# GENERALIZATIONS OF QUASIELLIPTIC CURVES

CESAR HILARIO AND STEFAN SCHRÖER

*Second revised version, 11 September 2023*

Abstract. We generalize the notion of quasielliptic curves, which have infinitesimal symmetries and exist only in characteristic two and three, to a hierarchy of regular curves having infinitesimal symmetries, defined in all characteristics and having higher genera. This relies on the study of certain infinitesimal group schemes acting on the affine line and certain compactifications. The group schemes are defined in terms of invertible additive polynomials over rings with nilpotent elements, and the compactification is constructed with the theory of numerical semigroups. The existence of regular twisted forms relies on Brion's recent theory of equivariant normalization. Furthermore, extending results of Serre from the realm of group cohomology, we describe non-abelian cohomology for semidirect products, to compute in special cases the collection of all twisted forms.

## Contents



## Introduction

Let $K$ be a ground field of characteristic $p > 0$. The goal of this paper is to generalize, in an equivariant way, the *rational cuspidal curve*

$$X = \operatorname{Spec} K[T^2, T^3] \cup \operatorname{Spec} K[T^{-1}] \tag{1}$$

from the cases $p = 2$ and $p = 3$, when the automorphism group scheme is non-reduced, to a hierarchy of integral curves $X_{p,n}$ whose automorphism group schemes

2010 *Mathematics Subject Classification.* 14G17, 14L15, 14L30, 14H45, 20M25, 20J06, 14D06.

are likewise non-reduced. Here the index $p > 0$ indicates the characteristic, and $p^{n(n+1)/2}$ gives the "size" of non-reducedness.

Our motivations originates from the *Enriques classification* of algebraic surfaces over ground fields $k = k^{\mathrm{alg}}$: This vast body of theorems on the structure of surfaces $S$ was extended by Bombieri and Mumford to positive characteristics ([6] and [5]). Their main insight was the introduction and analysis of *quasielliptic fibrations*, which are morphisms $f : S \to B$ whose generic fiber $Y = f^{-1}(\eta)$ is a so-called *quasielliptic curve*, in other words, a twisted form of (1) over the function field $K = k(B)$, with all local rings $\mathscr{O}_{Y,y}$ regular. One knows that such twisted forms exist only over imperfect fields of characteristic $p \leq 3$, and Queen gave explicit equations for them ([31] and [32]), although of rather extrinsic nature.

We discovered the hierarchy $X = X_{p,n}$ somewhat accidentally, while seeking a deeper and more intrinsic understanding of quasielliptic curves. The curves do not reveal themselves in any direct way; one has to understand them through their *automorphism group scheme* $\mathrm{Aut}_{X/K}$. Its crucial part are certain infinitesimal group schemes $U_n$ of order $p^{n(n+1)/2}$ acting in a canonical way on the affine line $\mathbb{A}^1 = \operatorname{Spec} K[T^{-1}]$. The underlying scheme is $\alpha_{p^n} \times \alpha_{p^{n-1}} \times \ldots \times \alpha_p$, a singleton formed with iterated Frobenius kernels of the additive group, but endowed with a non-commutative group law. Its definition relies on the so-called *additive polynomials* $\sum_{i=0}^{n} \lambda_i T^{-p^i}$, or equivalently the elements of the *skew polynomial ring* $R[F;\sigma]$, formed over rings with nilpotent elements.

According to Brion's recent theory of *equivariantly normal curves* [9], there is a unique compactification $\mathbb{A}^1 \subset X_{p,n}$ to which the action of $U_n$ extends in an optimal way. In general, it is very difficult to unravel the structure of such compactifications, but here we were able to "guess" an explicit description in terms of the *numerical semigroups*

$$\Gamma_{p,n} = \langle p^n, p^n - p^{n-1}, \ldots, p^n - p^0 \rangle \subset \mathbb{N},$$

a monoid that comprises all but finitely many natural numbers. The guesswork was assisted by computer algebra computations with Magma and GAP, performed in a handful of special cases. Our first main result is that the ensuing toric compactification has an intrinsic meaning:

**Theorem.** *(See Thm. 4.4 and Thm. 8.4) The $U_n$-action on the affine line extends to the compactification*

$$X_{p,n} = \operatorname{Spec} K[T^{\Gamma_{p,n}}] \cup \operatorname{Spec} K[T^{-1}],$$

*and this projective curve is equivariantly normal with respect to the $U_n$-action.*

For $3 \leq p^n \leq 4$ this is precisely the rational cuspidal curve. The second main result unravels the numerical invariants and infinitesimal symmetries of this hierarchy of projective curves:

**Theorem.** *(See Section 5 and Thm. 7.1) The curves $X = X_{p,n}$ have*

$$h^1(\mathscr{O}_X) = \frac{1}{2}(np^{n+1} - (n+2)p^n + 2) \quad \textit{and} \quad \mathrm{Aut}_{X/K} = \mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m.$$

In this *iterated semidirect product*, the additive group $\mathbb{G}_a$ is normalized by the infinitesimal group scheme $U_n$, and both are normalized by the multiplicative group

$\mathbb{G}_m$. Note that for $3 \leq p^n \leq 4$ this precisely gives back the computation of Bombieri and Mumford ([5], Proposition 6), and the above should be seen as a natural generalization.

The computation of the genus relies on general results of Delorme [11] on numerical semigroups, applied to our $\Gamma_{p,n}$. The determination of the automorphism group is based on further surprising properties of the projective curves $X = X_{p,n}$: The tangent sheaf $\Theta_{X/K} = \underline{\mathrm{Hom}}(\Omega^1_{X/K}, \mathscr{O}_X)$ turns out to be invertible, actually very ample, giving a canonical inclusion $X \subset \mathbb{P}(\mathfrak{g}) = \mathbb{P}^{n+1}$, where $\mathfrak{g} = H^0(X, \Theta_{X/K})$ is the Lie algebra of the automorphism group scheme $G = \mathrm{Aut}_{X/K}$. From the canonical linearization $\mathscr{O}_X(1) = \Theta_{X/K}$ we get a matrix representation for $G$, which is crucial to gain control on its structure. Furthermore, $X$ is *globally a complete intersection*, defined inside $\mathbb{P}^{n+1}$ by the following $n$ homogeneous equations of degree $p$:

$$U_{n-1}^p - V^{p-1}Z = 0 \quad \text{and} \quad U_j^p - V^{p-1}U_{j+1} = 0 \quad (0 \leq j \leq n-2).$$

Also note that the curves are related by a hierarchy of blowing-ups $X_{p,n-1} = \mathrm{Bl}_Z(X_{p,n})$, where the center is the singular point (Lemma 7.3).

Again building on Brion's theory of equivariantly normal curves [9], we show that our $X = X_{p,n}$ have, over ground fields $K$ with "enough" imperfection, twisted forms $Y$ where all local rings $\mathscr{O}_{Y,y}$ are regular (Theorem 8.4). These have the same structural properties of $X$, except that the singularities get "twisted away". In turn, the passage from the rational cuspidal curve to quasielliptic curves is generalized to our hierarchy $X = X_{p,n}$.

The above relies on rather general observations, which indeed form the third main result of this paper:

**Theorem.** *(See Section 8) Let $X$ be a geometrically integral curve with the action of a finite group scheme $G$. Suppose $\mathrm{Sing}(X/K)_{\mathrm{red}}$ is étale. Then $X$ is equivariantly normal if and only if for some field extension $K \subset L$, the base-change $X \otimes L$ admits a twisted form that is regular.*

Quasielliptic fibrations play a crucial role in the arithmetic of algebraic surfaces of special type, in particular for K3 surfaces and Enriques surfaces (for an example see [38]). We expect that twists over function fields of our $X = X_{p,n}$ play a similar role for surfaces of general type.

By the general theory of non-abelian cohomology and twisted forms, one may view the collection $\mathrm{Twist}(X)$ of isomorphism classes of twisted forms over $S = \mathrm{Spec}(K)$ as non-abelian cohomology $H^1(S, \mathrm{Aut}_{X/S})$. For our curves $X = X_{p,n}$ we determined the automorphism group scheme. This raises the question of how to compute non-abelian cohomology for semidirect products in general. We indeed establish effective techniques to do so, and are able apply them at least in the cases $n \leq 2$. Our fourth main result is:

**Theorem.** *(See Thm. 10.7) For $G = \mathbb{G}_a \rtimes U_2 \rtimes \mathbb{G}_m$, the non-abelian cohomology is*

$$H^1(S, G) = \bigcup K/\{u^{p^2} - v - \alpha v^p - \beta^p v^{p^2} \mid u, v \in K\},$$

*where the union runs over $(\alpha, \beta) \in \bigcup_{K/K^{p^2}} K/K^p$, with $\alpha \in K/K^{p^2}$ and $\beta \in K/K^p$.*

Perhaps this is the first explicit determination of $\mathrm{Twist}(X)$ via a purely non-abelian cohomological computation of $H^1(S, \mathrm{Aut}_{X/S})$, for some relevant hierarchy of schemes $X$. A crucial step in this is the determination of particular twisted forms ${}^P\mathbb{G}_a$ in the form given by Russell [35], a technique likely to be of independent interest.

Let us quote Bombieri and Mumford ([5], page 198): "The study of special low characteristics can be one of two types: amusing or tedious. It all depends on whether the peculiarities encountered are felt to be meaningful variations of the general picture [...] or are felt instead to be accidental and random, due for instance to numerological interactions [...]". We think that our results amply show that what Bombieri and Mumford have uncovered for $p \leq 3$ is indeed far from accidental, and belong to a structural hierarchy that indeed can be understood from general principles.

The paper is organized as follows: In Section 1 we develop the theory of additive polynomials, over rings that contain nilpotents, study the resulting groups of units, and introduce $U_n(R)$. The ensuing actions on polynomial rings are discussed in Section 2. Building on these preparations, we give in Section 3 a scheme-theoretic re-interpretation, and determine the Lie algebra and the upper and lower central series for the infinitesimal group scheme $U_n$. In Section 4 we examine the equivariant compactifications of the affine line $\mathbb{A}^1$, and introduce our numerical semigroup $\Gamma_{p,n}$ and the ensuing curve $X_{p,n}$, which turns out to be equivariantly normal. We determine the numerical invariants and deduce several crucial geometric consequences in Section 5. In Section 6 we show that our curve can also be seen as a global complete intersection $X_{p,n} \subset \mathbb{P}^{n+1}$. In Section 7 its automorphism group scheme is determined. Section 8 contains general results on the relation between equivariant normality and the existence of twisted forms that are regular, which is then applied to our curves $X_{p,n}$. Section 9 is devoted to twisting and the computation of non-abelian cohomology for semidirect products. We apply this in Section 10 to describe the collection of all twisted forms of $X_{p,n}$ in the cases $n = 1$ and $n = 2$.

**Acknowledgement.** We heartily thank the two referees for thorough reading and many valuable suggestions, which helped to improve the paper. The research was conducted in the framework of the research training group *GRK 2240: Algebro-Geometric Methods in Algebra, Arithmetic and Topology.*

## 1. Invertible additive polynomials

In this section we gather purely algebraic facts that go into the definition of our infinitesimal group scheme $U = U_n$ in Section 3. Fix some ring $R$ of characteristic $p > 0$, and let $x$ be an indeterminate. Recall that polynomials of the form

$$P(x) = \sum_{i=0}^{n} \lambda_i x^{p^i} = \lambda_0 x + \lambda_1 x^p + \ldots + \lambda_n x^{p^n} \in R[x]$$

are called *additive polynomials*. Another widespread designation is *p-polynomials*. Clearly, the set of all such polynomials is stable under addition $P(x) + Q(x)$ and substitution $P(Q(x))$. These two composition laws enjoy the distributive property. In fact, the additive polynomials form an *associative ring* with respect to these laws,

with zero element $P(x) = 0$ and unit element $P(x) = x$. Let us call it the *ring of additive polynomials*.

It can also be seen as the *skew polynomial ring* $R[F;\sigma]$, where $\sigma : R \to R$ designates the Frobenius map $\lambda \mapsto \lambda^p$. Elements are polynomials in the formal symbol $F$, and multiplication is subject to the relations $F\lambda = \lambda^p F$. In other words, we have

$$\sum_i \lambda_i F^i \cdot \sum_j \mu_j F^j = \sum_k \Big( \sum_{i+j=k} \lambda_i \mu_j^{p^i} \Big) F^k, \tag{2}$$

a modification of the usual Cauchy multiplication. The identification of the skew polynomial ring with the ring of additive polynomials is given by $\lambda \mapsto \lambda x$ and $F \mapsto x^p$, such that $\sum \lambda_i F^i$ corresponds to $\sum \lambda_i x^{p^i}$. For psychological reasons, we strongly prefer to make computations in the skew polynomial ring. In the next section, when it comes to actions on the affine line, we shall turn back to the ring of additive polynomials.

Over ground fields, the ring of additive polynomials was introduced and studied by Ore [30]. A discussion from the perspective of skew polynomial rings was given by Jacobson ([22], Chapter 3). More recent presentations appear in [18], Chapter 1 and [17], Chapter 2. For our purposes, however, it will be crucial to allow nilpotent elements. The following two propositions reveal that nilpotent and invertible elements in $R[F;\sigma]$ are characterized as in usual polynomial rings:

**Proposition 1.1.** *An element $\sum_{i=0}^n \lambda_i F^i$ of the skew polynomial ring $R[F;\sigma]$ is nilpotent if and only if $\lambda_0, \dots, \lambda_n \in \mathrm{Nil}(R)$.*

*Proof.* Suppose all coefficients are nilpotent, say $\lambda_i^d = 0$. For each $r \geq 0$ we have

$$\Big(\sum_i \lambda_i F^i\Big)^r = \sum_k \Big( \sum_{i_1+\ldots+i_r=k} \lambda_{i_1}^{v_1} \dots \lambda_{i_r}^{v_r} \Big) F^k$$

for certain exponents $v_1, \dots, v_r \geq 1$ whose precise values are irrelevant in the following reasoning: If $r > (n+1)(d-1)$, each tuple $0 \leq i_1, \dots, i_r \leq n$ must contain the $d$-fold repetition of at least one value $0 \leq i \leq n$. Then the product $\lambda_{i_1}^{v_1} \dots \lambda_{i_r}^{v_r}$ vanishes, and so does the above $r$-fold power.

Conversely, suppose some $\lambda_s \in R$ is not nilpotent. Choose a prime $\mathfrak{p} \subset R$ not containing $\lambda_s$, and set $K = \kappa(\mathfrak{p})$. Then the image of $\sum_{i=0}^n \lambda_i F^i$ in the skew polynomial ring $K[F;\sigma]$ is a non-zero nilpotent element. On the other hand, $K[F;\sigma]$ is a domain (this follows from [22], Chapter 3, Section 1, bottom paragraph on page 29), contradiction. □

This has an important consequence:

**Proposition 1.2.** *An element $P = \sum_{i=0}^n \lambda_i F^i$ of the skew polynomial ring $R[F;\sigma]$ is invertible if and only if $\lambda_0 \in R^\times$ and $\lambda_1, \dots, \lambda_n \in \mathrm{Nil}(R)$.*

*Proof.* The condition is sufficient: Set $\mu_i = -\lambda_i/\lambda_0$. By Proposition 1.1, the element $Q = \sum_{i=1}^n \mu_i F^i$ is nilpotent, say $Q^r = 0$. Then $1 - Q$ is a unit, with inverse $\sum_{j=0}^{r-1} Q^j$. Thus $P = \lambda_0(1-Q)$ is also a unit.

Conversely, suppose that $PQ = QP = 1$. From the group law (2) one immediately infers that $\lambda_0 \in R^\times$. Seeking a contradiction, we assume that some $\lambda_s \in R$, $s \geq 1$

is not nilpotent. Choose such $1 \leq s \leq n$ maximal. As above, we find some residue field $K = \kappa(\mathfrak{p})$ in which $\lambda_s$ is non-zero. Let $d \geq 0$ be the degree of the image of $Q$. From (2) one sees that the image of $1 = PQ$ has non-zero term in degree $s + d$, contradiction. □

Given a unit of the form $P = \sum \lambda_i F^i$, the inverse $P^{-1} = \sum \mu_j F^j$ can be computed as follows: The condition $P \cdot P^{-1} = 1$ means $\lambda_0 \mu_0^{p^0} = 1$, and $\sum_{i+j=k} \lambda_i \mu_j^{p^i} = 0$ for $k \geq 1$, which give the recursion formula

$$\mu_0 = \lambda_0^{-1} \quad \text{and} \quad \mu_k = -\frac{1}{\lambda_0} \sum_{i=1}^{k} \lambda_i \mu_{k-i}^{p^i} \quad (k \geq 1). \tag{3}$$

The skew polynomial ring comes with an infinite-dimensional matrix representation $R[F;\sigma] \to \mathrm{Mat}_\infty(R)$, already determined by the assignments

$$\lambda \longmapsto \begin{pmatrix} \lambda & & & \\ & \lambda^p & & \\ & & \lambda^{p^2} & \\ & & & \ddots \end{pmatrix} \quad \text{and} \quad F \longmapsto \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & 0 & 1 \\ & & & \ddots & \ddots \end{pmatrix}.$$

More explicitly, this homomorphism is given by

$$\sum_{i=0}^{n} \lambda_i F^i \longmapsto (\lambda_{s-r}^{p^r})_{0 \leq r \leq s < \infty} = \begin{pmatrix} \lambda_0 & \lambda_1 & \lambda_2 & \cdots & \\ & \lambda_0^p & \lambda_1^p & \lambda_2^p & \cdots \\ & & \lambda_0^{p^2} & \lambda_1^{p^2} & \lambda_2^{p^2} & \cdots \\ & & & \ddots & \ddots & \ddots \end{pmatrix}. \tag{4}$$

Obviously, the map is injective and takes values in the row-finite upper triangular matrices. Note that for each $d \geq 0$, the top left submatrix indexed by $0 \leq r, s \leq d-1$ yields a subrepresentation $R[F;\sigma] \to \mathrm{Mat}_d(R)$.

We now examine the unit group $R[F;\sigma]^\times$ in more detail, for the time being as an abstract group. It comes with matrix representations $R[F;\sigma]^\times \to \mathrm{GL}_d(R)$, $d \geq 0$. Note that this factors over the group of invertible upper triangular matrices $T_d(R) \subset \mathrm{GL}_d(R)$. Write $\mathrm{Fil}^d$ for the kernels. Clearly $\mathrm{Fil}^0 = R[F;\sigma]^\times$, whereas

$$\mathrm{Fil}^d = \{1 + \sum_{i=d}^{n} \lambda_i F^i \mid n \geq d \text{ and } \lambda_i \in \mathrm{Nil}(R)\} \quad (d \geq 1).$$

These form a descending chain of normal subgroups, in other words, a *normal series*. Clearly, their intersection contains only the unit element.

**Proposition 1.3.** *The normal series* $\mathrm{Fil}^d$ *on* $R[F;\sigma]^\times$ *has quotients*

$$\mathrm{Fil}^0 / \mathrm{Fil}^1 = R^\times \quad \textit{and} \quad \mathrm{Fil}^d / \mathrm{Fil}^{d+1} = \mathrm{Nil}(R) \quad (d \geq 1).$$

*Moreover, we have the commutator formula* $[\mathrm{Fil}^1, \mathrm{Fil}^d] \subset \mathrm{Fil}^{d+1}$ *for all* $d \geq 1$.

*Proof.* The first assertion is an immediate consequence of the group law (2). The commutator formula follows from a corresponding commutator formula for the *unitriangular group* $\mathrm{UT}_d(R) \subset \mathrm{GL}_d(R)$ comprising upper triangular matrices with the unit element on the diagonal (confer [23], Chapter 6, Example 16.1.2). □

The multiplicative character $R[F;\sigma]^\times \to \mathrm{GL}_1(R) = R^\times$ given by $\sum \lambda_i F^i \mapsto \lambda_0$ comes with a canonical splitting $\mu \mapsto \mu F^0$, so we get a semidirect product $R[F;\sigma]^\times = \mathrm{Fil}^1 \rtimes R^\times$. The ensuing conjugacy action of $R^\times$ is given by

$$\mu(\sum \lambda_i F^i)\mu^{-1} = \sum \mu^{1-p^i}\lambda_i F^i.$$

For our applications it will be important to consider certain smaller subgroups inside the unit group, and the following is crucial throughout:

**Proposition 1.4.** *For each integer $n \geq 0$, the set*

$$U_n(R) = \{1 + \sum_{i=1}^{n} \lambda_i F^i \mid \lambda_i^{p^{n-i+1}} = 0 \text{ for all } 1 \leq i \leq n\}$$

*is a subgroup inside the unit group $R[F;\sigma]^\times$, which is normalized by $R^\times \subset R[F;\sigma]^\times$.*

*Proof.* Clearly the set contains the unit element. Suppose $P = 1 + \sum_{i=1}^n \lambda_i F^i$ and $Q = 1+\sum_{j=1}^n \mu_j F^j$ belong to $U_n(R)$, and write the product as $PQ = 1+\sum_{k=1}^m \alpha_k F^k$, with coefficients $\alpha_k = \sum_{i+j=k} \lambda_i \mu_j^{p^i}$. For $k \geq n+1$, each summand $\lambda_i \mu_j^{p^i}$ vanishes: If $j \geq n+1$ we already have $\mu_j = 0$, and if $j \leq n$ we get $i = k - j \geq n + 1 - j$ and thus $\mu_j^{p^i} = 0$. For $k \leq n$, we have $\alpha_k^{p^{n-k+1}} = \sum_{i+j=k} \lambda_i^{p^{n-k+1}} \mu_j^{p^{n-j+1}}$, which vanishes because $\mu_j^{p^{n-j+1}} = 0$. Thus $PQ \in U_n(R)$.

Next consider the inverse element $P^{-1} = \sum_{j\geq 0} \beta_j F^j$. The recursion formula (3) gives $\beta_0 = 1$ and $\beta_k = -\sum_{i=1}^k \lambda_i \beta_{k-i}^{p^i}$ for $k \geq 1$. For $k \geq n+1$ each summand $\lambda_i \beta_{k-i}^{p^i}$ vanishes, because $i \geq n - (k-i) + 1$. For $k \leq n$ we have $(\lambda_i \beta_{k-i}^{p^i})^{p^{n-k+1}} = \lambda_i^{p^{n-k+1}} \beta_{k-i}^{p^{n-(k-i)+1}}$, where the second factor vanishes. Thus $P^{-1} \in U_n(R)$.

Finally, for each $\mu \in R^\times$, we have $\mu \cdot P \cdot \mu^{-1} = 1 + \sum_{i=1}^n \mu^{1-p^i}\lambda_i F^i$, which clearly belongs to $U_n(R)$. So the latter is normalized by $R^\times$. □

## 2. Actions on polynomial rings

We keep the set-up as in the previous section. Obviously, the multiplicative monoid of additive polynomials $\sum \lambda_i x^{p^i}$ acts on the polynomial ring $R[x]$ via substitution of the indeterminate, in other words by $P(x) \mapsto P(\sum \lambda_i x^{p^i})$, and one easily checks that this is an action *from the right*. In turn, we have a group action $R[x] \times R[F;\sigma]^\times \to R[x]$ from the right, given by

$$Q(x) * \sum \lambda_i F^i = Q(\sum \lambda_i x^{p^i}). \tag{5}$$

Note that the action of the multiplicative group $\mathbb{G}_m(R) = R^\times$ via $Q(x)*\lambda_0 = Q(\lambda_0 x)$ is a special case of this. Furthermore, we have the translation action of the additive group $\mathbb{G}_a(R) = R$, defined by

$$Q(x) * \alpha = Q(x + \alpha). \tag{6}$$

Obviously, these actions are faithful, and we arrive at inclusions of $\mathbb{G}_a(R)$ and $R[F;\sigma]^\times$ into the opposite automorphism group of $R[x]$.

**Proposition 2.1.** *Inside the opposite automorphism group of $R[x]$, the group $\mathbb{G}_a(R)$ is normalized by $R[F;\sigma]^\times$, and the intersection $\mathbb{G}_a(R) \cap R[F;\sigma]^\times$ is trivial.*

*Proof.* Suppose we have elements

$$\alpha \in \mathbb{G}_a(R) \quad \text{and} \quad \sum \lambda_i F^i \in R[F;\sigma]^\times.$$

For the first assertion, it suffices to check that $P \cdot \mathbb{G}_a(R) = \mathbb{G}_a(R) \cdot P$. This indeed holds, because one computes $\sum \lambda_i (x+\alpha)^{p^i} = (\sum \lambda_i x^{p^i}) + \alpha'$ with $\alpha' = \sum_{i=0}^n \lambda_i \alpha^{p^i}$. It remains to verify the assertion on the intersection. Suppose that $\alpha = P$ as automorphisms of $R[x]$, in other words $x + \alpha = \sum \lambda_i x^{p^i}$. Comparing coefficients at the constant terms gives $\alpha = 0$, hence the intersection $\mathbb{G}_a(R) \cap R[F;\sigma]^\times$ is trivial. □

In turn, we get an inclusion of $\mathbb{G}_a(R) \rtimes R[F;\sigma]^\times$ into the opposite automorphism group of $R[x]$. Later, we seek to extend part of this action to certain subrings of $R[x^{-1}]$ in a compatible way. The following observation will be useful: Let $S \subset R[x]$ be the multiplicative system of all monic polynomials. The resulting localization is denoted by $R(x) = S^{-1}R[x]$. Since monic polynomials are regular elements from the polynomial ring, the localization map is injective, and we get an inclusion $R[x] \subset R(x)$.

**Proposition 2.2.** *The action from the right of the group $\mathbb{G}_a(R) \rtimes R[F;\sigma]^\times$ on the polynomial ring $R[x]$ uniquely extends to $R(x)$.*

*Proof.* Uniqueness immediately follows from the universal property of localizations. To see existence, consider the larger multiplicative system $\tilde{S} \subset R[x]$ comprising the polynomials of the form $\lambda P + Q$ with $P$ monic, $Q$ nilpotent, and $\lambda \in R^\times$. Obviously, this system is stable with respect to the actions (5) and (6), and we thus get an induced action on $\tilde{S}^{-1}R[x]$. On the other hand, the inclusion $S \subset \tilde{S}$ gives a canonical map $S^{-1}R[x] \to \tilde{S}^{-1}R[x]$. It remains to verify that every $\lambda P + Q$ as above becomes invertible in $S^{-1}R[x]$. Indeed, in the factorization $\lambda P + Q = P/1 \cdot (\lambda + Q/P)$ also the second factor is a unit, because $\lambda$ is invertible and $Q/P$ is nilpotent. □

## 3. Scheme-theoretic reinterpretation

Fix a ground field $K$ of characteristic $p > 0$. In this section we take a more geometric point of view and reinterpret and extend the results of the preceding sections in terms of schemes and group schemes. We now regard

$$U_n(R) = U_{n,K}(R) = \{1 + \sum_{i=1}^n \lambda_i F^i \in R[T;\sigma]^\times \mid \lambda_i^{p^{n-i+1}} = 0 \text{ for } 1 \le i \le n\}$$

as a group-valued functor $U_n$ on the category of $K$-algebras $R$. Clearly, the natural transformation

$$\alpha_{p^n} \times \alpha_{p^{n-1}} \times \ldots \times \alpha_p \longrightarrow U_n, \quad (\lambda_1, \ldots, \lambda_n) \longmapsto 1 + \sum_{i=1}^n \lambda_i F^i \tag{7}$$

is an isomorphism of set-valued functors, with group laws ignored. In turn, $U_n$ is a finite group scheme with coordinate ring $\bigotimes_{i=1}^n K[x_i]/(x_i^{p^{n-i+1}})$ and order $|U_n| = h^0(\mathscr{O}_{U_n}) = p^{n(n+1)/2}$. It contains but one point, and is thus an *infinitesimal group scheme*.

One immediately sees that the restriction of (7) to $\alpha_p^{\oplus n} = \alpha_p \times \ldots \times \alpha_p$ respects the group laws, and gives an inclusion of group schemes $\alpha_p^{\oplus n} \subset U_n$. Furthermore, for every $m \leq n$ we have canonical inclusions $U_m \subset U_n$ of group schemes.

Recall that each scheme $X$ over our ground field $K$ comes with a *relative Frobenius map* $F : X \to X^{(p)}$, given in functorial terms by $X(R) \stackrel{F}{\to} X({}_FR) = X^{(p)}(R)$. Here ${}_FR$ denotes the abelian group $R$, viewed as an $R$-algebra via the absolute Frobenius map $f \mapsto f^p$, and $X^{(p)} = X \otimes_K ({}_FK)$. Note that $R = {}_FR$ as an $\mathbb{F}_p$-algebra. Hence $X(R) = X({}_FR)$ and thus $X = X^{(p)}$, provided that $X$ arises as base-change from the prime field $\mathbb{F}_p$. For our group scheme $U_n$, the relative Frobenius map takes the form

$$U_n(R) \longrightarrow U_n({}_FR) = U_n(R), \quad 1 + \sum \lambda_i F^i \longmapsto 1 + \sum \lambda_i^p F^i.$$

**Proposition 3.1.** *The image of $F : U_n \to U_n$ is the subgroup scheme $U_{n-1}$, and its kernel is given by $\alpha_p^{\oplus n}$. In particular, we have an identification of restricted Lie algebras* $\mathrm{Lie}(U_n) = K^n$.

*Proof.* Obviously, the Frobenius map factors over the subgroup scheme $U_{n-1} \subset U_n$. The resulting $F : U_n \to U_{n-1}$ is indeed an epimorphism, because any $R$-valued point $1 + \sum \mu_i F^i$ of $U_{n-1}$ arises of the $R'$-valued point $1 + \sum \lambda_i$ from $U_n$, for the fppf extension $R' = \bigotimes R[\lambda_i]/(\lambda_i^p - \mu_i)$.

An $R$-valued point $1 + \sum \lambda_i F^i$ belongs to the kernel of the Frobenius map if and only if $\lambda_i^p = 0$, and hence $U_n[F] = \alpha_p^{\oplus n}$. The last assertion follows, because $\mathrm{Lie}(\alpha_p^{\oplus n}) = K^n$, and for any group scheme the inclusion of the Frobenius kernel induces a bijection on Lie algebras. □

In turn, the relative Frobenius map $F : U_n \to U_n$ yields an extension

$$0 \longrightarrow \alpha_p^{\oplus n} \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1. \tag{8}$$

By induction on $n \geq 0$ we infer that the finite group scheme $U_n$ admits a composition series with quotients isomorphic to $\alpha_p$. In particular, $U_n$ is *unipotent*. Since all Lie brackets are trivial, the adjoint representation $\mathrm{ad} : \mathfrak{u}_n \to \mathfrak{gl}(\mathfrak{u}_n)$ of the Lie algebra $\mathfrak{u}_n = \mathrm{Lie}(U_n)$ is trivial, and the adjoint representation $\mathrm{Ad} : U_n \to \mathrm{GL}_{\mathfrak{u}_n/k}$ of the group scheme factors over the quotient $U_{n-1}$. It is not difficult to determine the latter representation: Since the group $U_n(K)$ is trivial, we have

$$\mathrm{Lie}(U_n) = U_n(K[\epsilon]) = \{1 + \epsilon \sum_{r=1}^{n} \alpha_r F^r \mid \alpha_r \in K\},$$

where $\epsilon$ denotes an indeterminate subject to $\epsilon^2 = 0$. The elements $1 + \epsilon F^r$, $1 \leq r \leq n$ form a basis of this $K$-vector space. With $P = \sum \lambda_i F^i$ where $\lambda_0 = 1$, and using the relations $\epsilon^2 = 0$ and $F\epsilon = 0$, we get

$$P^{-1} \cdot (1 + \epsilon F^s) \cdot P = 1 + \epsilon F^s P = 1 + \epsilon \sum_{i=0}^{n-s} \lambda_i^{p^s} F^{s+i} = \prod_{i=0}^{n-s} (1 + \epsilon \lambda_i^{p^s} F^{s+i}).$$

Consequently $\mathrm{Ad}(P^{-1})$ sends the basis vector $e_s = 1 + \epsilon F^s$ to the linear combination $\sum_{r=s}^{n} \lambda_{r-s}^{p^s} e_r$. Summing up, in the restricted Lie algebra $\mathrm{Lie}(U_n) = K^n$ all brackets and $p$-powers are zero, and the adjoint representation of the group scheme is given by $(\sum \lambda_i F^i)^{-1} \mapsto (\lambda_{r-s}^{p^s})_{n \geq r \geq s \geq 1}$.

As described in Section 2, the groups $U_n(R)$ act from the right on the polynomial ring $R[x]$ via $R$-linear maps. This is obviously functorial in $R$, and thus constitutes an action of the group scheme $U_n$ on the affine line $\mathbb{A}^1 = \operatorname{Spec} K[x]$. Note that this is indeed an action *from the left*. On $R$-valued points, it is given by

$$(\lambda_1, \dots, \lambda_n) * \mu = \sum_{i=0}^{n} \lambda_i F^i * \mu = \sum_{i=0}^{n} \lambda_i \mu^{p^i},$$

where we set $\lambda_0 = 1$ for convenience. Of course, we also have the canonical actions of the multiplicative group $\mathbb{G}_m$ and the additive group $\mathbb{G}_a$, given via $\lambda_0 * \mu = \lambda_0 \mu$ and $\alpha * \mu = \mu + \alpha$, respectively. The following generalizes a key observation of Bombieri and Mumford ([5], Proposition 6):

**Proposition 3.2.** *The above actions of the three group schemes on the affine line are faithful. Inside the sheaf* $\operatorname{Aut}_{\mathbb{A}^1/K}$*, the group scheme* $\mathbb{G}_a$ *is normalized by* $U_n$*, and both* $\mathbb{G}_a$ *and* $U_n$ *are normalized by* $\mathbb{G}_m$*. Moreover, the intersections*

$$\mathbb{G}_a \cap U_n \quad \textit{and} \quad (\mathbb{G}_a \rtimes U_n) \cap \mathbb{G}_m$$

*inside the sheaf* $\operatorname{Aut}_{\mathbb{A}^1/K}$ *are trivial.*

*Proof.* The assertions follow from Proposition 2.1 and Proposition 1.4. □

We thus have an *iterated semidirect product*, for simplicity written as

$$\mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m = (\mathbb{G}_a \rtimes U_n) \rtimes \mathbb{G}_m = \mathbb{G}_a \rtimes (U_n \rtimes \mathbb{G}_m), \tag{9}$$

acting faithfully on the affine line $\mathbb{A}^1 = \operatorname{Spec} K[x]$. In turn, we get an inclusion of restricted Lie algebras

$$K \rtimes \operatorname{Lie}(U_n) \rtimes \mathfrak{gl}_1(K) \subset \operatorname{Lie}(\operatorname{Aut}_{\mathbb{A}^1/K}) = \operatorname{Der}_K(K[x]).$$

The elements in the left-hand side can be seen as tuples $(\alpha, \lambda_1, \dots, \lambda_n, \lambda_0)$, and correspond to the $K$-derivation $\alpha \frac{\partial}{\partial x} + \sum_{i=1}^{n} \lambda_i x^{p^i} \frac{\partial}{\partial x} + \lambda_0 x \frac{\partial}{\partial x}$ of the polynomial ring $K[x]$. For example, the derivation $\lambda_1 x^p \partial/\partial x \in \operatorname{Lie}(U_n)$ acts via $x \mapsto x + \epsilon \lambda_1 x^p$, which coincides with the action of the group element $1 + \epsilon \lambda_1 F \in U_n(k[\epsilon])$.

The spectrum of the function field $K(x)$ comes with a monomorphism

$$\operatorname{Spec} K(x) \longrightarrow \operatorname{Spec} K[x] = \mathbb{A}^1. \tag{10}$$

According to Proposition 2.2, there is a unique action on $\operatorname{Spec} K(x)$ that makes the above morphism equivariant.

Let us close this section with some observations on central series. Recall that for a group $G$, the *lower central series* $\Gamma^r = \Gamma^r G$ and the *upper central series* $Z_s = Z_s G$ are inductively defined by

$$\Gamma^0 = G, \quad \Gamma^{r+1} = [G, \Gamma^r] \quad \text{and} \quad Z_0 = \{e\}, \quad Z_{s+1}/Z_s = Z(G/Z_s).$$

The group is *nilpotent* if $\Gamma^r = \{e\}$ for some $r \geq 0$, or equivalently $Z_s = G$ for some $s \geq 0$. Then the smallest such integers coincide, and this number $n$ is called the *nilpotency class* of the group. Note that $\Gamma_{n-r} \subset Z_r$, but usually this inclusion is not an equality. We refer to [19], Chapter 10 or [23], Chapter 6 for basic facts on nilpotent groups.

For group schemes $G$ of finite type one has basically the same construction, with sheafification involved. This is straightforward for the higher centers: An $x \in G(R)$

belongs to $Z_{s+1}(R)$ if and only if it commutes with all members of $G(R')$ up to elements of $Z_s(R')$, for all flat extensions $R \subset R'$. The situation is more complicated for the $\Gamma^r$, because their formation involves schematic images and group scheme closure with respect to the commutator maps $G \times \Gamma^r \to \Gamma^{r+1}$, see [13], Exposé $\mathrm{VI}_B$, Section 8.

Let us unravel this for our $G = U_n$: Consider the closed subschemes

$$\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = U_n \tag{11}$$

defined by $G_r(R) = \{1 + \sum_{i=n-r+1}^{n} \lambda_i F^i\}$.

**Proposition 3.3.** *The $G_r \subset U_n$ are subgroup schemes, and the series (11) coincides with both the upper and the lower central series for the group scheme $U_n$. The quotients are $G_{r+1}/G_r = \alpha_{p^{r+1}}$.*

*Proof.* With descending induction one easily checks that $G_r \subset G_{r+1}$ are subgroup schemes: The surjection $G_{r+1} \to \alpha_{p^{r+1}}$ given by $1 + \sum_{i=n-r}^{n} \lambda_i F^i \mapsto \lambda_{n-r}$ respects the group law, and has kernel $G_r$. The Isomorphism Theorem gives the statement on the quotients.

The arguments for the higher centers rely on the following observation: The recursion formula (3) for inverses $\sum \gamma_i F^i = (\sum \beta_i F^i)^{-1}$ shows that each coefficient $\gamma_i = \gamma_i(\beta_0, \ldots, \beta_n)$ actually depends only on $\beta_0, \ldots, \beta_i$. From this one easily infers

$$(\sum \alpha_i F^i) \cdot (\sum \beta_i F^i)^{-1} \in G_r(R) \quad \Longleftrightarrow \quad \alpha_i = \beta_i \text{ for } 0 \leq i \leq n-r. \tag{12}$$

Write $Z_r$ for the higher centers of $U_n$. We show $Z_r \subset G_r$ by induction on $0 \leq r \leq n$. The case $r = 0$ is trivial. Suppose now $r \geq 1$, and that the inclusion holds for $r-1$. For each $x = \sum \lambda_i F^i$ from $U_n(R)$ we compute

$$(1 - \mu F) \cdot x = x - \sum_{i=0}^{n-1} \mu \lambda_i^p F^{i+1} \quad \text{and} \quad x \cdot (1 - \mu F) = x - \sum_{i=0}^{n-1} \lambda_i \mu^{p^i} F^{i+1}.$$

Suppose that $x$ belongs to $Z_r(R)$. Then for all $\mu \in \alpha_{p^n}(R')$ in some ring extension $R \subset R'$, the above two expressions coincide modulo $Z_{r-1} \subset G_{r-1}$. From the equivalence (12) we obtain $\mu \lambda_i^p = \lambda_i \mu^{p^i}$ for $0 \leq i \leq n-r$. For $R' = R[\mu]/(\mu^{p^n})$ we are in position to compare coefficients and infer $\lambda_1 = \ldots = \lambda_{n-r} = 0$, and thus $x \in G_r(R)$.

This completes our induction, and establishes $Z_r \subset G_r$ for all $0 \leq r \leq n$. For the reverse inclusion we use our embedding $U_n \subset \mathrm{UT}_{n+1}$ into the group of unitriangular matrices. According to Lemma 3.4 below, the $r$-th higher center of $\mathrm{UT}_{n+1}(R)$ is given by the matrices that are zero on the $n-r$ secondary diagonals above the main diagonal. The intersection with $U_n(R)$ equals $G_r(R)$. Consequently $G_r \subset Z_r$, thus the $G_r = Z_r$ form the upper central series.

The arguments for the higher commutator groups rely on some preliminary observations. For elements of the form $b = 1 - \beta F^s - \gamma F^{s+1} + \ldots$ with any $s \geq 1$, the geometric series $(1-x)^{-1} = 1 + x + x^2 + \ldots$ gives

$$b^{-1} = (1 - \beta F^s - \gamma F^{s+1} + \ldots)^{-1} \equiv 1 + \beta F^s + \gamma F^{s+1} + \beta^{1+p^s} F^{2s},$$

where the congruence means up to terms of order $s+2$. Note that the last summand is only relevant in the special case $s = 1$. With $a = 1 - \alpha F$, the above formula shows

that the commutator $aba^{-1}b^{-1}$ is congruent to

$$(1-\beta F^s-\gamma F^{s+1})^{-1}+(1-\alpha F)(-\beta F^s-\gamma F^{s+1})(1+\alpha F)(1+\beta F^s)\equiv$$
$$1+\beta F^s+\gamma F^{s+1}+\beta^{1+p^s}F^{2s}-\beta F^s+\alpha\beta^p F^{s+1}-\beta\alpha^{p^s}F^{s+1}-\beta^{1+p^s}F^{2s}-\gamma F^{s+1}.$$

Most summands cancel, and the upshot is the commutator formula

$$aba^{-1}b^{-1}=1+(\alpha\beta^p-\beta\alpha^{p^s})F^{s+1}+\dots. \tag{13}$$

Write $\Gamma^r$ for the higher commutator subgroup schemes. According to general properties of nilpotent groups ([23], page 107) we have $\Gamma^r\subset Z_{n-r}=G_{n-r}$. We claim that the canonical projection

$$\Gamma^r=[U_n,\Gamma^{r-1}]\longrightarrow G_{n-r}/G_{n-r-1}=\alpha_{p^{n-r}} \tag{14}$$

is an epimorphism. We check this by induction on $r\geq 0$. The case $r=0$ is trivial. Suppose $r\geq 1$, and that the assertion is true for $r-1$. According to [12], Chapter IV, §2, Proposition 1.1 the iterated Frobenius kernels are the only subgroup schemes of $\alpha_{p^{n-r}}\subset\mathbb{G}_a$. Seeking a contradiction, we assume that the above map factors over $\alpha_{p^{n-r-1}}$. Consider the ring $R=K[\alpha,\beta]/(\alpha^{p^n},\beta^{p^{n-r+1}})$. By our induction hypothesis, there is some faithfully flat extension $R\subset R'$ and some $R'$-valued point of the form $b=1-\beta F^{r-1}-\gamma F^r+\dots$ from $\Gamma^{r-1}$. With $a=1-\alpha F$ the commutator formula (13) shows that $aba^{-1}b^{-1}$ projects to $\lambda=\alpha\beta^p-\beta\alpha^{p^r}$ under (14). So $\lambda^{p^{n-r-1}}=\alpha^{p^{n-r-1}}\beta^{p^{n-r}}-\beta^{p^{n-r-1}}\alpha^{p^{n-1}}$ vanishes in the ring $R'$. On the other hand, both of the appearing monomials belong to the monomial basis for $R$, contradiction. Thus (14) is an epimorphism.

We are now ready to prove that the inclusion $\Gamma^s\subset G_{n-s}$ is an equality. Fix some $x\in G_{n-s}(R)$, and write it as $x=1+\sum_{i=s+1}^n\lambda_iF^i$. We check that $x\in\Gamma^s(R)$ by descending induction on $s\leq n$. The case $s=n$ is trivial. Assume now $s<n$, and that the assertion holds for $s+1$. By the preceding paragraph, there is some faithfully flat extension $R\subset R'$ and some $R'$-valued point $y=1+\sum_{i=s+1}^n\mu_iF^i$ from $\Gamma^s$ with $\mu_{s+1}=-\lambda_{s+1}$. Then $xy=1+\sum_{i=s+2}\lambda_i'F^i$ belongs to $G_{n-s-1}(R')$. Using our induction hypothesis, together with the inclusion $\Gamma^{s+1}\subset\Gamma^s$, we see that $xy$ and hence $x$ belongs to $\Gamma^s(R')$, and by descent $x\in\Gamma^s(R)$. □

Let us point out that the ring $K[\alpha,\beta]/(\alpha^{p^n},\beta^{p^{n-r+1}})$ is not free as a module over $K[\lambda]$, which one sees by analyzing the size of the Jordan blocks for multiplication by $\lambda=\alpha\beta^p-\beta\alpha^{p^r}$. Thus it is not always possible to factor a given element of $\Gamma^{r+1}(R)$ into commutators, even over flat extensions $R\subset R'$.

In the preceding proof, we have used the following fact:

**Lemma 3.4.** *The unitriangular matrix group* $\mathrm{UT}_{n+1}(R)$*, over any ring* $R$*, has upper central series given by*

$$Z_s=\{E+(\zeta_{ij})\mid \zeta_{ij}=0 \text{ whenever } j-i\leq n-s\}. \tag{15}$$

*Proof.* Over fields, this appears in [23], Example 16.1.2. The general case is formulated in [33] as Exercise 5.1.13. For the sake of completeness, we sketch an argument, by induction on $s\geq 0$. The case $s=0$ is trivial. Suppose now that $s\geq 1$, and that

the assertion is true for $s-1$. By definition, a unitriangular $E+(\alpha_{ij})$ belongs to $Z_s$ if and only if

$$(E+(\alpha_{ij}))\cdot(E+(\beta_{ij})) \equiv (E+(\beta_{ij}))\cdot(E+(\alpha_{ij})) \quad \text{modulo } Z_{s-1}, \tag{16}$$

for every unitriangular matrix $E+(\beta_{ij})$. By induction hypothesis, each $E+(\zeta_{ij}) \in Z_{s-1}$ has $\zeta_{ij}=0$ for $j-i \le n+1-s$, and one easily checks that right multiplication with elements of $Z_{s-1}$ to a unitriangular matrix leaves the $(i,k)$-entries unchanged for $k-i \le n+1-s$. From this the inclusion $\supset$ of (15) easily follows. Conversely, suppose we have some $E+(\alpha_{ij}) \in Z_s$, so (16) holds. This means

$$\sum_j \alpha_{ij}\beta_{jk} = \sum_j \beta_{ij}\alpha_{jk} \quad \text{whenever } k-i \le n+1-s,$$

where $E+(\beta_{ij})$ is any unitriangular matrix, and the sums actually run over $i<j<k$. From this one easily infers by induction on $r=j-i$ that $\alpha_{ij}$ vanishes for $1 \le r \le n-s$. □

## 4. Compactifications and numerical semigroups

We keep the setting of the previous section, but now work with a new indeterminate $T=x^{-1}$. The iterated semidirect product $\mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m$ has as coordinate ring

$$\Gamma(\mathscr{O}_{\mathbb{G}_a\rtimes U_n\rtimes\mathbb{G}_m}) = K[\alpha,\lambda_1,\dots,\lambda_n,\lambda_0^{\pm}]/(\lambda_1^{p^n},\lambda_2^{p^{n-1}},\dots,\lambda_{n-1}^{p^2},\lambda_n^p),$$

endowed with a Hopf algebra structure, and acts on the affine line $\mathbb{A}^1 = \operatorname{Spec} K[T^{-1}]$. We now seek to extend this action to certain compactifications, all of which are denormalizations of the projective line $\mathbb{P}^1 = \operatorname{Spec} K[T] \cup \operatorname{Spec} K[T^{-1}]$. For this we have to make extensive computations in the first chart, which are much easier to carry out with $T$ rather than $x^{-1}$. Note that by Proposition 2.2 we have an induced action on the spectrum of the function field $K(T)=K(x)$, and this action takes the form

$$K(T) \longrightarrow \Gamma(\mathscr{O}_{\mathbb{G}_a\rtimes U_n\rtimes\mathbb{G}_m}) \otimes K(T), \quad T \longmapsto \left(\alpha + \sum_{i=0}^{n} \lambda_i T^{-p^i}\right)^{-1}. \tag{17}$$

Recall that an additive submonoid $\Gamma \subset \mathbb{N}$ whose complement is finite is called a *numerical semigroup*. Equivalently, the induced inclusions of groups $\Gamma^{\mathrm{grp}} \subset \mathbb{N}^{\mathrm{grp}} = \mathbb{Z}$ is an equality, or $\gcd(a_1,\dots,a_r)=1$ for some members $a_1,\dots,a_r \in \Gamma$. Each numerical semigroup comes with the following invariants: The *multiplicity* $e \ge 1$ is the smallest non-zero element in $\Gamma$. The *conductor* is the smallest integer $c \ge 0$ with $\{c, c+1, \dots\} \subset \Gamma$. The *genus* $g \ge 0$ is the cardinality of the complement $\Gamma \smallsetminus \mathbb{N}$, whose members are called *gaps*. As monoid, $\Gamma$ is finitely generated, and among all systems of generators there is a smallest one; its cardinality is called the *embedding dimension* $d \ge 1$. For general overviews, we refer to the textbooks [34] and [2].

For each numerical semigroup $\Gamma$, the ring $K[T^\Gamma] = K[T^a \mid a \in \Gamma]$ defines a *compactification*

$$X = \operatorname{Spec} K[T^\Gamma] \cup \operatorname{Spec} K[T^{-1}],$$

of the affine line $\mathbb{A}^1 = \operatorname{Spec} K[T^{-1}]$, obtained by adding a single rational point $x_0 \in X$. The gluing of the two affine open sets is given by the common localization

$K[T^{\pm 1}]$ of the coordinate rings. The normalization is $\mathbb{P}^1 = \operatorname{Spec} K[T] \cup \operatorname{Spec} K[T^{-1}]$, and the ensuing map $f : \mathbb{P}^1 \to X$ is described by the *conductor square*

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}^1 \\ \big\downarrow & & \big\downarrow f \\ B & \longrightarrow & X, \end{array} \tag{18}$$

which is both cartesian and cocartesian (for details see [14], Appendix A). The conductor loci $A \subset \mathbb{P}^1$ and $B \subset X$ are the closed subschemes whose respective coordinate rings are $K[T]/(T^c)$ and $K[T^\Gamma]/(T^c, T^{c+1}, \ldots)$. Consider the short exact sequence $0 \to \mathscr{O}_X \to f_*(\mathscr{O}_{\mathbb{P}^1}) \times \mathscr{O}_B \to f_*(\mathscr{O}_A) \to 0$ of sheaves on $X$, where the inclusion is the diagonal map, and the surjection is the difference map. It yields

$$h^0(\mathscr{O}_X) = 1, \quad h^1(\mathscr{O}_X) = g \quad \text{and} \quad e(\mathscr{O}_{X,x_0}) = e \quad \text{and} \quad \operatorname{edim}(\mathscr{O}_{X,x_0}) = d, \tag{19}$$

with the invariants $c, g, e, d$ of the numerical semigroup discussed above. Here $e(\mathscr{O}_{X,x_0})$ and $\operatorname{edim}(\mathscr{O}_{X,x_0})$ denote the *multiplicity* and the *embedding dimension* of the local ring, respectively.

Given a subgroup scheme $G \subset \mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m$, it is natural to ask whether the resulting $G$-action on the affine line $\mathbb{A}^1$ extends to the compactification $X$. If it exists, such an extension is unique, because the open set $\mathbb{A}^1 \otimes R$ is schematically dense in $X \otimes R$, for any ring $R$.

In the following assertion on the constituents of the iterated semidirect product, we regard the expression $P = (1 + \sum_{i=1}^n \lambda_i T^{1-p^i})^{-d}$ as a Laurent polynomial in the indeterminate $T$ with coefficients from $\mathbb{F}_p[\lambda_1, \ldots, \lambda_n]/(\lambda_1^{p^n}, \lambda_2^{p^{n-1}}, \ldots, \lambda_n^p)$, and $Q = (1 + \alpha T)^{-d}$ as a formal power series in $T$ with coefficients from $\mathbb{F}_p[\alpha]$. In both cases we use the ensuing notion of supports $\operatorname{Supp}(P)$ and $\operatorname{Supp}(Q)$ inside the group of exponents $\mathbb{Z}$.

**Proposition 4.1.** *Notation as above. Then the following holds:*

(i) *The multiplicative group $G = \mathbb{G}_m$ always admits an extension.*
(ii) *For the infinitesimal group scheme $G = U_n$ the extension exists if and only if for each $d \in \Gamma$ and $s \in \operatorname{Supp}(P)$, we also have $d + s \in \Gamma$, for the Laurent polynomial $P = (1 + \sum_{i=1}^n \lambda_i T^{1-p^i})^{-d}$.*
(iii) *For the additive group $G = \mathbb{G}_a$ the extension exists if and only if for each $d \in \Gamma$ and $s \in \operatorname{Supp}(Q)$ we have $d + s \in \Gamma$, for the formal power series $Q = (1 + \alpha T)^{-d}$.*

*Moreover, it suffices to verify these conditions for a set of generators $d \in \Gamma$.*

*Proof.* (i) Recall that $\mathbb{G}_m$-actions on affine schemes correspond to $\mathbb{Z}$-gradings, according to [13], Exposé I, Corollary 4.7.3.1. The action on $\operatorname{Spec} K[T^{-1}]$ is given by $\deg(T^{-i}) = -i$. This also defines compatible gradings on $K[T^\Gamma]$, which yields the desired extension of the action of $G = \mathbb{G}_m$.

(ii) The group scheme $G = U_n$ is infinitesimal, hence every open set on a $G$-scheme is $G$-stable. It follows that the $G$-action extends if and only if the map $K[T^\Gamma] \to \Gamma(\mathscr{O}_G) \otimes K(T)$ induced from (17) factors over the subring $\Gamma(\mathscr{O}_G) \otimes K[T^\Gamma]$. This map sends $T^{-1}$ to $T^{-1} + \sum \lambda_i T^{-p^i} = T^{-1}(1 + \sum \lambda_i T^{1-p^i})$. Note that the second factor is invertible, because its second summand is nilpotent. The monomial $T^d$ with

$d \in \Gamma$ is mapped to $T^d P(T)$. This belongs to the subring $R[T^\Gamma]$ if and only if for each $s \in \mathrm{Supp}(P)$ the resulting integer $d+s$ belongs to the numerical semigroup $\Gamma$.

(iii) The action of $G = \mathbb{G}_a$ on $\mathbb{A}^1 = \operatorname{Spec} K[T^{-1}]$ extends to the projective line $\mathbb{P}^1 = \operatorname{Proj} K[U_0, U_1]$ via the assignments $U_1 \mapsto U_1$ and $U_0 \mapsto U_0 + \alpha U_1$, with $T = U_1/U_0$. Note that the origin $0 \in \mathbb{P}^1$ is fixed but does not admit a stable affine open neighborhood. However, the infinitesimal neighborhoods and in particular the conductor locus $A \subset \mathbb{P}^1$ are stable.

Since $G$ is smooth, any $G$-action on $\mathbb{A}^1$ uniquely extends to $\mathbb{P}^1$, according to [8], Theorem 2. By [25], Lemma 3.5 the $G$-action on the projective line descends to an action on $X$ if and only if the action on the conductor locus $A$ descends to an action on $B$. The latter simply means the map

$$\Gamma(B, \mathscr{O}_B) \longrightarrow \Gamma(A, \mathscr{O}_A) \longrightarrow K[\alpha] \otimes \Gamma(A, \mathscr{O}_A) \tag{20}$$

factors over $K[\alpha] \otimes \Gamma(B, \mathscr{O}_B)$. Here the map on the right describes the $G$-action on $A$, and the coordinate ring on the left is $\Gamma(B, \mathscr{O}_B) = K[T^\Gamma]/(T^c, T^{c+1}, \ldots)$, where $c \geq 0$ is the conductor of the numerical semigroup. As $K$-vector space, this is generated by the residue classes of $T^d$, $d \in \Gamma$. The map (17) sends $T^{-1}$ to $T^{-1} + \alpha = T^{-1}(1 + \alpha T)$, so the monomial $T^d$ is mapped to $T^d Q(T)$. The class of the latter belongs to $K[T^\Gamma]/(T^c, T^{c+1}, \ldots)$ if and only if for all $s \in \mathrm{Supp}(Q)$, we have $d + s \in \Gamma$. □

Note that in the expansions of $P(T)$ and $Q(T)$ some multinomial coefficients appear, and the above conditions involve their congruence properties modulo the prime number $p$. Also note that one may view $X$ as a *non-normal torus embedding*, with respect to the one-dimensional torus $\mathbb{G}_m = \operatorname{Spec} K[T^{\pm 1}]$.

The passage from the constituents to the semidirect product is immediate, thanks to the following observation:

**Lemma 4.2.** *Suppose for each constituent of the iterated semidirect product $G = \mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m$, the action on $\mathbb{A}^1$ extends to $X$. Then the the whole $G$-action extends to $X$.*

*Proof.* This is a general fact: All relations between the $R$-valued points of the constituents stemming from the semidirect product structures hold on $\mathbb{A}^1$ and thus also on $X$, because the former is schematically dense in the latter. □

We now introduce a particular $\Gamma$ that is generated by $n+1$ numbers:

**Definition 4.3.** We write $\Gamma_{p,n} \subset \mathbb{N}$ for the numerical semigroup generated by

$$p^n \quad \text{and} \quad p^n - p^j \quad (0 \leq j \leq n-1). \tag{21}$$

This is indeed a numerical semigroup, because $\gcd(p^n, p^n - p^0) = 1$. Its multiplicity is given by

$$e_{p,n} = \begin{cases} p^{n-1}(p-1) & \text{if } p^n \geq 3; \\ 1 & \text{else,} \end{cases}$$

because in the first case the number $p^{n-1}(p-1)$ is smallest among the generators. Note that $e_{p,n} = 1$ is equivalent to $p^n \leq 2$, whereas $e_{p,n} = 2$ means $3 \leq p^n \leq 4$.

We came up with the above generators by determining for a handful of special cases the largest numerical semigroup for which the group scheme action extends,

and then guessed the general pattern. The computations were made with the computer algebra systems Magma [26] and Gap [15]. One of the main insights of this paper is that the resulting compactifications

$$X_{p,n} = \operatorname{Spec} K[T^{\Gamma_{p,n}}] \cup \operatorname{Spec} K[T^{-1}]$$

lead to the desired generalizations of the quasielliptic curves. Indeed, in the special cases $3 \leq p^n \leq 4$ we get $\Gamma_{p,n} = \langle 2, 3\rangle$, and the ensuing coordinate rings become $K[T^2, T^3]$. We now verify that the action of the iterated semidirect product extends to this compactification:

**Theorem 4.4.** *The action of the group scheme $\mathbb{G}_a \rtimes U_{p,n} \rtimes \mathbb{G}_m$ on the affine line $\mathbb{A}^1 = \operatorname{Spec} K[T^{-1}]$ extends to the compactification $X = X_{p,n}$.*

*Proof.* It suffices to extend the action for the three constituents of the iterated semidirect product, by Lemma 4.2, and for this we use Proposition 4.1: The case $G = \mathbb{G}_m$ is immediate. Suppose now $G = U_n$, and fix one of the generators $d \in \Gamma_{p,n}$ listed in (21). We have to understand the expression

$$P = (1 + \sum_{i=1}^{n} \lambda_i T^{1-p^i})^{-d}.$$

In the case $d = p^n$, the above simplifies to $P = 1^{-1} = 1$, by the Multinomial Theorem and $\lambda_i^{p^n} = 0$. Thus $\operatorname{Supp}(P) = \{0\}$, and obviously $d + 0 \in \Gamma_{p,n}$. In the case $d = p^n - p^j$ with $0 \leq j \leq n-1$, we get

$$P = (1 + \sum_{i=1}^{n} \lambda_i T^{1-p^i})^{-p^n} (1 + \sum_{i=1}^{n} \lambda_i T^{1-p^i})^{p^j} = 1 + \sum_{i=1}^{n} \lambda_i^{p^j} T^{p^j - p^{i+j}}.$$

Its support equals the set $\{0\} \cup \{p^j - p^{i+j} \mid 1 \leq i \leq n-j\}$, in light of the defining relations $\lambda_i^{p^{n-i+1}} = 0$. Obviously, $d + 0 = p^n - p^j$ and $d + (p^j - p^{i+j}) = p^n - p^{i+j}$ belong to $\Gamma_{p,n}$. Thus the action of $G = U_n$ extends.

It remains to treat the case $G = \mathbb{G}_a$. Again we fix one of the generators $d \in \Gamma_{p,n}$, and now have to examine the formal power series $Q = (1 + \alpha T)^{-d}$ with coefficients from the polynomial ring $\mathbb{F}_p[\alpha]$. For $d = p^n - p^j$, this becomes

$$Q = (1 + \alpha T)^{p^j} / (1 + \alpha T)^{p^n} = (1 + \alpha^{p^j} T^{p^j}) \sum_{i=0}^{\infty} (-\alpha T)^{ip^n}.$$

The support is contained in $\{ip^n \mid i \geq 0\} \cup \{p^j + ip^n \mid i \geq 0\}$. Clearly, $d + ip^n = (p^n - p^j) + ip^n$ and $d + (p^j + ip^n) = (i+1)p^n$ belongs to $\Gamma_{p,n}$. The argument for $d = p^n$ is likewise, and even simpler. Thus the action of $G = \mathbb{G}_a$ extends. □

Set $\Gamma = \Gamma_{p,n}$ and $X = X_{p,n}$. With respect to the infinitesimal group scheme $U_n$, all open sets in $X$ are stable, and the action on the affine open set $\operatorname{Spec} K[T^\Gamma]$ is given by the ring homomorphism

$$K[T^\Gamma] \longrightarrow \Gamma(\mathscr{O}_{U_n}) \otimes K[T^\Gamma], \quad T^d \longmapsto T^d (1 + \sum_{i=1}^{n} \lambda_i T^{-p^i})^{-d}$$

with exponents $d \in \Gamma$. The *orbit map* $x_0 : U_n \to X$ corresponding to the rational point $x_0 \in X$ is given by the homomorphism $\varphi : K[T^\Gamma] \to \Gamma(\mathscr{O}_{U_n})$ that is implicitly described by

$$\varphi(T^d) = T^d(1 + \sum_{i=1}^{n} \lambda_i T^{1-p^i})^{-d} \mid_{T=0} .$$

Note that one has to determine the product before substituting $T = 0$, because the second factor usually contains terms of negative degree. The computation for the generators (21) of our numerical semigroup is immediate: $\varphi(T^{p^n}) = 0$, and $\varphi(T^{p^n - p^j}) = \lambda_{n-j}^{p^j}$ for $0 \leq j \leq n-1$. Now recall that the *inertia group scheme* in $U_n$ is defined by the largest quotient of $\Gamma(\mathscr{O}_{U_n})$ in which $\varphi$ becomes the zero map. Setting $i = n - j$ we get:

**Proposition 4.5.** *Inside* $U_n = \operatorname{Spec} K[\lambda_1, \ldots, \lambda_n]/(\lambda_1^{p^n}, \lambda_2^{p^{n-1}}, \ldots, \lambda_n^p)$*, the inertia group scheme with respect to the rational point* $x_0 \in X$ *is defined by the equations* $\lambda_i^{p^{n-i}} = 0$ *for* $1 \leq i \leq n$*.*

This inertia group scheme coincides with the canonical inclusion of $U_{n-1} \subset U_n$, which is also the image of the relative Frobenius map, and we thus obtain an $U_n$-stable closed subscheme $U_n/U_{n-1} \subset X$. A priori, this is an effective Weil divisor supported by $x_0$, of degree $[U_n : U_{n-1}] = h^0(\mathscr{O}_{U_n})/h^0(\mathscr{O}_{U_{n-1}}) = p^n$. The following observation will be crucial in what follows:

**Proposition 4.6.** *The Weil divisor* $U_n/U_{n-1} \subset X$ *is an effective Cartier divisor.*

*Proof.* The closed subscheme lies in the affine open set $\operatorname{Spec} K[T^\Gamma]$ and corresponds to the ideal $\mathfrak{a} = \operatorname{Ker}(\varphi)$. This ideal contains the monomial $T^{p^n}$, and we claim that the inclusion $(T^{p^n}) \subset \mathfrak{a}$ is an equality. In other words, we have to verify that the resulting map

$$\varphi : K[T^\Gamma]/(T^{p^n}) \longrightarrow \Gamma(\mathscr{O}_G) = K[\lambda_1, \ldots, \lambda_n]/(\lambda_1^{p^n}, \lambda_2^{p^{n-1}}, \ldots, \lambda_n^p)$$

is injective. We computed above that its image is the subring generated by the powers $\lambda_i^{p^{n-i}}$ for $1 \leq i \leq n$, which is a $K$-algebra of degree $p^n$. So it suffices to verify that the $K$-algebra $K[T^\Gamma]/(T^{p^n})$ has degree at most $p^n$. This algebra is generated by the classes $x_j$ of $T^{p^n - p^j}$, with $0 \leq j \leq n-1$. From the relation

$$p(p^n - p^j) = (p-1)p^n + (p^n - p^{j+1})$$

in the numerical semigroup $\Gamma$ we infer a factorization $(T^{p^n - p^j})^p = (T^{p^n})^{p-1} \cdot T^{p^n - p^{j+1}}$ in the ring $K[T^\Gamma]$, and hence $x_j^p = 0$. Thus $K[T^\Gamma]/(T^{p^n})$ has degree at most $p^n$. □

## 5. The complete intersection property

We keep the notation as in the preceding section, and continue to study the algebra of the numerical semigroup $\Gamma = \Gamma_{p,n}$, and also the geometry of the compactification $X = X_{p,n}$ of the affine line $\mathbb{A}^1 = \operatorname{Spec} K[T^{-1}]$ defined by the coordinate ring $K[T^\Gamma]$.

Recall that any numerical semigroup $\Gamma$ given by a set of $d \geq 1$ generators $a_1, \ldots, a_d$ and ensuing surjection $\mathbb{N}^d \to \Gamma$ is called a *complete intersection* if the congruence $R = \mathbb{N}^d \times_\Gamma \mathbb{N}^d$ is generated by $d-1$ elements. According to [20], Corollary 1.13 this is equivalent to the condition that the complete local ring $A = K[[T^\Gamma]]$ is a

complete intersection in the sense of commutative algebra, in other words, $A \simeq K[[u_1,\dots,u_r]]/(f_1,\dots,f_s)$, for some $r \geq 0$ and some regular sequence $f_1,\dots,f_s$, here necessarily with $s = r-1$.

**Proposition 5.1.** *Our numerical semigroup $\Gamma_{p,n}$ is a complete intersection, and its conductor $c_{p,n}$ and genus $g_{p,n}$ are given by the formulas*

$$c_{p,n} = np^{n+1} - (n+2)p^n + 2 \quad \textit{and} \quad g_{p,n} = \frac{1}{2}c_{p,n}.$$

*Moreover, $G = \{p^n - p^{n-1}, p^n - p^{n-2}, \dots, p^n - 1, p^n\}$ is the smallest generating set provided $p \geq 3$; for the prime $p = 2$ and $n \geq 1$ one has to omit $p^n$.*

*Proof.* First note that for $p = 2$ and $n \geq 1$ the relation $p^n = 2(p^n - p^{n-1})$ shows that the generator $p^n$ does not belong to the smallest generating set.

We now proceed, for general $p > 0$, by induction on $n \geq 0$. For $n = 0$ we have $\Gamma = \mathbb{N}$, and all assertions are obvious. Suppose now $n \geq 1$, and that the assertion holds for $n-1$. Consider the sets of numbers

$$G_1 = \{p^{n-1} - p^{n-2}, p^{n-1} - p^{n-3}, \dots, p^{n-1} - 1, p^{n-1}\} \quad \text{and} \quad G_2 = \{1\}.$$

Both generate respective numerical semigroups $\Gamma_1$ and $\Gamma_2$, and the induction hypothesis applies to the former. The numbers $a_1 = p$ and $a_2 = p^n - 1$ are relatively prime, with $a_1 \in \Gamma_2$ and $a_2 = p(p^{n-1} - p^{n-2}) + (p^{n-1} - 1) \in \Gamma_1$. Furthermore $\Gamma = a_1\Gamma_1 + a_2\Gamma_2$. According to [11], Proposition 10 the monoid $\Gamma$ is a complete intersection, and the conductor is given by the formula

$$c = a_1c_1 + a_2c_2 + (a_1 - 1)(a_2 - 1) = pc_1 + (p-1)(p^n - 2). \tag{22}$$

Here $c_2 = 0$ is the conductor of $\Gamma_2$, and $c_1 = (n-1)p^n - (n+1)p^{n-1} + 2$ is the conductor of $\Gamma_1$, which we know by our induction hypothesis. Inserting the latter into (22) we get the desired formula for $c_{p,n}$. Every complete intersection semigroup is symmetric ([34], Corollary 9.12), which simply means that the conductor is twice the genus, and the formula for $g_{p,n}$ follows.

Suppose now $p \geq 3$. By induction, the $G_i \subset \Gamma_i$ are the smallest generating sets. The number $a_1a_2 = p^{n+1} - p$ does not belong to $a_1G_1 \cup a_2G_2 = G$. As explained in [11], proof for (ii) of Proposition 10, the subset $G \subset \Gamma$ is the smallest generating set. For $p = 2$ one argues likewise, with $p^n$ omitted. □

We see that the embedding dimension for the numerical semigroup $\Gamma_{p,n}$ and the local ring $\mathscr{O}_{X,x_0}$ is given by the formula

$$d_{p,n} = \begin{cases} n+1 & \text{if } p \geq 3 \text{ or } n = 0; \\ n & \text{if } p = 2 \text{ and } n \geq 1. \end{cases}$$

Let us also record the following geometric consequences:

**Corollary 5.2.** *The curve $X = X_{n,p}$ has invariants*

$$h^0(\mathscr{O}_X) = 1 \quad \textit{and} \quad h^1(\mathscr{O}_X) = \frac{1}{2}(np^{n+1} - (n+2)p^n + 2).$$

*Moreover, the dualizing sheaf $\omega_X$ is invertible, of degree $p^n(np - n - 2)$.*

*Proof.* The values for $h^i(\mathscr{O}_X)$ follow with (19) from the proposition. Being locally of complete intersection, $X$ must be Gorenstein, and the dualizing sheaf is invertible. Serre Duality gives $\deg(\omega_X) = -2\chi(\mathscr{O}_X) = p^n(np - n - 2)$. □

We actually can derive an explicit description for the ring $K[T^\Gamma]$ in terms of generators and relations. Write $a_j = p^n - p^j$ and $b = p^n$ for the generators of $\Gamma = \Gamma_{p,n}$. They give rise to a surjection $\mathbb{N}^{n+1} \to \Gamma$ of monoids, and an ensuing congruence $R = \mathbb{N}^{n+1} \times_\Gamma \mathbb{N}^{n+1}$. The $n+1$ generators satisfy the $n$ obvious relations

$$p \cdot a_{n-1} = (p-1) \cdot b \quad \text{and} \quad p \cdot a_j = p \cdot a_{n-1} + a_{j+1} \quad (0 \le j \le n-2), \tag{23}$$

which may be interpreted as members of the congruence $R$. To translate this into commutative algebra, let $x_j, y$ be indeterminates corresponding to the generators $a_j, b \in \Gamma$, and consider the surjection

$$\varphi : K[x_1, \ldots, x_{n-1}, y] \longrightarrow K[T^\Gamma]$$

given by $\varphi(x_j) = T^{a_j}$ and $\varphi(y) = T^b$. The map respects the gradings specified by $\deg(x_j) = a_j$, $\deg(y) = b$ and $\deg(T) = 1$.

**Proposition 5.3.** *The ideal $\mathfrak{a} = \mathrm{Ker}(\varphi)$ is generated by the polynomials $x_{n-1}^p - y^{p-1}$ and $x_j^p - x_{n-1}^p x_{j+1}$ for $0 \le j \le n-2$, corresponding to the obvious relations (23).*

*Proof.* This is an application of an observation of Delorme ([11], Lemma 8). Recall that our numerical semigroup is generated by the $n+1$ elements $a_0, \ldots, a_{n-1}, b \in \Gamma$. Delorme's observation hinges on two descending sequences

$$P_{n+1}, P_n, \ldots, P_1 \quad \text{and} \quad Z_{n+1}, Z_n, \ldots, Z_2.$$

The first sequence comprises *partitions* $P_i$ of the generating set $G = \{a_0, \ldots, a_{n-1}, b\}$, subject to the following condition: $P_{n+1}$ is the partition into singletons, and each $P_{i-1}$ is obtained from its precursor $P_i$ by replacing certain members $L_i, L_i' \in P_i$ by their union. The second sequence consists of *homogeneous polynomials* $Z_i$ in the indeterminates $x_0, \ldots, x_{n-1}, y$, taking the form $Z = H_i - H_i'$ for some monic monomials $H_i$ and $H_i'$, each involving only indeterminates indexed by $L_i$ and $L_i'$, respectively. In loc. cit. the sequences are denoted by $\mathscr{P}$ and $\mathscr{Z}$, and the pair $(\mathscr{P}, \mathscr{Z})$ is called a *suite distinguée*.

Note that the partitions $P_i$ are fully determined by the sets $L_i, L_i' \subset G$ with $2 \le i \le n+1$. We now define such a partition sequence by setting

$$L_i = \{a_{i-1}, \ldots, a_{n-1}, b\} \quad \text{and} \quad L_i' = \{a_{i-2}\}.$$

Note that this starts with the singletons $L_{n+1} = \{b\}$ and $L_{n+1}' = \{a_{n-1}\}$. The homogeneous polynomials are declared as

$$Z_{n+1} = y^{p-1} - x_{n-1}^p \quad \text{and} \quad Z_i = x_{i-2}^p - x_{n-1}^p x_{i-1}, \quad (2 \le i \le n).$$

These have $\deg(Z_i) = p^{n+1} - p^{i-1}$ for all $2 \le i \le n+1$. One sees

$$\gcd(L_i) = \gcd(p^{i-1}, \ldots, p^{n-1}, p^n) = p^{i-1} \quad \text{and} \quad \gcd(L_i') = p^n - p^{i-2}.$$

The least common multiple of the above two gcds is given by $p(p^n - p^{i-2})$, which coincides with $\deg(Z_i)$. Our assertion now follows from [11], Lemma 8. □

This has important consequences for Kähler differentials:

**Corollary 5.4.** *The sheaf* $\Omega^1_{X/K}/\mathrm{Torsion}$ *is invertible of degree* $-p^n$*, and the tangent sheaf* $\Theta_{X/K} = \underline{\mathrm{Hom}}(\Omega^1_{X/K}, \mathscr{O}_X)$ *is invertible of degree* $p^n$*.*

*Proof.* The main task is to compute the module of Kähler differentials for the integral domain $K[T^\Gamma]$. In light of the proposition, $\Omega^1_{K[T^\Gamma]/K}$ is generated by the $n+1$ differentials $dx_j$ and $dy$, modulo the $n$ relations

$$y^{p-2}dy \quad \text{and} \quad x_{n-1}^p dx_{j+1} \quad (0 \le j \le n-2). \tag{24}$$

The ring elements $y$ and $x_{n-1}$ are non-zero, because they correspond to monomials in $K[T^\Gamma]$, so $dy$ and $dx_{j+1}$ for $0 \le j \le n-2$ are torsion. We infer that the map $K[T^\Gamma] \to \Omega^1_{K[T^\Gamma]/K}$ given by the remaining differential $dx_0$ is bijective modulo torsion. The latter differential is given by $dT^{p^n-1}$.

Let $\mathscr{N}$ be the quotient of $\Omega^1_{X/K}$ by its torsion subsheaf, and consider the affine open covering $X = U_0 \cup U_1$ with $U_0 = \operatorname{Spec} K[T^\Gamma]$ and $U_1 = \operatorname{Spec} K[T^{-1}]$. We have trivializations $\mathscr{N}|U_0$ and $\mathscr{N}|U_1$, given by $dT^{p^n-1}$ and $dT^{-1}$. On the overlap these become $-T^{p^n-2}dT$ and $-T^{-2}dT$, which are related by the cocycle $T^{p^n} \in \Gamma(U_0 \cap U_1, \mathscr{O}_X^\times)$. This gives $\deg(\mathscr{N}) = -p^n$. The assertion for the dual sheaf $\Theta_{X/K} = \mathscr{N}^\vee$ is immediate. □

## 6. The projective model

We keep the set-up of the previous section, and now describe a projective model for our curve $X = X_{p,n}$. First note that the $n$ obvious relations (23) for our monoid $\Gamma = \Gamma_{p,n}$ can be replaced by

$$p \cdot a_{n-1} = (p-1)\cdot b \quad \text{and} \quad p \cdot a_j = (p-1)\cdot b + a_{j+1} \quad (0 \le j \le n-2), \tag{25}$$

by using the first of these relations. Now write $\mathbb{P}^{n+1} = \operatorname{Proj} K[U_0, \dots, U_{n-1}, V, Z]$ and consider the closed subscheme $C = C_{p,n}$ defined by the $n$ homogeneous equations

$$U_{n-1}^p - V^{p-1}Z = 0 \quad \text{and} \quad U_j^p - V^{p-1}U_{j+1} = 0 \quad (0 \le j \le n-2). \tag{26}$$

First observe that $C$ is covered by $D_+(Z) \cup D_+(V)$, because it contains only the point $(0 : \dots : 0 : 1 : 0)$ on the hyperplane given by $Z = 0$. On these two charts, we see that

$$T^{p^n - p^j} \longmapsto U_j/Z \quad \text{and} \quad T^{p^n} \longmapsto V/Z \quad \text{and} \quad T^{-1} \longmapsto U_0/V$$

constitute an isomorphism $C \to X$, which we regard as an identification.

**Proposition 6.1.** *The homogeneous polynomials* (26) *form a regular sequence in the polynomial ring, the curve* $X \subset \mathbb{P}^{n+1}$ *has degree* $p^n$*, and*

$$\omega_X = \mathscr{O}_X(np - n - 2) \quad \textit{and} \quad \Theta_{X/k} = \mathscr{O}_X(1).$$

*In particular,* $\Theta_{X/k}$ *is very ample, and* $\omega_X = \Theta_{X/k}^{\otimes r}$ *with the exponent* $r = np - n - 2$*.*

*Proof.* Let $\mathfrak{a}$ be the ideal generated by the $n$ homogeneous polynomials (26) inside the $n+2$-dimensional Cohen–Macaulay ring $A = K[U_0, \dots, U_{n-1}, V, Z]$. Since the scheme $C$ is one-dimensional, we must have $\dim(A/\mathfrak{a}) = 2$. It follows from [43], Tag 02JN that the polynomials in question form a regular sequence. The assertion on the dualizing sheaf immediately follows from $\omega_{\mathbb{P}^{n+1}} = \mathscr{O}_{\mathbb{P}^{n+1}}(-n-2)$ and the Adjunction Formula.

The intersection of $C \subset \mathbb{P}^{n+1}$ with the hyperplane given by $V = 0$ is a singleton, with generators $U_j/Z$ and relations $(U_j/Z)^p = 0$ for $0 \leq j \leq n-1$ in the homogeneous coordinate ring. Thus $\deg(C) = p^n$.

It remains to verify the statement on the tangent sheaf. As described in the last paragraph of the proof for Corollary 5.4, the invertible sheaf $\Theta_{X/K}$ is given by the cocycle $T^{-p^n}$ with respect to the open covering $W_0 = \operatorname{Spec} K[T^\Gamma]$ and $W_1 = \operatorname{Spec} K[T^{-1}]$. The latter correspond to the open sets $D_+(Z)$ and $D_+(V)$. On the union of these open sets, the invertible sheaf $\mathscr{O}_{\mathbb{P}^n}(1)$ is defined by the cocycle $Z/V$. This becomes $T^{-p^n}$ after restricting to $C$, and thus $\Theta_{X/k} = \mathscr{O}_X(1)$. □

Recall that a square root for the dualizing sheaf is called a *theta characteristic*, or *spin structure* ([3] and [29]). In our situation, the curve $X$ comes with what one might call an *r-fold* theta characteristic or spin structure.

Another highly relevant consequence: The very ample sheaf $\mathscr{O}_X(1) = \Theta_{X/K}$ has an intrinsic meaning, and $\mathfrak{g} = H^0(X, \mathscr{O}_X(1))$ becomes the Lie algebra for the automorphism group scheme $G = \operatorname{Aut}_{X/K}$. To exploit this we check that the closed embedding $X \subset \mathbb{P}^{n+1}$ is defined by the complete linear system:

**Proposition 6.2.** *The restriction map $H^0(\mathbb{P}^{n+1}, \mathscr{O}_{\mathbb{P}^{n+1}}(1)) \to H^0(X, \mathscr{O}_X(1))$ is bijective. In particular $h^0(\Theta_{X/K}) = n+2$.*

*Proof.* Since the defining polynomials (26) have degree $p \geq 2$, the homogeneous ideal for $X \subset \mathbb{P}^{n+1}$ contains no linear terms. It follows that the map in question is injective. It remains to compute $h^0(\mathscr{L})$ for $\mathscr{L} = \Theta_{X/K}$.

Let us proceed with some general considerations on invertible sheaves $\mathscr{L}$ on $X$ of arbitrary degree $m \geq 0$. Recall that the conductor loci for the normalization map $f : \mathbb{P}^1 \to X$ are given by

$$\Gamma(\mathscr{O}_A) = K[T]/(T^c) \quad \text{and} \quad \Gamma(\mathscr{O}_B) = K[T^\Gamma]/(T^c, T^{c+1}, \ldots),$$

where $c \geq 0$ is the conductor for the numerical semigroup $\Gamma$. From the cocartesian diagram (18), we now obtain an exact sequence

$$0 \longrightarrow H^0(\mathscr{L}) \longrightarrow \Gamma(\mathscr{L}_{\mathbb{P}^1}) \oplus \Gamma(\mathscr{L}_B) \longrightarrow \Gamma(\mathscr{L}_A) \longrightarrow H^1(\mathscr{L}) \longrightarrow 0.$$

It is not difficult to determine the map in the middle: Making the identification $\mathscr{L}_{\mathbb{P}^1} = \mathscr{O}_{\mathbb{P}^1}(m)$ and $\mathscr{L}_B = \mathscr{O}_B$ and $\mathscr{L}_A = \mathscr{O}_A$, we get

$$\Gamma(\mathscr{L}_{\mathbb{P}^1}) = \bigoplus_{a=0,\ldots,m} KT^a, \quad \Gamma(\mathscr{L}_B) = \bigoplus_{a\in\Gamma, a\leq c-1} KT^a \quad \text{and} \quad \Gamma(\mathscr{L}_A) = \bigoplus_{a=0,\ldots,c-1} KT^a.$$

If $m \leq c-1$, the former groups are contained in the latter, and $H^0(\mathscr{L})$ becomes their intersection, and hence $h^0(\mathscr{L}) = \operatorname{Card}(S)$ for the set

$$S = \{a \in \Gamma \mid a \leq m \text{ and } a \leq c-1\} = \{a \in \Gamma \mid a \leq m\}.$$

We have to determine this set for $m = p^n$, under the assumptions $n(p-1) \geq 3$. According to Proposition 5.1, the conductor is $c = np^{n+1} - (n+2)p^n + 2$, and thus $c/p^n = np - (n+2) + 2/p^n > n(p-1) - 2 \geq 1$. So our set $S$ comprises all $a \in \Gamma$ with $a \leq p^n$. It clearly contains the generators $p^n, p^n - 1, \ldots, p^n - p^{n-1}$, and also the zero element $a = 0$. It remains to check that for each pair of generators $a \leq b$ we

have $a+b \geq p^n$. This is obvious for $b = p^n$, so assume $a = p^n - p^i$ and $b = p^n - p^j$ with $0 \leq i \leq j < n$. Then $a + b - p^n = p^n - p^i - p^j \geq p^n - 2p^j \geq p^n - p^{j+1} \geq 0$. □

This leads to a matrix interpretation of the full automorphism group scheme $G = \mathrm{Aut}_{X/K}$: First note that the diagonal action of $G$ on $X \times X$, and its effects on graphs, induces the conjugacy action of $G$ on itself. Its restriction to the first infinitesimal neighborhood of the diagonal $\Delta_X$ yields the $G$-linearization of the tangent sheaf $\Theta_{X/k}$, and we infer that the resulting representation on the Lie algebra $\mathfrak{g} = H^0(X, \Theta_{X/K})$ coincides with the adjoint representation $G \to \mathrm{GL}(\mathfrak{g})$. Its projectivization $G \to \mathrm{PGL}(\mathfrak{g})$ is injective, because $\Theta_{X/k}$ is very ample, and it follows that $G \to \mathrm{GL}(\mathfrak{g})$ is injective as well. We thus have a canonical inclusion $G \subset \mathrm{GL}(\mathfrak{g})$ that intersects the center $\mathbb{G}_m \subset \mathrm{GL}(\mathfrak{g})$ trivially. Write $G \cdot \mathbb{G}_m = G \times \mathbb{G}_m$ for the resulting subgroup scheme, and $\mathfrak{a}_p \subset \mathrm{Sym}^p(\mathfrak{g})$ for the vector subspace generated by the homogeneous polynomials (26).

**Proposition 6.3.** *Notation as above. Then $G \cdot \mathbb{G}_m \subset \mathrm{GL}(\mathfrak{g})$ equals the stabilizer group scheme for the vector subspace $\mathfrak{a}_p \subset \mathrm{Sym}^p(\mathfrak{g})$.*

*Proof.* We start with some observations on the homogeneous coordinate rings

$$\Gamma_\bullet(\mathscr{O}_{\mathbb{P}^{n+1}}) = \mathrm{Sym}^\bullet(\mathfrak{g}) \quad \text{and} \quad \Gamma_\bullet(\mathscr{O}_X) = \bigoplus_{n \geq 0} \Gamma(X, \mathscr{O}_X(n)).$$

Both rings are integral, so the kernel $\mathfrak{p}$ of the canonical map $\Gamma_\bullet(\mathscr{O}_{\mathbb{P}^{n+1}}) \to \Gamma_\bullet(\mathscr{O}_X)$ is a prime ideal, which equals the radical for the ideal $\mathfrak{a}$ generated by the polynomials (26). The ideal $\mathfrak{a}$ becomes prime when localized with respect to any homogeneous $f \in \mathrm{Sym}^+(\mathfrak{g})$, because $X$ is integral. Since our generators form a regular sequence, this actually holds everywhere, and thus $\mathfrak{a} = \mathfrak{p}$.

Write $I \subset \mathrm{GL}(\mathfrak{g})$ for the stabilizer group scheme in question. It contains $\mathbb{G}_m$, because the polynomials are homogeneous, and its action on $\mathbb{P}^{n+1}$ stabilizes the curve $X$. Modulo $\mathbb{G}_m$, the induced action on $X$ is faithful, according to Proposition 6.2. Thus $I \subset G \cdot \mathbb{G}_m$. Conversely, let $f \in G(R)$ be some $R$-valued automorphism of $X$. It induces an action on the homogeneous coordinate rings $\Gamma_\bullet(\mathscr{O}_{\mathbb{P}^{n+1}} \otimes R) = \Gamma_\bullet(\mathscr{O}_{\mathbb{P}^{n+1}}) \otimes R$, and likewise for $\Gamma_\bullet(\mathscr{O}_X)$. These actions are compatible, thus $f$ stabilizes $\mathfrak{p}_p \otimes R = \mathfrak{a}_p \otimes R$. □

For $n = 1$, this means that $G \cdot \mathbb{G}_m \subset \mathrm{GL}_3$ is the stabilizer group scheme for the line generated by $U^p - V^{p-1}Z$ in the $p$-th symmetric power of $\mathfrak{g} = KU \oplus KV \oplus KZ$. In turn, $G \subset \mathrm{PGL}_3$ is the inertia group scheme for the rational point corresponding to this line.

## 7. The automorphism group scheme

Recall that our curves $X = X_{p,n}$ come with an inclusion

$$\mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m \subset \mathrm{Aut}_{X/K} \tag{27}$$

of group schemes. The following is one of the main results of this paper:

**Theorem 7.1.** *The above inclusion of group schemes is an equality, provided $p^n \geq 3$.*

The cases $p^n \leq 2$ indeed have to be excluded, because then $X = \mathbb{P}^1$. Also note that for $3 \leq p^n \leq 4$ our curve $X$ becomes the rational cuspidal curve, and the assertion was established by Bombieri and Mumford ([5], Proposition 6). The proof for the above theorem requires some preparation, and will be given step-wise. We start with a simple observation:

**Lemma 7.2.** *For $p^n \geq 3$ the ideal for the closed embedding (27) is nilpotent.*

*Proof.* For this we may assume that $K$ is algebraically closed. Seeking a contradiction, we suppose that there is an automorphism $\varphi : X \to X$ that does not yield a rational point in $\mathbb{G}_a \rtimes \mathbb{G}_m$. The assumption ensures $\mathrm{Sing}(X) = \{x_0\}$, and $\varphi$ fixes this singular point. Hence the induced automorphism on the normalization $\mathbb{P}^1 = \operatorname{Spec} K[T] \cup \operatorname{Spec} K[T^{-1}]$ fixes the point defined by $T = 0$. It thus belongs to the inertia group scheme $\mathbb{G}_a \rtimes \mathbb{G}_m$ inside $\mathrm{PGL}_2$. According to [7], Proposition 2.5.1 the action of any smooth group scheme on $X$ lifts to an action on the normalization. Thus $\varphi$ belongs to $\mathbb{G}_a \rtimes \mathbb{G}_m$ inside $\mathrm{Aut}_{X/k}$, contradiction. □

*Proof of Theorem 7.1 in the special case $n = 1$.* In this situation we have $X = \operatorname{Spec} K[T^p, T^{p-1}] \cup \operatorname{Spec} K[T^{-1}]$. According to Proposition 6.2, the tangent sheaf has $h^0(\Theta_{X/k}) = 3$. One easily computes that the rational vector fields

$$T^{2-p}\frac{\partial}{\partial T} \quad \text{and} \quad T^2\frac{\partial}{\partial T} \quad \text{and} \quad T\frac{\partial}{\partial T} \tag{28}$$

are everywhere defined, hence form a basis of $\mathfrak{g} = H^0(X, \Theta_{X/k})$. Moreover, the first two basis vectors generate a restricted subalgebra $K^2$, with trivial bracket and $p$-map, and the last basis vector yields a copy of $\mathfrak{gl}_1(K)$, giving a semidirect product $K^2 \rtimes \mathfrak{gl}_1(K)$. Such algebras play a prominent role in [36], [24], [41]. Bracket and $p$-map are given by $[(x,\lambda),(x',\lambda')] = \lambda x' - \lambda' x$ and $(x,\lambda)^{[p]} = (\lambda^p x, \lambda^{p-1})$, compare [24], Proposition 1.1. One sees that $K^2$ is the image of the bracket, thus the derived subalgebra. This also holds for $R$-valued points, hence $K^2$ is a subrepresentation for $G$.

As explained in Section 6, our curve $X$ may also be regarded as the curve in $\mathbb{P}^2 = \operatorname{Proj} K[U_0, V, Z]$ defined by the homogeneous polynomial $P = U_0^p - V^{p-1}Z$, with an identification via $T^{p-1} = U_0/Z$ and $T^p = V/Z$ and $T^{-1} = U_0/V$. According to Proposition 6.2, the monomials $Z, V, U_0$ yield a basis for $H^0(X, \mathscr{O}_X(1))$. By Proposition 6.1, the invertible sheaves $\mathscr{O}_X(1)$ and $\Theta_X$ are isomorphic. Computing the order of zeros for the homogeneous polynomials $Z, V, U_0$ and the vector fields (28) on $\mathbb{P}^1$, one sees that each identification $\mathscr{O}_X(1) = \Theta_X$ sends the former basis to the latter basis, at least up to a diagonal base-change matrix.

Combining this with Proposition 6.3, we have a functorial interpretation of the $R$-valued points of $H = G \cdot \mathbb{G}_m$ as the group of matrices

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{pmatrix} \in \mathrm{GL}_3(R)$$

subject to the sole condition

$$P(aU_0 + dV, bU_0 + eV, cU_0 + fV + gZ) = \lambda \cdot P(U_0, V, Z), \tag{29}$$

with some multipliers $\lambda \in R^\times$. The zero entries in the matrix $A$ stem from the fact that the derived subalgebra $[\mathfrak{g}, \mathfrak{g}] \subset \mathfrak{g}$ is a subrepresentation.

Suppose $A \in H(R)$ has $b = 0$. Comparing coefficients in (29) we get $ae^{p-1} = g^p$, and $c^p = 0$ and $de = f^p$, so the matrix takes the form

$$A = \begin{pmatrix} g^p e^{1-p} & 0 & c \\ f^p e^{-1} & e & f \\ 0 & 0 & g \end{pmatrix} \quad \text{with } c^p = 0.$$

The group $H_0 \subset H$ of such matrices contains the diagonal copy of $\mathbb{G}_m$, and $H_0/\mathbb{G}_m$ becomes our iterated semidirect product $\mathbb{G}_a \rtimes \alpha_p \rtimes \mathbb{G}_m$ inside $\mathrm{Aut}_{X/k} \subset \mathrm{PGL}_3$. Note that the projection $H_0 \to H_0/\mathbb{G}_m$ admits a splitting, by setting $g = 1$.

Seeking a contradiction, we assume that there is some $A \in H(R)$ with $b \neq 0$. By Lemma 7.2 we must have $b \in \mathrm{Nil}(R)$, and thus $a, e \in R^\times$. Making a flat extension of $R$, we can assume that there is some $f' \in R$ with $f'^p = -d/a$. Setting $a' = e' = g' = 1$ and $b' = c' = 0$ and left-multiplying with the resulting matrix $A' \in H(R)$, we may assume that both $b \neq 0$ and $d = 0$ hold. On the other hand, comparing coefficients in (29) immediately yields $b = 0$, contradiction.

This establishes $H_0 = H$. We already observed that $H/\mathbb{G}_m = \mathrm{Aut}_{X/K}$ inside $\mathrm{PGL}_3$, and that $H_0/\mathbb{G}_m$ equals our iterated semidirect product. □

To continue inductively we seek to relate the curves $X_{p,n}$ with different indices $n$. First recall a general fact on numerical semigroups $\Gamma = \langle b, a_2, \ldots, a_r \rangle$ with non-zero generators $b < a_2 < \ldots < a_r$: The *blowing-up* $\mathrm{Bl}_{\mathfrak{m}}(A)$ of the ring $A = K[T^\Gamma]$ with respect to the maximal ideal $\mathfrak{m} = (T^b, T^{a_2}, \ldots, T^{a_r})$ has coordinate ring $A' = K[T^{\Gamma'}]$ for the numerical semigroup $\Gamma' = \langle b, a_2 - b, \ldots, a_r - b \rangle$, compare [4], Proposition I.2.1, and also equation I.2.4.

For our $\Gamma = \Gamma_{p,n}$ with $n \geq 1$ we have $b = p^n - p^{n-1}$, with remaining generators $p^n$ and $p^n - p^j$ for $0 \leq j \leq n-2$. The resulting differences are $p^n - b = p^{n-1}$ and $(p^n - p^j) - b = p^{n-1} - p^j$. For $n \geq 2$ we write $b = p \cdot (p^{n-1} - p^{n-2})$, and in any case see $\Gamma' = \Gamma_{p,n-1}$. This reveals:

**Lemma 7.3.** *For $p^n \geq 3$ we have $X_{p,n-1} = \mathrm{Bl}_Z(X_{p,n})$ where the center $Z$ is the singular point $x_0 \in X_{p,n}$ endowed with the reduced scheme structure.*

Note that for every $m \leq n$ we get an inclusion $\Gamma_{p,n} \subset \Gamma_{p,m}$ of numerical semigroups inside $\mathbb{N}$. The resulting inclusions of coordinate rings $K[T^{\Gamma_{p,n}}] \subset K[T^{\Gamma_{p,m}}]$ define canonical morphisms $X_{p,m} \to X_{p,n}$ of compactifications of the affine line $\mathbb{A}^1 = \mathrm{Spec}\, K[T^{-1}]$.

*Proof of Theorem 7.1 in the general case.* We proceed by induction on $n \geq 1$. The case $n = 1$ was handled above. Suppose now $n \geq 2$, and that the assertion is true for $n - 1$. To simplify notation, set

$$X = X_{p,n} \quad \text{and} \quad G = \mathrm{Aut}_{X/K} \quad \text{and} \quad H = \mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m,$$

and let $I \subset G$ be the inertia group scheme for the singularity $x_0 \in X$. Likewise, we set $X' = X_{p,n-1}$. By induction, $H' = \mathbb{G}_a \rtimes U_{n-1} \rtimes \mathbb{G}_m$ coincides with $G' = \mathrm{Aut}_{X'/K}$. Also note that by the very definition of the group schemes, we have a canonical inclusion $H' \subset H$. Moreover, with Proposition 4.5 we get an inclusion $H' \subset I$,

and actually $H' = I \cap H$. By Lemma 7.3 combined with [27], Proposition 2.7 the blowing-up morphism $f : X' \to X$ is equivariant with respect to the action of $I$. We thus get inclusions $H' \subset I \subset G' = H'$, and infer $H' = I$.

The orbit map for the rational point $x_0 \in X$ gives an inclusion $H/H' \subset G/I$ of closed subschemes inside $X$. This is actually contained in the scheme of singularities $Z = \mathrm{Sing}(X/K)$, according to [10], Proposition 3.1. Our task is to show that the inclusion is an equality, and for this it suffices to verify that the coordinate rings have the same degree. We already saw that $h^0(\mathscr{O}_{H/H'}) = p^n$, and it remains to verify $h^0(\mathscr{O}_{G/I}) \leq p^n$. For this we may assume that $K$ is algebraically closed.

According to (24) and Proposition 5.3, the scheme of singularities $Z = \mathrm{Sing}(X/K)$ has coordinate ring of the form $A = K[x_0, \ldots, x_{n-1}, y]/(x_0^p, \ldots, x_{n-1}^p, y^{p-2})$. In light of [12], Chapter III, §3, Theorem 6.1 the homogeneous space $G/I$ has coordinate ring of the form $B = K[u_1, \ldots, u_r]/(u_1^{p^{\nu_1}}, \ldots, u_r^{p^{\nu_r}})$ for some $r \geq 0$ and certain exponents $\nu_i \geq 1$. From the canonical surjection

$$\varphi : A = \Gamma(\mathscr{O}_Z) \longrightarrow \Gamma(\mathscr{O}_{G/I}) = B$$

we infer $\nu_i = 1$ and $r \leq n + 1$. Using the relation $y^{p-2} = 0$ we see that $\varphi(y) \in \mathfrak{m}_B$ must be contained in $\mathfrak{m}_B^2$, and thus actually $r \leq n$. It follows that $h^0(\mathscr{O}_{G/I}) \leq p^n$, as desired. □

## 8. Equivariant normality and twisting

We now seek to construct twisted forms of our curves $X_{p,n}$ that are regular. Our methods to achieve this apply in many other contexts, and we first give a general discussion about twisted forms, their regularity properties, and Brion's recent notion of equivariant normality.

Fix a ground field $K$ and let $X$ be a scheme. Recall that another scheme $Y$ is called a *twisted form* of $X$ if we have $Y \otimes L \simeq X \otimes L$ for some field extension $K \subset L$. Such twisted forms may arise as follows: Suppose a group scheme $G$ acts on $X$, and let $P$ be a $G$-torsor. Then $G$ acts diagonally on $P \times X$, and the quotient

$${}^P X = G \backslash (P \times X)$$

is a twisted form of $X$. Note that the diagonal action is free, hence the quotient exists as an algebraic space. Such quotients are not necessarily schematic (for concrete examples see [37]). However, if $G$ is finite and $X$ is covered by affine open sets that are $G$-stable, the twisted form is indeed a scheme ([12], Chapter III, §2, Theorem 3.2).

Suppose now we are in positive characteristic $p > 0$. It then may happen that a noetherian scheme with singularities has twisted forms where all singularities are gone. We now describe a fairly general procedure to achieve this, relying on a combination of works of Brion and the second author ([9], [10], [36], [40]). For simplicity, we assume throughout that $X$ is a separated scheme of finite type that is geometrically integral. It is *normal* if all local rings $\mathscr{O}_{X,a}$ are integrally closed in the common function field $F = \mathrm{Frac}(\mathscr{O}_{X,a})$. Equivalently, each finite modification $f : X' \to X$ is an isomorphism. Here the term *modification* refers to an integral scheme $X'$, together with a proper surjective morphism $f : X' \to X$ inducing a bijection on function fields.

In what follows, we suppose that $X$ is endowed with the action of a finite group scheme $G$. We now consider only modifications $f : X' \to X$ where $X'$ is a $G$-scheme and $f$ is equivariant. For brevity, we call such a datum an *equivariant modification*, or *$G$-modification*. Examples are given by blowing-ups $X' = \mathrm{Bl}_Z(X)$ with respect to $G$-stable centers $Z \subset X$. Note that for a given modification $X'$, there is at most one $G$-action on $X'$ making $f : X' \to X$ equivariant.

One says that $X$ is *equivariantly normal*, or *$G$-normal*, if every finite equivariant modification $f : X' \to X$ is an isomorphism. This extremely useful notion was introduced and studied by Brion [9]. He showed that $X$ admits a finite equivariant modification $\tilde{X}$ that is equivariantly normal (loc. cit., Proposition 4.2). It is actually unique up to unique equivariant isomorphism, provided that $X$ is one-dimensional (loc. cit., Corollary 4.4).

From now on, we furthermore assume that our $G$-scheme $X$ is one-dimensional. One could also say that $X$ is a *$G$-curve*. Following [14], Section 2 we write $\mathrm{Sing}(X/K)$ for the closed subscheme defined by the first Fitting ideal for $\Omega^1_{X/K}$. This is the set of points $a \in X$ where the local ring $\mathscr{O}_{X,a}$ fails to be geometrically regular, endowed with a canonical scheme structure. Note that with respect to this scheme structure it must be $G$-stable ([10], Proposition 3.1). The existence of twisted forms that are regular is intimately related to equivariant normality:

**Theorem 8.1.** *Let $P$ be a $G$-torsor. Then the twisted form $Y = {}^PX$ is regular provided the following three conditions hold:*

(i) *The curve $X$ is $G$-normal.*
(ii) *The total space of the $G$-torsor $P$ is reduced.*
(iii) *The reduction of the finite scheme $\mathrm{Sing}(X/K)$ is étale.*

*Proof.* The residue fields $\kappa(a)$ for the points $a \in \mathrm{Sing}(X/K)$ are separable, by assumption (iii), and so is their join $L$. This ensures that the base-change $P_L$ remains reduced. Furthermore, the arguments for [9], Proposition 4.10 show that $X_L$ remains equivariantly normal. Replacing the ground field by $L$, we may assume that $\mathrm{Sing}(X/K) = \{a_1, \ldots, a_r\}$ comprises only rational points. Let $H_i \subset G$ be the inertia subgroup scheme, and $Z_i = G \cdot a_i = G/H_i$ be the orbit for $a_i \in X$. Clearly, the subscheme $Z_1 \cup \ldots \cup Z_r$ and its complementary open set $U$ are $G$-stable. The latter is geometrically regular, and so is the twisted form ${}^PU$.

It remains to verify that the integral curve $Y = {}^PX$ is regular at the points $b \in {}^PZ_i$. According to [9], Theorem 4.13 the orbit $Z_i \subset X$ is an effective Cartier divisor. In turn, its twist ${}^PZ_i \subset {}^PX$ is an effective Cartier divisor on ${}^PX$, so it suffices to verify that it is reduced. The latter becomes the quotient of $P \times G/H_i$ by the diagonal $G$-action, which can be identified with $H_i \backslash P$. Its coordinate ring is a subring inside $\Gamma(P, \mathscr{O}_P)$, which can be seen as a ring of invariants, and $\Gamma(P, \mathscr{O}_P)$ is reduced by assumption. □

Note that condition (iii) holds in particular if all $a \in \mathrm{Sing}(X/K)$ are rational points. The first two conditions can be achieved after ground field extensions:

**Proposition 8.2.** *Suppose that the curve $X$ is $G$-normal. Then there is a field extension $K \subset L$ such that the following holds:*

(i) *The base-change $X_L$ is $G_L$-normal.*

(ii) *There is a $G_L$-torsor $P$ whose total space is reduced.*

*Proof.* (ii) Choose a geometrically integral quasi-projective $G$-scheme $U$ with generically free action. This could arise from an embedding $G \subset H$ into a smooth group scheme of finite type, or could arise from a projective scheme $X$ with $G = \mathrm{Aut}^0_{X/K}$, according to [10], Proposition 1.7 or Theorem 2.1. The quotient $V = U/G$ is an integral quasi-projective scheme, and the quotient map $f : U \to V$ induces a finite extension of the function field $L = k(V)$ by $E = k(U)$. By construction, the reduced scheme $P = \mathrm{Spec}(E)$, viewed as an $L$-scheme, is torsor with respect to the base-change $G_L = G \otimes_K L$.

(i) The above extension $K \subset E$ is separable, because $U$ is geometrically reduced. In turn, the subextension $L$ is also separable. The arguments for [9], Proposition 4.10 show that $X_L$ remains equivariantly normal. □

In the reverse direction, we have the following result:

**Theorem 8.3.** *Suppose there is field extension $K \subset L$, a subgroup scheme $H \subset G_L$, and a $H$-torsor $P$ so that the twisted form ${}^P(X_L)$ is regular. Then the curve $X$ is $G$-normal.*

*Proof.* According to [9], Proposition 4.10 and Remark 4.3 it suffices to treat the case $L = K$ and $H = G$. Let $X' = {}^P X$ be the regular twisted form. According to [41], Lemma 3.1 we have a canonical identification $\mathrm{Aut}_{X'/K} = {}^P\mathrm{Aut}_{X/K}$ of the sheaves of automorphisms, where the term on the right is formed with respect to the conjugacy action of $G$ on $\mathrm{Aut}_{X/K}$. Setting $G' = {}^P G$ we get a homomorphism $G' \to \mathrm{Aut}_{X'/K}$, hence a $G'$-action on $X'$.

Let $Z \subset X$ be a finite closed subscheme that is $G$-stable. According to [9], Theorem 4.13 we have to check that $Z$ is Cartier. Its twist $Z' = {}^P Z$ defines a finite closed subscheme inside $X'$. The latter is regular, so $Z'$ is Cartier. Choose a point $p \in P$, and let $E = \kappa(p)$ be the resulting field extension. The resulting trivialization of $P \otimes E$ defines an isomorphism $g : X \otimes E \to X' \otimes E$ with $g(Z \otimes E) = Z' \otimes E$. It follows that $Z \otimes E$ and hence $Z$ is Cartier. □

Recall that a *quasielliptic curve* is a regular curve $Y$ that is a twisted form of the *rational cuspidal curve*

$$X = \mathrm{Spec}\, K[T^2, T^3] \cup \mathrm{Spec}\, K[T^{-1}].$$

Clearly, $\mathrm{Sing}(X/K)$ is a singleton, containing only the rational point $x_0$ given by $T^2 = T^3 = 0$. It turns out that quasielliptic curves exist only in characteristic two and three (compare the discussion after Proposition 10.1). For $p = 2$, the rational vector field $D = T^{-2}\partial/\partial T$ satisfies $D^{[p]} = 0$ and actually defines a global section $D \in H^0(X, \Theta_{X/K})$, hence corresponds to an action of $G = \alpha_p$, which is the Frobenius kernel of the additive group $\mathbb{G}_a$. The orbit $G \cdot x_0$ is the Cartier divisor defined by $T^2 = 0$. For $p = 3$, the same holds for $D = \partial/\partial T$ and the Cartier divisor $T^3 = 0$.

In both cases, we conclude that the rational cuspidal curve is equivariantly normal with respect to $G = \alpha_p$ (again by [9], Theorem 4.13). For this group scheme, torsors with regular total space exist if and only if $K$ is imperfect (for example [41], Lemma 7.1), and then quasielliptic curves exist by Theorem 8.1. Also note that $X$ is equivariantly normal with respect to any larger finite subgroup scheme inside the

full automorphism group scheme (obvious, see [9], Remark 4.3). According to [6], Proposition 6 we have an iterated semidirect product $\mathrm{Aut}_{X/K} = \mathbb{G}_a \rtimes U \rtimes \mathbb{G}_m$ for an infinitesimal group scheme $U$. For $p = 3$ it coincides with the copy of $\alpha_p$ described above, whereas for $p = 2$ it has order $|U| = 8$.

All this generalizes to our hierarchy of curves $X_{p,n}$:

**Theorem 8.4.** *The curve $X = X_{p,n}$ is equivariantly normal with respect to the finite group scheme $U_n$, and locally of complete intersection. Moreover, if there is a $U_n$-torsor $P$ so that the quotient $\bar{P} = U_{n-1}\backslash P$ is reduced, then the twisted form $Y = {}^P X$ is regular.*

*Proof.* The first assertion follows from [9], Theorem 4.13 and Corollary 4.18. If $P$ itself is reduced, the assertion on the twisted form $Y = {}^P X$ directly follows from Theorem 8.1. Its proof actually shows our slightly stronger claim, because the singularity $x_0 \in X$ is rational, with orbit $U_n/U_{n-1}$. □

Note that after some ground field extension $K \subset L$, there is a $U_n$-torsor $P$ that is reduced, according to Proposition 8.2, and our curve $X = X_{p,n}$ acquires twisted forms that are regular. However, the construction of $L$ relies, via [10], Proposition 1.7 and Theorem 2.1, among other things on embeddings of $U_n$ into smooth group schemes $H$, and here we have little control on $\dim(H)$ and $\mathrm{trdeg}(L)$.

Also note that the above argument for locally complete intersection relying on equivariant normality is independent from the arguments relying on numerical semigroups in the proof of Proposition 5.1.

## 9. Non-abelian cohomology and semidirect products

In this section we review the general notions of *torsors and twisting*, which will be used in the next section to understand the twisted forms of our curves $X_{p,n}$. The material is well-known, but it is not easy to find suitable references that are general enough for our purposes, yet not burdened by over-abstraction. Throughout, we are guided by [42], Chapter I, §5 and [16], Chapter III, §2.

Let $\mathscr{P} = \mathrm{Sh}(\mathcal{C})$ be the topos of sheaves on some site $\mathcal{C}$, having a final object $S$. For any group-valued object $G \in \mathscr{P}$, we write $H^0(S, G)$ for the group of global sections, and $H^1(S, G)$ for the set of isomorphism classes of *$G$-torsors* $P$. The latter is an object endowed with a $G$-action that is locally isomorphic to $P_0 = G$ with the translation action. Another widespread terminology is *principal homogeneous spaces*. For $G$ commutative our $H^1(S, G)$ coincides with the sheaf cohomology groups. In general, however, $H^1(S, G)$ is merely a set, containing the class of the trivial torsor $P_0 = G$ as a distinguished element.

An object $\tilde{X}$ is called a *twisted form* of an object $X$ if the two are locally isomorphic. If $X$ has a $G$-action, and $P$ is a $G$-torsor, we get such a twisted form by forming the quotient $\tilde{X} = {}^P X = P \wedge^G X = G\backslash(P \times X)$ with respect to the diagonal action $\sigma \cdot (p, x) = (\sigma p, \sigma x)$. Note that this could also be written as $(p\sigma^{-1}, \sigma x)$. For $G = \mathrm{Aut}_{X/S}$, the above construction gives an identification between the non-abelian cohomology $H^1(S, G)$ and the set $\mathrm{Twist}(X)$ of isomorphism classes of twisted forms $\tilde{X}$ of the object $X$. In any case, the $G$-action on $X$ induces a conjugacy action

on $\mathrm{Aut}_{X/S}$, and we have $\mathrm{Aut}_{(P\wedge^G X)/S} = P \wedge^G \mathrm{Aut}_{X/S}$, compare for example [41], Lemma 3.1.

Suppose now $X = G$ as sheaves of sets without group laws, and consider the homomorphism $G \times G^{\mathrm{op}} \to \mathrm{Aut}_{X/S}$ given by $(\sigma_1, \sigma_2) \cdot x = \sigma_1 x \sigma_2^{-1}$. One easily checks that the map is equivariant with respect to factorwise conjugation $\eta \cdot (\sigma_1, \sigma_2) = (\eta\sigma_1\eta^{-1}, \eta\sigma_2\eta^{-1})$ and conjugation with inner automorphisms on $\mathrm{Aut}_{X/S}$. In turn, we get an induced homomorphism

$$ {}^P\!G \times {}^P\!G^{\mathrm{op}} \longrightarrow \mathrm{Aut}_{(P\wedge^G X)/S} = \mathrm{Aut}_{P/S}\,. $$

Note that the equation stems from the identification $P \wedge^G X = P$. The above endows each $G$-torsor $P$ with the *additional structure* of a ${}^P\!G$-torsor and a ${}^P\!G^{\mathrm{op}}$-torsor. Furthermore, ${}^P\!G^{\mathrm{op}}$ is the automorphism group object of $P$ as a $G$-torsor, and $G$ is the automorphism group object of $P$ as a ${}^P\!G^{\mathrm{op}}$-torsor. In turn, we get what we like to call the *torsor translation map*

$$ H^1(S, {}^P\!G) \longrightarrow H^1(S, G), \quad T \longmapsto P \wedge^{{}^P\!G} T, \tag{30} $$

where the quotient on the right is formed with respect to the action $\tilde\sigma \cdot (p, t) = (p\tilde\sigma^{-1}, \tilde\sigma t)$, and the $G$-action on $P \wedge^G T$ stems from the action on the first factor $P$. The map (30) is bijective, but does not respect the distinguished points: Rather, it sends $T_0 = {}^P\!G$ to $P = P \wedge^{{}^P\!G} T_0$.

Suppose now we have a short exact sequence

$$ 1 \longrightarrow A \longrightarrow B \xrightarrow{\mathrm{pr}} C \longrightarrow 1 \tag{31} $$

of group objects. Then the group $H^0(S, C)$ acts from the right on the set $H^1(S, A)$ in the following way: For each global section $c \in H^0(S, C)$, the fiber $B_c = \mathrm{pr}^{-1}(c)$ with respect to the surjection $B \to C$ carries compatible $A$-torsor structures from both sides, coming from the group law in $B$. We now define $c \cdot [P] = [B_c \wedge^A P]$. The stabilizer group at each torsor class is the subgroup of global sections $c \in H^0(S, C)$ where the set of global sections $H^0(S, B_c)$ is non-empty.

Let us write $H^1(S, A)/H^0(S, C)^{\mathrm{op}} = H^0(S, C)\backslash H^1(S, A)$ for the quotient of the action. Using the distinguished point in $H^1(S, A)$, the orbit map $c \mapsto B_c$ yields $H^0(S, C) \to H^1(S, A)$. The latter serves as a *connecting map*, and yields a *six-term sequence* of sets

$$ 1 \to H^0(S, A) \to H^0(S, B) \to H^0(S, C) \xrightarrow{\partial} H^1(S, A) \to H^1(S, B) \to H^1(S, C). $$

The maps on the right come from extension of structure groups. Here all arrows preserve the distinguished points, and in degree zero the above is an exact sequence of groups.

The group object $B$ acts on itself and its quotient $C = B/A$ via conjugacy. On the normal subgroup $A$, we have an induced action. Twisting with respect to the $B$-actions gives another exact sequence

$$ 1 \longrightarrow {}^P\!A \longrightarrow {}^P\!B \longrightarrow {}^P\!C \longrightarrow 1, \tag{32} $$

which also yields a six-term sequence. Note that in general there is no map relating $H^1(S, A)$ and $H^1(S, {}^P\!A)$, because the $B$-action on $A$ usually fails to be inner.

We now choose for each $C$-torsor $\bar{P}$ whose class belongs to the image of the mapping $H^1(S,B) \to H^1(S,C)$ some $B$-torsor $P$ with $C \wedge^B T \simeq \bar{P}$. As in [42], Section 5.5, Corollary 2 one has:

**Theorem 9.1.** *The first cohomology of $B$ can be written as a disjoint union*

$$H^1(S,B) = \bigcup H^1(S, {}^P A)/H^0(S, {}^{\bar{P}}C)^{\mathrm{op}}$$

*running over all $[\bar{P}]$ from the image of $H^1(S,B) \to H^1(S,C)$. The inclusions are obtained by composing the induced maps $H^1(S, {}^P A) \to H^1(S, {}^P B)$ with the torsor translation maps $H^1(S, {}^P B) \to H^1(S,B)$ given by (30).*

We are interested in cases where the above simplifies. Recall that $\mathrm{pr} : B \to C$ is the canonical epimorphism. Let us call a morphism $s : C \to B$ a *set-theoretical section* if $\mathrm{pr} \circ s = \mathrm{id}_C$. The point here is that $s$ does not have to preserve the group laws. The resulting $A \times C \to B$ given by $(a,c) \mapsto a \cdot s(c)$ is an isomorphism of objects that does not necessarily respect the group laws. The latter is determined by the two-cocycle $\tau : C^2 \to A$ defined by $s(cc') = \tau_{c,c'} \cdot s(c)s(c')$. We like to indicate this situation by writing

$$B = A \tilde{\times} C = A \tilde{\times}_\tau C,$$

and say that the extension $C$ is *set-theoretically split*. Note that this always holds in the category of groups, but often fails in the category of group schemes (compare [39], discussion around Theorem 8.5). Also note that this property is not necessarily preserved in twisted extensions (32). If $s$ respects the group laws, the above becomes a semidirect product $B = A \rtimes C = A \rtimes_\varphi C$ where $\varphi$ is given by conjugacy, and the extension is called *split*.

**Corollary 9.2.** *Suppose for all $\bar{P}$ as above, the extension (32) is set-theoretically split or the group $H^0(S, {}^{\bar{P}}C)$ is trivial. Then we have a disjoint union*

$$H^1(S,B) = \bigcup H^1(S, {}^P A),$$

*running over all $[\bar{P}]$ from the image of $H^1(S,B) \to H^1(S,C)$. The latter map is actually surjective, provided that the extension (31) is split.*

*Proof.* Set $C' = {}^{\bar{P}}C$ and $A' = {}^P A$. If $B' = {}^P B$ is set-theoretically split, all fibers over $c' \in H^0(S,C')$ are trivial torsors, hence the action of $H^0(S,C')$ on $H^1(S,A')$ is trivial. The same holds, of course, if the group $H^0(S,C')$ itself is trivial. So the theorem implies the first assertion.

If the projection $\mathrm{pr} : B \to C$ admits a section $s$ that respects the group structure, the induced map on cohomology is right inverse to $H^1(S,B) \to H^1(S,C)$, so the latter is surjective. □

In particular, for $B = A \rtimes C$ satisfying the assumptions of the corollary, we get a disjoint union

$$H^1(S,B) = \bigcup H^1(S, {}^P A)$$

running over all $[\bar{P}] \in H^1(S,C)$. It is convenient to regard its elements as "pairs" $(\gamma, \alpha)$ with $\gamma = [P] \in H^1(S,C)$ and $\alpha \in H^1(S, {}^P A)$. If $H^1(S, \mathrm{Aut}_{A/S})$ is a singleton, the choice of isomorphisms $h : {}^P A \to A$ indeed identifies the above with the product

$H^1(S,C) \times H^1(S,A)$, independent of the $h$. Note that this carries a canonical group structure if $A$ and $C$ are commutative, which may happen without $B$ being commutative.

## 10. Description of the set of twisted forms

Let $K$ be a ground field of characteristic $p > 0$, and set $S = \operatorname{Spec}(K)$. Using the general results of the previous section, we seek to compute the first non-abelian cohomology for the iterated semidirect products $\mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m = \operatorname{Aut}_{X_{p,n}/K}$ and thereby the set of isomorphism classes of twisted forms for $X_{p,n}$. We are able to do so for $1 \leq n \leq 2$.

Throughout, we work over the site $\mathcal{C} = (\mathrm{Aff}/S)$, endowed with the fppf topology. Let us start with some general useful facts:

**Proposition 10.1.** *The following holds for group schemes $G$ of finite type:*

(i) *If $G = N \widetilde{\times} \mathbb{G}_m$ for some group scheme $N$ of finite type, then the canonical map $H^1(S,N) \to H^1(S,G)$ is bijective.*
(ii) *In the special case $G = \mathbb{G}_a^{\oplus r} \widetilde{\times} \mathbb{G}_m$ the set $H^1(S,G)$ is a singleton.*
(iii) *If $G$ is infinitesimal the group $H^0(S,G)$ is trivial.*

*Proof.* We have $H^1(S,\mathbb{G}_m) = 0$ by Hilbert 90, so (i) follows from Corollary 9.2. With $N = \mathbb{G}_a^{\oplus r}$ we use [28], Chapter III, Theorem 3.7 and Serre's Vanishing to get $H^1(S,N) = 0$, and (ii) follows as well. Assertion (iii) is obvious, because an infinitesimal group scheme has $G_{\mathrm{red}} = S$. □

Note that for $p \geq 5$ the automorphism group scheme for the rational cuspidal curve $X = \operatorname{Spec} K[T^2,T^3] \cup \operatorname{Spec} K[T^{-1}]$ is given by $G = \mathbb{G}_a \rtimes \mathbb{G}_m$, so this curve has no twisted forms besides itself. This purely cohomological argument shows again that quasielliptic curves are confined to characteristic $p \leq 3$. The following observation will also be useful:

**Lemma 10.2.** *Let $G_1$ and $G_2$ be twisted forms of $\mathbb{G}_a$. If they are isomorphic as schemes, they are isomorphic as group schemes.*

*Proof.* Let $f : G_1 \to G_2$ be an isomorphism of schemes. Composing with a translation, we may assume that $f(e_1) = e_2$. To verify that $f$ respects the group law, we may assume that $K = K^{\mathrm{alg}}$, and this reduces to the case $G_1 = G_2 = \mathbb{G}_a$. The induced map $\varphi : K[T] \to K[T]$ on the coordinate ring is given by $\varphi(T) = \lambda T + \mu$ for some $\lambda, \mu \in K$. We have $\lambda \neq 0$ because $f$ is non-constant, and $\mu = 0$ because $f$ respects the origin. So for each $\alpha \in \mathbb{G}_a(R)$ we have $f(\alpha) = \lambda\alpha$, which respects the group laws. □

For each pair $\Phi, \Psi \in K[u]$ of additive polynomials with $\gcd(\Phi,\Psi) \neq 0$, in other words not both polynomials vanish, the resulting homomorphism $(\Phi, -\Psi) : \mathbb{G}_a^{\oplus 2} \to \mathbb{G}_a$ given by $(u,v) \mapsto \Phi(u) - \Psi(v)$ is an epimorphism. The short exact sequence

$$0 \longrightarrow U_{\Phi,\Psi} \longrightarrow \mathbb{G}_a^{\oplus 2} \stackrel{(\Phi,-\Psi)}{\longrightarrow} \mathbb{G}_a \longrightarrow 0 \tag{33}$$

defines a unipotent group scheme $U_{\Phi,\Psi}$, and the resulting long exact sequence yields

$$H^1(S, U_{\Phi,\Psi}) = K/\{\Phi(u) - \Psi(v) \mid u, v \in K\}. \tag{34}$$

By Russell's Theorem ([35], Theorem 2.1) every twisted form of the additive group is isomorphic to $U_{\Phi,\Psi}$ with $\Phi(u) = u^{p^n}$ for some $n \geq 0$, and $\Psi(u)$ separable. The following sheds further light on this:

**Proposition 10.3.** *The unipotent group scheme $U_{\Phi,\Psi}$ is a twisted form of $\mathbb{G}_a$ if and only if $\gcd(\Phi, \Psi) = u$ inside the euclidean domain $K[u]$.*

*Proof.* It suffices to treat the case that $K$ is algebraically closed. Set $U = U_{\Phi,\Psi}$. Suppose first that there are $a, b \in k[u]$ with $a\Phi - b\Psi = u$. These yield a section for $(\Phi, -\Psi) : \mathbb{G}_a^{\oplus 2} \to \mathbb{G}_a$, defined via $u \mapsto (a(u), b(u))$, which does not have to preserve the group laws. It induces an identification $\mathbb{G}_a^{\oplus 2} = U \times \mathbb{G}_a$ of schemes. In turn, the coordinate ring $A = \Gamma(U, \mathscr{O}_U)$ has the property $A[y] = K[x, y]$. According to Zariski Cancellation ([1], Corollary 2.8) the underlying scheme is isomorphic to the affine line $\mathbb{A}^1$. By Lazard's Theorem ([12], Chapter IV, 4.1), we must have $U \simeq \mathbb{G}_a$ as group schemes.

Conversely, suppose that $\gcd(\Phi, \Psi) \neq u$. Since $K$ is algebraically closed, we have $\Phi(u) = \prod_{\omega \in A}(u-\omega)^{p^m}$ and $\Psi(u) = \prod_{\omega \in B}(u-\omega)^{p^n}$ for some exponents $m, n \geq 0$ and some finite subgroups $A, B \subset K$. Their intersection is non-zero, by the assumption on the gcd. Consequently we can write $\Phi(u) = \Phi_1(h(u))$ and $\Psi(u) = \Psi_1(h(u))$ for some additive polynomial of the form $h(u) = \prod_{i=0}^{p-1}(u - i\omega_0)$, with some non-zero $\omega_0 \in K$. In turn, the projection $(\Phi, -\Psi) : \mathbb{G}_a^{\oplus 2} \to \mathbb{G}_a$ factors over the morphism $h : \mathbb{G}_a \to \mathbb{G}_a$. In turn, the kernel $U_{\Phi,\Psi}$ is disconnected or non-reduced. □

**Proposition 10.4.** *For each group scheme of the form $G = \mathbb{G}_a \rtimes Q \rtimes \mathbb{G}_m$, where $Q$ is any infinitesimal group scheme of finite type, we have a canonical identification*

$$H^1(S, G) = \bigcup_{\alpha \in H^1(S,Q)} K/\{\Phi_\alpha(u) - \Psi_\alpha(v) \mid u, v \in K\}$$

*for certain additive polynomials $\Phi_\alpha, \Psi_\alpha \in K[u]$ with $\gcd(\Phi_\alpha, \Psi_\alpha) = u$.*

*Proof.* By Proposition 10.1, the canonical map $H^1(S, \mathbb{G}_a \rtimes Q) \to H^1(S, G)$ is bijective. Since $Q$ is infinitesimal, we can apply Proposition 9.2, and the assertion follows with (34). □

Roughly speaking, to understand this cohomology of $G$, one has to understand the cohomology of $Q$ and the dependence of the additive polynomials $\Phi_\alpha, \Psi_\alpha$ on the class $\alpha$. We now seek to unravel this with $G = \mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m$. For $n = 1$ the term in the middle becomes $U_1 = \alpha_p$. The short exact sequence $0 \to \alpha_{p^n} \to \mathbb{G}_a \xrightarrow{F^n} \mathbb{G}_a \to 0$ yields an identification $H^1(S, \alpha_{p^n}) = K/K^{p^n}$, for every $n \geq 1$. The dependence of the additive polynomials can be described as follows:

**Proposition 10.5.** *For the $\alpha_p$-torsor $P = \operatorname{Spec} K[y]/(y^p - \alpha)$, the additive polynomials $\Phi(u) = u^p$ and $\Psi(v) = v - \alpha v^p$ give the twisted form ${}^P\mathbb{G}_a = U_{\Phi,\Psi}$.*

*Proof.* Set $B = K[x, y]/(y^p - \alpha)$. By definition, the coordinate ring for ${}^P\mathbb{G}_a$ is the subring $A \subset B$ of elements that are invariant under $x \mapsto x + \lambda x^p$ and $y \mapsto y + \lambda$, for all group elements $\lambda \in \alpha_p(R)$ and all rings $R$. Clearly, $v = x^p$ and $u = x - x^p y$ are such invariants, satisfying the relation $u^p = v - \alpha v^p$. Its partial derivatives generate the unit ideal, and we conclude that the subring $A' \subset A$ generated by $u$ and $v$

is regular and one-dimensional, and can be identified with the residue class ring $K[u,v]/(u^p - v + \alpha v^p)$. The composite extension $K(x^p) \subset \mathrm{Frac}(A') \subset \mathrm{Frac}(A) \subset \mathrm{Frac}(B)$ has degree $p^2$, and the outer steps have degree $p$. Consequently $A' = A$. The assertion now follows from Lemma 10.2. □

To tackle the case $n = 2$ we use the short exact sequence

$$0 \longrightarrow \alpha_p \longrightarrow U_2 \longrightarrow \alpha_{p^2} \longrightarrow 0,$$

where the inclusion on the left is $\lambda \mapsto 1 + \lambda x^{p^2}$, and the surjection on the right $(1 + \lambda_1 x^p + \lambda_2 x^{p^2}) \mapsto \lambda_1$. Given $\alpha, \beta \in K$, the finite scheme $P = P_{\alpha,\beta}$ defined by

$$P(R) = \{(y,z) \in R^2 \mid y^{p^2} = \alpha \text{ and } z^p = \beta + \alpha y^p\} \tag{35}$$

carries an $U_2$-action via the formula $(\lambda_1, \lambda_2) \cdot (y,z) = (\lambda_1 + y, \lambda_2 + z + \lambda_1 y^p)$. One easily checks that this indeed takes values in $P(R)$, that it satisfies the axioms for group actions, and that the action is free and transitive. The induced $\alpha_{p^2}$-torsor $\bar{P}$ is obtained from $P$ as a quotient by $\alpha_p$, in other words, by the action of $\lambda_2$. This yields $\bar{P}(R) = \{y \in R \mid y^{p^2} = \alpha\}$. In turn, we get the description $H^1(S, U_2) = \bigcup_{K/K^{p^2}} K/K^p$. It remains to express the twisted form ${}^P\mathbb{G}_a$ in terms of additive polynomials:

**Proposition 10.6.** *For the $U_2$-torsor $P$ as above, the additive polynomials*

$$\Phi(u) = u^{p^2} \quad \textit{and} \quad \Psi(u) = u - \alpha u^p - \beta^p u^{p^2}$$

*give the twisted form ${}^P\mathbb{G}_a = U_{\Phi,\Psi}$.*

*Proof.* Set $B = K[x,y,z]/(y^{p^2} - \alpha, z^p - \beta - \alpha y^p)$. The coordinate ring for ${}^P\mathbb{G}_a$ is the subring $A \subset B$ of elements that are invariant under

$$x \longmapsto x + \lambda_1 x^p + \lambda_2 x^{p^2} \quad \text{and} \quad y \longmapsto y + \lambda_1 \quad \text{and} \quad z \longmapsto z + \lambda_2 + \lambda_1 y^p,$$

for all group elements $(\lambda_1, \lambda_2) \in U_2(R)$ and all rings $R$. One easily checks that $v = x^{p^2}$ and $u = x - x^p y - x^{p^2} z + x^{p^2} y^{p+1}$ are invariant, and that these invariants satisfy the relation $u^{p^2} = v - \alpha v^p - \beta^p v^{p^2}$. The argument concludes as in the preceding proof. □

Note that the invariant $u$ can be found by starting with the non-invariant $x$ and successively adding monomials to cancel non-invariance. Collecting all the above, we have determined for $G_n = \mathbb{G}_a \rtimes U_n \rtimes \mathbb{G}_m$ in the cases $1 \leq n \leq 2$ the non-abelian cohomology:

**Theorem 10.7.** *With the above notation, we have*

$$H^1(S, G_1) = \bigcup_{\alpha} K/\{u^p - v + \alpha v^p \mid u, v \in K\},$$

*where the union runs over all $\alpha \in K/K^p$, and*

$$H^1(S, G_2) = \bigcup_{(\alpha,\beta)} K/\{u^{p^2} - v - \alpha v^p - \beta^p v^{p^2} \mid u, v \in K\},$$

*where the union runs over $(\alpha, \beta) \in \bigcup_{K/K^{p^2}} K/K^p$, with $\alpha \in K/K^{p^2}$ and $\beta \in K/K^p$.*

Note that for $3 \leq p^n \leq 4$ this gives back, in an intrinsic fashion, Queen's descriptions for quasielliptic curves ([31], [32]).

Also note that for $n = 1$, the group $K/\{u^p - v + \alpha v^p \mid u, v \in K\}$ is trivial, provided that $K$ is separably closed or $\alpha \in K^p$. It follows that the Frobenius map

$$H^1(S, G_1) \longrightarrow H^1(S, G_1), \quad P \longmapsto P^{(p)} = P \otimes_F K$$

is trivial, in the sense that it sends every class to the distinguished class. In particular, every twisted form $Y$ of $X_{p,1}$ is untwisted by Frobenius pullback, and becomes a rational curve (compare [21]). Likewise for $n = 2$, the group $K/\{u^{p^2} - v - \alpha v^p - \beta^p v^{p^2} \mid u, v \in K\}$ is trivial if $K$ is separably closed or $\alpha \in K^{p^2}$, $\beta \in K^p$. Now the map $P \mapsto P^{(p^2)}$ is trivial, and every twisted form $Y$ of $X_{p,2}$ gets untwisted by the second Frobenius pullback.

With the notation from the theorem, let $T$ be a $G_n$-torsor, and $\alpha \in K/K^{p^n}$ be the ensuing class, for $1 \leq n \leq 2$. Write $\tilde{X}$ for the twisted form of $X = X_{p,n}$ corresponding to $T$.

**Proposition 10.8.** *With the above notation, the curve $\tilde{X}$ is regular provided that $\alpha \in K/K^{p^n}$ does not belong to $K^p/K^{p^n}$.*

*Proof.* The $G_n$-torsor $T$ is induced from some torsor $P$ with respect to $\mathbb{G}_a \rtimes U_n$, according to Proposition 10.1. By construction, the class $\alpha \in K/K^{p^n}$ corresponds to the quotient $\bar{P} = (\mathbb{G}_a \rtimes U_{n-1})\backslash P$, and the latter has coordinate ring $K[T]/(T^{p^n} - \alpha)$, where we write $\alpha$ also for the scalar rather than the class. The coordinate ring is reduced, in light of our assumption. According to Theorem 8.4, the curve $\tilde{X}$ is regular. □

It should be possible to extend the above results to all $n \geq 1$. For this one has to find an inductive description for the $U_n$-torsors, analogous to (35). The main problem is to cope with the non-commutativity involved in the torsors.

## References


[1] S. Abhyankar, W. Heinzer, P. Eakin: On the uniqueness of the coefficient ring in a polynomial ring. J. Algebra 23 (1972), 310–342.

[2] A. Assi, P. García-Sánchez: Numerical semigroups and applications. Springer, Cham, 2016.

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

[4] V. Barucci, D. Dobbs, M. Fontana: Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains. Mem. Amer. Math. Soc. 125 (1997), no. 598.

[5] E. Bombieri, D. Mumford: Enriques' classification of surfaces in char. $p$, III. Invent. Math. 35 (1976), 197–232.

[6] E. Bombieri, D. Mumford: Enriques' classification of surfaces in char. $p$, II. In: W. Baily, T. Shioda (eds.), Complex analysis and algebraic geometry, pp. 23–42. Cambridge University Press, London, 1977.

[7] M. Brion: Some structure theorems for algebraic groups. In: M. Can (ed.), Algebraic groups: structure and actions, pp. 53–126. Amer. Math. Soc., Providence, RI, 2017.

[8] M. Brion: On models of algebraic group actions. Proc. Indian Acad. Sci. Math. Sci. 132 (2022), Paper No. 61, 17 pp.

[9] M. Brion: Actions of finite group schemes on curves. Preprint, arXiv:2207.08209.

[10] M. Brion, S. Schröer: The inverse Galois problem for connected algebraic groups. Preprint, arXiv:2205.08117.

[11] C. Delorme: Sous-monoïdes d'intersection compléte de N. Ann. Sci. École Norm. Sup. 9 (1976), 145–154.
[12] M. Demazure, P. Gabriel: Groupes algébriques. Masson, Paris, 1970.
[13] M. Demazure, A. Grothendieck (eds.): Schémas en groupes I (SGA 3 Tome 1). Springer, Berlin, 1970.
[14] A. Fanelli, S. Schröer: Del Pezzo surfaces and Mori fiber spaces in positive characteristic. Trans. Amer. Math. Soc. 373 (2020), 1775–1843.
[15] The GAP Group: GAP – Groups, Algorithms, and Programming. https://www.gap-system.org, Version 4.12.1, 2022.
[16] J. Giraud: Cohomologie non abélienne. Springer, Berlin, 1971.
[17] K. Goodearl, R. Warfield: An introduction to noncommutative Noetherian rings. Second edition. Cambridge University Press, Cambridge, 2004.
[18] D. Goss: Basic structures of function field arithmetic. Springer,Berlin, 1996.
[19] M. Hall: The theory of groups. Macmillan, New York, 1959.
[20] J. Herzog: Generators and relations of abelian semigroups and semigroup rings. Manuscripta Math. 3 (1970), 175–193.
[21] C. Hilario, K.-O. Stöhr: On regular but non-smooth integral curves. Preprint, arXiv:2211.16962, 2022.
[22] N. Jacobson: The theory of rings. American Mathematical Society, New York, 1943.
[23] M. Kargapolov, J. Merzljakov: Fundamentals of the theory of groups. Springer, New York-Berlin, 1979.
[24] S. Kondō, S. Schröer: Kummer surfaces associated with group schemes. Manuscripta Math. 166 (2021), 323–342.
[25] B. Laurent: Almost homogeneous curves over an arbitrary field. Transform. Groups 24 (2019), 845–886.
[26] W. Bosma, J. Cannon, C. Playoust: The Magma algebra system. I. The user language. J. Symbolic Comput., 24 (1997), 235–265.
[27] G. Martin: Infinitesimal automorphisms of algebraic varieties and vector fields on elliptic surfaces. Algebra Number Theory 16 (2022), 1655–1704.
[28] J. Milne: Étale cohomology. Princeton University Press, Princeton, 1980.
[29] D. Mumford: Theta characteristics of an algebraic curve. Ann. Sci. École Norm. Sup. 4 (1971), 181–192.
[30] O. Ore: On a special class of polynomials. Trans. Amer. Math. Soc. 35 (1933), 559–584.
[31] C. Queen: Non-conservative function fields of genus one. I. Arch. Math. 22 (1971), 612–623.
[32] C. Queen: Non-conservative function fields of genus one. II. Arch. Math. 23 (1972), 30–37.
[33] D. Robinson: A course in the theory of groups. Springer, New York, 1993.
[34] J. Rosales, P. García-Sánchez: Numerical semigroups. Springer, New York, 2009.
[35] P. Russell: Forms of the affine line and its additive group. Pacific J. Math. 32 (1970), 527–539.
[36] S. Schröer: Kummer surfaces for the selfproduct of the cuspidal rational curve. J. Algebraic Geom. 16 (2007), 305–346.
[37] S. Schröer: Algebraic spaces that become schematic after ground field extension. Math. Nachr. 295 (2022), 1008–1012
[38] S. Schröer: There is no Enriques surface over the integers. Ann. of Math. 197 (2023), 1–63.
[39] S. Schröer: Albanese maps for open algebraic spaces. arXiv:2204.02613, to appear in Int. Math. Res. Not. IMRN.
[40] S. Schröer: The structure of regular genus-one curves over imperfect fields. Preprint, arXiv: 2211.04073.
[41] S. Schröer, N. Tziolas: The structure of Frobenius kernels for automorphism group schemes. arXiv:2105.07860, to appear in Algebra Number Theory.
[42] J.-P. Serre: Cohomologie galoisienne. Fifth edition. Lect. Notes Math. 5. Springer, Berlin, 1994.
[43] Stacks project authors: Stacks project. https://stacks.math.columbia.edu, 2018.

Mathematisches Institut, Heinrich-Heine-Universität, 40204 Düsseldorf, Germany
*Email address*: Cesar.Hilario@hhu.de

Mathematisches Institut, Heinrich-Heine-Universität, 40204 Düsseldorf, Germany
*Email address*: schroeer@math.uni-duesseldorf.de