COMPOSITIO MATHEMATICA

The essential dimension of congruence covers

Benson Farb, Mark Kisin and Jesse Wolfson

Compositio Math. **157** (2021), 2407–2432.

doi:10.1112/S0010437X21007594

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY
EST. 1865

Compositio Math. 157 (2021) 2407–2432
doi:10.1112/S0010437X21007594

The essential dimension of congruence covers

Benson Farb, Mark Kisin and Jesse Wolfson

Abstract

Consider the algebraic function $\Phi_{g,n}$ that assigns to a general g-dimensional abelian variety an n-torsion point. A question first posed by Klein asks: What is the minimal d such that, after a rational change of variables, the function $\Phi_{g,n}$ can be written as an algebraic function of d variables? Using techniques from the deformation theory of p-divisible groups and finite flat group schemes, we answer this question by computing the essential dimension and p-dimension of congruence covers of the moduli space of principally polarized abelian varieties. We apply this result to compute the essential p-dimension of congruence covers of the moduli space of genus g curves, as well as its hyperelliptic locus, and of certain locally symmetric varieties. These results include cases where the locally symmetric variety M is *proper*. As far as we know, these are the first examples of nontrivial lower bounds on the essential dimension of an unramified, nonabelian covering of a proper algebraic variety.

Contents

1. Introduction

Let K be an algebraically closed field of characteristic 0. Consider the (multi-valued) function $\Phi_{g,n}$ that assigns to a general g-dimensional principally polarized abelian K-variety

Received 20 January 2020, accepted in final form 21 June 2021.
2020 Mathematics Subject Classification 14G35 (primary), 11G18 (secondary).
Keywords: Shimura varieties, essential dimension, finite flat group schemes.
The authors are partially supported by NSF grants DMS-1811772 (BF), DMS-1601054 (MK) and DMS-1811846 (JW).

an n-torsion point. Thinking of $\Phi_{g,n}$ as an algebraic function on the moduli space of principally polarized abelian varieties over K, one can ask the following question.

Question 1. *Let $g, n \geq 2$. What is the minimum d such that, after a rational change of variables, the function $\Phi_{g,n}$ can be written as an algebraic function of d variables?*

Our interest in Question 1 was partly motivated by the work of Kronecker [Kr1861, p. 309] and Klein (see [Kl1888, p. 171] for the case $(g,n) = (2,3)$ and [Kl1890, § II.16] for $(g,n) = (3,2)$) who asked about the analogous minimum integer d for certain problems arising in classical algebraic geometry, and used 'modular' functions like $\Phi_{g,n}$, to investigate these problems.

We can rephrase Question 1 in more modern language, using the moduli space of principally polarized abelian varieties and the notion of *essential dimension* introduced by Tschebotarëw [Tsc34, § 4.8] (under the name 'true transcendence degree') and again by Buhler and Reichstein [BR97]. Let $\mathcal{A}_g$ denote the coarse moduli space of g-dimensional, principally polarized abelian varieties over K, and let $\mathcal{A}^1_{g,n}$ be the coarse moduli space of pairs (A, z) where A is a principally polarized abelian variety of dimension g, and z is an n-torsion point on A.

For any finite, generically étale map of K-schemes, $p : X' \to X$, define the *essential dimension* $\mathrm{ed}_K(X' \to X)$, or $\mathrm{ed}_K(X'/X)$ if the map is implicit, to be the minimal d for which there is a dense Zariski open $U \subset X$, such that $X'|_U$ is the pullback[1]

$$\begin{array}{ccc} X'|_U & \longrightarrow & Y' \\ \downarrow & & \downarrow \\ U & \xrightarrow{f} & Y \end{array}$$

of a finite map $Y' \to Y$ of d-dimensional K-varieties via a regular map $f : U \to Y$. In this case we call f a *(rational) compression* of p. Question 1 can be rephrased as asking for the value of $\mathrm{ed}_K(\mathcal{A}^1_{g,n} \to \mathcal{A}_g)$.

Following Klein [Kl1884], we can ask a related question, where we allow certain *accessory irrationalities*; that is, we can ask for

$$\min_{E \to \mathcal{A}_g} \mathrm{ed}_K(\mathcal{A}^1_{g,n}|_E \to E)$$

for some class of finite, generically étale maps $E \to \mathcal{A}_g$. For example, Reichstein and Youssin [RY00] define the *essential p-dimension* $\mathrm{ed}_K(X'/X; p)$ as the minimum of $\mathrm{ed}_K(X' \times_X E \to E)$ where $E \to X$ runs over finite, generically étale maps of K-varieties of degree prime to p. For any map $E \to X$ one always has

$$\mathrm{ed}_K(X' \times_X E \to E) = \mathrm{ed}_K(\tilde{X}' \times_X E \to E)$$

where $\tilde{X}'$ denotes the composite of Galois closures of the connected components of X' (see Lemmas 2.2.2, 2.2.3; cf. [BR97, Lemma 2.3]). In particular, for any class of maps $E \to \mathcal{A}_g$, the answer to the question above does not change if we replace $\mathcal{A}^1_{g,n}$ by $\mathcal{A}_{g,n}$, the coarse moduli space of pairs $(A, \mathcal{B})$ where A is a principally polarized abelian variety of dimension g, and $\mathcal{B}$ is a symplectic basis for the n-torsion $A[n]$. (Here and below we fix once and for all an isomorphism $\mu_n(K) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$, so that we may speak of a symplectic basis for $A[n]$.)

In this paper we apply techniques from the deformation theory of p-divisible groups and finite flat group schemes to compute the essential p-dimension of congruence covers of certain locally symmetric varieties, such as $\mathcal{A}_g$.

[1] Given maps $X' \to X$ and $U \to X$, we use the notation $X'|_U$ and $X' \times_X U$ interchangeably to denote the fiber product.

https://doi.org/10.1112/S0010437X21007594

THEOREM 2. *Let $g, n \geq 2$, and let p be any prime with $p|n$. Then*

$$\mathrm{ed}_K(\mathcal{A}_{g,n}/\mathcal{A}_g; p) = \mathrm{ed}_K(\mathcal{A}_{g,n}/\mathcal{A}_g) = \dim \mathcal{A}_g = \binom{g+1}{2}.$$

Theorem 2 thus answers Question 1: the minimal d equals $\binom{g+1}{2}$. We in fact prove a more general result, that for subvarieties of $\mathcal{Z} \subset \mathcal{A}_g$ satisfying some mild technical hypotheses, $\mathrm{ed}_K(\mathcal{A}_{g,n}|_{\mathcal{Z}}/\mathcal{Z}) = \dim \mathcal{Z}$. More precisely, we prove the following theorem (see Theorem 3.2.6 below for a slightly more general formulation, which is important in some applications).

THEOREM 3. *Let p be prime and let $N \geq 3$ be an integer prime to p. Suppose that $L = \bar{\mathbb{Q}}_p$, an algebraic closure of $\mathbb{Q}_p$, let $\mathcal{O}_L$ be its ring of integers and let k be its residue field. Let $\mathcal{Z} \subset \mathcal{A}_{g,N/\mathcal{O}_L}$ be a locally closed subscheme that is equidimensional and smooth over $\mathcal{O}_L$, and whose special fiber $\mathcal{Z}_k$ meets the ordinary locus $\mathcal{A}^{\mathrm{ord}}_{g,N} \subset \mathcal{A}_{g,N/k}$. Then*

$$\mathrm{ed}_L(\mathcal{A}_{g,p}|_{\mathcal{Z}_L}/\mathcal{Z}_L; p) = \mathrm{ed}_L(\mathcal{A}_{g,p}|_{\mathcal{Z}_L}/\mathcal{Z}_L) = \dim \mathcal{Z}_L.$$

We give three applications of Theorem 3. The first is an analogue of Theorem 2 for $\mathcal{M}_g$, the coarse moduli space of smooth, proper, genus $g \geq 2$ curves over K. For any integer n, consider the *level n congruence cover* $\mathcal{M}_g[n] \to \mathcal{M}_g$, where $\mathcal{M}_g[n]$ denotes the moduli space of pairs $(C, \mathcal{B})$ consisting of a smooth, proper curve C of genus g, together with a symplectic basis $\mathcal{B}$ for $J(C)[n]$, where $J(C)$ is the Jacobian of C. Applying Theorem 3 and the Torelli theorem, we will deduce the following result.

COROLLARY 4. *Let $g, n \geq 2$. Let p be any prime with $p|n$. Then*

$$\mathrm{ed}_K(\mathcal{M}_g[n]/\mathcal{M}_g) = \mathrm{ed}_K(\mathcal{M}_g[n]/\mathcal{M}_g; p) = \dim \mathcal{M}_g = 3g - 3.$$

As a second application of Theorem 3, let $\mathcal{H}_g$ denote the coarse moduli of smooth, hyperelliptic curves of genus $g \geq 2$ over K. For any integer n, consider the *level n congruence cover* $\mathcal{H}_g[n] \to \mathcal{H}_g$, where $\mathcal{H}_g[n]$ denotes the moduli space of pairs $(C, \mathcal{B})$ consisting of a hyperelliptic curve C together with a symplectic basis $\mathcal{B}$ for $J(C)[n]$. Analogously to the case of $\mathcal{M}_g$, we prove the following result.

COROLLARY 5. *Let $g, n \geq 2$. Let $p|n$ be any odd prime. Then*

$$\mathrm{ed}_K(\mathcal{H}_g[n]/\mathcal{H}_g) = \mathrm{ed}_K(\mathcal{H}_g[n]/\mathcal{H}_g; p) = \dim \mathcal{H}_g = 2g - 1.$$

For $g > 2$, the hypothesis that p is odd in Corollary 5 is necessary; see 3.3.5 below.

Our third application of Theorem 3 generalizes Theorem 2 to many locally symmetric varieties. Recall that a *locally symmetric variety* is a variety whose complex points have the form $\Gamma\backslash X^+$, where X^+ is a Hermitian symmetric domain and Γ is an arithmetic lattice in the corresponding real semisimple Lie group (see Lemma 4.2.3 below). Attached to Γ there is a semisimple algebraic group G over $\mathbb{Q}$, with X^+ the connected component of the identity in $X = G(\mathbb{R})/K_\infty$, for $K_\infty \subset G(\mathbb{R})$ a maximal compact subgroup. By a *principal p-level covering* $\Gamma_1\backslash X^+ \to \Gamma\backslash X^+$ we mean that the definition of Γ does not involve any congruences at p, and $\Gamma_1 \subset \Gamma$ is the subgroup of elements that are trivial mod p. A sample of what we prove is the following theorem (see Theorem 4.3.6 below for the most general statement).

THEOREM 6. *Suppose that each irreducible factor of $G^{\mathrm{ad}}_{\mathbb{R}}$ is the adjoint group of one of $U(n, n)$, $\mathrm{SO}(n, 2)$ with $n + 2 \neq 8$, or $\mathrm{Sp}(2n)$ for some positive integer n. If G is unramified at p (a condition*

https://doi.org/10.1112/S0010437X21007594

which holds for almost all p), then for any principal p-level covering $\Gamma_1\backslash X^+ \to \Gamma\backslash X^+$, we have

$$\mathrm{ed}_{\mathbb{C}}(\Gamma_1\backslash X^+ \to \Gamma\backslash X^+; p) = \dim X^+.$$

In fact our results apply to any Hermitian symmetric domain of classical type, but in general they require a more involved condition on the $\mathbb{Q}$-group G giving rise to Γ; this condition always applies if G splits over $\mathbb{Q}_p$. Note that these results include cases where the locally symmetric variety $\Gamma\backslash X^+$ is *proper*. As far as we know, these are the first examples of nontrivial lower bounds on the essential dimension of an unramified, nonabelian covering of a proper algebraic variety (although a certain abelian subgroup of the covering group plays an important role in the argument). The only prior result for unramified covers of proper varieties of which we are aware is due to Gabber [CT02, Appendix], who proved that if $\{E_i' \to E_i\}$ is a collection of connected, unramified $\mathbb{Z}/p\mathbb{Z}$ covers of elliptic curves E_i, then under certain conditions, the cover $E_1' \times \cdots \times E_r' \to E_1 \times \cdots \times E_r$ has essential dimension at p equal to r.

When $\Gamma\backslash X$ is proper, the use of more standard techniques involving fixed points to bound ed from below (see, for example, [Rei11]) is precluded by the fact that one cannot use 'ramification at infinity'. This is in analogy with Margulis superrigidity for irreducible lattices Γ in higher rank semisimple Lie groups where, for nonuniform Γ (equivalently, noncompact $\Gamma\backslash X$), unipotents in Γ play a crucial role. When Γ is uniform it contains no unipotents, and new ideas were needed (and were provided only later, also by Margulis).

There are many examples of finite simple groups of Lie type for which our methods give a lower bound on the essential p-dimension of a covering of locally symmetric varieties with that group. To state these, for H an absolutely simple (adjoint) algebraic group over $\mathbb{F}_q$, denote by $H(q)$ the image of $H^{\mathrm{sc}}(\mathbb{F}_q) \to H(\mathbb{F}_q)$, where H^{sc} denotes the simply connected cover of H.

Corollary 7. *Let H be a classical, absolutely simple group over $\mathbb{F}_q$, with $q = p^r$. If $p = 2$ we further assume that $8 \nmid r$, and $4 \nmid r$ if H is not split over $\mathbb{F}_q$.*

Then there is a congruence $H(q)$-cover of locally symmetric varieties $Y' \to Y$, whose associated real Lie group is of the same type (A, B, C or D) as H, and such that $e := \mathrm{ed}_K(Y'/Y; p)$ satisfies the following conditions.

- *If H is a form of PGL_n which is split if n is odd, then $e = r\lfloor n^2/4 \rfloor$.*
- *If H is PSp_{2n} then $e = r((n^2+n)/2)$.*
- *If H is a split form of PO_{2n} then $e = r((n^2-n)/2)$.*
- *If H is a form of PO_n and H is not of type D_4, then $e = r(n-2)$.*

Idea of the proof. To prove Theorem 2 and its generalization to subvarieties we use arithmetic techniques, specifically Serre–Tate theory, which describe the deformation theory of an ordinary abelian variety in characteristic p in terms of its p-divisible group. Let $N \geq 3$ be an integer coprime to p, and let $\mathcal{A}$ denote the universal abelian scheme over $\mathcal{A}_{g,N}$ (now considered over $\mathbb{Z}[\zeta_N][1/N]$). Let $\mathcal{A}[p]$ be its p-torsion group scheme, and let $\mathcal{A}_x$ denote the fiber of $\mathcal{A}$ at x. Given a rational compression of $\mathcal{A}_{g,pN} \to \mathcal{A}_{g,N}$ (in characteristic 0) onto a smaller-dimensional variety, we show that there exists an ordinary mod p point x of $\mathcal{A}_{g,N}$, and a tangent direction t_x at x such that the deformation of $\mathcal{A}_x[p]$ corresponding to t_x is trivial. From this we deduce that the deformation of $\mathcal{A}_x$ corresponding to t_x is trivial, a contradiction.

One might view our method as an arithmetic analogue of the 'fixed point method' in the theory of essential dimension (see [Rei11]), where the role of fixed points for a group action is now played by wild ramification at a prime. In the fixed point method one usually works over a field

https://doi.org/10.1112/S0010437X21007594

where the order of the group is invertible. In contrast, for us the presence of wild ramification plays an essential role.

Acknowledgements. We would like to thank Aaron Landesman and Zinovy Reichstein for detailed comments on an earlier version of this paper and for extensive helpful correspondence. We thank Frank Calegari for pointing out a mistake in an earlier version of this paper. We thank Yonathan Stone for help with the classical German literature. We also thank Maxime Bergeron, Mike Fried, Eric Rains, Alexander Polishchuk and Burt Totaro, for various helpful comments. Finally, we thank the referees for their incredibly thorough and thoughtful reports, and for many useful suggestions that helped to improve this paper.

2. Preliminary results

2.1 Finite étale maps

We begin with some general lemmas on finite étale maps.

2.1.1. Let $G \to G'$ be a homomorphism, and S a finite set with an action of G. We say that the action of G on S *lifts* to G' if there is an action of G' on S, which induces the given action of G on S. We call such a G'-action a *lifting* of the G-action on S. We say that the action of G on S *virtually lifts* to G' if there is a finite index subgroup $G'' \subset G'$, containing the image of G, such that the action of G on S lifts to G''.

For a positive integer n we denote by S^n the n-fold product equipped with the diagonal action of G, and by $\pi_i : S^n \to S$, $i = 1, \dots, n$, the projections.

Lemma 2.1.2. *Let $G \to G'$ be a map of groups, and S a finite set with an action of G.*

(i) *Suppose the action of G on S admits a lifting to an action of G' on S, and fix such a lifting. Then there exists a finite index subgroup $G'' \subset G'$ containing the image of G, such that G and G'' have the same image in* $\mathrm{Aut}(S)$.

(ii) *Let $T \subset S^n$ be a G-stable subset such that $\bigcup_{i=1}^n \pi_i(T) = S$. Then the action of G on S virtually lifts to G' if and only if the action of G on T virtually lifts to G'.*

Proof. Let $N \subset G'$ be the kernel of $G' \to \mathrm{Aut}(S)$, and $G'' \subset G'$ the subgroup generated by N and the image of G. Since S is finite, N and hence G'' has finite index in G', and so G'' satisfies the conditions in (i).

For (ii), suppose that the action of G on S virtually lifts to G'. By (i), after replacing G' by a finite index subgroup containing the image of G, we may assume that the action of G on S lifts to G', and that G and G' have the same image in $\mathrm{Aut}(S)$. Then T is G'-stable, so the action of G on T lifts to G'. Conversely, if the action of G on T virtually lifts to G', then, by (i), we may assume that the action of G on T lifts to G', and that G and G' have the same image in $\mathrm{Aut}(T)$. In particular, any element of G' acts on $\mathrm{Aut}(T)$ via an element of $\mathrm{Aut}(S)$. Since $\bigcup_{i=1}^n \pi_i(T) = S$ this element of $\mathrm{Aut}(S)$ is uniquely determined. The uniqueness implies that $G' \to \mathrm{Aut}(T)$ factors through a homomorphism $G' \to \mathrm{Aut}(S)$, which lifts the action of G on S. □

2.1.3. Let X be a separated, locally Noetherian scheme and $f : Y \to X$ a finite étale cover. We will say that f is Galois if any connected component of Y is Galois over its image.

Suppose that X is connected, and let $\bar{x}$ be a geometric point of X. Let $F_{\bar{x}}$ denote the functor which assigns to any finite étale cover $Y \to X$ the underlying topological space $|Y_{\bar{x}}|$ of its fiber over $\bar{x}$. Then $\mathrm{Aut}(F_{\bar{x}})$ is called the étale fundamental group and is denoted by $\pi_1(X, \bar{x})$, [SGA1, Exp. V, § 7]. It follows from [SGA1, Exp. V, § 7] that the association $Y \mapsto S(Y) := |Y_{\bar{x}}|$ induces

https://doi.org/10.1112/S0010437X21007594

a bijection between isomorphism classes of finite étale covers, and of finite sets with $\pi_1(X, \bar{x})$-action. If X is connected and S is a finite set with an action of $\pi_1(X, \bar{x})$, we denote by $Y(S)$ the corresponding finite étale cover of X.

In the next three lemmas we consider a map of separated, locally Noetherian schemes $g : X \to X'$ and a finite étale cover $f' : Y' \to X'$ equipped with an isomorphism $Y \xrightarrow{\sim} Y' \times_{X'} X$. If X and X' are connected, and $\bar{x}$ again denotes the geometric point of X' induced by $\bar{x}$, then such a Y' exists if and only if the action of $\pi_1(X, \bar{x})$ on $S(Y)$ lifts to $\pi_1(X', \bar{x})$.

Lemma 2.1.4. *If f is Galois, then there is a finite étale $h : X'' \to X'$ such that g factors through X'' and $Y'' = X'' \times_{X'} Y' \to X''$ is Galois.*

Proof. We may assume that X and X' are connected. We apply Lemma 2.1.2(i), to $\pi_1(X, \bar{x}) \to \pi_1(X', \bar{x})$ and $S = S(Y) = S(Y')$. Let $h : X'' \to X'$ be the finite étale map corresponding to the $\pi_1(X', \bar{x})$-set $\pi_1(X', \bar{x})/G''$. Since this set has a $\pi_1(X, \bar{x})$ fixed point, g factors through X''. By construction, the images of $\pi_1(X'', \bar{x})$ and $\pi_1(X, \bar{x})$ in $\mathrm{Aut}(S(Y')) = \mathrm{Aut}(S(Y))$ are equal. Denote this image by H, and for $s \in S(Y)$ denote the stabilizer by H_s. Since $Y \to X$ is Galois, H_s is a normal subgroup which does not depend on s, which implies that $Y'' \to X''$ is Galois. □

2.1.5. Let A be a finite ring. By an *A-local system* $\mathcal{F}$ on X we will mean an étale sheaf of A-modules which is locally isomorphic to the constant A-module A^n for some n. Such an $\mathcal{F}$ is representable by a finite étale map $Y(\mathcal{F}) \to X$. This is clear étale locally on X, and follows from étale descent in general. If X is connected, and equipped with a geometric point $\bar{x}$, then the association $\mathcal{F} \mapsto |Y(\mathcal{F})|_{\bar{x}}$ induces a bijection between isomorphism classes of A-local systems and conjugacy classes of representations $\pi_1(X, \bar{x}) \to \mathrm{GL}_n(A)$. Indeed, this follows easily from the bijection explained in 2.1.3.

For $X \to X_1$ a map of schemes, and $\mathcal{G}$ an A-local system on X_1, we will denote by $\mathcal{G}|_X$ the pullback of $\mathcal{G}$ to X.

Lemma 2.1.6. *Suppose that $f : Y = Y(\mathcal{F}) \to X$ corresponds to an A-local system $\mathcal{F}$. Then there is a finite étale $h : X'' \to X'$ such that g factors through X'' and $Y'' = X'' \times_X Y' \to X''$ represents an A-local system $\mathcal{F}''$, with $\mathcal{F}''|_X \xrightarrow{\sim} \mathcal{F}$.*

Proof. We may assume that X and X' are connected and choose X'' as in the proof of Lemma 2.1.4, using the construction in Lemma 2.1.2(i). Then the finite set $S(Y) = S(Y')$ naturally has the structure of a finite free A-module on which $\pi_1(X, \bar{x})$ acts A-linearly. Since the images of $\pi_1(X'', \bar{x})$ and $\pi_1(X, \bar{x})$ in $\mathrm{Aut}(S(Y))$ are equal, $\pi_1(X'', \bar{x})$ acts on $S(Y)$ A-linearly, which implies the statement of the lemma. □

2.1.7. We continue to assume that X is separated and locally Noetherian.

For any integer $N \geq 1$ we denote by μ_N the kernel of $\mathbb{G}_m \xrightarrow{N} \mathbb{G}_m$. This is a finite flat group scheme over $\mathbb{Z}$, and we denote by the same symbol its pullback to any scheme X. This pullback is étale if any only if X is a $\mathbb{Z}[1/N]$-scheme.

Suppose X is a $\mathbb{Z}[1/N]$-scheme. For any $\mathbb{Z}/N\mathbb{Z}$ algebra A, we again denote by μ_N or $A(1)$ the étale sheaf $\mu_N \otimes_{\mathbb{Z}/N\mathbb{Z}} A$. For any nonnegative integer i we write $A(i) = A(1)^{\otimes i}$. For i negative we set $A(i)$ equal to the A-linear dual of $A(-i)$.

Lemma 2.1.8. *Let $N \geq 1$ be an integer, i, j integers, and A a finite $\mathbb{Z}/N\mathbb{Z}$-algebra. Suppose that X is a $\mathbb{Z}[1/N]$-scheme and that $f : Y = Y(\mathcal{F}) \to X$ corresponds to an A-local system $\mathcal{F}$, which is an extension of $A(i)^r$ by $A(j)^s$, for some positive integers r, s.*

Then there is a finite étale map $X'' \to X'$ such that g factors through X'' and the cover $Y'' = X'' \times_X Y' \to X''$ represents an A-local system $\mathcal{F}''$, which is an extension of $A(i)^r$ by $A(j)^s$, with $\mathcal{F}''|_X \xrightarrow{\sim} \mathcal{F}$ as extensions.

Proof. Replacing $\mathcal{F}$ by $\mathcal{F}(-j) := \mathcal{F} \otimes_A A(-j)$, we may suppose that $j = 0$. By Lemma 2.1.6, we may assume Y'' represents an A-local system and $g^*(\mathcal{F}') \xrightarrow{\sim} \mathcal{F}$ as A-local systems. Let $\mathcal{F}_1 \subset \mathcal{F}$ denote the sub A-local system corresponding to $A(j)^s$, so that $\mathcal{F}_1$ corresponds to an A-submodule $S(Y')_1 \subset S(Y')$.

Let X'' and H be as in the proof of Lemma 2.1.4. Since the group H acts trivially on $S(Y')_1$, after replacing X' by X'', we may assume that $\mathcal{F}'$ is an extension of $\mathcal{F}'/A(i)^r$ by $A(j)^s$, and $g^*(\mathcal{F}') \xrightarrow{\sim} \mathcal{F}$ is an isomorphism of extensions. A similar argument, applied to $\mathcal{F}/A(j)^s \otimes A(-i)$, shows that we may assume that $\mathcal{F}'$ is an extension of $A(i)^r$ by $A(j)^s$, with $g^*(\mathcal{F}') \xrightarrow{\sim} \mathcal{F}$ as extensions. □

2.2 Essential dimension

2.2.1. Let K be a field, X a K-scheme of finite type, and $f : Y \to X$ a finite étale cover. The *essential dimension* [BR97, § 2] $\mathrm{ed}_K(Y/X)$ of Y over X is the smallest integer e such that there exists a finite type K-scheme W of dimension e, a dense open subscheme $U \subset X$, and a map $U \to W$, such that $Y|_U$ is the pullback of a finite étale covering over W. The *essential p-dimension* $\mathrm{ed}_K(Y/X; p)$ is defined as the minimum of $\mathrm{ed}_K(Y \times_X E/E)$ where $E \to X$ runs over dominant, generically finite maps, which have degree prime to p at all generic points of X.

Note that when X is irreducible, the definition does not change if we consider only coverings with E irreducible. Indeed, for any $E \to X$, as above, one of the irreducible components of E will have degree prime to p over the generic point of X.

Suppose X is connected. A *Galois closure* of $Y \to X$ is a union of Galois closures of the connected components of Y. If $Y_i \to X$, $i = 1, \dots r$, are finite étale, Galois and connected, then a *composite* of the Y_i is a connected component of $Y_1 \times_X \cdots \times_X Y_r$. Up to isomorphism, this does not depend on the choice of connected component. If we drop the assumption that X is connected, we define the Galois closure and composite by making these constructions over each connected component of X.

LEMMA 2.2.2. *Let $f : Y \to X$ be a finite étale cover, and $\tilde{Y}$ a Galois closure for Y. For any map of K-schemes $E \to X$, we have*

$$\mathrm{ed}_K(Y_E/E) = \mathrm{ed}_K(\tilde{Y}_E/E).$$

In particular, we have

$$\mathrm{ed}_K(Y/X; p) = \mathrm{ed}_K(\tilde{Y}/X; p).$$

Proof. We may assume that X is connected. Let $\bar{x}$ be a geometric point for X, and S a $\pi_1(X, \bar{x})$-set with $Y = Y(S)$. Suppose first that Y is connected. Let $N \subset \pi_1(X, \bar{x})$ be the (normal) subgroup which fixes S pointwise. If $s \in S$, and $\pi_1(X, \bar{x})_s$ is the stabilizer of s, then $N = \bigcap_{i=1}^n g_i \pi_1(X, \bar{x})_s g_i^{-1}$ for a finite collection of elements $g_1, \dots, g_n \in \pi_1(X, \bar{x})$. Let $\tilde{S}$ denote the $\pi_1(X, \bar{x})$-orbit of $(g_1 \cdot s, \dots, g_n \cdot s) \in S^n$. Then the stabilizer in $\pi_1(X, \bar{x})$ of any point of $\tilde{S}$ is N, so $\tilde{Y} = Y(\tilde{S})$ is a Galois closure of Y.

Now we drop the assumption that Y is connected, and let $Y_1, \dots, Y_r$ denote the connected components of Y, with Y_i corresponding to a subset $S_i \subset S$ on which $\pi_1(X, \bar{x})$ acts transitively. The above construction gives subsets $\tilde{S}_i \subset S_i^n$, (we may assume without loss of generality that n does not depend on i) with $\tilde{Y}_i = Y(\tilde{S}_i)$ a Galois closure of Y_i. If $\tilde{S} = \coprod_i \tilde{S}_i \subset S^n$, then $\tilde{Y} = Y(\tilde{S}) = \coprod_i \tilde{Y}_i$ is a Galois closure for Y.

https://doi.org/10.1112/S0010437X21007594

From the construction one sees that S, $T = \tilde{S}$ and $G = \pi_1(X, \bar{x})$ satisfy the conditions in Lemma 2.1.2(ii) (note that these conditions do not depend on the choice of G'). For any homomorphism $H \to G$, these conditions continue to hold if we instead view S and T as H-sets.

Now let $E \to X$ be a map of K-schemes, $U \subset E$ a connected open subset, and $U \to E'$ a map of K-schemes. Suppose U admits a geometric point $\bar{y}$ mapping to $\bar{x}$. Applying the above remark with $H = \pi_1(U, \bar{y})$, Lemma 2.1.2(ii) implies that the action of H on S virtually lifts to $\pi_1(E', \bar{y})$ if and only the action of H on T virtually lifts to $\pi_1(E', \bar{y})$. As in the proof of Lemma 2.1.4, this implies that $Y|_U$ arises by pullback from a cover of E'' for some finite étale $E'' \to E'$, if and only if the same condition holds for $\tilde{Y}|_U$. Since $\bar{x}$ was an arbitrary geometric point of X, this implies $\mathrm{ed}_K(Y|_E/E) = \mathrm{ed}_K(\tilde{Y}|_E/E)$. □

Lemma 2.2.3. *Let $Y_i \to X$, $i = 1, \dots, r$, be connected Galois coverings of K-schemes, and $Y \to X$ a composite of the Y_i. Then for any map of K-schemes $E \to X$, we have*

$$\mathrm{ed}_K(Y_E/E) = \mathrm{ed}_K\left(\left(\coprod_i Y_i\right)_E \Big/ E\right).$$

In particular, we have

$$\mathrm{ed}_K(Y/X; p) = \mathrm{ed}_K\left(\left(\coprod_i Y_i\right) \Big/ X; p\right).$$

Proof. Let $\bar{x}$ be a geometric point for X, and let S_i be a $\pi_1(X, \bar{x})$-set with $Y_i = Y(S_i)$. Let $S = \coprod_i S_i$. Then Y corresponds to a transitive $\pi_1(X, \bar{x})$ set $T \subset S_1 \times \cdots \times S_r$ which surjects onto each S_i. Viewing $T \subset S^r$, we see that T satisfies the conditions of Lemma 2.1.2. The lemma now follows as in the proof of Lemma 2.2.2. □

Lemma 2.2.4. *Let A be a finite ring, K a field, $\mathcal{F}$ an A-local system on a connected K-scheme X equipped with a geometric point $\bar{x}$, and $\rho_{\mathcal{F}} : \pi_1(X, \bar{x}) \to \mathrm{GL}_n(A)$ the representation corresponding to $\mathcal{F}$. Let Y be the covering of X corresponding to $\ker \rho_{\mathcal{F}}$.*

Then Y is the composite of Galois closures of the connected components of $Y(\mathcal{F})$. In particular,

$$\mathrm{ed}_K(Y'/X) = \mathrm{ed}_K(Y(\mathcal{F})/X).$$

For any prime p we also have

$$\mathrm{ed}_K(Y/X; p) = \mathrm{ed}_K(Y(\mathcal{F})/X; p).$$

Proof. Consider the action of $\pi_1(X, \bar{x})$ on A^n corresponding to $\mathcal{F}$. The connected components of $Y(\mathcal{F})$ correspond to the stabilizers $\pi_1(X)_s$ for $s \in A^n$. A Galois closure of such a component corresponds to

$$\bigcap_{g \in \pi_1(X)} g\pi_1(X)_s g^{-1} = \bigcap_{g \in \pi_1(X)} \pi_1(X)_{gs}.$$

Thus the composite of such Galois closures corresponds to $\bigcap_s \pi_1(X)_s = \ker \rho_{\mathcal{F}}$.

The lemma now follows from Lemmas 2.2.2 and 2.2.3. □

Lemma 2.2.5. *Let $K' \subset K$ be algebraically closed fields. If $Y \to X$ is a finite étale covering of finite type K'-schemes then*

$$\mathrm{ed}_{K'}(Y/X) = \mathrm{ed}_K(Y_K/X_K).$$

Proof. Let $U_K \subset X_K$ be a dense open and $U_K \to W_K$ a morphism with $\dim W_K = \mathrm{ed}_K(Y_K/X_K)$ such that $Y_K|_{U_K}$ arises from a finite cover $f' : Y'_K \to W_K$. Then U_K, the finite cover f' and the isomorphism $f'^* Y'_K \xrightarrow{\sim} Y_K|_{U_K}$ are all defined over some finitely generated K'-algebra $R \subset K$. Specializing by a map $R \to K'$ produces the required data for the covering $Y \to X$. □

2.2.6. It will be convenient to make the following definition. Suppose that $Y \to X$ is a finite étale covering of finite type R-schemes, where R is a domain of characteristic 0. Set $\overline{\mathrm{ed}}(Y/X) = \mathrm{ed}_{\bar{K}}(Y/X)$ where $\bar{K}$ is any algebraically closed field containing R, and similarly for $\overline{\mathrm{ed}}(Y/X;p)$. By Lemma 2.2.5, this does not depend on the choice of $\bar{K}$.

LEMMA 2.2.7. *Let K be an algebraically closed field, and $Y \to X$ a finite Galois covering of connected, finite type K-schemes with Galois group G. Let $H \subset G$ be a central, cyclic subgroup of order n with $\mathrm{char}(K) \nmid n$. Then for any prime p we have*

$$\overline{\mathrm{ed}}(Y \to X;p) \geq \overline{\mathrm{ed}}(Y/H \to X;p)$$

with equality if $p \nmid n$.

Proof. To show $\overline{\mathrm{ed}}(Y/X;p) \geq \overline{\mathrm{ed}}(Y/H \to X;p)$, after shrinking X, we may assume there is a map $f : X \to X'$ such that $Y = f^*Y'$ for a finite étale covering $Y' \to X'$, which may be assumed to be connected and Galois by Lemma 2.1.4. The Galois group of Y'/X' is necessarily equal to G, and we have $f^*(Y'/H) \xrightarrow{\sim} Y/H$.

For the converse inequality when $p \nmid n$, we may assume there is a map $f : X \to X'$ such that $Y/H = f^*Y'$ for a finite étale covering $Y' \to X'$, which we may again assume is connected and Galois with group G/H. The image, c, of $Y' \to X'$ under

$$H^1(X', G/H) \to H^2(X', H) \xrightarrow{\sim} H^2(X', \mu_n)$$

is the obstruction to lifting $Y' \to X'$ to a G-covering. Here, for the final isomorphism, we are using that K is algebraically closed of characteristic prime to n. Viewing c as a Brauer class, we see that it has order dividing n. This implies that (after perhaps shrinking X further) there is an étale covering $X'_1 \to X'$ of order dividing a power n such that $c|_{X_1}$ is trivial [FD93, Lemma 4.17]. In particular, $X'_1 \to X'$ has order prime to p. Replacing $Y \to X \to X'$ by their pullbacks to X'_1, we may assume that $c = 0$, and that $Y' = Y''/H$ for some Galois covering $Y'' \to X'$ with group G.

The difference between the G-coverings $Y \to X$ and $f^*Y'' \to X$ is measured by a class in $H^1(X, H)$. After replacing X by the H-covering corresponding to this class, we may assume that this class is trivial, and so $Y \xrightarrow{\sim} f^*Y''$. This shows that $\overline{\mathrm{ed}}(Y/X;p) \leq \overline{\mathrm{ed}}(Y/H \to X;p)$. □

3. Essential dimension and moduli of abelian varieties

3.1 Ordinary finite flat group schemes

In this subsection we fix a prime p, and we consider a complete discrete valuation ring V of characteristic 0, with perfect residue field k of characteristic p, and a uniformizer $\pi \in V$.

By a *finite flat group scheme* on a $\mathbb{Z}_p$-scheme X we will always mean a finite flat, commutative, group scheme on X of p-power order. A finite flat group scheme on X is called *ordinary* if étale locally on X, it is an extension of a constant group scheme $\bigoplus_{i\in I} \mathbb{Z}/p^{n_i}\mathbb{Z}$ by a group scheme of the form $\bigoplus_{j\in J} \mu_{p^{m_j}}$ for integers $n_i, m_j \geq 1$. In this subsection we study the classification of these extensions.

https://doi.org/10.1112/S0010437X21007594

3.1.1. Now let $\tilde{X} = \operatorname{Spec} A$ be an affine $\mathbb{Z}_p$-scheme, and set $X = \tilde{X} \otimes \mathbb{Q}$. Let $n \geq 1$, and consider the exact sequence of sheaves

$$1 \to \mu_{p^n} \to \mathbb{G}_m \xrightarrow{p^n} \mathbb{G}_m \to 1$$

in the flat topology of $\tilde{X}$. Taking flat cohomology of this sequence and its restriction to X, we obtain the following commutative diagram with exact rows.

$$\begin{array}{ccccccc} 1 & \longrightarrow & A^\times/(A^\times)^{p^n} & \longrightarrow & H^1(\tilde{X}, \mu_{p^n}) & \longrightarrow & H^1(\tilde{X}, \mathbb{G}_m) \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & A[1/p]^\times/(A[1/p]^\times)^{p^n} & \longrightarrow & H^1(X, \mu_{p^n}) & \longrightarrow & H^1(X, \mathbb{G}_m) \end{array}$$

The group $H^1(\tilde{X}, \mathbb{G}_m)$ classifies line bundles on $\tilde{X}$. Hence, if A is local it vanishes, and this can be used to classify extensions of $\mathbb{Z}/p^n\mathbb{Z}$ by μ_{p^n} as finite flat group schemes. We have

$$\operatorname{Ext}^1_{\tilde{X}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \xrightarrow{\sim} H^1(\tilde{X}, \mu_{p^n}) \xrightarrow{\sim} A^\times/(A^\times)^{p^n}.$$

Here and below, the group on the left denotes extensions as sheaves of $\mathbb{Z}/p^n\mathbb{Z}$-modules.

Similarly, we can classify extensions of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mu_{p^\infty} = \lim_n \mu_{p^n}$ as p-divisible groups. If $\mathcal{E}$ is such an extension, then $\mathcal{E}[p^n]$ is an extension of $\mathbb{Z}/p^n\mathbb{Z}$ by μ_{p^n} and we have

$$\hat{\theta}_A : \operatorname{Ext}^1_{\tilde{X}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \xrightarrow{\sim} \varprojlim_n A^\times/(A^\times)^{p^n}.$$

If A is complete and local with residue field k, then the right-hand side may be identified with $A^{\times,1} \subset A^\times$, the subgroup of units which map to 1 in $k^\times$. Thus we have

$$\hat{\theta}_A : \operatorname{Ext}^1_{\tilde{X}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \xrightarrow{\sim} A^{\times,1}.$$

3.1.2. For the rest of this subsection we assume that $A = V[\![x_1, \ldots, x_n]\!]$. Then $H^1(X, \mathbb{G}_m) = 0$ by [SGA2, XI, Thm 3.13], and we have the following commutative diagram.

$$\begin{array}{ccc} A^\times/(A^\times)^{p^n} & \xrightarrow{\sim} & H^1(\tilde{X}, \mu_{p^n}) \\ \downarrow & & \downarrow \\ A[1/p]^\times/(A[1/p]^\times)^{p^n} & \xrightarrow{\sim} & H^1(X, \mu_{p^n}) \end{array}$$

3.1.3. We call an element of $\operatorname{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) = H^1(X, \mu_{p^n})$ *syntomic* if it arises from an element of $A^\times$, or equivalently from a class in $\operatorname{Ext}^1_{\tilde{X}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$, and we denote the subgroup of syntomic elements by $\operatorname{Ext}^{1,\mathrm{syn}}_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \subset \operatorname{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$

Lemma 3.1.4. *The map* $\operatorname{Ext}^1_{\tilde{X}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \to \operatorname{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$ *is injective.*

Proof. If $a \in A^\times$ is a p^nth power in $A[1/p]$ then it is a p^nth power in A, as A is normal. Hence the map $A^\times/(A^\times)^{p^n} \to A[1/p]^\times/(A[1/p]^\times)^{p^n}$ is injective, and the lemma follows from the description of Ext^1s above. □

Lemma 3.1.5. *Let* $B = V[\![y_1, \ldots, y_s]\!]$ *for some integer* $s \geq 0$, *and*

$$f : \tilde{X} \to \tilde{Y} = \operatorname{Spec} B$$

a local flat map of complete local V*-algebras. Let* $Y = \operatorname{Spec} B[1/p]$, *and suppose that* $c \in H^1(Y, \mu_{p^n})$, *and that* $f^*(c) \in H^1(X, \mu_{p^n})$ *is syntomic. Then* c *is syntomic.*

https://doi.org/10.1112/S0010437X21007594

Proof. Let $b \in B[1/p]^\times$ be an element giving rise to c. Since B is a unique factorization domain we may write $b = b_0\pi^i$ with $b_0 \in B^\times$ and $i \in \mathbb{Z}$. Since $f^*(c)$ is syntomic, we may write $\pi^i = a_0 a^{p^n}$ with $a_0 \in A^\times$ and $a \in A[1/p]^\times$. Comparing the images of both sides in the group of divisors on A, one sees that $p^n | i$. So c arises from b_0. □

3.1.6. Let $\mathfrak{m}_A$ be the maximal ideal of A, and $\bar{\mathfrak{m}}_A$ its image in $A/\pi A$. The natural map

$$\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2 \overset{a\mapsto 1+a}{\to} k^\times \backslash (A/(\pi, \mathfrak{m}_A^2))^\times$$

is a bijection; both sides are k-vector spaces spanned by $x_1, \ldots, x_n$. We denote by θ_A the composite

$$\theta_A : \mathrm{Ext}^{1,\mathrm{syn}}_X(\mathbb{Z}/p\mathbb{Z}, \mu_p) \xrightarrow{\sim} A^\times/(A^\times)^p \to k^\times \backslash (A/(\pi, \mathfrak{m}_A^2))^\times \xrightarrow{\sim} \bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2.$$

Here we have used Lemma 3.1.4 to identify $\mathrm{Ext}^{1,\mathrm{syn}}_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ and $\mathrm{Ext}^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

LEMMA 3.1.7. *With the notation of Lemma 3.1.5, suppose that*

$$L \subset \mathrm{Ext}^{1,\mathrm{syn}}_Y(\mathbb{Z}/p\mathbb{Z}, \mu_p)$$

is a subset such that the k-span of $\theta_A(f^*(L))$ is $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$. Then f is an isomorphism.

Proof. By functoriality of the association $A \mapsto \theta_A$, we have $\theta_A(f^*(L)) = f^*(\theta_B(L))$. Hence the k-span of $\theta_A(f^*(L))$ is contained in image of $\bar{\mathfrak{m}}_B/\bar{\mathfrak{m}}_B^2$. It follows that $\bar{\mathfrak{m}}_B/\bar{\mathfrak{m}}_B^2$ surjects onto $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$. Since A and B are complete local V-algebras, this implies that B, which is a subring of A, surjects onto A. Hence f is an isomorphism. □

3.2 Monodromy of p-torsion in an abelian scheme

We now use the results of the previous section to obtain results about the essential dimension of covers of the moduli space of abelian varieties.

3.2.1. Recall that an abelian scheme $\mathcal{A}$ over a $\mathbb{Z}_p$-scheme is called ordinary if the group scheme $\mathcal{A}[p^n]$ is ordinary for all $n \geq 1$. This is equivalent to requiring the condition for $n = 1$.

Let k be an algebraically closed field of characteristic $p > 0$, and let V be a complete discrete valuation ring with residue field k, so that $W(k) \subset V$. Let $\mathcal{A}_0$ be an abelian scheme over k of dimension g. We assume that $\mathcal{A}_0$ is ordinary. Since k is algebraically closed, this implies that $\mathcal{A}_0[p^\infty]$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^g \oplus \mu_{p^\infty}^g$.

Consider the functor $D_{\mathcal{A}_0}$ on the category of Artinian V-algebras C with residue field k, which attaches to C the set of isomorphism classes of deformations of $\mathcal{A}_0$ to an abelian scheme over C. Recall [Kat81, § 2] that $D_{\mathcal{A}_0}$ is equivalent to the functor which attaches to C the set of isomorphism classes of deformations of $\mathcal{A}_0[p^\infty]$, and that $D_{\mathcal{A}_0}$ is pro-representable by a formally smooth V-algebra R of dimension g^2, called the universal deformation V-algebra of $\mathcal{A}_0$.

Denote by $\mathcal{A}_R$ the universal (formal) abelian scheme over R. Note that although $\mathcal{A}_R$ is only a formal scheme over R, the torsion group schemes $\mathcal{A}_R[p^n]$ are finite over R, and so can be regarded as genuine R-schemes. Since $\mathcal{A}_0$ is ordinary the p-divisible group, $\mathcal{A}_R[p^\infty] = \lim_n \mathcal{A}_R[p^n]$ is an extension of $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ by $\mu_{p^\infty}^g$. Hence $\mathcal{A}_R[p]$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g. This extension class is given by a $g \times g$ matrix of classes $(c_{i,j})$ with $c_{i,j} \in \mathrm{Ext}^1_R(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

LEMMA 3.2.2. *With the notation of § 3.1, the elements $\theta_R(\{c_{i,j}\}_{i,j})$ span $\bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$.*

Proof. Consider the isomorphism

$$\hat{\theta}_R : \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \xrightarrow{\sim} R^{\times,1}$$

https://doi.org/10.1112/S0010437X21007594

introduced in § 3.1. The universal extension of p-divisible groups over R gives rise to a $g \times g$ matrix of elements $(\hat{c}_{i,j}) \in \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty})$ which reduce to $(c_{i,j})$.

Let $L \subset \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$ be the k-span of the images of the elements $\hat{\theta}_R(\hat{c}_{i,j}) - 1$, or equivalently, the elements $\theta_R(c_{i,j}) - 1$, and set $R' = k \oplus L \subset R/(\pi, \mathfrak{m}_R^2)$. Using the isomorphism $\hat{\theta}_{R'}$, one sees that $\mathcal{A}_R[p^\infty]|_{R/(\pi,\mathfrak{m}_R^2)}$ is defined over R'. If $L \subsetneq \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$, then there exists a surjective map $R/(\pi, \mathfrak{m}_R^2) \to k[x]/x^2$ which sends L to zero. Specializing $\mathcal{A}_R[p^\infty]|_{R/(\pi,\mathfrak{m}_R^2)}$ by this map induces the trivial deformation of $\mathcal{A}_0[p^\infty]$ (that is, the split extension of $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ by μ_{p^∞}) over $\mathrm{Spec}\, k[x]/x^2$. This contradicts the fact that R pro-represents $D_{\mathcal{A}_0}$. Hence $L = \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$, which proves the lemma. □

3.2.3. Let A be a quotient of R which is formally smooth over V. That is, A is isomorphic as a complete V-algebra to $V[\![x_1, \dots x_n]\!]$. As in § 3.1, we set $X = \mathrm{Spec}\, A[1/p]$ and $\tilde{X} = \mathrm{Spec}\, A$.

Lemma 3.2.4. *Let $B = V[\![y_1, \dots y_s]\!]$ for some integer $s \geq 0$, and let*

$$f : \tilde{X} \to \tilde{Y} = \mathrm{Spec}\, B$$

be a local flat map of complete local V-algebras. Set $Y = \mathrm{Spec}\, B[1/p]$. Suppose that k is algebraically closed, and that there exists an $\mathbb{F}_p$-local system $\mathcal{L}$ on Y which is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g such that $f^*\mathcal{L} \xrightarrow{\sim} \mathcal{A}_R[p]|_X$ as extensions of $\mathbb{F}_p$-local systems. Then f is an isomorphism.

Proof. Using the notation of 3.2.1, we have that $\theta_R(\{c_{i,j}\}_{i,j})$ spans $\bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$ by Lemma 3.2.2. In particular, if we again denote by $c_{i,j}$ the restrictions of these classes to A, then $\theta_A(\{c_{i,j}\}_{i,j})$ spans $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$.

Now by Lemma 3.1.5 the g^2 extension classes defining $\mathcal{L}$ are syntomic. So $\mathcal{L}$ arises from an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g as finite flat group schemes over $\tilde{Y}$. If we denote by $(d_{i,j})$ the corresponding $g \times g$ matrix of elements of $\mathrm{Ext}^1_{\tilde{Y}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$, then Lemma 3.1.4, together with the fact that $f^*\mathcal{L} \xrightarrow{\sim} \mathcal{A}_R[p]|_X$, implies that $f^*(d_{i,j}) = c_{i,j}$. It follows that the elements $\theta_A(f^*(\{d_{i,j}\}))_{i,j}$ span $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$, which implies that f is an isomorphism by Lemma 3.1.7. □

3.2.5. Fix an integer $g \geq 1$, a prime $p \geq 2$, and a positive integer $N \geq 2$ coprime to p. Consider the ring $\mathbb{Z}[\zeta_N][1/N]$, where ζ_N is a primitive Nth root of 1. Using the isomorphism $\mathbb{Z}/N\mathbb{Z} \xrightarrow[1 \mapsto \zeta_N]{\sim} \mu_N$, for any $\mathbb{Z}[\zeta_N][1/N]$-scheme T, and any principally polarized abelian scheme A over T, the N-torsion scheme $A[N]$ is equipped with the (alternating) Weil pairing

$$A[N] \times A[N] \to \mathbb{Z}/N\mathbb{Z}.$$

We denote by $\mathcal{A}_{g,N}$ the $\mathbb{Z}[\zeta_N][1/N]$-scheme which is the coarse moduli space of principally polarized abelian schemes A of dimension g equipped with a symplectic basis of $A[N]$. When $N \geq 3$, this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_N][1/N]$. For a $\mathbb{Z}[\zeta_N][1/N]$-algebra B, we denote by $\mathcal{A}_{g,N/B}$ the base change of $\mathcal{A}_{g,N}$ to B. If no confusion is likely to result we sometimes denote this base change simply by $\mathcal{A}_{g,N}$.

Suppose that $N \geq 3$, and let $\mathcal{A} \to \mathcal{A}_{g,N}$ be the universal abelian scheme. The p-torsion subgroup $\mathcal{A}[p] \subset \mathcal{A}$ is a finite flat group scheme over $\mathcal{A}_{g,N}$ which is étale over $\mathbb{Z}[\zeta_N][1/Np]$. Let $x \in \mathcal{A}_{g,N}$ be a point with residue field $\kappa(x)$ of characteristic p, and $\mathcal{A}_x$ the corresponding abelian variety over $\kappa(x)$. The set of points x such that $\mathcal{A}_x$ is ordinary is an open subscheme $\mathcal{A}_{g,N}^{\mathrm{ord}} \subset \mathcal{A}_{g,N} \otimes \mathbb{F}_p$. For any N, we denote by $\mathcal{A}_{g,N}^{\mathrm{ord}} \subset \mathcal{A}_{g,N} \otimes \mathbb{F}_p$ the image of $\mathcal{A}_{g,NN'}$ for any $N' \geq 3$ coprime to N and p.

We now denote by k a perfect field of characteristic p, and $K/W[1/p]$ a finite extension with ring of integers $\mathcal{O}_K$ and uniformizer π. We assume that K is equipped with a choice of primitive

https://doi.org/10.1112/S0010437X21007594

Nth root of 1, $\zeta_N \in K$. We remind the reader regarding the convention for the definition of $\overline{\mathrm{ed}}$ and $\overline{\mathrm{ed}}(\,\cdot\,;p)$ introduced in 2.2.6.

THEOREM 3.2.6. *Let $g \geq 1$ and let p be any prime. Let $N \geq 3$ and coprime to p, and let*

$$\iota : \mathcal{Z} \to \mathcal{A}_{g,N/\mathcal{O}_K}$$

be a map of equidimensional, smooth $\mathcal{O}_K$-schemes, satisfying the following conditions.

(i) *If $x \in \mathcal{Z}$ is a closed point with image $y \in \mathcal{A}_{g,N/\mathcal{O}_K}$, then ι induces a surjection of complete local rings $\widehat{\mathcal{O}}_{\mathcal{A}_{g,N/\mathcal{O}_K},y} \twoheadrightarrow \widehat{\mathcal{O}}_{\mathcal{Z},x}$.*

(ii) *The image, under ι, of the special fiber $\mathcal{Z}_k$ meets the ordinary locus $\mathcal{A}^{\mathrm{ord}}_{g,N} \subset \mathcal{A}_{g,N/k}$.*

Then

$$\overline{\mathrm{ed}}(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K;p) = \dim \mathcal{Z}_K.$$

Proof. It suffices to prove the theorem when k is algebraically closed, which we assume from now on. Moreover, since K is an arbitrary finite extension of $W[1/p]$, it is enough to show that $\mathrm{ed}_K(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K;p) = \dim \mathcal{Z}_K$. We may replace $\mathcal{Z}$ by a component whose special fiber meets the ordinary locus, and assume that $\mathcal{Z}_K$ and $\mathcal{Z}_k$ are geometrically connected.

Suppose that $\overline{\mathrm{ed}}(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K;p) < \dim \mathcal{Z}_K$. Then there exists a dominant, generically finite map $U_K \to \mathcal{Z}_K$ of degree prime to p at the generic points of U_K, and a map $h : U_K \to Y_K$ to a finite type K-scheme Y_K with $\dim Y_K < \dim \mathcal{Z}_K$, such that $\mathcal{A}[p]|_{U_K}$ arises as the pullback of a finite étale covering of Y_K. We may assume that Y_K is the scheme-theoretic image of U_K under h. Next, after replacing both U_K and Y_K by dense affine opens, we may assume that both these schemes are affine corresponding to K-algebras B_K and C_K respectively, and that $U_K \to Y_K$ is flat.

Let $\tilde{\mathcal{Z}}$ be the normalization of $\mathcal{Z}$ in U_K. Let $\mathfrak{p}$ be the generic point of $\mathcal{Z}_k$, and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ the primes of $\tilde{\mathcal{Z}}$ over $\mathfrak{p}$. Since the degree of $\tilde{\mathcal{Z}} \to \mathcal{Z}$ over $\mathfrak{p}$ is prime to p, for some i the ramification degree $e(\mathfrak{q}_i/\mathfrak{p})$ and the degree of the residue field extension $\kappa(\mathfrak{q}_i)/\kappa(\mathfrak{p})$ are prime to p. In particular, the residue field extension is separable. By Abhyankar's Lemma, it follows that, after replacing K by a finite extension, we may assume that $e(\mathfrak{q}_i/\mathfrak{p}) = 1$ for some i, and that $\tilde{\mathcal{Z}} \to \mathcal{Z}$ is étale at $\mathfrak{q}_i$. Shrinking U_K further if necessary, we may assume that there is an affine open $\operatorname{Spec} B = U \subset \tilde{\mathcal{Z}}$ such that $U_k \to \mathcal{Z}_k$ has dense image, $U \otimes K = U_K$, and $U \to \mathcal{Z}$ is étale. In particular, U is smooth over $\mathcal{O}_K$.

Now choose a finitely generated $\mathcal{O}_K$-subalgebra $C \subset C_K \cap B$ such that $C \otimes K = C_K$. This is possible as C_K is finitely generated over K. Then h extends to a map $h : U \to Y = \operatorname{Spec} C$. Let $J \supset (p)$ be an ideal of C, and $Y_J \to Y$ the blow-up of J. Denote by U_J the proper transform of U by this blow-up. That is, U_J is the closure of U_K in $U \times Y_J$. By the Raynaud–Gruson Flattening Theorem [RG71, Theorem 5.2.2], we can choose J so that $U_J \to Y_J$ is flat. Since U is normal, the map $U_J \to U$ is an isomorphism over the generic points of $U \otimes k$. Hence, after replacing Y by an affine open in Y_J, and shrinking U, we may assume that $U \to Y$ is flat.

Shrinking U further, we may assume that the special fiber U_k maps to the ordinary locus of $\mathcal{A}_{g,N}$. Now let $\widehat{B}$ and $\widehat{C}$ denote the p-adic completions of B and C respectively, and set $\widehat{U} = \operatorname{Spec} \widehat{B}$ and $\widehat{Y} = \operatorname{Spec} \widehat{C}$.[2] Since $\mathcal{A}[p]|_{\widehat{U}}$ is ordinary, there is a finite étale covering $\widehat{U}' = \operatorname{Spec} \widehat{B}' \to \widehat{U}$ such that $\mathcal{A}[p]|_{\widehat{U}'}$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g. Hence by Lemmas 2.1.6 and

[2] Although it would in some sense be more natural to work with formal schemes here, we stay in the world of affine schemes so as to be able to apply the results proved in § 1, and to deal with generic fibers without resorting to p-adic analytic spaces.

https://doi.org/10.1112/S0010437X21007594

2.1.8, $\widehat{U}'_K \to \widehat{Y}_K$ factors through a finite étale map $\widehat{Y}'_K \to \widehat{Y}_K$ such that $\mathcal{A}[p]|_{\widehat{U}'_K}$ is the pullback of an extension $\mathcal{F}'$ of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g on $\widehat{Y}'_K$. As $\widehat{U}'$ is normal, we may assume $\widehat{Y}'_K$ is normal.

Let $\widehat{Y}' = \operatorname{Spec} \widehat{C}'$ be the normalization of $\widehat{Y}$ in $\widehat{Y}'_K$. As $\widehat{U}'$ is normal, we have

$$\widehat{U}' \to \widehat{Y}' \to \widehat{Y}.$$

As $\widehat{Y}'$ is normal, $\widehat{U}' \to \widehat{Y}'$ is flat over the generic points of $\widehat{Y}'_k$. Hence, there exists $f_0 \in \widehat{C}'/\pi\widehat{C}'$ which is nowhere nilpotent on $\widehat{Y}'_k$, and such that $\widehat{U}'_k \to \widehat{Y}'_k$ is flat over the complement of the support of the ideal (f_0). Now let $f \in \widehat{C}'$ be a lift of f_0, and let $\widehat{C}'' = \widehat{C'[1/f]}$ and $\widehat{B}'' = \widehat{B'[1/f]}$, the p-adic completions[3] of $C'[1/f]$ and $B'[1/f]$. Let $\widehat{U}'' = \operatorname{Spec} B''$ and $\widehat{Y}'' = \operatorname{Spec} \widehat{C}''$. Then $\widehat{U}''$ is flat over $\widehat{Y}''$ by [EGA, IV, 11.3.10.1]. Moreover, since $\widehat{U} \to \widehat{Y}$ is flat, the generic points of $\widehat{U}'_k$ map to generic points of $\widehat{Y}'_k$. So the image of $\widehat{U}''_k$ is dense in $\widehat{U}'_k$, and in particular $\widehat{U}''(k)$ is nonempty.

Now choose a point $x \in \widehat{U}''(k)$, and denote by $y \in \widehat{Y}''(k)$ its image. We write $\mathcal{O}_{\widehat{U}'',x}$ and $\mathcal{O}_{\widehat{Y}'',y}$ for the complete local rings at x and y. Since the maps

$$\widehat{U}'' \to \widehat{U}' \to \widehat{U} \to \mathcal{Z}$$

are formally étale, $\mathcal{O}_{\widehat{U}'',x}$ is naturally isomorphic to the complete local ring at the image of x in $\mathcal{Z}$. Let R be the universal deformation $\mathcal{O}_K$-algebra of the abelian scheme $\mathcal{A}_x$. By condition (i) of the theorem, $\mathcal{O}_{\widehat{U}'',x}$ is naturally a quotient of R. The map $\mathcal{O}_{\widehat{Y}'',y} \to \mathcal{O}_{\widehat{U}'',x}$ satisfies the conditions of Lemma 3.2.4 (cf. [EGA, IV, 17.5.3]), and it follows that this map is an isomorphism. In particular, this implies that

$$\dim Y_K = \dim \mathcal{O}_{\widehat{Y}'',y} - 1 = \dim \mathcal{O}_{\widehat{U}'',x} - 1 = \dim \mathcal{Z}_K$$

which contradicts our initial assumption. □

Corollary 3.2.7. *Let $g \geq 1$, be an integer, p any prime, and $N \geq 1$ an integer coprime to p. Let*

$$\iota : \mathcal{Z} \to \mathcal{A}_{g,N/\mathcal{O}_K}$$

be a map of equidimensional, smooth $\mathcal{O}_K$-schemes satisfying conditions (i) and (ii) of Theorem 3.2.6.

If $N = 1, 2$ we also assume the following condition: For any generic point $\eta \in \mathcal{Z}_k$, and $\bar{\eta}$ the spectrum of an algebraic closure of $\kappa(\eta)$, the abelian variety $\mathcal{A}_{\bar{\eta}}$ over $\bar{\eta}$, has automorphism group equal to $\{\pm 1\}$. Then

$$\overline{\operatorname{ed}}(\mathcal{A}_{g,pN}|_{\mathcal{Z}_K}/\mathcal{Z}_K; p) = \dim \mathcal{Z}_K.$$

Proof. If $N \geq 3$, the corollary follows from Theorem 3.2.6 and Lemma 2.2.4.

Suppose $N = 1$ or 2. Let $N' \geq 3$ be an integer coprime to pN. We may assume that K is equipped with a primitive pN'th root of 1, $\zeta_{pN'}$. The map of K-schemes $\mathcal{A}_{g,pN} \to \mathcal{A}_{g,N}$, is a covering with group $\operatorname{Sp}_{2g}(\mathbb{F}_p)/\{\pm 1\}$. Consider the maps

$$\mathcal{A}_{g,pNN'} \to \mathcal{A}_{g,pN} \times_{\mathcal{A}_{g,N}} \mathcal{A}_{g,NN'} =: \mathcal{A}'_{g,pNN'} \to \mathcal{A}_{g,NN'}.$$

Then $\mathcal{A}'_{g,pNN'} \to \mathcal{A}_{g,NN'}$ again corresponds to a $\operatorname{Sp}_{2g}(\mathbb{F}_p)/\{\pm 1\}$ covering, and $\mathcal{A}_{g,pNN'} \to \mathcal{A}_{g,NN'}$ corresponds to a $\operatorname{Sp}_{2g}(\mathbb{F}_p)$ covering. When $p = 2$ these two coverings coincide.

Let $\mathcal{Z}_{N'} = \mathcal{Z} \times_{\mathcal{A}_{g,N}} \mathcal{A}_{g,NN'}$. Our assumption on the automorphisms of $\mathcal{A}_{\bar{\eta}}$ implies that at the generic points of $\mathcal{Z}_k$, the map $\mathcal{Z}_{N'} \to \mathcal{Z}$ is étale. Thus, after replacing $\mathcal{Z}$ by a fiberwise dense

[3] $\widehat{C}''$ corresponds to a formal affine open in the formal scheme $\operatorname{Spf} \widehat{C}'$.

https://doi.org/10.1112/S0010437X21007594

open, we may assume that $\mathcal{Z}_{N'}$ is smooth over $\mathcal{O}_K$. The observations of the previous paragraph, Lemma 2.2.7 when $p > 2$, Lemma 2.2.4 and Theorem 3.2.6 imply that we have

$$\begin{aligned}\overline{\mathrm{ed}}(\mathcal{A}_{g,pN}|_{\mathcal{Z}_K}/\mathcal{Z}_K;p) &\geq \overline{\mathrm{ed}}(\mathcal{A}'_{g,pNN'}|_{\mathcal{Z}_{N',K}}/\mathcal{Z}_{N',K};p)\\ &= \overline{\mathrm{ed}}(\mathcal{A}_{g,pNN'}|_{\mathcal{Z}_{N',K}}/\mathcal{Z}_{N',K};p)\\ &= \overline{\mathrm{ed}}(\mathcal{A}[p]|_{\mathcal{Z}_{N',K}}/\mathcal{Z}_{N',K};p)\\ &= \dim \mathcal{Z}_K. \end{aligned} \tag{3.2.8}$$

□

COROLLARY 3.2.9. *Let $g, n \geq 2$ and N a positive integer coprime to n. Consider the finite étale map of $\mathbb{Q}(\zeta_{nN})$-schemes $\mathcal{A}_{g,nN} \to \mathcal{A}_{g,N}$. Then for any $p|n$, we have*

$$\overline{\mathrm{ed}}(\mathcal{A}_{g,nN}/\mathcal{A}_{g,N};p) = \dim \mathcal{A}_g = \binom{g+1}{2}.$$

Proof. *A fortiori* it suffices to consider the case when $n = p$ is prime, which is a special case of Corollary 3.2.7. □

3.3 Moduli spaces of curves

Using the Torelli theorem one can use Theorem 3.2.6 to deduce the essential p-dimension of certain coverings of families of curves.

3.3.1. Let $g \geq 2$, and let $\mathcal{M}_g$ denote the coarse moduli space of smooth, proper, genus g curves. For any integer n, let $\mathcal{M}_g[n]$ denote the $\mathbb{Z}[\zeta_n][1/n]$-scheme which is the coarse moduli space of pairs $(C, \mathcal{B})$ consisting of a proper smooth curve C of genus g together with a choice $\mathcal{B}$ of symplectic basis for $J(C)[n]$, where $J(C)$ denotes the Jacobian of C. For $n \geq 3$ this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_n][1/n]$ [DM69].

THEOREM 3.3.2. *Let $g, n \geq 2$, and let p be any prime dividing n. Then*

$$\overline{\mathrm{ed}}(\mathcal{M}_g[n]/\mathcal{M}_g;p) = \dim \mathcal{M}_g = 3g-3.$$

Proof. Let $N \geq 3$ be an integer. There is a natural map of $\mathbb{Z}[\zeta_N][1/N]$-schemes $\varpi : \mathcal{M}_g[N] \to A_{g,N}$ taking a curve to its Jacobian. For $(C, \mathcal{B})$ in $\mathcal{M}_g[N]$ the pairs $(J(C), \mathcal{B})$ and $(J(C), -\mathcal{B})$ are isomorphic via -1 on $J(C)$. Thus $(C, \mathcal{B}) \mapsto (C, -\mathcal{B})$ is an involution Σ of $\mathcal{M}_g[N]$, which is nontrivial, unless $g = 2$. We denote by $\mathcal{M}_g[N]'$ the quotient of $\mathcal{M}_g[N]$ by this involution. When $g \geq 3$, the fixed points of Σ in any fiber of $\mathcal{M}_g[N]$ over $\operatorname{Spec} \mathbb{Z}[\zeta_N][1/N]$ are contained in a proper closed subset. Thus $\mathcal{M}_g[N]'$ is generically smooth over every point of $\operatorname{Spec} \mathbb{Z}[\zeta_N][1/N]$.

By [OS80, 1.11, 2.7, 2.8], the map of $\mathbb{Z}[\zeta_N][1/N]$-schemes $\mathcal{M}_g[N] \to \mathcal{A}_{g,N}$ induces a map $\mathcal{M}_g[N]' \to \mathcal{A}_{g,N}$ which is injective, an immersion if $g = 2$ and an immersion outside the hyperelliptic locus if $g \geq 3$.

It suffices to prove the theorem with n replaced by the prime factor p. Let $N \geq 3$ be coprime to p, and let $\mathcal{M}_g[pN]'' = \mathcal{M}_g[p] \times_{\mathcal{M}_g} \mathcal{M}_g[N]'$. It is enough to show that $\overline{\mathrm{ed}}(\mathcal{M}_g[pN]''/\mathcal{M}_g[N]';p) = 3g-3$. If $p = 2$ then $\mathcal{M}_g[pN]'' = \mathcal{M}_g[pN]'$ as coverings of $\mathcal{M}_g[N]'$, and if $p \geq 3$ we have natural degree 2 maps of coverings of $\mathcal{M}_g[N]'$,

$$\mathcal{M}_g[pN]'' \leftarrow \mathcal{M}_g[pN] \to \mathcal{M}_g[pN]'.$$

Thus, using Lemma 2.2.7 when $p \geq 3$, it suffices to show that

$$\overline{\mathrm{ed}}(\mathcal{M}_g[pN]'/\mathcal{M}_g[N]';p) = 3g-3.$$

https://doi.org/10.1112/S0010437X21007594

Since $\mathcal{M}_g[pN]' = \mathcal{A}_{g,pN}|_{\mathcal{M}_g[N]'}$, for example by comparing the degrees of these coverings, and $\mathcal{M}_g[N]'$ meets the ordinary locus in $\mathcal{A}_{g,N} \otimes \mathbb{F}_p$ [FvdG04, 2.3], the theorem now follows from Theorem 3.2.6. □

3.3.3. We now prove the analogue of Theorem 3.3.2 for the moduli space of hyperelliptic curves. Let S be a $\mathbb{Z}[1/2]$-scheme. Recall that a *hyperelliptic curve* over S is a smooth proper curve C/S of genus $g \geq 1$, equipped with an involution σ such that $P = C/\langle\sigma\rangle$ has genus 0. Let $\mathcal{H}_g$ denote the coarse moduli space of genus g hyperelliptic curves over $\mathbb{Z}$. It is classical (and not hard to see) that over $\mathbb{Z}[1/2]$ one has

$$\mathcal{H}_g \cong \mathcal{M}_{0,2g+2}/S_{2g+2}$$

where $\mathcal{M}_{0,2g+2}$ is the moduli space of genus 0 curves with $2g+2$ ordered marked points, and S_{2g+2} is the symmetric group on $2g+2$ letters.

For any integer n, let $\mathcal{H}_g[n]$ denote the $\mathbb{Z}[\zeta_n][1/n]$-scheme which is the coarse moduli space of pairs $(C, \mathcal{B})$ consisting of a hyperelliptic curve C together with a symplectic basis $\mathcal{B}$ for $J(C)[n]$. As above, for $n \geq 3$ this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_n][1/n]$.

Theorem 3.3.4. *Let $g, n \geq 2$, and let p be any odd prime dividing n. Then*

$$\overline{\mathrm{ed}}(\mathcal{H}_g[n]/\mathcal{H}_g; p) = \dim \mathcal{H}_g = 2g - 1.$$

Proof. There is a natural map of $\mathbb{Z}[1/2]$-schemes $\mathcal{H}_g \to \mathcal{M}_g$ which is generically an injective immersion on every fiber over $\mathbb{Z}[1/2]$, as a general hyperelliptic curve has only one nontrivial automorphism [Poo00, Theorem 1]. By the Torelli theorem and [OS80, Corollary 3.2], the map $\mathcal{M}_g \to \mathcal{A}_g$ is also generically an injective immersion on every fiber over $\mathbb{Z}[1/2]$, and thus so is $\mathcal{H}_g \to \mathcal{A}_g$.

Now the Jacobian of a hyperelliptic curve over the generic point of $\mathcal{H}_g$ has automorphism group $\{\pm 1\}$ [Mat58, p. 790], and $\mathcal{H}_g$ meets the ordinary locus of $\mathcal{A}_g \otimes \mathbb{F}_p$ by [GP05, Theorem 1]. Hence the theorem follows from Corollary 3.2.7. □

3.3.5. We remark that when $g = 2$, Theorem 3.3.4 extends to $p = 2$, as this is a special case of Theorem 3.3.2. However, an extension to $p = 2$ is not possible when $g > 2$. To explain this, recall that for a finite group G and a prime p, $\overline{\mathrm{ed}}(G; p)$ denotes the supremum of $\mathrm{ed}_K(Y/X; p)$ taken over all G-covers Y/X of finite type K-schemes, for any algebraically closed field K of characteristic 0 (the definition being independent of K). The covering

$$\mathcal{M}_{0,2g+2} \to \mathcal{M}_{0,2g+2}/S_{2g+2} \xrightarrow{\sim} \mathcal{H}_g$$

is a component of $\mathcal{H}_g[2]$; for $g > 2$, the cover is disconnected, and all components are isomorphic.[4] We conclude that

$$\begin{aligned}\overline{\mathrm{ed}}(\mathcal{H}_g[2]/\mathcal{H}_g; 2) &= \overline{\mathrm{ed}}(\mathcal{M}_{0,2g+2}/\mathcal{H}_g; 2)\\ &= \overline{\mathrm{ed}}(S_{2g+2}; 2)\\ &= g + 1 < 2g - 1\end{aligned}$$

where the second equality follows from the versality of $\mathcal{M}_{0,2g+2}$ for S_{2g+2}, and the third follows from [MR09, Cor. 4.2].

[4] The monodromy of $\mathcal{H}_g[2] \to \mathcal{H}_g$ was computed by Jordan [Jo1870, p. 364, § 498] to factor as $SB_{2g+2} \twoheadrightarrow S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_2)$, where $SB_{2g+2} = \pi_1(\mathcal{H}_g)$ denotes the spherical braid group. See also [Dic08, p. 125], or for a more recent treatment, see the $q = 2$ case of [McM13, Theorem 5.2]. The connected components of the cover are in bijection with the cosets $\mathrm{Sp}_{2g}(\mathbb{F}_2)/S_{2g+2}$. The equivalence of the components follows from the monodromy computation.

The lower bound $\overline{\mathrm{ed}}(\mathcal{H}_g[2]/\mathcal{H}_g; 2) \geq g+1$ can actually be recovered using the techniques of this paper. The point is that although $\mathcal{H}_g \to \mathcal{A}_g$ is not generically an immersion in characteristic 2, one can show that the image of the map on tangent spaces at a generic point has dimension $g+1$. We are grateful to Aaron Landesman for showing us this calculation [Lan19].

4. Essential dimension of congruence covers

4.1 Forms of reductive groups

In this subsection we prove a variant of a result of Harder and Borel showing that, under some mild conditions, for a reductive group over a number field one can always find a form with given specializations at finitely many places.

4.1.1. Let F be a number field and $G = G^{\mathrm{ad}}$ an adjoint, connected reductive group over F. We fix algebraic closures $\bar{F}$ and $\bar{F}_v$ of F and F_v respectively, for every finite place v of F, as well as embeddings $\bar{F} \hookrightarrow \bar{F}_v$.

Recall [SGA3, XXIV, Theorem 1.3] that the *automorphism group scheme* of G is an extension

$$1 \to G \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \tag{4.1.2}$$

where $\mathrm{Out}(G)$ is a finite group scheme. If G is split, then this extension is split and $\mathrm{Out}(G)$ is a constant group scheme which can be identified with the group of automorphisms of the Dynkin diagram of G.

We will also make use of the notion of the *fundamental group* $\pi_1(G)$ [Bor96]. This is a finite abelian group equipped with a $\mathrm{Gal}(\bar{F}/F)$-action. As an étale sheaf on $\mathrm{Spec}\, F$, one has $\pi_1(G) \otimes \mu_n \xrightarrow{\sim} \ker(G^{\mathrm{sc}} \to G)$ where G^{sc} is the simply connected cover of G, and n is the order $\ker(G^{\mathrm{sc}} \to G)$. The following proposition is a variant of [HB78, Theorem B].

PROPOSITION 4.1.3. *Let G be a split, adjoint connected reductive group over F, and S a finite set of places of F. Let $\mathrm{Out}(G)' \subset \mathrm{Out}(G)$ be a subgroup and $\mathrm{Aut}'(G) \subset \mathrm{Aut}(G)$ the preimage of $\mathrm{Out}(G)'$. If the map of pointed sets*

$$H^1(F, \mathrm{Out}(G)') \to \prod_{v \in S} H^1(F_v, \mathrm{Out}(G)')$$

is surjective, then the natural map of pointed sets

$$H^1(F, \mathrm{Aut}(G)') \to \prod_{v \in S} H^1(F_v, \mathrm{Aut}(G)')$$

is surjective.

Proof. Recall the following facts about the cohomology of reductive groups over global and local fields [Kot86]: Let H be an adjoint connected reductive group over F. For any place v of F, there is a map

$$H^1(F_v, H) \to \pi_1(H)_{\mathrm{Gal}(\bar{F}_v/F_v)},$$

which is an isomorphism if v is finite. For any finite set of places T of F, consider the composite map

$$\xi : \prod_{v \in T} H^1(F_v, H) \to \prod_{v \in T} \pi_1(H)_{\mathrm{Gal}(\bar{F}_v/F_v)} \to \pi_1(H)_{\mathrm{Gal}(\bar{F}/F)}.$$

https://doi.org/10.1112/S0010437X21007594

Then by [Kot86, § 2.2], $(x_v)_{v\in T} \in \prod_{v\in T} H^1(F_v, H)$ is in the image of $H^1(F, H)$ if $\xi((x_v)) = 0$. Applying this to $T = S \cup \{v_0\}$ for some finite place $v_0 \notin S$, we see that

$$H^1(F, H) \to \prod_{v\in S} H^1(F_v, H) \tag{4.1.4}$$

is surjective.

Now let $(x_v) \in \prod_{v\in S} H^1(F_v, \mathrm{Aut}(G)')$ and let $(\bar{x}_v) \in \prod_{v\in S} H^1(F_v, \mathrm{Out}(G)')$ be the image of (x_v). By our assumptions on $\mathrm{Out}(G)'$, there exists $\bar{x} \in H^1(F, \mathrm{Out}(G)')$ mapping to $(\bar{x}_v)$. Since we are assuming G is split, (4.1.2) is a split extension, so there is a $x \in H^1(F, \mathrm{Aut}(G)')$ mapping to $\bar{x}$. Let H be the twist of G by x. Recall that this means that if we choose a cocycle $x = (x_\sigma)_{\sigma\in \mathrm{Gal}(\bar{F}/F)}$ representing x, then there is an isomorphism $\tau : G \xrightarrow{\sim} H$ over $\bar{F}$, such that, for $g \in G(\bar{F})$ and $\sigma \in \mathrm{Gal}(\bar{F}/F)$, we have $\tau(\sigma(g)) = (\sigma(\tau(g)))^{x_\sigma}$. We have a commutative diagram

$$\begin{array}{ccc} H^1(F, \mathrm{Aut}(G)) & \longrightarrow & \prod_{v\in S} H^1(F_v, \mathrm{Aut}(G)) \\ {\scriptstyle\tau}\downarrow{\scriptstyle\sim} & & {\scriptstyle\tau|F_v}\downarrow{\scriptstyle\sim} \\ H^1(F, \mathrm{Aut}(H)) & \longrightarrow & \prod_{v\in S} H^1(F_v, \mathrm{Aut}(H)) \end{array}$$

such that the vertical maps send x and $(x|_{F_v})_v$ to the trivial classes in the bottom line. Thus it suffices to show that

$$H^1(F, H) \to \prod_{v\in S} H^1(F_v, H)$$

is surjective, which we saw above. □

Corollary 4.1.5. *Let G, S, $\mathrm{Out}(G)'$ and $\mathrm{Aut}(G)'$ be as in Proposition 4.1.3. Suppose that $\mathrm{Out}(G)'$ is an abelian group, and let 2^s be the largest power of 2 such that $\mathrm{Out}(G)'$ has an element of order 2^s. If $v \in S$ with $v|2$ we assume that $F_v(\zeta_{2^s})/F_v$ is cyclic, where ζ_{2^s} is a primitive 2^s root of 1.*

Then

$$H^1(F, \mathrm{Aut}(G)') \to \prod_{v\in S} H^1(F_v, \mathrm{Aut}(G)')$$

is surjective.

Proof. By Proposition 4.1.3, it suffices to show that

$$H^1(F, \mathrm{Out}(G)') \to \prod_{v\in S} H^1(F_v, \mathrm{Out}(G)')$$

is surjective. The elements of $H^1(F, \mathrm{Out}(G))$ are in bijection with conjugacy classes of maps $\mathrm{Gal}(\bar{F}/F) \to \mathrm{Out}(G)$, and similarly for the local classes, so this follows from [Sal82, Theorem 5.10]. Note the condition there, that $F_v(\zeta_{2^s})/F_v$ is cyclic is automatic unless $v|2$, as otherwise this is an unramified extension. □

4.2 Shimura varieties

In this subsection we apply the results of § 3 to compute the essential dimension for congruence covers of Shimura varieties. This will be applied in the next subsection to give examples of congruence covers of locally symmetric varieties where our techniques give a lower bound on the essential dimension. Since our aim is to give lower bounds on essential dimension, it may seem odd that we work with the formalism of Shimura varieties rather than the locally symmetric

varieties which are their geometrically connected components. However, many of the results we need are in the literature only in the former language, and it would take more effort to make the (routine) translation.

4.2.1. Recall [Del79, § 1.2] that a *Shimura datum* is a pair (G, X) consisting of a connected reductive group G over $\mathbb{Q}$, and a $G(\mathbb{R})$ conjugacy class of maps of algebraic groups over $\mathbb{R}$:

$$h : \mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m \to G.$$

This datum is required to satisfy certain properties which imply that the commutant of $h(\mathbb{S}(\mathbb{R}))$ is a subgroup $K_\infty \subset G(\mathbb{R})$ whose image in $G^{\mathrm{ad}}(\mathbb{R})$ is maximal compact and $X = G(\mathbb{R})/K_\infty$ is a union of finitely many Hermitian symmetric domains.

Let $\mathbb{A}$ denote the adeles over $\mathbb{Q}$ and $\mathbb{A}_f$ the finite adeles. Let $K \subset G(\mathbb{A}_f)$ be a compact open subgroup. Recall that K is called *neat* if $G(\mathbb{Q}) \cap gKg^{-1}$ contains no torsion elements for all $g \in G(\mathbb{A}_f)$, and that sufficiently small compact open subgroups are neat. The conditions on (G, X) imply that if K is neat, the quotient

$$\mathrm{Sh}_K(G, X) = G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$$

has a natural structure of (the complex points of) an algebraic variety over a number field $E = E(G, X) \subset \mathbb{C}$, called the reflex field of (G, X), which does not depend on K. We denote this algebraic variety by the same symbol, $\mathrm{Sh}_K(G, X)$, and we assume from now on that K is neat.

Now let $V_{\mathbb{Z}} = \mathbb{Z}^{2g}$ equipped with a perfect symplectic form ψ. Set $V = V_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathrm{GSp} = \mathrm{GSp}(V, \psi)$. As in [Del79, 1.3.1], we denote by $S^{\pm}$ the conjugacy class of maps $h : \mathbb{S} \to \mathrm{GSp}$ satisfying the following two properties

(i) The action of the real Lie group $\mathbb{S}(\mathbb{R}) = \mathbb{C}^\times$ on $V_{\mathbb{C}}$ gives rise to a Hodge structure of type $(-1, 0)$ $(0, -1)$:

$$V_{\mathbb{C}} \xrightarrow{\sim} V^{-1,0} \oplus V^{0,-1}.$$

(ii) The pairing $(x, y) \mapsto \psi(x, h(i)y)$ on $V_{\mathbb{R}}$ is positive or negative definite.

Then $(\mathrm{GSp}, S^{\pm})$ is a Shimura datum called the *Siegel datum*, and $\mathrm{Sh}_K(\mathrm{GSp}, S^{\pm})$ has an interpretation as the moduli space of principally polarized abelian varieties with suitable level structure.

We say that (G, X) is of *Hodge type* if there is a map of reductive groups over $\mathbb{Q}$, $\iota : G \hookrightarrow \mathrm{GSp}$, which induces $X \to S^{\pm}$. By [Del71, Prop. 1.15], there exists a neat compact open $K' \subset \mathrm{GSp}(\mathbb{A}_f)$ such that $K = K' \cap G(\mathbb{A}_f)$, and ι induces a closed embedding of Shimura varieties

$$\mathrm{Sh}_K(G, X) \hookrightarrow \mathrm{Sh}_{K'}(\mathrm{GSp}, S^{\pm}).$$

Our conditions on K and K' imply that the right hand side carries a universal abelian scheme.

4.2.2. Now fix a prime p, and suppose that G is the generic fiber of a reductive group $G_{\mathbb{Z}_{(p)}}$ over $\mathbb{Z}_{(p)}$. If no confusion is likely to result we will sometimes write simply G for $G_{\mathbb{Z}_{(p)}}$. We take K (still assumed neat) to be of the form K_pK^p where $K_p = G(\mathbb{Z}_p)$ and $K^p \subset G(\mathbb{A}_f^p)$, where $\mathbb{A}_f^p$ denotes the finite adeles with trivial p-component.

Under these conditions, p is unramified in E, and for any prime $\lambda|p$ of E, $\mathrm{Sh}_K(G, X)$ has a canonical smooth model over $\mathcal{O}_{E_\lambda}$ [Kis10, Theorem 2.3.8], [KMP16, Theorem 1], which we will denote by $\mathscr{S}_K(G, X)$. In particular, we may apply this to $\mathrm{Sh}_{K'}(\mathrm{GSp}, S^{\pm})$ if we take $K' = K'_pK'^p$ with $K'_p = \mathrm{GSp}(V_{\mathbb{Z}}, \psi)(\mathbb{Z}_p)$.

https://doi.org/10.1112/S0010437X21007594

Given $G_{\mathbb{Z}_{(p)}}$ and (G, X) of Hodge type, we may always choose (V, ψ), ι and K' with $K'_p = \mathrm{GSp}(V_{\mathbb{Z}}, \psi)(\mathbb{Z}_p)$, such that $K = K' \cap G(\mathbb{A}_f)$, ι induces a map of smooth $\mathcal{O}_{E_\lambda}$-schemes

$$\iota : \mathscr{S}_K(G, X) \to \mathscr{S}_{K'}(\mathrm{GSp}, S^{\pm})$$

and for any closed point $x \in \mathscr{S}_K(G, X)$, the complete local ring at x is a quotient of the complete local ring at $\iota(x)$ - see [Kis10, Lem. 2.1.2, Prop. 2.3.5] when $p > 2$, and [KMP16, Prop. 3.6] and its proof for the case $p = 2$.

As in § 3, we denote by $\mathcal{A}$ the universal abelian scheme over $\mathscr{S}_{K'}(\mathrm{GSp}, S^{\pm})$. Then we have

Lemma 4.2.3. *Let $K_1 = K^p K_{1,p}$ where $K_{1,p} = \ker(G(\mathbb{Z}_p) \to G(\mathbb{F}_p)) \subset K_p$. Over any finite extension E'/E, the congruence cover*

$$\mathrm{Sh}_{K_1}(G, X) \to \mathrm{Sh}_K(G, X)$$

is a union of copies of Galois closures of the étale local system $\mathcal{A}[p]|_{\mathrm{Sh}_K(G,X)}$ on $\mathrm{Sh}_K(G, X)$.

If E, admits a prime $\lambda|p$ with residue field $\mathbb{F}_p$ then

$$\overline{\mathrm{ed}}(\mathrm{Sh}_{K_1}(G, X) \to \mathrm{Sh}_K(G, X); p) = \dim_{\mathbb{C}} X.$$

Proof. Write $\mathrm{Sh}_K = \mathrm{Sh}_K(G, X)$ and $\mathrm{Sh}_{K_1} = \mathrm{Sh}_{K_1}(G, X)$. Our assumptions imply that K/K_1 acts freely on Sh_{K_1}, so that $\mathrm{Sh}_{K_1} \to \mathrm{Sh}_K$ is a $K/K_1 = G(\mathbb{F}_p)$-torsor. As $G(\mathbb{F}_p)$ acts faithfully on the fibers of $\mathcal{A}[p]|_{\mathrm{Sh}_K}$, this implies the first claim. By Lemma 2.2.4 applied to the geometrically connected components of Sh_K, we then have

$$\overline{\mathrm{ed}}(\mathrm{Sh}_{K_1}(G, X) \to \mathrm{Sh}_K(G, X); p) = \overline{\mathrm{ed}}(\mathcal{A}[p]|_{\mathrm{Sh}_K}/\mathrm{Sh}_K; p).$$

Now suppose that E admits a prime $\lambda|p$ with residue field $\mathbb{F}_p$, and consider the map of integral models ι, corresponding to λ. Since λ has residue field $\mathbb{F}_p$, every component of the image of ι meets the ordinary locus of $\mathscr{S}_{K'}(\mathrm{GSp}, S^{\pm})$ by [Wor, Theorem 1.1]. Now using that for some N with $(N, p) = 1$, there is a surjective map $\mathcal{A}_{g,N} \to \mathrm{Sh}_{K'}(\mathrm{GSp}, S^{\pm})$, and Theorem 3.2.6, we conclude

$$\overline{\mathrm{ed}}(\mathcal{A}[p]|_{\mathrm{Sh}_K}/\mathrm{Sh}_K; p) = \dim \mathrm{Sh}_K = \dim X. \qquad \square$$

4.3 Congruence covers

It will be more convenient to state the results of this subsection in terms of locally symmetric varieties. These are geometrically connected components of the Shimura varieties discussed in the previous subsection.

4.3.1. For any reductive group G over $\mathbb{Q}$, a *congruence subgroup* $\Gamma \subset G(\mathbb{Q})$ is a group of the form $G(\mathbb{Q}) \cap K$ for some compact open subgroup $K \subset G(\mathbb{A}_f)$. An *arithmetic lattice* $\Gamma \subset G(\mathbb{Q})$ is a finite index subgroup of a congruence subgroup. If $i : G' \to G$ is a surjective map of reductive groups whose kernel is in the center of G', and $\Gamma' \subset G'(\mathbb{Q})$ is an arithmetic lattice, then $i(\Gamma') \subset G(\mathbb{Q})$ is an arithmetic lattice.

Now suppose that $X = G(\mathbb{R})/K_\infty$ is a union of Hermitian symmetric domains and let $X^+ \subset X$ be the connected component of the identity. If $\Gamma \subset G^{\mathrm{ad}}(\mathbb{Q})$ is an arithmetic lattice that acts freely on X^+ (so in particular leaves X^+ stable), then $\Gamma\backslash X^+$ has a natural structure of algebraic variety over $\bar{\mathbb{Q}}$ [Del79, § 2]. For any arithmetic lattice $\Gamma \subset G^{\mathrm{ad}}(\mathbb{Q})$ there is a finite index subgroup which acts freely on X^+.

If (G, X) is a Shimura datum, then the geometrically connected components of $\mathrm{Sh}_K(G, X)$ have the form $\Gamma\backslash X^+$, where $X^+ \subset X$ is a connected component and $\Gamma \subset G^{\mathrm{ad}}(\mathbb{Q})$ is the image of a congruence subgroup of $G^{\mathrm{der}}(\mathbb{Q})$ [Del79, 2.1.2].

https://doi.org/10.1112/S0010437X21007594

4.3.2. Now let G be a semisimple, almost simple group over $\mathbb{Q}$. We will assume that G is of classical type, so that (the connected components of) its Dynkin diagram are of type A, B, C or D.

Let $K_\infty \subset G(\mathbb{R})$ be a maximal compact subgroup, and denote by $G(\mathbb{R})^+ \subset G(\mathbb{R})$ the connected component of the identity. We will assume that $X^+ = G(\mathbb{R})^+/K_\infty$ is a Hermitian symmetric domain. The group $G^{\mathrm{ad}}(\mathbb{R})$ is a product of simple groups $G_i(\mathbb{R})$, for i in some index set I. We denote by I_{nc} (respectively, I_{c}) the set of i with G_i noncompact (respectively, compact). Then X^+ is a product of the irreducible Hermitian symmetric domains $X_i^+ = G_i(\mathbb{R})^+/K_i$, for $i \in I_{\mathrm{nc}}$, where $K_i \subset G_i(\mathbb{R})$ is maximal compact. We use Deligne's notation [Del79] for the classification of these irreducible Hermitian symmetric domains. Since we are assuming G is of classical type, for $i \in I_{\mathrm{nc}}$, X_i^+ is of type A, B, C, $D^{\mathbb{R}}$ or $D^{\mathbb{H}}$. The group $G_i(\mathbb{R})$ is either the adjoint group of $U(p,q)$ in the case of type A, of $\mathrm{Sp}(2n)$ in the case of type C, of $\mathrm{SO}(n,2)$ in the case of type B or $D^{\mathbb{R}}$, and of $\mathrm{SO}^*(2n)$, an inner form of $\mathrm{SO}(2n)$, if G_i is of type $D^{\mathbb{H}}$.

Since G is almost simple, for $i \in I_{\mathrm{nc}}$ the X_i^+ are all of the same type, except possibly if G is of type D, in which case it is possible that both factors of type $D^{\mathbb{R}}$ and $D^{\mathbb{H}}$ occur among the X_i^+. We will say that G is of *Hodge type* if all the factors X_i^+ are of the same type $A, B, C, D^{\mathbb{R}}, D^{\mathbb{H}}$ and the following condition holds: G is simply connected unless the X_i^+ are of type $D^{\mathbb{H}}$, in which case $G(\mathbb{C})$ is a product of special orthogonal groups.

4.3.3. The Dynkin diagram $\Delta(G)$ is equipped with a set of vertices $\Sigma(G)$ which is described as follows (cf. [Del79], § 1.2, 1.3). For $i \in I_{\mathrm{nc}}$, $K_i \subset G_i$ is the centralizer of a rank 1 compact torus $U(1) \subset G_i$, which is the center of K_i. Thus there are two cocharacters $h, h^{-1} : U(1) \to G_i$ which identify $U(1)$ with this compact torus. These cocharacters are minuscule, and each corresponds to a vertex of $\Delta(G_i)$. The two vertices are distinct exactly when h, h^{-1} are not conjugate cocharacters. In this case, they are exchanged by the *opposition involution* of $\Delta(G_i)$, which also gives the action of complex conjugation on $\Delta(G_i)$. We set $\Sigma(G)$ to be the union of all the vertices above. Thus $\Sigma(G) \cap \Delta(G_i)$ is empty if $i \in I_{\mathrm{c}}$, and consists of one or two vertices if $i \in I_{\mathrm{nc}}$. In the latter case it consists of two vertices if and only if $G_i(\mathbb{R})$ is either the adjoint group of $U(p,q)$ with $p \neq q$, or of $\mathrm{SO}^*(2n)$ with n odd.

4.3.4. Fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$. The Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\Delta(G)$. We consider a subset $\Sigma \subset \Sigma(G)$ such that $\Delta(G_i) \cap \Sigma$ consists of one element for $i \in I_{\mathrm{nc}}$.

We say that G is *unramified at* p if G is quasi-split over $\mathbb{Q}_p$ and splits over an unramified extension of $\mathbb{Q}_p$. We call G *p-admissible* if G is unramified, and for some embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, and some choice of Σ, the action of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ leaves Σ invariant. This definition may look slightly odd; it will be used to guarantee that the reflex field of a Shimura variety built out of G has at least one prime where the Shimura variety has a nonempty ordinary locus.

4.3.5. Now suppose that G is unramified at p. Then G extends to a reductive group $G_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$. The isomorphism class of the algebraic group $G_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{F}_p$ over $\mathbb{F}_p$ depends only on G and not on $G_{\mathbb{Z}_p}$, and we call this group the *reduction* of G.

Let $K = K^p K_p \subset G(\mathbb{A}_f)$ and $K_1 = K^p K_{1,p} \subset G(\mathbb{A}_f)$ be compact open, with $K^p \subset G(\mathbb{A}_f^p)$, $K_p = G_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and $K_{1,p} = \ker(G_{\mathbb{Z}_p}(\mathbb{Z}_p) \to G_{\mathbb{Z}_p}(\mathbb{F}_p))$. Let $\Gamma = G(\mathbb{Q}) \cap K$ and $\Gamma_1 = G(\mathbb{Q}) \cap K_1$. We will assume that $\Gamma \subset G(\mathbb{R})^+$, and that Γ acts freely on X^+. By [Del79, 2.0.7], these conditions are satisfied if K^p is sufficiently small. In particular, this allows us to view Γ as an arithmetic subgroup of $G^{\mathrm{ad}}(\mathbb{Q})$. We call a covering of the form $\Gamma_1 \backslash X^+ \to \Gamma \backslash X^+$, with Γ satisfying the above conditions, a *principal p-level covering.*

https://doi.org/10.1112/S0010437X21007594

Theorem 4.3.6. *Let G be an almost simple, p-admissible group of Hodge type, and let $X^+ = G(\mathbb{R})^+/K_\infty$. Then for any principal p-level covering $\Gamma_1\backslash X^+ \to \Gamma\backslash X^+$, we have*

$$\overline{\mathrm{ed}}(\Gamma_1\backslash X^+ \to \Gamma\backslash X^+; p) = \dim X^+.$$

Proof. Let $\Sigma \subset \Sigma(G)$ be a subset of the form described above. This corresponds to a $G^{\mathrm{ad}}(\mathbb{R})$-conjugacy class of cocharacters $h : U(1) \to G^{\mathrm{ad}}$, which we denote by X^{ad}. Then $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ is a Shimura datum and its reflex field corresponds to the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which takes Σ to itself [Del79, Prop. 2.3.6]. Since G is p-admissible, there is a choice of Σ, and a prime $\lambda'|p$ of $E(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ with $\kappa(\lambda') = \mathbb{F}_p$.

Then one sees using [Del79, Prop. 2.3.10] that one can choose a Shimura datum of Hodge type (G', X) with $G'^{\mathrm{der}} = G$ and adjoint Shimura datum $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$, and so that all primes of $E(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ above p split completely in $E(G', X)$. In particular, any prime $\lambda|\lambda'$ of $E(G', X)$ has residue field $\mathbb{F}_p$. We have verified that (G', X) satisfies the hypotheses of Lemma 4.2.3.

Now let $G'_{\mathbb{Z}_p}$ be a reductive group over $\mathbb{Z}_p$, extending G', and containing $G_{\mathbb{Z}_p}$. The existence of $G'_{\mathbb{Z}_p}$ may be seen, for example, using the classification of split reductive groups in terms of root data [SGA3, Exp XXV, Theorem 1], and the fact that the inner forms of a reductive group and its derived group are in bijection. Set $K'_p = G'_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and $K'_{1,p} = \ker(G'_{\mathbb{Z}_p}(\mathbb{Z}_p) \to G'_{\mathbb{Z}_p}(\mathbb{F}_p))$. Choose $K'^p \subset G'(\mathbb{A}_f^p)$ compact open such that $K' = K'_p K'^p$ is neat and $K'^p \cap G(\mathbb{A}_f^p) \subset K^p$, and set $K'_1 = K'_{1,p} K'^p$.

Let $\Gamma' = K' \cap G(\mathbb{Q}) \subset \Gamma$ and $\Gamma'_1 = K'_1 \cap G(\mathbb{Q})$. *A fortiori*, it suffices to prove that

$$\overline{\mathrm{ed}}(\Gamma'_1\backslash X^+ \to \Gamma'\backslash X^+; p) = \dim X^+.$$

This follows from Lemma 4.2.3 applied to the groups $K'_1 \subset K'$, by restricting the map of that lemma to geometrically connected components, and using the description of these components in [Del79, 2.1.2]. □

4.3.7. We can make the condition of p-admissibility of G in Theorem 4.3.6 somewhat more explicit if we assume that $G^{\mathrm{ad}}(\mathbb{R})$ has no compact factors.

Corollary 4.3.8. *Let G be an almost simple group which is unramified at p. Suppose that either*

(i) *G splits over $\mathbb{Q}_p$, or*
(ii) *the irreducible factors of $G^{\mathrm{ad}}(\mathbb{R})$ are all isomorphic to the adjoint group of one of $U(n,n)$, $\mathrm{SO}(n,2)$ with $n \neq 6$, or $\mathrm{Sp}(2n)$ for some positive integer n.*

Then G is p-admissible, and for any principal p-level covering $\Gamma_1\backslash X^+ \to \Gamma\backslash X^+$ we have

$$\overline{\mathrm{ed}}(\Gamma_1\backslash X^+ \to \Gamma\backslash X^+; p) = \dim X^+.$$

Proof. If G splits over $\mathbb{Q}_p$ then $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts trivially on $\Delta(G)$, and so leaves any choice of Σ stable. For (ii), one checks using the classification of [Del79] that in each of these cases, $\Sigma = \Sigma(G)$, and a vertex $v \in \Sigma(G)$ is stable by any automorphism of the connected component of $\Delta(G)$ containing v. It follows that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ leaves $\Sigma(G)$ stable. □

4.3.9. The above results give examples of coverings for which one can compute the essential p-dimension. These values are in general far from the essential p-dimension of the corresponding group. For example, Hannah Knight [Kni21] has shown that for $p \neq 2$,

$$\overline{\mathrm{ed}}(\mathrm{Sp}_{2g}(\mathbb{F}_{p^r}); p) = rp^{r(g-1)}.$$

The case $r = 1$ was computed independently by D. Benson [BF20, Appendix B].

We call a reductive group H almost absolutely simple if H is semisimple and H^{ad} is absolutely simple. (That is, it remains simple over an algebraic closure). We have the following result.

PROPOSITION 4.3.10. *Let H be a classical, almost absolutely simple group over $\mathbb{F}_q$, with $q = p^r$. If $p = 2$ we further assume that $8 \nmid r$, and $4 \nmid r$ if H is not split over $\mathbb{F}_q$.*

Then there exists a semisimple $\mathbb{Q}$-group G, such that $X^+ = G(\mathbb{R})^+/K_\infty$ is a Hermitian symmetric domain, and G is unramified at p with reduction isomorphic to $\mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p} H$, and a principal p-covering $\Gamma_1\backslash X^+ \to \Gamma\backslash X^+$ such that

$$e = \overline{\mathrm{ed}}(\Gamma_1\backslash X^+ \to \Gamma\backslash X^+; p)$$

satisfies the following properties.

- *If H is a form of SL_n which is split if n is odd, then $e = r\lfloor n^2/4 \rfloor$.*
- *If H is Sp_{2n} then $e = r((n^2+n)/2)$.*
- *If H is a split form of SO_{2n} then $e = r((n^2-n)/2)$.*
- *If H is a form of Spin_n and H is not of type D_4, then $e(H(\mathbb{F}_q)) = r(n-2)$.*

Proof. Let $\bar{G} = \mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p} H$. There is a unique (up to canonical isomorphism) connected reductive group $G_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$ with $G_{\mathbb{Z}_p} \otimes \mathbb{F}_p = \bar{G}$. If H is not one of the four types listed, then the condition on e is vacuous, and the proposition follows easily from Corollary 4.1.5.

We may now assume that H is one of the four types listed, and in each of these cases we define a semisimple Lie group $G_{\mathbb{R}}$ over $\mathbb{R}$ as follows. If H is a form of SL_n, we take $G_{\mathbb{R}}$ to be $\mathrm{SU}(n/2, n/2)^r$ if n is even and $\mathrm{SU}((n-1)/2, (n+1)/2)^r$ if n is odd. If H is Sp_{2n} we take $G_{\mathbb{R}} = \mathrm{Sp}_{2n}^r$. If H is a form of SO_{2n} we take $G_{\mathbb{R}}$ to be $\mathrm{SO}^*(2n)^r$, the inner form of (the compact group) $\mathrm{SO}(2n)$ which gives rise to the Hermitian symmetric domain of type $D_n^{\mathbb{H}}$ (cf. [Del79, 1.3.9, 1.3.10]). If H is a form of Spin_n we take $G_{\mathbb{R}}$ to be $\mathrm{Spin}(n-2, 2)^r$.

In all cases $G_{\mathbb{R}}$ and $G_{\mathbb{Z}_p}$ are forms of the same split group G^{split}. The actions of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p)$ on $\Delta(G^{\mathrm{split}})$ generate a group which is isomorphic to either C or $C \times \mathbb{Z}/2\mathbb{Z}$, with C a cyclic group. Indeed, in each case $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on $\Delta(G^{\mathrm{split}})$ by an automorphism of order 1 or 2 which lies in the center of $\mathrm{Aut}(\Delta(G^{\mathrm{split}}))$. If $p = 2$, our assumptions on r imply that $8 \nmid |C|$. Thus by Corollary 4.1.5 there exists a semisimple reductive group G over $\mathbb{Q}$, which gives rise to $G_{\mathbb{R}}$ and $G_{\mathbb{Z}_p}$ over $\mathbb{R}$ and $\mathbb{Z}_p$ respectively.

By construction G is of Hodge type, and we now check that it can be chosen to be p-admissible. This is necessarily the case by Corollary 4.3.8, except when n is odd and H is a form of SL_n or H is a form of $\mathrm{SO}(2n)$. In these cases, we are assuming that H is a split form, so $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ permutes the components of $\Delta(G)$ simply transitively. If H is a form of SL_n or $\mathrm{SO}(2n)$ with n odd, then $\Delta(G_i)$ contains two points in $\Sigma(G)$ (the opposition involution is nontrivial on $\Delta(G_i)$ in these cases), and we can take $\Sigma \subset \Sigma(G)$ to be a $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of any point $v \in \Sigma(G)$.

When H is a form of $\mathrm{SO}(2n)$ with n even, then the opposition involution is trivial on $\Delta(G_i)$, and hence so is the action of complex conjugation. The set $\Sigma(G)$ meets each component of $\Delta(G)$ in one vertex. Let Σ_1 be the $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of any vertex in $\Sigma(G)$. There is an inner form $G_{1,\mathbb{R}}$ of G over $\mathbb{R}$ such that $\Sigma(G_{1,\mathbb{R}}) = \Sigma_1$. (Note that the Dynkin diagrams of inner forms are identified, so this makes sense.) Explicitly, let $a \in \mathrm{Out}(G)$ be an automorphism which preserves the connected components of $\Delta(G)$ and such that $a(\Sigma(G)) = \Sigma_1$. (Such an a is unique unless H is of type D_4.) Then $G_{1,\mathbb{R}}$ is given by twisting G by the cocycle $\tilde{a}\sigma(\tilde{a})^{-1}$ where $\tilde{a} \in \mathrm{Aut}(G)(\mathbb{C})$ lifts a. Using the surjection (4.1.4), we see that there is an inner twisting G_1 of G over $\mathbb{Q}$ which

is isomorphic to $G_{1,\mathbb{R}}$ over $\mathbb{R}$ and to G over $\mathbb{Q}_p$, as an inner twist. As $\Sigma(G_1) = \Sigma_1$ is stable by $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, G_1 is p-admissible.

Thus, the proposition follows from Theorem 4.3.6 and the formulae for the dimensions of Hermitian symmetric domains. □

4.3.11. As in the introduction, if H is a simple reductive group over $\mathbb{F}_q$, we denote by $H(q)$ the image of $H^{\mathrm{sc}}(\mathbb{F}_q)$ in $H(\mathbb{F}_q)$.

Corollary 4.3.12. *Let H be a classical, absolutely simple group over $\mathbb{F}_q$, with $q = p^r$. If $p = 2$ we further assume that $8 \nmid r$, and $4 \nmid r$ if H is not split over $\mathbb{F}_q$.*

Then there is a congruence $H(q)$-cover of locally symmetric varieties $Y' \to Y$ whose associated real Lie group is of the same type (A, B, C or D) as H, and such that $e := \overline{\mathrm{ed}}(Y'/Y; p)$ satisfies the following properties.

- *If H is a form of PGL_n which is split if n is odd, then $e = r\lfloor n^2/4 \rfloor$.*
- *If H is PSp_{2n} then $e = r((n^2+n)/2)$.*
- *If H is a split form of PO_{2n} then $e = r((n^2-n)/2)$.*
- *If H is a form of PO_n and H is not of type D_4, then $e = r(n-2)$.*

Proof. The group H has the form $\tilde{H}^{\mathrm{ad}}$, where $\tilde{H}$ is a group as in one of the four cases of Proposition 4.3.10. We apply Proposition 4.3.10 to $\tilde{H}$ to obtain a semi-simple $\mathbb{Q}$-group G and principal p-covering $\Gamma_1\backslash X^+ \to \Gamma\backslash X^+$. By assumption, Γ acts freely on X^+, so this covering has group Γ/Γ_1. We will show that $H(q)$ is a subquotient of Γ/Γ_1, and take $Y' \to Y$ to be the corresponding $H(q)$ cover.

Since G has reduction isomorphic to $\mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p}\tilde{H}$, we have

$$\Gamma/\Gamma_1 \subset \mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p}\tilde{H}(\mathbb{F}_p) = \tilde{H}(\mathbb{F}_q).$$

Moreover, since $\tilde{H}$ is almost simple, and G is associated to a Hermitian symmetric domain, G does not have any compact factors over $\mathbb{Q}$. Thus, we may apply the strong approximation theorem to G^{sc} to conclude that Γ/Γ_1 contains $\mathrm{Im}(H^{\mathrm{sc}}(\mathbb{F}_q) \to \tilde{H}(\mathbb{F}_q))$.

If $Z_{H^{\mathrm{sc}}}$ denotes the center of H^{sc}, then $H(q)$ is a normal subgroup of $(\Gamma/\Gamma_1)/Z_{H^{\mathrm{sc}}}(\mathbb{F}_q)$, and

$$H(q)\backslash(\Gamma/\Gamma_1)/Z_{H^{\mathrm{sc}}}(\mathbb{F}_q) \subset H(\mathbb{F}_q)/H(q) \simeq H^1(\mathrm{Spec}\,\mathbb{F}_q, Z_{H^{\mathrm{sc}}}).$$

Since H is absolutely simple, there is a finite extension $\mathbb{F}_{q'}/\mathbb{F}_q$, such that the group scheme $Z_{H^{\mathrm{sc}}}$ is isomorphic to μ_r over $\mathbb{F}_{q'}$, for some integer r. Thus $Z_{H^{\mathrm{sc}}}(\mathbb{F}_q) \subset Z_{H^{\mathrm{sc}}}(\mathbb{F}_{q'}) \subset \mathbb{F}_{q'}^{\times}$, and $H^1(\mathrm{Spec}\,\mathbb{F}_q, Z_{H^{\mathrm{sc}}})$ is an extension of a subgroup of $\mathbb{F}_{q'}^{\times}/(\mathbb{F}_{q'}^{\times})^r$ by $H^1(\mathrm{Gal}(\mathbb{F}_{q'}/\mathbb{F}_q), Z_{H^{\mathrm{sc}}}(\mathbb{F}_{q'}))$. In particular, $Z_{H^{\mathrm{sc}}}(\mathbb{F}_q)$ is cyclic of order prime to p, and $H^1(\mathrm{Spec}\,\mathbb{F}_q, Z_{H^{\mathrm{sc}}})$ has order prime to p.

That the cover corresponding to $H(q)$ satisfies the conclusion of the corollary now follows from Proposition 4.3.10 and Lemma 2.2.7. □

Remark 4.3.13. For $H = \mathrm{PSL}_4$ and $q = 2$ there is an exceptional isomorphism $H(2) = \mathrm{SL}_4(\mathbb{F}_2) \cong A_8$. Corollary 4.3.12 thus gives examples of incompressible covers $\Gamma'\backslash X^+ \to \Gamma\backslash X^+$ with Galois group A_8 where $\Gamma\backslash X^+$ is a 4-fold. It would be of interest to investigate these in connection with solutions of the general octic polynomial, for example as in Hilbert's Octic Conjecture [Hil27].

References

BF20 P. Brosnan and N. Fakhruddin, *Fixed points, local monodromy, and incompressibility of congruence covers*, Preprint (2020), arXiv:2007.01752.

Bor96 M. Borovoi, *Abelianization of the first Galois cohomology of reductive groups*, Int. Math. Res. Not. (IMRN) **8** (1996), 401–407.

BR97 J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compos. Math. **106** (1997), 159–179.

CT02 J. L. Colliot-Thélène, *Exposant et indice d'algèbres simples centrales non ramifiées. (With an appendix by Ofer Gabber.)*, Enseign. Math. **48** (2002), 127–146.

Del71 P. Deligne, *Travaux de Shimura*, *Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389*, Lecture Notes in Mathematics, vol. 244 (Springer, Berlin, 1971), 123–165.

Del79 P. Deligne, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, in *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2* (American Mathematical Society, Providence, RI, 1979), 247–289.

DM69 P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Publ. Math. Inst. Hautes Études Sci. **36** (1969), 75–109.

Dic08 L. E. Dickson, *Representations of the general symmetric group as linear groups in finite and infinite fields*, Trans. Amer. Math. Soc. **9** (1908), 121–148.

EGA A. Grothendieck, *Éléments de géométrie algébrique*: I–IV, Publ. Math. Inst. Hautes Études Sci. **4, 8, 11, 17, 20, 24, 32** (1960–1967).

FvdG04 C. Faber and G. van der Geer, *Complete subvarieties of moduli spaces and the Prym map*, J. Reine Angew. Math. **573** (2004), 117–137.

FD93 B. Farb and R. K. Dennis, *Noncommutative algebra*, Graduate Texts in Mathematics, vol. 144 (Springer, New York, 1993).

GP05 D. Glass and R. Pries, *Hyperelliptic curves with prescribed p-torsion*, Manuscripta Math. **117** (2005), 299–317.

HB78 G. Harder and A. Borel, *Existence of discrete cocompact subgroups of reductive groups over local fields*, J. Reine Angew. Math. **298** (1978), 53–64.

Hil27 D. Hilbert, *Uber die Gleichung neunten Grades*, Math. Ann. **97** (1927), 43–250.

Jo1870 C. Jordan, *Traité des substitutions* (Gauthier-Villars, Paris, 1870).

Kat81 N. Katz, *Serre-Tate local moduli*, in *Algebraic surfaces (Orsay, 1976–78)* (Springer, Berlin, 1981).

KMP16 W. Kim and K. M. Pera, *2-adic integral canonical models*, Forum Math. Sigma **4** (2016), e28.

Kis10 M. Kisin, *Integral models for Shimura varieties of abelian type*, J. Amer. Math. Soc. **23** (2010), 967–1012.

Kl1884 F. Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade (Lectures on the Icosahedron and the Solution of the Equation of the Fifth Degree)* (Teubner, Leipzig, 1884).

Kl1888 F. Klein, *Sur la resolution, par les fonctions hyperelliptiques de l'equation du vingt-septieme degre, de laquelle depend la determination des vingt-sept droites d'une surface cubique*, J. Math. Pures Appl. **4** (1888), 169–176.

Kl1890 F. Klein, *Zur Theorie der Abel'schen Functionen*, Math. Ann. **36** (1890), 1–83.

Kni21 H. Knight, *The essential p-dimension of quasi-simple finite groups of Lie type*, Preprint (2021), arXiv:2109.02698.

Kot86 R. E. Kottwitz, *Stable trace formula: elliptic singular terms*, Math. Ann. **275** (1986), 365–399.

Kr1861 L. Kronecker, *Ueber die Gleichungen fünften g rades*, J. Reine Angew. Math. **59** (1861), 306–310.

Lan19 A. Landesman, *The Torelli map restricted to the hyperelliptic locus*, Preprint (2019), arXiv:1911.02084.

Mat58 T. Matsusaka, *On a theorem of Torelli*, Amer. J. Math. **80** (1958), 784–800.

McM13 C. McMullen, *Braids and Hodge theory*, Math. Ann. **355** (2013), 893–946.

MR09 A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra Number Theory **3** (2009), 467–487.

Poo00 B. Poonen, *Varieties without extra automorphisms. II. Hyperelliptic curves*, Math. Res. Lett. **7** (2000), 77–82.

OS80 F. Oort and J. Steenbrink, *The local Torelli problem for algebraic curves*, in *Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979* (Sijthoff & Noordhoff, Alphen aan den Rijn, 1980), 157–204.

RG71 M. Raynaud and L. Gruson, *Critères de platitude et de projectivité. Techniques de 'platification' d'un module*, Invent. Math. **13** (1971), 1–89.

Rei11 Z. Reichstein, *Essential dimension*, in *Proceedings of the International Congress of Mathematicians* (ICM2010) (Hindustan Book Agency, 2011).

RY00 Z. Reichstein and B. Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), 1018–1056; with an appendix by János Kollár and Endre Szabó.

SGA1 A. Grothendieck, *Revêtements étales et groupe fondamental (SGA1)*, in *Séminaire de géométrie algébrique*, vol. 1960/61 (Institut des Hautes Études Scientifiques, Paris, 1963).

SGA2 A. Grothendieck, *Séminaire de Géométrie Algébrique du Bois-Marie, 1962 – Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux (SGA 2)*, Advanced Studies in Pure Mathematics, vol. 2 (North-Holland/Masson & Cie, Amsterdam/Éditeur, Paris, 1968).

SGA3 M. Demazure and A. Grothendieck, *Schémas en groupes (SGA3). Fasc. 7: Exposés 23 à 26*, in *Séminaire de géométrie algébrique de l'Institut des Hautes Études Scientifiques*, vol. 1963/64 (Institut des Hautes Études Scientifiques, Paris, 1965/1966).

Tsc34 N. G. Tschebotaröw, *Die Probleme der modernen Galoisschen Theorie*, Comment. Math. Helv. **6** (1934), 235–283.

Sal82 David J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.

Wor D. Wortmann, *The μ-ordinary locus for Shimura varieties of Hodge type*, Preprint (2013), arXiv:1310.6444.

Benson Farb farb@math.uchicago.edu
Department of Mathematics, University of Chicago, 5734 S. University Avenue, Chicago, IL 60637, USA

Mark Kisin kisin@math.harvard.edu
Department of Mathematics, Harvard University, Science Center Room 325, 1 Oxford Street, Cambridge, MA 02138, USA

Jesse Wolfson wolfson@uci.edu
Department of Mathematics, University of California–Irvine, Rowland Hall 340H, Irvine, CA 92697, USA