mathcal{E}_n = ((\mathbb{Z}/2\mathbb{Z})^n \rtimes_\theta (\mathbb{Z}/9\mathbb{Z}) \twoheadrightarrow \mathbb{Z}/9\mathbb{Z}, \alpha)$ have solution for some θ iff $0 < n = 6, 12, 18, 24, 30; 2, 8, 14, 20, 26, 32$.

• Let $H = (\mathbb{Z}/2\mathbb{Z})^{18} \cong (\mathbb{F}_2[T]/(T^6 + T^3 + 1))^3$ as a $(\mathbb{Z}/9\mathbb{Z})$-module, and θ_1 be the corresponding action (σ acts by multiplication by T). We will show that $NSExt(\theta_1, \alpha) = 69827305537$.

Let $X_1 \longrightarrow \mathbb{P}^1_k$ be the intermediate cover, with function field $k(x, x_1)$ $(\subset k(V))$. Clearly, $V \longrightarrow \mathbb{P}^1_k$ is ramified only at ∞. Since f_1 has pole of order 2 only at ∞, the genus of X_1 is $g_1 = \frac{(3-1)(2-1)}{2} = 1$. Note that x and x_1 has poles of respective orders 3, 2 at ∞. Clearly, $x_1^7 - x_1^5 - f_2$ has pole of order 14 at the point in X_1 above ∞ and so the genus of V is $g_V = \frac{2+3(2g_1-2)+(14+1)(3-1)}{2} = 16$. Note that $d_1 = 2$, $d_2 = 6$.

By Corollary 5.26 $n_1 = 2g_1 - 0 = 2$, $n_2 = 2g_V - 2g_1 = 30$. By Theorem 4.12, the above EP $\mathcal{E}_n$ will have a proper solution for some G-action θ iff $n = 0 + 2\gamma_1 + 6\gamma_2$, $\gamma_1 \leq \frac{2}{2} = 1$, $\gamma_2 \leq \frac{30}{6} = 5$. Hence the values of n are as mentioned above.

Since $d_1 = 2$ and $d_2 = 6$, $\Phi_3(T) = T^2 + T + 1$ and $\Phi_9(T) = T^6 + T^3 + 1$ are irreducible over $\mathbb{F}_2$. Hence $P_2(V \setminus \psi^{-1}(\{\infty\})) \cong \frac{\mathbb{F}_2[T]}{(T^2+T+1)} \oplus \left(\frac{\mathbb{F}_2[T]}{(T^6+T^3+1)}\right)^5$ as G-modules. By Theorem 4.13, $NSExt(\theta, \alpha) = \frac{\prod_{r=0}^{3-1}\sum_{s=r}^{5-1} 2^{6s}}{\prod_{r=0}^{3-1}\sum_{s=r}^{3-1} 2^{6s}} = \frac{17043521 \times 17043520 \times 17043456}{4161 \times 4160 \times 4096} = 69827305537$.

We can replace l by any square-free integer in Theorem 4.12.

Corollary 5.29. *Let G be a cyclic group of order p^a, σ be a generator of G, m be a square free integer prime to p, $m = l_1 \dots l_T$, for distinct prime numbers l_τ; $d_{b\tau}$ be the order of l_τ in $(\mathbb{Z}/p^b\mathbb{Z})^*$, $H = (\mathbb{Z}/m\mathbb{Z})^n$, $n_{0\tau}$ (resp. $n_{b\tau}$, $1 \le b \le a$) be the dimension of $P_{l_\tau}(V \setminus S_V)^G$ (resp. $\ker_\tau(\Phi_{p^b}(\sigma)) \subset P_{l_\tau}(V \setminus S_V)$) over $\mathbb{F}_{l_\tau}$. Then for each $\tau \le T$, n can be expressed as $n = u_\tau + \Sigma_{b=1}^{a} v_{b\tau} d_{b\tau}$ for non-negative integers $u_\tau \le n_{0\tau}$, $v_{b\tau} \le n_{b\tau}/d_{b\tau}, \forall b \le a$ if and only if the embedding problem $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G)$ has a proper solution for some group homomorphism $\theta : G \longrightarrow \mathrm{Aut}(H)$.*

Proof. The abelian groups $P_m(V \setminus S_V), H$ have unique G-stable decompositions: $P_m(V \setminus S_V) = \oplus_{\tau=1}^{T} P_{l_\tau}(V \setminus S_V)$, $H \cong \oplus_{\tau=1}^{T} (\mathbb{Z}/l_\tau\mathbb{Z})^n$. Now apply Theorem 4.12 for each $P_{l_\tau}(V \setminus S_V), H_\tau := (\mathbb{Z}/l_\tau\mathbb{Z})^n$. □

Remark 5.30. By Corollary 5.26, $n_b = n_{b\tau}$ for each $1 \le \tau \le T$.

Let σ be a generator of a cyclic group G of order p^a, c be a positive integer. Then, like Theorem 4.12 and Corollary 5.29, we can give a sufficient condition for solving an EP when the kernel H is an l^c-torsion abelian group.

Let $M = P_{l^c}(V \setminus S_V)$, a $\mathbb{Z}/l^c\mathbb{Z}[G]$-module. Let ζ_{p^b} be a primitive p^b-th root of unity in $\mathbb{C}$, Φ_{p^b} be the monic polynomial of ζ_{p^b} over $\mathbb{Q}$ and $r_b = \frac{p^{b-1}(p-1)}{d_b}$ for $1 \le b \le a$. Let the minimal primes of $l\mathbb{Z}[\zeta_{p^b}]$ be $Q_{b1}, \dots, Q_{br_b}$ (by Proposition 3.34). For $1 \le i \le c$ and $1 \le b \le a$, let f_i' denote $\dim_{(\mathbb{Z}_l/l\mathbb{Z}_l)}(\frac{l^i M^G}{l^{i+1}M^G})$ and f_{bij} denote $\dim_{(\mathbb{Z}[\zeta_{p^b}]/Q_{bj})}(\frac{Q_{bj}^i N_{bj}}{Q_{bj}^{i+1} N_{bj}})$ for $N_{bj} = M/Q_{bj}^c M$.

Corollary 5.31. *Let $H = \oplus_{i=0}^{c} (\mathbb{Z}/l^i\mathbb{Z})^{e_i}$ for non-negative integers e_i and $M = P_{l^c}(V \setminus S_V)$. Let f_i' and f_{bij} be as in the above lemma. If e_i can be expressed as $e_i = e_i' + \sum_{b=1}^{a} d_b e_{bi}''$ for $0 \le e_i' \le f_{i-1}' - f_i'$, $0 \le e_{bi}'' \le \sum_{j=1}^{r_b} (f_{b,i-1,j} - f_{bij})$, $1 \le i \le c$, then the embedding problem $(\beta : H \rtimes_\theta G \twoheadrightarrow G, \alpha : \pi_1^{\text{ét}}(X \setminus S_X) \twoheadrightarrow G)$ has a proper solution for some group homomorphism $\theta : G \longrightarrow \mathrm{Aut}(H)$.*

Proof. Let R denote $\mathbb{Z}[\zeta_{p^b}]$, $N_{bij} = R/Q_{bj}^i \cong R_{Q_{bj}}/(Q_{bj}R_{Q_{bj}})^i$. It is a module over $\mathbb{Z}/l^i\mathbb{Z}$. Note that $N_{bij}/lN_{bij} \cong R_{Q_{bj}}/Q_{bj}R_{Q_{bj}}$ and the latter is of dimension d_b over $\mathbb{Z}/l\mathbb{Z}$. By Nakayama's lemma N_{bij} has a minimal generating set of cardinality d_b over $\mathbb{Z}/l^i\mathbb{Z}$. Since $|N_{bij}| = l^{id_b}$, we have an isomorphism of abelian groups $R/Q_{bj}^i \cong (\mathbb{Z}/l^i\mathbb{Z})^{d_b}$. Then $(\mathbb{Z}/l^i\mathbb{Z})^{e_i'} \oplus (\oplus_{b=1}^{a} (\mathbb{Z}/l^i\mathbb{Z})^{d_b})^{e_{bi}''}$ can be identified as a G-stable submodule of $(\mathbb{Z}/l^i\mathbb{Z})^{f_{i-1}' - f_i'} \oplus (\oplus_{b=1}^{a} \oplus_{j=1}^{r_b} (\mathbb{Z}[\zeta_{p^b}]/(t_{bj}^i))^{f_{b,i-1,j} - f_{bij}})$ (which is a direct summand of $P_{l^c}(V \setminus S_V)$ by Equation (3.3.2)). Hence we get a G-module monomorphism from H into $P_{l^c}(V \setminus S_V)$. The result now follows from Theorem 1.1. □

Bibliography

[1] Abhyankar, Shreeram. *Coverings of algebraic curves*, American Journal of Mathematics 79, no. 4 (1957), 825–856.

[2] Abhyankar, Shreeram. *Tame coverings and fundamental groups of algebraic varieties. Part I. Branch loci with normal crossings; Applications: Theorems of Zariski and Picard*, Amer. J. Math. 81 (1959).

[3] Abhyankar, Shreeram. *Galois theory on the line in nonzero characteristic.* Bull. Amer. Math. Soc. (N.S.) 27 (1992), no. 1, 68–133, DOI 10.1090/S0273-0979-1992-00270-7. MR1118002. 3.2.2, 4.5

[4] Abhyankar, Shreeram. *Resolution of singularities and modular Galois theory.* Bull. Amer. Math. Soc. (N.S.) 38 (2001), no. 2, 131–169, DOI 10.1090/S0273-0979-00-00892-2. MR1816069. 2.1, 4.1, 4.2, 5.2, 5.3, 6

[5] Bost, Jean-Benoit; Loeser, Francois and Raynaud, Michel eds. *Courbes semi-stables et groupe fondamental en g´eom´etrie alg´ebrique.* Progress in Mathematics, vol. 187, Birkhäuser, Basel (2000).

[6] Bary-Soroker, Lior and Kumar, Manish. *Subgroup structure of fundamental groups in positive characteristic*, Communications in Algebra. 41:10, 3705-3719, DOI: 10.1080/00927872.2012.676115 (2013).

[7] Bouw, Irene, I. *Construction of covers in positive characteristic via degeneration*, Proc. Amer. Math. Soc. 137 (2009), no. 10, 3169–3176.

[8] Bouw, Irene I. *Covers of the affine line in positive characteristic with prescribed ramification.* WIN—women in numbers, Fields Inst. Commun., vol. 60, Amer. Math. Soc., Providence, RI, 2011, pp. 193–200. MR2777805.

[9] Eilenberg, Samuel and Saunders, MacLane. *Cohomology theory in abstract groups. II: group extensions with a non-abelian kernel.* Annals of Mathematics 48, no. 2 (1947): 326–41. https://doi.org/10.2307/1969174.

[10] Esnault, Hélène and Viehweg, Eckart. *Lectures on vanishing theorems.* DMV Seminar, Birkhäuser, Basel, 1992.

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

[12] Grothendieck, Alexander. Brief an G. Faltings. In: Schneps L, Lochak P, eds. *Geometric Galois Actions.* London Mathematical Society Lecture Note Series. Cambridge University Press; 1997:49-58.

[13] Gruendken, Linda M., Laura L. Hall-Seelig, Bo-Hae Im, Ekin Ozman, Rachel J. Pries and Katherine F. Stevenson. *Semi-direct Galois covers of the affine line.* WIN - Women in Numbers (2011).

[14] Harbater, David. *Abhyankar's conjecture on Galois groups over curves.* Invent. Math. 117 (1994), no. 1, 1–25, DOI 10.1007/BF01232232. MR1269423.

[15] Harbater, David. *Abhyankar's conjecture and embedding problems.* vol. 2003, no. 559, 2003, pp. 1-24. https://doi.org/10.1515/crll.2003.049

[16] Harbater, David. *Patching and Galois theory*, Galois groups and fundamental groups, Math. Sci. Res. Inst. Publ., vol. 41, Cambridge Univ. Press, Cambridge (2003), pp. 313–424.

[17] Harbater, David and Stevenson, Katherine. *Embedding problems and open subgroups.* Proc. Amer. Math. Soc., 139(4):1141–1154, 2011.

[18] Harbater, David; Obus, Andrew; Pries, Rachel and Stevenson, Katherine. *Abhyankar's Conjectures in Galois Theory: Current Status and Future Directions.* Bull. Amer. Math. Soc. 55, no. 2 (2018), 239–287.

[19] Hirschfeld, James William Peter; Korchmáros, Gábor and Torres, F. *Algebraic curves over a finite field. Princeton Series in Applied Mathematics.* Princeton University Press, Princeton, NJ, 2008.

[20] Kaplansky, Irving. *Modules over Dedekind rings and valuation rings.* Transactions of the American Mathematical Society, 72(2) (1952), pp. 327-340.

[21] Kumar, Manish. *Embedding problems For open subgroups of the fundamental group.* Annales de l'Institut Fourier, Tome 67 (2017) no. 6, pp. 2623-2649. doi : 10.5802/aif.3145.

[22] Lidl, Rudolf and Niederreiter, Harald. *Introduction to finite fields and their applications.* Cambridge University Press, Cambridge, 1986.

[23] Lang, Serge and Serre, Jean-Pierre. *Sur les revêtements non ramifiés des variétés algébriques.* Amer. J. Math. 79 (1957), 319–330.

[24] Milne, James S. *Etale Cohomology.* (PMS-33). Princeton University Press, 1980. JSTOR, http://www.jstor.org/stable/j.ctt1bpmbk1.

[25] Mochizuki, Shinichi. *Absolute anabelian cuspidalizations of proper hyperbolic curves.* J. Math. Kyoto Univ. 47 (2007), no. 3, 451–539.

[26] Muskat, Jeremy and Pries, Rachel. *Alternating group covers of the affine line.* Isr. J. Math. 187, 117–139 (2012).

[27] Neukirch, Jürgen. *Algebraic number theory.* Vol. 322. Springer Science & Business Media (2013).

[28] Osserman, Brian. *Linear series and the existence of branched covers*, Compos. Math. 144 (2008), no. 1, 89–106.

[29] Pries, Rachel J. *Wildly ramified covers with large genus*, J. Number Theory 119 (2006), no. 2, 194–209.

[30] Pop, Florian. $\frac{1}{2}$ *Riemann existence theorem with Galois action.* Algebra and number theory (Essen, 1992), 193-218, de Gruyter, Berlin, 1994.

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

[32] Raynaud, Michel. *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar.* (French), Invent. Math. 116 (1994), no. 1-3, 425–462.

[33] Sengupta, Ambar N. *Representing finite groups: a semisimple introduction.* Springer Science & Business Media, (2011).

[34] Serre, Jean-Pierre. *Linear representations of finite groups.* Vol. 42. New York: Springer (1977).

[35] Serre, Jean-Pierre. *Local Fields.* Springer–Verlag, 1979 (GTM 67).

[36] Serre, Jean-Pierre. *Construction de revêtements étales de la droite affine en caractéristique p.* (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. 311 (1990), no. 6, 341–346.

[37] Saïdi, M. and Tamagawa, Akio. *A prime-to-p version of the Grothendieck anabelian conjecture for hyperbolic curves in characteristic $p > 0$.* Publ. Res. Inst. Math. Sci. 45 (2009), no. 1, 135–186.

[38] Szamuely Tamás. *Galois Groups and Fundamental Groups.* Cambridge: Cambridge University Press; 2009. doi:10.1017/CBO9780511627064

[39] Tamagawa, Akio. *The Grothendieck conjecture for affine curves.* Compositio Math. 109 (1997), no. 2, 135–194.

[40] Tamagawa, Akio. *On the tame fundamental groups of curves over algebraically closed fields of characteristic > 0.* MSRI Publications, Volume 41, 2003.

[41] Tamagawa, Akio. *Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental groups.* J. Algebraic Geom. 13 (2004), 675–724.

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

[43] Uchida, Koji. *Isomorphisms of Galois groups of algebraic function fields.* Ann. Math. (2) 106 (1977), no. 3, 589–598.

[44] Weibel, Charles A. *An introduction to homological algebra (Cambridge Studies in Advanced Mathematics).* (Reprinted 1997) Cambridge: Cambridge University Press. doi:10.1017/CBO9781139644136.

List of Publications

Kumar, Manish and Mandal, Poulami. *A criterion for solving embedding problems for the etale fundamental group of curves.* arXiv preprint arXiv:2303.01187v3 (2023).