ISSN 0081-5438, Proceedings of the Steklov Institute of Mathematics, 2019, Vol. 307, pp. 245–266. © Pleiades Publishing, Ltd., 2019.
Published in Russian in Trudy Matematicheskogo Instituta imeni V.A. Steklova, 2019, Vol. 307, pp. 267–290.

The Tate–Oort Group Scheme $\mathbb{TO}_p$

Miles Reid[a]

Received May 25, 2019; revised June 27, 2019; accepted November 25, 2019

In memory of Igor Rostislavovich Shafarevich,
from whom we have all learned so much

Abstract—Over an algebraically closed field of characteristic p, there are three group schemes of order p, namely the ordinary cyclic group $\mathbb{Z}/p$, the multiplicative group $\boldsymbol{\mu}_p \subset \mathbb{G}_{\mathrm{m}}$ and the additive group $\boldsymbol{\alpha}_p \subset \mathbb{G}_{\mathrm{a}}$. The Tate–Oort group scheme $\mathbb{TO}_p$ puts these into one happy family, together with the cyclic group of order p in characteristic zero. This paper studies a simplified form of $\mathbb{TO}_p$, focusing on its representation theory and basic applications in geometry. A final section describes more substantial applications to varieties having p-torsion in Pic^τ, notably the 5-torsion Godeaux surfaces and Calabi–Yau threefolds obtained from $\mathbb{TO}_5$-invariant quintics.

DOI: 10.1134/S0081543819060154

1. INTRODUCTION

The Tate–Oort group scheme aims to extend what we know about the usual cyclic group of order p and its representation theory to work over a field of characteristic p, and in mixed characteristic. It exists in several forms, split and nonsplit.

This paper concentrates on an easy version that I call t-split. (See Subsection 6.3 for the nonsplit form.) As an oversimplified slogan,

- $\mathbb{TO}_p$ is a group scheme over the base ring $B = \mathbb{Z}[S,t]/(P)$, where $P = St^{p-1} + p$;
- its underlying scheme is the closed subscheme $\mathbb{TO}_p \subset \mathbb{A}^1_B$ defined by $x^p - Sf_p(t,x)$, where f_p is set up in order that the congruence $(1+tx)^p \equiv 1$ holds modulo the ideal (P,F) (see Subsection 3.2 for the specific formula);
- its group law $G \times G \to G$ is
$$(y,z) \mapsto x = y + z + tyz \tag{1.1}$$
where $y = x \otimes 1$ and $z = 1 \otimes x$ are coordinates on the two factors (see the discussion below). The details and the main properties are discussed in Subsection 3.2.

The main feature of this definition is that the coordinate ring $A = B[\mathbb{TO}_p]$ contains the function $\tau = 1 + tx$ with $\tau^p = 1$. Thus when t is invertible, $\mathbb{TO}_p$ has p distinct characters τ^i for $i = 0, \dots, p-1$, and one-dimensional representations $\frac{1}{p}(i)$ on which $\mathbb{TO}_p[1/t]$ acts by multiplication by τ^i (cf. Lemma 2.1). Thus its representation theory is reductive: every representation splits into eigenspaces as $\frac{1}{p}(a_1, \dots, a_m)$, exactly as representations of $\boldsymbol{\mu}_p$ over $\mathbb{C}$. This is what I mean by t-split.

1.1. Background. Three different group schemes of order p in characteristic p play the same role as the cyclic group $\mathbb{Z}/p$ in characteristic 0. These are

- $\mathbb{F}_p^+$ defined by $x^p = x$ with the group operation $(y,z) \mapsto y + z$;
- $\boldsymbol{\alpha}_p$ defined by $x^p = 0$ with $(y,z) \mapsto y + z$;
- $\boldsymbol{\mu}_p$ defined by $x^p = 1$ with $(y,z) \mapsto yz$.

[a] Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK.
E-mail address: Miles.Reid@warwick.ac.uk

In each case, the underlying scheme is a hypersurface in the affine x-line $\mathbb{A}^1_{\langle x\rangle}$ defined by a monic equation, and the group law is the restriction of a polynomial map $\mathbb{A}^1 \times_k \mathbb{A}^1 \to \mathbb{A}^1$, where y, z denote coordinates on the two factors.[1] The induced k-algebra homomorphism on the coordinate ring $A = B[\mathbb{TO}_p]$ is traditionally described as a Hopf algebra (or bigebra) structure $A \to A \otimes_k A$ on the coordinate ring A, given by $x \mapsto x \otimes 1 + 1 \otimes x$ in the two additive cases or $x \mapsto x \otimes x$ in the case of $\boldsymbol{\mu}_p$, but for the present this obscures rather than enlightens; I prefer to write $y = x \otimes 1$ and $z = 1 \otimes x$. The bigebra comes into its own in the discussion of Cartier duality in Section 4.

The Tate–Oort group scheme $\mathbb{TO}_p$ puts these three together as a deformation family. By the above description, as a hypersurface defined by a monic equation, its coordinate ring $A = B[\mathbb{TO}_p]$ is free over B with basis $\{1, \dots, x^{p-1}\}$. When $S \neq 0$, the polynomial $x^p - Sf_p$ is separable in x, so $\mathbb{TO}_p[1/S]$ is etale over B, and is a *form* of $\mathbb{Z}/p$. When $t \neq 0$, I can rewrite (1.1) as $(y,z) \mapsto ((1+ty)(1+tz)-1)/t$, which makes $\mathbb{TO}_p[1/t]$ isomorphic to $\boldsymbol{\mu}_p$ under $x \mapsto 1 + tx$. The fibre of $\mathbb{TO}_p$ over the point $p = S = t = 0$ is $\boldsymbol{\alpha}_p$.

The regular representation of a finite group scheme is its coordinate ring. In this case, the coordinate ring $A = B[\mathbb{TO}_p]$ has basis $\{1, x, \dots, x^{p-1}\}$, so the regular representation of $\mathbb{TO}_p$ is the $(p-1)$th symmetric power of the two-dimensional representation $\{1, x\}$. The affine space $\mathbb{A}^p$ corresponding to the regular representation, or its projectivisation $\mathbb{P}^{p-1}$, serves as an ambient space for $\mathbb{TO}_p$-equivariant varieties. $\mathbb{TO}_p$-invariant ideals of polynomial functions on $\mathbb{A}^p$ lead to nonsingular projective algebraic varieties of interest. The 5-torsion Godeaux surfaces of [5] (see also Subsection 6.1.1 and [10]) serve as a guiding case.

1.2. Philosophical principle. Wherever you see a $\mathbb{Z}/p$ symmetry or a $\boldsymbol{\mu}_p$ action over $\mathbb{C}$, you should expect to see $\mathbb{Z}/p$, $\boldsymbol{\mu}_p$ and $\boldsymbol{\alpha}_p$ in characteristic p, and $\mathbb{TO}_p$ in mixed characteristic. In characteristic p, it is a mistake to view an inseparable field extension or a geometric quotient by a nonreduced group scheme (containing $\boldsymbol{\mu}_p$ or $\boldsymbol{\alpha}_p$) as pathological, while viewing a separable Galois extension or an etale cover of degree divisible by p as virtuous. A $\mathbb{Z}/p$ Galois extension is Artin–Schreier, which is as pathological as it gets: wild ramification gives curves of arbitrary genus as etale covers of $\mathbb{A}^1$, and makes basic techniques such as counting Hurwitz numbers useless. By contrast, the group scheme $\boldsymbol{\mu}_p$ is reductive, and quotients of linear spaces by $\boldsymbol{\mu}_p$ are just toric varieties. In calculations such as those of Section 5, $\boldsymbol{\alpha}_p$ is in many ways the easiest of all to work with.

There is a rich theory of inseparable field extensions (see, for example, [4]), but it rarely makes it to the surface in introductory courses, which commonly define inseparable extensions only to get rid of them.

1.2.1. *Website.* This paper is accompanied by the website [10]. This includes links to more advanced applications, and computer files illustrating many of the calculations of the paper. Except possibly for some of the proofs of nonsingularity, no deep or large-scale computation is involved, just hundreds of experiments and sanity checks without which the paper would not be viable. My computer work is written in Magma [2], and everything here works instantly in the free online calculator [7].

2. HYBRID ADDITIVE–MULTIPLICATIVE GROUP

2.1. The algebraic group $\mathbb{G}$. For any base ring B and $t \in B$, write $\mathbb{G} = \operatorname{Spec} A$, where $A = B[x, 1/(1+tx)]$. That is, x is the coordinate on the affine line $\mathbb{A}^1_B$ over B, and $\mathbb{G}$ is the standard open subscheme $(1 + tx \neq 0) \subset \mathbb{A}^1_B$. Then (1.1) defines the structure of an affine group scheme on $\mathbb{G}$, with unit element $x = 0$ and inverse $x \mapsto -x/(1+tx)$. This is a hybrid of the multiplicative group $\mathbb{G}_\mathrm{m}$ and the additive group $\mathbb{G}_\mathrm{a}$: over the open set $\operatorname{Spec} B[1/t]$ where t is invertible, it is

[1] In the language of SGA 3, (1.1) can be viewed as a map of functors taking any two S-valued points $y, z \in \mathbb{TO}_p[S]$ to $y + z + tyz \in \mathbb{TO}_p[S]$.

isomorphic to $\mathbb{G}_\mathrm{m}$ under $x \mapsto 1+tx$, and over the closed subscheme $V(t) = \operatorname{Spec}(B/t)$ where $t=0$, it is isomorphic to $\mathbb{G}_\mathrm{a}$.

View $\mathbb{G}_{B,t}$ as the subgroupscheme

$$\mathbb{G}_{B,t} := \left\{ \begin{pmatrix} 1 & 0 \\ x & 1+tx \end{pmatrix} \right\} \subset \operatorname{Aff}(1,B) \subset \operatorname{GL}(2,B) \tag{2.1}$$

of the affine group $\operatorname{Aff}(1,B)$. The matrix form (2.1) writes the group law (1.1) in the form

$$(1+ty, 1+tz) \mapsto (1+ty)(1+tz), \tag{2.2}$$

while specifying how to cancel t top and bottom in $(y,z) \mapsto ((1+ty)(1+tz)-1)/t$, even where $t=0$. This gives the unchanging (1.1). It follows that the matrices (2.1) commute, and that the bth power map in $\mathbb{G}_{B,t}$ is given by

$$x \mapsto \frac{(1+tx)^b - 1}{t} = \sum_{i=1}^{b} \binom{b}{i} t^{i-1} x^i = t^{b-1}x^b + \ldots + bx \tag{2.3}$$

for any $b \geq 1$.

2.2. The given representation $(B^{\oplus 2})^\vee$ of $\mathbb{G}$. Formula (2.1) defines an action of $\mathbb{G}$ on $\mathbb{A}^1$, and on the space $B^{\oplus 2}$ of inhomogeneous linear forms on it. The notation hides two ambiguities. To cure the first, let x be the usual coordinate of $\mathbb{G} = \operatorname{Spec} B[x, 1/(1+tx)]$ and y the linear coordinate on $\mathbb{A}^1$. Then the action $\mathbb{G} \times_B \mathbb{A}^1 \to \mathbb{A}^1$ is the polynomial map $m\colon (x,y) \mapsto x+y+txy$. On the level of coordinate rings, it corresponds to the B-algebra homomorphism $m^*\colon B[y] \to B[x,y]$ sending $y \mapsto x+y+txy$.

The second issue is that I want the action of $\mathbb{G}$ on the affine space $\mathbb{A}^2_B$ of inhomogeneous linear forms on $\mathbb{A}^1$, the dual of that expressed by the matrix in (2.1). Write $B^{\oplus 2}$ for the free module $B \cdot 1 \oplus B \cdot y$ of linear forms, and let w_0, w_1 be the dual basis of $(B^{\oplus 2})^\vee$, so that the affine space $\mathbb{A}^2_B$ of inhomogeneous linear forms is $\operatorname{Spec} B[w_0, w_1]$. Then the action of $\mathbb{G}$ on $(B^{\oplus 2})^\vee$ is given by right multiplication $(w_0, w_1) \mapsto (w_0, w_1)\left(\begin{smallmatrix} 1 & 0 \\ x & 1+tx \end{smallmatrix}\right)$ by the matrix of (2.1), that is, the polynomial map

$$\mathbb{A}^2_B \times_B \mathbb{G} \to \mathbb{A}^2_B \qquad \text{given by} \quad \begin{cases} w_0 \mapsto w_0 + xw_1, \\ w_1 \mapsto (1+tx)w_1. \end{cases} \tag{2.4}$$

2.3. Symmetric power $U_d = \operatorname{Sym}^d((B^{\oplus 2})^\vee)$. The next Section 3 treats the t-split Tate–Oort group $\mathbb{TO}_p$ as a subgroupscheme of the hybrid group $\mathbb{G}$; the representations I need invariably come by restricting representations of the algebraic group $\mathbb{G}$. To prepare for this, I treat the dth symmetric power of the given representation of $\mathbb{G}$, that is, the affine space $\mathbb{A}^{d+1}$ of forms of degree d. With w_0, w_1 as above, the dth symmetric power of $(B^{\oplus 2})^\vee$ is based by $\{u_0, u_1, \ldots, u_d\}$, corresponding to $\operatorname{Sym}^d(w_0, w_1) = \{w_0^d, w_0^{d-1}w_1, \ldots, w_1^d\}$, the dual basis to $\{1, x, \ldots x^d\}$. Its $\mathbb{G}$ action is defined by right multiplication $(u_0, u_1, \ldots, u_d) \mapsto (u_0, u_1, \ldots, u_d)M$ where

$$M = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ x & 1+tx & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ x^d & dx^{d-1}(1+tx) & \binom{d}{2}x^{d-2}(1+tx)^2 & \ldots & (1+tx)^d \end{pmatrix}, \tag{2.5}$$

with entries $m_{ij} = \binom{i}{j} x^{i-j}(1+tx)^j$ if $i \geq j$, or 0 if $j > i$.

One strategy in subsequent calculations involves reducing to the case t invertible, where the representation theory of $\mathbb{TO}_p$ is reductive, and every representation splits into one-dimensional eigenspaces. The following observation plays a key role in this.

Lemma 2.1. (i) *The matrix M has $d+1$ eigenvalues $(1+tx)^k$ for $k=0,\dots,d$.*

(ii) *Write*

$$v_0 = u_0, \qquad v_1 = u_0 + tu_1, \qquad v_2 = u_0 + 2tu_1 + t^2u_2, \qquad \dots \tag{2.6}$$

or, more formally,

$$v_k = \sum_{i=0}^{k} \binom{k}{i} t^i u_i = u_0 + ktu_1 + \binom{k}{2} t^2 u_2 + \ldots + kt^{k-1}u_{k-1} + t^k u_k. \tag{2.7}$$

That is, $v_k = \bigl(1, kt, \binom{k}{2}t^2, \dots \binom{k}{i}t^i, \dots, t^k, 0, \dots, 0\bigr)$, with entries the terms in the binomial expansion of $(1+t)^k$. Then v_k is an eigenvector with eigenvalue $(1+tx)^k$, or $v_kM = (1+tx)^k v_k$.

(iii) *Where t is invertible, the v_k for $k=0,1,\dots,d$ form an eigenbasis of U_d. Moreover, relations (2.7) can be inverted to give the lower triangular basis $\{u_i\}$ in terms of the eigenbasis $\{v_i\}$:*

$$u_0 = v_0, \qquad u_1 = \frac{-v_0+v_1}{t}, \qquad u_2 = \frac{v_0 - 2v_1 + v_2}{t^2}, \qquad \dots, \tag{2.8}$$

or systematically

$$u_k = \frac{1}{t^k}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i} v_i = \frac{(-1)^k v_0 + (-1)^{k-1}kv_1 + \ldots - kv_{k-1} + v_k}{t^k}. \tag{2.9}$$

Proof. (i) Subtracting $(1+tx)^k$ times the identity matrix from M leaves a matrix with a $k\times(d+1-k)$ block of zeros, which is clearly singular, so that $(1+tx)^k$ is an eigenvalue.

(ii) To understand the eigenvector identities, write out the cases $d=2,3,\dots$ by hand. For example,

$$(1, 2t, t^2)\cdot\begin{pmatrix} 1 & 0 & 0 \\ x & 1+tx & 0 \\ x^2 & 2x(1+tx) & (1+tx)^2 \end{pmatrix} = (1+tx)^2\cdot(1,2t,t^2). \tag{2.10}$$

More formally, v_k has ith entry $\binom{k}{i}t^i$ or 0, and $m_{ij} = \binom{i}{j}x^{i-j}(1+tx)^j$ or 0. Therefore, the jth entry of the vector v_kM equals $\sum_{i=j}^{k}\binom{k}{i}t^i\binom{i}{j}x^{i-j}(1+tx)^j$. Fix j and replace the sum over i by a sum over $l=i-j$ to get

$$\sum_{i=j}^{k}\binom{k}{i}t^i\binom{i}{j}x^{i-j}(1+tx)^j = (1+tx)^j t^j \sum_{l=0}^{k-j}\binom{k}{j+l}\binom{j+l}{j}t^l x^l. \tag{2.11}$$

Now the binomial coefficient identity

$$\binom{k}{j+l}\binom{j+l}{j} = \frac{k!}{(k-j-l)!\,(j+l)!}\,\frac{(j+l)!}{j!\,l!} = \frac{k!}{(k-j)!\,j!}\,\frac{(k-j)!}{(k-j-l)!\,l!} = \binom{k}{j}\binom{k-j}{l} \tag{2.12}$$

transforms the right-hand side to

$$(1+tx)^j t^j \sum_{l=0}^{k-j}\binom{k}{j}\binom{k-j}{l}t^l x^l = (1+tx)^k\binom{k}{j}t^j. \tag{2.13}$$

This proves (ii).

Assertion (iii) is the matrix identity

$$\begin{pmatrix} 1 & 0 & 0 & \dots \\ 1 & t & 0 & \dots \\ 1 & 2t & t^2 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & \dots \\ -1/t & 1/t & 0 & \dots \\ 1/t^2 & -2/t^2 & 1/t^2 & \dots \\ -1/t^3 & 3/t^3 & -3/t^3 & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} = I_{d+1}, \tag{2.14}$$

which is proved similarly. $\square$

Other associated representations of $\mathbb{G}$ usually have lower triangular bases and eigenbases where t is invertible, which are related in a similar way.

3. CONSTRUCTION OF $\mathbb{TO}_p$

3.1. Group $\overline{\mathbb{TO}}_p$ in characteristic p. The hybrid group $\mathbb{G}$ puts $\mathbb{G}_\mathrm{m}$ and $\mathbb{G}_\mathrm{a}$ in one family. The first step towards linking the three characteristic p group schemes $\mathbb{Z}/p$, $\boldsymbol{\mu}_p$ and $\boldsymbol{\alpha}_p$ as one family is to work over the base ring $\overline{B} = \mathbb{F}_p[S,t]/(St)$ or its Spec, the line pair $\operatorname{Spec}\overline{B}\colon (St=0) \subset \mathbb{A}^2_{\mathbb{F}_p}$.

The construction uses the parameter $S \in \overline{B}$ to choose a p-torsion subgroupscheme of $\mathbb{G}_{\overline{B},t}$. Set $\overline{\mathbb{TO}}_p\colon (x^p = Sx) \subset \mathbb{G}_{\overline{B},t}$. Using the identity $(a+b)^p = a^p + b^p$ and relations (2.2) and (2.3) of Subsection 2.1 gives

$$\begin{pmatrix} 1 & 0 \\ x & 1+tx \end{pmatrix}^p = \begin{pmatrix} 1 & 0 \\ t^{p-1}x^p & 1+t^p x^p \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1+t^p x^p \end{pmatrix}. \tag{3.1}$$

In the second equality, $t^{p-1}x^p = 0$ comes from $x^p = Sx$ and $St = 0 \in \overline{B}$.

Proposition 3.1. *The closed subscheme $\overline{\mathbb{TO}}_p = (x^p - Sx) \subset \mathbb{G}_{\overline{B},t}$ is a subgroupscheme. It has the following properties*:

(i) *$\overline{\mathbb{TO}}_p$ is the hypersurface in $\mathbb{A}^1_{\overline{B},\langle x\rangle}$ over* $\operatorname{Spec}\overline{B} = (St=0) \subset \mathbb{A}^2_{\mathbb{F}_p}$ *defined by $x^p = Sx$*;

(ii) *its coordinate ring is free of rank p over $\overline{B}$ with basis $1, x, \dots, x^{p-1}$*;

(iii) *where S is invertible, $\overline{\mathbb{TO}}_p$ is etale over $\overline{B}$; it becomes isomorphic to the additive group $\mathbb{F}_p^+ = \mathbb{Z}/p$ on pulling back by $S = s^{p-1}$*;

(iv) *where t is invertible, $\overline{\mathbb{TO}}_p$ is isomorphic to the multiplicative group scheme $\boldsymbol{\mu}_p$*;

(v) *where $S = t = 0$, it is $\boldsymbol{\alpha}_p$.*

Proof. The only thing requiring proof is

$$(y+z+tyz)^p - S(y+z+tyz) \in \operatorname{Ideal}(y^p - Sy, z^p - Sz). \tag{3.2}$$

In fact, it is

$$(y^p - Sy) + (z^p - Sz) + t^p z^p (y^p - Sy) + St(t^{p-1}yz^p - yz). \tag{3.3}$$

The point of (iii) is that if I set $S = s^{p-1}$, the equation of $\overline{\mathbb{TO}}_p$ splits into linear factors

$$x^p - s^{p-1}x = \prod_{a\in\mathbb{F}_p^+} (x - as), \tag{3.4}$$

so the pulled-back group becomes $\mathbb{F}_p^+$ where s is invertible. However, without $s = \sqrt[p-1]{S}$, the $p-1$ generators of $\mathbb{F}_p^+ \cong \mathbb{Z}/p$ are Galois conjugate over $\overline{B}$, and the coordinate x of $\mathbb{A}^1$ cannot distinguish them, so $\overline{\mathbb{TO}}_p[1/S]$ is a *nonsplit* form of $\mathbb{Z}/p$. $\square$

3.2. Group $\mathbb{TO}_p$ in mixed characteristic. In this step p is a prime integer, and the base ring is

$$B = \mathbb{Z}[S,t]/(P), \qquad \text{where} \quad P = St^{p-1} + p. \tag{3.5}$$

I can view this as $B = \mathbb{Z}[t, p/t^{p-1}] \subset \mathbb{Z}[t, t^{-1}] \subset \mathbb{Q}(t)$, so it is an integral domain. It turns out that I can still construct $\mathbb{TO}_p$ as a subgroupscheme of the p-torsion of the algebraic group $\mathbb{G}_{B,t}$.

The intermediate binomial coefficients $\binom{p}{i}$ for $i = 1, \dots, p-1$ are divisible by p; set[2]

$$f_p(t,x) = \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} t^{i-1} x^i = \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} t^{i-1} x^i = \frac{(1+tx)^p - 1 - t^p x^p}{pt}. \tag{3.6}$$

Thus (3.6) cancels a factor of p and of t, even where they are zero. I take

$$F = x^p - S f_p(t,x) \tag{3.7}$$

as the equation of $\mathbb{TO}_p \subset \mathbb{G}_{B,t}$. For example,

$$\begin{aligned} p = 2&: \quad F = x^2 - Sx, \\ p = 3&: \quad F = x^3 - S(tx^2 + x), \\ p = 5&: \quad F = x^5 - S(t^3x^4 + 2t^2x^3 + 2tx^2 + x), \\ p = 7&: \quad F = x^7 - S(t^5x^6 + 3t^4x^5 + 5t^3x^4 + 5t^2x^3 + 3tx^2 + x). \end{aligned} \tag{3.8}$$

Lemma 3.2 verifies that (3.7) defines a group subscheme $\mathbb{TO}_p \subset \mathbb{G}_{B,t}$ with the unwavering group law (1.1). Equation (3.7) has the following key properties:

(i) it is monic of degree p in x;

(ii) the linear term in x is $-Sx$, and all the intermediate terms are divisible by t.

The base is stratified according to which of S and t are invertible or zero. Where S is invertible, F in (3.7) is separable in x, so that $\mathbb{TO}_p[1/S]$ is etale and finite over the base, and is therefore a form of $\mathbb{Z}/p$. Where t is invertible, $\mathbb{TO}_p[1/t]$ is isomorphic under $x \mapsto 1 + tx$ to the subgroupscheme $\boldsymbol{\mu}_p \subset \mathbb{G}_\mathrm{m}$. Where S and t are both zero, $\mathbb{TO}_p$ is isomorphic to $\boldsymbol{\alpha}_p \subset \mathbb{G}_\mathrm{a}$.

Lemma 3.2. (i) $(1+tx)^p - 1 \equiv t^p F \bmod P$.

(ii) *Let x_1 and x_2 be indeterminates, and set $x_3 = x_1 + x_2 + tx_1x_2$. Then $x_3^p - S f_p(x_3, t)$ belongs to the ideal*

$$\bigl(x_1^p - S f_p(x_1,t),\, x_2^p - S f_p(x_2,t),\, P\bigr) \subset \mathbb{Z}[x_1, x_2, S, t]. \tag{3.9}$$

Proof. (i) In view of (3.6), (3.7) and (3.5), I get

$$(1+tx)^p - 1 = t^p x^p + pt f_p(x,t) = t^p F + t f_p(t,x) P. \tag{3.10}$$

(ii) Since $1 + tx_3 = (1+tx_1)(1+tx_2)$, I get the identities

$$(1+tx_3)^p - 1 \equiv (1+tx_1)^p(1+tx_2)^p - 1 \equiv A((1+tx_1)^p - 1) + B((1+tx_2)^p - 1), \tag{3.11}$$

with (say) $A = (1+tx_2)^p$ and $B = 1$. The argument of (3.10) gives

$$(1+tx_i)^p - 1 \equiv t^p(x_i^p - S f_p(t, x_i)) \bmod P \qquad \text{for} \quad i = 1,2,3 \tag{3.12}$$

[2]The polynomials $f_p(t) = ((1+t)^p - 1 - t^p)/(pt)$ have some pedigree: they go back to Cauchy and Liouville in the context of Fermat's last theorem. For p prime, f_p has the trivial factor $(1+t)(1+t+t^2)$ if $p \equiv 5$ or $(1+t)(1+t+t^2)^2$ if $p \equiv 1 \bmod 6$; the nontrivial factor, the Cauchy–Mirimanoff polynomial, is conjectured or known to be irreducible (cf. [8, 9]). I am indebted to John Cremona and Marc Masdeu for these references.

as equalities in $\mathbb{Z}[x_1, x_2, S, t]/(P)$. Apply (3.12) to the three terms in (3.11) to get

$$t^p(x_3^p - Sf_p(t, x_3)) \equiv t^p A(x_1^p - Sf_p(t, x_1)) + t^p B(x_2^p - Sf_p(t, x_2)) \qquad (3.13)$$

modulo P. Now $\mathbb{Z}[x_1, x_2, S, t]/(P) = B[x_1, x_2]$ is an integral domain, so the factor t^p cancels. $\square$

3.3. Representation theory of $\mathbb{TO}_p$. The regular representation of $\mathbb{TO}_p$ is its action on its own coordinate ring $A[\mathbb{TO}_p] = B[x]/(F)$. Since F is monic of degree p, this gives rise to the affine space $\mathbb{A}^p = \operatorname{Spec} B[U]$ or projective space $\mathbb{P}^{p-1} = \operatorname{Proj} B[U]$ corresponding to the $(p-1)$th symmetric power $U = \operatorname{Sym}^{p-1}((B^{\oplus}2)^\vee)$ of the dual of the given representation.

As discussed in Subsection 2.3, U is the free B-module based by $\{u_0, \dots, u_{p-1}\}$, with the $\mathbb{TO}_p$ action given by $\underline{u} \mapsto \underline{u}M$, with M the lower triangular matrix (2.5). Over $B[1/t]$, it has the eigenbasis $\{v_0, \dots, v_{p-1}\}$ of Lemma 2.1.

To define ideals of $\mathbb{TO}_p$-invariant subschemes of $\mathbb{P}^{p-1}$ (such as the quintic hypersurfaces in $\mathbb{P}^3$ or $\mathbb{P}^4$ for the 5-torsion Godeaux surfaces or threefolds discussed in Subsection 6.1.1), I need other representations of $\mathbb{TO}_p$, usually arising as associated representations of U. Notably, symmetric powers $\operatorname{Sym}^k(U)$, exterior powers $\bigwedge^2 U$, or more complicated cases such as $\operatorname{Sym}^l(\operatorname{Sym}^k(U))$ or $U \otimes \bigwedge^2 U$. These usually also have lower triangular bases over B, and eigenbases over $B[1/t]$. Passing between the two eventually becomes harder than Lemma 2.1, with calculations involving the relations $P = St^{p-1} + p$ and $F = x^p - f_p(t, x)$ defining $B = \mathbb{Z}[S, t]/(P)$ and $B[\mathbb{TO}_p] = B[x]/(F)$ (see Section 5 for a trailer).

4. THE CARTIER DUAL $(\mathbb{TO}_p)^\vee$

4.1. Cartier duality. The t-split Tate–Oort group $\mathbb{TO}_p$ has base ring $B = \mathbb{Z}[S, t]/(P)$, where $P = St^{p-1} + p$. Its coordinate ring $A = B[x]/(F)$ (with F as in (3.7)) is a B-bigebra: it is a commutative algebra, with Hopf algebra structure induced by the never varying group structure (1.1).

Cartier duality corresponds philosophically to Pontryagin duality between the additive group $\mathbb{Z}/n$ and the multiplicative group $\boldsymbol{\mu}_n \subset \mathbb{C}^\times$ (or a finite Abelian group A and its character group $\widehat{A} = \operatorname{Hom}(A, \mathbb{C}^\times)$). It is based on the observation that for a finite commutative group scheme $G = \operatorname{Spec} A$ with coordinate ring A, the axioms satisfied by its algebra multiplication $\alpha\colon A \otimes A \to A$ and its symmetric Hopf algebra structure $\gamma\colon A \to A \otimes A$ (induced on coordinate rings by the group law $G \times G \to G$) are precisely dual to one another. Interchanging the two determines the Cartier dual group scheme $G^\vee$.

Remark 4.1. For a finite commutative group scheme G and a scheme X (all over a base B), morphisms $G \to \operatorname{Pic} X$ correspond one-to-one to $G^\vee$-torsors $Y \to X$. This generalises the traditional $\boldsymbol{\mu}_n$ etale cover for a subgroup $\mathbb{Z}/n \subset \operatorname{Pic}^0 X$, and is a key point motivating my construction (although not really essential for the proofs), so I give a brief sketch.

Given $\sigma\colon G \to \operatorname{Pic} X$, the $G^\vee$-torsor $Y \to X$ comes from the Poincaré line bundle $\mathcal{L}$ on $X \times_B \operatorname{Pic} X$: pull $\mathcal{L}$ back to a line bundle $\sigma^*(\mathcal{L})$ on $G \times_B X$, and then push down to a sheaf $\mathcal{A} = \pi_{X*}(\sigma^*(\mathcal{L}))$ of $\mathcal{O}_X$-modules. Then $\mathcal{A}$ can be made into an $\mathcal{O}_X$-algebra via the group multiplication $G \times G \to G$. Also, $\mathcal{A}$ is Zariski locally free of rank 1 as an $\mathcal{O}_X[G]$-module. Then $Y = \operatorname{Spec}_X \mathcal{A}$ is the $G^\vee$-torsor corresponding to σ.

Alternatively, in the language of SGA 3, G is defined as a functor that takes a B-scheme S to a finite commutative group $G(S)$. The Cartier dual $G^\vee$ is then the functor that takes S to the character group $\operatorname{Hom}(G(S), \mathbb{G}_{\mathrm{m},B})$ (this is discussed in [12, (2.10)]). A morphism $G \to \operatorname{Pic} X = H^1(X, \mathcal{O}_X^\times)$ defines a class in $H^1(X, G^\vee)$ (in the Zariski topology), which is the group of $G^\vee$-torsors.

Cartier duality swaps additive and multiplicative structures in the same way as Pontryagin duality. It also interchanges the effect of t-splitting and S-nonsplitting. I explain: $\mathbb{TO}_p[1/t]$ is reductive, with p eigenvalues $(1 + tx)^k$ or one-dimensional representations, as in Lemma 2.1; and

$\mathbb{TO}_p[1/S]$ is a form of $\mathbb{Z}/p$ whose nonzero points form an irreducible scheme (that is, they are all conjugate over B, as in Proposition 3.1(iii)).

The opposite holds for the Cartier dual: $(\mathbb{TO}_p)^\vee[1/t]$ is the split cyclic group $\mathbb{Z}/p$ (see Theorem 4.3 below), so its underlying scheme has p irreducible components; and $(\mathbb{TO}_p)^\vee[1/S]$, while reductive, has only the trivial one-dimensional representation and an irreducible $(p-1)$-dimensional representation, which only splits into eigenspaces after a cyclic Galois extension of order $p-1$.

4.2. Notation. In my case, A is a free B-module, based by x^i for $i=0,\dots,p-1$. Write $A^\vee$ for the dual B-module, with dual basis $u_0,\dots,u_{p-1}$. The Hopf algebra structure of (1.1) is the B-algebra homomorphism $\gamma\colon A\to A\otimes A$ defined by

$$x\mapsto y+z+tyz=x\otimes 1+1\otimes x+tx\otimes x. \tag{4.1}$$

The dual of γ defines a B-module homomorphism $\beta\colon A^\vee\otimes A^\vee\to A^\vee$, making $A^\vee$ into a commutative B-algebra. Theorem 4.3 calculates the practical effect of taking the dual; allowing denominators dividing $(p-1)!$ gives the multiplicative structure of the algebra $A^\vee$ in a pleasing form. This treatment does not involve the relation F, so it could be viewed in terms of the algebraic group $\mathbb{G}_{B,t}$ of Section 2.

The Cartier dual group scheme $(\mathbb{TO}_p)^\vee$ of $\mathbb{TO}_p$ has underlying scheme $\operatorname{Spec} A^\vee$, and so is a closed subscheme of the affine space $\mathbb{A}^p_B$ with coordinates $u_0,\dots,u_{p-1}$. The usual structure α of A as a B-algebra gives the dual Hopf algebra structure $\delta\colon A^\vee\to A^\vee\otimes A^\vee$ in a way that is conceptually similar, although computationally more involved, as explained below. Theorem 4.5 describes the comultiplication δ explicitly.

For operations involving the tensor product $A^\vee\otimes A^\vee$, I introduce new notation $v_i=u_i\otimes 1$ and $w_i=1\otimes u_i$ for coordinates on the two factors of $\mathbb{A}^p\times_B\mathbb{A}^p$. This is the same device as my use of $y=x\otimes 1$ and $z=1\otimes x$ in treating the structures of A, explained in Subsection 1.1.

Remark 4.2. I allow denominators dividing $(p-1)!$ in this section, but refrain from burdening the notation with $\mathbb{TO}_p[1/(p-1)!]$ or $(\mathbb{TO}_p)_{(p)}$. The localisation does not change anything near p, but it simplifies the treatment considerably (notably Theorems 4.3–4.5). Cartier duality works perfectly well without denominators, but the explicit calculations I favour would then be inadequate. I treat the Cartier dual for theoretical purposes here, and I do not really use it seriously in applications.

4.3. The algebra structure $\beta\colon A^\vee\otimes A^\vee\to A^\vee$. Psychologically, the really hard first step is to take the notion of dual map literally. The Hopf algebra structure $\gamma\colon x\mapsto y+z+tyz$ of A is a B-algebra homomorphism, so

$$\gamma(x^a)=(y+z+tyz)^a=\sum_{i+j+k=a}\binom{a}{i,j,k}t^ky^{i+k}z^{j+k}, \tag{4.2}$$

where $\binom{a}{i,j,k}$ is the multinomial coefficient, with $i+j+k=a$. To nail down the dual map, I solemnly express (4.2) in terms of structure constants of the Hopf algebra, writing the right-hand side as a sum of monomials y^bz^c:

$$\gamma(x^a)=\sum_{bc}c^a_{bc}y^bz^c, \tag{4.3}$$

where c^a_{bc} is the coefficient of y^bz^c in $(y+z+tyz)^a$. With perseverance, one reads from (4.2) that

$$c^a_{bc}=\binom{a}{i,j,k}t^k \qquad \text{where}\quad k=b+c-a,\quad i=b-k,\quad j=c-k. \tag{4.4}$$

In (4.2), the exponents $i+k$ and $j+k$ must be nonnegative and $i+j+k=a$. This translates in terms of a, b and c as saying that c^a_{bc} is nonzero exactly for b and c in the triangle bounded by $b,c\le a\le b+c$, with corner monomials y^a, z^a and $(yz)^a$. That is, $\beta(u_bu_c)=\sum c^a_{bc}u_a$ only involves a with $\max\{b,c\}\le a\le b+c$.

The multiplication $\beta\colon A^\vee\otimes A^\vee\to A^\vee$ is the dual of γ, so is given on the basis $u_0,\dots,u_{p-1}$ as $u_bu_c\mapsto\sum c^a_{bc}u_a$ with the same structure constants.

Theorem 4.3. (i) *The multiplication $\beta\colon A^\vee\otimes A^\vee\to A^\vee$ is given on the basis $u_0,\dots,u_{p-1}$ by*

$$u_bu_c=\sum_a c^a_{bc}u_a \tag{4.5}$$

where the structure constants c^a_{bc} are as in (4.4).

(ii) *Viewed as a list of relations on the u_i, the multiplication table of* (4.5) *generates the ideal*

$$k!\,u_k=\prod_{i=0}^{k-1}(u_1-it)\quad\textit{for}\quad k=2,\dots,p-1\qquad\textit{and}\qquad\prod_{i=0}^{p-1}(u_1-it)=0. \tag{4.6}$$

In other words, $u_0=1_{A^\vee}$ is the identity element of $A^\vee$, and after u_1, I can view the remaining generators as *t-binomial coefficients*, the expressions

$$u_k=t\text{-}\binom{u_1}{k}=\frac{u_1(u_1-t)\dots(u_1-(k-1)t)}{k!}, \tag{4.7}$$

with the final line $u_1(u_1-t)\dots(u_1-(p-1)t)=\prod_{a\in\mathbb{F}_p^+}(u_1-at)=0$.

Rather than denominators, the factorials $k!$ could possibly be viewed as the statement that the products $u_1(u_1-t)(u_1-2t)$, etc., are divisible in $A^\vee$. Without denominators, I would need to include more relations such as $u_2u_3=\dots$, and so on. The product over $\mathbb{F}_p^+$ in the final relation is reminiscent of the s-splitting of (3.4) when $S=s^{p-1}$.

Example 4.4 ($p=5$)**.** First, no $(y+z+tyz)^a$ with $a>0$ has a constant term so $u_0=1$ has $1^2=1$. The argument for $u_0\times u_i=u_i$ is similar; I write $u_0=1$ from now on. Now writing $u_1\times u_1$ requires finding all occurrences of yz in all $(y+z+tyz)^a$. For $a=1$ there is one with coefficient t, and for $a=2$ there is one with coefficient 2. So,

$$u_1\times u_1=tu_1+2u_2,\qquad\text{or}\qquad 2u_2=u_1(u_1-t). \tag{4.8}$$

Next, $u_1\times u_2$ needs all occurrences of yz^2 in all $(y+z+tyz)^a$. Here $2tyz^2$ comes from $a=2$ and $3yz^2$ from $a=3$. Thus,

$$u_1\times u_2=2tu_2+3u_3,\qquad\text{or}\qquad 3u_3=u_2(u_1-2t). \tag{4.9}$$

In the same way, yz^3 appears in $(y+z+tyz)^a$ with coefficient $3t$ for $a=3$ and with coefficient 4 for $a=4$, giving

$$u_1\times u_3=3tu_3+4u_4,\qquad\text{or}\qquad 4u_3=u_3(u_1-3t). \tag{4.10}$$

Finally, yz^4 appears in $(y+z+tyz)^4$ only. This gives

$$u_1\times u_4=4tu_4,\qquad\text{or}\qquad (u_1-4t)u_4=0. \tag{4.11}$$

The proof of Theorem 4.3 for all p is just the same, and I omit it.

4.4. The Hopf algebra structure $\delta\colon A^\vee\to A^\vee\otimes A^\vee$. The algebra $A=B[x]/(F)$ is a hypersurface, a staple object of commutative algebra. However, the Hopf algebra comultiplication of $A^\vee$ needs the multiplication table written out in the basis $1,x,\dots,x^{p-1}$, recording the residue mod $I=(P,F)$ of $x^i\times x^j=x^{i+j}$. Applying F replaces x^p by a sum of $p-1$ terms involving S and different powers of t. Expressing x^k in this basis needs $k+1-p$ iterations of the reduction, so deriving the structure constants is a cumbersome calculation. However, the answer given by computer algebra and a certain amount of guesswork turned out simpler than expected, leading to the comparatively humane treatment of Theorem 4.5.

Since by Theorem 4.3 u_1 generates $A^\vee$ as a B-algebra (with denominators at most $(p-1)!$), and comultiplication δ is a B-algebra homomorphism, I fortunately only need the image of u_1.

Theorem 4.5. *The comultiplication* $\delta\colon A^\vee \to A^\vee \otimes A^\vee$ *takes* u_1 *to*

$$\delta(u_1) = v_1 + w_1 + S\left(\sum_{i=1}^{p-1} v_i w_{p-i}\right) + \sum_{n=p+1}^{2p-2} c_n \left(\sum_{i=n-p+1}^{p-1} v_i w_{n-i}\right), \tag{4.12}$$

where c_n *is the coefficient of* x *in* $x^n \bmod I = (P, F)$. *Specifically,*

$$c_n = \begin{cases} 0 & \text{for } n = 0,\\ 1 & \text{for } n = 1,\\ 0 & \text{for } 2 \le n \le p-1,\\ S & \text{for } n = p, \end{cases} \tag{4.13}$$

$$c_{p+n} = (-1)^{n-1}\,\frac{1}{p}\binom{p+n-1}{n} S^2 t^{p-n-1} \qquad \text{for} \quad 1 \le n \le p-2. \tag{4.14}$$

Equivalently,

$$\begin{aligned} \delta(u_1) &= v_1 + w_1 + S(v_1 w_{p-1} + \ldots + v_{p-1} w_1) \\ &\quad + \frac{1}{p}\binom{p}{1} S^2 t^{p-2} (v_2 w_{p-2} + \ldots + v_{p-2} w_2) - \ldots + \frac{1}{p}\binom{2p-3}{p-2} S^2 t v_{p-1} w_{p-1}. \end{aligned} \tag{4.15}$$

For $p = 3$ and $p = 5$ this gives

$$\delta(u_1) = v_1 + w_1 + S(v_1 w_2 + v_2 w_1) + S^2 t v_2 w_2$$

and

$$\begin{aligned} \delta(u_1) &= v_1 + w_1 + S(v_1 w_4 + v_2 w_3 + v_3 w_2 + v_4 w_1) \\ &\quad + S^2 t^3 (v_2 w_4 + v_3 w_3 + v_4 w_2) - 3S^2 t^2 (v_3 w_4 + v_4 w_3) + 7S^2 t v_4 w_4. \end{aligned} \tag{4.16}$$

These formulas were suggested by computer experiments; you recognise at once the factor

$$(-1)^{n-1}\,\frac{1}{p}\binom{p+n-1}{n}$$

from (say) the coefficients when $p = 11$:

$$\begin{aligned} &0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, S, S^2 t^9, -6S^2 t^8, 26S^2 t^7, -91S^2 t^6, \\ &\qquad 273S^2 t^5, -728S^2 t^4, 1768S^2 t^3, -3978S^2 t^2, 8398S^2 t. \end{aligned} \tag{4.17}$$

Lemma 4.6. *For* $n = 1, \ldots, p-2$, *the coefficients* c_{p+n} *of* (4.14) *are given by the following inductive formula, starting out from* $c_p = S = -\frac{1}{p} S^2 t^{p-1}$:

$$c_{p+n} = -\sum_{i=1}^{n} \binom{p}{i} t^{-i} c_{p+n-i} \qquad \text{for} \quad n = 1, \ldots, p-2. \tag{4.18}$$

Proof. Each term of (4.14) has S to power 2, and c_{p+n} has t to power $p-n-1$, which verifies the exponents in (4.18).

The coefficient of c_{p+n} in (4.14) (including sign) equals $-1/p$ times the coefficient of t^n in the binomial expansion of $(1+t)^{-p}$. Then for $n\ge 1$, (4.18) just states that the coefficient of t^n in the product $(1+t)^{-p}\sum_{i\ge 0}(-1)^i\binom{p+i-1}{i}t^i$ is zero. $\square$

Proof of Theorem 4.5. The first three lines of (4.13) are clear, since the product $x^i\times x^j$ is already reduced for $i+j\le p-1$.

The basis of A over B is $\{x^i\}$ for $i=0,\dots,p-1$. However, since $\delta(u_1)$ has no constant term, I omit $x^0=1_A$, and work with the partial basis $\{x^i\}$ for $i=1,\dots,p-1$. Multiplying this basis by x and replacing x^p by $Sf_p(t,x)$ means multiplying the column vector $(x,\dots,x^{p-1})$ on the left by the $(p-1)\times(p-1)$ matrix

$$M=\begin{pmatrix}0&1&0&\dots&0&0\\ 0&0&1&\dots&0&0\\ \vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\ 0&0&0&\dots&1&0\\ 0&0&0&\dots&0&1\\ S&\frac1p\binom p2 St&\frac1p\binom p3 St^2&\dots&\frac1p\binom p2 St^{p-3}&St^{p-2}\end{pmatrix}. \tag{4.19}$$

The bottom row does $x^p\mapsto Sf_p(t,x)=\bigl(\frac1p\binom pi St^{i-1}\bigr)\cdot\operatorname{column}(x,\dots,x^{p-1})$.

The case $k=p$ of (4.13) asks for the coefficient of x^1 in the reduction of x^p mod F. This corresponds to $x\times x^{p-1}$, so to the bottom left entry $m_{p-1,1}$ of M, giving $c_p=S$. For the same reason, c_{p+n} in (4.14) is the bottom left $(p-1,1)$ entry of M^{n+1} reduced mod $P=St^{p-1}+p$.

In more detail: multiplication by x does $x^i\mapsto x^{i+1}$ (the superdiagonal ones of M), except that the final basis element x^{p-1} goes to $Sf_p(t,x)$, the "carry" of long multiplication. Multiplication by x^2 does $x^i\mapsto x^{i+2}$, except for $x^{p-2}\mapsto Sf_p(t,x)$ and $x^{p-1}\mapsto x\times Sf_p(t,x)$, which involves a second "carry" of its top term,

$$\frac1p\binom p1 St^{p-2}x^{p-1}\mapsto S^2t^{p-2}f_p(t,x). \tag{4.20}$$

This gives the value $c_{p+1}=S^2t^{p-2}$ in (4.14). The term S^2t^{p-2} is not divisible by St^{p-1}, so is already reduced mod P. However, for each i with $3\le i\le p-2$, treating $x^i\times x^{p-1}$ leads to repeated reduction mod F, and the result always has terms divisible by S^3t^{p-1}, which reduce mod P.

Consider $x^3\times x^{p-1}$. A first reduction step $x^{p+2}-x^2F$ gets rid of the leading term x^{p+2} but leaves $St^{p-2}x^{p+1}$. After several reductions, one verifies that

$$x^{p+2}-\left(x^2+St^{p-2}x+S^2t^{2p-4}+\frac1p\binom p2 St^{p-3}\right)F \tag{4.21}$$

has degree at most $p-1$ in x, and ends in $\bigl(S^3t^{2p-4}+\frac1p\binom p2 S^2t^{p-3}\bigr)x$. To reduce the coefficient of x mod P, replace S^3t^{2p-4} by $-pS^2t^{p-3}$, which gives

$$c_{p+2}=\left(-p+\frac1p\binom p2\right)S^2t^{p-3}=-\frac1p\binom{p+1}{2}S^2t^{p-3}. \tag{4.22}$$

I now prove by induction that for $n=1,\dots,p-2$, the bottom left $(p-1,1)$th entry of M^{n+1} equals c_{p+n} as stated in (4.14). Obviously $M^{n+1}=M\times M^n$, and its bottom left entry comes by multiplying the bottom row of M (made up of the coefficients of $Sf_p(t,x)$) by the left column of M^n. Now the left column of M^n is made up of $p-n-1$ zeros, followed by the quantities c_{p+i} for $i=0,\dots,n-1$; indeed, for each j, the effect of doing $M^j\mapsto M\times M^j$ just lifts each row of the matrix by one, and puts the new entry c_{p+j} into the bottom left. The products add to c_{p+n} by Lemma 4.6, completing the proof. $\square$

5. GEOMETRIC APPLICATIONS

I discuss free $\mathbb{TO}_p$ actions on varieties V. The main inspiration comes from Godeaux's construction of quintic hypersurfaces invariant under a free $\boldsymbol{\mu}_5$ action. The Fermat hypersurface $F_5\colon (\sum_{i=0}^4 x_i^5 = 0) \subset \mathbb{P}^4$ over $\mathbb{C}$ (for example) has the free $\boldsymbol{\mu}_5$ action $\frac{1}{5}(0,1,2,3,4)$, with quotient $X = F_5/\boldsymbol{\mu}_5$ a Calabi–Yau threefold; the section $x_0 = 0$ is a classical Godeaux surface S. Both X and S have $\pi_1 = \mathbb{Z}/5$, and torsion $\mathbb{Z}/5 \subset \operatorname{Pic}$ given by the eigensheaves of the group action.

This construction and many similar ones can also be done in mixed characteristic, with $\boldsymbol{\mu}_p$ or $\mathbb{Z}/p$ replaced by $\mathbb{TO}_p$. The case of 5-torsion Godeaux surfaces is described in Subsection 6.1.1. The real cases of interest unfortunately involve large-scale calculations that can only be done by computer. Rather than getting into an explanation of computer algebra, I give here a handful of initial cases that illustrate some of the main techniques. Subsection 6.1 discusses some more advanced results.

A constantly recurring observation: a G-equivariant variety V is usually a simpler object to work with than its quotient V/G. The issue is even more pronounced in mixed characteristic: whereas the families of equivariant varieties I construct are flat over the base B, with constant cohomology groups, the corresponding families of quotients usually have fibres with nonreduced Pic (so having jumping $h^1(\mathcal{O})$ and not Cohen–Macaulay).

5.1. Background. Several of the sections below treat curves of genus 1 with a p-torsion group action. These topics can be viewed as including local deformations of supersingular curves with $\boldsymbol{\alpha}_p$ actions. I discuss briefly the cultural background, and what this material relates to.

The Shimura surface $S \to X_1(p)$ is the universal family of elliptic curves with a marked point of order p over the modular curve $X_1(p)$, the completion of $\mathcal{H}/\Gamma_1(p)$. Away from p, it has p disjoint sections forming a copy of $\mathbb{Z}/p \subset E$ in each fibre. The p-torsion of an elliptic curve E over a field of characteristic p is a group scheme of order p^2 that includes the kernel of Frobenius, so that its p-torsion subgroup contains a nonreduced group scheme, and has at most p distinct points. Over the prime p, the base curve $X_1(p)$ of the Shimura surface breaks up into two curve components that parametrise curves E with marked subgroup $\mathbb{Z}/p$ or $\boldsymbol{\mu}_p$, and intersect at a point corresponding to the supersingular elliptic curve with marked subgroup $\boldsymbol{\alpha}_p$. The standard reference[3] is [3, Ch. V] (especially Theorems 2.12–2.18 on pp. 250–252).

5.2. Plane cubics $C_3 \subset \mathbb{P}^2$ with free $\mathbb{TO}_3$ action. This section illustrates a key technique for calculating with $\mathbb{TO}_p$ actions: start from the reductive case with t invertible, and then cancel powers of t to achieve good reduction.

I set $p = 3$ and aim to produce a modular family of plane cubic curves with $\mathbb{TO}_3$ action; start over the base ring $\mathbb{Z}[t, 1/t]$ and set $S = -p/t^{p-1}$. The group action is then reductive, making it easy to find the invariants as monomials in the eigenbasis $\{v_i\}$ of Lemma 2.1. For my plane cubics to have good reduction at 3, I need to cancel as many powers of t as possible in linear combinations of these invariants, substituting $p \mapsto -St^{p-1}$ where necessary. Doing so leads to a flat family over $\operatorname{Spec} B$ on which $\mathbb{TO}_p$ acts freely, with a nonsingular fibre over $S = t = 0$. Nonsingularity is an open condition, so this implies without any further calculation that nearby fibres with $S \neq 0$ or $t \neq 0$ are also nonsingular.

Write $U = [u_0, u_1, u_2]$ with the action (2.5). Over $B[1/t]$, in terms of the eigenbasis v_0, v_1, v_2 of Lemma 2.1, the invariant cubics are v_0^3, $v_0v_1v_2$, v_1^3 and v_2^3. Substituting back into the u_0 gives $v_0^3 = u_0^3$, and then

$$v_0v_1v_2 - v_0^3 = t^3u_0u_1u_2 + 2t^2u_0u_1^2 + t^2u_0^2u_2 + 3tu_0^2u_1. \tag{5.1}$$

[3] I thank John Cremona for pointing out this reference.

Substituting $3 \mapsto -St^2$ makes this divisible by t^2, giving the invariant

$$tu_0u_1u_2 + 2u_0u_1^2 + u_0^2u_2 - Stu_0^2u_1. \tag{5.2}$$

The same substitution makes $v_1^3 - v_0^3 = t^3u_1^2 + 3t^2u_0u_1^2 + 3tu_0^2u_1$ divisible by t^3, giving the invariant

$$u_1^3 - Su_0^2u_1 - Stu_0u_1^2. \tag{5.3}$$

The final reduction must take t^6 out of something involving v_2^3. Starting as before from $v_2^3 - v_0^3$ and substituting for 3 gives

$$\begin{aligned} t^6u_2^3 + 6t^5u_1u_2^2 + 3t^4u_0u_2^2 + 12t^4u_1^2u_2 + 8t^3u_1^3 \\ - St^4u_0^2u_2 - 4St^5u_0u_1u_2 - 4St^4u_0u_1^2 - 2St^3u_0^2u_1, \end{aligned} \tag{5.4}$$

which is divisible by t^3, but the term in u_1^3 only contains t^3, and the next term in $u_0^2u_2$ only has t^4. To proceed, subtract off appropriate multiples of the invariants of (5.2) and (5.3):

$$\begin{aligned} &v_2^3 - 8(v_1^3 - v_0^3) + 6(v_0v_1v_2 - v_0^3) \\ &\quad = t^6u_2^3 + 6t^5u_1u_2^2 + 3t^4u_0u_2^2 + 12t^4u_1^2u_2 + 18t^3u_0u_1u_2 + 9t^2u_0^2u_2. \end{aligned} \tag{5.5}$$

Then two iterations of the substitution $3 \mapsto -St^2$ give the invariant

$$u_2^3 - S(u_0u_2^2 + 4u_1^2u_2 + 2tu_1u_2^2) + S^2(u_0^2u_2 + 2tu_0u_1u_2). \tag{5.6}$$

Remark 5.1. (i) There were choices in the above reductions, and I do not claim the answer is in a canonical form. In more complicated cases, I do not know if the algebra of invariants is always locally free over B.

(ii) There are alternative derivations of the invariants. Any reasonable ordering on the cubic monomials $S^3(u_0, u_1, u_2)$ gives the action on S^3U as a 10×10 lower triangular matrix having diagonal entries (that is, eigenvalues)

$$1, \quad \tau, \quad \tau^2, \quad \tau^2, \quad \tau^3, \quad \tau^3, \quad \tau^4, \quad \tau^4, \quad \tau^5, \quad \tau^6. \tag{5.7}$$

Since $\tau^3 = 1$, the invariant eigenspace is four-dimensional, and can be found easily enough by computer algebra.

5.2.1. *Nonsingularity.* The $\mathbb{TO}_3$-invariant cubic forms of (5.2), (5.3) and (5.6) are

$$\begin{aligned} c_0 &= u_0^3, \\ c_1 &= u_0(u_0u_2 + 2u_1^2 + tu_1u_2 - Stu_0u_1), \\ c_2 &= u_1^3 - Su_0^2u_1 - Stu_0u_1^2, \\ c_3 &= u_2^3 - S(u_0u_2^2 + 4u_1^2u_2 + 2tu_1u_2^2) + S^2(u_0^2u_2 + 2tu_0u_1u_2). \end{aligned} \tag{5.8}$$

Consider the plane cubic $E_3 \subset \mathbb{P}^2_{B\langle u_0,u_1,u_2\rangle}$ defined by $F = c_0 + c_1 + c_2 + c_3$, or $c_\lambda = c_0 + \lambda c_1 + c_2 + c_3$ if you want to see a modular invariant. In characteristic zero, E is projectively equivalent to the Hesse cubic $y_0^3 + y_1^3 + y_2^3 + \lambda y_0y_1y_2$. On the other hand, it is flat over $\mathbb{Z}[S,t]/(St^2+3)$, and when $S = t = 3 = 0$ and $\lambda \neq 0$ one sees that it defines a nonsingular curve.

5.2.2. *Supersingularity.* Fans of computer algebra should enjoy playing with the consequences of $u_0^3+u_0(u_0u_2+2u_1^2)+u_1^3+u_2^3$ being supersingular. It means that the eigenvalues of Frobenius are zero, which gives straightforward formulas for the number of points of E_3 over $\mathbb{F}_{p^n}$. For $q=3,9,\dots,3^n,\dots$, the number of points over $\mathbb{F}_q$ is $4=1+3$, $16=1+2\times\sqrt{9}+9$, $28=1+27$, $64=1-2\times\sqrt{81}+81$, or more generally, $1+q$ if n is odd, $1+2\sqrt{q}+q$ if $n\equiv 2 \bmod 4$, and $1-2\sqrt{q}+q$ if $n\equiv 0 \bmod 4$.

5.2.3. *Question*: *quasielliptic degeneration.* The referee raises the following interesting question, which I have not had time to study properly: The rational elliptic surface given by the Hesse pencil is known to degenerate in characteristic 3 to the quasielliptic surface with equation $\lambda x_1(x_0^2-x_1^2)=x_2(x_0^2-x_2^2)$. Can this degeneration, or this quasielliptic surface, be related to my construction in terms of the $\mathbb{TO}_3$-invariant cubics (5.8)?

5.3. $\mathbb{TO}_2$-invariant quartic curve $E_4\subset\mathbb{P}(1,1,2)$. I include this briefly because it is instructive and easy. Set $p=2$, and as usual, $B=\mathbb{Z}[S,t]/(St+2)$ and $\mathbb{TO}_2=\operatorname{Spec}(B[x]/(x^2-Sx))$. Write u_0,u_1,v for coordinates on $\mathbb{P}(1,1,2)$ over B, and guess the $\mathbb{TO}_2$ action

$$u_0\mapsto u_0,\qquad u_1\mapsto xu_0+\tau u_1,\qquad v\mapsto x^3u_0^2+3x^2\tau u_0u_1+3x\tau^2u_1^2+\tau^3v \tag{5.9}$$

where $\tau=1+tx$. I leave it as an exercise to check that the invariant subring of this action is generated by

$$\begin{gathered} a=u_0,\qquad b=u_1^2-Su_0u_1,\qquad c=(u_0+tu_1)v+3u_1^3-2Su_0u_1^2,\\ \text{and}\qquad e=v^2-3Su_1^2v+3S^2u_0u_1v-S^3u_0^2v \end{gathered} \tag{5.10}$$

in degrees 1, 2, 3 and 4. [Hint: the method is always to start from the reductive case with $1/t$, calculate eigenforms, and then take out as many powers of t as possible.]

An invariant form such as a^4+ac+e defines a relative curve in $\mathbb{P}(1,1,2)_B$, and one sees that this one reduces modulo $(S,t,2)$ to the nonsingular genus 1 curve

$$(v^2+u_0^2v=u_0^4+u_0u_1^3)\subset\mathbb{P}(1,1,2)_{\mathbb{F}_2}. \tag{5.11}$$

5.4. Enriques surfaces after Bombieri and Mumford. Consider first a complete intersection of three quadrics $Y(2,2,2)\subset\mathbb{P}^5$ (over $\mathbb{C}$) having a free $\boldsymbol{\mu}_2=\{\pm1\}$ action. Then Y is a K3 surface, in general nonsingular, and the quotient $X=Y/\boldsymbol{\mu}_2$ is an Enriques surface with general moduli, and with a chosen polarisation. In coordinates y_1,y_2,y_3,z_1,z_2,z_3 with action $(+,+,+,-,-,-)$, the invariant quadrics are $\operatorname{Sym}^2(y_1,y_2,y_3)\oplus\operatorname{Sym}^2(z_1,z_2,z_3)$.

This generalises in a straightforward way to the case of $\mathbb{TO}_2$ in mixed characteristic at 2, and gives nonsingular Enriques surfaces in characteristic 2 with torsion group $\mathbb{Z}/2$, $\boldsymbol{\mu}_2$ and $\boldsymbol{\alpha}_2$, all living together in a single deformation family with surfaces in characteristic 0 (cf. [6] for a similar treatment).

5.4.1. *Sketch of the problem of singularities.* In the inseparable cases, it is known that the "K3-like cover" Y must be singular (see [1, § 3]). If it were a nonsingular surface, an everywhere nonzero vector field would imply the Euler number is 0, whereas as a nonsingular K3, it must be 24. Proposition 5.3 shows that, for a general choice of parameters, Y is a K3 surface with 12 nodes, whose Jacobian subscheme consists of 12 orbits of the group action. As a rough description, the singular point is locally analytically $y_1y_2=z^2$, with Jacobian subscheme $V(y_1,y_2,z^2)$, and the group action is locally $z\mapsto z+\alpha$ with $\alpha^2=0$ (the p-closed vector field $x\frac{\partial}{\partial z}$, with x the coordinate of $\mathbb{TO}_p$), so that the quotient is nonsingular, with local analytic coordinates y_1,y_2. This is the sufficient condition of [5, Sect. 4.4] for the quotient by a $\boldsymbol{\mu}_p$ or $\boldsymbol{\alpha}_p$ action to be nonsingular. (We hope to return to the question of nonsingularity criteria for quotients by inseparable group actions; cf. Subsection 6.2.2.)

5.4.2. *Invariant quadrics.* First fix the $\mathbb{TO}_2$ action on coordinates: choose three copies of the rank 2 given representation $(B^{\oplus 2})^\vee$ of Subsection 2.2, with $\mathbb{TO}_2$ action $(y_i, z_i) \mapsto (y_i, xy_i + \tau z_i)$ where $\tau = 1 + tx$.

Lemma 5.2. *The $\mathbb{TO}_2$-invariant quadratic forms are the 12 expressions*

$$y_i^2, \quad z_i^2 - Sy_iz_i, \quad y_iy_j, \quad y_iz_j + y_jz_i + tz_iz_j \qquad \textit{for} \quad i,j = 1,2,3. \tag{5.12}$$

Derivation. As before, the calculation proceeds in two steps: first work over $B[1/t]$, when the action diagonalises as in Lemma 2.1, and then cancel powers of t. In y_i, z_i only (for $i = 1,2,3$), the squares of the ± 1 eigenforms give the invariants y_i^2 and $(y_i + tz_i)^2$. Taking the difference and substituting $2 \mapsto -St$ gives the combination

$$(y_i + tz_i)^2 - y_i^2 = 2ty_iz_i + t^2z_i^2 = t^2(-Sy_iz_i + z_i^2), \tag{5.13}$$

and dividing by t^2 gives $z_i^2 - Sy_iz_i$.

Working in a similar way with ± 1 eigenforms in mixed y_i, z_i, y_j, z_j gives the invariants y_iy_j and $(y_i + tz_i)(y_j + tz_j)$, and the difference divided by t.

Proposition 5.3. *Set $S = t = 0$, so that $\mathbb{TO}_2$ reduces to $\boldsymbol{\alpha}_2$. Then three general linear combinations of the invariants* (5.12) *define a surface $Y(2,2,2) \subset \mathbb{P}^5$ that is a* K3 *surface with* 12 *nodes having a free action of $\boldsymbol{\alpha}_2$, so that the quotient $X = Y/\boldsymbol{\alpha}_2$ is a nonsingular Enriques surface.*

An explicit example over $\mathbb{F}_2$ is given by the three quadrics

$$(y_1 + y_2)y_2 + z_2^2 + z_3^2, \qquad (y_1 + y_3)y_3 + y_1z_3 + y_3z_1 + z_1^2, \qquad y_1^2 + y_2z_3 + y_3z_2 + z_1^2 + z_2^2. \tag{5.14}$$

The proof reduces to a number of verifications in computer algebra (see the website [10] for the Magma code).

The action of $\boldsymbol{\alpha}_2$ on $\mathbb{P}^5$ corresponds to the vector field $\alpha\frac{\partial}{\partial z_i}$ with $\alpha^2 = 0$. The action has fixed locus the plane $\mathbb{P}^2_{\langle y_1,y_2,y_3\rangle}$. The three quadrics of (5.14) restrict to $(y_1 + y_2)y_2$, $(y_1 + y_3)y_3$ and y_1^2, so that Y is disjoint from the fixed plane. It follows that the vector field defines a free group action, and Y has dimension 2, so is a complete intersection.

I ask the computer for the degree of the Jacobian subscheme (defined by the 3×3 minors of the Jacobian matrix $\frac{\partial Q_i}{\partial x_j}$, where Q_i are the three forms and x_j the six coordinates) and for the degree of its reduced subscheme. The answer is 24 and 12, and this proves the proposition.

5.5. $\mathbb{TO}_5$-invariant quintic curves $E_5 \subset \mathbb{P}^4$. As in Subsection 3.2, let $B = \mathbb{Z}[S,t]/(P)$ with $P = St^4 + 5$, and $\mathbb{TO}_5 = \operatorname{Spec}(B[x]/(F))$ with $F = x^5 - S(t^3x^4 + 2t^2x^3 + 2tx^2 + x)$. As discussed in Subsections 2.3 and 3.3, the dual regular representation $U = (V^{\text{reg}})^\vee$ is the free B-module based by $\{u_0, \dots, u_4\}$ with the $\mathbb{TO}_5$ action given by the lower triangular matrix (2.5) with $d = 4$, which I denote by D_u.

Here I write down 5×5 skew matrices with entries in U that base the module of $\mathbb{TO}_5$-invariant homomorphisms $\varphi\colon \bigwedge^2 U \to U$. The ideal of 4×4 Pfaffians of a general such homomorphism defines a relative curve $E_5 \subset \mathbb{P}^4_B$ whose fibre over $(S = t = 0)$ is a nonsingular curve of genus 1.

When t is invertible, the representation theory is reductive, and the coordinate change of Lemma 2.1 from lower triangular coordinates u_i to eigencoordinates v_i applies. Rather than working directly with the 50-dimensional representation $\operatorname{Hom}(\bigwedge^2 U, U)$, I determine the eigenspace decomposition of the domain $\bigwedge^2 U$ and then view the invariant maps as those that take the eigenvectors $v_i \wedge v_j$ of $\bigwedge^2 U$ to the τ^{i+j} eigenspace of U, based by v_{i+j}. (Here $\tau = 1 + tx$, and satisfies $\tau^5 = 1$.)

I write $\bigwedge^2 U$ as skew 5×5 matrices. As a B-module it has basis $w_{ij} = u_i \wedge u_j$ with $i < j$, lexicographically ordered, corresponding to elementary skew matrices. Then $\mathbb{TO}_5$ acts on skew matrices by $N \mapsto D_u N\, {}^tD_u$. In the basis w_{ij}, this works out as right multiplication by the 10×10 matrix

$$D_w = \begin{pmatrix}
\tau & . & . & . & . & . & . & . & . & . \\
2x\tau & \tau^2 & . & . & . & . & . & . & . & \\
3x^2\tau & 3x\tau^2 & \tau^3 & . & . & . & . & . & . & \\
4x^3\tau & 6x^2\tau^2 & 4x\tau^3 & \tau^4 & . & . & . & . & . & \\
x^2\tau & x\tau^2 & 0 & 0 & \tau^3 & . & . & . & . & \\
2x^3\tau & 3x^2\tau^2 & x\tau^3 & 0 & 3x\tau^3 & \tau^4 & . & . & . & . \\
3x^4\tau & 6x^3\tau^2 & 4x^2\tau^3 & x\tau^4 & 6x^2\tau^3 & 4x\tau^4 & \tau^5 & . & . & . \\
x^4\tau & 2x^3\tau^2 & x^2\tau^3 & 0 & 3x^2\tau^3 & 2x\tau^4 & 0 & \tau^5 & . & . \\
2x^5\tau & 5x^4\tau^2 & 4x^3\tau^3 & x^2\tau^4 & 8x^3\tau^3 & 8x^2\tau^4 & 2x\tau^5 & 4x\tau^5 & \tau^6 & . \\
x^6\tau & 3x^5\tau^2 & 3x^4\tau^3 & x^3\tau^4 & 6x^4\tau^3 & 8x^3\tau^4 & 3x^2\tau^5 & 6x^2\tau^5 & 3x\tau^6 & \tau^7
\end{pmatrix}. \tag{5.15}$$

For example, D_u does $u_1 \mapsto xu_0 + \tau u_1$ and $u_2 \mapsto x^2u_0 + 2x\tau u_1 + \tau^2 u_2$, so that

$$u_1\wedge u_2 \mapsto (xu_0+\tau u_1)\wedge(x^2u_0+2x\tau u_1+\tau^2u_2) = x^2\tau u_0\wedge u_1 + x\tau^2 u_0\wedge u_2 + \tau^3 u_1\wedge u_2, \tag{5.16}$$

which is the fifth row of D_w. Each diagonal term $\tau, \tau^2, \dots$ of D_w is an eigenvalue. Using $\tau^5 = 1$, one sees that each eigenvalue τ^i for $i = 0,\dots,4$ appears twice.

Calculating the kernel of $D_w - \tau^i$ gives the following 10 skew matrices as τ^i eigenvectors (I write the upper triangular entries m_{ij} with $ij = 01, 02, \dots,$ and omit the diagonal zeros and jith entry $-m_{ij}$):

$$1\colon\qquad M_{14} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 1 \\ & & 0 & -2/t \\ & & & 3/t^2 \end{pmatrix}, \qquad M_{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 1 & -4/t \\ & & & 6/t^2 \end{pmatrix},$$

$$\tau\colon\qquad M_{01} = \begin{pmatrix} 1 & -2/t & 3/t^2 & -4/t^3 \\ & 1/t^2 & -2/t^3 & 3/t^4 \\ & & 1/t^4 & -2/t^5 \\ & & & 1/t^6 \end{pmatrix}, \qquad M_{24} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 0 & 1 \\ & & & -3/t \end{pmatrix},$$

$$\tau^2\colon\qquad M_{02} = \begin{pmatrix} 0 & 1 & -3/t & 6/t^2 \\ & -1/t & 3/t^2 & -6/t^3 \\ & & -2/t^3 & 5/t^4 \\ & & & -3/t^5 \end{pmatrix}, \qquad M_{34} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 0 & 0 \\ & & & 1 \end{pmatrix},$$

$$\tau^3\colon\qquad M_{03} = \begin{pmatrix} 0 & 0 & 1 & -4/t \\ & 0 & -1/t & 4/t^2 \\ & & 1/t^2 & -4/t^3 \\ & & & 3/t^4 \end{pmatrix}, \qquad M_{12} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 1 & -3/t & 6/t^2 \\ & & 3/t^2 & -8/t^2 \\ & & & 6/t^4 \end{pmatrix},$$

$$\tau^4\colon\qquad M_{04} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ & 0 & 0 & -1/t \\ & & 0 & 1/t^2 \\ & & & -1/t^3 \end{pmatrix}, \qquad M_{13} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 1 & -4/t \\ & & -2/t & 8/t^2 \\ & & & -8/t^3 \end{pmatrix}.$$

Thus M_{24} is in the τ eigenspace because

$$\begin{pmatrix} \tau^6 & 0 \\ 3x\tau^6 & \tau^7 \end{pmatrix}\begin{pmatrix} t \\ -3 \end{pmatrix} = \tau\begin{pmatrix} t \\ -3 \end{pmatrix}$$

in view of $\tau = 1 + tx$ and $\tau^5 = 1$.

The basis elements $M_{ij} \in \bigwedge^2 U$ and $v_{i+j} \in U$ are in the same eigenspace of $\boldsymbol{\mu}_5 = \mathbb{TO}_5[1/t]$. Thus I can define a $\boldsymbol{\mu}_5$-invariant linear map

$$h_{ij}\colon \bigwedge^2 U \to U, \qquad M_{ij} \mapsto v_{i+j}.$$

These 10 elements base $\operatorname{Hom}_{\boldsymbol{\mu}_5}(\bigwedge^2 U, U)$ for t invertible.

I explain what $\boldsymbol{\mu}_5$-invariance means, and why it solves my problem of constructing invariant ideals for a group action. For a matrix M with entries in $B[1/t][u_0,\dots,u_4]$ or $B[u_0,\dots,u_4]$, write $D_u(M)$ for the matrix obtained by applying D_u to the entries of M.

Proposition 5.4. (a) *Each matrix $v_{i+j}M_{ij}$ satisfies*

$$D_u(v_{i+j}M_{ij})\,{}^tD_u = D_u(v_{i+j}M_{ij}). \tag{5.17}$$

The same holds for any linear combination $\sum b_{ij}v_{i+j}M_{ij}$ with coefficients $b_{ij} \in B[1/t]$.

(b) *Let M be a 5×5 skew matrix with entries in $B[1/t][u_0,\dots,u_4]$ or $B[u_0,\dots,u_4]$ and assume $D_uM\,{}^tD_u = D_u(M)$. Then the ideal of 4×4 Pfaffians of M is invariant under D_u.*

Proof. In fact both sides of (5.17) are equal to $\tau^{i+j}v_{i+j}M_{ij}$. The point is that on the left of (5.17), D_u acts by invertible row and column operations with coefficients in $B[1/t]$, without doing anything to the u_i or v_i, whereas on the right it acts on each entry of the matrix, without doing anything to the rows and columns. Now M_{ij} was constructed as an eigenvector, so satisfies $D_uM_{ij}\,{}^tD_u = \tau^{i+j}M_{ij}$ and multiplying M_{ij} by v_{i+j} on both sides of (5.17) is completely harmless. On the other hand, D_u acts trivially on the entries of M_{ij}, so applied to $v_{i+j}M_{ij}$ it just multiplies each entry by τ^{i+j}. This proves assertion (a).

For (b), D_u acts on $B[1/t][u_0,\dots,u_4]$ as a B-algebra homomorphism, so takes a Pfaffian of M to a Pfaffian of $D_u(M)$; by the invariance assumption, this is a Pfaffian of an equivalent matrix. This proves assertion (b). $\square$

Returning to $\mathbb{TO}_5$ itself, to find $\operatorname{Hom}_{\mathbb{TO}_5}(\bigwedge^2 U, U)$, I *only* need to get rid of the denominators. The next result establishes this.

Proposition 5.5. *The* 10 *matrices*

$$\begin{aligned}
N_{34} &= v_2M_{34},\\
N_{24} &= v_1M_{24} + \frac{3}{t}v_2M_{34},\\
N_{23} &= v_0M_{23} + \frac{4}{t}v_1M_{24} + \frac{6}{t^2}v_2M_{34},\\
N_{14} &= v_0M_{14} + \frac{2}{t}v_1M_{24} + \frac{3}{t^2}v_2M_{34},\\
N_{13} &= v_4M_{13} + \frac{4}{t}v_0M_{14} + \frac{2}{t}v_0M_{23} + \frac{8}{t^2}v_1M_{24} + \frac{8}{t^3}v_2M_{34},\\
N_{12} &= v_3M_{12} + \frac{3}{t}v_4M_{13} + \frac{6}{t^2}v_0M_{14} + \frac{3}{t^2}v_0M_{23} + \frac{8}{t^3}v_1M_{24} + \frac{6}{t^4}v_2M_{34},\\
N_{04} &= v_4M_{04} + \frac{1}{t}v_0M_{14} + \frac{1}{t^2}v_1M_{24} + \frac{1}{t^3}v_2M_{34},\\
N_{03} &= v_3M_{03} + \frac{4}{t}v_4M_{04} + \frac{1}{t}v_4M_{13} + \frac{4}{t^2}v_0M_{14} + \frac{1}{t^2}v_0M_{23} + \frac{4}{t^3}v_1M_{24} + \frac{3}{t^4}v_2M_{34},\\
N_{02} &= v_2M_{02} + \frac{3}{t}v_3M_{03} + \frac{6}{t^2}v_4M_{04} + \frac{1}{t}v_3M_{12} + \frac{3}{t^2}v_4M_{13}\\
&\quad + \frac{6}{t^3}v_0M_{14} + \frac{2}{t^3}v_0M_{23} + \frac{5}{t^4}v_1M_{24} + \frac{3}{t^5}v_2M_{34},
\end{aligned}$$

$$N_{01} = v_1M_{01} + \frac{2}{t}v_2M_{02} + \frac{3}{t^2}v_3M_{03} + \frac{4}{t^3}v_4M_{04} + \frac{1}{t^2}v_3M_{12} + \frac{2}{t^3}v_4M_{13} + \frac{3}{t^4}v_0M_{14} + \frac{1}{t^4}v_0M_{23} + \frac{2}{t^5}v_1M_{24} + \frac{1}{t^6}v_2M_{34}$$

have entries linear forms in $u_0,\dots,u_4$ *with coefficients in* B. *They form a basis of* $\operatorname{Hom}_{\mathbb{T}\mathbb{O}_5}(\bigwedge^2 U, U)$ (*in degree* 1 *in the* u_i). *Each* N_{ij} *has* v_{i+j} *as leading entry in the* ij-*th place, which contains* u_0, *and no other occurrence of* u_0.

The derivation of these matrices is a computer algebra calculation, and is documented on [10]. These matrices get quite bulky; I write out just a few as an illustration:

$$N_{34} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 0 & 0 \\ & & & u_0 + 2tu_1 + t^2u_2 \end{pmatrix}, \quad N_{24} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & 0 & u_0 + tu_1 \\ & & & 3(u_1 + tu_2) \end{pmatrix}, \quad N_{23} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 \\ & & u_0 & 4u_1 \\ & & & 6u_2 \end{pmatrix},$$

$$N_{14} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ & 0 & 0 & u_0 \\ & & 0 & 2u_1 \\ & & & 3u_2 \end{pmatrix}, \qquad N_{04} = \begin{pmatrix} 0 & 0 & 0 & v_4 \\ & 0 & 0 & -4u_1 - 6tu_2 - 4t^2u_3 - t^3u_4 \\ & & 0 & -St^3u_1 + 6u_2 + 4tu_3 + t^2u_4 \\ & & & St^2u_1 + St^3u_2 - 4u_3 - tu_4 \end{pmatrix},$$

and the final one

$$N_{01} = \begin{pmatrix} v_1 & 2u_1 + 2tu_2 & 3u_2 + 3tu_3 & 4u_3 + 4tu_4 \\ & u_2 + tu_3 & 2u_3 + 2tu_4 & 3Stu_1 + 6St^2u_2 + 6St^3u_3 - 12u_4 \\ & & Stu_1 + 2St^2u_2 + 2St^3u_3 - 4u_4 & -8Su_1 - 14Stu_2 - 12St^2u_3 - 4St^3u_4 \\ & & & -2S^2t^3u_1 + 16Su_2 + 13Stu_3 + 4St^2u_4 \end{pmatrix}.$$

To define my curve $E_5 \subset \mathbb{P}^4$ over B, rather than a general linear combination, it is enough to take $N = N_{01} + N_{04} + N_{23}$. Substituting $S = t = 0$ in this gives

$$\overline{N} = \overline{N}_{01} + \overline{N}_{04} + \overline{N}_{23} = \begin{pmatrix} u_0 & 2u_1 & 3u_2 & u_0 - u_3 \\ & u_2 & 2u_3 & u_1 + 3u_4 \\ & & u_0 + u_4 & -u_1 + u_2 \\ & & & u_2 + u_3 \end{pmatrix}. \tag{5.18}$$

Proposition 5.6. *The* 4×4 *Pfaffians of* $\overline{N}$ *define a nonsingular genus* 1 *curve* $E_5 \subset \mathbb{P}^4$ *with a free* $\boldsymbol{\alpha}_5$ *action.*

The $\boldsymbol{\alpha}_5$ action is given by the matrix D_u of (2.5) with S and t set to 0, so that $x^5 = 0$. It acts on $\mathbb{P}^4$ as a p-closed vector field D with $D^5 = 0$, nowhere zero outside the coordinate point $P_0 = (1,0,0,0)$. On the other hand, E does not pass through P_0, because x_0^2 is a term of the Pfaffian $\mathrm{Pf}_{01.23}$ of $\overline{N}$. The computer asserts that its Pfaffians define a nonsingular curve E.

In a little more detail the Pfaffians are

$$u_0(u_0+u_4) + u_1u_3 + 3u_2^2,$$

$$u_0(-u_1+u_2) - 2u_1(u_1+3u_4) + u_2(u_0-u_3) = -(u_0u_1 + 3u_0u_2 + 2u_1^2 + u_1u_4 + u_2u_3),$$

$$u_0(u_2+u_3) + 2u_2(u_1+3u_4) + 2u_3(u_0-u_3),$$

$$2u_1(u_2+u_3) + 2u_2(-u_1+u_2) + (u_0+u_4)(u_0-u_3) = u_0^2 - u_0u_3 + u_0u_4 + 2u_1u_3 + 2u_2^2 - u_3u_4,$$

$$u_2(u_2+u_3) + 2u_3(u_1-u_2) + (u_0+u_4)(u_1+3u_4).$$

The curve E has $6 = 1 + p$ rational points over $\mathbb{F}_5$:

$$\begin{aligned} &P_1 = (0,2,0,0,1), && P_2 = (-1,0,0,0,1), && P_3 = (-1,0,0,1,1), \\ &P_4 = (1,0,1,2,1), && P_5 = (2,2,3,1,1), && P_6 = (3,2,2,3,1). \end{aligned} \tag{5.19}$$

The pencil of hyperplanes $\langle u_0 + 2u_1 + u_4, u_2\rangle$ through P_1, P_2, P_3 defines a double cover $\pi\colon E \to \mathbb{P}^1$. The first hyperplane $u_0 + 2u_1 + u_4$ intersects E in the divisor $3P_1 + P_2 + P_3$ (that is, has inflexional tangent at P_1), whereas $u_0 + 2u_1 + u_4 + 3u_2$ is tangent to E at P_4 (so has divisor $P_1 + P_2 + P_3 + 2P_4$). This identifies two of the ramification points as $(1,0), (1,3) \in \mathbb{P}^1$.

In fact, $E \cong \big(y^2 = x(x-3)((x-1)^2-2)\big)$, with the other ramification points $1 \pm \sqrt{2} \in \mathbb{F}_{25}$. (It is supersingular, so has $36 = 1 + p^2 + 2\sqrt{p^2}$ points over $\mathbb{F}_{25}$. As in Subsection 5.2.2, it is also fun to count its points in $\mathbb{F}_{5^n}$.)

6. BIGGER APPLICATIONS, OPEN PROBLEMS

6.1. Godeaux and Campedelli surfaces. The constructions of Section 5 illustrate some of the methods needed in future work: Subsection 5.2 on the $\mathbb{TO}_3$-invariant cubic hypersurfaces $E_3 \subset \mathbb{P}^2$ is a trailer for the $\mathbb{TO}_5$-invariant quintic hypersurfaces that make the 5-torsion Godeaux surfaces and Calabi–Yau threefolds of [10]. The 5×5 Pfaffian format of E_5 of Subsection 5.5 illustrates the methods for the 7×7 Pfaffian format that construct 7-torsion Campedelli surfaces and Calabi–Yau threefolds. And the case of the weighted quartics $E_4 \subset \mathbb{P}(1,1,2)$ of Subsection 5.3 (especially the point (5.9), where I must *guess* the $\mathbb{TO}_p$ action on the degree 2 forms) illustrates one aspect of my construction (in progress) of 3-torsion Godeaux surfaces and Calabi–Yau threefolds in $\mathbb{P}(1^3, 2^3, 3^3)$, using Gorenstein codimension 4 methods.

6.1.1. *Godeaux surfaces with* 5*-torsion.* Godeaux surfaces obtained as quotients $S = T_5/G_5$ of a hypersurface $T_5 \subset \mathbb{P}^3$ by $G_5 = \boldsymbol{\mu}_5$, $\mathbb{Z}/5$ and $\boldsymbol{\alpha}_5$ were constructed by Bill Lang, Rick Miranda and Christian Liedtke, respectively. Kim Soonyoung [5] showed how to make these constructions in a more-or-less uniform way, with the extra symmetry by $\mathrm{Aut}(G_5) = \mathbb{F}_5^\times \cong \mathbb{Z}/4$ corresponding to the *holomorph* $G_5 \rtimes \mathrm{Aut}(G_5)$. She also clarified the issue discussed in Subsection 5.4.1 of the singularities of the cover.

Our forthcoming joint work with Kim Soonyoung unifies the three separate cases $\boldsymbol{\mu}_5$, $\mathbb{Z}/5$ and $\boldsymbol{\alpha}_5$ into a single construction, with $\mathbb{TO}_5$ acting on a hypersurface in $T_5 \subset \mathbb{P}^3$ or $F_5 \subset \mathbb{P}^4$. The calculations of invariants in Magma [2] and the final computation for the nonsingularity of the quotient are available from the website [10].

6.1.2. *Campedelli surfaces with* 7*-torsion.* The ambient space for the construction is the projective space $\mathbb{P}^6 = \mathbb{P}(U_{p-1})$ corresponding to the dual regular representation of $\mathbb{TO}_7$ introduced in Subsections 2.2 and 3.3. I write out the $\mathbb{TO}_7$-invariant homomorphisms $\bigwedge^2 U \to U$ as skew matrices exactly as in Subsection 5.5, except that there are 21 skew 7×7 matrices with some much bigger entries. The 6×6 Pfaffians of a general combination of these are seven cubics that define a Calabi–Yau threefold $Y_{14} \subset \mathbb{P}^6_B$ with a free $\mathbb{TO}_7$-action. The same singularity calculation on Y_{14} gives that the quotient of the central $\boldsymbol{\alpha}_7$ fibre $S = t = 7 = 0$ is nonsingular. The surface section $x_0 = 0$ gives a family of Campedelli surfaces with torsion $\mathbb{Z}/7$, $\boldsymbol{\mu}_7$ or $\boldsymbol{\alpha}_7$. The Magma calculations proving these claims are online at [10] (documenting them is work in progress).

6.1.3. *Godeaux surfaces with* 3*-torsion.* Over $\mathbb{C}$, the $\boldsymbol{\mu}_3$ cover of a Godeaux surface with 3-torsion is comparatively well understood in terms of a triple unprojection format $\mathbb{P}(1^3, 2^3, 3^3)$. It also extends naturally to a Calabi–Yau threefold. Making this work as a $\mathbb{TO}_3$ construction is currently in progress, but I expect it to work. One issue that arises illustrates a tricky point of representation theory: in the reductive $\boldsymbol{\mu}_3$ case, each of the three sets of coordinates x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3

forms a new copy of the regular representation $\frac{1}{3}(0,1,2)$ as a direct summand in its component of the graded ring; whereas in the $\mathbb{TO}_3$ case, they only appear as a complement to stuff from lower degree, and how $\mathbb{TO}_3$ acts on the extension has to be determined or guessed (as with v in (5.9)).

6.2. Problems.

6.2.1. *Does the restriction to* $\mathbb{TO}_p[1/t]$ *predict a representation*? The case t invertible is always easier in applications, because it is reductive, and eigenforms usually provide generators of the modules or rings we need. It might be valuable to formalise this more generally: to what extent is a $\mathbb{TO}_p$-module determined by its restriction to the t invertible case, and when does a $\mathbb{TO}_p[1/t]$-module extend to a $\mathbb{TO}_p$-module? Can we exploit the reductive case to find a working substitute for character theory for $\mathbb{TO}_p$? In geometric applications, one usually knows the required representation from Riemann–Roch or its orbifold versions.

6.2.2. *Singularities of inseparable covers.* It is familiar when constructing Enriques surfaces or Godeaux surfaces as quotients $Y \to X$ that, in the inseparable case, the cover Y usually has to be singular, even when the final X is nonsingular (cf. Subsection 5.4). It would be interesting to know if there is a more general criterion for X to be nonsingular, complementing the sufficient condition of [5, Sect. 4.4] in the isolated case.

It is striking to consider G-torsors over a curve C of genus ≥ 2, which are in plentiful supply from torsion subgroups of $\operatorname{Pic} C$, or can be constructed in an ad hoc way by the methods of Section 5 (for example, $D_8 \subset \mathbb{P}(1,1,4)$ that is a $\boldsymbol{\mu}_2$- or $\boldsymbol{\alpha}_2$-torsor over $C_6 \subset \mathbb{P}(1,1,3)$, a curve of genus 2 in its canonical embedding). An inseparable torsor $D \to C$ is singular, since it has the same etale Betti numbers and geometric genus as C, but has an everywhere nonvanishing vector field. It is not clear to me how to resolve the little paradox that the group scheme acts on D but cannot act regularly on its normalisation: a vector field must have poles on $\widetilde{D}$ when genus is at least 2.

Cyclic covers also play an essential role in the singularities of the higher dimensional minimal model program. A terminal threefold singularity has local class group $\mathbb{Z}/r$, generated by the canonical class, and over $\mathbb{C}$ the index 1 cover is an isolated rational hypersurface singularity. For this to make sense when the characteristic p divides the index r, one needs an inseparable $\boldsymbol{\mu}_r$ cover, and it is an open problem to say something useful about its singularities.

The referee suggested an idea along the following lines: an inseparable morphism $Y \to X$ of degree p is locally $z^p = s$, where $s \in \mathcal{O}_X$ is defined up to addition of $k(X)^p$. The gradient of s is thus well defined, and corresponds to a local section $\mathrm{d}s \in \Omega^1_X$. If the variety X is normal, then locally over any prime divisor of X, I can assume that $\operatorname{div} s$ is reduced, so that $\mathrm{d}s \neq 0$ in codimension 1. If X itself is nonsingular, the singularities of Y lie over the critical points of s, that is, over the zeros of $\mathrm{d}s$. The criterion of [5] discussed in Subsection 5.4.1 corresponds to s having Morse critical points.

Having a copy of $\mathbb{Z}/p$ or $\boldsymbol{\mu}_p$ in $\operatorname{Pic} X$ certainly gives rise to a $\boldsymbol{\mu}_p$- or $\boldsymbol{\alpha}_p$-torsor $Y \to X$ by Remark 4.1, so to an inseparable map of degree p, and hence to a p-closed codimension 1 foliation on X and (locally defined) section $\mathrm{d}s \in \Omega^1_X$, but at present I do not have too much understanding of how this works, or how to use it in applications.

6.3. The T-nonsplit form $\mathbb{TO}_{p,0}$. This paper has developed the t-split form $\mathbb{TO}_{p,1}$ of $\mathbb{TO}_p$ with a view towards its representation theory and geometric applications. I conclude with some indications of how to pass from the t-split form of Section 3 to the T-nonsplit form $\mathbb{TO}_{p,0}$, attempting to copy the original treatment of Tate and Oort [13].

There are several reasons for wanting to do this: to describe the moduli stack of varieties with p-torsion in Pic, without fixing in advance a generator of $\mathbb{Z}/p$; to treat Cartier duality as a strict isomorphism that interchanges S and T; to recover the treatment of the universal group scheme $\mathbb{TO}_p$ of [13] as a construction in algebra (without recourse to p-adic methods).

The construction combines two different naturally occurring order $p-1$ symmetries of the t-split group $\mathbb{TO}_{p,1}$: first, any group or group scheme G of order p over a base S automatically has the $\operatorname{Aut}(\mathbb{F}_p^+) = (\mathbb{Z}/p)^\times$ symmetry over S defined by $g \mapsto g^a$ for $a \in (\mathbb{Z}/p)^\times$. It is traditional to choose a primitive root a mod p and view this as a cyclic $\mathbb{Z}/(p-1)$ symmetry.

The second symmetry is the $\boldsymbol{\mu}_{p-1}$ Galois symmetry of the base B_1 given by $t \mapsto \varepsilon t$ for $\varepsilon \in \boldsymbol{\mu}_{p-1}$. To identify this as a cyclic $\mathbb{Z}/(p-1)$ symmetry requires a primitive $(p-1)$th root of unity ε, so an extension of scalars from $\mathbb{Z}$ to a ground ring containing at least the cyclotomic ring of integers $\mathbb{Z}[\varepsilon]$.

Since I increase the ground ring $\mathbb{Z}$ to $\mathbb{Z}[\varepsilon]$, possibly localised further as explained below, the construction fits into the following diagram:

$$\begin{array}{lcl} B_1 = \mathbb{Z}[S,t]/(St^{p-1}+p) & & B_0 \subset B_1 \otimes_{\mathbb{Z}} \mathbb{Z}[\varepsilon] \\ \cap & \text{with} & \cap \\ A_1 = B_1[x]/(x^p - Sf_p(t,x)) & & A_0 \subset A_1 \otimes_{\mathbb{Z}} \mathbb{Z}[\varepsilon] \end{array} \tag{6.1}$$

where $B_1 \subset A_1$ are as in Section 3 and $B_0 \subset A_0$ the invariant subrings.

Identifying the two symmetry groups with $\mathbb{Z}/(p-1)$ and with each other (in other words, choosing both a and ε) gives the $\mathbb{Z}/(p-1)$ Galois symmetry generated by

$$t \mapsto \varepsilon t \qquad \text{and} \qquad (1+tx) \mapsto (1+tx)^a, \qquad \text{hence} \qquad x \mapsto \varepsilon^{-1}\frac{(1+tx)^a - 1}{t}. \tag{6.2}$$

The invariant subrings of this $\mathbb{Z}/(p-1)$ symmetry and the associated schemes $\operatorname{Spec} A_0 \to \operatorname{Spec} B_0$ will provide the T-nonsplit group scheme $\mathbb{TO}_{p,0}$ after restricting to a neighbourhood of the prime ideal $(p, a-\varepsilon)$ in $\operatorname{Spec}\mathbb{Z}[\varepsilon]$ by an appropriate localisation.

To be clear: the $\mathbb{Z}/(p-1)$ symmetry and $\operatorname{Spec} A_0 \to \operatorname{Spec} B_0$ are already defined over $\operatorname{Spec}\mathbb{Z}[\varepsilon]$, but the localisation described below is needed to ensure that the bigebra structure $\delta_1\colon A_1 \to A_1 \otimes_{B_1} A_1$ restricts to a bigebra structure $\delta_0\colon A_0 \to A_0 \otimes_{B_0} A_0$. In other words, the localisation provides the denominators of δ_0.

Tate and Oort [13] work with the smallest possible ground ring that achieves this, namely

$$\Lambda_p = \mathbb{Z}[\varepsilon]\left[\frac{1}{p-1}\right]\left[\frac{a-\varepsilon}{p}\right]. \tag{6.3}$$

Here the denominator $p-1$ is no surprise: averages over $\boldsymbol{\mu}_{p-1}$ are used for the eigenspace decomposition of a cyclic Galois extension in Kummer's proof that a cyclic extension is radical ("Hilbert's Theorem 90"). It also appears in an essential way in the formula for δ_0.

It is well known that the prime p splits in $\mathbb{Z}[\varepsilon]$ into $\varphi(p-1)$ prime ideals with multiplicity 1. In the above notation, they are $(p, a-\varepsilon^i)$ for i coprime to $p-1$. The element $\frac{a-\varepsilon}{p}$ of the cyclotomic field $\mathbb{Q}[\varepsilon]$ is thus regular at the prime $P_1 = (p, a-\varepsilon)$, but has a pole at all the other primes over p. Allowing it in the coordinate ring of $\mathbb{TO}_{p,0}$ thus keeps a neighbourhood of P_1, but localises away from the other primes over p. In fact without this localisation, $\operatorname{Spec} A_0$ has orbifold singularities at each of the other primes over p, and the restriction of δ_1 to A_0 would map to the invariants $(A_1 \otimes A_1)^{\boldsymbol{\mu}_{p-1}}$, but not to $A_0 \otimes A_0$.

An addendum on this construction is on the website [10], supplementing the treatment of [13] with a detailed treatment of the case $p = 11$, and computer algebra routines that work instantly for primes up to 30.

ACKNOWLEDGMENTS

The context for this work includes p-closed vector fields and inseparable covers, much of which I learned from Shafarevich while he was working on his paper on K3 surfaces [11] with Rudakov. It is a pleasure to acknowledge this debt by dedicating the paper to his memory.

My involvement with group schemes of order p started during a visiting professorship at Sogang University, Seoul, on a Korean government grant, in connection with Soonyoung Kim's 2014 PhD thesis [5] on Godeaux surfaces. I am extremely grateful to Yongnam Lee for his work setting up and administering the grant, for his generous hospitality, and for setting the thesis problem. Different aspects of my work benefited from extended stays at Sogang University and at KIAS over many years.

FUNDING

The bulk of this paper was written during a spring 2019 residence at MSRI, Berkeley, California, supported by NSF grant no. 1440140.

REFERENCES

1. E. Bombieri and D. Mumford, "Enriques' classification of surfaces in char. p. III," Invent. Math. **35**, 197–232 (1976).
2. W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I: The user language," J. Symb. Comput. **24** (3–4), 235–265 (1997).
3. P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques," in *Modular Functions of One Variable II: Proc. Int. Summer Sch., Antwerp, 1972* (Springer, Berlin, 1973), Lect. Notes Math. **349**, pp. 143–316.
4. N. Jacobson, *Lectures in Abstract Algebra,* Vol. III: *Theory of Fields and Galois Theory* (D. Van Nostrand, Princeton, NJ, 1964).
5. S. Kim, "Numerical Godeaux surfaces with an involution in positive characteristic," Proc. Japan Acad., Ser. A **90** (8), 113–118 (2014).
6. C. Liedtke, "Arithmetic moduli and lifting of Enriques surfaces," J. Reine Angew. Math. **706**, 35–65 (2015).
7. "Magma calculator," http://magma.maths.usyd.edu.au/calc/
8. P. M. Nanninga, "Cauchy–Mirimanoff and related polynomials," J. Aust. Math. Soc. **92** (2), 269–280 (2012).
9. P. M. Nanninga, "On Cauchy–Mirimanoff and related polynomials," PhD Thesis (Aust. Natl. Univ., Canberra, 2013).
10. M. Reid, "The Tate–Oort group scheme $\mathbb{TO}_p$ and Godeaux surfaces," https://www.warwick.ac.uk/staff/Miles.Reid/TOp
11. A. N. Rudakov and I. R. Šafarevič, "Inseparable morphisms of algebraic surfaces," Math. USSR, Izv. **10** (6), 1205–1237 (1976) [transl. from Izv. Akad. Nauk SSSR, Ser. Mat. **40** (6), 1269–1307 (1976)].
12. J. Tate, "Finite flat group schemes," in *Modular Forms and Fermat's Last Theorem: Papers from a Conf., Boston, 1995* (Springer, New York, 1997), pp. 121–154.
13. J. Tate and F. Oort, "Group schemes of prime order," Ann. Sci. Éc. Norm. Supér., Sér. 4, **3**, 1–21 (1970).