MODULAR TOWERS AND TORSION ON ABELIAN VARIETIES

ANNA CADORET

ABSTRACT. The general philosophy of this paper is to provide a link between regular inverse Galois theory - in particular modular towers theory - and the theory of abelian varieties.

For this, we construct finite quotients of Fried’s modular towers - we call abelianized modular towers and the arithmetic properties of which are connected with torsion on abelian varieties. As a first consequence, we show that the strong torsion conjecture for abelian varieties implies the disappearance of rational points of bounded degree along abelianized modular towers.

Our construction enables us to apply the machinery of abelian varieties to regular inverse Galois theory. For instance, given a profinite group $\tilde{G}$ extension of a finite group $G$ by a pro-$p$ group $P$ such that $P^{ab}$ is not torsion, we prove that for any number field $k$, there is no Galois extension $K$ with group $\tilde{G}$ and field of moduli $k$. Equivalently, there is no projective system of $k$-rational points on any tower of Hurwitz spaces associated with $\tilde{G}$ (and, in particular, on any modular towers). The above result can be improved by showing there is no projective system of $k^{gp}$-rational points (where $k^{gp}$ denotes the cyclotomic closure of $k$ in $\overline{Q}$) on any abelianized modular towers. In particular, the dihedral groups $D_{2n}$, $n \geq 1$ cannot be regularly realized over $\overline{Q}$ in a compatible way with only order 2 inertia groups. However, we prove this becomes true when removing the compatibility condition that is any dihedral group $D_{2n}$ can be regularly realized over $\overline{Q}$ with only order 2 inertia groups.

Conversely, using arithmetic properties of abelianized modular towers which stem from patching methods for $G$-covers, we prove that several well-known results for abelian varieties over number fields no longer hold for henselian valued field or ample fields of characteristic 0. 2000 Mathematic Subject Classification. Primary: 11G10, 14G05, 12F12; Secondary: 11S25, 14G32.

INTRODUCTION

Given a finite group $G$ and a $r$-tuple $C$ of non trivial conjugacy classes of $G$ denote by $\mathcal{H}_{G}^{rd}(C)$ the reduced Hurwitz space classifying $G$-covers of the projective line with group $G$ and inertia canonical invariant $C$ modulo the natural action of $PGL_2$. Write $D_{2n}$ for the dihedral group of order $2n$ and $I$ for the conjugacy class of non trivial involutions in $D_{2n}$. Then, according to [11, §5], the tower of Hurwitz spaces $\mathcal{H}^{rd}(p, D_{2p}, I) = (\mathcal{H}^{rd}_{D_{2p}^{n+1}}(I^{1}) \rightarrow \mathcal{H}^{rd}_{D_{2p}^{n+1}}(I^{1}))_{n \geq 0}$ is the tower of modular curves $(Y_{1}(p^{n+1}) \rightarrow Y_{1}(p^{n}))_{n \geq 0}$ classifying pairs of elliptic curves with a torsion point of order exactly $p^{n}$. This is the starting point of Fried’s theory of modular towers which [15, p.6] “generalize the tower of modular curves” in the setting of Hurwitz space theory.

In Fried’s construction, the triple $(p, D_{2p}, I)$ is replaced by a triple $(p, G, C)$ where $G$ is a perfect finite group and $C$ a $r$-tuple of non trivial $p'$-conjugacy classes. Using the universal $p$-Frattini cover of $G$, such a triple defines canonically a tower of Hurwitz spaces $\mathcal{H}^{rd}(p, G, C)$ called the modular tower associated with $(p, G, C)$.

Keeping on with our original example, consider the following problem: given an integer $r \geq 3$, can we realize all the dihedral groups $D_{2p^{n}}$ as the Galois group of an extension $K_{n}/\overline{Q}(T)$ regular over $\overline{Q}$ and with less than $r$ ramification points, $n \geq 2$? The lack of roots of unity in $\overline{Q}$ imposes that if this can be done, then the extensions $K_{n}/\overline{Q}(T)$ only have inertia groups of order 2 for $n >> 0$; these are precisely the extensions classified by the modular towers $\mathcal{H}^{rd}(p, D_{2p}, I^{2r})$, $s \geq 2$. For $s \geq 2$ ($r = 4$), Mazur-Merel’s theorem shows that the answer is no (and shows even much more, namely that, for each integer $d \geq 1$ there exists an integer $N(d) \geq 1$ such that, for $n \geq N(d)$, none of the dihedral group $D_{2n}$ can be regularly realized over a degree $\leq d$ extension of $\overline{Q}$ with only four ramification points.) For $s \geq 3$, the problem is open. Fried’s conjectures for modular towers are conjectural generalizations of Manin’s theorem and Mazur-Merel’s theorem that is, they predict the disappearance of rational points along modular towers. In terms of the regular inverse Galois problem, this is equivalent to the fact that for any integer $r \geq 3$, only finitely many of the groups encoded in a modular tower can be regularly realized over $\overline{Q}$ with less than $r$ ramification points (theorem 5.1).
To study the arithmetico-geometric properties of modular towers, we construct finite quotients of them - we call abelianized modular towers, which enables us to provide a link with what could be the generalization of the moduli problem classified by the tower of modular curves that is, abelian varieties with torsion points. In particular, we show that the strong torsion conjecture for abelian varieties implies the disappearance of rational points of bounded degree along abelianized modular towers and, in particular, Fried’s conjectures for modular towers.

This construction, combined with Galois cohomology, is the corner stone of most of the results obtained in this paper. For instance, given a profinite group \( \tilde{G} \) extension of a finite group by a pro-\( p \) \( P \) such that \( P^{ab} \) is not torsion\(^1\), we prove in section 4 that for any number field \( k \), there is no Galois extension \( K/\overline{K}(T) \) with group \( \tilde{G} \) and field of moduli \( k \) ((1) of theorem 4.7). Equivalently, there is no projective system of \( k \)-rational points on any tower of Hurwitz spaces associated with \( \tilde{G} \) (and, hence, on any modular towers). In particular, according to Faltings’ theorem, Fried’s conjecture “à la Manin” when \( r = 4 \) amounts to proving that the genus of all the geometrically irreducible components of level \( n \) of a reduced modular tower becomes larger than 2 for \( n >> 0 \). We can even improve the above result by showing there is no projective system of \( k^{cyc} \)-rational points (where \( k^{cyc} \) denotes the cyclotomic closure of \( k \) in \( \overline{Q} \)) on any abelianized modular towers ((2) of theorem 4.7). In particular, the dihedral groups \( D_{2p^n}, n \geq 1 \) cannot be regularly realized over \( \mathbb{Q}^{ab} \) in a compatible way with only order 2 inertia groups. We prove in section 5 that this becomes true when removing the compatibility condition and allowing the number of ramification points to increase (corollary 5.6).

Conversely, in section 6, using arithmetic properties of abelianized modular towers which stem from patching methods for \( G \)-covers, we prove that several results for abelian varieties over number fields no longer hold for henselian valued fields (and, in some cases, even ample fields) of characteristic 0. For instance, Manin’s theorem for the uniform boundedness of the \( p \)-part of the torsion subgroup of the group of \( k \)-rational points [26], Ribet’s theorem for the finiteness of the torsion subgroup of the group of \( k^{cyc} \)-rational torsion points [35] or Falting’s finiteness isogeny theorem [13] fail in this setting.

The paper is organized as follows. In section 1, we define modular towers and their abelianized variants. Section 2 and 3 are devoted to constructing technical tools. In section 2, we introduce the functors \( F_n, n \geq 0 \), which describe the representability properties of abelianized modular towers; this is the tool which enables us to prove arithmetical results for stacks. In section 3, we carry out the construction of a generalized cohomological obstruction for a projective system of \( G \)-covers to be (compatibly) defined over its field of moduli; this is the tool which enables us to extend our results about projective systems from stacks to coarse moduli spaces. In section 4, we prove the main arithmetic statements for general abelianized modular towers whereas, in section 5, we focus on dihedral towers, which have good representability properties and, in particular, encode the strong torsion conjecture for hyperelliptic jacobians. Section 6 is about henselian valued field of characteristic 0.

Acknowledgement

I would like to thank M. Jarden for suggesting several simplifications in the proof of theorem 4.7 and B. Poonen for telling me about Flynn’s paper [14]. The connection between regular realization of dihedral groups with only order 2 inertia groups and torsion points on hyperelliptic curves already appears in [11, §5], where, in particular, the converse of proposition 5.5 (2) is shown.

1 Modular towers and abelianized modular towers

1.1 Basic definitions and notation. Given a field \( k \) of characteristic 0, we denote its absolute Galois group by \( \Gamma_k \) and we always assume a compatible system \( (\zeta_n)_{n \geq 1} \) of primitive roots of unity is given in the algebraic closure \( \overline{k} \) of \( k \) (that is, \( \zeta_n^n = \zeta_m \), \( n, m \geq 1 \)). Also, given an integer \( n \geq 0 \), we write \( \mathbb{Z}/n \) for the trivial \( \Gamma_k \)-module and \( \mathbb{Z}/n(1) \) for the abelian group \( \mathbb{Z}/n \) on which \( \Gamma_k \) acts via the cyclotomic character (in other words, \( \mathbb{Z}/n(1) \) is the \( \Gamma_k \)-module of \( n \)th roots of unity in \( \overline{k} \)).

For any \( r \geq 3 \), let \( U^r/\mathbb{Z} \) be the fine moduli space for the stack \( U^r \) of \( r \) ordered marked points on the

\(^1\) That is \( P^{ab} \cong \text{Tors}(P^{ab}) \oplus \mathbb{Z}_p^r \) with \( r \geq 1 \). This condition is equivalent to requiring that \( P \) admits a quotient isomorphic to \( \mathbb{Z}_p \).
(fixed) projective line and let $U_r(:= U^r/S_r)/\mathbb{Z}$ be the fine moduli space for the stack $U_r$ of $r$ unordered marked points on the (fixed) projective line.

Finally, given any field $k$ and a variety $X/k$ and an integer $d$, write $X^{(d)}(k) = \bigcup_{[K:k]\leq d} X(K)$. Also, given a smooth, projective, geometrically irreducible curve $X/k$, we will denote its function field by $k(X)$; conversely, given a finite extension $E/k(T)$ regular over $k$, we will denote by $X_E/k$ a smooth, projective, geometrically irreducible model of it.

Let $X/k$ be a smooth, projective, geometrically irreducible curve and fix an algebraic closure $k(\overline{X})$ of $k(X)$. For any $\Gamma_k$-invariant finite subset $t \subset X(\overline{\mathbb{Q}})$, denote by $M_{k,X,t}/k(X)$ the maximal algebraic extension of $k(X)$ in $k(\overline{X})$ unramified outside $t$. Then $M_{k,X,t}/k(X)$ and $M_{k,X,t}/k(X)$ are Galois extensions with groups we denote by $\pi_1(X_{\overline{X}} \setminus t)$ and $\pi_1(X \setminus t)$ respectively. In particular, we have the fundamental short exact sequence from Galois theory

$$1 \longrightarrow \pi_1(X_{\overline{X}} \setminus t) \longrightarrow \pi_1(X \setminus t) \longrightarrow \Gamma_k \longrightarrow 1$$

which splits provided $X(k) \neq \emptyset$.

A $G$-cover of $X$ over $k$ is a pair $(f : Y \rightarrow X, \alpha)$ where $f : Y \rightarrow X$ is a Galois cover and $\alpha : Aut(f) \rightarrow G$ a group isomorphism. In the following, we will almost always drop the $\alpha$ in our notation though it remains part of the data. Fix a finite group $G$ and a $\Gamma_k$-invariant finite subset $t \subset X(\overline{\mathbb{Q}})$ then the function field functor defines an equivalence between the categories

- (C1) of $G$-covers of $X$ over $k$ with Galois group $G$ and ramification divisor $t$.
- (C2) of continuous group epimorphisms $\Phi : \pi_1(X \setminus t) \rightarrow G$ such that $\Phi(\pi_1(X_{\overline{X}} \setminus t)) = G$.

In the category (C1) a morphism from $(f_1, \alpha_1)$ to $(f_2, \alpha_2)$ is a morphism of covers $\nu : f_1 \rightarrow f_2$ such that $\alpha_2(ugu^{-1}) = \alpha_1(g)$, $g \in Aut(f_1)$. In the category (C2) a morphism from $\Phi_1$ to $\Phi_2$ is an inner automorphism $i_g \in Inn(G)$ such that $i_g \circ \Phi_1 = \Phi_2$.

When $X = \mathbb{P}^1_k$, by Riemann’s existence theorem, $\pi_1(\mathbb{P}^1_{\overline{k}} \setminus t)$ is the profinite completion of the group defined by the generators $\gamma_{t_1}, \ldots, \gamma_{t_r}$ with the single relation $\gamma_{t_1} \cdots \gamma_{t_r} = 1$. For each $t \in t$, the element $\gamma_t$ is a distinguished generator of the inertia group $I(\mathcal{P}_t|t)$ at some place $\mathcal{P}_t$ of $M_{k,t}$ above $t$. Let $e_t$ be the profinite order of the cyclic group $I(\mathcal{P}_t|t)$ and choose a uniformizing parameter $u_t$ of $\mathcal{P}_t$ at $t$. Then, by distinguished we meant that $\gamma_t$ is the preimage of $\zeta_{e_t}$ via the group monomorphism $I(\mathcal{P}_t|t) \rightarrow \mathbb{F}_p^\times$, $\omega \rightarrow \frac{\omega(u_t)}{t}$ mod $\mathcal{P}_t$. The action of $\Gamma_k$ on $\pi_1(\mathbb{P}^1_{\overline{k}} \setminus t)$ has the following property [40, lemma 2.8].

**Lemma 1.1.** For any $\sigma \in \Gamma_k$, $t \in t$, the element $s(\sigma)\gamma_t$ is conjugate in $\pi_1(\mathbb{P}^1_{\overline{k}} \setminus t)$ to $\gamma_{\chi(\sigma)(t)}$, where $\chi : \Gamma_k \rightarrow \hat{\mathbb{Z}}$ is the cyclotomic character of $k$.

Let $f : X \rightarrow \mathbb{P}^1_k$ be a $G$-cover over $k$ corresponding to a continuous group epimorphism $\Phi_f : \pi_1(\mathbb{P}^1_{\overline{k}} \setminus t) \rightarrow G$. Then the conjugacy class $C_t$ of $\Phi_f(\gamma_t)$ in $G$ is called the inertia canonical class of $f$ at $t \in t$ and the $r$-tuple $\mathbf{C} = (C_t)_{t \in t}$ is called the inertia canonical invariant of $f$.

Given a finite group $G$, an integer $r \geq 3$ and an $r$-tuple $\mathbf{C} = (C_1, \ldots, C_r)$ of non-trivial conjugacy classes of $G$, denote by $\mathcal{H}_G(\mathbf{C})$ the corresponding (inner) Hurwitz space that is the coarse moduli space (fine assuming $Z(G) = \{1\}$) for the (inner) Hurwitz stack $H_G(\mathbf{C})$ of $G$-covers of $\mathbb{P}^1$ with group $G$ and inertia canonical invariant $\mathbf{C}$. The projective general linear group $PGL_2$ acts naturally on $H_G(\mathbf{C})$, $\mathcal{H}_G(\mathbf{C})$; the quotient stack (resp. coarse moduli space) are called (inner) reduced Hurwitz stack (resp. reduced (inner) Hurwitz space) and denoted by $H_G^{red}(\mathbf{C})$ (resp. $\mathcal{H}_G^{red}(\mathbf{C})$). Finally, let $\mathcal{H}_G^{red}(\mathbf{C})$ be the corresponding (absolute) Hurwitz space that is the coarse moduli space for the (absolute) Hurwitz stack $H_G^{red}(\mathbf{C})$ of $G$-covers of $\mathbb{P}^1$ with Galois group isomorphic to $G$ and inertia canonical invariant $\mathbf{C}$. The forgetful functor $H_G(\mathbf{C}) \rightarrow H_G^{red}(\mathbf{C})$ gives rise to an etale Galois cover $\Lambda : \mathcal{H}_G(\mathbf{C}) \rightarrow H_G^{red}(\mathbf{C})$ with group the stabilizer of $\mathbf{C}$ (up to re-ordering) in the outer automorphism group $Out(G)$. We will freely use the general theory of Hurwitz spaces [18], [40], [41].

In particular, given a field $k$, the $k$-rational points on stacks correspond to objects defined over $k$.
whereas the $k$-rational points on coarse moduli spaces correspond objects with field of moduli $k$. We refer to section 3 for further details about fields of moduli and fields of definition of G-covers.

The construction of Hurwitz spaces being functorial in $G$, any complete projective system $((G_{n+1}, C_{n+1}) \rightarrow (G_n, C_n))_{n \geq 0}$ defines a tower of Hurwitz spaces $\mathcal{H} = (\mathcal{H}_{G_{n+1}}(C_{n+1}) \rightarrow \mathcal{H}_{G_n}(C_n))_{n \geq 0}$ corresponding to the tower of Hurwitz stacks $\mathcal{H} = (H_{G_{n+1}}(C_{n+1}) \rightarrow H_{G_n}(C_n))_{n \geq 0}$.

1.2. Construction. Fried’s modular towers are special towers of (reduced) inner Hurwitz spaces. We begin with a slightly more general construction that we specialize to Fried’s modular towers.

We start from an extension of profinite groups

$$1 \rightarrow P \rightarrow \hat{G} \xrightarrow{\phi} G \rightarrow 1$$

where $G$ is a finite group and $P$ a pro-$p$ group such that $P^{ab} = \mathbb{Z}_p^{ab} \oplus \text{Tors}(P^{ab})$ with $1 \leq p < \infty$ and $|\text{Tors}(P^{ab})| < \infty$. Then, we consider its quotient modulo the commutator subgroup of $P$

$$1 \rightarrow P \rightarrow \hat{G} \xrightarrow{\phi} G \rightarrow 1$$

$$1 \rightarrow P^{ab} \rightarrow \hat{G} \xrightarrow{\phi} G \rightarrow 1$$

The Frattini series of $P$, defined inductively by $P_0 := P, P_1 = P_0[P_0, P_0], ..., P_{n+1} = P_n[P_n, P_n]$ etc. is a fundamental system of neighborhoods of 1 in $P$ thus in $\hat{G}$ (since $P$ is closed of finite index in $\hat{G}$). As a result, writing $\hat{G}_n$ for the quotient $\hat{G}/P_n, n \geq 0$ one obtains a canonical complete projective system of finite groups of exponent $p^n (\hat{G}_{n+1} \rightarrow \hat{G}_n)_{n \geq 0}$ with $\hat{G} = \lim \hat{G}_n$.

Similarly, the Frattini series of $P^{ab}$ which is simply $(P^{ab})_n = P^n P^{ab}, n \geq 0$ is a fundamental system of neighborhoods of 1 in $P^{ab}$ thus in $\overline{G}$ and, writing $\overline{G}_n$ for the quotient $\overline{G}/p^n P^{ab}, n \geq 0$ one obtains a canonical complete projective system of finite groups $(\overline{G}_{n+1} \rightarrow \overline{G}_n)_{n \geq 0}$ with $\overline{G} = \lim \overline{G}_n$.

These two projective systems fit in a diagram of short exact sequences

$$1 \rightarrow P/P_n \rightarrow \hat{G}_n \rightarrow G \rightarrow 1$$

$$1 \rightarrow P^{ab}/p^n P^{ab} \rightarrow \overline{G}_n \rightarrow G \rightarrow 1$$

where the main point is that, considering the quotient $\hat{G}_n \rightarrow \overline{G}_n$, we replace the (in general) non abelian kernel $P/P_n$ by an abelian one $P^{ab}/p^n P^{ab}$. A direct consequence of Schur-Zassenhaus is that any non trivial $p'$-conjugacy class of $G$ lifts to a unique conjugacy class $\tilde{C}_n$ of $G_n$ (resp. $\overline{C}_n$ of $\overline{G}_n$) with the property that its elements have the same order as those of $C$.

Thus, any $r$-tuple $C = (C_1, ..., C_r)$ of non trivial $p'$-conjugacy classes of $G$ defines two canonical compatible complete projective systems of finite groups and $r$-tuples.

$$(\hat{G}_{n+1}, \hat{C}_{n+1}) \rightarrow (\hat{G}_n, \hat{C}_n), \ n \geq 0$$

$$(\overline{G}_{n+1}, \overline{C}_{n+1}) \rightarrow (\overline{G}_n, \overline{C}_n)$$

and we call the resulting towers of Hurwitz spaces

$$\mathcal{H}(\hat{\phi}, C_0) \rightarrow \mathcal{H}^{ab}(\hat{\phi}, C_0)$$

the modular tower associated with the data $(\hat{\phi}, C)$ and the abelianized modular tower associated with the data $(\hat{\phi}, C)$ respectively. We call their quotient $\mathcal{H}^{rd}(\hat{\phi}, C)$ and $\mathcal{H}^{ab, rd}(\hat{\phi}, C)$ modulo $\text{PGL}_2$ the reduced $^2$This can be shown by induction using that $p, |\text{Tors}(P^{ab})| < \infty$ to prove the finiteness and that $P$ admits a quotient isomorphic to $\mathbb{Z}_p$ to prove $G_n$ has exponent $p^n$.}
modular tower associated with the data \((\bar{\phi}, C)\) and the reduced abelianized modular tower associated with the data \((\tilde{\phi}, C)\) respectively.

**Example 1.2. (Fried’s modular towers)** Fried’s modular towers and their abelianized version are a special case of the above construction. Fix a finite group \(G\) and a prime number \(p\) dividing \(|G|\). Assume that \(G\) is \(p\)-perfect that is \(p | G\) and \(G\) admits no quotient isomorphic to \(\mathbb{Z}/p\). The extension \(\bar{\phi}\) we consider is the universal \(p\)-Frattini cover of \(G\) ([?, Chap. 22, §11-14])

\[
1 \to P \to \tilde{G} \xrightarrow{\pi} G \to 1
\]

So, according to the preceding paragraph, any \(r\)-tuple \(C = (C_1, ..., C_r)\) of non-trivial \(p\)-conjugacy classes of \(G\) canonically yields

\[
\mathcal{H}(\bar{\phi}, C) \to \mathcal{H}^{ab}(\bar{\phi}, C)
\]

that we will denote by

\[
\mathcal{H}(p, G, C) \to \mathcal{H}^{ab}(p, G, C)
\]

In general, \(\bar{\phi}\) and \(\phi\) are not well understood at all. However, when \(G\) contains only one \(p\)-Sylow (that is \(G\) can be written as a semi-direct product \(G = P \times Q\) with \(P\) a \(p\)-group and \(Q\) a \(p'\)-group), the structure of \(\bar{\phi}\) and \(\phi\) can be described explicitly theorem [?, Prop. 22.12.2]. For instance, when \(G = D_{2p}, \bar{\phi} G = \mathbb{C} = D_{2p infinite} = \mathbb{Z} \times \mathbb{Z}/2\) and \(\bar{\phi}_n = \mathbb{C} = \mathbb{Z}/p^n, n \geq 0\). In particular, when \(C\) is four copies of the conjugacy class \(I\) of involutions, the reduced modular tower \(\mathcal{T}^I(p, D_{2p}, I^I)\) is the classical tower of modular curves \((Y_1(p^n + 1) \to Y_1(p^n))_{n \geq 0}\) [11, §5].

By convention, we will always assume that \((\bar{\phi}, C)\) are chosen in such a way that \(\mathcal{H}_n(\bar{\phi}, C) \neq \emptyset, n \geq 0\). In the case of Fried’s modular towers, this is equivalent to \(\mathcal{H}_0(\bar{\phi}, C) \neq \emptyset\) because each group cover \(\tilde{G}_{n+1} \to \tilde{G}_n\) is Frattini, \(n \geq 0\).

2. The functors \(F_n, n \geq 0\)

As mentioned in example 1.2, Fried’s modular towers generalize the tower of modular curves in the setting of Hurwitz spaces theory. However, there is no longer obvious connection between Fried’s construction and a moduli problem “of the kind” represented by \((Y_1(p^n + 1) \to Y_1(p^n))_{n \geq 0}\).

The reason for introducing abelianized modular towers is to re-establish such a connection. This can be done - at the stack level - thanks to the two classical theorems below.

**Theorem 2.1.** ([37] see also [32]) Let \(k/\mathbb{Q}\) be a number field, \(X/k\) a geometrically irreducible, smooth, projective curve over \(k\) and \(f : X \to X_0\) an abelian etale cover defined over \(k\). Choose a finite extension \(k_0/k\) such that \(X_0(k_0) \neq \emptyset\). Then, for any \(P_0 \in X_0(k_0)\), one obtains a canonical embedding \(j_{P_0} : X_0, k_0 \hookrightarrow J_{X_0, k_0}\) and there exists a unique isogeny \(\alpha : A \to J_{X_0, k_0}\) such that \(j_{P_0}\) is obtained by pulling back \(\alpha\) via \(j_P\), i.e. we have a cartesian square

\[
\begin{array}{ccc}
X_0, k_0 & \xrightarrow{\alpha} & A \\
\downarrow j_{P_0} & & \downarrow \alpha \\
\downarrow f_{P_0} & & \downarrow \\
J_{X_0, k_0} & & J_{X_0, k_0}
\end{array}
\]

Furthermore \(\text{Ker}(\alpha)(\bar{k})\) is isomorphic to \(\text{Aut}(f)\) as a \(\Gamma_{k_0}\)-module. In particular, if \(f\) is a \(G\)-cover defined over \(k\) with group \(N\) then \(\text{Ker}(\alpha)(\bar{k})\) is canonically isomorphic to the trivial \(\Gamma_{k_0}\)-module \(N\).

**Theorem 2.2.** (Weil’s pairing for the kernel of isogeny [?], [?]) Let \(k\) be a field of characteristic 0 and \(\alpha : A \to B\) be a degree \(m\) isogeny. Denote by \(\alpha^\vee : B^\vee \to A^\vee\) the dual isogeny. Then there exists a non-degenerate pairing of \(\Gamma_k\)-modules

\[
e_{\alpha} : \text{Ker}(\alpha)(\bar{k}) \times \text{Ker}(\alpha^\vee)(\bar{k}) \to \mathbb{Z}/m(1).
\]

Let \(A/k\) be an abelian variety. For any integer \(n \geq 1\), we write \(A[n]\) for the kernel of the multiplication by \(n\) map \([n] : A \to A\) and for any prime \(p\), we write \(T_p(A) = \lim A[p^n](\bar{k})\) for the corresponding Tate module [?]. When \(X/k\) is a non singular geometrically irreducible projective curve, we will write \(T_p(X)\) for the Tate module of its jacobian variety \(J_X/k\).

\[\text{We can replace the } k_0\text{-rational point } P \in X_0(k_0) \text{ by a degree } 1 \text{ } k_0\text{-rational divisor } D \text{ on } X_0 \text{ which, in some cases, avoids extending the field of constants from } k \text{ to } k_0.\]
From now on, let \( 1 \to P \to \tilde{G} \xrightarrow{\delta} G \to 1 \) be a profinite group extension as in section 1.2.

2.1. **Local construction.** Fix a genus \( g \) curve \( X_0/k_0 \) together with a \( k_0 \)-rational point \( P_0 \in X_0(k_0) \) and denote by \( H_n(X_0) \) the stack of etale \( G \)-covers \( f_n : X_n \to X_0 \) with group \( P^{ab}/p^n P^{ab} \).

Also, given an integer \( n \geq 1 \), let \( T_{X_0,n}(k) \) be the the set of all \( \Gamma_k \)-module extensions \( 0 \to M \to J_{X_0,k}[p^n](\overline{k}) \xrightarrow{T_n} P^{ab}/p^n P^{ab} \to 0 \). Equivalently, by theorem 2.2, \( T_{X_0,n}(k) \) is the the set of all \( \Gamma_k \)-module monomorphisms \( T^\vee : (P^{ab}/p^n P^{ab})^\vee \hookrightarrow J_{X_0,k}[p^n](\overline{k}) \), where \( (P^{ab}/p^n P^{ab})^\vee \) is the dual \( \Gamma_k \)-module of \( P^{ab}/p^n P^{ab} \) with respect to Weil’s pairing for the isogeny \( \alpha_n \) in the diagram over \( k \)

\[
\begin{array}{c}
J_{X_0,k}/M \xrightarrow{\beta_n} J_{X_0,k} \\
\alpha_n \downarrow \quad [p^n] \\
J_{X_0,k}
\end{array}
\]

Finally, consider the natural stack morphisms \( T_{X_0,n+m}(k) \to T_{X_0,n}(k) \) sending the extension \( 0 \to M \to J_{X_0,k}[p^{n+m}](\overline{k}) \xrightarrow{T_{n+m}} P^{ab}/p^{n+m} P^{ab} \to 0 \) to the extension \( 0 \to p^n M \to J_{X_0,k}[p^n](\overline{k}) \xrightarrow{T_n} P^{ab}/p^n P^{ab} \to 0 \) where

\[
\begin{array}{ccc}
0 & \to & M \\
& \downarrow{[p^n]} & \downarrow{[p^n]} \\
0 & \to & p^n M
\end{array}
\]

or equivalently, by theorem 2.2, \( T_{X_0,n+m}(k) \) is the set of all \( \Gamma_k \)-module extensions \( 0 \to M \to J_{X_0,k}[p^n](\overline{k}) \xrightarrow{T_n} P^{ab}/p^n P^{ab} \to 0 \) where

\[
\begin{array}{c}
0 \to M \to J_{X_0,k}[p^n](\overline{k}) \\
\downarrow{[p^n]} \\
0 \to p^n M
\end{array}
\]

The uniqueness in theorem 2.1 defines stack morphisms

\[
F_n(X_0, P_0) : H_n(X_0) \to T_{X_0,n}, \quad n \geq 0
\]

such that the following diagrams commute

\[
\begin{array}{c}
H_n(X_0) \xrightarrow{\beta_n} T_{X_0,n+m} \\
\downarrow{F_{n+m}(X_0, P_0)} \\
H_n(X_0) \xrightarrow{F_n(X_0, P_0)} T_{X_0,n}
\end{array}
\]

More precisely, \( F_n(X_0, P)(k) : H_n(X_0)(k) \to T_{X_0,n}(k) \) sends the isomorphism class of \( f_n : X_n \to X_0 \) to the isomorphism class of

\[
0 \to M_n \to J_{X_0,k}[p^n](\overline{k}) \xrightarrow{T_n} P^{ab}/p^n P^{ab} \to 0
\]

where \( M_n \) is the kernel of the isogeny \( \beta_n \) in the diagram over \( k \)

\[
\begin{array}{c}
X_n \xrightarrow{\beta_n} J_X \\
\downarrow{[p^n]} \\
X_{0,k} \xrightarrow{j_0} J_{X_0,k}
\end{array}
\]

and \( T_n : P^{ab}/p^n P^{ab} \to J_{X_0,k}[p^n]/M_n \) the \( \Gamma_k \)-module isomorphism induced by the \( G \)-structure of \( f_n \).

In particular, we get a natural pro-stack functor

\[
\lim \ F_n(X_0, P_0) : \lim H_n(X_0) \to \lim T_{X_0,n}
\]

And, by definition, \( \lim T_{X_0,n}(k) \) is the set of \( \Gamma_k \)-module extensions \( 0 \to M \to T_p(X_0,k) \xrightarrow{T} \mathbb{Z}_p \to 0 \). Equivalently, \( \lim T_{X_0,n}(k) \) is the the set of all \( \Gamma_k \)-module monomorphism \( T^\vee : (\mathbb{Z}_p(1))^\vee \to T_p(X_0,k) \).
2.2. global construction. Given an abelianized stack modular tower $H_{ab}^\phi(\phi, C)$ denote by $H_{ab,pt}^\phi(\phi, C)$ the corresponding pointed abelianized stack modular tower defined as follows. For each field $k$, let $H_{0,pt}^\phi(\phi, C)(k)$ be the set of pairs $(f_0 : X_0 \to \mathbb{P}^1_k, P_0)$, where $f_0 : X_0 \to \mathbb{P}^1_k$ is a $G$-cover with invariants $G$, $C$ and $P_0$ is a ramified $k$-rational point of $f_0$. Then define $H_{n,pt}^\phi(\phi, C)$ as the fiber product

$$
H_{n,pt}^\phi(\phi, C) \to H_0^\phi(\phi, C), \quad n \geq 0.
$$

Note that the degree of the projection maps $H_{n,pt}^\phi(\phi, C)(\overline{k}) \to H_0^\phi(\phi, C)(\overline{k})$ is

$$
d(C) := |G| \sum_{1 \leq i \leq r} \frac{1}{o(C_i)}
$$

and does not depend on $n \geq 0$ (given a conjugacy class $C$ in $G$, $o(C)$ denotes the common order of the elements in $C$). In particular, for any field $k$ the maps

$$
H_{n,pt}^\phi(\phi, C)(d(C))(k) \to H_{n,pt}^\phi(\phi, C)(k), \quad n \geq 0
$$

are surjective.

Also, given an integers $g, n \geq 1$, let $T_{g,n}(k)$ be the the set of all isomorphism classes of pairs $(A/k, 0 \to M \to A[p^n](\overline{k}) \to P^{ab}/p^n P^{ab} \to 0)$, where $A/k$ is a $g$-dimensional principally polarized abelian variety defined over $k$ and $0 \to M \to A[p^n](\overline{k}) \to P^{ab}/p^n P^{ab} \to 0$ is a $\Gamma_k$-modules extension. Equivalently, by theorem 2.2, $T_{g,n}(k)$ is the the set of all isomorphism classes of pairs $(A/k, T^\nu)$ where $T^\nu : (P^{ab}/p^n P^{ab})^\nu \to X_p[p^n](\overline{k})$ is a $\Gamma_k$-module monomorphism. Finally, consider the natural stack morphisms $T_{g,n+m}(k) \to T_{g,n}(k)$ sending the isomorphism class of $(A/k, 0 \to M \to A[p^{n+m}](\overline{k}) \to T_{n+m} P^{ab}/p^{n+m} P^{ab} \to 0)$ to the isomorphism class of $(A/k, 0 \to p^n M \to A[p^n](\overline{k}) \to T_p P^{ab}/p^n P^{ab} \to 0)$ where this latter extension is defined as in diagram (1) replacing $J_{X_0, k}$ by $A$.

The uniqueness in theorem 2.1 defines stack morphisms

$$
F_n : H_{n,pt}^\phi(\phi, C) \to T_{g(C), n}, \quad n \geq 0
$$

(4)

(where, by Riemann-Hurwitz, $g(C) := \frac{1}{2}((r-2)|G|+1-\sum_{1 \leq i \leq r} \frac{1}{o(C_i)})$) such that the following diagrams commute

$$
\begin{array}{ccc}
H_{n+m}^{ab,pt}(\phi, C) & \xrightarrow{F_{n+m}} & T_{g(C), n+m} \\
| & | & | \\
H_n^{ab,pt}(\phi, C) & \xrightarrow{F_n} & T_{g(C), n}
\end{array}
$$

More precisely, $F_n(k) : H_{n,pt}^\phi(\phi, C)(k) \to T_{g(C), n}(k)$ sends the isomorphism class of $(f_n : X_n \to \mathbb{P}^1_k, P_0)$ to $F_n(X_0, P_0)(k)(f_0^n)$ where $f_0 : X_0 \to \mathbb{P}^1_k$ is the quotient of $f_n$ modulo $P^{ab}/p^n P^{ab}$ and $f_0^n : X_n \to X_0$ is the factor cover, which is etale by assumption (recall that the elements of $C_{n,i}$ and $C_i$ have the same common order, $i = 1, ..., r$).

In particular, we get a natural pro-stack functor

$$
\lim F_n : \lim H_{n,pt}^\phi(\phi, C) \to \lim T_{g(C), n}
$$

(5)

And, by definition, $T_{g(C), n}(k)$ is the set of isomorphism classes of pairs $(A/k, 0 \to M \to T_p(A)) ^T \to \mathbb{Z}_p \to 0$. Equivalently, $T_{g(C), n}(k)$ is the the set of all isomorphism classes of pairs $(A/k, T^\nu)$, where
$T^\nu : (\mathbb{Z}_p(1))^\theta \hookrightarrow T_p(A)$ is a $\Gamma_k$-module monomorphism.

**Remark 2.3.** If we denote by $H_n^{ab,pt,rd}(\tilde{\phi}, C)$ the quotient stack of $H_n^{ab,pt}(\tilde{\phi}, C)$ modulo PGL$_2$, the functor $F_n$ factors through

$$
\begin{array}{c}
H_n^{ab,pt}(\tilde{\phi}, C) \\
\downarrow F_n \\
T_g(C), n
\end{array}
\quad
\begin{array}{c}
\rightarrow \\
\leftarrow
\end{array}
\quad
\begin{array}{c}
H_n^{ab,pt,rd}(\tilde{\phi}, C) \\
T_g(C), n
\end{array}
$$

3. **Field of moduli versus field of definition: profinite generalization**

This section is devoted to the definition and construction of the cohomological tools which are required to prove step 2 of section 4.2.1 i.e. to pass from stacks to coarse moduli spaces.

3.1. **The finite obstruction.** We begin this section by recalling the notion of field of moduli and field of definition of a G-cover. Let $f : Y \rightarrow X_\mathbb{C}$ be a $\overline{\mathbb{k}}$ G-cover with a $\mathbb{k}$-rational ramification divisor $t \subset X(\overline{\mathbb{k}})$ corresponding to a continuous group epimorphism $\Phi_f : \pi_1(X_\mathbb{C} \setminus t) \twoheadrightarrow G$ then

- (fod) $k$ is a field of definition for $f$ if the two following equivalent conditions are fulfilled:
  (i) There exists a G-cover $f_k$ defined over $k$ such that $f \simeq f_k \times_k \overline{\mathbb{k}}$.
  (ii) $\Phi_f : \pi_1(X_\mathbb{C} \setminus t) \twoheadrightarrow G$ extends to a continuous group epimorphism $\Phi_{f,k} : \pi_1(X \setminus t) \twoheadrightarrow G$.

- (fom) $k$ is the field of moduli for $f$ (relatively to the extension $\overline{\mathbb{k}}/k$) if the two following equivalent conditions are fulfilled:
  (i) $k = \mathbb{k}^{M_{f,k}}$ where $M_{f,k} = \{ \sigma \in \Gamma_k \mid f \simeq \sigma f \} \subset \Gamma_k$ is the closed subgroup (of finite index) of $\Gamma_k$ fixing the isomorphism class of $f$.
  (ii) There exists a map $h_{f,k} : \Gamma_k \rightarrow G$ such that $\Phi_f(\sigma(\gamma)) \equiv h_{f,k}(\sigma) \cdot \Phi_f(\gamma) \cdot (h_{f,k}(\sigma))^{-1}$, for all $\gamma \in \pi_1(X_\mathbb{C} \setminus t)$, $\sigma \in \Gamma_k$. (Observe that the map $h_{f,k}$ depends on the section $s : \Gamma_k \hookrightarrow \pi_1(X \setminus t)$ but the notion of field of moduli does not).

Clearly (fod) implies (fom) but the converse is false in general. When $X(k) \neq \emptyset$ the fundamental exact sequence from Galois theory (cf. section 1.1) admits a group-theoretic section and, fixing a group-theoretic section $s$, one can define a cohomological obstruction $[\omega_{f,k}] \in \mathbb{H}^2(k, Z(G))$ for a G-cover $f$ with group $G$ and field of moduli $k$ to be defined over $k$ [10]. With the notation above, the map

$$
\overline{\phi}_{f,k} : \Gamma_k \rightarrow G/Z(G) \\
\sigma \rightarrow h_{f,k}(\sigma) \mod Z(G)
$$

is a well-defined group morphism, which only depends on $s$ and not on the particular representative $h_{f,k}$. Considering $Z(G)$ as a trivial $\Gamma_k$-module, the cochain

$$
\omega_{f,k} : \Gamma_k \times \Gamma_k \rightarrow Z(G) \\
(\sigma, \tau) \rightarrow h_{f,k}(\sigma \tau)^{-1} h_{f,k}(\sigma) h_{f,k}(\tau)
$$

defines a class $[\omega_{f,k}] \in \mathbb{H}^2(k, Z(G))$ which does not depend on $s$. Classically, $[\omega_{f,k}] \in \mathbb{H}^2(k, Z(G))$ is trivial in $\mathbb{H}^2(k, Z(G))$ if and only if $f$ is defined over $k$ which, in turn, is equivalent to the existence of a continuous group morphism $\phi_{f,k} : \Gamma_k \rightarrow G$ making the following diagram commute

$$
\begin{array}{cccccc}
1 & \rightarrow & Z(G) & \rightarrow & G & \rightarrow & G/Z(G) & \rightarrow & 1 \\
\downarrow & \downarrow & \overline{\phi}_{f,k} & & \downarrow & & \overline{\phi}_{f,k} \\
1 & \rightarrow & \Gamma_k & \rightarrow & G & \rightarrow & G/Z(G) & \rightarrow & 1
\end{array}
$$

(this occurs in particular if $Z(G) = \{1\}$ or if $Z(G)$ is a direct factor of $G$). We call $[\omega_{f,k}] \in \mathbb{H}^2(k, Z(G))$ the cohomological obstruction for $f$ to be defined over $k$.

The following lemma will play an essential part in the descent step of our proofs.
Lemma 3.1. Let $G$ be a finite group and $K < G$ a normal subgroup. Consider a a curve $X$ defined over $k$ and $G$-cover $f : Z \to X_{\overline{k}}$ with group $G$ and field of moduli $k$. Assume that the quotient $c_f : Y \to X_{\overline{k}}$ modulo $K$ is defined over $k$. Then the $G$-cover $f_0 : Z \to Y$ has field of moduli $k$.

Proof. The main point is that $f$ has field of moduli $k$ as $G$-cover and not only as Galois cover that is, for any $\sigma \in \Gamma_k$ there exists a cover isomorphism $f^u \sim \sigma f$ such that $u_\sigma g^{-1}u_\sigma^{-1} = \sigma g$, $g \in \text{Aut}(f)$; in particular, $u_\sigma$ induces a $G$-cover isomorphism $c_f^u \sim \sigma c_f$. Now, any $\epsilon_\sigma \in \text{Aut}(f)$ such that $\epsilon_\sigma|_Y = u_\sigma|_Y$ yields a cover isomorphism $f_0^u \sim \sigma f_0$ such that
\[
\sigma \alpha((u_\sigma \epsilon_\sigma^{-1})g(u_\sigma \epsilon_\sigma^{-1})^{-1}) = \sigma \alpha(u_\sigma (\epsilon_\sigma^{-1}g \epsilon_\sigma)u_\sigma^{-1}) = \sigma \alpha(\epsilon_\sigma^{-1} \sigma g \epsilon_\sigma) = \alpha(\epsilon_\sigma)^{-1}\alpha(g)\alpha(\epsilon_\sigma),
\]

$g \in \text{Aut}(f)$. In other words, $f_0^u \sim \sigma f_0$ is a $G$-cover isomorphism. □

3.2. The profinite obstruction. The results of this section hold for any field $k$ of characteristic 0 or any projective field $F$ of positive characteristic $\neq p$ (for instance, finite fields) and not only for number fields. It relies on a profinite generalization of the usual cohomological obstruction for $G$-covers. We first carry out the construction of this profinite cohomological obstruction and then apply it to our specific situation. We give the proof for a field $k$ of characteristic 0. Replacing $\pi_1(X_{\overline{E},\overline{k}} \backslash \mathfrak{t})$, $\pi_1(X_{E \backslash \mathfrak{t}})$ by their tame analogue $\pi_1^{\text{tame}}(X_{\overline{E},\overline{k}} \backslash \mathfrak{t})$, $\pi_1^{\text{tame}}(X_{E \backslash \mathfrak{t}})$, the proof remains unchanged for projective fields $F$ of positive characteristic $\neq p$ except for step 3.2.2, for which a specific argument should be given.

3.2.1. Notation: Let $(G_{n+1} \to G_n)_{n \geq 0}$ be a complete projective system of finite groups and $\tilde{G} := \varprojlim G_n$. For each $n \geq 0$, denote by $s_n : \tilde{G} \to G_n$ the canonical projection and by $P_n$ its kernel. Given a field $k$ of characteristic 0, let $E/k(T)$ be a finite extension regular over $k$ and carrying a $k$-rational place $t_0 \in X_E(k)$. Then any Galois extension $K/E,\overline{k}$ with group $\tilde{G}$ and field of moduli $k$ yields a projective system $(f_n : X_n \to X_{E,\overline{k}})_{n \geq 0}$ of $G$-covers $f_n$ with group $G_n$ and field of moduli $k$ and conversely. Indeed, if $K/E,\overline{k}$ has field of moduli contained in $k$ then so do the $f_n$, $n \geq 0$. Conversely, if for each $n \geq 0$, $f_n$ has field of moduli contained in $k$, for each $\sigma \in \Gamma_k$ the set of $\overline{k}$-isomorphisms $f_n \sim \sigma f_n$ being non-empty and finite, there exists a compatible choice $(\chi_{\sigma,n})_{n \geq 0}$ of $\overline{k}$-isomorphisms $\chi_{\sigma,n} : f_n \to \sigma f_n$, which implies that $K/E,\overline{k}$ also has field of moduli $k$.

For each $n \geq 0$, let $\mathfrak{t}_n \subset X_E(k)$ be the ramification divisor of $f_n$ and write $\Phi_n : \pi_1(\mathfrak{p}_n^{\overline{k}} \backslash \mathfrak{t}_n) \to G_n$ for the corresponding group epimorphism. We get the commutative diagrams

\[
\begin{array}{ccc}
\pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_{n+1}) & \xrightarrow{e_n} & \pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_n) \\
\Phi_{n+1} \downarrow & & \Phi_n \\
G_{n+1} & \xrightarrow{\Phi_n} & G_n
\end{array}
\]

where $e_n : \pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_{n+1}) \to \pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_n)$ is the canonical restriction epimorphism defined by the Galois extensions $\overline{k}E < M_{k,X_{E,\mathfrak{t}_n}} < M_{k,X_{E,\mathfrak{t}_{n+1}}}$, $n \geq 0$. Here, we re-use the notation of §1.1.

3.2.2. Projective system of splitting morphisms: Next, considering the projective system of fundamental short exact sequences

\[
\begin{array}{cccc}
1 & \to & \pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_{n+1}) & \xrightarrow{s_{\mathfrak{t}_{n+1}}} \\
\xrightarrow{e_{n+1}} & & \pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_n) & \xrightarrow{s_{\mathfrak{t}_n}} \\
1 & \to & \pi_1(X_{E,\overline{k}} \backslash \mathfrak{t}_n) & \xrightarrow{1_k} 1
\end{array}
\]
observe that one can take the splitting morphisms $s_{t_n}$ in such a way that $e_n \circ s_{t_{n+1}} = s_{t_n}$, $n \geq 0$. Indeed,

- If $k$ has characteristic 0 then set $M = \bigcup_{n \geq 0} M_{k,E,t_n}$ and choose a uniformizing parameter $\pi_0$ for $t_0 \in X(E(k))$; the Galois extension $M/E,\kappa$ can be embedded into the field of Puiseux series $\overline{k}\{\pi_{0}\}$, on which $\Gamma_\kappa$ acts naturally. This defines a splitting morphism $s : \Gamma_k \to \text{Gal}(M|E)$ and so, via the restriction $\text{Gal}(M/E) \to \pi_1(X(E \t n))$, a compatible system of splitting morphisms $(s_{t_n} : \Gamma_k \to \pi_1(X(E \t n)))_{n \geq 0}$. If $X(E(k)) \setminus (X(E(k) \cap \cup_{n \geq 0} t_n) \neq \emptyset$ (which, for instance, always occurs if $X(E) = \mathbb{P}^1_k$ and $k$ is uncountable), one can choose $t_0 \in X(E(k)) \setminus (X(E(k) \cap \cup_{n \geq 0} t_n)$, embedding then $M/\kappa(T)$ into the field of Laurent series $\overline{k}\{((\pi_{0})\}$ as usual.

- If $k$ has positive characteristic, the algebraic closure of $k(\pi_0)$ in $\kappa((\pi_{0}))$ is no longer the field of Puiseux series $\kappa\{\pi_{0}\}$. But, if we assume that $\Gamma_k$ is projective then the natural epimorphism $\text{Gal}(M/E) \to \Gamma_k$ admits a section $s : \Gamma_k \to \text{Gal}(M/E)$ and, as above, this yields, via the restriction $\text{Gal}(M/E) \to \pi_1(X(E \t n))$, a compatible system of splitting morphisms $(s_{t_n} : \Gamma_k \to \pi_1(X(E \t n)))_{n \geq 0}$.

Note also that, as a consequence of $s_{t_n} = e_n \circ s_{t_{n+1}}$, we have, for any $\gamma \in \pi_1(X(E \t n+1))$ and $\sigma \in \Gamma_k$

$$e_n(s_{t_{n+1}}(\gamma)\gamma s_{t_{n+1}}(\sigma)^{-1}) = s_{t_n}(\gamma) e_n(\gamma)s_{t_n}(\sigma)^{-1}$$

3.2.3. Projective system of cohomological obstructions: If $k$ is the field of moduli of $f_n$, $n \geq 0$ then, for any $n \geq 0$, $\sigma \in \Gamma_k$, there exists $h_n(\sigma) := h_{f_n,k}(\sigma) \in G_n$ such that

$$\Phi_n(s_{t_n}(\sigma)\gamma s_{t_n}(\sigma)^{-1}) = h_n(\sigma)\Phi_n(\gamma)h_n(\sigma)^{-1}, \ \gamma \in \pi_1(\mathbb{P}^1_k \t t_n)$$

Denote by $H_n(\sigma) \subset G_n$ the set of all such elements. It is straightforward that $(H_{n+1}(\sigma) \to H_n(\sigma))_{n \geq 0}$ is a projective system of finite sets; as they also are non empty the inverse limit $\lim_{\leftarrow} H_n(\sigma)$ is non empty. Let $h : \Gamma_k \to G$ be the map sending $\sigma$ to $h(\sigma) = (h_n(\sigma))_{n \geq 0} \in \lim_{\leftarrow} H_n(\sigma)$. Write $\phi_n : \Gamma_k \to G_n/Z(G_n)$, $\omega_n : \Gamma_k \times \Gamma_k \to Z(G_n)$ and $[\omega_n] \in H^2(k,Z(G_n))$, $n \geq 0$ for the group morphism, cochains and cohomological classes associated with $h_n : \Gamma_k \to G_n$, $n \geq 0$.

3.2.4. The profinite cohomological obstruction: Using the map $h : \Gamma_k \to G$, we can introduce

$$\overline{\phi} : \Gamma_k \to G/Z(G), \quad h(\sigma) [\text{mod } Z(G)]$$

$$\omega_n : \Gamma_k \times \Gamma_k \to Z(G), \quad (\sigma, \tau) \to h(\sigma)^{-1} h(\sigma) h(\tau)$$

As in the finite case, $[\omega_n]$ is trivial in $H^2(k,Z(G))$ if and only if the morphism $\overline{\phi} : \Gamma_k \to G/Z(G)$ can be lifted to a morphism $\phi : \Gamma_k \to G$. This is equivalent to the existence of $\Phi_{n,k} : \pi_1(X(E \t t_n)) \to G_n$$_{n \geq 0}$ such that $\Phi_{n,k}(\pi_1(X(E \t t_n))) = \Phi_n$ and the following diagrams commute$^4$

$$\begin{array}{ccc}
\pi_1(X(E \t t_{n+1})) & \xrightarrow{e_n} & \pi_1(X(E \t t_n)) \\
\Phi_{n+1,k} \downarrow & & \Phi_{n,k} \\
G_{n+1} & \xrightarrow{\Phi_{n,k}} & G_n
\end{array}$$

that is, to the existence of a projective system $(f_{n,k} : X_{n,k} \to X_{E,k})_{n \geq 0}$ of $k$-models of the $(f_n : X_n \to X_{E,k})_{n \geq 0}$ which, in turn, define a regular Galois extension $K_{E}/E$ with group $G$ such that $K_{k,E} = K$.

So we call $[\omega_n] \in H^2(k,Z(G))$ the cohomological obstruction for the projective system of $G$-covers $(f_n)_{n \geq 0}$ to be defined over $k$ (as projective system).

$^4$Given $\phi : \Gamma_k \to G$, for any $n \geq 0$, define $\Phi_{n,k} : \pi_1(X(E \t t_n)) \to G_n$ by $\Phi_{n,k}(\gamma s_{t_n}(\sigma)) = \Phi_n(\gamma) s_{t_n} \circ \phi(\sigma)$, $(\gamma \in \pi_1(\mathbb{P}^1_k \t t_n)$, $\sigma \in \Gamma_k$). Conversely, given $(\Phi_{n,k} : \pi_1(X(E \t t_n)) \to G_n)_{n \geq 0}$ define $\phi = \lim_{\leftarrow} \Phi_{n,k} \circ s_{t_n}$.


3.2.5. Concluding remark. We end this section by comparing the global cohomological obstruction $[\omega] \in H^2(k, Z(G))$ and the projective system of cohomological obstructions $(\omega_n)_{n \geq 0} \in \varprojlim H^2(k, Z(G_n))$.

Clearly, $i \circ \phi = \lim \phi_n$ where $i : G/Z(G) \hookrightarrow G_n/Z(G_n)$ is the canonical monomorphism (note that $\lim Z(G_n) = Z(G)$). Likewise, $\omega = \lim \omega_n$ and $j([\omega]) = ([\omega_n])_{n \geq 0}$ where $j : H^2(k, Z(G)) \rightarrow \lim H^2(k, Z(G_n))$ is the canonical morphism. In general $j$ is not injective and non trivial global cohomological obstructions $[\omega]$ lying in the kernel of $j$ correspond to projective systems of $\overline{k}$ $G$-covers $(f_n)_{n \geq 0}$ such that for each $n \geq 0$ the set $G_{f_n}(k)$ of all the $k$-models of $f_n$ is not empty but the projective limit $\lim G_{f_n}(k)$ is. In terms of Hurwitz spaces, if $j$ is injective then any projective system $p = \lim H_{G_n}(C_n)(k)$ with the property that each $p_n \in H_{G_n}(C_n)(k)$ can be lifted to a $k$-rational point $p'_n \in H_{G_n}(C_n)(k)$ on the stack, $n \geq 0$ can be lifted to a projective system $p^0 = \lim H_{G_n}(C_n)(k)$.

A sufficient condition for $j$ to be injective is classically given by the Mittag-Leffler property [23, III.10] for the projective system of 1-cocycles $(C^1(k, Z(G_{n+1})) \rightarrow C^1(k, Z(G_n)))_{n \geq 0}$. It holds, for instance, when one of the following three condition is fulfilled.

- $Z(G) = \{0\}$.
- The morphism $Z(G_{n+1}) \rightarrow Z(G_n)$ is an epimorphism and any morphism $\Gamma_k \rightarrow Z(G_n)$ can be lifted to a morphism $\Gamma_k \rightarrow Z(G_{n+1})$ (for instance if $k$ is of cohomological dimension $\leq 1$), $n \geq 0$.
- $k$ is $p$-closed for each prime $p$ dividing $|Z(G)|$.

3.2.6. Lifting criteria. The profinite cohomological obstruction has the same properties as the usual one, namely

**Proposition 3.2.** Let $\tilde{G}$ be a profinite group and $K/\overline{E}$ a Galois extension with group $\tilde{G}$ and field of moduli $k$. Assume furthermore that $E/k$ has a $k$-rational place. Then

(i) If there exists a closed normal subgroup $N \subset \tilde{G}$ such that $N \cap Z(\tilde{G}) = \{0\}$ and $[\tilde{G} : NZ(\tilde{G})] < \infty$ then $K/\overline{E}$ is defined over a finite extension $k_0/k$ with $[k_0 : k] \leq [\tilde{G} : NZ(\tilde{G})]$.

(ii) If $Z(\tilde{G})$ is a direct summand of $\tilde{G}$ then $K/\overline{E}$ is defined over $k$.

**Proof.** The fact $E/k$ has a $k$-rational place allows us to use the profinite cohomological obstruction constructed in the preceding paragraphs. Regard the Galois extension $K/\overline{E}$ with field of moduli $k$ and group $\tilde{G}$ as a projective system $(f_n : X_n \rightarrow X_{E,\overline{k}})_{n \geq 0}$ of $G$-covers $f_n$ with group $G_n$ and field of moduli $k$. We re-use the notation $\phi : \Gamma_k \rightarrow \tilde{G}/Z(\tilde{G})$ and $[\omega] \in H^2(k, Z(\tilde{G}))$ from the above.

(i) Denote by $\phi : \tilde{G} \rightarrow \tilde{G}/N$ the natural quotient map and consider the commutative diagram

$$
\begin{array}{cccccc}
1 & \longrightarrow & \tilde{G}/N & \longrightarrow & (\tilde{G}/N)/\phi(Z(\tilde{G})) & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & \\
1 & \longrightarrow & Z(\tilde{G}) & \longrightarrow & \tilde{G}/Z(\tilde{G}) & \longrightarrow & 1 \\
\end{array}
$$

As $N \cap Z(\tilde{G}) = \{0\}$, the restriction $\phi|_{Z(\tilde{G})} : Z(\tilde{G}) \rightarrow \phi(Z(\tilde{G}))$ is an isomorphism, so $\phi : H^2(k, Z(\tilde{G})) \rightarrow H^2(k, \phi(Z(\tilde{G})))$ is an isomorphism too and, consequently, it is enough to prove that $\tilde{\phi}(\omega)$ becomes trivial in $H^2(k, \phi(Z(\tilde{G})))$. But $\phi(\omega)$ is the cohomological obstruction for lifting $\phi \circ \phi : \Gamma_k \rightarrow (\tilde{G}/N)/\phi(Z(\tilde{G}))$ to a morphism $\Gamma_k \rightarrow \tilde{G}$, hence $[\omega]$ becomes trivial over the fixed field $k_0$ of $\text{Ker}(\phi \circ \phi)$ in $\overline{k}$ and $[k_0 : k] \leq [\tilde{G}/N : Z(\tilde{G}/N)] = [\tilde{G} : NZ(\tilde{G})]$.

(ii) If $Z(\tilde{G})$ is a direct summand of $\tilde{G}$ then $\phi : \tilde{G}/Z(\tilde{G})$ admits a continuous section $s : \tilde{G}/Z(\tilde{G}) \hookrightarrow \tilde{G}$ which, composed with $\phi$ yields a lift $s \circ \phi$ of $\phi$ to $\tilde{G}$. \(\square\)
4. Proofs of the main results for abelianized modular towers

4.1. About the modular tower conjecture. Reduced abelianized modular towers are generalization of the tower of modular curves \((Y_1(p^{n+1}) \rightarrow Y_1(p^n))_{n \geq 0}\) in the setting of Hurwitz spaces theory. So, one expects that the arithmetical properties of \((Y_1(p^{n+1}) \rightarrow Y_1(p^n))_{n \geq 0}\) remain true for general modular towers. In particular, Merel’s theorem [30], whose conjectural generalization is the modular tower conjecture.

**Conjecture 4.1.** (Modular tower conjecture) For any integer \(d \geq 1\) there exists an integer \(N := N(C, d) \geq 0\) such that \(\mathcal{H}_{n}^{ab, rd}(\tilde{\phi}, C)(d)(Q) = \emptyset, n \geq N\).

But considering the moduli problem attached to the tower of modular curves \((Y_1(p^{n+1}) \rightarrow Y_1(p^n))_{n \geq 0}\), there is also a classical modular conjectural generalization of Merel’s theorem.

**Conjecture 4.2.** (Strong torsion conjecture) For any integers \(g, d \geq 1, n \geq 1\), denote by \(A(g, d, n)\) the set of abelian varieties \(A\) such that (i) \(A\) is defined over a number field \(k\) of degree \(\leq d\) over \(Q\), (ii) \(\text{dim}(A) = g\) and (iii) \(\mathbb{Z}/n \subset A(k)\). Then there exists an integer \(N := N(g, d)\) such that \(A(g, d, n) = \emptyset, n \geq N\).

The following proposition is proved in section 4.1.1.

**Proposition 4.3.** The strong torsion conjecture implies the modular tower conjecture.

Then, in section 4.1.2, we relate the disappearance of rational point of bounded degree along an abelianized modular tower to reduction properties of the corresponding G-covers.

4.1.1. **Proof of proposition 4.3.** In [4, §3.5], the reduced and non reduced forms of conjecture 4.1 are proved to be equivalent. So, we focus here on the non reduced forms of conjecture 4.1.

Consider the natural morphisms of stacks

\[ \mathcal{H}^{ab, pt}(\tilde{\phi}, C) \to \mathcal{H}^{ab}(\tilde{\phi}, C) \to \mathcal{H}^{ab}(\tilde{\phi}, C) \]

**Lemma 4.4.** Set \(\delta(C) = d(C)|G : Z(G)||G|\). Then, for any number field \(k\), the maps \(\mathcal{H}^{ab, pt}(\tilde{\phi}, C)\delta(C)(k) \to \mathcal{H}^{ab}(\tilde{\phi}, C)(k), n \geq 0\) are surjective.

**Proof.** Let \(p_n \in \mathcal{H}^{ab}(\tilde{\phi}, C)(k)\) with \([k : Q] \leq d\) corresponding to a G-cover \(f_n : X_n \to \mathbb{P}^1_k\) with field of moduli \(k\) and invariants \(\mathcal{C}_n, \mathcal{C}_n\). Denote by \(f_0 : X_0 \to \mathbb{P}^1_k\) its quotient modulo \(P^{ab}/p^n P^{ab}\) and by \(f_0^n : X_n \to X_0\) the factor G-cover. Then, by definition of \(d(C)\), one can always find a finite extension \(k_0/k\) such that \(X_0\) carries a \(k_0\)-rational ramified point and \([k_0 : k] \leq d(C)\). So, up to replacing \(k_0\) by a finite extension of degree \(\leq [G : Z(G)]\), one can furthermore assume that \(f_0\) is defined over \(k_0\). But then, by lemma 3.1, the factor G-cover \(f_0^n : X_n \to X_0\) is a G-cover with group \(P^{ab}/p^n P^{ab}\) and field of moduli \(k_0\) hence, being abelian, it is defined over \(k_0\).

Recall from paragraph 2.2 that we have functors \(F_n(k_0) : H_n^{pl, ab}(\tilde{\phi}, C)(k_0) \to T_{g(C), n}(k_0), n \geq 0\). Hence \(H_n^{pl, ab}(\tilde{\phi}, C)(k_0) \neq \emptyset\) implies \(T_{g(C), n}(k_0) \neq \emptyset\) But, by definition, any pair \((A/k_0, 0 \to M \to A[p^n](\mathcal{K}) \mathcal{S}_{ab}/p^n P^{ab} \to 0\) in \(T_{g(C), n}(k_0)\) yields a \(g(C)\)-dimensional abelian variety \(A/M\) defined over \(k_0\) and a \(\Gamma_{k_0}\)-module monomorphism \(P^{ab}/p^n P^{ab} \hookrightarrow (A/M)[p^n]/(\mathcal{K})\). In particular, \(A/M \in \mathcal{A}(g(C), \delta(C)d, p^n)\). But, according to the strong torsion conjecture, this set is empty for \(p^n\) larger than the constant \(N(g(C), \delta(C)d)\).

4.1.2. Effective bounds and bad reduction. Theorem 6.3 ([9, Th. 4.2]) states that, contrary to the case of number fields, given a Henselian valued field \(k\) of characteristic 0, modular towers carry projective systems of \(k\)-rational points. However, at least when the residue field is finite, there are some reduction restrictions on the corresponding G-covers. Denote by \(v\) the valuation of \(k\) and by \(\kappa\) its residue field; assume that \(\kappa\) is finite and \(\text{char}(\kappa) = q \neq p\).
4.1.2.1. **The reduction argument.** Given an abelian variety $A/k$, we say that $A/k$ has potentially good reduction at $v$ if, for any finite extension $k_0/k$ over which $A$ is defined, $A$ has potentially good reduction at the place $v_0$ of $k_0$ above $v$. Given an integer $d \geq 1$, we write $\mathcal{H}^{ab}_n(\tilde{\phi}, C, v)^{(d)}$ for the subset of $\mathcal{H}^{ab}_n(\tilde{\phi}, C, v)$ corresponding to G-covers $f_n : X_n \rightarrow \mathbb{P}^1_k$ such that $J_{X_0}$ has potentially good reduction at $v$. With this notation, we have the following weak (but effective) version of the modular tower conjecture.

**Proposition 4.5.** Given an integer $d \geq 1$, there exists an explicit bound $LW := LW(p, q, d, G, C)$ such that

$$\mathcal{H}^{ab}_n(\tilde{\phi}, C, v)^{(d)} = \emptyset, \quad n \geq LW.$$

**Proof.** Let $p_n \in \mathcal{H}^{ab}_n(\tilde{\phi}, C, v)^{(d)}$ corresponding to a G-cover $f_n : X_n \rightarrow \mathbb{P}^1_k$ with field of moduli $k$ and invariants $\overline{G}_n, \overline{G}_n$. With the notation of paragraph 4.1.1. After extending $k$ to $k_0/k$ with $[k_0 : k] \leq [G : Z(G)]|G|$, we can assume that $f_n^0$ is defined over $k_0$ and $X_0(k_0) \neq \emptyset$. By assumption, $J_{X_0}$ has potentially good reduction at the place $v_0$ of $k_0$ above $v$. So, if $k_1/k_0$ denotes the extension of $k_0$ generated $J_{X_0}[15](\overline{k})$ we have $[k_1 : k_0] \leq 15^{2g(C)}$ and $J_{X_0,k_1}$ has good reduction at the place $v_1$ of $k_1$ above $v$ ([38, §2, cor. 2 (b)]).

We denote by $\mathcal{A}$ the reduction modulo $v_1$ and by $\kappa_1$ the residue field of $k_1$ at $Q_1$; in particular $|\kappa_1| = q^{n_1}$ with $m \leq d[G|Z(G)]15^{2g(C)}$. As $q \nmid p$ and $\deg(\alpha_n) = p^n$, by lemma 4.6 below, $\alpha_n$ reduces modulo $v_1$ to an isogeny $\overline{\alpha}_n : \overline{A}_n \rightarrow \overline{J}_{X_0,k_1}$ over $\kappa_1$. In particular $[\overline{J}_{X_0,k_1}(\kappa_1)] = [\overline{\alpha}_n(\kappa_1)]$. Finally, as $q \nmid p$, reduction modulo $v_1$ is injective on the $p^n$-torsion subgroup of $A_n$ thus $p^n \mid [\overline{J}_{n}(\kappa_1)]$, hence, in particular, $p^n \leq [\overline{J}_{X_0,k_1}(\kappa_1)]$. Then, according to [31, Thm. 19.1], $[\overline{J}_{X_0,k_1}(\kappa_1)] \leq m^n(1 + 2g(C) + 2^{g(C)})$, which forces $p^n \leq m^n(1 + 2g(C) + 2^{g(C)})$. So, precisely, one can take $LW(p, q, d, G, C) = \frac{1}{\ln(p)}(\ln(q) + \ln(1 + 2g(C) + 2^{g(C)}))$, with $m = d[G|Z(G)]15^{2g(C)}$. \hfill $\square$

**Lemma 4.6.** Let $k$ be a Henselian valued field of characteristic 0 and with residue field $\kappa$ of characteristic $q$. let $\alpha : A \rightarrow J$ an isogeny of abelian varieties over $k$ of degree $n$ such that $q \nmid n$ and $J$ has good reduction at $v$. Then $\alpha$ reduces modulo $v$ to an isogeny of abelian varieties $\overline{\alpha} : \overline{A} \rightarrow \overline{J}$ over $\kappa$.

**Proof.** As $\text{Ker}(\alpha) \subset A[n]$, multiplication by $n$ on $A$ factors through the isogeny $\alpha$ to give rise to an isogeny $\beta : J \rightarrow A$ such that $\beta \circ \alpha = n\text{Id}_A$. Now, let $J/\mathcal{O}_k$ and $A/\mathcal{O}_k$ be the Neron models of $J/k$ and $A/k$ over the ring of integer $\mathcal{O}_k$ of $k$. By the universal property of Neron models, $\alpha$ and $\beta$ lift uniquely to group schemes morphisms $\tilde{\alpha} : \tilde{A} \rightarrow \tilde{J}$ and $\tilde{\beta} : \tilde{J} \rightarrow \tilde{A}$ over $\mathcal{O}_k$. The uniqueness of these lifts imposes $\beta \circ \tilde{\alpha} = n\text{Id}_{\tilde{A}}$. By [38, Cor.2], $A$ has good reduction at $v$ as well so, taking the special fibre yields morphisms $\overline{\alpha} : \overline{A} \rightarrow \overline{J}$ and $\overline{\beta} : \overline{J} \rightarrow \overline{A}$ between abelian varieties over $\kappa$ such that $\overline{\beta} \circ \overline{\alpha} = n\text{Id}_{\overline{A}}$. In particular $\overline{\alpha}$ has finite kernel. Also, $J/\mathcal{O}_k$ and $A/\mathcal{O}_k$ being smooth hence flat over $\mathcal{O}_k$, we get $\text{dim}([\overline{A}]) = \text{dim}(A) = \text{dim}(J) = \text{dim}(\overline{J})$, which concludes the proof by [31, Prop. 8.1]. \hfill $\square$

4.1.2.2. **Bad reduction of G-covers.** One can deduce from proposition 4.5 several facts about the reduction properties of the objects classified by abelianized modular towers.

(1) **G-covers over henselian valued fields of characteristic 0:**

**Fact (1):** For any projective system $(p_n)_{n \geq 0} \in \lim \mathcal{H}^{ab}_n(\tilde{\phi}, C, v)(k)$, let $(f_n : X_n \rightarrow \mathbb{P}^1_k)_{n \geq 0}$ be the corresponding system of G-covers with invariants $\overline{G}_n, \overline{G}_n$ and field of moduli $k$. Then $J_{X_n}$ has bad reduction at $v$ (in the sense that it has not potentially good reduction at $v$), $n \geq 0$.

**Fact (2):** Let $p_n \in \mathcal{H}^{ab}_n(\tilde{\phi}, C, v)(k)$ corresponding to a G-cover $f_n : X_n \rightarrow \mathbb{P}^1_k$. Then $f_n$ has bad reduction at $v$ (in the sense that it has not potentially good reduction at $v$ on any finite extension $k_0/k$ over which it is defined), $n \geq LW$. (Indeed, one can show that if $f_n$ has potentially good reduction at $v$ then so does its quotient G-cover $f_0 : X_0 \rightarrow \mathbb{P}^1_k$ [21, App to Chap. 7] and,

\[ \text{Note that this bound does not depend on} \ \tilde{\phi} \ \text{but only on the level 0 data} \ (p, G, C) \ \text{and thus, is probably very coarse.} \]
hence, $J_{X_0}$).

The G-covers constructed by formal or rigid patching methods always have bad reduction at $v$. The above observation suggests that G-covers defined over $k$ and with a ramification divisor having good reduction at $v$ may be rather exceptional and, also, that they are the more likely to come from G-covers defined over $\mathbb{Q}$ since a G-cover defined over $\mathbb{Q}$ has this property over $\mathbb{Q}_l$ for all but finitely many primes $l$ (those primes $l$ where its ramification divisor $t$ has bad reduction).

(2) Bad reduction of ramification divisors: Given a G-cover $f : X \to \mathbb{P}^1_k$ defined over $k$ with group $G$ and ramification divisor $t \in \mathcal{U}_t(k)$, let $S(|G|)$ be the set of non archimedean places of $k$ with residue characteristic not dividing $|G|$. Also denote by $\text{Bad}(t)$, $\text{Bad}(f)$, $\text{Bad}(X)$ and $\text{Bad}(J_X)$ the sets of non archimedean places of $k$ where $t$, $f$, $X$ and $J_X$ have bad reduction respectively. Then

$$\text{Bad}(J_X) \subset \text{Bad}(X) \subset \text{Bad}(f) \subset \text{Bad}(t) \cup S(|G|)$$

It is a classical problem to compute effectively the places of bad reduction of a given algebraic object. For instance, if one could prove that the places of bad reduction of $J_{X_0}$ for $f_0 : X_0 \to \mathbb{P}^1_k$ corresponding to a point $p_0 \in H^0_{\text{ab}}(\check{\phi}, \mathbb{C})(\mathbb{Q})$ were uniformly bounded then, by the reduction argument, the modular tower conjecture would hold. But this, however, can never happen. Indeed, assume that $H^0_{\text{rd}}(\check{\phi}, \mathbb{C})(k)$ is not finite and that $g(C) \geq 2$. Denote by $M_g(C)$ the stack of genus $g(C)$ curves. Then the fibers of the map $H^0_{\text{rd}}(\check{\phi}, \mathbb{C})(k) \to M_g(C)(k)$ sending a G-cover $f_0 : X_0 \to \mathbb{P}^1$ to $X_0$ are either empty or finite. So there are infinitely many isomorphism classes of $X_0/k$ corresponding to G-covers $f_0 : X_0 \to \mathbb{P}^1_k$ as above. By Torelli’s theorem [32, Cor. 12.2], there are infinitely many isomorphism classes of canonically polarized jacobian varieties $J_{X_0}$. But, by [13, Th. 5], there are only finitely many isomorphism classes of principally polarized $g(C)$-dimensional abelian varieties having good reduction outside $S(|G|)$. In particular all but finitely many G-covers $f_0$ and corresponding $X_0/k$, $t$ and $J_{X_0}$ have bad reduction outside $S(|G|)$ that is at some places of $\text{Bad}(t)$. This shows in particular that for all but finitely many G-covers $f_0$ we have $\text{Bad}(t) \cap \text{Bad}(J_{X_0}) \neq \emptyset$.

4.2. Projective systems of rational points. Considering the modular tower conjecture, the case $r = 4$, $d = 1$ is the most accessible one. Indeed, when $r = 4$, reduced modular towers are towers of curves and, at least in theory, we can compute their geometrically irreducible components and genus via topological methods. Assume that (i) the genus of each geometrically irreducible component of $\mathcal{H}^{\text{ab}, \text{rd}}(\check{\phi}, \mathbb{C})(k)$ becomes greater than 2 for $n >> 0$ and (ii) for any number field $k$, $\lim_{n \to \infty} \mathcal{H}^{\text{ab}, \text{rd}}(\check{\phi}, \mathbb{C})(k) = \emptyset$. Then, by Faltings’ theorem, for any number field $k$, $\mathcal{H}^{\text{ab}, \text{rd}}(\check{\phi}, \mathbb{C})(k) = \emptyset$, $n >> 0$. Point (i) remains a technical step - even when considering simple cases - mostly because the structure of $\check{\phi}$, $\check{C}$ is still mysterious [1], [16]. As for point (ii), it was partly proved in [1, Th. 6.1] (in the non reduced non abelianized stack case for Fried’s modular towers) and [22] (in the reduced non abelianized moduli space case for Fried’s modular towers). A complete proof is obtained combining [3, Chap 5, Th. 5.2] and [4, §3.5].

As for the strong torsion conjecture [4, §3.5] shows that the reduced and non reduced forms of (ii) are equivalent. Point (ii) is a special case of the following theorem that we prove in sections 3 and 4.

**Theorem 4.7.** Let $k$ be a number field and $E/k(T)$ a finite extension regular over $k$. Let $\tilde{G}$ be a profinite extension of a finite group $G$ by a pro-$p$ group $P$ such that $P^{\text{ab}}$ is not torsion. Then

1. There is no Galois extension $K/\overline{k}.E$ with group $\tilde{G}$ and field of moduli $k$.

2. There is no unramified Galois extension $K/\overline{k}.E$ with group $\tilde{G}$ and field of moduli $k^{\text{cycl}}$ (where $k^{\text{cycl}}/k$ is the cyclotomic closure of $k$ that is, the extension obtained by adjoining all roots of unity (in a given algebraic closure $\overline{k}$ of $k$) to $k$).

Point (1) remains true if $k$ is a finite field of characteristic $\neq p$. 

In terms of Hurwitz spaces, (1) of theorem 4.7 for \( E = k(T) \) states that, for any tower of Hurwitz spaces \(( \mathcal{H}_{G_n+1}(C_{n+1}) \to \mathcal{H}_{G_n}(C_n))_{n \geq 0} \) such that \( \lim G_n \) is an extension of a finite group \( G \) by a pro-\( p \) group \( P \) such that \( P^{ab} \) is not torsion we have \( \lim \mathcal{H}_{G_n}(C_n)(k) = \emptyset \).

Similarly, (2) of theorem 4.7 for \( E = k(T) \) states that, for any reduced abelianized modular tower we have \( \lim \mathcal{H}^{ab,rd}_n(\overline{\phi}, C)(k^{cyc}) = \emptyset \).

Theorem 4.7 also emphasizes the gap between finite and profinite regular inverse Galois theory. Indeed, for any finite group \( G \) there exists a finite extension \( E/G \) regular over \( \mathbb{Q} \) such that \( G \) can be realized as the Galois group of an extension \( K/E \) regular over \( \mathbb{Q} \) [8]. Theorem 4.7 illustrates that even this much weaker version of the regular inverse Galois problem does not hold for profinite groups.

### 4.2.1. Proof of theorem 4.7

We first remark that it is enough to prove these statements when \( \bar{G} = \mathbb{Z}_p \). Indeed, the condition \( P^{ab} \) is not torsion is equivalent to the condition \( P \) admits a quotient isomorphic to \( \mathbb{Z}_p \). Assume there exists a Galois extension \( \mathbb{K}/E \) with group \( \bar{G} \) and field of moduli \( k \) (resp. \( k^{cyc} \)) and denote by \( N \) the kernel of the quotient \( P \to \mathbb{Z}_p \). Choose a finite extension \( k_0/k \) such that the \( G \)-cover \( X_{K^p} \to X_{\mathbb{K}/E} \) is defined over \( k_0 \) then, by lemma 3.1, \( K/K^p \) also has field of moduli \( k \) (resp. \( k^{cyc} \)). This yields the \( \mathbb{Z}_p \)-extension \( K^N/K^p \) with field of moduli \( k^{cyc} \) and \( X_{K^p} \) is defined over \( k_0 \).

We divide the proof into two steps.

- **Step 1**: (1) There is no Galois extension \( K/E \) regular over \( k \) with group \( \mathbb{Z}_p \).

- **Step 2**: Any \( \mathbb{Z}_p \)-Galois extension \( K/\mathbb{K} \) with field of moduli \( k \) is defined over a finite extension \( k_0/k \).

We first deal with the number field case. We make then some comments about the finite field case.

#### 4.2.1.1. The number field case

**Proof of step 1** Assume there exists a Galois extension \( F/E \) regular over \( k \) (resp. an unramified \( F/k^{cyc} \) with group \( \mathbb{Z}_p \). In terms of G-covers, this corresponds to a projective system \( (f_n : X_n \to X_E)_{n \geq 0} \) of G-covers with group \( \mathbb{Z}/p^n \) and defined over \( k \) (resp. a projective system \( (f_n : X_n \to X_{E,k^{cyc}})_{n \geq 0} \) of etale G-covers with group \( \mathbb{Z}/p^n \) and defined over \( k^{cyc} \)).

First case: \( F/E \) is unramified. It is enough to prove step 1 in case (2). Fix a finite extension \( k_0/k \) such that \( X_E(k_0) \neq \emptyset \) and choose \( P_0 \in X_E(k_0) \). Then \( f_n \) is defined over \( k_0^{cyc} \) hence over a finite extension \( k^n_0 \).

Thus, according to paragraph 2.1, \( f_n(X_E,k_0^n)(f_n) \) is a \( \Gamma_{k_n} \)-module monomorphism \( \mathbb{Z}/p^n(1) \hookrightarrow J_{X_E(k_0^n)}(k) \), which contradicts Ribet’s theorem for the finiteness of the torsion subgroup of \( J_{X_E(k_0^n)}(k) \) [35, Th. 1] when \( n > 0 \).

Second case: \( F/E \) is ramified. Let \( Q \) be a place of \( F \) which ramifies in \( F/E \). As the inertia group \( I_{F/E}(Q) \) is a non trivial open subgroup of \( \text{Gal}(F|E) \simeq \mathbb{Z}_p \), \( (\text{Gal}(F|E) : I_{F/E}(Q)) = p^n < +\infty \) and, up to replacing \( E \) by the fixed field of \( I_{F/E}(Q) \) in \( F/E \), we can assume that \( Q \) is totally ramified in \( F/E \). For all \( n \geq 0 \), denote by \( E_n/E \) the unique cyclic subextension of \( F/E \) with group \( \mathbb{Z}/p^n \) and let \( Q_n \) be a place of \( E_n \). Above \( Q_n \) we denote completion by \( \mathbb{Q}_n \). The resulting extension \( E_\mathbb{Q}_n = E_n \cdot \mathbb{Q}_n \) is cyclic with group \( \text{Gal}(E_\mathbb{Q}_n|E) \simeq \text{Gal}(E_n/E) \). By lemma 4.8 below, \( E_\mathbb{Q}_n \) contains all the \( p^n \)-th roots of unity thus so does \( E_\mathbb{Q}_n(k) = E_\mathbb{Q}_n \), which cannot occur since \( E_\mathbb{Q}_n|k \) is a finite extension.

**Lemma 4.8.** There exists \( x_n \in \mathbb{E}_n(k) \) such that \( E_\mathbb{Q}_n = E_n(x_n) \) and \( x_n^{p^n} \in \mathbb{E}_n \).

**Proof.** Indeed, let \( a_n \in \mathbb{E}_n \), \( a \in E_n \) such that \( v_{\mathbb{Q}_n}(a_n) = 1 \), \( v_{\mathbb{Q}_n}(a) = 1 \) so one can write \( a_n^{p^n} = u_n a \) with \( u_n \in \mathbb{E}_n \) such that \( v_{\mathbb{Q}_n}(u_n) = 0 \). But as the residue fields are equal \( E_\mathbb{Q}_n \) is \( E_\mathbb{Q}_n(k) = E_\mathbb{Q}_n(k) \), there exists
u ∈ \hat{E} such that \( \overline{u^n} = \overline{u^n_a} \). So, up to replacing \( u_n \) with \( u^{-1}u_n \) and \( a \) with \( ua \), we can furthermore assume that \( u^n_{n_a} = 1 \). So, applying Hensel's lemma to \( X^{\rho_n} - u_n \) produces a \( u_{0,n} \in \hat{E}_n \) such that \( u^n_{0,n} = u_n \) and setting \( x_n := u^{-1}_0a_n \) yields the announced result. □

**Proof of step 2:** Proposition 3.2 (ii) concludes the proof of theorem 4.7. Indeed, if we assume that \( K/\overline{k}.E \) is a \( Z_p \)-extension with field of moduli \( k \) then it is defined over any finite extension \( k_0/k \) such that \( E/k \) has a \( k_0 \)-rational place.

### 4.2.1.2. Comments about the finite field case.

The assumption that \( \text{char}(k) \neq p \) allows one to adapt step 1 to the finite field case. For the unrational case, observe that \( (F_{(X_0,k_0,p),n}(k_0)(j_{n,k_0}))_{n \geq 0} \) produces a \( \Gamma_{k_0} \)-module extension \( 0 \to M \to T_p(X_0) \to Z_p \to 1 \), which imposes that \( 1 \) is an eigenvalue for the Frobenius. But this contradicts Riemann's hypothesis [31, Th. 19.1].

As for the second case, just observe that \( \overline{E}(\overline{Q}) \) is a finite field of characteristic \( \neq p \) so it contains only finitely many \( p^n \)th roots of unity.

The cohomological step 2 remains unchanged.

When \( \text{char}(k) = p \), things work rather differently as shown by the following statement.

**Theorem 4.9.** Let \( G \) be a finite group with \( p \mid |G| \) and \( k \) a finite field of characteristic \( p \). Then any regular realization of \( G \) over \( k \) yields a regular realization of \( p\hat{G} \) over \( k \).

**Proof (sketch of).** Starting from a regular realization \( K_0/k(T) \) of \( G \), we construct inductively a projective system \( (K_n/k(T))_{n \geq 0} \) of regular extensions \( K_n/k(T) \) with group \( \hat{G}_n \), \( n \geq 0 \). So, assume \( K_n/k(T) \) exists, corresponding to a group epimorphism \( \phi_n : \Gamma_k(T) \to \hat{G}_n \) and observe that the canonical projection \( \hat{G}_{n+1} \to \hat{G}_n \) is a Frattini cover with elementary \( p \)-abelian kernel \( P_n/P_{n+1} \approx (\mathbb{Z}/p)^r \) for some \( r_n \geq 1 \). The corresponding embedding problem

\[
\begin{array}{cccc}
\Gamma_k(T) & \downarrow \phi_n & \to & \hat{G}_{n+1} \\
1 \longrightarrow (\mathbb{Z}/p)^{r_n} & \longrightarrow & \hat{G}_n & \longrightarrow 1
\end{array}
\]

is thus a geometric Frattini embedding problem with \( p \)-group kernel. Consequently, by [25, Th. IV.8.3], it has a solution \( \phi_{n+1} : \Gamma_k(T) \to \hat{G}_{n+1} \). And by [25, Prop. IV.5.1], any solution is a geometric proper solution. So take for \( K_{n+1} \) the fixed field of \( \text{Ker}(\phi_{n+1}) \) in \( k(T)^s \) (which is regular over \( k \)). □

### 4.2.2. Remarks.

**4.2.2.1.** Let \( k \) be a number field and \( k^{ab} \) be the maximal abelian extension of \( k \). What can one say about projective systems of \( k^{ab} \)-rational points on abelianized modular towers? Zarhin's theorem [?, Th. 1] asserts that, for a number field \( k \) and an abelian variety \( A/k \) defined over \( k \), the torsion subgroup of \( A(k^{ab}) \) is finite if and only if \( A \) has no simple factor which is of CM type over \( k \). Since \( k^{cyc} \subset k^{ab} \), the argument used to prove (2) of step 1 shows that for any \( \mathbf{p}_0 = (f_0 : X_0 \to \mathbb{P}^1_k, P_0) \in \mathcal{H}_{0}^{ab,pt}(\hat{\phi}, C)(k) \) there exists a projective system of \( k^{ab} \)-rational points on \( \mathcal{H}_{0}^{ab,pt}(\hat{\phi}, C) \) above \( \mathbf{p}_0 \) if and only if \( J_{X_0} \) has a simple factor of CM type over \( k \).

**4.2.2.2.** According to section 4.1.1, the bad reduction of the ramification divisor is an obstruction to obtain an absolute bound for the disappearance of rational points along a modular tower. However, when \( t \) is fixed, we can control the ramification in the field of moduli and, in particular, describe partially the fields of definition of projective systems of points on abelianized modular towers. This is a consequence of proposition 4.10 below.

Given a finite set \( S \) of places of \( \mathbb{Q} \), let \( \mathbb{Q}_S/\mathbb{Q} \) be the maximal algebraic extension of \( \mathbb{Q} \) unramified outside \( S \).
Proposition 4.10. Let $\tilde{G}$ be a profinite group of finite rank and such that the set $S(|\tilde{G}|)$ of prime divisors of $|\tilde{G}|$ is finite. Assume furthermore that $\tilde{G}$ satisfies one of the hypotheses of proposition 3.2. Then there exists a finite set $S$ (containing $S(|\tilde{G}|)$) of places of $\mathbb{Q}$ such that $\tilde{G}$ is the Galois group of a Galois extension $K/\mathbb{Q}_S(T)$ regular over $\mathbb{Q}_S$. If, furthermore, $\tilde{G}$ is a Frattini cover of a finite group $G$ then $\tilde{G}$ is the Galois group of a Galois extension $K/\mathbb{Q}_{S,(q)}$, where $q$ is any prime not in $S$.

Proof. Write $\tilde{G} = \varprojlim \tilde{G}_n$ as a projective limit of finite groups. As $\tilde{G}$ has finite rank, there exists a generating system $\tilde{g}_1, ..., \tilde{g}_r \in \tilde{G}$ such that $\tilde{g}_1 \cdots \tilde{g}_r = 1$. Denoting by $\tilde{C}_i$ the conjugacy class of $\tilde{g}_i$ in $\tilde{G}$ and $\tilde{C}_{n,i}$ its canonical image in $\tilde{G}_n$, one obtains a tower of non empty Hurwitz spaces $(\mathcal{H}_{\tilde{C}_{n+1}}(\mathbb{C}_{n+1}) \to \mathcal{H}_{\tilde{C}_n}(\mathbb{C}_n))_{n \geq 0}$. Now choose any $t \in \mathcal{U}_r(\mathbb{Q})$ and a projective system $(p_n)_{n \geq 0} \in \prod_{n \geq 0} \mathcal{H}_{\tilde{C}_n}(\mathbb{C}_n)(\mathbb{Q})$ above $t$. Then any $p_n$ corresponds to a $G$-cover $f_n : X_n \to \mathbb{P}^1_{\mathbb{Q}}$ with group $\tilde{G}_n$, ramification divisor $t$ and field of moduli $k_n$. But, by Beckmann’s theorem [2], the only primes which may ramify in $k := \cup_{n \geq 0} k_n$ are those from $S^0 := \operatorname{Bad}(t) \cup S(|\tilde{G}|)$. So, by proposition 3.2, there exists a finite extension $k/\mathbb{Q}_{S^0}$ such that $(p_n)_{n \geq 0}$ lifts to a projective system in $\lim \mathcal{H}_{\tilde{C}_n}(\mathbb{C}_n)(k)$. Take for $S$ the union of $S_0$ and the places which ramify in $k/\mathbb{Q}_{S^0}$.

If, furthermore, $\tilde{G}$ is a Frattini cover of a finite group $G$ then, for any $q \notin S$, $\mathbb{Q}_S(\sqrt{q})/\mathbb{Q}_S$ is a proper quadratic extension (indeed, $q$ ramifies in $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$) and $\mathbb{Q}_S/\mathbb{Q}$ being Galois, deduce from Weiausser’s theorem that $\mathbb{Q}_S(\sqrt{q})$ is Hilbertian. The end of the proof rests on [37, §10.6], which shows that if $\tilde{G}$ is a profinite group such that $[\tilde{G} : \Phi(\tilde{G})] < \infty$ then for any hibertian field $k$ and Galois extension $K/k(T)$ (i) unramified outside a finite set $S$ of places of $k(T)$ and (ii) with Galois group $\tilde{G}$, there exists infinitely many $t \in k$ such that the specialized extension $K_t/k$ is Galois with group $\tilde{G}$. $\square$

5. Diherdal towers and torsion points on hyperelliptic Jacobian

5.1. Reformulation of the Modular tower conjecture. Theorem 5.1 provides a reformulation of the modular tower conjecture for Fried’s modular and abelianized modular towers (that is in the setting of §1.2).

Theorem 5.1. The modular tower conjecture for Fried’s modular towers (resp. Fried’s abelianized modular towers) is equivalent to the following. Given two integers $d \geq 1$ and $r \geq 3$ only finitely many of the $\tilde{G}_n$ (resp. $\tilde{C}_n$) can be realized as the Galois group of an extension of $\mathbb{Q}(T)$ with field of moduli of degree $\leq d$ over $\mathbb{Q}$ and with less than $r$ branch points.

Proof. We first prove that, given a number field $k/\mathbb{Q}$, if $\mathcal{H}_n(p, G, C)(k) = \emptyset$, $n \gg 0$ (resp. $\mathcal{H}_{ab}(p, G, C)(k) = \emptyset$, $n \gg 0$) then only finitely many of the $\tilde{G}_n$ (resp. $\tilde{C}_n$) can be realized over $\mathbb{Q}(T)$ with field of moduli $k$ and less than $r$ branch points.

The case of non abelianized Fried’s modular towers was proved in [17, §4] (see also [7, Th. 2.5]). The proof in the case of Fried’s abelianized modular towers follows the same pattern but with some differences. The key point is lemma 5.2.

If infinitely many $\tilde{G}_n$ could be realized regularly over the same number field $k$ with less than $r$ branch points then there would be a projective system of tuples of non trivial conjugacy classes $(\tilde{C}_{n+1} = (\tilde{C}_{n+1,1}, ..., \tilde{C}_{n+1,r+1}) \to \tilde{C}_n = (\tilde{C}_{n,1}, ..., \tilde{C}_{n,r+1}))_{n \geq 0}$ such that $r_n \leq r$ and $\mathcal{H}_{p, C}(\tilde{C}_n)(k) \neq \emptyset$, $n \geq 0$. Up to replacing 0 by some $n \geq 0$, one can assume $r_n = r_0$ is constant. If, $\tilde{C}_{n,i}$ is a $p$’th conjugacy class, $i = 1, ..., r_0$, $n \geq 0$, the assumption that $\mathcal{H}_{ab}(p, G, C)(k) = \emptyset$, $n \gg 0$ would give a contradiction. So - up to reordering and replacing 0 by some $n \geq 0$ - assume that $p$ divide the common order of elements in $\tilde{C}_{n,i}$, $n \geq 0$. Choose $g = (g_n)_{n \geq 0} \in \lim_{n \geq 1} C_{n,i}$ then $\gamma := g^{<g_0>} \in P^{ab}$ and, by lemma 5.2, $\gamma$ is non zero.

So there exists $n \geq 0$ such that $\gamma \in p^nP^{ab} \setminus p^{n+1}P^{ab}$. Now, by lemma 1.1, $\{g\chi(\sigma)\}_{\sigma \in \Gamma_k/\operatorname{Inn}(\tilde{C}_n)} \leq r_0$, $n \geq 0$ thus $\{g\chi(\sigma)\}_{\sigma \in \Gamma_k/\operatorname{Inn}(\tilde{C}_n)} \leq r_0$ and, as well, $\{\gamma\chi(\sigma)\}_{\sigma \in \Gamma_k/\operatorname{Inn}(\tilde{G})} \leq r_0$. But an element of

---

6The statements of [17, §4] and [7, Th. 2.5] are for field of definition instead of field of moduli but, as K. Kimura noticed in his master thesis [22], their proof actually work for field of moduli.
$P^{ab}$ has at most $|G|$ conjugate in $p\overline{G}$ thus $\{|\gamma^{(\sigma)}\}_{\sigma\in\Gamma_k}\leq r_0|G|$ and this contradicts the fact that $\chi(\sigma)$ takes infinitely many values (since $k$ contains only finitely many roots of unity).

The above argument relies on the fact a number field contains only finitely many roots of unity. Hence, it can be extended to prove theorem 5.1 by lemma 5.3. □

**Lemma 5.2.** The $p$-Sylow subgroups of $p\overline{G}$ are torsion free.

**Proof.** Let $\overline{g} \in p\overline{G}$ such that $|<\overline{g}>|=p^\alpha$ for some $1 \leq \alpha < \infty$. Set $g := p\overline{\phi}(\overline{g}) \in G$ and $U(g) := p\overline{\phi}^{-1}(<g>) \subseteq p\overline{G}$. Then $U(g)$ is a closed subgroup of finite index of some $p$-Sylow $\overline{S}$ of $p\overline{G}$. As $\overline{S}$ is a free pro-$p$ group of finite rank so is $U(g)$. In particular $U(g)^{ab} \simeq \mathbb{Z}^{\text{rank}(U(g))}$ is torsion free. So, necessarily, $\overline{g} \in [U(g), U(g)]/[P,P]$. But $[U(g), U(g)]/[P,P]$ maps to $|[<g>,<g>]| = \{1\}$ in $G$ thus $[U(g), U(g)]/[P,P]$ is contained in $P^{ab}$, which is torsion free whence a contradiction. □

**Lemma 5.3.** Fix an integer $d \geq 1$ and denote by $\overline{Q}(d)/\overline{Q}$ the compositum (in a fixed algebraic closure $\overline{Q}$ of $\overline{Q}$) of all degree $\leq d$ extensions of $\overline{Q}$. Then $\overline{Q}(d)$ contains only finitely many roots of unity.

**Proof.** Consider the canonical group monomorphism induced by restrictions

$$i_d: \text{Gal}(\overline{Q}(d)|\overline{Q}) \hookrightarrow \prod_{[k:\overline{Q}] \leq d} \text{Gal}(k|\overline{Q}), \quad \sigma \mapsto (\sigma|_{k})_{[k:\overline{Q}] \leq d}.$$ 

Now, for any number field $k$ with $[k: \overline{Q}] \leq d$, $|\text{Gal}(k|\overline{Q})| \leq d!$ thus $\text{Gal}(\overline{Q}(d)|\overline{Q})$ is a $(d!)$-torsion group. Conclude using that $|\overline{Q}(\zeta_n):\overline{Q}| = \phi(n) \to +\infty$, $n \to +\infty$ where $\phi$ denotes the Euler function. □

The meaning of theorem 5.1, is that, for $r \geq 3$ and $d \geq 1$ and for $n$ large enough, the only possible realizations of the $\overline{G}_n$ (resp. $\overline{G}_n$) with less than $r$ ramification points and field of moduli of degree $\leq d$ over $\overline{Q}$ lay on modular towers. So the modular tower conjecture predicts that, in order to realize all the $\overline{G}_n$ (resp. $\overline{G}_n$), $n \geq 0$ with field of moduli of degree $\leq d$ over $\overline{Q}$, one has to make the number of ramification points increase. According to theorem 4.7, there is also no hope, even when allowing $r$ to increase, to realize all the $\overline{G}_n$ (resp. $\overline{G}_n$), $n \geq 0$ in a compatible way.

The modular tower conjecture 4.1 is about a fixed modular tower. But what if, instead, we consider an infinite family of modular towers associated with a given extension $\phi$? Conjecture 5.4 below predicts in particular that, for any prime $p$ and integer $n \geq 1$, there exists $g_{p,n} \geq 1$ such that $\mathcal{H}_n(p, D_{2p}, I^{2g_{p,n}+2})(\overline{Q}) \neq \emptyset$.

**Conjecture 5.4.** (Dihedral) Any dihedral group can be regularly realized over $\overline{Q}$ with only order 2 inertia groups.

We prove below the dihedral conjecture over $\overline{Q}^{ab}$ (corollary 5.6). The underlining result is that dihedral towers represent the functors $\overline{F}_{n,\alpha} g_{\geq 0}, g \geq 1$. This also allows us to reformulate the strong torsion conjecture for hyperelliptic jacobians in terms of arithmetic properties of dihedral towers (section 5.3).

### 5.2. Constructing dihedral G-covers with only order 2 inertia groups.

Consider an extension of finite groups $1 \to N \to G \to Q \to 1$ with abelian kernel $N$. Let $f: X \to \mathbb{P}^1_k$ be a G-cover with group $G$ such that its quotient $f^0: X \to Y$ modulo $N$ is etale. Assume furthermore that $Y(k) \neq \emptyset$. Then, according to theorem 2.1, for any $P \in Y(k)$ the G-cover $f^0$ is obtained by pulling back via $j_P: Y \leftarrow J_Y$ an isogeny $\alpha: A \to J_Y$ such that $\ker(\alpha)(\overline{K})$ is the trivial $\Gamma_k$-module $N$.

Conversely, pulling back an isogeny $\alpha: A \to J_Y$ via $j_P$ yields an abelian etale Galois cover $f^0: X \to Y$ with group isomorphic to $\ker(\alpha)(\overline{K})$ as $\Gamma_k$-module. But this cover, composed with $c: Y \to \mathbb{P}^1_k$, yields a cover $f: X \to \mathbb{P}^1_k$ which is not Galois in general.
But, in this section, we will focus on dihedral groups $D_{2n} = \mathbb{Z}/n \rtimes \mathbb{Z}/2$, for which Galois covers $f$ can be effectively constructed by the above method.

We give here a general method to construct dihedral G-covers with only order 2 inertia groups. We start with a genus $g$ hyperelliptic curve $c : X \to \mathbb{P}^1_k$ (presented here as a degree 2 cover of $\mathbb{P}^1_k$) admitting a $k$-rational Weierstrass point $P \in X(k)$. Denote by $jp : X \to J_X$ the canonical embedding defined by $P \in X(k)$ and by $i \in \text{Aut}(c)$ the hyperelliptic involution. Then, as $i(P) = P$, we obtain a commutative diagram

\[
P^1_k \xrightarrow{c} X \xrightarrow{jp} J_X \xrightarrow{-1} X \xrightarrow{jp} J_X
\]

Fix an integer $n \geq 3$ and assume there exists an isogeny $\alpha : A \to J_X$ with cyclic kernel $\text{ker}(\alpha)(\overline{k}) = \langle T \rangle$ of order exactly $n$. This yields another commutative diagram

\[
J_X \xrightarrow{\alpha} A \xrightarrow{-1} J_X \xrightarrow{\alpha} A
\]

and we can stick diagrams 6 and 7 into a whole commutative diagram:

\[
P^1_k \xrightarrow{c} X \xrightarrow{jp} J_X \xrightarrow{\alpha} A \xrightarrow{-1} J_X \xrightarrow{\alpha} A
\]

Now, let $f^0 : Y \to X$ be the cover obtained by pulling back $\alpha : A \to J_X$ via $jp$ and compose it with $c : X \to \mathbb{P}^1_k$ to obtain a degree 2n cover $f : Y \to \mathbb{P}^1_k$. Let $t : Y \to Y$ the automorphism obtained by pulling back the translation $t_T$ via $jp$. As $i(P) = P$, the pull-back of $[-1] : Q^\vee \to Q^\vee$ via $jp$ yields an involution $i^0 : Y \to Y$ lifting the hyperelliptic involution $i$. Finally, from $[-1] \circ t_T = t_T^{-1} \circ [-1]$ we get $i^0 \circ t = t^{-1} \circ i^0$ that is the automorphism group of $f$ contains the copy $\langle t \rangle \rtimes \langle i^0 \rangle$ of the dihedral group $D_{2n}$. Hence, $f$ is a Galois cover with group $D_{2n}$, inertia canonical invariant $I^{2g+2}$ and is defined over $k$ as a cover and $\text{Aut}(f)$ is isomorphic, as a $\Gamma_k$-module, to $\langle T \rangle \rtimes \langle [-1] \rangle$.

So, constructing dihedral G-covers with only order 2 inertia groups defined over $k$ amounts to constructing isogenies $\alpha : A \to J_X$ with $\text{ker}(\alpha)(\overline{k})$ isomorphic to $\mathbb{Z}/n$ as $\Gamma_k$-module. We give below two ways of constructing such isogenies.

5.2.1. **First construction.** Let $T \in J_X(\overline{k})$ of order exactly $n$; $T$ defines an isogeny $\alpha : J_X \to J_X/\langle T \rangle =: Q$ and we write $\alpha^\vee : Q^\vee \to J_X$ for its dual. Any principal polarization $\varphi : J_X \to J_X$ is a group automorphism, hence commutes with $[-1]$. So we can stick diagrams 6 and 7 into a single commutative diagram

\[
P^1_k \xrightarrow{c} X \xrightarrow{jp} J_X \xrightarrow{\varphi} J_X^\vee \xrightarrow{\alpha^\vee} Q^\vee \xrightarrow{-1} J_X \xrightarrow{\varphi} J_X^\vee \xrightarrow{\alpha^\vee} Q^\vee
\]

and we can apply our preliminary observation to the isogeny $\varphi^{-1} \circ \alpha^\vee : Q^\vee \to J_X$. Furthermore, $\text{ker}(\varphi^{-1} \circ \alpha^\vee)$ is isomorphic, as a $\Gamma_k$-module, to $\langle T^\vee \rangle \rtimes \langle [-1] \rangle$. But, from theorem 2.2 $\langle T^\vee \rangle$ is the $\Gamma_k$-module dual of $\langle T \rangle$ with respect to the Weil’s pairing for the kernels. In particular, if $\langle T \rangle$ is isomorphic to $\mathbb{Z}/n$ then $\langle T^\vee \rangle$ is isomorphic to $\mathbb{Z}/n(1)$ and, conversely, if $\langle T \rangle$ is
isomorphic to \( \mathbb{Z}/n(1) \) then \( < T^v > \) is isomorphic to \( \mathbb{Z}/n \).

Hence, we have proved:

**Proposition 5.5.**

(1) If \( J_X(\overline{k}) \) contains the trivial \( \Gamma_k \)-module \( \mathbb{Z}/n \) then there exists a \( G \)-cover \( f_n : X_n \to \mathbb{P}^1_{k(\zeta_n)} \) defined over \( k(\zeta_n) \) with group \( D_{2n} \) and inertia canonical invariant \( I^{2g+2} \).

(2) If \( J_X(\overline{k}) \) contains the \( \Gamma_k \)-module \( \mathbb{Z}/n(1) \) then there exists a \( G \)-cover \( f_n : X_n \to \mathbb{P}^1_k \) defined over \( k \) with group \( D_{2n} \) and inertia canonical invariant \( I^{2g+2} \).

**Corollary 5.6.** For any integer \( n \geq 1 \) there exists a regular realization of \( D_{2n} \) over \( \mathbb{Q}(\zeta_n) \) with only order 2 inertia groups and \( n - 1 \) ramification points if \( n \) is odd, \( n \) ramification points if \( n \) is even.

**Proof.** A special case of Flynn’s results in [14, §1] is that the jacobian of the hyperelliptic curve \( X_{1,g} \) given by \( Y^2 + Y = X^{2g+1} + X^{2g} + X^g \) admits a \( \mathbb{Q} \)-rational torsion point of order \( 2g+1 \) and the jacobian of the hyperelliptic curve \( X_{2,g} \) given by \( Y^2 + X^gY = X^{2g+1} + X^{g+1} \) admits a \( \mathbb{Q} \)-rational torsion point of order \( 2g+2 \). The corresponding degree 2 cover \( X_{1,g} \to \mathbb{P}^1 \) is defined over \( \mathbb{Q} \) and admits a \( \mathbb{Q} \)-rational ramified point (above \( \infty \) ), \( i = 1, 2 \). Taking \( g = \frac{n-1}{2} \) and \( X_{1,g} \) if \( n \) is odd, \( g = \frac{n-2}{2} \) and \( X_{2,g} \) if \( n \) is even yields the announced result. \( \square \)

**Remark 5.7.** There is no known analog of Flynn’s result replacing \( \mathbb{Z}/n \) by \( \mathbb{Z}/n(1) \) and only a few very dihedral group are regularly realized over \( \mathbb{Q} \) with only order 2 inertia groups. More precisely, we have: there exists a regular realization of \( D_{2n} \) over \( \mathbb{Q} \) with only order 2 inertia groups for \( n = 1, ..., 12, 23, 29 \) and 35. For \( n = 1, ..., 10 \) and 12, this is a consequence of Mazur’s theorem [28], [29] classifying the torsion subgroups of the group of \( \mathbb{Q} \)-rational points on an elliptic curve combined with the fact that \( \mathcal{H}^{2g}_n(1^1) \) is the modular curve \( Y_1(n) \). In that case, there are infinitely many regular realizations of \( D_{2n} \) over \( \mathbb{Q} \) with only order 2 inertia groups since the corresponding modular curves have genus 0. Then, according to [28], for \( n = 11, 7, 5, 3, 10, 23, 29, 35 \) and \( N = 23, 29, 31, 37, 41, 47, 59, 71 \) respectively, the modular curve \( X_0(N) \) classifying pairs of elliptic curves with a cyclic subgroup of order \( N \) has property (2) of proposition 5.5 with \( k = \mathbb{Q} \).

5.2.2. Second construction.

**Lemma 5.8.** Let \( A/k \) be an abelian variety defined over \( k \) and let \( p \) be a prime such that \( A[p](\overline{k}) = A[p](k^{ab}) \). Then \( A[p](\overline{k}) \) is a semi-simple \( \Gamma_k \)-module.

**Proof.** The natural Galois representation \( \rho_p : \Gamma_k \to \text{Aut}(A[p](\overline{k})) \) factors through \( \Gamma_k^{ab} \) hence its image is a commutative subgroup \( G_p \) of \( \text{Aut}(A[p](\overline{k})) \). Now, let \( W \subset A[p](\overline{k}) \) be a simple \( \Gamma_k \) submodule. By Schur’s lemma, \( \text{End}_{\Gamma_k}(W) \) is nothing but the field \( \mathbb{F}_W \) with \( p^m \) elements where \( m = \dim(\text{End}_{\Gamma_k}(W)) \) and the image \( G_{p,W} \) of \( \rho_p \) restricted to \( W \) lies in \( \mathbb{F}_W^{*} \). In particular, \( p \not| |G_{p,W}| \). As this is true for any simple \( \Gamma_k \)-submodule \( W \) of \( A[p](\overline{k}) \), we also have \( p \not| |G_{p}| \) and we can apply Maschke’s theorem. \( \square \)

Now, assume that there exists a prime \( p \) such that \( J_X[p](\overline{k}) = J_X[p](k^{ab}) \) and that there exists \( T \subset J_X(k) \) of order exactly \( p \). As \( J_X(\overline{k}) \) is a semi-simple \( \Gamma_k \)-module, one can write \( < T > \) has a complement \( M \subset J_X[p](\overline{k}) \). Then \( M \) defines an isogeny \( \alpha \) factorizing \( [p] \) on \( J_X \) as follows

\[
\begin{CD}
J_X @> [p] >> J_X \\
@VV \alpha V @VV \alpha V \\
J_X/M @> \alpha >> J_X/M
\end{CD}
\]

and such that \( \ker(\alpha) = < T > \).

If \( A/k \) is an abelian variety of CM type over \( k \) then it satisfies the hypothesis of lemma 5.8 for all prime \( p \). Hence we have proved:
Proposition 5.9. If $J_X$ is CM over $k$ and $n=p$ is a prime such that $J_X(k)$ contains the trivial $\Gamma_k$-module $\mathbb{Z}/p$ then there exists a $G$-cover $f_n : X_n \to \mathbb{P}^1_k$ defined over $k$ with group $D_{2n}$ and inertia canonical invariant $I^{2g+2}$.

The generalization of the above constructions to superelliptic curves with a rational totally ramified point is straightforward.

5.3. Representability property of dihedral towers. Note that a dihedral tower $H(p, D_{2p}, I^{2g+2})$ can be regarded as the modular tower associated to the extension

$$1 \to \mathbb{Z}_p \to D_{2p} \to D_2 \to 1$$

or to the extension

$$1 \to \mathbb{Z}_p \to D_{2p} \to \mathbb{Z}/2 \to 1$$

since $U_{2g+2} = H_{\mathbb{Z}/2}(I^{2g+2})$.

So, write $H_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2}) = U_{2g+2}$. Then the scheme $H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2})$ represents $H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2})$ and, hence, the schemes $H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2}) = H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2}) \times \mathbb{Z}/2$.

Denote by $T J H_{g,n} \subset T_{g,n}$ the substack corresponding to jacobian of hyperelliptic curves. The proof of proposition 5.5 shows the following.

Corollary 5.10. We have the following isomorphisms of projective systems of stacks:

$$(T J H_{g,n})_{n \geq 0}^{(F_{g,n})_{n \geq 0}} \simeq (H^\text{pt,rd}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2}) - H^\text{pt,rd}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2}))$$

In particular, we obtain the following refinement of paragraph 4.2.2:

Proposition 5.11. Given a number field $k$ and an integer $g \geq 1$, there exists a projective system of $k^{ab}$-rational points on $(p_{n})_{n \geq 1} \in \lim (H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2})(k^{ab}))$ above some $k$-rational point $p_{-1} \in H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2})(k)$ if and only if there exists a a genus $g$ hyperelliptic curve with a $k$-rational Weierstrass point and a simple factor of CM type over $k$.

Proof. According to section 2, $(p_{n})_{n \geq 1} \in \lim (H^\text{pt}_{\mathbb{Z}/2}(p, D_{2p}, I^{2g+2})(k^{ab}))$ gives rise to a $\Gamma_{k^{ab}}$-monomorphism $\mathbb{Z}_p = \mathbb{Z}_p(1) \hookrightarrow T_{p}(X_{-1})$ (where $f_{-1} : X_{-1} \to \mathbb{P}^1_k$ is the genus $g$ hyperelliptic curve corresponding to $p_{-1}$). Hence, according to Zarhin’s theorem [?, Th. 1], $J_{X_{-1}}$ has a simple factor which is CM over $k$.

Conversely, if we are given a genus $g$ hyperelliptic curve $f_{-1} : X_{-1} \to \mathbb{P}^1_k$ defined over $k$, having a $k$-rational Weierstrass point and such that $J_{X_{-1}}$ has a simple factor $A/k$ which is CM over $k$. Consider a $k$-isogeny $\alpha : A \times B \to J_{X_{-1}}$ and denote by $K_A$ (resp. $K_B$) the kernel of $\alpha$ composed with the canonical embedding $A \hookrightarrow A \times B$ (resp. $A \hookrightarrow A \times B$). Up to composing $\alpha$ by $[p] \times Id$, one can assume that $A[p] \subset K_A$. One can mod out $\alpha$ by $K_A[p]$ to get a $k$-isogeny $\overline{\alpha} : \overline{A} \times \overline{B} \to J_{X_{-1}}$ such that $\ker(\overline{\alpha})$ is a $p$-group of exponent at least $p$. If the exponent of $\ker(\overline{\alpha})$ is $p^n$ with $n > 1$, we mod out $\ker(\overline{\alpha})$ by its maximal subgroup of exponent $p^{n-1}$. Hence we can assume that $\ker(\overline{\alpha}) \subset \overline{A}[p]$. Finally, write $\alpha_n := \overline{\alpha} \circ ([p^n] \times Id)$, $n \geq 0$. This defines a projective system of $k$-isogenies $(\alpha_n : \overline{A} \times \overline{B} \to J_{X_{-1}})_{n \geq 0}$ with kernel $K_n \subset \overline{A}[p^n]$ of exponent $p^{n+1}$, $n \geq 0$. As $\overline{A}$ is of CM type over $k$, $\overline{A}[p^n](\overline{k})$, $n \geq 0$ and $p_{T_{p}}(\overline{A})$ are trivial $\Gamma_{k^{ab}}$-modules. In particular, one can find a projective system $T = (T_n)_{n \geq 0} \in \lim \cong K_n$ of $k^{ab}$-rational points of order exactly $p^n$, $n \geq 0$. By construction, $T \in T_{p}(\overline{A}) \setminus T_{p}(\overline{A})$ hence there exists a sub-$\mathbb{Z}_p$-module $M \subset T_{p}(\overline{A})$ such that $T_{p}(\overline{A}) =< T > \oplus M$. Setting $M_n := K_n \cap M$, $n \geq 0$ we get a projective system $(M_{n+1} \to M_n)_{n \geq 0}$ such that $K_n =< T > \oplus M_n$, $n \geq 0$ and this, in turn, defines a projective systems of $k^{ab}$-isogenies $(\overline{\alpha}_n : (\overline{A}/M_n) \times \overline{B} \to J_{X_{-1}})_{n \geq 0}$ such that $\ker(\overline{\alpha}_n)(\overline{k}) =< T >$, $n \geq 0$. □
Also, the strong torsion conjecture for hyperelliptic jacobians can be reformulated in terms of arithmetic properties of dihedral towers. Recall the etale Galois covers
\[ \Lambda_n^d : \mathcal{H}_{n, pt, rd}(p, D_{2p}, I^{2g+2}) \to \mathcal{H}_{n, pt, rd}(p, D_{2p}, I^{2g+2}), \quad n \geq -1 \]
which are defined over \( \mathbb{Q} \) with group \( \text{Out}(D_{2p^n}) = (\mathbb{Z}/p^n)\times, \quad n \geq -1 \). Let \( T\mathcal{J}_H f_{g,n} \) the stack obtained from \( T\mathcal{J}_H f_{g,n} \) by forgetting the \( \Gamma_k \)-modules isomorphism \( A[p^n]\mathbb{K}/M \to P^{ab}/p^nP^{ab} \) (in other words, \( T\mathcal{J}_H f_{g,n}(k) \) is the set of isomorphism classes of pairs \( (A/k, M) \), where \( M \subseteq A[p^n]\mathbb{K} \) is a \( \Gamma_k \)-submodule such that \( A[p^n]\mathbb{K}/M \) is isomorphic to \( P^{ab}/p^nP^{ab} \) as a \( \mathbb{Z} \)-module - but not necessarily as a \( \Gamma_k \)-module), \( n \geq 0 \). Also, denote by \( \Lambda_n : T\mathcal{J}_H f_{g,n} \to T\mathcal{J}_H f_{g,n} \) the corresponding forgetful functor, \( n \geq 0 \). Then we have the commutative diagram of stacks (where the vertical arrows are isomorphisms):
\[ \begin{array}{ccc}
H_{n, pt, rd}(p, D_{2p}, I^{2g+2}) & \xrightarrow{\Lambda_n^d} & H_{n, pt, rd}(p, D_{2p}, I^{2g+2}) \\
(T\mathcal{J}_H f_{g,n})_{n \geq 0} & \xrightarrow{\Lambda_n^d} & (T\mathcal{J}_H f_{g,n})_{n \geq 0}
\end{array} \]

Now, a genus \( g \) hyperelliptic curve \( X/k \) such that \( J_X \) contains the trivial \( \Gamma_k \)-module \( \mathbb{Z}/p^n \) is the same thing as a pair \( (J_X/k, M) \in T\mathcal{J}_H f_{g,n}(k) \) where \( J_X[p^n]\mathbb{K} \) is isomorphic to \( \mathbb{Z}/p^n(1) \) as a \( \Gamma_k \)-module. Using diagram 8, this can be translated as follows. Let \( p_n \in H_{n, pt, rd}(p, D_{2p}, I^{2g+2})(k) \) be a \( k \)-rational point and let \( p_{1,n} = (f_n, \alpha) \in \Lambda_{n}^{-1}(p_n) \). Then the bijection \( \text{Out}(D_{2p^n}) \to \Lambda_{n}^{-1}(p_n) \) sending \( u \in \text{Out}(D_{2p^n}) \) to \( (f_n, u\alpha) \in \Lambda_{n}^{-1}(p_n) \) is independent of the choice of \( p_{1,n} = (f_n, \alpha) \in \Lambda_{n}^{-1}(p_n) \). And, via this identification, the \( \Gamma_k \)-set structure of \( \Lambda_{n}^{-1}(p_n) \) endows \( \text{Out}(D_{2p^n}) \) with a \( \Gamma_k \)-module structure that we call the \( \Gamma_k \)-module structure of \( \text{Out}(D_{2p^n}) \) induced by \( p_n \).

**Proposition 5.12.** Given an integer \( g \geq 1 \) and a number field \( k \), there exists a genus \( g \) hyperelliptic curve \( X/k \) with a \( k \)-rational Weierstrass point and such that \( J_X(k) \) contains the trivial \( \Gamma_k \)-module \( \mathbb{Z}/p^n \) if and only if there exists a \( k \)-rational point \( p_n \in H_{n, pt, rd}(p, D_{2p}, I^{2g+2})(k) \) such that the \( \Gamma_k \)-module structure of \( \text{Out}(D_{2p^n}) \) induced by \( p_n \) is \( \mathbb{Z}/p^n(1) \).

In particular, given an integer \( g \geq 1 \), if for any integer \( d \geq 1 \) \( H_{n}(p, D_{2p}, I^{2g+2})(d)(\mathbb{Q}) = 0 \), \( n \geq 0 \) or \( H_{n}(p, D_{2p}, I^{2g+2})(d)(\mathbb{Q}^{ab}) = 0 \), \( n \geq 0 \) then the strong torsion conjecture holds for \( g \)-dimensional hyperelliptic jacobians.

**Remark 5.13.** Proposition 5.12 for \( g = 2 \) gives a reformulation of the strong torsion conjecture for abelian varieties of dimension \( g \) having a polarization of degree \( \delta^2 \), \( \delta \geq 1 \).

Indeed, following the notation of conjecture 4.2, denote by \( A_{k}(g,d,n) \) the subset of \( A(g,d,n) \) corresponding to polarized abelian varieties of degree \( \delta^2 \) and assume there exists an integer \( N_1 = N_1(g,d) \) such that \( A_{k}(g,d,n) = \emptyset \), \( n \geq N_1 \). Let \( L \in A_{k}(g,d,n) \) defined over a number field \( k \) and let \( p \) be a prime dividing \( \delta \). Then, according to the proof of [31, Cor. 16.10], there exists a degree \( \delta \) isogeny \( \alpha : A \to A_0 \) defined over a degree \( \leq \delta \) extension of \( k \) and such that \( A_{0} \) has a polarization of degree \( (\delta/p)^2 \). Iterating the process, there exists an integer \( d(\delta) \geq 1 \) depending only on \( \delta \) and a degree \( d(\delta) \) isogeny \( \alpha : A \to A_0 \) defined over degree \( \leq d(\delta) \) extension \( k_0 \) of \( k \) with \( A_0 \) a principally polarized abelian variety. In particular, if \( T \in A(k_0) \) is of order \( \geq nd(\delta) \) then \( \alpha(T) \in A_0(k_0) \) is of order \( \geq n \), which can’t occur if \( n \geq N_1(g,d(\delta)) \). Conclude from [20, rem. (2), p. 1678], which states that the strong torsion conjecture for 2-dimensional principally polarized abelian varieties is equivalent to the strong torsion conjecture for Jacobian varieties of genus 2 curves.\footnote{Note that, by Zarhin’s trick, the strong torsion conjecture for principally polarized abelian varieties of dimension \( \leq 8g \) implies the strong torsion conjecture for abelian varieties of dimension \( \leq g \)}

6. **Abelian varieties over henselian valued fields.**

We explain here how arithmetic properties of abelianized modular towers yields results about abelian varieties over henselian valued fields of characteristic 0. For this, we combine theorem 2.2 with formal or rigid patching methods for covers [19], [24], [33], [34].

Let \( k \) be a number field and consider the following statements:
(a) \( \lim_{n \to \infty} \mathcal{H}_n(\bar{\phi}, \mathbb{C})(k) = \emptyset \) and \( (a)^{cyc} \lim_{n \to \infty} \mathcal{H}_n(\bar{\phi}, \mathbb{C})(k^{cyc}) = \emptyset \),

(b) \( \mathcal{H}_n(\bar{\phi}, \mathbb{C})(k)(k) = \emptyset, n >> 0 \),

(c) (torsion part of Mordell-Weil theorem) for any abelian variety \( A/k \), \( A(k)_{tors} \) is finite and

\( (c)^{cyc} \) (Ribet’s theorem) for any abelian variety \( A/k \), \( A(k^{cyc})_{tors} \) is finite,

(d) (Faltings’ isogeny theorem) For any abelian variety \( A/k \), the \( k \)-isogeny class of \( A \) contains only finitely many \( k \)-isomorphism classes of abelian varieties.

Then (c) and (d) imply (a)\(^8\) and \( (c)^{cyc} \) implies \( (a)^{cyc} \) (cf. the proof of theorem 4.7 (2)). If we replace the number field \( k \) by a henselian valued field of characteristic 0, statements (a) (hence \( (a)^{cyc} \)) and (b) are no longer true (theorem 6.3 and proposition 6.1 respectively) but statement (c) still holds (this is Mattuck’s theorem [27]). However, the proofs of (c) and (d) imply (a) and \( (c)^{cyc} \) implies \( (a)^{cyc} \) remain unchanged when the number field \( k \) is replaced by a henselian valued field of characteristic 0. So we deduce that statement \( (c)^{cyc} \) and (d) no longer holds for henselian valued field of characteristic 0 (proposition 6.4).

A first application of patching methods is a generalized version of Cassels’ result [6, Lemma 17.1] - which states that, for any \( p \)-adic field \( k \) and integer \( n \geq 1 \) there exists an elliptic curve \( E_n/k \) defined over \( k \) such that \( E(k) \) contains the trivial \( \Gamma_k \)-module \( \mathbb{Z}/n \). Cassels’ argument rests on Tate’s \( p \)-adic uniformization for elliptic curves over \( p \)-adic fields (cf. [?, Chap. V] for a survey of Tate’s \( p \)-adic uniformization over \( p \)-adic fields and [36] for the general statements over complete valued fields). Our method extends Cassels’ result to jacobian of hyperelliptic curves and ample field of characteristic 0.

A field \( k \) is said to be amped if for any smooth geometrically irreducible curve \( X \) defined over \( k \), the set \( X(k) \) is infinite provided it is non empty. By [34, Prop. 1.1] a field \( k \) is ample if and only if it is existentially closed in its formal Laurent series field \( k((X)) \).

Typical examples of ample fields are P.A.C. fields, henselian valued fields, fields of totally \( S \)-adic numbers \( k^{S} \) [34, App. 1] (recall that if \( k/\mathbb{Q} \) is a number field and \( S \) a finite set of place of \( k \) then \( k^{S} \subset \mathcal{O} \) is the maximal extension of \( k \) in \( \mathcal{O} \) which is totally split at each place of \( S \)).

**Proposition 6.1.** Let \( k \) be an ample field of characteristic 0. Then, for any integers \( g, n \geq 1 \) there exists a \( g \)-dimensional abelian variety \( A_{g,n} \) \( k \)-isogenous to the jacobian variety of a genus \( g \) hyperelliptic curve and such that \( A_{g,n}(k)_{tors} \) contains the trivial \( \Gamma_k \)-module \( \mathbb{Z}/n \).

**Proof.** Assume first that \( k \) is a henselian valued field of characteristic 0 and let \( k_0 \subset k \) be a dense subfield. For \( i = 1, ..., g+1 \), choose a G-covers \( f_i : X_i \to \mathbb{P}_k^1 \) defined over \( \mathbb{Q} \) with group \( \mathbb{Z}/2 \), a degree 2 ramification divisor \( t_i = \{ t_{i,1}, t_{i,2} \} \) and a totally \( \mathbb{Q} \)-rational unramified fiber. Then, according to [12, lemma 2.3.1], one can patch \( f_1, ..., f_{g+1} \) into a G-cover \( f : X_n \to \mathbb{P}_k^1 \) defined over \( k \), with group \( D_{2n} \), inertia canonical invariant \( I^{2g+2} \), a \( k_0 \)-rational ramification divisor \( t \in U_{2g+2}(k_0) \) and a totally \( k \)-rational unramified fiber. In particular, the quotient \( X_0 \) of \( X_n \) modulo \( \mathbb{Z}/n \) carries a \( k \)-rational point \( P_n \) and, by construction, \( X_0 \) is a genus \( g \)-hyperelliptic curve. By theorem 2.1, \( f_0 \) is obtained by pulling back via the embedding \( j_{P_n} : X_0 \to J_{X_0} \) an isogeny \( \alpha_n : A_n \to J_{X_0} \) defined over \( k \) and the kernel of which is isomorphic to \( \mathbb{Z}/n \) as a \( \Gamma_k \)-module. Thus \( A_n \) works.

Now, let \( k \) be an ample field of characteristic 0 and apply the above to construct a G-cover \( f : X_n \to \mathbb{P}_k^1 \) defined over \( k((X)) \), with group \( D_{2n} \), inertia canonical invariant \( I^{2g+2} \) and a totally \( k((X)) \)-rational unramified fiber. By the specialization argument of [8, §4.2], this G-cover specializes to a G-cover \( f : X_n \to \mathbb{P}_k^1 \) defined over \( k \), with group \( D_{2n} \), inertia canonical invariant \( I^{2g+2} \)

\(^8\)Indeed, there exists a finite extension \( k_0/k \) such that (a) produces a family of abelian varieties \( A_n/k_0 \) all isogenous over \( k_0 \) and such that \( A_n(\overline{k}) \) contains the trivial \( \Gamma_{k_0} \)-module \( \mathbb{Z}/p^n \), \( n \geq 0 \). Now, according to (d), there exists infinitely many \( n \geq 0 \) such that the corresponding \( A_n \) are all isomorphic over \( k_0 \). But this contradicts (c).
and a totally $k$-rational unramified fiber. So we can conclude as above. □

**Remark 6.2.** (1) When $g = 1$ and $k$ is a complete non archimedean valued field of characteristic 0, the $G$-covers we construct in the proof of proposition 6.1 correspond to Tate’s curves. Indeed, to patch the two $G$-covers $f_1 : X_1 \to \mathbb{P}^1_k$ defined over $k$ and with ramification divisors $t_i = \{ t_{1i}, \ldots, t_{ri} \}$, $i = 1, 2$, the following technical conditions must be fulfilled (*) $| t_{11} - t_{21} |$, $| t_{12} - t_{22} | < | t_{11} - t_{12} |$ (where $p$ denotes the residue characteristic of $k$). But, this forces $| \lambda | = \frac{| t_{21} - t_{11} | | t_{22} - t_{12} |}{| t_{12} - t_{11} |} > p^{\frac{1}{2n}}$. Hence $| j | = \frac{\lambda^2}{\lambda^2 - \lambda + 1} | 1 | > 1$. Theorem 6.3. (2) Actually, for $g = 1$, we could have used directly Tate’s curves to prove proposition 6.1 for ample fields of characteristic 0 (hence, in particular, henselian valued fields of characteristic 0). Indeed, let $k$ be such a field and fix $q_0 \in k((X))^*$ such that $0 < | q_0 | < 1$, and let $E_n/k(X)$ be the Tate curve parametrized by $k((X))^*/q_0^n$, where $q_n = q_0^n$, $n \geq 0$. Then $q_0^n$ is a totally ramified fiber. In particular, if $f_0 : X_0 \to \mathbb{P}^1_k$ denotes as usual the quotient of $f_0$ modulo $\mathbb{Z}/p^n$, we have $X_0(k) \neq \emptyset$. So theorem 2.1 yields a corresponding projective system of isogenies $(\alpha_n : A_{n,g} \to J_{X_0})_{n \geq 0}$ defined over $k$ such that $ker(\alpha_n(\overline{F}))$ is isomorphic to $\mathbb{Z}/p^n$ as a $\Gamma_k$-module, $n \geq 0$. According to theorem 2.2 (point (1)) and Mattuck’s theorem (point (2)) we have proved:

**Theorem 6.3.** [9, Th. 4.2] Let $k$ be an henselian valued field of characteristic $0$ and residue characteristic $q \geq 0$. Then

$$\lim_{n \to \infty} H_n(\tilde{\phi}, C)(k) \neq \emptyset.$$ 

Furthermore, if $k_0 \subset k$ is a dense subfield of $k$ and if $\tilde{k}_0$ is the algebraic closure of $k_0$ in $k$ then

$$\lim_{n \to \infty} H_n(\tilde{\phi}, C)(\tilde{k}_0) \neq \emptyset.$$ 

- one can always construct $(p_n)_{n \geq 0} \in \lim_{n \to \infty} H_n(\tilde{\phi}, C)(\tilde{k}_0)$ such that the corresponding $G$-covers $(f_n : X_n \to \mathbb{P}^1_{\tilde{k}_0})_{n \geq 0}$ have a totally $k$-rational unramified fiber.

Applying this theorem to $\mathbb{D}^{ab}(p, D_{2p}, I^{2g+2})$, we obtain projective systems $(f_n : X_n \to \mathbb{P}^1_{k_0})_{n \geq 1}$ of $G$-covers defined over $\tilde{k}_0$, with group $D_{2n}$, inertia canonical invariant $I^{2g+2}$ and a totally $k$-rational unramified fiber. In particular, if $f_0 : X_0 \to \mathbb{P}^1_{k_0}$ denotes as usual the quotient of $f_0$ modulo $\mathbb{Z}/p^n$, we have $X_0(k) \neq \emptyset$. So theorem 2.1 yields a corresponding projective system of isogenies $(\alpha_n : A_{n,g} \to J_{X_0})_{n \geq 0}$ defined over $k$ such that $ker(\alpha_n(\overline{F}))$ is isomorphic to $\mathbb{Z}/p^n$ as a $\Gamma_k$-module, $n \geq 0$. According to theorem 2.2 (point (1)) and Mattuck’s theorem (point (2)) we have proved:

**Proposition 6.4.** Let $k$ be an henselian valued field of characteristic 0 and $g \geq 2$ an integer then there exists a genus $g$ hyperelliptic curve $X/k$ such that

(1) $J_X(k^{qc})_{tors}$ is infinite.

(2) the $k$-isogeny class of $J_X$ contains infinitely many $k$-isomorphism classes of abelian varieties. Furthermore, if $k_0 \subset k$ is a dense subfield of $k$ then $X/k$ (hence $J_X$) can be defined over a finite extension of $k_0$ in $k$.

**Remark 6.5.** Once again, when $k$ is complete non archimedean valued field of characteristic 0, we could have used directly Tate’s uniformization to construct projective systems of $k$-rational points on $(Y_1(p^{n+1}) \to Y_1(p^n))_{n \geq 1}$. For this, choose $q_0 \in k^*$ such that $0 < | q_0 | < 1$, and let $E_n/k$ be the Tate curve parametrized by $k/q_0^n$, where $q_n = q_0^n$ and by $T_n \in E_n(k)$ the $k$-rational torsion point of order $p^n$ corresponding to $\mathbb{Q}mod q_n^\mathbb{Z} \in k^*/q_0^n$, $n \geq 0$. Then the analytic group epimorphism $k/q_0^n \to k/q_0^n$, $q_0 mod q_0^n \to q_0 mod q_0^n$ sends the $p^{n+1}$-torsion point $q_0 mod q_0^{n+1}$ to the $p^n$-torsion point $q_0 mod q_0^n \in k^*/q_0^n$. So it induces a $k$-isogeny $(E_{n+1}, T_{n+1}) \to (E_n, T_n)$ as expected.

**References**


