JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Shahed SHARIF

A descent map for curves with totally degenerate semi-stable reduction

Tome 25, n° 1 (2013), p. 211-244.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_1_211_0>

Journal de Théorie des Nombres
de Bordeaux **25** (2013), 211-244

A descent map for curves with totally degenerate semi-stable reduction

par Shahed SHARIF

Résumé. Soit K un corps local de caractéristique résiduelle p. Soit C une courbe sur K dont le modèle régulier propre mimimal a réduction semi-stable totalement dégénérée. Sous certaines hypothèses, nous calculons le sous-groupe rationnel de torsion première à p dans la jacobienne de C. Nous déterminons aussi la divisibilité de fibrés en droites sur C, incluant la rationalité des thêta-caractéristiques et des structures de spin supérieures. Ces calculs utilisent l'arithmétique de la fibre spéciale de C.

Abstract. Let K be a local field of residue characteristic p. Let C be a curve over K whose minimal proper regular model has totally degenerate semi-stable reduction. Under certain hypotheses, we compute the prime-to-p rational torsion subgroup on the Jacobian of C. We also determine divisibility of line bundles on C, including rationality of theta characteristics and higher spin structures. These computations utilize arithmetic on the special fiber of C.

1. Introduction

Let K be a local field with residue field k of characteristic $p > 0$; that is, K is a finite extension of the p-adic field $\mathbb{Q}_p$, or it is $\mathbb{F}_q((T))$ where q is a power of p. Write G for the absolute Galois group of K, and $\mathfrak{g}$ for the absolute Galois group of the residue field. Let C be a smooth, proper, geometrically integral curve over K with genus $g \geq 2$. Letting $\mathscr{C}$ be the minimal proper regular model for C over the discrete valuation ring $\mathscr{O}_K$ of K, we write C_k for the special fiber. Let $C_{\overline{k}}$ be the base-extension of the special fiber to $\overline{k}$, the algebraic closure of the residue field; it equals the special fiber of the minimal proper regular model for C over K^u, the maximal unramified extension of K. We will assume that C has totally degenerate semi-stable reduction; that is, $C_{\overline{k}}$ is connected, reduced and consists of a finite collection of $\mathbb{P}^1$s such that a formal neighborhood of each singularity is isomorphic to $\operatorname{Spec} \overline{k}[[x, y]]/(xy)$.

Manuscrit reçu le 8 mars 2012.

Let $\mathrm{Pic}_{C/K}$ denote the Picard scheme of C/K, and $\mathrm{Pic}\, C$ the Picard group, with $\mathrm{Pic}\, C \subseteq \mathrm{Pic}_{C/K}(K)$. (These are equal if $C(K) \neq \varnothing$, but not generally.) Let r be a positive integer. As $\mathrm{Pic}_{C/K}$ is an abelian scheme, we have a multiplication-by-r morphism

$$[r] : \mathrm{Pic}_{C/K} \longrightarrow \mathrm{Pic}_{C/K}$$

which induces group homomorphisms $[r] : \mathrm{Pic}_{C/K}(K) \to \mathrm{Pic}_{C/K}(K)$ and $[r] : \mathrm{Pic}\, C \to \mathrm{Pic}\, C$. Little is known in general about the image of these maps. The canonical sheaf defines a canonical element in $\mathrm{Pic}\, C$, and it is natural to wonder whether this element is in the image of any of the maps $[r]$. In this article, we investigate this problem in the case $p \nmid r$ (which we henceforth assume), and provide a method for answering this type of question when the reduction of the Jacobian of the curve is purely toric. Under certain conditions on C_k, we will define a subgroup $\mathrm{Pic}^{\{r\}}\, C \subseteq \mathrm{Pic}\, C$, a finite set of classes D_i, a finite collection of finite cyclic groups μ_i, and maps $\gamma_i : \mathrm{Pic}^{\{r\}}\, C \to \mu_i$ which satisfy the following condition:

Theorem 1.1. *Given $L \in \mathrm{Pic}^{\{r\}}\, C$, we have $L \in r\,\mathrm{Pic}\, C$ if and only if there is some D_j such that $L + D_j \in \ker \gamma_i$ for every i.*

The above result, phrased more explicitly, appears as Corollary 3.2 below.

The strength of the theorem lies in the explicit description of the γ_i. Recall that a *theta characteristic* (also called *spin structure*) is an invertible sheaf L whose square $L^{\otimes 2}$ equals the canonical class. As examples we will show, for C lying in certain families of hyperelliptic curves, or in a specific family of genus 4 curves, how to determine if C has a rational theta characteristic, and we will also show how to compute the prime-to-p rational torsion in the Jacobian of C.[1] Note that there is no known algorithm to determine in general either the reduction type or the size of the rational torsion in the Jacobian of curves of genus $g \geq 3$.

We will prove the following results:

Theorem 4.1. *Let K be a local field with discrete valuation ring $\mathscr{O}_K$, uniformizer π, and residue field k of characteristic p. Let $g \in \mathscr{O}_K[x]$ be monic of degree $d \geq 3$ and such that $p \nmid 2d$. Let $h \in \mathscr{O}_K[x]$ be a polynomial of degree e with $e \leq 2d$. Suppose that (π, g, g') and (π, g, h) are both the unit ideal in $\mathscr{O}_K[x]$. Let C be the nonsingular projective curve with affine piece given by*

$$y^2 = g^2 + \pi h.$$

For $x \in \mathscr{O}_K$, write $\overline{x}$ for the reduction of $x \pmod{\pi}$. Similarly for $f \in \mathscr{O}_K[x]$, write $\overline{f}$ for the reduction in $k[x]$.

[1] In practice, if $K = \mathbb{Q}_p$ then our method often gives the full rational torsion on the Jacobian; see the Remark following Lemma 3.5.

(1) *Suppose d is odd and $\overline{g}$ factors over k as*

$$\overline{g}(x) = (x - \alpha_0)g_1(x)\cdots g_s(x)$$

where $\alpha_0 \in k$ and each of the g_i is irreducible over k. Let $\alpha_i \in \overline{k}$ be a root of $g_i(x)$. Then C has a rational theta characteristic if and only if $\operatorname{Nm}\overline{h}(\alpha_0)\overline{h}(\alpha_i) \in k^{\times 2}$ for all i; here $\overline{h}(\alpha_i) \neq 0$ for all i, and the norm is computed from $k(\alpha_i)$ to k.

(2) *If d is even or $\overline{g}$ is irreducible, then C has a rational theta characteristic.*

Given C/K, we construct its Jacobian J/K and the Néron model $\mathscr{J}$ over $\mathscr{O}_K$. Recall that if C has totally degenerate semi-stable reduction, then the special fiber of $\mathscr{J}$ is an extension of a finite group by a torus T.

Theorem 4.2. *Let C be as in the previous theorem, but now suppose $\overline{g}$ splits into linear factors over k. Suppose $q = \#k$. Let $J(K)(p')$ be the largest subgroup of the K-rational torsion on the Jacobian of C which has order prime to p. Let α_i be the roots of $\overline{g}$. Let H be the subgroup of $k^\times$ generated by the numbers $\overline{h}(\alpha_i)/\overline{h}(\alpha_0)$. Let n be the order of $\frac{H\cdot k^{\times d}}{k^{\times d}}$ and let $m = d/n$. Then*

$$J(K)(p') \cong \left(\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\right)^{d-2} \oplus \frac{\mathbb{Z}}{n(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

In § 5, there are similar results for the family of nonhyperelliptic genus 4 curves given in $\mathbb{P}^3_K$ as the intersection of the quadric $XY = ZW$ and the cubic $(X - Y)(Z - W)(Z + W) = \pi\varepsilon$, where ε varies in a Zariski open subset of the set of all homogeneous cubic forms in $\mathscr{O}_K[X, Y, Z, W]$. In Theorem 5.1, we calculate the prime-to-p K-rational torsion on the Jacobian of such a curve, and in Theorems 5.2 and 5.3 we determine whether there exists a rational theta characteristic and a rational *cube root* of the canonical class. (The literature sometimes refers to rth roots of the canonical class as *r-spin structures*.)

The methods described below so far only work when the normalizations of the components of C_k are all isomorphic over k to $\mathbb{P}^1_k$. In particular, the *index* of such C/K, the gcd of degrees of K-rational divisors on C, is 1. The idea is simple: suppose we wish to determine if $L \in \operatorname{Pic} C$ is r-divisible. We translate L by a rational divisor which is known to be r-divisible, and such that the class of the translate represents a point on the toric part of the Jacobian. We then apply the theory of algebraic tori. There are a number of technical difficulties to resolve along the way, one of which involves computation of the K-rational prime-to-p torsion on the Jacobian—see Propositions 3.3 and Corollary 3.1.

Results for determining rationality of theta characteristics, but with other methods, were proven by a number of different authors. Atiyah [1,

§5] showed that if the Galois action on the 2-torsion of the Jacobian factors through a cyclic group, then C has a rational theta characteristic; when $\operatorname{char} k \neq 2$ and C has good reduction, this immediately implies the existence of a rational theta characteristic, and motivates our study of degenerating curves. Mumford [11, §4] in the case of hyperelliptic curves gave explicit representations of the theta characteristics in terms of the Weierstrass points of C; thus, knowing the Galois action on the Weierstrass points enables one to determine if there is a rational theta characteristic. He showed furthermore that when $\operatorname{char} K = 2$, C always has a rational theta characteristic. Taken together with Atiyah's result, we have that except when $\operatorname{char} K = 0$ and $\operatorname{char} k = 2$, there is a rational theta characteristic over K^u. Parimala and Scharlau [14, Thm. 2.4 et seq.] in results extended by Suresh [17, Thm. 1.2] found a condition for the rationality of theta characteristics of hyperelliptic curves involving the splitting of a particular quaternion algebra. Suresh also gives a method for computing the order of the 2-torsion subgroup of the Jacobian.

Given a curve C as above, a related question is whether all of the r-torsion on the Jacobian of C, or more generally all of the rth roots of a given line bundle on C, are rational over K^u. This is essentially a geometric question, and has been considered in Chiodo [5, §3]. Pacini gives a more explicit answer for the case of theta characteristics [13]. See also Gross-Harris [7, Corollary 7.3] for a description of the rational points on the moduli space of curves all of whose theta characteristics are rational. Finally, see Poonen-Rains [15] for a relationship of the rationality of theta characteristics to a certain cup product over an abelian variety.

Acknowledgments to Dino Lorenzini, Wayne Aitken, and the referee for many helpful comments.

2. Basic facts on algebraic tori over finite fields

In the following, we let $q = \#k$, let T be a g-dimensional algebraic torus defined over k, and let $X(T)$ be the character group of $T_{\overline{k}}$. Let σ be the Frobenius automorphism acting on $\overline{k}$ with fixed field k. The character group $X(T)$ is a free $\mathbb{Z}$-module of rank g equipped with an action of $\mathfrak{g}$. In this section we will compute the group of rational points $T(k)$ based on knowledge of $X(T)$ as a $\mathbb{Z}[\mathfrak{g}]$-module.

Henceforth, unless otherwise stated, all modules are $\mathbb{Z}[\mathfrak{g}]$-modules. For example, "$X(T)$ is generated by χ" means generated over $\mathbb{Z}[\mathfrak{g}]$.

Definition. Let X be a $\mathbb{Z}[\mathfrak{g}]$-module. We say X is *principal* if it can be generated by a single element. We say X is *principally decomposable* if it can be written as a direct sum of principal submodules.

If $X = X(T)$, the character group of an algebraic torus, we use the above terms to describe X and T interchangeably. We say that $T = \prod T_j$

is a *principal decomposition* of T if T is the fiber product over k of the T_j, and each T_j is a principal torus.

Example. Let ℓ/k be the unique degree g extension. Let T be the Weil restriction of scalars $R_{\ell/k}\mathbb{G}_m$. Recall that T has the universal property that for any k-scheme S, we have a functorial isomorphism

$$T(S) = \mathbb{G}_m(S_\ell)$$

where S_ℓ means the base-extension $S \times_{\mathrm{Spec}\ k} \mathrm{Spec}\ \ell$. Explicitly, $T_\ell \cong (\mathbb{G}_{m,\ell})^g$, and the usual action of σ is twisted by the automorphism which cyclically permutes the factors; that is,

$$\sigma(x_1, \ldots, x_g) = (\sigma x_g, \sigma x_1, \ldots, \sigma x_{g-1}).$$

Alternatively, we can characterize T by setting $X(T) = \mathbb{Z}[\chi]/(\chi^g - 1)$, and σ acts as multiplication by χ. We observe that T is principal.

Remark. Suppose $T = \prod T_i$ is a principal decomposition of T. The projection $T \to T_i$ induces an inclusion $X(T_i) \subseteq X(T)$. This inclusion will be used without comment from here on.

From now on, we will assume that unless otherwise stated all tori under discussion are principally decomposable.

Definition. If $T_{/k}$ is the restriction of scalars $R_{\ell/k}\mathbb{G}_m$ for some finite extension ℓ/k, then we say that T is a *norm torus*, or *ℓ-norm torus* for clarity. If T is a product of norm tori, we say it is a *normal torus*.

Proposition 2.1 (Ono [12], Prop. 1.2.2)**.** *Given $x \in T(\overline{k})$, define the homomorphism $e_x : X(T) \to \overline{k}^\times$ by $e_x(\chi) = \chi(x)$. Then the map $x \mapsto e_x$ induces an isomorphism of abelian groups $T(k) \xrightarrow{\sim} \mathrm{Hom}_{\mathfrak{g}}(X(T), \overline{k}^\times)$.*

If the action of $\mathfrak{g}$ is trivial, we see that $T(k) = \mathrm{Hom}(X(T), k^\times)$. If the action of $\mathfrak{g}$ factors through $\mathrm{Gal}(\ell/k)$, since $T(k) \hookrightarrow T(\ell)$, we observe that we may replace $\overline{k}^\times$ in the proposition with $\ell^\times$. Given a $\mathbb{Z}$-basis of $X(T)$, the action of σ may be represented by an element of $\mathrm{GL}(g, \mathbb{Z})$. We let $f(x)$ be the characteristic polynomial of the matrix obtained this way; it is independent of the choice of basis. Given a positive integer n for which $(n, q) = 1$, let μ_n denote the étale sheaf over k of nth roots of unity.

Proposition 2.2. *Suppose T is principal. Then $T(k) \cong \mu_{f(q)}(\overline{k}^\times)$.*

Since $f(q) \equiv \pm 1 \pmod{q}$, $\mu_{f(q)}$ is an étale sheaf over k.

Proof. As T is principal, there is some $\chi \in X(T)$ such that χ is a $\mathbb{Z}[\mathfrak{g}]$-generator for $X(T)$. We will show that the map

$$\begin{aligned} T(k) &\longrightarrow \mu_{f(q)}(\overline{k}^\times) \\ x &\longmapsto \chi(x) \end{aligned}$$

is an isomorphism.

First observe that χ, χ^σ, $\ldots$, $\chi^{\sigma^{g-1}}$ form a $\mathbb{Z}$-basis for $X(T)$. Thus, the values of these characters uniquely characterize points in $T(\overline{k})$. Given $x \in T(k)$, by Proposition 2.1 we must have

$$\chi^{\sigma^i}(x) = \sigma^i \chi(x) = \chi(x)^{q^i}$$

for every i. Therefore the value $\chi(x)$ determines all of the values $\chi^{\sigma^i}(x)$ for $i = 1, \ldots, g-1$. This tells us that $\chi : T(k) \to \overline{k}^\times$ is injective.

Now choose $\omega \in \mu_{f(q)}(\overline{k}^\times)$. We will construct a $\mathfrak{g}$-equivariant homomorphism $e_x : X(T) \to \overline{k}^\times$ for which $e_x(\chi) = \omega$. In order for e_x to be $\mathfrak{g}$-equivariant, we must have

$$e_x(\chi^{\sigma^i}) = e_x(\chi)^{q^i}$$

for all i. For $0 \leq i \leq g-1$, these are independent constraints. The only additional constraint is given by the characteristic polynomial; that is, we have the identity of characters $\chi^{f(\sigma)} = 0$, or $e_x(\chi)^{f(q)} = 1$. This holds by our choice of ω, and so the proposition follows. □

We give some simple examples to demonstrate the proposition. If $T = \mathbb{G}_m$, then $f(x) = x - 1$ and $f(q) = q - 1$. The right hand side above becomes $\mu_{q-1}(\overline{k}^\times) = k^\times$.

Now suppose that T is an ℓ-norm torus, where $[\ell : k] = g$. Our description of $X(T)$ as a $\mathbb{Z}[\mathfrak{g}]$-module shows that $f(x) = x^g - 1$. Then $T(k) \cong \mu_{q^g-1}(\overline{k}^\times) = \ell^\times$. We verify this by the universal property of Weil restriction of scalars: $T(k) = \mathbb{G}_m(\ell) = \ell^\times$.

Corollary 2.1. *Suppose $T = \prod T_i$ is a principal decomposition of T over k. Let $f_i(x)$ be the characteristic polynomial of Frobenius acting on $X(T_i)$. Let χ_i be a $\mathbb{Z}[\mathfrak{g}]$-generator for $X(T_i)$. Then the map*

$$\oplus \chi_i : T(k) \longmapsto \oplus \mu_{f_i(q)}(\overline{k}^\times)$$

is an isomorphism.

We will often write $\mu(T_i)$ in place of $\mu_{f_i(q)}(\overline{k}^\times)$. Note that $f_i(q)$, and hence $\mu(T_i)$, depend on the base field.

Corollary 2.2. *Let T be principally decomposable torus over k, and let $f(x)$ be the characteristic polynomial of Frobenius acting on $X(T)$. Then $\#T(k) = f(q)$.*

The previous corollary in fact holds for general algebraic tori; see Ono [12, eq. (1.2.6)].

3. The descent map

In the remainder, we will assume that C is a smooth, proper, geometrically integral curve over K with minimal proper regular model $\mathscr{C}$ having totally degenerate semi-stable reduction and special fiber C_k. It then holds that the Jacobian J of C_k has a Néron model $\mathscr{J}$ whose special fiber J_k lies in a short exact sequence of group schemes

$$0 \longrightarrow T \longrightarrow J_k \longrightarrow \Phi \longrightarrow 0, \tag{3.1}$$

where T is an algebraic torus and Φ is a finite étale group scheme. The scheme Φ is the *component group* of J_k.

3.1. Overview. Starting in § 3.3, we will assume that the normalization of every irreducible component of C_k is isomorphic to $\mathbb{P}^1_k$. This implies that $\operatorname{Pic} C = (\operatorname{Pic} \overline{C})^G$; that is, any divisor linearly equivalent to its Galois conjugates is linearly equivalent to a rational divisor. In the remainder of this overview, we will operate under this assumption.

Let $\operatorname{Div}^{\{1\}} C$ be the group of divisors D on C supported away from points with singular reduction. Note that for any $L \in \operatorname{Pic} C$, there exists some $D \in \operatorname{Div}^{\{1\}} C$ which represents it by [6, Theorem 2.3]. Let

$$\tau : \operatorname{Div}^{\{1\}} C \longrightarrow \operatorname{Div} C_k$$

be the specialization map; that is, given $D \in \operatorname{Div}^{\{1\}} C$, let $\mathscr{D}$ be the Zariski closure of D in $\mathscr{C}$ under the canonical inclusion $C \hookrightarrow \mathscr{C}$. Then $\tau(D)$ is $\mathscr{D} \cap C_k$. (See for example [2, §2.1] or [10, ch. 10.1.3].) If C_i is an irreducible component of C_k, the intersection pairing $(\tau(D) \cdot C_i)$ is well-defined; by abuse of notation, we will also write it $(D \cdot C_i)$.

Given $L \in \operatorname{Pic} C$, we wish to determine if L lies in $r \operatorname{Pic} C$. Evidently it is necessary that L lie in $\operatorname{Pic}^r C$. We will define a group $\operatorname{Pic}^{\{r\}} C$ lying in a filtration

$$\operatorname{Pic}^r C \supset \operatorname{Pic}^{\{r\}} C \supset r \operatorname{Pic} C. \tag{3.2}$$

In Proposition 3.1 below, we show how to determine if $L \in \operatorname{Pic}^r C$ lies in $\operatorname{Pic}^{\{r\}} C$. Then, in the following sections, we will show how to determine if $L \in \operatorname{Pic}^{\{r\}} C$ lies in $r \operatorname{Pic} C$. The two quotients defined by the filtration may be viewed as giving, respectively, geometric and arithmetic obstructions to r-divisibility.

Our first step is to define a degree map

$$\deg : \operatorname{Div} C_k \longrightarrow \mathbb{Z}^v$$

where v is the number of irreducible components of C_k. Now letting $C_1, \ldots, C_v$ be the irreducible components of C_k, the degree map is defined by

$$\deg(D) = ((D \cdot C_i))$$

where $\cdot$ denotes the intersection pairing. Then $\mathrm{Pic}^{\{r\}} C$ is defined to be the set of divisor classes containing a divisor $D \in \mathrm{Div}^{\{1\}} C$ such that $\deg(\tau(D)) \in r\mathbb{Z}^v$. (For $D \in \mathrm{Div}^{\{1\}} C$, we will usually write $\deg(D)$ in place of $\deg(\tau(D))$.) Furthermore, we certainly have the filtration (3.2).

We now show how to determine if a given $L \in \mathrm{Pic}^r C$ lies in $\mathrm{Pic}^{\{r\}} C$. Let M_{fib} be the subgroup of $\mathbb{Z}^v$ generated by the vectors $v_i = ((C_i \cdot C_j))$.

Proposition 3.1. *Suppose $L \in \mathrm{Pic}^r C$. Let $D \in \mathrm{Div}^{\{1\}} C$ represent L. Then $L \in \mathrm{Pic}^{\{r\}} C$ if and only if $\deg(D)$ lies in $r\mathbb{Z}^v + M_{fib}$.*

Observe that the equivalent conditions of the proposition are stable under unramified base change; in particular, we may base extend to K^u. This explains the terminology "geometric obstruction" mentioned above.

Proof. Certainly if $L \in \mathrm{Pic}^{\{r\}} C$, we may find a divisor E with class L such that $\deg(E) \in r\mathbb{Z}^v$. Since D is linearly equivalent to E, if we consider D and E as horizontal divisors on $\mathscr{C}$ via the inclusion $C \hookrightarrow \mathscr{C}$, then $(D - E)$ is linearly equivalent to a fibral divisor F. Therefore $\deg(D) = \deg(E) + \deg(F) \in r\mathbb{Z}^v + M_{fib}$.

Suppose now that $\deg(D) \in r\mathbb{Z}^v + M_{fib}$. Then there exists a divisor D' such that $\deg(D - rD') \in M_{fib}$. Replacing D with $D - rD'$, we see that we wish to show that if $\deg D \in M_{fib}$, then $L \in \mathrm{Pic}^{\{r\}} C$.

Let $F \in \mathrm{Div}\,\mathscr{C}$ be a fibral divisor for which $\deg F = \deg D$. We wish to replace F with a linearly equivalent horizontal divisor. On each irreducible component C_i of C_k, choose a smooth point $x_i \in C_i(\overline{k})$. By [6, Prop. 6.2], there is a divisor F' linearly equivalent to F which avoids each of the x_i; this latter condition forces F' to be horizontal. Observe that $\deg(F') = \deg(F)$. Furthermore, if we consider F' as a divisor on C by restricting to the generic fiber of $\mathscr{C}$, one sees that F' must be principal. Thus D is linearly equivalent to $D - F'$. But $\deg(D - F') = \deg(D - F) = 0$, from which the claim follows. □

Therefore to determine if $L \in \mathrm{Pic}\, C$ is divisible by r, we may assume that $L \in \mathrm{Pic}^{\{r\}} C$. In this section, we will associate to every character of T a homomorphism γ from $\dfrac{\mathrm{Pic}^{\{r\}} C}{r\,\mathrm{Pic}\, C}$ to a finite cyclic group, so that the intersection of the kernels of the γs is trivial. The idea behind the homomorphism is as follows.

Given $L \in \mathrm{Pic}^{\{r\}} C$, choose $D \in \mathrm{Div}^{\{r\}} C$ representing it. We may translate D to $\mathrm{Div}^{\{0\}} C$ via an r-divisible divisor, map the resulting divisor to some $x \in T(k)$, then evaluate characters of T on x to determine if it lies in $rT(k)$. If it does, then L was r-divisible. But even if $x \notin rT(k)$, L may still be r-divisible in $J(k)$! Under our hypotheses, Φ is a constant group scheme

(see Prop. 3.2). We have a short exact sequence

$$\Phi[r] \longrightarrow \frac{T(k)}{rT(k)} \longrightarrow \frac{J(k)}{rJ(k)}.$$

In order for L to be r-divisible, we must test if the resulting $x \in T(k)$ lies in $rT(k) + \mathrm{im}(\Phi[r])$. As we will see, determining $\mathrm{im}(\Phi[r])$ will have the pleasant consequence of telling us the prime-to-p torsion in $J(K)$.

3.2. One-cycles on Γ. Let Γ be the dual graph of C_k; that is, the graph whose vertices correspond to the irreducible components of $C_{\overline{k}}$, and whose edges correspond to the nodes of $C_{\overline{k}}$. The graph Γ comes equipped with a natural $\mathfrak{g}$-action. Let $H_1(\Gamma, \mathbb{Z})$ be the group of closed, oriented 1-cycles on Γ; it is a $\mathfrak{g}$-module. Define a group $F_1(\Gamma)$ as the set of pairs $(\gamma, (t_i))$ where $\gamma \in H_1(\Gamma, \mathbb{Z})$ and (t_i) is a collection of functions, each t_i being a function on the irreducible component $C_i \subseteq C_k$ such that the zeroes and poles of t_i occur only at nodes. (If any C_i is itself a nodal curve, construct t_i on its normalization.) The group structure is

$$(\gamma_1, (s_i)) \cdot (\gamma_2, (t_i)) = (\gamma_1 + \gamma_2, (s_i \cdot t_i)).$$

We will often use the more compact notation t_γ for the pair (γ, t_i) when the t_i are understood. Observe that σ^{-1} acting on C_k induces a map $(\sigma C_i)(\overline{k}) \to C_i(\overline{k})$. Then the group $F_1(\Gamma)$ comes equipped with a natural $\mathfrak{g}$-action; namely,

$$\sigma(\gamma, (t_i)) = (\sigma\gamma, (t_i^\sigma))$$

where $t_i^\sigma(x) = \sigma t_i(\sigma^{-1}x)$ for every $x \in (\sigma C_i)(\overline{k})$. There is a canonical Galois-equivariant projection

$$F_1(\Gamma) \longrightarrow H_1(\Gamma, \mathbb{Z}).$$

We define a subset $F_1(\Gamma)(1) \subseteq F_1(\Gamma)$ as follows. Let $\gamma \in H_1(\Gamma, \mathbb{Z})$ be an oriented 1-cycle. Let $C_1, \ldots, C_v$ be some labeling of the components of $C_{\overline{k}}$. Over $C_{\overline{k}}$, γ corresponds to an ordered sequence of components $C_{i_0}, \ldots, C_{i_n}$, connected by some choice of nodes. Let $x_j \in C_{\overline{k}}(\overline{k})$ be the corresponding choice of node in $C_{i_j} \cap C_{i_{j+1}}$. The orientation is given by the order of the components as given; observe that we may have $C_{i_j} = C_{i_h}$ and/or $x_j = x_h$ for some $j \neq h$. Then $F_1(\Gamma)(1)$ consists of pairs $(\gamma, (t_i))$, where t_i is given as follows:

(1) if C_i does not appear in γ, then $t_i = 1$;
(2) if C_i appears with multiplicity one, then t_i is a degree 1 local parameter on C_i such that $t_i(x_{i-1}) = 0$ and $t_i(x_i) = \infty$; and
(3) if C_i appears with higher multiplicity, compute a degree 1 local parameter as above for each C_{i_j} for which $C_{i_j} = C_i$, then let t_i be their product.

3.3. Evaluation of divisors on 1-cycles. In this section, we will assume that the normalization of every irreducible component of C_k is isomorphic to $\mathbb{P}^1_k$.

Recall from § 3.1 that $\mathrm{Div}^{\{1\}} C$ is the group of divisors D on C supported away from points with singular reduction, and that

$$\tau : \mathrm{Div}^{\{1\}} C \longrightarrow \mathrm{Div}\, C_k$$

is the specialization map.

Let $\gamma \in \mathrm{H}^1(\Gamma, \mathbb{Z})$ be an oriented 1-cycle, and let t_γ be an element of $F_1(\Gamma)(1)$ lying over γ. We now define a homomorphism, also written t_γ, as

$$\begin{aligned} t_\gamma : \mathrm{Div}^{\{1\}} C &\longrightarrow \overline{k}^\times \\ D &\longmapsto \prod t_i(\tau(D) \cap C_i) \end{aligned}$$

where the product is over all i. By abuse of notation, we will often write $D \cap C_i$ for $\tau(D) \cap C_i$, or more concisely just D_i.

Recall the degree map from § 3.1, and that $\mathrm{Div}^{\{r\}} C \subseteq \mathrm{Div}^{\{1\}} C$ is the subgroup of divisors D with $\deg D \in r\mathbb{Z}^v$. Let $\mathrm{Pic}^{\{r\}} C$ be the set of divisor classes L such that L contains some divisor in $\mathrm{Div}^{\{r\}} C$.

Lemma 3.1. *For $\gamma \in H_1(\Gamma, \mathbb{Z})$, choose some $t_\gamma \in F_1(\Gamma)(1)$ lying over it and consider the homomorphism $t_\gamma : \mathrm{Div}^{\{0\}} C_{K^u} \to \overline{k}^\times$. Then the latter homomorphism factors through $\mathrm{Pic}^{\{0\}} C_{\overline{k}}$. Via the identification of $\mathrm{Pic}^{\{0\}} C_{\overline{k}}$ with $T(\overline{k})$, the map $\gamma \mapsto t_\gamma$ induces a well-defined Galois-equivariant isomorphism*

$$H_1(\Gamma, \mathbb{Z}) \longrightarrow X(T)$$

where $X(T)$ is the character group of the torus T.

Proof. First, observe that if $t_\gamma = (\gamma, (t_i))$, $t'_\gamma = (\gamma, (t'_i))$ are two lifts of γ to $F_1(\Gamma)(1)$, that $t'_i = \alpha_i t_i$ for some $\alpha_i \in \overline{k}^\times$. For $L \in \mathrm{Div}^{\{0\}} C$, since $(L \cdot C_i) = 0$, we have $t_i(L \cap C_i) = t'_i(L \cap C_i)$. Thus the homomorphism $\mathrm{Div}^{\{0\}} C_{K^u} \to \overline{k}^\times$ is independent of the choice of t_γ.

Now base-extend to K^u. Let χ be the character associated to γ; we recall its definition. Suppose γ consists of the components $C_{i_0}, \ldots, C_{i_{n-1}}$, where C_{i_j} is connected to $C_{i_{j+1}}$ via a node x_j (viewing subscripts modulo n). The orientation of γ is given by ordering the components with increasing subscripts. Choose $t_\gamma \in F_1(\Gamma)(1)$ lying over γ, and let t_i be the corresponding functions. Given $L \in \mathrm{Div}^{\{0\}} C$ supported away from the nodes, let $L \cap C_i = \sum_j e_{ij} y_{ij}$, where $e_{ij} \in \mathbb{Z}$ and $y_{ij} \in C_i(\overline{k})$. Observe that $\sum_j e_{ij} = 0$ for every i. Let

$$f_i = \prod_j (t_i - t_i(y_{ij}))^{e_{ij}}$$

be a function on C_i; we see that f is regular at x_{i-1} and x_i. Also,

$$f_i(x_{i-1}) = \prod_j t_i(y_{ij})^{e_{ij}},\ f_i(x_i) = 1$$

where the first equality uses the fact that $\sum_j e_{ij} = 0$. Then

$$\chi([L]) = \prod_i \frac{f_{i+1}(x_i)}{f_i(x_i)} = \prod_{ij} t_i(y_{ij})^{e_{ij}} = t_\gamma(L).$$

The lemma follows. □

Suppose $T = \prod T_i$ is a principal decomposition of T, and let χ be a generator for $X(T_i)$. Via the canonical inclusion $X(T_i) \subseteq X(T)$, we consider χ as an element of $X(T)$. Let $\gamma \in H_1(\Gamma, \mathbb{Z})$ be the 1-cycle which corresponds, via Lemma 3.1, to χ. We define a subset of "rational" elements $F_1(\gamma, k) \subseteq F_1(\Gamma)(1)$ lying over γ as follows. We may write γ as an ordered sequence of components $C_{i_0}, C_{i_1}, \ldots$ such that C_{i_j} and $C_{i_{j+1}}$ are connected by the node x_j. Since $\mathbb{P}^1_k(k)$ has at least 3 elements, we can always find a point $b_j \in C_{i_j}(k)$ such that $b_j \neq x_{j-1}, x_j$. (Of course, b_j might itself be a node.) Choose b_j for each C_{i_j} in the list of components in γ; note that if a component appears more than once, then the corresponding base points b_j may be different. Then we define $F_1(\gamma, k)$ to be the set of $t_\gamma = (\gamma, (t_i))$ such that

(1) if C_i does not appear in γ, then $t_i = 1$;
(2) if C_i appears with multiplicity one, say equal to C_{i_j}, then t_i is a degree 1 local parameter on C_i such that $t_i(x_{j-1}) = 0$, $t_i(x_j) = \infty$, and $t_i(b_j) \in \mu(T_i)$; and
(3) if C_i appears with higher multiplicity, compute a degree 1 local parameter as above for each C_{i_j} for which $C_{i_j} = C_i$, then let t_i be their product.

If T is a split torus and no C_i appears with higher multiplicity, this condition is equivalent to $t_i \in k(C_i)^\times$ for all i.

Lemma 3.2. *Let $T = \prod T_i$ be a principal decomposition, let χ be a generator for $X(T_i)$, and let $\gamma \in H_1(\Gamma, \mathbb{Z})$ correspond to χ via the inclusion $X(T_i) \subseteq X(T)$ and the isomorphism of Lemma 3.1. Suppose that $t_\gamma = (\gamma, (t_i)), t'_\gamma = (\gamma, (t'_i)) \in F_1(\gamma, k)$ lie over γ. Then there exist $\alpha_i \in \mu(T_i)$ such that $t'_i = \alpha_i t_i$ for every i.*

One consequence of the lemma is that $F_1(\gamma, k)$ does not depend on the choice of base-points b_i.

Proof. It suffices to consider the case where C_i appears in γ with multiplicity 1. Let $b_i, b'_i \in C_i(k)$ be the base-points corresponding to t_i, t'_i,

respectively. Then

$$t_i(b_i') = t_i(b_i)\frac{t_i(b_i')}{t_i(b_i)} = t_i(b_i)t_\gamma((b_i') - (b_i)),$$

where $(b_i') - (b_i)$ means the natural divisor on C_k. But this divisor lies in the reduction of $\mathrm{Div}^{\{0\}} C$, hence by Lemma 3.1 and Corollary 2.1, $t_\gamma((b_i')-(b_i)) \in \mu(T_j)$. The claim follows from setting $\alpha_i = t_\gamma((b_i')-(b_i))$. □

3.4. Torsion and descent. Given a principal decomposition $T = \prod T_i$, and χ a generator for $X(T_i)$, let $\gamma \in H_1(\Gamma, \mathbb{Z})$ be a one-cycle such that, via the isomorphism of Lemma 3.1, $t_\gamma = \chi$. Write $r\mu(T_i)$ for the group of all α^r, $\alpha \in \mu(T_i)$. We define a map

$$\mathrm{Div}^{\{r\}} C \longrightarrow \frac{\mu(T_i)}{r\mu(T_i)}$$

which, by abuse of notation, we also denote γ. This map is defined by

$$\gamma(D) = t_\gamma(D) \pmod{r\mu(T_i)}$$

where t_γ is any element of $F_1(\gamma, k)$ lying over γ.

Lemma 3.3. *γ is a well-defined homomorphism.*

Proof. For convenience, we assume that T is itself principal, so that $T = T_i$. We need to show that the image of the map γ lies in $\mu(T)/r\mu(T)$, and that the map does not depend on the choice of t_γ. Lemma 3.2 implies that $t_\gamma(D) \in \mu(T)$ for any $t_\gamma \in F_1(\gamma, k), D \in \mathrm{Div}^{\{r\}} C$. Also by that lemma, choosing a different t_γ is the same as replacing the t_i with $\alpha_i t_i$, where $\alpha_i \in \mu(T)$. But since D_i has degree divisible by r, $(\alpha_i t_i)(D_i)$ differs from $t_i(D_i)$ by a power of α_i^r, hence an element of $r\mu(T)$. Finally, the fact that γ is a homomorphism is clear from the definition. □

Lemma 3.4. *Let $f, g \in \overline{K}(C)^\times$, and suppose $\operatorname{div} f, \operatorname{div} g \in \mathrm{Div}^{\{1\}} C$. If $\deg(\operatorname{div} f) = \deg(\operatorname{div} g)$, then for any $t_\gamma \in F_1(\Gamma)(1)$,*

$$t_\gamma(\operatorname{div} f) = t_\gamma(\operatorname{div} g).$$

Proof. It suffices to show that

$$t_\gamma\left(\operatorname{div}\left(\frac{f}{g}\right)\right) = 1.$$

This follows from Lemma 3.1. □

Recall that Φ denotes the component group of J_k; it is a finite étale group scheme on $\operatorname{Spec} k$. Recall also the exact sequence of group schemes

$$0 \longrightarrow T \longrightarrow J_k \longrightarrow \Phi \longrightarrow 0.$$

(Note that Φ depends on the base field K, and in particular becomes larger upon ramified base change.) The group $\Phi(\overline{k})$ is effectively computable;

see [16, Proposition 8.1.2] or [2, Appendix A]. The rational component group, $\Phi(k)$, can be computed via Theorem 1.11 of [3].

Proposition 3.2. *Let $\mathscr{C}$ be a proper, flat, regular curve over $\mathscr{O}_K$ with geometrically connected generic fiber. Let J be the Jacobian of the generic fiber.*

(1) *If every component of the special fiber C_k is geometrically irreducible, then the component group Φ of J is a constant group scheme.*
(2) *If ℓ is an extension of k which is a finite field, or if C_k is totally degenerate, then the map $J_k(\ell) \to \Phi(\ell)$ is surjective.*

The two statements are respectively Corollary 1.8 and Lemma 2.1b of [3]. As the hypothesis of part 1 holds for us, by abuse of notation Φ will denote $\Phi(\overline{k})$ as well as its usual meaning. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T(k) & \longrightarrow & J_k(k) & \longrightarrow & \Phi & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r} & & \\ 0 & \longrightarrow & T(k) & \longrightarrow & J_k(k) & \longrightarrow & \Phi & \longrightarrow & 0, \end{array} \tag{3.3}$$

where the vertical maps are multiplication by r and the horizontal sequences are exact by the last proposition. Applying the Snake Lemma, we obtain the exact sequence

$$J_k(k)[r] \longrightarrow \Phi[r] \xrightarrow{\nu} \frac{T(k)}{rT(k)} \longrightarrow \frac{J_k(k)}{rJ_k(k)}. \tag{3.4}$$

We now show how to compute ν.

Proposition 3.3. *Let r be an integer not divisible by p. Let $D \in \operatorname{Div}^{\{1\}} C$ represent $\delta \in \Phi[r]$. Let $T = \prod T_i$ be a principal decomposition. For each i, let χ_i be a generator for $X(T_i)$, and let $\gamma_i \in H_1(\Gamma, \mathbb{Z})$ correspond to χ_i via the inclusion $X(T_i) \subseteq X(T)$ and the isomorphism of Lemma 3.1. Then there exists $f \in \overline{K}(C)^\times$ such that $\deg(\operatorname{div} f) = -r \deg(D)$, and for every i*

$$\chi_i(\nu(\delta)) \equiv \gamma_i(\operatorname{div} f) \pmod{r\mu(T_i)},$$

where by abuse of notation we write χ_i for the induced homomorphism $\frac{T(k)}{rT(k)} \to \frac{\mu(T_i)}{r\mu(T_i)}$.

Proof. Observe that $-rD$ maps to the trivial class in Φ. Therefore the reduction of the divisor class of $-rD$ lies in $T(k)$. As observed in Lemma 3.1, divisor classes in $T(k)$ can be represented by elements of $\operatorname{Div}^{\{0\}} C$, so that $-rD$ is linearly equivalent to some $D' \in \operatorname{Div}^{\{0\}} C$. Let f be chosen so that $\operatorname{div} f = -rD - D'$. By our choice of D', we have $\deg(\operatorname{div} f) = -r \deg(D)$.

For convenience, we will append the subscript t or b to the groups in (3.3) to distinguish objects in the top row from objects in the bottom row; e.g., $T(k)_t$ refers to the top left object in (3.3). Also, for a divisor E, write $[E]$

for the divisor class of E; whether this class lies in $\operatorname{Pic}\overline{C}$ or $\operatorname{Pic}C_{\overline{k}}$ will be clear from context.

We proceed with an explicit diagram-chase: start with $\delta \in \Phi[r]$, and consider it as an element of Φ_t. Choose $D \in \operatorname{Div}^{\{1\}} C$ so that the class $[\tau(D)] \in J_k(k)_t$ maps to δ. Then $[r\tau(D)] \in J_k(k)_b$ maps to 0 in Φ_b, and so lies in the subgroup $T(k)_b$; the class of this element in $T(k)/rT(k)$ is none other than $\nu(\delta)$.

Now $[rD] = [rD + \operatorname{div} f]$. But by our choice of f, $rD + \operatorname{div} f$ is $-D' \in \operatorname{Div}^{\{0\}} C$. For each i, Lemma 3.1 tells us that

$$\chi_i(\nu(\delta)) = t_{\gamma_i}(rD + \operatorname{div} f)$$

for any choice of $t_{\gamma_i} \in F_1(\gamma_i, k)$ lying over γ_i. The first claim now follows by observing that

$$t_{\gamma_i}(rD + \operatorname{div} f) \equiv \gamma_i(\operatorname{div} f) \pmod{r\mu(T_i)}.$$

□

Corollary 3.1. *Fix the notation of Prop. 3.3. If $\widetilde{\delta} \in J(k)$ maps to δ, then*

$$\nu(\delta) \equiv r\widetilde{\delta} \pmod{rT(k)}.$$

Proof. One observes that $\widetilde{\delta}$ is identical to $[\tau(D)]$ in the proof of Prop. 3.3. From this observation and the snake lemma argument in the above proof, the claim follows. □

If M is an abelian group, write $M(p')$ for the torsion in M with order prime to p.

Lemma 3.5. *Let J be the Jacobian of C with special fiber J_k. Then*

$$J(K)(p') = J_k(k)(p').$$

Proof. The reduction map $J(K)(p') \to J_k(k)(p')$ is injective, since the torsion in the kernel of reduction is a p-group. For r not divisible by p, let $\overline{x} \in J_k(K)[r]$. By Hensel's Lemma, there is $x \in J(K)$ which maps to $\overline{x}$. But rx lies in the kernel of the reduction map, which is r-divisible; therefore $rx = ry$ for some y in the kernel of reduction. Then $(x - y) \in J(K)[r]$ maps to $\overline{x}$. □

Remark. By varying r, one can use Proposition 3.3, Corollary 3.1, and Lemma 3.5 to effectively compute the torsion subgroup $J(K)(p')$. For example, if for all r $(p \nmid r)$ we find that ν is the zero map, then $J(K)(p') \cong T(k) \oplus \Phi(p')$.

If $K = \mathbb{Q}_p$ with $p \neq 2$, then the kernel of reduction is torsion-free [9, Appendix]; if in addition $\Phi[p] = 0$, then we are able to compute the full torsion subgroup of $J(K)$. Even when $K \neq \mathbb{Q}_p$ but $\Phi[p] = 0$, one can still compute $J(K)(p)$ by Mumford-Tate uniformization. This will be explored in future work.

Theorem 3.1. *Let $T = \prod T_j$ be a principal decomposition of T. Let $\gamma_j \in H_1(\Gamma, \mathbb{Z})$ be such that χ_j is a $\mathbb{Z}[\mathfrak{g}]$-generator for $X(T_j)$. Given $D \in \operatorname{Div}^{\{r\}} C$, $[D] \in r \operatorname{Pic} C$ if and only if there exists some $\delta \in \Phi[r]$ such that*

$$\gamma_j(D) \in \chi_j(\nu(\delta)) \cdot r\mu(T_j)$$

for all j.

Proof. Let $D' \in \operatorname{Div}^{\{1\}} C$ satisfy $r(D' \cdot C_i) = (D \cdot C_i)$ for all i. Then $[D] \in r \operatorname{Pic} C$ if and only if $[D - rD'] \in r \operatorname{Pic} C$. Furthermore

$$\gamma_j(D) \equiv \gamma_j(D - rD') \pmod{r\mu(T_j)}$$

for all j. Therefore we may assume that $D \in \operatorname{Div}^{\{0\}} C$. In particular, the reduction of $[D]$ to the special fiber of the Jacobian J_k lies in the torus $T(k)$. Let $x \in T(k)$ be the point corresponding to $[D]$. From the exact sequence (3.4), $[D]$ is divisible by r in $J_k(k)$ if and only if x lies in the subgroup generated by $rT(k)$ and $\operatorname{im} \nu$. The claim follows. □

Remark. The proof, together with Lemma 3.4, shows that for $L \in \operatorname{Pic}^{\{r\}} C$, we may use any $D \in \operatorname{Div}^{\{r\}} C_{K^u}$ which represents L; then $\gamma_i(D) \in \mu(T_i)$, and the above theorem holds.

Corollary 3.2. *For each $\delta \in \Phi[r]$, let $D_\delta \in \operatorname{Div}^{\{1\}} C_{K^u}$ represent it, and choose f_δ so that $\deg(\operatorname{div} f_\delta) = -r \deg(D_\delta)$. Given $D \in \operatorname{Div}^{\{r\}} C_{K^u}$ with $[D] \in \operatorname{Pic} C$, we have $[D] \in r \operatorname{Pic} C$ if and only if there exists some δ such that $\gamma_i(D + \operatorname{div} f_\delta) \in r\mu(T_i)$ for every i.*

Proof. Combine Theorem 3.1, the Remark above, and Proposition 3.3. □

Theorem 3.2. *Let C be a smooth, projective, geometrically integral curve over a local field K. Suppose either $\operatorname{char} K = 2$ or the residue characteristic is odd. If the minimal proper regular model of C has totally degenerate semistable reduction, then C has a rational theta characteristic over the unique degree 2 unramified extension of K.*

Proof. If $\operatorname{char} K = 2$, then Mumford [11, §4] shows that C already has a rational theta characteristic over K. Suppose then that the residue characteristic is odd. Then the 2-torsion in the Jacobian of C is tamely ramified, so over K^u the Galois representation on the 2-torsion is cyclic. By Atiyah [1, §5], C has a rational theta characteristic over K^u, and therefore the canonical class of C lies in $\operatorname{Pic}^{\{2\}} C$. Let T be the toric part of the Jacobian of C, and L the degree 2 unramified extension of K; let ℓ/k be the respective residue fields. Observe that $T(k) \subseteq 2T(\ell)$. The claim now follows from Theorem 3.1. □

3.5. Simplifications for normal tori. We suppose that T is a principal torus with $X(T)$ generated by χ. Let $\gamma \in H_1(\Gamma, \mathbb{Z})$ correspond to χ. Consider $t_\gamma \in F_1(\gamma, k)$. Let m be the smallest positive integer such that $\sigma^m \gamma = \gamma$. We define $\operatorname{Nm} t_\gamma$ to be

$$\operatorname{Nm} t_\gamma = \prod_{i=0}^{m-1} \sigma^i t_\gamma$$

where the product is computed in $F_1(\Gamma)$. The projection of $\operatorname{Nm} t_\gamma$ lies over the 1-cycle $\operatorname{Nm} \gamma := \sum_{i=0}^{m-1} \sigma^i \gamma$, which generates $H_1(\Gamma, \mathbb{Z})^{\mathfrak{g}}$. Given a torus with a fixed principal decomposition, extend Nm in the obvious way to generators γ_i for each principal subtorus. For $\gamma \in H_1(\Gamma, \mathbb{Z})^{\mathfrak{g}}$, we may write it as

$$\gamma = \sum e_i \operatorname{Nm} \gamma_i$$

for some integers e_i; if T is a normal torus, this representation is unique. For each γ_i, choose $t_{\gamma_i} \in F_1(\gamma_i, k)$. We then consider $t_\gamma \in F_1(\gamma, k)$ of the form

$$t_\gamma = \prod (\operatorname{Nm} t_{\gamma_i})^{e_i}.$$

Note that the map $t_\gamma : \operatorname{Div}^{\{r\}} C \longrightarrow k^\times$ induces a well-defined map

$$\gamma : \operatorname{Pic}^{\{r\}} C \longrightarrow \frac{k^\times}{k^{\times r}}.$$

Corollary 3.3. *Suppose T is a normal torus and $r \mid (q-1)$. Given $D \in \operatorname{Div}^{\{r\}} C_{K^u}$ with $[D] \in \operatorname{Pic} C$, we have $[D] \in r \operatorname{Pic} C$ if and only if there exists some $\delta \in \Phi[r]$ such that*

$$\gamma(D) \in \chi_\gamma(\nu(\delta)) \cdot k^{\times r}$$

for all $\gamma \in H_1(\Gamma, \mathbb{Z})^{\mathfrak{g}}$; here, χ_γ is the character associated to γ via Lemma 3.1.

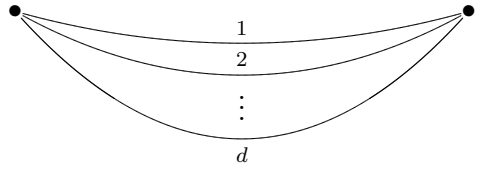
Proof. It suffices to consider the case where T is a norm torus; say $X(T) \cong \mathbb{Z}[\chi]/(\chi^g - 1)$, with Frobenius acting as multiplication by χ. Let ℓ be the unique degree g extension of k. Then $\chi : T(k) \to \ell^\times$ is an isomorphism. Furthermore, $X(T)^{\mathfrak{g}}$ is generated by $\operatorname{Nm} \chi := 1 + \chi + \chi^\sigma + \cdots + \chi^{\sigma^{g-1}}$. Observe that the diagram

$$\begin{array}{ccc} T(k) & & \\ \downarrow{\scriptstyle \chi} & \searrow^{\operatorname{Nm} \chi} & \\ \ell^\times & \xrightarrow{\operatorname{Nm}} & k^\times \end{array}$$

commutes. Now we tensor everything in the diagram with $\mathbb{Z}/r\mathbb{Z}$ and observe that since $r \mid (q-1)$, the induced norm map $\operatorname{Nm} : \frac{\ell^\times}{\ell^{\times r}} \longrightarrow \frac{k^\times}{k^{\times r}}$ is an isomorphism. The claim follows. □

4. Curves with $\Gamma = B_d$

The graph B_d is the so-called *banana graph*; it consists of 2 vertices connected to each other by d edges:



Equivalently, the special fiber of a curve C having dual graph B_d consists of two $\mathbb{P}^1$s which intersect transversely at d points; the involution swapping the two components shows that such a curve must be hyperelliptic. For certain families of curves with dual graph B_d, we determine rationality of theta characteristics and then compute the order of the prime-to-p rational torsion on the Jacobian. In all that follows, we fix $d \geq 3$.

4.1. Rationality of theta characteristics when $\Gamma = B_d$. We apply Theorem 3.1 in this section to determine if certain curves with dual graph B_d have rational theta characteristics. Recall that a theta characteristic is a square root of the canonical class. Note that Mumford [11, §4] and Suresh [17, Thm. 1.2] give alternate methods for determining the existence of a rational theta characteristic for hyperelliptic curves.

Suppose that C is given by $y^2 = g^2 + \pi h$ subject to the following:

- K is a local field with uniformizer π and residue characteristic p, with $p \nmid 2d$;
- $g(x) \in \mathscr{O}_K[x]$ is a monic polynomial of degree d such that $(\pi, g, g') \subseteq \mathscr{O}_K[x]$ is the unit ideal; and
- $h(x) \in \mathscr{O}_K[x]$ is a polynomial of degree $e \leq 2d$ such that $(\pi, g, h) \subseteq \mathscr{O}_K[x]$ is the unit ideal.

We say such a curve satisfies hypothesis (H). Observe that C is smooth of genus $d - 1$.

Lemma 4.1. *Let C satisfy hypothesis (H), and let $\mathscr{C}$ be the associated arithmetic surface over $\mathscr{O}_K$; i.e., use the same equation and adjoin the usual two points at infinity. Then $\mathscr{C}$ is minimal and regular, the special fiber has dual graph B_d, and the component group Φ of the Jacobian of C over K is $\mathbb{Z}/d\mathbb{Z}$.*

Proof. One checks that the special fiber of $\mathscr{C}$ at infinity is smooth. Then for the given affine piece, we obtain the equation $y^2 = g^2$, which looks like two rational curves intersecting d times, once at each root of g. Regularity of $\mathscr{C}$ need only be checked at these nodes. But $(\pi, g, h) = \mathscr{O}_K[x]$ implies that the reduction of h modulo π does not vanish at any of the nodes; regularity

follows. One also observes that the dual graph is B_d. Minimality follows from checking Castelnuovo's criterion.

For the component group, we follow the standard method (see [16, Prop. 8.1.2] or [4, Thm. 9.6.1]). Since every component of C_k possesses a k-rational point, the component group is unchanged upon base-extension to the maximal unramified extension K^u. One checks that the intersection matrix M for C_k is

$$M = \begin{bmatrix} -d & d \\ d & -d \end{bmatrix}.$$

Then Φ is the homology of $\mathbb{Z}^2 \xrightarrow{M} \mathbb{Z}^2 \to \mathbb{Z}$, where the first map is multiplication by M and the second is $(x, y) \mapsto x + y$. We obtain $\Phi \cong \mathbb{Z}/d\mathbb{Z}$. □

The special fiber C_k has 2 components C^+ and C^- meeting transversely at d points, given by the roots of $\overline{g}$. Label the components so that the point at infinity on C given by $\frac{y}{x^d} = 1$ lies on C^+; we call this point ∞^+, and the other point at infinity ∞^-. Observe that C^+ is given by $y - g(x) = \pi = 0$ and C^- by $y + g(x) = \pi = 0$. That means the coordinate x may be used to specify points on each of C^+ and C^-. Given $\alpha \in k \cup \{\infty\}$, we write α^+ for the point $P \in C^+$ such that $x(P) = \alpha$, and similarly α^- for the point $P \in C^-$ such that $x(P) = \alpha$; this is consistent with our labeling of $\infty^\pm$. Also, $\alpha^+ = \alpha^-$ if and only if $\overline{g}(\alpha) = 0$. Finally, one sees that the set of edges of the dual graph Γ is isomorphic as a $\mathfrak{g}$-set to the set of roots of $\overline{g}$.

Lemma 4.2. *Let $\beta_1, \ldots, \beta_e$ be the roots, counted with multiplicity, of $\overline{h}$ over $\overline{k}$. Let $D = \tau(\mathrm{div}(y - g))$, where τ is the specialization map described in § 3.1. Then*

$$D = \sum \beta_i^+ + (d - e)\infty^+ - d\infty^-.$$

Proof. We first consider the divisor of $y - g$ as a function on $\mathscr{C}$. Write $\mathrm{div}_{\mathscr{C}}(y - g) = \widetilde{D} + D_f$, where $\widetilde{D}$ is horizontal and agrees with the generic divisor $\mathrm{div}_C(y - g)$, and D_f is fibral. As observed earlier, $D_f = C^+$. Since $\widetilde{D} + D_f$ is principal, we have

$$(\widetilde{D} \cdot C^+) = -(D_f \cdot C^+) = d$$
$$(\widetilde{D} \cdot C^-) = -(D_f \cdot C^-) = -d.$$

Thus we may write $D = D^+ - D^-$, where $D^\pm$ is a degree d divisor supported on $C^\pm$, respectively.

To compute the x-coordinates of the points in the support of D, we solve $y^2 = g^2$, which yields $h(x) \equiv 0 \pmod{\pi}$. Since $(\pi, g, h) \subseteq \mathscr{O}_K[x]$ is the unit ideal, $\overline{g}(\beta_i) \neq 0$ for all i. Furthermore, the points $(\beta_i, \overline{g}(\beta_i))$ lie on C^+. Therefore

$$D^+ = \sum \beta_i^+ + (d - e)\infty^+.$$

The remaining points in the support of D must be $\infty^{\pm}$. By degree considerations, the claim follows. □

Lemma 4.3. *Let $\alpha_0, \alpha_i \in \overline{k}$ be distinct roots of $\overline{g}$. Let e_j be the edge of Γ corresponding to α_j for $j = 0, i$ oriented from C^+ to C^-. Let γ_i be the one-cycle $e_i - e_0$ with uniformizers $t_+ = \frac{x-\alpha_0}{x-\alpha_i}$ on C^+ and $t_- = \frac{x-\alpha_i}{x-\alpha_0}$ on C^-. Then*

$$\gamma_i(\infty^+) = \gamma_i(\infty^-) = 1, \text{ and}$$
$$\gamma_i(\operatorname{div}(y-g)) = \frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_i)}.$$

Proof. Since $t_{\pm}(\infty^{\pm}) = 1$ for all four combinations, the first line of equalities follows. Let h_e be the lead coefficient of $\overline{h}$. Observe that

$$\prod_j (\beta_j - \alpha_0) = (-1)^e \frac{\overline{h}(\alpha_0)}{h_e}$$

and similarly for α_i. Therefore

$$\prod_j t_+(\beta_j^+) = \frac{\overline{h}(\alpha_0)}{h_e} \frac{h_e}{\overline{h}(\alpha_i)} = \frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_i)}.$$

But by Lemma 4.2 and the first part of this lemma, the left hand side is equal to $\gamma_i(\operatorname{div}(y-g))$. □

Theorem 4.1. *Let C satisfy hypothesis (H).*

(1) *Suppose d is odd and $\overline{g}$ factors over k as*

$$\overline{g}(x) = (x - \alpha_0) g_1(x) \cdots g_s(x)$$

where $\alpha_0 \in k$ and each of the g_i is irreducible. Let $\alpha_i \in \overline{k}$ be a root of $g_i(x)$. Then C has a rational theta characteristic if and only if $\operatorname{Nm} \overline{h}(\alpha_0)\overline{h}(\alpha_i) \in k^{\times 2}$ for all i. Here $\overline{h}(\alpha_i) \neq 0$ for all i, and the norm is computed from $k(\alpha_i)$ to k.

(2) *If d is even or $\overline{g}$ is irreducible, then C has a rational theta characteristic.*

Proof. In order to apply Theorem 3.1, we must find $L \in \operatorname{Div}^{\{2\}} C$ which is a canonical divisor. The standard choice is $(d-2)(\infty^+ + \infty^-)$; if d is even, then this divisor is clearly divisible by 2, and we have found a rational theta characteristic. We henceforth assume that d is odd, in which case the latter divisor meets each component with odd multiplicity. Let L be $(d-2)(\infty^+ + \infty^-) + \operatorname{div}(y-g)$. Letting D be as in Lemma 4.2, and using the fact that the genus of C is $d-1$, we have

$$\begin{aligned} \tau(L) &:= D + (d-2)\infty^+ + (d-2)\infty^- \\ &= \sum \beta_i^+ + (2g-e)\infty^+ - 2\infty^-. \end{aligned}$$

The g here denotes the genus of C. Observe that $(L{\cdot}C^+) = 2g$ and $(L{\cdot}C^-) = -2$, so $L \in \mathrm{Div}^{\{2\}} C$.

Lemma 4.1 implies that $\Phi[2] = 0$. Thus we need only evaluate L on the relevant 1-cycles. Suppose we are in the first case. We show that the toric part of the special fiber of the Jacobian is in fact a normal torus. Let γ_i be as in Lemma 4.3. Observe that the γ_i form a $\mathbb{Z}[\mathfrak{g}]$-basis for $H_1(\Gamma, \mathbb{Z})$. Let $d_i = \deg g_i$. Let $\chi_i \in X(T)$ correspond to γ_i. The subtorus T_i with character subgroup $\mathbb{Z}[\mathfrak{g}] \cdot \chi_i \subseteq X(T)$ is a norm torus, as the character module is isomorphic to $\mathbb{Z}[Y]/(Y^{d_i} - 1)$—the isomorphism is given by $\chi_i \mapsto Y$, and Frobenius acts as multiplication by Y. But $T = \prod T_i$, which proves that T is a normal torus.

It remains to apply Corollary 3.3. The group $H_1(\Gamma, \mathbb{Z})^{\mathfrak{g}}$ is generated by the elements

$$\operatorname{Nm} \gamma_i := (1 + \sigma + \sigma^2 + \cdots + \sigma^{d_i - 1})\gamma_i.$$

It follows from Lemma 4.3 that

$$(\operatorname{Nm} \gamma_i)(L) = (\operatorname{Nm} \gamma_i)(\operatorname{div}(y - g)) \equiv \operatorname{Nm} \overline{h}(\alpha_0)\overline{h}(\alpha_i) \pmod{k^{\times 2}},$$

and the first case of the theorem is proved.

Let us now consider the case where $\overline{g}(x)$ is irreducible (and d is odd). Let α be any root of $\overline{g}(x)$, and let e be the edge on the dual graph corresponding to α, oriented in either direction. Then the 1-cycles $\sigma^{i+1}e - \sigma^i e$ form a $\mathbb{Z}$-basis for $X(T)$. The characteristic polynomial of Frobenius may then be calculated to be $x^{d-1} + x^{d-2} + \cdots + 1 = 0$. Via Proposition 2.2,

$$\#T(k) = q^{d-1} + q^{d-2} + \cdots + 1$$

which is *odd*; therefore $T(k)/2T(k) = 0$, and there is a rational theta characteristic. □

When d is even, C is an odd genus hyperelliptic curve, and the above argument shows that such curves always have a rational theta characteristic given by $\frac{(g-1)}{2}(\infty^+ + \infty^-)$, regardless of the shape of the special fiber.

Example. If C is given by

$$y^2 = (x^3 - x)^2 + \pi,$$

then $h \equiv 1$, and C has a rational theta characteristic. The Weierstrass points are all rational over $K(\sqrt{\pi})$, so the Galois action on $J[2]$ factors through a cyclic group of order 2. Atiyah [1, §5] showed that if the Galois action on $J[2]$ factors through a cyclic group, then C has a rational theta characteristic; this verifies our result.

On the other hand, if C is given by

$$y^2 = (x^3 - x)^2 + \pi x + 2\pi,$$

then $h(x) = x + 2$, $\alpha_i = 0, \pm 1$, and $h(0)h(1) = 6$, $h(0)h(-1) = 2$. Therefore given $p \geq 5$, the curve C has a rational theta characteristic over $\mathbb{Q}_p$ if and only if $p \equiv \pm 1 \pmod{24}$.

4.2. Calculating torsion on Jacobians when $\Gamma = B_d$. We now apply Proposition 3.3 and the calculations in the proof of Theorem 4.1 to compute the prime-to-p rational torsion on Jacobians of curves satisfying hypothesis (H) under the additional hypothesis that $g(x)$ factors completely over K. We also give a complete description of the prime-to-p torsion when $d = 3$. As far as the author knows, these results furnish the first known examples of curves where the component group of the Jacobian is not a direct summand of the rational torsion group; i.e., the exact sequence (3.1) does not split.

Theorem 4.2. *Let C satisfy hypothesis (H), and suppose that $g(x)$ splits completely. Let α_i be the roots of $\overline{g}$. Let $q = \#k$. Let H be the subgroup of $k^\times$ generated by the numbers $\frac{\overline{h}(\alpha_i)}{\overline{h}(\alpha_0)}$. Let n be the order of $\frac{H \cdot k^{\times d}}{k^{\times d}}$ and let $m = d/n$. Then*

$$J(K)(p') \cong \left(\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\right)^{d-2} \oplus \frac{\mathbb{Z}}{n(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Proof. Since g splits completely, T is a split torus of dimension $d-1$. By Lemma 4.1, $\Phi \cong \mathbb{Z}/d\mathbb{Z}$. Then there is a generator δ for Φ represented by a divisor D' with $(D' \cdot C^-) = -(D' \cdot C^+) = 1$. Observe that $\deg(\mathrm{div}(y-g)) = (-d, d)$. Let γ_i be as in the statement of Lemma 4.3, and $\chi_i \in X(T)$ the corresponding character. Observe that we have an isomorphism

$$\oplus \chi_i : T(k) \xrightarrow{\sim} (k^\times)^{d-1} \cong \left(\frac{\mathbb{Z}}{(q-1)}\right)^{d-1}.$$

Applying Proposition 3.3 with $r = d$, we have that $\chi_i(\nu(\delta))$ equals $\gamma_i(\mathrm{div}(y-g))$. Furthermore

$$\gamma_i(\mathrm{div}(y-g)) = \frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_i)}.$$

It follows that the order of $\nu(\delta)$ is n, and the order of $\ker \nu$ is m. The claim now follows from Proposition 3.3 and Lemma 3.5. □

Theorem 4.3. *Let C satisfy hypothesis (H) with $d = 3$. Let $\alpha_0, \alpha_1, \alpha_2$ be the roots of $\overline{g}(x)$ in $\overline{k}$. Suppose the order of k is q. Let $J(K)(p')$ be the largest torsion subgroup of the rational points on the Jacobian of C with order coprime to p.*

(1) *Suppose $\overline{g}(x)$ has a single root in k, say α_0. If $q \equiv 1 \pmod 3$ and $\frac{\overline{h}(\alpha_0)^2}{\overline{h}(\alpha_1)\overline{h}(\alpha_2)}$ lies in $k^{\times 3}$, or if $q \equiv 2 \pmod 3$ and*

$$\overline{h}(\alpha_1)^{\frac{q^2-1}{3}} = 1,$$

then

$$J(K)(p') \cong \frac{\mathbb{Z}}{(q^2-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Otherwise

$$J(K)(p') \cong \frac{\mathbb{Z}}{3(q^2-1)\mathbb{Z}}$$

(2) *Suppose* $\overline{g}(x)$ *is irreducible over* k. *If* $q \equiv 2 \pmod 3$, *or both* $q \equiv 1 \pmod 3$ *and*

$$\overline{h}(\alpha_0)^{\frac{q^3-1}{3}} = 1,$$

then

$$J(K)(p') \cong \frac{\mathbb{Z}}{(q^2+q+1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Otherwise

$$J(K)(p') \cong \frac{\mathbb{Z}}{3(q^2+q+1)\mathbb{Z}}.$$

Proof. According to Lemma 4.1, $\Phi \cong \mathbb{Z}/3\mathbb{Z}$. Let δ be a generator for Φ such that δ is represented by a divisor D' with $(D' \cdot C^-) = -(D' \cdot C^+) = 1$. We will apply Proposition 3.3 with $r = 3$ to compute $\nu(\delta)$. Since $3 \deg D' = \deg D$, this is equivalent to computing $\gamma(\operatorname{div}(y-g))$ for various choices of γ.

In the first case, let γ_1, γ_2 be as in Lemma 4.3, and let χ_1, χ_2 be the corresponding characters. We see that T is an ℓ-norm torus, where ℓ/k is the unique quadratic extension, and χ_1 yields an isomorphism

$$\chi_1 : T(k) \xrightarrow{\sim} \ell^\times \cong \frac{\mathbb{Z}}{(q^2-1)\mathbb{Z}}$$

Observe that $3 \mid (q^2-1)$. By Proposition 3.3, $\ker \nu \cong \mathbb{Z}/3\mathbb{Z}$ if and only if $\gamma_i(\operatorname{div}(y-g))$ lies in $\ell^{\times 3}$ for $i = 1, 2$, and $\ker \nu = 0$ otherwise. By Lemma 4.3, $\gamma_i(\operatorname{div}(y-g)) = \overline{h}(\alpha_0)/\overline{h}(\alpha_i)$. If $3 \mid (q-1)$, then the map induced by the norm

$$\frac{\ell^\times}{\ell^{\times 3}} \longrightarrow \frac{k^\times}{k^{\times 3}}$$

is an isomorphism, and the claim follows. If $3 \nmid (q-1)$, then $\overline{h}(\alpha_0) \in k^\times = k^{\times 3}$, and since $\overline{h}(\alpha_i)$ for $i = 1, 2$ are conjugate over k, it suffices to determine whether $\overline{h}(\alpha_1)$ lies in $\ell^{\times 3}$. But $\ell^\times$ is cyclic of order q^2-1, so the first case is proved.

In the second case, T is principal, but not a norm torus. As stated in the proof of Theorem 4.1, the characteristic polynomial of Frobenius acting on $X(T)$ is $f(x) = x^2 + x + 1$, and by Proposition 2.2,

$$T(k) \cong \frac{\mathbb{Z}}{(q^2+q+1)\mathbb{Z}}$$

If $q \equiv 2 \pmod 3$, then $3 \nmid (q^2+q+1)$ and $T(k)/3T(k) = 0$. Therefore $\ker \nu = \mathbb{Z}/3\mathbb{Z}$, and we obtain the corresponding conclusion.

Now suppose $q \equiv 1 \pmod 3$. Without loss of generality $\alpha_i = \sigma^i \alpha_0$ for $i = 1, 2$. Then $\gamma_1(\mathrm{div}(y - g)) = \overline{h}(\alpha_0)/\overline{h}(\alpha_1)$; since $\mu(T)$ is cyclic, this lies in $3\mu(T)$ if and only if

$$\left(\frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_1)}\right)^{\frac{q^2+q+1}{3}} = 1.$$

Observe that

$$\frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_1)} \cdot \sigma\left(\frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_1)}\right) = \frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_2)}$$

and so $\overline{h}(\alpha_0)/\overline{h}(\alpha_1) \in 3\mu(T)$ if and only if $\overline{h}(\alpha_0)/\overline{h}(\alpha_2) \in 3\mu(T)$. Via $\alpha_1 = \alpha_0^q$, we have

$$\left(\frac{\overline{h}(\alpha_0)}{\overline{h}(\alpha_1)}\right)^{\frac{q^2+q+1}{3}} = \left(\overline{h}(\alpha_0)^{q+1}\right)^{-\frac{q^2+q+1}{3}} = \overline{h}(\alpha_0)^{-\frac{q^3-1}{3}}.$$

This completes the proof. □

5. A genus 4 nonhyperelliptic family

In this section, we obtain similar results as in § 4 on a family of nonhyperelliptic genus 4 curves. As $2g - 2 = 6$, one can also speak of *cube roots* of the canonical class (also called 3-spin structures); we determine if any of these are rational as well.

Let the base field K be a local field with discrete valuation ring $\mathscr{O}_K$, uniformizer π, and residue characteristic p with $p \geq 5$. For any "integral" element ($x \in \mathscr{O}_K$, $f \in \mathscr{O}_K[X]$, etc.), we use a bar to denote reduction modulo π ($\overline{x}$, $\overline{f}$, etc.). Our family will then be the intersection in $\mathbb{P}^3_K$ of the quadric surface $XY = ZW$ and the family of cubics

$$(X - Y)(Z - W)(Z + W) = \pi\varepsilon$$

where ε varies in a subset of integral homogeneous cubic forms.

Given a projective variety V over K defined by integral equations, we will use script $\mathscr{V}$ to denote the model of V over $\mathscr{O}_K$ obtained by using the same equations. We also write V_k for the special fiber of $\mathscr{V}$.

The recipe is as follows. We first record some general facts about our curves, including the shape of the special fiber. Then we compute the prime-to-p rational torsion on the Jacobian of our curves. Finally, we will determine if there are any rational square roots and cube roots of the canonical class.

5.1. General facts. A nonhyperelliptic genus 4 curve may be given as the intersection of an irreducible quadric surface and an irreducible cubic surface in $\mathbb{P}^3$; this in fact gives the curve in its canonical embedding (see

for example [8, IV.5.2.2 and IV.5.5.2]). Our quadric Q will be given in projective coordinates $[X : Y : Z : W]$ by

$$Q : XY = ZW.$$

Let $\mathscr{Q}$ be the corresponding arithmetic scheme in $\mathbb{P}^3_{\mathscr{O}_K}$; i.e. we use the same equation. Set

$$L_{XY} = X - Y$$
$$L_{ZW} = Z - W$$
$$L_{-ZW} = Z + W.$$

Let ε be a homogeneous cubic form in $\mathscr{O}_K[X, Y, Z, W]$. Let S be the cubic surface given by $L_{XY} \cdot L_{ZW} \cdot L_{-ZW} = \pi\varepsilon$. Let $\mathscr{S}$ be the corresponding arithmetic scheme in $\mathbb{P}^3_{\mathscr{O}_K}$. Let $\mathscr{C}$ be the (scheme-theoretic) intersection $\mathscr{Q} \cap \mathscr{S}$ with generic fiber C.

Lemma 5.1. *If $\overline{\varepsilon} \in k[X, Y, Z, W]$ does not vanish at any of the points*

$$[1 : 1 : 1 : 1], [-1 : -1 : 1 : 1]$$
$$[i : i : -1 : 1], [-i : -i : -1 : 1]$$
$$[1 : 0 : 0 : 0], [0 : 1 : 0 : 0]$$

where i denotes any fixed square root of -1 in $\overline{k}$, then $\mathscr{C}$ is a minimal regular arithmetic surface such that the components of the special fiber are geometrically integral, and such that the dual graph of the special fiber is as pictured in Figure 5.1.

As an example of such an ε when $p \geq 7$, let

$$\varepsilon_0 = X^3 + Y^3 + WZ^2.$$

Proof. We first compute the dual graph. The special fiber of $\mathscr{C}$ is given by

$$XY = ZW, \quad L_{XY} \cdot L_{ZW} \cdot L_{-ZW} = 0.$$

Write C_{XY} for the intersection of Q_k and $L_{XY} = 0$ on the special fiber; define C_{ZW} and C_{-ZW} similarly. Then the special fiber has 3 components: C_{XY}, C_{ZW}, and C_{-ZW}. These are each type $(1, 1)$ divisors on the quadric, and so every pair intersects in two points. Solving for these intersections, we obtain the dual graph in the figure.

For regularity, we need only check that $\mathscr{C}$ is regular at the nodes of the special fiber. By hypothesis, $\overline{\varepsilon}$ does not vanish at any of the nodes, whence the claim follows. Minimality follows from checking Castelnuovo's criterion. □

In the figure, four loops are labeled γ_1, γ_2, γ_3 and $\widetilde{\gamma}$, where γ_3 is the loop consisting of the three outside edges; we orient each loop counterclockwise. We define a fifth loop γ_4 as $\gamma_3 - \widetilde{\gamma}$.

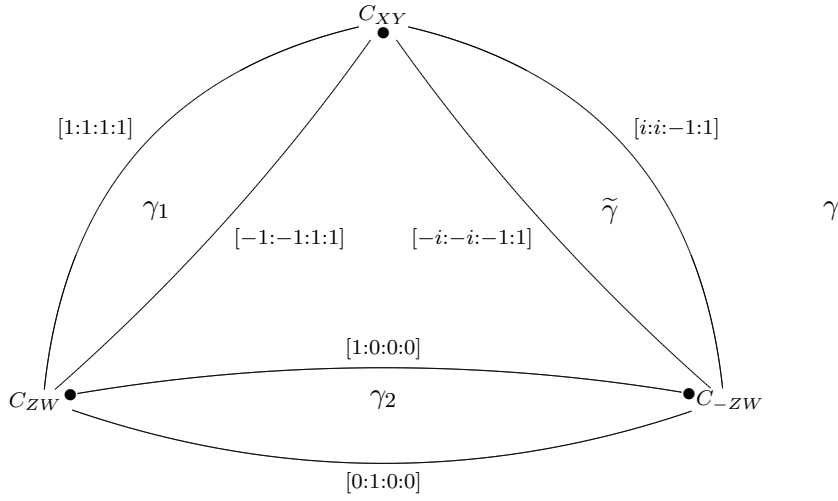


FIGURE 5.1. Dual graph of C_k

Henceforth, we will assume that ε satisfies the lemma.

The Jacobian J of C is an extension of a torus T by the component group Φ; see Lemma 5.3 for the computation of Φ. The torus T is a normal torus: if $i \in k^\times$, then T is split, and $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ form a basis for $H_1(\Gamma, \mathbb{Z})^{\mathfrak{g}} = H_1(\Gamma, \mathbb{Z})$. If $i \notin k^\times$, then T is the product of $\mathbb{G}_m^2$ with the $k(i)$-norm torus. We have $\sigma\gamma_3 = \gamma_4$ and $H_1(\Gamma, \mathbb{Z})^{\mathfrak{g}}$ is generated by γ_1, γ_2, and $\gamma_3 + \gamma_4$.

5.2. Setup for descent. Given a divisor $D \in \operatorname{Div}^{\{1\}} C$, we wish to determine how to evaluate $\gamma_i(D)$ for each i. For each loop, we construct on each component a local parameter which is supported on the nodes. The specific support is determined by the loop. Furthermore, each function must be normalized so as to lie in $F_1(\gamma, k)$ for the appropriate choice of γ. An easy, if lengthy, calculation yields Table 5.1 below.

Each function is written as one on $\mathbb{P}^3_k$, which we then restrict to the appropriate component. When two functions are listed, they agree on an open dense set; one can go from one to the other by using the equations for the given component. For example, on C_{XY} one has $X^2 = ZW$. We have omitted γ_4; it can be obtained from γ_3 by applying the substitution $i \mapsto -i$. (Warning: this map is not in general a homomorphism on $k^\times$; for example, let $k = \mathbb{F}_5$, $i = 2$, and compare $1 + i$ with $1 - i$.) The functions for $\gamma_3 + \gamma_4$ are obtained by computing $\operatorname{Nm}(\gamma_3, (t_i))$. As every component in $\gamma_3 + \gamma_4$ appears with multiplicity 2, it makes sense that the functions are of degree 2 (when interpreted as maps from the relevant component to $\mathbb{P}^1_k$). The divisors for $\gamma_3 + \gamma_4$ are omitted, but may be obtained as the sum of the divisors of γ_3 and γ_4.

Loop	Component	Divisor	Local function
γ_1	C_{XY}	$[-1:-1:1:1]-[1:1:1:1]$	$\dfrac{Z+X}{Z-X}\equiv\dfrac{X+W}{X-W}$
	C_{ZW}	$[1:1:1:1]-[-1:-1:1:1]$	$\dfrac{Z-X}{Z+X}$
γ_2	C_{ZW}	$[1:0:0:0]-[0:1:0:0]$	$\dfrac{Z-Y}{Z-X}$
	C_{-ZW}	$[0:1:0:0]-[1:0:0:0]$	$\dfrac{Z-X}{Z+Y}\equiv\dfrac{X+Z}{Y-Z}$
γ_3	C_{XY}	$[i:i:-1:1]-[1:1:1:1]$	$\dfrac{Z-iX}{Z-X}\equiv\dfrac{X-iW}{X-W}$
	C_{ZW}	$[1:1:1:1]-[0:1:0:0]$	$\dfrac{Z-Y}{Z}$
	C_{-ZW}	$[0:1:0:0]-[i:i:-1:1]$	$\dfrac{X}{Z-iX}$
$\gamma_3+\gamma_4$	C_{XY}	–	$\dfrac{Z^2+X^2}{(Z-X)^2}$
	C_{ZW}	–	$\dfrac{(Z-Y)^2}{Z^2}$
	C_{-ZW}	–	$\dfrac{X^2}{Z^2+X^2}$

TABLE 5.1. Local functions for a basis of $H_1(\Gamma,\mathbb{Z})^{\mathfrak{g}}$

Each function must also be normalized properly. If $i\in k$, then every node is rational over k, and the normalization condition is simply that each function is also defined over k. Clearly, this is satisfied. If $i\notin k$, then we will use evaluation on the cycles γ_1, γ_2, and $\gamma_3+\gamma_4$. Our construction of the functions for $\gamma_3+\gamma_4$ guarantees that the normalization is correct.

5.3. Calculation of torsion on Jacobian. As observed earlier, the prime-to-p rational torsion in the Jacobian $J(K)(p')$ contains a subgroup isomorphic to $T(k)$; we now compute this latter group.

Lemma 5.2. *Let i be any square root of -1 in $\overline{k}$. If $i\in k^\times$, then*

$$T(k)\cong\left(\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\right)^4.$$

If $i \notin k^\times$, then

$$T(k) \cong \left(\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\right)^2 \oplus \frac{\mathbb{Z}}{(q^2-1)\mathbb{Z}}.$$

Proof. As observed in the end of §5.1, if $i \in k^\times$, then T is a split torus, and so $T \cong \mathbb{G}_m^4$; the first claim follows. Note that if we fix an identification of $k^\times$ with $\mathbb{Z}/(q-1)\mathbb{Z}$, then by abuse of notation the isomorphism is given by

$$\oplus\chi_i : T(k) \longrightarrow \left(\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\right)^4.$$

We also observed that if $i \notin k^\times$, then $T \cong \mathbb{G}_m^2 \times R_{k(i)/k}\mathbb{G}_m$. As $R_{k(i)/k}\mathbb{G}_m(k) \cong \mathbb{G}_m(k(i)) \cong \mathbb{Z}/(q^2-1)\mathbb{Z}$, the second assertion follows. The isomorphism is given by

$$(\chi_1, \chi_2, \chi_3) : T(k) \longrightarrow \frac{\mathbb{Z}}{(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(q^2-1)\mathbb{Z}}.$$

□

We now use the descent map to compute the remaining factor in the prime-to-p torsion. Let $\tau : \mathrm{Div}^{\{1\}} C \longrightarrow \mathrm{Div}\, C_k$ be the specialization map, as in § 3.1. We define our degree map by

$$\begin{aligned} \deg : \mathrm{Div}\, C_k &\longrightarrow \mathbb{Z}^3 \\ D &\longmapsto ((D \cdot C_{XY}), (D \cdot C_{ZW}), (D \cdot C_{-ZW})). \end{aligned}$$

Lemma 5.3. *The component group of the Jacobian of C over K is*

$$\Phi \cong \frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

There are generators δ_1, δ_2 for the respective cyclic subgroups represented by divisors $D_1, D_2 \in \mathrm{Div}^{\{1\}} C$ respectively such that

$$\begin{aligned} \deg \tau(D_1) &= (0, 1, -1) \\ \deg \tau(D_2) &= (1, -1, 2). \end{aligned}$$

Proof. The intersection matrix for C_k is

$$\begin{bmatrix} -4 & 2 & 2 \\ 2 & -4 & 2 \\ 2 & 2 & -4 \end{bmatrix}.$$

One then verifies the claims via [16, Proposition 8.1.2]. □

Consider the pullback of $\mathscr{O}(1)$ to C. Given a linear form L in X, Y, Z, W, we write $\mathrm{div}\, L$ to mean the divisor of the corresponding section of the pullback sheaf; as observed earlier, this is a section of the canonical bundle of C. Similarly, for any function f on $\mathbb{P}^3$, $\mathrm{div}\, f$ means the divisor of the restriction of f to C.

Lemma 5.4. *We have*

$$\deg\left(\tau\left(\operatorname{div}\frac{Z-W}{Z+W}\right)\right) = (0,6,-6)$$
$$\deg\left(\tau\left(\operatorname{div}\frac{X+Y}{Z+W}\right)\right) = (2,2,-4).$$

Proof. The divisor of each linear section is effective of degree 6. Clearly the specialization of the divisor of $Z-W$ lies entirely on C_{ZW}, and similarly for $Z+W$ and C_{-ZW}. As for $X+Y$, we consider the special fiber C_k as the intersection of Q_k with the degenerate cubic form $L_{XY}L_{ZW}L_{-ZW}=0$. Each of L_{XY}, L_{ZW}, L_{-ZW} gives rise to a type $(1,1)$ divisor on Q_k, as does $X+Y=0$. Thus the divisor of $X+Y$ intersects each component of C_k in two points (up to multiplicity). The claim follows. □

To calculate the prime-to-p torsion of $J(K)$, we will evaluate the functions in Table 5.1 on the specializations of the divisors of $X+Y$, $Z-W$, and $Z+W$.

Lemma 5.5. *The specialization of the divisor* $\operatorname{div}(X+Y)$ *on* C_k *is*

$$[0:0:1:0]+[0:0:0:1]$$
$$+[i:-i:1:1]+[-i:i:1:1]$$
$$+[-1:1:-1:1]+[1:-1:-1:1].$$

The first pair lies on C_{XY}*, the second on* C_{ZW}*, and the third on* C_{-ZW}*.*

Proof. As mentioned earlier, the hyperplane $X+Y=0$ in $\mathbb{P}^3_k$ intersects every component transversely in two points, and so the calculation of $\operatorname{div}(X+Y)$ is straightforward. The second claim is easily verified. □

Let

$$h_{ZW}(x) = x^3\overline{\varepsilon}\left(x,\frac{1}{x},1,1\right)$$
$$h_{-ZW}(x) = x^3\overline{\varepsilon}\left(x,-\frac{1}{x},-1,1\right)$$

Let $\alpha_1,\cdots,\alpha_6$ be the roots of $h_{ZW}(x)$ counted with multiplicity, and similarly let $\beta_1,\cdots,\beta_6$ be the roots of $h_{-ZW}(x)$.

Lemma 5.6. *The specialization of the divisor of* $Z-W$ *is*

$$\sum\left[\alpha_i:\frac{1}{\alpha_i}:1:1\right].$$

The specialization of the divisor of $Z+W$ *is*

$$\sum\left[\beta_i:-\frac{1}{\beta_i}:-1:1\right].$$

Proof. We first consider $Z - W$. Generically, we wish to solve the system

$$XY = ZW, \quad Z = W, \quad \varepsilon(X, Y, Z, W) = 0.$$

Lemma 5.1 implies that $\varepsilon = aX^3 + bY^3 + \cdots$, where $a, b \in \mathscr{O}_K$ are units. If $Z = W = 0$, this implies that $X = Y = 0$, which does not occur in $\mathbb{P}^3$. Therefore we may assume that $Z = W = 1$. Together with the fact that the coefficient $\overline{b} \neq 0$, the claim for $Z - W$ now follows.

Similar reasoning holds for the divisor of $Z + W$. □

Lemma 5.7. *For $c \neq 0$, the following equalities hold:*

$$\prod(c - \alpha_i) = \prod(\alpha_i - c) = c^3 \frac{\overline{\varepsilon}(c, \frac{1}{c}, 1, 1)}{\overline{\varepsilon}(1, 0, 0, 0)}$$

$$\prod(c - \beta_i) = \prod(\beta_i - c) = c^3 \frac{\overline{\varepsilon}(c, -\frac{1}{c}, -1, 1)}{\overline{\varepsilon}(1, 0, 0, 0)}$$

$$\prod \alpha_i = -\prod \beta_i = \frac{\overline{\varepsilon}(0, 1, 0, 0)}{\overline{\varepsilon}(1, 0, 0, 0)}$$

Proof. Observe that the lead coefficients of h_{ZW} and of h_{-ZW} are the coefficient of X^3 in $\overline{\varepsilon}$, which equals $\overline{\varepsilon}(1, 0, 0, 0)$. From this, the first two claims are trivial. To evaluate $\prod \alpha_i$, we see that the product equals $h_{ZW}(0)$ divided by its lead coefficient, which is the constant term of $x^3\overline{\varepsilon}(x, \frac{1}{x}, 1, 1)$ divided by its lead coefficient. Since $\overline{\varepsilon}$ is a homogeneous cubic, the constant term is the coefficient of Y^3, which equals $\overline{\varepsilon}(0, 1, 0, 0)$. The argument for $\prod \beta_i$ is similar. □

We now evaluate the γ_i on the divisors discussed above, as well as on certain linear combinations of these divisors. For convenience, we only summarize the results in Table 5.2 below—the calculations are routine. The only two "tricks" are liberal use of Lemma 5.7 and that, for each point in the support of the given divisor, one should choose the local parameter in Table 5.1 which is regular and nonvanishing at that point. (The Table 5.1 is constructed so that there is always such a choice for the divisors below.) In Table 5.2, we write ε in place of $\overline{\varepsilon}$ for convenience. In the interests of space, we omit $\gamma_4(D)$, which can be obtained by replacing i with $-i$ in $\gamma_3(D)$.

Theorem 5.1. *Let K be a local field with uniformizer π and residue field k of characteristic $p \geq 5$ and order q. Let $i \in \overline{k}^\times$ be a fixed square root of -1. Let C be the locus in $\mathbb{P}^3_K$ given by $XY = ZW$ and*

$$(X - Y)(Z - W)(Z + W) = \pi\varepsilon$$

with $\varepsilon \in \mathscr{O}_K[X, Y, Z, W]$ a homogeneous cubic satisfying Lemma 5.1. Let J be its Jacobian, $J(K)(p')$ the largest torsion subgroup of $J(K)$ with order

D	$\gamma_1(D)$	$\gamma_2(D)$	$\gamma_3(D)$	$\gamma_4(D)$
$\operatorname{div} X+Y$	-1	-1	$-i$	–
$\operatorname{div} Z-W$	$\frac{\varepsilon(1,1,1,1)}{\varepsilon(-1,-1,1,1)}$	$\frac{\varepsilon(1,0,0,0)}{\varepsilon(0,1,0,0)}$	$\frac{\varepsilon(1,1,1,1)}{\varepsilon(0,1,0,0)}$	–
$\operatorname{div} Z+W$	1	$-\frac{\varepsilon(0,1,0,0)}{\varepsilon(1,0,0,0)}$	$i\frac{\varepsilon(0,1,0,0)}{\varepsilon(i,i,-1,1)}$	–
$\operatorname{div} \frac{Z-W}{Z+W}$	$\frac{\varepsilon(1,1,1,1)}{\varepsilon(-1,-1,1,1)}$	$-\frac{\varepsilon(1,0,0,0)^2}{\varepsilon(0,1,0,0)^2}$	$-i\frac{\varepsilon(1,1,1,1)\varepsilon(i,i,-1,1)}{\varepsilon(0,1,0,0)^2}$	–
$\operatorname{div} \frac{X+Y}{Z+W}$	-1	$\frac{\varepsilon(1,0,0,0)}{\varepsilon(0,1,0,0)}$	$-\frac{\varepsilon(i,i,-1,1)}{\varepsilon(0,1,0,0)}$	–
$\operatorname{div} \frac{Z-W}{X+Y}$	$-\frac{\varepsilon(1,1,1,1)}{\varepsilon(-1,-1,1,1)}$	$-\frac{\varepsilon(1,0,0,0)}{\varepsilon(0,1,0,0)}$	$i\frac{\varepsilon(1,1,1,1)}{\varepsilon(0,1,0,0)}$	–
$\operatorname{div} \frac{Z^2-W^2}{X+Y}$	$-\frac{\varepsilon(1,1,1,1)}{\varepsilon(-1,-1,1,1)}$	1	$-\frac{\varepsilon(1,1,1,1)}{\varepsilon(i,i,-1,1)}$	–
$\operatorname{div} \frac{(Z+W)^2}{Z-W}$	$\frac{\varepsilon(-1,-1,1,1)}{\varepsilon(1,1,1,1)}$	$\frac{\varepsilon(0,1,0,0)^3}{\varepsilon(1,0,0,0)^3}$	$-\frac{\varepsilon(0,1,0,0)^3}{\varepsilon(i,i,-1,1)^2\varepsilon(1,1,1,1)}$	–

TABLE 5.2. Evaluation of loops on certain divisors

not divisible by p, and T the toric part of the reduction of a Néron model for J over $\mathscr{O}_K$. Then $J(K)(p')$ lies in a short exact sequence

$$0 \longrightarrow T(k) \longrightarrow J(K)(p') \longrightarrow \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \longrightarrow 0.$$

More precisely, we have the following.

(1) *Suppose $i \in k^\times$. Then $J(K)(p')$ is isomorphic to*

$$\frac{\mathbb{Z}}{a_0\mathbb{Z}} \oplus \frac{\mathbb{Z}}{b_0\mathbb{Z}} \oplus \frac{\mathbb{Z}}{a_1(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{b_1(q-1)\mathbb{Z}} \oplus \left(\frac{\mathbb{Z}}{(q-1)\mathbb{Z}}\right)^2$$

where $a_0a_1 = 6$, $b_0b_1 = 2$, and these constants are computed as follows:

Let $H_1 \subseteq k^\times$ be the subgroup generated by the entries in the row $\operatorname{div} \frac{Z-W}{Z+W}$ of Table 5.2, let H_2 be the group generated by the entries in the row $\operatorname{div} \frac{X+Y}{Z+W}$, and let H_3 be the group generated by the entries in the row $\operatorname{div} \frac{Z-W}{X+Y}$. (Recall that the last entry $\gamma_4(D)$ is obtained from $\gamma_3(D)$ by replacing i with $-i$.)

Then a_1 is the order of $\frac{H_1 \cdot k^{\times 6}}{k^{\times 6}}$ and $a_0 = 6/a_1$.

If $H_3 \subseteq k^{\times 2}$, set $b_1 = 1$ and $b_0 = 2$. Otherwise, b_1 is the order of $\frac{H_2 \cdot k^{\times 2}}{k^{\times 2}}$ and $b_0 = 2/b_1$.

(2) *Suppose $i \notin k^\times$. Then $J(K)(p')$ is isomorphic to*

$$\frac{\mathbb{Z}}{a_0\mathbb{Z}} \oplus \frac{\mathbb{Z}}{c_0\mathbb{Z}} \oplus \frac{\mathbb{Z}}{a_1(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{b_1(q-1)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{b_3c_3(q^2-1)\mathbb{Z}}$$

where $a_0a_1 = b_1b_3 = 2$, $c_0c_3 = 3$, and these constants are computed as follows:

Let $\ell = k(i)$. Let $H_1 \subseteq k^\times$ be the subgroup generated by the first two entries of row $\operatorname{div} \frac{Z-W}{Z+W}$ *of Table 5.2 and the norm from ℓ to k of the third entry. Let $H_3 \subseteq k^\times$ be the subgroup generated by the first two entries of row* $\operatorname{div} \frac{Z-W}{X+Y}$ *and the norm from ℓ to k of the third entry.*

If $3 \mid (q-1)$ and $H_1 \subseteq k^{\times 3}$, or $3 \nmid (q-1)$ and

$$\varepsilon(i, i, -1, 1)^{(q^2-1)/3} = 1,$$

then $c_0 = 3$. Otherwise $c_0 = 1$. In either case, $c_3 = 3/c_0$.

If $\operatorname{Nm}_{\ell/k} \varepsilon(i, i, -1, 1) \in k^{\times 2}$, then $b_1 = 2$ and $b_3 = 1$. Otherwise, $b_1 = 1$ and $b_3 = 2$.

If $H_3 \subseteq k^{\times 2}$, then $a_0 = 2$ and $a_1 = 1$. Otherwise, $a_0 = 1$ and $a_1 = 2$.

A word about the notation: letting δ_1 and δ_2 be generators for Φ as in Lemma 5.3, the a_j give the contribution of δ_1 to $J(K)(p')$ and the b_j give the contribution of δ_2 in the case $i \in k^\times$. When $i \notin k^\times$, the a_j give the contribution of $3\delta_1$ while the c_j give the contribution of $2\delta_1$. The subscripts on the constants roughly refer to the subscript on the corresponding one-cycle, except the subscript 0 refers to contributions coming from the kernel of ν as in Proposition 3.3. For example, letting $r = 2$ in that proposition, if $\gamma_1(3\delta_1)$ is nontrivial, then $a_1 = 2$. This is not quite correct in all cases; for example, when $i \in k^\times$, we use $a_1 = 2$ if $\gamma_j(3\delta_1)$ is nontrivial for any j. By the symmetry of the factors in $T(k)$ (according to Lemma 5.2), it doesn't matter which γ_j yields a nontrivial value.

Proof. The short exact sequence follows from Proposition 3.2 and the calculation of the component group Φ in Lemma 5.3.

Suppose $i \in k^\times$. Let $r = 2$ in Proposition 3.3. Note that the nontrivial elements of $\Phi[2]$ are $3\delta_1$, δ_2, and $3\delta_1 - \delta_2$, with notation as in Lemma 5.3. By Lemma 5.4, the relevant functions in Proposition 3.3 are $\operatorname{div} \frac{Z-W}{Z+W}$, $\operatorname{div} \frac{X+Y}{Z+W}$, and $\operatorname{div} \frac{Z-W}{X+Y}$ respectively. The conditions on the b_j and the 2-part of the a_j now follow from the latter proposition and Corollary 3.2. For example, $\nu(\delta_2) = 0$ if and only if $\gamma_j(\operatorname{div} \frac{X+Y}{Z+W}) \equiv 1 \pmod{k^{\times 2}}$ for all j, which is equivalent to $[H_2 \cdot k^{\times 2} : k^{\times 2}] = 1$.

For $r = 3$, we wish to determine whether $\nu(2\delta_1)$ is trivial or not; if it is, $3 \mid a_0$ and $3 \nmid a_1$. If it is not, then $3 \mid a_1$ and $3 \nmid a_0$. The determination of $\nu(2\delta_1)$ proceeds in a similar way as in the $r = 2$ case above.

The $i \notin k^\times$ case is similar, but with the following additional complications. First, suppose $r = 2$. Observe that neither $\gamma_2(\operatorname{div} \frac{Z-W}{Z+W})$ nor $\gamma_1(\operatorname{div} \frac{X+Y}{Z+W})$ lie in $k^{\times 2}$ in this case. Next, the factors $\mu(T_j) := \chi_j(T(k))$ for $j = 1, 2, 3$ are not all isomorphic to each other by Lemma 5.2. Let $x \in J(k)$ be any element mapping to $3\delta_1 \in \Phi[2]$. Then even though $\nu(3\delta_1) \neq 0$, the 2-part of the order of x depends on whether $\gamma_3(\operatorname{div} \frac{Z-W}{Z+W})$ lies in $2\mu(T_3)$ or not. Since $\mu(T_3) = \ell^\times$ and the norm gives an isomorphism

$$\frac{\ell^\times}{\ell^{\times 2}} \longrightarrow \frac{k^\times}{k^{\times 2}}$$

one sees that $\gamma_3(\operatorname{div} \frac{Z-W}{Z+W})$ lies in $2\mu(T_3)$ if and only if $\operatorname{Nm}_{\ell/k} \varepsilon(i, i, -1, 1) \in k^{\times 2}$. This explains the condition on the b_j; the condition on the a_j follows easily.

Lastly, let $r = 3$. If $3 \nmid (q-1)$, then γ_1 and γ_2 automatically take values in $k^{\times 3} = k^\times$. Therefore in order to determine if $\nu(2\delta_1) = 0$, we need to determine if $\gamma_3(\operatorname{div} \frac{Z-W}{Z+W})$ lies in $\ell^{\times 3}$. The condition for the c_j now follows from the observations that $i^3 = -i$ and $k^\times \subseteq \ell^{\times 3}$. □

5.4. Rationality of theta characteristics and cube roots of the canonical class.

Theorem 5.2. *Let C be as in the hypotheses of Theorem 5.1. Let $i \in \overline{k}^\times$ be a fixed square root of -1. Define groups $T_j \subseteq k^\times$ for $j = 1, \ldots, 4$ as follows.*

If $i \in k^\times$, let T_1 be the subgroup generated by the entries in row $\operatorname{div}(X + Y)$ of Table 5.2. Similarly, let T_2, T_3, T_4 be the subgroups generated by rows $\operatorname{div}(Z - W)$, $\operatorname{div}(Z + W)$, and $\operatorname{div} \frac{Z^2-W^2}{X+Y}$ respectively.

If $i \notin k^\times$, let $\ell = k(i)$, and let each T_j be computed for the corresponding row as above, but this time taking the subgroup generated by the first two entries of the row, plus the norm from ℓ to k of the third entry.

Then C has a rational theta characteristic if and only if some T_j lies in $k^{\times 2}$.

Proof. We apply Corollary 3.2. The canonical divisor may be given by $\operatorname{div} X + Y$, which lies in $\operatorname{Div}^{\{2\}} C$. There are 4 elements in $\Phi[2]$; the corresponding functions as in Corollary 3.2 are 1, $\frac{Z-W}{X+Y}$, $\frac{Z+W}{X+Y}$, and $\frac{Z^2-W^2}{(X+Y)^2}$. Observe that

$$\gamma_i\left(\operatorname{div}(X + Y) + \operatorname{div} \frac{Z - W}{X + Y} \right) = \gamma_i(\operatorname{div} Z - W);$$

one does similar calculations for the other functions.

When $i \notin k^\times$, by Corollary 3.3 we need to evaluate γ_1, γ_2, and $\gamma_3 + \gamma_4$. This explains why we take the norm of the third entry. □

Theorem 5.3. *Let C be as in Theorem 5.1. If $i \in k^\times$, let $S_1 \subseteq k^\times$ be the subgroup generated by the entries of row* $\operatorname{div}(Z-W)$ *in Table 5.2. Similarly, let S_2, S_3 be the subgroups generated by the rows* $\operatorname{div} Z + W$ *and* $\operatorname{div} \frac{(Z+W)^2}{Z-W}$ *respectively. If $i \notin k^\times$ and $3 \mid (q-1)$, let S_i be the subgroups generated by the first two entries of the corresponding rows and the norm from ℓ to k of the third entry. In these two cases, C has a rational cube root of the canonical class if and only if some S_i lies in $k^{\times 3}$.*

If $i \notin k^\times$ and $3 \nmid (q-1)$, then C has a rational cube root of the canonical class if and only if $\varepsilon(i, i, -1, 1)^{(q^2-1)/3} = 1$.

Proof. The proof is analogous to that of Theorem 5.2. Here, we use $\operatorname{div}(Z - W)$ as our canonical divisor, observing that it lies in $\operatorname{Div}^{\{3\}} C$. We have $\Phi[3]$ has 3 elements with corresponding functions 1, $\frac{Z+W}{Z-W}$, and $\frac{(Z+W)^2}{(Z-W)^2}$. Thus in Theorem 3.1, we set $r = 3$ and use the divisors of the sections in the statement above. The case when $i \in k^\times$ follows from Theorem 3.1. The case when $i \notin k^\times$ but $3 \mid (q-1)$ follows from Corollary 3.3.

Now suppose that $i \notin k^\times$ and $3 \nmid (q-1)$. Since $k^{\times 3} = k^\times$, we automatically have $\gamma_1(D) = \gamma_2(D) = 1$ for D the three relevant divisors. Therefore C has a rational cube root of the canonical class if and only if $\gamma_3(D)$ and $\gamma_4(D)$ lie in $\ell^{\times 3}$. Since these are conjugate, it suffices that $\gamma_3(D) \in \ell^{\times 3}$. The claim now follows from the observations that $k^\times \subseteq \ell^{\times 3}$ and $i^3 = -i$. □

Example. If $K = \mathbb{Q}_p$ with $p \equiv 5 \pmod{12}$, then $i \in \mathbb{F}_p^\times$ and $\frac{\mathbb{F}_p^\times}{\mathbb{F}_p^{\times 3}} = 1$. Therefore C has a rational cube root of the canonical class for every ε satisfying Lemma 5.1.

References

[1] M. F. Atiyah, *Riemann surfaces and spin structures.* Ann. Sci. École Norm. Sup. **4** (1971), 47–62.

[2] M. Baker, *Specialization of linear systems from curves to graphs.* Algebra Number Theory **2** (2008), 613–653.

[3] S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model.* Manuscripta Math. **98** (1999), 275–293.

[4] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models.* Springer-Verlag, 1990.

[5] A. Chiodo, *Stable twisted curves and their r-spin structures.* Ann. Inst. Fourier **58** (2008), 1635–1689.

[6] O. Gabber, Q. Liu, and D. Lorenzini, *The index of an algebraic variety.* Inventiones mathematicae (2012), 1–60.

[7] B. H. Gross and J. Harris, *On some geometric constructions related to theta characteristics.* Contributions to automorphic forms, geometry, and number theory, Johns Hopkins Univ. Press, 2004, 279–311.

[8] R. Hartshorne, *Algebraic geometry.* Springer-Verlag, 1977.

[9] N. M. Katz, *Galois properties of torsion points on abelian varieties.* Inventiones Mathematicae **62** (1981), 481–502.

[10] Q. Liu, *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics **6**, Oxford, 2002.

[11] D. Mumford, *Theta characteristics of an algebraic curve*. Ann. Sci. École Norm. Sup. **4** (1971), 181–192.
[12] T. Ono, *Arithmetic of algebraic tori*. Ann. of Math. **74** (1961), 101–139.
[13] M. Pacini, *On Néron models of moduli spaces of theta characteristics*. J. Algebra **323** (2010), 658–670.
[14] R. Parimala and W. Scharlau, *On the canonical class of a curve and the extension property for quadratic forms*. Recent advances in real algebraic geometry and quadratic forms, AMS, Providence, 1994, 339–350.
[15] B. Poonen and E. Rains, *Self cup products and the theta characteristic torsor*. Math. Res. Letters **18** (2011), 1305–1318.
[16] M. Raynaud, *Spécialisation du foncteur de Picard*. Inst. Hautes Études Sci. Publ. Math. **38** (1970), 27–76.
[17] V. Suresh, *On the canonical class of hyperelliptic curves*. Recent advances in real algebraic geometry and quadratic forms, AMS, Providence, 1994, 399–404.

Shahed Sharif
California State University San Marcos
333 S. Twin Oaks Valley Rd.
San Marcos, CA 92096, USA
E-mail: ssharif@csusm.edu
URL: http://public.csusm.edu/ssharif