Explicit arithmetic of Jacobians of generalized Legendre curves over global function fields

Lisa Berger

Chris Hall

René Pannekoek

Jennifer Park

Rachel Pries

Shahed Sharif

Alice Silverberg

Douglas Ulmer

Author address:

Department of Mathematics, Stony Brook University, Stony Brook, NY 11794, USA
E-mail address: lbrgr@math.sunysb.edu

Department of Mathematics, Western University, London, Ontario, N6A 5B7, Canada
E-mail address: chall69@uwo.ca

Department of Mathematics, Imperial College London SW7 2AZ, United Kingdom
E-mail address: pannekoek@gmail.com

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA
E-mail address: jmypark@umich.edu

Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA
E-mail address: pries@math.colostate.edu

Department of Mathematics, CSU San Marcos, San Marcos, CA 92096, USA
E-mail address: ssharif@csusm.edu

Department of Mathematics, UC Irvine, Irvine, CA 92697, USA
E-mail address: asilverb@math.uci.edu

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332, USA
E-mail address: ulmer@math.gatech.edu

Contents

Introduction 1
Historical background 2
The main results 3
Overview of the paper 4
Guide 5
Notation 6

Chapter 1. The curve, explicit divisors, and relations 7
1.1. A generalization of the Legendre curve 7
1.2. Explicit points and the visible subgroup 9
1.3. Relations 11
1.4. Torsion 12
1.5. First main theorem 14
1.6. Complement: Other curves 15

Chapter 2. Descent calculations 17
2.1. The isogeny ϕ 17
2.2. The homomorphism $(x - T)$ 18
2.3. The image of $(x - T)$ 21
2.4. Proof of the main theorem 21

Chapter 3. Minimal regular model, local invariants, and domination by a product of curves 23
3.1. Models 23
3.2. Local invariants of the Néron model 32
3.3. Domination by a product of curves 33

Chapter 4. Heights and the visible subgroup 39
4.1. Height pairing 39
4.2. A group-theoretic pairing 49
4.3. Structure of the visible subgroup 51
4.4. Discriminants 56

Chapter 5. The L-function and the BSD conjecture 59
5.1. The L-function 59
5.2. The conjecture of Birch and Swinnerton-Dyer for J 61
5.3. Elementary calculation of the L-function 62
5.4. Ranks 65

Chapter 6. Analysis of $J[p]$ and $\mathrm{NS}(\mathcal{X}_d)_{\mathrm{tor}}$ 71
6.1. Kodaira-Spencer and p-torsion 71

6.2. Néron-Severi of $\mathcal{X}_d$ is torsion-free 81

Chapter 7. Index of the visible subgroup and the Tate-Shafarevich group 91
7.1. Visible versus Mordell-Weil 91
7.2. Tamagawa number 94
7.3. Application of the BSD formula 98

Chapter 8. Monodromy of ℓ-torsion and decomposition of the Jacobian 101
8.1. Statement of results 101
8.2. New and old 102
8.3. Endomorphism rings 104
8.4. The Λ-module structure of $J[\ell]$ 107
8.5. Monodromy of $J[\lambda]$ 108
8.6. Independence 113
8.7. Conclusion 118

Appendix A. An additional hyperelliptic family 121
A.1. Introduction 121
A.2. The BSD conjecture 121
A.3. Descent 122
A.4. Degree of the L-function 126
A.5. Additional remarks 127

Bibliography 129

Abstract

We study the Jacobian J of the smooth projective curve C of genus $r-1$ with affine model $y^r = x^{r-1}(x+1)(x+t)$ over the function field $\mathbb{F}_p(t)$, when p is prime and $r \geq 2$ is an integer prime to p. When q is a power of p and d is a positive integer, we compute the L-function of J over $\mathbb{F}_q(t^{1/d})$ and show that the Birch and Swinnerton-Dyer conjecture holds for J over $\mathbb{F}_q(t^{1/d})$. When d is divisible by r and of the form $p^\nu + 1$, and $K_d := \mathbb{F}_p(\mu_d, t^{1/d})$, we write down explicit points in $J(K_d)$, show that they generate a subgroup V of rank $(r-1)(d-2)$ whose index in $J(K_d)$ is finite and a power of p, and show that the order of the Tate-Shafarevich group of J over K_d is $[J(K_d) : V]^2$. When $r > 2$, we prove that the "new" part of J is isogenous over $\overline{\mathbb{F}_p(t)}$ to the square of a simple abelian variety of dimension $\phi(r)/2$ with endomorphism algebra $\mathbb{Z}[\mu_r]^+$. For a prime ℓ with $\ell \nmid pr$, we prove that $J[\ell](L) = \{0\}$ for any abelian extension L of $\overline{\mathbb{F}}_p(t)$.

2010 *Mathematics Subject Classification.* 11G10, 11G30, (primary), 11G40, 14G05, 14G25, 14K15 (secondary).

Key words and phrases. curve, function field, Jacobian, abelian variety, finite field, Mordell-Weil group, torsion, rank, L-function, Birch and Swinnerton-Dyer conjecture, Tate-Shafarevich group, Tamagawa number, endomorphism algebra, descent, height, Néron model, Kodaira-Spencer map, monodromy.

This project was initiated at the workshop on Cohomological methods in abelian varieties at the American Institute of Mathematics, March 26–30, 2012. We thank AIM and the workshop organizers for making this paper possible. The first seven authors thank the last for initiating this project at the AIM workshop and for his leadership of the project. Author Hall was partially supported by Simons Foundation award 245619 and IAS NSF grant DMS-1128155. Author Park was partially supported by NSF grant DMS-10-69236 and NSERC PGS-D and PDF grants. Author Pries was partially supported by NSF grants DMS-11-01712 and DMS-15-02227. Author Silverberg was partially supported by NSF grant CNS-0831004. Author Ulmer was partially supported by Simons Foundation award 359573. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the supporting agencies. We also thank Karl Rubin and Yuri G. Zarhin for helpful conversations and an anonymous referee for a careful reading and productive comments.

Introduction

It is known that for every prime p and every genus $g > 0$, there exist Jacobians J of dimension g over the rational function field $K = \mathbb{F}_p(t)$ such that the rank of $J(K)$ is arbitrarily large [**49**]. One of the main goals in this work is to make this phenomenon more explicit. Specifically, for any prime number p and infinitely many positive integers g, we exhibit a curve of genus g over K and explicit divisors on that curve that generate a subgroup V of large rank in the Mordell-Weil group of the Jacobian of the curve. We also prove precise results on the conjecture of Birch and Swinnerton-Dyer for these Jacobians, giving information about the index of the subgroup V in the Mordell-Weil group, and about the Tate-Shafarevich group of the Jacobian.

All of this work generalizes previous results in the case $g = 1$ from [**52, 10, 53**]. In those papers, the authors analyze the arithmetic of the Legendre curve $y^2 = x(x + 1)(x + t)$, an elliptic curve defined over K. For each field K_d appearing in a tower of field extensions of K, they prove that the Legendre curve over K_d satisfies the conjecture of Birch and Swinnerton-Dyer. Furthermore, for infinitely many d, they find explicit divisors on the Legendre curve that generate a subgroup V of large rank in the Mordell-Weil group. They bound the index of the subgroup V in the Mordell-Weil group and give results about the Tate-Shafarevich group.

The statements of the main results in this paper are quite parallel to those for the Legendre elliptic curve. However, since we work in higher genus—where the curve and its Jacobian are distinct objects—the proofs are more complicated and require more advanced algebraic geometry. For example, we have to construct the regular minimal model of our curve from first principles (rather than relying on Tate's algorithm), the relations among the points we write down are less evident, and the analysis of torsion in the Jacobian requires more work. Moreover, our results cast new light on those of [**52**] insofar as we determine the structure of the group of points under consideration as a module over a suitable group ring.

As part of our analysis, we prove several results in more generality than needed here, and these results may be of use in analyzing the arithmetic of other curves over function fields. These include a proof that the Néron-Severi group of a general class of surfaces is torsion-free (Propositions 6.18 and 6.21) and an integrality result for heights on Jacobians (Proposition 7.2). We also note that the monodromy questions answered in the last chapter inspired a related work [**18**] in which a new method to compute monodromy groups of superelliptic curves is developed.

Historical background

Let g be a positive integer. Over a fixed number field, it is not known whether there exist Jacobian varieties of dimension g whose Mordell-Weil groups have arbitrarily large rank. In contrast, there are several results of this type over a fixed function field, some of which we describe below.

In [**46**], Shafarevich and Tate construct elliptic curves with arbitrarily large rank over $\mathbb{F}_q(t)$. The curves in their construction are isotrivial, i.e., each is isomorphic, after a finite extension, to a curve defined over $\mathbb{F}_q$.

In [**42**], Shioda studies the elliptic curve over $k(t)$ defined by $y^2 = x^3 + at^n x + bt^m$ where k is an arbitrary field and $a, b \in k$ satisfy $ab(4a^3t^{3n} + 27b^2t^{2m}) \neq 0$. When $\mathrm{char}(k) = 0$, he proves the rank of the Mordell-Weil group has a uniform upper bound of 56, and he gives necessary and sufficient conditions on m and on n for meeting this bound. When $\mathrm{char}(k) = p \equiv -1 \pmod 4$ and when $d = (p^\nu + 1)/2$ as ν varies over positive odd integers, he proves that the elliptic curves over $\overline{k}(t)$ defined by $y^2 = x^3 + x + t^d$ achieve arbitrarily large rank. These curves are given as examples of the main result of [**42**], in which Shioda computes the Picard number for Delsarte surfaces. Fundamental to this work is the realization of any Delsarte surface as a quotient of a Fermat surface.

Motivated by this work of Shioda, in [**50**] Ulmer proves that the non-isotrivial elliptic curve $y^2 + xy = x^3 - t$ over $\mathbb{F}_p(t)$ obtains arbitrarily large rank over the fields $\mathbb{F}_p(t^{1/d})$, where d ranges over divisors of $p^n + 1$. He realizes the corresponding elliptic surface as a quotient of a Fermat surface; from earlier work of Shioda and Katsura [**44**], this Fermat surface admits a dominant rational map from a product of Fermat curves. It follows that this elliptic curve satisfies the conjecture of Birch and Swinnerton-Dyer. Furthermore, the zeta function of the elliptic surface can be determined from that of the Fermat surface. Using Jacobi sums, lower bounds are found for the rank of the elliptic curve over towers of function fields.

The geometric construction in [**44**] is later generalized in the work of Berger [**5**], where towers of surfaces dominated by products of curves are constructed as suitable blow-ups of products of smooth curves. In [**50**], Ulmer elaborates on the geometry and arithmetic of this construction, proving a formula for the ranks of the Jacobians of the curves constructed in [**5**].

In [**55**], Ulmer and Zarhin combine this rank formula with work on endomorphisms of abelian varieties. For k a field of characteristic zero, they construct absolutely simple Jacobians over $k(t)$ with bounded ranks in certain towers of extensions of $k(t)$. As one example, they prove that the Mordell-Weil group of the Jacobian of the genus g curve defined by $ty^2 = x^{2g+1} - x + t - 1$ has rank $2g$ over the field $\overline{\mathbb{Q}}(t^{1/p^r})$ for any prime power p^r. In [**34**], Pries and Ulmer introduce an analogous construction of surfaces that are dominated by a product of curves at each layer in a tower of Artin-Schreier extensions. They prove a formula for the ranks of the Jacobians of their curves, and produce examples of Jacobians with bounded and with unbounded ranks.

Another example from [**50**] is the curve over $k(t)$ defined by $y^2 + xy + ty = x^3 + tx^2$. For k an algebraically closed field of characteristic zero and d a positive integer, the curve has rank zero over the fields $k(t^{1/d})$. For $k = \overline{\mathbb{F}}_p$ and $d = p^n + 1$, the curve has rank $d - 2$ over $k(t^{1/d})$, and explicit generators are found. Later, in [**52**], a 2-isogeny to the Legendre curve $y^2 = x(x + 1)(x + t)$ is obtained, and this construction motivates our work.

The main results

Let p be an odd prime, let $r \geq 2$ be an integer not divisible by p, and let $K = \mathbb{F}_p(t)$. Generalizing the results in **[52]**, **[10]**, and **[53]**, we consider the smooth projective curve $C = C_r$ of genus $g = r - 1$ over K with affine model

$$y^r = x^{r-1}(x+1)(x+t).$$

The Jacobian J_r of C_r is a principally polarized abelian variety over K of dimension g.

We study the arithmetic of $J = J_r$ over extensions of K of the form $\mathbb{F}_q(u)$ where $u \in \overline{K}$ satisfies $u^d = t$, e.g., the extension $K_d = \mathbb{F}_p(\mu_d, u)$. Some of our results hold for general data p, q, r, d, while others hold under specific constraints. We first state a result in a specific case:

THEOREM 1. Let p be a prime number, let $d = p^\nu + 1$ for some integer $\nu > 0$, and let r be a divisor of d. Then there is an explicit group of divisors generating a subgroup $V \subset J(K_d)$ with the following properties:

(1) The $\mathbb{Z}$-rank of V is $(r-1)(d-2)$ and the torsion of V has order r^3.
(2) The index of V in $J(K_d)$ is finite and a power of p.
(3) The Tate-Shafarevich group $Ш(J/K_d)$ of J/K_d is finite of order

$$|Ш(J/K_d)| = [J(K_d) : V]^2.$$

We prove even more about V, describing it completely as a module over a certain group ring and as a lattice with respect to the canonical height pairing on J.

In the general case, we compute the L-function and prove the BSD conjecture:

THEOREM 2. Let p be a prime number, let q be a power of p, and let r and d be positive integers not divisible by p. Then:

(1) The conjecture of Birch and Swinnerton-Dyer holds for J over $\mathbb{F}_q(u)$.
(2) The L-function of $J/\mathbb{F}_q(u)$ can be expressed explicitly in terms of Jacobi sums. (See Theorem 5.4 below for the precise statement.)
(3) For sufficiently large q, the order of vanishing of $L(J/\mathbb{F}_q(u), s)$ at $s = 1$ can be expressed in terms of the action on the set $(\mathbb{Z}/d\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z})$ of the subgroup of $(\mathbb{Z}/\operatorname{lcm}(d, r)\mathbb{Z})^\times$ generated by p. (See Proposition 5.9 below for the precise statement.)

The rank calculation in this result of course agrees with that given by the explicit points in the case $d = p^\nu + 1$, $r \mid d$, and $\mathbb{F}_q = \mathbb{F}_p(\mu_d)$. We expect that there are many other values of q, r and d yielding large ranks, as in **[10]**.

Finally, we prove very precise results about the decomposition of J up to isogeny into simple abelian varieties and about torsion in abelian extensions. To state them, note that if $r' \mid r$, then there is a surjective map of curves $C_r \to C_{r'}$ and a corresponding homomorphism of Jacobians $J_r \to J_{r'}$ induced by push-forward of divisors. We define J_r^{new} to be the identity component of the intersection of the kernels of these homomorphisms over all divisors r' of r with $r' < r$.

THEOREM 3.

(1) If $r = 2$, then J_r^{new} equals J_r, which is an abelian variety of dimension 1, and thus J_r^{new} is absolutely simple.

(2) If $r > 2$, then J_r^{new} is simple over $\overline{\mathbb{F}}_p(t)$, while over $\overline{\mathbb{F}_p(t)}$ it is isogenous to the square of a simple abelian variety of dimension $\phi(r)/2$ whose endomorphism algebra is the real cyclotomic field $\mathbb{Q}(\mu_r)^+$.
(3) If L is an abelian extension of $\overline{\mathbb{F}}_p(t)$ and if ℓ is prime with $\ell \nmid r$, then $J_r(L)$ contains no non-trivial elements of order ℓ.

Overview of the paper

Our study involves more than one approach to the key result of part (1) of Theorem 1 (the lower bound on the rank of J over K_d when $d = p^\nu + 1$). Some of the arguments are more elementary or less elementary than others, with correspondingly weaker or stronger results. We include these multiple approaches so that the reader may see many techniques in action, and may choose the approaches that suit his or her temperament and background.

In Chapter 1, we give basic information about the curve C and Jacobian J we are studying. We write down explicit divisors in the case $d = p^\nu + 1$, and we find relations satisfied by the classes of these divisors in J. These relations turn out to be the only ones, but that is not proved in general until much later in the paper.

In Chapter 2, we assume that r is prime and use descent arguments to bound the rank of J from below in the case when $d = p^\nu + 1$. The reader who is willing to assume r is prime need only read these first two chapters to obtain one of the main results of the paper.

In Chapter 3, we construct the minimal, regular, proper model $\mathcal{X} \to \mathbb{P}^1$ of $C/\mathbb{F}_q(u)$ for any values of d and r. In particular, we compute the singular fibers of $\mathcal{X} \to \mathbb{P}^1$. This allows us to compute the component groups of the Néron model of J. We also give a precise connection between the model $\mathcal{X}$ and a product of curves.

In Chapter 4, we consider the case where $d = p^\nu + 1$ and $r \mid d$, and we compute the heights of the explicit divisors introduced in Chapter 1. This allows us to compute the rank of the explicit subgroup V and its structure over the group ring $\mathbb{Z}[\mu_r \times \mu_d]$.

In Chapter 5, we give an elementary calculation of the L-function of J over $\mathbb{F}_q(u)$ (for any d and r) in terms of Jacobi sums. We also show that the BSD conjecture holds for J, and we give an elementary calculation of the rank of $J(\mathbb{F}_q(u))$ for any d and r and all sufficiently large q.

In the fairly technical Chapters 6 and 7, we prove several results about the surface $\mathcal{X}$ that allow us to deduce that the index of V in $J(K_d)$ is a power of p when $d = p^\nu + 1$ and r divides d. We also use the BSD formula to relate this index to the order of the Tate-Shafarevich group.

In the equally technical Chapter 8, we prove strong results on the monodromy of the ℓ-torsion of J for ℓ prime to pr. This gives precise statements about torsion points on J over abelian or solvable extensions of $\overline{\mathbb{F}}_p(t)$ and about the decomposition of J up to isogeny into simple abelian varieties.

The methods of this paper can be used to study other curves as well. We give an explicit family of curves in Section 1.6 and point out how some of the results of this paper extend to the Jacobians of these curves. At the request of the referee, we include Appendix A, in which we give more details on these examples. Specifically, we prove a lower bound on the rank of the Jacobian of the hyperelliptic curve X over $\mathbb{F}_q(t)$ defined by $y^2 = x\prod_{i=1}^{g}(x + a_i)(t + a_i x)$ with g odd and with distinct nonzero $a_i \in \mathbb{F}_q$ over fields of the form $K_d = \mathbb{F}_q(\mu_d, t^{1/d})$ with $d = q^\nu + 1$. We also

show that the BSD conjecture holds for the Jacobian of X over $\mathbb{F}_{q^n}(t^{1/d})$ for all n and all d prime to p, and we give an upper bound on the rank using the L-function.

Recently, Ulmer and Voloch [**54**] introduced a family of curves generalizing those treated in this paper. They study curves defined by the equation

$$y^r = h(x)h(t/x),$$

where h is a polynomial that is not of the form f^m, for any $m \neq 1$, $m \mid r$. (The generalized Legendre curves studied in this paper and the hyperelliptic curves discussed in the appendix are all examples from this family.) They prove that the number of points in an arithmetic family of such curves is unbounded, and they also show that the surface over k defined by this equation is dominated by a product of curves. The emphasis in [**54**] is on rational points on the curves, whereas techniques from this paper may be useful for proving interesting results on the Jacobians of these curves.

Guide

The leitfaden below indicates dependencies among the chapters of the paper. We also record here the chapters or sections needed to prove various parts of the main results.

A proof of lower bounds as in Theorem 1(1) (i.e., that the rank of $J(K_d)$ is at least $(r-1)(d-2)$ and the torsion has order r^3) in the case where r is prime and divides $d = p^\nu + 1$ is contained in Chapters 1 and 2, and more specifically follows from Proposition 1.5 and Theorem 2.1.

The lower bounds of Theorem 1(1) in the case of general r dividing $d = p^\nu + 1$ are proved in Section 4.3.2 using results from Chapter 1, Section 4.1, and earlier parts of Chapter 4. Theorem 1(1) is established in full generality in Corollary 4.20.

Parts (2) and (3) of Theorem 1 are proved in Chapter 7, specifically in Theorem 7.1 and Theorem 7.7 respectively, using results from Chapters 1, 3, 4, 5, and 6.

Theorem 2 is proved in Chapter 5 using results from Chapters 1 and 3.

Finally, Theorem 3 is proved in Chapter 8 using definitions from Chapter 1 and precise information on the Néron model of J deduced from properties of the regular proper model $\mathcal{X}$ of Chapter 3. (To be precise, the claim about p-torsion is not treated in Chapter 8, but a stronger result is proved in Section 6.1.)

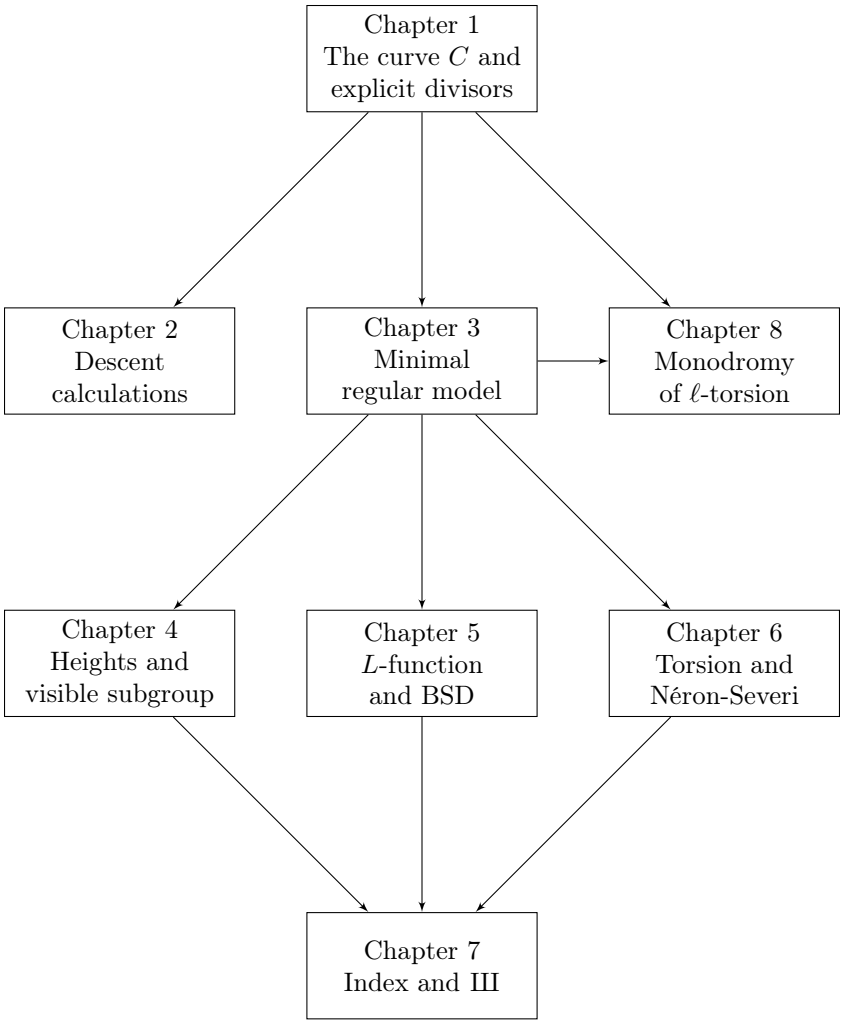


FIGURE 1. Leitfaden

Notation

Throughout, k is a field of characteristic $p \geq 0$ and K is the rational function field $k(t)$. We write $\mathbb{F}_q$ to denote a finite ground field of cardinality q, with q being a power of p. If n is positive and not divisible by the characteristic p of k, we write μ_n for the group of n-th roots of unity in an algebraic closure of k. For a prime p and a positive integer d not divisible by p, we write K_d for the extension $\mathbb{F}_p(\mu_d, u)$ of $\mathbb{F}_p(t)$ with $u^d = t$. We view $k(u)$ as the function field of $\mathbb{P}^1_u$ where the subscript u reminds us that the coordinate is u.

CHAPTER 1

The curve, explicit divisors, and relations

In this chapter, we define a curve C over $K = k(t)$ whose Jacobian J is the main object of study. When $k = \mathbb{F}_p$, there is a rich supply of explicit points on C defined over certain extensions of K, and the divisors supported on these points turn out to generate a subgroup of J of large rank.

More precisely, we study the arithmetic of C and J over extensions of $\mathbb{F}_p(t)$ of the form $\mathbb{F}_q(t^{1/d})$ for q a power of p and $d \in \mathbb{N}$ relatively prime to p. Let $K = \mathbb{F}_p(t)$ and $K_d = \mathbb{F}_p(\mu_d, u)$ where μ_d denotes the d-th roots of unity and $u = t^{1/d}$. These fields are the most important fields in the paper, especially when d has the form $d = p^\nu + 1$ for an integer $\nu > 0$, although we consider more general extensions of the form $\mathbb{F}_q(t^{1/d})$ as well.

1.1. A generalization of the Legendre curve

Choose a positive integer r not divisible by $p = \mathrm{char}(k)$. We consider the smooth, absolutely irreducible, projective curve C over $k(t)$ associated to the affine curve

$$y^r = x^{r-1}(x+1)(x+t). \tag{1.1}$$

Note that when $r = 2$, this is an elliptic curve called the Legendre curve which was studied in **[52]**.

1.1.1. Constructing a smooth model. We explicitly construct the smooth projective model of C. First, consider the projective curve in $\mathbb{P}^2$ over $\mathbb{F}_p(t)$ given by

$$C' : \qquad Y^r Z = X^{r-1}(X+Z)(X+tZ).$$

A straightforward calculation using the Jacobian criterion shows that C' is smooth when $r = 2$, in which case we take $C = C'$. If $r > 2$, then the Jacobian criterion reveals that C' is singular at the point $[0,0,1]$ and is smooth elsewhere. We produce a smooth projective curve by blowing up this point.

Let V be the complement of $[0,0,1]$ in C'. Let U be the affine curve with equation

$$v = u^{r-1}(uv+1)(uv+t).$$

Another Jacobian criterion calculation shows that U is smooth. The map

$$X = uv, \qquad Y = v, \qquad Z = 1$$

gives an isomorphism π between $U \backslash \{u = v = 0\}$ and $V \backslash \{[-1,0,1],[-t,0,1],[0,1,0]\}$. Gluing U and V along this map yields a smooth projective curve which we denote C.

We claim that $\pi : C \to C'$ is the normalization of C'. Indeed, π factors through the normalization of C' since C is smooth and thus normal. Moreover, π is visibly

finite and birational. Since a finite birational morphism to a normal scheme is an isomorphism, $\pi : C \to C'$ is indeed the normalization of C.

Note that π is a bijection as well. In fact, it is a universal homeomorphism[1], so for every field extension L of $\mathbb{F}_p(t)$, there is a bijection of rational points

$$C(L) \xrightarrow{\sim} C'(L).$$

It is convenient to specify points of C by giving the corresponding points of C' using the affine coordinates $x = X/Z$ and $y = Y/Z$.

The reader who prefers to avoid the abstraction in the last two paragraphs is invited to work directly with the smooth curve C. This adds no significant inconvenience to what follows.

1.1.2. First points. Let Q_∞ be the point of C corresponding to the point at infinity on C', namely $[0, 1, 0]$. Let Q_0, Q_1, and Q_t be the points of C given by $(x, y) = (0, 0)$, $(-1, 0)$, and $(-t, 0)$ respectively. (Here we use the convention mentioned at the end of the preceding subsection, namely we define points of C via C'.)

1.1.3. Genus calculation.

LEMMA 1.1. *The curve C has genus $g = r - 1$.*

PROOF. Consider the covering

$$f : C \to \mathbb{P}^1$$

induced by the function x. The ramification points of f are Q_0, Q_1, Q_t and Q_∞, each with ramification index r. The Riemman-Hurwitz formula implies

$$2g - 2 = -2r + 4(r - 1),$$

thus $g = r - 1$. □

1.1.4. Immersion in J. Let J be the Jacobian of C; it is a principally polarized abelian variety of dimension $g = r - 1$. We imbed C in J via the Abel-Jacobi map using Q_∞ as a base point:

$$C \to J$$
$$P \mapsto [P - Q_\infty]$$

where $[P - Q_\infty]$ is the class of $P - Q_\infty$ in $\mathrm{Pic}^0(C) = J$.

1.1.5. Automorphisms. Note that if k contains μ_r, the r-th roots of unity, then every element of μ_r gives an automorphism of C. More precisely, we have automorphisms

$$(x, y) \mapsto (x, \zeta_r^j y)$$

where ζ_r is a primitive r-th root of unity and $0 \le j < r$. These automorphisms fix Q_∞, so the induced automorphisms of J are compatible with the embedding $C \hookrightarrow J$.

As we verify below, these are not all of the automorphisms of C, but they are the only ones that play an important role in this paper.

[1]Indeed, π is projective, so universally closed and surjective, and it is injective and induces isomorphisms on the residue fields, so is universally injective by [**15**, 3.5.8].

1.1.6. Complement: Hyperelliptic model and 2-torsion. We remark that the curve C is hyperelliptic. More precisely, making the substitution $(x, y) \to (x, xy)$ in the equation $y^r = x^{r-1}(x+1)(x+t)$, we see that C is birational to the curve given by

$$x^2 + (t + 1 - y^r)x + t = 0$$

and projection on the y-coordinate makes this a (separable) 2-to-1 cover of the projective line. If $p \neq 2$, we may complete the square and make the appropriate change of coordinates (a translation of x) to arrive at the equation

$$\begin{aligned} x^2 &= y^{2r} - 2(t+1)y^r + (t-1)^2 \\ &= \left(y^r - (\sqrt{t}+1)^2\right)\left(y^r - (\sqrt{t}-1)^2\right). \end{aligned}$$

If, in addition, d is even and r is odd, then $\sqrt{t} \in k(u)$ and the two factors on the right hand side are irreducible in $k(u)[y]$. It follows from **[33**, Lemma 12.9**]** that J has no 2-torsion over $k(u)$.

This is a first hint towards later results. For example, $J(K_d)_{tor}$ has order r^3 when r divides $d = p^\nu + 1$ (Theorem 7.1). More generally (Corollary 6.1 and Theorem 8.1), J has no torsion of order prime to r over any abelian extension of $\overline{k}(t)$.

1.2. Explicit points and the visible subgroup

Next, we write down several points on C defined over the extensions K_d, and we consider the subgroup they generate in the Jacobian.

1.2.1. Special extensions. For the rest of Chapter 1, we assume that $d = p^\nu + 1$ for some integer $\nu > 0$, and we assume that r divides d. In this situation, it turns out that C has a plentiful supply of points defined over K_d, and the divisors supported on these points generate a subgroup of $J(K_d)$ of large rank.

The extension K_d/K is Galois with Galois group the semidirect product of $\mathrm{Gal}(\mathbb{F}_p(\mu_d, t)/K) \cong \mathrm{Gal}(\mathbb{F}_p(\mu_d)/\mathbb{F}_p)$ (a cyclic group of order 2ν generated by the p-power Frobenius) by $\mathrm{Gal}(K_d/\mathbb{F}_p(\mu_d, t))$ (a cyclic group of order d generated by a primitive d-th root of unity).

Remark 1.2. There are many triples p, r, d satisfying our hypotheses. Indeed, for a fixed prime p, there are infinitely many integers $r > 1$ such that r divides $p^\mu + 1$ for some μ. (The number of such r less that X is asymptotic to $X/(\log X)^{2/3}$; see **[32**, Theorem 4.2**]**.) For any such p and r, there are infinitely many ν such that r divides $p^\nu + 1$. Indeed, $p^\mu + 1$ divides $p^\nu + 1$ whenever $\nu = m\mu$ with m odd.

Alternatively, for a fixed r, there are infinitely many primes p such that r divides $p^\mu + 1$ for some μ. These p are determined by congruence conditions modulo r, namely by the requirement that -1 be in the subgroup of $(\mathbb{Z}/r\mathbb{Z})^\times$ generated by p.

1.2.2. Explicit points. We continue to assume that $d = p^\nu + 1$ and $r|d$. Under these hypotheses, we note that

$$P(u) := \left(u, u(u+1)^{d/r}\right)$$

is a point on C defined over K_d. Indeed,

$$\begin{aligned} u^{r-1}(u+1)(u+t) &= u^r(u+1)(1+u^{p^\nu}) \\ &= u^r(u+1)^{p^\nu+1} \\ &= \left(u(u+1)^{d/r}\right)^r. \end{aligned}$$

We find other points by applying the automorphisms ζ_r^j discussed in Section 1.1.5 above and the action of the elements of the Galois group of K_d/K. In all, this yields rd distinct points.

Although it is arguably unnatural, for typographical convenience we fix a primitive d-th root of unity $\zeta_d \in K_d$ and we set $\zeta_r = \zeta_d^{d/r}$. Then the points just constructed can be enumerated as

$$P_{i,j} = \left(\zeta_d^i u, \zeta_r^j \zeta_d^i u(\zeta_d^i u + 1)^{d/r}\right)$$

where $i \in \mathbb{Z}/d\mathbb{Z}$ and $j \in \mathbb{Z}/r\mathbb{Z}$.

Identifying C with its image in J via the map in Section 1.1.4 produces divisor classes in $J(K_d)$ that we also denote by $P_{i,j}$. The subgroup generated by these points is one of the main objects of study in this paper.

1.2.3. R-module structure. Next we introduce a certain group ring acting on $J(K_d)$. We noted above that there is an action of $\mu_r \subset \mathrm{Aut}(C)$ on C and on J. There are also actions of $\mu_d \cong \mathrm{Gal}(K_d/\mathbb{F}_p(\mu_d, t)) \subset \mathrm{Gal}(K_d/K)$ on $C(K_d)$ and on $J(K_d)$, and these actions are compatible with the inclusion $C \hookrightarrow J$.

Let R be the integral group ring of $\mu_d \times \mu_r$, i.e., let

$$R = \frac{\mathbb{Z}[\sigma, \tau]}{(\sigma^d - 1, \tau^r - 1)}.$$

The natural action of R on the points $P_{i,j}$ is:

$$\sigma^i \tau^j (P_{a,b}) = P_{a+i,b+j}.$$

(Here and below we read the indices i modulo d and j modulo r.)

1.2.4. The "visible" subgroup. We define $V = V_{r,d}$ to be the subgroup of $J(K_d)$ generated by the $P_{i,j}$. It is evident that V is also the cyclic R-submodule of $J(K_d)$ generated by $P_{0,0}$. In other words, there is a surjective homomorphism of R-modules

$$\begin{aligned} R &\to V \\ \sum_{ij} a_{ij}\sigma^i\tau^j &\mapsto \sum_{ij} a_{ij}\sigma^i\tau^j(P_{0,0}) = \sum_{ij} a_{ij}P_{i,j}. \end{aligned}$$

One of the main results of the paper is a complete determination of the "visible" subgroup V. Here we use visible in the straightforward sense that these are divisors we can easily see. As far as we know, there is no connection with the Mazur-Stein theory of visible elements in the Tate-Shafarevich group.

1.3. Relations

As above, let $V = V_{r,d}$ be the R-submodule of $J(K_d)$ generated by $P_{0,0}$. The goal of this section is to work toward computing the structure of V as a group and as an R-module. Explicitly, we show that V is a quotient of R/I for a certain ideal I. Ultimately, in Chapter 4, we verify that V is isomorphic to R/I as an R-module and compute the structure of R/I as a group.

Throughout, we identify $C(K_d)$ with its image in $J(K_d)$ via the immersion $P \mapsto [P - Q_\infty]$.

Considering the divisors of x, $x+1$, and $x+t$, one finds that the classes of Q_0, Q_1, and Q_t are r-torsion. Considering the divisor of y, one finds that $Q_t \sim Q_0 - Q_1$, so Q_t is in the subgroup generated by Q_0 and Q_1.

Now consider the functions $x - \zeta_d^i u$,

$$\Delta_j := \zeta_d^{-jd/r} y - x(x+1)^{d/r},$$

and

$$\Gamma_j := \zeta_d^{-jd/r} y x^{d/r-1} - u^{d/r}(x+1)^{d/r}.$$

Calculating as in [**52**, Proposition 3.2], we find that

$$\operatorname{div}(x - \zeta_d^i u) = \sum_{j=0}^{r-1} P_{i,j} - rQ_\infty,$$

$$\operatorname{div}(\Delta_j) = \sum_{i=0}^{d-1} P_{i,j} + (r-1)Q_0 + Q_1 - (r+d)Q_\infty,$$

and

$$\operatorname{div}(\Gamma_j) = \sum_{i=0}^{d-1} P_{i,-i+j} + Q_1 - (d+1)Q_\infty.$$

Considering the divisor of Γ_j for any j shows that Q_1 is in V, and then considering the divisor of Δ_j for any j shows that Q_0 is also in V. (Here we use the fact that Q_0 is r-torsion.) Thus V contains the classes of Q_0, Q_1 and Q_t.

Now for $1 \le j \le r-1$ we set

$$D_j := \operatorname{div}(\Delta_j/\Delta_{j-1}) = \sum_i (P_{i,j} - P_{i,j-1}),$$

and

$$E_j := \operatorname{div}(\Gamma_j/\Gamma_{j-1}) = \sum_i (P_{i,j-i} - P_{i,j-1-i}),$$

and for $0 \le i \le d-1$ we set

$$F_i := \operatorname{div}(x - \zeta_d^i u) = \sum_j P_{i,j} - rQ_\infty.$$

These divisors are zero in the Jacobian $J_r(K_d)$.

Restating this in terms of the module homomorphism $R \to V$, we see that for $1 \le j \le r-1$ the elements

$$d_j := \sum_i (\sigma^i \tau^j - \sigma^i \tau^{j-1}) = (\tau^j - \tau^{j-1}) \sum_i \sigma^i,$$

$$e_j := \sum_i (\sigma^i \tau^{j+d-i} - \sigma^i \tau^{j-1+d-i}) = (\tau^j - \tau^{j-1}) \sum_i \sigma^i \tau^{d-i},$$

and for $0 \leq i \leq d-1$ the elements

$$f_i := \sum_j \sigma^i \tau^j = \sigma^i \sum_j \tau^j$$

map to zero in V.

Let I be the ideal of R generated by

$$(\tau - 1)\sum_i \sigma^i, \qquad (\tau - 1)\sum_i \sigma^i \tau^{d-i}, \quad \text{and} \quad \sum_j \tau^j.$$

Then it is easy to see that d_j, e_j, and f_i all lie in I, that they generate it as an ideal, and in fact that they form a basis of I as a $\mathbb{Z}$-module.

Thus there is a surjection of R-modules $R/I \to V$. We will eventually show that this surjection is in fact an isomorphism; see Theorem 1.6.

Note that R has rank rd as a $\mathbb{Z}$-module, so the rank of R/I as a $\mathbb{Z}$-module is $rd - d - 2(r-1) = (r-1)(d-2)$. Thus the rank of V is at most $(r-1)(d-2)$.

1.4. Torsion

In this section, we show that certain torsion divisors are not zero; more precisely that the order of the torsion subgroup of V is divisible by r^3. The main result is Proposition 1.5 below.

LEMMA 1.3. *The classes of Q_0 and Q_1 each have order r and generate a subgroup of V isomorphic to $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$.*

PROOF. It suffices to prove the claim over $\overline{\mathbb{F}}_p K_d = \overline{\mathbb{F}}_p(u)$. We have already seen that Q_0 and Q_1 have order dividing r. Suppose that $aQ_0 + bQ_1 = 0$ in V for integers $a,\ b \in \{0, 1, \cdots r-1\}$, not both equal to zero. Then there is a function h in the function field of the curve C with $\operatorname{div}(h) = (a/r)\operatorname{div}(x) + (b/r)\operatorname{div}(x+1)$. Since we are working over $\overline{\mathbb{F}}_p$, we may choose h such that $h^r = x^a(x+1)^b$. Let Y denote the curve with function field $K_d(x,h)$. Consider the inclusions $K_d(x) \hookrightarrow K_d(x,h) \hookrightarrow K_d(C)$ and the corresponding surjections $C \to Y \to \mathbb{P}^1$. The map $Y \to \mathbb{P}^1$ is of degree greater than one, and $C \to \mathbb{P}^1$ is fully ramified over $x = -t$. This is a contradiction, since $Y \to \mathbb{P}^1$ is unramified over $x = -t$. Hence, $aQ_0 + bQ_1 = 0$ only when r divides both a and b, and Q_0 and Q_1 generate independent cyclic subgroups of order r. □

Next we introduce elements of $V \subset J(K_d)$ as follows:

$$Q_2 := \sum_{j=0}^{r-1} \sum_{k=0}^{r-1-j} \sum_{i \equiv k \bmod r} P_{i,j}$$

and

$$Q_3 := Q_0 - 2Q_2.$$

LEMMA 1.4.

(1) $(1 - \zeta_r)Q_2 = Q_0$.
(2) *If r is odd, then $rQ_2 = 0$.*
(3) *If r is even, then $2rQ_2 = 0$ and $(r/2)Q_3 = 0$.*

PROOF. (1) We have

$$\begin{aligned}(1-\zeta_r)Q_2 &= (1-\zeta_r)\sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r} P_{i,j}\\ &= \sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r}(P_{i,j}-P_{i,j+1})\\ &= \sum_{k=0}^{r-1}\sum_{i\equiv k \bmod r}\sum_{j=0}^{r-1-k}(P_{i,j}-P_{i,j+1})\\ &= \sum_{k=0}^{r-1}\sum_{i\equiv k \bmod r}(P_{i,0}-P_{i,r-k})\\ &= \sum_{i=0}^{d-1}(P_{i,0}-P_{i,-i})\,.\end{aligned}$$

Considering the divisor of Δ_0/Γ_0 shows that the last quantity is equal to Q_0 in J.

(2) Assume that r is odd, which implies that $j(j-r)/2$ is an integer for all integers j. Consider the element of R given by

$$\rho_{odd} := \sum_{j=0}^{r-1}\left(\frac{j(j-r)}{2}(d_j-e_j)+(r-j)\sum_{i\equiv j \bmod r} f_i\right),$$

where d_j, e_j, and f_i are as in the previous subsection. We compute that

$$\rho_{odd} = r\left(\sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r}\sigma^i\tau^j\right).$$

Applying both sides of this equality to $P_{0,0}$ proves that $rQ_2 = 0$ in J.

(3) Now assume that r is even and consider

$$\rho_{even} := \sum_{j=0}^{r-1}\left(j(j-r)(d_j-e_j)+2(r-j)\sum_{i\equiv j \bmod r} f_i\right).$$

A calculation similar to the one above shows that

$$\rho_{even} = 2r\left(\sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r}\sigma^i\tau^j\right),$$

and applying both sides of this equality to $P_{0,0}$ proves that $2rQ_2 = 0$ in J.

Finally, we note that when r is even, then $(1-j)(j-r)/2$ is an integer for all integers j. Consider

$$\rho'_{even} := \sum_{j=1}^{r-1}\left(\frac{(1-j)(j-r)}{2}(d_j-e_j)\right)-\sum_{j=0}^{r-1}\sum_{i\equiv j \bmod r}(r-j)f_i.$$

We compute that

$$\rho'_{even} = (r/2)\left(\sum_{i=0}^{d-1}\left(\sigma^i-\sigma^i\tau^{-i}\right)-2\sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r}\sigma^i\tau^j\right).$$

Applying both sides of this equality to $P_{0,0}$ and noting as above that $Q_0 = \sum_i P_{i,0} - P_{i,-i}$ shows that $(r/2)(Q_0 - 2Q_2) = 0$ in J.

This completes the proof of the lemma. □

The reader who wonders where Q_2 and Q_3 come from should consult the proof of Proposition 4.17.

We write $\langle Q_0, Q_1, Q_2\rangle$ for the subgroup of $J(K_d)$ generated by Q_0, Q_1, and Q_2. Note that $\langle Q_1, Q_2, Q_3\rangle = \langle Q_0, Q_1, Q_2\rangle$.

PROPOSITION 1.5. *Let T be the subgroup $\langle Q_0, Q_1, Q_2\rangle$ of $J(K_d)$. Then the order of T is r^3. More precisely:*

1. *If r is odd, then the map $(a, b, c) \mapsto aQ_0 + bQ_1 + cQ_2$ induces an isomorphism $(\mathbb{Z}/r\mathbb{Z})^3 \cong T$.*
2. *If r is even, then the map $(a, b, c) \mapsto aQ_1 + bQ_2 + cQ_3$ induces an isomorphism $(\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/2r\mathbb{Z}) \times (\mathbb{Z}/(r/2)\mathbb{Z}) \cong T$.*

PROOF. (1) Assume that r is odd. Lemmas 1.3 and 1.4(2) show that the map under consideration is well-defined. It is surjective by the definition of T. To see that it is injective, suppose that $aQ_0 + bQ_1 + cQ_2 = 0$. Applying $(1 - \zeta_r)$ and using Lemma 1.4(1) shows that $cQ_0 = 0$. By Lemma 1.3, $c = 0$ in $\mathbb{Z}/r\mathbb{Z}$, and applying Lemma 1.3 again shows that $a = b = 0$ in $\mathbb{Z}/r\mathbb{Z}$. This shows the map is injective, thus an isomorphism.

(2) Now assume that r is even. Lemmas 1.3 and 1.4(3) show that the map under consideration is well-defined. It is again surjective by the definition of T. To see that it is injective, suppose that $aQ_1 + bQ_2 + cQ_3 = 0$. Applying $(1 - \zeta_r)$ and using Lemma 1.4(1) and Lemma 1.3 shows that $b - 2c = 0$ in $\mathbb{Z}/r\mathbb{Z}$ and, in particular, that b is even. Using that $2Q_2 = Q_0 - Q_3$, we compute

$$\begin{aligned} 0 &= aQ_1 + bQ_2 + cQ_3 \\ &= cQ_0 + aQ_1 + (b - 2c)Q_2 \\ &= cQ_0 + aQ_1 + \frac{b - 2c}{2}(Q_0 - Q_3) \\ &= (b/2)Q_0 + aQ_1. \end{aligned}$$

By Lemma 1.3, $b/2 = a = 0$ in $\mathbb{Z}/r\mathbb{Z}$ and therefore $b = 0$ in $\mathbb{Z}/2r\mathbb{Z}$. Since $b - 2c = 0$ in $\mathbb{Z}/r\mathbb{Z}$, we see that $c = 0$ in $\mathbb{Z}/(r/2)\mathbb{Z}$, and this shows the map is injective, thus an isomorphism.

This completes the proof of the Proposition. □

1.5. First main theorem

We can now state the main "explicit points" theorem of this paper.

Recall that the group ring $R = \mathbb{Z}[\sigma, \tau]/(\sigma^d - 1, \tau^r - 1)$ acts on $J(K_d)$ and that V is the cyclic submodule of $J(K_d)$ generated by $P_{0,0}$. Recall also that $I \subset R$ is the ideal generated by

$$(\tau - 1)\sum_i \sigma^i, \qquad (\tau - 1)\sum_i \sigma^i\tau^{d-i}, \quad \text{and} \quad \sum_j \tau^j.$$

THEOREM 1.6.

(1) *The map*

$$R \to V$$
$$\sum_{ij} a_{ij}\sigma^i\tau^j \mapsto \sum_{ij} a_{ij}P_{i,j}$$

induces an isomorphism $R/I \cong V$ of R-modules.

(2) *As a $\mathbb{Z}$-module, V has rank $(r-2)(d-2)$, and its torsion subgroup has order r^3 and is equal to the group T defined in Proposition 1.5.*

We prove Theorem 1.6 in Chapter 4 by computing the canonical height pairing on V; see Theorem 4.19. In the case when r is an odd prime, we give a more elementary proof of part (2) in Chapter 2 using a descent calculation; see Theorem 2.1.

1.6. Complement: Other curves

The basic "trick" allowing one to write down points on C extends to many other curves. In this section, we briefly discuss one class of examples. A more detailed analysis is provided in Appendix A.

Let p be an odd prime and k a field of characteristic p and cardinality q. Fix an odd integer $g > 1$ and a polynomial $h(x) \in k[x]$ of degree g. Assume h has distinct, nonzero roots.

Let X be the smooth, projective curve over $K = k(t)$ defined by

$$y^2 = xh(x)x^g h(t/x).$$

Since the right hand side has degree $2g+1$ in x, the genus of X is g. Let ∞ be the (K-rational) point at infinity on X.

Let J be the Jacobian of X. We embed X in J using ∞ as the base point.

If $d = q^\nu + 1$ and $K_d = k(\mu_d, u)$ with $u^d = t$, then X has a K_d-rational point, namely

$$P(u) : (x, y) = \left(u, u^{(g+1)/2}h(u)^{d/2}\right).$$

Letting the Galois group of K_d over K act on $P(u)$ yields points $P_j = P(\zeta_d^j u)$ where ζ_d is a primitive d-th root of unity and $j = 0, \ldots, d-1$. We consider the subgroup V of $J(K_d)$ generated by the images of the d points P_j, and the images of the points where $y = 0$.

By writing down the divisors of certain functions, as in Section 1.3, we show that the rank of the subgroup V is at most d.

It is natural to bound the rank of V from below by computing a coboundary map related to 2-descent. More precisely, extending k if necessary we may assume that the roots of h lie in k. Then the Weierstrass points of X are defined over K and the divisors of degree zero supported on them generate the full 2-torsion subgroup of J. In particular, $J[2] \cong \mu_2^{2g} \cong (\mathbb{Z}/2\mathbb{Z})^{2g}$ over K. We obtain a coboundary map

$$J(K_d)/2J(K_d) \hookrightarrow H^1(K_d, J[2]) \cong \left(K_d^\times/K_d^{\times 2}\right)^{2g}.$$

Analyzing the image of V under this map (along the lines of [**52**, Section 4]) allows one to show that the rank of V is at least $d-2$ when d is of the form $q^\nu + 1$ (and at least $d-1$ when $g > 1$). This work is also closely related to the calculations in Chapter 2 for the curve C that is our main object of study.

In the appendix, we also consider a certain surface $\mathcal{X}_d$ equipped with a morphism $\mathcal{X}_d \to \mathbb{P}^1$ whose generic fiber is X/K_d, and we prove that this surface is dominated by a product of curves. This shows that the BSD conjecture holds for J over $\mathbb{F}_q(u)$ where $u^d = t$, q is any power of p, and d is any positive integer prime to p. All this is closely related to our work in Chapters 3 and 5 on C.

In the last part of the appendix, we obtain an upper bound on the order of vanishing of the L-function of J/K_d at $s = 1$, thereby bounding the rank of $J(K_d)$ from above. This is closely related to our work in Chapter 5 on the L-function of J_C.

We note that some of the finer analysis of this paper is unlikely to go through without much additional work. For example, the upper and lower bounds on the rank of J over K_d differ significantly, and we have not determined the exact rank. Indeed, the degree of the L-function of J over K_d is asymptotic to $g^2 d$ as $d \to \infty$, whereas the rank of V is less than d. This suggests that the leading coefficient of $L(J/K_d, s)$ at $s = 1$ is likely to be of arithmetic nature, and that the connection between the index of V in $J(K_d)$ and the order of $Ш(J/K_d)$ may not be as simple as it is for the curve C studied in the rest of this paper. We would be delighted if readers of this paper took up these questions.

CHAPTER 2

Descent calculations

Throughout this chapter, r is an odd, positive, prime number dividing d, and $d = p^\nu + 1$ for some integer $\nu > 0$. Let $K_d = \mathbb{F}_p(\mu_d, u)$ where $u^d = t$. In this context, there is a fairly short and elementary proof that the visible subgroup of $J(K_d)$ has large rank.

More precisely, let C be the curve studied in Chapter 1, let J be its Jacobian, and let V be the "visible" subgroup of $J(K_d)$ defined in Section 1.2, so that V is generated by the image of the point $P = (u, u(u+1)^{d/r})$ under the Abel-Jacobi mapping $C \hookrightarrow J$ and its Galois conjugates. Recall that the choices made in Chapter 1 allow us to index these points as $P_{i,j}$ with $i \in \mathbb{Z}/d\mathbb{Z}$ and $j \in \mathbb{Z}/r\mathbb{Z}$.

Using the theory of descent, as developed in **[8]**, we prove the following theorem.

THEOREM 2.1. *The subgroup V of $J(K_d)$ has rank $(r-1)(d-2)$. Moreover,*

$$J(K_d)[r^\infty] \cong V[r^\infty] \cong (\mathbb{Z}/r\mathbb{Z})^3.$$

The proof is given in Section 2.4.

2.1. The isogeny ϕ

Recall that there is an action of the r-th roots of unity μ_r on C and an induced action on J. Recall also that $\zeta_r = \zeta_d^{d/r} \in K_d$ is a fixed r-th root of unity. If D is a divisor of degree 0 on C/K_d then the divisor

$$(1 + \zeta_r + \cdots + \zeta_r^{r-1})^*(D)$$

is easily seen to be the pullback of a divisor of degree 0 on $\mathbb{P}^1$ under the map $C \to \mathbb{P}^1$ that is the projection on the x coordinate. Since the Jacobian of $\mathbb{P}^1$ is trivial, the endomorphism $(1 + \zeta_r + \cdots + \zeta_r^{r-1})$ acts trivially on J.

We want to restate this in terms of the endomorphism ring of J. To avoid notational confusion, write H for the cyclic group of order r and let $\mathbb{Z}[H]$ be the group ring of H. Somewhat abusively, we use ζ_r also to denote an r-th root of unity in characteristic zero. Then, as usual, $\mathbb{Z}[\zeta_r]$ will denote the ring of integers in the cyclotomic field $\mathbb{Q}(\zeta_r)$. The action of μ_r on J induces a homomorphism $\mathbb{Z}[H] \to \mathrm{End}(J)$ where $\mathrm{End}(J)$ denotes the endomorphism ring of J over K_d.

There is a surjective ring homomorphism $\mathbb{Z}[H] \to \mathbb{Z}[\zeta_r]$ sending the elements of H to the powers of ζ_r. The kernel is generated by $\sum_{h \in H} h$. The discussion above shows that the homomorphism $\mathbb{Z}[H] \to \mathrm{End}(J)$ factors through $\mathbb{Z}[\zeta_r]$. The induced map $\mathbb{Z}[\zeta_r] \to \mathrm{End}(J)$ is an embedding, since $\mathrm{End}(J)$ is torsion-free.

Let $\phi : J \to J$ be the endomorphism $1 - \zeta_r$.

PROPOSITION 2.2. *The endomorphism $\phi = 1 - \zeta_r$ is a separable isogeny of degree r^2.*

PROOF. In $\mathbb{Z}[\zeta_r]$, there is an equality of ideals $(1-\zeta_r)^{r-1} = (r)$, i.e., the ratio of $(1-\zeta_r)^{r-1}$ and r is a unit. It follows that $(1-\zeta_r)^{r-1}$ and the separable isogeny $r : J \to J$ factor through each other. Therefore $1-\zeta_r$ is an isogeny, and

$$\deg(1-\zeta_r)^{r-1} = \deg r = r^{2g} = r^{2(r-1)}.$$

Since $\phi = 1-\zeta_r$, this proves that $\deg(\phi) = r^2$. Since r is prime to p, it follows that ϕ is separable. □

We write $J(K_d)[\phi]$ and $V[\phi]$ for the kernel of ϕ on $J(K_d)$ and V respectively.

COROLLARY 2.3. *$J(K_d)[\phi]$ is a two-dimensional vector space over $\mathbb{F}_r$ with basis Q_0 and Q_1. Moreover, $V[\phi] = J(K_d)[\phi]$.*

PROOF. For the first assertion, we verify that the divisor classes Q_0 and Q_1 are contained in the kernel of ϕ, and they generate a subgroup of $J(K_d)$ of order r^2 by Lemma 1.3. Since ϕ has degree r^2, it follows that Q_0 and Q_1 generate the kernel. Since Q_0 and Q_1 lie in $V[\phi] \subset J(K_d)[\phi]$ we also have $V[\phi] = J(K_d)[\phi]$. □

For any element $\epsilon \in \mathrm{End}(J)$, let $\epsilon^\vee$ denote its Rosati dual, that is, its image under the Rosati involution on $\mathrm{End}(J)$. If ϵ is an automorphism of J coming from an automorphism of C, then one has $\epsilon^\vee = \epsilon^{-1}$. It follows that $\phi^\vee = 1-\zeta_r^{-1}$.

LEMMA 2.4. *We have $J[\phi] = J[\phi^\vee]$, as group subschemes of J.*

PROOF. Since $(1-\zeta_r)/(1-\zeta_r^{-1})$ is a unit in $\mathbb{Z}[\zeta_r]$, it is clear that the endomorphisms $\phi = 1-\zeta_r$ and $\phi^\vee = 1-\zeta_r^{-1}$ factor through each other and thus have the same kernel. □

2.2. The homomorphism $(x-T)$

Let $\Delta = \{Q_0, Q_1, Q_t\}$, the set of affine ramification points of the morphism $C \to \mathbb{P}^1$, $(x,y) \mapsto x$, which lie over $x = 0$, $x = -1$, and $x = -t$ respectively. We write $\mathrm{Div}(C_{K_d})$ for the K_d-rational divisors on C and $\mathrm{Div}^0(C_{K_d})$ for those of degree 0. There is a canonical surjective homomorphism $\mathrm{Div}^0(C_{K_d}) \to J(K_d)$.

Following ideas from **[8]**, we define a homomorphism

$$(x-T) : \mathrm{Div}(C_{K_d}) \to \prod_{Q\in\Delta} K_d^\times / K_d^{\times r}$$

that plays a crucial role in the proof of Theorem 2.1. Its properties are described in Proposition 2.5. For an element $v \in \prod_{Q\in\Delta} K_d^\times/K_d^{\times r}$, we write $v = (v_0, v_1, v_t)$, where v_i is the coordinate corresponding to Q_i.

Let $C^\circ \subset C$ be the complement of $\Delta \cup \{Q_\infty\}$. We define the homomorphism

$$(x-T)' : \mathrm{Div}(C^\circ_{K_d}) \to \prod_{Q\in\Delta} K_d^\times / K_d^{\times r}$$

by setting

$$P \mapsto (x(P) - x(Q))_{Q\in\Delta},$$

and defining $(x-T)'$ on divisors by multiplicativity. (The individual points P in a divisor D need not be K_d-rational, but if D is K_d-rational, then $(x-T)'$ takes values in $\prod K_d^\times/K_d^{\times r}$.)

We now define the homomorphism

$$(x-T) : \mathrm{Div}(C_{K_d}) \to \prod_{Q\in\Delta} K_d^\times / K_d^{\times r}$$

as follows: let $D \in \mathrm{Div}(C_{K_d})$ be a divisor on C_{K_d} and choose $D' \in \mathrm{Div}(C^\circ_{K_d}) \subset \mathrm{Div}(C_{K_d})$ such that D' is linearly equivalent to D. Then set

$$(x-T)(D) := (x-T)'(D').$$

For a proof that $(x - T)$ is well-defined, see [**8**, 6.2.2].

Fix a separable closure K_d^{sep} of K_d, and let $\mathcal{G}$ be $\mathrm{Gal}(K_d^{\mathrm{sep}}/K_d)$. For any $\mathcal{G}$-module M and integer $i \geq 0$, we abbreviate the usual notation $H^i(\mathcal{G}, M)$ for the i-th Galois cohomology group of M to $H^i(M)$. For a finite $\mathcal{G}$-module M of cardinality not divisible by p, we denote by $M^\vee$ the dual $\mathcal{G}$-module $\mathrm{Hom}(M, K_d^{\mathrm{sep}\,\times})$.

PROPOSITION 2.5. *There is a homomorphism $\alpha : H^1(J[\phi]) \to \prod_{Q\in\Delta} K_d^\times/K_d^{\times r}$ such that:*

(1) *there is a short exact sequence of $\mathcal{G}$-modules*

$$0 \to H^1(J[\phi]) \xrightarrow{\alpha} \prod_{Q\in\Delta} K_d^\times/K_d^{\times r} \xrightarrow{N} K_d^\times/K_d^{\times r} \to 0,$$

where N is the map sending (v_0, v_1, v_t) to v_1v_t/v_0; and

(2) *the homomorphism $(x - T)$ restricted to $\mathrm{Div}^0(C_{K_d})$ is the composition*

$$\mathrm{Div}^0(C_{K_d}) \twoheadrightarrow J(K_d)/\phi J(K_d) \xhookrightarrow{\partial} H^1(J[\phi]) \xrightarrow{\alpha} \prod_{Q\in\Delta} K_d^\times/K_d^{\times r},$$

where ∂ is induced by the Galois cohomology coboundary map for ϕ.

PROOF. The proof is an application of the general theory of descent as developed in [**8**].

Let E be $(\mathbb{Z}/r\mathbb{Z})^\Delta$, the $\mathcal{G}$-module of $\mathbb{Z}/r\mathbb{Z}$-valued functions on Δ. Note that the $\mathcal{G}$-action on E is trivial. We define a $\mathcal{G}$-module map $\alpha^\vee : E \to J[\phi]$ defined by $h \mapsto \sum_{Q\in\Delta} h(Q) \cdot [Q]$. Note that this is well-defined since $J[\phi]$ is annihilated by r. Proposition 2.2 shows that $\alpha^\vee$ is surjective. Its kernel R_0 is the $\mathbb{Z}/r\mathbb{Z}$-submodule of E generated by the map ρ that sends $Q_0 \mapsto -1, Q_1 \mapsto 1, Q_t \mapsto 1$. The resulting short exact sequence of $\mathcal{G}$-modules

$$0 \to R_0 \to E \xrightarrow{\alpha^\vee} J[\phi] \to 0 \tag{2.1}$$

is split-exact, since it consists of modules that are free as $\mathbb{Z}/r\mathbb{Z}$-modules and have trivial $\mathcal{G}$-action. Dualizing (2.1) and taking Galois cohomology, we obtain

$$0 \to H^1(J[\phi]^\vee) \to H^1(E^\vee) \to H^1(R_0^\vee) \to 0, \tag{2.2}$$

which is again split-exact by functoriality. Then

$$H^1(J[\phi]^\vee) = H^1(J[\phi^\vee]) = H^1(J[\phi]),$$

where the last step follows from Lemma 2.4. Next, we compute that

$$H^1(E^\vee) = H^1(\mu_r^\Delta) = \prod_{Q\in\Delta} K_d^\times/K_d^{\times r},$$

the last step being a consequence of Hilbert's Theorem 90. Choosing the isomorphism $\mathbb{Z}/r\mathbb{Z} \xrightarrow{\sim} R_0$ given by $1 \mapsto \rho$, we identify $H^1(R_0^\vee)$ with $H^1(\mu_r) = K_d^\times/K_d^{\times r}$, where the last step again follows from Hilbert's Theorem 90. With these identifications, the short exact sequence (2.2) becomes the short exact sequence in the statement of part (1). Part (2) follows from Proposition 6.4 in [**8**]. □

It follows from Proposition 2.5 that $(x-T)$ induces a map

$$J(K_d) \longrightarrow \prod_{Q\in\Delta} K_d^\times/K_d^{\times r}.$$

We denote this map also by $(x-T)$. The map $(x-T)$ can be seen as a computation-friendly substitute for the coboundary map $\delta : J(K_d) \to H^1(J[\phi])$, since $(x-T) = \alpha\circ\delta$, where α is an injection.

The rest of this section is devoted to the computation of $(x-T)(Q)$ for $Q\in\Delta$, $Q = Q_\infty$, and $Q = P_{i,j}$.

The following lemma states that $(x-T)$ can be "evaluated on the coordinates for which it makes sense to do so."

LEMMA 2.6. *Suppose $Q\in\Delta$ and let $D\in \mathrm{Div}(C_{K_d})$ be a divisor with support outside of $\{Q, Q_\infty\}$. Then*

$$(x-T)(D)_Q = \prod_P (x(P)-x(Q))^{\mathrm{ord}_P(D)},$$

where the product is taken over all points P in the support of D.

PROOF. Choose $D'\in \mathrm{Div}(C^\circ_{K_d})$ linearly equivalent to D and $g\in K_d(C)^\times$ such that $D' = D+\mathrm{div}(g)$. Observe that $\mathrm{div}(g)$ is supported outside Q and Q_∞. Then

$$\begin{aligned}(x-T)(D)_Q = (x-T)'(D')_Q &= \prod_P (x(P)-x(Q))^{\mathrm{ord}_P(D')}\\ &= \prod_P (x(P)-x(Q))^{\mathrm{ord}_P(D+\mathrm{div}(g))}\\ &= \prod_P (x(P)-x(Q))^{\mathrm{ord}_P(D)}\prod_P (x(P)-x(Q))^{\mathrm{ord}_P(g)}.\end{aligned}$$

In the last expression however, the contribution of the second product is trivial:

$$\prod_P (x(P)-x(Q))^{\mathrm{ord}_P(g)} = \prod_P g(P)^{\mathrm{ord}_P(x-x(Q))} = g(Q)^r g(Q_\infty)^{-r} = 1,$$

where the first equality is due to Weil reciprocity and the second one rests on the calculation that $\mathrm{div}(x-x(Q)) = r\cdot Q - r\cdot Q_\infty$ for $Q\in\Delta$. □

We end this section by applying Proposition 2.5 and Lemma 2.6 to compute the images under $(x-T)$ of various divisors.

PROPOSITION 2.7. *We have:*

$$\begin{aligned}(x-T)(Q_0) &= (t,1,t),\\ (x-T)(Q_1) &= (-1,1/(1-t),t-1),\\ (x-T)(Q_t) &= (-t,1-t,t/(t-1)),\\ (x-T)(Q_\infty) &= (1,1,1),\end{aligned}$$

and

$$(x-T)(P_{i,j}) = (\zeta_d^i u, \zeta_d^i u+1, \zeta_d^i u+t).$$

PROOF. Let $(x-T)(Q_0) = (v_0,v_1,v_t)$. By Lemma 2.6, $v_1 = 1$ and $v_t = t$. By Proposition 2.5, $v_1v_t/v_0 = 1$ in $K_d^\times/K_d^{\times r}$, so $v_0 = t$. This shows that $(x-T)(Q_0) = (t,1,t)$. The calculations for Q_1 and Q_t are similar and will be left as an exercise for the reader. Using the linear equivalence $(r+1)Q_\infty \sim (r-1)Q_0 + Q_1 + Q_t$ yields

that $(x-T)(Q_\infty) = (1,1,1)$. Finally, the assertions for $P_{i,j}$ follow immediately from the definition of $(x-T)$. □

2.3. The image of $(x-T)$

Recall that $V \subset J(K_d)$ is the subgroup generated by the classes of $P_{i,j}$, where $i \in \mathbb{Z}/d\mathbb{Z}$ and $j \in \mathbb{Z}/r\mathbb{Z}$ and where we identify C with its image in J by $P \mapsto [P - Q_\infty]$. Observe that the known torsion elements Q_0, Q_1, Q_t and Q_2 (with Q_2 defined as in Section 1.4) are all contained in V.

PROPOSITION 2.8. *The dimension of $(x-T)(V)$ is*

$$\dim_{\mathbb{F}_r}((x-T)(V)) = d.$$

PROOF. First, $\dim_{\mathbb{F}_r}(x-T)(V) \leq d$ since

$$(x-T)(P_{i,j} - Q_\infty) = (x-T)(P_{i,0} - Q_\infty).$$

To show that the dimension is precisely d, we project from $\prod_{Q\in\Delta} K_d^\times / K_d^{\times r}$ to a finite-dimensional quotient space of dimension d, and conclude by showing that the projection is surjective.

For an irreducible polynomial π in $k[u]$, the valuation it induces on $K_d^\times$ is denoted $\mathrm{val}_\pi : K_d^\times \to \mathbb{Z}$. We define the following map:

$$\begin{aligned} \mathrm{pr} : \prod_{Q\in\Delta} K_d^\times / K_d^{\times r} &\to \mathbb{F}_r^d \\ (v_0, v_1, v_t) &\mapsto \left(\mathrm{val}_{u+\zeta_d^{-1}}(v_1), \mathrm{val}_{u+\zeta_d^{-2}}(v_1), \ldots, \mathrm{val}_{u+\zeta_d}(v_1), \mathrm{val}_{u+1}(v_1)\right) \end{aligned}$$

By Proposition 2.7, $(x-T)(P_{i,j} - Q_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$. We see that pr maps the image of $P_{i,j} - Q_\infty$ to the i-th basis vector. Hence pr maps $(x-T)(V)$ surjectively onto $\mathbb{F}_r^d$. This establishes the proposition. □

LEMMA 2.9. *The images under $(x-T)$ of Q_1 and Q_2 are linearly independent.*

PROOF. Since $(x-T)(P_{i,j} - Q_\infty) = (x-T)(P_{i,0} - Q_\infty)$, as noted in the proof of Proposition 2.8, the image of $Q_2 = \sum_{j=0}^{r-1} \sum_{k=0}^{r-1-j} \sum_{i\equiv k \mod r} P_{i,j}$ is the same as that of $\sum_{i=0}^{d-1}(d-i)(P_{i,0} - Q_\infty)$. Using the notation of the proof of Proposition 2.8, we find $\mathrm{pr}((x-T)(Q_2)) = (-1, -2, \ldots, -d+1, 0) \in \mathbb{F}_r^d$.

Proposition 2.7 gives $(x-T)(Q_1 - Q_\infty) = (-1, 1/(1-t), t-1)$. The factorization $1 - t = \prod_{i=0}^{d-1}(1 - \zeta_d^i u)$ in K_d yields that $\mathrm{pr}((x-T)(Q_1 - Q_\infty)) = (-1, -1, -1, \ldots, -1)$. The lemma now follows. □

2.4. Proof of the main theorem

We now use properties of V as a module over $S = \mathbb{Z}[\zeta_r]$ to prove Theorem 2.1. Write $\phi = 1 - \zeta_r$ both for the element of S and for the corresponding isogeny of J. Note that $S/\phi S \cong \mathbb{F}_r$.

PROPOSITION 2.10. $\dim_{\mathbb{F}_r}(V/\phi V) = d$ *and* $\dim_{\mathbb{F}_r}(V[\phi]) = 2$.

PROOF. V is generated over S by the $P_{i,0}$ with $i \in \mathbb{Z}/d\mathbb{Z}$, so $\dim_{\mathbb{F}_r} V/\phi V$ is at most d. On the other hand, the map

$$(x-T) : V \to \prod_{Q\in\Delta} K_d^\times / K_d^{\times r}$$

factors through $V/\phi V$ (Proposition 2.5 or Proposition 2.7) and its image has $\mathbb{F}_r$-dimension d (Proposition 2.8), so $\dim_{\mathbb{F}_r} V/\phi V \geq d$ and therefore $= d$. That $\dim_{\mathbb{F}_r} V[\phi] = 2$ was proven in Corollary 2.3. □

PROOF OF THEOREM 2.1. Let V_{tor} be the torsion submodule of V. Then V/V_{tor} is torsion-free, so projective over S, so locally free of some rank ρ. We use the preceding proposition to compute that $\rho = d - 2$.

Let $S_{(\phi)}$ and $V_{(\phi)}$ denote the localizations of S and V respectively at the (prime) ideal generated by ϕ. By the structure theorem for modules over a PID, we have

$$V_{(\phi)} \cong S_{(\phi)}^{\rho} \oplus \bigoplus_{i=1}^{t} S/(\phi^{e_i})$$

for some integers t and $e_1, \ldots, e_t$ with the $e_i > 0$. Also,

$$\rho + t = \dim_{\mathbb{F}_r} V_{(\phi)}/\phi V_{(\phi)} = \dim_{\mathbb{F}_r} V/\phi V = d$$

and

$$t = \dim_{\mathbb{F}_r} V_{(\phi)}[\phi] = \dim_{\mathbb{F}_r} V[\phi] = 2.$$

It follows that $\rho = d - 2$. Therefore

$$\operatorname{rank}_{\mathbb{Z}} V = (\operatorname{rank}_{\mathbb{Z}} S)(\operatorname{rank}_S V) = (r-1)(d-2).$$

For the torsion assertions, we note from Lemma 2.9 that Q_1 and Q_2 are linearly independent in $V/\phi V$, since their images in $\prod_{Q \in \Delta} K_d^{\times}/K_d^{\times r}$ are linearly independent. Thus they form a basis of $V_{tor}/\phi V_{tor}$. Moreover, since $\phi Q_1 = 0$, $\phi Q_2 = Q_0$ (Lemma 1.4), and $\phi Q_0 = 0$, we have that

$$V[r^{\infty}] = V[\phi^{\infty}] \cong S/(\phi) \oplus S/(\phi^2)$$

as S-modules and

$$V[r^{\infty}] \cong \mathbb{F}_r^3 = (\mathbb{Z}/r\mathbb{Z})^3$$

as $\mathbb{Z}$-modules. Finally, since $J(K_d)[\phi] = V[\phi]$ (Corollary 2.9), we have that

$$J(K_d)[r^{\infty}] = V[r^{\infty}] \cong (\mathbb{Z}/r\mathbb{Z})^3.$$

This completes the proof of the theorem. □

REMARK 2.11. With very small changes, the proof of Theorem 2.1 can be modified to handle the case where r is an odd prime power. On other hand, these methods do not suffice to treat the general case, because if r is divisible by two distinct odd primes, then $1 - \zeta_r$ is a unit in $\mathbb{Z}[\zeta_r]$.

CHAPTER 3

Minimal regular model, local invariants, and domination by a product of curves

In Section 3.1 of this chapter, we construct two useful models for the curve C/K_d over $\mathbb{P}^1_u$, i.e., surfaces $\mathcal{X}$ and $\mathcal{Y}$ equipped with projective morphisms to $\mathbb{P}^1_u$ with generic fibers C/K_d. The model $\mathcal{X}$ is a smooth surface, whereas the model $\mathcal{Y}$ is normal with mild singularities. We also work out the configuration of the components of the singular fibers of $\mathcal{X} \to \mathbb{P}^1_u$ (i.e., their genera, intersections, and self-intersections). The explicit model $\mathcal{X}$ and the analysis of the fibers play a key role in the height calculations of Chapter 4 and in the monodromy calculations of Chapter 8.

The analysis of the fibers of $\mathcal{X} \to \mathbb{P}^1_u$ is used in Section 3.2 to obtain important local invariants of the Néron model of J including its component groups and the connected component of the identity. The local invariants of the Néron model are used in our analysis of the L-function of J in Chapter 5.

Finally, in Section 3.3 we discuss a precise connection between the model $\mathcal{Y}$ and a certain product of curves. The fact that $\mathcal{X}$ and $\mathcal{Y}$ are birationally dominated by a product of curves, as shown in Section 3.3.1, allows us to prove the BSD conjecture for J. The finer analysis of the geometry of the dominating map, which occupies the rest of Section 3.3, may be of use in further study of explicit points on C, but it is not crucial for the rest of the current paper and may be omitted by readers not interested in the details.

3.1. Models

In this section, k is an arbitrary field. We fix positive integers r and d both prime to the characteristic of k, and we let C be the curve over $k(u)$ defined as in Section 1.1 where $u^d = t$. In the applications later in the paper, k is a finite extension of $\mathbb{F}_p(\mu_d)$ for some prime p not dividing rd.

For convenience, in the first part of this section, we assume that d is a multiple of r. The general case is treated in Section 3.1.5.

The model $\mathcal{Y}$ we construct is a suitable compactification of a blow-up of the irreducible surface in affine 3-space over k defined by $y^r = x^{r-1}(x+1)(x+u^d)$. The model $\mathcal{X}$ we construct is obtained by resolving isolated singularities of $\mathcal{Y}$.

3.1.1. Construction of $\mathcal{Y}$. Let $R = k[u]$, $U = \operatorname{Spec} R$, $R' = k[u']$, and $U' = \operatorname{Spec} R'$. We glue U and U' via $u' = u^{-1}$ to obtain $\mathbb{P}^1_u$ over k.

On $\mathbb{P}^1$ over k define

$$\mathcal{E} = \mathcal{O}_{\mathbb{P}^1}(d) \oplus \mathcal{O}_{\mathbb{P}^1}(d + d/r) \oplus \mathcal{O}_{\mathbb{P}^1}$$

so that $\mathcal{E}$ is a locally free sheaf of rank 3 on $\mathbb{P}^1$. Its projectivization $\mathbb{P}(\mathcal{E})$ is a $\mathbb{P}^2$ bundle over $\mathbb{P}^1$. We introduce homogeneous coordinates X, Y, Z on the part of $\mathbb{P}(\mathcal{E})$

over U and homogeneous coordinates X', Y', Z' on the part over U'. Then $\mathbb{P}(\mathcal{E})$ is the result of gluing $\operatorname{Proj}(R[X,Y,Z])$ and $\operatorname{Proj}(R'[X',Y',Z'])$ via the identifications $u = u'^{-1}$, $X = u^d X'$, $Y = u^{d+d/r} Y'$, and $Z = Z'$.

Now define $\mathcal{Z} \subset \mathbb{P}(\mathcal{E})$ as the closed subset where

$$Y^r Z = X^{r-1}(X+Z)(X+u^d Z)$$

in $\operatorname{Proj}(R[X,Y,Z])$ and

$$Y'^r Z' = X'^{r-1}(X'+u'^d Z')(X'+Z')$$

in $\operatorname{Proj}(R'[X',Y',Z'])$. Then $\mathcal{Z}$ is an irreducible, projective surface equipped with a morphism to $\mathbb{P}^1_u$. The generic fiber is the curve denoted C' in Section 1.1, which is singular at $[0,0,1]$.

We write $\mathcal{Z}_U$ and $\mathcal{Z}_{U'}$ for the parts of $\mathcal{Z}$ over U and U' respectively. Then $\mathcal{Z}_{U'}$ is isomorphic to $\mathcal{Z}_U$; indeed, up to adding primes to coordinates, they are defined by the same equation. (This is why it is convenient to assume that r divides d.) We thus focus our attention on $\mathcal{Z}_U$, i.e., on

$$\operatorname{Proj}\left(R[X,Y,Z]/(Y^r Z - X^{r-1}(X+Z)(X+u^d Z))\right).$$

We next consider the standard cover of $\mathcal{Z}_U$ by affine opens where X, Y, or Z are non-vanishing. These opens are

$$\begin{aligned}
\mathcal{Z}_1 &:= \operatorname{Spec}\left(R[x_1,y_1]/(y_1^r - x_1^{r-1}(x_1+1)(x_1+u^d))\right),\\
\mathcal{Z}_2 &:= \operatorname{Spec}\left(R[x_2,z_2]/(z_2 - x_2^{r-1}(x_2+z_2)(x_2+u^d z_2))\right),\\
\mathcal{Z}_3 &:= \operatorname{Spec}\left(R[y_3,z_3]/(y_3^r z_3 - (1+z_3)(1+u^d z_3))\right).
\end{aligned}$$

The surface $\mathcal{Z}_1$ is singular along the curve $x_1 = y_1 = 0$, so we blow up along that curve. (Strictly speaking, $\mathcal{Z}_1$ is singular along this curve only if $r > 2$. Nevertheless, we proceed as follows even if $r = 2$.) More precisely, we define

$$\begin{aligned}
\mathcal{Z}_{11} &:= \operatorname{Spec}\left(R[x_{11},y_{11}]/(y_{11} - x_{11}^{r-1}(x_{11}y_{11}+1)(x_{11}y_{11}+u^d))\right),\\
\mathcal{Z}_{12} &:= \operatorname{Spec}\left(R[x_{12},y_{12}]/(x_{12}y_{12}^r - (x_{12}+1)(x_{12}+u^d))\right),
\end{aligned}$$

and let $\tilde{\mathcal{Z}}_1$ be the glueing of $\mathcal{Z}_{11}$ and $\mathcal{Z}_{12}$ given by $(x_{11},y_{11}) = (1/y_{12}, x_{12}y_{12})$. The morphism $\tilde{\mathcal{Z}}_1 \to \mathcal{Z}_1$ defined by $(x_1,y_1) = (x_{11}y_{11}, y_{11}) = (x_{12}, x_{12}y_{12})$ is projective, surjective, and an isomorphism away from $x_1 = y_1 = 0$.

We define $\mathcal{Y}_U$ to be the glueing of $\mathcal{Z}_2$, $\mathcal{Z}_3$, and $\tilde{\mathcal{Z}}_1$ by the identifications

$$(x_2,z_2) = (1/y_3, z_3/y_3) \quad \text{and} \quad (y_3,z_3) = (1/x_{11}, 1/(x_{11}y_{11})).$$

Define $\mathcal{Y}_{U'}$ similarly (by glueing opens $\mathcal{Z}'_2$, $\mathcal{Z}'_3$, $\mathcal{Z}'_{11}$, and $\mathcal{Z}'_{12}$), and let $\mathcal{Y}$ be the glueing of $\mathcal{Y}_U$ and $\mathcal{Y}_{U'}$ along their open sets lying over $\operatorname{Spec} k[u,u^{-1}]$. The result of this glueing is a projective surface with a morphism to $\mathbb{P}^1_u$ whose generic fiber is the curve $C/k(u)$. Note that, directly from its definition, $\mathcal{Y}$ is a local complete intersection.

It is easy to see that $\mathcal{Y}$ is already covered by the affine opens $\mathcal{Z}_{11}$, $\mathcal{Z}_2$, and $\mathcal{Z}_3$, and we use this cover in some calculations later in Section 6.1. On the other hand, the coordinates of $\mathcal{Z}_{12}$ are also convenient, which is why they are included in the discussion.

A straightforward calculation with the Jacobian criterion shows that $\mathcal{Y}_U \to U$ and $\mathcal{Y}_U \to \operatorname{Spec} k$ are smooth except at the points

$$u = y_{11} = 0, \qquad x_{11}^r = 1,$$

and, when $d > 1$, at the points

$$u^d = 1, \qquad y_3 = 0, \qquad z_3 = -1.$$

The fibers of $\mathcal{Y}_U \to U$ are irreducible except over $u = 0$, where the fiber has irreducible components $y_{11} = 0$ and $x_{11}^r(x_{11}y_{11} + 1) = 1$, both of which are smooth rational curves. The points of intersection of these irreducible components are the singular points in the fiber over $u = 0$. Similar results hold for $\mathcal{Y}_{U'}$.

To finish our analysis of $\mathcal{Y}$, we note that it satisfies Serre's conditions S_n for all $n \geq 0$ since it is a local complete intersection. Moreover, it has isolated singularities, so it satisfies condition R_1 (regularity in codimension 1). It follows from Serre's criterion that $\mathcal{Y}$ is normal.

Summarizing, the discussion above proves the following result.

PROPOSITION 3.1. *The surface $\mathcal{Y}$ and morphism $\mathcal{Y} \to \mathbb{P}^1_u$ have the following properties:*

1. *$\mathcal{Y}$ is irreducible, projective, and normal.*
2. *The morphism $\mathcal{Y} \to \mathbb{P}^1_u$ is projective and generically smooth.*
3. *The singularities of $\mathcal{Y} \to \mathbb{P}^1_u$ consist of r points in the fiber over $u = 0$, one point in each fiber over points $u \in \mu_d$ and r points in the fiber over $u = \infty$. When $d > 1$, these are also the singularities of $\mathcal{Y}$, whereas if $d = 1$, only the singularities of $\mathcal{Y} \to \mathbb{P}^1_u$ over points $u \in \mu_d$ are singularities of $\mathcal{Y}$.*
4. *The fibers of $\mathcal{Y} \to \mathbb{P}^1_u$ are irreducible except over $u = 0, \infty$ where they are unions of two smooth rational curves meeting transversally in r points.*
5. *The generic fiber of $\mathcal{Y} \to \mathbb{P}^1_u$ is a smooth projective model of the curve defined by $y^r = x^{r-1}(x + 1)(x + u^d)$ over $k(u)$.*

REMARK 3.2. It is tempting to guess that $\mathcal{Y}$ is the normalization of $\mathcal{Z}$, but this is not correct. Indeed, the morphism $\mathcal{Y} \to \mathcal{Z}$ contracts the curve $u = y_{11} = 0$ in $\mathcal{Z}_{11}$, so is not finite. It is not hard to check that the normalization of $\mathcal{Z}$ is in fact the surface obtained from $\mathcal{Y}$ by contracting this curve and the analogous curve over $u = \infty$.

3.1.2. Singularities of $\mathcal{Y}$. We now show that $\mathcal{Y}$ has mild singularities. Recall that rational double points on surfaces are classified by Dynkin diagrams of type ADE. (See for example [**3**, 3.31–32].) In particular, to say that a point $y \in \mathcal{Y}$ is a rational double point of type A_n is to say that y is a double point and that there is a resolution $\mathcal{X} \to \mathcal{Y}$ such that the intersection matrix of the fiber over y is of type A_n.

PROPOSITION 3.3. *The singularities of $\overline{\mathcal{Y}} := \mathcal{Y} \times_k \overline{k}$ are all rational double points. More precisely, the singularities in the fibers over $u = 0$ and $u = \infty$ are analytically equivalent to the singularity $\alpha\beta = \gamma^d$ and are thus double points of type A_{d-1}.[1] The singularities over the points $u \in \mu_d$ are analytically equivalent to the singularity $\alpha\beta = \gamma^r$ and are thus double points of type A_{r-1}.*

PROOF. For notational simplicity, we assume that k is algebraically closed, so that $\overline{\mathcal{Y}} = \mathcal{Y}$.

First consider the fiber over $u = 0$. We use the coordinates of the open $\mathcal{Z}_{11}$, that is, the hypersurface in $\mathbb{A}^3$ defined by $y - x^{r-1}(xy + 1)(xy + u^d) = 0$. (We drop the subscripts to lighten notation.) The singularities are at the points with

[1] Of course, a "double point" of type A_0 is in fact a smooth point.

$u = y = 0$, and $x^r = 1$, and we work in the completed local ring of $\mathbb{A}^3$ at each one of these points. Choose an r-th root of unity ζ and change coordinates $x = x' + \zeta$ so that x', y, and u form a system of parameters at one of the points of interest. In the completed local ring, the element

$$x^{r-1}(xy+1) = (x'+\zeta)^{r-1}((x'+\zeta)y+1)$$

is a unit, and since d is prime to the characteristic of k, it is also a d-th power. Defining γ by $u = \gamma(x^{r-1}(xy+1))^{-1/d}$, then x', y, and γ are a system of parameters, and in these parameters, the defining equation becomes

$$y\,(1-(x'+\zeta)^r((x'+\zeta)y+1)) - \gamma^d = 0.$$

Finally, note that

$$(1-(x'+\zeta)^r((x'+\zeta)y+1) = -r\zeta^{r-1}x' - \zeta y + (\deg \geq 2)$$

where "deg ≥ 2" stands for terms of degree at least two in x' and y. Since r is prime to the characteristic of k, the coefficient of x' is not zero so we may set

$$\alpha = y, \qquad \beta = (1-(x'+\zeta)^r((x'+\zeta)y+1),$$

and have α, β, γ as a system of parameters. In these coordinates, the defining equation becomes $\alpha\beta = \gamma^d$. This proves that the singularities of $\mathcal{Y}$ over $u = 0$ are analytically equivalent to $\alpha\beta = \gamma^d$.

The argument for the points over $u = \infty$ is identical to the above.

Now consider the fiber over a point $u \in \mu_d$, using the coordinates of the open $\mathcal{Z}_3$, that is, the hypersurface in $\mathbb{A}^3$ defined by $y^r z - (1+z)(1+u^d z) = 0$. (Again we omit subscripts to lighten notation.) Choose a d-th root of unity ζ and let $u = u' + \zeta$. The singular point over $u = \zeta$ has coordinates $u' = y = 0$, $z = -1$. Setting $z = \alpha - 1$, the defining equation becomes

$$y^r(\alpha-1) - \alpha\left(1+(u'+\zeta)^d(\alpha-1)\right) = 0.$$

As before, $\alpha - 1$ is an r-th power in the completed local ring, and we set $y = \gamma(\alpha-1)^{-1/r}$. Moreover,

$$\left(1+(u'+\zeta)^d(\alpha-1)\right) = -d\zeta^{d-1}u' + \alpha + (\deg \geq 2)$$

so we may set $\beta = \left(1+(u'+\zeta)^d(\alpha-1)\right)$ and have α, β, γ as a set of parameters. In these parameters, the defining equation becomes $\gamma^r = \alpha\beta$.

To finish, it remains to observe that the singularity at the origin defined by $\alpha\beta = \gamma^n$ is a rational double point of type A_{n-1}. This is classical and due to Jung over the complex numbers. That it continues to hold in any characteristic not dividing n is stated in many references (for example [**2**, Page 15]), but we do not know of a reference for a detailed proof of this calculation.[2] It is, however, a straightforward calculation, and we leave it as an exercise for the reader. □

Remark 3.4. This paper contains two other proofs that the singularities of $\mathcal{Y}$ are rational double points. The first comes from resolving the singularity with an explicit sequence of blow-ups; see Section 3.1.4. Doing this reveals that the configurations of exceptional curves are those of rational double points of type A_n with $n = d-1$ or $r-1$. (It also reveals that the singularities are "absolutely isolated double points," i.e., double points such that at every blow up the only singularities

[2]In connection with a related proof, Artin writes "Following tradition, we omit the rather tedious verification of these results."

are isolated double points. This is one of the many characterizations of rational double points.) The calculation in Section 3.1.4 is independent of Proposition 3.3, so there is no circularity.

The second alternative proof (given in Section 3.3 below) uses the fact that $\mathcal{Y}$ is a quotient of a smooth surface by a finite group acting with isolated fixed points and cyclic stabilizers. This shows that the singularities of $\mathcal{Y}$ are cyclic quotient singularities, therefore rational singularities, and it is clear from the equations that they are double points. (The action is explicit, and we may also apply [**3**, Exercise 3.4].)

3.1.3. Construction of $\mathcal{X}$. With $\mathcal{Y}$ in hand, $\mathcal{X}$ is very simple to describe: We define $\mathcal{X} \to \mathcal{Y}$ to be the minimal desingulariztion of $\mathcal{Y}$.

Let us recall how to desingularize a rational double point of type A_n. The resolution has an exceptional divisor consisting of a string of $n-1$ smooth, rational curves, each meeting its neighbors transversally and each with self-intersection -2. If n is odd, we blow up $(n-1)/2$ times, each time introducing 2 rational curves. If n is even, the first $(n-2)/2$ blow-ups each introduce 2 rational curves, and the last introduces a single rational curve.

3.1.4. Fibers of $\mathcal{X} \to \mathbb{P}^1_u$. In this subsection, we record the structure of the bad fibers of $\mathcal{X} \to \mathbb{P}^1_u$. More specifically, we work out the configuration of irreducible components in the fibers: their genera, intersection numbers, and multiplicities in the fiber.

First consider the fiber of $\mathcal{Y} \to \mathbb{P}^1_u$ over $u = 0$. Using the coordinates of the chart $\mathcal{Z}_{11}$ above, this fiber is the union of two smooth rational curves $y = 0$ and $1 - x^r(xy+1) = 0$ meeting at the r points $y = 0$, $x^r = 1$. These crossing points are singularities of $\mathcal{Y}$ of type A_{d-1}. In the resolution $\mathcal{X} \to \mathcal{Y}$, each of them is replaced with a string of $d-1$ rational curves. It is not hard to check (by inspecting the first blow-up) that the components $y = 0$ and $1 - x^r(xy+1) = 0$ meet the end components of these strings transversely and do not meet the other components. We label the components so that those in the range $j(d-1)+\ell$ with $1 \le \ell \le d-1$ come from the point with $x = \zeta_r^j$.

Resolving the singularities thus yields the configuration of curves displayed in Figure 1 below. (This picture is for $d > 1$. If $d = 1$, then $\mathcal{Y}$ does not have singularities in the fibers over $u = 0$, and the fiber consists of a pair of smooth rational curves meeting tranversally at r points.) In the figure, C_0 is the strict transform of $1 - x^r(xy+1) = 0$, $C_{r(d-1)+1}$ is the strict transform of $y = 0$, and the other curves are the components introduced in the blow-ups.

Each component is a smooth rational curve, and all intersections are transverse. The components introduced in the blow-up have self-intersection -2. Since the intersection number of any component of the fiber with the total fiber is 0, the self-intersections of the strict transforms of C_0 and $C_{r(d-1)+1}$ are both $-r$. Those components are reduced in the fiber of $\mathcal{Y} \to \mathbb{P}^1_u$, so they must also be reduced in the fiber of $\mathcal{X} \to \mathbb{P}^1_u$. It follows that all components of the fiber of $\mathcal{X} \to \mathbb{P}^1_u$ are reduced. We note that the fiber at 0 is thus semi-stable.

As already noted, a neighborhood of $u = 0$ in $\mathcal{Y}$ is isomorphic to a neighborhoood of $u = \infty$ in $\mathcal{Y}$, so the the fiber at $u = \infty$ of $\mathcal{X} \to \mathbb{P}^1_u$ is isomorphic to that at $u = 0$. (Note that r divides d in the construction of $\mathcal{Y}$ in Section 3.1.1. We

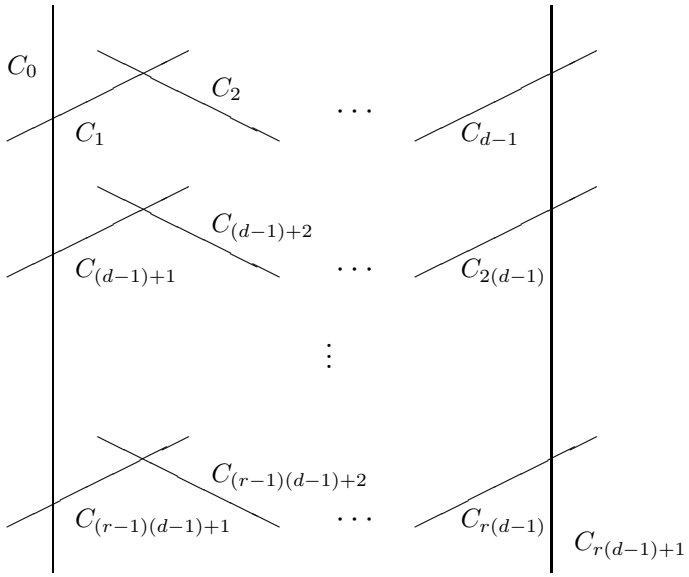


FIGURE 1. Special fiber at $u = 0$ for $d > 1$. We have $g(C_i) = 0$ for all i, $C_0^2 = C_{r(d-1)+1}^2 = -r$, and $C_i^2 = -2$ for $1 \leq i \leq r(d-1)$. All components are reduced in the fiber.

see in Section 3.1.5 that the fibers over $u = 0$ and $u = \infty$ are not isomorphic for general d.)

We now turn to the fiber over a point $u \in \mu_d$. Since $\mathbb{P}^1_u \to \mathbb{P}^1_t$ is unramified over $t = 1$, the fibers of $\mathcal{X} \to \mathbb{P}^1_u$ over the points with $u^d = 1$ are independent of d, and we may thus assume that $d = 1$. We work in the chart $\mathcal{Z}_3$ with equation $y^r z - (1+z)(1+tz) = 0$ where the singularity has coordinates $t = 1$, $y = 0$, $z = -1$. Replacing t with $t+1$ and z with $z-1$, the equation becomes $y^r(z-1) - z(z-t+tz) = 0$, and the singularity is at the origin and is of type A_{r-1}. The fiber is the curve $y^r(z-1) = z^2$, which has geometric genus $(r-2)/2$ or $(r-1)/2$ as r is even or odd, with a double point at $y = z = 0$.

We know that the singular point blows up into a chain of $r-1$ rational curves, and our task now is to see how the proper transform of the fiber intersects these curves. Since the case $r = 2$ already appears in [**52**], we assume $r > 2$ for convenience. It is also convenient to separate the cases where r is odd and where r is even.

First consider the case where r is odd. After the first blow-up, the relevant piece of the strict transform of $\mathcal{Y}$ has equation $y^{r-2} - y^{r-1}z + z(z - t + tyz) = 0$; the exceptional divisor is $z(z-t) = 0$, the union of two reduced lines meeting at the origin; and the proper transform of the original fiber meets the exceptional divisor at the origin. The next blow up introduces two lines meeting transversally at one point, and they have multiplicity 2 in the fiber. The strict transform of the original fiber passes through the intersection point and meets the components transversally. This picture continues throughout each of the blowups, and after $(r-1)/2$ steps the strict transform of the original fiber meets the chain of $r-1$ rational curves at

the intersection point of the middle two curves, and it meets each of these curves transversally.

The picture for r odd is as in Figure 2 below. The curves D_i and E_i appear at the i-th blow up; their multiplicities in the fiber are i; and the self intersections of each D_i or E_i is -2, The curve F is the proper transform of the original fiber, the smooth projective curve of genus $(r-1)/2$ associated to $y^r = x^{r-1}(x+1)^2$. Also F is reduced in the fiber and its self-intersection is $-(r-1)$. The intersections of distinct adjacent components are transversal.

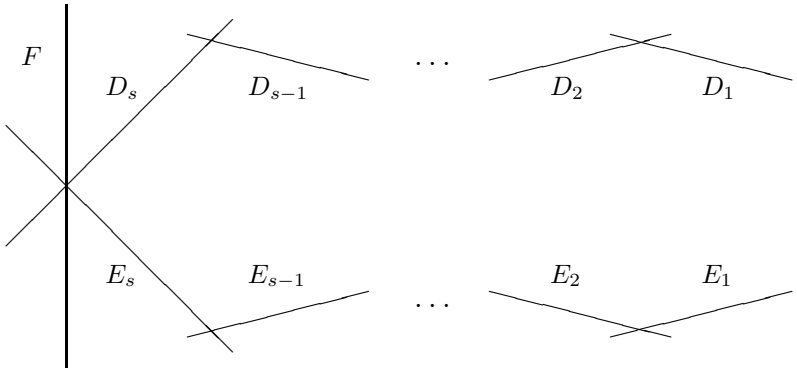


FIGURE 2. Special fiber when $u^d = 1$ and $r = 2s+1$. Here $g(D_i) = g(E_i) = 0$, $g(F) = (r-1)/2$, $D_i^2 = E_i^2 = -2$, and $F^2 = 1-r$. Multiplicities in the fiber are $m(D_i) = m(E_i) = i$ and $m(F) = 1$.

The case where r is even is similar until the last stage. After $(r-2)/2$ blow-ups, there is a chain of $r-2$ rational curves and the strict transform of the original fiber passes through the intersection point of the middle two curves. The equation at this point is $y^2 - y^{(r+2)/2}z + z(z - t + ty^{(r-2)/2}z) = 0$. The tangent cone is $y^2 + z^2 - tz = 0$, a smooth irreducible conic, so the last blow up introduces one smooth rational curve. After the last blow-up, the equation becomes $1 - y^{r/2}z + z(z - t + ty^{r/2}z) = 0$, and the strict transform of the original fiber meets the last exceptional divisor in two points namely $t = y = 0$, $z = \pm 1$. (Note that r even implies $p \neq 2$, so there really are two points of intersection.)

The picture for r even is given in Figure 3 below. Again D_i and E_i have multiplicity i in the fiber and self-intersection -2. The curve G has multiplicity $s = r/2$ in the fiber and self-intersection -2. The curve F is the strict transform of the original fiber and is the smooth projective curve associated to $y^r = x^{r-1}(x+1)^2$. It is reduced in the fiber, has genus $(r-2)/2$, and has self-intersection $-r$.

Note that the fibers of $\mathcal{X} \to \mathbb{P}^1_u$ over points with $u^d = 1$ are not semi-stable. However, it follows from [**36**, Theorem 3.11] that C/K_d acquires semi-stable reduction at these places after a tamely ramified extension. All other fibers of $\mathcal{X} \to \mathbb{P}^1_u$ are semi-stable. This yields the second part of proposition below.

Summarizing this subsection:

PROPOSITION 3.5. *The configurations of components in the singular fibers of $\mathcal{X} \to \mathbb{P}^1_u$ (genera, intersection numbers, and multiplicity in the fiber) are as described above and pictured in Figures 1, 2, and 3. The action of* $\mathrm{Gal}(K^{sep}/K)$ *on* $H^1(C \times_K \overline{K}, \mathbb{Q}_\ell)$ *is at worst tamely ramified at every place of* K.

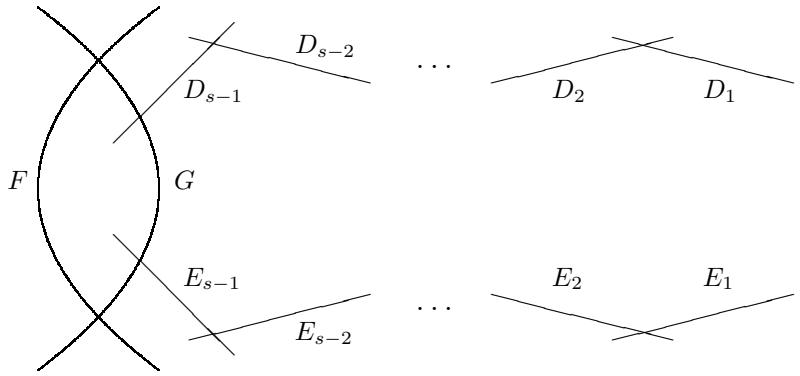


FIGURE 3. Special fiber when $u^d = 1$ and $r = 2s$. We have $g(D_i) = g(E_i) = g(G) = 0$, $g(F) = (r-2)/2 = s-1$, $D_i^2 = E_i^2 = G^2 = -2$, and $F^2 = -r$. Multiplicities in the fiber are $m(D_i) = m(E_i) = i$, $m(G) = s$, and $m(F) = 1$.

3.1.5. General d. Until now in this section, we have worked under the hypothesis that r divides d. In this subsection, we briefly sketch the construction of a regular minimal model $\mathcal{X} \to \mathbb{P}^1_u$ for general d.

In fact, the only issue is near $u = \infty$: The charts $\mathcal{Z}_2$, $\mathcal{Z}_3$, and $\mathcal{Z}_{11}$ are well defined without assuming that r divides d, and they glue as above to give an irreducible, normal surface $\mathcal{Y}^o$ with a projective morphism $\mathcal{Y}^o \to \mathbb{A}^1_u$ that is a model of C over $k(u)$. Over $u = 0$ and $u \in \mu_d$, the same steps as before lead to a regular, minimal model $\mathcal{X}^o \to \mathbb{A}^1_u$. This model is semi-stable at $u = 0$ with reduction exactly as pictured in Figure 1, and the reduction at points $u \in \mu_d$ is as pictured in Figures 2 and 3.

The situation over $u = \infty$ is more complicated, and the most efficient way to proceed is to first "go up" to level $d' = \operatorname{lcm}(d, r)$ and then take the quotient by the roots of unity of order $d'/d = r/\gcd(d, r)$. Let $\mathcal{H} = \mu_{d'/d} \subset \mu_{d'}$.

They key point to note is that in constructing the model $\mathcal{X}_{d'} \to \mathbb{P}^1_u$ where $u^{d'} = t$, we started with a completion of the affine model $y = x^{r-1}(x+1)(x+u^{d'})$, made a change of coordinates $u = u'^{-1}$, $x = u^{d'}x'$, $y = u^{d'+d'/r}y'$, and then performed a blow-up by substituting $x' \to x'y'$, $y' \to y'$. This yields the chart with equation $y' - x'^{r-1}(x'y' + u'^d)(x'y' + 1) = 0$. The action of $\mathcal{H}$ on these last coordinates is thus $\zeta(u', x', y') = (\zeta^{-1}u', \zeta^{d'/r}x', \zeta^{-d'/r}y')$. Further blowing up yields the regular minimal model $\mathcal{X}_{d'}$ whose fiber over $u' = 0$ is as described in Figure 1. The action of $\mathcal{H}$ lifts canonically to the model $\mathcal{X}_{d'}$.

We now consider the action of $\mathcal{H}$ on the special fiber over $u' = 0$. This action preserves the end components and permutes the horizontal chains with $\gcd(d, r)$ orbits. The action has 4 isolated fixed points, which are roughly speaking at the points where x' or y' are 0 or ∞. (Specifying them exactly requires considering other charts, and we omit the details since they are not important for what follows.) The exponents on the action on the tangent space are $(1, 1)$ or $(1, -1)$ with one of each type on each component. Resolving these quotient singularities leads to chains of rational curves of length 1 and $d'/d - 1 = r/\operatorname{lcm}(d, r) - 1$ respectively. (The

configuration of the component is computed using the "Hirzebruch-Jung continued fraction" as in [**4**, III.5-6].)

The picture is given in Figure 4 below. In that picture, all components are smooth rational curves. The components labeled $R_{i,j}$ with $1 \leq i \leq \gcd(r,d)$ and $1 \leq j \leq d-1$ are the images of the components C_ℓ with $1 \leq \ell \leq r(d'-1)$ in Figure 1. The components labeled $D_{d'/d}$ and $E_{d'/d}$ are the images of C_0 and $C_{r(d'-1)+1}$ respectively. The components C_1 and C_2 in Figure 4 come from resolving the singularity with local exponents $(1,1)$, and the components D_i and E_i with $1 \leq i \leq d'/d-1$ come from resolving the singularities with local exponents $(1,-1)$.

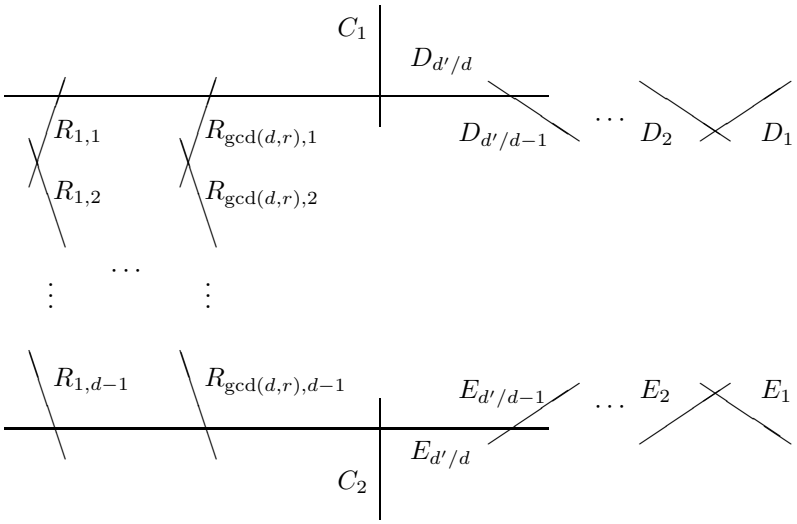


FIGURE 4. Special fiber at $u=\infty$, where $u^d = t$, d not divisible by r. All components are smooth rational curves. We have $R_{i,j}^2 = -2$, $C_i^2 = -d'/d$, $D_i^2 = E_i^2 = -2$ for $1 \leq i \leq d'/d-1$ and $D_{d'/d}^2 = E_{d'/d}^2 = -\gcd(r,d)-1$. Multiplicities in the fiber are $m(E_{i,j}) = d'/d$, $m(C_i) = 1$, and $m(D_i) = m(E_i) = i$ for $1 \leq i \leq d'/d$.

Since the components of the fiber pictured in Figure 1 are reduced and the quotient map is étale away from the isolated fixed points, the multiplicites in the fiber of the components $R_{i,j}$, $D_{d'/d}$, and $E_{d'/d}$ are d'/d and the self-intersections of the $R_{i,j}$ are all -2. The components C_1 and C_2 are reduced in the fiber and have self-intersection $-d'/d$. The components D_i and D_i with $1 \leq i \leq d'/d-1$ have self-intersection -2 and multiplicity i in the fiber. The components $D_{d'/d}$ and $E_{d'/d}$ have self intersection $-\gcd(d,r)-1$ and multiplicity d'/d in the fiber.

REMARK 3.6. The strings of rational curves in the fiber over $u=0$ correspond to r-th roots of unity, and the components in the string corresponding to $\zeta \in \mu_r$ are defined over $\mathbb{F}_p(\zeta)$. Similarly, the strings of curves R_{ij} correspond to roots of unity of order $\gcd(d,r)$. On the other hand, over places u corresponding to a d-th root of unity $\zeta' \in \mu_d$, components in the fibers are all rational over the field $\mathbb{F}_p(\zeta')$.

Also, when r is even, the two points of intersection of the curves F and G over a place with $u = \zeta'$ are defined over $\mathbb{F}_p(\zeta')$.

3.2. Local invariants of the Néron model

In this section we record the local invariants of the Néron model of J, i.e., its component group and connected component of the identity.

3.2.1. Component groups. The results of [**6**] Chapter 9, Section 6 allow us to read off the group of components of the special fiber of the Néron model of J_C from our knowledge of the fibers of $\mathcal{X} \to \mathbb{P}^1_u$.

PROPOSITION 3.7. *Suppose that r divides d and consider the group of connected components of the Néron model of J at various places of $\overline{\mathbb{F}}_p(u)$.*

1. *At $u = 0$ and $u = \infty$, the group of connected components is isomorphic to $(\mathbb{Z}/rd\mathbb{Z}) \times (\mathbb{Z}/d\mathbb{Z})^{r-2}$.*
2. *At places where $u^d = 1$, the group of connnected components is isomorphic to $\mathbb{Z}/r\mathbb{Z}$.*

PROOF. Part (1) is exactly the situation treated as an example in [**6**]; see 9.6 Corollary 11. Part (2) is an exercise using [**6**, 9.6, Theorem 1] and the well-known fact that the determinant of the matrix of a root system of type A_{r-1} is r. □

REMARK 3.8. All components of all fibers of $\mathcal{X} \to \mathbb{P}^1_u$ are rational over $\mathbb{F}_p(\mu_d)$. It follows that the group of connected components of J_C at each place of $\mathbb{F}_p(\mu_d, u)$ is split, i.e., $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p(\mu_d))$ acts trivially on it.

3.2.2. Connected components. Recall that the connected component of a smooth, commutative algebraic group over a perfect field has a filtration whose subquotients are a unipotent group (itself a repeated extension of copies of the additive group $\mathbb{G}_a$), a torus, and an abelian variety. For a place v of K_d, let a_v, m_v, and g_v be the dimensions of the unipotent (additive), toral (multiplicative), and abelian variety subquotients of the connected component of the Néron model of J_C at v. Since C has genus $r-1$, there is an equality $a_v + m_v + g_v = r - 1$. At places of good reduction, $g_v = r - 1$.

PROPOSITION 3.9. *Let $K_d = \mathbb{F}_p(\mu_d, u)$.*

1. *If v is the place of K_d over $u = 0$, then $a_v = g_v = 0$ and $m_v = r - 1$.*
2. *If v is a place of K_d over $u \in \mu_d$ and r is even, then $a_v = (r-2)/2$, $m_v = 1$, and $g_v = (r-2)/2$.*
3. *If v is a place of K_d over $u \in \mu_d$ and r is odd, then $a_v = (r-1)/2$, $m_v = 0$, and $g_v = (r-1)/2$.*
4. *If v is the place of K_d over $u = \infty$, then $a_v = r - \gcd(r,d)$, $m_v = \gcd(r,d)$, and $g_v = 0$.*

PROOF. It suffices to compute m_v and g_v. We note that [**6**, Section 9.2] gives g_v and m_v in terms of the special fiber at v of a minimal regular model of C, i.e., in terms of $\mathcal{X}$. Over $u = 0$, where $\mathcal{X} \to \mathbb{P}^1_u$ has semi-stable reduction, [**6**, 9.2, Example 8] shows that $g_v = 0$ and $m_v = r - 1$, proving part (1).

In general, both m_v and g_v only depend on the reduced curve underlying the fiber [**6**, 9.2, Proposition 5]. By [**6**, 9.2, Proposition 10], g_v is the sum of the genera of the irreducible components of the reduced special fiber. When r is even, the

reduced fiber is semi-stable, and again [**6**, 9.2, Example 8] shows that $m_v = 1$, proving part (2). When r is odd, applying [**6**, 9.2, Proposition 10] (with C' and C the reduced special fiber, which is tree-like) shows that $m_v = 0$, proving part (3). Over $u = \infty$, all components are rational curves, so $g_v = 0$. The reduced fiber is semistable of arithmetic genus $\gcd(d, r) - 1$, so $m_v = \gcd(d, r) - 1$, which completes the proof of part (4). □

3.3. Domination by a product of curves

In Section 3.3.1, we show that the surface $\mathcal{Y}$ constructed in Section 3.1.1 is dominated by a product of curves. In the following subsections, we upgrade this to a precise isomorphism between $\mathcal{Y}$ and a quotient of a product of curves by a finite group in the style of Berger's construction [**5**] and of [**50**]. This casts some light on the singularities of $\mathcal{Y}$, and it may prove useful later for constructing explicit points on C over K_d for values of d other than divisors of $p^f + 1$ as in [**10**, Section 10].

Throughout, k is a field of characteristic $p \geq 0$, and r and d are positive integers prime to p such that r divides d. We assume also that k contains the d-th roots of unity.

3.3.1. Domination of $\mathcal{Y}$ by a product of curves. The surface $\mathcal{Y}$ is birational to the affine surface over k given by $y^r = x^{r-1}(x+1)(x+u^d)$. Consider the smooth projective curves over k given by

$$\mathcal{C} = \mathcal{C}_{r,d} : z^d = x^r - 1 \quad \text{and} \quad \mathcal{D} = \mathcal{D}_{r,d} : w^d = y^r - 1.$$

Then a simple calculation shows that the assignment

$$\begin{aligned} \phi^*(u) &= zw, \\ \phi^*(x) &= z^d, \\ \phi^*(y) &= xyz^d \end{aligned} \tag{3.1}$$

defines a dominant rational map $\phi : \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathcal{Y}$.

In the rest of this section, we analyze the geometry of this map more carefully.

3.3.2. Constructing $\mathcal{C}$ with its G action. First, we construct a convenient model of the curve $\mathcal{C}$ over k with equation $z^d = x^r - 1$. Namely, we glue the smooth k-schemes

$$\mathcal{U}_1 = \operatorname{Spec} k[x_1, z_1] / \left(z_1^d - x_1^r + 1\right)$$

and

$$\mathcal{U}_2 = \operatorname{Spec} k[x_2, z_2] / \left(x_2^r(z_2^d + 1) - 1\right)$$

via the identifications $x_1 = x_2^{-1} z_2^{-d/r}$ and $z_1 = z_2^{-1}$. The result is a smooth projective curve that we call $\mathcal{C}$.

There is an action of $G = \mu_r \times \mu_d$ on $\mathcal{C}$ defined by

$$(\zeta_r, \zeta_d)(x_1, z_1) = (\zeta_r x_1, \zeta_d z_1) \quad \text{and} \quad (\zeta_r, \zeta_d)(x_2, z_2) = (\zeta_r^{-1} \zeta_d^{-d/r} x_2, \zeta_d^{-1} z_2).$$

There are three collections of points on $\mathcal{C}$ with non-trivial stabilizers: the r points where $z_1 = 0$ and $x_1^r = 1$, which each have stabilizer $1 \times \mu_d$; the d points where $x_1 = 0$ and $z_1^d = -1$, which each have stabilizer $\mu_r \times 1$; and the r points where $z_2 = 0$ and $x_2^r = 1$, which each have stabilizer

$$H := \left\{ (\zeta_d^{-di/r}, \zeta_d^i) \,\middle|\, 0 \leq i \leq d-1 \right\}.$$

We call these fixed points of type μ_d, μ_r, and H respectively.

3.3.3. $\mathcal{C} \times_k \mathcal{D}$ and its fixed points. We let $\mathcal{D}$ be the curve defined just as $\mathcal{C}$ was, but with opens $\mathcal{V}_1$ and $\mathcal{V}_2$ defined with coordinates y_1, y_2, w_1, w_2 in place of $x_1,\ldots,z_2$. We let G act "anti-diagonally" on the product surface $\mathcal{C} \times_k \mathcal{D}$, i.e., by the action on $\mathcal{C}$ defined above, and by the inverse action on $\mathcal{D}$ (so that $(\zeta_r, \zeta_d)(y_1, w_1) = (\zeta_r^{-1} y_1, \zeta_d^{-1} w_1)$).

If $(c, d) \in \mathcal{C} \times_k \mathcal{D}$, then the stabilizer of (c, d) is the intersection of the stabilizers c and d in G. This yields the following list of points (c, d) of $\mathcal{C} \times_k \mathcal{D}$ with non-trivial stabilizers:

(i) if both c and d are fixed points of type μ_d, then $\mathrm{Stab}(c, d) = \mu_d$;

(ii) if both c and d are fixed points of type μ_r, then $\mathrm{Stab}(c, d) = \mu_r$;

(iii) if both c and d are fixed points of type H, then $\mathrm{Stab}(c, d) = H$;

(iv) if c is of type μ_d and d is of type H, then $\mathrm{Stab}(c, d) = (1 \times \mu_d) \cap H$, a cyclic group of order d/r;

(v) if c is of type H and d is of type μ_d, then $\mathrm{Stab}(c, d) = (1 \times \mu_d) \cap H$.

We call the fixed points of types (i)-(iii) "unmixed" and the fixed points of types (iv) and (v) "mixed." Note that at an unmixed fixed point, the action on the tangent space in suitable coordinates is of the form (ζ, ζ^{-1}), while at a mixed fixed point, the action is by scalars ζ.

3.3.4. $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ with its G-action. We define $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ to be the blow up of $\mathcal{C}_D \times_k \mathcal{D}$ at each of its $2r^2$ mixed fixed points. The action of G on $\mathcal{C}_D \times_k \mathcal{D}$ lifts uniquely to $\widetilde{\mathcal{C} \times_k \mathcal{D}}$. By the remark above about the action of G on the tangent space at the mixed fixed points, G fixes the exceptional divisor of $\widetilde{\mathcal{C} \times_k \mathcal{D}} \to \mathcal{C} \times_k \mathcal{D}$ pointwise. These are "divisorial" fixed points. The other fixed points of G acting on $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ are the inverse images of the unmixed fixed points of $\mathcal{C} \times_k \mathcal{D}$.

Now consider the quotient $\widetilde{\mathcal{C} \times_k \mathcal{D}}/G$. It is smooth away from the images of the unmixed fixed points. Those of type (i) fall into r orbits and their images in the quotient are rational double points of type A_{d-1}. Those of type (ii) fall into d orbits and their images in the quotient are rational double points of type A_{r-1}. Those of type (iii) fall into r orbits and their images in the quotient are rational double points of type A_{d-1}.

3.3.5. An isomorphism. The main goal of this section is the following isomorphism. Recall $\mathcal{Y}$, the model of C/K_d defined in Section 3.1.1.

Proposition 3.10. *There is a unique isomorphism*

$$\rho : \left(\widetilde{\mathcal{C} \times_k \mathcal{D}}\right)/G \to \mathcal{Y}$$

such that the composition

$$\mathcal{C} \times_k \mathcal{D} \dashrightarrow \widetilde{\mathcal{C} \times_k \mathcal{D}} \to \widetilde{\mathcal{C} \times_k \mathcal{D}}/G \to \mathcal{Y}$$

is the rational map $\phi : \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathcal{Y}$ of equation (3.1) *in Section 3.3.1.*

Uniqueness is clear. The key point in the proof of existence is the following lemma.

Lemma 3.11. *There exists a G-equivariant, quasi-finite morphism $\psi : \widetilde{\mathcal{C} \times_k \mathcal{D}} \to \mathcal{Y}$ (with G acting trivially on $\mathcal{Y}$) inducing the rational map $\phi : \mathcal{C} \times_k \mathcal{D} \dashrightarrow \mathcal{Y}$.*

PROOF. The rational map ϕ induces a rational map $\widetilde{\mathcal{C} \times_k \mathcal{D}} \dashrightarrow \mathcal{Y}$, and what has to be shown is that there is a quasi-finite morphism ψ representing this rational map. To do so, we cover $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ with affine opens and check that each is mapped by a quasi-finite morphism (the unique one compatible with ϕ) into $\mathcal{Y}$. The details are tedious but straightforward calculations with coordinates.

It is helpful to have a standard representation of elements of the function field $\mathcal{Y}$. Using the coordinates of $\mathcal{Z}_1$, the field $k(\mathcal{Y})$ is generated by x, y, and u with relation $y^r = x^{r-1}(x+1)(x+u^d)$. (We drop the subscripts 1 to avoid confusion with coordinates on $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ below.) Inclusion of the opens $\mathcal{Z}_2$, $\mathcal{Z}_3$, $\mathcal{Z}_{11}$, $\mathcal{Z}_{12}$, $\mathcal{Z}'_2$, $\mathcal{Z}'_3$, $\mathcal{Z}'_{11}$, and $\mathcal{Z}'_{12}$ into $\mathcal{Y}$ induces isomorphisms between the function fields of the opens and that of $\mathcal{Y}$. This leads to the following equalities in $k(\mathcal{Y})$:

$$\begin{aligned}
&x_2 = x/y, && y_3 = y/x, && x_{11} = x/y, && x_{12} = x,\\
&z_2 = 1/y, && z_3 = 1/x, && y_{11} = y, && y_{12} = y/x,\\
&u' = u^{-1},\\
&x'_2 = u^{d/r}x/y, && y'_3 = u^{-d/r}y/x, && x'_{11} = u^{d/r}x/y, && x'_{12} = u^{-d}x,\\
&z'_2 = u^{d+d/r}/y, && z'_3 = u^d/x, && y'_{11} = u^{-d-d/r}y, && y'_{12} = u^{-d/r}y/x.
\end{aligned}$$

Similarly, the function field of $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ is generated by x_1, z_1, y_1, w_1 with relations $z_1^d = x_1^r - 1$ and $w_1^d = y_1^r - 1$. Inclusion of the opens $\mathcal{U}_i \times \mathcal{V}_j$ leads to the equalities:

$$\begin{aligned}
&z_2 = z_1^{-1}, && w_2 = w_1^{-1},\\
&x_2 = z_1^{d/r}/x_1, && y_2 = w_1^{d/r}/y_1.
\end{aligned}$$

The blowing up of points in $\mathcal{U}_1 \times \mathcal{V}_2$ and $\mathcal{U}_2 \times \mathcal{V}_1$ made to pass from $\mathcal{C} \times_k \mathcal{D}$ to $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ leads to additional equalities stated below.

For the last key piece of data, we recall the field inclusion $\phi^* : k(\mathcal{Y}) \hookrightarrow k(\mathcal{C} \times_k \mathcal{D})$. It yields equalities

$$\phi^*(u) = z_1 w_1, \qquad \phi^*(x) = z_1^d, \qquad \phi^*(y) = x_1 y_1 z_1^d.$$

We now cover $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ with affine opens (many of them, unfortunately) and for each of them check that there is a quasi-finite morphism from the open to $\mathcal{Y}$ that induces the field inclusion ϕ^*. The compatibility with ϕ^* shows that these morphisms agree on the overlaps, so this yields a global quasi-finite morphism $\psi : \widetilde{\mathcal{C} \times_k \mathcal{D}} \to \mathcal{Y}$. Since the image of ϕ^* is generated by $z_1 w_1$, z_1^d, and $x_1 y_1$, it lies inside the G-invariant subfield of $k(\widetilde{\mathcal{C} \times_k \mathcal{D}})$, and this shows that ψ collapses the orbits of G; this is the claimed equivariance.

We now make the necessary coordinate calculations, starting with the open $\mathcal{U}_1 \times \mathcal{V}_1$. The formulae above show that

$$\phi^*(u) = z_1 w_1, \qquad \phi^*(x_{12}) = z_1^d, \qquad \phi^*(y_{12}) = x_1 y_1.$$

This shows that there is a morphism $\psi_{11} : \mathcal{U}_1 \times \mathcal{V}_1 \to \mathcal{Z}_{12} \hookrightarrow \mathcal{Y}$ inducing ϕ. To see that ψ_{11} is quasi-finite, we note that fixing the value of x_{12} implies at most d choices for z_1, which in turn allows for at most r choices of x_1. Fixing y_{12} then determines y_1 and fixing u determines w_1. This shows that ψ_{11} has fibers of cardinality at most rd (and generically equal to rd).

The rest of the proof proceeds similarly with other affine opens of $\widetilde{\mathcal{C} \times_k \mathcal{D}}$. Considering $\mathcal{U}_2 \times \mathcal{V}_2$, we note that

$$\phi^*(u') = z_2 w_2, \qquad \phi^*(x'_{12}) = w_2^d, \qquad \phi^*(y'_{12}) = x_2^{-1} y_2^{-1}.$$

Since x_2 and y_2 are units on $\mathcal{U}_2 \times \mathcal{V}_2$, these formulae define a morphism $\psi_{22} : \mathcal{U}_2 \times \mathcal{V}_2 \to \mathcal{Z}'_{12} \hookrightarrow \mathcal{Y}$ that is compatible with ϕ. The reader may check that ψ_{22} and the other morphisms defined below are quasi-finite.

These formulae define ψ away from the blow ups of the mixed fixed points.

Now we focus our attention near a particular mixed fixed point in $\mathcal{U}_1 \times_k \mathcal{V}_2$, say P_{ij} given by $x_1 = \zeta_r^i$, $z_1 = 0$, $y_2 = \zeta_r^j$, and $w_2 = 0$. Let

$$f = \frac{(x_1^r - 1)}{(x_1 - \zeta_r^i)} \frac{(y_2^r - 1)}{(y_2 - \zeta_r^j)}.$$

Inverting f gives an affine open subset of $\mathcal{U}_1 \times_k \mathcal{V}_2$ on which the only solution of $z_1 = w_2 = 0$ is P_{ij}. We may cover the blow up at P_{ij} of this open with two affine opens:

$$T_{ij}^1 = \operatorname{Spec} \frac{k[x_1, s, y_2, w_2][1/f]}{(...)}$$

and

$$T_{ij}^2 = \operatorname{Spec} \frac{k[x_1, z_1, y_2, t][1/f]}{(...)}$$

where $z_1 = s w_2$ on T_{ij}^1 and $w_2 = t z_1$ on T_{ij}^2.

Noting that

$$\phi^*(u) = s, \qquad \phi^*(x_{11}) = y_2 w_2^{d/r} x_1^{-1}, \qquad \phi^*(y_{11}) = x_1 s^d w_2^{d-d/r} y_2^{-1},$$

we define a morphism ψ_{121ija} from the open of T_{ij}^1 where $x_1 \neq 0$ to $\mathcal{Z}_{11}$. Noting that

$$\phi^*(u) = s, \qquad \phi^*(x_{12}) = s^d w_2^d, \qquad \phi^*(y_{12}) = x_1 y_2^{-1} w_2^{-d/r},$$

we define a morphism ψ_{121ijb} from the open of T_{ij}^1 where $w_2 \neq 0$ to $\mathcal{Z}_{12}$. Since w_2 and x_1 do not vanish simultaneously on T_{ij}^1, this defines a morphism $\psi_{121ij} : T_{ij}^1 \to \mathcal{Y}$.

Similarly, noting that

$$\phi^*(u') = t, \qquad \phi^*(x'_{12}) = t^d z_1^d, \qquad \phi^*(y'_{12}) = x_1 y_2^{-1} z_1^{-d/r},$$

we define a morphism ψ_{122ija} from the open of T_{ij}^2 where $z_1 \neq 0$ to $\mathcal{Z}'_{12}$. Noting that

$$\phi^*(u') = t, \qquad \phi^*(x'_{11}) = y_2 z_1^{d/r} x_1^{-1}, \qquad \phi^*(y'_{11}) = t^d x_1 z_1^{d-d/r} y_2^{-1},$$

we define a morphism ψ_{122ijb} from the open of T_{ij}^2 where $x_1 \neq 0$ to $\mathcal{Z}'_{11}$. Since z_1 and x_1 do not vanish simultaneously on T_{ij}^2, this defines a morphism $\psi_{122ij} : T_{ij}^2 \to \mathcal{Y}$.

The morphisms ψ_{121ij} and ψ_{122ij} for varying ij patch together to give a morphism ψ_{12} from the part of $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ lying over $\mathcal{U}_1 \times \mathcal{V}_2$ to $\mathcal{Y}$.

It remains to consider neighborhoods of the blow ups of the mixed fixed points in $\mathcal{U}_2 \times_k \mathcal{V}_1$. Let Q_{ij} be the point where $x_2 = \zeta_r^i$, $z_2 = 0$, $y_1 = \zeta_r^j$, and $w_1 = 0$. Let

$$g = \frac{(x_2^r - 1)}{(x_2 - \zeta_r^i)} \frac{(y_1^r - 1)}{(y_1 - \zeta_r^j)}.$$

Inverting g gives an affine open subset of $\mathcal{U}_2 \times_k \mathcal{V}_1$ on which the only solution of $z_2 = w_1 = 0$ is Q_{ij}. We may cover the blow up at Q_{ij} of this open with two affine opens:

$$T^3_{ij} = \operatorname{Spec} \frac{k[x_2, s, y_1, w_1][1/g]}{(...)}$$

and

$$T^4_{ij} = \operatorname{Spec} \frac{k[x_2, z_2, y_1, t][1/g]}{(...)}$$

where $z_2 = sw_1$ on T^3_{ij} and $w_1 = tz_2$ on T^4_{ij}.

Noting that

$$\phi^*(u') = s, \qquad \phi^*(y'_3) = y_1 x_2^{-1} w_1^{-d/r}, \qquad \phi^*(z'_3) = w_1^d,$$

we define a morphism ψ_{213ija} from the open of T^3_{ij} where $w_1 \neq 0$ to $\mathcal{Z}'_3$. Noting that

$$\phi^*(u') = s, \qquad \phi^*(x'_2) = x_2 w_1^{d/r} y_1^{-1}, \qquad \phi^*(z'_2) = x_2 w_1^{d+d/r} y_1^{-1},$$

we define a morphism ψ_{213ijb} from the open of T^3_{ij} where $y_1 \neq 0$ to $\mathcal{Z}'_2$. Since w_1 and y_1 do not vanish simultaneously on T^3_{ij}, this defines a morphism $\psi_{213ij} : T^3_{ij} \to \mathcal{Y}$.

Noting that

$$\phi^*(u) = t, \qquad \phi^*(x_2) = x_2 z_2^{d/r} y_1^{-1}, \qquad \phi^*(z_2) = x_2 z_2^{d+d/r} y_1^{-1},$$

we define a morphism ψ_{214ija} from the open of T^4_{ij} where $y_1 \neq 0$ to $\mathcal{Z}_2$. Noting that

$$\phi^*(u) = t, \qquad \phi^*(y_3) = y_1 x_2^{-1} z_2^{-d/r}, \qquad \phi^*(z_3) = z_2^d,$$

we define a morphism ψ_{214ijb} from the open of T^4_{ij} where $z_2 \neq 0$ to $\mathcal{Z}_3$. Since y_1 and z_2 do not vanish simultaneously on T^4_{ij}, this defines a morphism $\psi_{214ij} : T^4_{ij} \to \mathcal{Y}$.

The morphisms ψ_{213ij} and ψ_{214ij} for varying ij patch together to give a morphism ψ_{21} from the part of $\widetilde{\mathcal{C} \times_k \mathcal{D}}$ lying over $\mathcal{U}_2 \times \mathcal{V}_1$ to $\mathcal{Y}$.

Finally, the morphisms ψ_{11}, ψ_{22}, ψ_{12}, and ψ_{21} patch together to give a quasi-finite morphism $\psi : \widetilde{\mathcal{C} \rtimes \mathcal{D}} \to \mathcal{Y}$ that collapses the orbits of G and induces ϕ. This completes the proof of the lemma. □

Proof of Proposition 3.10. By Lemma 3.11, there is a quasi-finite morphism $\psi : \widetilde{\mathcal{C} \times_k \mathcal{D}} \to \mathcal{Y}$ of generic degree rd. By G-equivariance, this factors through the quotient to give a quasi-finite morphism $\rho : \widetilde{\mathcal{C} \times_k \mathcal{D}}/G \to \mathcal{Y}$. Considering degrees shows that ρ is birational. On the other hand, ρ is proper (because $\mathcal{C} \times_k \mathcal{D}$ is projective) and quasi-finite, so finite. But $\mathcal{Y}$ is normal and a birational, finite morphism to a normal scheme is an isomorphism. This establishes that ρ gives the desired isomorphism. □

Remark 3.12. Examining the morphism above shows that the fixed points of types (i) and (iii) map to the singular points of $\mathcal{Y}$ in the fibers over $u = 0$ and ∞. The fixed points of type (ii) map to the singular points in the fibers over points $u \in \mu_d$. This gives another proof that the singularities of $\mathcal{Y}$ are rational double points of type A_{d-1} and A_{r-1}.

CHAPTER 4

Heights and the visible subgroup

In this chapter, we work over $K_d = \mathbb{F}_p(\mu_d, u)$ with $u^d = t$, and we assume that $d = p^\nu + 1$ and r divides d. We have explicit points P_{ij} defined in Chapter 1 and the subgroup V of $J(K_d)$ generated by their classes. Our first main task is to compute the Néron-Tate canonical height pairing on V. We then compare this with a group-theoretic pairing defined on R/I where R is the group ring $\mathbb{Z}[\mu_d \times \mu_r]$ and I is the ideal defined in Section 1.3. This allows us to show that there is an R-module isomorphism $V \cong R/I$. We also compute the discriminant of the height pairing on V.

4.1. Height pairing

In this section, we compute the height pairing on various points of $J(K_d)$. Recall that we identify C with its image in J by $P \mapsto [P - Q_\infty]$. We consider the Néron-Tate canonical height pairing divided by $\log|\mathbb{F}_p(\mu_d)|$, as discussed for example in [**51**, Section 4.3]. This is a $\mathbb{Q}$-valued, non-degenerate, bilinear pairing that is defined at the beginning of the next subsection.

We compute $\langle P_{ij}, P_{00}\rangle$ for $0 \le i \le d-1$ and $0 \le j \le r-1$. This determines the pairing, since its compatibility with the action of $\mu_d \times \mu_r$ implies that $\langle P_{ij}, P_{i'j'}\rangle = \langle P_{i-i',j-j'}, P_{00}\rangle$.

THEOREM 4.1. *The height pairing $\langle P_{ij}, P_{00}\rangle$ is given by*

$$\langle P_{ij}, P_{00}\rangle = -\frac{d-1}{rd} \cdot \begin{cases} -(r-1)(d-2) & \text{if } (i,j) = (0,0), \\ r-2 & \text{if } i \not\equiv 0 \bmod r, j = 0, \\ 2r-2 & \text{if } i \neq 0, i \equiv 0 \bmod r, j = 0, \\ d-2 & \text{if } i = 0, j \neq 0, \\ r-2 & \text{if } i \neq 0, j \neq 0, i+j \equiv 0 \bmod r, \\ -2 & \text{if } i \neq 0, j \neq 0, i+j \not\equiv 0 \bmod r. \end{cases}.$$

This was already proved in [**52**, Section 8] in the case $r = 2$, so to avoid distracting special cases, we assume $r > 2$ for the rest of this section.

4.1.1. Basic theory. Let P and P' be two points on $C(K_d)$ identified as usual with a subset of $J(K_d)$ using Q_∞ as a base point; we later set $P = P_{00}$ and $P' = P_{ij}$. Then the height pairing is defined by

$$\begin{aligned} \langle P, P'\rangle &= -(P - Q_\infty - D_P) \cdot (P' - Q_\infty) \\ &= -P \cdot P' + P \cdot Q_\infty + P' \cdot Q_\infty - Q_\infty^2 - D_P \cdot P', \end{aligned}$$

with notation as follows: we identify a point of C with the corresponding section of the regular proper model $\pi : \mathcal{X} \to \mathbb{P}^1_u$ and the dot indicates the intersection pairing on $\mathcal{X}$. The divisor D_P is a divisor with $\mathbb{Q}$-coefficients that is supported on

components of fibers of π and satisfies $(P-Q_\infty+D_P)\cdot Z = 0$ for every component Z of every fiber of π. We may also insist that $D_P \cdot Q_\infty = 0$ in which case D_P is uniquely determined. The "correction term" $D_P \cdot P'$ is a sum of local terms that depend only on the components of the fiber that P and P' meet. The other intersection pairings can be computed as sums of local terms, except the self-intersection $Q_\infty \cdot Q_\infty$ and (when $P' = P$) $P \cdot P$. The latter two are computable in terms of the degree of a conormal bundle.

4.1.2. Auxiliary results. The following results are useful for computing the various intersection numbers.

In the first result, we focus attention on the special fiber at a place v with components $C_0, C_1, \ldots, C_n$ and let A_{ij} (with indices $0 \le i, j \le n$) be the intersection matrix: $A_{ij} = C_i \cdot C_j$. We number the components so that Q_∞ meets C_0. We write $(D_P \cdot P')_v$ for the part of the intersection multiplicity coming from intersections in the fiber over v. With these conventions, it is easy to see that if P or P' meets C_0, then $(D_P \cdot P')_v = 0$.

LEMMA 4.2. *Suppose that P intersects C_k, and P' intersects C_ℓ, with $k, \ell > 0$. Let B be the matrix obtained by deleting the 0-th row and column from A. Let B' be the submatrix obtained by deleting the k-th row and ℓ-th column from B. Finally, let D_P denote the fibral divisor satisfying the conditions described above. Then*

$$D_P \cdot P' = (-1)^{k+\ell+1}\frac{\det(B')}{\det(B)} = (-1)^{k+\ell}\frac{\det(-B')}{\det(-B)}.$$

PROOF. Write $D_P = \sum_{h=0}^{n} d_h C_h$ with $d_h \in \mathbb{Q}$. The conditions on D_P imply $D_P \cdot C_h = (Q_\infty - P)\cdot C_h$ for all h. Also $d_0 = 0$ because $D_P \cdot Q_\infty = 0$. The intersection number $(D_P \cdot P')_v$ is just d_ℓ.

Writing $\mathbf{d} = (d_1, \ldots, d_n)^t$, the conditions on D_P are equivalent to

$$B\mathbf{d} = -\mathbf{e}_k,$$

where $\mathbf{e}_k$ is the k-th standard basis vector. Since B is non-singular, the unique solution $\mathbf{d}$ is given by Cramer's rule, and thus

$$(D_P \cdot P')_v = d_\ell = (-1)^{k+\ell+1}\frac{\det(B')}{\det(B)},$$

as desired. □

LEMMA 4.3. *Let A_m be the $m \times m$ root matrix of type A, in other words, the matrix whose entries are given by*

$$a_{ij} = \begin{cases} -2 & \text{if } i = j, \\ 1 & \text{if } |i-j| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\det(-A_m) = (m+1)$.

PROOF. This is a standard exercise using induction on m. See [**21**, Page 63]. □

LEMMA 4.4. *Let $d_1, \dots, d_r$ be positive integers, and let $B = B(d_1, \dots, d_r)$ be the block matrix*

$$\begin{bmatrix} A_{d_1-1} & & & & e_{d_1-1} \\ & A_{d_2-1} & & & e_{d_2-1} \\ & & \ddots & & \vdots \\ & & & A_{d_r-1} & e_{d_r-1} \\ e_{d_1-1}^T & e_{d_2-1}^T & \cdots & e_{d_r-1}^T & -r \end{bmatrix},$$

where A_m is the $m \times m$ root matrix discussed in Lemma 4.3, and e_m is the column vector of length m with a 1 in the last spot and 0 everywhere else. (If $m = 0$, then A_m and e_m are by convention empty blocks.) Then

$$\det(-B) = \Big(\prod d_i\Big)\Big(\sum \frac{1}{d_i}\Big).$$

PROOF. We compute the determinant of $-B$ by applying Laplace (cofactor) expansion, first across the bottom row, and then down the rightmost column. Using Lemma 4.3, the cofactor corresponding to the entry r is $r \prod d_i$. Another application of Lemma 4.3 shows that the cofactor corresponding to removing the bottom row, the row containing the 1 in e_{d_i-1}, the rightmost column, and the column containing the 1 of $e_{d_j-1}^T$ is $-(d_i - 1)\prod_{j \neq i} d_j$ if $i = j$ and zero otherwise. This shows that the determinant of $-B$ is

$$r \prod_{i=1}^{r} d_i - \sum_{i=1}^{r} (d_i - 1) \prod_{j \neq i} d_j,$$

which is equal to $(\prod d_i)(\sum 1/d_i)$ as desired. □

LEMMA 4.5. *Let $d \geq 2$ and $r \geq 2$ be integers and let $B = B(d, d, \dots, d)$ (with d repeated r times, using the notation of Lemma 4.4).*

1. *Let B' be the matrix obtained from B by deleting the first row and the d-th column. Then $\det(-B') = (-1)^{d-1} d^{r-2}$.*
2. *Let B'' be the matrix obtained from B by deleting row $d-1$ and column $2(d-1)$. Then $\det(-B'') = (-1)^{d-1}(d-1)^2 d^{r-2}$.*

PROOF. (1) For $1 \leq n \leq d-2$, let R_n be the matrix obtained from A_{d-1} by deleting the first n rows and the first $n-1$ columns. Similarly, let S_n be the matrix obtained from A_{d-1} by deleting the first n columns and the first $n-1$ rows. The matrix B' under discussion is thus

$$B' = B_1' = \begin{bmatrix} R_1 & & & & & e_{d-2} \\ & S_1 & & & & e_{d-1} \\ & & A_{d-1} & & & e_{d-1} \\ & & & \ddots & & \vdots \\ & & & & A_{d-1} & e_{d-1} \\ e_{d-1}^T & e_{d-2}^T & e_{d-1}^T & \cdots & e_{d-1}^T & -r \end{bmatrix}$$

where there are $r-2$ blocks of A_{d-1}. Note that if $d \geq 3$, the upper left entry of B_1' is 1 and the rest of the first column is zero. Expanding in cofactors down the first

column shows that $\det(B_1') = \det(B_2')$ where

$$B_2' = \begin{bmatrix} R_2 & & & & & e_{d-3} \\ & S_1 & & & & e_{d-1} \\ & & A_{d-1} & & & e_{d-1} \\ & & & \ddots & & \vdots \\ & & & & A_{d-1} & e_{d-1} \\ e_{d-2}^T & e_{d-2}^T & e_{d-1}^T & \cdots & e_{d-1}^T & -r \end{bmatrix}.$$

Continuing in similar fashion for another $d-3$ steps shows that $\det(B_1') = \det(B_{d-1}')$ where

$$B_{d-1}' = \begin{bmatrix} 0 & S_1 & & & & e_{d-1} \\ & & A_{d-1} & & & e_{d-1} \\ & & & \ddots & & \vdots \\ & & & & A_{d-1} & e_{d-1} \\ 1 & e_{d-2}^T & e_{d-1}^T & \cdots & e_{d-1}^T & -r \end{bmatrix}.$$

Now we expand across rows of the S_1, finding that $\det(B_1') = -\det(B_d')$ where

$$B_d' = \begin{bmatrix} 0 & S_2 & & & & e_{d-2} \\ & & A_{d-1} & & & e_{d-1} \\ & & & \ddots & & \vdots \\ & & & & A_{d-1} & e_{d-1} \\ 1 & e_{d-3}^T & e_{d-1}^T & \cdots & e_{d-1}^T & -r \end{bmatrix}.$$

Continuing in similar fashion for another $d-3$ steps shows that $\det(B_1') = (-1)^d \det(B_{2d-3}')$ where

$$B_{2d-3}' = \begin{bmatrix} 0 & & & & 1 \\ & A_{d-1} & & & e_{d-1} \\ & & \ddots & & \vdots \\ & & & A_{d-1} & e_{d-1} \\ 1 & e_{d-1}^T & \cdots & e_{d-1}^T & -r \end{bmatrix}.$$

Expanding in cofactors across the top row and then the leftmost column shows that $\det(B_{2d-3}') = (-1)^{r(d-1)+1} d^{r-2}$. Thus

$$\det(-B_1') = (-1)^{r(d-1)} \det(B_1') = (-1)^{r(d-1)+d} \det(B_{2d-3}') = (-1)^{d-1} d^{r-2},$$

as desired.

(2) The matrix B'' has the form

$$\begin{bmatrix} A_{d-2} & e_{d-2} & & & & e_{d-2} \\ & & A_{d-2} & & & \\ & & e_{d-2}^T & & & 1 \\ & & & A_{d-1} & & e_{d-1} \\ & & & & \ddots & \vdots \\ & 1 & e_{d-2}^T & e_{d-1}^T & \cdots & -r \end{bmatrix}.$$

To compute the determinant, we expand in cofactors along $(d-1)^{\text{st}}$ column. There are two cofactors; the first one, corresponding the the last entry of e_{d-2}, has the matrix R_2' in the upper left corner, where R_n' is defined like R_n except we delete the *last* n rows and the last $n-1$ columns. This cofactor is zero since the corresponding

matrix visibly has less-than-maximal rank. The other term comes from the 1 in the last row, yielding

$$\det(-B'') = (-1)^{r(d-1)+1} \det \left(- \begin{bmatrix} A_{d-2} & & & & & \\ & A_{d-2} & & & & \\ & e_{d-2}^T & & & & 1 \\ & & A_{d-1} & & & e_{d-1} \\ & & & & \ddots & \vdots \\ & & & & A_{d-1} & e_{d-1} \end{bmatrix} \right).$$

Expanding in cofactors along $(2d-3)^{\text{rd}}$ row and using similar reasoning leads to

$$\det(-B'') = (-1)^{(d-1)} \det \left(- \begin{bmatrix} A_{d-2} & & & & \\ & A_{d-2} & & & \\ & & A_{d-1} & & \\ & & & \ddots & \\ & & & & A_{d-1} \end{bmatrix} \right).$$

The claim now follows by Lemma 4.3. □

The next result is useful for finding the component that a section meets at a bad fiber. To set it up, let k be a field, let $R = k[u]_{(u)}$ (localization of the polynomial ring at $u = 0$), and let $\mathcal{Z} = \operatorname{Spec} R[\alpha, \beta]/(\alpha\beta - u^n)$ where n is prime to the characteristic of k. Suppose that $\mathcal{Y} \to \operatorname{Spec} R$ is a proper relative curve and that P is a point in the special fiber of $\mathcal{Y}$ near which $\mathcal{Y}$ is étale locally isomorphic to $\mathcal{Z}$. More precisely, we assume that there is a Zariski open neighborhood U of P in $\mathcal{Y}$ and an étale R-morphism $\phi : U \to \mathcal{Z}$ sending P to the origin ($u = \alpha = \beta = 0$) in $\mathcal{Z}$. Let $f = \phi^*(\alpha)$ and $g = \phi^*(\beta)$. Let $\pi : \mathcal{X} \to \mathcal{Y}$ be the minimal regular model of $\mathcal{Y}$ and suppose that $s : \operatorname{Spec} R \to \mathcal{X}$ is a section such that $\pi \circ s$ passes through P. Let Q be the closed point of $\operatorname{Spec} R$.

LEMMA 4.6. *With the notation above:*

1. *The fiber of π over P consists of a chain of $n-1$ rational curves $Z_1, \dots, Z_{n-1}$ that can be numbered so that Z_i meets Z_j if and only if $|i-j| = 1$ and so that E_1 meets the strict transform of $f = 0$ in $\mathcal{X}$.*
2. *$s(Q)$ meets E_i if and only if $g \circ s \in R$ has $\operatorname{ord}_u(g \circ s) = i$.*
3. *g/u^i restricted to E_i induces an isomorphism $E_i \cong \mathbb{P}^1$. In particular, two sections s and s' meeting E_i intersect there if and only if $g \circ s \equiv g \circ s' \bmod u^{i+1}$.*

PROOF. Blowing up $\mathcal{Z}$ at the origin $\lfloor n/2 \rfloor$ times yields a minimal resolution $\tilde{\mathcal{Z}} \to \mathcal{Z}$ with exceptional divisor a chain of rational curves $Z_1 \cup \cdots \cup Z_{n-1}$ as in the statement, with E_1 meeting the strict transform of $\alpha = 0$. The fiber product of $\tilde{\mathcal{Z}} \to \mathcal{Z}$ with $U \to \mathcal{Z}$ is isomorphic to a neighborhood of the inverse image of P in $\mathcal{X}$, and this gives the first claim. Moreover, the other two claims are reduced to the analogous statements on $\mathcal{Z}$, and these are easily checked by considering the explicit blow-ups used to pass from $\mathcal{Z}$ to $\tilde{\mathcal{Z}}$. □

4.1.3. First global intersection numbers. We abuse notation somewhat and use P_{ij} and Q_∞ to denote the sections of $\mathcal{X} \to \mathbb{P}^1$ or $\mathcal{Y} \to \mathbb{P}^1$ induced by the K_d-rational points with those names, but we try to make clear the context in each such case.

The section P_{ij} of $\mathcal{Y} \to \mathbb{P}^1$ lies in the union of the opens $\mathcal{Z}_{12}$ and $\mathcal{Z}'_{12}$ discussed in Section 3.1.1, and it has coordinates:

$$(x_{12}, y_{12}) = \left(\zeta_d^i u, \zeta_r^j(\zeta_d^i u + 1)^{d/r}\right) \quad \text{and} \quad (x'_{12}, y'_{12}) = \left(\zeta_d^i u'^{d-1}, \zeta_r^j(\zeta_d^i + u')^{d/r}\right).$$

Since the section Q_∞ does not meet these opens, it follows that the global intersection number $P_{ij} \cdot Q_\infty = 0$ for all i and j.

Examining the coordinates above, it is clear that if $i \neq 0$, then P_{ij} and P_{00} do not meet in $\mathcal{Y}$ (and *a fortiori* in $\mathcal{X}$) except possibly over $u = 0$ or $u = \infty$. Also, if $j \neq 0$, then P_{0j} and P_{00} visibly do not meet except possibly over $u = -1$. Thus to finish the height computation it suffices to compute local intersection numbers for $u \in \{0, \mu_d, \infty\}$, the "correction factors" $D_{P_{00}} \cdot P_{ij}$ at those same places, and the self-intersections P_{00}^2 and Q_∞^2.

4.1.4. Pairings at $u = 0$. We now consider the configuration of Q_∞ and the P_{ij} with respect to the components of the special fiber of $\mathcal{X} \to \mathbb{P}^1$ over $u = 0$, which is pictured in Figure 1 in Chapter 3.

First, we note that the component labeled C_0 is the strict transform of the component $u = y_{12}^r - x_{12} - 1 = 0$ in the chart $\mathcal{Z}_{12}$ and also of the component $u = z_2 - x_2^r(x_2 + z_2) = 0$ in the chart $\mathcal{Z}_2$. The point Q_∞ extends to the section $x_2 = z_2 = 0$ in the chart $\mathcal{Z}_2$, so it lies on the component C_0.

Next, we note that the section P_{ij} of $\mathcal{Y} \to \mathbb{P}^1$ specializes to the point $x_{12} = 0$, $y_{12} = \zeta_r^i$, so the corresponding section of $\mathcal{X} \to \mathbb{P}^1$ must meet one of the components $C_{j(d-1)+k}$ with $1 \leq k \leq d-1$.

To find the component that P_{ij} meets, we use Lemma 4.6. To that end, let $f = y_{12}^r - x_{12} - 1$ and $g = x_{12}/(x_{12} + 1)$. In a neighborhood of the points $u = x_{12} = y_{12}^r - 1 = 0$, the equation defining $\mathcal{Z}_{12}$ is $fg = u^d$. We claim that near each of these points, f and g define an étale morphism to the scheme $\mathcal{Z}$ defined just before Lemma 4.6. (Here by "near" we mean in a Zariski open neighborhood U of the point of interest in the fiber product of $\mathcal{Y} \to \mathbb{P}^1$ and $\operatorname{Spec} R \to \mathbb{P}^1$.) The claim follows easily from the Jacobian criterion, as discussed for example in [**6**, Definition 3, Page 36]. Indeed, we define

$$\phi : U \to \mathbb{A}^2_{\mathcal{Z}} = \operatorname{Spec} R[\alpha, \beta, \gamma, \delta]/(\alpha\beta - u^d)$$

by $\phi^*(\alpha) = y_{12}^r - x_{12} - 1$, $\phi^*(\beta) = x_{12}/(x_{12} + 1)$, $\phi^*(\gamma) = x_{12}$, and $\phi^*(\delta) = y_{12}$. Then in the notation of [**6**], the image of ϕ is cut out by $g_1 = \alpha - \delta^r - \gamma - 1$ and $g_2 = (\gamma + 1)\beta - \gamma$, and they have independent relative differentials of $\mathbb{A}^2_{\mathcal{Z}}/\mathcal{Z}$ wherever $\beta \neq 1$ and $\delta \neq 0$, which is satisfied in a neighborhood of the points of interest.

The upshot is that the hypotheses of Lemma 4.6 are satisfied. Since $g = x_{12}/(x_{12}+1) = \zeta_d^i u/(\zeta_d^i+1)$ has $\operatorname{ord}_u(g) = 1$, it follows that P_{ij} lands on component $C_{j(d-1)+1}$. Note also that the value of g/u on P_{ij} at $u = 0$ is ζ_d^i, so the P_{ij} all land on distinct points. In other words, their local intersection multiplicity is zero.

To finish the analysis, we need to compute the local correction factor $(D_{P_{00}} \cdot P_{ij})_{u=0}$. Recall that the matrix B constructed in Lemma 4.2 is obtained by deleting the first row and column from the intersection matrix for the special fiber. Using the ordering given above for the components, then $B = B(d, d, \ldots, d)$ as in Lemma 4.4. There are r copies of A_{d-1} in B, so that B is an $m \times m$ matrix where $m = r(d-1)+1$.

First suppose that $j = 0$. Let B' be the matrix obtained by deleting the first row and column from B; a straightforward calculation shows that $B' = B(d-1, d, \ldots, d)$

as in Lemma 4.4. Therefore $\det(-B')$ is equal to

$$(d-1)d^{r-1}\left(\frac{1}{d-1}+\frac{r-1}{d}\right)=d^{r-2}(rd-r+1).$$

Since $\det(-B)=rd^{r-1}$, applying Lemma 4.2 yields that

$$(D_{P_{00}}\cdot P_{ij})_{u=0}=\det(-B')/\det(-B)=\frac{d-1}{d}+\frac{1}{rd}.$$

Next we consider the case $j\neq 0$. By symmetry, it suffices to treat the case $j=1$. Letting B' be the matrix obtained by deleting the first row and the d-th column of B, Lemma 4.5(1) implies that $\det(-B')=(-1)^{d-1}d^{r-2}$. Applying Lemma 4.2 yields that

$$(D_{P_{00}}\cdot P_{ij})_{u=0}=(-1)^{1+d}\det(-B')/\det(-B)=\frac{1}{rd}.$$

Summarizing this subsection:

PROPOSITION 4.7. *The local intersection numbers $(P_{00}\cdot P_{ij})_{u=0}$ are zero for all $(i,j)\neq(0,0)$. The local correction factor at $u=0$ is given by:*

$$(D_{P_{00}}\cdot P_{ij})_{u=0}=\begin{cases}\frac{d-1}{d}+\frac{1}{rd} & \text{if } j=0,\\ \frac{1}{rd} & \text{if } j\neq 0.\end{cases}$$

4.1.5. Pairings at $u=\infty$. The argument here is very similar to that at $u=0$. In particular, the configuration of components is again given by Figure 1 in Chapter 3 and the section of $\mathcal{X}\to\mathbb{P}^1$ corresponding to Q_∞ meets the component C_0. The section P_{ij} of $\mathcal{Y}\to\mathbb{P}^1$ specializes to the point $x'_{12}=0$, $y'_{12}=\zeta_r^{i+j}$ so the corresponding section of $\mathcal{X}\to\mathbb{P}^1$ meets component $C_{(i+j)(d-1)+k}$ for some k with $1\leq k\leq d-1$. (Here and below, we read $i+j$ modulo r and take a representative in $\{0,\dots,r-1\}$.)

Applying Lemma 4.6 with $f=y'^r_{12}-x'_{12}-1$ and $g=x'_{12}/(x'_{12}+1)$, we find that P_{ij} meets component $C_{(i+j+1)(d-1)}$ and there are no intersections among the distinct P_{ij}.

It remains to compute the correction factor $D_{P_{00}}\cdot P_{ij}$ using the lemmas in Section 4.1.2. If $i+j\equiv 0 \mod r$, then the matrix obtained by deleting row and column $d-1$ from B has the form:

$$B'=\begin{bmatrix}A_{d-2} & 0\\ 0 & B(0,d,\dots,d)\end{bmatrix}.$$

Applying Lemmas 4.3 and 4.4 shows that $\det(-B')$ is

$$(d-1)d^{r-1}\left(1+\frac{1}{d}+\cdots+\frac{1}{d}\right)=(d-1)d^{r-1}\frac{d+r-1}{d}.$$

Thus the local correction factor in this case is

$$(D_{P_{00}}\cdot P_{ij})_{u=\infty}=\det(-B')/\det(-B)=\frac{(d-1)(r+d-1)}{rd}.$$

If $i+j\not\equiv 0 \mod r$, by symmetry we may assume that $i+j\equiv 1 \mod r$. In this case, the matrix obtained by deleting row $d-1$ and column $2(d-1)$ is the matrix B'' of Lemma 4.5(2), which has $\det(-B'')=(-1)^{d-1}(d-1)^2d^{r-2}$. Thus

$$(D_{P_{00}}\cdot P_{ij})_{u=\infty}=(-1)^{d-1}\det(-B'')/\det(-B)=\frac{(d-1)^2}{rd}.$$

Summarizing this section:

PROPOSITION 4.8. *The local intersection numbers $(P_{00} \cdot P_{ij})_{u=\infty}$ are zero for all $(i,j) \neq (0,0)$. The local correction factor at $u = \infty$ is given by*

$$(D_{P_{00}} \cdot P_{ij})_{u=\infty} = \begin{cases} \frac{(d-1)(r+d-1)}{rd} & \text{if } i+j \equiv 0 \bmod r, \\ \frac{(d-1)^2}{rd} & \text{if } i+j \not\equiv 0 \bmod r. \end{cases}$$

4.1.6. Pairings at $u = \zeta_d^k$. We now focus attention on the fiber of $\mathcal{X} \to \mathbb{P}^1$ over $u = \zeta_d^k$. The configuration of components is given in Figures 2 (r odd) and 3 (r even) of Chapter 3. The component F there is the strict transform of the fiber of $\mathcal{Y} \to \mathbb{P}^1$ at $u = \zeta_d^k$, and the section Q_∞ of $\mathcal{X} \to \mathbb{P}^1$ meets this component.

In the coordinates of the chart $\mathcal{Z}_{12}$, where $P_{ij} = (\zeta_d^i u, \zeta_r^j(\zeta_d^i u + 1)^{d/r})$, the section of $\mathcal{Y} \to \mathbb{P}^1$ corresponding to P_{ij} passes through the singular point in the fiber if and only if $\zeta_d^{i+k} = -1$, or equivalently, if and only if d is even and $i+k \equiv d/2 \bmod d$. In this case, the section of $\mathcal{X} \to \mathbb{P}^1$ corresponding to P_{ij} meets one of the components D_i, E_i, or G. Since P_{ij} is a section, it has to meet a component of multiplicity one in the fiber, i.e., either D_1 or E_1. Which one it meets is a matter of labeling conventions, but we need to show that all P_{ij} with $\zeta_d^{i+k} = -1$ land on *the same* component, so we must work out a few more details.

Dropping subscripts, consider the chart $\mathcal{Z} = \mathcal{Z}_{12}$ defined by the equation $xy^r = (x+1)(x+u^d)$. Changing coordinates $x = x' - 1$ and $u = u' + \zeta_d^k$, the equation is $(x'-1)y^r = x'(x' + u'v)$ where v is a unit in the local ring at $x' = y = u' = 0$. The section P_{ij} of $\mathcal{Y} \to \mathbb{P}^1$ has coordinates

$$(x'(P), y(P)) = \left(\zeta_d^{i+k} + 1 + \zeta_d^i u', \zeta_r^j(\zeta_d^{i+k} + 1 + \zeta_d^i u')^{d/r}\right) = \left(\zeta_d^i u', \zeta_r^{i+j} u'^{d/r}\right)$$

where the second equality uses that $\zeta_d^{i+k} = -1$.

Now we blow up the origin in x', y, u' space and consider the chart with coordinates x'', y', u' where $x' = u'x''$ and $y = u'y'$. The strict transform of $\mathcal{Z}$ is defined by

$$(u'x'' - 1)u'^{r-2}y'^r = x''(x'' + v') \tag{4.1}$$

where v' is a unit near the origin. It is possible to check that v' reduces to $d\zeta_d^{k(d-1)} = \zeta_d^{-k}$ modulo the maximal ideal. The exceptional divisor is $u' = x''(x'' + \zeta_d^{-k}) = 0$, with two components that we label D_1 ($x'' = 0$) and E_1 ($x'' + \zeta_d^{-k} = 0$). Note that the original fiber of $\mathcal{Y} \to \mathbb{P}^1$ does not meet the chart under consideration. The section P_{ij} has coordinates $x''(P_{ij}) = \zeta_d^i$, $y'(P_{ij}) = \zeta_r^{i+j} u'^{d/r-1}$ and thus meets the component E_1. Moreover, when $\zeta_d^k = -1$, then P_{00} and P_{0j} intersect on E_1 with multiplicity $d/r - 1$.

Recapping the geometry, the section P_{ij} of $\mathcal{X} \to \mathbb{P}^1$ meets the component E_1 over $u = \zeta_d^k$ if and only if $\zeta_d^{i+k} = -1$, otherwise it meets F. The sections P_{00} and P_{ij} ($(i,j) \neq (0,0)$) meet over $u = \zeta_d^k$ if and only if $\zeta_d^k = -1$, $i = 0$, and $d/r > 1$, in which case their intersection multiplicity is $d/r - 1$.

It remains to compute the correction factor $D_{P_{00}} \cdot P_{ij}$. It is zero except when $\zeta_d^k = -1$ and $i = 0$, in which case both P_{00} and P_{ij} meet component E_1. The intersection matrix of the fiber omitting the component F is $B = A_{r-1}$, and B' the matrix obtained by deleting the last row and column of B is A_{r-2}. Lemma 4.2 implies that

$$D_{P_{00}} \cdot P_{0j} = \det(-B')/\det(-B) = (r-1)/r.$$

Summarizing this section:

PROPOSITION 4.9. *The local intersection numbers at $u = \zeta_d^k$ are given by*

$$(P_{00} \cdot P_{ij})_{u=\zeta_d^k} = \begin{cases} d/r - 1 & \text{if } i = 0,\ j \neq 0, \text{ and } \zeta_d^k = -1, \\ 0 & \text{if } i \neq 0 \text{ or } \zeta_d^k \neq -1. \end{cases}$$

The local correction factor at $u = \zeta_d^k$ is given by

$$(D_{P_{00}} \cdot P_{ij})_{u=\zeta_d^k} = \begin{cases} (r-1)/r & \text{if } \zeta_d^k = -1 \text{ and } i = 0, \\ 0 & \text{if } \zeta_d^k \neq -1 \text{ or } i \neq 0. \end{cases}$$

REMARK 4.10. Recall that $d = p^\nu + 1$. If p is odd, then d is even, and there is exactly one value of k modulo d, namely $d/2$, such that $\zeta_d^k = -1$. If $p = 2$, then $-1 = 1$ and $\zeta_d^k = -1$ again for exactly one value of k modulo d, namely $k = 0$. Thus for a fixed P_{ij} with $i = 0$, there is exactly one value of k such that the intersection number is non-zero and the correction factor is non-zero at $u = \zeta_d^k$.

4.1.7. Self-intersections. We now compute the self-intersections of P_{00} and Q_∞, proceeding as follows. For a point $P \in C(K_d)$, we continue to identify P with the corresponding section of $\mathcal{X} \to \mathbb{P}^1$. Let $\mathcal{I}$ be the ideal sheaf of P, considered as a divisor on $\mathcal{X}$. Recall that the conormal sheaf to P is the sheaf $\mathcal{I}/\mathcal{I}^2$ on P. By [**20**, V, 1.4.1], $P^2 = -\deg \mathcal{I}/\mathcal{I}^2$. Thus the method is to compute the divisor of a global section of this sheaf.

It is convenient to rephrase this in terms of differentials. Because P is both a smooth subvariety of $\mathcal{X}$ and a section of $\mathcal{X} \to \mathbb{P}^1$, the exact sequence

$$0 \to \mathcal{I}/\mathcal{I}^2 \to \left(\Omega^1_{\mathcal{X}}\right)_{|P} \to \Omega^1_P \to 0$$

splits canonically, and we obtain an identification $\mathcal{I}/\mathcal{I}^2 \cong (\Omega^1_{\mathcal{X}/\mathbb{P}^1})_{|P}$. In other words, $\mathcal{I}/\mathcal{I}^2$ is identified with the sheaf of relative differentials restricted to P. For typographical convenience, we write ω_P for $(\Omega^1_{\mathcal{X}/\mathbb{P}^1})_{|P}$.

Consider Q_∞. As a section of $\mathcal{Y} \to \mathbb{P}^1$, it is given by x_2 in the chart $\mathcal{Z}_2$ and x_2' in $\mathcal{Z}_2'$; these are related by $x_2' = u^{d/r} x_2$ on the overlap. It follows that dx_2 defines a global section of ω_{Q_∞} that generates it away from $u = \infty$ and has a zero of order d/r there. We conclude that $Q_\infty^2 = -d/r$ in $\mathcal{Y}$. Since $\mathcal{X} \to \mathcal{Y}$ is an isomorphism in a neighborhood of Q_∞, the same equality holds in $\mathcal{X}$.

Now consider P_{00}. In the chart $\mathcal{Z}_{12}$, which is defined (dropping subscripts) by $xy^r - (x+1)(x+u^d)$, there is an equality

$$0 = (y^r - 2x - u^d - 1)dx + rxy^{r-1}dy$$

in $\Omega^1_{\mathcal{Z}_2/\mathbb{P}^1}$. It follows that dx generates $\Omega^1_{\mathcal{Z}_2/\mathbb{P}^1}$ wherever $xy \neq 0$. In particular, restricted to P_{00}, it generates $\omega_{P_{00}}$ away from $u = 0$, $u = -1$, and $u = \infty$. We extend dx to a global section s of $\omega_{P_{00}}$ and compute its divisor.

Near $u = 0$, passing from $\mathcal{Y}$ to $\mathcal{X}$ requires several blow ups. We have already seen that after the first blow up, the strict transform of P_{00} lies in the smooth locus, so the rest of the blow ups are irrelevant for the current calculation. We make the first blow up more explicit. First, let $y = y' + 1$, so the equation defining $\mathcal{Z}_{12}$ is

$$x((y'+1)^r - 1) - x^2 - u^d - xu^d = 0.$$

Blowing up the origin, the equation becomes

$$(x'(ry'' + \cdots + u^{r-1}y''^r) - x'^2 - u^{d-2} - x'u^{d-1}$$

and the section P_{00} becomes $x' = 1$, $y' = ((u+1)^{d/r} - 1)/u$. Differentiating the equation, one checks that dx' generates ω near $u = 0$, and since $x = ux'$, it follows that dx extends to a section with a simple zero at $u = 0$.

Near $u = -1$, several blow ups are required to pass from $\mathcal{Y}$ to $\mathcal{X}$. After the first blow up, P_{00} lies in the smooth locus and the later blow ups are irrelevant for the current calculation. The relevant chart after the first blow up was given in (4.1); for reference, we copy it here:

$$(u'x'' - 1)u'^{r-2}y'^{r} = x''(x'' + v').$$

Differentiating this relation, one finds that the coefficient of dx'' is non-zero near $u' = 0, x'' = 1$, and this shows that shows that dy' generates $\omega_{P_{00}}$ there. Considering the valuation of the coefficient of dy' shows that dx'' vanishes to order $d - d/r - 1$. Since $dx = dx' = u'dx''$, it follows that dx vanishes to order $d - d/r$.

Finally, near $u = \infty$, a calculation very similar to that near $u = 0$ shows that dx has a simple pole there. In all, the divisor of dx has degree $d - d/r$ and so $P_{00}^2 = d/r - d$.

Summarizing this subsection:

PROPOSITION 4.11. *The self-intersections of P_{00} and Q_∞ are*

$$P_{00}^2 = -d + \frac{d}{r} \quad \textit{and} \quad Q_\infty^2 = -\frac{d}{r}.$$

4.1.8. Proof of Theorem 4.1. We now put all the calculations together. The local contributions to $D_{P_{00}} \cdot P_{ij}$ were computed in Propositions 4.7, 4.8, and 4.9; the results of these propositions are summarized in Table 1. In that table, all congruences are mod r. In the third column, we sum all local contributions over the places $u = \zeta_d^k$ with $k = 0, \ldots, d-1$.

(i,j)	$u = 0$	$u = \infty$	$u^d = 1$
$(0,0)$	$\frac{rd - r + 1}{rd}$	$\frac{(d-1)(r+d-1)}{rd}$	$\frac{r-1}{r}$
$i \not\equiv 0, j = 0$	$\frac{rd - r + 1}{rd}$	$\frac{(d-1)^2}{rd}$	0
$i \neq 0, i \equiv 0, j = 0$	$\frac{rd - r + 1}{rd}$	$\frac{(d-1)(r+d-1)}{rd}$	0
$i = 0, j \neq 0$	$\frac{1}{rd}$	$\frac{(d-1)^2}{rd}$	$\frac{r-1}{r}$
$i \neq 0, j \neq 0, i + j \equiv 0$	$\frac{1}{rd}$	$\frac{(d-1)(r+d-1)}{rd}$	0
$i \neq 0, j \neq 0, i + j \not\equiv 0$	$\frac{1}{rd}$	$\frac{(d-1)^2}{rd}$	0

TABLE 1. Local contributions to $D_{P_{00}} \cdot P_{ij}$

By summing the local contributions to the intersection numbers $P_{00} \cdot P_{ij}$ given in Propositions 4.7, 4.8, and 4.9, noting that $P_{ij} \cdot Q_\infty = 0$ for all i and j as in Section 4.1.3, and recalling the self-intersection numbers in the preceding subsection,

we deduce that:

$$P_{ij} \cdot P_{00} = \begin{cases} -d + \frac{d}{r} & \text{if } (i,j) = (0,0), \\ \frac{d}{r} - 1 & i = 0,\ j \neq 0, \\ 0 & \text{if } i \neq 0, \end{cases}$$
$$P_{ij} \cdot Q_\infty = 0,$$
$$Q_\infty^2 = -\frac{d}{r}.$$

Finally, recalling that

$$\langle P_{00}, P_{ij} \rangle = -P_{00} \cdot P_{ij} + P_{00} \cdot Q_\infty + P_{ij} \cdot Q_\infty - Q_\infty^2 - D_{P_{00}} \cdot P_{ij}$$

and summing the contributions above yields the theorem. □

REMARK 4.12. At this point, it would be possible to deduce from Theorem 4.1 and an elaborate exercise in row reduction that the rank of V is equal to $(r-1)(d-2)$. We take a slightly more indirect approach in the next two sections that yields more information about V, ultimately allowing us to determine V precisely as a module over the group ring $R = \mathbb{Z}[\mu_d \times \mu_r]$.

4.2. A group-theoretic pairing

Recall the group ring

$$R = \mathbb{Z}[\mu_d \times \mu_r] \cong \frac{\mathbb{Z}[\sigma, \tau]}{(\sigma^d - 1, \tau^r - 1)}$$

introduced in Section 1.2.3 of Chapter 1 and the ideal $I \subset R$ introduced in Section 1.3. In this section, we define a positive definite bilinear form on R/I and compare it with the height pairing on V via the map $R/I \to V$. This comparison plays a key role in showing that the map $R/I \to V$ is an isomorphism and thus that $J(K_d)$ has large rank.

4.2.1. A rational splitting. For notational simplicity, in this and the following subsection we write G for $\mu_d \times \mu_r$. Let $R^0 = R \otimes \mathbb{Q} = \mathbb{Q}[G]$ be the rational group ring. Because G is abelian, the regular representation of R^0 on itself breaks up into $\mathbb{Q}$-irreducibles each appearing with multiplicity one. As a result of the multiplicity condition, if I^0 is any ideal of R^0 and $\pi : R^0 \to R^0/I^0$ is the projection, then there is a unique G-equivariant splitting $\rho : R^0/I^0 \to R^0$.

We work this out explicitly in the case where I is as in Section 1.3 and $I^0 = I \otimes \mathbb{Q}$. We write

$$s_j = \sum_{i \equiv j \bmod r} \sigma^i,$$

so that

$$\sum_{i=0}^{d-1} \sigma^i \tau^{d-i} = \sum_{j=0}^{r-1} s_j \tau^{r-j}.$$

Recall that I is the ideal of R generated by

$$(\tau - 1) \sum_{i=0}^{d-1} \sigma^i, \qquad (\tau - 1) \sum_{j=0}^{r-1} s_j \tau^{r-j}, \qquad \text{and} \qquad \sum_{j=0}^{r-1} \tau^j.$$

LEMMA 4.13. *The unique G-equivariant splitting $\rho : R^0/I^0 \to R^0$ is determined by*

$$\rho(\sigma^a\tau^b) = \sigma^a\tau^b\left(1 + \frac{2}{rd}\sum_{i=0}^{d-1}\sigma^i\sum_{j=0}^{r-1}\tau^j - \frac{1}{d}\sum_{i=0}^{d-1}\sigma^i - \frac{1}{d}\sum_{j=0}^{r-1}s_j\tau^{r-j} - \frac{1}{r}\sum_{j=0}^{r-1}\tau^j\right).$$

PROOF. The formula defines a G-equivariant map $R \to R$. We have to check that it kills the ideal I^0, so that it descends to $\rho : R^0/I^0 \to R^0$, and that it is a splitting.

The fact that ρ kills I^0 follows from the following easily checked identities in R:

$$\left(\sum_{i=0}^{d-1}\sigma^i\right)^2 = d\sum_{i=0}^{d-1}\sigma^i,$$

$$\left(\sum_{i=0}^{d-1}\sigma^i\right)\left(\sum_{j=0}^{r-1}s_j\tau^{r-j}\right) = \frac{d}{r}\left(\sum_{i=0}^{d-1}\sigma^i\right)\left(\sum_{j=0}^{r-1}\tau^j\right),$$

$$\left(\sum_{j=0}^{r-1}s_j\tau^{r-j}\right)^2 = d\sum_{j=0}^{r-1}s_j\tau^{r-j},$$

$$\left(\sum_{j=0}^{r-1}\tau^j\right)^2 = r\sum_{j=0}^{r-1}\tau^j,$$

$$\left(\sum_{j=0}^{r-1}\tau^j\right)\left(\sum_{j=0}^{r-1}s_j\tau^{r-j}\right) = \left(\sum_{i=0}^{d-1}\sigma^i\right)\left(\sum_{j=0}^{r-1}\tau^j\right).$$

Using these, it is a straightforward computation to check that $\rho(I^0) = 0$.

To see that ρ is a splitting, it suffices to check that the expression in parentheses on the right hand side of Lemma 4.13 has the form $1 + \iota$ where $\iota \in I^0$. But

$$r\sum\sigma^i = (1 + \tau + \cdots + \tau^{r-1})(1 - \tau)(\sum\sigma^i) \in I$$

and

$$r\sum s_j\tau^{r-j} = (1 + \tau + \cdots + \tau^{r-1})(1 - \tau)(\sum s_j\tau^{r-j}) \in I,$$

so $\sum\sigma^i$ and $\sum s_j\tau^{r-j}$ lie in I^0. Since $\sum\tau^j$ also lies in I^0, it follows that ρ has the form $\rho(r) = r(1 + \iota)$ with $\iota \in I^0$, so $\rho : R^0/I^0 \to R^0$ is a splitting. □

4.2.2. A pairing. Now we introduce an inner product on R^0 by declaring that

$$\left\langle\sum_g a_g g, \sum_g b_g g\right\rangle_{R^0} = \sum_g a_g b_g.$$

In other words $\langle g, h\rangle_{R^0} = \delta_{gh}$. Crucially, this inner product is *positive definite*.

The splitting ρ produces an inner product on R^0/I^0 that is also positive definite. Namely, we set

$$\langle a, b\rangle_{R^0/I^0} := \langle\rho(a), \rho(b)\rangle_{R^0}.$$

The values of this pairing are determined by the following proposition and G-equivariance.

PROPOSITION 4.14. *With notation as above,*

$$\left\langle \sigma^i\tau^j, 1\right\rangle_{R^0/I^0} = \frac{1}{rd}\begin{cases} (r-1)(d-2) & \text{if } i=j=0,\\ 2-r & \text{if } i\not\equiv 0 \bmod r,\ j=0,\\ 2-2r & \text{if } i\equiv 0 \bmod r,\ i\not\equiv 0 \bmod d,\ j=0,\\ 2-d & \text{if } i=0,\ j\not\equiv 0 \bmod r,\\ 2-r & \text{if } i\not\equiv 0 \bmod r,\ i+j\equiv 0 \bmod r,\\ 2 & \text{if } i\not\equiv 0 \bmod d,\ j\not\equiv 0 \bmod r,\ i+j\not\equiv 0 \bmod r. \end{cases} \tag{4.2}$$

We leave the proof as an exercise for the reader. It is convenient for the calculation to note that if a and b are in R^0/I^0 and if $\tilde{b}$ is any lift of b to R^0, then

$$\langle \rho(a), \rho(b)\rangle_{R^0} = \langle \rho(a), \tilde{b}\rangle_{R^0}.$$

This follows from the fact that the pairing is G-equivariant, plus the fact that the irreducible subrepresentations of R appear with multiplicity one. Using this observation and G-equivariance shows that computing the pairing on R^0/I^0 amounts to reading off the coefficients of $\rho(1)$.

4.2.3. Comparison of pairings. We now compare the group-theoretic pairing of the preceding subsections to the height pairing.

More precisely, there is a well-defined map $R^0/I^0 \to J(K_d)\otimes\mathbb{Q}$ given by $r \mapsto r(P_{00})$ whose image is by definition $V\otimes\mathbb{Q}$. There is a pairing on R^0/I^0 obtained by using the map to $V\otimes\mathbb{Q}$ and the height pairing on $J(K_d)\otimes\mathbb{Q}$.

Comparing the height pairing (computed in Theorem 4.1) with the group-theoretic pairing (computed in Proposition 4.14) shows that they are the same up to a scalar: the height pairing is $(d-1)$ times the group theoretic pairing. More formally, we have shown the following.

PROPOSITION 4.15. *For all $a, b \in R$, there is an equality*

$$\langle a(P_{00}), b(P_{00})\rangle = (d-1)\,\langle a, b\rangle_{R^0/I^0}.$$

Here, the left hand pairing is the height pairing on $J_r(K_d)$.

COROLLARY 4.16. *The map $(R/I)/tor \to V/tor$ is injective and therefore an isomorphism. The rank of V is thus $(r-1)(d-2)$.*

PROOF. Proposition 4.15 shows that the pairing on $(R/I)/tor$ induced by the homomorphism $(R/I)/tor \hookrightarrow R^0/I^0 \to V\otimes\mathbb{Q}$ is positive definite. It follows immediately that the homomorphism $(R/I)/tor \to V/tor$ is injective, and it is surjective by the definition of V, so it is an isomorphism. □

4.3. Structure of the visible subgroup

In this section, we complete our analysis of V by showing that it is isomorphic to R/I as an R-module and by analyzing the torsion in R/I as an abelian group.

4.3.1. R/I as a group. We noted in Section 1.3 that I is a free $\mathbb{Z}$-module of rank $d+2(r-1)$, so R/I has rank $(r-1)(d-2)$. With more work we can compute the torsion subgroup of R/I.

PROPOSITION 4.17. *There is an isomorphism of $\mathbb{Z}$-modules*

$$R/I \cong \mathbb{Z}^{(r-1)(d-2)} \oplus T$$

where

$$T = \begin{cases} (\mathbb{Z}/r\mathbb{Z})^3 & \text{if } r \text{ is odd,} \\ \mathbb{Z}/(r/2)\mathbb{Z} \oplus \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/(2r)\mathbb{Z} & \text{if } r \text{ is even.} \end{cases}$$

Thus the torsion subgroup of R/I has order r^3.

PROOF. The plan for the proof is to choose bases of R and I as $\mathbb{Z}$-modules, use them to write down the matrix of the inclusion of $\mathbb{Z}$-modules $I \to R$, and use row operations to compute the invariant factors of this matrix.

Here is some useful notation. Let $\phi : \mathbb{Z}^r \to \mathbb{Z}^d$ be the homomorphism

$$\phi(a_1, \ldots, a_r) = (a_1, \ldots, a_r, a_1, \ldots, a_r, \ldots, a_1, \ldots, a_r).$$

In words, ϕ simply repeats its argument d/r times. Let $\psi : \mathbb{Z}^r \to \mathbb{Z}^{dr}$ be the homomorphism

$$\psi(a_1, \ldots, a_r) = (\phi(a_1, \ldots, a_r), \phi(a_2, a_3, \ldots, a_r, a_1), \ldots, \phi(a_r, a_1, \ldots, a_{r-1})).$$

In words, ψ rotates its argument r times and repeats each result d/r times. It is convenient to apply ψ to an $s \times r$ matrix, by applying it to each row, thus obtaining a map from $s \times r$ matrices to $s \times dr$ matrices. Let I_d denote the $d \times d$ identity matrix; let $\mathbf{0}_r$ denote the zero vector in $\mathbb{Z}^r$, and let $\mathbf{1}_r$ denote the vector $(1, 1, \ldots, 1) \in \mathbb{Z}^r$.

As an ordered basis of R we choose

$$1, \sigma, \ldots, \sigma^{d-1}, \tau, \sigma\tau, \ldots, \sigma^{d-1}\tau, \tau^2, \ldots, \sigma^{d-1}\tau^{r-1}.$$

As an ordered basis of I we choose

$$f_0, f_1, \ldots, f_{d-1}, d_1, \ldots, d_{r-1}, e_1, \ldots, e_{r-1},$$

defined as in Section 1.3.

With respect to these bases, the first $d+r-1$ rows of the matrix of the inclusion $I \to R$ have the form

$$\begin{array}{ccccccc} I_d & I_d & I_d & \cdots & I_d & I_d \\ \phi(-\mathbf{1}_r) & \phi(\mathbf{1}_r) & \phi(\mathbf{0}_r) & \cdots & \phi(\mathbf{0}_r) & \phi(\mathbf{0}_r) \\ \phi(\mathbf{0}_r) & \phi(-\mathbf{1}_r) & \phi(\mathbf{1}_r) & \cdots & \phi(\mathbf{0}_r) & \phi(\mathbf{0}_r) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \phi(\mathbf{0}_r) & \phi(\mathbf{0}_r) & \phi(\mathbf{0}_r) & \cdots & \phi(-\mathbf{1}_r) & \phi(\mathbf{1}_r) \end{array}.$$

The last $r-1$ rows are ψ applied to the $(r-1) \times r$ matrix:

$$\begin{pmatrix} -1 & 1 & 0 & \cdots & 0 \\ 0 & -1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & -1 & 1 \end{pmatrix}.$$

We refer to the rows by the names of the corresponding generators of I. Thus f_i for $i = 0, \dots, d-1$ refers to the first d rows, d_j for $j = 1, \dots, r-1$ refers to the next $r-1$ rows, and e_j for $j = 1, \dots, r-1$ refers to the last $r-1$ rows.

We now perform row operations on this matrix as follows. First, we replace row d_1 with

$$\sum_{j=1}^{r-1} j d_j + \sum_i f_i,$$

which has the effect of replacing row d_1 with

$$\phi(\mathbf{0}_r) \quad \phi(\mathbf{0}_r) \quad \phi(\mathbf{0}_r) \quad \cdots \quad \phi(\mathbf{0}_r) \quad \phi(r\mathbf{1}_r).$$

Next, we replace row e_1 with

$$\sum_{j=1}^{r-1} j e_j,$$

which has the effect of replacing row e_1 with

$$\psi(-1, -1, \dots, -1, r-1).$$

Now we replace row e_2 with

$$\sum_{j=2}^{r-1} \binom{j}{2} e_j,$$

which has the effect of replacing row e_2 with

$$\psi\left(0, -1, -2, \dots, -(r-2), \binom{r-1}{2}\right).$$

Now we subtract a suitable combination of the f_i rows from the last $r-1$ rows so as to make the lower left $(r-1) \times d$ block identically zero. The last $r-1$ rows $e_1, \dots, e_{r-1}$ then take the form

$$\begin{array}{llll}
\phi(0) & \phi(0, \dots, 0, r, -r) & & \phi(0, \dots, 0, r, 0, -r) \\
 & & \dots & \phi(r, 0, \dots, 0, -r) \\
\phi(0) & \phi\big(-1, -1, \dots, \tbinom{r}{2} - 1, \tfrac{-2-r(r-3)}{2}\big) & & \phi\big(-2, \dots, \tbinom{r}{2} - 2, r-2, \tfrac{-4-r(r-3)}{2}\big) \\
 & & \dots & \phi\big(1 - r + \tbinom{r}{2}, 1, \dots, 1, \tfrac{2(1-r)-r(r-3)}{2}\big) \\
\phi(0) & \phi(0, -1, 2, -1, 0 \dots, 0) & & \dots \\
\phi(0) & \phi(0, 0, -1, 2, -1, 0 \dots, 0) & & \dots \\
 & \vdots & & \\
\phi(0) & \phi(0, \dots, -1, 2, -1) & & \dots.
\end{array}$$

Now we replace row e_2 with $e_2 - \sum_{j=2}^{r-1} \binom{j}{2} d_j$, which yields

$$\begin{array}{llll}
\phi(0) & \phi(0, \dots, \tbinom{r}{2}, \tfrac{r(3-r)}{2}) & \phi(0, \dots, \tbinom{r}{2}, r, \tfrac{r(3-r)}{2}) & \dots \\
 & \phi(0, \tbinom{r}{2}, r, \dots, r, \tfrac{r(3-r)}{2}) & \phi(0, \tfrac{r(3-r)}{2}, \dots, \tfrac{r(3-r)}{2}, r(2-r)). &
\end{array}$$

We now divide into two cases according to the parity of r. If r is odd, we replace e_2 with

$$e_2 - \frac{r-1}{2} e_1 + \frac{r-1}{2} d_1,$$

which yields

$$\phi(0) \quad \phi(0,\dots,0,r) \quad \phi(0,\dots,r,r) \quad \dots \quad \phi(0,r,\dots,r).$$

Note that every entry in this vector is divisible by r. Arranging the rows in the order

$$f_0,\dots,f_{d-1},d_2,e_3,\dots,e_{r-1},e_1,e_2,d_3,\dots,d_{r-1},d_1$$

yields a matrix in row-echelon form and with the property that the leading entry of each row divides every entry to the right. Looking at the leading terms then reveals that the invariant factors are 1 repeated $d+2r-5$ times and r repeated 3 times.

Now we turn to the case when r is even. Replacing row e_2 with

$$e_2 - \frac{r}{2}e_1$$

yields

$$\phi(0) \quad \phi(0,\dots,0,-\tfrac{r}{2},\tfrac{3r}{2}) \quad \phi(0,\dots,-\tfrac{r}{2},r,\tfrac{3r}{2}) \quad \dots \quad \phi\big(-\tfrac{r^2}{2},-\tfrac{r(r-3)}{2},\dots,-\tfrac{r(r-3)}{2},-\tfrac{r(r-4)}{2}\big).$$

Note that every entry in this vector is divisible by $r/2$.

Now we replace e_1 with

$$e_1 + 2e_2 + (r-1)d_1,$$

which yields

$$\phi(0) \qquad \phi(0,\dots,0,2r) \qquad \phi(0,\dots,0,2r,2r) \qquad \dots \qquad \phi(0,2r,2r,\dots,2r).$$

Note that every entry in this vector is divisible by $2r$. Arranging the rows in the order

$$f_0,\dots,f_{d-1},d_2,e_3,\dots,e_{r-1},e_2,e_1,d_3,\dots,d_{r-1},d_1$$

yields a matrix in row-echelon form and with the property that the leading entry of each row divides every entry to the right. Looking at the leading terms then reveals that the invariant factors are 1 repeated $d+2r-5$ times and $r/2$, r, and $2r$ each appearing once.

This completes the proof of the theorem. □

We record the torsion classes provided by the proof. They are not used later in the paper, but they help explain the definition of the elements Q_2 and $Q_3 \in J(K_d)$ introduced in Section 1.4.

PROPOSITION 4.18. *If r is odd, the classes of*

$$\sum_i \sigma^i, \qquad \sum_i \sigma^i\tau^{d-i}, \quad \textit{and} \quad \sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r}\sigma^i\tau^j$$

in R/I are torsion of order r and generate a group of order r^3. If r is even, the classes of

$$\sum_i \sigma^i, \qquad \sum_{j=0}^{r-1}\sum_{k=0}^{r-1-j}\sum_{i\equiv k \bmod r}\sigma^i\tau^j, \quad \textit{and}$$
$$-\sum_{j=0}^{r-2}\sum_{i\equiv r-1-j \bmod r}\sigma^i\tau^j + \sum_{i\not\equiv 0 \bmod r}\sigma^i\tau^{r-1} + 2\sum_{j=1}^{r-1}\sum_{k=r-j}^{r-1}\sum_{i\equiv k \bmod r}\sigma^i\tau^j$$

in R/I are torsion of orders r, $2r$, and $r/2$ respectively, and they generate a group of order r^3.

PROOF. Considering the row d_1, after row reduction as above, we find that $\sum_i \sigma^i \tau^{r-1}$ is r torsion, and this element is equivalent in R/I to $\sum_i \sigma^i$.

Assume r is odd. Considering the row e_1, we see that

$$\sum_{j=1}^{r-1} \left(\sum_{i \equiv r-1-j \bmod r} \sigma^i - \sum_{i \equiv r-1 \bmod r} \sigma^i \right) \tau^j$$

is r-torsion. Adding $\sum_{i \equiv r-1 \bmod r} f_i$, one checks that this is equivalent in R/I to

$$\sum_{j=0}^{r-1} \sum_{i \equiv r-1-j \bmod r} \sigma^i \tau^j,$$

which in turn is equivalent to $\sum_i \sigma^i \tau^{d-i}$. Also, from the row e_2, we can see that

$$\sum_{j=1}^{r-1} \sum_{k=r-j}^{r-1} \sum_{i \equiv k \bmod r} \sigma^i \tau^j$$

is r-torsion. The negative of this element is equivalent in R/I to

$$\sum_{j=0}^{r-1} \sum_{k=0}^{r-1-j} \sum_{i \equiv k \bmod r} \sigma^i \tau^j.$$

Since the three r-torsion elements just exhibited are associated to distinct rows of a matrix in row-echelon form, they are independent, i.e., they generate a subgroup of order r^3. This completes the proof in the case that r is odd.

When r is even, the proof for the first class is as in the case for r odd. From the relation from row e_1, we can conclude that

$$\sum_{j=1}^{r-1} \sum_{i=r-j}^{r-1} \sum_{i \equiv k \bmod r} \sigma^i \tau^j$$

is $2r$-torsion. Since $\sum_j \tau^j = 0$ in R/I, the negative of this is equivalent to

$$\sum_{j=0}^{r-1} \sum_{k=0}^{r-1-j} \sum_{i \equiv k \bmod r} \sigma^i \tau^j.$$

Combining the relation from row e_2 with the fact that $\sum_i \sigma^i$ is r-torsion, we can check that

$$2 \sum_{\substack{1 \le j \le r-1 \\ r-j \le k \le r-1 \\ i \equiv k \bmod r}} \sigma^i \tau^j + \sum_{\substack{i \equiv r-1 \bmod r \\ 0 \le j \le r-1}} \sigma^i \tau^j + \sum_{i \not\equiv 0 \bmod r} \sigma^i \tau^{r-1} - \sum_{\substack{0 \le j \le r-2 \\ i \equiv r-1-j \bmod r}} \sigma^i \tau^j$$

is $\frac{r}{2}$-torsion. Since $\sum_j \tau^j = 0$ in R/I, the second term is zero, and the result follows as above. □

4.3.2. R/I and V. We can now finish the proof that V is isomorphic as an R-module to R/I.

THEOREM 4.19. *The projection $R/I \to V$ defined by $r \mapsto r(P_{00})$ is an isomorphism.*

PROOF. Write W for R/I. We have a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_{tor} & \longrightarrow & W & \longrightarrow & W/W_{tor} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & V_{tor} & \longrightarrow & V & \longrightarrow & V/V_{tor} & \longrightarrow & 0. \end{array}$$

By definition, the middle vertical arrow is surjective, thus so is the right vertical arrow. By Corollary 4.16, the right vertical arrow is injective, so it is an isomorphism. The snake lemma then shows that the left vertical arrow is surjective. But Proposition 4.17 shows that W_{tor} has order r^3, whereas Proposition 1.5 shows that V_{tor} has order at least r^3. It follows that the left vertical arrow is also an isomorphism. Now another application of the snake lemma shows the middle vertical arrow is an isomorphism as well, and this is our claim. □

COROLLARY 4.20. *The subgroup V of $J(K_d)$, generated by P_{00} and its conjugates under $\mathrm{Gal}(K_d/K)$, is isomorphic as a $\mathbb{Z}$-module to*

$$\mathbb{Z}^{(r-1)(d-2)} \oplus \begin{cases} (\mathbb{Z}/r\mathbb{Z})^3 & \text{if } r \text{ is odd,} \\ \mathbb{Z}/(r/2)\mathbb{Z} \oplus \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/(2r)\mathbb{Z} & \text{if } r \text{ is even.} \end{cases}$$

REMARK 4.21. It would be possible at this point to give lower bounds on the rank of J over various subfields of $\overline{\mathbb{F}}_p(t^{1/d})$, along the lines of [**52**, Corollary 4.4]. However, we delay the discussion of ranks until the end of the following chapter, where it is possible to give exact values for the rank.

4.4. Discriminants

In this section we work out the discriminant of the height pairing on V/tor. This is used in Chapter 7 to obtain information on the index of V in $J(K_d)$ and on the Tate-Shafarevich group of J/K_d.

With notation as in the previous subsection, let $W = R/I$. Recall that there is a canonical G-equivariant splitting $\rho : W \to R^0$ and a pairing on W given by $\langle a, b\rangle_{R^0/I^0} = \langle \rho(a), \rho(b)\rangle_{R^0}$ where the second pairing is the Euclidean pairing on R^0. Recall that, up to a scalar $(d-1)$, the pairing on W is the canonical height pairing on V.

Write $\det(W/tor)$ for the discriminant of this pairing on W modulo torsion and $\det(I)$ for the discriminant of the pairing on I induced by that on R.

We would like to relate these discriminants to each other. To that end, we consider a slightly more general situation: let H be an arbitrary ideal of R, and $U = R^0/H^0$. One still has a G-equivariant splitting $\varrho : U \to R^0$ and an induced pairing on U.

PROPOSITION 4.22. *With notation as above,*

$$\det(H) = \frac{|U_{tor}|^2}{\det(U/tor)}.$$

PROOF. First suppose that H is saturated, i.e., that U is torsion-free. Let $e_1, \dots, e_k$ be a $\mathbb{Z}$-basis of H and extend it to a $\mathbb{Z}$-basis $e_1, \dots, e_n$ of R. Write $\overline{e}_i$ for the image of e_i in U, so that $\overline{e}_{k+1}, \dots, \overline{e}_n$ is a $\mathbb{Z}$-basis of U. Because the pairing on R is the Euclidean pairing, the discriminant

$$|\det(\langle e_i, e_j \rangle)| = 1.$$

Now let

$$f_i = \begin{cases} e_i & \text{if } i \leq k, \\ \varrho(\overline{e}_i) & \text{if } i > k. \end{cases}$$

This is a $\mathbb{Q}$-basis of R^0. The change of basis matrix is upper triangular with 1's on the diagonal, so it has determinant 1 and

$$|\det(\langle f_i, f_j \rangle)| = |\det(\langle e_i, e_j \rangle)| = 1.$$

Now $\varrho(U)$ is orthogonal to H, so the new Gram matrix $(\langle f_i, f_j \rangle)$ is block diagonal. Its upper left $k \times k$ block is just $(\langle e_i, e_j \rangle)$ and the determinant of this block is $\pm \det(H)$. The lower right $(n-k) \times (n-k)$ block is just $(\langle \varrho(\overline{e}_i), \varrho(\overline{e}_j) \rangle)$ and the determinant of this block is $\pm \det(U) = \pm \det(U/tor)$. Thus these two discriminants are reciprocal and this proves the claim in the case when H is saturated.

For general H, let H' be the saturation, so that $|H'/H| = |U_{tor}|$ and $R/H' = U/tor$. Then

$$\det(H) = |H'/H|^2 \det(H') = |U_{tor}|^2 \det(H') = \frac{|U_{tor}|^2}{\det(U/tor)},$$

as desired. □

PROPOSITION 4.23. *We have*

$$\det(I) = r^{d+2} d^{2r-2}.$$

PROOF. It is not hard to check that the following is a $\mathbb{Z}$-basis for I:

$$\begin{aligned} \alpha_i &= \sigma^i \sum \tau^j \qquad i = 0, \dots, d-1, \\ \beta_j &= (\tau^j - 1) \sum \sigma^i \qquad j = 1, \dots, r-1, \\ \gamma_j &= (\tau^j - 1) \sum \sigma^i \tau^{d-i} \qquad j = 1, \dots, r-1. \end{aligned}$$

The values of the pairing are

$$\begin{aligned} \langle \alpha_i, \alpha_{i'} \rangle &= r\delta_{ii'}, \\ \langle \alpha_i, \beta_j \rangle &= 0, \\ \langle \alpha_i, \gamma_j \rangle &= 0, \\ \langle \beta_j, \beta_{j'} \rangle &= d(\delta_{jj'} + 1), \\ \langle \beta_j, \gamma_{j'} \rangle &= 0, \\ \langle \gamma_j, \gamma_{j'} \rangle &= d(\delta_{jj'} + 1), \end{aligned}$$

so the Gram matrix for this basis of I is block diagonal. An inductive argument shows that if A is the sum of an identity matrix of size $a \times a$ and a matrix of the same size with all entries 1, then $\det(A) = a + 1$. Thus $\det(I) = r^{d+2} d^{2r-2}$ as desired. □

COROLLARY 4.24. *If $W = R/I$, then*

$$\det(W/tor) = r^{4-d}d^{2-2r}.$$

Also

$$\det(V/tor) = (d-1)^{(r-1)(d-2)}r^{4-d}d^{2-2r}.$$

PROOF. The first claim follows from Proposition 4.17. The second follows from Theorem 4.19 and Corollary 4.24, keeping in mind the scalar $(d-1)$ relating the group-theoretic and height pairings as in Proposition 4.15. □

CHAPTER 5

The L-function and the BSD conjecture

In this chapter, we compute the Hasse-Weil L-function of the Jacobian J of C over certain extensions of $\mathbb{F}_p(t)$ and prove the conjecture of Birch and Swinnerton-Dyer for J. This leads to a combinatorial calculation of the rank of J. We use the refined BSD conjecture in Chapter 7 to relate the Tate-Shafarevich group of J to the visible subgroup V defined in Section 1.2.4.

We work in the context of general r and d in this chapter; namely, $k = \mathbb{F}_q$ is any finite field of characteristic p, d is any integer prime to p, $K = k(u)$ with $u = t^{1/d}$, r is any integer prime to p, C is the curve of genus $r-1$ over K defined as in Section 1.1 of Chapter 1, and J is the Jacobian of C. Unless stated otherwise we do not assume that r divides d nor that d divides $q-1$.

5.1. The L-function

5.1.1. Definition and first properties. We fix a prime $\ell \neq p$ and consider

$$H^1(C \times \overline{K}, \mathbb{Q}_\ell) \cong H^1(J \times \overline{K}, \mathbb{Q}_\ell)$$

as a representation of $\mathrm{Gal}(K^{sep}/K)$ where $K = \mathbb{F}_q(u)$.

The corresponding L-function $L(J/K, s) = L(C/K, s)$ is defined by the Euler product

$$L(J/K,s) = \prod_v \det\left(1 - \mathrm{Fr}_v \; q_v^{-s} \,\middle|\, H^1(J \times \overline{K}, \mathbb{Q}_\ell)^{I_v}\right)^{-1}.$$

Here v runs through the places of K, Fr_v is the (geometric) Frobenius element at v, q_v is the cardinality of the residue field at v, I_v is the inertia group at v, and $H^1(J \times \overline{K}, \mathbb{Q}_\ell)^{I_v}$ is the subspace of $H^1(J \times \overline{K}, \mathbb{Q}_\ell)$ invariant under I_v.

It is known that $L(J/K, s)$ is a rational function in q^{-s} (where $q = \#k = \#\mathbb{F}_q$). Proposition 6.31 in the next chapter shows that the K/k-trace of J vanishes. This implies that $L(J/K, s)$ is in fact a polynomial in q^{-s}.

The Grothendieck-Ogg-Shafarevich formula gives the degree of $L(J/K, s)$ as a rational function in q^{-s} (and therefore as a polynomial in our case) in terms of the conductor of the representation $H^1(J \times \overline{K}, \mathbb{Q}_\ell)$. We review this in Section 5.1.3 below.

See [**51**, Section 6.2] for more details and references about the preceding two paragraphs. We do not need to go into details about these assertions here, because we give an elementary calculation of $L(J/K, s)$ from its definition in Section 5.3 below that shows that it is a polynomial of known degree.

5.1.2. Analysis of local factors. In this subsection, we make the local factor

$$L_v := \det\left(1 - \mathrm{Fr}_v \; q_v^{-s} \,\middle|\, H^1(J \times \overline{K}, \mathbb{Q}_\ell)^{I_v}\right)$$

more explicit using the regular proper model $\mathcal{X}$ constructed in Section 3.1. Roughly speaking, the familiar fact that we may calculate the local L-factor at places of good

reduction by counting points continues to hold at all places. Some care is required because the genus is greater than 1 and the result ultimately depends on delicate properties of the Néron model.

PROPOSITION 5.1. *For a place v of $K = k(u)$, let D_v be a decomposition group at v and let $I_v \subset D_v$ be the corresponding inertia group. Let $\mathcal{X}_v$ be the fiber of $\mathcal{X} \to \mathbb{P}^1_u$ over the corresponding point of $\mathbb{P}^1_u$. Then there is a canonical isomorphism*

$$H^1(J \times \overline{K}, \mathbb{Q}_\ell)^{I_v} \cong H^1(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell)$$

that is compatible with the actions of $D_v/I_v \cong \mathrm{Gal}(\overline{k}/k)$.

PROOF. This seems to be well-known to experts, but it is hard to find an early reference. A recent preprint of Bouw and Wewers [**7**] has a nice exposition that we include here for the convenience of the reader.[1]

First, we have the standard fact that H^1 is closely connected to the Picard group: Writing V_ℓ for the Tate module, then

$$H^1(J \times \overline{K}, \mathbb{Q}_\ell) \cong V_\ell \mathrm{Pic}^0(C) \quad \text{and} \quad H^1(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell) \cong V_\ell \mathrm{Pic}^0(\mathcal{X}_v).$$

Second, let $\mathcal{J} \to \mathbb{P}^1_u$ be the Néron model of the Jacobian J, and let $\mathcal{J}^0_v$ be the connected component of the identity of the fiber at v. Then by [**41**, Lemma 2],

$$\big(V_\ell \mathrm{Pic}^0(C)\big)^{I_v} \cong V_\ell \mathcal{J}^0_v.$$

Finally, and this is the delicate point, the hypotheses of [**6**, 9.5, Theorem 4b] are satisfied and this implies that

$$\mathcal{J}^0_v \cong \mathrm{Pic}^0(\mathcal{X}_v).$$

(Roughly speaking, this result says that the Néron model represents the relative Picard functor. In order to apply it, we need to know that $\mathcal{X}$ is a regular proper model and that the gcd of the multiplicites of the components of $\mathcal{X}_v$ is one. This last point was shown directly in Section 3.1, and it also follows from the fact that C/K has a rational point so $\mathcal{X} \to \mathbb{P}^1$ has a section.)

Combining the displayed isomorphisms completes the proof. □

Next we make the connection with point counting. Write k_v for the residue field at v and $k_{v,n}$ for the extension of k_v of degree n. Then the Grothendieck-Lefschetz trace formula applied to $\mathcal{X}_v$ says:

$$|\mathcal{X}_v(k_{v,n})| = \sum_{i=0}^{2} (-1)^i \mathrm{tr}\left(\mathrm{Fr}_v^n \,|H^i(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell)\right). \tag{5.1}$$

The fibers $\mathcal{X}_v$ are connected, so $H^0(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$ with trivial Frobenius action. On the other hand, $H^2(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell)$ has dimension equal to the number of irreducible components of $\mathcal{X}_v \times \overline{k}$ and is isomorphic to $\mathbb{Q}_\ell(-1)$ tensored with a permutation representation keeping track of the action of Frobenius on the set of irreducible components. In particular, the trace of Fr_v^n on $H^2(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell)$ is equal to $c_{v,n}|k_{v,n}|$ where $c_{v,n}$ is the number of irreducible components of $\mathcal{X}_v \times \overline{k}$ that are rational over $k_{v,n}$ and $|k_{v,n}|$ is the cardinality of $k_{v,n}$. Thus, computing

[1] The main point of [**7**] is that local L-factors can be computed efficiently from semi-stable models rather than regular models, especially for superelliptic curves. This is relevant for our work, but we need the regular proper model $\mathcal{X}$ for other reasons, e.g., computing heights, so the approach of [**7**] would not in the end save us anything.

$H^1(\mathcal{X}_v \times \overline{k}, \mathbb{Q}_\ell)$ with its Frobenius action is reduced to counting points. The end result is recorded in Proposition 5.6 below once we establish the necessary notation for characters.

5.1.3. Conductors and degree of the L-function. We write c_v for the exponent of the conductor of the representation $H^1(J \times \overline{K}, \mathbb{Q}_\ell)$ at v. Since the latter is tamely ramified (by Proposition 3.5), the conductor at v is simply the codimension of $H^1(J \times \overline{K}, \mathbb{Q}_\ell)^{I_v}$ in $H^1(J \times \overline{K}, \mathbb{Q}_\ell)$. Using Proposition 5.1, c_v is the difference between the $\mathbb{Q}_\ell$-dimension of the Tate module of the generic fiber and that of the special fiber. In terms of the notation in Proposition 3.9, the dimension of the Tate module of the special fiber is $2g_v + m_v$. It follows that $c_v = 2(r-1) - 2g_v - m_v$, and using Proposition 3.9, we find that

$$c_v = \begin{cases} r-1 & \text{if } v \text{ lies over } t=0 \text{ or } t=1, \\ 2r - \gcd(d,r) - 1 & \text{if } v \text{ lies over } t=\infty, \\ 0 & \text{otherwise.} \end{cases} \tag{5.2}$$

Assuming Proposition 6.31 below, we know that the L-function is a polynomial in $T = q^{-s}$. In this case, the Grothendieck-Ogg-Shafarevich formula gives its degree as

$$\deg L(J/K, T) = -4(r-1) + \sum_v c_v = (d-1)(r-1) - (\gcd(d,r) - 1). \tag{5.3}$$

We confirm this below with a more elementary proof that avoids the forward reference to Proposition 6.31.

5.2. The conjecture of Birch and Swinnerton-Dyer for J

In this section we continue studying the arithmetic of J in the case of general r and d, so $K = k(u)$ with $u^d = t$, and k is finite of characteristic p not dividing rd. As above, let $L(J/K, s)$ be the Hasse-Weil L-function of J. We write $L^*(J/K, 1)$ for the leading coefficient in the Taylor expansion of $L(J/K, s)$ near $s = 1$. (This is defined because we know that $L(J/K, s)$ is a rational function that is regular in a neighborhood of $s = 1$.)

We let $Ш(J/K)$ be the Tate-Shafarevich group of J. This is not yet known *a priori* to be finite, but we show that it is finite in our case. We let R be the determinant of the canonical height pairing on $J(K)$ modulo torsion. (This is $(\log q)^{\operatorname{rank} J(K)}$ times the determinant of the $\mathbb{Q}$-valued pairing discussed in Chapter 4.) Finally, we let $\tau = \tau(J/K)$ be the Tamagawa number associated to J. This is defined precisely and computed explicitly in Section 7.2.

THEOREM 5.2. *The conjecture of Birch and Swinnerton-Dyer holds for J over $K = \mathbb{F}_q(t^{1/d})$. More precisely, we have*

$$\operatorname{ord}_{s=1} L(J/K, s) = \operatorname{rank} J(K),$$

and $Ш(J/K)$ is finite, and

$$L^*(J/K, 1) = \frac{|Ш(J/K)|\, R\, \tau}{|J(K)_{tor}|^2}.$$

PROOF. We saw in Section 3.3 that the surface $\mathcal{X}$ is dominated by a product of curves. This implies the Tate conjecture for $\mathcal{X}$ and therefore the BSD conjecture for J. See [**51**, Sections 8.2 and 6.3] for more details on these implications. □

REMARK 5.3. The most complete reference for the leading term part of the BSD conjecture (i.e., the second displayed equation in the Theorem) is **[22]**. The formulation in **[22]** differs slightly from that above. We compare the two formulations and show they are equivalent in Section 7.3.1 below.

5.3. Elementary calculation of the L-function

In this section we calculate the Hasse-Weil L-function of J in terms of Jacobi sums. The arguments here are quite parallel to those in Section 3 of **[10]**, so we use some of the definitions and notations of that paper, and we omit some of the details.

5.3.1. Characters and Jacobi sums. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and let $\mathcal{O}_{\overline{\mathbb{Q}}}$ be the ring of integers of $\overline{\mathbb{Q}}$. Choose a prime $\mathfrak{p} \subset \mathcal{O}_{\overline{\mathbb{Q}}}$ over p and define $\overline{\mathbb{F}}_p := \mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}$, so that $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. All finite fields in this section are considered as subfields of $\overline{\mathbb{F}}_p$. Reduction modulo p defines an isomorphism between the roots of unity with order prime to p in $\mathcal{O}_{\overline{\mathbb{Q}}}^\times$ and $\overline{\mathbb{F}}_p^\times$. The Teichmüller character $\tau : \overline{\mathbb{F}}_p^\times \to \mathcal{O}_{\overline{\mathbb{Q}}}^\times$ is the unique homomorphism that gives a right inverse to the reduction map.

Consider a multiplicative character $\chi : k^\times \to \overline{\mathbb{Q}}^\times$ for the finite field k. We employ the usual convention that $\chi(0) = 0$ if χ is non-trivial, and $\chi_{triv}(0) = 1$.

If χ_1 and χ_2 are multiplicative characters $k^\times \to \overline{\mathbb{Q}}^\times$, we define a Jacobi sum

$$J(\chi_1, \chi_2) := \sum_{u+v+1=0} \chi_1(u)\chi_2(v)$$

where the sum is over $u, v \in k$. If we need to emphasize the underlying field, we write $J_k(\chi_1, \chi_2)$.

5.3.2. Orbits and Jacobi sums. We write $\langle a \rangle$ for the fractional part of a rational number a, so that $\langle a \rangle \in [0, 1)$ and $a - \langle a \rangle \in \mathbb{Z}$. If $i \in \mathbb{Z}/n\mathbb{Z}$, and if $\tilde{\imath}$ and $\tilde{\imath}' \in \mathbb{Z}$ are representatives of i, then $\langle \tilde{\imath}/n \rangle = \langle \tilde{\imath}'/n \rangle$, so we may unambiguously define $\langle i/n \rangle$ as $\langle \tilde{\imath}/n \rangle$.

Define

$$S = \left\{ (i,j) \in \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} \;\middle|\; i \neq 0, j \neq 0, \left\langle \frac{i}{d} \right\rangle + \left\langle \frac{j}{r} \right\rangle \notin \mathbb{Z} \right\}. \tag{5.4}$$

Then $(\mathbb{Z}/\operatorname{lcm}(d,r)\mathbb{Z})^\times$ acts on S diagonally by

$$t \cdot (i,j) = (ti, jj) \quad \text{for} \quad t \in (\mathbb{Z}/\operatorname{lcm}(d,r)\mathbb{Z})^\times.$$

We write O for the set of orbits of S under the diagonal action of the cyclic subgroup of $(\mathbb{Z}/\operatorname{lcm}(d,r)\mathbb{Z})^\times$ generated by q.

If $o \in O$ is an orbit, we write $|o|$ for the cardinality of o. Define a Jacobi sum by

$$J_o = J(\chi_i, \rho_j), \tag{5.5}$$

where $(i,j) \in o$, where the sum is over $\mathbb{F}_{q^{|o|}}$, and where

$$\chi_i = \tau^{i(q^{|o|}-1)/d}, \;\; \rho_j = \tau^{j(q^{|o|}-1)/r}.$$

Well-known properties of Jacobi sums show that J_o is independent of the choice of (i,j) and that it is a Weil integer of size $q^{1/2}$.

5.3.3. The L-function in terms of Jacobi sums.

THEOREM 5.4. *With notations as above, the Hasse-Weil L-function of J/K is*

$$L(J/K,s)=\prod_{o\in O}\left(1-J_o^2q^{-|o|s}\right).$$

The proof of Theorem 5.4 is given in Section 5.3.5 after some preliminaries in the next subsection.

REMARK 5.5. Note that the degree of $L(J/K,s)$ as a polynomial in q^{-s} is the cardinality of S, namely $(d-1)(r-1)-(\gcd(d,r)-1)$. This confirms the calculation of the degree in Section 5.1.3.

5.3.4. Explicit local L-factors. We now turn to some preliminaries toward the proof of Theorem 5.4.

If β is an $\mathbb{F}_{q^n}$-rational point of $\mathbb{P}^1_u$ and v is the place of $k=\mathbb{F}_q(u)$ under β, we write a_{β,q^n} for the trace of the q^n-power Frobenius on $H^1(J\times\overline{K},\mathbb{Q}_\ell)^{I_v}$, or equivalently (by Proposition 5.1) on $H^1(\mathcal{X}_v\times\overline{k},\mathbb{Q}_\ell)$. We may compute this trace using Equation (5.1) and the remarks in the paragraph following it.

PROPOSITION 5.6. *Let $s=\gcd(r,q^n-1)$ and $\phi=\tau^{(q^n-1)/s}$. For all $\beta\in\mathbb{F}_{q^n}$, we have*

$$a_{\beta,q^n}=-\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)(\gamma+\alpha)\right)$$

where $\alpha=\beta^d$. If $\beta=\infty$, then

$$a_{\beta,q^n}=\gcd(d,s)-1=\gcd(d,r,q^n-1)-1.$$

PROOF. If $\beta\notin\{0,\mu_d,\infty\}$, then the fiber $\mathcal{X}_v$ is the smooth projective model of the affine curve $y^r=x^{r-1}(x+1)(x+\beta^d)$ with one point at infinity. A standard exercise gives the number of points as an exponential sum:

$$\begin{aligned}|\mathcal{X}_v(\mathbb{F}_{q^n})|&=1+\sum_{j=0}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)(\gamma+\alpha)\right)\\&=q^n+1+\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)(\gamma+\alpha)\right).\end{aligned}$$

Since $\mathcal{X}_v\times\overline{k}$ is irreducible, using Equation (5.1) and the remarks in the paragraph following it shows that

$$a_{\beta,q^n}=-\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)(\gamma+\alpha)\right),$$

as claimed.

If $\beta=0$, then the calculations in Section 3.1.4 (see Figure 1) show that

$$|\mathcal{X}_v(\mathbb{F}_{q^n})|=(s(d-1)+2)\,q^n+2-s.$$

On the other hand, the number $c_{v,n}$ of rational components is $s(d-1)+2$, so the trace is $s-1$. The displayed formula in the Proposition simplifies:

$$\begin{aligned}-\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)(\gamma+\alpha)\right) &= -\sum_{j=1}^{s-1}\sum_{\gamma\in(\mathbb{F}_{q^n})^\times}\phi^j(\gamma+1)\\ &= s-1,\end{aligned}$$

so the exponential sum is the trace, as desired.

If $\beta^d=1$, we consider the cases r odd (§3.1.4, Figure 2) and r even (§3.1.4, Figure 3) separately. Let F be the smooth projective model of the curve $y^r = x^{r-1}(x+1)^2$. In both cases, the number $c_{v,n}$ of irreducible components is r. When r is odd, the number of $\mathbb{F}_{q^n}$-rational points is $(r-1)q^n+|F(\mathbb{F}_{q^n})|$, and the curve F has unibranch singularities at $(0,0)$ and $(-1,0)$ and one point at infinity. We see that

$$q^n+1-a_{\beta,q^n} = |F(\mathbb{F}_{q^n})| = q^n+1+\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)^2\right),$$

and this gives the desired result. If r is even, we have

$$|\mathcal{X}_v(\mathbb{F}_{q^n})| = (r-1)q^n-1+|F(\mathbb{F}_{q^n})|,$$

and the curve F has a unibranch singularity at $(0,0)$, a singularity with two branches at $(-1,0)$, and one point at infinity. We see that

$$q^n+1-a_{\beta,q^n} = |F(\mathbb{F}_{q^n})|-1 = q^n+1+\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)^2\right)$$

and this gives the desired result.

Finally, at $\beta=\infty$ (§3.1.4, Figure 4), we have that $c_{v,n} = 2d'/d+2+\gcd(d,r,q^n-1)$ and $|\mathcal{X}_v(\mathbb{F}_{q^n})| = c_{v,n}q^n+2-\gcd(d,r,q^n-1)$, so we find that $a_{\beta,q^n} = \gcd(d,r,q^n-1)-1$, as desired.

This completes the proof of the Proposition. □

5.3.5. Proof of Theorem 5.4. The proof is very similar to that of [**10**, Theorem 3.2.1], so we omit many details. We keep the notation of Proposition 5.6.

By a standard unwinding, we have

$$\log L(J/K,T) = \sum_{n\geq 1}\frac{T^n}{n}\sum_{\beta\in\mathbb{P}^1(\mathbb{F}_{q^n})}a_{\beta,q^n} \tag{5.6}$$

where, as in the previous subsection, a_{β,q^n} is the trace of the q^n-power Frobenius on $H^1(\overline{C},\mathbb{Q}_\ell)^{I_v}$ with v the place of $K=\mathbb{F}_q(u)$ under β.

Now let $e=\gcd(d,q^n-1)$ and $\psi=\tau^{(q^n-1)/e}$. Grouping points $\beta\in\mathbb{P}^1(\mathbb{F}_{q^n})$ by their images under $\beta\mapsto\alpha=\beta^d$ and using Proposition 5.6, we have

$$\sum_{\beta\in\mathbb{P}^1(\mathbb{F}_{q^n})}a_{\beta,q^n} = a_{\infty,q^n}-\sum_{\alpha\in\mathbb{F}_{q^n}}\sum_{i=0}^{e-1}\psi^i(\alpha)\sum_{j=1}^{s-1}\sum_{\gamma\in\mathbb{F}_{q^n}}\phi^j\left(\gamma^{r-1}(\gamma+1)(\gamma+\alpha)\right).$$

Changing the order of summation and replacing α with $\alpha\gamma$, the last displayed quantity is equal to

$$a_{\infty,q^n}-\sum_{i=0}^{e-1}\sum_{j=1}^{s-1}J_{\mathbb{F}_{q^n}}(\psi^i,\phi^j)^2.$$

Note that $a_{\infty,q^n} = \gcd(e,s) - 1$; $J(\psi^0, \phi^j) = 0$ for $0 < j < s$; $J(\psi^i, \phi^j) = \pm 1$ when $0 < i < e$, $0 < j < s$; and $\langle i/e \rangle + \langle j/s \rangle \in \mathbb{Z}$. We find that

$$\sum_{\beta \in \mathbb{P}^1(\mathbb{F}_{q^n})} a_{\beta,q^n} = - \sum_{\substack{0<i<e \\ 0<j<s \\ \langle i/e \rangle + \langle j/s \rangle \notin \mathbb{Z}}} J_{\mathbb{F}_{q^n}}(\psi^i, \phi^j)^2. \tag{5.7}$$

On the other hand,

$$\log \prod_{o \in O} \left(1 - J_o^2 T^{|o|}\right) = - \sum_{n \geq 1} \frac{T^n}{n} \sum_{\substack{o \text{ such that} \\ |o| \text{ divides } n}} J_o^{2n/|o|} |o|. \tag{5.8}$$

The coefficient of T^n/n can be rewritten as

$$\sum_{\substack{(i,j) \in S \\ (q^n-1)(i,j) = (0,0)}} J_{\mathbb{F}_{q^{|o|}}} \left(\tau^{i(q^{|o|}-1)/d}, \tau^{j(q^{|o|}-1)/r}\right)^{2n/|o|}.$$

Using the Hasse-Davenport relation, we have

$$\sum_{\substack{(i,j) \in S \\ (q^n-1)(i,j) = (0,0)}} J_{\mathbb{F}_{q^n}} \left(\tau^{i(q^n-1)/d}, \tau^{j(q^n-1)/r}\right)^2 = \sum_{\substack{i \in (0,e),\ j \in (0,s) \\ \langle i/e \rangle + \langle j/s \rangle \notin \mathbb{Z}}} J_{\mathbb{F}_{q^n}} \left(\tau^{i(q^n-1)/e}, \tau^{j(q^n-1)/s}\right)^2.$$

Therefore

$$\sum_{\substack{o \text{ such that} \\ |o| \text{ divides } n}} J_o^{2n/|o|} |o| = \sum_{\substack{i \in (0,e),\ j \in (0,s) \\ \langle i/e \rangle + \langle j/s \rangle \notin \mathbb{Z}}} J_{\mathbb{F}_{q^n}} \left(\tau^{i(q^n-1)/e}, \tau^{j(q^n-1)/s}\right)^2. \tag{5.9}$$

Comparing (5.9) and (5.8) with (5.7) and (5.6) gives the desired equality. □

5.4. Ranks

We give a combinatorial formula for the rank of $J(K)$ where $K = \mathbb{F}_q(t^{1/d})$ for general d when q is sufficiently large. We also consider special values of d where we have better control on the variation of the rank with q. Recall that $K = \mathbb{F}_q(u)$ and $K_d = \mathbb{F}_p(u, \mu_d)$ where $u = t^{1/d}$.

5.4.1. The case when r divides d and $d = p^\nu + 1$.

COROLLARY 5.7. *If r divides d, $d = p^\nu + 1$, and d divides $q - 1$, then*

$$\operatorname{rank}_{\mathbb{Z}} V = \operatorname{rank}_{\mathbb{Z}} J(\mathbb{F}_q(u)) = \operatorname{ord}_{s=1} L(J/\mathbb{F}_q(u), s) = (r-1)(d-2).$$

In particular, the index of V in $J(K_d)$ is finite. Moreover, the leading term of the L-function satisfies

$$L^*(J/\mathbb{F}_q(u), 1) = (\log q)^{(r-1)(d-2)}.$$

PROOF. When $r \mid d$, then $\operatorname{ord}_{s=1} L(J/\mathbb{F}_q(u), s) \leq (r-1)(d-2)$ by the calculation of the degree of the L-function in (5.3). Note that $K_d \subset K$ since $d \mid (q-1)$. Thus we have *a priori* inequalities

$$\operatorname{rank}_{\mathbb{Z}} V \leq \operatorname{rank}_{\mathbb{Z}} J(K_d) \leq \operatorname{rank}_{\mathbb{Z}} J(K) \leq \operatorname{ord}_{s=1} L(J/K, s),$$

where the right hand inequality relies on the known part of the BSD conjecture for abelian varieties over function fields, see [**51**, Proposition 6.7] for example. We saw in Corollary 4.16 that V has rank $(r-1)(d-2)$, so the inequalities are all equalities.

For the assertion on the leading coefficient, we simply note that the equalities in the preceding paragraph show that

$$L(J/\mathbb{F}_q(u)), s) = \left(1 - q^{1-s}\right)^{(r-1)(d-2)}.$$

One then computes the leading term by taking the $(r-1)(d-2)$-th derivative. □

5.4.2. The case when r and d divide $p^\nu + 1$. We have seen that the rank of $J(K_d)$ is large when r divides d and d has the form $p^\nu + 1$. In this subsection, we show that the rank is also large over various subfields of K_d, along the lines of [**52**, Corollary 4.4]. The case of $\mathbb{F}_p(t^{1/d})$ is of particular interest.

We write $\varphi(e)$ for Euler's φ function, i.e., for the cardinality of $(\mathbb{Z}/e\mathbb{Z})^\times$. If q and e are relatively prime positive integers, let $o_q(e)$ denote the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$.

COROLLARY 5.8. *Suppose that r and d divide $p^\nu+1$ for some ν. Then the rank of J over $\mathbb{F}_q(t^{1/d})$ is equal to*

$$\sum_{\substack{e|d \\ 1<s|r}} \frac{\varphi(e)\varphi(s)}{o_q(\mathrm{lcm}(e,s))} - 2\sum_{1<s|r} \frac{\varphi(s)}{o_q(s)}.$$

In particular, for every p, and every genus $g = r-1$ with r dividing $p^\nu+1$, the rank over $\mathbb{F}_p(u)$ of Jacobians of curves of genus g is unbounded.

The conclusion in the last sentence is known for every p and every genus g by [**49**], but the ideas of this paper give a new, constructive, and relatively elementary proof.

PROOF. Choose an integer ν such that d and r divide $d' = p^\nu + 1$. Let $u^d = (u')^{d'} = t$. We have field containments $\mathbb{F}_q(u) \subset \mathbb{F}_q(\mu_{d'}, u')$ and $K_{d'} = \mathbb{F}_p(\mu_{d'}, u') \subset \mathbb{F}_q(\mu_{d'}, u')$, and an equality

$$J(\mathbb{F}_q(u)) \otimes \mathbb{Q} \cong \left(J(\mathbb{F}_q(\mu_{d'}, u')) \otimes \mathbb{Q}\right)^G$$

where $G = \mathrm{Gal}(\mathbb{F}_q(\mu_{d'}, u')/\mathbb{F}_q(u))$. To bound $\mathrm{rank}\, J(\mathbb{F}_q(u)) = \dim_{\mathbb{Q}} J(\mathbb{F}_q(u)) \otimes \mathbb{Q}$ we just need to compute the dimension of a space of invariants. Moreover, by Corollary 5.7,

$$J(\mathbb{F}_q(\mu_{d'}, u')) \otimes \mathbb{Q} = J(K_{d'}) \otimes \mathbb{Q}.$$

Thus, without loss we may replace q with $\gcd(q, |\mathbb{F}_p(\mu_{d'})|)$, so that $\mathbb{F}_q(u)$ is a subfield of $K_{d'}$.

Our task then is to compute

$$\dim_{\mathbb{Q}} \left(J(K_{d'}) \otimes \mathbb{Q}\right)^G = \dim_{\mathbb{Q}} \left(V_{d'} \otimes \mathbb{Q}\right)^G$$

where $G = \mathrm{Gal}(K_{d'}/\mathbb{F}_q(u))$ and $V_{d'} \subset J(K_{d'})$ is the explicit subgroup. We have that $V_{d'} \otimes \mathbb{Q} \cong R^0_{d'}/I^0_{d'}$ where $R^0_{d'}$ and $I^0_{d'}$ are as in Sections 1.3 and 4.2.1, with d replaced by d'.

Now G is the semi-direct product of the normal subgroup $d\mathbb{Z}/d'\mathbb{Z}$ by $\langle q \rangle$, the cyclic subgroup of $(\mathbb{Z}/d'\mathbb{Z})^\times$ generated by q. The action of d sends P_{ij} to $P_{i+d,j}$ and

the action of q sends P_{ij} to $P_{qi,qj}$. Transfering this action to $R^0_{d'}/I^0_{d'}$, and noting that

$$\left(R^0_{d'}\right)^{d\mathbb{Z}/d'\mathbb{Z}} \cong R^0_d,$$

we see that the dimension of $\left(R^0_{d'}/I^0_{d'}\right)^G$ is equal to the dimension of the Fr_q-invariants on

$$\mathbb{Q}[\mu_d \times \mu_r]/I^0_d$$

where I^0_d is the $\mathbb{Q}$-subspace of the group ring $\mathbb{Q}[\mu_d \times \mu_r] \cong \mathbb{Q}[\sigma,\tau]/(\sigma^d - 1, \tau^r - 1)$ generated by the elements

$$(\tau^j - 1)\sum \sigma^i \ (j = 1, \ldots, r-1), \qquad (\tau^j - 1)\sum \sigma^i\tau^{d-i} \ (j = 1, \ldots, r-1),$$
$$\text{and} \qquad \sigma^i \sum \tau^j \ (i = 0, \ldots, d-1),$$

as in Section 1.3.

Now both $\mathbb{Q}[\mu_d \times \mu_r]$ and I_d have bases that are permuted by Fr_q, so to compute the dimension of the space of invariants, we just need to count the number of orbits of Fr_q on the basis. One sees easily that the space of Fr_q invariants on $\mathbb{Q}[\mu_d \times \mu_r]$ has dimension

$$\sum_{\substack{e|d \\ s|r}} \frac{\varphi(e)\varphi(s)}{o_q(\mathrm{lcm}(e,s))},$$

and the space of Fr_q invariants on I^0_d has dimension

$$\sum_{e|d} \frac{\varphi(e)}{o_q(e)} + 2\sum_{1<s|r} \frac{\varphi(s)}{o_q(s)}.$$

Subtracting the last displayed quantity from the previous gives the desired dimension as stated in the Corollary.

To establish the last sentence of the statement, it suffices to note that for a fixed $q = p$ and r, the dimension computed above is unbounded as d varies through numbers of the form $p^\nu + 1$ divisible by r. Indeed, the negative terms depend only on p and r and the "main" term in the first sum is

$$\phi(p^\nu + 1)\phi(r)/o_p(p^\nu + 1) \geq \phi(p^\nu + 1)\phi(r)/(2\nu),$$

and this is clearly unbounded as ν varies. □

5.4.3. General r, d, q. Now we treat the most general case, but with slightly less control on the rank as a function of q.

Recall the set $S \subset \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ from (5.4) in Section 5.3.2. We decompose S into two disjoint pieces, $S = A \cup B$ where

$$A = \{(i,j) \in S \mid \langle i/d\rangle + \langle j/r\rangle > 1\},$$
$$B = \{(i,j) \in S \mid \langle i/d\rangle + \langle j/r\rangle < 1\}.$$

Consider $\langle p\rangle \subset (\mathbb{Z}/\mathrm{lcm}(d,r)\mathbb{Z})^\times$. We say that an element $(i,j) \in S$ is *balanced* if, for every $t \in (\mathbb{Z}/\mathrm{lcm}(d,r)\mathbb{Z})^\times$, the set $\langle p\rangle t(i,j)$ is evenly divided between A and B, i.e.,

$$|\langle p\rangle t(i,j) \cap A| = |\langle p\rangle t(i,j) \cap B|.$$

Recall that O is the set of orbits of S under $\langle q\rangle$. Note that (i,j) is balanced if and only if (qi,qj) is balanced. We say that $o \in O$ is balanced if each $(i,j) \in o$ is balanced and not balanced otherwise.

PROPOSITION 5.9. *Let $K = \mathbb{F}_q(t^{1/d})$. The order of vanishing $\mathrm{ord}_{s=1}L(J/K,s)$ (and therefore the rank of $J(K)$) is at most the number of orbits $o \in O$ that are balanced in the sense above. If $\mathbb{F}_q$ is a sufficiently large extension of $\mathbb{F}_p$ (depending only on d and r), then the rank is equal to the number of balanced orbits.*

This generalizes [**10**, Theorem 2.2] except that we have less control on how large q should be to have equality.

PROOF. We use the notations of the earlier parts of this chapter, in particular the Jacobi sums J_o from (5.5) in Section 5.3. By Theorem 5.4, the order of vanishing of $L(J/K,s)$ at $s=1$ is equal to the number of orbits $o \in O$ such that $J_o^2 = q^{|o|}$. The proposition follows from the claim that J_o is a root of unity times $q^{|o|/2}$ if and only if the orbit o is balanced. Indeed, the number of o such that $J_o^2 = q^{|o|}$ is certainly at most the number of o where J_o is a root of unity times $q^{|o|/2}$, and this gives the asserted inequality. Moreover, if we replace q with q^n, each J_o is replaced with J_o^n, so if q is a sufficiently large power of p, any J_o that is a root of unity times $q^{|o|/2}$ satisfies $J_o^2 = q^{|o|}$. Here "sufficiently large" is certainly bounded by the degree of the L-function as a polynomial in T, and this is a function only of r and d.

We finish by proving the claim that J_o is a root of unity times $q^{|o|/2}$ if and only if o is balanced. If $|o|$ is odd, then the orbit cannot be balanced and the proof below will show it is also impossible for J_o to be a root of unity times $q^{|o|/2}$. For this reason, we focus on the case that $|o|$ is even.

The argument generalizes that of [**10**, Proposition 4.1], which is the special case $r=2$. Recall the set $S \subset \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ from (5.4) and its decomposition $S = A \cup B$ as in Section 5.4.3, where

$$A = \{(i,j) \in S \mid \langle i/d\rangle + \langle j/r\rangle > 1\},\ B = \{(i,j) \in S \mid \langle i/d\rangle + \langle j/r\rangle < 1\}.$$

Given $(i,j) \in S$, let $i' = i/\gcd(d,i)$ and $j' = j/\gcd(r,j)$. Let $d' = d/\gcd(d,i)$ and $r' = r/\gcd(r,j)$. Let $e = \mathrm{lcm}(d',r')$. Recall that

$$J_o = J(\chi_i, \rho_j) = J(\tau^{i(q^{|o|}-1)/d}, \tau^{j(q^{|o|}-1)/r}).$$

Thus $J_o \in \mathbb{Q}(\mu_e)$. For $a \in (\mathbb{Z}/e\mathbb{Z})^\times$, let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_e)/\mathbb{Q})$ be the automorphism with $\sigma_a(\zeta_e) = \zeta_e^a$.

Let ν be such that $q^{|o|} = p^\nu$. Write $\mathfrak{p}$ for the prime of $\mathbb{Q}(\mu_e)$ induced by the fixed prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$. By Stickelberger's Theorem (e.g., [**9**, Thm. 3.6.6 and Prop. 2.5.14]), if the valuation of p is 1, then the valuation of J_o at the prime $\sigma_a(\mathfrak{p})$ is

$$-\nu + \sum_{\ell=0}^{\nu-1} \langle \frac{aj'p^\ell}{r'}\rangle + \langle \frac{ai'p^\ell}{d'}\rangle + \langle \frac{a(-i'r' - j'd')p^\ell}{r'd'}\rangle. \tag{5.10}$$

Since $J_o^2/q^{|o|}$ is a unit away from primes over p, it is a root of unity if and only if its valuation at every prime over p is 0. This is equivalent to the property that the quantity in (5.10) equals $\nu/2$ for each $a \in (\mathbb{Z}/e\mathbb{Z})^\times$.

Fix a and ℓ. The sum of the three fractional parts in (5.10) is either 1 or 2 since the three fractions add up to 0. The sum is 1 if and only if $\langle \frac{aj'p^\ell}{r'}\rangle + \langle \frac{ai'p^\ell}{d'}\rangle < 1$. Choose a representative $t \in \mathbb{Z}/\gcd(d,r)\mathbb{Z}$ for a and note that the fractional terms in the last inequality do not depend on this choice. Thus the sum is 1 if and only if $tp^\ell \cdot (i,j)$ is in B.

For fixed a, it follows that the quantity in (5.10) equals $\nu/2$ if and only if exactly half of the values of $\ell \in \{0,\dots,\nu-1\}$ have the property that $tp^\ell \cdot (i,j)$ is in B,

which is the definition of (i, j) being balanced. Thus the quantity in (5.10) equals $\nu/2$ for all $a \in (\mathbb{Z}/e\mathbb{Z})^\times$ if and only if o is balanced. □

Remarks 5.10.

(1) When $r = 2$, it is proved in [**52**, Proposition 4.1] that the order of vanishing is always the number of balanced orbits, i.e., there is no need to enlarge q. Numerical experiments show that this is no longer the case for $r > 2$. It would be interesting to have a sharp bound on the value of q needed to obtain the maximal rank for a given r and d.

(2) If r divides d and d divides $p^\nu + 1$, then it is easy to see that every orbit o is balanced, and the argument in [**48**, Section 8] shows that $J_o^2 = q$ for all o and any q. Thus in this case we get an exact calculation of the rank, which the reader may check agrees with Corollary 5.8.

CHAPTER 6

Analysis of $J[p]$ and $\mathrm{NS}(\mathcal{X}_d)_{\mathrm{tor}}$

In this chapter, we investigate more deeply the arithmetic and geometry of the smooth projective curve $C : y^r = x^{r-1}(x+1)(x+t)$ of genus $g = r-1$ and its Jacobian J. We prove several technical results about the minimal regular model $\mathcal{X}$ and the Néron model $\mathcal{J} \to \mathbb{P}^1$. Specifically, in Section 6.1, we analyze the Kodaira-Spencer map to show that the Jacobian J of C has no p-torsion over any separable extension of $K = \mathbb{F}_q(t)$ (see Corollary 6.1). In Section 6.2, we prove that the Néron-Severi group of $\mathcal{X}_d$ is torsion-free (see Theorem 6.13). These results will be used in Chapter 7 to understand the index of the visible subgroup V in $J(K_d)$.

6.1. Kodaira-Spencer and p-torsion

Our goal in this section is to show that the Jacobian J of C has no p-torsion over any separable extension of $K = \mathbb{F}_q(t)$, a result stated more formally as follows:

COROLLARY 6.1. *The p-torsion of J satisfies $J(K)[p] = J(K^{sep})[p] = 0$.*

To prove Corollary 6.1, we apply a result of Voloch after showing that the Kodaira-Spencer map of the Néron model $\mathcal{J} \to \mathbb{P}^1_t$ is generically an isomorphism and that J is ordinary.

6.1.1. Background on the Kodaira-Spencer map and p-torsion. Before launching into the technicalities of the proof of Corollary 6.1, we provide some background on the Kodaira-Spencer map and its connection to p-torsion of abelian varieties. This subsection is purely motivational and nothing in it will be used later in the paper. Thus the expert or impatient reader may skip directly to Subsection 6.1.2.

Consider a non-isotrivial elliptic curve E over a function field $K = \mathbb{F}_q(\mathcal{C})$ of characteristic p. It is known [**47**, Prop. I.7.3] that if $E(K)[p]$ is non-trivial, then the j-invariant of E is a p-th power, i.e., $j(E) \in K^p$. Since E is non-isotrivial, the j-invariant is non-constant, and it is a p-th power if and only if the morphism $j : \mathcal{C} \to \mathbb{P}^1$ is inseparable, if and only if its derivative vanishes identically. Passing to the contrapositive, we see that if the derivative of $j : \mathcal{C} \to \mathbb{P}^1$ does not vanish identically, then $E(K)$ has no non-trivial p-torsion. In [**57**], Voloch extends this result to higher-dimensional abelian varieties, where "derivative of j" is replaced with a suitable Kodaira-Spencer map.

Next, we give a brief overview of the Kodaira-Spencer map for a family of abelian varieties. More precisely, let B be a smooth (possibly non-projective) curve over an algebraically closed field k and let $\pi : \mathcal{A} \to B$ be an abelian scheme over B. Fix a closed point $b \in B$ and let A be the fiber $\pi^{-1}(b)$. There is an exact sequence of tangent sheaves on A:

$$0 \to T_A \to (T_{\mathcal{A}})|_A \to (\pi^*(T_B))|_A \to 0.$$

Taking cohomology, we see that $H^0(A, (\pi^*(T_B))|_A) \cong T_{B,b}$ as k-vector spaces, and the coboundary map is a homomorphism

$$T_{B,b} \to H^1(A, T_A). \tag{6.1}$$

This should be thought of as the derivative at the point b of the map from B to the moduli space of abelian varieties. Indeed, $H^1(A, T_A)$ is the space of first-order deformations of A, i.e., the tangent space to the moduli space at A, and the map (6.1) measures the variation of the family $\pi : \mathcal{A} \to B$ at the point b. (For more details, we suggest the following references: In [**26**, Ch. 4], one of the originators of the theory explains the interpretation of the H^1 and the map above in the context of complex varieties; [**56**, III.9.1] gives a compact but clear presentation of the same material; and [**20**, III.9.13.2] gives the interpretation of the H^1 in the context of schemes.)

We now reformulate (6.1). The tangent bundle to an abelian variety is trivial, so

$$H^1(A, T_A) \cong H^1(A, T_{A,0} \otimes_k \mathcal{O}_A) \cong T_{A,0} \otimes_k H^1(A, \mathcal{O}_A).$$

Thus the map (6.1) can be rewritten as an element of

$$\mathrm{Hom}_k\left(T_{B,b}, T_{A,0} \otimes_k H^1(A, \mathcal{O}_A)\right) \cong \mathrm{Hom}_k\left(\Omega^1_{A,0}, \Omega^1_{B,b} \otimes_k H^1(A, \mathcal{O}_A)\right).$$

Next, we note that $\Omega^1_{A,0}$ is canonically isomorphic to the stalk of $\pi_*\Omega^1_{\mathcal{A}/B}$ at b, and $H^1(A, \mathcal{O}_A)$ is the stalk at b of $R^1\pi_*\mathcal{O}_{\mathcal{A}}$. If we now let the point b vary, the last description of the derivative (6.1) globalizes to a morphism

$$KS : \pi_*\Omega^1_{\mathcal{A}/B} \to \Omega^1_B \otimes_{\mathcal{O}_B} R^1\pi_*\mathcal{O}_{\mathcal{A}}$$

of $\mathcal{O}_B$-modules.

Voloch's theorem then states that if the Kodaira-Spencer map KS is generically an isomorphism (i.e., an isomorphism over a dense open subset of B), then the generic fiber of $\mathcal{A}$ over B has no p-torsion points over the field $k(B)$.

In the next subsection, we restart from the beginning, defining the Kodaira-Spencer map for our context, and in the following subsections we prove that it is generically an isomorphism.

6.1.2. The Kodaira-Spencer map for $\mathcal{J}$ and $\mathcal{Y}$. In this subsection we work over $\mathbb{F}_q(u)$ where $u^d = t$ and r and d are relatively prime to p. We make no further assumptions on r, d, or q.

Let $U \subseteq \mathbb{P}^1_u$ be the open subset where $u^d \notin \{0, 1, \infty\}$. In Section 3.1.1 we constructed a proper smooth model $\pi : \mathcal{Y} \to U$ of $C/\mathbb{F}_q(u)$, i.e., a scheme with a proper smooth morphism to U whose generic fiber is C. The Néron model $\sigma : \mathcal{J} \to U$ is an abelian scheme whose fiber over a point of U is just the Jacobian of the fiber of π over that point.

Consider the sheaves of relative differentials (of 1-forms)

$$\Omega^1_U,\ \Omega^1_{\mathcal{J}},\ \Omega^1_{\mathcal{J}/U}$$

on the schemes $U/\mathbb{F}_q$, $\mathcal{J}/\mathbb{F}_q$, and $\mathcal{J}/U$ respectively (see [**27**, §6.1.2]). The following lemma, applied with $S = \mathrm{Spec}(\mathbb{F}_q)$ and $f = \sigma$, implies there is an exact sequence of locally free $\mathcal{O}_{\mathcal{J}}$-modules

$$0 \to \sigma^*\Omega^1_U \to \Omega^1_{\mathcal{J}} \to \Omega^1_{\mathcal{J}/U} \to 0 \tag{6.2}$$

since $\mathcal{J}/\mathbb{F}_q$, $U/\mathbb{F}_q$, and σ are smooth and of finite type.

LEMMA 6.2. *Let X, Y, and S be locally Noetherian schemes and let $f\colon X \to Y$ and $g\colon Y \to S$ be smooth morphisms of finite type. Then there is an exact sequence*

$$0 \to f^*\Omega^1_{Y/S} \to \Omega^1_{X/S} \to \Omega^1_{X/Y} \to 0$$

of locally free $\mathcal{O}_X$-modules.

PROOF. First, there is an exact sequence

$$f^*\Omega^1_{Y/S} \to \Omega^1_{X/S} \to \Omega^1_{X/Y} \to 0 \tag{6.3}$$

of $\mathcal{O}_X$-modules since X, Y, S are all schemes (see [**27**, 6.1.24]). We must show that the terms of this sequence are all locally free as $\mathcal{O}_X$-modules and that the first map is injective.

Let $x \in X$ be a geometric point, and let $y = f(x)$ and $s = g(y)$. Then the fibers

$$\Omega^1_{X/S,x},\ \Omega^1_{Y/S,y},\ \Omega^1_{X/Y,x}$$

are smooth of ranks

$$\dim_x X_s,\ \dim_y Y_s,\ \dim_x X_y$$

respectively, since gf, g, f are smooth (see [**27**, 6.2.5]). Hence $\Omega^1_{X/S}$ and $\Omega^1_{X/Y}$ are locally free $\mathcal{O}_X$-modules and $f^*\Omega^1_{Y/S}$ is a locally free $f^*\mathcal{O}_Y$-module (and thus a locally free $\mathcal{O}_X$-module). Finally,

$$\dim_x X_s = \dim_x X_y + \dim_y Y_s$$

so the first map of (6.3) is injective as claimed. □

Taking the direct image of (6.2) under σ and applying the projection formula (see [**27**, 5.2.32]) leads to a morphism

$$\mathrm{KS}_{\mathcal{J}} : \sigma_*\Omega^1_{\mathcal{J}/U} \to \Omega^1_U \otimes_{\mathcal{O}_U} R^1\sigma_*\mathcal{O}_{\mathcal{J}}$$

which is the "Kodaira-Spencer map" of the family $\sigma : \mathcal{J} \to U$. Similarly, Lemma 6.2 implies there is an exact sequence of $\mathcal{O}_{\mathcal{Y}}$-modules

$$0 \to \pi^*\Omega^1_U \to \Omega^1_{\mathcal{Y}} \to \Omega^1_{\mathcal{Y}/U} \to 0 \tag{6.4}$$

and a morphism

$$\mathrm{KS}_{\mathcal{Y}} : \pi_*\Omega^1_{\mathcal{Y}/U} \to \Omega^1_U \otimes_{\mathcal{O}_U} R^1\pi_*\mathcal{O}_{\mathcal{Y}}.$$

The main technical point of this section is the following.

THEOREM 6.3. *The maps $\mathrm{KS}_{\mathcal{J}}$ and $\mathrm{KS}_{\mathcal{Y}}$ are isomorphisms of locally free $\mathcal{O}_U$-modules of rank $r-1$.*

The proof is given in the remaining part of this section. The key point is to explicitly calculate the "Kodaira-Spencer pairing" on

$$H^0(U, \Omega^1_{\mathcal{Y}/U}) \times H^0(U, \Omega^1_{\mathcal{Y}/U})$$

and to show that it is non-degenerate.

Our motivation for considering the Kodaira-Spencer map $\mathrm{KS}_{\mathcal{J}}$ is that we use Theorem 6.3 to prove Corollary 6.1.

PROOF THAT THEOREM 6.3 IMPLIES COROLLARY 6.1. The statement over K follows from that over K^{sep}. The latter follows from [**57**, Page 1093, Proposition], which says that if an abelian variety over a global function field is ordinary and its Kodaira-Spencer map is generically an isomorphism, then it has no p-torsion over any separable extension. Proposition 6.12 (see Section 6.1.8) states that J is ordinary, and Theorem 6.3 states that the Kodaira-Spencer map is generically an isomorphism. □

REMARK 6.4. The proof that J has no p-torsion over K^{sep} via Kodaira-Spencer is not so simple. The ideas of [**53**, 9.4], also not so simple, yield a proof that J has no p-torsion over $\mathbb{F}_q(u)$ where $u^d = t$ and $d = p^\nu + 1$. The more straightforward idea of using p-descent (i.e., calculating the p-Selmer group and comparing with the rank) is simpler, but yields a much weaker result, namely that J has no torsion over $\mathbb{F}_q(u)$ where $u^d = t$ and $d = p^\nu + 1$ with $\nu \leq 2$. As soon as $\nu > 2$, the p-part of the Tate-Shafarevich group is non-trivial and the p-descent strategy fails.

6.1.3. Reductions to $\mathcal{Y}$. The following statement is probably well-known, but we have not found a suitable reference.

PROPOSITION 6.5. *There are isomorphisms*

$$\sigma_*\Omega^1_{\mathcal{J}/U} \cong \pi_*\Omega^1_{\mathcal{Y}/U} \quad \textit{and} \quad R^1\sigma_*\mathcal{O}_{\mathcal{J}} \cong R^1\pi_*\mathcal{O}_{\mathcal{Y}}$$

of locally free $\mathcal{O}_U$-modules of rank g such that the following diagram commutes:

$$\begin{array}{ccc} \sigma_*\Omega^1_{\mathcal{J}/U} & \xrightarrow{\mathrm{KS}_{\mathcal{J}}} & \Omega^1_U \otimes_{\mathcal{O}_U} R^1\sigma_*\mathcal{O}_{\mathcal{J}} \\ \downarrow & & \downarrow \\ \pi_*\Omega^1_{\mathcal{Y}/U} & \xrightarrow{\mathrm{KS}_{\mathcal{Y}}} & \Omega^1_U \otimes_{\mathcal{O}_U} R^1\pi_*\mathcal{O}_{\mathcal{Y}}. \end{array}$$

In particular, $\mathrm{KS}_{\mathcal{J}}$ *is an isomorphism of $\mathcal{O}_U$-modules if and only if* $\mathrm{KS}_{\mathcal{Y}}$ *is.*

PROOF. The map $\pi : \mathcal{Y} \to U$ admits a section $U \to \mathcal{Y}$ since it is proper and its generic fiber C has a rational point. The section can be used to construct a map $\mathrm{AJ} : \mathcal{Y} \to \mathcal{J}$, the so-called Abel-Jacobi map. It is a closed immersion (cf. [**31**, Proposition 2.3]), and thus AJ_* is exact. Therefore there are isomorphisms of $\mathcal{O}_U$-modules

$$R^i\sigma_*(\mathrm{AJ}_*\mathcal{O}_{\mathcal{Y}}) \cong R^i\pi_*\mathcal{O}_{\mathcal{Y}}, \quad \sigma_*(\mathrm{AJ}_*\Omega^1_{\mathcal{Y}/U}) \cong \pi_*\Omega^1_{\mathcal{Y}/U},$$

isomorphisms of $\mathcal{O}_{\mathcal{J}}$-modules

$$\mathrm{AJ}_*(\pi^*\Omega^1_U) \cong \mathrm{AJ}_*(\mathrm{AJ}^*(\sigma^*\Omega^1_U)) \cong \sigma^*\Omega^1_U \otimes_{\mathcal{O}_{\mathcal{J}}} \mathrm{AJ}_*\mathcal{O}_{\mathcal{Y}},$$

and an exact sequence of $\mathcal{O}_{\mathcal{J}}$-modules

$$0 \to \sigma^*\Omega^1_U \otimes_{\mathcal{O}_{\mathcal{J}}} \mathrm{AJ}_*\mathcal{O}_{\mathcal{Y}} \to \mathrm{AJ}_*\Omega^1_{\mathcal{Y}} \to \mathrm{AJ}_*\Omega^1_{\mathcal{Y}/U} \to 0.$$

The structure map $\mathcal{O}_{\mathcal{J}} \to \mathrm{AJ}_*\mathcal{O}_{\mathcal{Y}}$ associated to $\mathrm{AJ} : \mathcal{Y} \to \mathcal{J}$ induces a morphism $R^1\sigma_*\mathcal{O}_{\mathcal{J}} \to R^1\sigma_*\left(\mathrm{AJ}_*\mathcal{O}_{\mathcal{Y}}\right)$ and thus a morphism

$$R^1\sigma_*\mathcal{O}_{\mathcal{J}} \to R^1\pi_*\mathcal{O}_{\mathcal{Y}}.$$

Similarly, the pull-back map on 1-forms $\Omega^1_{\mathcal{J}/U} \to \mathrm{AJ}_*\Omega^1_{\mathcal{Y}/U}$ induces a morphism

$$\sigma_*\Omega^1_{\mathcal{J}/U} \to \pi_*\Omega^1_{\mathcal{Y}/U}.$$

Both displayed morphisms are isomorphisms of locally free $\mathcal{O}_U$-modules of rank g since the respective fibers at each $x \in U$ are isomorphisms of g-dimensional vector spaces (cf. [**31**, Proposition 2.1 and Proposition 2.2]).

The displayed exact sequence lies in a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \sigma^*\Omega^1_U & \longrightarrow & \Omega^1_{\mathcal{J}} & \longrightarrow & \Omega^1_{\mathcal{J}/U} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \sigma^*\Omega^1_U \otimes_{\mathcal{O}_U} \mathrm{AJ}_*\mathcal{O}_{\mathcal{Y}} & \longrightarrow & \mathrm{AJ}_*\Omega^1_{\mathcal{Y}} & \longrightarrow & \mathrm{AJ}_*\Omega^1_{\mathcal{Y}/U} & \longrightarrow & 0 \end{array}$$

of $\mathcal{O}_{\mathcal{J}}$-modules whose first row is exact and where the right two vertical maps are pull-back maps on 1-forms. Applying σ_*, the projection formula, and the isomorphisms displayed above yields a commutative diagram whose rows are long exact sequences of $\mathcal{O}_U$-modules and a portion of which is the desired diagram

$$\begin{array}{ccc} \sigma_*\Omega^1_{\mathcal{J}/U} & \longrightarrow & \Omega^1_U \otimes_{\mathcal{O}_U} R^1\sigma_*\mathcal{O}_{\mathcal{J}} \\ \downarrow & & \downarrow \\ \pi_*\Omega^1_{\mathcal{Y}/U} & \longrightarrow & \Omega^1_U \otimes_{\mathcal{O}_U} R^1\pi_*\mathcal{O}_{\mathcal{Y}}. \end{array}$$

□

6.1.4. Reduction to the Kodaira-Spencer pairing. For the rest of this section, we suppose that $d = 1$. This suffices to prove Theorem 6.3 since U is an étale cover of $\mathbb{P}^1_t \smallsetminus \{0, 1, \infty\}$.

Rather than showing that $\mathrm{KS}_{\mathcal{Y}}$ is an isomorphism directly, it is more convenient for us to consider the "Kodaira-Spencer pairing" on global 1-forms

$$\begin{array}{ccccc} H^0(U, \pi_*\Omega^1_{\mathcal{Y}/U}) \times H^0(U, \pi_*\Omega^1_{\mathcal{Y}/U}) & \longrightarrow & H^0(U, \Omega^1_U) \cong R\,dt \\ \omega_i \times \omega_j & \longmapsto & (\omega_i, \omega_j) \end{array}$$

where $R = H^0(U, \mathcal{O}_U)$. The pairing is defined by taking the cup product

$$\mathrm{KS}_{\mathcal{Y}}(\omega_i) \cup \omega_j \in H^0(U, \Omega^1_U \otimes_{\mathcal{O}_U} R^1\pi_*\Omega^1_{\mathcal{Y}/U})$$

followed by the map

$$H^0(U, \Omega^1_U \otimes_{\mathcal{O}_U} R^1\pi_*\Omega^1_{\mathcal{Y}/U}) \quad \tilde{\to} \quad H^0(U, \Omega^1_U \otimes_{\mathcal{O}_U} \mathcal{O}_U) \cong H^0(U, \Omega^1_U)$$

induced by the relative trace

$$R^1\pi_*\Omega^1_{\mathcal{Y}/U} \quad \tilde{\to} \quad \mathcal{O}_U.$$

In particular, to show that $\mathrm{KS}_{\mathcal{Y}}$ is an isomorphism is the same as to show that the Kodaira-Spencer pairing is a perfect pairing of free R-modules. Proposition 6.5 then implies that $\mathrm{KS}_{\mathcal{J}}$ is an isomorphism, completing the proof of Theorem 6.3.

After some preparatory material, a proof that the pairing is perfect is given in Section 6.1.7.

6.1.5. Relative 1-forms. Recall that $d = 1$ and thus $R = H^0(U, \mathcal{O}_U) = \mathbb{F}_q[t][1/(t(t-1))]$. Recall also that C is the smooth proper curve over K associated to the affine curve $y^r = x^{r-1}(x+1)(x+t)$, that $\mathcal{Y} \to U$ is a proper smooth map with generic fiber C, and that $\mathcal{Y}$ is covered by the sets

$$\begin{aligned}
\mathcal{Y}_1 &:= \mathrm{Spec}\left(R[x_{11}, y_{11}]/(y_{11} - x_{11}^{r-1}(x_{11}y_{11}+1)(x_{11}y_{11}+t))\right), \\
\mathcal{Y}_2 &:= \mathrm{Spec}\left(R[x_2, z_2]/(z_2 - x_2^{r-1}(x_2+z_2)(x_2+tz_2))\right), \\
\mathcal{Y}_3 &:= \mathrm{Spec}\left(R[y_3, z_3]/(y_3^r z_3 - (1+z_3)(1+tz_3))\right)
\end{aligned}$$

(cf. Section 3.1.1). These coordinates are related by the identities

$$(x, y) = (x_{11}y_{11}, y_{11}) = (x_2/z_2, 1/z_2) = (1/z_3, y_3/z_3).$$

For $1 \le i \le r-1$, the expression $x^{i-1}dx/y^i$ corresponds to a unique meromorphic 1-form ω_i on $\mathcal{Y}$. The restrictions of ω_i to the open sets $\mathcal{Y}_1$, $\mathcal{Y}_2$, $\mathcal{Y}_3$ are

$$\frac{x_{11}^i dy_{11}}{y_{11}} + x_{11}^{i-1}dx_{11}, \quad x_2^i\left(\frac{dx_2}{x_2} - \frac{dz_2}{z_2}\right), \quad -\frac{dz_3}{y_3^i z_3}$$

respectively. These are clearly non-zero forms.

LEMMA 6.6. *ω_i is everywhere regular, i.e., is an element of $H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U})$.*

PROOF. On the one hand, ω_i is clearly regular on $\mathcal{Y}_1$ away from $y_{11} = 0$. On the other hand, if $y_{11} = 0$, then dy_{11}/y_{11} has a pole of order one and x_{11}^i vanishes to order i, so ω_i is regular on $\mathcal{Y}_1$. For use just below, we record that ω_i vanishes to order exactly $i-1$ along the divisor $x_{11} = 0$.

Similarly, if x_2 or z_2 vanish, then both vanish and ω_i is regular on $\mathcal{Y}_2$.

Finally, z_3 never vanishes, and if $y_3 = 0$, then the identity

$$ry_3^{r-1}z_3dy_3 + (y_3^r - (1+tz_3) - t(1+z_3))dz_3 = 0$$

on $\mathcal{Y}_3$ shows that dz_3 has a zero of order at least $r-1$. More precisely, the coefficient of dz_3 is a unit in a neighborhood of $y_3 = 0$ while the coefficient of dy_3 has a zero of order at least $r-1$. Hence ω_i is regular on $\mathcal{Y}_3$. □

LEMMA 6.7. *The relative 1-forms ω_i form an R-basis of $H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U})$.*

PROOF. There is an isomorphism $H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U}) \cong H^0(U, \pi_*\Omega^1_{\mathcal{Y}/U})$. Since π is a family of smooth projective curves of genus $g = r-1$, the sheaf $\pi_*\Omega^1_{\mathcal{Y}/U}$ is a locally free sheaf of $\mathcal{O}_U$-modules of rank $r-1$ whose fiber at a closed point $u \in U$ is $H^0(\pi^{-1}(u), \Omega^1_{\pi^{-1}(u)/\kappa(u)})$. This last is a vector space of dimension $r-1$ over the residue field $\kappa(u)$, and to prove the lemma it suffices to show that the images of the ω_i in $H^0(\pi^{-1}(u), \Omega^1_{\pi^{-1}(u)/\kappa(u)})$ form a $\kappa(u)$ basis for all $u \in U$. But, as mentioned above, ω_i has a zero of order $i-1$ at the point $x_{11} = y_{11} = 0$ in each fiber, so the restrictions of the ω_i to the fibers are linearly independent. Since there are $r-1$ of them, they form a basis. □

Let $\overline{C} = C \times_K \overline{K}$.

COROLLARY 6.8. *The relative 1-forms $\omega_1, \ldots, \omega_{r-1}$ form a K-basis of $H^0(C, \Omega^1_{C/K})$ and a $\overline{K}$-basis of $H^0(\overline{C}, \Omega^1_{\overline{C}/\overline{K}})$.*

PROOF. This is immediate from Lemma 6.7 since

$$H^0(C, \Omega^1_{C/K}) \cong H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U}) \otimes_R K$$

and

$$H^0(C, \Omega^1_{\overline{C}/\overline{K}}) \cong H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U}) \otimes_R \overline{K}.$$

□

6.1.6. Lifting 1-forms. Recall that there is an exact sequence of $\mathcal{O}_{\mathcal{Y}}$-modules

$$0 \to \pi^*\Omega^1_U \to \Omega^1_{\mathcal{Y}} \to \Omega^1_{\mathcal{Y}/U} \to 0$$

and that $\mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$ is an open affine cover of $\mathcal{Y} \to U$. In this subsection, we regard ω_i as a section in $H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U})$ and find, for each $j = 1, 2, 3$, a lift of ω_i to a section in $H^0(\mathcal{Y}_j, \Omega^1_{\mathcal{Y}})$ so that we can calculate $\mathrm{KS}_{\mathcal{Y}}(\omega_i)$.

PROPOSITION 6.9. *The 1-forms*

$$\frac{x_{11}^i dy_{11}}{y_{11}} + x_{11}^{i-1} dx_{11}, \quad x_2^i \left(\frac{dx_2}{x_2} - \frac{dz_2}{z_2} \right), \quad -\frac{dz_3}{y_3^i z_3} - \frac{1 + z_3}{y_3^i} \frac{dt}{t-1}.$$

are sections in $H^0(\mathcal{Y}_j, \Omega^1_{\mathcal{Y}})$ for $j = 1, 2, 3$ respectively, and each lifts ω_i.

The proof occupies the remainder of this subsection.

First consider $\mathcal{Y}_1$, where (dropping subscripts) there is an equality

$$0 = y - x^{r-1}(xy + 1)(xy + t), \tag{6.5}$$

the differential of which leads to the relation

$$\begin{aligned} 0 = {} & (1 - x^r(xy + t) - x^r(xy + 1))\, dy - x^{r-1}(xy + 1)\, dt \\ & - x^{r-2}\left((r-1)(xy + 1)(xy + t) + xy(xy + t) + (xy + 1)xy\right) dx. \end{aligned} \tag{6.6}$$

Now consider the naive lift of ω_i to a 1-form on $\mathcal{Y}_1$

$$\frac{x^{i-1} d(xy)}{y} = \frac{x^i dy}{y} + x^{i-1} dx.$$

This is obviously regular away from $y = 0$. The equality (6.5) shows that, in an open neighborhood of $y = 0$, the function y is a unit times x^{r-1}. Also, the coefficients of dx and dt in (6.6) are divisible by x^{r-2} and, near $y = 0$, the coefficient of dy is a unit. Therefore, we may rewrite $x^i dy$ (with $i \geq 1$) as a regular 1-form times x^{r-1}, and thus $x^i dy/y$ is everywhere regular on $\mathcal{Y}_1$. This shows that the naive lift of ω_i is a section in $H^0(\mathcal{Y}_1, \Omega^1_{\mathcal{Y}})$.

Next we turn to $\mathcal{Y}_2$, where (dropping subscripts) there is an equality

$$0 = z - x^{r-1}(x + z)(x + zt), \tag{6.7}$$

the differential of which leads to the relation

$$\begin{aligned} 0 = {} & \big(1 - x^{r-1}(x + zt) - x^{r-1}(x + z)t\big)\, dz - x^{r-1}(x + z)z\, dt \\ & - x^{r-2}\left((r-1)(x + z)(x + zt) + x(x + zt) + x(x + z)\right) dx. \end{aligned} \tag{6.8}$$

Now consider the naive lift of ω_i to a 1-form on $\mathcal{Y}_2$:

$$\frac{x^{i-1} d(x/z)}{1/z} = x^i \left(\frac{dx}{x} - \frac{dz}{z} \right).$$

This is obviously regular away from $z = 0$. Near $z = 0$, the equality (6.7) shows that z is a unit times x^{r+1}. Also, near $z = 0$, the coefficient of dz in (6.8) is a unit

and the coefficients of dx and dt are divisible by x^r. Therefore, we may rewrite $x^i dz$ (with $i \geq 1$) as a regular 1-form times x^{r+1}, and thus $x^i dz/z$ is everywhere regular on $\mathcal{Y}_2$. This shows that the naive lift of ω_i is a section in $H^0(\mathcal{Y}_2, \Omega^1_{\mathcal{Y}})$.

Finally, we turn to $\mathcal{Y}_3$, where (dropping subscripts) there is an equality

$$0 = y^r z - (1+z)(1+tz), \tag{6.9}$$

the differential of which leads to the relation

$$0 = \left(ry^{r-1}z\right) dy + (y^r - (1+tz) - (1+z)t)\, dz - ((1+z)z)\, dt. \tag{6.10}$$

This time it is necessary to work harder since the naive lift of ω_i turns out not to be regular on all of $\mathcal{Y}_3$. Instead of it, we add a term involving dt and consider

$$\frac{-dz}{y^i z} - \frac{1+z}{y^i}\frac{dt}{t-1}.$$

This is regular where $y \neq 0$ since $t-1$ and z are units on all of $\mathcal{Y}_3$, so it remains to show it is regular in a neighborhood of $y = 0$. The equations (6.9) and (6.10) and some algebra allow us to rewrite this lift as

$$\frac{ry^{r-i-1}}{f}\, dy - \frac{1+z}{y^i}\left(\frac{1}{f} + \frac{1}{t-1}\right) dt = \frac{y^{r-1-i}}{f}\left(r\, dy + \frac{y(z-1)}{t-1}\, dt\right)$$

where $f = y^r - (1+tz) - (1+z)t$. The right side is regular in a neighborhood of $y = 0$ since then $t-1$ and f are units. Therefore this lift of ω_i is a section in $H^0(\mathcal{Y}_3, \Omega^1_{\mathcal{Y}})$.

6.1.7. Computing the Kodaira-Spencer pairing. In this section we calculate the pairing

$$\begin{array}{ccc} H^0(U, \pi_*\Omega^1_{\mathcal{Y}/U}) \times H^0(U, \pi_*\Omega^1_{\mathcal{Y}/U}) & \to & H^0(U, \Omega^1_U) \\ \omega_i \times \omega_j & \mapsto & (\omega_i, \omega_j). \end{array}$$

The proof of the following proposition occupies the remainder of this subsection:

PROPOSITION 6.10. *$(\omega_i, \omega_j) = \frac{r\, dt}{t(t-1)}$ if $i + j = r$, and otherwise $(\omega_i, \omega_j) = 0$.*

In particular, Proposition 6.10 and Corollary 6.7 together imply that the pairing is a perfect pairing of free R-modules since $r/t(t-1)$ is a unit in R.

Recall that $H^i(\mathcal{Y}, \mathcal{F}) \cong H^0(U, R^i\pi_*\mathcal{F})$ for any coherent sheaf $\mathcal{F}$ on $\mathcal{Y}$ since U is affine. Recall also that there is a long exact sequence of $\mathcal{O}_U$-modules

$$\cdots \to R^i\pi_*\pi^*\Omega^1_U \to R^i\pi_*\Omega^1_{\mathcal{Y}} \to R^i\pi_*\Omega^1_{\mathcal{Y}/U} \to \cdots$$

obtained by applying π_* and its right derived functors to (6.4). Therefore the corresponding sequence of global sections

$$\cdots \to H^0(U, R^i\pi_*\pi^*\Omega^1_U) \to H^0(U, R^i\pi_*\Omega^1_{\mathcal{Y}}) \to H^0(U, R^i\pi_*\Omega^1_{\mathcal{Y}/U}) \to \cdots$$

is equal to the long exact cohomology sequence

$$\cdots \to H^i(\mathcal{Y}, \pi^*\Omega^1_U) \to H^i(\mathcal{Y}, \Omega^1_{\mathcal{Y}}) \to H^i(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U}) \to \cdots.$$

In particular, $\mathrm{KS}_{\mathcal{Y}}$ induces a map

$$H^0(U, \pi_*\Omega^1_{\mathcal{Y}/U}) \to H^1(U, R^1\pi_*\pi^*\Omega^1_U),$$

which is the boundary map of cohomology

$$H^0(\mathcal{Y}, \Omega^1_{\mathcal{Y}/U}) \to H^1(\mathcal{Y}, \pi^*\Omega^1_U).$$

Fixing i and taking differences, on $\mathcal{Y}_j \cap \mathcal{Y}_k$, for $j,k \in \{1,2,3\}$, of the lifts in Proposition 6.9 yields the following Čech cocycle in $H^1(\mathcal{Y}, \pi^*\Omega^1_U)$ representing $\mathrm{KS}_{\mathcal{Y}}(\omega_i)$:

$$g_{12} = g_{21} = 0, \qquad g_{23} = -g_{32} = g_{13} = -g_{31} = \frac{1+z_3}{y_3^i}\frac{dt}{t-1}$$

where g_{jk} is a section in $H^0(\mathcal{Y}_j \cap \mathcal{Y}_k, \pi^*\Omega^1_U)$.

Taking the cup product of $\mathrm{KS}_{\mathcal{Y}}(\omega_i)$ with ω_j yields a class in

$$\begin{aligned} H^1(\mathcal{Y}, \pi^*\Omega^1_U \otimes_{\mathcal{O}_Y} \Omega^1_{\mathcal{Y}/U}) &\cong H^0(U, \Omega^1_U \otimes_{\mathcal{O}_U} R^1\pi_*\Omega^1_{\mathcal{Y}/U}) \\ &\cong H^0(U, \Omega^1_U) \otimes_R H^0(U, R^1\pi_*\Omega^1_{\mathcal{Y}/U}) \end{aligned}$$

given by the product of $\frac{dt}{t-1}$ and the class h in $H^0(U, R^1\pi_*\Omega^1_{\mathcal{Y}/U})$ represented by the Čech cocycle

$$h_{12} = h_{21} = 0, \qquad h_{23} = -h_{32} = h_{13} = -h_{31} = \frac{1+z_3}{y_3^{i+j}}\frac{dz_3}{z_3}.$$

It remains to calculate the image of h via the relative trace map

$$H^0(U, R^1\pi_*\Omega^1_{\mathcal{Y}/U}) \to H^0(U, \mathcal{O}_U).$$

Consider, for $j = 1,2,3$, the *meromorphic* relative 1-forms σ_j on $\mathcal{Y}_j$ given by

$$\sigma_1 = \sigma_2 = 0, \qquad \sigma_3 = -\frac{1+z_3}{y_3^{i+j}}\frac{dz_3}{z_3}.$$

On $\mathcal{Y}_j \cap \mathcal{Y}_k$, they satisfy $h_{jk} = \sigma_j - \sigma_k$. Therefore, for $z \in U$ and $P \in \mathcal{Y}_{j,z}$, the residue $r_P = \mathrm{Res}_P(\sigma_j)$ satisfies $r_P = \mathrm{Res}_P(\sigma_k)$ if $P \in \mathcal{Y}_{k,z}$. In particular, the relative trace of h is the global section of $\mathcal{O}_U$ whose restriction to $\mathcal{O}_{U,z}$ is $\sum_{P\in\mathcal{Y}_z} r_P$.

It is clear that $r_P = 0$ except possibly at the points $(y_3, z_3) = (0,-1)$ and $(0,-1/t)$ in $\mathcal{Y}_{3,z}$. The identities

$$y_3^r z_3 - (1+z_3)(1+tz_3) = 0 \quad \text{and} \quad r y_3^{r-1} z_3\, dy_3 = (y_3^r - (1+tz_3) - t(1+z_3))\, dz_3$$

allow us to rewrite σ_3 as

$$-\frac{r z_3(1+z_3)}{1-z_3^2 t}\frac{dy_3}{y_3^{1+i+j-r}} = -\frac{r z_3^2}{(1+tz_3)(1-z_3^2 t)}\frac{dy_3}{y_3^{1+i+j-2r}}.$$

The specializations of the left and right at $z_3 = -1/t$ and $z_3 = -1$ are

$$-\frac{r(-1/t)(1+(-1/t))}{1-(1/t^2)t}\frac{dy_3}{y_3^{1+i+j-r}} = \frac{r}{t}\frac{dy_3}{y_3^{1+i+j-r}}$$

and

$$-\frac{r}{(1-t)(1-t)}\frac{dy_3}{y_3^{1+i+j-2r}}$$

respectively. In particular, if $P \in \mathcal{Y}_3$, then

$$r_P = \begin{cases} \frac{r}{t} & \text{if } P = (0,-1/t) \text{ and } i+j = r, \\ 0 & \text{otherwise,} \end{cases}$$

since $1+i+j-2r \le -2$. Therefore

$$(\omega_i, \omega_j) = \begin{cases} \frac{dt}{t-1}\frac{r}{t} & \text{if } i+j = r, \\ 0 & \text{otherwise,} \end{cases}$$

as claimed.

REMARK 6.11. Variants of this calculation for $r = 2$, i.e., for the Legendre curve, go back to the origins of hypergeometric functions and appear in many places in the literature, sometimes lifted to the level of the Gauss-Manin connection, and with varying conventions, bases, and signs.

6.1.8. J is ordinary. We recall that "J is ordinary" means that $J(\overline{K})[p]$ has cardinality p^g where $g = r - 1$ is the dimension of J. This property is obviously preserved under change of ground field.

Recall (e.g., [**37**, Section 2]) that the Cartier operator

$$\mathrm{Car} : H^0(\overline{C}, \Omega^1_{\overline{C}/\overline{K}}) \to H^0(\overline{C}, \Omega^1_{\overline{C}/\overline{K}})$$

is a semi-linear operator satisfying

$$\mathrm{Car}(\omega + \omega') = \mathrm{Car}(\omega) + \mathrm{Car}(\omega') \text{ and } \mathrm{Car}(f^p\omega) = f\,\mathrm{Car}(\omega)$$

for all f in the function field $\overline{K}(\overline{C})$. Also, for $x \in \overline{K}(\overline{C})$,

$$\mathrm{Car}\left(\frac{x^i dx}{x}\right) = 0 \text{ if } p \nmid i \text{ and } \mathrm{Car}\left(\frac{dx}{x}\right) = \frac{dx}{x}.$$

It is known that J being ordinary is equivalent to the Cartier operator of C being an isomorphism. (This can be deduced from [**37**, Proposition 10, page 41].)

PROPOSITION 6.12. *The operator* $\mathrm{Car} : H^0(\overline{C}, \Omega^1_{\overline{C}/\overline{K}}) \to H^0(\overline{C}, \Omega^1_{\overline{C}/\overline{K}})$ *is an isomorphism. In particular, the Jacobian J of C is ordinary.*

PROOF. Corollary 6.8 says that $\omega_1, \ldots, \omega_{r-1}$ form a K-basis of $H^0(\overline{C}, \Omega^1_{\overline{C}/\overline{K}})$. We show, for all $1 \le i \le r-1$, that $\mathrm{Car}(\omega_i)$ is a non-zero multiple of ω_a where $pa \equiv i \mod r$. This implies that Car is an isomorphism, as required.

Since $p \nmid r$, given i with $1 \le i \le r-1$, we may solve $ap - br = i$ in integers a, b. Moreover, adjusting a, b by mr, mp, for some m, we may assume that $0 \le b < p$, and having done this, it follows that $0 < a < r$. We then have

$$\omega_i = \left(\frac{x}{y}\right)^i \frac{dx}{x} = \frac{x^i y^{br}}{y^{ap}} \frac{dx}{x} = \frac{h(x)}{y^{ap}} \frac{dx}{x}$$

where $h(x) = x^{i+(r-1)b}(x+1)^b(x+t)^b$. Thus

$$\mathrm{Car}(\omega_i) = y^{-a}\,\mathrm{Car}\left(h(x)\frac{dx}{x}\right).$$

Now the exponents of x appearing in h are in the range

$$[i + (r-1)b, i + (r+1)b] = [ap - b, ap + b],$$

and the only multiple of p in this range is ap. Letting c be the coefficient of x^{ap} in $h(x)$, then $\mathrm{Car}(h(x)dx/x) = c^{1/p}x^a\,dx/x$ and

$$\mathrm{Car}(\omega_i) = c^{1/p}(x/y)^a dx/x = c^{1/p}\omega_a.$$

Thus it remains to prove that $c \neq 0$.

It is clear that c is the coefficient of x^b in $(x+1)^b(x+t)^b$, and so

$$c = \sum_{j=0}^{b} \binom{b}{j}^2 t^j = 1 + b^2 t + \cdots + b^2 t^{b-1} + t^b.$$

Since t is transcendental over $\mathbb{F}_p$, this expression is not zero in $\overline{K}$, and this completes the proof. □

6.2. Néron-Severi of $\mathcal{X}_d$ is torsion-free

In this section, we assume that k is a perfect field of characteristic $p \geq 0$ not dividing d and containing μ_d and that r divides d. Let $\mathcal{X}_d \to \mathbb{P}^1_u$ be the minimal regular model of C/K_d constructed in Section 3.1. We regard $\mathcal{X}_d$ as a surface over k. Our aim in this section is to prove the following result.

THEOREM 6.13. *The Néron-Severi group of $\mathcal{X}_d$ is torsion-free.*

Along the way we work in more generality so that the same result may be deduced for most surfaces related to the Berger construction. It would be possible to remove the restrictions that r divides d and that k contains μ_d, but we leave this as an exercise for the reader.

We occasionally refer to the Néron-Severi and Picard groups of certain singular surfaces. We recall here three familiar facts that continue to hold for singular but normal surfaces. Namely, if $\mathcal{S}$ is a projective, normal, geometrically irreducible surface over a perfect field k, then the Picard functor $\mathrm{Pic}_{\mathcal{S}/k}$ is represented by a scheme locally of finite type over k, the identity component is represented by a projective algebraic group, and the tangent space at the identity is canonically isomorphic to $H^1(\mathcal{S}, \mathcal{O}_{\mathcal{S}})$. See 9.4.8, 9.5.4, and 9.5.11 in **[24]** and recall that $\mathcal{S}$ is integral and normal over $\overline{k}$ since it is integral and normal over the perfect field k.

By definition, the Néron-Severi group of a projective, normal, irreducible surface $\mathcal{S}$ over a field k is the image $\mathrm{NS}(\mathcal{S})$ of $\mathrm{Pic}(\mathcal{S})$ in

$$\mathrm{NS}(\mathcal{S} \times_k \overline{k}) := \mathrm{Pic}(\mathcal{S} \times_k \overline{k})/\mathrm{Pic}^0(\mathcal{S} \times_k \overline{k}).$$

Thus $\mathrm{NS}(\mathcal{S})$ is a subgroup of $\mathrm{NS}(\mathcal{S} \times_k \overline{k})$. Therefore, to prove Theorem 6.13 it suffices to treat the case where k is algebraically closed; in this section, we assume $k = \overline{k}$ when convenient, but in some places we consider more general fields k.

6.2.1. Shioda-Tate isomorphism. Let k be a perfect field, let $\mathcal{B}$ be a smooth, projective, geometrically irreducible curve over k, and let $\mathcal{S}$ be a smooth, projective, geometrically irreducible surface over k equipped with a generically smooth and surjective morphism $\pi : \mathcal{S} \to \mathcal{B}$. Let $K = k(\mathcal{B})$ be the function field of $\mathcal{B}$, let J/K be the Jacobian of the generic fiber of π, and let (A, τ) be the K/k-trace of J.

Recall that $L^1\mathrm{Pic}(\mathcal{S})$ is the subgroup of $\mathrm{Pic}(\mathcal{S})$ consisting of classes of divisors orthogonal to a fiber of π, that $L^2\mathrm{Pic}(\mathcal{S})$ is the subgroup of $L^1\mathrm{Pic}(\mathcal{S})$ consisting of classes of divisors supported in the fibers of π, and that $L^i\,\mathrm{NS}(\mathcal{S})$, for $i = 1, 2$ is the corresponding subgroup of $\mathrm{NS}(\mathcal{S})$.

PROPOSITION 6.14. *There is a homomorphism*

$$\frac{L^1\,\mathrm{NS}(\mathcal{S})}{L^2\,\mathrm{NS}(\mathcal{S})} \to \mathrm{MW}(J) = \frac{J(K)}{\tau A(k)}$$

with finite kernel and cokernel. It is an isomorphism if π has a section and if k is either finite or algebraically closed.

See [**51**, Proposition 4.1].

6.2.2. $\mathrm{NS}_{\mathrm{tor}}$ and J_{tor}. We continue the notation of the previous section. We further assume that k is finite or algebraically closed.

If $\mathrm{Pic}^0(\mathcal{S}) = 0$, then $\mathrm{NS}(\mathcal{S}) \cong \mathrm{Pic}(\mathcal{S})$ and the K/k-trace of J vanishes. Therefore Proposition 6.14 implies that there is an isomorphism

$$\frac{L^1\mathrm{Pic}(\mathcal{S})}{L^2\mathrm{Pic}(\mathcal{S})} \cong J(K).$$

If, moreover, π admits a section, then $L^2\mathrm{Pic}(\mathcal{S})$ is torsion-free. (See, for example, Section 4.1 in [**51**].) Finally, $\mathrm{NS}(\mathcal{S})_{\mathrm{tor}}$ is contained in $L^1\mathrm{Pic}(\mathcal{S})$ since its elements are numerically equivalent to zero. Therefore we conclude the following:

PROPOSITION 6.15. *If $\mathrm{Pic}^0(\mathcal{S}) = 0$ and if π admits a section, then the Shioda-Tate isomorphism induces an injection $\mathrm{NS}(\mathcal{S})_{\mathrm{tor}} \to J(K)_{\mathrm{tor}}$.*

Later in the paper, we use Proposition 6.15 and bounds on $\mathrm{NS}(\mathcal{X})_{\mathrm{tor}}$ to bound $J(K)_{\mathrm{tor}}$. The reverse is also possible: good control on $J(K)_{\mathrm{tor}}$ suffices to bound $\mathrm{NS}(\mathcal{X})_{\mathrm{tor}}$.

6.2.3. Birational invariance.

PROPOSITION 6.16. *Suppose $\mathcal{S}_1$ and $\mathcal{S}_2$ are projective, normal surfaces over k and $f : \mathcal{S}_1 \to \mathcal{S}_2$ is a birational map. Then $\mathrm{NS}(\mathcal{S}_1)_{\mathrm{tor}} \cong \mathrm{NS}(\mathcal{S}_2)_{\mathrm{tor}}$ and $\mathrm{Pic}^0(\mathcal{S}_1) \cong \mathrm{Pic}^0(\mathcal{S}_2)$.*

PROOF. By resolution of singularities and [**20**, V.5.5], there is a smooth projective surface $\mathcal{S}$ with birational maps $f_1 : \mathcal{S} \to \mathcal{S}_1$ and $f_2 : \mathcal{S} \to \mathcal{S}_2$ satisfying $f = f_2 \circ f_1^{-1}$. It suffices to prove the proposition with $(\mathcal{S}, \mathcal{S}_1, f_1)$ and $(\mathcal{S}, \mathcal{S}_2, f_2)$ in lieu of $(\mathcal{S}_1, \mathcal{S}_2, f)$. Therefore we may suppose, without loss of generality, that $\mathcal{S}_1$ is smooth and projective and that f is a birational morphism, in other words, that f is a morphism and induces a birational isomorphism.

If $s \in \mathcal{S}_2$ is a point over which f is not an isomorphism, then since $\mathcal{S}_1$ is smooth, it is known (e.g., Corollary 2.7 in [**3**]) that

$$f^{-1}(s) = \sum_{i=1}^{n} r_i E_i$$

where the E_i are pairwise distinct integral curves on $\mathcal{S}_1$ and the r_i are positive integers. Moreover, the restriction of the intersection pairing on $\mathcal{S}_1$ to the subgroup of $\mathrm{NS}(\mathcal{S}_1)$ generated by the classes of the E_i is negative definite.

Let $\{s_1, \ldots, s_m\}$ be the set of points over which f is not an isomorphism, let n_i be the number of components of $f^{-1}(s_i)$, let $E_{i1}, \ldots, E_{in_i}$ denote the components of $f^{-1}(s_i)$, and let $N = \sum_{i=1}^{m} n_i$ so that N is the total number of exceptional curves introduced in passing from $\mathcal{S}_2$ to $\mathcal{S}_1$.

There is a homomorphism $\mathbb{Z}^N \to \mathrm{Pic}(\mathcal{S}_1)$ given by sending $(a_{11}, \ldots, a_{mn_m})$ to the class of $\sum_{i=1}^{m} \sum_{j=1}^{n_i} a_{ij} E_{ij}$. We also have $f^* : \mathrm{Pic}(\mathcal{S}_2) \to \mathrm{Pic}(\mathcal{S}_1)$. Trivial modifications of the proof of V.3.2 in [**20**], show that these maps induce an isomorphism

$$\mathrm{Pic}(\mathcal{S}_1) \cong \mathrm{Pic}(\mathcal{S}_2) \oplus \mathbb{Z}^N.$$

It follows that $\mathrm{Pic}^0(\mathcal{S}_1) \cong \mathrm{Pic}^0(\mathcal{S}_2)$ as claimed. It also follows that $\mathrm{NS}(\mathcal{S}_1) \cong \mathrm{NS}(\mathcal{S}_2) \oplus \mathbb{Z}^N$ and thus that $\mathrm{NS}(\mathcal{S}_1)_{\mathrm{tor}} \cong \mathrm{NS}(\mathcal{S}_2)_{\mathrm{tor}}$ as claimed. □

6.2.4. Geometric method. In this subsection, we use a geometric method to kill torsion in Néron-Severi under suitable hypotheses. In the application to $\mathcal{X}_d$, this method suffices to kill torsion of order coprime to r and not divisible by $p = \mathrm{Char}(k)$; however, by itself, it does not seem to handle primes dividing r.

Let $\mathcal{S}$ be a smooth, irreducible, projective surface over k, and let $G \subseteq \mathrm{Aut}_k(\mathcal{S})$ be a finite subgroup.

LEMMA 6.17. *The quotient $\mathcal{S}/G$ is normal, irreducible, and projective.*

PROOF. It is clear that $\mathcal{S}/G$ is irreducible. It follows from [**39**, Chapter III, Section 12, Corollary] that it is normal and from [**19**, Lecture 10] that it is projective. □

Therefore $\mathrm{Pic}(\mathcal{S}/G)$ has the properties detailed in the second paragraph after the statement of Theorem 6.13.

PROPOSITION 6.18. *Suppose some fiber of $\mathcal{S} \to \mathcal{S}/G$ contains exactly one point. If $\ell \neq p$ is a prime number such that $\mathrm{Pic}(\mathcal{S})[\ell]^G = 0$, then $\mathrm{NS}(\mathcal{S}/G)[\ell] = \mathrm{Pic}(\mathcal{S}/G)[\ell] = 0$.*

PROOF. Every element of $\mathrm{NS}(\mathcal{S}/G)[\ell]$ lifts to $\mathrm{Pic}(\mathcal{S}/G)[\ell]$ since $\mathrm{Pic}^0(\mathcal{S}/G)$ is divisible, and thus it suffices to show that $\mathrm{Pic}(\mathcal{S}/G)[\ell]{=}0$. Suppose that $\mathcal{L}$ is a line bundle on $\mathcal{S}/G$ whose class in $\mathrm{Pic}(\mathcal{S}/G)$ is ℓ-torsion. We must show that it is trivial in $\mathrm{Pic}(\mathcal{S}/G)$.

If we choose an isomorphism $\mathcal{L}^\ell \cong \mathcal{O}_{\mathcal{S}/G}$, then the $\mathcal{O}_{\mathcal{S}/G}$-module

$$\mathcal{A} = \mathcal{O}_{\mathcal{S}/G} \oplus \mathcal{L} \oplus \mathcal{L}^2 \oplus \cdots \oplus \mathcal{L}^{\ell-1}$$

inherits the structure of a sheaf of $\mathcal{O}_{\mathcal{S}/G}$-algebras. Let

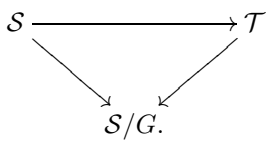
$$\mathcal{T} = \underline{\mathrm{Spec}}_{\mathcal{O}_{\mathcal{S}/G}} \mathcal{A}$$

(global Spec) so that there is a finite étale morphism $\mathcal{T} \to \mathcal{S}/G$ of degree ℓ. This morphism has a section if and only if $\mathcal{L}$ is trivial, i.e., $\mathcal{L} \cong \mathcal{O}_{\mathcal{S}/G}$.

The pull back of $\mathcal{L}$ to $\mathcal{S}$ is trivial since $\mathrm{Pic}(\mathcal{S})[\ell]^G = 0$. Therefore, the fiber product $\mathcal{S} \times_{\mathcal{S}/G} \mathcal{T}$ is trivial as an étale cover of $\mathcal{S}$; in other words, there is a section of the projection

$$\mathcal{S} \times_{\mathcal{S}/G} \mathcal{T} \to \mathcal{S}.$$

This yields a commutative diagram



On one hand, by hypothesis some fiber of the quotient map $\mathcal{S} \to \mathcal{S}/G$ contains exactly one point. On the other hand, $\mathcal{T} \to \mathcal{S}/G$ is finite étale of degree ℓ. It follows that the image of $\mathcal{S}$ in $\mathcal{T}$ has degree 1 over $\mathcal{S}/G$ and that $\mathcal{T} \to \mathcal{S}/G$ is not connected. Hence the covering $\mathcal{T} \to \mathcal{S}/G$ is trivial, i.e., $\mathcal{T} \cong (\mathcal{S}/G) \times (\mathbb{Z}/\ell\mathbb{Z})$. Therefore $\mathcal{L}$ is trivial in $\mathrm{Pic}(\mathcal{S}/G)$ as claimed. □

6.2.5. Some group cohomology. In this subsection, we collect some facts about the group cohomology of $G = \mu_r$.

Let g be a generator of G. Recall that for an $\mathbb{F}_\ell[G]$-module M, the elements $D = 1 - g$ and $N = 1 + g + \cdots + g^{r-1}$ of $\mathbb{F}_\ell[G]$ act on M and there are isomorphisms

$$H^i(G, M) \cong \begin{cases} \ker(D) & \text{if } i = 0, \\ \ker(N)/\mathrm{im}(D) & \text{if } i \geq 1 \text{ is odd}, \\ \ker(D)/\mathrm{im}(N) & \text{if } i \geq 2 \text{ is even}. \end{cases}$$

Let $R = \mathbb{F}_\ell[G]$ be the regular representation of G, and let W be the quotient of R by the subspace of G-invariants R^G.

LEMMA 6.19.

(1) $H^i(G, R) \cong \begin{cases} \mathbb{F}_\ell & \text{if } i = 0, \\ 0 & \text{if } i > 0; \end{cases}$

(2) $H^i(G, \mathbb{F}_\ell) \cong \begin{cases} \mathbb{F}_\ell & \text{if } i = 0 \text{ or } \ell \mid r, \\ 0 & \text{if } i > 0 \text{ and } \ell \nmid r; \end{cases}$

(3) $H^i(G, W) \cong H^{i+1}(G, \mathbb{F}_\ell)$ *for* $i \geq 0$;

(4) $H^i(G, W \otimes W) \cong H^{i+1}(G, W)$ *for* $i > 0$.

PROOF. We may identity R^G with the trivial $\mathbb{F}_\ell[G]$-module $\mathbb{F}_\ell$, which is the $i = 0$ part of (1). The rest of part (1) follows from [**40**, page 112, Proposition 1] since $\mathbb{F}_\ell[G]$ is co-induced. Part (2) is a simple exercise using the isomorphisms displayed just before the lemma. For part (3), by the definition of W, there is an exact sequence

$$0 \to \mathbb{F}_\ell \to R \to W \to 0. \tag{6.11}$$

Taking cohomology yields an exact sequence

$$0 \to H^0(G, \mathbb{F}_\ell) \to H^0(G, R) \to H^0(G, W) \to H^1(G, \mathbb{F}_\ell) \to 0$$

and identities $H^i(G, W) \cong H^{i+1}(G, \mathbb{F}_\ell)$, for $i \geq 0$.

Since $R \otimes W$ is co-induced, applying [**40**, p. 112, Proposition 1] implies that $H^i(G, R \otimes W) = 0$ for $i > 0$. Tensoring (6.11) with W and taking cohomology produces an exact sequence

$$0 \to H^0(G, W) \to H^0(G, R \otimes W) \to H^0(G, W \otimes W) \to H^1(G, W) \to 0$$

and identities $H^i(G, W \otimes W) \cong H^{i+1}(G, W)$ for $i > 0$. □

Consider an exact sequence of $\mathbb{F}_\ell[G]$-modules

$$0 \to \mathbb{F}_\ell \to \tilde{W} \to W \to 0.$$

LEMMA 6.20. $\tilde{W} \cong \mathbb{F}_\ell \oplus W$ *or* $\tilde{W} \cong R$ *as* $\mathbb{F}_\ell[G]$*-modules.*

PROOF. There is an element $w \in W$ that generates W as an $\mathbb{F}_\ell[G]$-module, that is, W is cyclic as an $\mathbb{F}_\ell[G]$-module. Let $\tilde{w} \in \tilde{W}$ be a lift of w. The $\mathbb{F}_\ell[G]$-submodule of $\tilde{W}$ generated by $\tilde{w}$ maps surjectively to $\tilde{W}$. If this map is an isomorphism, the above sequence is split and $\tilde{W} \cong \mathbb{F}_\ell \oplus W$. Otherwise the submodule must be all of $\tilde{W}$, in which case $\tilde{W}$ is cyclic and has $\mathbb{F}_\ell$-dimension r, so is isomorphic to R. □

Note that $R \cong \mathbb{F}_\ell \oplus W$ if $\ell \nmid r$.

6.2.6. Cohomological method. Recall that $r > 1$ is an integer not divisible by p. In this subsection, we develop a more elaborate, cohomological method to kill torsion in Néron-Severi. We need it to kill ℓ-torsion in $\mathrm{NS}(\mathcal{X}_d)$ when ℓ is a prime dividing r.

To state the result, let $\mathcal{C} \to \mathbb{P}^1$ (resp., $\mathcal{D} \to \mathbb{P}^1$) be a Galois branched cover with group $G = \mu_r$ that is totally ramified over $b_1 > 0$ (resp., $b_2 > 0$) points of $\mathbb{P}^1$ and unramified elsewhere. Let G act diagonally on $\mathcal{S} = \mathcal{C} \times_k \mathcal{D}$.

PROPOSITION 6.21. $\mathrm{NS}(\mathcal{S}/G)[\ell] = \mathrm{Pic}(\mathcal{S}/G)[\ell] = 0$ *for any prime number* $\ell \neq p$.

The proof occupies the remainder of this subsection. It suffices to treat the case where k is algebraically closed, so we make this assumption for the rest of this section.

To lighten notation, for a scheme $\mathcal{Y}$ over k we write $H^i(\mathcal{Y})$ for the étale cohomology group $H^i(\mathcal{Y}_{et}, \mathbb{F}_\ell)$ and $H^i_c(\mathcal{Y})$ for the étale cohomology group with compact supports.

LEMMA 6.22. *The following G-modules are isomorphic:*

(1) $H^0(\mathcal{C}) \cong H^2(\mathcal{C}) \cong H^0(\mathcal{D}) \cong H^2(\mathcal{D}) \cong \mathbb{F}_\ell$;

(2) $H^1(\mathcal{C}) \cong W^{b_1-2}$ *and* $H^1(\mathcal{D}) \cong W^{b_2-2}$.

PROOF. The first part is well known since $\mathcal{C}, \mathcal{D}$ are irreducible projective curves, and it suffices to prove the second part for $\mathcal{C}$ since the argument for $\mathcal{D}$ is identical.

Let $\mathcal{C}^o$ denote the maximal open subset of $\mathcal{C}$ where $\mathcal{C} \to \mathbb{P}^1$ is unramified and let $\mathcal{P}^o$ be the image of $\mathcal{C}^o$ in $\mathbb{P}^1$. Then $\mathcal{P}^o$ is $\mathbb{P}^1$ minus b_1 points and $f : \mathcal{C}^o \to \mathcal{P}^o$ is an étale Galois cover with group G. We first check that there is an isomorphism

$$H^1(\mathcal{C}^o) \cong \mathbb{F}_\ell \oplus R^{b_1-2}.$$

Indeed, $H^1(\mathcal{C}^o) \cong H^1(\mathcal{P}^o, f_*\mathbb{F}_\ell)$ since f is finite. The stalk of $f_*\mathbb{F}_\ell$ at the generic point of $\mathcal{P}^o$ may be identified as a G-module with R, and it has an action of $\pi_1^{(p)}$, the prime-to-p fundamental group of $\mathcal{P}^o$. Moreover [**30**, V.2.17], $H^1(\mathcal{P}^o, f_*\mathbb{F}_\ell)$ is isomorphic to the Galois cohomology group $H^1(\pi_1^{(p)}, R)$. Using the fact that $\pi_1^{(p)}$ is the free pro-prime-to-p group on $b_1 - 1$ generators $\sigma_1, \ldots, \sigma_{b_1-1}$, it is an easy exercise to check that $H^1(\pi_1^{(p)}, R)$ is isomorphic to the cokernel of the map

$$R \to R^{b_1-1}, \qquad \lambda \mapsto (\sigma_1\lambda - \lambda, \ldots, \sigma_{b_1-1}\lambda - \lambda).$$

Since each generator σ_i acts on R as multiplication by some generator of G (by our hypothesis that $\mathcal{C} \to \mathbb{P}^1$ is totally ramified at each branch point), the cokernel is isomorphic to $\mathbb{F}_\ell \oplus R^{b_1-2}$, as desired.

To finish, we note that $H^1(\mathcal{C}^o) \cong H^1_c(\mathcal{C}^o)^*$ by Poincaré duality and that, by excision, there is an exact sequence

$$0 \to H^0(\mathcal{C}) \to H^0(\mathcal{C} \setminus \mathcal{C}^o) \to H^1_c(\mathcal{C}^o) \to H^1(\mathcal{C}) \to 0.$$

Since $H^0(\mathcal{C} \setminus \mathcal{C}^o) \cong \mathbb{F}_\ell^d$ as a G-module, the result follows easily. □

LEMMA 6.23. *Let X be a variety over k. Let $\mathcal{G}$ be a finite group of order prime to p which acts on X, and let $Y = X/\mathcal{G}$. Then for $i \geq 1$,*

$$H^i(Y, \mathcal{O}) = H^i(X, \mathcal{O})^{\mathcal{G}}.$$

PROOF. Recall that by a variety over k, we mean a separated scheme of finite type over k. Let (V_i) be a cover of Y by open affines. Let $U_i \subset X$ be the preimage of V_i; the V_i are $\mathcal{G}$-invariant and, since $X \to Y$ is finite, are also affine. Separability implies that intersections of the V_i (resp. U_i) are also affine. If $\check{H}$ denotes Čech cohomology, by [**20**, III.4.5], then

$$\check{H}^i((V_i), \mathcal{O}) = H^i(Y, \mathcal{O})$$

and similarly for X. For $i \geq 1$, consider the Čech complex

$$\cdots \longrightarrow C^{i-1}((U_i), \mathcal{O}) \longrightarrow C^i((U_i), \mathcal{O}) \longrightarrow C^{i+1}((U_i), \mathcal{O}) \longrightarrow \cdots .$$

If we take $\mathcal{G}$-invariants, we obtain the corresponding Čech complex for Y. All of the groups above are k-vector spaces and the order of $\mathcal{G}$ is prime to p, so taking $\mathcal{G}$-invariants commutes with taking homology. The claim follows. □

Recall $G = \mu_r$, and let $\mathcal{T} = \mathcal{S}/G$.

LEMMA 6.24. $\mathrm{Pic}^0(\mathcal{T}) = 0$.

PROOF. Lemma 6.23 and the Künneth formula imply

$$H^1(\mathcal{T}, \mathcal{O}) = H^1(\mathcal{S}, \mathcal{O})^G = \big(H^1(\mathcal{C}, \mathcal{O}) \oplus H^1(\mathcal{D}, \mathcal{O})\big)^G = 0.$$

In particular, $\mathrm{Pic}^0(\mathcal{T}) = 0$ since its tangent space space is $H^1(\mathcal{T}, \mathcal{O})$ and thus is trivial. □

Therefore, $\mathrm{NS}(\mathcal{T}) = \mathrm{Pic}(\mathcal{T})$ and

$$\mathrm{NS}(\mathcal{T})[\ell] = \mathrm{Pic}(\mathcal{T})[\ell] = H^1(\mathcal{T}, \mu_\ell) = H^1(\mathcal{T}),$$

since k is algebraically closed. The rest of the proof of Proposition 6.21 is a somewhat elaborate calculation of $H^1(\mathcal{T})$; in particular, we show it vanishes.

Let $Z \subset \mathcal{S}$ be the reduced subscheme of fixed points, which by our hypotheses consists simply of $b_1 b_2$ distinct points. We identify Z with its image in $\mathcal{T}$ as well. Let $\mathcal{S}^o = \mathcal{S} \setminus Z$ and $\mathcal{T}^o = \mathcal{T} \setminus Z$ and note that $\mathcal{S}^o \to \mathcal{T}^o$ is an étale Galois cover with group G and that $\mathcal{T}^o$ is smooth.

LEMMA 6.25. *We have the following isomorphisms of $\mathbb{F}_\ell[G]$-modules:*

$$H^i(\mathcal{S}) \cong \begin{cases} \mathbb{F}_\ell & \text{if } i = 0 \text{ or } 4, \\ W^{b_1+b_2-4} & \text{if } i = 1 \text{ or } 3, \\ \mathbb{F}_\ell^2 \oplus (W \otimes W)^{(b_1-2)(b_2-2)} & \text{if } i = 2. \end{cases}$$

PROOF. This follows from the Künneth formula

$$H^i(\mathcal{S}) \cong \oplus_{j=0}^i \big(H^j(\mathcal{C}) \otimes H^{i-j}(\mathcal{D})\big)$$

and Lemma 6.22. □

By excision, there is an exact sequence

$$0 \to H^0(\mathcal{T}) \to H^0(Z) \to H^1_c(\mathcal{T}^o) \to H^1(\mathcal{T}) \to 0$$

and an isomorphism

$$H^j_c(\mathcal{T}^o) \cong H^j(\mathcal{T}),$$

for $j \geq 2$, since Z is zero dimensional. We also have the Poincaré duality isomorphism

$$H^j_c(\mathcal{T}^o) \cong H^{4-j}(\mathcal{T}^o)^*$$

for $0 \leq j \leq 4$. Therefore, to show that $H^1(\mathcal{T}) = 0$ we must show that $H^3(\mathcal{T}^o)$ has dimension $b_1 b_2 - 1$ as an $\mathbb{F}_\ell$-vector space; its dimension is at least this. To show equality we use the Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i(G, H^j(\mathcal{S}^o)) \Longrightarrow H^{i+j}(\mathcal{T}^o). \tag{6.12}$$

To compute the E_2 term, we begin by computing $H^j(\mathcal{S}^o)$.

LEMMA 6.26. *We have the following isomorphisms of $\mathbb{F}_\ell[G]$-modules:*

$$H_c^j(\mathcal{S}^o) \cong \begin{cases} \mathbb{F}_\ell^{a_1} \oplus R^{a_2} \oplus W^{a_3} & \text{if } j = 1, \\ \mathbb{F}_\ell^2 \oplus (W \otimes W)^{(b_1-2)(b_2-2)} & \text{if } j = 2, \\ W^{b_1+b_2-4} & \text{if } j = 3, \\ \mathbb{F}_\ell & \text{if } j = 4, \\ 0 & \text{otherwise} \end{cases}$$

where $a_1 + a_2 = b_1 b_2 - 1$ and $a_2 + a_3 = b_1 + b_2 - 4$.

PROOF. By excision, there is an exact sequence

$$0 \to H^0(\mathcal{S}) \to H^0(Z) \to H_c^1(\mathcal{S}^o) \to H^1(\mathcal{S}) \to 0$$

and isomorphisms

$$H_c^j(\mathcal{S}^o) \cong H^j(\mathcal{S})$$

for $j \geq 2$, since Z is zero dimensional and non-empty. Therefore, Lemmas 6.20 and 6.25 imply that $H_c^{4-j}(\mathcal{S}^o)$ has the desired form. (Roughly speaking, a_3 is the number of copies of W in $H^1(\mathcal{C})$ over which the extension $H_c^1(\mathcal{S}^o)$ is split.) □

COROLLARY 6.27. *We have the following isomorphisms of $\mathbb{F}_\ell[G]$-modules:*

$$H^j(\mathcal{S}^o) \cong \begin{cases} \mathbb{F}_\ell & \text{if } j = 0, \\ W^{b_1+b_2-4} & \text{if } j = 1, \\ \mathbb{F}_\ell^2 \oplus (W \otimes W)^{(b_1-2)(b_2-2)} & \text{if } j = 2, \\ \mathbb{F}_\ell^{a_1} \oplus R^{a_2} \oplus W^{a_3} & \text{if } j = 3, \\ 0 & \text{otherwise,} \end{cases}$$

where $a_1 + a_2 = b_1 b_2 - 1$ and $a_2 + a_3 = b_1 + b_2 - 4$.

PROOF. The Poincaré duality isomorphism states that

$$H^j(\mathcal{S}^o)^* \cong H_c^{4-j}(\mathcal{S}^o)$$

for $0 \leq j \leq 4$. In particular, $\mathbb{F}_\ell, R, W$ are self-dual as $\mathbb{F}_\ell[G]$-modules, so $H^j(\mathcal{S}^o)^*$ is also self-dual, and thus $H^j(\mathcal{S}^o)$ has the desired form. □

Applying Lemma 6.19 and Corollary 6.27, we find that if $\ell \nmid r$, then

$$\dim E_2^{i,j} = \dim(H^i(G, H^j(\mathcal{S}^o))) = \begin{cases} b_1 b_2 - 1 & \text{if } i = 0, j = 3, \\ 0 & \text{if } i \geq 1, j \geq 0. \end{cases} \tag{6.13}$$

One can deduce more, but when $\ell \nmid r$ this already suffices to show that (6.12) degenerates and

$$\dim H^3(\mathcal{T}^o) = \dim E_2^{0,3} = b_1 b_2 - 1$$

as claimed. Therefore, we suppose for the remainder of this subsection that $\ell \mid r$ and apply Lemma 6.19 and Corollary 6.27 to deduce

$$\dim E_2^{i,j} = \begin{cases} 1 & \text{if } i \geq 0,\ j = 0, \\ b_1 + b_2 - 4 & \text{if } i \geq 0,\ j = 1, \\ b_1 b_2 - 2b_1 - 2b_2 + 6 & \text{if } i > 0,\ j = 2, \\ b_1 b_2 - 1 + a_3 & \text{if } i = 0,\ j = 3, \\ b_1 b_2 - b_1 - b_2 + 3 + 2a_3 & \text{if } i > 0,\ j = 3. \end{cases} \tag{6.14}$$

One can also deduce more in this case, but these suffice for our purposes. More precisely, to show $\dim H^3(\mathcal{T}^o) = b_1 b_2 - 1$, it suffices to show that $a_3 = 0$ and $\dim H^3(\mathcal{T}^o) \leq \dim E_2^{0,3}$.

The spectral sequence (6.12) has non-zero groups only in the first quadrant and has only four non-trivial rows, i.e., $E_h^{i,j} = 0$ unless $i \geq 0$ and $0 \leq j \leq 3$. It follows immediately that $d_h^{i,j} = 0$ if $h > 4$ or if $j > 3$ or if $h > j + 1$, and also that $E_\infty^{i,j} = E_5^{i,j}$.

LEMMA 6.28. *The differentials $d_h^{i,j}$ in the spectral sequence* (6.12) *satisfy the following: For $h \geq 2$ and $i \geq 1$, $\operatorname{rank} d_h^{i,3} = \dim E_2^{i+h,4-h}$. Moreover, with notation as in Corollary 6.27, $a_3 = 0$.*

PROOF. Since $\mathcal{T}^o$ is not complete and $\dim(\mathcal{T}^o) = 2$, it follows that $H^{i+j}(\mathcal{T}^o)$ vanishes for $i \geq 1$ and $j = 3$. Thus $E_5^{i,3}$ vanishes, and the definitions of $E_h^{i,3}$ for $h = 1, 2, 3$ imply that

$$\dim E_2^{i,3} = \operatorname{rank} d_2^{i,3} + \operatorname{rank} d_3^{i,3} + \operatorname{rank} d_4^{i,3}$$

for $i \geq 1$. Moreover,

$$\operatorname{rank} d_2^{i,3} + \operatorname{rank} d_3^{i,3} + \operatorname{rank} d_4^{i,3} \leq \dim E_2^{i+2,2} + \dim E_2^{i+3,1} + \dim E_2^{i+4,0}$$

and so

$$\dim E_2^{i,3} \leq \dim E_2^{i+2,2} + \dim E_2^{i+3,1} + \dim E_2^{i+4,0}$$

for $i \geq 1$. Comparing dimensions using (6.14), we see that $a_3 = 0$ and that

$$\operatorname{rank} d_h^{i,3} = \dim E_2^{i+h,4-h} \tag{6.15}$$

for $i \geq 1$ and $h = 2, 3, 4$. Trivially, $\operatorname{rank} d_h^{i,3} = 0$ for $h \geq 5$ since $E_2^{i+h,4-h} = 0$ for $h \geq 5$. This establishes the claims of the lemma. □

LEMMA 6.29. *The differentials $d_h^{i,j}$ in the spectral sequence* (6.12) *satisfy*

$$d_h^{2,2} = d_h^{3,1} = d_h^{4,0} = 0$$

for $h \geq 2$.

PROOF. By Lemma 6.28, $\operatorname{rank} d_3^{1,3} = \dim E_2^{4,1}$. Therefore, $\dim E_3^{4,1} = \dim E_2^{4,1}$ and $d_2^{2,2} = 0$. Similarly, Lemma 6.28 says that $\operatorname{rank} d_4^{1,3} = \dim E_2^{5,0}$ which implies that $d_2^{3,1} = d_3^{2,2} = 0$. Trivially, $d_h^{2,2}$ vanishes for $h > 3$, $d_h^{3,1}$ vanishes for $h > 2$, and $d_h^{4,0}$ vanishes for $h > 1$. This completes the proof of the lemma. □

LEMMA 6.30. *With notation as above,* $\dim H^3(\mathcal{T}^o) \leq \dim E_2^{0,3} = b_1 b_2 - 1$.

PROOF. On one hand, the previous lemma says that all the differentials $d_h^{i,j}$ with domain $E_h^{i,j}$ vanish when $i+j=4$, $i\geq 2$, and $h\geq 2$. On the other hand, $H^4(\mathcal{T}^o)=0$, so $E_\infty^{i,j}=0$ for $i+j=4$. It follows that

$$\dim H^3(\mathcal{T}^o)=\sum_{i+j=3}\dim E_\infty^{i,j}\leq\sum_{i+j=3}\dim E_2^{i,j}-\sum_{\substack{i+j=4\\ i\geq 2}}\dim E_2^{i,j}.$$

Applying Equation (6.14), this last difference is $\dim E_2^{0,3}$ and (6.14) together with Lemma 6.28 shows that $\dim E_2^{0,3}=b_1b_2-1$. This completes the proof of the lemma. □

As noted after Lemma 6.25, the inequality $\dim H^3(\mathcal{T}^o)\leq b_1b_2-1$ completes the proof that $H^1(\mathcal{T})=0$ and that of Proposition 6.21.

6.2.7. Proof of Theorem 6.13. The statement of Theorem 6.13 is that $\mathrm{NS}(\mathcal{X}_d)_{\mathrm{tor}}=0$. By Proposition 6.15, there is an injection $\mathrm{NS}(\mathcal{X}_d)_{\mathrm{tor}}\to J(K)_{\mathrm{tor}}$. Moreover, we proved in Corollary 6.1 that $J(K)$ has no p-torsion, thus neither does $\mathrm{NS}(\mathcal{X}_d)$. It thus suffices to prove that $\mathrm{NS}(\mathcal{X}_d)[\ell]=0$ for every prime $\ell\neq p$.

For the rest of the proof, suppose $\ell\neq p$. By Proposition 6.16, it suffices to prove $\mathrm{NS}(\mathcal{T}_1)[\ell]=0$ for some $\mathcal{T}_1$ that is birational to $\mathcal{X}_d$. Recall from Section 3.3 that $\mathcal{X}_d$ is birational to the quotient $\mathcal{S}/(\mu_r\times\mu_d)$ constructed as follows:

Let $\mathcal{C}_d$ and $\mathcal{D}_d$ be the smooth, projective curves over k with affine models

$$\mathcal{C}_d: z^d=x^r-1\quad\text{and}\quad\mathcal{D}_d: w^d=y^r-1$$

respectively, and let $\mathcal{S}=\mathcal{C}_d\times_k\mathcal{D}_d$. The action of $\mu_r\times\mu_d$ on $\mathbb{A}^2\times_k\mathbb{A}^2$ given by

$$(x,y,z,w)\mapsto(\eta x,\eta^{-1}y,\zeta z,\zeta^{-1}w)$$

induces an action on $\mathcal{S}$.

Let $\mathcal{T}=\mathcal{S}/\mu_r$. Observe that Proposition 6.21 implies $\mathrm{NS}(\mathcal{T})[\ell]=0$ and that Lemma 6.24 implies $\mathrm{Pic}^0(\mathcal{T})=0$. Now let $\mathcal{S}_1\to\mathcal{T}$ be a resolution of singularities of $\mathcal{T}$ that is an isomorphism away from the singular points. The action of μ_d on $\mathcal{S}$ has isolated fixed points that are disjoint from the fixed points of the action of μ_r. It also descends to an action on $\mathcal{T}$ and then lifts (uniquely) to an action on $\mathcal{S}_1$ with isolated fixed points (cf. [**20**, II.7.15]). Proposition 6.16 implies that $\mathrm{Pic}^0(\mathcal{S}_1)=\mathrm{Pic}^0(\mathcal{T})=0$, and so $\mathrm{Pic}(\mathcal{S}_1)[\ell]=\mathrm{NS}(\mathcal{S}_1)[\ell]=0$. *A fortiori*, $\mathrm{Pic}(\mathcal{S}_1)[\ell]^G=0$, and thus we may apply Proposition 6.18 to deduce that $\mathrm{NS}(\mathcal{T}_1)[\ell]=0$ for $\mathcal{T}_1=\mathcal{S}_1/\mu_d$ and $\ell\neq p$. This completes the proof since $\mathcal{T}_1$ is birational to $\mathcal{S}/(\mu_r\times\mu_d)$ and thus to $\mathcal{X}_d$. □

For future use, we record one other byproduct of our analysis.

PROPOSITION 6.31. $\mathrm{Pic}^0(\mathcal{X}_d)=0$ *and thus the K/k-trace of J is trivial.*

PROOF. As observed in the proof of Theorem 6.13, Lemma 6.24 implies that $\mathrm{Pic}^0(\mathcal{S}/\mu_r)=0$. Using the fact that $H^1(\mathcal{S}/\mu_r,\mathcal{O})$ is the tangent space of $\mathrm{Pic}^0(\mathcal{S}/\mu_r)$ (and similarly for $\mathcal{S}/(\mu_r\times\mu_d)$) along with Lemma 6.23, we see that

$$\mathrm{Pic}^0(\mathcal{S}/(\mu_r\times\mu_d))=0.$$

Therefore $\mathrm{Pic}^0(\mathcal{X}_d)=0$ since $\mathcal{X}_d$ and $\mathcal{S}/(\mu_r\times\mu_d)$ are birational. Finally, the K/k-trace of J vanishes since it is inseparably isogenous to $\mathrm{Pic}^0(\mathcal{X}_d)/\mathrm{Pic}^0(\mathbb{P}^1)$—see [**11**] or [**43**]—and since $\mathrm{Pic}^0(\mathcal{X}_d)$ vanishes. □

CHAPTER 7

Index of the visible subgroup and the Tate-Shafarevich group

In this chapter, we work under the hypotheses that r divides d, $d = p^\nu + 1$, and d divides $q - 1$. The first goal is to understand the index of the visible subgroup V in $J(K_d)$. Ultimately, we find that the index is a power of p and equal to the square root of the order of the Tate-Shafarevich group $Ш(J/K_d)$. Specifically, in Section 7.1, we determine the torsion subgroup $J(\mathbb{F}_q(u))_{\mathrm{tor}}$ and prove that the index of V in $J_r(\mathbb{F}_q(u))$ is a power of p, Theorem 7.1. In Section 7.2, we find the Tamagawa number $\tau(J/\mathbb{F}_q(u))$ of the Jacobian J of C over $\mathbb{F}_q(u)$, Proposition 7.5. Finally, in Section 7.3, we prove an analytic class number formula relating the Tate-Shafarevich group $Ш(J/\mathbb{F}_q(u))$ and the index $[J(\mathbb{F}_q(u)) : V]$, Theorem 7.7.

7.1. Visible versus Mordell-Weil

Let V be the visible subgroup of $J(\mathbb{F}_q(u))$, that is, the subgroup generated by

$$P = (u, u(u+1)^{d/r}) \in C(\mathbb{F}_q(u)) \hookrightarrow J(\mathbb{F}_q(u))$$

and its Galois conjugates. By Corollary 5.7, we know that

$$\operatorname{rank} V = \operatorname{rank} J(\mathbb{F}_q(u)) = (r-1)(d-2).$$

In particular, V has finite index in $J(\mathbb{F}_q(u))$. In this section, we show that this index is a power of p thus completing our knowledge of $J(\mathbb{F}_q(u))$. More precisely:

THEOREM 7.1. *Suppose that r divides d, that $d = p^\nu + 1$, and that d divides $q-1$. The torsion subgroup $J(\mathbb{F}_q(u))_{\mathrm{tor}}$ equals V_{tor} and has order r^3. The index of V in $J_r(\mathbb{F}_q(u))$ is a power of p.*

The proof is given later in this section. Before giving it, we prove a general integrality result for regulators of Jacobians over function fields.

7.1.1. Integrality. Let $\mathcal{B}$ (resp. $\mathcal{S}$) be a curve (resp. surface) over $k = \mathbb{F}_q$. We assume that $\mathcal{B}$ and $\mathcal{S}$ are smooth, projective, and geometrically irreducible, that $\mathcal{S}$ is equipped with a surjective and generically smooth morphism $\pi : \mathcal{S} \to \mathcal{B}$, and that π has a section whose image we denote O. Let $\mathrm{NS}(\mathcal{S})$ be the Néron-Severi group of $\mathcal{S}$, and let $L^1\,\mathrm{NS}(\mathcal{S})$ and $L^2\,\mathrm{NS}(\mathcal{S})$ be the subgroups of $\mathrm{NS}(\mathcal{S})$ defined in Section 6.2.1.

Let $K = k(\mathcal{B})$ be the function field of $\mathcal{B}$, let J/K be the Jacobian of the generic fiber of π, let (A, τ) be the K/k-trace of J, and let $\mathrm{MW}(J)$ be the Mordell-Weil group $J(K)/\tau A(k)$. By Proposition 6.14 there is an isomorphism

$$\frac{L^1\,\mathrm{NS}(\mathcal{S})}{L^2\,\mathrm{NS}(\mathcal{S})} \to \mathrm{MW}(J),$$

since π has a section and since k is finite.

We write $\det(\mathrm{MW}(J)/\mathrm{tor})$ for the discriminant of the height pairing on $\mathrm{MW}(J)$ modulo torsion. Also, for each place v of K, we write N_v for the subgroup of $\mathrm{NS}(\mathcal{S})$ generated by non-identity components of $\pi^{-1}(v)$ and d_v for the discriminant of the intersection pairing of $\mathcal{S}$ restricted to N_v; by convention, we set $d_v = 1$ if $N_v = 0$. If $\mathcal{J} \to \mathcal{B}$ is the Néron model of J/K, then it follows from [**6**, Section 9.6, Theorem 1] that d_v is also the order of the group of connected components of the fiber of $\mathcal{J} \to \mathcal{B}$ over v.

With these notations, our integrality result is as follows.

PROPOSITION 7.2. *The rational number*

$$|\,\mathrm{NS}(\mathcal{S})_{\mathrm{tor}}|^2 \left(\prod_v d_v\right) \frac{\det(\mathrm{MW}(J)/\mathrm{tor})}{|\,\mathrm{MW}(J)_{\mathrm{tor}}|^2}$$

is an integer.

This generalizes [**52**, Proposition 9.1], which is the case where $\dim(J) = 1$ and $A = 0$. (In that case, $\mathrm{NS}(S)_{\mathrm{tor}}$ is known to be trivial.) The general case is closely related to, but apparently not contained in, the discussion in [**13**, Section 5].

PROOF. Let F be the class in $\mathrm{NS}(S)$ of a fiber of π. Then $L^1\,\mathrm{NS}(S)$ is the subgroup of $\mathrm{NS}(S)$ consisting of classes orthogonal to F.

The intersection form on $\mathcal{S}$ is degenerate when restricted to $L^1\,\mathrm{NS}(S)$; indeed its radical is $\mathbb{Z}F$. We write $\bar{L}^1\,\mathrm{NS}(S)$ and $\bar{L}^2\,\mathrm{NS}(S)$ for the respective quotients of $L^1\,\mathrm{NS}(S)$ and $L^2\,\mathrm{NS}(S)$ by $\mathbb{Z}F$ so that the intersection pairing on $\mathcal{S}$ then defines a non-degenerate pairing on $\bar{L}^1\,\mathrm{NS}(S)$. For any torsion-free subgroup $L \subset \bar{L}^1\,\mathrm{NS}(S)$, we write $\mathrm{Disc}(L)$ for the discriminant of the intersection form restricted to L (i.e., the absolute value of the determinant of the matrix of pairings on a basis); by convention, we set $\mathrm{Disc}(0) = 1$.

We identify N_v with its image in $\bar{L}^2\,\mathrm{NS}(S)$ so that $\mathrm{Disc}(N_v) = d_v$ and so that there is an orthogonal direct sum decomposition

$$\bar{L}^2\,\mathrm{NS}(S) = \bigoplus_v N_v.$$

We also let $d = \prod_v d_v$ so that $d = \mathrm{Disc}(\bar{L}^2\,\mathrm{NS}(S))$.

Choose elements $Q_1, \ldots, Q_m \in \mathrm{MW}(J)$ that map to a basis of $\mathrm{MW}(J)/\mathrm{tor}$ and thus a basis of

$$\mathrm{MW}(J) \otimes \mathbb{Q} = \frac{\bar{L}^1\,\mathrm{NS}(S) \otimes \mathbb{Q}}{\bar{L}^2\,\mathrm{NS}(S) \otimes \mathbb{Q}}.$$

Each Q_i has a naive lift $\tilde{Q}_i$ to $\bar{L}^1\,\mathrm{NS}(S) \otimes \mathbb{Q}$ represented by a $\mathbb{Z}$-linear combination of "horizontal" divisors. The projection of $\tilde{Q}_i$ onto the orthogonal complement of $\bar{L}^2\,\mathrm{NS}(S) \otimes \mathbb{Q}$ is represented by a $\mathbb{Q}$-linear combination of divisors. It follows from Cramer's rule that the denominator appearing in the coefficient of a component of $\pi^{-1}(v)$ divides d_v. In particular, the multiple $R_i = dQ_i$ has a lift $\tilde{R}_i$ to $\bar{L}^1\,\mathrm{NS}(S)$ (i.e., with *integral* coefficients) that is orthogonal to $\bar{L}^2\,\mathrm{NS}(S)$.

By the definition of the height pairing,

$$\langle R_i, R_j \rangle = -(\tilde{R}_i) \cdot (\tilde{R}_j)$$

where the dot on the right hand side signifies the intersection pairing on $\bar{L}^1\,\mathrm{NS}(S)$. It follows that

$$\mathrm{Disc}\left(\mathbb{Z}\tilde{R}_1 + \cdots + \mathbb{Z}\tilde{R}_m\right) = d^{2m} \det(\mathrm{MW}(J)/\mathrm{tor}),$$

since the $\tilde{R}_i$ map to a basis of $d \cdot (\mathrm{MW}(J)/\mathrm{tor})$. Now let N be the subgroup of $\bar{L}^1\,\mathrm{NS}(S)$ generated by the $\tilde{R}_i$ and by $\bar{L}^2\,\mathrm{NS}(S)$.

On the one hand, there is an orthogonal direct sum decomposition

$$N = \left(\mathbb{Z}\tilde{R}_1 + \cdots + \mathbb{Z}\tilde{R}_m\right) \oplus \bar{L}^2\,\mathrm{NS}(S)$$

and so

$$\mathrm{Disc}(N) = d^{2m+1}\det(\mathrm{MW}(J)/\mathrm{tor}).$$

Moreover, the assumption that π has a section implies that $L^2\,\mathrm{NS}(S)$ is torsion-free and that F is indivisible in $L^2\,\mathrm{NS}(S)$, and thus $\bar{L}^2\,\mathrm{NS}(S)$ and N are also torsion-free.

On the other hand, the index of N in $\bar{L}^1\,\mathrm{NS}(S)$ is $d^m|\,\mathrm{MW}(J)_{\mathrm{tor}}|$. It follows that

$$\frac{\mathrm{Disc}(\bar{L}^1\,\mathrm{NS}(S)/\mathrm{tor})}{|\bar{L}^1\,\mathrm{NS}(S)_{\mathrm{tor}}|^2} = \frac{\mathrm{Disc}(N/\mathrm{tor})}{d^{2m}|\,\mathrm{MW}(J)_{\mathrm{tor}}|^2|N_{\mathrm{tor}}|^2} = d\frac{\det(\mathrm{MW}(J)/\mathrm{tor})}{|\,\mathrm{MW}(J)_{\mathrm{tor}}|^2},$$

since N is torsion-free. Finally, if we note that

$$\bar{L}^1\,\mathrm{NS}(S)_{\mathrm{tor}} = L^1\,\mathrm{NS}(S)_{\mathrm{tor}} = \mathrm{NS}(S)_{\mathrm{tor}},$$

then we find that

$$\mathrm{Disc}(\bar{L}^1\,\mathrm{NS}(S)/\mathrm{tor}) = |\,\mathrm{NS}(S)_{\mathrm{tor}}|^2\left(\prod_v d_v\right)\frac{\det(\mathrm{MW}(J)/\mathrm{tor})}{|\,\mathrm{MW}(J)_{\mathrm{tor}}|^2}.$$

In particular, the left side is an integer since the intersection pairing on $\mathcal{S}$ is integer valued, and thus the right side is an integer as claimed. □

7.1.2. Proof of Theorem 7.1. We apply the integrality result Proposition 7.2 to $\mathcal{X}_d$ and J.

On the one hand, $\mathrm{NS}(\mathcal{X}_d)$ is torsion-free by Theorem 6.13. Moreover,

$$\prod_v d_v = d^{2r-2}r^{d+2}$$

by Proposition 3.7.

On the other hand, the $\mathbb{F}_q(u)/\mathbb{F}_q$-trace of J vanishes by Proposition 6.31, and thus $\mathrm{MW}(J) = J(\mathbb{F}_q(u))$. Moreover,

$$\frac{\det(J(\mathbb{F}_q(u))/\mathrm{tor})}{|J(\mathbb{F}_q(u))_{\mathrm{tor}}|^2} = [J(\mathbb{F}_q(u)) : V]^{-2}\frac{\det(V/\mathrm{tor})}{|V_{\mathrm{tor}}|^2}.$$

We also have

$$\frac{\det(V/\mathrm{tor})}{|V_{\mathrm{tor}}|^2} = (d-1)^{(r-1)(d-2)}r^{-d-2}d^{2-2r}.$$

by Corollaries 4.20 and 4.24.

Applying Proposition 7.2 gives that

$$\frac{(d-1)^{(r-1)(d-2)}}{[J(\mathbb{F}_q(u)) : V]^2}$$

is an integer. Since $d = p^\nu + 1$, this shows that the index is a power of p. By Corollary 6.1, $J(\mathbb{F}_q(u))$ has no p-torsion, so $J(\mathbb{F}_q(u))_{\mathrm{tor}} = V_{\mathrm{tor}}$. This completes the proof of the theorem. □

7.2. Tamagawa number

In this section we compute the Tamagawa number $\tau(J/\mathbb{F}_q(u))$ of the Jacobian J of C over $\mathbb{F}_q(u)$. First, we review the definition for a general abelian variety over a function field and show how to calculate τ in terms of more familiar invariants. Next, we specialize to the case of a Jacobian and relate τ to invariants of the curve. Finally, we specialize to the Jacobian J over $\mathbb{F}_q(u)$ studied in the rest of this paper.

7.2.1. Tamagawa numbers of abelian varieties over function fields. Let $\mathcal{B}$ be a curve of genus $g_{\mathcal{B}}$ over $k = \mathbb{F}_q$. Let $F = \mathbb{F}_q(\mathcal{B})$ be the function field of $\mathcal{B}$, and let $\mathbb{A}_F$ be the adèles of F. There is a natural measure $\mu = \prod \mu_v$ on $\mathbb{A}_F$ where μ_v is the Haar measure that assigns measure 1 to the ring of integers $\mathcal{O}_v$ in the completion F_v for each place v of F. The quotient $\mathbb{A}_F/F$ is compact and we set $D_F = \mu(\mathbb{A}_F/F)$. By [**59**, 2.1.3],

$$D_F = q^{g_{\mathcal{B}}-1}. \tag{7.1}$$

Let A be an abelian variety of dimension g over F and ω a top-degree differential on A. For each v, the differential ω induces a differential ω_v on the base change A_v of A to F_v. Using μ_v, this produces a measure $|\omega_v|\mu_v^g$ on $A_v(F_v)$. When the differential ω_v is a Néron differential, then Tate has shown (cf. [**45**, 1.4]) that

$$\int_{A_v(\mathcal{O}_v)} |\omega_v|\mu_v^g = \frac{\#\mathcal{A}(\mathbb{F}_v)}{q_v^g} \tag{7.2}$$

where $\mathbb{F}_v$ is the residue field at v, $q_v = q^{\deg(v)}$ is its cardinality, and $\#\mathcal{A}(\mathbb{F}_v)$ is the number of points on the special fiber of the Néron model of A. Thus if $\#\mathcal{A}(\mathbb{F}_v)^\circ$ is the number of points on the identity component of the special fiber of the Néron model of A and we set

$$\lambda_v = \frac{\#\mathcal{A}(\mathbb{F}_v)^\circ}{q_v^g}, \tag{7.3}$$

then $\{\lambda_v\}$ is a set of convergence factors in the sense of Weil [**59**, 2.3]. In this situation, we may form the product measure

$$\Omega = \Omega(F, \omega, (\lambda_v)) = D_F^{-g} \prod_v \lambda_v^{-1} |\omega_v|\mu_v^g.$$

By the product formula, Ω is independent of the choice of ω. Finally, we define the *Tamagawa number* $\tau(A/F)$ to be the measure of the set of $\mathbb{A}_F$ points of A with respect to Ω.

Since A is a projective variety, $A(\mathbb{A}_F) = \prod_v A(\mathcal{O}_v)$ and the measure can be computed as a product of local factors:

$$\tau(A/F) = D_F^{-g} \prod_v \lambda_v^{-1} \int_{A_v(\mathcal{O}_v)} |\omega_v|\mu_v^g.$$

Using (7.2) and (7.3), the local factor $\lambda_v^{-1} \int_{A_v(\mathcal{O}_v)} |\omega_v|\mu_v^g$ is equal to $q_v^{f_v} d_v$ where d_v is the order of the group of components on the Néron model at v and f_v is the integer such that $\pi_v^{f_v}\omega_v$ is a Néron differential at v. (Here π_v is a uniformiser at v.) Thus the product of local terms is

$$\prod_v q_v^{f_v} d_v = q^{\sum_v \deg(v) f_v} \prod_v d_v.$$

We want to write $\sum_v \deg(v) f_v$ as a global invariant. Let $\sigma : \mathcal{A} \to \mathcal{B}$ be the Néron model of A/L, let $z : \mathcal{B} \to \mathcal{A}$ be the zero section, and let

$$\omega = z^* \left(\bigwedge^{g_X} \Omega^1_{\mathcal{J}/\mathcal{B}} \right) = \bigwedge^{g_X} \left(z^* \Omega^1_{\mathcal{J}/\mathcal{B}} \right).$$

This is an invertible sheaf on $\mathcal{B}$ whose degree we denote $\deg \omega$. It is then clear from the definition above of f_v that $\sum_v \deg(v) f_v = -\deg \omega$. Combined with the local calculation in the preceding paragraph, this yields

$$\tau(A/F) = q^{g(1-g_{\mathcal{B}})-\deg(\omega)} \prod_v d_v. \tag{7.4}$$

7.2.2. Tamagawa numbers of Jacobians. Let $\mathcal{B}$ be a smooth, projective, geometrically irreducible curve of genus $g_{\mathcal{B}}$ over $k = \mathbb{F}_q$. Let $F = k(\mathcal{B})$ be its function field, and let X/F be a smooth, projective, and geometrically irreducible curve of genus g_X.

We give ourselves two sorts of models of X. First, let $\mathcal{S}'$ be a normal, projective, geometrically irreducible surface over $k = \mathbb{F}_q$ equipped with a surjective morphism $\pi' : \mathcal{S}' \to \mathcal{B}$ whose generic fiber is X/F. We assume that π' is smooth away from a finite set of points. We also assume that π' admits a section $s : \mathcal{B} \to \mathcal{S}'$ whose image lies in the smooth locus of $\mathcal{S}'$. Furthermore, assume that $\mathcal{S}'$ has at worst rational double point singularities (cf. [**3**, Ch. 3]). Note that the singularities of $\mathcal{S}'$ lie in the singularities of π', since $\mathcal{B}$ is smooth.

Second, let $\sigma : \mathcal{S} \to \mathcal{S}'$ be a minimal resolution of singularities, so that the composition $\pi = \pi' \circ \sigma : \mathcal{S} \to \mathcal{S}' \to \mathcal{B}$ is a minimal regular model of X/F. In the applications, $\mathcal{S}'$ is the model $\mathcal{Y}$ constructed in Chapter 3 and $\mathcal{S}$ is $\mathcal{X}$.

Now let A/F be the Jacobian of X/F, and let $\tau : \mathcal{A} \to \mathcal{B}$ be the Néron model of A/F, with zero section $z : \mathcal{B} \to \mathcal{A}$. Our goal in this subsection is to describe the invariants entering into the Tamagawa number of A in terms of the surfaces $\mathcal{S}$ or $\mathcal{S}'$.

We first consider the local term d_v, the order of the group of connected components of the fiber of the Néron model at v. The next proposition is not strictly necessary for our purposes (because we were able to determine the d_v from examples treated in [**6**, Section 9.6]), but we include it for completeness.

Let $X_0, \ldots, X_n$ be the reduced irreducible components of $\pi^{-1}(v)$. We number them so that the section s passes through X_0. Let M be the $n \times n$ matrix of intersection numbers:

$$M_{i,j} = (X_i \cdot X_j), \qquad 1 \leq i, j \leq n.$$

(Note that we do not include intersections with X_0.)

PROPOSITION 7.3. *$d_v = \det M$.*

PROOF. This follows from [**6**, Theorem 9.6.1]. Indeed, let $I = \{0, \ldots, n\}$, and for $i \in I$, let δ_i be the multiplicity of X_i in $\pi^{-1}(v)$ and e_i the geometric multiplicity of X_i. (These integers are defined more precisely in [**6**, Definition 9.1.3].) Since the section s passes through X_0, we have $\delta_0 = 1$. Since the residue field $\mathbb{F}_v$ is a finite extension of $\mathbb{F}_q$, and is therefore perfect, we have $e_i = 1$ for all i. (A reduced scheme over $\mathbb{F}_v$ remains reduced after base change to the algebraic closure of $\mathbb{F}_v$.)

Let $\mathbb{Z}^I$ be the free abelian group on I. Let $\beta : \mathbb{Z}^I \to \mathbb{Z}$ be given by $\beta(a_0, \dots, a_n) = \sum a_i \delta_i$, and let $\alpha : \mathbb{Z}^I \to \mathbb{Z}^I$ be given by the intersection matrix

$$\left(e_i^{-1}(X_i \cdot X_j)\right)_{i,j \in I} = (X_i \cdot X_j)_{i,j \in I}\,.$$

Then [**6**, Theorem 9.6.1] says that the group of connected components of $\mathcal{A}$ at v is canonically isomorphic to $\ker\beta/\operatorname{im}\alpha$. Because $\delta_0 = 1$, we may identify $\ker\beta$ with the free abelian group on $X_1, \dots, X_n$, and the result then follows immediately from the definition of M. □

Next we turn to the global invariant $\deg(\omega)$.

PROPOSITION 7.4. *Let $\mathcal{S}^o \subset \mathcal{S}'$ be the smooth locus, and let $\pi^o : \mathcal{S}^o \to \mathcal{B}$ the restriction of π' to $\mathcal{S}^o$. Then there is an isomorphism*

$$z^*\Omega^1_{\mathcal{A}/\mathcal{B}} \cong \pi^o_*\Omega^1_{\mathcal{S}^o/\mathcal{B}}.$$

In particular,

$$\omega \cong \bigwedge^{g_X} \left(\pi^o_*\Omega^1_{\mathcal{S}^o/\mathcal{B}}\right).$$

PROOF. Let $\underline{\mathrm{Lie}}(G) \to \mathcal{B}$ be the Lie algebra of a group scheme $G \to \mathcal{B}$ (see [**12**, II.2]). By [**6**, 9.7/1], the Néron model $\mathcal{A} \to \mathcal{B}$ represents the relative Picard functor $\mathrm{Pic}^0_{\mathcal{S}/\mathcal{B}}$ since $\mathcal{S}$ is smooth and π admits a section. Therefore

$$(z^*\Omega^1_{\mathcal{A}/\mathcal{B}})^\vee \cong \underline{\mathrm{Lie}}(\mathcal{A}/\mathcal{B}) \cong \underline{\mathrm{Lie}}(\mathrm{Pic}^0(\mathcal{S}/\mathcal{B})) \cong \underline{\mathrm{Lie}}(\mathrm{Pic}(\mathcal{S}/\mathcal{B})) \cong R^1\pi_*\mathcal{O}_{\mathcal{S}}$$

by [**28**, 1.1 and 1.3].

By [**23**, Corollary 24] (with $X = \mathcal{S}$, $Y = \mathcal{B}$, and $S = \operatorname{Spec} k$), the relative dualizing sheaf $\omega_{\mathcal{S}/\mathcal{B}}$ exists and satisfies

$$(R^1\pi_*\mathcal{O}_{\mathcal{S}})^\vee \cong \pi_*\omega_{\mathcal{S}/\mathcal{B}}$$

and

$$\omega_{\mathcal{S}/\mathcal{B}} \cong \Omega^2_{\mathcal{S}/k} \otimes \pi^*(\Omega^1_{\mathcal{B}/k})^\vee.$$

Combining these facts and using the projection formula, we have

$$z^*\Omega^1_{\mathcal{A}/\mathcal{B}} \cong \pi_*\Omega^2_{\mathcal{S}/k} \otimes (\Omega^1_{\mathcal{B}/k})^\vee.$$

To finish the proof, we show that

$$\pi_*\Omega^2_{\mathcal{S}/k} \cong \pi^o_*\Omega^1_{\mathcal{S}^o/\mathcal{B}} \otimes \Omega^1_{\mathcal{B}/k}.$$

To that end, let $\omega_{\mathcal{S}/k}$, $\omega_{\mathcal{S}'/k}$, and $\omega_{\mathcal{S}^o/k}$ be the dualizing sheaves of $\mathcal{S}$, $\mathcal{S}'$, and $\mathcal{S}^o$ respectively. Since these surfaces have at worst rational double points, their dualizing sheaves are invertible [**3**, §3.11, Corollary 4.19], and since $\mathcal{S}$ and $\mathcal{S}^o$ are smooth, $\omega_{\mathcal{S}/k} \cong \Omega^2_{\mathcal{S}/k}$ and $\omega_{\mathcal{S}^o/k} \cong \Omega^2_{\mathcal{S}^o/k} \cong \omega_{\mathcal{S}'/k}|_{\mathcal{S}^o}$. Moreover, by [**3**, Corollary 4.19], $\sigma_*\omega_{\mathcal{S}} \cong \omega_{\mathcal{S}'}$. Thus

$$\pi_*\Omega^2_{\mathcal{S}/k} \cong \pi'_*\omega_{\mathcal{S}'} \cong \pi^o_*\Omega^2_{\mathcal{S}^o/k}$$

where the second isomorphism holds because the complement of $\mathcal{S}^o$ in $\mathcal{S}'$ has codimension 2. Finally, since $\pi^o : \mathcal{S}^o \to \mathcal{B}$ is smooth, there is an exact sequence of locally free sheaves

$$0 \to \pi^{o*}\Omega^1_{\mathcal{B}/k} \to \Omega^1_{\mathcal{S}^o/k} \to \Omega^1_{\mathcal{S}^o/\mathcal{B}} \to 0,$$

and so, taking the second exterior power,

$$\Omega^2_{\mathcal{S}^o/k} \cong \pi^{o*}\Omega^1_{\mathcal{B}/k} \otimes \Omega^1_{\mathcal{S}^o/\mathcal{B}}.$$

□

7.2.3. The Tamagawa number of J. We now specialize to the Jacobian J that is the subject of this paper. The main result of this section is the following calculation of the Tamagawa number of J.

PROPOSITION 7.5. *If r divides d and if d divides $q-1$, then*

$$\tau(J/\mathbb{F}_q(u)) = q^{-(d-2)(r-1)/2} d^{2r-2} r^{d+2}.$$

The proof occupies the rest of this subsection.

Suppose that r divides d and that d divides $q-1$. Recall that in Section 3.1.1 we constructed proper models $\pi' : \mathcal{Y} \to \mathcal{B}$ and $\pi : \mathcal{X} \to \mathcal{B}$ of $C/\mathbb{F}_q(u)$ over $\mathcal{B} = \mathbb{P}^1_u$, i.e., schemes with proper morphisms to $\mathcal{B}$ whose generic fibers are C. The models $\mathcal{X} \to \mathcal{B}$ and $\mathcal{Y} \to \mathcal{B}$ have the properties required of $\mathcal{S}$ and $\mathcal{S}'$ in the preceding section, so Propositions 7.3 and 7.4 apply.

However, rather than applying Proposition 7.3, we simply refer to Proposition 3.7 to obtain:

$$\prod_v d_v = (rd^{r-1})^2 r^d = d^{2r-2} r^{d+2}.$$

To finish the proof, we must compute $q^{g_C(1-g_{\mathcal{B}})-\deg(\omega)} = q^{r-1-\deg(\omega)}$.

Recall from Lemma 6.7 the relative 1-forms ω_i which form a basis of the R-module $H^0(U, \pi'_* \Omega^1_{\mathcal{Y}/\mathcal{B}})$.

LEMMA 7.6. *Each ω_i extends to a section in $H^0(\mathcal{B}, \pi_* \Omega^1_{\mathcal{Y}/\mathcal{B}})$ that has order of vanishing di/r at $u = \infty$ and is non-vanishing everywhere else.*

PROOF. The proof of Lemma 6.6 shows that ω_i extends to a nowhere vanishing section of $\pi_* \Omega^1_{\mathcal{Y}/\mathcal{B}}$ over $\mathcal{B} \smallsetminus \{\infty\}$. There is an involution

$$(x, y, u) \mapsto (x/u^d, y/u^{d(r+1)/r}, 1/u),$$

since r divides d. The pullback of $x^{i-1}dx/y^i$ via this involution is $u^{di/r} x^{i-1} dx/y^i$ and thus it takes the non-zero regular 1-form of $\mathcal{Y}_0$ to a regular 1-form on $\mathcal{Y}_\infty$ with order of vanishing di/r. □

Clearly the sections $\omega_i \in H^0(\mathcal{B}, \pi_* \Omega^1_{\mathcal{Y}/\mathcal{B}})$ restrict to elements of $H^0(\mathcal{B}, \pi^o_* \Omega^1_{\mathcal{Y}^o/\mathcal{B}})$ where $\mathcal{Y}^o$ is the complement in $\mathcal{Y}$ of the finitely many singularities of $\mathcal{Y} \to \mathcal{B}$ (which, since $d > 1$, also happen to be the finitely many singular points of $\mathcal{Y}$, see Proposition 3.1).

We conclude that

$$\omega_1 \wedge \cdots \wedge \omega_{r-1}$$

yields a global section of $\wedge^{r-1} \pi^o_* \Omega^1_{\mathcal{Y}^o/\mathcal{B}}$. Moreover, the proof of Lemma 6.7 shows that the ω_i are linearly independent on each fiber of $\mathcal{Y} \to \mathcal{B}$ where u is finite, and over $u = \infty$, the sections $u^{di/r}\omega_i$ are (non-vanishing and) linearly independent. It follows that $\omega_1 \wedge \cdots \wedge \omega_{r-1}$ is everywhere regular, non-vanishing away from $u = \infty$, and has a zero of order

$$\sum_{i=1}^{r-1} \frac{di}{r} = \frac{d(r-1)}{2}$$

at $u = \infty$. We conclude that $\deg(\omega) = d(r-1)/2$ and

$$\tau(J/K) = q^{(r-1)-d(r-1)/2} \prod_v d_v = q^{-(d-2)(r-1)/2} d^{2r-2} r^{d+2},$$

as desired. This completes the proof of Proposition 7.5. □

7.3. Application of the BSD formula

We saw in Theorem 5.2 that the Birch and Swinnerton-Dyer conjecture holds for $J/\mathbb{F}_q(u)$. Moreover, under the assumptions that r divides d, that $d = p^\nu + 1$, and that d divides $q-1$, we have calculated most of the terms appearing in the leading coefficient formula of this conjecture. Synthesizing this leads to a beautiful analytic class number formula relating the Tate-Shafarevich group $Ш(J/\mathbb{F}_q(u))$ and the index $[J(\mathbb{F}_q(u)) : V]$.

Before deriving this result, we compare the formulation of the BSD conjecture in Theorem 5.2 to that in **[22]**.

7.3.1. Two variants of the refined BSD conjecture. At the time that Tate stated the BSD conjecture in its most general form in **[45]**, there was uncertainty as to the right local factors of the L-function at places of bad reduction. Tate therefore used the Tamagawa principle to state the leading coefficient part of the BSD conjecture. The correct local factors were defined later by Serre in **[38]**, and using them we formulate the leading coefficient conjecture (as Theorem 5.2) in what we feel is its most natural form. However, the best reference for the proof of the leading coefficient conjecture, namely **[22]**, uses Tate's formulation. In this subsection, we compare the two formulations and show that they are equivalent for Jacobians of curves with a rational point.

To that end, let F be the function field of a curve over $\mathbb{F}_q$, let Y/F be a smooth projective curve of genus g with an F-rational point, and let A be the Jacobian of Y. Define local L-factors for each place v of F by

$$L_v(q_v^{-s}) := \det\left(1 - \mathrm{Fr}_v \; q_v^{-s} \,\middle|\, H^1(A \times \overline{F}, \mathbb{Q}_\ell)^{I_v}\right).$$

Let $\mu = \prod \mu_v$ and D_L be as in Section 7.2. Choose a top-degree differential ω on A and form the local integrals

$$\int_{A(F_v)} |\omega_v| \mu_v^g$$

and the convergence factors

$$\lambda_v := \frac{\#\mathcal{A}_v(\mathbb{F}_v)^0}{q_v^g}$$

as in Section 7.2. Finally, choose a finite set S of places of F containing all places where Y has bad reduction.

Tate's formulation of the leading term conjecture is that the leading term as $s \to 1$ of

$$\frac{D_F^g}{\left(\prod_{v\in S} \int_{A(F_v)} |\omega_v| \mu_v^g\right)\left(\prod_{v \notin S} L_v(q_v^{-s})\right)}$$

is $|Ш(A/F)|R/|A(F)_{tor}|^2$. On the other hand, our formulation asserts that the latter quantity (i.e., $|Ш(A/F)|R/|A(F)_{tor}|^2$) is the leading coefficient as $s \to 1$ of

$$\frac{L(A/F, s)}{\tau(A/F)} = \left(\prod_v L_v(q_v^{-s})^{-1}\right) D_F^g \left(\prod_v \frac{\lambda_v}{\int_{A(F_v)} |\omega_v| \mu_v^g}\right)$$

where both products are over all places of F. The factor on the right is 1 if $v \notin S$, so to see that the two formulations are equivalent, it will suffice to show that

$$L_v(q_v^{-1}) = \lambda_v$$

for all $v \in S$.

In fact this equality holds for all v. Indeed, [**29**, Lemma, page 182] implies that $L_v(q_v^{-1})$ is equal to $\#\mathrm{Pic}^0(Y_v)/q_v^g$ where Y_v is the fiber at v of a regular minimal model of Y. But as we noted in the proof of Proposition 5.1, the assumption that Y has a rational point implies that $\mathrm{Pic}^0(Y_v)$ is the group of $\mathbb{F}_v$ rational points on $\mathcal{A}_v^0$, the identity component of the Néron model of A at v. Thus

$$L_v(q_v^{-1}) = \frac{\#\mathrm{Pic}^0(Y_v)}{q_v^g} = \frac{\#\mathcal{A}_v^0(\mathbb{F}_v)}{q_v^g} = \lambda_v.$$

This completes the verification that the two formulations of the BSD conjecture are equivalent.

7.3.2. An analytic class number formula. Now we turn to the application of the BSD conjecture to a formula for the order of $Ш(J/\mathbb{F}_q(u))$.

THEOREM 7.7. *Assume that r divides d, that $d = p^\nu + 1$, and that d divides $q-1$. Then the Tate-Shafarevich group $Ш(J/\mathbb{F}_q(u))$ has order*

$$|Ш(J/\mathbb{F}_q(u))| = [J(\mathbb{F}_q(u)) : V]^2 \left(\frac{q}{p^{2\nu}}\right)^{(r-1)(d-2)/2}.$$

In particular, its order is a power of p. In the special case $\mathbb{F}_q(u) = K_d$, then

$$|Ш(J/K_d)| = [J(K_d) : V]^2.$$

PROOF. By Corollary 5.7 the leading coefficient of the L-function is

$$L^*(J/\mathbb{F}_q(u), 1) = (\log q)^{(r-1)(d-2)}.$$

Taking into account the factor of $\log q$ relating the $\mathbb{Q}$-valued height pairing of Chapter 4 and the Néron-Tate canonical height, the BSD formula for the leading coefficient says

$$1 = \frac{|Ш(J/\mathbb{F}_q(u))|\ \det(J(\mathbb{F}_q(u))/\mathrm{tor})\,\tau(J/\mathbb{F}_q(u))}{|J(\mathbb{F}_q(u)))_{\mathrm{tor}}|^2}.$$

Using that

$$\det(J(\mathbb{F}_q(u))/\mathrm{tor}) = \frac{\det(V/\mathrm{tor})}{[J(\mathbb{F}_q(u)) : V]^2}$$

and our calculations

$$\det(V/\mathrm{tor}) = (d-1)^{(r-1)(d-2)} r^{4-d} d^{2-2r}$$

(Corollary 4.24),

$$\tau(J/\mathbb{F}_q(u)) = q^{-(d-2)(r-1)/2} d^{2r-2} r^{d+2}$$

(Proposition 7.5), and

$$|J(\mathbb{F}_q(u))_{\mathrm{tor}}| = r^3$$

(Theorem 7.1), we find

$$|Ш(J/\mathbb{F}_q(u))| = [J(\mathbb{F}_q(u)) : V]^2 \left(\frac{q}{p^{2\nu}}\right)^{(r-1)(d-2)/2},$$

as desired.

We showed in Theorem 7.1 that $[J(\mathbb{F}_q(u)) : V]$ is a power of p, so the same is true of $|Ш(J/\mathbb{F}_q(u))|$.

The assertion for the special case $\mathbb{F}_q(u) = K_d$ follows from the fact that the field of constants of K_d is $\mathbb{F}_p(\mu_d) = \mathbb{F}_{p^{2\nu}}$. □

REMARK 7.8. Under the hypotheses of this section, it is possible to describe $Ш(J/\mathbb{F}_q(u))$ and $J(\mathbb{F}_q(u))/V$ as modules over the group ring $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{F}_q(u)/\mathbb{F}_p(t))]$ in terms of the combinatorics of the action by multiplication of the cyclic group $\langle p \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ on the set $\mathbb{Z}/d\mathbb{Z} \times \mu_r$. See [**53**, Section 9.4] for details.

CHAPTER 8

Monodromy of ℓ-torsion and decomposition of the Jacobian

In this chapter, we consider the action of Galois on torsion points of the Jacobian J and use the results to understand the decomposition of J up to isogeny into a sum of simple abelian varieties. Our results depend heavily on knowledge of the regular proper model $\mathcal{X} \to \mathbb{P}^1$ constructed in Chapter 3. Interested readers are referred to **[18]**, where a general technique for computing monodromy groups of certain superelliptic curves is developed. The methods of **[18]** yield results similar to those in this chapter in a more general context without the need to construct regular models.

8.1. Statement of results

Let k be an algebraically closed field of characteristic $p \geq 0$, let $r \geq 2$ be an integer not divisible by p, and let ℓ be a prime satisfying $\ell \neq p$ and $\ell \nmid r$. As in the rest of this paper, let $C = C_r$ be the smooth, projective curve over $K = k(t)$ birational to the affine curve given by

$$y^r = x^{r-1}(x+1)(x+t), \tag{8.1}$$

let J be its Jacobian, and let $J[\ell]$ be the Galois module of ℓ-torsion.

In this chapter, we study the structure of a monodromy group, namely the Galois group of $K(J[\ell])$ over K. We use the results about the monodromy group to bound ℓ-torsion over solvable extensions of K and to determine how J decomposes up to isogeny into a sum of simple abelian varieties, both over K and over $\overline{K}$.

We first state the consequences of the monodromy result that motivated its study, then discuss the monodromy result itself.

THEOREM 8.1. *If L/K is an abelian extension, then $J[\ell](L) = \{0\}$. If $\ell > 3$ or r is odd, then the same holds for any solvable extension L/K.*

In the following section we define the "new part" of J, denoted J_r^{new}, and we show that there is an isogeny

$$\bigoplus_{s|r} J_s^{new} \longrightarrow J \tag{8.2}$$

over K, where the sum runs over positive divisors s of r and J_s^{new} is the new part of the Jacobian of C_s. It turns out that $J_1^{new} = J_1 = 0$ and that J_s^{new} has dimension $\phi(s)$ where $\phi(s)$ is the cardinality of $(\mathbb{Z}/s\mathbb{Z})^\times$ when $s > 1$. Moreover, the action of μ_r on C_r induces an action of the ring of integers $\mathbb{Z}[\zeta_r] \subset \mathbb{Q}(\zeta_r)$ on J_r^{new}. Our second main result says that J_r^{new} does not decompose further over certain extensions of K:

THEOREM 8.2. *The new part J_r^{new} is simple over K, and $\mathrm{End}_K(J_r^{new}) \cong \mathbb{Z}[\zeta_r]$. The same conclusions hold over $K(u)$ where $u^d = t$ for any positive integer d not divisible by p.*

If $r = 2$, J_r^{new} is an elliptic curve, so is obviously absolutely simple. Moreover, it is non-isotrivial, so $\mathrm{End}_{\overline{K}}(J_r^{new}) = \mathbb{Z}$. For $r > 2$, although J_r^{new} is simple over many extensions of K, we see below it is not absolutely simple.

Write $\mathbb{Z}[\zeta_r]^+ = \mathbb{Z}[\zeta_r + \zeta_r^{-1}]$ for the ring of integers in the real cyclotomic field $\mathbb{Q}(\zeta_r)^+$.

THEOREM 8.3. *Suppose that $r > 2$, and let $K' = K((1-t)^{1/r})$. Then there is an abelian variety B defined over K such that:*

1. *There is an isogeny $J_r^{new} \to B^2$ defined over K' whose kernel is killed by multiplication by $2r$.*
2. *$\mathrm{End}_K(B) = \mathrm{End}_{\overline{K}}(B) = \mathbb{Z}[\zeta_r]^+$, and B is absolutely simple.*

In particular, $\mathrm{End}_{\overline{K}}(J_r^{new})$ is isomorphic to an order in $M_2(\mathbb{Z}[\zeta_r]^+)$.

In Section 8.5.2 below, we introduce a twist C_χ of C (closely related to the extension K'/K) with Jacobian J_χ and new part $A_\chi := J_\chi^{new}$. The curve C_χ has an involution σ that allows us to show that A_χ is isogenous to $B \times B$ over K. Since A_χ becomes isomorphic to J_r^{new} over K', this explains the factorization in Theorem 8.3.

The theorems above are applications of results on the monodromy groups of $J[\ell]$ and $J_\chi[\ell]$, in other words on the image of the natural homomorphisms from $\mathrm{Gal}(K^{sep}/K)$ to $\mathrm{Aut}_{\mathbb{F}_\ell}(J[\ell])$ and $\mathrm{Aut}_{\mathbb{F}_\ell}(J_\chi[\ell])$. Our detailed knowledge of the regular proper model $\mathcal{X} \to \mathbb{P}^1$ of C and of the Néron model of J (in Chapter 3) together with some group theory allow us to determine the monodromy groups.

To define the group-theoretic structure of the monodromy group, consider $\Lambda = \mathbb{F}_\ell[z]/(z^{r-1} + \cdots + 1)$, which is a quotient of the group ring of μ_r over $\mathbb{F}_\ell$. The torsion points $J[\ell]$ and $J_\chi[\ell]$ have natural structures of free, rank 2 modules over Λ, and $J_\chi[\ell]$ admits an action of σ that "anti-commutes" with the μ_r action. We ultimately find that for $\ell > 3$, the monodromy group of $J_\chi[\ell]$ is

$$\mathrm{SL}_2(\Lambda^+) \subset \mathrm{GL}_2(\Lambda)$$

where Λ^+ is the subring of Λ generated by $\zeta + \zeta^{-1}$ and ζ is the class of z in Λ. This is very natural, because $\mathrm{SL}_2(\Lambda^+)$ is the commutator subgroup of the centralizer in $\mathrm{GL}_2(\Lambda)$ of the semi-direct product $\mu_r \rtimes \langle\sigma\rangle$. The results of **[18]** extend this conclusion to a broad class of superelliptic Jacobians.

8.2. New and old

In this section, we establish the decomposition of J into new and old parts, leading to the isogeny (8.2).

It is convenient to work with coordinates on C different than those in (8.1). Namely, for s a positive divisor of r, let C_s be the smooth, projective curve birational to the affine curve

$$x_s y_s^s = (x_s + 1)(x_s + t). \tag{8.3}$$

(For $s = r$, the coordinates here are related to those in (8.1) by $(x, y) = (x_r, x_r y_r)$.) For positive divisors s and s' of r with s' dividing s, there is a morphism $\pi_{s,s'} : C_s \to C_{s'}$ defined by $\pi_{s,s'} : (x_s, y_s) \mapsto (x_{s'}, y_{s'}) = (x_s, y_s^{s/s'})$.

Let J_s be the Jacobian of C_s; it is a principally polarized abelian variety of dimension $s-1$. By Albanese functoriality (push forward of divisors), $\pi_{s,s'}$ induces a map $J_s \to J_{s'}$, which we denote again by $\pi_{s,s'}$. Picard functoriality (pull back of divisors) induces another map $\pi_{s,s'}^* : J_{s'} \to J_s$. Considering $\pi_{s,s'}$ and $\pi_{s,s'}^*$ at the level of divisors shows that the endomorphism $\pi_{s,s'} \circ \pi_{s,s'}^*$ of $J_{s'}$ is multiplication by s/s'.

The group $\mu_r \subset k^\times$ acts on C_r by $\zeta_r(x_r, y_r) = (x_r, \zeta_r y_r)$. We let μ_r act on C_s via the quotient map $\mu_r \to \mu_s$, so that $\zeta_r(x_s, y_s) = (x_s, \zeta_r^{r/s} y_s)$. With these definitions, the induced maps $\pi_{s,s'} : J_s \to J_{s'}$ and $\pi_{s,s'}^* : J_{s'} \to J_s$ are equivariant for the μ_r actions.

Let R be the group ring $\mathbb{Z}[\mu_r]$. (This agrees with the definition of R in Section 1.2.3 since $d = 1$.) Then $\pi_{s,s'}$ and $\pi_{s,s'}^*$ are homomorphisms of R-modules.

Now we define J_s^{new} as the identity component of the intersection of the kernels of $\pi_{s,s'}$ where s' runs through positive divisors of s strictly less than s:

$$J_s^{new} := \left(\bigcap_{s'<s} \ker\left(\pi_{s,s'} : J_s \to J_{s'}\right) \right)^0 .$$

Note that J_s^{new} is preserved by the action of μ_r on J_s.

The main result of this section is a decomposition of J_r up to isogeny.

PROPOSITION 8.4. *For $s > 1$, the dimension of J_s^{new} is $\phi(s)$ and $J_1^{new} = J_1 = 0$. The homomorphism*

$$\begin{aligned} \bigoplus_{s|r} J_s^{new} &\to J \\ (z_s) &\mapsto \sum_{s|r} \pi_{r,s}^*(z_s) \end{aligned}$$

is an isogeny whose kernel is killed by multiplication by r.

PROOF. The cotangent space at the origin of J_s is canonically isomorphic to the space of 1-forms $H^0(C_s, \Omega^1_{C_s/k})$, so we may compute the differential of $\pi_{s,s'}^* : J_{s'} \to J_s$ by examining its effect on 1-forms.

We computed the space of 1-forms on C_s in the proof of Lemma 6.7. In terms of the coordinates used here, $H^0(C_s, \Omega^1_{C_s/k})$ has a basis consisting of eigenforms for the action of μ_r, namely $\omega_{s,i} = y_s^{-i} dx_s/x_s$ for $i = 1, \ldots, s-1$. It is then evident that $\pi_{s,s'}^*$ induces the inclusion on 1-forms

$$H^0(C_{s'}, \Omega^1_{C_{s'}/k}) \hookrightarrow H^0(C_s, \Omega^1_{C_s/k})$$

that sends $\omega_{s',i}$ to $\omega_{s,(s/s')i}$.

It follows that the cotangent space of J_s^{new} is spanned by the 1-forms $\omega_{s,i}$ where i is relatively prime to s. In particular, for $s > 1$, the dimension of J_s^{new} is $\phi(s)$. For $s = 1$, C_s has genus 0, so $J_1^{new} = J_1 = 0$.

It is also clear that the map displayed in the statement of the proposition induces an isomorphism on the cotangent spaces, so it is a separable isogeny. It remains to prove that the kernel is killed by r.

Write r as a product of primes $r = \ell_1 \cdots \ell_m$. We proceed by induction on m. If $r = \ell_1$ is prime, the result is obvious, since $J_1 = 0$ and $J_{\ell_1}^{new} = J_{\ell_1}$.

Before giving the proof for general r, we note that if ℓ_1 divides r, considering the action of the maps $\pi_{s,s'}$ on divisors yields the formula:

$$\pi_{r,r/\ell_1} \circ \pi_{r,s}^* = \begin{cases} \ell \pi_{r/\ell_1,s} & \text{if } s \text{ divides } r/\ell_1, \\ \pi_{r/\ell_1,s/\ell_1}^* \circ \pi_{s,s/\ell_1} & \text{otherwise.} \end{cases} \tag{8.4}$$

Now suppose that $(z_s)_{s|r}$ is in the kernel, i.e.,

$$0 = \sum_{s|r} \pi_{r,s}^*(z_s)$$

in J_r. Applying $\pi_{r,r/\ell_1}$ and using the formula (8.4), we have

$$\begin{aligned} 0 &= \sum_{s|r} \pi_{r,r/\ell_1} \pi_{r,s}^*(z_s) \\ &= \ell_1 \sum_{s|(r/\ell_1)} \pi_{r/\ell_1,s}(z_s) + \sum_{s\nmid(r/\ell_1)} \pi_{r/\ell_1,s/\ell_1}^* \pi_{s,s/\ell_1}(z_s) \\ &= \ell_1 \sum_{s|(r/\ell_1)} \pi_{r/\ell_1,s}(z_s) \end{aligned}$$

where the last equality holds because z_s is in J_s^{new}, so is killed by $\pi_{s,s/\ell_1}$. By induction, each $\ell_1 z_s$ is killed by r/ℓ_1, so each z_s with $s|(r/\ell_1)$ is r-torsion. Repeating the argument with ℓ_1 replaced by the other ℓ_i implies that all the z_s with $s < r$ are r-torsion. Finally, the equality $0 = \sum_{s|r} \pi_{r,s}^*(z_s)$ in J_r implies that z_r is r-torsion as well. □

Remarks 8.5.

(1) We used that $J_1 = 0$, but this is not necessary. A slight variant of the argument works for the new part of any cyclic cover $C_r \to C_1$ even when C_1 is not assumed to be rational.

(2) Temporarily write $J_r^{new,sub}$ for J_r^{new} as defined above. We could also consider a new quotient:

$$J_r^{new,quot} = \frac{J_r}{\sum_{s<r} \pi_{r,s}^* J_s}.$$

Arguments similar to those in the proof above show that the natural map $J_r^{new,sub} \to J_r \to J_r^{new,quot}$ is an isogeny whose kernel is killed by r.

Corollary 8.6. *Suppose that ℓ is a prime not dividing r. Then there is an isomorphism of $\mathbb{F}_\ell$-vector spaces*

$$\bigoplus_{s|r} J_s^{new}[\ell] \cong J_r[\ell]$$

compatible with the action of μ_r and the action of the Galois group $\mathrm{Gal}(K^{sep}/K)$.

Proof. The isomorphism is immediate from Proposition 8.4, since ℓ does not divide r. □

8.3. Endomorphism rings

In this section we define a ring Λ that acts naturally on $J[\ell]$ and record some auxiliary results about it. As always, $r > 1$ is an integer and ℓ is a prime not dividing r.

8.3.1. Definition of Λ. For each positive divisor s of r, let $\Phi_s(z)$ be the s-th cyclotomic polynomial, and let $\Psi_s(z) = z^{s-1} + \cdots + 1$. Then

$$\prod_{s|r} \Phi_s(z) = z^r - 1 \quad \text{and} \quad \prod_{1<s|r} \Phi_s(z) = \Psi_r(z).$$

Consider the group ring of μ_r over $\mathbb{F}_\ell$:

$$\mathbb{F}_\ell[\mu_r] \cong \frac{\mathbb{F}_\ell[z]}{(z^r - 1)}$$

and its quotient

$$\Lambda := \frac{\mathbb{F}_\ell[z]}{(\Psi_r(z))} = \frac{\mathbb{F}_\ell[z]}{(z^{r-1} + \cdots + 1)}.$$

We often write ζ for the class of z in $\mathbb{F}_\ell[\mu_r]$ or Λ.

Since ℓ does not divide r, the r-th roots of unity are distinct in $\overline{\mathbb{F}}_\ell$, so the polynomials Φ_s are pairwise relatively prime in $\mathbb{F}_\ell[z]$. By the Chinese Remainder Theorem,

$$\Lambda = \frac{\mathbb{F}_\ell[z]}{(\Psi_r(z))} \cong \prod_{1<s|r} \frac{\mathbb{F}_\ell[z]}{(\Phi_s(z))}$$

and

$$\mathbb{F}_\ell[\mu_r] \cong \mathbb{F}_\ell \oplus \Lambda$$

where $(1 + \zeta + \cdots + \zeta^{r-1})/r$ on the left corresponds to $(1, 0)$ on the right.

Note that $\mathcal{O}_s := \mathbb{Z}[z]/(\Phi_s(z))$ is isomorphic to the ring of integers $\mathbb{Z}[\zeta_s]$ in the cyclotomic field $\mathbb{Q}(\zeta_s)$ and that $\mathcal{O}_s/\ell \cong \mathbb{F}_\ell[z]/(\Phi_s(z))$. Therefore

$$\Lambda \cong \prod_{1<s|r} \mathcal{O}_s/\ell,$$

and ζ on the left maps to an s-th root of unity ζ_s in the factor $\mathcal{O}_s/\ell$ on the right, justifying the notational use of ζ on the left. This isomorphism is convenient as it allows us to use certain well-known results from the theory of cyclotomic fields.

8.3.2. The subring Λ^+. Consider the involution of $\mathbb{F}_\ell[\mu_r]$ that sends ζ to ζ^{-1}. We write $\mathbb{F}_\ell[\mu_r]^+$ for the subring of invariant elements. The factors in the decomposition $\mathbb{F}_\ell[\mu_r] \cong \mathbb{F}_\ell \oplus \Lambda$ are preserved by the involution, and we write Λ^+ for the invariant subring $\mathbb{F}_\ell[\mu_r]^+ \cap \Lambda$.

LEMMA 8.7.

(1) *Λ^+ is the subring of Λ generated by $\zeta + \zeta^{-1}$.*
(2) *Let $\mathcal{O}_s^+$ be the ring of integers in the real cyclotomic field $\mathbb{Q}(\zeta_s + \zeta_s^{-1})$. Then*

$$\Lambda^+ \cong \prod_{1<s|r} \mathcal{O}_s^+/\ell.$$

PROOF. (1) The group ring $\mathbb{F}_\ell[\mu_r]$ has $\mathbb{F}_\ell$-basis $1, \zeta, \ldots, \zeta^{r-1}$, and Λ is the quotient by the line generated by $1 + \cdots + \zeta^{r-1}$. Let $\tau_i = \zeta^i + \zeta^{-i}$. If r is odd, it is clear that $\mathbb{F}_\ell[\mu_r]^+$ has basis $1, \tau_1, \ldots, \tau_{(r-1)/2}$. If r is even, a basis of $\mathbb{F}_\ell[\mu_r]^+$ is given by $1, \tau_1, \ldots, \tau_{(r-2)/2}, \zeta^{r/2}$. Since $\ell \neq 2$ when r is even, $\tau_{r/2} = 2\zeta^{r/2}$ and another basis is $1, \tau_1, \ldots, \tau_{r/2}$. Projecting to Λ, we see that $1, \ldots, \tau_u$ is a basis of Λ^+, where u is $(r-3)/2$ or $(r-2)/2$ as r is odd or even. Since $\tau_1^i = \tau_i$ plus a linear combination of 1 and the τ_j with $j < i$, it follows that Λ^+ is generated as a ring by τ_1.

(2) Under the isomorphism $\Lambda \cong \prod_{1<s|r} \mathcal{O}_s/\ell$, the involution on the left corresponds to complex conjugation on the right. Taking invariants yields

$$\Lambda^+ \cong \prod_{1<s|r} (\mathcal{O}_s/\ell)^+.$$

By part (1), $(\mathcal{O}_s/\ell)^+$ is generated as a ring by the image of $\zeta + \zeta^{-1}$. Since $\mathcal{O}_s^+$ is generated as a ring by $\zeta_s + \zeta_s^{-1}$ [**58**, Proposition 2.16], the reduction map $\mathcal{O}_s^+ \to (\mathcal{O}_s/\ell)^+$ is surjective, so $(\mathcal{O}_s/\ell)^+ \cong \mathcal{O}_s^+/\ell$, and this completes the proof. □

8.3.3. Primes of Λ and Λ^+. Since ℓ does not divide r, the roots of $\Psi_r(z)$ are distinct modulo ℓ, and so Λ and Λ^+ are semi-simple algebras over $\mathbb{F}_\ell$.

We write λ for a prime ideal of Λ and $\mathbb{F}_\lambda$ for the quotient Λ/λ. This is a finite extension field of $\mathbb{F}_\ell$. We say that λ *has level* s if the quotient map $\Lambda \to \Lambda/\lambda$ factors through $\Lambda \to \mathcal{O}_s/\ell$, or equivalently, if $\Phi_s(z) \in \lambda$. Clearly each λ has a well-defined level $s > 1$ that is a divisor of r, and we may identify the primes of Λ of level s with the primes of $\mathcal{O}_s$ over ℓ.

Similarly, for a prime $\lambda^+ \subset \Lambda^+$, we define $\mathbb{F}_{\lambda^+} := \Lambda^+/\lambda^+$, and we define the level of λ^+ to be the divisor s of r such that the quotient $\Lambda^+ \to \Lambda^+/\lambda^+$ factors through $\Lambda^+ \to \mathcal{O}_s^+/\ell$. Thus the primes of Λ^+ of level s are naturally identified with the primes of $\mathcal{O}_s^+$ over ℓ.

We say that $\lambda \subset \Lambda$ lies over $\lambda^+ \subset \Lambda^+$ if $\lambda \cap \Lambda^+ = \lambda^+$. In this case, if λ has level s then so does λ^+, and the prime of $\mathcal{O}_s$ corresponding to λ lies over the prime of $\mathcal{O}_s^+$ corresponding to λ^+.

8.3.4. Splitting of primes. In this subsection, we focus on the "new" quotients $\mathcal{O}_r/\ell$ and $\mathcal{O}_r^+/\ell$ of Λ and Λ^+. For typographical convenience, we omit the subscript and write $\mathcal{O}$ and $\mathcal{O}^+$ for $\mathcal{O}_r$ and $\mathcal{O}_r^+$.

We review the structure of $\mathcal{O}^+/\ell$ and $\mathcal{O}/\ell$, dividing into three cases: First, if $r = 2$, then $\mathcal{O} = \mathcal{O}^+ = \mathbb{Z}$ and $\mathcal{O}^+/\ell = \mathcal{O}/\ell = \mathbb{F}_\ell$.

Before defining the second and third cases, we introduce some notation. Let $o_r(\ell)$ be the order of ℓ in $(\mathbb{Z}/r\mathbb{Z})^\times$. Let $o_r^+(\ell)$ be the order of ℓ in $(\mathbb{Z}/r\mathbb{Z})^\times/\langle \pm 1 \rangle$. Standard results in cyclotomic fields (see, e.g., [**58**], Chapter 2) indicate that ℓ splits into $h = \phi(r)/(2o_r^+(\ell))$ primes in $\mathcal{O}^+$. Write $\lambda_1^+ \ldots, \lambda_h^+$ for the primes of $\mathcal{O}^+$ over ℓ. Let $\mathbb{F}_{\lambda_i} := \mathcal{O}/\lambda_i$ and $\mathbb{F}_{\lambda_i^+} := \mathcal{O}^+/\lambda_i^+$ be the residue fields.

The second case, which we call the inert case, is when $r > 2$ and -1 is congruent to a power of ℓ modulo r. In this case, $o_r(\ell) = 2o_r^+(\ell)$. Each λ_i^+ remains prime in $\mathcal{O}$, i.e., $\lambda_i = \lambda_i^+\mathcal{O}$ is a prime ideal of $\mathcal{O}$. The residue field $\mathbb{F}_{\lambda_i}$ is a quadratic extension of $\mathbb{F}_{\lambda_i^+}$.

The third case, which we call the split case, is when $r > 2$ and -1 is not congruent to a power of ℓ modulo r. In this case, $o_r^+(\ell) = o_r(\ell)$ and the h primes λ_i^+ of $\mathcal{O}^+$ over ℓ each split into two primes, call them λ_i and λ_{g-i}, in $\mathcal{O}$, where $g = 2h$. The residue fields satisfy $\mathbb{F}_{\lambda_i} \cong \mathbb{F}_{\lambda_{g-i}} \cong \mathbb{F}_{\lambda_i^+}$ and $\mathcal{O}/\lambda_i^+$ is a semi-simple quadratic algebra over $\mathbb{F}_{\lambda_i^+}$, namely $\mathbb{F}_{\lambda_i} \oplus \mathbb{F}_{\lambda_{g-i}}$.

Via the identification of primes of $\mathcal{O}$ and $\mathcal{O}^+$ over ℓ with primes of Λ and Λ^+ of level r, the discussion in the second and third cases applies to the splitting behavior of primes $\lambda^+ \subset \Lambda^+$ in Λ.

One of the reasons it is convenient to focus on the new part $\mathcal{O} = \mathcal{O}_r$ is the possibility that the primes of $\mathcal{O}_r^+$ over ℓ may be inert in $\mathcal{O}_r$ while the primes of $\mathcal{O}_s^+$ over ℓ may be split in $\mathcal{O}_s$ for a divisor s of r.

8.3.5. Auxiliary results. We record two lemmas to be used later.

Note that Λ is a direct sum of fields $\mathbb{F}_\lambda$ and that $\mathbb{F}_\lambda \cong \mathbb{F}_{\ell^{o_r(\ell)}}$ for all λ of level r. However, the various $\mathbb{F}_\lambda$ are non-isomorphic as Λ-modules. Similarly, the various $\mathbb{F}_{\lambda^+}$ are non-isomorphic as Λ^+-modules. We state this more formally for later use:

LEMMA 8.8. *Suppose that λ_1^+ and λ_2^+ are distinct primes of Λ^+. Then there does not exist an isomorphism of fields $\mathbb{F}_{\lambda_1^+} \cong \mathbb{F}_{\lambda_2^+}$ carrying the class of $\zeta + \zeta^{-1}$ in $\mathbb{F}_{\lambda_1^+}$ to its class in $\mathbb{F}_{\lambda_2^+}$.*

PROOF. Since Λ^+ is generated over $\mathbb{F}_\ell$ by $\zeta + \zeta^{-1}$, a field isomorphism $\mathbb{F}_{\lambda_1^+} \cong \mathbb{F}_{\lambda_2^+}$ as in the statement would induce an isomorphism of Λ^+-modules. But the Λ^+-modules $\mathbb{F}_{\lambda_1^+}$ and $\mathbb{F}_{\lambda_2^+}$ are not isomorphic since they have distinct annihilators. □

LEMMA 8.9. *Suppose that $\ell = 3$. Then the number of primes $\lambda^+ \subset \Lambda^+$ such that $\mathbb{F}_{\lambda^+} \cong \mathbb{F}_3$ is*

$$\begin{cases} 0 & \text{if } r \text{ is odd,} \\ 1 & \text{if } r \equiv 2 \pmod 4, \\ 2 & \text{if } r \equiv 0 \pmod 4. \end{cases}$$

If $r \equiv 2 \pmod 4$, the prime has level 2, and if $r \equiv 0 \pmod 4$ one of the primes has level 2 and the other has level 4.

PROOF. Suppose there is a prime $\lambda^+ \subset \Lambda^+$ with $\mathbb{F}_{\lambda^+} \cong \mathbb{F}_3$ and choose a prime $\lambda \subset \Lambda$ over it. Then $\mathbb{F}_\lambda$ is a subfield of $\mathbb{F}_9$, so the multiplicative order of ζ in $\mathbb{F}_\lambda$ must divide 8 and the level of λ must divide 8. (In particular, λ^+ does not exist if r is odd.) To finish, we note that the unique prime of $\mathcal{O}_8^+$ over $\ell = 3$ has residue field $\mathbb{F}_9$, while $\mathcal{O}_4^+$ and $\mathcal{O}_2^+$, both being isomorphic to $\mathbb{Z}$, have unique primes over 3, each with residue field $\mathbb{F}_3$. □

8.4. The Λ-module structure of $J[\ell]$

Recall that Λ is $\mathbb{F}_\ell[z]/(z^{r-1} + \cdots + 1)$ and that $J[\ell]$ denotes the ℓ-torsion in J.

PROPOSITION 8.10. *The action of μ_r on J gives $J[\ell]$ the structure of a free Λ-module of rank 2. For every prime λ of Λ, the submodule $J[\lambda] \subset J[\ell]$ of λ-torsion has the structure of a free $\mathbb{F}_\lambda = \Lambda/\lambda$-module of rank 2.*

PROOF. The action of μ_r on $C = C_r$ and $J = J_r$ gives the Tate module

$$V_\ell J \cong H^1(C, \mathbb{Q}_\ell)$$

the structure of a module over

$$\mathbb{Q}_\ell[\mu_r] \cong \prod_{s|r} \mathbb{Q}_\ell[z]/\Phi_s(z).$$

The map $C_r \to C_1 = \mathbb{P}^1$ presents C_r as a Galois branched cover of $\mathbb{P}^1$ with Galois group μ_r. In this context, a formula of Artin gives the character of $H^1(C_r, \mathbb{Q}_\ell)$ as a representation of μ_r in terms of the ramification data of $C_r \to C_1$. See [**30**, Corollary 2.8] for the precise statement. One finds that the character is $2(\chi_{reg} - \chi_{triv})$ where χ_{reg} and χ_{triv} are the characters of regular and trivial representations respectively. Thus $V_\ell J$ is isomorphic to the direct sum of two copies of the regular

representation modulo the trivial representation. Equivalently,

$$V_\ell J \cong \left(\prod_{1<s|r} \mathbb{Q}_\ell[z]/\Phi_s(z) \right)^2$$

where the product is over divisors of r that are > 1.

Since $T_\ell J \subset V_\ell J$ is preserved by the action of μ_r and ℓ is prime to r, we have that

$$T_\ell J \cong \left(\prod_{1<s|r} \mathbb{Z}_\ell[z]/\Phi_s(z) \right)^2$$

and

$$\begin{aligned} J[\ell] &\cong \left(\prod_{1<s|r} \mathbb{F}_\ell[z]/\Phi_s(z) \right)^2 \\ &\cong \Lambda^2. \end{aligned}$$

This is the first assertion of the proposition. The second follows immediately from the equality

$$\Lambda[\lambda] \cong \Lambda/\lambda.$$

□

A slight elaboration of this argument shows that $J_s^{new}[\ell]$ is a free module of rank 2 over $\mathcal{O}_s/\ell$ for each divisor s of r.

8.5. Monodromy of $J[\lambda]$

Our next task is to study the action of $\mathrm{Gal}(K^{sep}/K)$ on $J[\lambda]$ where λ is a prime of Λ.

8.5.1. Fundamental groups. Let $\mathbb{P}^1_k$ be the projective line over k with coordinate t, so that the function field of $\mathbb{P}^1_k$ is $K = k(t)$. Let U be the Zariski open subset $\mathbb{P}^1_k \setminus \{0, 1, \infty\}$. We saw in Chapter 3 that J has good reduction at every place of U. Proposition 3.5 and the discussion in Section 3.1.5 show that the action of $\mathrm{Gal}(K^{sep}/K)$ on $H^1(C, \mathbb{Q}_\ell)$ is at worst tamely ramified at places in $\mathbb{P}^1_k \setminus U$. It follows that the actions of $\mathrm{Gal}(K^{sep}/K)$ on $J[\ell]$ and on $J[\lambda] \subset J[\ell]$ factor through the quotient $\mathrm{Gal}(K^{sep}/K) \to \pi_1^t(U)$ where $\pi_1^t(U)$ is the tame fundamental group (with base point the geometric generic point given by the choice of K^{sep}, which we omit from the notation).

It is known ([**16**, Corollary to Theorem 14] or [**17**, XIII.2.12]) that $\pi_1^t(U)$ is topologically generated by elements $\gamma_0, \gamma_1, \gamma_\infty$ with $\gamma_0\gamma_1\gamma_\infty = 1$ and with γ_x topologically generating the inertia group at x.

Choose a basis of the free, rank 2 Λ-module $J[\ell]$, and fix the corresponding isomorphism

$$\mathrm{Aut}_\Lambda(J[\ell]) \cong \mathrm{GL}_2(\Lambda).$$

Let $\rho : \pi_1^t(U) \to \mathrm{GL}_2(\Lambda)$ be the representation giving the action of $\pi_t^1(U)$ on $J[\ell]$. Also, let $\rho_\lambda : \pi_1^t(U) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ be the composition

$$\pi_1^t(U) \to \mathrm{GL}_2(\Lambda) \to \mathrm{GL}_2(\mathbb{F}_\lambda),$$

giving the action of $\pi_1^t(U)$ on $J[\lambda]$. Later in this section, we determine the image of ρ_λ.

8.5.2. Twisting. It is convenient to consider a twist of C and of its Jacobian. Let C_χ be the smooth projective curve over K associated to the affine curve

$$(1-t)xy^r = (x+1)(x+t).$$

It is evident that C_χ becomes isomorphic to C over the Kummer extension $K(v)$ where $v^r = 1-t$.

The extension $K(v)/K$ is unramified over U, so the action of $\mathrm{Gal}(K^{sep}/K)$ on $K(v)$ factors through $\pi_1^t(U)$, and Kummer theory shows that the character $\chi : \pi_1^t(U) \to \mu_r$ with $\chi(g) := g(v)/v$ satisfies $\chi(\gamma_0) = 1$, $\chi(\gamma_1) = \zeta^{-1}$ and $\chi(\gamma_\infty) = \zeta$ for some primitive r-th root of unity $\zeta \in k$.

Now consider the Jacobian J_χ of C_χ. It admits an action of $\mathbb{Z}[\mu_r]$ and we may define $A_\chi := J_\chi^{new}$ and $J_\chi[\lambda]$ in the same manner we defined $A = J^{new}$ and $J[\lambda]$. Over $K(v)$, since J_χ and J are isomorphic, it follows that $J_\chi[\ell] \cong J[\ell] \cong \Lambda^2$ and $J_\chi[\lambda] \cong J[\lambda] \cong \mathbb{F}_\lambda^2$.

Since the action of μ_r on C and C_χ is via the y coordinate, we may identify ζ above with an element of $\mu_r \subset \Lambda \to \mathbb{F}_\lambda$. Let

$$\rho_\chi : \pi_1^t(U) \to \mathrm{Aut}(J_\chi[\ell]) \cong \mathrm{GL}_2(\Lambda)$$

be the representation giving the action of $\pi_1^t(U)$ on $J_\chi[\ell]$, and let $\rho_{\chi,\lambda} : \pi_1^t(U) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ be the quotient giving the action on $J_\chi[\lambda]$. Then the discussion above shows that there are isomorphisms $\rho_\chi \cong \rho \otimes \chi$ and $\rho_{\chi,\lambda} \cong \rho_\lambda \otimes \chi$. We use this "twisting" to deduce information about ρ_λ and ρ.

8.5.3. Local monodromy. Our next goal is to record the Jordan forms of the matrices $\rho_\lambda(\gamma_x)$ and $\rho_{\chi,\lambda}(\gamma_x)$.

PROPOSITION 8.11. *Suppose that $\lambda \subset \Lambda$ is a prime of level $r > 2$. For $x \in \{0, 1, \infty\}$, let $g_x = \rho_\lambda(\gamma_x)$ and $g_{\chi,x} = \rho_{\chi,\lambda}(\gamma_x)$. Let $\zeta \in \mathbb{F}_\lambda$ be the primitive r-th root of unity $\zeta = \chi(\gamma_\infty)$. Then:*

(1) *g_0 is unipotent and non-trivial, g_1 is semi-simple with eigenvalues 1 and ζ^2, and g_∞ is non-semi-simple with eigenvalue ζ^{-1} repeated twice. Equivalently, writing $\sim$ for conjugacy in $\mathrm{GL}_2(\mathbb{F}_\lambda)$,*

$$g_0 \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad g_1 \sim \begin{pmatrix} 1 & 0 \\ 0 & \zeta^2 \end{pmatrix}, \qquad \text{and} \qquad g_\infty \sim \begin{pmatrix} \zeta^{-1} & 1 \\ 0 & \zeta^{-1} \end{pmatrix}.$$

(2) *$g_{\chi,0}$ and $g_{\chi,\infty}$ are unipotent and non-trivial, and $g_{\chi,1}$ is semi-simple with eigenvalues ζ^{-1} and ζ. Equivalently,*

$$g_{\chi,0} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad g_{\chi,1} \sim \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix}, \qquad \text{and} \qquad g_{\chi,\infty} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Note that parts (1) and (2) are equivalent via the isomorphism $\rho_{\chi,\lambda} \cong \rho_\lambda \otimes \chi$, but we use both ρ_λ and $\rho_{\chi,\lambda}$ in the proof.

PROOF OF PROPOSITION 8.11. By Proposition 3.9, the minimal regular model $\mathcal{X}$ of C has semi-stable reduction at $t = 0$. Indeed, the fiber at 0 of $\mathcal{X}$, call it $\mathcal{X}_0$, is a pair of smooth rational curves crossing transversally at r points. It follows that the action of γ_0 on $J[\ell]$ is unipotent (see [**1**, Theorem 1.4] for a modern account) and therefore that the action of γ_0 on $J[\lambda]$ is unipotent. It remains to see that it

is non-trivial. To that end, let $\mathcal{J}_0$ be the fiber at 0 of the Néron model of J. If $I_0 \subset \pi_1^t(U)$ denotes the inertia subgroup at 0, we have

$$J[\ell]^{I_0} \cong \mathcal{J}_0[\ell].$$

By [**6**, 9.5, Corollary 11], the group of connected components of $\mathcal{J}_0$ has order r, so is prime to ℓ. By Proposition 3.9, the identity component of $\mathcal{J}_0$ is a torus of dimension $r-1$. It follows that

$$\mathcal{J}_0[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{r-1}.$$

We need to understand the action of μ_r on this group. Since $\mathcal{X} \to \mathbb{P}^1$ admits a section, [**6**, 9.5, Theorem 4] shows that $\mathcal{J}_0 \cong \mathrm{Pic}^0(\mathcal{X}_0)$. Noting that μ_r acts on $\mathcal{X}_0$ by cyclically permuting the points where the two components cross, we see that there is an isomorphism of Λ-modules

$$\mathcal{J}_0[\ell] \cong \Lambda.$$

It follows that

$$J[\lambda]^{I_0} \cong \mathbb{F}_\lambda.$$

Since this has dimension 1 over $\mathbb{F}_\lambda$, we deduce that g_0 is not the identity. This proves our claim for g_0.

Our claim for $g_{\chi,0}$ follows from the isomorphism $\rho_{\chi,\lambda} \cong \rho_\lambda \otimes \chi$. Alternatively, it also follows from the fact that $1-t$ is an r-th power in the completed local ring $k[[t]]$, so the regular minimal models of C and C_χ are isomorphic over $k[[t]]$ and the action of inertia is the same.

Now we turn to C_χ in a neighborhood of $t=\infty$. Changing coordinates $(x,y) \mapsto (tx,y)$, the defining equation of C_χ becomes

$$\frac{1-t}{t} xy^r = (x+1)(x+t^{-1}).$$

But $(1-t)/t$ is a unit, and thus an r-th power, in $k[[t^{-1}]]$ so we may change coordinates $(x,y) \mapsto (x,(t/(1-t))^{1/r}y)$, yielding

$$xy^r = (x+1)(x+t^{-1}).$$

Up to substituting t^{-1} for t, this is exactly the defining equation of C. We conclude that the action of γ_∞ on $J_\chi[\ell]$ is the same as the action of γ_0 on $J[\ell]$ and similarly for the submodules $J_\chi[\lambda]$ and $J[\lambda]$. In particular, $g_{\chi,\infty}$ is unipotent and non-trivial, as claimed.

The claim for g_∞ follows from that for $g_{\chi,\infty}$ and the isomorphism $\rho_{\chi,\lambda} \cong \rho_\lambda \otimes \chi$.

Now we turn to a consideration of g_1. Letting $I_1 \subset \pi_1^t(U)$ be the inertia group at $t=1$, our first claim is that $J[\lambda]^{I_1}$ is a one-dimensional $\mathbb{F}_\lambda$-vector space. The proof is very similar to the proof above that $J[\lambda]^{I_0}$ is 1-dimensional. First we note that

$$J[\ell]^{I_1} \cong \mathcal{J}_1[\ell]$$

where $\mathcal{J}_1$ is the fiber of the Néron model of J at $t=1$. By Proposition 3.7, the component group of $\mathcal{J}_1$ has order r (the hypothesis that r divides d is not needed at $t=1$), and by Proposition 3.9, the identity component is an extension of a 1-dimensional torus by an abelian variety of dimension $(r-2)/2$ if r is even, and is an abelian variety of dimension $(r-1)/2$ if r is odd. In both cases, this abelian variety is the Jacobian of the smooth model of the curve $zy^r = (1+z)^2$. Viewing

this curve as a μ_r-Galois cover of the line allows us to compute the structure of the ℓ-torsion of its Jacobian as a Λ-module, and we find that

$$\mathcal{J}_1[\ell] \cong \Lambda.$$

It follows that

$$J[\ell]^{I_1} \cong \Lambda$$

and that

$$J[\lambda]^{I_1} \cong \mathbb{F}_\lambda.$$

Since this has dimension 1 over $\mathbb{F}_\lambda$, we deduce that g_1 has 1 as an eigenvalue. Our second claim is that $\det(g_1) = \zeta^2$, which follows from the equality $g_1 = g_0^{-1} g_\infty^{-1}$ and from previous computations for g_0 and g_∞. Thus the eigenvalues of g_1 are 1 and ζ^2, and since $r > 2$, these are distinct and g_1 is semi-simple as claimed.

Finally, our claim about $g_{\chi,1}$ follows from the isomorphism $\rho_{\chi,\lambda} \cong \rho_\lambda \otimes \chi$. □

PROPOSITION 8.12. *Suppose $r = 2$. For $x \in \{0, 1, \infty\}$, let $g_x = \rho_\lambda(\gamma_x)$ and let $g_{\chi,x} = \rho_{\chi,\lambda}(\gamma_x)$. Then g_0 and g_1 are unipotent and non-trivial, and g_∞ is non-semi-simple with eigenvalue -1 repeated twice. Equivalently, writing $\sim$ for conjugacy in* $\mathrm{GL}_2(\mathbb{F}_\lambda)$,

$$g_0 \sim g_1 \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \text{and} \qquad g_\infty \sim \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},$$

and

$$g_{\chi,0} \sim g_{\chi,\infty} \sim \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \text{and} \qquad g_{\chi,1} \sim \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

PROOF. The same proof as in the case $r > 2$ works up until the penultimate paragraph, where g_1 has eigenvalues 1 and $\zeta^2 = 1$, and thus we can no longer deduce that g_1 is semi-simple. If it were semi-simple, g_1 would be the identity, contradicting the fact that $C = J$ has bad reduction at $t = 1$. Thus g_1 is unipotent and non-semi-simple in this case. □

8.5.4. Group theory. We write G_λ for $\rho_\lambda(\pi_1^t(U))$ and $G_{\chi,\lambda}$ for $\rho_{\chi,\lambda}(\pi_1^t(U))$. The main result of this section is a calculation of these groups.

PROPOSITION 8.13. *Let $\lambda \subset \Lambda$ be a prime of level r.*

1. *If $\ell = 2$, then $G_{\lambda,\chi}$ is isomorphic to the dihedral group D_{2r} of order $2r$.*
2. *If $\ell = 3$ and $r = 10$, then $G_{\chi,\lambda} \subsetneq \mathrm{SL}_2(\mathbb{F}_{\lambda^+}) = \mathrm{SL}_2(\mathbb{F}_9)$ and $G_{\chi,\lambda}$ is isomorphic to $\tilde{A}_5$, a double cover of the alternating group A_5.*
3. *If $\ell > 3$ or $\ell = 3$ and $r \neq 10$, then*
$$G_{\chi,\lambda} \cong \mathrm{SL}_2(\mathbb{F}_{\lambda^+}) \subset \mathrm{GL}_2(\mathbb{F}_\lambda)$$
where λ^+ is the prime of Λ^+ under λ.
4. *For all ℓ and r,*
$$G_\lambda \cong \mu_r \cdot G_{\chi,\lambda}.$$

PROOF. We first prove part (4): To see that $G_\lambda \cong \mu_r \cdot G_{\chi,\lambda}$, note that $G_\lambda \subset \mu_r \cdot G_{\chi,\lambda}$, since the values of χ lie in μ_r. For the opposite containment, we observe that if m is an integer such that $\ell m \equiv 1 \pmod{r}$, then $g_\infty^{\ell m}$ is the scalar matrix ζ^{-1} and it follows that μ_r and $G_{\chi,\lambda}$ are contained in G_λ.

Next we claim that the lines fixed by $g_{\chi,0}$ and $g_{\chi,\infty}$ are distinct. Indeed, if they were not, then $g_{\chi,1} = g_{\chi,0}^{-1} g_{\chi,\infty}^{-1}$ would fix the same line, but by Proposition 8.11, 1 is not an eigenvalue of $g_{\chi,1}$. Thus there is a basis e_1, e_2 of $J[\lambda]$ such that $g_{\chi,0}$ fixes

e_1 and $g_{\chi,\infty}$ fixes e_2. Scaling e_2 if necessary, the matrices of $g_{\chi,0}$ and $g_{\chi,\infty}$ in the new basis have the form

$$g_{\chi,0} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad g_{\chi,\infty} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

for some uniquely determined $c \in \mathbb{F}_\lambda$ with $c \neq 0$. Proposition 8.11 implies that $g_{\chi,1}$ has trace $\zeta + \zeta^{-1}$. Since $g_{\chi,1} = g_{\chi,0}^{-1} g_{\chi,\infty}^{-1}$, we calculate that $c = \zeta + \zeta^{-1} - 2$.

If $\ell = 2$, setting

$$h = \begin{pmatrix} 1 & 1 \\ 1+\zeta & 1+\zeta^{-1} \end{pmatrix},$$

the reader may check that

$$h^{-1} g_{\chi,\infty} h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad h^{-1} g_{\chi,0}^{-1} g_{\chi,\infty}^{-1} h = \begin{pmatrix} \zeta^{-1} & 0 \\ 0 & \zeta \end{pmatrix}.$$

It follows that $G_{\chi,\lambda}$ is dihedral of order $2r$, and this proves part (1).

To prove parts (2) and (3), we assume that $\ell > 2$, and we apply Dickson's theorem [**14**, page 44]. It says that if $\ell > 2$, then the subgroup of $\mathrm{SL}_2(\overline{\mathbb{F}}_\ell)$ generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

is $\mathrm{SL}_2(\mathbb{F}_\ell(c))$ except for one exceptional case, namely where $\ell = 3$ and $c^2 = -1$, in which case the group is a double cover of A_5.[1] For our c, $\mathbb{F}_\ell(c) = \mathbb{F}_{\lambda^+}$ so, apart from the possible exceptional case, we have $G_{\chi,\lambda} \cong \mathrm{SL}_2(\mathbb{F}_{\lambda^+})$. Equality holds here in particular when $\ell > 3$.

Note that in the exceptional case $\mathbb{F}_{\lambda^+} = \mathbb{F}_3(c) = \mathbb{F}_9$ since $[\mathbb{F}_3(c) : \mathbb{F}_3] \leq 2$ and since -1 is not a square in $\mathbb{F}_3$. If $\mathbb{F}_{\lambda^+} = \mathbb{F}_9$, then $\zeta \in \mathbb{F}_\lambda \subset \mathbb{F}_{81}$, so r divides $80 = 16 \cdot 5$. We cannot be in the exceptional case if $20|r$ or $8|r$, because the order of $g_{\chi,1}$ in PSL_2 is r or $r/2$ as r is odd or even, and A_5 has no elements of order 10 or 4. Also, c does not generate $\mathbb{F}_9$ if $r = 4$ or $r = 2$, so the only possible exceptional cases are when $r = 5$ and $r = 10$.

Recalling that $c = \zeta_r + \zeta_r^{-1} - 2$ and $\ell = 3$, we have

$$c^2 = \zeta_r^2 + \zeta_r^{-2} - \zeta_r - \zeta_r^{-1}.$$

When $r = 5$, we have $(c^2)^3 = -c^2$, so $c^2 \notin \mathbb{F}_3$ and we are not in the exceptional case. When $r = 10$, $-\zeta_{10} = \zeta_5$ and we see that

$$\begin{aligned} c^2 &= \zeta_{10}^2 + \zeta_{10}^{-2} - \zeta_{10} - \zeta_{10}^{-1} \\ &= \zeta_5^2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} \\ &= -1, \end{aligned}$$

so we are in the exceptional case, i.e., $G_{\chi,\lambda}$ is a double cover of A_5. □

REMARK 8.14. Note that if $\lambda \subset \Lambda$ is a prime of level $s > 2$, then $J[\lambda] \cong J_s[\lambda]$ as a module over $\pi_1^t(U)$, so Proposition 8.13 determines the monodromy of $J[\lambda]$ for all primes λ.

[1] Gorenstein does not state explicitly which c give rise to the exceptional case, but the paragraph containing the first display on page 45 of [**14**] shows that we are in the exceptional case exactly when $\ell = 3$ and $c^2 = -1$.

8.6. Independence

8.6.1. Statement. In the previous section, we determined G_λ and $G_{\chi,\lambda}$, the images of $\pi_1^t(U)$ in $\mathrm{Aut}_{\mathbb{F}_\lambda}(J[\lambda])$ and $\mathrm{Aut}_{\mathbb{F}_\lambda}(J_\chi[\lambda])$. Our goal in this section is to determine G and G_χ, the images of $\pi_1^t(U)$ in $\mathrm{Aut}_\Lambda(J[\ell])$ and $\mathrm{Aut}_\Lambda(J_\chi[\ell])$, i.e., the image of the representations

$$\rho_\ell : \pi_1^t(U) \to \mathrm{Aut}_\Lambda(J[\ell]) \cong \mathrm{GL}_2(\Lambda)$$

and

$$\rho_{\chi,\ell} : \pi_1^t(U) \to \mathrm{Aut}_\Lambda(J_\chi[\ell]) \cong \mathrm{GL}_2(\Lambda)$$

where Λ is the ring of endomorphisms discussed in Section 8.3. Since $\rho_{\chi,\ell} \cong \rho_\ell \otimes \chi$, it suffices to determine G_χ. It turns out that G_χ is the product over a suitable set of λ of the $G_{\chi,\lambda}$; the set in question is not all λ, because there is one obvious dependency among the $G_{\chi,\lambda}$.

To motivate the main result, consider a prime λ^+ of Λ^+ that splits in Λ into primes λ_1 and λ_2. The proof of Proposition 8.13 shows that after choosing suitable bases, the image of

$$\pi_1^t(U) \to \mathrm{Aut}_{\mathbb{F}_{\lambda_1}}(A[\lambda_1]) \times \mathrm{Aut}_{\mathbb{F}_{\lambda_2}}(A[\lambda_2]) \cong \mathrm{GL}_2(\mathbb{F}_{\lambda_1}) \times \mathrm{GL}_2(\mathbb{F}_{\lambda_2})$$

is generated by the elements

$$\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right) \quad \text{and} \quad \left(\begin{pmatrix}1 & 0\\ c_1 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ c_2 & 1\end{pmatrix}\right)$$

where c_1 and c_2 are the images of $\zeta + \zeta^{-1} - 2$ in $\mathbb{F}_{\lambda_1}$ and $\mathbb{F}_{\lambda_2}$. Since λ_1 and λ_2 lie over the same prime λ^+ of Λ^+, and since c_1 and c_2 lie in $\mathbb{F}_{\lambda^+}$, there is a field isomorphism $\mathbb{F}_{\lambda_1} \cong \mathbb{F}_{\lambda_2}$ that carries c_1 to c_2. This shows that the image of the map under consideration is "small": it is the graph of an isomorphism $G_{\chi,\lambda_1} \cong G_{\chi,\lambda_2}$. The main result of this section shows that when $\ell > 2$ this is the only relation among the $G_{\chi,\lambda}$.

THEOREM 8.15. *Let S be a set of primes of Λ such that for every prime λ^+ of Λ^+ there is a unique prime in S over λ^+. Let G_χ be the image of*

$$\rho_{\chi,\ell} : \pi_1^t(U) \to \mathrm{Aut}_\Lambda(J_\chi[\ell]) \cong \mathrm{GL}_2(\Lambda)$$

and let G be the image of

$$\rho_\ell : \pi_1^t(U) \to \mathrm{Aut}_\Lambda(J[\ell]) \cong \mathrm{GL}_2(\Lambda).$$

(1) *If $\ell > 2$, then there is an isomorphism*

$$G_\chi \cong \prod_{\lambda \in S} G_{\chi,\lambda}.$$

In particular, if $\ell > 3$ or $\ell = 3$ and $10 \nmid r$, then

$$G_\chi \cong \mathrm{SL}_2(\Lambda^+) \subset \mathrm{GL}_2(\Lambda).$$

(2) *If $\ell = 2$, then*

$$G_\chi \cong D_{2r}.$$

(3) $G \cong \mu_r \cdot G_\chi$.

The proof of the theorem occupies the rest of this section. In the next subsection, we dispose of the easy parts of the proof. The remaining sections deal with the main issue, namely the isomorphism $G_\chi \cong \prod_{\lambda \in S} G_{\chi,\lambda}$ for $\ell > 2$.

8.6.2. First part of the proof of Theorem 8.15. The proof of part (3) is essentially identical to that of part (4) of Proposition 8.13 and is left to the reader.

Now consider part (2), the case $\ell = 2$. In view of part (1) of Proposition 8.13, the conclusion here is exactly the opposite of that in part (1): the $G_{\chi,\lambda}$ are highly dependent. To prove it, we note that C_χ is hyperelliptic, as we see from the defining equation $(1-t)xy^r = (x+1)(x+t)$ via projection to the x-line. Rewriting the equation as

$$x^2 + (t+1+(t-1)y^r)\,x + t = 0$$

and completing the square (as we may do since $p \neq \ell = 2$), the equation takes the form

$$z^2 = y^{2r} + 2\left(\frac{t+1}{t-1}\right)y^r + 1.$$

The 2-torsion points on the Jacobian of a hyperelliptic curve $z^2 = f(y)$ are represented by divisors of degree zero supported on the points $(y, 0)$ where y is a zero of f. It follows that the monodromy group of the 2-torsion is equal to the Galois group of f. In our case, the Galois group is D_{2r}. Indeed, the roots of f are the solutions of $y^r = w_1$ and $y^r = w_2$ where w_1 and $w_2 = 1/w_1$ are the roots of $w^2 + (t+1)/(t-1)w + 1$. The discriminant of this quadratic polynomial is $16t/(t-1)^2$, so its roots lie in $K(t^{1/2})$. The splitting field K_0 of f is thus a degree r Kummer extension of $K(t^{1/2})$, and $\mathrm{Gal}(K(t^{1/2})/K)$ acts on $\mathrm{Gal}(K_0/K(t^{1/2}))$ by inversion, so $G_\chi \cong \mathrm{Gal}(K_0/K) \cong D_{2r}$. This proves part (2).

For use in the next section, we note that the fixed field of the cyclic group $C_r \subset D_{2r}$ is the quadratic extension $K(t^{1/2})$ of $K = k(t)$.

To end this subsection, we prove the "in particular" part of (1). Recall that we have shown that if $\ell > 3$ or $\ell = 3$ and the level of λ is not 10, then $G_{\chi,\lambda} \cong \mathrm{SL}_2(\mathbb{F}_{\lambda^+})$. Let S^+ be the set of all primes of Λ^+ and let S be as in the statement of the theorem, so that there is a bijection $S \to S^+$ that sends a prime λ to the prime λ^+ under it. Then the image of $\mathrm{SL}_2(\Lambda^+) \subset \mathrm{SL}_2(\Lambda)$ under the projection

$$\mathrm{SL}_2(\Lambda) = \prod_\lambda \mathrm{SL}_2(\mathbb{F}_\lambda) \to \prod_{\lambda\in S} \mathrm{SL}_2(\mathbb{F}_\lambda)$$

is the product $\prod_{\lambda^+\in S^+} \mathrm{SL}_2(\mathbb{F}_{\lambda^+})$. Since

$$\prod_{\lambda\in S} G_{\chi,\lambda} = \prod_{\lambda^+\in S^+} \mathrm{SL}_2(\mathbb{F}_{\lambda^+}),$$

this establishes the desired isomorphism $G_\chi \cong \mathrm{SL}_2(\Lambda^+)$.

To finish the proof of the theorem, it remains to establish the first sentence of part (1). We do this in Section 8.6.5 below.

8.6.3. Several lemmas. We collect together several group-theoretic lemmas to be used below. Recall that a group is said to be *perfect* if it is its own commutator subgroup, or equivalently, if it has no non-trivial abelian quotients, and it is said to be *solvable* if its Jordan-Holder factors are all abelian.

Lemma 8.16.

(1) $\mathrm{SL}_2(\mathbb{F}_q)$ *is perfect unless* $q = 2, 3$*, in which case it is solvable.*
(2) *The group* $\tilde{A}_5$ *of Proposition 8.13(2) is perfect.*

(3) *If $q > 3$, the non-trivial quotients of $\mathrm{SL}_2(\mathbb{F}_q)$ are $\mathrm{SL}_2(\mathbb{F}_q)$ and $\mathrm{PSL}_2(\mathbb{F}_q)$. The non-trivial quotients of $\mathrm{SL}_2(\mathbb{F}_3)$ are $\mathrm{SL}_2(\mathbb{F}_3)$, $\mathrm{PSL}_2(\mathbb{F}_3)$, and $\mathbb{Z}/3\mathbb{Z}$. The non-trivial quotients of $\tilde{A}_5$ are $\tilde{A}_5$ and A_5.*
(4) *Suppose $\ell \geq 3$ and let $H_a = \mathrm{SL}_2(\mathbb{F}_{\ell^a})$ for $a \geq 1$. If H is a non-trivial quotient of both H_a and H_b, then $a = b$. If $\ell = 3$, then for all a, $\tilde{A}_5$ and H_a have no common non-trivial quotients.*

PROOF. The assertions in (1) and (3) related to $\mathrm{SL}_2(\mathbb{F}_q)$ are well known, see [**60**, Section 3.3.2]

The group $\tilde{A}_5 \subset \mathrm{SL}_2(\mathbb{F}_9)$ is generated by $h_0 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $h_\infty = \left(\begin{smallmatrix} 1 & 0 \\ i & 1 \end{smallmatrix}\right)$ where $i^2 = -1$. If $\tilde{A}_5 \to H$ is a non-trivial quotient with kernel N, then N projects to a normal subgroup of A_5, i.e., to the trivial group or all of A_5 since A_5 is simple [**60**, Section 2.3.3]. In the former case, N is either $\tilde{A}_5$ or A_5. In the latter case, since H is non-trivial, $N \neq \tilde{A}_5$, so projects isomorphically to A_5. We claim no such N exists. Indeed, if it did, $\tilde{A}_5$ would be the product of A_5 and ± 1. On the other hand, the reader may check that $(h_\infty h_0 h_\infty^{-1} h_0)^2 = -1$, which shows that $\tilde{A}_5$ is not the product $A_5 \times \{\pm 1\}$. This shows that the quotients of $\tilde{A}_5$ are as stated in part (3).

Since A_5 is non-abelian and simple, and thus perfect, the commutator subgroup of $\tilde{A}_5$ projects onto A_5. The analysis of the preceding paragraph shows it is all of $\tilde{A}_5$, i.e., $\tilde{A}_5$ is perfect. This establishes part (2).

Part (3) gives us a list of quotients of $\mathrm{SL}_2(\mathbb{F}_q)$ and $\tilde{A}_5$, and part (4) is then reduced to an easy exercise by considering the orders of the quotients. Indeed, if $\ell > 3$, the non-trivial quotients of $\mathrm{SL}_2(\mathbb{F}_{\ell^a})$ have order $\ell^a(\ell^{2a} - 1)$ or $\ell^a(\ell^{2a} - 1)/2$ and these numbers are all distinct for distinct values of a. If $\ell = 3$, the non-trivial quotients have order $\ell^a(\ell^{2a} - 1)$ or $\ell^a(\ell^{2a} - 1)/2$ or 3, with 3 occuring only if $a = 1$. Again, there are no coincidences, and this establishes the part of (4) related to H_a and H_b. To establish the last sentence, note that the non-trivial quotients of $\tilde{A}_5$ have order 120 or 60. These numbers are divisble by 3 and not by 9, and they are not $3(3^2 - 1) = 24$ nor $3(3^2 - 1)/2 = 12$, so $\tilde{A}_5$ and $\mathrm{SL}_2(\mathbb{F}_{3^a})$ have no common non-trivial quotients. □

Given a field automorphism $\phi : \mathbb{F}_q \to \mathbb{F}_q$, we define an automorphism $\mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{SL}_2(\mathbb{F}_q)$ by applying ϕ to the matrix entries. Similarly, ϕ gives a well-defined automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$.

LEMMA 8.17. *Assume that q is odd.*

(1) *Every automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$ is given by congugation by an element of $\mathrm{GL}_2(\mathbb{F}_q)$ composed with a field automorphism as above.*
(2) *Every automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$ lifts (uniquely) to $\mathrm{SL}_2(\mathbb{F}_q)$.*

PROOF. For (1), see [**35**, p. 795]. It follows immediately that an automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$ lifts to $\mathrm{SL}_2(\mathbb{F}_q)$ since conjugation and field automorphisms both preserve the kernel $\{\pm 1\}$ of $\mathrm{SL}_2(\mathbb{F}_q) \to \mathrm{PSL}_2(\mathbb{F}_q)$. Since the kernel is central, any two lifts would differ by a homomorphism $\mathrm{PSL}_2(\mathbb{F}_q) \to \{\pm 1\}$, and there are no non-trivial such homomorphisms by Lemma 8.16 part (3). This establishes part (2). □

LEMMA 8.18.

(1) (*"Goursat's lemma"*) *Let H_1 and H_2 be groups, and let $H \subset H_1 \times H_2$ be a subgroup that projects surjectively onto H_1 and H_2. Identify the kernel N_i of $H \to H_{3-i}$ with a subgroup of H_i. Then the image of H in $H/N_1 \times H/N_2$ is the graph of an isomorphism $H/N_1 \to H/N_2$.*
(2) *With assumptions as in part (1), assume that H_1 and H_2 have no common non-trivial quotients. Then $H = H_1 \times H_2$.*
(3) *Suppose that $H_1, \dots, H_n$ are groups with each H_i perfect, and suppose that $H \subset H_1 \times \cdots \times H_n$ is a subgroup such that for all $1 \leq i < j \leq n$, the projection $H \to H_i \times H_j$ is surjective. Then $H = H_1 \times \cdots \times H_n$.*

PROOF. Part (1) is proved in [**35**, Lemma 5.2.1]. Part (2) is immediate from part (1). Part (3) is [**35**, Lemma 5.2.2]. □

8.6.4. Pairwise independence. Our aim in this section is to prove the following pairwise independence result.

PROPOSITION 8.19. *If $\lambda_1 \neq \lambda_2$ are distinct primes in S, then*

$$\pi_1^t(U) \to G_{\chi,\lambda_1} \times G_{\chi,\lambda_2}$$

is surjective.

PROOF. Note that if $r = 2$ then S is a single prime, so the proposition is vacuous. Thus we assume $r > 2$.

We write G_{12} for the image in the proposition, and we note that by the definition of the $G_{\chi,\lambda}$, G_{12} projects surjectively onto each factor G_{χ,λ_i}.

We first treat the case $\ell > 3$. Fix isomorphisms $G_{\chi,\lambda_i} \cong \mathrm{SL}_2(\mathbb{F}_{\lambda_i^+})$ for $i = 1, 2$. Here and below, we write λ_i^+ for the prime of Λ^+ under λ_i . Let $g_{i,0}$ and $g_{i,\infty}$ be the images of γ_0 and $\gamma_\infty \in \pi_1^t(U)$ in $\mathrm{SL}_2(\mathbb{F}_{\lambda_i^+})$. By Proposition 8.11, these are unipotent matrices.

By Lemma 8.18(2) we may assume that G_{χ,λ_1} and G_{χ,λ_2} have common non-trivial quotients. By Lemma 8.16(3) this occurs if and only if $\mathbb{F}_{\lambda_1^+}$ and $\mathbb{F}_{\lambda_2^+}$ have the same cardinality.

If G_{12} is not all of the product, the Lemma 8.18(1) yields either an isomorphism $\mathrm{SL}_2(\mathbb{F}_{\lambda_1^+}) \to \mathrm{SL}_2(\mathbb{F}_{\lambda_2^+})$ or an isomorphism $\mathrm{PSL}_2(\mathbb{F}_{\lambda_1^+}) \to \mathrm{PSL}_2(\mathbb{F}_{\lambda_2^+})$. In the former case, since this isomorphism is induced by the image of $\pi_1^t(U)$ in G_{12}, it sends $g_{1,0}$ to $g_{2,0}$ and $g_{1,\infty}$ to $g_{2,\infty}$. In the latter case, the isomorphism lifts to SL_2 by Lemma 8.17(2). Moreover, the lifted isomorphism sends $g_{1,0}$ to $\pm g_{2,0}$. In fact, by Lemma 8.17(3) the image must be $+g_{2,0}$ because $g_{1,0}$ is unipotent and $-g_{2,0}$ is not. Similarly, the lifted automorphism must send $g_{1,\infty}$ to $g_{2,\infty}$.

Summarizing, if G_{12} is not all of the product, we have an isomorphism

$$\psi : \mathrm{SL}_2(\mathbb{F}_{\lambda_1^+}) \to \mathrm{SL}_2(\mathbb{F}_{\lambda_2^+})$$

such that $\psi(g_{1,0}) = g_{2,0}$ and $\psi(g_{1,\infty}) = g_{2,\infty}$. But such an isomorphism is impossible. Indeed, by Lemma 8.17(1), ψ is the composition of conjugation and a field automorphism $\phi : \mathbb{F}_{\lambda_1^+} \to \mathbb{F}_{\lambda_2^+}$. Since $\psi(g_{1,0}^{-1} g_{1,\infty}^{-1}) = g_{2,0}^{-1} g_{2,\infty}^{-1}$, ϕ must send the trace of $g_{1,0}^{-1} g_{1,\infty}^{-1}$ to the trace of $g_{2,0}^{-1} g_{2,\infty}^{-1}$. By Proposition 8.11(2), these traces are the images of $\zeta + \zeta^{-1} \in \Lambda^+$ in $\mathbb{F}_{\lambda_1^+}$ and $\mathbb{F}_{\lambda_2^+}$. But Lemma 8.8 shows that no such ϕ exists, so no such ψ exists either. We conclude that G_{12} is all of the product, as desired.

Now assume $\ell = 3$. If G_{χ,λ_i} are both $\mathrm{SL}_2(\mathbb{F}_{\ell^a})$ with $a > 1$, then the argument above applies verbatim. Thus it remains to treat the possibilities that $G_{\chi,\lambda_i} \cong \tilde{A}_5$ or $\mathrm{SL}_2(\mathbb{F}_3)$. The $\tilde{A}_5$ case does not in fact occur. Indeed, $G_{\chi,\lambda} \cong \tilde{A}_5$ if and only of $r = 10$, and $\mathcal{O}_{10}^+$ has a unique prime over $\ell = 3$, so there do not exist two distinct primes $\lambda_i \in S$ with $G_{\chi,\lambda_i} \cong \tilde{A}_5$.

The last case to discuss is when $G_{\chi,\lambda_i} \cong \mathrm{SL}_2(\mathbb{F}_3)$, and by Lemma 8.9 this does indeed occur exactly when $4|r$, the two primes being the unique primes over $\ell = 3$ of levels 2 and 4. The argument above is not sufficient in this case, because $\mathrm{SL}_2(\mathbb{F}_3)$ has an additional quotient, namely $\mathbb{Z}/3\mathbb{Z}$. But we may argue directly as follows: By Proposition 8.11, in this case G_{12} is generated by

$$h_0 = \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right) \quad \text{and} \quad h_\infty = \left(\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right).$$

Then we compute directly that

$$\left(g_0 g_\infty g_0^{-1} g_\infty g_0 g_\infty^{-1}\right)^2 = \left(\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

and

$$\left(g_\infty g_0 g_\infty^{-1} g_0 g_\infty g_0^{-1}\right)^2 = \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

It follows immediately that $G_{12} = \mathrm{SL}_2(\mathbb{F}_3) \times \mathrm{SL}_2(\mathbb{F}_3)$. This completes the proof of the proposition. □

8.6.5. End of the proof of Theorem 8.15. We divide S into the disjoint union of

$$S_1 = \{\lambda \in S \,|\, G_{\chi,\lambda} \ncong \mathrm{SL}_2(\mathbb{F}_3)\}$$

and

$$S_2 = \{\lambda \in S \,|\, G_{\chi,\lambda} \cong \mathrm{SL}_2(\mathbb{F}_3)\}.$$

If $\lambda \in S_1$, then by Lemma 8.16, $G_{\chi,\lambda}$ is perfect. Applying Proposition 8.19 and Lemma 8.18(3), we conclude that

$$\pi_1^t(U) \to \prod_{\lambda \in S_1} G_{\chi,\lambda} =: H_1$$

is surjective.

Note that by Lemma 8.9, S_2 has at most two elements, so Proposition 8.19 shows that

$$\pi_1^t(U) \to \prod_{\lambda \in S_2} G_{\chi,\lambda} =: H_2$$

is surjective.

Now H_1 is a product of perfect groups, so is perfect, whereas H_2 is a product of solvable groups, so is solvable. Therefore H_1 and H_2 have no common non-trivial quotients. It follows from Lemma 8.18(2) that

$$\pi_1^t(U) \to H_1 \times H_2$$

is surjective. Since

$$H_1 \times H_2 = \prod_{\lambda \in S} G_{\chi,\lambda},$$

this completes the proof of the theorem. □

8.7. Conclusion

We are now in position to prove the results stated in Section 8.1.

8.7.1. Torsion. In view of Corollary 8.6, the following is a slight strengthening of Theorem 8.1.

THEOREM 8.20. *If L/K is an abelian extension, then $J_r^{new}[\ell](L) = 0$. If $r \neq 2, 4$ or $\ell > 3$, then the same conclusion holds for any solvable extension L/K.*

PROOF. Let L/K be a finite extension and write A for J_r^{new}. Noting that $A[\ell](L) = A[\ell](L \cap K(A[\ell]))$ and that the intersection of a Galois extension with a solvable or abelian extension is again solvable or abelian, we may replace L with $L \cap K(A[\ell])$.

If L/K is abelian, we have $\mathrm{Gal}(K(A[\ell])/L) \supset [G, G]$ where $[G, G]$ is the commutator subgroup of $G = \mathrm{Gal}(K(A[\ell]/K))$. Thus $A[\ell](L) \subset A[\ell](F)$ where F is the subfield of $K(A[\ell])$ fixed by $[G, G]$, and it suffices to show that $A[\ell](F) = 0$.

If $r \neq 2, 4$ or $\ell > 3$, then by Theorem 8.15, $G = \mathrm{Gal}(K(A[\ell]/K))$ is isomorphic to $\mu_r \cdot \mathrm{SL}_2(\mathcal{O}^+/\ell)$ and $\mathrm{SL}_2(\mathcal{O}^+/\ell)$ is a product of groups $\mathrm{SL}_2(\mathbb{F}_\lambda)$ with $|\mathbb{F}_\lambda| > 3$. It follows that the commutator subgroup $[G, G]$ satisfies

$$[G, G] \cong \prod_\lambda \mathrm{SL}_2(\mathbb{F}_\lambda).$$

The invariants of this group acting on $A[\ell] \cong \prod_\lambda \mathbb{F}_\lambda^2$ are trivial, so $A[\ell](F) = 0$ as desired.

If $\ell = 3$ and $r = 2$ or 4, then $G \cong \mu_r \cdot \mathrm{SL}_2(\mathbb{F}_3)$ and $[G, G]$ is the subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ generated by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} -1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$. (This is the 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$.) Since the eigenvalues of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ are $\pm\sqrt{-1}$, already this matrix has no invariants on $\mathbb{F}_3^2$, so *a fortiori* $[G, G]$ has no invariants, and again $A[\ell](F) = 0$ as desired.

If $\ell = 2$, then $G \cong D_{2r}$ and $[G, G] \cong C_r$, the cyclic group of order r. This groups acts on $A[\ell]$ by characters of order r, so has no non-zero invariants, and we again have $A[\ell](F) = 0$.

If L is only assumed to be solvable, the same argument works provided that $\ell > 3$ or $r \neq 2, 4$, because in these cases the derived series of G stabilizes at $\prod_\lambda \mathrm{SL}_2(\mathbb{F}_\lambda)$. □

8.7.2. Decomposition of A_χ. In this section, we prove a slight refinement of Theorem 8.3. Throughout, we assume $r > 2$.

Recall that C_χ was defined by

$$(1 - t)xy^r = (x + 1)(x + t).$$

We observe that there is an involution $\sigma : C_\chi \to C_\chi$ defined by

$$\sigma(x, y) = \left(\frac{-x - t}{x + 1}, \frac{1}{y}\right)$$

and that we have the equality $\sigma\zeta_r = \zeta_r^{-1}\sigma$ of automorphisms of C_χ. There is an induced action of σ on J_χ that preserves $A_\chi = J_\chi^{new}$, and the equality $\sigma\zeta_r = \zeta_r^{-1}\sigma$ holds in the endomorphism ring of A_χ as well.

Let $K' = K((1-t)^{1/r})$, so that A_χ and A become isomorphic over K'. In view of this isomorphism, Theorem 8.3 is implied by the following.

THEOREM 8.21. *Let B be the abelian subvariety $(1+\sigma)A_\chi \subset A_\chi$.*

1. *There is an isogeny $A_\chi \to B^2$ over K whose kernel is killed by multiplication by $2r$.*
2. *$\mathrm{End}_K(B) = \mathrm{End}_{\overline{K}}(B) = \mathbb{Z}[\zeta_r]^+$, and B is absolutely simple.*

PROOF. Define morphisms

$$\begin{aligned} A_\chi &\to (1+\sigma)A_\chi \times (1-\sigma)A_\chi \\ P &\mapsto ((1+\sigma)P, (1-\sigma)P) \end{aligned}$$

and

$$\begin{aligned} (1+\sigma)A_\chi \times (1-\sigma)A_\chi &\to A_\chi \\ (P_1, P_2) &\mapsto P_1 + P_2. \end{aligned}$$

Using that $\sigma^2 = 1$, we find that the compositions are both multiplication by 2. This proves that A_χ is isogenous to $(1+\sigma)A_\chi \times (1-\sigma)A_\chi$ by an isogeny whose kernel is killed by 2.

Now consider the element $\delta = \zeta_r - \zeta_r^{-1}$ of $\mathrm{End}(A_\chi)$. Using that $r > 2$ and considering the action on differentials we see that δ is an isogeny, and since the norm of δ as an element of $\mathbb{Z}[\zeta_r]$ divides r, the kernel of δ is killed by r.

We compute that $(1+\sigma)\delta = \delta(1-\sigma)$ and $(1-\sigma)\delta = \delta(1+\sigma)$, so the isogeny $\delta : A_\chi \to A_\chi$ exchanges the subvarieties $(1+\sigma)A_\chi$ and $(1-\sigma)A_\chi$. In particular, $(1-\sigma)A_\chi$ is isogenous to $B = (1+\sigma)A_\chi$ by an isogeny whose kernel is killed by r.

Combining this with the isogeny $A_\chi \to (1+\sigma)A_\chi \times (1-\sigma)A_\chi$, we see that A_χ is isogenous to $B \times B$ by an isogeny with kernel killed by $2r$. This proves the first part of the theorem.

For the second part, since

$$(1+\sigma)(\zeta_r + \zeta_r^{-1}) = (\zeta_r + \zeta_r^{-1})(1+\sigma),$$

we have that $\mathcal{O}^+ = \mathbb{Z}[\zeta_r]^+ \subset \mathrm{End}_K(B)$. Thus it suffices to prove that $\mathrm{End}_{\overline{K}}(B) = \mathcal{O}^+$.

Let F be a finite extension of K such that all elements of $\mathrm{End}_{\overline{K}}(B)$ are defined over F. Let ℓ be a prime $\neq p$ and not dividing $2r$ such that $\ell > [F:K]$. We claim that restriction induces an isomorphism $\mathrm{Gal}(F(A_\chi[\ell])/F) \cong \mathrm{Gal}(K(A_\chi[\ell])/K)$. Clearly it is injective, so it suffice to show it is onto. Let H be the image, a subgroup of $G_\chi = \mathrm{Gal}(K(A_\chi[\ell])/K)$ and note that the index of H in G_χ is at most $[F:K]$. If $g \in G_\chi$ has order ℓ, then the orbits of g on the coset space G_χ/H have size 1 or ℓ. Since $|G_\chi/H| \leq [F:K] < \ell$, they must have order 1, so $g \in H$. But Theorem 8.15 and the proof of Proposition 8.13 show that G_χ is generated by elements of order ℓ, so $H = G_\chi$, establishing our claim.

Next we note that the existence of the isogeny $A_\chi \to B \times B$ and the isogeny $\delta : A_\chi \to A_\chi$ switching the two factors shows that $F(B[\ell]) = F(A_\chi[\ell])$. Thus we have

$$\mathrm{Gal}(F(B[\ell])/F) \cong \mathrm{Gal}(F(A_\chi[\ell])/F) \cong \mathrm{Gal}(K(A_\chi[\ell])/K) \cong \mathrm{SL}_2(\mathcal{O}^+/\ell)$$

where the last isomorphism is Theorem 8.15.

Now we assume for convenience that ℓ splits completely in $\mathbb{Q}(\zeta_r)^+$, i.e., that $\ell \equiv \pm 1 \in (\mathbb{Z}/r\mathbb{Z})^\times$. In this case $\mathcal{O}^+/\ell$ is the product of $\phi(r)/2$ copies of $\mathbb{F}_\ell$ and $\mathrm{SL}_2(\mathcal{O}^+/\ell)$ is the product of $\phi(r)/2$ copies of $\mathrm{SL}_2(\mathbb{F}_\ell)$. The $\mathbb{F}_\ell$-subalgebra of $\mathrm{Aut}_{\mathbb{F}_\ell}(B[\ell]) \cong M_{\phi(r)}(\mathbb{F}_\ell)$ generated by $\mathrm{SL}_2(\mathcal{O}^+/\ell)$ is then isomorphic to the

product of $\phi(r)/2$ copies of $M_2(\mathbb{F}_\ell)$ and thus has dimension $2\phi(r)$. By the double centralizer theorem **[25**, Theorem. 2.43], the centralizer of $\mathrm{SL}_2(\mathcal{O}^+)$ in $\mathrm{Aut}_{\mathbb{F}_\ell}(B[\ell])$ has dimension $\phi(r)/2$ over $\mathbb{F}_\ell$. Since $\mathrm{End}_F(B)/\ell$ lies in this centralizer, it has dimension at most $\phi(r)/2$, and thus $\mathrm{End}_F(B)$ has $\mathbb{Z}$-rank at most $\phi(r)/2$. But $\mathcal{O}^+ \subset \mathrm{End}_F(B)$ has $\mathbb{Z}$-rank $\phi(r)/2$ and is a maximal order in its fraction field, so we have $\mathcal{O}^+ = \mathrm{End}_F(B) = \mathrm{End}_{\overline{K}}(B)$, as desired.

Finally, we note that since $\mathrm{End}_{\overline{K}}(B)$ is a domain, B is absolutely simple.

This completes the proof. □

8.7.3. Simplicity of A. Note that $k(t^{1/d})$ is linearly disjoint from $k((1-t)^{1/r})$ for any value of d. Thus the following implies Theorem 8.2.

THEOREM 8.22. *Suppose that F is a finite extension of K that is linearly disjoint from $k((1-t)^{1/r})$. Then $A = J_r^{new}$ is simple over F, and we have $\mathrm{End}_F(A) \cong \mathbb{Z}[\zeta_r]$.*

PROOF. $\mathcal{O} = \mathbb{Z}[\zeta_r]$ is a domain, so if $\mathrm{End}_F(A) \cong \mathcal{O}$, then A is simple over F. It thus suffices to show that $\mathrm{End}_F(A) \cong \mathcal{O}$.

Noting that $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q} = M_2(\mathbb{Q}(\zeta_r)^+)$ is a central simple algebra of dimension 4 over $\mathbb{Q}(\zeta_r)^+$, the double centralizer theorem implies that

$$\dim_{\mathbb{Q}(\zeta_r)} (\mathrm{End}_F(A) \otimes \mathbb{Q}) \leq 2.$$

But $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ is generated over $\mathbb{Q}(\zeta_r)$ by 1 and σ. Our hypothesis on F and Proposition 8.15 imply that there is an element of $\mathrm{Gal}(F(A[\ell])/F)$ acting on $A[\ell]$ as ζ_r. Since σ does not commute with ζ_r, we conclude that $\sigma \notin \mathrm{End}_F(A)$ and therefore $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q} = \mathbb{Q}(\zeta_r)$. Since $\mathcal{O}$ is the maximal order in $\mathbb{Q}(\zeta_r)$, we have $\mathrm{End}_F(A) \cong \mathcal{O}$, as desired. □

APPENDIX A

An additional hyperelliptic family

A.1. Introduction

In Section 1.6, we write that the methods used in this paper may be applied to the study of the arithmetic of Jacobians of other generalizations of the Legendre curve. In this appendix, we give more details on a family of curves mentioned in that section.

Let g denote an odd positive integer, p an odd prime, and k a finite field of characteristic p and cardinality q. Let $a_1, \ldots, a_g \in k$ be distinct and non-zero, and let X be the smooth, projective, hyperelliptic curve over $K = k(t)$ with affine model

$$y^2 = x \prod_{i=1}^{g} (x + a_i)(a_i x + t). \tag{A.1}$$

Note that X has genus g. When $g = 1$, X is essentially the Legendre curve, and there are differences between the cases $g = 1$ and $g > 1$, so from now on we assume that $g > 1$.

Write J_X for the Jacobian of X. Let ν be a nonnegative integer, $d = q^\nu + 1$, and set $K_d = k(\mu_d, u)$ where $u^d = t$. Our main object of study is the Mordell-Weil group $J_X(K_d)$ and a certain subgroup of it generated by explicit divisors on X.

The principal results of this appendix are:

Theorem A.1.

(1) *J_X satisfies the conjecture of Birch and Swinnerton-Dyer over each of the fields K_d.*
(2) *The 2-power torsion subgroup of $J(K_d)$ has the form*

$$(\mathbb{Z}/2^a\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^{2g-1}$$

for some integer $a > 1$.
(3) *The rank of $J_X(K_d)$ is at least $d - 1$.*
(4) *The rank of $J_X(K_d)$ is at most $g^2 d$.*

The proof of the theorem will occupy the rest of the appendix. For point (3), we will exhibit explicit divisors generating a subgroup of $J_X(K_d)$ of rank at least $d - 1$.

A.2. The BSD conjecture

In this section, we prove part (1) of Theorem A.1.

Consider the curve X over K_d and let $\mathcal{X}_d$ be a smooth, projective surface over $k(\mu_d)$ equipped with a morphism $\mathcal{X}_d \to \mathbb{P}^1$ whose generic fiber is X/K_d. One may

construct $\mathcal{X}_d$ starting from the affine surface over $k(\mu_d)$ defined by

$$y^2 = x\prod_{i=1}^{g}(x+a_i)(a_ix+u^d)$$

together with its projection to the affine line with coordinate u.

As reviewed in [**51**] (and already used in Theorem 5.2), in order to show that $\mathcal{X}_d$ satisfies the Tate conjecture and J_X satisfies the BSD conjecture, it suffices to show that $\mathcal{X}_d$ is dominated by a product of curves.

To show that the surface $\mathcal{X}_d$ admits a dominant rational map from a product of curves, we consider the affine surface $\mathcal{Y}_d$ defined by the equation

$$x^g y^2 = \prod_{i=1}^{g}(x+a_i)(a_ix+u^d).$$

Observe that since g is odd, $\mathcal{Y}_d$ is birational to $\mathcal{X}_d$.

Let $\mathcal{C}_d$ denote the smooth, affine curve defined by the equation

$$w^2 = \prod_{i=1}^{g}(z^d+a_i).$$

Define a morphism

$$\varphi : \mathcal{C}_d \times \mathcal{C}_d \to \mathcal{Y}_d$$

by $(w_1, z_1, w_2, z_2) \mapsto (x, y, u) = (z_1^d, w_1w_2, z_1z_2)$. It is easy to see that φ is generically finite of degree $2d$. This proves that $\mathcal{Y}_d$, and thus $\mathcal{X}_d$, is dominated by a product of curves, and it completes the proof of part (1) of Theorem A.1.

Since it is easy to do so, we add some further details on φ. First, note that $\mathcal{C}_d$ admits an action of the group $G = \mu_2 \times \mu_d$. Let G act on $\mathcal{C}_d \times \mathcal{C}_d$ "anti-diagonally"; that is, for $g \in G$ and $P, Q \in \mathcal{C}_d(\overline{K})$, we define

$$(P,Q)^g = (P^g, Q^{g^{-1}}).$$

We claim that φ induces a birational isomorphism from the quotient $(\mathcal{C}_d \times \mathcal{C}_d)/G$ to the surface $\mathcal{X}_d$. Indeed, it is clear from the expression defining φ that φ factors through the quotient, and therefore induces a dominant rational map of degree 1, in other words, a birational isomorphism.

We note that the arguments of this section prove more generally that the BSD conjecture holds for X over the fields $\mathbb{F}_{q^n}(t^{1/d})$ for any n and any d prime to p.

A.3. Descent

In this section, we prove parts (2) and (3) of Theorem A.1.

Let Q_∞ be the unique point at infinity with respect to the model (A.1). We embed X in J_X using Q_∞ as a base point:

$$\begin{aligned} X &\to J_X \\ P &\mapsto P - Q_\infty, \end{aligned}$$

and we identify points of X with their images in J_X.

Let Q_0 denote the point $(0,0)$. For $1 \le j \le g$, let Q_j denote the point $(-a_j, 0)$, and let Q_j' denote the point $(-t/a_j, 0)$. These (together with Q_∞) are the Weierstrass points of X, they are K-rational, and it is well known that their images in

J_X generate its 2-torsion subgroup. The divisor of the function y is

$$Q_0 + \sum_{j=1}^{g} \left(Q_j + Q'_j\right) - (2g+1)Q_\infty,$$

so

$$Q_0 = -\sum_{j=1}^{g} \left(Q_j + Q'_j\right) = \sum_{j=1}^{g} \left(Q_j + Q'_j\right) \tag{A.2}$$

in J_X. Thus the points Q_j and Q'_j for $1 \leq j \leq g$ form a basis of the $\mathbb{F}_2$-vector space $J_X(K)[2]$.

Fix a primitive d-th root of unity ζ_d in K_d. For $0 \leq j \leq d-1$, let

$$P_j = \left(\zeta_d^j u, (\zeta_d^j u)^{(g+1)/2} \prod_{i=1}^{g} (\zeta_d^j u + a_i)^{d/2}\right).$$

Recall that g is odd, and that q is odd, so $d = q^\nu + 1$ is even. Observe that the P_j are in $X(K_d)$. Indeed, substituting $\zeta_d^j u$ for x in the right hand side of (A.1), we find

$$\begin{aligned} \zeta_d^j u \prod_{i=1}^{g} (\zeta_d^j u + a_i)(a_i \zeta_d^j u + u^d) &= \zeta_d^j u \prod_{i=1}^{g} (\zeta_d^j u + a_i) \zeta_d^j u (\zeta_d^{-j} u^{q^\nu} + a_i) \\ &= (\zeta_d^j u)^{g+1} \prod_{i=1}^{g} (\zeta_d^j u + a_i)^{q^\nu + 1} \end{aligned}$$

since $a_i^{q^\nu} = a_i$ and $\zeta_d^{q^\nu} = \zeta_d^{-1}$.

Let T be the subgroup of $J_X(K_d)$ generated by the Q_j and Q'_j, and let V be the subgroup of $J_X(K_d)$ generated by T and the P_j. Using a map related to 2-descent, we are going to prove that the image of T in $J_X(K_d)/2J_X(K_d)$ has dimension $2g-1$ and that the image of V in $J_X(K_d)/2J_X(K_d)$ has dimension $d + 2g - 1$.

These assertions imply parts (2) and (3) of Theorem A.1 by a standard descent argument which we now review. We have already seen that T, the subgroup generated by the Q_j and Q'_j, is equal to $J_X(K_d)[2]$. By the structure theorem for finitely generated abelian groups, the 2-power torsion subgroup $J_X(K_d)[2^\infty]$ satisfies

$$J_X(K_d)[2^\infty] \cong \bigoplus_{\ell=1}^{t} (\mathbb{Z}/2^{e_\ell}\mathbb{Z})$$

for uniquely determined integers t and e_ℓ with $e_1 \geq e_2 \geq \cdots \geq e_t > 0$. Since $J_X(K_d)[2]$ has dimension $2g$ over $\mathbb{F}_2$, we have that $t = 2g$. Once we know that the image of $J_X(K_d)[2]$ in $J_X(K_D)/2J_X(K_d)$ has dimension $2g-1$, we find that exactly one of the e_ℓ is > 1. This reduces part (2) of Theorem A.1 to our claim that the image of T in $J_X(K_d)/2J_X(K_d)$ has dimension $2g-1$.

For part (3), we note that the structure theorem for finitely generated abelian groups plus the calculation that $J_X(K_d)[2]$ has dimension $2g$ over $\mathbb{F}_2$ implies that

$$\dim_{\mathbb{F}_2} \left(J_X(K_d)/2J_X(K_d)\right) = \rho + 2g$$

where ρ is the rank of $J_X(K_d)$. Once we know that the dimension of the image of V in $J_X(K_d)/2J_X(K_d)$ is $d+2g-1$, we may conclude that $\rho \geq d-1$. This reduces part (3) of Theorem A.1 to our claim that the image of V in $J_X(K_d)/2J_X(K_d)$ has dimension $d + 2g - 1$.

We now turn to calculating the dimensions of the images of T and V in $J_X(K_d)/2J_X(K_d)$. In parallel with the discussion in Section 2.2, we define a 2-descent map

$$(x-T)\colon \operatorname{Div} X(K_d) \longrightarrow \left(K_d^\times/K_d^{\times 2}\right)^{2g+1}$$

to serve as a substitute for the coboundary map from $J_X(K_d)/2J_X(K_d)$ to the cohomology group $H^1(K_d, J_X[2])$. We start by defining a map

$$(x-T)\colon X(K_d) \longrightarrow \left(K_d^\times/K_d^{\times 2}\right)^{2g+1}$$

and then extend by $\mathbb{Z}$-linearity to $\operatorname{Div} X(K_d)$.

To lighten notation, write W for $(K_d^\times/K_d^{\times 2})^{2g+1}$ and

$$\underline{w} = (w_0, w_1, \dots, w_g, w_1', \dots, w_g')$$

for an element of W. If $P \in X(K_d)$ and $P \neq Q_j, Q_j', Q_\infty$, then the map is defined by

$$(x-T)(P) = (w_0, w_1, \dots, w_g, w_1', \dots, w_g')$$

where

$$\begin{aligned} w_0 &= x(P), \\ w_i &= x(P) + a_i \qquad \text{for } 1 \le i \le g, \\ w_i' &= a_i x(P) + t \qquad \text{for } 1 \le i \le g. \end{aligned}$$

When $P = Q_j$ or Q_j', this expression needs further clarification, since it gives zero for one coordinate. Instead, we set the value at that coordinate to be the product of the other coordinates (cf. Prop 2.7). Finally, we define $(x-T)(Q_\infty) = (1, 1, \dots, 1)$.

An analysis parallel to that in Chapter 2 and [**8**] shows that the composition

$$\begin{aligned} \operatorname{Div}^0 X(K_d) \to J_X(K_d) \to J_X(K_d)/2J_X(K_d) \\ \hookrightarrow H^1(K_d, J_X[2]) \subset \left(K_d^\times/K_d^{\times 2}\right)^{2g+1} \end{aligned}$$

is equal to the restriction of $(x-T)$ to $\operatorname{Div}^0 X(K_d)$. In particular, to compute the images of T and V in $J_X(K_d)/2J_X(K_d)$, it will suffice to compute their images in W, i.e., their images under $(x-T)$.

Note that t and the elements of $k = \mathbb{F}_q$ are squares in $K_d^\times$, i.e., trivial in $K_d^\times/K_d^{\times 2}$. From this it follows that $(x-T)(Q_0)$ is trivial, and in view of (A.2), we have

$$(x-T)\left(\sum_{j=1}^{g}\left(Q_j + Q_j'\right)\right) = (1, \dots, 1).$$

(This can also of course be checked directly.) It follows that the dimension of the image of T in W is at most $2g-1$ and the dimension of V in W is at most $d+2g-1$. To complete the proof, we must show that these inequalities are in fact equalities.

Observe that the field of constants in K_d is isomorphic to $\mathbb{F}_{q^{2\nu}}$. The norm map

$$\mathbb{F}_{q^{2\nu}}^\times \longrightarrow \mathbb{F}_{q^\nu}^\times$$

is given by $\alpha \mapsto \alpha^d$ and is surjective. It follows that any $a \in k = \mathbb{F}_q$ has a d-th root in K_d, and the place of $K = k(t)$ where $t-a$ vanishes splits into d places in K_d. These are the places where $u - \zeta_d^j \alpha$ vanishes with $0 \le j \le d-1$ and α a fixed d-th root of a.

Now fix a d-th root α_i of $a_1 a_i$ for $1 \le i \le g$. It will be convenient later to assume that $\alpha_1 = -a_1$. (This is legitimate, since $a_1 \in \mathbb{F}_q$ so $(-a_1)^d = (-a_1)^{q+1} = a_1^2$.) Let π_i be the place of K_d where $u - \alpha_i$ vanishes, and let ord_{π_i} be the corresponding valuation.

In parallel with the proof of Prop. 2.8, define a linear map $pr_1 : W \to \mathbb{F}_2^{2g}$ by

$$pr_1(\underline{w}) = \left(\mathrm{ord}_{\pi_1}(w_1), \ldots, \mathrm{ord}_{\pi_g}(w_1), \mathrm{ord}_{\pi_1}(w_1'), \ldots, \mathrm{ord}_{\pi_g}(w_1')\right).$$

Let I be the $g \times g$ identity matrix over $\mathbb{F}_2$ and let B be the $g \times g$ matrix over $\mathbb{F}_2$ whose first row entries are all 1 and whose other entries are 0. Then a straightforward application of the definitions shows that the matrix whose rows are $\mathrm{pr}_1 \circ (x - T)(Q_j)$ (for $1 \le j \le g$) followed by $\mathrm{pr}_1 \circ (x - T)(Q_j')$ (for $1 \le j \le g$) has the form

$$\begin{pmatrix} B & I \\ I & B \end{pmatrix}. \tag{A.3}$$

This matrix has rank $2g - 1$ which implies that the dimension of the image of T in W is $2g - 1$. This completes the proof of part (2) of Theorem A.1.

Working toward part (3) of the theorem, we next consider the images of the points P_j under $pr_1 \circ (x - T)$. Keeping in mind our choice of α_1 above, we find that

$$pr_1 \circ (x - T)(P_j) = \begin{cases} (1, 0, \ldots, 0, 1, 0, \ldots, 0) & \text{if } j = 0 \\ (0, \ldots, 0) & \text{if } j \ne 0 \end{cases} \tag{A.4}$$

where the entries 1 appear in columns 1 and $g + 1$. In particular, using equations (A.3) and (A.4), we have

$$pr_1 \circ (x - T)(P_0) = pr_1 \circ (x - T) \left(Q_1 + \sum_{j=2}^{g} Q_j' \right) \tag{A.5}$$

$$= pr_1 \circ (x - T) \left(Q_1' + \sum_{j=2}^{g} Q_j \right). \tag{A.6}$$

It follows that the image of V in $\mathbb{F}_2^{2g}$ is the same as the image of T in $\mathbb{F}_2^{2g}$, and this image has dimension $2g - 1$. Let V_1 denote the kernel of the map

$$pr_1 \circ (x - T) : V \to \mathbb{F}_2^{2g}.$$

We have that V_1 contains $2V$, P_j for $1 \le j \le d - 1$, and (by equations (A.5) and (A.6)) the elements

$$P_0 + Q_1 + \sum_{j=2}^{g} Q_j' \quad \text{and} \quad P_0 + Q_1' + \sum_{j=2}^{g} Q_j.$$

A dimension count then shows that these elements generate V_1.

Now we introduce a second projection $pr_2 : W \to \mathbb{F}_2^d$. Namely, let ρ_j be the place of K_d where $u + \zeta_d^{-j} a_1$ vanishes, and let ord_{ρ_j} be the corresponding valuation. Then define

$$pr_2(\underline{w}) = \left(\mathrm{ord}_{\rho_0}(w_1), \ldots, \mathrm{ord}_{\rho_{d-1}}(w_1)\right).$$

Let $e_0, \ldots, e_{d-1}$ be the standard basis of $\mathbb{F}_2^d$ with a shift of one in the indexing (so $e_0 = (1, 0, \ldots, 0)$ and $e_{d-1} = (0, \ldots, 0, 1)$). Then a straightforward calculation

reveals that

$$\begin{aligned} pr_2 \circ (x-T)(P_j) &= e_j, \\ pr_2 \circ (x-T)(Q_1) &= \sum_{\ell=0}^{d-1} e_\ell, \\ pr_2 \circ (x-T)(Q_j) &= 0 \quad \text{for } 2 \le j \le g, \\ pr_2 \circ (x-T)(Q'_1) &= \sum_{\ell=0}^{d-1} e_\ell, \end{aligned}$$

and

$$pr_2 \circ (x-T)(Q'_j) = 0 \quad \text{for } 2 \le j \le g.$$

It follows easily that $pr_2 \circ (x-T)$ sends V_1 surjectively onto the codimension 1 subspace of $\mathbb{F}_2^d$ where the first entry vanishes. Denoting by V_2 the kernel of $pr_2 \circ (x-T)$ on V_1, we also see that V_2 is generated by $2V$ and the element

$$\sum_{j=0}^{d-1} P_j + Q_1 + \sum_{j=2}^{g} Q'_j.$$

To finish the proof, we note that

$$(x-T)\left(\sum_{j=0}^{d-1} P_j + Q_1 + \sum_{j=2}^{g} Q'_j\right) \neq 0.$$

For example, its component w_2 is

$$\prod_{\ell=3}^{g} (t - a_2 a_\ell),$$

and this is not a square in K_d since the a_i are distinct.

In summary, we have shown that V/V_1 has dimension $2g-1$, V_1/V_2 has dimension $d-1$ and V_2 has a 1-dimensional image in W. This shows that the image of V in W has dimension $d+2g-1$, and this completes the proof of part (3) of Theorem A.1.

A.4. Degree of the L-function

In this section, we sketch a proof of part (4) of Theorem A.1.

Since the BSD conjecture holds for J_X, the rank of $J_X(K_d)$ is equal to the order of vanishing of $L(J_X/K_d, s)$ at $s = 1$. We will show that the L-function is a polynomial in q^{-s} and estimate its degree, thus giving an upper bound on the order of vanishing and the rank.

It is known that $L(J_X/K_d, s)$ is a rational function in q^{-s} and that it is a polynomial in q^{-s} if and only if the K/k-trace of J_X (or more precisely, the $K_d/k(\mu_d)$-trace) vanishes; see [**51**, Chap. 5, Lemma 6.5]. Arguing as in Proposition 6.31 and using the explicit domination of $\mathcal{X}_d$ by a product of curves given in Section A.2, we see that the trace vanishes and the L-function is a polynomial.

To complete this sketch we estimate the degree of the L-function of the Jacobian, and thus determine the upper bound on the rank. By the Grothendieck-Ogg-Shafarevich formula, the degree of the L-function is

$$-4g_X + \deg(\mathfrak{n})$$

where $\mathfrak{n}$ denotes conductor of J_X over K_d and $\deg(\mathfrak{n})$ denotes its degree.

We start by considering the case $d = 1$.

For $1 \leq i \leq j \leq g$, let S be the set of places corresponding to the polynomials $t - a_i a_j$. Letting c_v be as in Section 5.1.3, one checks that $\mathcal{X}_1$ has semistable reduction at each such place and that

$$\sum_{v \in S} c_v = g + 2\binom{g}{2} = g^2.$$

More precisely, for each pair $i \leq j$, the reduction of X at $t - a_i a_j$ has ordinary double points at $(x, y) = (a_i, 0)$ and $(x, y) = (a_j, 0)$, and their contribution to the conductor is 1 when $i = j$ and 2 when $i < j$. Moreover, the reduction of X is smooth away from such double points, so it suffices to count the number of pairs (i, j) with $1 \leq i, j \leq g$.

The only other places of (possibly) bad reduction are at $t = 0, \infty$. We claim the Tate module of J_X has tame reduction there and thus the corresponding contribution to the conductor equals the drop of the degree of the corresponding Euler factor (which is between 0 and $2g$). Indeed, the extension $K(J_X[4])$ is Galois over K_1 of degree a power of two, so it is a tamely ramified extension of K. Moreover, J_X acquires semiabelian reduction over it. In particular, this implies the Tate module of J_X is everywhere tamely ramified over the extension $K(J_X[4])$ and hence over K.

Now we consider the case $d > 1$.

For each of the d places of K_d over $t - a_i a_j$, the contribution to the conductor remains unchanged, so is 1 when $i = j$ and 2 when $i < j$. Moreover, the contribution to the conductor is between 0 and $2g$ for $u = 0, \infty$. Therefore we have

$$\deg(\mathfrak{n}) \leq d \cdot \sum_{v \in S} c_v + 2 \cdot 2g = dg^2 + 4g$$

which implies that the degree of the L-function is $\leq dg^2$. It follows that the rank of the Mordell-Weil group of $J_X(K_d)$ is also at most $g^2 d$. This completes our sketch of the proof of part (4) of Theorem A.1.

A.5. Additional remarks

REMARK A.2. It is interesting to note the differences between the Jacobian studied in this appendix and the Legendre curve E studied in **[52]**. In particular, the rank of $J_X(K_d)$ is either $d - 1$ or d, whereas the rank of $E(K_d)$ is $d - 2$. There are two relations among the analogues of the P_j on E which seem not to generalize readily to X, although it is possible that there is one relation.

REMARK A.3. There is an interesting involution of X, given in the coordinates above by

$$\iota(x, y) = \left(t/x, yt^{(g+1)/2}/x^{g+1}\right).$$

(An analogous involution exists for E, where it is translation by Q_0.) On X, we have $\iota(Q_0) = Q_\infty$, $\iota(Q_i) = Q_i'$ for $1 \leq i \leq g$, and $\iota(P_j) = P_j'$ where the P_j' are new points with coordinates

$$P_j' = \left(\zeta_d^{-j} u^{q^\nu}, (\zeta_d^{-j} u^{q^\nu})^{(g+1)/2} \prod_{i=1}^{g} (\zeta_d^j u + a_i)^{d/2} \right).$$

We do not know whether these points are independent of the P_j.

It would be interesting to investigate the consequences for the monodromy of $J_X[\ell]$ of the existence of ι, along the lines of Chapter 8.

Bibliography

[1] Ahmed Abbes, *Réduction semi-stable des courbes d'après Artin, Deligne, Grothendieck, Mumford, Saito, Winters, ...*, Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., vol. 187, Birkhäuser, Basel, 2000, pp. 59–110.

[2] Michael Artin, *Coverings of the rational double points in characteristic p*, Complex analysis and algebraic geometry, Iwanami Shoten, Tokyo, 1977, pp. 11–22.

[3] Lucian Bădescu, *Algebraic surfaces*, Universitext, Springer-Verlag, New York, 2001, Translated from the 1981 Romanian original by Vladimir Maşek and revised by the author.

[4] Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius Van de Ven, *Compact complex surfaces*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 4, Springer-Verlag, Berlin, 2004.

[5] Lisa Berger, *Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields*, J. Number Theory **128** (2008), no. 12, 3013–3030.

[6] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

[7] Irene Bouw and Stefan Wewers, *Computing L-functions and semi-stable reduction of superelliptic curves*, `http://arxiv.org/abs/1211.4459`, 2014.

[8] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, `http://arxiv.org/abs/1205.4456`, 2012.

[9] Henri Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007. MR 2312337

[10] Ricardo Conceição, Chris Hall, and Douglas Ulmer, *Explicit points on the Legendre curve II*, Math. Res. Lett. **21** (2014), no. 2, 261–280.

[11] Brian Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*, Enseign. Math. (2) **52** (2006), 37–108.

[12] Michel Demazure and Alexander Grothendieck, *Schémas en groupes. I: Propriétés générales des schémas en groupes*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151, Springer-Verlag, Berlin-New York, 1970.

[13] William J. Gordon, *Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer*, Compositio Math. **38** (1979), 163–199.

[14] Daniel Gorenstein, *Finite groups*, Harper & Row, Publishers, New York-London, 1968.

[15] Alexander. Grothendieck, *Éléments de géométrie algébrique. I. Le langage des schémas*, Inst. Hautes Études Sci. Publ. Math. (1960), no. 4, 228.

[16] Alexander Grothendieck, *Géométrie formelle et géométrie algébrique*, Séminaire Bourbaki, Vol. 5, Soc. Math. France, Paris, 1995, pp. Exp. No. 182, 193–220, errata p. 390.

[17] Alexander Grothendieck and Michel Raynaud, *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3, Société Mathématique de France, Paris, 2003.

[18] Chris Hall, *Monodromy of some superelliptic curves*, in preparation.

[19] Joe Harris, *Algebraic geometry: A first course*, Graduate Texts in Mathematics, vol. 133, Springer-Verlag, New York, 1992.

[20] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977.

[21] James E. Humphreys, *Introduction to Lie algebras and representation theory*, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, New York-Berlin, 1978, Second printing, revised.

[22] Kazuya Kato and Fabien Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$*, Invent. Math. **153** (2003), no. 3, 537–592.
[23] Steven L. Kleiman, *Relative duality for quasicoherent sheaves*, Compositio Math. **41** (1980), no. 1, 39–60.
[24] ———, *The Picard scheme*, Fundamental algebraic geometry, Math. Surveys Monogr., vol. 123, Amer. Math. Soc., Providence, RI, 2005, pp. 235–321.
[25] Anthony W. Knapp, *Advanced algebra*, Cornerstones, Birkhäuser Boston Inc., Boston, MA, 2007.
[26] K. Kodaira, *Complex manifolds and deformation of complex structures*, english ed., Classics in Mathematics, Springer-Verlag, Berlin, 2005, Translated from the 1981 Japanese original by Kazuo Akao.
[27] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002.
[28] Qing Liu, Dino Lorenzini, and Michel Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. Math. **157** (2004), 455–518.
[29] James S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.
[30] ———, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
[31] ———, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.
[32] Carl Pomerance and Douglas Ulmer, *On balanced subgroups of the multiplicative group*, Number Theory and Related Fields: In Memory of Alf van der Poorten, Springer, New York, 2013, pp. 253–270.
[33] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.
[34] Rachel Pries and Douglas Ulmer, *Arithmetic of abelian varieties in Artin-Schreier extensions*, to appear in the Transactions of the American Mathematical Society. `http://arxiv.org/abs/1305.5247`, 2013.
[35] Kenneth Ribet, *Galois action on division points of abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804.
[36] Takeshi Saito, *Vanishing cycles and geometry of curves over a discrete valuation ring*, Amer. J. Math. **109** (1987), no. 6, 1043–1085.
[37] Jean-Pierre Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium internacional de topología algebraica International symposium on algebraic topology, Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958, pp. 24–53.
[38] ———, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou: 1969/70, Théorie des Nombres, Fasc. 2, Exp. 19, Secrétariat mathématique, Paris, 1970, p. 12.
[39] ———, *Groupes algébriques et corps de classes*, Hermann, Paris, 1975, Deuxième édition, Publication de l'Institut de Mathématique de l'Université de Nancago, No. VII, Actualités Scientifiques et Industrielles, No. 1264.
[40] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979.
[41] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.
[42] Tetsuji Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), no. 2, 415–432.
[43] ———, *Mordell-Weil lattices for higher genus fibration over a curve*, New trends in algebraic geometry (Warwick, 1996), London Math. Soc. Lecture Note Ser., vol. 264, Cambridge Univ. Press, Cambridge, 1999, pp. 359–373.
[44] Tetsuji Shioda and Toshiyuki Katsura, *On Fermat varieties*, Tôhoku Math. J. (2) **31** (1979), no. 1, 97–115.
[45] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1966, pp. Exp. No. 306, 415–440.
[46] John Tate and Igor R. Shafarevich, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), 770–773.

[47] D. Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions (Park City, UT, 2009), IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280.

[48] Douglas Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), 295–315.

[49] ———, *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, Invent. Math. **167** (2007), 379–408.

[50] ———, *On Mordell-Weil groups of Jacobians over function fields*, J. Inst. Math. Jussieu **12** (2013), no. 1, 1–29.

[51] ———, *Curves and Jacobians over function fields*, Arithmetic Geometry over Global Function Fields, Advanced Courses in Mathematics CRM Barcelona, Springer Basel, 2014, pp. 281–337.

[52] ———, *Explicit points on the Legendre curve*, J. Number Theory **136** (2014), 165–194.

[53] ———, *Explicit points on the Legendre curve III*, Algebra and Number Theory **8** (2014), no. 10, 2471–2522.

[54] Douglas Ulmer and José Felipe Voloch, *On the number of rational points on special families of curves over function fields*, `http://arXiv.org/abs/1612.04325`, 2016.

[55] Douglas Ulmer and Yuri G. Zarhin, *Ranks of Jacobians in towers of function fields*, Math. Res. Lett. **17** (2010), no. 4, 637–645.

[56] C. Voisin, *Hodge theory and complex algebraic geometry. I*, english ed., Cambridge Studies in Advanced Mathematics, vol. 76, Cambridge University Press, Cambridge, 2007, Translated from the French by Leila Schneps.

[57] José Felipe Voloch, *Diophantine approximation on abelian varieties in characteristic p*, Amer. J. Math. **117** (1995), no. 4, 1089–1095.

[58] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[59] André Weil, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser, Boston, Mass., 1982, with appendices by M. Demazure and Takashi Ono.

[60] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009.