Asian J. Math.
Vol. 19, No. 5, pp. 951–986, November 2015

007

WILD QUOTIENT SURFACE SINGULARITIES WHOSE DUAL GRAPHS ARE NOT STAR-SHAPED*

HIROYUKI ITO† AND STEFAN SCHRÖER‡

Abstract. We obtain results that answer certain questions of Lorenzini on wild quotient singularities in dimension two: Using Kato's theory of log structures and log regularity, we prove that the dual graph of exceptional curves on the resolution of singularities contains at least one node. Furthermore, we show that diagonal quotients for Hermitian curves by analogues of Heisenberg groups lead to examples of wild quotient singularities where the dual graph contains at least two nodes.

Key words. Wild quotient singularities, local fundamental groups, Hermitian curves.

AMS subject classifications. 14B05, 14H37.

Introduction. Quotient singularities arise in algebraic geometry and commutative algebra whenever finite groups act on complex spaces, schemes, or rings. Roughly speaking, a *quotient singularity* is a local ring $R = A^G$ arising as the ring of invariants inside a regular local ring with respect to a finite group of automorphisms. It is called *wild* if the characteristic of the residue field $k = R/\mathfrak{m}_R$ is positive and divides the order of the group G, and *tame* otherwise. Although quotient singularities play a crucial role in various areas (toric varieties, McKay correspondence, stable reduction, singularity theory, surfaces of general type etc.), only few concrete examples and general results seem to be known for the wild case.

Lorenzini initiated a systematic study of *wild quotient singularities in dimension two* in a series of papers ([39], [40], and [41]). The goal of this article is to further investigate such singularities. Let R be a local noetherian ring that is normal and 2-dimensional. For simplicity we suppose that the ring is complete, with separably closed residue field. Attached to this situation is the so-called *dual graph*. This is the graph whose vertices correspond to the irreducible components of the exceptional divisor $E \subset X$ on the minimal good resolution of singularities $X \to \operatorname{Spec}(R)$, with edges indicating intersections. It is well-known that the dual graph of a quotient singularity is a *tree*, and that the irreducible components are copies of $\mathbb{P}^1$.

Brieskorn's characteristic zero classification of quotient singularities [10] reveals that the number of nodes in the dual graph is either zero or one. In stark contrast, little seems to be known about the structure of dual graphs for wild quotient singularities. In this context the term *node* refers to vertices of valency ≥ 3, that is, having at least three neighbors.

Lorenzini recently posed a list of striking questions on such singularities [42]. Among other things, he asks whether there are wild quotient singularities whose *dual graphs have no node*, or some whose *dual graphs have at least two nodes*, and whether the dual graphs occurring *over fields are the same as those occurring in mixed characteristics*. Our first main result answers the first question to the negative:

Theorem (see Corollary 2.2). *Dual graphs of wild quotient singularities in dimension two contain at least one node.*

*Received October 12, 2012; accepted for publication September 12, 2014.
†Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, 2641 Yamazaki, Noda, Chiba, 278-8510, Japan (ito_hiroyuki@ma.noda.tus.ac.jp).
‡Mathematisches Institut, Heinrich-Heine-Universität, 40204 Düsseldorf, Germany (schroeer@math.uni-duesseldorf.de).

We prove this by computing the *local fundamental group* $\pi_1^{\mathrm{loc}}(R)$ of 2-dimensional singularities whose exceptional divisor is a chain of projective lines. Such are called *Hirzebruch–Jung singularities*. Note that we do not suppose that R contains a field. It turns out that the local fundamental group is cyclic of order prime to the characteristic exponent of the residue field. This generalizes Artin's observation on rational double points over fields [3]. Our approach hinges on Kato's theory of *log structures* [32], and in particular his results on *log regularity* [33], a notion that generalizes toroidal embeddings to mixed characteristics. We refer to Ogus's lecture notes [46] for an in-depth exposition of this theory.

The second part of this paper deals with the construction of wild quotient singularities having at least two nodes. Here we work over a ground field k of characteristic $p > 0$. The idea is rather simple: Take a curve C with unusually large automorphism group, and look at the quotient $G\backslash(C \times C)$ of the selfproduct by the diagonal action of the Sylow-p-subgroup $G \subset \mathrm{Aut}(C)$. Quotients of the form $G\backslash(C \times C')$ were already studied by Lorenzini [41], who treated the case that one factor is ordinary, and ourselves [30] in the case that both factors are certain Artin–Schreier curves, chosen in such a way that local computations become feasible.

Here we study the case where

$$C: \quad y^q - y = x^{q+1}$$

are so-called *Hermitian curves*, for prime powers $q = p^m$. By results of Stichtenoth, the number of automorphisms way exceeds the Hurwitz bound. In fact, these curves have the largest possible number of automorphisms in relation to the genus, even by characteristic p standards ([52] and [53]). The Sylow-p-subgroup $G \subset \mathrm{Aut}(C)$ has order $\mathrm{ord}(G) = q^3$. It turns out that G is a so-called *special p-group*. These are certain nonabelian groups analogous to Heisenberg groups, which play a role in the classification of the finite simple groups. All in all, $G\backslash(C \times C)$ is a very natural candidate to look for non-star-shaped dual graphs. Our second main result tells us that this indeed something happens:

Theorem (see Theorem 6.1). *The dual graph for the minimal resolution of singularities for the wild quotient singularity on $G\backslash(C \times C)$ contains at least two nodes.*

Note that our arguments are indirect, such that we gain no control over the precise form of the dual graph nor its exact number of nodes, let alone the formal equations for the singularity. In some sense, this answers Lorenzini's second question in a positive way. He had, however, only the case $G = \mathbb{Z}/p\mathbb{Z}$ in mind. Note also that he had already constructed an example of a wild quotient singularity in mixed characteristics over the 2-adic numbers with two nodes [39].

Finally, we analyze the induced group action on the étale cohomology $H^1(C, \mathbb{Q}_l)$. Note that there are many formulas expressing cohomology as representations for tame actions, for example due to Chevalley and Weil [12], Ellingsrud and Lønsted [19], Köck [36], and others, but all breaks down in the wild case. Rather, we have to apply brute force, and completely determine the irreducible representations of our special p-groups over various fields, and then single out the given representation via the Lefschetz Trace Formula. Our third main result is an explicit description of the cohomology as representation. It might be stated as follows:

Theorem (see Theorem 11.1). *Let $l \neq p$ be a prime different from the characteristic p. In case $p \geq 3$ we assume that p does not divide $l-1$. Then the G-representation*

$H^1(C, \mathbb{Q}_l)$ is the direct sum over a basic set of irreducible G-representations over $\mathbb{Q}_l$ that do not factor over the abelianization G^{ab}.

See Sections 10 for an explicit description of irreducible representations over various fields. It turns out that under the assumptions of the preceding Theorem, the cohomology $H^1(C, \mathbb{Q}_l)$ is irreducible as a representation of the full automorphism group $\mathrm{Aut}(C)$, which appears to be rather peculiar. Furthermore, knowing cohomology as representation allows us to compute the Chern numbers for the relative minimal model of $G\backslash(C \times C)$.

The paper is organized as follows. Section 1 contains general facts on wild quotients. In Section 2 we give an abstract criterion to express certain local fundamental group as Galois groups and state our result on the local fundamental group of Hirzebruch–Jung singularities. We prove this result in Section 3, using Kato's theory of log schemes and log regularity. A technical step, which is elementary but somewhat lengthy, is completed in Section 4. In Section 5 we turn to Hermitian curves and their automorphism groups. In Section 6 we state that the corresponding diagonal quotients yield wild quotient singularities with at least two nodes. The proof occupies Sections 7 and 8. We return to Hermitian curves in Section 9, where the ramification groups and Swan conductors are computed. In Section 10 we examine the extraspecial p-groups acting on Hermitian curves and make a comprehensive investigation of their representation theory. This is applied in Section 11, in which the first l-adic cohomology of Hermitian curves is computed as a representation. In Section 12, we observe that such curves are supersingular. Section 13 contains a general investigation of diagonal quotients and their Picard numbers in terms of cohomology as representation. We apply this in the final Section 14 to compute the Chern numbers of the minimal smooth model of the diagonal quotient for Hermitian curves.

Acknowledgement. The first author would like to thank the Mathematisches Institut of the Heinrich-Heine-Universität Düsseldorf, where this work has progressed, for its warm hospitality. Research of the first author was partially supported by Grand-in-Aid for Scientific Research (C) 24540051, MEXT.

We also would like to thank the referee for careful reading and suggestions to improve the paper.

1. Generalities on wild quotient singularities. Let G be a finite group acting on a regular local noetherian ring A. Then the invariant ring $R = A^G$ is a normal local noetherian ring, and the ring extension $R \subset A$ is finite. If the induced G-action on $X = \mathrm{Spec}(A)$ is free in codimension one, the ring R and its spectrum $Y = \mathrm{Spec}(R)$ are called *quotient singularity*. Note that we do not assume that our rings contain fields.

At various places it will be convenient to use the *characteristic exponent* of a field; recall that this is 1 if the field has characteristic zero, and equal to the characteristic of the field otherwise. A quotient singularity R is called *tame* if the order of G is prime to the characteristic exponent $p \geq 1$ of the residue field $k = A/\mathfrak{m}_A$. The situation becomes particularly simple if $A = \mathcal{O}_{X,x}^\wedge$ is a complete local ring for a point $x \in X$ on a complex manifold: By results going back to H. Cartan [11], the group G acts linearly on a suitable regular system of parameters. If G is abelian, one may diagonalize simultaneously, and the situation is easily described in terms of toric varieties.

A quotient singularity R is called *wild* if the order of G is not prime to the characteristic exponent of the residue field. Many properties of tame quotient singularities do not hold true: First of all, it is unclear whether or not *resolutions of singularities* exists in higher dimensions. Next, wild quotient singularities are usually not *Cohen–Macaulay*. This was first observed by Fossum and Griffith [21], and studied in more detail by Ellingsrud and Skjelbred [20], for groups G acting on polynomial rings by permutation of the indeterminates.

Another problem is that the *Grauert–Riemenschneider Vanishing Theorem* does not necessarily hold. To give an explicit example, let S be a smooth surface over a ground field k, and consider the symmetric product $\mathrm{Sym}^n(S) = (S \times \ldots \times S)/G$, where G is the symmetric group on n letters acting by permutation of the factors. The Hilbert–Chow morphisms gives a resolution of singularities

$$f : X = \mathrm{Hilb}^n(S) \longrightarrow \mathrm{Sym}^n(S) = Y,$$

which is a crepant resolution. If the characteristic p is positive with $p \leq n$, then $R^i f_*(\omega_{X/Y}) = R^i f_*(\mathcal{O}_X) \neq 0$, because otherwise the augments in [35], page 49–51 show that Y would be Cohen–Macaulay. But this is not the case by the work of Ellingsrud and Skjelbred.

In this paper we are mainly interested in *wild quotient singularities in dimension two*. Let R be an arbitrary local noetherian ring that is normal. To simplify, we also assume that the residue field is separably closed and R is complete. The latter ensures that there is a resolution of singularities $f : X \to \mathrm{Spec}(R)$ without further assumptions, according to Lipman [38]. Let $E \subset X$ be the exceptional divisor, viewed as a reduced closed subscheme, and $E_1, \ldots, E_r$ be its irreducible components. We shall consider the *intersection matrix* $(E_i \cdot E_j)_{1 \leq i,j \leq r}$ and the *dual graph*, which is the graph whose vertices corresponds to the irreducible components E_i. Two vertices are joined by an edge if $E_i \cap E_j \neq \emptyset$. Here we tacitly assume that E has simple normal crossings. It is well-known that dual graphs for quotient singularities $R = A^G$ in dimension two are necessarily *trees*, and that all irreducible components are $E_i \simeq \mathbb{P}^1$ (see [15], Theorem 1 or [39], Theorem 2.8).

Brieskorn [10] gave a complete classification of quotient singularities in characteristic zero, which builds on the ADE-classification of the rational double points. From this one sees that dual graphs of tame quotient singularities are always *star-shaped*, that is, contain at most one node. Absence of nodes means that the group G is abelian. Following Lorenzini, we call *nodes* the vertices of valency ≥ 3, that is, with at least three neighboring vertices.

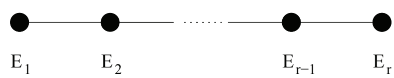
In the wild case, the dual graphs may become rather complicated. Shioda [49] and later Katsura [34] analyzed the Kummer surface $\{\pm 1\}\backslash A$ in characteristic 2, and observed certain minimally elliptic singularities. In [30], we studied quotients $G\backslash(C \times C')$, where the curves C, C' are Artin–Schreier curves of the form $y^q - y = f(x)$, where the right hand side is a polynomial of degree $q-1$. It turned out that the corresponding wild quotient singularity is star-shaped, with $q+1$ chains of length $q-1$ sprouting from the node. Moreover, the geometric genus of this wild quotient singularity grows at least quadratically in q. Here q denotes an arbitrary p-power. Among other things, Lorenzini [42] asks whether there are wild quotient singularities whose *dual graph has no node*, or some whose *dual graph has at least two nodes*, and whether the dual graphs occurring *over fields are the same as those occurring in mixed characteristics*.

2. Dual graphs without nodes. Let R be a complete local noetherian ring that is normal and 2-dimensional, and whose residue field $k = R/\mathfrak{m}_R$ is separably closed. Note that we do not assume that R contains a field. Let $f : X \to \mathrm{Spec}(R)$ be the minimal resolution of singularities, with exceptional divisor $E \subset X$. Let

$E_1, \ldots, E_r \subset E$ be the integral components, and $(E_i \cdot E_j)_{1 \leq i,j \leq r}$ be the intersection matrix, which is negative-definite. We say that R is a *Hirzebruch–Jung singularity* if all $E_i \simeq \mathbb{P}^1_k$, and for some suitable ordering of the irreducible components, the intersection matrix has the form

$$(E_i \cdot E_j)_{1 \leq i,j \leq r} = \begin{pmatrix} -s_1 & 1 & & & \\ 1 & -s_2 & 1 & & \\ & 1 & -s_3 & \ddots & \\ & & \ddots & \ddots & 1 \\ & & & 1 & -s_r \end{pmatrix} \tag{1}$$

for some integers $s_i \geq 2$. Whence the dual graph attached to the singularity is a chain:



We may assign a reduced fraction $m/b \in \mathbb{Q}_{>1}$ to the Hirzebruch–Jung singularity, defined by the continued fraction

$$\frac{m}{b} = s_1 - \cfrac{1}{s_2 - \cfrac{1}{\ddots - \cfrac{1}{s_r}}}. \tag{2}$$

Writing the exceptional curves in reverse order, one obtains the fraction m/b' where $0 < b' < m$ is the unique integer with $bb' \equiv 1$ modulo m. We say that R is a *Hirzebruch–Jung singularity of type m/b*. Note that R is also a Hirzebruch–Jung singularity of type m/b'. In the special case $b = m - 1$ we have $s_1 = \ldots = s_r = 2$ and $r = m - 1$. In other words, the Hirzebruch–Jung singularities of type $m/(m-1)$ are precisely the *rational double points* of type A_{m-1}. In the special case $r = 1$ we have $m = s_1$ and $b = 1$, and the Hirzebruch–Jung singularities of type $m/1$ are obtained by contracting a curve $E = E_i \simeq \mathbb{P}^1$ of self-intersection $-m$.

Recall that the *local fundamental group* $\pi_1^{\mathrm{loc}}(R)$ of a complete local noetherian domain R is the fundamental group of the open subscheme $\mathrm{Reg}(R) \subset \mathrm{Spec}(R)$, say with respect to a chosen separable closure of the field of fractions. If R is a normal and 2-dimensional, it is possible to compute the *maximal quotient* of $\pi_1^{\mathrm{loc}}(R)$ that is prime to the characteristic exponent of the residue field, in terms of the intersection matrix of the exceptional divisor, as explained by Cutkosky and Srinivasan [15], Theorem 3. Our first main result is a computation of the *full* local fundamental group:

THEOREM 2.1. *Let R be a Hirzebruch–Jung singularity of type m/b, and $p \geq 1$ the characteristic exponent of the residue field $k = R/\mathfrak{m}_R$. Then the local fundamental group $\pi_1^{\mathrm{loc}}(R)$ is isomorphic to the prime-to-p part of the cyclic group $\mathbb{Z}/m\mathbb{Z}$.*

Of course, this is well-known in the case that R contains a field of characteristic zero. For rational double points of type A_{m-1}, with R containing a field of characteristic $p > 0$, it was remarked by Artin (see [3], Section 2). The really new part in our result seems to be the case of mixed characteristics. The proof will stretch over the next two sections.

The theorem implies that the local fundamental group of a Hirzebruch–Jung singularity contains no elements of order p. Whence the following immediate consequence for wild quotient singularities, which answers a question of Lorenzini to the negative ([42], Question 1.1 (a)):

Corollary 2.2. *The dual graph attached to a wild quotient singularity in dimension two contains at least one node.*

To compute the local fundamental group of a Hirzebruch–Jung singularity, we shall use the following fact, which already appeared in a special form in [3], Corollary 1.2. We state it in a rather general way: Let $A \subset A' \subset A''$ be three complete local noetherian normal domains, with respective fields of fractions $K \subset K' \subset K''$. Assume that the extension $A \subset A'$ and $A' \subset A''$ are finite.

Proposition 2.3. *In the preceding situation, suppose the following:*
(i) *The local ring A has separably closed residue field.*
(ii) *The local ring A'' is regular.*
(iii) *The finite field extension $K \subset K'$ is Galois.*
(iv) *The ring extension $A \subset A'$ is étale in codimension one.*
(v) *The ring extension $A' \subset A''$ is totally ramified at some prime $\mathfrak{q} \subset A'$ of height one.*

Then there is a canonical identification $\pi_1^{\mathrm{loc}}(A) = \mathrm{Gal}(K'/K)$, where the former is taken with respect to some separable closure of K'.

Proof. This identification arises as follows: Let $Y \subset \mathrm{Spec}(A)$ be the regular locus, which is an open subscheme by Nagata's Theorem ([25], Theorem 6.12.7), and $Y' \subset \mathrm{Spec}(A')$ be its preimage. Consider the *Galois categories* $\mathcal{C}$ of all finite étale morphisms $\tilde{Y} \to Y$, and $\mathcal{C}'$ of all finite left $\mathrm{Gal}(K'/K)$-sets (compare [27], Exposé V). We have a functor

$$\Psi : \mathcal{C} \longrightarrow \mathcal{C}', \quad \tilde{Y} \longmapsto \tilde{Y}(K'),$$

where $\tilde{Y}(K')$ denotes the set of K'-rational points of the finite K-scheme $\tilde{Y}_K = \tilde{Y} \times_Y \mathrm{Spec}(K)$. The task now is to show that this functor is an equivalence of categories. Indeed, from this it follows that the set-valued functor that forgets the Galois action yields compatible fiber functors on $\mathcal{C}$ and $\mathcal{C}'$, such that $\pi_1^{\mathrm{loc}}(A)$ and $\mathrm{Gal}(K'/K)$, which by definition are the automorphism groups of these fiber functors, become equal.

It is easy to see that the functor Ψ is faithful: The restriction functor $\tilde{Y} \mapsto \tilde{Y}_K$ is faithful, because $\mathcal{O}_Y$ is torsion free, and the functor $\tilde{Y}_K \mapsto \tilde{Y}(K)$ is faithful by Galois descent.

We next check that Ψ is essentially surjective: Set $G = \mathrm{Gal}(K'/K)$. Since $A \subset A'$ is étale in codimension one and both rings are normal, the projection $Y' \to Y$ must be a G-torsor with respect to the canonical right G-action on Y', by the Zariski–Nagata Purity Theorem ([28], Exposé X, Theorem 3.4). For every subgroup $H \subset G$, the scheme $\tilde{Y} = Y'/H$ is étale over Y, with $\tilde{Y}(K') = G/H$. Using that every finite left G-set is isomorphic to a disjoint union of sets of the form G/H, we infer that Ψ is essentially surjective.

It remains to verify that Ψ is full. For this, it suffices to show that every finite étale $g : \tilde{Y} \to Y$ acquires a section over K', because then the scheme $\tilde{Y}_{K'}$ becomes the disjoint union of copies of $\mathrm{Spec}(K')$ indexed by the finite set $\tilde{Y}(K')$. The latter ensures that any two morphisms $h, h' : \tilde{Y} \to \tilde{Z}$ between finite étale Y-scheme that induce the same map on K'-rational points must be equal.

By We first extend the quasifinite morphism

$$\tilde{Y}'' = \tilde{Y} \times_Y \operatorname{Spec}(A'') \to \operatorname{Spec}(A'')$$

to a finite morphism $\operatorname{Spec}(\tilde{A}'') \to \operatorname{Spec}(A'')$ with $\tilde{A}''$ normal, using Zariski's Main Theorem [26], Corollary 18.12.13. Then $A'' \subset \tilde{A}''$ is étale in codimension one by construction. Since A'' is regular, the finite ring extension must be be étale everywhere, again by the Zariski–Nagata Purity Theorem. Since A'' is strictly henselian, the étale extension $A'' \subset \tilde{A}''$ admits a retraction, by [26], Proposition 18.8.1. Choosing such a retraction, we obtain a factorization $Y'' \to \tilde{Y}' \to Y'$, where $Y'' \subset \operatorname{Spec}(A'')$ is the preimage of Y, and $\tilde{Y}' = \tilde{Y} \times_Y Y'$. We conclude that $\widetilde{Y}' \to Y'$ is totally ramified on some connected component of $\tilde{Y}'$ over the point $y' \in Y'$ corresponding to $\mathfrak{q} \subset A'$. Being finite and étale, $\tilde{Y}' \to Y'$ must have a section, in particularly $\tilde{Y}(K') \neq \emptyset$. □

3. Local fundamental groups. Let R be a Hirzebruch–Jung singularity of type m/b, as in the preceding section, with residue field $k = R/\mathfrak{m}_R$. The goal of this section is to compute the local fundamental group $\pi_1^{\text{loc}}(R)$, and thus to prove Theorem 2.1.

Let $E = E_1 + \ldots + E_r$ be the reduced exceptional divisor on the minimal good resolution of singularities $f : X \to \operatorname{Spec}(R)$. Recall that the *fundamental cycle* $Z \subset X$ is the smallest exceptional divisor containing E with $(Z \cdot E_i) \leq 0$ for all $1 \leq i \leq r$.

PROPOSITION 3.1. *Our Hirzebruch–Jung singularity R has fundamental cycle $Z = E$, and is a rational singularity. Also, $E \subset X$ is the schematic closed fiber of the resolution $f : X \to \operatorname{Spec}(R)$.*

Proof. Since $(E \cdot E_i) \leq 2 - s_i \leq 0$ we must have $Z = E$. Clearly, $H^1(Z, \mathcal{O}_Z) = 0$. Whence the singularity is rational by Artin's Criterion [1], Theorem 3. The final statement is contained in loc. cit., Theorem 4. □

The main idea now is to use certain *log structures* on $\operatorname{Spec}(R)$, in the sense of Kato [32]. To this end, choose k-valued points $x \in E_1 \smallsetminus E_2$ and $x' \in E_r \smallsetminus E_{r-1}$. We may extend these points to effective Cartier divisors $D, D' \subset X$ with $D \cap E = \{x\}$ and $D' \cap E = \{x'\}$, because R is henselian (compare [26], Proposition 21.9.11). Their images

$$C = f(D) \quad \text{and} \quad C' = f(D')$$

are Weil divisors on $\operatorname{Spec}(R)$. Consider the submonoid

$$M = \{g \in R \mid \operatorname{Spec}(R/gR) \text{ is supported by } C \cup C'\}$$

inside the multiplicative monoid R. It comes with a homomorphism of monoids

$$\nu : M \longrightarrow \mathbb{N} \oplus \mathbb{N}, \quad g \longmapsto (\operatorname{val}_C(g), \operatorname{val}_{C'}(g)),$$

sending $g \in M$ to the values of the valuations corresponding to the generic points of C, C'. Let $P \subset \mathbb{N} \oplus \mathbb{N}$ be its image. Then we have a sequence of monoids

$$1 \longrightarrow R^\times \longrightarrow M \longrightarrow P \longrightarrow 0.$$

This sequence is exact, in the sense that the monoid P is the quotient of the monoid M by the congruence relation $\{(g, g') \mid g = ug' \text{ for some } u \in R^\times\}$.

We may describe P in terms of the intersection matrix as follows. Let Φ be the *discriminant group* of the intersection matrix $(E_i \cdot E_j)_{1\leq i,j\leq r}$, that is, the cokernel of the map $\mathbb{Z}^{\oplus r} \to \mathbb{Z}^{\oplus r}$ defined by the intersection matrix. Its structure is well-known:

PROPOSITION 3.2. *The discriminant group Φ is cyclic of order m.*

Proof. Recall that the reduced fraction m/b is defined as the continued fraction (2). Glancing at the intersection matrix (1), we see that it contains as submatrix an $(r-1)\times(r-1)$ identity matrix, so Φ must be cyclic. By induction on $r \geq 1$, one easily infers

$$m = (-1)^r \det(E_i \cdot E_j)_{1\leq i,j\leq r} \quad \text{and} \quad b = (-1)^{r-1} \det(E_i \cdot E_j)_{2\leq i,j\leq r},$$

whence Φ has order m. ∎

Consider the homomorphism of groups $\varphi : \mathbb{Z}\oplus\mathbb{Z} \to \Phi$ sending (n, n') to the class of the r-tuple $(n, 0, \ldots, 0, n')$.

PROPOSITION 3.3. *We have $P = \ker(\varphi) \cap (\mathbb{N}\oplus\mathbb{N})$ inside $\mathbb{Z}\oplus\mathbb{Z}$.*

Proof. Let $n, n' \geq 0$ be natural numbers. Suppose $(n, n') \in P$, such that $nC+n'C'$ is Cartier. Its preimage $nD + \sum \lambda_j E_j + n'D'$ is a Cartier divisor on X that is numerically trivial on E. Whence $(nD + n'D')\cdot E_i = -\sum \lambda_j E_j \cdot E_i$ for all $1 \leq i \leq r$, thus $\varphi(n, n') = 0$.

Conversely, if the tuple of intersection numbers $(n, 0, \ldots, 0, n')$ is of the form $(-\sum \lambda_j E_j \cdot E_i)_{1\leq i\leq r}$, then the invertible sheaf $\mathcal{L} = \mathcal{O}_X(nD + \sum \lambda_j E_j + n'D')$ is numerically trivial on E. It must be trivial on the formal neighborhood of E, since the singularity R is rational, thus $f_*(\mathcal{L})$ remains invertible. Hence this is also the reflexive sheaf of rank one attached to the Weil divisor $nC + n'C'$, therefore $(n, n') \in P$. ∎

This ensures that our monoid P has all sorts of good properties. Throughout, all monoids are assumed to be commutative. Recall that a monoid Q is called *fine* if it is finitely generated and integral. It is called *saturated* if it is integral, and the inclusion $Q \subset Q^{\mathrm{gp}}$ into its groupification has the property that whenever $a \in Q^{\mathrm{gp}}$ has a multiple in Q, then it is already contained in Q. A fine saturated monoid is called *fs*. A monoid Q is *sharp* if $Q^\times = \{1\}$. We refer to Kato's original article [32] or the in-depth manuscript of Ogus [46] for all standard fact on monoids.

COROLLARY 3.4. *The monoid P is sharp and fs, and the surjective homomorphism of monoids $M \to P$ has a section. Moreover, $(\mathbb{Z}\oplus\mathbb{Z})/P^{\mathrm{gp}}$ is a cyclic group of order m.*

Proof. By definition, $P = M/R^\times$ is sharp. In light of Proposition 3.3, the monoid P can be described as the set of integral solutions of finitely many inequalities with integral coefficients, and is thus fs (for example, [24], Proposition 8.5). It is easy to see that $P^{\mathrm{gp}} = \ker(\varphi)$, such that $(\mathbb{Z}\oplus\mathbb{Z})/P^{\mathrm{gp}} = \Phi$ is cyclic of order m. A section exists because the abelian group P^{gp} is free, thus admits only trivial extensions. ∎

This has a geometric interpretation in terms of toric varieties: Let F be an arbitrary ring. The inclusion $P^{\mathrm{gp}} \subset \mathbb{Z}\oplus\mathbb{Z}$ of free abelian groups of rank 2 corresponds to an isogeny $\operatorname{Spec} F[\mathbb{Z}\oplus\mathbb{Z}] \to \operatorname{Spec} F[P^{\mathrm{gp}}]$ between families of 2-dimensional tori over F. Its kernel is the diagonalizable groups scheme $H = \operatorname{Spec} F[N]$, which represents the functor on F-algebras $A \mapsto \operatorname{Hom}(N, A^\times)$, as explained in [16], Expose VIII. This isogeny extends to a toric morphism $\operatorname{Spec} F[\mathbb{N}\oplus\mathbb{N}] \to \operatorname{Spec} F[P]$ between families of affine toric surfaces over F. In fact, this toric morphism is the quotient morphisms for the canonical H-action on $\mathbb{A}^2_F = \operatorname{Spec} F[\mathbb{N} \oplus \mathbb{N}]$. Let us regard $\operatorname{Spec} F$ as the closed subscheme of $\operatorname{Spec} F[P]$ corresponding to the ideal $(P \smallsetminus P^\times) \subset F[P]$. The following seems to be well-known:

Proposition 3.5. *The quotient morphism* $\operatorname{Spec} F[\mathbb{N} \oplus \mathbb{N}] \to \operatorname{Spec} F[P]$ *is a* H*-torsor over the complement of* $\operatorname{Spec}(F) \subset \operatorname{Spec}(F[P])$.

Proof. It suffices to check this on geometric fibers, so we may assume that F is an algebraically closed field. The H-action commutes with the torus action, whence the torus orbits are H-invariant. It suffices to check that H acts freely on each of the the three non-closed torus orbits. This is clear for the dense torus orbit. For the remaining two non-closed torus orbits, it suffices to check that the subgroups $\mathbb{Z} \times 0$ and $0 \times \mathbb{Z}$ surject onto N under the projection $\mathbb{Z}^2 \to N$. This is independent of the ground field F, so it suffices to treat the case $F = \mathbb{C}$. Then the statement follows from the theory of complex toric surface singularities: According to [6], Theorem 5.1, all complex Hirzebruch–Jung singularities of type m/b are formally isomorphic, and in particular isomorphic to the toric surface singularity coming from the convex rational polyhedral cone $\mathbb{R}_{\geq 0}(1,0) + \mathbb{R}_{\geq 0}(m, -b) \subset \mathbb{R}^2$, see [13], Theorem 10.2.3. It then follows from loc. cit., Proposition 10.1.2 that the H-action on $\operatorname{Spec} \mathbb{C}[\mathbb{N} \oplus \mathbb{N}]$ is free outside the origin. $\square$

To proceed, choose a section of $M \to P$, and write $M = R^\times \oplus P$. In this way, we regard P as a submonoid of R, and revert to multiplicative notation. Now recall that every monoid Q has a unique maximal ideal, namely the complement of the units $Q \smallsetminus Q^\times$. For sharp monoids, this is just $Q \smallsetminus \{1\}$. We come to a key observation:

Lemma 3.6. *For every choosen section of* $M \to P$*, the maximal ideal* $P \smallsetminus P^\times$ *of the monoid generates the maximal ideal* $\mathfrak{m}_R \subset R$ *of the ring.*

The proof is elementary but somewhat lengthy, so we defer it into the next section. To proceed, we have to distinguish two cases: If R contains a field, $W \subset R$ denotes a *field of representatives*, that is, a subfield so that the projection $W \to R/\mathfrak{m}_R$ is bijective. If R does not contain a field, choose a *Cohen subring* $W \subset R$. In our situation, this is a complete discrete valuation ring so that $p \in W$ is a uniformizer, and $W/pW \to R/\mathfrak{m}_R$ is bijective (compare [8], Chapter IX, §2-3).

In any case, Lemma 3.6 ensures that the map

$$W[[P]] \longrightarrow R$$

is surjective. Note that this map is defined with the help of the choosen section of $M \to P$. Here $W[[P]]$ is the ring of formal power sequences $\sum_{g \in P} w_g g$ with coefficients $w_g \in W$. The ring structure comes from the interpretation $W[[P]] = \varprojlim W[P]/I^n W[P]$ as I-adic completion of the monoid ring, where $I \subset W[P]$ is the ideal generated by $P \smallsetminus P^\times$. In Kato's terminology [33], Definition 2.1 the *log structure* on $\operatorname{Spec}(R)$ attached to $P \to R$ is *log regular*. Here, this means that the residue class ring $\bar{R} = R/(P \smallsetminus P^\times)$ is regular, which is a consequence of Lemma 3.6, and

$$\dim(R) = \dim(\bar{R}) + \operatorname{rank}_{\mathbb{Z}}(P^{\mathrm{gp}}),$$

which holds because the numbers are $2 = 0+2$. We refrain from recalling more details, since the full strength of Kato's theory is not needed, but stress again that his ideas play a paramount role throughout. From loc. cit., Theorem 3.1 and Theorem 3.2, it follows:

Proposition 3.7. *The kernel of the surjection $W[[P]] \to R$ is generated by a formal power series of the form*

$$\psi = \begin{cases} p + \sum_{g \in P \smallsetminus P^\times} w_g g & \text{if } R \text{ does not contain a field;} \\ 0 & \text{if } R \text{ contains a field.} \end{cases}$$

In particular, the map $W[[P]] \to R$ is bijective if the ring R contains a field.

Consider the commutative diagram of monoids and groups

$$\begin{tikzcd} P \arrow[r] \arrow[d] & Q \arrow[r] \arrow[d] & \mathbb{N} \oplus \mathbb{N} \arrow[d] \\ P^{\mathrm{gp}} \arrow[r] & Q^{\mathrm{gp}} \arrow[r] & \mathbb{Z} \oplus \mathbb{Z} \end{tikzcd}$$

Here $P^{\mathrm{gp}} \subset Q^{\mathrm{gp}} \subset \mathbb{Z} \oplus \mathbb{Z}$ is the unique intermediate group whose index $[\mathbb{Z} \oplus \mathbb{Z} : Q^{\mathrm{gp}}]$ is a p-power, and that the other index $[Q^{\mathrm{gp}} : P^{\mathrm{gp}}]$ is prime to p. Recall once more that $p \geq 1$ denotes the characteristic exponent of the residue field $R/\mathfrak{m}_R$. The monoid Q is defined by demanding that the square on the right is cartesian. This Q is sharp and fs, compare the arguments for Corollary 3.4. We now define rings

$$R' := R \otimes_{W[[P]]} W[[Q]] = W[[Q]]/(\psi),$$
$$R'' := R \otimes_{W[[P]]} W[[\mathbb{N} \oplus \mathbb{N}]] = W[[\mathbb{N} \oplus \mathbb{N}]]/(\psi).$$

This gives finite extensions $R \subset R' \subset R''$ between complete local noetherian rings.

Proposition 3.8. *Both rings R', R'' are integral domains. The ring R' is normal, the ring R'' is regular, the ring extension $R \subset R'$ is étale in codimension one, and the ring extension $R' \subset R''$ is totally ramified at some prime $\mathfrak{q} \subset R'$ of height one.*

Proof. The rings in question are integral by [33], Lemma 3.4. Endowed with their canonical log structures, they become log regular, whence are normal, according to loc. cit., Theorem 3.1 and Theorem 4.1. Obviously, $W[[\mathbb{N} \oplus \mathbb{N}]]$ is regular. Its residue class ring R'' must be regular as well, in light of the description in Proposition 3.7.

Set

$$Y = \operatorname{Spec}(W[[P]]) \quad \text{and} \quad Y' = \operatorname{Spec}(W[[Q]]) \quad \text{and} \quad Y'' = \operatorname{Spec} W[[\mathbb{N} \oplus \mathbb{N}]],$$

and consider the ensuing morphisms $Y'' \to Y' \to Y$. The ring $W[[\mathbb{N} \oplus \mathbb{N}]]$ is endowed with a natural grading by the finite cyclic group $N = (\mathbb{Z} \oplus \mathbb{Z})/P^{\mathrm{gp}}$: The formal power series $\sum w_g g$, with $g \equiv d$ modulo P^{gp} are the homogeneous elements of degree $[d] \in N$. In turn, we get an action of the finite flat diagonalizable group scheme $H = \operatorname{Spec} W[N]$ on Y'' with quotient $Y = Y''/H$, as explained in [16], Expose VIII. According to Proposition 3.5, the quotient morphism $Y'' \to Y$ is a H-torsor over the complement of the closed subscheme $\operatorname{Spec}(W) \subset \operatorname{Spec}(W[[P]])$ defined by the ideal $(P \smallsetminus P^{\mathrm{gp}}) \subset W[[P]]$.

Now consider the finite flat subgroup scheme $H' \subset H$ corresponding to the finite cyclic group $N' = (\mathbb{Z} \oplus \mathbb{Z})/Q^{\mathrm{gp}}$, such that $Y' = Y''/H'$. Restricted to the residue field $W/\mathfrak{m}_W$, the group scheme $H' = \operatorname{Spec} W[N']$ becomes radical, because this residue field has characteristic exponent p and the group N has order a power of p. We conclude that $R' \subset R''$ must be totally ramified along some prime of height one. Note that this holds for trivial reasons if R contains a field of characteristic zero, for then $R' = R''$.

Finally, consider the finite flat quotient group scheme $G = H/H'$ corresponding to the finite cyclic group $M = Q^{\mathrm{gp}}/P^{\mathrm{gp}}$, such that $Y = Y'/G$. The group scheme G is étale, because the order of M is prime to the characteristic exponent of the residue field $W/\mathfrak{m}_W$. Using Proposition 3.5 again, we easily deduce that the quotient morphism $Y' \to Y$ is a G-torsor over the complement of $\operatorname{Spec}(W) \subset \operatorname{Spec} W[[P]]$ defined by the ideal $(P \smallsetminus P^{\mathrm{gp}}) \subset W[[P]]$. From the description of the closed subscheme $\operatorname{Spec}(R) \subset \operatorname{Spec} W[[P]]$ in Proposition 3.7, we infer that $R \subset R'$ must be a G-torsor in codimension one, and in particular is étale in codimension one. ☐

Let $R \subset K$ and $R' \subset K'$ be the field of fractions.

PROPOSITION 3.9. *The finite field extension $K \subset K'$ is cyclic, and* $\operatorname{Gal}(K'/K)$ *is isomorphic to the prime-to-p part of $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Let $\mathbb{Z}/m'\mathbb{Z}$ be the prime-to-p part of $\mathbb{Z}/m\mathbb{Z}$. This group is isomorphic to $M = Q^{\mathrm{gp}}/P^{\mathrm{gp}}$, by definition of Q^{gp}. Since m' is invertible in W and the residue field $W/\mathfrak{m}_W$ is separably closed, the group scheme G representing $A \mapsto \operatorname{Hom}(M, A^\times)$ comes from the abstract group $\mathbb{Z}/m'\mathbb{Z}$. We say in the proof of the previous proposition that $\operatorname{Spec}(K') \to \operatorname{Spec}(K)$ is a G-torsor, in other words, $K \subset K'$ is Galois, with Galois group $\operatorname{Gal}(K'/K) \simeq \mathbb{Z}/m'\mathbb{Z}$. ☐

Proof of Theorem 2.1. Using Proposition 2.3, together with Proposition 3.8 and 3.9, we find that $\pi_1^{\mathrm{loc}}(R) = \operatorname{Gal}(K'/K)$ is isomorphic to the prime-to-p part of $\mathbb{Z}/m\mathbb{Z}$, where R is a Hirzebruch–Jung singularity of type m/b. ☐

4. Cotangent spaces. The goal of this section is to prove Lemma 3.6, which says that the maximal ideal of Hirzebruch–Jung singularities is generated by the nonunits of certain monoids.

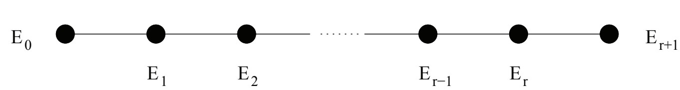
We start with some preparatory considerations. Let k be a field, and E be a proper reduced curve over k whose irreducible components $E_1, \ldots, E_r$ are isomorphic to $\mathbb{P}^1_k$, with

$$h^0(\mathcal{O}_{E_i \cap E_j}) = \dim_k H^0(\mathcal{O}_{E_i \cap E_j}) = \begin{cases} 1 & \text{if } |i-j| = 1; \\ 0 & \text{if } |i-j| \geq 2. \end{cases}$$

To rule out triple intersections, we furthermore demand that each point $x \in E$ lies in at most two irreducible components. We also consider noetherian reduced 1-dimensional schemes having the form

$$\tilde{E} = E \cup D \cup D',$$

where D, D' are the spectra of certain discrete valuation rings, not necessarily containing k, so that $h^0(\mathcal{O}_{E_i \cap D}) = \delta_{i,0}$ and $h^0(\mathcal{O}_{E_i \cap D'}) = \delta_{i,r}$ (Kronecker delta). As we saw in the preceding section, such curves occur on the resolution of singularities for Hirzebruch–Jung singularities. To make formulas more elegant, we also write $E_0 = D$ and $E_{r+1} = D'$. Thus the dual graph of $\tilde{E}$ is:



Now let $\mathcal{L}$ be an invertible sheaf on E with intersection numbers

$$d_i = (\mathcal{L} \cdot E_i) = \begin{cases} \geq 0 & \text{if } i = 1 \text{ or } i = r; \\ \geq 1 & \text{if } 2 \leq i \leq r-1. \end{cases}$$

Here the intersection numbers are defined as $(\mathcal{L} \cdot E_i) = \chi(\mathcal{L}_{E_i}) - \chi(\mathcal{O}_{E_i})$ via k-vector space dimensions. For the proof of Lemma 3.6, it will be useful to have a specific basis for the finite dimensional k-vector space $H^0(E, \mathcal{L})$ adapted to our problem. The dimension is easy:

PROPOSITION 4.1. *We have* $h^0(\mathcal{L}) = 1 + \sum_{i=1}^r d_i$.

Proof. The dualizing sheaf ω_E is invertible, since E is locally of complete intersection (by [26], Corollary 19.3.4, it suffices to check this over the algebraic closure of k, where it is well-known), and has intersection numbers

$$(\omega_E \cdot E_i) = \begin{cases} -1 & \text{if } i = 1 \text{ or } i = r; \\ 0 & \text{if } 2 \leq i \leq r-1. \end{cases}$$

Thus $(\mathcal{L}^\vee \otimes \omega_E \cdot E_i) < 0$. By Serre duality, $H^0(E, \mathcal{L}^\vee \otimes \omega_E) \simeq H^1(E, \mathcal{L})$, and the latter vanishes since E is reduced. Whence

$$h^0(\mathcal{L}) = \chi(\mathcal{L}) = \deg(\mathcal{L}) + \chi(\mathcal{O}_E) = (\sum_{i=1}^r d_i) + 1$$

from Riemann–Roch. $\square$

We now define k-rational points

$$a_i, b_i \in E_i, \qquad 1 \leq i \leq r$$

by the condition $E_i \cap E_{i-1} = \{a_i\}$ and $E_i \cap E_{i+1} = \{b_i\}$. Note that we have $a_i = b_{i+1}$ as points in $E = E_1 \cup \ldots \cup E_r$. We also set $b_0 = a_1$ and $a_{r+1} = b_r$, and call the rational points

$$a_1 = b_0, \quad a_2 = b_1, \quad \ldots \quad a_{r+1} = b_r \in E$$

the *special points* of the curve E. These are precisely the singular points on the extended curve $\tilde{E}$. Using these special points, one obtains an exact sequence

$$0 \longrightarrow H^0(E, \mathcal{L}) \longrightarrow \bigoplus H^0(E_i, \mathcal{L}|_{E_i}) \longrightarrow \bigoplus_{i=1}^{r-1} \frac{\kappa(b_i) \oplus \kappa(a_{i+1})}{k}, \tag{3}$$

where the map on the left is the sum of the restriction maps, the quotients on the right are with respect to the diagonal inclusions of the ground field in the residue fields, and the map on the right is induced from the evaluation map

$$(f_1, \ldots, f_r) \longmapsto (f_1(b_1), f_2(a_2), f_2(b_2), f_3(a_3), \ldots, f_{r-1}(b_{r-1}), f_r(a_r)).$$

Here $f_i \in H^0(E_i, \mathcal{L}|_{E_i})$. Now for each $1 \leq i \leq r$, choose $d_i - 1$ sections

$$s_{ij} \in H^0(E_i, \mathcal{L}|_{E_i}), \qquad 1 \leq j \leq d_i - 1$$

so that s_{ij} vanishes at the special point $a_i \in E_i$ of order j, and at the special point $b_i \in E_i$ of order $d_i - j$. For example, if one writes $E_i = \operatorname{Proj} k[T_0, T_1]$ as a homogeneous spectrum and identifies $\mathcal{L}|_{E_i}$ with $\mathcal{O}_{\mathbb{P}^1}(d_i)$, then one may choose $s_{ij} = T_0^j T_1^{d_i - j}$. Using the exact sequence (3), we may regard these sections over E_i also as global sections $s_{ij} \in H^0(E, \mathcal{L})$, because the s_{ij} vanish at all special points.

PROPOSITION 4.2. *The* $\sum_{i=1}^r (d_i - 1)$ *sections*

$$s_{ij} \in H^0(E, \mathcal{L}), \quad 1 \le i \le r, \quad 1 \le j \le d_i - 1$$

form a basis for the vector subspace $V \subset H^0(E, \mathcal{L})$ *of all sections vanishing at the special points.*

Proof. Using that the locus on nonvanishing $E_{s_{ij}} = E_i \smallsetminus \{a_i, b_i\}$ are pairwise disjoint for $1 \le i \le r$, and that the $s_{ij} \in H^0(E_i, \mathcal{L}|_{E_i})$ are linearly independent for $1 \le j \le d_i - 1$, one infers that the $s_{ij} \in H^0(E, \mathcal{L})$ are linearly independent. On the other hand, we have an inclusion

$$V \subset \bigoplus H^0(E_i, \mathcal{L}|_{E_i}(-a_i - b_i)),$$

and the right hand side is a vector space of dimension $\sum_{i=1}^r (d_i - 1)$. If follows that the $s_{ij} \in V$ form a basis. $\square$

Next, suppose we have sections

$$t_i \in H^0(E, \mathcal{L}), \quad 1 \le i \le r + 1$$

with $t_i(a_i) \neq 0$ in the residue field $\kappa(a_i)$, and $t_i|_{E_n} = 0$ as elements of $H^0(E_i, \mathcal{L}|_{E_i})$ for all indices $n \neq i, i - 1$. This will give us the desired basis:

PROPOSITION 4.3. *Assumptions as above. The set*

$$\{s_{ij} \mid 1 \le i \le r, 1 \le j \le d_i - 1\} \quad \cup \quad \{t_i \mid 1 \le i \le r + 1\}$$

comprise a basis for the k*-vector space* $H^0(E, \mathcal{L})$.

Proof. The set has cardinality $\sum_{i=1}^r (d_i - 1) + (r + 1) = h^0(\mathcal{L})$, so it suffices to check that the sections form a generating system. Let $s \in H^0(E, \mathcal{L})$ be arbitrary. Subtracting a suitable linear combination of the t_i, we may assume that s vanishes at the special points. Then our s becomes a linear combination of the s_{ij} by Proposition 4.2. $\square$

Now let R be a Hirzebruch–Jung singularity, with minimal resolution of singularities $f : X \to \operatorname{Spec}(R)$. The reduced exceptional divisor $E \subset X$ is a proper reduced curve over the residue field $k = R/\mathfrak{m}_R$ as studied above. In the preceding section, we have chosen two integral Cartier divisors $D, D' \subset X$, which give us the 1-dimensional scheme $\tilde{E} = E \cup D \cup D'$, and whose images are integral Weil divisors $C, C' \subset \operatorname{Spec}(R)$. From this, we have constructed a sharp fs submonoid $P \subset R$. Our task now is to prove Lemma 3.6, that is $P \smallsetminus P^\times$ generates the maximal ideal $\mathfrak{m}_R$.

To do so we recall Artin's description of the cotangent space $\mathfrak{m}_R/\mathfrak{m}_R^2$ in term of the fundamental cycle $Z \subset X$ of a rational singularity in dimension two. The definition of the fundamental cycle ensures that the ideal $\mathfrak{m}_R \mathcal{O}_X \subset \mathcal{O}_X$ is contained in the ideal $\mathcal{O}_X(-Z) \subset \mathcal{O}_X$. Using the short exact sequence

$$0 \to \mathcal{O}_X(-2Z) \to \mathcal{O}_X(-Z) \to \mathcal{O}_Z(-Z) \to 0,$$

one obtains a map

$$\mathfrak{m}_R/\mathfrak{m}_R^2 \longrightarrow H^0(Z, \mathcal{O}_Z(-Z)).$$

It follows from [1], Theorem 4 that this map is bijective. In our Hirzebruch–Jung situation, the fundamental cycle is $Z = E$. Setting $\mathcal{L} = \mathcal{O}_E(-E)$, we have degrees

$$d_i = (\mathcal{L} \cdot E_i) = \begin{cases} s_i - 2 & \text{for } 2 \leq i \leq r-1; \\ s_i - 1 & \text{for } i = 1 \text{ or } i = r, \end{cases}$$

with the numbers $s_i = -E_i^2 \geq 2$. Now consider an effective divisor $A = \sum_{n=0}^{r+1} \lambda_n E_n$ that is numerically trivial on E. The latter is equivalent to the system of equations

$$s_n \lambda_n = \lambda_{n-1} + \lambda_{n+1}, \quad 1 \leq n \leq r. \tag{4}$$

In particular, we have the mean value estimates

$$\lambda_n \leq \frac{\lambda_{n-1} + \lambda_{n+1}}{2}, \quad 1 \leq n \leq r. \tag{5}$$

Since R is rational, the ideal of the closed subscheme $A \subset X$ is of the form $\mathcal{O}_X(-A) = g\mathcal{O}_X$ for some $g \in \mathfrak{m}_R$, which is unique up to $R^\times$, and in turn gives a global section $\bar{g} \in H^0(E, \mathcal{L})$, the latter being unique up to $k^\times$. Now recall the construction of our basis $s_{ij}, t_i \in H^0(E, \mathcal{L})$ from Proposition 4.3.

Proposition 4.4. *Notation as above. Suppose for some $1 \leq i \leq r$, we have $\lambda_i = 1$ and $\lambda_n \geq 2$ for $n = 1, \ldots, i-1$ and $n = i+1, \ldots, r$. Then $\bar{g} \in H^0(E, \mathcal{L})$ is a nonzero multiple of s_{ij}, with $j = \lambda_{i-1} - 1$.*

Proof. It is clear that $\bar{g}$ vanishes on each E_n, $n \neq i$, but does not vanish on $E_i \smallsetminus \{a_i, b_i\}$. It thus suffices to check that $\bar{g}$ vanishes of order j at $a_i \in E_i$. This is a local problem: Set $x = a_i$, and let $u, v \in \mathcal{O}_{X,x}$ be a system of parameters whose zero locus is E_{i-1}, E_i, respectively. Up to units, we have $g = u^j \cdot uv$. Under the canonical surjection $\mathcal{O}_X(-E) \to \mathcal{O}_{E_i}(-E)$, the element g becomes the class of u^j in $\mathcal{O}_{X,x}/(v) = \mathcal{O}_{E_i,x}$. $\square$

In the same way, one checks:

Proposition 4.5. *Notation as above. Suppose for some index $1 \leq i \leq r+1$ we have $\lambda_{i-1} = \lambda_i = 1$ and $\lambda_n \geq 2$ for $n = 1, \ldots, i-1$ and $n = i+1, \ldots, r$. Then $\bar{g} \in H^0(E, \mathcal{L})$ is a nonzero multiple of t_i.*

We come to the final goal of this section:

Proof of Lemma 3.6. By the Nakayama Lemma, it suffices to check that the image of $P \smallsetminus P^\times$ generates the vector space $\mathfrak{m}_R/\mathfrak{m}_R^2 = H^0(E, \mathcal{L})$, for the invertible sheaf $\mathcal{L} = \mathcal{O}_E(-E)$.

Fix a basis element $s_{ij} \in H^0(E, \mathcal{L})$, for some $1 \leq i \leq r$ and $1 \leq j \leq d_i - 1$. We define an effective Cartier divisor $A = \sum_{i=0}^{r+1} \lambda_i E_i$ as follows: First set

$$\lambda_i = 1 \quad \text{and} \quad \lambda_{i-1} = j + 1 \quad \text{and} \quad \lambda_{i+1} = s_i - 1 - j,$$

and then define the preceding multiplicities $\lambda_{i-2}, \ldots, \lambda_0$ by descending induction through the equations (4), and similarly for the subsequent $\lambda_{i+2}, \ldots, \lambda_{r+1}$. The mean value estimates (5) ensure that the sequence of integers $\lambda_0, \ldots, \lambda_{r+1}$ is strictly decreasing until its minimum $\lambda_i = 1$, after which it becomes strictly increasing. By construction, the effective Cartier divisor $A = \sum_{i=0}^{r+1} \lambda_i E_i$ is numerically trivial on E and has multiplicities ≥ 1, thus yields an element $g \in P \smallsetminus P^\times \subset \mathfrak{m}_R$. In light of Proposition 4.4, the induced section $\bar{g} \in H^0(E, \mathcal{L})$ is a nonzero scalar multiple of s_{ij}.

Now fix a basis element $t_i \in H^0(E, \mathcal{L})$. Then we define an effective Cartier divisor $A = \sum_{i=0}^{r+1} \lambda_i E_i$ in a similar way: First set

$$\lambda_{i-1} = \lambda_i = 1 \quad \text{and} \quad \lambda_{i-2} = s_{i-1} - 1 \quad \text{and} \quad \lambda_{i+1} = s_i - 1,$$

and define the remaining multiplicities as in the preceding paragraph. We infer with Proposition 4.5 that $\bar{g}$ is a nonzero scalar multiple of t_i.

Proposition 4.3 tells us that the image of $P \smallsetminus P^\times \to H^0(E, \mathcal{L})$ contains a basis. Thus $P \smallsetminus P^\times$ generates the maximal ideal $\mathfrak{m}_R$. □

5. Hermitian curves and special p-groups. In the remaining sections, we investigate certain curves with very large automorphism groups, in order to produce new examples of wild quotient surface singularities whose dual graph contains at least two nodes.

Let $p > 0$ be a prime number, k an algebraically closed ground field of characteristic p, and $q = p^m$ be a fixed prime power. Consider the smooth projective curve given by the affine equation

$$C : \quad y^q - y = x^{q+1},$$

which has genus $g = q(q-1)/2$. These are the so-called *Hermitian curves*, and are known for extremal behavior with respect to automorphisms and rational points, compare [52], [47]. Shioda kindly informed us that this curve is isomorphic to the Fermat curve of degree $q+1$, which are discussed in [50], an isomorphism being defined over the field $\mathbb{F}_{q^2}$. We prefer, however, to work with the equation for the Hermitian curve.

The substitution $x = x' + r$ and $y = y' + sx' + t$ transforms the equation into

$$y'^q - y' = x'^{q+1} + (r - s^p)x'^q + (r^q + s)x' + (r^{q+1} - t^q + t).$$

Such a substitution leaves the original equation of the Hermitian curve invariant if and only if $r - s^q = 0$, $r^q + s = 0$, $r^{q+1} - t^q + t = 0$, which is equivalent to

$$r^{q^2} + r = 0 \quad \text{and} \quad t^q - t = r^{q+1} \quad \text{and} \quad s = -r^q.$$

Summing up, we may regard the set

$$G = \left\{ (t, r) \in k^2 \mid r^{q^2} + r = 0 \text{ and } t^q - t = r^{q+1} \right\}$$

as a group of automorphisms, where the elements act via

$$(t, r) : \quad x \longmapsto x + r \qquad y \longmapsto y - r^q x + t. \tag{6}$$

The group law, viewed as composition of functions, is

$$(t, r) \circ (t', r') = (t + t' - rr'^q, r + r').$$

However, we endow the set G with the opposite group law

$$(t,r)\cdot(t',r') = (t+t'-r^q r', r+r')$$

since we want to regard G as a group of automorphisms of the scheme C rather than its coordinate ring.

PROPOSITION 5.1. *The group G has order* $\mathrm{ord}(G) = q^3$. *It is a Sylow-p-subgroup of* $\mathrm{Aut}(C)$ *when* $q \neq 2$.

Proof. Polynomials over k of the form $T^{q^2}+T$ or $T^q - T - \lambda$ are separable, so the statement about the order follows. For $q \neq 2$, the full automorphism group $\mathrm{Aut}(C)$ has order $q^3(q^3+1)(q^2-1)$, according to [52], Hauptsatz. □

Note that for $q = 2$, the curve C is the supersingular elliptic curve in characteristic two, and then the group of automorphisms fixing the origin has order 24. So G is a Sylow-p-subgroup as well.

Recall that the *Frattini subgroup* of a group is the intersection of all maximal proper subgroups. For our given group G, we denote by $\Phi, G', Z \subset G$ the Frattini subgroup, the commutator subgroup, and the center, respectively.

PROPOSITION 5.2. *In our group G, Frattini subgroup, commutator subgroup and center coincide: $\Phi = G' = Z$. This subgroup is given by $\{(t,0) \mid t \in \mathbb{F}_q\} \subset G$.*

Proof. A direct computations shows that the centralizer of an element $(t,r) \in G$ with $r \neq 0$ consists of those (t',r') with $r' = \lambda r$ for some $\lambda \in \mathbb{F}_q$. It follows that $Z = \{(t,0) \mid t \in \mathbb{F}_q\}$, and this is obviously the kernel of the homomorphism

$$G \longrightarrow k, \quad (t,r) \longmapsto r.$$

The inclusion $G' \subset \Phi$ holds for arbitrary finite p-groups, because then the Frattini subgroup is generated by the commutators and p-powers (see [43], Theorem 9.26). Thus G/Φ is the largest elementary abelian quotient, and we conclude $\Phi \subset Z$.

It remains to check that each central element $(t,0)$ is a commutator. Indeed, inverses and commutators are given by the respective formulas

$$(t,r)^{-1} = (-r^{q+1}-t, -r) \quad \text{and} \quad [(t,r),(t',r')] = (r^q r' - r r'^q, 0). \tag{7}$$

Now observe that the formula for commutators is $\mathbb{F}_q$-linear in r and r' with respect to the $\mathbb{F}_q$-vector space structures. Since there is at least one nontrivial commutator, each element $(t,0)$ is automatically a commutator. □

In other words, our group G is a *special p-group*, which by definition means that $\Phi = G' = Z$. These groups play a role in the classification of finite simple groups. It follows from the definition that abelianization $G^{\mathrm{ab}} = G/G'$ is elementary abelian, and the same holds for the center $Z \subset G$, see [4], (23.7). Moreover, the pairing

$$G^{\mathrm{ab}} \times G^{\mathrm{ab}} \longrightarrow Z, \quad (\bar{a},\bar{b}) \longmapsto [a,b] = aba^{-1}b^{-1}$$

is nondegenerate and alternating.

In the extremal case where $\Phi = G' = Z$ is cyclic, hence of order p, the group G is called *extraspecial*; then the pairing is a symplectic form, and one has $\mathrm{ord}(G) = p^{1+2n}$ for some $n \geq 0$. There is a classification of extraspecial p-groups: For each order, there are precisely two isomorphism classes, compare [17], Chapter B, §9. For odd

p, they are distinguished by the exponent of the group. The situation is somewhat more complicated for $p = 2$: The two extraspecial 2-groups of order eight are the dihedral group $D_4 = C_4 \rtimes \{\pm 1\}$ and the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. In our situation, we have:

PROPOSITION 5.3. *Our special p-group $G \subset \mathrm{Aut}(C)$ has exponent*

$$\exp(G) = \begin{cases} p & \text{if } p \neq 2; \\ p^2 & \text{if } p = 2. \end{cases}$$

Moreover, for $p = 2$ all noncentral elements in G have order four.

Proof. Since Z and G^{ab} are elementary abelian, the exponent divides p^2. One easily computes that p-th powers are given by $(t, r)^p = (\sum_{i=1}^{p-1} i r^{p+1}, 0)$. The first entry is $\sum_{i=1}^{p-1} i r^{p+1} = r^{p+1} \cdot p(p-1)/2$, and the result follows. □

6. Quotient singularities with two nodes. Fix a prime $p > 0$ and let $q = p^m$ be a prime power. Let $C: \ y^q - y = x^{q+1}$ be the Hermitian curve and G be the special p-group of order $\mathrm{ord}(G) = q^3$ acting on C, as described in the previous section. The G-action is free on the affine part of C, and the point $\infty \in C$ at infinity is fixed. We now consider the diagonal action of G on the smooth proper surface $C \times C$. Form the quotient surface

$$Y = G \backslash (C \times C).$$

This is a normal proper surface, whose singular locus is the point $y \in Y$ corresponding to the fixed point $(\infty, \infty) \in C \times C$. Our second main result is a statement on the dual graph of this wild quotient singularity, which gives a partial answer to Lorenzinis Question 1.1 b) in [42]:

THEOREM 6.1. *The dual graph for the minimal resolution of the wild quotient singularity $y \in Y = G\backslash(C \times C)$ contains at least two nodes.*

Note that we have no explicit description of this wild quotient singularity in terms of formal equations, nor do we know the precise number of nodes or the exact shape of the dual graph. We shall deduce the theorem by comparing with another singularity that can be handled. To this end we consider the fibration

$$\varphi : Y = G\backslash(C \times C) \longrightarrow G\backslash C = \mathbb{P}^1$$

induced from the projection onto the first factor. This fibration admits a section, given by $\{\infty\} \times C$. Now consider the commutative diagram

$$\begin{tikzcd}
 & \tilde{Y} \arrow[dl] \arrow[dr] & & \\
S \arrow[dr, "\psi"'] & & Y = G\backslash(C \times C) \arrow[dl, "\varphi"] & C \times C \arrow[l] \arrow[d, "\mathrm{pr}_1"] \\
 & \mathbb{P}^1 = G\backslash C & & C, \arrow[ll]
\end{tikzcd}$$

where $\tilde{Y} \to Y$ is the minimal resolution of singularities, and $\psi : S \to \mathbb{P}^1$ is the relative minimal model, that is, the model obtained by successively contracting (-1)-curves in the singular fiber of $\tilde{Y} \to \mathbb{P}^1$. By abuse of notation, we write $\infty \in \mathbb{P}^1$ for the point corresponding to the fixed point $\infty \in C$, such that $\psi^{-1}(\infty) \subset S$ is the singular fiber.

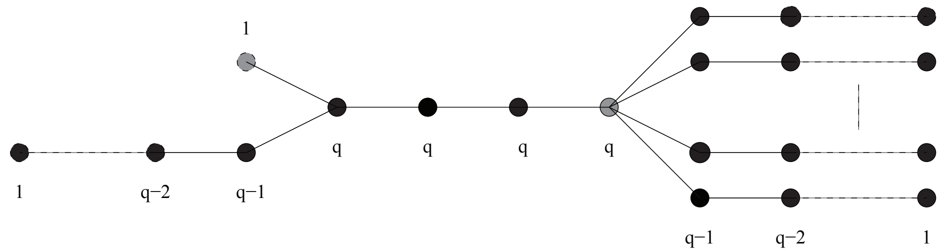


FIG. 1. *Dual graph of $\psi^{-1}(\infty)$ with multiplicities.*

PROPOSITION 6.2. *The reduced singular fiber $\psi^{-1}(\infty)_{\mathrm{red}} \subset S$ is a divisor with strictly normal crossings whose irreducible components are copies of $\mathbb{P}^1$, and its dual graph is depicted in Figure 1. There are q strings on the right hand side, each of length $q-1$. The numbers indicate multiplicities of integral components in the schematic fiber $\psi^{-1}(\infty)$. Integral components corresponding to the black vertices have self-intersection -2, whereas the other two have self-intersection number $-q$.*

For this we proceed in two steps: First, we determine an explicit equation for the generic fiber $\psi^{-1}(\eta)$, where $\eta \in \mathbb{P}^1 = G\backslash C$ denotes the generic point. Second, we use this equation to find an explicit resolution for the ensuing singularities, which finally will produces the dual graph $\psi^{-1}(\infty)$. The arguments will occupy the next two sections.

Proof that Proposition 6.2 implies Theorem 6.1. Consider the induced fibration $\tilde{Y} \to \mathbb{P}^1$. Its reduced singular fiber consists of two parts: On the one hand, the strict transform $F \subset \tilde{Y}$ of the singular fiber of $\varphi : Y \to \mathbb{P}^1$. On the other hand, the exceptional divisor $E \subset \tilde{Y}$ coming from the resolution of singularities.

The multiplicity of the integral component F in the schematic fiber is $q^3 = \mathrm{ord}(G)$, compare [30], Proposition 2.1. By Proposition 6.2, there are no integral components of multiplicity $> q$ in the singular fiber $\psi^{-1}(\infty) \subset S$. Whence F gets contracted by $\tilde{Y} \to S$. Therefore, the dual graph of $\psi^{-1}(\infty)$ is obtained from the dual graph of E by a sequence of vertex contractions. Again by Proposition 6.2, the dual graph for $\psi^{-1}(\infty)_{\mathrm{red}}$ contains precisely two nodes. This obviously implies that the dual graph for E contains at least two nodes. ∎

7. Description of the generic fiber. Our goal here is to describe the generic fiber $\varphi^{-1}(\eta)$ of the fibration

$$\varphi : G\backslash(C \times C) \to G\backslash C = \mathbb{P}^1$$

induced from projection onto the first factor. Recall that $q = p^m$ is our fixed prime power, and $C : \ y^q - y = x^{q+1}$ is our Hermitian curve on which the group G of order $\mathrm{ord}(G) = q^3$ acts.

Let R be an arbitrary ring of characteristic p, and consider the R-algebra

$$A = R[X, Y]/(Y^q - Y - X^{q+1}),$$

endowed with the canonical G-action as in (6). Here we temporarily use upper case symbols X, Y in order to distinguish later the two factors in the selfproduct $C \times C$. Let $\tau \in A$ be the residue class of $X^{q^2} + X$. From the description of the action one sees that τ is G-invariant.

PROPOSITION 7.1. *The subring $R[\tau] \subset A$ is the ring of G-invariants.*

Proof. Considering the intermediate ring $R[X]$, one sees that the ring A is free of rank $q^3 = \mathrm{ord}(G)$ as module over $R[\tau]$. To finish the argument, it suffices to treat the case that R is noetherian. By the Nakayama Lemma, we are reduced to the case that R is a field. Then both $R[\tau]$ and A are integral and normal. Now Galois theory and Zariski's Main Theorem yield the result. ☐

We view $U = \operatorname{Spec} k[\tau]$ as the open subset of $\mathbb{P}^1 = G\backslash C$ over which the fibration $\varphi : G\backslash(C \times C) \to \mathbb{P}^1$ is smooth. In particular, the preimage $\varphi^{-1}(U)$ becomes a flat family of smooth projective curves over U.

PROPOSITION 7.2. *The family of smooth projective curves $\varphi^{-1}(U) \to U$ is given by the homogenization of the equation $y^q - y = x^{q+1} + \tau x^q$.*

Proof. Let us point out that the challenge was to *guess* the right equation. Once an equation is found, it is not too difficult to verify its correctness with the abstract theory of twisted forms, as exposed at length by Giraud in his monograph [22].

Consider the smooth projective families of curves $\mathcal{C} \to U$ and $\mathcal{C}' \to U$ given by the homogenizations of the equations

$$y^q - y = x^{q+1} \quad \text{and} \quad y'^q - y' = x'^q + \tau x'^q,$$

respectively. To compare them we use the functor $\underline{\mathrm{Isom}}(\mathcal{C}, \mathcal{C}')$, whose values on $k[\tau]$-algebras R is the set of R-isomorphisms $\mathcal{C} \otimes_{k[\tau]} R \to \mathcal{C}' \otimes_{k[\tau]} R$. It contains as a subfunctor

$$I(R) = \left\{ (b, a) \in R^2 \mid a^{q^2} + a + \tau = 0 \quad \text{and} \quad b - b^q + \tau^{q+1} - a^{q^2+q} = 0 \right\},$$

where the inclusion $I(R) \subset \underline{\mathrm{Isom}}(\mathcal{C}, \mathcal{C}')(R)$ comes from the substitutions $x' \mapsto x + a$ and $y' \mapsto y - a^q x + b$. To proceed, we consider another functor

$$P(R) = \left\{ (b, a) \in R^2 \mid a^{q^2} + a - \tau = 0 \quad \text{and} \quad b^q - b - a^{q+1} = 0 \right\},$$

which is representable by the spectrum of $k[\tau, X, Y]/(X^{q^2} + X - \tau, Y^q - Y - X^{q+1})$. Note that the latter is a finite étale $k[\tau]$-algebra. We have a natural transformation

$$\Upsilon : P(R) \longrightarrow I(R), \quad (b, a) \longmapsto (-b - a^{q+1}, -a).$$

Our special p-group

$$G = \left\{ (t, r) \in k^2 \mid r^{q^2} + r = 0 \quad \text{and} \quad t^q - t = r^{q+1} \right\} \subset \mathrm{Aut}(C)$$

acts on the right on $\underline{\mathrm{Isom}}(\mathcal{C}, \mathcal{C}')$ by composition, and one easily computes that this action is given by

$$(b, a) \circ (t, r) = (b + t - a^q r, a + r).$$

On the other hand, P is endowed with a canonical G-action from the left, given by $(t,r)\cdot(b,a) = (b - r^q a + t, a + r)$ as in (6). In fact, the structure morphism $P \to U$ becomes a G-torsor. The corresponding *right* action is

$$(b,a)\cdot(t,r) = (t,r)^{-1}\cdot(b,a) = (-r^{q+1} - t + b + r^q a, a - r),$$

compare (7). A straightforward computation reveals that the natural transformation $\Upsilon : P \to I$ respects the right G-actions. Actually, it is a u-morphism, where $u : G \to \underline{\mathrm{Aut}}(\mathcal{C})$ denotes the canonical inclusion. In turn, we obtain a morphism

$$P \wedge^G \underline{\mathcal{C}} \longrightarrow \underline{\mathrm{Isom}}(\mathcal{C}, \mathcal{C}')$$

of right $\underline{\mathrm{Aut}}(\mathcal{C})$-torsors. Being a morphism of torsors, it is automatically an isomorphism. According to [22], Chapter III, Theorem 2.5.1, the family of curves $\mathcal{C}'$ is a twisted form of $\mathcal{C}$ with respect to the étale topology on U, and one has $\mathcal{C}' \simeq P \wedge^G \mathcal{C}$. The latter denotes the *contracted product* and is defined as the quotient of $P \times \mathcal{C}$ by the left G-actions $g \cdot (p, c) = (pg^{-1}, gc) = (gp, gc)$. But this coincides with the very definition of $\varphi^{-1}(U) \subset G\backslash(C \times C)$. The upshot is the $\varphi^{-1}(U)$ must be isomorphic to the family of curves $\mathcal{C}'$. ∎

Corollary 7.3. *The surface $G\backslash(C \times C)$ is rational.*

Proof. The function field of the our quotient surface is the field of fractions F of the ring $k[x, y, \tau]/(y^q - y - x^{q+1} - \tau x^q)$. The residue class of x is clearly a regular element. Thus we have an equation $\tau = -x + (y^q - y)/x^q$ in the field F. Hence $F = k(x, y)$, which shows that the surface in question is birational to $\mathbb{P}^2$. ∎

For $q = 2$, Shioda [49] already observed that the partial quotient by the center $Z\backslash(C \times C)$ is rational. The same thus holds for all further quotients (see for example [5], Theorem 13.27).

Setting $\tau = 1/z$ and clearing denominators for the equation in Proposition 7.2, we obtain the following description of the generic fiber:

Corollary 7.4. *The smooth projective curve $\varphi^{-1}(\eta)$ over the function field $k(z)$ of the quotient $\mathbb{P}^1 = G\backslash C$ is given by the homogenization of the equation*

$$y^q - z^{q^2-1} y = x^{q+1} + z^{q-1} x^q,$$

where $z \in \mathcal{O}_{\mathbb{P}^1,\infty}$ is a uniformizer.

8. Computation of the singular fiber. In this section we shall finish the proof for Proposition 6.2. In other words, we have to determine the dual graph for the singular fiber $\psi^{-1}(\infty)$ on the relative minimal model $\psi : S \to \mathbb{P}^1$ of the quotient surface $G\backslash(C \times C)$. In light of Corollary 7.4, the task boils down to compute the minimal resolution of singularities for the spectrum of residue class ring of $k[x, y, z]$ by the ideal genereated by the equation

$$y^q - z^{q^2-1} y - x^{q+1} - z^{q-1} x^q = 0. \tag{8}$$

As it turns out, this will produce no (-1)-curves in the singular fiber, and thus yield the desired description of $\psi^{-1}(\infty)$. It is worth to examine the simplest special case $q = 2$ first. Then $\psi : S \to \mathbb{P}^1$ becomes a jacobian elliptic fibration, whose singular fibers are classified in terms of *Kodaira symbols*.

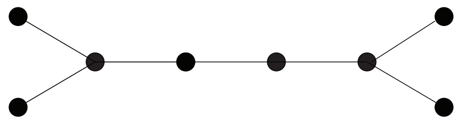


FIG. 2. *Dual graph for Kodaira symbol* I_3^*.

PROPOSITION 8.1. *For $q = 2$, the Weierstrass equation $y^2 - z^3y = x^3 + zx^2$ defines a rational double point of type D_7, and the singular fiber of the elliptic fibration $\psi : S \to \mathbb{P}^1$ has type I_3^*.*

Proof. This follows from the classification of jacobian elliptic fibrations on rational surfaces obtained by W. Lang: Our Weierstrass equation appears as case in [37], Section 2, Case 13C, and is listed there with type I_3^*. Independently, the structure of the singularity can be determined with the algorithm of Greuel and Kröning [23]. □

We now turn to the general case, and depict the dual graph again in Figure 3, where symbols $E_1, \ldots, E_{q-1}, F_0, F_1, F_2, F_3, F_4$ are assigned to certain irreducible components.

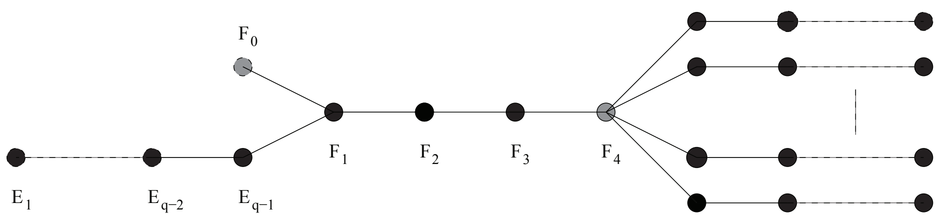


FIG. 3. *Dual graph of* $\psi^{-1}(\infty)$.

The resolution of singularities will be carried out in several steps, in which the indicated irreducible components show up successively. In some sense, our procedure generalizes the part of the *Tate Algorithm* [54] dealing with reduction types I_n^*, $n \geq 0$. The main idea already present in the Tate Algorithm is to blow-up Weil divisors, rather than points.

Step 0. The fiber for the initial equation (8) is given by $z = 0$, hence equals the spectrum of the ring $k[x, y]/(y^q - x^{q+1})$, which is clearly a rational curve with a single singularity at the origin. It corresponds to the irreducible component E_1 in Figure 3.

Step 1. Let us pass to the variables $z, x/z^{q-1}, y/z^{q-1}$, and examine the strict transform

$$\left(\frac{y}{z^{q-1}}\right)^q - z^{2q-2}\left(\frac{y}{z^{q-1}}\right) - \left(\frac{x}{z^{q-1}}\right)^{q+1} z^{q-1} - z^{q-1}\left(\frac{x}{z^{q-1}}\right)^q = 0 \tag{9}$$

of our initial equation (8), which is obtained by making substitutions $x = x/z^{q-1} \cdot z^{q-1}$ and $y = y/z^{q-1} \cdot z^{q-1}$, and afterwards dividing by the highest possible z-power. The schematic fiber on this chart is given by $z = 0$, and thus a copy of the affine line with multiplicity q. This will be the irreducible component F_1 in Figure 3. Note that for $q \neq 2$, the Equation (9) defines a divisor that is singular along the fiber.

Step 2. We next blow-up the reduced fiber for the previous Equation (9). In other words, the center is given by the ideal $(z, y/z^{q-1})$. This gives us two new charts. We start by describing the y/z^{q-1}-chart, which features as new variables $z^q/y, x/z^{q-1}, y/z^{q-1}$, allowing for the substitution $z = z^q/y \cdot y/z^{q-1}$. The resulting strict transform is

$$\frac{y}{z^{q-1}} - \left(\frac{z^q}{y}\right)^{2q-2}\left(\frac{y}{z^{q-1}}\right)^q - \left(\frac{x}{z^{q-1}}\right)^{q+1}\left(\frac{z^q}{y}\right)^{q-1} - \left(\frac{z^q}{y}\right)^{q-1}\left(\frac{x}{z^{q-1}}\right)^q = 0. \tag{10}$$

Computing partial derivatives one sees that this chart is smooth. The fiber is given by $z^q/y \cdot y/z^{q-1} = 0$, thus becomes the spectrum of residue class ring of $k[z^q/y, x/z^{q-1}]$ by the equation

$$\left(\frac{z^q}{y}\right)^q \left(\frac{x}{z^{q-1}}\right)^q \left(\frac{x}{z^{q-1}} - 1\right) = 0.$$

The three factors give the three irreducible components $qF_1 + qF_2 + F_0$ in Figure 3, respectively. To see that there are no further intersections, one has to look at the other chart, the z-chart. Here the variables are $z, x/z^{q-1}, y/z^q$. The substitution is $y/z^{q-1} = y/z^q \cdot z$, and the resulting strict transform is

$$\left(\frac{y}{z^q}\right)^q z - z^q \frac{y}{z^q} - \left(\frac{x}{z^{q-1}}\right)^{q-1} - \left(\frac{x}{z^{q-1}}\right)^q = 0. \tag{11}$$

The fiber is given by $z = 0$, whence isomorphic to $k[x/z^{q-1}, y/z^q]$ modulo the equation

$$\left(\frac{x}{z^{q-1}}\right)^q \left(\frac{x}{z^{q-1}} - 1\right).$$

This shows that there are no further intersection numbers. Computing partial derivatives, one sees that the Equation (11) has just one singularity, which is located at the origin.

Step 3. Now we make a blowing-up of (11) along the reduced fiber, which is given by the ideal $(z, x/z^{q-1})$. Let us treat the z-chart first. Here we have variables $z, x/z^q, y/z^q$, resulting in the strict transform

$$\left(\frac{y}{z^q}\right)^q - z^{q-1}\frac{y}{z^q} - \left(\frac{x}{z^q}\right)^{q+1} z^q - z^{q-1}\left(\frac{x}{z^q}\right)^q = 0. \tag{12}$$

The fiber on this chart is given by $z = 0$, which is a copy of the affine line with multiplicity q. It corresponds to the irreducible component qF_3 in Figure 3. Computing partial derivatives, one sees that the singular locus is contained in the fiber. A computation of the x/z^{q-1}-chart left to the reader reveals that $F_2 \cdot F_3 = 1$, and that there are no additional singularities.

Step 4. We blow-up the previous equation (12) along the reduced fiber for the previous equation, which is given by the ideal $(z, y/z^q)$. The z-chart has variables $z, x/z^q, y/z^{q+1}$, and the ensuing strict transform is

$$\left(\frac{y}{z^{q+1}}\right)^q z - z\frac{y}{z^{q+1}} - \left(\frac{x}{z^q}\right)^{q+1} z - \left(\frac{x}{z^q}\right)^q = 0. \tag{13}$$

The fiber on this chart is given by $z = 0$, which is a copy of the affine line with multiplicity q. It corresponds to the irreducible component F_4 in Figure 3. Computing partial derivatives, one sees that the singular locus is given by $z = x/z^q = 0$ and $(y/z^{q+1})^q - y/z^{q+1} = 0$. In other words, there are exactly q singular points, in a canonical way parameterized by the finite field $\mathbb{F}_q$. Looking at the formal completions of the local rings at these singularities, one easily sees that the singular points are rational double points of type A_{q-1}, that is, formally isomorphic to $k[[u,v,w]]/(u^q - vw)$, and that the resulting irreducible components intersect F_4 as in Figure 3. This accounts for the q strings of length $q-1$ on the right hand side of Figure 3. Computing the y/z^q-chart, one checks that $F_3 \cdot F_4 = 1$.

Step 5. It remains to understand how the string of $q-1$ curves on the left hand side of Figure 3 arises. For this return to the initial equation (8), and blow-up the *nonreduced 0-dimensional center* given by (z^{q-1}, x, y). We have already computed the z-chart in Step 1. The task now is to understand the x-chart. Here we have four variables $z^{q-1}/x, z, x, y/x$, and the strict transform is described by two equations

$$(14) \qquad z^{q-1} = z^{q-1}/x \cdot x \quad \text{and} \quad \left(\frac{y}{x}\right)^q - \left(\frac{z^{q-1}}{x}\right)^2 \frac{y}{x} x^2 - x - \frac{z^{q-1}}{x} x = 0.$$

The fiber $z = 0$ becomes thus the spectrum of the residue class ring of $k[z^{q-1}/x, x]$ by the equation $z^{q-1}/x \cdot (\frac{y}{x})^q = 0$. Its two irreducible components correspond to E_1 and qF_1. Now we complete the local ring at the origin. The second equation, together with the Implicit Function Theorem, tells us that $x = u(y/x)^q$, where u is in invertible formal power series. By the first equation, our complete local ring is isomorphic to

$$k[[u,v,w]]/(u^{q-1} - vw^q).$$

By the classical theory of quotient singularities, the normalization of this ring contains a unique singularity, which is a Hirzebruch–Jung singularity, compare [6], Chapter III, Section 5. The self-intersection numbers of the irreducible components on the minimal resolution of singularities are given by the continued fraction development:

$$\frac{q-1}{q-2} = 2 - \underbrace{\cfrac{1}{\ddots - \cfrac{1}{2}}}_{q-2 \text{ entries}}$$

In other words, we have a string of $q-2$ rational curves with self-intersection (-2), so our singularity is actually a rational double point of type A_{q-2}. This gives the irreducible components $E_2, \ldots, E_{q-1}$ in Figure 3. One easily computes the multiplicities in the fibers are $\sum_{i=2}^{q-1} iE_i$. A straightforward computation of the y-chart left to the reader reveals that there are no further singularities appear.

Step 6. By now we have verified that the dual graph of the fiber $\psi^{-1}(\infty)$ is as in Figure 1, and that the multiplicities of the irreducible components are as indicated. Using the fact that the divisor $\psi^{-1}(\infty)$ is numerically trivial on itself, one easily computes the self-intersection numbers by induction, starting with the irreducible components having only one neighbor. This concludes the proof for Proposition 6.2, and thus also for Theorem 6.1.

9. Higher ramification groups and Swan conductor. We now take a closer look at the action of the special p-group G on the Hermitian curve $C: \ y^q - q = x^{q+1}$ at infinity. The closure of the affine part of the scheme C inside $\mathbb{P}^2$ is given by the homogeneous equation

$$Y^q Z - Y Z^q = X^{q+1}, \qquad y = Y/Z, \quad x = X/Z.$$

Clearly, only the point $(0:1:0)\in\mathbb{P}^2$ lies on the closure at infinity. Dehomogenizing with respect to Y, we obtain the equation

$$Z/Y-(Z/Y)^q=(X/Y)^{q+1}.$$

Completing and using the implicit function theorem, one sees that

$$k[[X/Y]]=k[[X/Y,Z/Y]]/(Z/Y-(Z/Y)^q-(X/Y)^{q+1}),$$

and furthermore

$$Z/Y=(X/Y)^{q+1}+\ldots.$$

Note that here and throughout, dots in power series expansions are shorthand notation for "higher order terms".

Summing up, we have an embedding $C\subset\mathbb{P}^2$ of the regular proper curve C, and the complete local ring of the curve at the point $c=(0:1:0)$ is $\mathcal{O}^\wedge_{C,c}=k[[X/Y]]$. The action of G on C leaves $c\in C$ fixed. We now compute its *higher ramification groups*

$$G_i=\left\{\sigma\in G\mid \sigma=\mathrm{id}\text{ on }\mathcal{O}^\wedge_{C,c}/\mathfrak{m}^{i+1}\right\}.$$

These form a descending filtration $G_0\supset G_1\supset G_2\supset\ldots$ of normal subgroups inside G.

Proposition 9.1. *The higher ramification groups are*

$$G_0=G_1=G,\quad G_2=\ldots=G_{q+1}=Z,\quad G_{q+2}=0.$$

Proof. We first determine the position in the descending filtration for the nontrivial central group elements $\sigma=(t,0)$, $t\neq 0$. The action on the uniformizer in $\mathcal{O}^\wedge_{C,c}$ is

$$X/Y=x/y\longmapsto x/(y+t)=x/y\cdot(1+t/y)^{-1}.$$

We have $1/y=Z/Y=(X/Y)^{q+1}+\ldots$, whence

$$(1+t/y)^{-1}=\sum_{n\geq 0}(-t/y)^n=1-t(X/Y)^{q+1}+\ldots\ .$$

The upshot is that $\sigma\in G_{q+1}$ but $\sigma\notin G_{q+2}$. Now we consider noncentral group elements $\sigma=(t,r)$, $r\neq 0$. Here the action on the uniformizer is

$$X/Y=x/y\longmapsto(x+r)/(y-r^qx+t)=x/y\cdot(1+r/x)\cdot(1-r^qx/y+t/y)^{-1}.$$

The factors on the right hand side come from

$$1-r^qx/y+t/y=1-r^q(X/Y)+t(X/Y)^{q+1}+\ldots$$

and

$$1+r/x=1+r\cdot Z/Y\cdot(X/Y)^{-1}=1+r(X/Y)^q+\ldots\ .$$

Arguing as in the preceding paragraph with the geometric series, we infer that $\sigma\in G_1$ but $\sigma\notin G_2$. □

Now let l be a prime different from p, and let M be a finite dimensional $\mathbb{F}_l$-vector space endowed with a G-representation. Then one way to define the *Swan conductor* is

$$\delta = \delta(G, M) = \sum_{i \geq 1} \frac{1}{[G : G_i]} \dim(M/M^{G_i}).$$

As explained in [48], Chapter 19, this rational number is actually an integer. For later use we record:

Corollary 9.2. *In our situation, the Swan conductor is*

$$\delta = \dim(M/M^G) + q^{-1} \dim(M/M^Z).$$

10. Representations of certain special p-groups. In the next section we shall determine the l-adic cohomology group $H^1(C, \mathbb{Q}_l)$ as G-representation, where $C:\ y^q - y = x^{q+1}$ is a Hermitian curve, and G is the special p-group acting on C. To this end, we now make a digression and examine the representation theory of G over various fields. For general facts about representations of finite groups, we refer to the monographs of Serre [48], Curtis and Reiner [14] and Isaacs [29]. The representation theory of extraspecial p-groups is well-known (for example [17], Section B.9 or [31], Section 26).

It seems natural to deal with a somewhat more general class of groups. Throughout this section, we fix a prime power $q = p^n$, and assume that G is a finite special p-group. To keep the exposition in bounds, we demand that $\exp(G) = p$ for odd p. In contrast, we stipulate that each noncentral element has order four in case $p = 2$, as suggested by Proposition 5.3.

Moreover, we suppose that the group is endowed with the following *additional structure*: The center Z and the abelianization $G^{\mathrm{ab}} = G/Z$, which are elementary abelian groups and thus $\mathbb{F}_p$-vector spaces, are endowed with an $\mathbb{F}_q$-vector space structure so that the commutator pairing

$$G^{\mathrm{ab}} \times G^{\mathrm{ab}} \longrightarrow Z, \quad (\bar{a}, \bar{b}) \longmapsto [a, b] = aba^{-1}b^{-1}$$

are $\mathbb{F}_q$-bilinear and $\dim_{\mathbb{F}_q}(Z) = 1$. In turn, the abelianization G^{ab} may be regarded as a symplectic $\mathbb{F}_q$-vector space. Obviously, the order of the group is of the form

$$\mathrm{ord}(G) = q^{1+2n}, \qquad n = \dim_{\mathbb{F}_q}(G^{\mathrm{ab}}).$$

Clearly, the automorphism group $G \subset \mathrm{Aut}(C)$ considered in Section 5 is endowed with such an additional structure in an obvious way. To start with, we record:

Proposition 10.1. *The conjugacy classes of the special p-group G are the subsets*

$$\{z\} \subset G \quad \text{and} \quad f^{-1}(\bar{b}) \subset G,$$

with $z \in Z$ and $\bar{b} \in G^{\mathrm{ab}} \smallsetminus 0$, where $f : G \to G^{\mathrm{ab}}$ is the canonical projection.

Proof. We only have to verify that the fibers $f^{-1}(\bar{b})$, $\bar{b} \neq 0$ are whole conjugacy classes. Since $b \notin Z$, there is a nontrivial commutator $[a, b]$. Since the commutator pairing is $\mathbb{F}_q$-linear in $\bar{a}$, the commutators $[a, b]$, $a \in G$ fill out the whole center $Z \subset G$. In turn, the conjugate elements $aba^{-1} = [a, b] \cdot b$ fill out the whole coset $f^{-1}(\bar{b}) \subset G$. ∎

Given an arbitrary field K, we write $R_K(G)$ for the Grothendieck group of finite-dimensional G-representations over K, modulo the relations $[V] = [V'] + [V'']$ coming from short exact sequences $0 \to V' \to V \to V'' \to 0$. Let

$$\mathrm{Irr}_K(G) = \{[V_1], \ldots, [V_r]\}$$

be the set of isomorphism classes of irreducible G-representations over K or, what amounts to the same, simple KG-modules. Then $\mathrm{Irr}_K(G)$ is a basis for the abelian group $R_K(G)$, and we say that the $V_1, \ldots, V_r$ from a *basic set of irreducible representations*. We now shall determine basic sets of irreducible G-representations for various fields K. Our further analysis hinges on the following observation:

PROPOSITION 10.2. *Let K be a field of characteristic zero. Then the set* $\mathrm{Irr}_K(G)$ *has cardinality*

$$\mathrm{Card}(\mathrm{Irr}_K(G)) = \begin{cases} 1 + (q^{2n} + q - 2)/(p-1) & \text{if } \mu_p(K) = \{1\}; \\ q^{2n} + q - 1 & \text{else.} \end{cases}$$

Proof. First note that over algebraically closed fields of characteristic zero, the number of irreducible representations equals the number of conjugacy classes of elements; then our statement follows from Proposition 10.1.

Now let $\xi \in \mu_{p^2}(\bar{K})$ be a primitive p^2-th root of unity. The field extension $E = K(\xi)$ is abelian, with Galois group $\Gamma \subset (\mathbb{Z}/p^2\mathbb{Z})^\times$. Since each element $a \in G$ has $a^{p^2} = e$, we have a natural action of the group Γ on the set G, where $\sigma \in \Gamma$ acts via $a \mapsto a^\sigma$. According to [48], Section 12.4, the cardinality of $\mathrm{Irr}_K(G)$ coincides with the number of Γ-orbits of conjugacy classes in G. Since Z and G^{ab} are elementary abelian, the p-torsion subgroup $(1 + p\mathbb{Z})/p^2\mathbb{Z} \subset \Gamma$ acts trivially on the the set of conjugacy classes, and the formula in the second case of the statement follows.

Now suppose that $\mu_p(K) = \{1\}$. Then Γ acts via its quotient $(\mathbb{Z}/p\mathbb{Z})^\times$, and the latter group permutes transitively the nonzero central elements $z \in Z$ generating the same subgroup, and permutes transitively the fibers $f^{-1}(\bar{b})$ where $\bar{b} \in G^{\mathrm{ab}}$, $\bar{b} \neq 0$ generates the same subgroup in G^{ab}. Clearly, center and abelianization contain $(q-1)/(p-1)$ and $(q^{2n}-1)/(p-1)$ nonzero cyclic subgroups, respectively, and the first case of the statement follows. $\square$

Our next task is to construct and describe the irreducible G-representations over $K = \mathbb{Q}$. Of course there is the trivial representation, which we simply denote by $\mathbb{Q}$. Next, let $\varphi : G \to \mathbb{C}^\times$ be a nonzero homomorphism; in other words, a nonzero homomorphism $\varphi^{\mathrm{ab}} : G^{\mathrm{ab}} \to \mathbb{C}^\times$. It factors over the subgroups $\mu_p(\mathbb{C}) \subset \mathbb{Q}(e^{2\pi i/p})^\times \subset \mathbb{C}^\times$, because G^{ab} is elementary abelian, so we obtain a G-representations $(\mathbb{Q}(e^{2\pi i/p}), \varphi)$ over $\mathbb{Q}$ of degree $p-1$. Up to isomorphism, this representation depends only on the $\mathbb{F}_p$-hyperplane $\ker(\varphi) \subset G^{\mathrm{ab}}$, as the action of the Galois group for the Galois extension $\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/p})$ shows. Using Grothendieck's convention, we regard such hyperplanes as rational points $y \in \mathbb{P}(G^{\mathrm{ab}}) \simeq \mathbb{P}^{mn-1}_{\mathbb{F}_p}$, and set

$$W_y = (\mathbb{Q}(e^{2\pi i/p}), \varphi).$$

By the very construction, its degree and isomorphism algebra is given by

$$\dim(W_y) = p - 1 \quad \text{and} \quad \mathrm{End}(W_y) = \mathbb{Q}(e^{2\pi i/p}). \tag{15}$$

In particular, the representation is irreducible, and its complexification splits as $W_y \otimes_{\mathbb{Q}} \mathbb{C} = \bigoplus(\mathbb{C}, \varphi)$, where the sum extends over all nonzero homomorphisms $\varphi : G \to \mathbb{C}^\times$ satisfying $y = \ker(\varphi^{\mathrm{ab}})$.

To construct the remaining irreducible representations, one makes a construction involving induction from the center $Z \subset G$. Choose once and for all a Lagrangian $\mathbb{F}_q$-subvector space in G^{ab}, that is, a totally isotropic vector subspace of maximal dimension, and let $H \subset G$ be its preimage. This is an abelian normal subgroup of index $[G : H] = q^n$ with $Z \subset H$. By our standing assumption $Z \subset H$ is a direct summand if and only if p is odd. At this point it is most convenient to distinguish that cases that p is even or odd.

Suppose p is odd. Given a nonzero homomorphism $\chi : Z \to \mathbb{C}^\times$, we extend it in an arbitrary way to a homomorphism $\tilde{\chi} : H \to \mathbb{C}^\times$. Since H is elementary abelian, it factors over the subgroups $\mu_p(\mathbb{C}) \subset \mathbb{Q}(e^{2\pi i/p}) \subset \mathbb{C}^\times$, thus turning $\mathbb{Q}(e^{2\pi i/p})$ into an irreducible H-representation of degree $p-1$. As above, the Galois action shows that the underlying Z-representation representation depends only $\ker(\chi) \subset Z$, which we regard as a rational point $x \in \mathbb{P}(Z) \simeq \mathbb{P}^{m-1}_{\mathbb{F}_p}$. Now consider the induced G-representation

$$V_x = \mathrm{ind}_H^G(\mathbb{Q}(e^{2\pi i/p}), \tilde{\chi}) = \mathbb{Q}(e^{2\pi i/p}) \otimes_{\mathbb{Q}H} \mathbb{Q}G$$

over $\mathbb{Q}$. A priori, this seems to depend on the chosen extension $\tilde{\chi}$. However, it will follow from Theorem 10.4 below that its isomorphism class depends only on x.

LEMMA 10.3. *Suppose $p \neq 2$. The G-representations V_x, $x \in \mathbb{P}(Z)$ are irreducible. Their degrees and endomorphism algebras are*

$$\dim(V_x) = q^n(p-1) \quad \textit{and} \quad \mathrm{End}(V_x) = \mathbb{Q}(e^{2\pi i/p}).$$

Proof. The degree is obvious, and irreducibility follows from the statement about the endomorphism ring. By definition, we have $V_x = \mathrm{ind}_H^G(M)$ for the irreducible H-representation $M = (\mathbb{Q}(e^{2\pi i/p}), \tilde{\chi})$. Frobenius Reciprocity gives

$$\mathrm{End}(V_x) = \mathrm{Hom}_H(M, \mathrm{Res}_H^G(\mathrm{ind}_H^G(M))),$$

and $\mathrm{Res}_H^G(\mathrm{ind}_H^G(M))$ is the direct sum of the H-representations ${}^bM$ obtained by transport of structure, where $bH \subset G$ runs over all cosets. The H-action on ${}^bM$ is defined as $bhb^{-1} \cdot m = hm$. Therefore, we merely have to check that $\chi \circ \gamma_b \neq \chi$ for all $b \in G \smallsetminus H$. Since Lagrangian are maximally totally isotropic, there must be some $a \in H$ that does not commute with b. Now choose some some $z \in Z$ not contained in the kernel of $\chi : Z \to \mathbb{C}^\times$. Multiplying by a suitable $\lambda \in \mathbb{F}_q$ if necessary, we may assume that $[a, b] = z$. Then $\chi(bab^{-1}) \neq \chi(a)$. ☐

THEOREM 10.4. *Suppose $p \neq 2$. Then the representations*

$$V_x,\, x \in \mathbb{P}(Z), \quad \textit{and} \quad W_y,\, y \in \mathbb{P}(G^{\mathrm{ab}}), \quad \textit{and} \quad \mathbb{Q}$$

form a basic set of irreducible representations over $K = \mathbb{Q}$. Moreover, they remain a basic set of irreducible representations after scalar extensions $\mathbb{Q} \subset K$ if and only if $\mu_p(K) = \{1\}$.

Proof. We saw above that the given representations are irreducible. It is obvious that the $(q^{2m} - 1)/(p - 1)$ representations W_y are pairwise nonisomorphic, and that no V_x is isomorphic to some W_y. To see that the $(q-1)/(p-1)$ representations V_x are pairwise nonisomorphic, look at their characters on Z. For $K = \mathbb{Q}$, the statement now follows from Proposition 10.2.

Now let $\mathbb{Q} \subset K$ be a field extension with $\mu_p(K) = \{1\}$. Then the endomorphism algebra of $V_x \otimes_{\mathbb{Q}} K$ is isomorphic to $\mathbb{Q}(e^{2\pi i/p}) \otimes_{\mathbb{Q}} K$, which remains a field, so the representation stays irreducible. The same argument applies for the representations W_y and $\mathbb{Q}$. A second application of Proposition 10.2 concludes the proof. ◻

Now we have to deal with the case $p = 2$. Let $\chi : Z \to \mathbb{C}^\times$ be a nonzero homomorphism, and extend it in an arbitrary way to $\tilde{\chi} : H \to \mathbb{C}^\times$. Then χ factors over $\mu_2(\mathbb{C}) = \{\pm 1\}$, yet this is not the case for $\tilde{\chi}$, because $Z \subset H$ is not a direct summand by our standing assumption. However, it factors over $\mu_4(\mathbb{C}) \subset \mathbb{Q}(i)^\times \subset \mathbb{C}^\times$. We now define a G-representation

$$2V_x = \operatorname{ind}_H^G(\mathbb{Q}(i), \tilde{\chi}) = \mathbb{Q}(i) \otimes_{\mathbb{Q}H} \mathbb{Q}G.$$

Here $x \in \mathbb{P}(Z)$ is the rational point corresponding to $\chi : Z \to \mathbb{C}^\times$ via $x = \ker(\chi)$. Beware that $2V_x$ is just a formal symbol; there is no representation V_x over $\mathbb{Q}$; the latter will acquire meaning only after certain scalar extensions.

Now recall that $(a, b)_K$ with $a, b \in K^\times$ denotes the *quaternion algebra* over a field K generated by symbols i, j modulo the relations $i^2 = a$, $j^2 = b$ and $ij = -ji$. This a central simple algebra of degree two. Up to isomorphism, it depends only on the classes of a, b modulo $\mathbb{Q}^{\times 2}$. For example, $(-1, -1)_{\mathbb{R}} = \mathbb{H}$ are the classical Hamilton quaternions.

Lemma 10.5. *Suppose $p = 2$. The G-representations $2V_x$, $x \in \mathbb{P}(Z)$ are irreducible. Their degree and endomorphism algebra is given by*

$$\dim(2V_x) = 2q^n \quad \textit{and} \quad \operatorname{End}(2V_x) = (-1, -1)_{\mathbb{Q}}.$$

Proof. It is easy to see that $\mathbb{Q}(i)$ is irreducible as Z-representations, and the irreducibility of the induced G-representation follows with Mackey's criterion as in the proof of Lemma 10.3. The dimension formula is obvious.

The endomorphism algebra $D = \operatorname{End}(2V_x)$ is a division ring. According to Proposition 10.2, the cardinality of $\operatorname{Irr}_K(G)$ does not depend on the field $\mathbb{Q} \subset K$. We infer that $\mathbb{Q}$ must be the center of the division ring D. According to Roquette's result (compare [29], Corollary 10.14), the degree $d = \deg(D)$, which is defined as the square root of $\dim_{\mathbb{Q}}(D)$ and in this context called the *Schur index*, is either $d = 1$ or $d = 2$. We have an obvious inclusion $\mathbb{Q}(i) \subset D$. Whence $d = 2$, and our division ring is of the form $D = (a, b)_{\mathbb{Q}}$, and we may assume that $a, b \neq 0$ are square-free integers. Clearly $K = \mathbb{R}$ is not a splitting field for the H-representation $\mathbb{Q}(i)$, and therefore not for $2V_x$. It follows $a, b < 0$. Similarly, $K = \mathbb{Q}(\sqrt{n})$ is not a splitting field, for all square free integers $n > 0$. So the only remaining possibility is $a, b = -1$. ◻

Theorem 10.6. *Suppose $p = 2$. Then the representations*

$$2V_x,\ x \in \mathbb{P}(Z) \quad \textit{and} \quad W_y,\ y \in \mathbb{P}(G^{\mathrm{ab}}) \quad \textit{and} \quad \mathbb{Q}$$

form a basic set of irreducible representations over $K = \mathbb{Q}$. Moreover, they stay a basic set of irreducible representations after scalar extension $\mathbb{Q} \subset K$ if and only if the equation $T_0^2 + T_1^2 + T_2^2 = 0$ has no nontrivial solution in K.

Proof. We saw above that the given representations are irreducible. It is obvious that the $(q^{2m}-1)/(p-1)$ representations W_y are pairwise nonisomorphic, and that no V_x is isomorphic to some W_y. To see that the $(q-1)/(p-1)$ representations V_x are pairwise nonisomorphic, simply look at their characters on Z. For $K=\mathbb{Q}$, the statement now follows from Proposition 10.2. For $\mathbb{Q}\subset K$ arbitrary, $2V_x$ stays irreducible over K is and only if this field does not split $\operatorname{End}(2V_x)=(-1,-1)_{\mathbb{Q}}$, whence the result. ☐

If $\mathbb{Q}\subset K$ is any field extension, we set

$$V_{x,K}=V_x\otimes_{\mathbb{Q}}K \quad \text{and} \quad W_{y,K}=W_y\otimes_{\mathbb{Q}}K$$

for the G-representations obtained by scalar extension. Note that for $p=2$, the former only makes sense if $T_0^2+T_1^2+T_2^2=0$ has a nontrivial solution in K; in this case, $V_{x,K}$ is defined as an irreducible summand in $2V_x\otimes_{\mathbb{Q}}K$.

Over the field $K=\mathbb{Q}_l$ of l-adic numbers, $l\neq p$, we have the following almost uniform description of irreducible representation:

PROPOSITION 10.7. *Suppose either $p=2$, or that p does not divide $l-1$. Then the $V_{x,\mathbb{Q}_l}$, $W_{y,\mathbb{Q}_l}$, $\mathbb{Q}_l$ form a basic set of irreducible G-representations over $K=\mathbb{Q}_l$.*

Proof. Suppose first that p is odd. By assumption, $\mu_p(\mathbb{F}_l)$ is trivial, thus the same holds for $\mu_p(\mathbb{Q}_l)$, and the statement follows from Proposition 10.4. Now suppose $p=2$. The quadric $T_0^2+T_1^2+T_2^2$ has a nontrivial solution over any finite field, thus also over $\mathbb{Q}_l$ by Hensel's Lemma, so $V_{x,\mathbb{Q}_l}$ makes sense. By (15), the $W_{x,\mathbb{Q}_l}$ stay irreducible, and the statement easily follows from Proposition 10.6. ☐

11. Cohomology as representations. We return to our Hermitian curve $C: y^q-y=x^{q+1}$, on which the special p-group G of order $\operatorname{ord}(G)=q^3$ acts, as discussed in Section 5. We seek to compute the l-adic cohomology group $H^1(C,\mathbb{Q}_l)$, viewed as a G-representation of degree $q(q-1)$ over the field $K=\mathbb{Q}_l$. In the previous section, we have introduced the G-representation $V_{x,\mathbb{Q}_l}=V_x\otimes_{\mathbb{Q}}\mathbb{Q}_l$. We now set

$$V_{\mathbb{Q}_l}=\bigoplus_x V_{x,\mathbb{Q}_l}$$

where the sum runs over all points $x\in\mathbb{P}(Z)\simeq\mathbb{P}^{m-1}_{\mathbb{F}_p}$. Recall that $Z\subset G$ is the center.

THEOREM 11.1. *For each prime $l\neq p$, the G-representations $H^1(C,\mathbb{Q}_l)$ and $V_{\mathbb{Q}_l}$ are isomorphic.*

Proof. Choose a nonzero element $z\in Z$, and consider its *Lefschetz number*

$$\Lambda(z)=\sum_{i=0}^{2}(-1)^i\operatorname{Tr}(z,H^i(C,\mathbb{Q}_l))\in\mathbb{Q}_l.$$

By the Lefschetz Trace Formula (for example [44], Theorem 12.3), the number $\Lambda(z)$ equals the length of the fixed scheme on C. We saw in Proposition 9.1 that $z\in G_{q+1}$ but $z\notin G_{q+2}$, hence the fixed scheme has length $q+2$. We conclude

$$\operatorname{Tr}(z,H^1(C,\mathbb{Q}_l))=-\Lambda(z)+2=-q.$$

Before we continue, note that it suffices to argue for a single prime $l\neq p$, because the irreducible components in all the $V_{x,\mathbb{C}}$ are pairwise nonisomorphic. So we may assume that p does not divide l in case $p \neq 2$. Now we are in a situation that the $V_{x,\mathbb{Q}_l}$, $W_{y,\mathbb{Q}_l}$, $\mathbb{Q}_l$ form a basic set of irreducible representations over $K = \mathbb{Q}_l$. Write the isomorphism class of $H^1(C, \mathbb{Q}_l)$ as

$$\sum_{x \in \mathbb{P}(Z)} m_x [V_{x,\mathbb{Q}_l}] + \sum_{y \in \mathbb{P}(G^{\mathrm{ab}})} n_y [W_{y,\mathbb{Q}_l}] + n[\mathbb{Q}_l],$$

for certain integral coefficients $m_x, n_y, n \geq 0$. Obviously, $\mathrm{Tr}(z, W_y) = p - 1$ and $\mathrm{Tr}(z, \mathbb{Q}) = 1$ are positive. As the Lefschetz number $\Lambda(z)$ is negative, at least one m_x must be nonzero. Since

$$\dim H^1(C, \mathbb{Q}_l) = q(q-1) = \frac{q-1}{p-1} q(p-1) = \dim(V_{\mathbb{Q}_l}),$$

it suffices to verify that the coefficients m_x do not depend on the index $x \in \mathbb{P}(Z)$. To achieve this, we use further symmetries of the Hermitian curve $C:\ y^q - y = x^{q+1}$. Namely, the group $\mu_{q^2-1}(k) = \mathbb{F}_{q^2}^\times$ acts on C via

$$x \longmapsto \zeta x, \quad y \longmapsto \zeta^{q+1} y, \qquad \text{for } \zeta \in \mathbb{F}_{q^2}^\times,$$

as remarked in [53], proof of Satz 5. One easily computes that the subgroup $\mathbb{F}_{q^2}^\times \subset \mathrm{Aut}(C)$ normalizes the subgroup $G \subset \mathrm{Aut}(C)$, and the induced conjugacy action

$$c : \mathbb{F}_{q^2}^\times \longrightarrow \mathrm{Aut}(G), \quad \zeta \longmapsto \big((t,r) \mapsto \zeta \circ (t,r) \circ \zeta^{-1}\big)$$

is given by $(t,r) \mapsto (\zeta^{q+1} t, \zeta r)$. We infer that the linear bijection $\zeta : H^1(C, \mathbb{Q}_l) \to H^1(C, \mathbb{Q}_l)$ is an isomorphism between the original G-representation and the new G-representation obtained by transport of structure

$$G \xrightarrow{c_\zeta} G \longrightarrow \mathrm{GL}(H^1(C, \mathbb{Q}_l)).$$

A straightforward computation shows that the G-representation ${}^\zeta V_x$ obtained by transport of structure is precisely $V_{\zeta^{q+1} x}$. But the ζ^{q+1} range over all elements in $\mu_{q-1}(k) = \mathbb{F}_q^\times$; thus the group $\mathbb{F}_{q^2}^\times$ acts transitively on the nonzero elements in Z, and in particular transitively on the $\mathbb{F}_p$-hyperplanes $x \subset Z$. From this we deduce that the multiplicities $m_x \geq 0$ do not depend on the index $x \in \mathbb{P}(Z)$. ☐

For later use, we record the following consequence:

Corollary 11.2. *For each prime $l \neq p$, the G-invariant part of $H^1(C, \mathbb{Q}_l)$ is trivial, whereas the G-invariant part of the tensor product $H^1(C, \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} H^1(C, \mathbb{Q}_l)$ has dimension $q - 1$.*

Proof. As in the previous proof, it suffices to verify this for a single prime $l \neq p$, and we thus may assume that the $V_{x,\mathbb{Q}_l}$ are irreducible. The first statement immediately follows from the Theorem. As to the second part, it suffices to check that the G-invariant part of $V_{x,\mathbb{Q}_l} \otimes V_{x,\mathbb{Q}_l}$ has dimension $p-1$, because $H^1(C, \mathbb{Q}_l)$ contains $(q-1)/(p-1)$ such irreducible summands. Looking at traces, one easily sees that the $V_{x,\mathbb{Q}_l}$ are selfdual, hence we have

$$V_{x,\mathbb{Q}_l} \otimes V_{x,\mathbb{Q}_l} \simeq \mathrm{End}(V_{x,\mathbb{Q}_l}).$$

The statement follows from Lemmas 10.3 and 10.5. ☐

COROLLARY 11.3. *Let $l \neq p$ be a prime. Suppose either $p = 2$, or that p does not divide $l - 1$. Then $H^1(C, \mathbb{Q}_l)$ is irreducible as representation of* $\mathrm{Aut}(C)$.

Proof. According to the Theorem, we have a decomposition

$$H^1(C, \mathbb{Q}_l) = \bigoplus_{x \in \mathbb{P}(Z)} V_{x,\mathbb{Q}_l}.$$

The assumption ensures that the summands $V_{x,\mathbb{Q}_l}$ are irreducible by Proposition 10.7. In the proof of the Theorem, we saw that the summands are permuted transitively by the subgroup $\mathbb{F}_{q^2}^\times \subset \mathrm{Aut}(C)$. It follows that $H^1(C, \mathbb{Q}_l)$ is irreducible as representation of $G \rtimes \mathbb{F}_{q^2}^\times \subset \mathrm{Aut}(C)$. ∎

Applying Corollary 9.2, one easily obtains:

COROLLARY 11.4. *Let $l \neq p$ be a prime. The Swan conductor for the G-representation $H^1(C, \mathbb{F}_l)$ is given by $\delta(G, H^1(C, \mathbb{F}_l)) = q^2 - 1$.*

12. Curves with irreducible cohomology. In this section we shall examine curves whose first l-adic cohomology is irreducible as representation of the full automorphism group for some prime $l \neq p$. The precise setting is as follows. Fix a prime power $q = p^m$, and consider smooth proper geometrical connected curves C_0 over the finite field $\mathbb{F}_q$, and let $C = C_0 \otimes_{\mathbb{F}_q} k$ be the induced curve over the algebraic closure $k = \bar{\mathbb{F}}_q$.

The power $\mathrm{Fr}_{C_0}^m$ of the absolute Frobenius morphism $\mathrm{Fr}_{C_0} : C_0 \to C_0$ is a $\mathbb{F}_q$-morphism, and induces by base change a bijective morphism

$$\Phi = \mathrm{Fr}_{C_0}^m \otimes_{\mathbb{F}_q} k : C \longrightarrow C.$$

We now consider the induced action

$$\Phi : H^1(C, \mathbb{Q}_l) \longrightarrow H^1(C, \mathbb{Q}_l), \quad e \geq 1$$

on l-adic cohomology, which are $\mathbb{Q}_l$-linear bijections. The resulting polynomial

$$P_1(C_0, T) = \det(1 - \Phi T \mid H^1(C, \mathbb{Q}_l)) \in \mathbb{Q}_l[T]$$

is called the *characteristic polynomial* of the curve C. Recall that its degree equals the Betti number $b_1 = \dim H^1(C, \mathbb{Q}_l)$. Factoring $P_1(C, T) = \prod_{j=1}^{b_1}(1 - \alpha_j T)$, one finds that the reciprocal roots $\alpha_j \in \bar{\mathbb{Q}}_l$ have absolute value $||\iota(\alpha_j)|| = q^{m/2}$ for all complex embeddings $\iota : \mathbb{Q}_l \to \mathbb{C}$. Note that extending the ground field by $\mathbb{F}_q \subset \mathbb{F}_{q^f}$ replaces Φ by the power Φ^f and the reciprocal roots α_j by α_j^f.

In general, it is difficult to compute the characteristic polynomial. The following connects characteristic polynomials with symmetries of the curve:

THEOREM 12.1. *Suppose there is a prime $l \neq p$ so that $H^1(C, \mathbb{Q}_l)$ is irreducible as representation of* $\mathrm{Aut}(C_0)$. *Then the characteristic polynomial is of the form*

$$P_1(C_0, T) = (1 \pm q^{1/2} T)^{b_1}.$$

Proof. Set $A = \mathrm{Aut}(C_0)$. Choose a very ample invertible sheaf $\mathcal{L}_0$ on C_0 endowed with an A-linearizion, and consider the resulting embeddings $C_0 \subset \mathbb{P}^n_{\mathbb{F}_q}$ and $A \subset \mathrm{PGL}_n(\mathbb{F}_q)$. The latter shows that $\mathrm{Fr}_{C_0}^m$ commutes with each automorphism $a \in A$.

Consequently, the induced bijection $\Phi : H^1(C, \mathbb{Q}_l) \to H^1(C, \mathbb{Q}_l)$ is a morphism of A-representation. By Schur's Lemma, it is multiplication by some scalar $\alpha^{-1} \in \mathbb{Q}_l^\times$, so the characteristic polynomial is $P_1(C,T) = (1-\alpha T)^{b_1}$, and α is a Weil q-number. On the other hand, on knows that the characteristic polynomial has integral coefficients. Its linear coefficient it $-b_1\alpha$, so $\alpha \in \mathbb{Q}$. The only rational numbers that are also Weil q-numbers are $\pm q^{1/2}$. ∎

Recall that the curve C is called *supersingular* if its jacobian $J = \mathrm{Pic}^0_{C/k}$ is supersingular, that is, isogeneous to a product of supersingular elliptic curve. We now have a criterion for supersingularity:

Corollary 12.2. *Suppose there is a prime $l \neq p$ so that $H^1(C, \mathbb{Q}_l)$ is irreducible as representation of* $\mathrm{Aut}(C)$. *Then the curve C is supersingular.*

Proof. Replacing $\mathbb{F}_q$ by a suitable finite extension, we may assume that $\mathrm{Aut}(C_0) = \mathrm{Aut}(C)$. Then $\Phi = (1 \pm q^{1/2}T)^{b_1}$ by the Theorem. As explained in [55], the formal completion of the jacobian $J = \mathrm{Pic}^0_{C/k}$ is isogeneous to a selfproduct of the formal group scheme $G_{1,1}$. The latter is equivalent to the supersingularity of J. ∎

Using Corollary 11.3, we obtain as a special case:

Corollary 12.3. *The Hermitian curves $C: \; y^q - y = x^{q+1}$ are supersingular.*

13. Diagonal quotients. We now collect some facts about quotients of products of curves. The situation is as follows: Fix an algebraically closed ground field k of characteristic $p > 0$, and let C, C' be two smooth proper curves, say of genus g, g', respectively. We consider the surface $X = C \times C'$. The Betti numbers of this smooth proper surface are

$$b_1(X) = g + g' \quad \text{and} \quad b_2(X) = 2 + gg'.$$

Suppose that we have a finite group G, together with homomorphisms

$$\mathrm{Aut}(C) \longleftarrow G \longrightarrow \mathrm{Aut}(C'),$$

and consider the proper normal surface $Y = (C \times C')/G$. We assume that G acts faithfully on each curve, hence freely on some open dense subsets.

Proposition 13.1. *Suppose that the G-representations $H^1(C, \mathbb{Q}_l)$ and $H^1(C', \mathbb{Q}_l)$ contain no copy of the trivial G-representation $\mathbb{Q}_l$. Then the Picard scheme $\mathrm{Pic}_{Y/k}$ of the proper normal surface $Y = G\backslash(C \times C')$ is zero-dimensional.*

Proof. Since Y is normal, the connected component $\mathrm{Pic}^0_{Y/k}$ is an extension of an abelian variety by a zero-dimensional group scheme. We thus have to show that $\mathrm{Pic}^0_{Y/k}$ contains no abelian variety. Suppose to the contrary that it does. According to [9], Exposé XIII, Theorem 3.8, the pullback morphism of group schemes $\mathrm{Pic}_{Y/k} \to \mathrm{Pic}_{X/k}$ is quasiaffine. It follows that its image contains an abelian variety. In turn, the homomorphism

$$H^1(Y, \mathbb{Q}_l) \longrightarrow H^1(X, \mathbb{Q}_l)^G \subset H^1(X, \mathbb{Q}_l) = H^1(C, \mathbb{Q}_l) \oplus H^1(C', \mathbb{Q}_l)$$

is nonzero. By assumption, however, the G-invariant part of $H^1(X, \mathbb{Q}_l)$ is trivial, contradiction. ∎

Recall that the *Néron–Severi group* $\mathrm{NS}(Y)$ of a proper scheme Y is the Picard group $\mathrm{Pic}(Y)$ modulo algebraic equivalence. This is a finitely generated abelian group, whose rank is called the *Picard number* $\rho(Y)$.

PROPOSITION 13.2. *If C, C' are supersingular, then the Picard number of the proper normal surface $Y = G\backslash(C \times C')$ is given by $\rho(Y) = 2 + d$, where d is the multiplicity of the trivial G-representation $\mathbb{Q}_l$ in the tensor product $H^1(C, \mathbb{Q}_l) \otimes H^1(C', \mathbb{Q}_l)$.*

Proof. Consider the following commutative diagram

$$\begin{array}{ccc} \mathrm{NS}(X) \otimes \mathbb{Q}_l & \longrightarrow & H^2(X, \mathbb{Q}_l) \\ \uparrow & & \uparrow \\ \mathrm{NS}(Y) \otimes \mathbb{Q}_l & \longrightarrow & H^2(Y, \mathbb{Q}_l), \end{array}$$

where the horizontal maps are induced from the l-adic cycle class maps. These maps are injective, as can be seen by using intersection numbers on the smooth surface X and the $\mathbb{Q}$-factorial surface Y. Using the projection formula for intersection numbers, one also sees that the vertical map on the left is injective. According to [55], Theorem 2.5, the upper horizontal map is bijective, because our curves C, C' are supersingular.

It only remains to check that each each G-invariant class $[\mathcal{L}] \in \mathrm{NS}(X)$ descends to a class on Y, at least after passing to some multiple. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Pic}^0(X)^G & \longrightarrow & \mathrm{Pic}(X)^G & \longrightarrow & \mathrm{NS}(X)^G & \longrightarrow & H^1(G, \mathrm{Pic}^0(X)) \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathrm{Pic}^0(Y) & \longrightarrow & \mathrm{Pic}(Y) & \longrightarrow & \mathrm{NS}(Y). & & \end{array}$$

The group $\mathrm{Pic}^0(X)$ of algebraically trivial invertible sheaves is a divisible group, whence its cohomology vanishes. By a diagram chase, it suffices to check that each G-invariant invertible sheaf $\mathcal{L}$ on X descends to Y, at least after passing to some multiple.

To this end, consider the G-invariant open subset $U \subset X$ on which the G-action is free, and let $V \subset Y$ be its image. Clearly, the complements of these open subsets are zero-dimensional. Since the action is free, we have a short exact sequence

$$H^1(G, k^\times) \longrightarrow \mathrm{Pic}(V) \longrightarrow \mathrm{Pic}^G(U) \longrightarrow H^2(G, k^\times),$$

and the outer terms are torsion groups. Passing to some multiple, we see that $\mathcal{L}|_U$ descends to some invertible sheaf $\mathcal{N}_V$ on V. Having only quotient singularities, the scheme Y is $\mathbb{Q}$-factorial. Passing again to some suitable multiple, we see that $\mathcal{N}_V$ extends to Y. This extension $\mathcal{N}$ has the property that its preimage $\mathcal{N}_X$ coincides with $\mathcal{L}$ over the open subset $U \subset X$ whose complement is zero-dimensional. It then follows that $\mathcal{N}_X \simeq \mathcal{L}$. ☐

The projections $\mathrm{pr}_1 : C \times C' \to C$ induces a fibration

$$f : Y = (C \times C')/G \longrightarrow C/G.$$

The generic fibers $Y_\eta = f^{-1}(\eta)$ is a smooth proper curve over the function field $F = k(C/G) = k(C)^G$. By construction, Y_η is a twisted form of $C' \otimes_k F$. In particular, it is smooth of genus $g(Y_\eta) = g'$. Combining the preceding two results, we obtain:

PROPOSITION 13.3. *Suppose that the curves C, C' are supersingular, and that the G-representations $H^1(C, \mathbb{Q}_l)$ and $H^1(C', \mathbb{Q}_l)$ contain no copy of the trivial G-representation $\mathbb{Q}_l$. Then the abelian group $\operatorname{Pic}^0(Y_\eta)$ is finitely generated of rank d, where d is the multiplicity of the trivial G-representation $\mathbb{Q}_l$ in the tensor product $H^1(C, \mathbb{Q}_l) \otimes H^1(C', \mathbb{Q}_l)$.*

Proof. The group $\operatorname{Pic}(Y)$ is finitely generated by Proposition 13.1. Its rank is given by $\rho = 2 + d$ by Proposition 13.2. Consider the restriction map $r : \operatorname{Pic}(Y) \to \operatorname{Pic}(Y_\eta)$. Its kernel is a finitely generated group of rank one, since all fibers of $Y \to C/G$ are irreducible. Hence the image $\operatorname{im}(r) \subset \operatorname{Pic}(Y_\eta)$ is finitely generated of rank $1 + d$. The cokernel of this map is n-torsion for some integer $n \geq 1$, because the scheme Y is $\mathbb{Q}$-factorial. It remains to check that $\operatorname{coker}(r)$ is finitely generated. To this end, set $E = k(C)$, and regard C_E as the generic fiber of the projection $X = C \times C' \to C$. This gives a commutative diagram

$$\begin{array}{ccccccccc}
 & & \operatorname{Pic}(Y) & \longrightarrow & \operatorname{Pic}(Y_\eta) & \longrightarrow & \operatorname{coker}(r) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H & \longrightarrow & \operatorname{Pic}(X_E) & \longrightarrow & \operatorname{Pic}(X_E)/H, & &
\end{array}$$

where H is the image of the composite map $\operatorname{Pic}(Y) \to \operatorname{Pic}(X) \to \operatorname{Pic}(X_E)$. The kernel of the vertical map in the middle is finite according to [9], Exposé XIII, Theorem 3.8. By the Five Lemma, it thus suffices to check that the n-torsion in $\operatorname{Pic}(X_E)/H$ is finite. This follows from a general fact stated below. ∎

LEMMA 13.4. *Let Z be a proper, geometrically normal scheme over a ground field E, and $H \subset \operatorname{Pic}(Z)$ be a finitely generated subgroup. Then the n-torsion subgroup of $\operatorname{Pic}(Z)/H$ is finite for all integers $n \geq 1$.*

Proof. For any field extension $E \subset E'$, the induced morphism $\operatorname{Pic}(Z) \to \operatorname{Pic}(Z \otimes E')$ is injective. Thus we may assume that E is algebraically closed. Set $D = \operatorname{Pic}(Z)$. The short exact sequence $0 \to H \to D \to D/H \to 0$ yields an exact sequence

$$\operatorname{Tor}_1(D, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \operatorname{Tor}_1(D/H, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H \otimes \mathbb{Z}/n\mathbb{Z}.$$

Therefore, is suffices to check that the n-torsion in $D = \operatorname{Pic}(Z)$ is finite. This follows from [9], Exposé XIII, Theorem 5.1, toether with the fact that the reduction of Pic^0_Z is an abelian variety. ∎

14. Chern invariants. In this final chapter we return to the relative minimal smooth model $\psi : S \to \mathbb{P}^1$ of the fibration $G\backslash(C \times C) \to G\backslash C$, where $C : y^q - q = x^{q+1}$ is our Hermitian curve. We saw in Corollary 7.3 that S is a rational surface. Here we compute its numerical invariants:

THEOREM 14.1. *The Chern invariants for the rational surface S are*

$$c_2 = e = q^2 + q + 6 \quad \textit{and} \quad c_1^2 = K_S^2 = -q^2 - q + 6.$$

The Picard number is given by the formula $\rho = q^2 + q + 4$.

Proof. We use Dolgachev's Formula [18]

$$e(S) = e(S_{\bar{\eta}})e(\mathbb{P}^1) + e(S_\infty) - e(S_{\bar{\eta}}) + \delta$$

for the fibration $\psi : S \to \mathbb{P}^1$. Here $S_{\bar{\eta}}$ is the geometric generic fiber, S_∞ is the singular fiber, and $\delta = \delta(G, H^1(C, \mathbb{F}_l)$ is the Swan conductor for the G-representation $H^1(C, \mathbb{F}_l)$ for some prime l different from the characteristic p. The curve C has genus $q(q-1)/2$, thus $e(S_{\bar{\eta}}) = e(C) = -q^2+q+2$. According to Proposition 6.2, the singular fiber is a tree of $q^2 + 4$ projective lines, thus $e(S_\sigma) = q^2 + 5$. The Swan conductor is given by $\delta = q^2 - 1$ by 11.4. Substituting these values into the right hand side of Dolgachev's Formula, we obtain $e = q^2 + q + 6$. Since the surface S is rational, we have $b_1 = b_3 = 0$, thus $\rho = b_2 = q^2 + q + 4$.

We may compute this with the Tate–Shioda Formula for the fibration $S \to \mathbb{P}^1$ as well, which gives $\rho = 2 + (c-1) + r$, where c is the number of irreducible components in the singular fiber S_∞, and r is the Mordell–Weil rank, that is, the rank of $\mathrm{Pic}^0(S_\eta)$. We already saw that $c = q^2 + 4$, and $r = q - 1$ by Proposition 13.3, together with Corollary 11.2. Thus this second computation also gives $\rho = q^2 + q + 4$. □

REFERENCES

[1] M. Artin, *On isolated rational singularities of surfaces*, Am. J. Math., 88 (1966), pp. 129–136.

[2] M. Artin, *Wildly ramified $Z/2$ actions in dimension two*, Proc. Amer. Math. Soc., 52 (1975), pp. 60–64.

[3] M. Artin, *Coverings of the rational double points in characteristic p*, in: W. Baily, T. Shioda (eds.), Complex analysis and algebraic geometry, pp. 11–22. Iwanami Shoten, Tokyo, 1977.

[4] M. Aschbacher, *Finite group theory*, Cambridge University Press, Cambridge, 1986.

[5] L. Bădescu, *Algebraic surfaces*, Universitext. Springer-Verlag, New York, 2001.

[6] W. Barth, C. Peters, and A. Van de Ven, *Compact complex surfaces*, Springer, Berlin, 1984.

[7] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergeb. Math. Grenzgebiete (3) 21. Springer, Berlin, 1990.

[8] N. Bourbaki, *Algèbre commutative*, Chapitre 8–9. Masson, Paris, 1983.

[9] P. Berthelot, A. Grothendieck, and L. Illusie (eds.), *Théorie des intersections et théorème de Riemann–Roch (SGA 6)*, Springer, Berlin, 1971.

[10] E. Brieskorn, *Rationale Singularitäten komplexer Flächen*, Invent. Math., 4 (1968), pp. 336–358.

[11] H. Cartan, *Quotient d'un espace analytique par un groupe d'automorphismes*, in: R. Fox (ed.), Algebraic geometry and topology, pp. 90–102. Princeton University Press, Princeton, 1957.

[12] C. Chevalley and A. Weil, *Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers*, Abh. Math. Semin. Univ. Hamb., 10 (1934), pp. 358–361.

[13] D. Cox, J. Little, and H. Schenck, *Toric varieties*, American Mathematical Society, Providence, RI, 2011.

[14] W. Curtis and I. Reiner, *Methods of representation theory*, Vol. I. Wiley, New York, 1990.

[15] S. Cutkosky and H. Srinivasan, *Local fundamental groups of surface singularities in characteristic p*, Comment. Math. Helv., 68 (1993), pp. 319–332.

[16] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes II (SGA 3 Tome 2)*, Springer, Berlin, 1970.

[17] K. Doerk and T. Hawkes, *Finite soluble groups*, de Gruyter, Berlin, 1992.

[18] I. Dolgačev, *The Euler characteristic of a family of algebraic varieties*, Math. USSR-Sb., 18 (1972), pp. 303–319.

[19] G. Ellingsrud and K. Lønsted, *An equivariant Lefschetz formula for finite reductive groups*, Math. Ann., 251 (1980), pp. 253–261.

[20] G. Ellingsrud and T. Skjelbred, *Profondeur d'anneaux d'invariants en caractristique p*, Compositio Math., 41 (1980), pp. 233–244.

[21] R. Fossum and P. Griffith, *Complete local factorial rings which are not Cohen-Macaulay in characteristic p*, Ann. Sci. École Norm. Sup., 8 (1975), pp. 189–199.

[22] J. Giraud, *Cohomologie non abélienne*, Grundlehren Math. Wiss. 179. Springer, Berlin, 1971.

[23] G.-M. Greuel and H. Kröning, *Simple singularities in positive characteristic*, Math. Z., 203 (1990), pp. 339–354.

[24] P. Grillet, *Commutative semigroups*, Kluwer Academic Publishers, Dordrecht, 2001.

[25] A. Grothendieck, *Éléments de géométrie algébrique IV: Étude locale des schémas et des morphismes de schémas*, Publ. Math., Inst. Hautes Étud. Sci., 24 (1965).

[26] A. Grothendieck, *Éléments de géométrie algébrique IV: Étude locale des schémas et des morphismes de schémas*, Publ. Math., Inst. Hautes Étud. Sci., 32 (1967).

[27] A. Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Springer, Berlin, 1971.

[28] A. Grothendieck, *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux (SGA 2)*, North-Holland Publishing Company, Amsterdam, 1968.

[29] M. Isaacs, *Character theory of finite groups*, Academic Press, New York-London, 1976.

[30] H. Ito and S. Schröer, *Wildly Ramified Actions and Surfaces of General Type Arising from Artin–Schreier Curves*, in C. Faber, G. Farkas, R. de Jong (eds.), Geometry and Arithmetic, pp. 213–241. Eur. Math. Soc., Zürich, 2012.

[31] G. James and M. Liebeck, *Representations and characters of groups*, Cambridge University Press, New York, 2001.

[32] K. Kato, *Logarithmic structures of Fontaine-Illusie*, in: J.-I. Igusa (ed.) et. al., Algebraic analysis, geometry, and number theory, pp. 191–224. Johns Hopkins Univ. Pr., Baltimore, 1989.

[33] K. Kato, *Toric singularities*, Amer. J. Math., 116 (1994), pp. 1073–1099.

[34] T. Katsura, *On Kummer surfaces in characteristic* 2, in: M. Nagata (ed.), Proceedings of the international symposium on algebraic geometry, pp. 525–542. Kinokuniya Book Store, Tokyo, 1978.

[35] G. Kempf, F. Knudsen, D. Mumford, and B. Saint-Donat, *Toroidal embeddings I*, Lect. Notes Math. 339. Springer, Berlin, 1973.

[36] B. Köck, *Computing the equivariant Euler characteristic of Zariski and étale sheaves on curves*, Homology, Homotopy Appl., 7 (2005), pp. 83–98.

[37] W. Lang, *Extremal rational elliptic surfaces in characteristic p. II. Surfaces with three or fewer singular fibres*, Ark. Mat., 32 (1994), pp. 423–448.

[38] J. Lipman, *Desingularization of two-dimensional schemes*, Ann. Math., 107 (1978), pp. 151–207.

[39] D. Lorenzini, *Wild quotient singularities of surfaces*, Math. Z., 275 (2013), pp. 211-232.

[40] D. Lorenzini, *Wild models of curves*, Algebra Number Theory, 8 (2014), pp. 331–367.

[41] D. Lorenzini, *Wild quotients of products of curves*, preprint, `http://www.math.uga.edu/~lorenz/paper.html`.

[42] D. Lorenzini, *Questions on wild* $\mathbb{Z}/p\mathbb{Z}$*-quotient singularities in dimension 2*, preprint, `http://www.math.uga.edu/~lorenz/paper.html`.

[43] I. Macdonald, *The theory of groups*, Clarendon Press, Oxford, 1968.

[44] J. Milne, *Étale cohomology*, Princeton Mathematical Series, 33. Princeton University Press, Princeton, 1980.

[45] A. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math., 89 (1967), pp. 1–21.

[46] A. Ogus, *Lectures on Logarithmic Algebraic Geometry*, manuscript. `http://math.berkeley.edu/~ogus/`

[47] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math., 457 (1994), pp. 185–188.

[48] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1978.

[49] T. Shioda, *Kummer surfaces in characteristic* 2, Proc. Japan Acad., 50 (1974), pp. 718–722.

[50] T. Shioda, *Arithmetic and geometry of Fermat curves*, in: M. Nagata, T. Peng: Algebraic Geometry Seminar, pp. 95–102. World Sci. Publishing, Singapore, 1988.

[51] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts Math. 151. Springer, New York etc., 1994.

[52] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, I*, Arch. Math., 24 (1973), pp. 527–544.

[53] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, II*, Arch. Math., 24 (1973), pp. 615–631.

[54] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in: B. Birch, W. Kuyk (eds.), Modular functions of one variable IV, pp. 33–52. Lecture Notes in Math. 476. Springer, Berlin, 1975.

[55] N. Yui, *The arithmetic of the product of two algebraic curves over a finite field*, J. Algebra, 98 (1986), pp. 102–142. Erratum: 98 (1986), pp. 102–142.