Chapter 1
Note on the gonality of abstract modular curves

Anna Cadoret

Abstract Let S be a curve over an algebraically closed field k of characteristic $p \geq 0$. To any family of representations $\rho = (\rho_\ell : \pi_1(S) \to \mathrm{GL}_n(\mathbb{F}_\ell))$ indexed by primes $\ell \gg 0$ one can associate *abstract modular curves* $S_{\rho,1}(\ell)$ and $S_\rho(\ell)$ which, in this setting, are the modular analogues of the classical modular curves $Y_1(\ell)$ and $Y(\ell)$. The main result of this paper is that, under some technical assumptions, the gonality of $S_\rho(\ell)$ goes to $+\infty$ with ℓ. These technical assumptions are satisfied by $\mathbb{F}_\ell$-linear representations arising from the action of $\pi_1(S)$ on the étale cohomology groups with coefficients in $\mathbb{F}_\ell$ of the geometric generic fiber of a smooth proper scheme over S. From this, we deduce a new and purely algebraic proof of the fact that the gonality of $Y_1(\ell)$, for $p \not| \ell(\ell^2-1)$, goes to $+\infty$ with ℓ.

Key words: 2010 MSC Primary: 14H30, 14K99; Secondary: 14K10.

1.1 Introduction

Let k be an algebraically closed field of characteristic $p \geq 0$ and S a smooth, separated and connected curve over k with generic point η. Let $\pi_1(S)$ denote its étale fundamental group. Fix an integer $n \geq 1$. For each prime $\ell \gg 0$, let H_ℓ be an $\mathbb{F}_\ell$ vector space of dimension n on which $\pi_1(S)$ acts continuously. We will write ρ for the family of the resulting $\mathbb{F}_\ell$-linear representations

$$\rho_\ell \ : \ \pi_1(S) \to \mathrm{GL}(H_\ell) \simeq \mathrm{GL}_n(\mathbb{F}_\ell).$$

To such data, one can associate families of *abstract modular curves* $S_{\rho,1}(\ell) \to S$ and $S_\rho(\ell) \to S$, see Section 1.2, which, in this setting, are the modular analogues

Anna Cadoret
Université Bordeaux 1, 351 Cours de la Libération, F 33405 TALENCE Cedex FRANCE e-mail: anna.cadoret@math.u-bordeaux1.fr

of the classical modular curves $Y_1(\ell) \to Y(0)$ and $Y(\ell) \to Y(0)$ classifying ℓ-torsion points and full level-ℓ structures of elliptic curves respectively.

The main examples of such representations we have in mind are the $\mathbb{F}_\ell$-linear representations arising from the action of $\pi_1(S)$ on the étale cohomology groups with coefficients in $\mathbb{F}_\ell$ of the geometric generic fiber of a smooth proper scheme over S. In particular, this includes those representations arising from the action of $\pi_1(S)$ on the group of ℓ-torsion points of the geometric generic fiber of an abelian scheme over S, see Subsection 1.2.3.

The properties satisfied by these representations motivated, in [CT10b], the introduction of technical conditions on ρ, denoted by (A), (WA) and (AWA) for *abelianization*, *weak abelianization* and *alternating weak abelianization* respectively, (I) for *isotriviality*, (T) for *tame* and (U) for *unipotent*. See Subsection 1.2.2 for a precise formulation of these conditions.

Let $g_{\rho,1}(\ell)$ and $g_\rho(\ell)$ (resp. $\gamma_{\rho,1}(\ell)$ and $\gamma_\rho(\ell)$) denote the genus (resp. the k-gonality) of the abstract modular curves $S_{\rho,1}(\ell)$ and $S_\rho(\ell)$ respectively. The main result of [CT10b] ([CT10b, Thm. 2.1]) asserts that, if conditions (AWA), (I), (U) are satisfied then:

$$\lim_{\ell \to +\infty} g_{\rho,1}(\ell) = +\infty.$$

An intermediate step in the proof of this result is that, if conditions (WA), (I), (T) are satisfied then:

$$\lim_{\ell \to +\infty} g_\rho(\ell) = +\infty.$$

In this note, we prove that the same holds with gonality replacing genus, that is:

Theorem 1. *If conditions (WA), (I), (T) are satisfied then:*

$$\lim_{\ell \to +\infty} \gamma_\rho(\ell) = +\infty.$$

The proof of Theorem 1 is purely algebraic and based on the equivariant-primitive decompositions introduced by A. Tamagawa in [T04] to estimate the gonality of Galois covers. The method, however, fails to prove:

Conjecture 2. Assume that conditions (WA), (T), (U) are satisfied. Then:

$$\lim_{\ell \to +\infty} \gamma_{\rho,1}(\ell) = +\infty.$$

Our method shows Conjecture 2 only when we restrict to $n = 2$ and primes ℓ with $p \not| \ell(\ell^2 - 1)$, or, more generally, for the variant of $S_{\rho,1}(\ell)$ classifying points $v \in H_\ell$ whose $\pi_1(S)$-orbit generates a subspace of rank 2, see Proposition 14. This provides in particular an algebraic proof of the well-known fact, cf. [A96], [P07], that:

Corollary 3.

$$\lim_{\substack{\ell \to +\infty \\ p | \ell(\ell^2-1)}} \gamma_{Y_1(\ell)} = +\infty.$$

When $p = 0$, it seems that variants of Theorem 1 can be proved by the techniques from differential geometry and Cayley-Schreier graph theory generalizing [A96] and developed in [EHK10].

Apart from their intrinsic geometric interest, statements as Theorem 1 and Conjecture 2 also have arithmetic consequences. In characteristic 0, this follows from the following corollary of [F91].

Corollary 4. *[Fr94]) Let k be a finitely generated field of characteristic 0 and let S be a smooth, proper, geometrically connected curve over k with k-gonality γ. Then, for any integer $1 \leq d \leq \left[\frac{\gamma-1}{2}\right]$, the set of all closed points s of S with residue field $k(s)$ of degree $[k(s) : k] \leq d$ is finite.*

So, for instance, Conjecture 2 for $p = 0$ combined with [CT10a, Prop. 3.18], to rule out the $\bar{k}$-isotrivial torsion points of $A_{\overline{\eta}}$, would imply:

For any finitely generated field k of characteristic 0, smooth, separated and geometrically connected curve S over k, abelian scheme $A \to S$ and integer $d \geq 1$ the set of closed points s of S with degree $[k(s) : k] \leq d$ and such that A_s carries a $k(s)$-rational torsion point of order ℓ is finite for $\ell \gg 0$.

Acknowledgements

I am very indebted to Jakob Stix for his impressive editorial work (from which the exposition of this paper gained a lot) and for pointing out mathematical gaps in the last part of the proof of theorem 1 and in the proof of corollary 3. I am also grateful to Akio Tamagawa for his careful reading of the first version of this text as well as to the referee for his detailed and constructive report.

1.2 Abstract modular curves

We fix once and for all an algebraically closed field k of characteristic $p \geq 0$. By a curve over k we mean a connected, smooth and separated k-scheme of dimension 1.

1.2.1 Notation

Let S be a curve over k with a geometric generic point $\overline{\eta}$ above its generic point $\eta \in S$. We will write $S \hookrightarrow S^{cpt}$ for the smooth compactification of S and $\pi_1(S)$ for its étale fundamental group with base point $\overline{\eta}$. Fix an integer $n \geq 1$, and, for each prime $\ell \gg 0$, let H_ℓ be an $\mathbb{F}_\ell$-module of rank n on which $\pi_1(S)$ acts. We will write ρ for the family of the resulting $\mathbb{F}_\ell$-linear representations

$$\rho_\ell : \pi_1(S) \to \mathrm{GL}(H_\ell) \simeq \mathrm{GL}_n(\mathbb{F}_\ell).$$

For every prime $\ell \gg 0$, set $G_\ell = \mathrm{im}(\rho_\ell)$ and for any subgroup $U \subset G_\ell$, the **abstract modular curve** associated to U is the connected étale cover $S_U \to S$ corresponding to the open subgroup $\rho_\ell^{-1}(U) \subset \pi_1(S)$. We write g_{S_U} and γ_{S_U} for genus and gonality of S_U respectively.

Remark 5. As we are only interested in the asymptotic behaviour of abstract modular curves, it is enough to consider only *big enough* primes ℓ. Furthermore, in practice, H_ℓ will be an étale cohomology group $H^i(X_{\overline{\eta}}, \mathbb{F}_\ell)$ for some smooth proper morphism $X \to S$ with connected geometric generic fibre $X_{\overline{\eta}}$. In particular, the dimension of $H^i(X_{\overline{\eta}}, \mathbb{F}_\ell)$ may become constant only for $\ell \gg 0$, see Subsection 1.2.2.

In the following, we will consider only specific classes of abstract modular curves of two kinds. First, for $v \in H_\ell$ we denote by $S_v \to S$ the abstract modular curve associated to the stabilizer of $G_{\ell,v} \subset G_\ell$ of v, and let g_v and γ_v denote its genus and gonality respectively.

Secondly, for a $\pi_1(S)$-submodule $M \subset H_\ell$, we denote by $S_M \to S$ the abstract modular curve associated to $\mathrm{Fix}(M) := \{g \in G_\ell \mid g|_M = \mathrm{Id}_M\}$, and let g_M and γ_M denote its genus and gonality respectively. The connected étale cover $S_M \to S$ is Galois with Galois group $G_M = G_\ell/Fix(M)$, which is the image of the induced representation $\rho_M : \pi_1(S) \to \mathrm{GL}(M)$.

For $v \in H_\ell$ and the $\pi_1(S)$-submodule $M(v) := \mathbb{F}_\ell[G_\ell \cdot v] \subset H_\ell$ generated by v, the cover $S_{M(v)} \to S$ is the Galois closure of $S_v \to S$.

Let $\mathscr{F} = (\mathscr{F}_\ell)$ denote a sequence of non-empty families of subgroups of G_ℓ. We will say that:

$$S_{\rho,\mathscr{F}}(\ell) := \bigsqcup_{U \in \mathscr{F}_\ell} S_U \to S$$

is the *abstract modular curve associated with* $\mathscr{F}_\ell$ and define:

$$\begin{aligned} d_{\rho,\mathscr{F}}(\ell) &:= \min\{[G_\ell : U] \ ; \ U \in \mathscr{F}_\ell\} \\ g_{\rho,\mathscr{F}}(\ell) &:= \min\{g_{S_U} \ ; \ U \in \mathscr{F}_\ell\} \\ \gamma_{\rho,\mathscr{F}}(\ell) &:= \min\{\gamma_{S_U} \ ; \ U \in \mathscr{F}_\ell\}, \end{aligned}$$

which we call the degree, genus and gonality of the abstract modular curve $S_{\rho,\mathscr{F}}(\ell)$. Following the notation for the usual modular curves, we will write:

$$S_{\rho,1}(\ell),\ d_{\rho,1}(\ell),\ g_{\rho,1}(\ell),\ \gamma_{\rho,1}(\ell)$$

when $\mathscr{F}_\ell$ is the family of all stabilizers $G_{\ell,v}$ for $0 \neq v \in H_\ell$, and

$$S_\rho(\ell),\ d_\rho(\ell),\ g_\rho(\ell),\ \gamma_\rho(\ell)$$

when $\mathscr{F}_\ell$ is the family of all $\mathrm{Fix}(M)$, for $0 \neq M \subset H_\ell$. Note that by construction

$$d_\rho(\ell) \geq d_{\rho,1}(\ell),\ g_\rho(\ell) \geq g_{\rho,1}(\ell) \ \text{ and } \gamma_\rho(\ell) \geq \gamma_{\rho,1}(\ell).$$

1.2.2 Conditions (WA), (I), (T)

Given an integer $1 \leq m \leq n$ and a $\pi_1(S)$-submodule $M \subset \Lambda^m H_\ell$, write again

$$\rho_M : \pi_1(S) \to \mathrm{GL}(M)$$

for the induced representation. We consider the following technical conditions on ρ:

(WA) For any open subgroup $\Pi \subset \pi_1(S)$, there exists an integer $B_\Pi \geq 1$ such that, for every prime ℓ, integer $1 \leq m \leq n$ and Π-submodule $M \subset \Lambda^m H_\ell$, one has:

$$\rho_M(\Pi) \text{ abelian of prime-to-}\ell \text{ order} \Rightarrow |\rho_M(\Pi)| \leq B_\Pi.$$

(WA)' For any open subgroup $\Pi \subset \pi_1(S)$, there exists an integer $B_\Pi \geq 1$ such that, for every prime ℓ, integer $1 \leq m \leq n$ and Π-submodule $M \subset \Lambda^m H_\ell$, one has:

$$\rho_M(\Pi) \text{ abelian} \Rightarrow |\rho_M(\Pi)| \leq B_\Pi.$$

(I) For any open subgroup $\Pi \subset \pi_1(S)$ the $\mathbb{F}_\ell$-submodule H_ℓ^Π of fixed vectors under Π is trivial for $\ell \gg 0$.

(T) For any $P \in S^{cpt} \smallsetminus S$ there exists an open subgroup T_P of the inertia group $I_P \subset \pi_1(S)$ at P such that $\rho_\ell(T_P)$ is tame for $\ell \gg 0$.

In [CT10b], we introduce an additional condition (U), which asserts that for any $P \in S^{cpt} \smallsetminus S$ there exists an open subgroup U_P of the inertia group $I_P \subset \pi_1(S)$ at P such that $\rho_\ell(U_P)$ is unipotent for $\ell \gg 0$. Condition (U) is stronger than condition (T); we will not use it in the following.

See [CT10b, §2.3] for more details, in particular for the following lemma.

Lemma 6. ([CT10b, Lem. 2.2, 2.3 and 2.4])

(1) Assume that condition (T) is satisfied. Set $K := \bigcap_\ell \ker(\rho_\ell)$. Then $\pi_1(S)/K$ is topologically finitely generated.

(2) Conditions (I) and (T) imply $\lim_{\ell \to +\infty} d_{\rho,1}(\ell) = +\infty$.

(3) Conditions (I), (T) and (WA) imply condition (WA)'.

Assume that conditions (I), (T) and (WA) are satisfied. Since $d_\rho(\ell) \geq d_{\rho,1}(\ell)$, it follows from Lemma 6 (2) and (3) that for $\ell \gg 0$ and any $\pi_1(S)$-submodule $0 \neq M \subset H_\ell$ the group G_M cannot be abelian.

Corollary 7. *Assume that conditions (I), (T) and (WA) hold. Then, for any integer $B \geq 1$, for every $\pi_1(S)$-submodule $0 \neq M \subset H_\ell$ and for every abelian subgroup A of G_M one has $[G_M : A] \geq B$ for $\ell \gg 0$.*

Proof. Otherwise, there exists an integer $B \geq 1$ and an infinite set of primes $\mathscr{S}$ such that, for every $\ell \in \mathscr{S}$, there exists a $\pi_1(S)$-submodule $0 \neq M_\ell \subset H_\ell$ and an abelian subgroup A_ℓ of G_{M_ℓ} with $[G_{M_\ell} : A_\ell] \leq B$. But, since it follows from Lemma 6 (1)

that $\pi_1(S)$ acts through a topologically finitely generated quotient, there are only finitely many isomorphism classes of connected étale covers of S corresponding to the $\rho_{M_\ell}^{-1}(A_\ell) \subset \pi_1(S)$, $\ell \in \mathscr{S}$. Hence at least one of them, say $S' \to S$, appears infinitely many times. Up to base-changing by $S' \to S$, we may assume that G_{M_ℓ} is abelian for infinitely many $\ell \in \mathscr{S}$, which contradicts Lemma 6 (2) and (3). □

1.2.3 Etale cohomology

Let $X \to S$ be a smooth, proper morphism with geometrically connected fibers. For every integer $i \geq 0$ the $\mathbb{F}_\ell$-rank $n_{i,\ell}$ of $H_\ell^i := \mathrm{H}^i(X_{\overline{\eta}}, \mathbb{F}_\ell)$ is finite and independent of ℓ for $\ell \gg 0$. Indeed, when $p = 0$, this follows from the comparison isomorphism between Betti and étale cohomology with finite coefficients and the fact that Betti cohomology with coefficient in $\mathbb{Z}$ is finitely generated. More generally, when $p \geq 0$, this follows from the fact that ℓ-adic cohomology with coefficients in $\mathbb{Z}_\ell$ is torsion free for $\ell \gg 0$ [G83] and that the $\mathbb{Q}_\ell$-rank of ℓ-adic cohomology with coefficients in $\mathbb{Q}_\ell$ is independent of ℓ. So, we will simply write n_i instead of $n_{i,\ell}$ for $\ell \gg 0$.

For each $i \geq 1$ and $\ell \gg 0$, the action of $\pi_1(S)$ on H_ℓ^i gives rise to a family $\rho^i = (\rho_\ell^i)$ of n_i-dimensional $\mathbb{F}_\ell$-linear representations

$$\rho_\ell^i : \pi_1(S) \to \mathrm{GL}(H_\ell^i) \simeq \mathrm{GL}_{n_i}(\mathbb{F}_\ell).$$

It follows from [CT10b, Thm. 2.4] that the families ρ^i for $i \geq 1$ satisfy conditions (T) and (WA). As for condition (I), if X_η is projective over $k(\eta)$ then, for $i = 1$ it can be ensured by the condition:

$\mathrm{Pic}^0_{X_{\overline{\eta}}/k(\overline{\eta})}$ contains no non-trivial k-isotrivial abelian subvarieties.

1.3 Technical preliminaries

The proof of Theorem 1 is based on a combination of Lemma 6 with the use of E-P decomposition and group-theoretic ingredients. We gather the results we will need in Subsections 1.3.1, 1.3.2 and 1.3.3 respectively.

1.3.1 E-P decompositions

Consider a diagram of proper curves over k

$$\begin{array}{ccc} Y & \xrightarrow{f} & B \\ {\scriptstyle\pi}\downarrow & & \\ Y', & & \end{array} \tag{1.1}$$

where $f : Y \to B$ is a non-constant morphism of proper curves over k and $\pi : Y \to Y'$ is a G-cover with group G (that is G acts faithfully on Y and $\pi : Y \to Y'$ is the quotient morphism $Y \to Y/G$). We will say that a pair of maps (π, f) as in (1.1) is *equivariant* if for any $\sigma \in G$ there exists $\sigma_B \in \mathrm{Aut}_k(B)$ such that $f \circ \sigma = \sigma_B \circ f$ and that (π, f) as in (1.1) is *primitive* if it does not have any equivariant nontrivial subdiagram that is, more precisely, if for any commutative diagram (1.2) of morphisms of proper curves over k

$$\begin{array}{ccccc} & & \overset{f}{\frown} & & \\ Y & \xrightarrow[f']{} & B' & \xrightarrow[f'']{} & B \\ {\scriptstyle\pi}\downarrow & & & & \\ Y' & & & & \end{array} \tag{1.2}$$

with f' and f'' of degree ≥ 2, the pair (π, f') is not equivariant.

We will resort to the following corollary of the Castelnuovo-Severi inequality.

Lemma 8. ([T04, Thm. 2.4]). *If the pair of maps (π, f) as in (1.1) is primitive then:*

$$\deg(f) \geq \sqrt{\frac{g_Y + 1}{g_B + 1}}.$$

For a pair (π, f) as in diagram (1.1), among all equivariant decompositions, i.e., diagrams as (1.2) with the pair (π, f') equivariant, we choose a pair $(\pi, f' : Y \to C)$ with $\deg(f')$ maximal. This exists as (π, id) is equivariant and $\deg(f') \leq \deg(f)$ is bounded. By definition, the action of G on Y induces an action on C, hence we obtain a homomorphism $G \to \mathrm{Aut}_k(C)$. We set $\overline{G} = G/K$ where

$$K := \mathrm{Ker}(G \to \mathrm{Aut}_k(C)).$$

Then diagram (1.1) for (π, f) can be enriched to a commutative diagram with respect to the maximal equivariant decomposition (π, f') as follows:

$$\begin{array}{ccccc} Y & & & & \\ \downarrow & \overset{f}{\searrow} & & & \\ Z & \longrightarrow & C & \longrightarrow & B \\ \downarrow & & \downarrow & & \\ Y' & \longrightarrow & C' & & \end{array} \tag{1.3}$$

where the vertical maps $Y \to Z = Y/K$, $Z \to Y' = Z/\overline{G}$ and $C \to C' = C/\overline{G}$ are the quotient morphisms. By construction, the pair $(Z \to Y', Z \to C)$ is equivariant and the pair $(C \to C', C \to B)$ is primitive. We will call such a decomposition an *equivariant-primitive decomposition* (E-P decomposition for short).

1.3.2 Review of the classification of finite subgroups of SL_2

We remind that k is a fixed algebraically closed field of characteristic $p \geq 0$. Then we have the following description of finite subgroups of $\mathrm{SL}_2(k)$.

Theorem 9. ([Su82, Thm. 3.6.17]) *A finite subgroup G of $\mathrm{SL}_2(k)$ is one from the following list:*

(1) *a cyclic group,*
(2) *for some $n \geq 2$ a group with presentation*

$$\langle x, y \mid x^n = y^2,\ y^{-1}xy = x^{-1} \rangle,$$

(3) $\mathrm{SL}_2(3)$, *or* $\mathrm{SL}_2(5)$,
(4) *the representation group $\hat{\mathscr{S}}_4$ of the permutation group $\mathscr{S}_4$ in which transpositions lift to elements of order 4,*
(5) *an extension*

$$1 \to A \to G \to Q \to 1,$$

where A is an elementary abelian p-group and Q is a cyclic group of prime-to-p order,
(6) *a dihedral group,*
(7) $\mathrm{SL}_2(k_r)$, *where k_r denotes the subfield of k with p^r elements,*
(8) $\langle \mathrm{SL}_2(k_r), d_\pi \rangle$, *where d_π is the scalar matrix with diagonal entries given by a $\pi \in k$ such that $k_r(\pi)$ has p^{2r} elements and π^2 is a generator of $k_r^\times$.*

Case (6) occurs only when $p = 2$ and cases (7) and (8) occur only when $p > 0$.

We will use two easy corollaries of Theorem 9. Namely, observing that when k is algebraically closed $\mathrm{PGL}_2(k) = \mathrm{PSL}_2(k)$, we get the well known corollary:

Corollary 10. *A finite subgroup G of $\mathrm{PGL}_2(k)$ is of the following form:*

(1) *a cyclic group,*
(2) *a dihedral group,*
(3) $\mathscr{A}_4$, $\mathscr{S}_4$, $\mathscr{A}_5$,
(4) *an extension*

$$1 \to A \to G \to Q \to 1,$$

where A is an elementary abelian p-group and Q is a cyclic group of prime-to-p order,
(5) $\mathrm{PSL}_2(k_r)$,

(6) $\mathrm{PGL}_2(k_r)$.

The last three cases occur only when $p > 0$.

Also, regarding $\mathrm{SL}_2(\mathbb{F}_\ell)$ as a subgroup of $\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)$ and ruling out the groups that cannot lie in $\mathrm{SL}_2(\mathbb{F}_\ell)$, we get:

Corollary 11. *Assume that $\ell \geq 5$. A subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ is isomorphic to one of the following.*

(1) *a cyclic group,*
(2) *for some $n \geq 2$ a group with presentation*

$$\langle x, y \mid x^n = y^2,\ y^{-1}xy = x^{-1} \rangle,$$

(3) $\mathrm{SL}_2(\mathbb{F}_3)$, *or* $\mathrm{SL}_2(\mathbb{F}_5)$,
(4) *the representation group $\hat{\mathscr{S}}_4$ of the permutation group $\mathscr{S}_4$ in which transpositions lift to elements of order* 4,
(5) *a semi-direct product $\mathbb{F}_\ell \rtimes C$ contained in a Borel subgroup with C a cyclic group of prime-to-ℓ order,*
(6) $\mathrm{SL}_2(\mathbb{F}_\ell)$.

1.3.3 A group-theoretic lemma

The following lemma provides a practical condition for a finite group to contain a large normal abelian subgroup.

Lemma 12. *Let G be a finite group and assume that G fits into a short exact sequence of finite groups*

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

with Q abelian and generated by $\leq r$ elements. Then the group G contains a normal abelian subgroup A with index

$$[G : A] \leq \mu(Z(N))^r \cdot |\mathrm{Aut}(N)|,$$

where $\mu(Z(N))$ denotes the least common multiple of the order of the elements in the center $Z(N)$ of N.

Proof. The short exact sequence $(*)$ induces by conjugation representations

$$\tilde{\phi} : G \to \mathrm{Aut}(N) \quad \text{and} \quad \phi : Q \to \mathrm{Out}(N)$$

and induces on the centralizer $Z_G(N) = \ker(\tilde{\phi})$ of N in G the structure of a central extension

$$1 \to Z(N) \to Z_G(N) \to \ker(\phi) \to 1.$$

Because the extension is central, taking the commutator of lifts to $Z_G(N)$ defines an alternating bilinear form $[\ ,\ ]$ on $\ker(\phi)$ with values in $Z(N)$. The radical of $[\ ,\ ]$

$$R = \{q \in \ker(\phi)\ ;\ [q,q'] = 0 \text{ for all } q' \in \ker(\phi)\} \subset \ker(\phi),$$

contains $\mu(Z(N))\ker(\phi)$. We find an extension

$$1 \to Z(N) \to Z(Z_G(N)) \to R \to 1$$

where $A = Z(Z_G(N))$ is the center of $Z_G(N)$. Since N is normal in G, the abelian group A is also normal in G. We can estimate the index $[G:A]$ as

$$[G:A] = \frac{|G|}{|Z_G(N)|} \cdot \frac{|Z_G(N)|}{|A|} \leq |\mathrm{Aut}(N)| \cdot \frac{|\ker(\phi)|}{|R|}$$

$$\leq |\mathrm{Aut}(N)| \cdot \frac{|\ker(\phi)|}{|\mu(Z(N))\ker(\phi)|} \leq |\mathrm{Aut}(N)| \cdot \mu(Z(N))^r$$

since $\ker(\phi) \subset Q$ is also generated by $\leq r$ elements. □

1.4 Proof of Theorem 1

Observe first that if $S' \to S$ is any connected finite étale cover then $\pi_1(S'_M) = \pi_1(S_M) \cap \pi_1(S')$. In particular, one has:

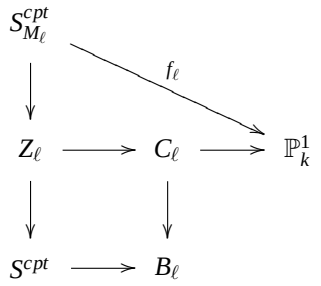
$$\gamma_{S_M} \leq \gamma_{S'_M} \leq \gamma_{S_M}\deg(S'_M \to S_M) \leq \gamma_{S_M}\deg(S' \to S)$$

and, as a result, $\lim\limits_{\ell \to +\infty} \gamma_{\rho|_{\pi_1(S')}}(\ell) = +\infty$ if and only if $\lim\limits_{\ell \to +\infty} \gamma_\rho(\ell) = +\infty$. This allows to perform arbitrary base changes by connected étale covers. In particular, from condition (T), one may assume that $\pi_1(S)$ acts through its tame quotient $\pi_1^t(S)$.

For every prime ℓ, consider a $\pi_1(S)$-submodule $0 \neq M_\ell \subset H_\ell$ such that $\gamma_{M_\ell} = \gamma_\rho(\ell)$. We thus have a diagram of proper curves over k

$$\begin{array}{ccc} S^{cpt}_{M_\ell} & \xrightarrow{f_\ell} & \mathbb{P}^1_k \\ \downarrow & & \\ S^{cpt} & & \end{array} \tag{1.4}$$

with $\deg(f_\ell) = \gamma_\rho(\ell)$. We can consider an E-P decomposition of (1.4)



(1.5)

where $S^{cpt}_{M_\ell} \to Z_\ell = S^{cpt}_{M_\ell}/K_\ell$ and, with $\overline{G}_{M_\ell} = G_{M_\ell}/K_\ell$ faithfully acting on C_ℓ, also $C_\ell \to B_\ell = C_\ell/\overline{G}_{M_\ell}$ are the respective quotient maps.

If $\gamma_\rho(\ell)$ does not diverge, then there exists an infinite subset $\mathscr{S}$ of primes and an integer $\gamma \geq 1$ such that $\gamma_\rho(\ell) \leq \gamma$ for all $\ell \in \mathscr{S}$. In particular $|K_\ell| \leq \gamma$, hence

$$|\overline{G}_{M_\ell}| \geq \frac{d_\rho(\ell)}{|K_\ell|} \geq \frac{d_\rho(\ell)}{\gamma}.$$

So, from Lemma 6 (2) one has $\lim\limits_{\substack{\ell\to+\infty \\ \ell\in\mathscr{S}}} |\overline{G}_{M_\ell}| = +\infty$.

To get the contradiction, we distinguish between three cases. In the first case we assume that $g_{C_\ell} \geq 2$ for all but finitely many $\ell \in \mathscr{S}$. Since by [St73] the size of the automorphism group of a genus $g \geq 2$ curve over an algebraically closed field of characteristic p is bounded by $P_p(g)$ for a polynomial $P_p(T) \in \mathbb{Z}[T]$ depending only on p, we find for $\ell \in \mathscr{S}$ that $|\overline{G}_{M_\ell}| \leq P_p(g_{C_\ell})$, which forces

$$\lim_{\substack{\ell\to+\infty \\ \ell\in\mathscr{S}}} g_{C_\ell} = +\infty.$$

But from Lemma 8 applied to the primitive pair $(C_\ell \to B_\ell, C_\ell \to \mathbb{P}^1_k)$ in diagram (1.4), one has

$$\gamma_\rho(\ell) = \deg(f_\ell) \geq \deg(C_\ell \to \mathbb{P}^1_k) \geq \sqrt{g_{C_\ell}+1},$$

which therefore also diverges for $\ell \in \mathscr{S}$ contradicting the choice of $\mathscr{S}$.

If we are not in the first case, then $g_{C_\ell} \leq 1$ for infinitely many $\ell \in \mathscr{S}$. In the second case, we assume that for infinitely many $\ell \in \mathscr{S}$, and in fact by replacing $\mathscr{S}$ by a subset, that for all $\ell \in \mathscr{S}$ we have $g_{C_\ell} = 1$. Then for $\ell \in \mathscr{S}$, the group $\overline{G}_{M_\ell}$ is an extension

$$1 \to A_\ell \to \overline{G}_{M_\ell} \to Q_\ell \to 1$$

with A_ℓ a finite quotient of $\hat{\mathbb{Z}}^2$ and $|Q_\ell| \leq 24$. Since by Lemma 6 $\pi_1(S)$ acts through a topologically finitely generated quotient, there are only finitely many isomorphism classes of étale covers of S with degree ≤ 24 corresponding to the inverse image of A_ℓ via

$$\pi_1(S) \overset{\rho_{M_\ell}}{\twoheadrightarrow} G_{M_\ell} \twoheadrightarrow \overline{G}_{M_\ell}.$$

So, by replacing S by the composite of all these étale covers of degree ≤ 24, we may assume that $\overline{G}_{M_\ell} = A_\ell$ for all $\ell \in \mathscr{S}$. Now Lemma 12 applied to

$$1 \to K_\ell \to G_{M_\ell} \to A_\ell \to 1$$

shows, since $|K_\ell| \leq \gamma$, that G_{M_ℓ} has an abelian subgroup of index bounded above independently of $\ell \in \mathscr{S}$ in contradiction to Corollary 7.

In the last case we can and do assume that $g_{C_\ell} = 0$ for all $\ell \in \mathscr{S}$. As above, Corollary 7 shows that the subgroup $\overline{G}_{M_\ell} \subset \mathrm{Aut}(C_\ell) \cong \mathrm{PGL}_2(k)$ can be only of type (4), (5) or (6) as in Corollary 10 for $\ell \gg 0$, and $\ell \in \mathscr{S}$. This occurs only if $p > 0$. Without loss of generality, by replacing $\mathscr{S}$ by an infinite subset, we may assume that $\overline{G}_{M_\ell}$ is of the same type for all $\ell \in \mathscr{S}$. To rule out these cases, we are going to use the following theorem.

Theorem 13 ([N87, Thm. C]). *For any integer $n \geq 1$ there exists an integer $d(n) \geq 1$ such that for any prime $\ell \geq n$, integer $m \leq n$ and subgroup G of $\mathrm{GL}_m(\mathbb{F}_\ell)$ the following holds. Let G^+ denote the (normal) subgroup of G generated by the elements of order ℓ in G. Then, there exists an abelian subgroup $A \subset G$ such that AG^+ is normal in G and $[G : AG^+] \leq d(n)$.*

Assume that $\overline{G}_{M_\ell}$ is of type (4) for all $\ell \in \mathscr{S}$, that is of the form

$$(\mathbb{Z}/p)^{r_\ell} \rtimes Z/N_\ell$$

for some integers $r_\ell, N_\ell \geq 1$ with $p \not| N_\ell$.

Claim. There exists an integer $r(n) \geq 1$ such that $r_\ell \leq r(n)$ for $\ell \gg 0$ in $\mathscr{S}$.

Proof. Let T_ℓ denote the inverse image of $(\mathbb{Z}/p)^{r_\ell}$ in G_{M_ℓ} that is T_ℓ fits into the short exact sequence of finite groups

$$1 \to K_\ell \to T_\ell \to (\mathbb{Z}/p)^{r_\ell} \to 1.$$

Because $|K_\ell| \leq \gamma$ we see that ℓ does not divide $|T_\ell|$ for $\ell \gg 0$ and, in particular, that T_ℓ^+ is trivial. Theorem 13 implies that T_ℓ fits into a short exact sequence

$$1 \to A_\ell \to T_\ell \to Q_\ell \to 1$$

with A_ℓ abelian and $|Q_\ell| \leq d(n)$. In turn, A_ℓ fits into the sort exact sequence

$$1 \to K_\ell \cap A_\ell \to A_\ell \to (\mathbb{Z}/p)^{s_\ell} \to 1$$

with $s_\ell \leq r_\ell$. In particular, A_ℓ is an abelian subgroup of $\mathrm{GL}(M_\ell)$ of prime-to-ℓ order and of $\mathbb{Z}$-rank $\geq s_\ell$. This implies $s_\ell \leq n$ since any abelian subgroup A of order prime-to-ℓ in $\mathrm{GL}_n(\mathbb{F}_\ell)$ is conjugate in $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ to a diagonal torus. So the claim follows from $r_\ell \leq s_\ell + \log_p |Q_\ell|$ and the bounds for s_ℓ and $|Q_\ell| \leq d(n)$. □

By the claim and Lemma 12, the group $\overline{G}_{M_\ell}$ contains a normal abelian subgroup A_ℓ with index bounded by

$$[\overline{G}_{M_\ell} : A_\ell] \leq p \cdot |\mathrm{GL}_{r(n)}(\mathbb{F}_p)|.$$

Invoking again that $\pi_1(S)$ acts through a topologically finitely generated quotient, without loss of generality we may assume that $\overline{G}_{M_\ell} = A_\ell$ and then, as above the contradiction follows from the bound $|K_\ell| \leq \gamma$, Lemma 12 and Corollary 7.

Assume now that $\overline{G}_{M_\ell}$ is of type (5) or (6) for all $\ell \in \mathscr{S}$, that is either $\mathrm{PSL}_2(k_{r_\ell})$ or $\mathrm{PGL}_2(k_{r_\ell})$ for some integer $r_\ell \geq 1$.

For any non zero vector $v \in M_\ell$ the cover $S_{M(v)} \to S$ is a quotient of $S_{M_\ell} \to S$ hence $\gamma_{S_{M(v)}} \leq \gamma_{S_{M_\ell}}$. So, without loss of generality, we may assume that M_ℓ is a simple $\pi_1(S)$-module. In particular, there exists a non zero vector $v \in M_\ell$ such that $M_\ell = M(v)$ and $M_\ell^+ := \mathbb{F}_\ell[G_{M_\ell}^+ v] \subset M$ is a simple $G_{M_\ell}^+$-submodule.

Claim. The group $G_{M_\ell}^+$ is nontrivial for $\ell \gg 0$, $\ell \in \mathscr{S}$.

Proof. Theorem 13 applied to $G_{M_\ell} \subset \mathrm{GL}(M_\ell)$ shows that one can write $G_{M_\ell}/G_{M_\ell}^+$ as an extension

$$1 \to A_\ell G_{M_\ell}^+/G_{M_\ell}^+ \to G_{M_\ell}/G_{M_\ell}^+ \to Q_\ell \to 1$$

with $A_\ell G_{M_\ell}^+/G_{M_\ell}^+$ abelian and $|Q_\ell| \leq d(n)$, because $\dim_{\mathbb{F}_\ell}(M_\ell) \leq n$. As a result, if $G_{M_\ell}^+ = 1$, we get a contradiction to Corollary 7. This proves the claim. □

Since $\mathrm{PSL}_2(k_{r_\ell})$ is simple and the only nontrivial normal subgroups of $\mathrm{PGL}_2(k_{r_\ell})$ are $\mathrm{PSL}_2(k_{r_\ell})$ and $\mathrm{PGL}_2(k_{r_\ell})$, the second claim implies that the normal subgroup

$$\overline{G}_{M_\ell}^+ := G_{M_\ell}^+/G_{M_\ell}^+ \cap K_\ell$$

of $\overline{G}_{M_\ell}$ contains $\mathrm{PSL}_2(k_{r_\ell})$.

Claim. $Z_\ell := K_\ell \cap G_{M_\ell}^+$ is a central subgroup of $G_{M_\ell}^+$ for $\ell \gg 0$, $\ell \in \mathscr{S}$.

Proof. Because $|Z_\ell| \leq \gamma$ we see that (i) $\ell \not| |Z_\ell|$ and (ii) $\ell \not| |\mathrm{Aut}(Z_\ell)|$ for $\ell \gg 0$, $\ell \in \mathscr{S}$. From (i) and Schur-Zassenhauss, for any ℓ-Sylow $S_\ell \subset G_{M_\ell}$, the group $Z_\ell S_\ell$ is a semidirect product $Z_\ell \rtimes S_\ell$ and, from (ii), the semidirect product $Z_\ell \rtimes S_\ell$ is actually a direct product that is S_ℓ is contained in the centralizer $Z_{G_{M_\ell}^+}(H_\ell)$ of H_ℓ in $G_{M_\ell}^+$. But, by definition, for $\ell \gg 0$ the group $G_{M_\ell}^+$ is generated by the ℓ-Sylow subgroups S_ℓ of G_{M_ℓ} hence $G_{M_\ell}^+ = Z_{G_{M_\ell}^+}(Z_\ell)$. □

Because Z_ℓ is commutative and of prime-to-ℓ order, Z_ℓ is conjugate in $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ to a diagonal torus. For any $z \in Z_\ell$ let $VP(z) \subset \overline{\mathbb{F}}_\ell^\times$ denote the set of eigenvalues of z and set

$$V := \prod_{z \in Z_\ell} VP(z).$$

Then, $M\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell$ can be decomposed into a direct sum

$$M\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell=\bigoplus_{\underline{\lambda}\in V}E(\underline{\lambda}),$$

where, for any $\underline{\lambda}=(\lambda_z)_{z\in Z_\ell}$ we write

$$E(\underline{\lambda}):=\bigcap_{z\in Z_\ell}\ker(z-\lambda_z Id).$$

From the second claim, $G_{M_\ell}^+$ stabilize each $\overline{\mathbb{F}}_\ell$-submodule $E(\underline{\lambda})$ of $M\otimes_{\mathbb{F}_\ell}\overline{\mathbb{F}}_\ell$ and from the first claim, it acts non diagonally at least on one of the nonzero $E(\underline{\lambda})$, say E. The action of $G_{M_\ell}^+$ on E induces a non trivial action on the projective space

$$\mathbb{P}(E):=E/\overline{\mathbb{F}}_\ell^\times$$

and, by definition of E, this action factors through $\overline{G}_{M_\ell}^+$. This shows that $\mathrm{PSL}_2(k_{r_\ell})$ embeds into $\mathrm{PGL}(E)$. But E is of $\overline{\mathbb{F}}_\ell$-dimension $\leq n$ so, from [LS74, Thm. p. 419], this can occur only for finitely many values of r_ℓ. which, in turn, contradicts the fact that $r_\ell\to\infty$ for $\ell\in\mathscr{S}$ by Lemma 6 (2).

The proof of Theorem 1 is now complete.

1.5 The case of $S_{\rho,1}(\ell)$

Whenever it is defined, we set for $i=1,\dots,n=\dim_{\mathbb{F}_\ell}(H_\ell)$

$$\gamma_{\rho,1}^i(\ell):=\min\{\gamma_v\ ;\ 0\neq v\in H_\ell \text{ and } \dim_{\mathbb{F}_\ell}(M(v))=i\}$$

Note that, when $n=i$, one has $\gamma_{\rho,1}^n(\ell)=\gamma_{\rho,1}(\ell)$.

Let $\mathscr{S}$ denote the set of all primes ℓ such that H_ℓ contains a $\pi_1(S)$-submodule of $\mathbb{F}_\ell$-rank 2. Assume that $\mathscr{S}$ is infinite. In this section, we prove:

Proposition 14. *Assume that conditions (WA), (I) and (T) are satisfied. Then:*

$$\lim_{\substack{\ell\to+\infty\\ p|\ell(\ell^2-1)}}\gamma_{\rho,1}^2(\ell)=+\infty.$$

and deduce from this result the proof of Corollary 3. The proof of Proposition 14 needs some preparation.

We first study the possible structure of the group G_M when $\dim_{\mathbb{F}_\ell}(M)=2$ and $\ell\gg 0$.

Lemma 15. *Assume that conditions (WA), (I) and (T) are satisfied. Then, for $\ell\gg 0$ and any $\pi_1(S)$-submodule $M\subset H_\ell$ of $\mathbb{F}_\ell$-rank 2 one has $\mathrm{SL}(M)\subset G_M$.*

Proof. We write G_M as an extension

$$1 \to G_M \cap \mathrm{SL}(M) \to G_M \xrightarrow{\det} D_M \to 1,$$

where $D_M = \det(G_M) \subset \mathbb{F}_\ell^\times \simeq \mathbb{Z}/(\ell-1)$.

Let us show first that $|G_M \cap \mathrm{SL}(M)|$ diverges with $\ell \to \infty$ in $\mathscr{S}$ and M is any $\pi_1(S)$-submodule $M \subset H_\ell$ of $\mathbb{F}_\ell$-rank 2. Otherwise, up to replacing $\mathscr{S}$ by an infinite subset, we may assume that there exists an upper bound

$$|G_M \cap \mathrm{SL}(M)| \leq B$$

for all possible M. From Lemma 6 (2), one has

$$\lim_{\substack{\ell \to +\infty \\ \ell \in \mathscr{S}}} |G_{M_\ell}| = +\infty,$$

which forces $|D_M|$ to diverge when $\ell \to \infty$ in $\mathscr{S}$. Let $o(B)$ denote the maximal order of the automorphism group of a group of order $\leq B$. Then, as D_M is cyclic, it follows from Lemma 12 that G_M contains a normal abelian subgroup of index $\leq B \cdot o(B)$, which contradicts Corollary 7 for $\ell \gg 0$ in $\mathscr{S}$.

Hence, for $\ell \gg 0$ in $\mathscr{S}$ and any $\pi_1(S)$-submodule $M \subset H_\ell$ of $\mathbb{F}_\ell$-rank 2, the only possibilities with respect to the list of Corollary 11 for $G_M \cap \mathrm{SL}(M)$ are (1), (2), (5) or (6). The types (1) and (2) are ruled out by condition (WA)' and Lemma 6, and type (6) is exactly what the lemma claims. It remains to rule out type (5).

If $G_M \cap \mathrm{SL}(M)$ is of type (5), then it is contained in a Borel and thus fixes a line $\mathbb{F}_\ell \cdot v \subset M$ for some $0 \neq v \in H_\ell$. The line is uniquely determined since the ℓ-Sylow of $G_M \cap \mathrm{SL}(M)$ is nontrivial, and thus $\mathbb{F}_\ell \cdot v$ is also invariant under G_M. However, by condition (WA) and Lemma 6 (2), the group G_M cannot fix $\mathbb{F}_\ell \cdot v$, which is the desired contradiction. □

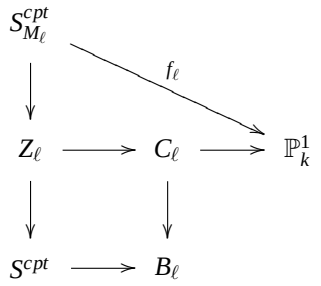
Lemma 16. *Assume that conditions (WA), (I) and (T) are satisfied. Then, there exists an integer $D \geq 1$ such that for $\ell \gg 0$ and any $\pi_1(S)$-submodule $M \subset H_\ell$ one has $|\det(G_M)| \leq D$.*

Proof. Let m denote the $\mathbb{F}_\ell$-rank of M. Then the action of G_M on the line $\Lambda^m M$ factors through a faithfull action of $D_M := \det(G_M)$. So the conclusion follows from condition (WA)'. □

Now we can prove Proposition 14. Let $\mathscr{S}$ denote the set of all primes ℓ such that there exists $v \in H_\ell$ with $M(v)$ of $\mathbb{F}_\ell$-rank 2. Assume that $\mathscr{S}$ is infinite and for every $\ell \in \mathscr{S}$, choose $v_\ell \in H_\ell$ with $M_\ell := M(v_\ell)$ of $\mathbb{F}_\ell$-rank 2 such that $\gamma_{v_\ell} = \gamma^2_{\rho,1}(\ell)$. By Lemma 15 and for $\ell \gg 0$ in $\mathscr{S}$ we write again G_{M_ℓ} as an extension

$$1 \to \mathrm{SL}(M_\ell) \to G_{M_\ell} \xrightarrow{\det} D_\ell \to 1,$$

where $D_\ell = \det(G_{M_\ell}) \subset \mathbb{F}_\ell^\times \simeq \mathbb{Z}/(\ell-1)$. From lemma 16, we have $|D_\ell| \leq D$. Consider an E-P decomposition



(1.6)

where $S^{cpt}_{M_\ell} \to Z_\ell = S^{cpt}_{M_\ell}/K_\ell$ and, with $\overline{G}_{M_\ell} = G_{M_\ell}/K_\ell$ faithfully acting on C_ℓ, also $C_\ell \to B_\ell = C_\ell/\overline{G}_{M_\ell}$ are the respective quotient maps, and $\deg(f_\ell) = \gamma_{M_\ell}$. We set D^K_ℓ for the image of K_ℓ in D_ℓ. Then K_ℓ fits into the short exact sequence

$$1 \to K_\ell \cap \mathrm{SL}(M_\ell) \to K_\ell \to D^K_\ell \to 1.$$

As the only normal subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ are 1, $\mathbb{Z}/2$ and $\mathrm{SL}_2(\mathbb{F}_\ell)$, there are only two possibilities for $K_\ell \cap \mathrm{SL}(M_\ell)$, namely

(1) $K_\ell \cap \mathrm{SL}(M_\ell) = \mathrm{SL}(M_\ell)$.
(2) $K_\ell \cap \mathrm{SL}(M_\ell) = 1,\ \mathbb{Z}/2$,

In case (1), one has the estimate

$$\gamma_{M_\ell} = \deg(f_\ell) \geq \deg(S^{cpt}_{M_\ell} \to Z_\ell) = |K_\ell| = \ell(\ell^2-1)\cdot|D^K_\ell| = |G_{M_\ell}| \cdot \frac{|D^K_\ell|}{|D_\ell|}.$$

Since $\mathrm{SL}(M_\ell)$ acts transitively on $M_\ell \setminus \{0\}$, the stabilizer G_{M_ℓ,v_ℓ} of v_ℓ under the action of G_{M_ℓ}, namely the Galois group of $S_{M(v)} \to S_v$, has index ℓ^2-1 and so

$$\gamma^2_{p,1}(\ell) = \gamma_{v_\ell} \geq \frac{\gamma_{M_\ell}}{|G_{M_\ell,v_\ell}|} \geq (\ell^2-1)\cdot\frac{|D^K_\ell|}{|D_\ell|} \geq \frac{\ell^2-1}{D} \to +\infty.$$

In case (2), the stabilizer has size

$$|G_{M_\ell,v_\ell}| = \frac{|G_{M_\ell}|}{\ell^2-1} = \ell\cdot|D_\ell|,$$

and thus Lemma 8 applied to the primitive pair $(C_\ell \to B_\ell, C_\ell \to \mathbb{P}^1_k)$ in diagram (1.6) yields the estimate

$$\gamma^2_{p,1}(\ell) = \gamma_{v_\ell} \geq \frac{\gamma_{M_\ell}}{|G_{M_\ell,v_\ell}|} \geq \frac{\deg(S^{cpt}_{M_\ell} \to Z_\ell)\cdot\deg(C_\ell \to \mathbb{P}^1_k)}{\ell\cdot|D_\ell|} \geq \frac{|K_\ell|\cdot\sqrt{g_{C_\ell}+1}}{\ell\cdot|D_\ell|} \quad (1.7)$$

For $\ell \gg 0$ and in particular $\ell > p$, the group $\overline{G}_{M_\ell}$ contains $\mathrm{SL}(M_\ell)$ or $\mathrm{PSL}(M_\ell)$, and so it is not a subgroup of the automorphism group of a curve of genus 0 or 1 over an algebraically closed field of characteristic $p \geq 0$. As a result, one may assume that

C_ℓ has genus ≥ 2. If p does not divide $\ell(\ell^2-1)$ then p does not divide $|\mathrm{GL}(M_\ell)|$ hence, *a fortiori*, does not divide $|\overline{G}_{M_\ell}|$. Consequently, the cover $C_\ell \to B_\ell$ lifts to characteristic 0 and we have the Hurwitz bound for the automorphism group

$$\frac{\ell(\ell^2-1)|D_\ell|}{|K_\ell|} = |\overline{G}_{M_\ell}| \leq 84(g_{C_\ell}-1).$$

In combination with (1.7) this yields

$$\gamma^2_{\rho,1}(\ell) \geq \frac{|K_\ell|\cdot\sqrt{g_{C_\ell}+1}}{\ell\cdot|D_\ell|} \geq \frac{|K_\ell|}{\ell\cdot|D_\ell|}\sqrt{\frac{\ell(\ell^2-1)|D_\ell|}{84|K_\ell|}+2}$$

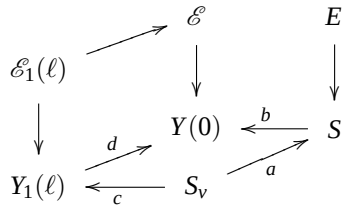
Hence

$$\gamma^2_{\rho,1}(\ell) \geq \sqrt{\frac{(\ell^2-1)}{84\cdot\ell\cdot|D|}} \to +\infty.$$

This completes the proof of Proposition 14.

Remark 17. When $p|\ell(\ell^2-1)$, one can assert only that $\ell(\ell^2-1) \leq P_p(g_{C_\ell})$ so the resulting lower bound for g_{C_ℓ} is too small to conclude. Also, from condition (T), one could observe that $Z_\ell \to S^{cpt}$ is tame for $\ell \gg 0$ but, if $p|\ell(\ell^2-1)$ and $S^{cpt} \to B_\ell$ is wildly ramified, it may happen that $C_\ell \to B_\ell$ is wildly ramified as well hence does not necessarily lift to characteristic 0.

Finally, we give a proof of Corollary 3. Let $Y(0)$ and $Y_1(\ell)$ denote the coarse moduli schemes of the stack $\mathscr{E}$ of elliptic curves and of the stack $\mathscr{E}_1(\ell)$ of elliptic curves with a torsion point of order exactly ℓ as stacks over k. For any nonisotrivial relative elliptic curve $E \to S$ and $0 \neq v \in E_{\overline{\eta}}[\ell]$, one has the following commutative diagram



In particular we can estimate the gonality as

$$\gamma_{Y_1(\ell)} \geq \frac{\gamma_v}{\deg(c)} = \frac{\gamma_v \deg(d)}{\deg(a)\deg(b)} = \frac{\gamma_v(\ell^2-1)/2}{|G_\ell\cdot v|\deg(b)} \geq \frac{\gamma_v}{2\deg(b)}$$

with $\deg(b)$ independent of v and ℓ. Applying Proposition 14 to the family of rank-2 $\mathbb{F}_\ell$-linear representations

$$\rho_\ell \,:\, \pi_1(S) \to \mathrm{GL}(E_{\overline{\eta}}[\ell])$$

gives the conclusion of Corollary 3.

References

[A96] D. ABRAMOVICH, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **20**, 1996, p. 1005-1011.

[CT10a] A. CADORET and A. TAMAGAWA, *On a weak variant of the geometric torsion conjecture*, preprint, 2010.

[CT10b] A. CADORET and A. TAMAGAWA, *On a weak variant of the geometric torsion conjecture II*, preprint, 2010.

[EHK10] J. ELLENBERG, C. HALL and E. KOWALSKI *Expander graphs, gonality and variation of Galois representations*, preprint, 2010.

[F91] G. FALTINGS, *Diophantine approximation on abelian varieties*, Annals of Math. **133**, 1991, p. 549-576.

[Fr94] G. FREY *Curves with infinitely many points of fixed degree*, Israel J. Math. **85**, 1994, p. 79-83.

[G83] O. GABBER *Sur la torsion dans la cohomologie ℓ-adique d'une variété*, C.R. Acad. Sci. Paris Ser. I Math. **297**, 1983, p. 179-182.

[LS74] V. LANDAZURI and G.M. SEITZ, *On the minimal degree of projective representations of the finite Chevalley groups*, J. Algebra **32**, 1974, p. 418-443.

[N87] M.V. NORI, *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$, Inventiones. Math. **88**, p. 257-275, 1987.

[P07] B. POONEN, *Gonality of modular curves in characteristic p*, Math. Res. Letters **14**, 2007, p. 691-701.

[St73] H. STICHTENOTH, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I, II*, Arch. der Math. (Basel) **24**, 1973, p. 524-544 and p. 615-631.

[Su82] M. SUZUKI, *Group theory I*, Grundlehren der Mathematischen Wissenschaften **247**, Springer-Verlag, 1982.

[T04] A. TAMAGAWA, *Finiteness of isomorphism classes of curves in positive characteristic with prescribed fundamental group*, J. Algebraic Geometry **13**, 2004, p. 675-724.

anna.cadoret@math.u-bordeaux1.fr
Institut de Mathématiques de Bordeaux - Université Bordeaux 1,
351 Cours de la Libération,
F33405 TALENCE cedex, FRANCE.