

EXPLICIT COMPUTATION OF GALOIS REPRESENTATIONS OCCURRING IN FAMILIES OF CURVES

ABSTRACT. In view of computing mod ℓ Galois representations occurring in the étale cohomology of surfaces over \mathbb{Q} , we present a method to compute division polynomials of Jacobians of curves over the rational fraction field $\mathbb{Q}(t)$. We demonstrate the use of this method on a couple of examples. We thus obtain explicit families of Galois representations over $\mathbb{P}_{\mathbb{Q}}^1$, and we study their degeneration at values of t at which the curve has bad reduction. We use these data to propose a conjectural geometric explanation extending the Néron-Ogg-Shafarevich criterion for the ramification of these degenerate Galois representations.

ACKNOWLEDGEMENTS. The author thanks Jean Gillibert for setting him on track to understanding the material presented in Section 5.2. Experiments presented in this paper were carried out using the [PlaFRIM] experimental testbed, supported by Inria, CNRS (LABRI and IMB), Université de Bordeaux, Bordeaux INP, and Conseil Régional d'Aquitaine (see <https://www.plafrim.fr/>), and on the Warwick mathematics institute computer cluster provided by the EPSRC Programme Grant EP/K034383/1 “LMF: L-Functions and Modular Forms”. The computer algebra package used was [Pari/GP], along with [Magma] for comparison.

Keywords: Galois representation, division polynomial, étale cohomology, Jacobian, surface, family of curves, bad reduction, degeneration, ramification, inverse Galois problem.

1. INTRODUCTION

Let S be an algebraic surface defined over \mathbb{Q} , and let $\ell \in \mathbb{N}$ be a prime number. The purpose of this article is twofold: to describe a practical algorithm to compute explicitly the mod- ℓ Galois representations occurring in the étale cohomology space $H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ of S , and to formulate a conjectural generalisation of the Néron-Ogg-Shafarevich criterion [ST68] to the degenerate Galois representations which we obtain as a byproduct of this algorithm (our motivation for this is explained in Remark 1.4 below).

1.1. First goal: Computing with the étale cohomology of surfaces. More specifically, suppose that $H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ contains a Galois-submodule which affords a mod ℓ Galois representation ρ that we wish to compute explicitly. By this, we mean computing a polynomial in $\mathbb{Q}[x]$ which encodes ρ in the following sense:

Definition 1.1. Let K be a number field, and let $\rho : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}(V_{\rho})$ be a mod ℓ Galois representation, where V_{ρ} is an \mathbb{F}_{ℓ} -vector space of finite dimension. We say that a separable polynomial $F(x) \in K[x]$ *encodes* ρ if we are given an explicit bijection between $V_{\rho} \setminus \{0\}$ and the roots of $F(x)$ in some extension Ω of K over which $F(x)$ splits completely, in such a way that the Galois action on the roots

of $F(x)$ matches that on V_ρ . In particular, the splitting field of $F(x)$ then agrees with the number field $\overline{K}^{\text{Ker } \rho}$ cut out by ρ .

In [Mas22, 2], we sketched a method to compute $\rho \subset H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ based on *dévissage* [SGA4 $\frac{1}{2}$, 3.4], and which may be informally summarised as follows. Pick a proper dominant morphism $\pi : S \rightarrow B$ from S to a curve B over \mathbb{Q} , and write S_b for the fibre of π at a point $b \in B$. Roughly speaking, the Leray spectral sequence [MilEC, 12.7] attached to π then shows that $H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ is made up of $H_{\text{ét}}^p(B_{\overline{\mathbb{Q}}}, H_{\text{ét}}^q(S_b, \mathbb{Z}/\ell\mathbb{Z}))$ for $p + q = 2$. Since the terms for $p = 0, q = 2$ and for $p = 2, q = 0$ consist of uninteresting bits, we can expect that ρ occurs in $H_{\text{ét}}^1(B_{\overline{\mathbb{Q}}}, H_{\text{ét}}^1(S_b, \mathbb{Z}/\ell\mathbb{Z}))$. As B and the S_b are curves, and as the $H_{\text{ét}}^1$ of a curve is essentially the torsion of its Jacobian (see the first part of Theorem 1.2 below for a precise statement), it is thus reasonable to hope to compute compute $\rho \subset H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ by:

- (1) Computing the family of Galois representations parametrised by $b \in B$ afforded by the ℓ -torsion of the Jacobian of the fibre S_b ,
- (2) Gluing these data into an explicit model of a cover $C \rightarrow B$ of curves,
- (3) Catching ρ in the ℓ -torsion of the Jacobian of the curve C .

Strategy 1.1: Computing in the $H_{\text{ét}}^2$ of surfaces by looking at the torsion of Jacobians of curves.

The situation is illustrated on Figure 1.1.

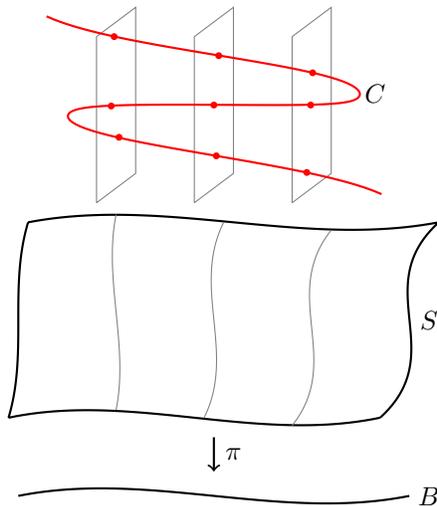


Figure 1.1: The surface S with some of the fibres S_b of π . The rectangles above them represent the Jacobian of these fibres, inside which the red dots represent ℓ -torsion points. These points define a curve C whose Jacobian should contain ρ in its ℓ -torsion.

More precisely, we have the following result:

Theorem 1.2. *Given an \mathbb{F}_ℓ -Galois-module M and an integer $n \in \mathbb{Z}$, write $M(n)$ for the twist of M by the n -th power of the mod ℓ cyclotomic character.*

- (1) *Let X be a nonsingular, geometrically irreducible curve over a number field K , and let J be the Jacobian of the completion of X . If X is complete, then $H_{\text{ét}}^1(X_{\overline{K}}, \mathbb{Z}/\ell\mathbb{Z}) \simeq J[\ell](-1)$ as Galois modules. If X is not complete, then $H_{\text{ét}}^1(X_{\overline{K}}, \mathbb{Z}/\ell\mathbb{Z})$ is an extension of $J[\ell](-1)$ by copies of $(\mathbb{Z}/\ell\mathbb{Z})(-1)$.*
- (2) *Suppose ρ is a mod ℓ Galois representation contained in $H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$ (up to semi-simplification). Let $B' = B \setminus Z$, where $Z \subset B$ is the locus of bad fibres of π . Assume that ρ has no Jordan-Hölder components of the form $(\mathbb{Z}/\ell\mathbb{Z})(n)$ for any $n \in \mathbb{Z}$, and no component in common with $\eta(-1)$, where η is the mod ℓ permutation representation induced by the Galois action on the geometrically irreducible components of the bad fibres of π . Then ρ is also contained (up to semi-simplification) in $H_{\text{ét}}^1(C_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})(-1)$, where C is the completion of the cover of B' formed by the nonzero ℓ -torsion points of the Jacobian of the S_b .*

Part 1 is standard (cf. [MilEC, 14.2,14.4,16.2]), and part 2 is [Mas22, Thm 7]. In particular, if ρ satisfies the assumptions of part 2, and if C is geometrically irreducible, then ρ is found (up to twist) in the ℓ -torsion of the Jacobian of C . More generally, if C is not geometrically irreducible, consider a Galois number field $K \subset \overline{\mathbb{Q}}$ such that the geometrically irreducible components C_i of C are defined over K ; then ρ will be found in the induction to $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the representation of $\text{Gal}(\overline{\mathbb{Q}}/K)$ afforded by the ℓ -torsion of the Jacobians of the C_i .

Let us now explain in more detail how to turn these observations into an algorithm to compute ρ explicitly, assuming for simplicity that C is geometrically irreducible. In [Mas19], we described an algorithm which, given a proper, nonsingular, and geometrically irreducible curve C over a number field¹ K and a prime $\ell \in \mathbb{N}$, computes what may be called an ℓ -division polynomial $R_{C,\ell}(x) \in K[x]$ of C , that is to say a polynomial which encodes the representation afforded by the ℓ -torsion of the Jacobian J of C in the sense of Definition 1.1. This algorithm is also capable of computing the subrepresentation afforded by a Galois-submodule V of $J[\ell]$, provided that there exists a prime $\mathfrak{p} \nmid \ell$ of K where C has good reduction and such that $V \subset J[\ell]$ may be characterised by the characteristic polynomial of $\text{Frob}_{\mathfrak{p}}$ acting on V .

Suppose for the sake of the exposition that we are given an equation $f(x, y, t) \in \mathbb{Q}[x, y, t]$ such that our surface S is the desingularisation of the projective closure of the patch defined by $f(x, y, t) = 0$. It is then natural to choose $B = \mathbb{P}_{\mathbb{Q}}^1$ and π the projection $(x, y, t) \mapsto t$, thereby viewing the surface S as a curve \mathcal{S} over $\mathbb{Q}(t)$. Suppose furthermore we generalised our division polynomial algorithm [Mas19] to curves over $\mathbb{Q}(t)$. We would then be able to compute a division polynomial $R_{\mathcal{S},\ell}(x, t) \in \mathbb{Q}(t)[x]$ for \mathcal{S} , whose specialisation $R_{\mathcal{S},\ell}(x, t_0) \in \mathbb{Q}(t_0)[x]$ at any good fibre $t = t_0 \in B$ of π would be an ℓ -division polynomial of the fibre S_{t_0} . Then the equation $R_{\mathcal{S},\ell}(x, t) = 0$ would define the curve C such that ρ occurs (up to twist by the cyclotomic character) in the ℓ -torsion of the Jacobian of C , so that we may compute ρ by applying the original version of [Mas19] to C , by isolating the twist

¹At present, this algorithm is only implemented for $K = \mathbb{Q}$, but its generalisation to number fields is straightforward.

of ρ in the Jacobian J_C of C from the knowledge of the characteristic polynomial of $\rho(\text{Frob}_{\mathfrak{p}})$ where \mathfrak{p} is as described above (cf. [Mas22] for a successfully worked out example of this approach).

In particular, we would not even need to compute all of the ℓ^{2g_C} points of $J_C[\ell]$, which would be impractical even for $\ell = 2$ as soon as the genus g_C of C is moderately large, but only the $\ell^{\deg \rho}$ points of the subspace affording the twist of ρ contained in $J_C[\ell]$. On the other hand, this method forces us to compute all the ℓ -torsion points of the Jacobian of \mathcal{S} in order to get an equation for C , and this therefore only applicable when the genus of \mathcal{S} is reasonably small.

The first purpose of this article is to explain how [Mas19] can indeed be generalised to curves over $\mathbb{Q}(t)$, thereby making it theoretically possible to compute explicitly mod ℓ Galois representations which occur in the $H_{\text{ét}}^2$ of surfaces.

Remark 1.3. Very general but unfortunately impractical algorithms to compute with étale cohomology are presented in [MO15] and [PTvL15]. In contrast, our goal is to obtain a practical method for the specific case of the $H_{\text{ét}}^2$ of surfaces.

We show how [Mas19] can be generalised to curves over $\mathbb{Q}(t)$ in Section 2. Since [Mas19] requires the curve to be given as a Riemann-Roch space whereas the plane equation $R_{\mathcal{S},\ell}(x,t) = 0$ is likely to be badly singular, in Section 3 we briefly recall how to perform various computations with plane algebraic curves, including the determination of the genus of the normalised curve and the calculation of Riemann-Roch spaces.

As an application, in Section 4 we compute division polynomials $R_{\mathcal{S},\ell}(x,t)$ for three curves \mathcal{S} over $\mathbb{Q}(t)$, of respective genera 1, 2, and 3. This makes it possible, in principle, to compute with the $H_{\text{ét}}^2$ of the corresponding surfaces over \mathbb{Q} ; but unfortunately, the equations which we obtain for the curves of genera 2 and 3 are too complicated for this to practical.

1.2. Second goal: Understanding geometrically the ramification of degenerate representations attached to bad fibres. Even when we are unable to complete the calculation of the original Galois representation $\rho \subset H_{\text{ét}}^2(S_{\overline{\mathbb{Q}}}, \mathbb{Z}/\ell\mathbb{Z})$, we still obtain a division polynomial $R_{\mathcal{S},\ell}(x,t)$ which is worthy of our attention, as it encodes a *family* of Galois representations over $B = \mathbb{P}_{\mathbb{Q}}^1$.

In this family, good fibres S_{t_0} of $\pi : S \rightarrow B$ correspond to representations which simply describe the Galois action on the ℓ -torsion of the Jacobian of S_{t_0} , and whose ramification can therefore be predicted by the Néron-Ogg-Shafarevich criterion [ST68]. In contrast, the degenerate representations corresponding to the bad fibres of π are more intriguing. In Section 5, we thus formulate a conjectural geometric explanation generalising the Néron-Ogg-Shafarevich criterion for the ramification of these degenerations, which we support by analysing the data obtained in Section 4.

Remark 1.4. The reason why this generalisation is required is that Néron-Ogg-Shafarevich only applies to models of Abelian varieties over a 1-dimensional basis, whereas our ramification considerations mean we are implicitly working over the basis $\mathbb{P}_{\mathbb{Z}}^1$ which has two dimensions, namely a geometric one (in t) and an arithmetic one (in the primes of \mathbb{Q}). In particular, we do not have a satisfying theory of Néron models at our disposal as far as the author is aware. The fact that we are in uncharted territory is the reason that motivates us to make an experimental study of these degenerate representations the second goal of this article.

2. DIVISION POLYNOMIALS OVER $\mathbb{Q}(t)$

Let still $\ell \in \mathbb{N}$ be prime. The purpose of this Section is to present algorithms to compute ℓ -division polynomials for Jacobians of curves over \mathbb{Q} and $\mathbb{Q}(t)$.

2.1. Sketch of the algorithm over \mathbb{Q} . In [Mas19], we presented the following p -adic algorithm to compute an ℓ -division polynomial of the Jacobian of a curve C over \mathbb{Q} :

- (1) Pick a prime $p \neq \ell$ of good reduction of C . Determine $a \in \mathbb{N}$ such that the ℓ -torsion of the Jacobian J of C is defined over \mathbb{F}_q , where $q = p^a$.
- (2) Generate points of $J(\mathbb{F}_q)[\ell]$ which span $J[\ell]$ as an $\mathbb{F}_\ell[\text{Frob}_p]$ -module.
- (3) Lift these points to $J(\mathbb{Z}_q/p^e)[\ell]$, where \mathbb{Z}_q is the ring of integers of the unramified extension of \mathbb{Q}_p with residue field \mathbb{F}_q , and $e \in \mathbb{N}$ is an accuracy parameter.
- (4) Construct an evaluation map $\alpha \in \mathbb{Q}(J)$.
- (5) Expand $\tilde{F}(x) = \prod_{0 \neq t \in J[\ell]} (x - \alpha(t)) \in (\mathbb{Z}/p^e\mathbb{Z})[x]$, and identify it as an element $F(x)$ of $\mathbb{Q}[x]$.

Algorithm 2.1: Division polynomial of a curve over \mathbb{Q} .

The idea is thus to pick an auxiliary prime p , and to rely on the fact that $J[\ell]$ is étale at p to construct p -adic approximations of points of $J[\ell]$.

The polynomial $F(x)$ is then an ℓ -division polynomial of C in the sense of Definition 1.1. This supposes that α is defined and injective on $J[\ell]$; if this is not the case, we start over with another α . This also supposes that the accuracy parameter e is large enough to identify $F(x)$ from its mod p^e approximation $\tilde{F}(x)$. In particular, the correctness of this method is not rigorously guaranteed, although this could be done by confirming that the elements of $J(\mathbb{Z}_q/p^e)[\ell]$ are indeed p -adic approximations of ℓ -torsion points defined over the stem fields of the irreducible factors of $F(x)$. Besides, in most cases, one easily convinces oneself beyond reasonable doubt that the output $F(x)$ is correct, e.g. by checking that it has the appropriate Galois group and ramification.

In order to compute in J , this algorithm relies on Makdisi's algorithms [KM04, KM07]. These algorithms were originally designed to work over a field, so in [Mas19] we generalised them to work over a local ring such as \mathbb{Z}_q/p^e . These algorithms also require the knowledge of an explicit basis of a Riemann-Roch space of C of high-enough degree so as to represent C internally (cf. the bottom of page 1421 in [Mas19]), so we will explain in Section 3 below how such a basis may be computed from a (possibly singular) plane model of C .

2.2. Sketch of the algorithm over $\mathbb{Q}(t)$. By analogy with the embedding of \mathbb{Q} into its completion \mathbb{Q}_p , it is natural to extend Algorithm 2.1 to curves over $\mathbb{Q}(t)$ by embedding $\mathbb{Q}(t)$ into the p -adic Laurent series field $\mathbb{Q}_p((t))$. This leads to the following idea to compute an ℓ -division polynomial of a curve C over $\mathbb{Q}(t)$:

- (1) If required, shift the parameter t so that \mathcal{C} has good reduction C_0 at $t = 0$. Pick a prime $p \neq \ell$ of good reduction of C_0 , and determine $a \in \mathbb{N}$ such that the ℓ torsion of the Jacobian J_0 of C_0 is defined over \mathbb{F}_q , where $q = p^a$.
- (2) Generate points of $J_0(\mathbb{F}_q)[\ell]$ which span $J_0[\ell]$ as an $\mathbb{F}_\ell[\text{Frob}_p]$ -module.
- (3) Lift these points to $\mathcal{J}(R)[\ell]$, where \mathcal{J} is the Jacobian of \mathcal{C} and R is a finite quotient of the formal power series ring $\mathbb{Z}_q[[t]]$.
- (4) Construct an evaluation map $\alpha \in \mathbb{Q}(t)(\mathcal{J})$.
- (5) Expand $\tilde{F}(x) = \prod_{0 \neq t \in J[\ell]} (x - \alpha(t)) \in R[x]$, and identify it as an element $F(x)$ of $\mathbb{Q}(t)[x]$.

Algorithm 2.2: Division polynomial of a curve over $\mathbb{Q}(t)$.

This assumes that we manage to extend Makdisi’s algorithms to finite quotients of $\mathbb{Z}_q[[t]]$. This is actually not an issue, because the extension which we designed in [Mas19] works with any finite local ring R over which one can perform linear algebra in “good reduction cases” in the following sense:

Definition 2.1. Let $R = \mathcal{O}/\mathfrak{a}$ be finite quotient of a local domain \mathcal{O} . Let K be the fraction field of \mathcal{O} , and let k be the residue field of \mathcal{O} . We say that *we can perform linear algebra over R in cases of good reduction* if, given the reduction mod \mathfrak{a} of a matrix A over \mathcal{O} such that the rank of A is the same over K and over k , we can compute an approximation in \mathcal{O}/\mathfrak{a} of a K -basis of the kernel of A .

Similarly, the construction [Mas19, 2.2.3] of evaluation maps α generalises to Jacobians of curves over $\mathbb{Q}(t)$ without change.

Finally, we can identify the coefficients of $\tilde{F}(x)$ as elements of $\mathbb{Q}(t)$ by a combination of p -adic rational reconstruction (as we did in the original version of [Mas19]) and of Padé approximants (see Remark 2.2 below for practical details).

2.3. Lifting torsion points (p, t)-adically. In order to turn these ideas into a proper algorithm to compute division polynomials over $\mathbb{Q}(t)$, we still must explain what kind of finite quotients R of $\mathbb{Z}_q[[t]]$ we will work with, and how to lift an ℓ -torsion point from \mathbb{F}_q to R .

A first natural choice for R would be $R_e = \mathbb{Z}_q[[t]]/\mathfrak{m}^e$, where $\mathfrak{m} = (p, t)$ is the maximal ideal of $\mathbb{Z}_q[[t]]$ and $e \in \mathbb{N}$ is an accuracy parameter as in Algorithm 2.1. This choice may be appealing at first, as it would give us the hope of being able to raise the p -adic and the t -adic accuracy of torsion points simultaneously; but unfortunately, we will see below that R_e having Krull dimension 2 actually results in an algorithmic obstacle to lifting torsion points. Furthermore, elements of R_e are of the form $\sum_{j < e} \lambda_j t^j$ where $\lambda_j \in \mathbb{Z}/p^{e-j}\mathbb{Z}$ is known with poor accuracy for large j ; as a result, in $\tilde{F}(x)$, the coefficients of high powers of t would be known with poor p -adic accuracy, which would force us to increase the value of e so as to identify them, so we would end up lugging around high powers of t throughout the calculation only to drop them at the final stage since they are p -adically too imprecise to be identified as rational numbers, and thus result in a major waste of time.

We have therefore decided to work with the quotients $R = R_{e,h} = (\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)$, where $h \in \mathbb{N}$ is a second accuracy parameter. The introduction of this new parameter grants us the flexibility of setting the p -adic accuracy independently from the t -adic one, which turns out to be useful in practice. Furthermore, this makes it possible to generalise our algorithm to lift torsion points. In order to see why, recall how we proceeded over \mathbb{Q} in [Mas19]:

Let $\mathcal{O} = \mathbb{Z}_q$, $\varpi = p$, $\mathfrak{m} = \varpi\mathcal{O}$, $K = \mathbb{Q}_q$, and let J be the Jacobian of a curve over K which has good reduction at \mathfrak{m} . Given $e \in \mathbb{N}$, a point $x \in J(\mathcal{O}/\mathfrak{m}^e)$ is represented in Makdisi's algorithms (as generalised in [Mas19]) by a matrix W_x with entries in $\mathcal{O}/\mathfrak{m}^e$; but conversely, most such matrices do not represent any point of J . We thus began with an algorithm [Mas19, Algorithm 9] which, given an integer $e \in \mathbb{N}$ and a matrix W_x representing $x \in J(\mathcal{O}/\mathfrak{m}^e)$, computes a lift of W_x to $\mathcal{O}/\mathfrak{m}^{2e}$ which represents a lift of x to $J(\mathcal{O}/\mathfrak{m}^{2e})$.

Due to the tangent space of J at x , this lift of x is not unique, and indeed this algorithm can return several matrices representing different random lifts of x if required. But this also means that even if x was ℓ -torsion in $J(\mathcal{O}/\mathfrak{m}^e)$, none of these lifts to $J(\mathcal{O}/\mathfrak{m}^{2e})$ are guaranteed (nor even likely) to be ℓ -torsion.

In order to circumvent this problem, we showed how to construct an algebraic ‘‘coordinate chart’’ $\kappa : U \hookrightarrow \mathcal{O}^n$, where n is a fixed integer not smaller than the genus g of the curve. This chart is defined on an \mathfrak{m} -adic neighbourhood U of the origin $0 \in J(\mathcal{O})$, and turns the mod \mathfrak{m}^e representation in Makdisi form of a point $x \in U$ into a vector $\kappa(x) \in (\mathcal{O}/\mathfrak{m}^e)^n$ such that for all $e' \leq e$, $\kappa(x) = 0 \pmod{\mathfrak{m}^{e'}}$ if and only if $x = 0$ in $J(\mathcal{O}/\mathfrak{m}^{e'})$. As \mathcal{O} is furthermore principal with uniformiser $\varpi = p$, we then designed a second algorithm [Mas19, Algorithm 11], which computes the unique lift to $J(\mathcal{O}/\mathfrak{m}^{2e})[\ell]$ of a point $x \in J(\mathcal{O}/\mathfrak{m}^e)[\ell]$ as follows:

- (1) Use algorithm [Mas19, Algorithm 9] to generate $g + 1$ matrices W_0, \dots, W_g representing random lifts x_0, \dots, x_g of x to $J(\mathcal{O}/\mathfrak{m}^{2e})$.
- (2) For each of these lifts, compute the vectors $k_i = \frac{1}{\varpi^e} \kappa([\ell]x_i) \in (\mathcal{O}/\mathfrak{m}^e)^n$.
- (3) Try to find scalars $\lambda_1, \dots, \lambda_g \in \mathcal{O}/\mathfrak{m}^{2e}$ such that $\sum_{i=0}^g \lambda_i k_i = 0 \pmod{\mathfrak{m}^e}$ and $\sum_{i=0}^g \lambda_i = 1 \pmod{\mathfrak{m}^{2e}}$, and return the matrix $\sum_{i=0}^g \lambda_i W_i$.

Algorithm 2.3: Lifting an ℓ -torsion point in Makdisi form.

The idea is that with high probability, the lifts x_i form an affine coordinate frame of the tangent space of J at x , which guarantees the existence and uniqueness of the λ_i (and otherwise, we start over with other random lifts x_i). Note that since x is assumed to be ℓ -torsion mod \mathfrak{m}^e , we have $\kappa(x_i) = 0 \pmod{\mathfrak{m}^e}$ for all i , so division by ϖ^e does result in the k_i being integral. This division is essential so that we can find the λ_i by solving a linear system over the local ring $\mathcal{O}/\mathfrak{m}^{2e}$, since it ensures that this system will have good reduction in the sense of Definition 2.1 provided as long as the x_i do form an affine frame.

Let us now see how to generalise Algorithm 2.3 to the case where $\mathcal{O} = \mathbb{Z}_q[[t]]$. We can now see why working with quotients of $\mathbb{Z}_q[[t]]$ of the form $\mathbb{Z}_q[[t]]/(p, t)^e$ would be an issue: In step 2, we would obtain vectors $\kappa([\ell]x_i)$ with entries in $(p, t)^e/(p, t)^{2e}$, but since the ideal (p, t) is not principal, we would not be able to renormalise

the linear system defining the λ_i into a system of good reduction in the sense of Definition 2.1.

In contrast, by working with quotients of the form $(\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)$, we can generalise Algorithm 2.1 as follows: given a point $x \in J_0(\mathbb{F}_q)[\ell]$, we can first lift it p -adically to $J(\mathbb{Z}_q/p^e)[\ell]$ by using the original version of Algorithm 2.3 as described in [Mas19], and then, we can lift this lift t -adically to $\mathcal{J}((\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h))[\ell]$, by applying Algorithm 2.3 with $\mathcal{O} = (\mathbb{Z}_q/p^e\mathbb{Z}_q)[[t]]$ and $\varpi = t$. Indeed, even though $\mathfrak{m} = t\mathcal{O}$ is no longer maximal, the point is that the quotient $\mathcal{O}/\mathfrak{m}^h = (\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h)$ is still a local ring with “residue ring” $k = \mathbb{Z}_q/p^e$ which is still local, so that our generalisation of Makdisi to local rings is able to handle working over it.

We are thus able to lift torsion points from $J_0(\mathbb{F}_q)[\ell]$ to $\mathcal{J}((\mathbb{Z}_q/p^e\mathbb{Z}_q)[t]/(t^h))[\ell]$, and thus to extend our method [Mas19] to curves defined over $\mathbb{Q}(t)$.

Remark 2.2. In practice, when we identify elements $c \in \mathbb{Q}(t)$ from an approximation in $(\mathbb{Z}/p^e\mathbb{Z})[t]/(t^h)$ at the end of Algorithm 2.2, rather than first identifying c as an element of $\mathbb{Q}[t]/(t^h)$ by p -adic rational reconstruction and then as an element of $\mathbb{Q}(t)$ by Padé approximants over \mathbb{Q} , it is much more efficient to proceed in the reverse order, that is to say to first use Padé approximants over \mathbb{Q}_p so as to identify c as an element of $\mathbb{Q}_p(t)$ whose coefficients are known mod p^e , and then to reconstruct these coefficients as rational numbers. The reason for this is that unless h is quite small, the Taylor coefficients of c up to $O(t^h)$ will typically have a very large arithmetic height, so that identifying them would require the p -adic precision parameter e to be very high, which would drastically reduce the execution speed of the whole of Algorithm 2.2. For example, in Section 4.3 below, identifying the coefficients of a 2-division polynomial of a family of plane quartics requires $h = 128$, and experimentation has shown to us that this in turn requires $e = 4096$ with the first method, but only $e = 128$ with the second one.

3. COMPUTING WITH PLANE ALGEBRAIC CURVES

When we apply Strategy 1.1, on both occasions when we use our algorithm to compute an ℓ -division polynomial of a curve (first over $\mathbb{Q}(t)$ with Algorithm 2.2, and then over \mathbb{Q} with Algorithm 2.1), that curve is given to us by a plane equation, which is possibly singular. However, as explained in the previous Section, our ℓ -division polynomial algorithm relies on Makdisi’s algorithms, which require the curve to be represented by a Riemann-Roch space of high-enough degree.

The purpose of this Section is therefore to explain how one may perform explicit computations, such as determining the genus and computing Riemann-Roch spaces, with curves given by possibly singular plane models. Such functionalities are already available in some computer algebra packages such as [Magma], but our implementation of the ℓ -division polynomial algorithm is based on [Pari/GP], and converting data from [Magma] to [Pari/GP] is tedious and tends to break the flow of automation. We have therefore implemented our own package to compute with plane algebraic curves in [Pari/GP], in a way which is tailored towards our needs.

3.1. Representing the desingularised curve. Fix a ground field K over which one can algorithmically factor polynomials and perform linear algebra. For example, K could be \mathbb{Q} or $\mathbb{Q}(t)$. We also assume that K has characteristic 0, although this hypothesis is not essential (see Remark 3.4 below).

Suppose we are given an irreducible polynomial $f(x, y) \in K[x, y]$. It defines an affine curve C over K , but instead one typically wants to work with \tilde{C} , the desingularisation of the projective completion of C . Nonsingular points of C may be identified with points of \tilde{C} , so we only need a specific representation for points of \tilde{C} at infinity or above singular points of C .

One possibility would be to construct an explicit model of \tilde{C} made up of several charts in a higher-dimensional ambient space; however, this approach would lead to Gröbner bases calculations in many variables, which could be very slow. Therefore, we have instead decided to represent these points of \tilde{C} by formal series parametrisations. For instance, if $f(x, y) = xy + \dots$ so that C has a node at the origin, the two points of \tilde{C} corresponding to the two branches of this node can be represented by parametrisations of the form

$$x = t, y = t + O(t^2) \quad \text{and} \quad x = t, y = -t + O(t^2).$$

In order to compute such parametrisations, we can take advantage of the fact that the field $\overline{K}\{\{x\}\}$ of Puiseux series over \overline{K} contains an algebraic closure of $K(x)$: for each root $y = \sum_{m \geq m_0} a_m x^{m/e} \in \overline{K}\{\{x\}\}$ of $f(x, y) \in K(x)[y]$, we obtain the parametrisation

$$(3.1) \quad x = t^e, y = \sum_{m \geq m_0} a_m t^m \in \overline{K}((t)).$$

One might thus hope for a bijection between the points of \tilde{C} above $x = 0$ and parametrisations of the form $x = t^e, y \in \overline{K}((t))$ with x and y not both series in t^m for any $m \geq 2$; but unfortunately, this is not the case, because (3.1) can be reparametrised as

$$x = t'^e, y = \sum_{m \geq m_0} \zeta^m a_m t'^m$$

where $t = \zeta t'$ for any e -th root of unity $\zeta \in \overline{K}$. In particular, with this approach, there would be no hope to match the extension of K generated by the coefficients a_j with the field of definition of the corresponding point².

Fortunately, Duval [Duv89] has shown that these problems can be circumvented by allowing parametrisations of the form $x = bt^e, y \in \overline{K}((t))$ where $b \in \overline{K}$ is a constant:

Theorem 3.2. *Let $f(x, y) \in K[x, y]$ be irreducible of degree n in y . There exists a finite set of parametrisations*

$$x = b_j t^{e_j}, y = \sum_{m \geq m_j} a_{j,m} t^m$$

where for each j , the b_j and the $a_{j,m}$ lie in \overline{K} and span a finite extension L_j of K , and such that the n roots of f in $\overline{K}\{\{x\}\}$ are obtained without repetition as

$$y = \sum_{m \geq m_j} a_{j,m}^\sigma (\beta x^{1/e_j})^m$$

where σ ranges over the K -embeddings of L_j into \overline{K} and β ranges over $\{\beta \in \overline{K} \mid \beta^{-e_j} = b_j^\sigma\}$ (so that $t = \beta x^{1/e_j}$ is what one obtains when solving $x = b_j t^{e_j}$ for t).

²Unless of course K happens to contain the roots of unity of all orders, which typically will not be the case for the applications which we have in mind since we will be working over $K = \mathbb{Q}$ or $\mathbb{Q}(t)$.

This means that we have a Galois-equivariant bijection between this set of parametrisations and the set of places of the function field $K(C) = K(x)[y]/f(x, y)$ of C above $x = 0$, and therefore with the points of \tilde{C} above $x = 0$. In particular, we have

$$\sum_j e_j f_j = n$$

where the $f_j = [L_j : K]$ are the residue degrees and the e_j are the ramification indices, so that the L_j are the fields of definition of the corresponding points of \tilde{C} , and that the

$$(3.3) \quad \prod_{\sigma: L_j \hookrightarrow \bar{K}} \prod_{\beta^{-e_j} = b_j} \left(y - \sum_{m \geq m_j} a_{j,m}^\sigma (\beta x^{1/e_j})^m \right)$$

are the irreducible factors of $f(x, y)$ over $K((x))$. Note the analogy with the determination of the decomposition of a prime number p in a number field by studying the factorisation over \mathbb{Q}_p of a polynomial defining that number field.

Duval explains that these parametrisations can be computed as follows:

- (1) Draw the Newton polygon of $f(x, y)$, that is to say the lower convex hull of the points $(i, j) \in \mathbb{Z}^2$ such that the coefficient $a_{i,j}$ of $y^j x^i$ in $f(x, y) = \sum_{i,j} a_{i,j} y^j x^i$ is nonzero.
- (2) For each segment $pi + qj = r$ of the Newton polygon, where $p, q, r \in \mathbb{Z}$ and $\gcd(p, q) = 1$, find $u, v \in \mathbb{Z}$ such that $up + vq = 1$, and let $f_0 = \sum_{pi+qj=r} a_{i,j} x^j y^i$. Then for each $b \in \bar{K}$ such that $f_0(b^{-u}t^q, b^v t^p) = 0$, let $f_1(x, y) = f(b^{-u}x^q, b^v x^p(1 + y))$. If f_1 is nonsingular in y , stop; else, go back to step 1 with f replaced with f_1 .

Algorithm 3.1: Computing parametrisations.

The idea is that we use the Newton polygon to determine the valuation of the roots y of $f(x, y) = 0$, and then view f_0 as the “leading terms”, the other terms being thought of as higher-order perturbations. After finitely many iterations, the equation obtained will be nonsingular in y , so its roots can be found by Newton iteration. We thus obtain explicit parametrisations representing the points of \tilde{C} above $x = 0$ such that the field of definition of each point is the extension generated by the coefficients of the corresponding parametrisation. Parametrisations for the points above other values of x can be of course obtained similarly, by shifting the variable x appropriately.

Remark 3.4. The only reason why we have assumed that K has characteristic 0 was to ensure that $f(x, y) \in K(x)[y]$ splits completely over $\bar{K}\{\{x\}\}$. Theorem 3.2 and Algorithm 3.1 actually remain valid in positive characteristic π as long as there is no wild ramification, that is to say that none of the places has ramification index divisible by π , which is equivalent to having $\pi \nmid q$ whenever we consider a segment $pi + qj = r$ of a Newton polygon in step 1. All the algorithms presented in this section therefore remain valid in positive characteristic as long as \tilde{C} is at most tamely ramified as a cover of \mathbb{P}_x^1 , which in practice means we typically only

exclude really small characteristics such as 2, 3, or 5. Furthermore, by checking whether $\pi \mid q$ during the execution of algorithm 3.1, we can reliably detect when this algorithm is going to fail.

3.2. Regular differentials and the genus. Now that we have computed parametrisations representing singular points and points at infinity, we can find a basis of regular differentials on \tilde{C} . Indeed, it is well-known [DP13, 2.9] that for all $(i, j) \in \mathbb{Z}$ strictly in the interior of the full (as opposed to lower) convex hull of the support of $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j$, the differential $\omega_{i,j} = \frac{x^{j-1} y^{i-1}}{\partial f / \partial y} dx$ is regular everywhere except possibly at singular points, and that every regular differential on \tilde{C} is a K -linear combination of those. We thus obtain a basis of regular differentials by finding the linear combinations whose expansion along the parametrisations corresponding to singular points do not have any polar part, which amounts to linear algebra over K . In particular, we recover the genus of \tilde{C} as the size of this basis.

While there exist more direct ways to compute the genus, having an actual basis of regular differentials is very useful in practice. For example, it makes it possible to test whether the curve is hyperelliptic, and to find an explicit change of variables which puts it in Weierstrass form if it is [vH2]. And if the curve is not hyperelliptic, one can instead compute its canonical image, which provides a way of finding simpler models for curves defined by a complicated, highly-singular equation (for example, this is the approach that we followed in [Mas22, 3]).

3.3. Riemann-Roch spaces and extra functionalities. With our parametrisations representing singular points and points at infinity, we can also compute the integral closure

$$\mathcal{O} = \{s \in K(C) \mid \text{the only poles of } s \text{ are above } x = \infty\}$$

of $K[x]$ in $K(C)$ in a similar way to the number field case [Coh00, 2.4]: for each irreducible $d(x) \in K[x]$ such that $d(x)^2 \mid \text{disc}_y f(x, y)$, we construct a local basis by starting with the approximation $(\omega_j = y_1^{j-1})_{1 \leq j \leq n}$ where $y_1 = a(x)y$ and $a(x)$ is the leading coefficient of $f(x, y) \in K(x)[y]$, and refining it as long as we can find scalars $\lambda_j \in K[x]/(d(x))$ such that $\frac{\sum_j \lambda_j \omega_j}{d(x)}$ has no polar part when evaluated along the parametrisations representing the points above $d(x) = 0$. We then join these local bases into a $K[x]$ -basis of \mathcal{O} by computing a Hermite normal form over $K[x]$.

Thanks to this $K[x]$ -basis of \mathcal{O} , we can check whether C is geometrically irreducible, by finding which elements of \mathcal{O} are also regular above $x = \infty$.

We can also compute Riemann-Roch spaces, since it is easy, given a divisor on C , to compute a “common denominator” $d(x) \in K[x]$ such that the corresponding Riemann-Roch space is contained in $\frac{1}{d(x)}\mathcal{O}$.

This makes it possible to find conic models for curves of genus 0. If K is a number field, we can then test whether the curve has a rational point by a constructive version of Hasse-Minkowski, in which case another use of Riemann-Roch provides us with an explicit rational parametrisation of the curve [vH0]. Riemann-Roch spaces also make it possible to turn curves of genus 1 on which a rational point is known into elliptic curves in Weierstrass form.

Finally, now that we are able to compute Riemann-Roch spaces, we can initialise Makdisi’s algorithms so as to compute in the Jacobian of \tilde{C} .

We have implemented all the functionalities described in this section in [Pari/GP]. Our code, which compares quite decently to [Magma], is available for use in a development branch of [Pari/GP], which also contains the generalisation of [Mas19] to $\mathbb{Q}(t)$ described in Section 2.

4. EXAMPLES

In order to demonstrate the use of the algorithm described in Section 2, we have computed some division polynomials over $\mathbb{Q}(t)$. The calculations took place on the [PlaFRIM] cluster.

4.1. Warmup. As a sanity check, we first used our new algorithm in order to recover an equation for the 3-torsion of the elliptic surface \mathcal{E} defined by

$$y^2 = t(1 + 2t - t^2)(x^2 - 1)(t^2x^2 - 1)$$

that was the object of our attention in [Mas22]. Even though using Makdisi's algorithms on elliptic curves is obviously out-of-proportion, we instantaneously obtained the division polynomial

$$3x^8 + 4t(t^2 + 1)(t^2 - 2t - 1)x^6 + 6t^4(t^2 - 2t - 1)x^4 - t^8(t^2 - 2t - 1)^2 \in \mathbb{Q}(t)[x],$$

which is incomparably simpler than what we obtained in [Mas22] with [Pari/GP]'s `elldivpol` function, and even prettier than the nicest model that we were able to achieve in [Mas22]. To boost, this polynomial reminisces about $t = 0$ and $t^2 - 2t - 1 = 0$ being places of bad reduction of \mathcal{E} .

4.2. A hyperelliptic family. Encouraged by this first example, we then computed an ℓ -division polynomial for $\ell = 3$ of the curve over $\mathbb{Q}(t)$ of genus $g = 2$ corresponding to the hyperelliptic surface H defined by the equation

$$y^2 = x^6 - x^4 + (t - 1)(x^2 + x).$$

Remark 4.1. The equation $y^2 = x^6 - x^4 + t(x^2 + x)$ would have been more natural, but we shifted the parameter t so as to have good reduction at $t = 0$. We did the same for the previous example, but the polynomial which we presented there was the un-shifted version.

We chose to use the auxiliary prime $p = 17$, since having the ℓ -torsion defined over $\mathbb{Q}_{p^a}((t))$ then merely requires $a = 6$; and we computed the ℓ -torsion mod (p^e, t^h) for $e = 48$ and $h = 16$. The computation took 2 minutes, and we obtained an ℓ -division polynomial $R_{H,3}(x, t) \in \mathbb{Q}(t)[x]$ of degree $\ell^{2g} - 1 = 80$ and whose coefficients have numerators of degree up to 12 and coefficients of up to 27 decimal digits, and common denominator $d_H(t) = 3^3(t + 1)^2$.

This denominator can probably be explained by the fact that H has bad reduction at $t = -1$; even though it can be observed that $d_H(t)$ is not divisible by $t - 1$ whereas H clearly has bad reduction at $t = 1$ as well.

4.3. A plane quartic family. As a final example, we computed an ℓ -division polynomial for $\ell = 2$ of the family Q of plane quartics of generic genus $g = 3$ defined by the equation

$$x^4 + (2 - t)y^4 + 2x^3 + x(x + y) + (t - 1)(y + x^2 + x) = 0.$$

This time, we took $p = 5$ as it allows $a = 7$, and the accuracy parameters were $e = h = 128$. After one hour and a half, we obtained a division polynomial $R_{Q,2}(x, t) \in \mathbb{Q}(t)[x]$ of degree $\ell^{2g} - 1 = 63$ with common denominator $d_Q(x) = (t - 2)(2t - 3)^4 d_{22}(t)$ where $d_{22}(t) \in \mathbb{Z}[t]$ is irreducible of degree 22 and has leading coefficient 2^{16} , and whose coefficient numerators have degree up to 54 and coefficients of up to 39 digits.

It should be noted that one of the places of \mathbb{P}_t^1 at which Q has bad reduction has degree 14 over \mathbb{Q} ; since this must somehow be reflected in an anomalous behaviour of the specialisation of $R_{Q,2}$ at this value of t , this explains why the coefficients of $R_{Q,2}$ are so complicated, and why the t -adic accuracy ($h = 128$) required to identify them was so much larger than in the previous example. This in turn explains why this computation took so much longer than the previous one.

This time, most of the “geometric content” of the denominator, that is to say the factors $(2t - 3)^4$ and $d_{22}(t)$, do not correspond to places of bad reduction of Q (but $t - 2$ does), and should instead probably be interpreted as values of t for which the evaluation map $\alpha \in \mathbb{Q}(t)(\mathcal{J})$ fails to be defined on all the 2-torsion points (see Section 2 for the definition and context around α). However, it is still interesting to note that in all three examples, the “arithmetic content”, that is to say the leading coefficient of the common denominator, is a power of ℓ ; we do not know the explanation for this.

Remark 4.2. Our calculations rely on [Pari/GP]’s polynomial arithmetic, which unfortunately does not benefit from fast algorithms for multiplication of polynomials of high degree. In view of the high t -adic accuracy that it required, it is likely that the computation of $R_{Q,2}$ would have been faster if fast polynomial arithmetic had been available.

Remark 4.3. As explained in the Introduction, our identification of the coefficients of our division polynomials as elements of $\mathbb{Q}(t)$ from approximations in $\mathbb{Q}_p[[t]]$ is not rigorous. However, it is easy to convince oneself that these division polynomials are correct beyond reasonable doubt, for example by checking that their at nonzero values of t of good reduction has Galois group contained in $\mathrm{GSp}(2g, \ell)$, and that their ramification agrees what is predicted by Néron-Ogg-Shafarevich [ST68]. The geometric interpretation of the ramification of the specialisations of these division polynomials at bad values of t which we will establish in the next section is also evidence that their coefficients have been correctly identified.

5. DEGENERATION OF GALOIS REPRESENTATIONS AND THEIR RAMIFICATION

Disappointingly, the division polynomials $R_{H,3}(x, t)$ and $R_{Q,2}(x, t)$ which we have obtained in the previous Section are so complicated that neither [Magma] nor our plane curves package presented in Section 3 are able to determine their genus, let alone compute Riemann-Roch spaces required to use Makdisi’s algorithms to work in their Jacobian. As a result, we are unfortunately unable to conclude our calculation of the Galois representations occurring in the étale cohomology of the corresponding surfaces.

However, these division polynomials are still very valuable data, in that each of them encodes a family of Galois representations parametrised by $\mathbb{P}_{\mathbb{Q}}^1$.

To begin with, one easily checks with [Magma] that the specialisation of $R_{H,3}(x, t)$ at a rational value of t of good reduction of H (for example, at $t = 0$) has Galois

group $\mathrm{GSp}(4, 3)$ over \mathbb{Q} , which proves that $R_{H,3}(x, t)$ has Galois group $\mathrm{GSp}(4, 3)$ over $\mathbb{Q}(t)$; therefore, most specialisations of $R_{H,3}(x, t)$ will have Galois group $\mathrm{GSp}(4, 3)$ by Hilbert irreducibility, so that the polynomial $R_{H,3}(x, t)$ that we have computed may be viewed as a family (in t) of polynomials (in x) with generic Galois group $\mathrm{GSp}(4, 3)$. One similarly checks that $R_{Q,2}(x, t)$ defines a family of polynomials with generic Galois group $\mathrm{GSp}(6, 2) = \mathrm{Sp}(6, 2)$, which happens to be a simple group.

Furthermore, it is especially interesting to study how these families of Galois representations degenerate at values $t = t_0$ which are places of bad reduction of the corresponding curves over $\mathbb{Q}(t)$. In particular, we would like to understand geometrically where the ramification of these degenerate representations comes from, in a manner similar to the Néron-Ogg-Shafarevich criterion [ST68] for good fibres.

By analogy with the good fibres, we would thus expect that ramification at a prime $p \neq \ell$ results from “something bad” happening to “the” bad fibre $S_{t_0} \bmod p$. However, this idea is not mathematically meaningful, not only because the fibre is already bad over \mathbb{Q} , but also because this fibre is not canonically defined since, as explained in Remark 1.4, studying ramification along this family implies working over the 2-dimensional basis $\mathbb{P}_{\mathbb{Z}}^1$, so that we no longer have nice theories of minimal models of fibred surfaces nor of Néron models of the Jacobian.

Suppose thus for a moment that we dropped the arithmetic dimension and worked over \mathbb{Q} . When calculating the special fibre, the fact we are working over \mathbb{Q} would mean that we are inverting a finite set Π_{t_0} of primes of \mathbb{Q} ; in other words, these are the primes which we would have to handle separately if we now wanted to work over \mathbb{Z} because we suddenly remembered that we also have an arithmetic dimension. In colourful but approximate language, we could say that Π_{t_0} is the set of primes p such that the determination of the special fibre of S at $t = t_0$ does not commute with reduction mod p .

By analogy with Néron-Ogg-Shafarevich, we are led to the following explanation for ramification:

Conjecture 5.1. *The primes at which the degenerate representation at $t = t_0$ ramifies are contained³ in $\Pi_{t_0} \cup \{\ell\}$.*

We are going to provide evidence for this conjecture by checking it on the family of representations attached to the surfaces H and Q introduced in Section 4. We will first determine the primes at which the degenerate representations ramify in Section 5.1, and we will then compare this list of primes with the geometric picture in Section 5.2.

Remark 5.2. S. Morel has pointed out to the author that the theory of *nearby cycles* exposed in [SGA7II] may lead to a proof of this Conjecture 5.1. Such a proof does not however seem to be straightforward, because this theory is limited to Lefschetz pencils, and also because the connection between the degenerate representation at a bad fibre $t = t_0$ and the restriction to the decomposition group at $t = t_0$ of the representation of $\mathrm{Gal}(\overline{\mathbb{Q}(t)}/\mathbb{Q}(t))$ defined by the division polynomial of the curve $\mathcal{S}/\mathbb{Q}(t)$ is not completely obvious.

³Recall that Néron-Ogg-Shafarevich states that the ℓ -power torsion ramifies exactly at ℓ and at the primes of bad reduction of the Jacobian. However, it may happen that the ℓ -torsion only ramifies at a strict subset of these primes; furthermore, the Jacobian may have good reduction at a prime p even though the curve itself has bad reduction at p .

Remark 5.3. Instead of defining Π_{t_0} in terms of special fibres of the minimal regular model, it would also make sense to consider the semistable fibres. The fact that we are working over a 2-dimensional basis makes it difficult to guess which choice is the right one for Conjecture 5.1 to be correct, so we content ourselves with this imprecision. See the study of the fibre of H at $t = \infty$ in Section 5.2 below for a case where considering the semistable fibre is necessary to explain ramification.

5.1. Decomposition of the bad places. The bad places of our hyperelliptic family H defined by

$$y^2 = x^6 - x^4 + (t - 1)(x^2 + x)$$

are easily determined by examining the discriminant of the right-hand side, and turn out to be $t = 1$, $t = -1$, $t = 283/256$, and $t = \infty$. In order to analyse the degeneration of the family of mod 3 Galois representations defined by $R_{H,3}(x, t)$ at these places, one must not simply substitute these values for t , as this would be as incorrect as trying to understand the decomposition of a prime p in a number field by factoring a polynomial mod p without taking into consideration the index of the order attached to this polynomial. Instead, we must study the factorisation over $\mathbb{Q}((t))$ of versions of $R_{H,3}(x, t)$ shifted in such a way that the bad place under consideration is now $t = 0$. In view of (3.1), this is equivalent to determining the ramification in t and the field of definitions of the points above $t = 0$ of the desingularisation of the curve $R_{H,3}(x, t) = 0$, which we can achieve thanks to our implementation of Duval’s method described in Section 3.1. We thus obtain the following data:

t	Place decomposition	Galois group	Ramification
1	$\mathbb{Q}(\sqrt{3})^1 \cdot \mathbb{Q}(\sqrt{-1})^3 \cdot (\mathbb{Q}(\zeta_9)^+(\sqrt{-1}))^9 \cdot (\mathbb{Q}(\zeta_{36})^+)^3$	$(\mathbb{Z}/36\mathbb{Z})^\times$	2, 3
-1	$\mathbb{Q}(\sqrt{-21})^1 \cdot K_6^1 \cdot K_{18}^1 \cdot K_{18}^{\prime 3}$	$C_2 \times C_3 \cdot S_3^2$	2, 3, 7, 11
$\frac{283}{256}$	$\mathbb{Q}(\sqrt{-14})^1 \cdot K_{18}^{\prime\prime 3} \cdot K_{24}^1$	$(C_2 \times C_3 \rtimes S_3) \cdot S_4$	2, 3, 7, 11
∞	$\mathbb{Q}^2 \cdot \mathbb{Q}^6 \cdot \mathbb{Q}(\sqrt{3})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^4 \cdot \mathbb{Q}(\sqrt[4]{12})^{12}$	D_4	2, 3

Table 5.1: Decomposition of the bad places of H .

In this table, the second column shows the decomposition of the place of $\mathbb{Q}(t)$ in the function field $\mathbb{Q}(t)[x]/(R_{H,3}(x, t))$; for example, there are five places above $t = \infty$, two with residue field \mathbb{Q} and respective ramification indices 2 and 6, one with residue field $\mathbb{Q}(\sqrt{3})$ and ramification index 4, and two with residue field $\mathbb{Q}(\sqrt[4]{12})$ and respective ramification indices 4 and 12. The third column shows the Galois group⁴ of the compositum of the Galois closures of the residue fields, and the last column lists the prime numbers which ramify in this Galois closure, or, equivalently, in at least one of the residue fields. Still in this table, $\mathbb{Q}(\zeta_m)^+$ denotes the intersection of the cyclotomic field $\mathbb{Q}(\zeta_m)$ with \mathbb{R} , and K_d, K'_d, K''_d , and so on stand for pairwise non-isomorphic number fields of degree d . As for Galois groups, $C_n, D_{2n},$ and S_n respectively denote cyclic, dihedral, and symmetric groups, and $A \cdot B$ stands for a nonsplit group extension with normal subgroup A and quotient B . For $t = 1$,

⁴This Galois group is thus the image of the degenerate Galois representation. It is slightly disappointing to the author that these groups are not particularly exciting subgroups of the symplectic group; one may hope that other surfaces would yield more exotic Galois groups.

we have exceptionally expressed the Galois group as $(\mathbb{Z}/36\mathbb{Z})^\times$ instead of $C_6 \times C_2$ because the Galois closure is the 36th cyclotomic field.

As for our family of quartics Q , the places of bad reduction are $t = 1$, $t = 2$, $t = \infty$, as well as the place of degree 14 mentioned in the previous Section. The high degree of this last place makes explicit computations with it impractical, so we ignore it from now on. We obtain the following data:

t	Place decomposition	Galois group	Ramification
1	$\mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot \mathbb{Q}^1 \cdot K_8^1 \cdot K_8^1 \cdot K_8'^2 \cdot K_8''^2 \cdot K_{12}^1$	$C_2^3 \rtimes S_4$	2, 229
2	$\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}^8 \cdot \mathbb{Q}(\sqrt{2})^4 \cdot \mathbb{Q}(\sqrt{2}, \sqrt{15})^8$	C_2^2	2, 3, 5
∞	$\mathbb{Q}^1 \cdot \mathbb{Q}^2 \cdot \mathbb{Q}^4 \cdot K_3^2 \cdot K_3^4 \cdot K_6^1 \cdot K_8'''^4$	$S_4 \times C_2$	2, 23

Table 5.2: Decomposition of some of the bad places of Q .

5.2. Visualising ramification on the special fibre. We now check that Conjecture 5.1 provides a satisfactory explanation for the ramification of these degenerate representations. We will also elucidate the nature of some of the residue fields along the way. We denote by π the characteristic at which we calculate the special fibre.

The fibre of H at $t = 1$.

The surface H is not regular above $t = 1$, but in characteristic $\pi \neq 2$, it becomes regular after one blowup, and its special fibre then consists of two rational curves arranged as shown on Figure 5.1:

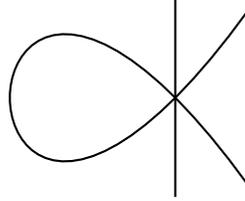


Figure 5.1: The special fibre of H at $t = 1$ when $\pi \neq 2$.

In contrast, in characteristic $\pi = 2$, it takes many more blowups to obtain a regular model of H above $t = 1$. This explains the ramification at $p = 2$ observed in Table 5.1 for $t = 1$. As for ramification at $p = 3$, it is simply explained by the fact that we are looking at 3-torsion.

The fibre of H at $t = -1$.

For $t = -1$, in characteristic $\pi \notin \{2, 7, 11\}$, we again obtain a regular surface after one blowup. Its special fibre is made up of an elliptic curve and a rational curve, as shown on Figure 5.2.

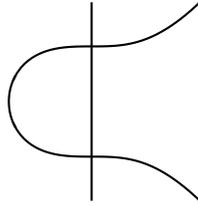


Figure 5.2: The special fibre of H at $t = -1$ when $\pi \notin \{2, 7, 11\}$.

Our plane curve package described in Section 3 informs us that over \mathbb{Q} , the elliptic component is the curve of [LMFDB] label 176.a2, whose conductor $176 = 2^4 \cdot 11$. As a result, in characteristic $\pi = 11$, the elliptic curve degenerates, and the special fibre becomes what is shown on Figure 5.3:

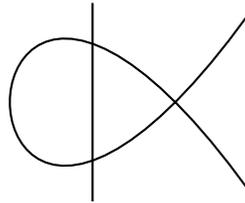


Figure 5.3: The special fibre of $H \bmod 11$ at $t = -1$. Both components are now rational.

This explains why we observed ramification at $p = 11$. As for $\pi = 2$, the special fibre is the same as for $t = 1$, since t is defined over \mathbb{Z} and $-1 \equiv 1 \pmod{2}$.

To summarise, ramification at $p \in \{2, 11\}$ is explained by the elliptic component having bad reduction, and ramification at $p = 3$ is explained by the fact that we are looking at 3-torsion; however, it still remains to explain ramification at $p = 7$.

A closer inspection of the special fibre over \mathbb{Q} (as shown on Figure 5.2) shows that the intersection points of the two components are not rational, but defined over $\mathbb{Q}(\sqrt{7})$ and Galois-conjugates of each other; as a result, when we reduce mod $\pi = 7$, these intersection points coalesce, and accordingly the special fibre in characteristic $\pi = 7$ is what is shown on Figure 5.4, which finally explains ramification at $p = 7$:

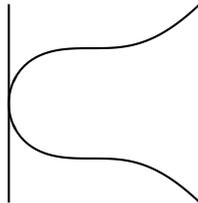


Figure 5.4: The special fibre of $H \bmod 7$ at $t = -1$.

Remark 5.4. As one would expect, our residue fields pick up the 3-torsion of the elliptic curve component of the special fibre. More specifically, this elliptic

curve 176.a2 acquires two of its 3-torsion points over $\mathbb{Q}(\sqrt{-1})$, whereas each of its remaining six points of order 3 is defined over one of the Galois conjugates of a number field F of degree 6. The field K_6 appearing in Table 5.1 is actually an extension of $\mathbb{Q}(\sqrt{-1})$ of degree 3 and relative discriminant $(1 + \sqrt{-1})^2 \cdot 3^3 \cdot 7$, whereas the field K_{18} appearing in the same table is an extension of F of degree 3 ramified only above 2 and 7. The fact that these extensions have degree 3 can be interpreted in terms of generalised Jacobians, since we are looking at 3-torsion. Curiously, there does not seem to be a similar interpretation for K'_{18} , but we still note that K_{18} and K'_{18} have the same Galois closure, which also contains K_6 .

The fibre of H at $t = \infty$.

The surface H is actually already regular at $t = \infty$ in any characteristic, so we can directly visualise its special fibre, which turns out to have a rather nasty singularity:

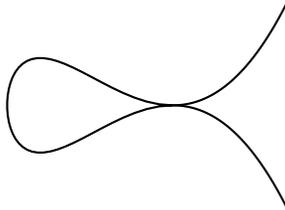


Figure 5.5: The special fibre of H at $t = \infty$ in any characteristic.

The fact that H is regular at $t = \infty$ even mod $\pi = 2$ fails to explain why we observed ramification at $p = 2$ in Table 5.1. However, the special fibre which we have obtained is clearly not semistable, so we may be looking at the “wrong” fibre (see Remark 5.3 above).

In order to investigate further, we can look in the direction of the semistable fibre, which means we must perform a ramified base change [IM98, 3.47]. The simplest candidate is to base-change to $\mathbb{Q}(t^{1/2})$, meaning that we replace t with t^2 in our equation. This results in H no longer being regular, even in characteristic $\pi = 0$; after several blowups, we find that in characteristic $\pi \neq 2$, the special fibre is made up of four rational curves, one of which has multiplicity two, as shown on Figure 5.6:

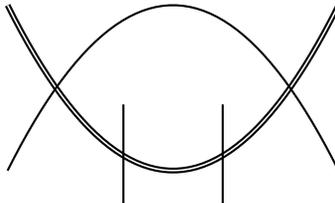


Figure 5.6: The special fibre of the base change of H to $\mathbb{Q}(t^{1/2})$ at $t = \infty$ in characteristic $\pi \neq 2$.

In contrast, in characteristic $\pi = 2$, the desingularisation requires more blowups, which finally explains the ramification that we observed at $p = 2$.

Remark 5.5. Because of the presence of a double component, the special fibre which we have obtained after base-changing to $\mathbb{Q}(t^{1/2})$ is still not semistable, and a further base change would be required to remedy this. However, as explained in Remark 5.3, since we do not have a clear notion of “good” model, we content ourselves with this reasonably satisfying explanation.

The fibre of H at $t = 283/256$.

In characteristic $\pi \notin \{2, 3, 7, 11\}$, H is already regular at $t = 283/256$, and its special fibre is a curve of genus 1 with a nodal self-intersection. Over \mathbb{Q} , the desingularisation of this fibre is the elliptic curve of [LMFDB] label 528.c2, whose conductor is $528 = 2^4 \cdot 3 \cdot 11$, and as expected, the phenomenon described in Remark 5.4 occurs again, in that the number field K_{24} displayed in Table 5.1 is an extension of degree 3 of the field of degree 8 over the Galois conjugates of which the points of order 3 of this elliptic curve are defined. We do not, however, have a similar interpretation for the field K''_{18} , but we note that its Galois closure is the same as that of K_{24} , and also contains the other residue field $\mathbb{Q}(\sqrt{-14})$ appearing in the corresponding row of Table 5.1.

In characteristics $\pi = 2, 3, 7, 11$, we respectively have $283/256 \equiv \infty, 1, -1, -1$, which are cases for which we have already found an explanation for the corresponding ramification.

The fibre of Q at $t = 1$.

We now proceed to the same analysis of ramification for the family of plane quartics Q . At $t = 1$, in characteristic $\pi \notin \{2, 229\}$, we find that the special fibre has three components, two of which are rational, whereas the third one has genus 2; see Figure 5.7. Over \mathbb{Q} , our plane curves package informs us that the component of genus 2 is isomorphic to the hyperelliptic curve of equation $y^2 = x(x^4 - x + 1)$ whose [LMFDB] label is 29312.a.58624.1; in particular, the conductor of its Jacobian is $29312 = 2^7 \cdot 229$. As expected, the phenomenon described in Remark 5.4 occurs again, in that the number field K_8 displayed in Table 5.2 is defined by the irreducible polynomial $x^8 - x^2 + 1$ and is therefore clearly a quadratic extension of a the quartic field of discriminant 229 defined by $x^4 - x + 1$ over which the Jacobian of this hyperelliptic curve acquires a point of order 2. We do not have any similar interpretation for the fields K'_8, K''_8 , nor K_{12} appearing in the same row of this table, but we still mention that K_8, K'_8 , and K''_8 share the same Galois closure, which is a quadratic extension of the Galois closure of K_{12} .

Since 229 divides the discriminant of this hyperelliptic curve, when we reduce mod $\pi = 229$, this curve degenerates into a curve of genus 1 with a nodal self-intersection:



Figure 5.7: The special fibre of Q at $t = 1$ when $\pi \notin \{2, 229\}$ (left), vs. mod 229 (right).

This explains the ramification that we have observed at $p = 229$. As for the ramification at $p = 2$, it is explained both by the fact that we are now looking at the 2-torsion, and the fact that determining the special fibre in characteristic $\pi = 2$ requires extra blowups.

The fibre of Q at $t = 2$.

In characteristic $\pi \notin \{3, 5\}$, we obtain a special fibre made up of three rational components, one of which has a cusp, and which are arranged as shown on figure 5.8.

Working in characteristic $\pi = 5$ does not result in requiring more blowups; however, the rightmost fibre, which is a conic, degenerates into a union of two curves, which explains the ramification at $p = 5$:



Figure 5.8: The special fibre of Q at $t = 2$ when $\pi \notin \{3, 5\}$ (left), vs. mod 5 (right).

The same degeneration occurs mod $\pi = 3$, and furthermore resolving the singularities of Q at $t = 2$ also requires more blowups in characteristic 3. Both these facts explain the ramification at $p = 3$.

The fibre of Q at $t = \infty$.

Mod $\pi \notin \{2, 23\}$, our model for Q is already regular at $t = \infty$, whence a special fibre formed of one component of genus 1 with a nasty self-intersection, as shown on Figure 5.9. Over \mathbb{Q} , our plane curve package informs us that the desingularisation of this curve is the elliptic curve with [LMFDB] label 92.a1, whose conductor is $92 = 2^2 \cdot 23$; and the field K_3 displayed in Table 5.2, which is the cubic field of discriminant -23 , is also the field over which this elliptic curve acquires a point of order 2. Furthermore, K_6 is a quadratic extension of K_3 which is only ramified above 2 and 23. We do not have a similar explanation for K_8''' , but we observe that the Galois closure of K_8''' , which has degree 48, contains K_6 and therefore K_3 .

That 23 divides the conductor of this elliptic curve also results in this curve acquiring an extra node mod $\pi = 23$, which explains the ramification at $p = 23$.

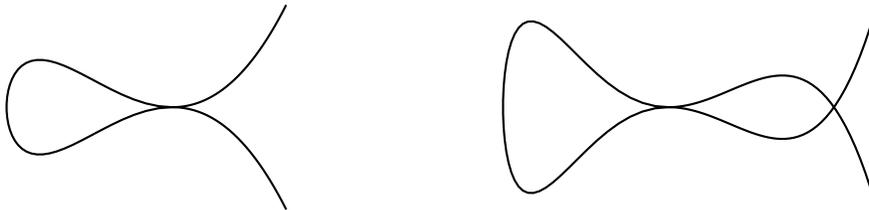


Figure 5.9: The special fibre of Q at $t = \infty$ when $\pi \notin \{2, 23\}$ (left), vs. mod 23 (right).

REFERENCES

- [Coh00] Cohen, Henri, **Advanced topics in computational number theory**. Graduate Texts in Mathematics, 193. Springer-Verlag, New York, 2000. ISBN: 0-387-98727-4.
- [DP13] Deconinck, Bernard; Patterson, Matthew S., **Computing with plane algebraic curves and Riemann surfaces: the algorithms of the Maple package “al-curves”**. pp. 67–123 in **Computational approach to Riemann surfaces**, 2013.
- [Duv89] Duval, Dominique, **Rational puiseux expansions**. *Compositio mathematica* 70, no. 2 (1989), 119–154.
- [GT94] van Geemen, Bert; Top, Jaap, **A non-selfdual automorphic representation of GL_3 and a Galois representation**. *Invent. Math.* 117 (1994), no. 3, 391–401.
- [IM98] Harris, Joe; Morrison, Ian, **Moduli of curves**. Graduate Texts in Mathematics, 187. Springer-Verlag, New York, 1998. ISBN: 0-387-98438-0; 0-387-98429-1.
- [KM04] Khuri-Makdisi, Kamal, **Linear algebra algorithms for divisors on an algebraic curve**. *Math. Comp.* 73 (2004), no. 245, 333–357.
- [KM07] Khuri-Makdisi, Kamal, **Asymptotically fast group operations on Jacobians of general curves**. *Mathematics of Computation* 76 (2007), no. 260, 2213–2239.
- [LMFDB] The LMFDB Collaboration, **The L-functions and Modular Forms Database**. <http://www.lmfdb.org>.
- [Magma] Bosma, Wieb; Cannon, John; Playoust, Catherine, **The Magma algebra system. I. The user language** *J. Symbolic Comput.*, 24 (1997), 235–265.
- [Mas] Mascot, Nicolas, Personal web page. <https://www.maths.tcd.ie/~mascotn/>.
- [Mas19] Mascot, Nicolas, **Hensel-lifting torsion points on Jacobians and Galois representations**. *Mathematics of Computation*, 2020, vol. 89, no. 323, 1417–1455.
- [Mas22] Mascot, Nicolas, **Explicit computation of a Galois Representation attached to an eigenform over SL_3 from the $H_{\text{ét}}^2$ of a surface**. *Foundations of Computational Mathematics*, 2022, 1–25.
- [MilEC] Milne, James S., **Lectures on Etale cohomology**, version 2.21. <https://www.jmilne.org/math/>.
- [MO15] Madore, David A.; Orgogozo, Fabrice, **Calculabilité de la cohomologie étale modulo ℓ** . *Algebra Number Theory* 9 (2015), no. 7, 1647–1739.
- [Pari/GP] The PARI Group, **PARI/GP development version 2.16.0**, Bordeaux, 2023. <http://pari.math.u-bordeaux.fr/>.
- [PlaFRIM] **Plateforme Fédérative pour la Recherche en Informatique et Mathématiques**, supercomputing cluster, <https://www.plafrim.fr/>.
- [PTvL15] Poonen, Bjorn; Testa, Damiano; van Luijk, Ronald, **Computing Néron-Severi groups and cycle class groups**. *Compos. Math.* 151 (2015), no. 4, 713–734.
- [ST68] Serre, Jean-Pierre; Tate, John, **Good reduction of abelian varieties**. *Annals of Mathematics* (1968), 492–517.
- [SGA4 $\frac{1}{2}$] Deligne, Pierre, **Cohomologie étale**. Séminaire de géométrie algébrique du Bois-Marie (SGA 4 $\frac{1}{2}$). *Lecture Notes in Mathematics*, 569. Springer-Verlag, Berlin, 1977. ISBN: 3-540-08066-X; 0-387-08066-X.
- [SGA7II] Deligne, Pierre; Katz, Nicholas, **Groupes de monodromie en géométrie algébrique II**. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II). *Lecture Notes in Mathematics*, 340. Springer-Verlag, Berlin-New York, 1973.
- [vH0] van Hoeij, Mark, **Computing parameterizations of rational algebraic curves**. *Proceedings of the international symposium on Symbolic and algebraic computation*, 1994, 187–190.
- [vH2] van Hoeij, Mark, **An algorithm for computing the Weierstrass normal form of hyperelliptic curves**. arXiv:0203130, 2002.