TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 11, Pages 5025–5043
S 0002-9947(00)02572-1
Article electronically published on July 12, 2000

UNIPOTENT GROUPS ASSOCIATED TO REDUCED CURVES

DAVID PENNISTON

ABSTRACT. Let X be a curve defined over an algebraically closed field k with $\mathrm{char}(k) = p > 0$. Assume that X/k is reduced. In this paper we study the unipotent part U of the Jacobian $J_{X/k}$. In particular, we prove that if p is large in terms of the dimension of U, then U is isomorphic to a product of additive groups $\mathbb{G}_a$.

1. INTRODUCTION

Let k be an algebraically closed field with $\mathrm{char}(k) = p \geq 0$. Let X be a proper, reduced, connected, possibly singular curve over k. Write $J_{X/k}$ for the Jacobian of X. By Chevalley's Theorem, $J_{X/k}$ contains a smooth connected linear subgroup L such that its quotient by L is an abelian variety, which we denote by B. Since k is algebraically closed, we can factor L as $T \times U$, where T is a torus and U is unipotent. So the structure of $J_{X/k}$ can be summarized by the following exact sequence of smooth connected commutative group schemes over k:

$$0 \to U \times T \to J_{X/k} \to B \to 0.$$

Note that if X is smooth, then $U = T = 0$. We call U the *unipotent part* of $J_{X/k}$, and this is our object of study.

If k has characteristic zero, it is known that U is isomorphic to $\mathbb{G}_a \times \cdots \times \mathbb{G}_a$ (see [Ser], Ch. VII, no. 7, Corollaire to Proposition 8). In this case we will say that U is *split*. However, it can happen that U is not split when k has positive characteristic. Assume that $\mathrm{char}(k) = p > 0$ from now on. We say that $m \in \mathbb{N}$ *kills* a group G if $mx = 1_G$ for every $x \in G$, and that m kills a group scheme G if the multiplication-by-m morphism on G is constant. We call the smallest such m the *exponent* of G. Since U is unipotent, it is a successive extension of additive groups of type $\mathbb{G}_a$, so U has exponent a positive power of p less than or equal to $p^{\dim(U)}$.

As an example of a U that is not split, suppose that X has one singular point P, and that at P, X is isomorphic to the plane curve $y^2 = x^5$ at $(0,0)$. Then as a set, $U(k)$ is in bijection with $k \times k$, but the group law is not componentwise addition. It is given by

$$(a,b) + (c,d) = (a + c, b + d - ac(a + c)).$$

Under this group law, $(0,0)$ is the identity, and if $\mathrm{char}(k) = 3$, we find that $3(1,0) = (0,1) \neq (0,0)$. Therefore 3 does not kill $U(k)$, and it follows that $U \ncong \mathbb{G}_a \times \mathbb{G}_a$ when $\mathrm{char}(k) = 3$. The group U in this case is an example of a *Witt group* (the

Received by the editors September 13, 1998 and, in revised form, March 17, 1999.
1991 *Mathematics Subject Classification.* Primary 14H40; Secondary 14L17, 14H20.

Witt group of dimension m over a field of characteristic p is a unipotent group whose exponent is p^m).

Although U may not be split, we expect that U should be split "for p large." We prove in section 2 the following result.

Theorem 2.1. *Let X/k be a proper, reduced, connected curve. Denote by U the unipotent part of $J_{X/k}$. If $p^e \geq 2\dim(U)$, then p^e kills U.*

If p kills U, it is known that U is split (see [Ser], Ch. VII, no. 11, Proposition 11). Hence Theorem 2.1 shows that if X is reduced and $p \geq 2\dim(U)$, then U is split.

As an application of Theorem 2.1, consider the following situation. Let K be a field complete with respect to a discrete valuation v, with $\mathrm{char}(K) = 0$ and residue field k. If Z/K is a smooth, proper, geometrically connected curve, then determining the structure of the group of K-rational torsion points on the Jacobian of Z is in general a difficult problem. In the case where the Jacobian of Z has purely additive reduction, Lenstra and Oort [L-O] first proved results putting restrictions on what the K-rational prime-to-p torsion can be, and later Lorenzini [Lor2] and Edixhoven [Edi] fully settled this question. As for the K-rational p-torsion in this situation, we prove in section 7 the following result.

Theorem 7.1. *Let Z/K be a smooth, proper, geometrically connected curve of genus g with $Z(K) \neq \emptyset$. Denote by A/K the Jacobian of Z. Let $\mathcal{Z}/\mathcal{O}_K$ be a regular model of Z, with special fiber $\mathcal{Z}_k$. Suppose that $\mathcal{Z}_k$ is reduced and $v(p) < p-1$. Further suppose that the unipotent part U of $J_{\mathcal{Z}_k/k}$ has dimension g. If $p > 2g+1$, then $A(K)$ has no element of order p^2.*

As we saw above, U and T are nontrivial only if X is not smooth. Indeed, we may analyze U in terms of the singularities of X. Since X is reduced, it has finitely many singular points, and so the analysis of U is completely a local matter. In particular, the group $U(k)$ is isomorphic to a direct sum of groups

$$\bigoplus_{\substack{P \in X \\ P \text{ singular}}} U_P.$$

To each point P of X, we assign in section 2 a nonnegative integer δ_P which is a measure of how singular P is ($\delta_P = 0$ if X is smooth at P). This definition of δ_P differs slightly from the usual one (see [Ser], Ch. IV, no. 2) in that it is calculated by passing to the *seminormalization* of X, rather than to its normalization. Given X/k a proper, reduced, connected curve, the seminormalization of X is defined to be the maximal curve between X and its normalization whose points are in bijection with X.

With this definition of δ_P, we have that $\sum \delta_P = \dim(U)$. We prove Theorem 2.1 by showing that, for each singular point P, p^e kills U_P when $p^e \geq 2\delta_P$. With this in mind, the following result from section 3 allows us in some cases to improve the bound given by Theorem 2.1.

Theorem 3.1. *Let X/k be a proper, reduced, connected curve. Let P be a singular point of X. Denote by n the number of branches of X intersecting at P. Suppose the maximal ideal of the local ring of X at P is minimally generated by w elements. Assume that $n \geq w$ and $\delta_P - n + w \neq 1$, and let e be a positive integer. If $p^e \geq 2\delta_P - 2(n-w)$, then p^e kills U_P.*

In cases where U is not split, it is natural to wonder if we can still say something about the structure of U. For example, we might ask whether U has a large subgroup scheme which is split. We prove in section 5 the following result in this direction. Given $\beta \in \mathbb{Q}$, we denote by $\lceil \beta \rceil$ the smallest integer greater than or equal to β, and by $\lfloor \beta \rfloor$ the largest integer less than or equal to β.

Theorem 5.3. *Let X/k be a proper, reduced, connected curve. Assume that X has at least one singular point and that the seminormalization of X is smooth. Then U contains a subgroup scheme U' such that U' is split and*

$$\dim(U') \geq \dim(U) - \lceil 2\dim(U)/p \rceil + 1.$$

With an additional assumption about the nature of the singularities of X, we prove in section 6 a result that in many cases is an improvement on Theorem 5.3, and which can be made independent of p.

2. General results

Let k be an algebraically closed field with $\mathrm{char}(k) = p > 0$. Let X be a curve over k, i.e., a scheme of dimension 1, of finite type over $\mathrm{Spec}(k)$. Assume also that X/k is proper and connected. Denote by $\mathrm{Pic}_{X/k}$ the *Picard scheme* of X. This is a smooth group scheme over k. Note that if we write $\mathrm{Pic}(X)$ for the group of isomorphism classes of invertible sheaves on X, then we have a group isomorphism $\mathrm{Pic}_{X/k}(k) \cong \mathrm{Pic}(X)$ (see [BLR], Proposition 8.1/4). Denote by $J_{X/k}$ the identity component of $\mathrm{Pic}_{X/k}$. The group scheme $J_{X/k}$ is called the Jacobian of X/k.

Now assume that X is reduced. Let $\widetilde{X}$ be the normalization of X. The canonical projection $\widetilde{X} \to X$ induces a surjection $J_{X/k} \to J_{\widetilde{X}/k}$. The kernel L of this map is a smooth connected linear algebraic group (see [BLR], Corollary 9.2/11). Since k is algebraically closed, $L = U \times T$, where U is a unipotent group and T is a torus. Moreover, since $\widetilde{X}$ is smooth and proper over k, $J_{\widetilde{X}/k}$ is an abelian variety. So we have the following exact sequence of smooth connected commutative group schemes over k:

$$0 \to U \times T \to J_{X/k} \to J_{\widetilde{X}/k} \to 0.$$

The main result of this section can be stated as follows:

Theorem 2.1. *Let X/k be a proper, reduced, connected curve. Denote by U the unipotent part of $J_{X/k}$. If $p^e \geq 2\dim(U)$, then p^e kills U.*

The group L arose as the kernel of a map which was induced from the map of curves $\widetilde{X} \to X$. We may realize U in a similar fashion as follows. Denote by $\overline{X}$ the seminormalization of X, which we recall is the largest curve between X and $\widetilde{X}$ that is homeomorphic to X (for a description of how $\overline{X}$ is constructed, see [BLR], pp. 247-8). Each singularity of $\overline{X}$ is analytically isomorphic to the crossing of the coordinate axes in $\mathbb{A}^n_k$ for some n. The projection $\widetilde{X} \to X$ factors as $\widetilde{X} \to \overline{X} \xrightarrow{h} X$, so we get surjections

$$J_{X/k} \xrightarrow{\psi} J_{\overline{X}/k} \xrightarrow{\phi} J_{\widetilde{X}/k}.$$

By [BLR], Propositions 9.2/9 and 10, the kernel of ψ is unipotent and the kernel of ϕ is a torus. Hence $U \cong \ker(\psi)$.

Denote by $\mathcal{O}$ (resp. $\bar{\mathcal{O}}$) the structure sheaf on X (resp. $\overline{X}$), and write $\mathcal{O}^*$ (resp. $\bar{\mathcal{O}}^*$) for the sheaf of units on X (resp. $\overline{X}$). Let $h_*\bar{\mathcal{O}}^*$ be the pushforward of $\bar{\mathcal{O}}^*$ on

X. Then $\mathcal{O}^*$ is a subsheaf of $h_*\bar{\mathcal{O}}^*$, and we have an exact sequence of sheaves of groups on X:

$$1 \to \mathcal{O}^* \to h_*\bar{\mathcal{O}}^* \to \mathcal{Q} \to 1,$$

where we have written $\mathcal{Q}$ for the quotient sheaf $h_*\bar{\mathcal{O}}^*/\mathcal{O}^*$. Then associated to this short exact sequence, we have a long exact sequence of cohomology groups

$$1 \to H^0(X, \mathcal{O}^*) \to H^0(X, h_*\bar{\mathcal{O}}^*) \to H^0(X, \mathcal{Q}) \to H^1(X, \mathcal{O}^*)$$

$$\to H^1(X, h_*\bar{\mathcal{O}}^*) \to H^1(X, \mathcal{Q}) \to \cdots .$$

Since X and $\overline{X}$ are proper, reduced and connected curves over k, we have that

$$H^0(X, \mathcal{O}^*) = \Gamma(X, \mathcal{O}^*) = k^* \quad \text{and} \quad H^0(X, h_*\bar{\mathcal{O}}^*) = \Gamma(X, h_*\bar{\mathcal{O}}^*) = \Gamma(\overline{X}, \bar{\mathcal{O}}^*) = k^*.$$

Moreover, the sheaf $\mathcal{Q}$ is concentrated at the finitely many singular points of X. Hence $H^1(X, \mathcal{Q})$ is trivial. Thus we obtain the short exact sequence

$$1 \to H^0(X, \mathcal{Q}) \to H^1(X, \mathcal{O}^*) \to H^1(X, h_*\bar{\mathcal{O}}^*) \to 1.$$

Now, $H^1(X, \mathcal{O}^*) \cong \mathrm{Pic}(X)$ and $H^1(X, h_*\bar{\mathcal{O}}^*) \cong H^1(\overline{X}, \bar{\mathcal{O}}^*) \cong \mathrm{Pic}(\overline{X})$ (note that for this last isomorphism we use that X and $\overline{X}$ are homeomorphic). Moreover, the map $H^1(X, \mathcal{O}^*) \to H^1(X, h_*\bar{\mathcal{O}}^*)$ induces the natural map $\mathrm{Pic}(X) \to \mathrm{Pic}(\overline{X})$. Hence we have a group isomorphism $U(k) \cong H^0(X, \mathcal{Q})$. Since $\mathcal{Q}$ is concentrated at the finitely many singular points of X,

$$U(k) \cong H^0(X, \mathcal{Q}) = \Gamma(X, \mathcal{Q}) = \bigoplus_{\substack{P \in X \\ P \text{ singular}}} \mathcal{Q}_P = \bigoplus_{\substack{P \in X \\ P \text{ singular}}} (h_*\bar{\mathcal{O}}^*)_P/(\mathcal{O}^*)_P.$$

We now have an expression for the group of closed points of U. Indeed, if we write $U_P := (h_*\bar{\mathcal{O}}^*)_P/(\mathcal{O}^*)_P$, then we have $U(k) \cong \bigoplus U_P$. Let us now turn our attention to calculating the dimension of U. To do this, consider the exact sequence of sheaves on X:

$$0 \to \mathcal{O} \to h_*\bar{\mathcal{O}} \to \mathcal{C} \to 0,$$

where we denote by $\mathcal{C}$ the quotient $h_*\bar{\mathcal{O}}/\mathcal{O}$. Just as in the case of the sheaves of units, we obtain a short exact sequence

$$0 \to H^0(X, \mathcal{C}) \to H^1(X, \mathcal{O}) \to H^1(X, h_*\bar{\mathcal{O}}) \to 0. \tag{1}$$

Since $\mathcal{C}$ is concentrated at the finitely many singular points of X, we have

$$H^0(X, \mathcal{C}) = \Gamma(X, \mathcal{C}) = \bigoplus_{\substack{P \in X \\ P \text{ singular}}} \mathcal{C}_P = \bigoplus_{\substack{P \in X \\ P \text{ singular}}} (h_*\bar{\mathcal{O}})_P/\mathcal{O}_P. \tag{2}$$

For each $P \in X$, write $\delta_P := \dim_k((h_*\bar{\mathcal{O}})_P/\mathcal{O}_P)$ (so $\delta_P = 0$ if P is a nonsingular point of X). Since $J_{X/k}$ and $J_{\overline{X}/k}$ are smooth over k, by [BLR], Theorem 8.4/1, we have that $\dim J_{X/k} = \dim_k H^1(X, \mathcal{O})$ and

$$\dim J_{\overline{X}/k} = \dim_k H^1(\overline{X}, \bar{\mathcal{O}}) = \dim_k H^1(X, h_*\bar{\mathcal{O}}).$$

Then by (1) and (2) we have

$$\dim(U) = \dim J_{X/k} - \dim J_{\overline{X}/k} = \dim_k H^0(X, \mathcal{C}) = \sum_{P \in X} \delta_P. \tag{3}$$

We now have expressions for $\dim(U)$ and $U(k)$. Notice that both are completely local in nature. To facilitate computations involving them, we now pass to completions. To ease notation, given $P \in X$, write $\mathcal{R}_P := (h_*\bar{\mathcal{O}})_P$. Then $\mathcal{R}_P$ and $\mathcal{O}_P$ are dimension one local k-algebras; denote their maximal ideals by N_P and M_P respectively.

Write C_P for the conductor ideal of $\mathcal{O}_P$ in $\mathcal{R}_P$. By the construction of $\overline{X}$, C_P is nonzero. It follows that $N_P^\ell \subset M_P$ for some ℓ. Write $\hat{\mathcal{R}}_P$ and $\hat{\mathcal{O}}_P$ respectively for the completions of $\mathcal{R}_P$ and $\mathcal{O}_P$ at their maximal ideals. Then $\hat{\mathcal{R}}_P$ and $\hat{\mathcal{O}}_P$ are dimension one local k-algebras. Denote their maximal ideals by $\hat{N}_P$ and $\hat{M}_P$ respectively. Then $\hat{\mathcal{R}}_P = k \oplus \hat{N}_P$ as k-vector spaces, and as sets, $\hat{\mathcal{R}}_P^* = k^* + \hat{N}_P$. Analogous statements hold for $\hat{\mathcal{O}}_P$. Furthermore, we have a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_P & \longrightarrow & \hat{\mathcal{O}}_P \\ \downarrow & & \downarrow \\ \mathcal{R}_P & \longrightarrow & \hat{\mathcal{R}}_P \end{array}$$

of inclusions of k-algebras. The fact that $N_P^\ell \subset M_P$ for some ℓ implies that $\mathcal{R}_P/\mathcal{O}_P$ and $\hat{\mathcal{R}}_P/\hat{\mathcal{O}}_P$ are isomorphic as k-vector spaces (i.e., that δ_P is invariant under completion), and that $\mathcal{R}_P^*/\mathcal{O}_P^*$ and $\hat{\mathcal{R}}_P^*/\hat{\mathcal{O}}_P^*$ are isomorphic as abelian groups. Therefore

$$\delta_P = \dim_k(\hat{\mathcal{R}}_P/\hat{\mathcal{O}}_P) = \dim_k(\hat{N}_P/\hat{M}_P) \qquad \text{and} \qquad U_P \cong \hat{\mathcal{R}}_P^*/\hat{\mathcal{O}}_P^*.$$

Recall that, given $P \in X$, $\overline{X}$ is analytically isomorphic at P to the crossing of the coordinate axes in $\mathbb{A}_k^{n_P}$ for some $n_P \geq 1$ (since X and $\overline{X}$ are in bijection, let us identify them as sets). Therefore we may write

$$\hat{\mathcal{R}}_P = k[[x_1, \ldots, x_{n_P}]]/(\ldots, x_i x_j, \ldots),$$

where $i \neq j$ (see [Bom]). Note that, geometrically, n_P is the number of branches of X intersecting at P. Moreover, $\hat{N}_P = (x_1, \ldots, x_{n_P})$. Let us now begin our study of the exponent of U.

Lemma 2.2. *p^e kills $U_P \iff x_i^{p^e} \in \hat{M}_P$ for all $1 \leq i \leq n_P$.*

Proof. Assume that $x_i^{p^e} \in \hat{M}_P$ for all $1 \leq i \leq n_P$. Recall that $U_P \cong \hat{\mathcal{R}}_P^*/\hat{\mathcal{O}}_P^*$ as groups, and that $\hat{\mathcal{R}}_P^* = k^* + \hat{N}_P$ and $\hat{\mathcal{O}}_P^* = k^* + \hat{M}_P$ as sets. Since $\hat{N}_P = (x_1, \ldots, x_{n_P})$ and $x_i x_j = 0$ for $i \neq j$, we can write any element x of $\hat{\mathcal{R}}_P^*$ in the form

$$x = \gamma + \sum_{i=1}^{n_P} \left(\sum_{j=1}^{\infty} \gamma_{i,j} x_i^j \right)$$

with $\gamma \in k^*$, $\gamma_{i,j} \in k$. Then, since k has characteristic p,

$$x^{p^e} = \gamma^{p^e} + \sum_{i=1}^{n_P} \left[\sum_{j=1}^{\infty} \gamma_{i,j}^{p^e} x_i^{p^e \cdot j} \right]. \tag{4}$$

To prove that p^e kills U_P, we need to show that $x^{p^e} \in \hat{\mathcal{O}}_P^*$. To see this, we note that for a fixed i, $x_i^{p^e \cdot j} \in \hat{M}_P^j$ for all $j \geq 1$. Hence, by the completeness of $\hat{\mathcal{O}}_P$, the infinite sum in brackets in (4) is an element of $\hat{M}_P$. It follows that $x^{p^e} \in \hat{\mathcal{O}}_P^*$.

Now suppose that $x_i^{p^e} \notin \hat{M}_P$ for some i. Then $1 + x_i \in \hat{\mathcal{R}}_P^*$, and $(1 + x_i)^{p^e} = 1 + x_i^{p^e} \notin \hat{\mathcal{O}}_P^*$. Thus p^e does not kill U_P. □

In order to make the connection between the exponent of U and the dimension of U, we now rephrase the problem of bounding the exponent of U_P into the language of *semigroups*. A semigroup of the positive integers $\mathbb{N}$ is a subset of $\mathbb{N}$ that is closed under addition. For each $1 \leq i \leq n_P$, define

$$S_{P,i} := \{m \in \mathbb{N} \mid \text{ there is a power series } \Sigma_{j \geq m} \gamma_j x_i^j \text{ in } \hat{M}_P \text{ with } \gamma_j \in k, \gamma_m \neq 0\}.$$

Also, define $T_{P,i} := (\mathbb{N} \setminus S_{P,i})$. Since $\hat{M}_P$ is closed under multiplication, we have

Lemma 2.3. *$S_{P,i}$ is a semigroup of $\mathbb{N}$ for all $1 \leq i \leq n_P$.*

The next lemma, along with Lemma 2.2, allows us to translate the question of bounding the exponent of U_P into a question regarding semigroups.

Lemma 2.4. *Suppose that $\{m \in \mathbb{N} \mid m \geq a\} \subset S_{P,i}$ for all $1 \leq i \leq n_P$. Then $x_i^a \in \hat{M}_P$ for all $1 \leq i \leq n_P$.*

Proof. By symmetry we need only show that $x_1^a \in \hat{M}_P$. By assumption, for each $m \geq a$, we have an element of $\hat{M}_P$ of the form

$$\epsilon_m = x_1^m + \sum_{j=m+1}^{\infty} \gamma_{m,j} x_1^j,$$

where $\gamma_{m,j} \in k$. Then there exist $\kappa_m \in k$ such that $x_1^a = \epsilon_a - \sum_{m=a+1}^{\infty} \kappa_m \epsilon_m$. □

The next lemma will allow us to relate $\dim(U)$ to the semigroups $S_{P,i}$.

Lemma 2.5. *For every $1 \leq i \leq n_P$, the set $\{x_i^j \mid j \in T_{P,i}\}$ is k-linearly independent in $\hat{N}_P/\hat{M}_P$.*

Proof. Suppose some k-linear combination $\sum_{j \in T_{P,i}} \gamma_j x_i^j$ were an element of $\hat{M}_P$. By the definition of $T_{P,i}$, $\hat{M}_P$ contains no power series in x_i whose lowest degree term has degree an element of $T_{P,i}$. It follows that $\gamma_j = 0$ for all $j \in T_{P,i}$. □

Corollary 2.6. *For every $1 \leq i \leq n_P$, $\#T_{P,i} \leq \delta_P$.*

Proof. Follows directly from Lemma 2.5, since $\delta_P = \dim_k(\hat{N}_P/\hat{M}_P)$. □

Write $t_{P,i} := \#T_{P,i}$.

Lemma 2.7 ([N-W], Theorem 1)**.** *Let S be a semigroup of $\mathbb{N}$ such that $\mathbb{N} \setminus S$ is finite. Write $t = \#(\mathbb{N} \setminus S)$. Then S contains every integer greater than or equal to $2t$.*

Proof. For any $m \geq 2t$, S contains one of the sets $\{m\}, \{1, m-1\}, \{2, m-2\}, \ldots, \{\lfloor \frac{m}{2} \rfloor, \lceil \frac{m}{2} \rceil\}$. □

Putting all this together, we have

Lemma 2.8. *If $p^e \geq 2\delta_P$, then p^e kills U_P.*

Proof. Since $t_{P,i} = \#(\mathbb{N} \setminus S_{P,i})$, Corollary 2.6 and Lemma 2.7 imply that $\{m \in \mathbb{N} \mid m \geq 2\delta_P\} \subset S_{P,i}$ for all $1 \leq i \leq n_P$. Therefore $\{m \in \mathbb{N} \mid m \geq p^e\} \subset S_{P,i}$ for all i. By Lemma 2.4, $x_i^{p^e} \in \hat{M}_P$ for all i, and so Lemma 2.2 tells us that p^e kills U_P. □

We can now prove a result relating the exponent of U to the δ_P's.

Theorem 2.9. *Let X/k be a proper, reduced, connected curve. Denote by U the unipotent part of $J_{X/k}$. Let $\delta = \max_{P\in X} \delta_P$. If $p^e \geq 2\delta$, then p^e kills U.*

Proof. Since $U(k) \cong \bigoplus U_P$ as groups, this follows directly from Lemma 2.8. □

Now Theorem 2.1 follows from Theorem 2.9 because, by (3), $\dim(U) = \sum \delta_P \geq \delta$.

The most important instance of Theorem 2.1 is the case where $e = 1$, because it then becomes a structure theorem on U. We say that U is *split* if $U \cong \mathbb{G}_a \times \cdots \times \mathbb{G}_a$.

Corollary 2.10. *If $p \geq 2\dim(U)$, then U is split.*

Proof. By Theorem 2.1, p kills U. Then the result follows from [Ser], Ch. VII, no. 11, Proposition 11. □

Example 2.11. Let b and c be integers greater than one with $(b, c) = 1$, and suppose that X is a curve which, in a neighborhood of P, is isomorphic to the plane curve $y^b = x^c$ around $(0, 0)$. Since the affine curve $y^b = x^c$ is parametrized by $\mathbb{A}^1_k$ via $r \mapsto (r^b, r^c)$, we have that

$$\mathcal{O}_P = \big(k[x, y]/(y^b - x^c)\big)_{(x,y)} \quad \text{and} \quad \mathcal{R}_P = k[r]_{(r)}.$$

Hence

$$\hat{\mathcal{O}}_P = k[[r^b, r^c]] \subset k[[r]] = \hat{\mathcal{R}}_P$$

(note that we are writing r for x_1). Then $S_{P,1}$ is the semigroup of $\mathbb{N}$ generated by b and c, so $(b - 1)(c - 1) - 1$ is the largest integer not contained in $S_{P,1}$, and $\delta_P = \#(\mathbb{N} \setminus S_{P,1}) = (b - 1)(c - 1)/2$ (postage stamp problem).

Now suppose that p is odd, $e > 0$, and let $b = 2$, $c = p^e$ in the above situation. Furthermore, suppose that P is the only singularity of X. Then $r^{p^e} \in \hat{M}_P$ and $r^{p^{e-1}} \notin \hat{M}_P$. By Lemma 2.2, U_P, and therefore U, has exponent p^e, while $2\dim(U) = 2\delta_P = p^e - 1$. This shows that Theorem 2.1 is sharp.

3. An improvement on the 2δ bound

We assume in this section that X is a proper, reduced, connected curve over k. We retain the notation established in section 2. Our proof of Theorem 2.1 was based on a local result (Lemma 2.8) which says that, for each $P \in X$, p^e kills U_P when $p^e \geq 2\delta_P$. By Lemmas 2.2 and 2.4, we reduced Lemma 2.8 to showing that $\{m \in \mathbb{N} \mid m \geq 2\delta_P\} \subset S_{P,i}$ for all $1 \leq i \leq n_P$. We will show in this section, under certain conditions on P, that $\{m \in \mathbb{N} \mid m \geq a\} \subset S_{P,i}$ holds (for all i) for some a which is less than $2\delta_P$. This allows us to get a better bound on the exponent of U_P, and thus a potentially better bound on the exponent of U.

Fix a point P of X. Recall that $\hat{\mathcal{R}}_P \cong k[[x_1, \ldots, x_{n_P}]]/(\ldots, x_i x_j, \ldots)$, where $i \neq j$, n_P is the number of branches of X meeting at P, and $\hat{N}_P = (x_1, \ldots, x_{n_P})$. The maximal ideal M_P of the local ring $\mathcal{O}_P$ is finitely generated; say that it is minimally generated by w_P elements (so $w_P = 1$ if and only if X is smooth at P). If we denote by $\alpha_1, \ldots, \alpha_{w_P}$ the images under the inclusion $\mathcal{O}_P \hookrightarrow \hat{\mathcal{O}}_P$ of a minimal set of generators of M_P, then $\hat{\mathcal{O}}_P$ is generated as a power series ring over k by $\alpha_1, \ldots, \alpha_{w_P}$. That is, $\hat{\mathcal{O}}_P = k[[\alpha_1, \ldots, \alpha_{w_P}]]$, and $\hat{M}_P = (\alpha_1, \ldots, \alpha_{w_P})$. For the rest of this section, we will think of P as being fixed, so let us suppress the subscript P on n and w, and simply write $n = n_P$ and $w = w_P$. The main result of this section is

Theorem 3.1. *Suppose X is a proper, reduced, connected curve over k. Let P be a point of X. Denote by n the number of branches of X intersecting at P. Suppose that the maximal ideal of the local ring of X at P is minimally generated by w elements. Assume that $n \geq w$ and $\delta_P - n + w \neq 1$, and let e be a positive integer. If $p^e \geq 2\delta_P - 2(n-w)$, then p^e kills U_P.*

Remark 3.2. The integer $\delta_P - n + w$ is always nonnegative. To see this, first note that since $\hat{M}_P^2$ is generated by all the elements of the form $\alpha_i\alpha_j$ $(1 \leq i, j \leq w)$, we have

$$w = \dim_k(\hat{M}_P/\hat{M}_P^2).$$

Similarly, since $\hat{N}_P^2 = (x_1^2, \ldots, x_n^2)$, we have

$$n = \dim_k(\hat{N}_P/\hat{N}_P^2).$$

Now, the inclusion $\hat{M}_P \hookrightarrow \hat{N}_P$ induces a k-linear map $\pi\colon \hat{M}_P/\hat{M}_P^2 \to \hat{N}_P/\hat{N}_P^2$. And the identity map on $\hat{N}_P$ induces a surjection $\hat{N}_P/\hat{M}_P \to \operatorname{coker}(\pi)$. Therefore

$$\begin{aligned}\delta_P = \dim_k(\hat{N}_P/\hat{M}_P) &\geq \dim_k \operatorname{coker}(\pi) \\ &\geq \dim_k(\hat{N}_P/\hat{N}_P^2) - \dim_k(\hat{M}_P/\hat{M}_P^2) = n - w.\end{aligned}$$

Before we prove Theorem 3.1, we begin with two lemmas that will be useful in its proof.

Recall that any element x of $\hat{\mathcal{R}}_P$ can be written in the form

$$x = \gamma + \sum_{j=1}^{\infty}\sum_{i=1}^{n} \gamma_{i,j} x_i^j,$$

where γ and the $\gamma_{i,j}$ are in k. Also note that $x \in \hat{N}_P$ if and only if $\gamma = 0$. We call $\sum_{i=1}^n \gamma_{i,1}x_i$ the *linear part* of x.

Lemma 3.3. *Let $A_1, \ldots, A_w$ be the linear parts of $\alpha_1, \ldots, \alpha_w$ respectively. Then the linear part of any element of $\hat{M}_P$ is a k-linear combination of $A_1, \ldots, A_w$.*

Proof. The only monomials $\alpha_1^{i_1} \cdots \alpha_w^{i_w}$ that can have a nonzero linear part are $\alpha_1, \ldots, \alpha_w$. □

Lemma 3.4. *Suppose there exist w elements $\beta_1, \ldots, \beta_w$ of $\hat{M}_P$ whose linear parts are k-linearly independent. Then $k[[\beta_1, \ldots, \beta_w]] = k[[\alpha_1, \ldots, \alpha_w]] = \hat{\mathcal{O}}_P$.*

Proof. Write $B_1, \ldots, B_w$ for the linear parts of $\beta_1, \ldots, \beta_w$ respectively. Then the k-span of $\{B_1, \ldots, B_w\}$ and the k-span of $\{A_1, \ldots, A_w\}$ are equal by Lemma 3.3. Therefore we can write

$$\begin{pmatrix} A_1 \\ \vdots \\ A_w \end{pmatrix} = C \cdot \begin{pmatrix} B_1 \\ \vdots \\ B_w \end{pmatrix},$$

where $C = (c_{ij}) \in GL_w(k)$. If we define β_i', $1 \leq i \leq w$, by

$$\beta_i' = \sum_{j=1}^{w} c_{ij}\beta_j,$$

it follows that $k[[\beta'_1, \ldots, \beta'_w]] = k[[\beta_1, \ldots, \beta_w]]$. Now, since β'_i is an element of $\hat{M}_P = (\alpha_1, \ldots, \alpha_w)$ and has linear part equal to A_i, it must have the form $\alpha_i + \nu_i$, where $\nu_i \in \hat{M}_P^2$. Since

$$k[[\alpha_1 + \nu_1, \ldots, \alpha_w + \nu_w]] = k[[\alpha_1, \ldots, \alpha_w]],$$

the lemma is proven. □

Now let us prove Theorem 3.1. Recall that we already have proven the result is true for $n = w$ (Lemma 2.8), so assume from now on that $n \geq w + 1$. If $\delta_P - n + w = 0$, then by Lemmas 2.2 and 2.4 it certainly suffices to show that

$$\{m \in \mathbb{N} \mid m \geq 2\} \subset S_{P,i}$$

for all $1 \leq i \leq n$. Similarly, if $\delta_P - n + w \geq 2$, then it suffices to show that $\{m \in \mathbb{N} \mid m \geq 2\delta_P - 2(n - w)\} \subset S_{P,i}$ for all $1 \leq i \leq n$. By symmetry, we need only prove these containments for $i = 1$.

We first claim that $t_{P,1} \leq \delta_P - n + (w + 1)$. By Corollary 2.6 we know that $t_{P,1} \leq \delta_P$, so our claim is certainly true if $n = w + 1$. Assume now that $n \geq w + 2$. We argue by contradiction. Suppose that $t_{P,1} > \delta_P - n + (w+1)$. Then $t_{P,1} = \delta_P - d$ for some $0 \leq d \leq n - (w + 2)$. Hence the set

$$\{x_2, \ldots, x_{d+2}\} \cup \{x_1^m \mid m \in T_{P,1}\}$$

has $\delta_P + 1$ elements, and therefore is a k-linearly dependent set when thought of in $\hat{N}_P/\hat{M}_P$. So we can find a nontrivial k-linear combination

$$\sum_{i=2}^{d+2} \gamma_{2,i} x_i + \sum_{j \in T_{P,1}} \mu_{2,j} x_1^j$$

in $\hat{M}_P$, and by Lemma 2.5, not all the $\gamma_{2,i}$ are zero. Without loss, assume $\gamma_{2,2} \neq 0$. In exactly the same way, we find elements of $\hat{M}_P$ of the form

$$\sum_{i=3}^{d+3} \gamma_{3,i} x_i + \sum_{j \in T_{P,1}} \mu_{3,j} x_1^j \quad , \quad \cdots \quad , \quad \sum_{i=w+2}^{d+w+2} \gamma_{w+2,i} x_i + \sum_{j \in T_{P,1}} \mu_{w+2,j} x_1^j,$$

with $\gamma_{3,3}, \ldots, \gamma_{w+2,w+2} \neq 0$. By the construction of these $w + 1$ elements, their linear parts are k-linearly independent. This contradicts Lemma 3.3, and our claim is proved.

By Lemma 2.7, then, $\{m \in \mathbb{N} \mid m \geq 2\delta_P - 2n + 2(w + 1)\} \subset S_{P,1}$. As we have seen, this concludes the proof of Theorem 3.1 in the case that $\delta_P - n + w = 0$. Assume from now on that $\delta_P - n + w \geq 2$. To finish the proof of Theorem 3.1, we just need to show that $2\delta_P - 2n + 2w$ and $2\delta_P - 2n + 2w + 1$ are elements of $S_{P,1}$. We now show that the latter is an element of $S_{P,1}$; the proof for the former is analogous.

We again argue by contradiction. Suppose that $2\delta_P - 2n + 2w + 1 \notin S_{P,1}$. Then $t_{P,1} \geq \delta_P - n + w + 1$ by Lemma 2.7, and so $t_{P,1} = \delta_P - n + w + 1$ by the above. Consider the set $\{x_2, \ldots, x_{n-w+1}\} \cup \{x_1^i \mid i \in T_{P,1}\}$. Since it has $n - w + t_{P,1} = \delta_P + 1$ elements, this set is k-linearly dependent when thought of in $\hat{N}_P/\hat{M}_P$. So we can find a nontrivial k-linear combination $\sum_{i=2}^{n-w+1} \gamma_{2,i} x_i + \sum_{j \in T_{P,1}} \mu_{2,j} x_1^j$ in $\hat{M}_P$; call this element ϵ_2. By Lemma 2.5, not all the $\gamma_{2,i}$ are zero. Assume without loss that

$\gamma_{2,2} \neq 0$. In exactly the same way we find elements $\epsilon_3, \ldots, \epsilon_{w+1}$ of $\hat{M}_P$ of the form

$$\sum_{i=3}^{n-w+2} \gamma_{3,i}x_i + \sum_{j\in T_{P,1}} \mu_{3,j}x_1^j \quad , \quad \cdots \quad , \quad \sum_{i=w+1}^{n} \gamma_{w+1,i}x_i + \sum_{j\in T_{P,1}} \mu_{w+1,j}x_1^j$$

with $\gamma_{3,3}, \ldots, \gamma_{w+1,w+1} \neq 0$. Note that, by their construction, the linear parts of $\epsilon_2, \ldots, \epsilon_{w+1}$ are k-linearly independent. By Lemma 3.4, we conclude that $k[[\epsilon_2, \ldots, \epsilon_{w+1}]] = \hat{\mathcal{O}}_P$. Notice that we cannot have $\mu_{i,j} = 0$ for all $2 \leq i \leq w+1$ and all $j \in T_{P,1}$, for if this were the case, then none of the ϵ_i (the generators of $\hat{\mathcal{O}}_P$) would involve any power of x_1. This would imply that $T_{P,1} = \mathbb{N}$, which contradicts Corollary 2.6. Let a be the least integer j such that $\mu_{i,j} \neq 0$ for some $2 \leq i \leq w+1$. Assume without loss that $\mu_{2,a} \neq 0$.

Claim 3.5. If $m \in S_{P,1}$, then $m + a \in S_{P,1}$. To see this, note that $m \in S_{P,1}$ implies that there is an element of $\hat{M}_P$ of the form $x_1^m + \sum_{j=m+1}^{\infty} \rho_j x_1^j$, where $\rho_j \in k$. Since $x_i x_j = 0$ when $i \neq j$, multiplying this element by ϵ_2 gives a power series in x_1 with lowest degree term $\mu_{2,a}x_1^{m+a}$, so $m + a \in S_{P,1}$.

We assert that $a > 1$. For if $a = 1$, then since $2\delta_P - 2n + 2w + 1 \notin S_{P,1}$, Claim 3.5 shows that $\{1, 2, \ldots, 2\delta_P - 2n + 2w + 1\} \subset T_{P,1}$. This implies that $t_{P,1} \geq 2\delta_P - 2n + 2w + 1 > \delta_P - n + w + 1$, a contradiction.

Next we assert that $1, 2, \ldots, 2a-1 \in T_{P,1}$. To see this, recall that $k[[\epsilon_2, \ldots, \epsilon_{w+1}]] = \hat{\mathcal{O}}_P$ and that the linear parts of the ϵ_i are k-linearly independent and do not involve x_1 (since $a > 1$). Since the only monomials $\epsilon_2^{i_2} \cdots \epsilon_{w+1}^{i_{w+1}}$ that could involve powers of x_1 less than $2a$ are $\epsilon_2, \ldots, \epsilon_{w+1}$, the assertion follows. Hence $2a - 1 \leq t_{P,1} = \delta_P - n + w + 1$, and since $\delta_P - n + w \geq 2$, this implies that $a \leq \delta_P - n + w$.

Now consider the two-element sets

$$\{1, 2\delta_P - 2n + 2w\}, \{2, 2\delta_P - 2n + 2w - 1\}, \ldots, \{\delta_P - n + w, \delta_P - n + w + 1\}.$$

Since the elements of each set add up to $2\delta_P - 2n + 2w + 1$, and $2\delta_P - 2n + 2w + 1$ is not in the semigroup $S_{P,1}$, it follows that $S_{P,1}$ contains none of these sets; i.e., $T_{P,1}$ contains at least one element of each of these $\delta_P - n + w$ sets. Also, $2\delta_P - 2n + 2w + 1 \in T_{P,1}$, and is contained in none of these sets. Since $t_{P,1} = \delta_P - n + w + 1$, we conclude that $T_{P,1}$ contains exactly one element from each of these two-element sets. Since $a \in T_{P,1}$ and $a \leq \delta_P - n + w$, it follows that $2\delta_P - 2n + 2w + 1 - a \in S_{P,1}$. But then Claim 3.5 implies that $2\delta_P - 2n + 2w + 1 \in S_{P,1}$, a contradiction. Thus $2\delta_P - 2n + 2w + 1 \in S_{P,1}$.

As we mentioned above, the proof that $2\delta_P - 2n + 2w \in S_{P,1}$ is entirely similar to that for $2\delta_P - 2n + 2w + 1$, except that it involves considering the two-element sets

$$\{1, 2\delta_P - 2n + 2w - 1\}, \{2, 2\delta_P - 2n + 2w - 2\}, \ldots, \{\delta_P - n + w - 1, \delta_P - n + w + 1\}.$$

This completes the proof of Theorem 3.1.

Remark 3.6. All of the proof of Theorem 3.1 in the case that $\delta_P - n + w \geq 2$ remains valid when $\delta_P - n + w = 1$, except for the proof that $2\delta_P - 2n + 2w \in S_{P,1}$. This is because the two-element sets involved in that part of the proof are nonexistent if $\delta_P - n + w = 1$. Thus we have the following result in the case that $\delta_P - n + w = 1$: if $p^e \geq 3$, then p^e kills U_P.

4. The case of planar singularities

We assume in this section that X is a proper, reduced, connected curve over k, and retain the notation established in the preceding sections. We say that a singular point P of X is *planar* if $w_P = 2$, i.e., if $\hat{\mathcal{O}}_P = k[[\alpha, \beta]]$ for some $\alpha, \beta \in \hat{N}_P$. For example, all the singularities of X will be planar if X lies on a regular surface. In this situation, as a special case of Theorem 3.1, we get

Theorem 4.1. *Suppose X is a proper, reduced, connected curve over k. Let P be a planar singularity of X, and denote by n_P the number of branches of X intersecting at P. Suppose that $n_P \geq 2$, and let e be a positive integer. If $p^e \geq 2\delta_P - 2(n_P - 2)$, then p^e kills U_P, except in the case that $n_P = 4$ and $\delta_P = 3$, or in the case that $n_P = 3$ and $\delta_P = 2$.*

In light of Theorem 3.1, to prove Theorem 4.1 we just need to find a comprehensive list of the cases in which $\delta_P = n_P - 1$. Fix a planar singular point P of X. Recall that $\hat{\mathcal{R}}_P \cong k[[x_1, \dots, x_{n_P}]]/(\dots, x_i x_j, \dots)$, where n_P is the number of branches of X intersecting at P, and $i \neq j$.

Lemma 4.2. $\delta_P \geq (n_P - 1)(n_P - 2)/2$.

Proof. The result is clearly true if $n_P = 1$ or $n_P = 2$, so assume from now on that $n_P \geq 3$. Denote by S the k-vector space $\hat{N}_P/\hat{N}_P^{n_P - 1}$. Since $\hat{N}_P^a = (x_1^a, \dots, x_{n_P}^a)$, it follows that S has as a k-basis the classes of

$$\{x_1, \dots, x_{n_P}, x_1^2, \dots, x_{n_P}^2, \dots, x_1^{n_P - 2}, \dots, x_{n_P}^{n_P - 2}\},$$

and so $\dim_k(S) = n_P(n_P - 2)$. Define a map of k-vector spaces $\pi\colon \hat{M}_P \to S$ to be the composition of the inclusion $\hat{M}_P \hookrightarrow \hat{N}_P$ and the quotient map $\hat{N}_P \to S$. Then we have a surjection

$$\hat{N}_P/\hat{M}_P \to S/\pi(\hat{M}_P),$$

so $\delta_P = \dim_k(\hat{\mathcal{R}}_P/\hat{\mathcal{O}}_P) = \dim_k(\hat{N}_P/\hat{M}_P) \geq \dim_k(S/\pi(\hat{M}_P))$. Let us now investigate this latter dimension. Recall that $\hat{\mathcal{O}}_P = k[[\alpha, \beta]]$ for some $\alpha, \beta \in \hat{N}_P = (x_1, \dots, x_{n_P})$. Therefore the only monomials in α and β that can have a nonzero image under π are those of the form $\alpha^i \beta^j$ with i and j nonnegative and $1 \leq i + j \leq n_P - 2$; this is because they are the only monomials in α and β that can involve powers of the x_i lower than $n_P - 1$. This list comprises $n_P(n_P - 1)/2 - 1$ elements. Thus

$$\begin{aligned} \delta_P &\geq \dim_k(S/\pi(\hat{M}_P)) = \dim_k(S) - \dim_k(\pi(\hat{M}_P)) \\ &\geq [n_P(n_P - 2)] - [n_P(n_P - 1)/2 - 1] = (n_P - 1)(n_P - 2)/2. \quad \square \end{aligned}$$

Corollary 4.3. *$\delta_P \geq n_P$ except in the following cases:*

(a) $n_P = 4, \quad \delta_P = 3,$
(b) $n_P = 3, \quad \delta_P = 2,$
(c) $n_P = 3, \quad \delta_P = 1,$
(d) $n_P = 2, \quad \delta_P = 1,$
(e) $n_P = 2, \quad \delta_P = 0,$
(f) $n_P = 1, \quad \delta_P = 0.$

Proof. First note that, by Lemma 4.2,

$$n_P > \delta_P \Rightarrow n_P > (n_P-1)(n_P-2)/2 \Rightarrow n_P^2 - 5n_P + 2 < 0$$
$$\Rightarrow (n_P - 5/2)^2 < 17/4 \Rightarrow n_P \in \{1,2,3,4\}.$$

From here we simply examine the inequality $(n_P-1)(n_P-2)/2 \leq \delta_P < n_P$ for these four values of n_P. □

To complete the proof of Theorem 4.1, note that Lemma 2.8 already gives the desired result in cases (d) and (f), so that (a) and (b) are the only two exceptional cases.

Example 4.4. Theorem 4.1 shows that when $w_P = 2$, one often has that p^e kills U_P for prime powers smaller than $2\delta_P$ when $n_P \geq 3$. This example shows that when $n_P = 2$, one cannot in general improve the $2\delta_P$ bound.

Suppose p is odd. To avoid excessive subscripts, write $\hat{\mathcal{R}}_P = k[[r,s]]/(rs)$ (so in our notation we are writing r for x_1 and s for x_2). Recalling that $\hat{\mathcal{O}}_P = k[[\alpha,\beta]]$, we have that $\hat{N}_P = (r,s)$ and $\hat{M}_P = (\alpha,\beta)$. Let $\alpha = r+s^2$, $\beta = r+s^{2a+1}$ for an integer $a \geq 2$. Notice that these elements satisfy the relation $(\beta-\alpha)(\beta^2-\alpha^{2a+1}) = 0$, since $rs = 0$, $\beta-\alpha$ is a polynomial in s and $\beta^2-\alpha^{2a+1}$ is a polynomial in r. Hence $\hat{\mathcal{O}}_P$ is the completion of the local ring of a curve at a point P, which near P is isomorphic to the intersection at the origin of the plane curves $y = x$ and $y^2 = x^{2a+1}$. We calculate

$$\beta^2 - \alpha^{2a+1} = r^2 - r^{2a+1}, \quad \alpha(\beta^2-\alpha^{2a+1}) = r^3 - r^{2a+2},$$

$$\alpha^{a+\ell}(\alpha-\beta) = s^{2a+2+2\ell} - s^{4a+1+2\ell}, \quad \alpha^\ell\beta(\alpha-\beta) = s^{2a+3+2\ell} - s^{4a+2+2\ell},$$

for every $\ell \geq 0$. So in $\hat{M}_P$ we have a power series in r beginning with r^2, as well as one beginning with r^3. Since 2 and 3 generate the semigroup $\{m \in \mathbb{N} \mid m \geq 2\}$, by the completeness of $\hat{\mathcal{O}}_P$ we have that $\{r^m \mid m \geq 2\} \subset \hat{M}_P$. By a similar argument, $\{s^m \mid m \geq 2a+2\} \subset \hat{M}_P$. Therefore the ideal I of $\hat{N}_P$ generated by r^2 and s^{2a+2} is contained in $\hat{M}_P$. Then $\delta_P = \dim_k(\hat{N}_P/\hat{M}_P) = \dim_k((\hat{N}_P/I)/(\hat{M}_P/I))$. Now, $\{r, s, s^2, \ldots, s^{2a+1}\}$ ($2a+2$ elements) is clearly a set of representatives for a k-basis of $\hat{N}_P/I$. Furthermore, $\{\alpha, \alpha^2, \ldots, \alpha^a, \beta\}$ ($a+1$ elements) is a set of representatives for a k-basis of $\hat{M}_P/I$. To see this, we simply note that these are the only monomials $\alpha^i\beta^j$ which are not contained in I, and that these elements are k-linearly independent modulo I. Therefore $\delta_P = (2a+2) - (a+1) = a+1$. So $2\delta_P = 2a+2$, and it is clear that $s^m \notin \hat{M}_P$ for all odd numbers $m \leq 2a+1$. By Lemma 2.2, if $p^e < 2a+2 = 2\delta_P$, then p^e does not kill U_P.

By Remark 3.6, we may state the following lemmas dealing with the exceptional cases of Theorem 4.1.

Lemma 4.5. *Suppose that X has a planar singularity at P with $n_P = 4$ and $\delta_P = 3$. If $p^e \geq 3$, then p^e kills U_P.*

Lemma 4.6. *Suppose that X has a planar singularity at P with $n_P = 3$ and $\delta_P = 2$. If $p^e \geq 3$, then p^e kills U_P.*

Example 4.7. The following example shows that Lemma 4.5 cannot be improved. Suppose $\mathrm{char}(k) = 2$. As in Example 4.4, we avoid excessive subscripts by writing

$$\hat{\mathcal{R}}_P = k[[r,s,t,u]]/(rs, rt, ru, st, su, tu).$$

Recalling that $\hat{\mathcal{O}}_P = k[[\alpha,\beta]]$, we have $\hat{N}_P = (r,s,t,u)$ and $\hat{M}_P = (\alpha,\beta)$. Let $\alpha = r+t+u$, $\beta = s+t+\epsilon u$, where $\epsilon \in k$, $\epsilon \neq 0,1$. Notice that α and β satisfy the relation $\alpha\beta(\beta-\epsilon\alpha)(\beta-\alpha)=0$. Hence $\hat{\mathcal{O}}_P = k[[\alpha,\beta]]$ is the completion of the local ring of a curve at a point P, which near P is isomorphic to four distinct lines in the plane passing through the origin. By a similar calculation as in Example 4.4, we find that $\delta_P = 3$.

We want to show that 2 does not kill U_P. By Lemma 2.2, we just need to show that $\hat{M}_P = (\alpha,\beta)$ does not contain all four of the elements r^2, s^2, t^2, u^2. To see this, simply note that only three monomials $\alpha^i\beta^j$ involve these elements, namely α^2,$\alpha\beta$, and β^2. Thus, Lemma 4.5 is best possible.

Example 4.8. This example shows that Lemma 4.6 cannot be improved. Suppose $\mathrm{char}(k) = 2$. As above, write $\hat{\mathcal{R}}_P = k[[r,s,t]]/(rs,rt,st)$, $\hat{\mathcal{O}}_P = k[[\alpha,\beta]] \subset \hat{\mathcal{R}}_P$. Let $\alpha = r+t$, $\beta = s+t^2$. Notice that α and β satisfy the relation $\alpha\beta(\beta-\alpha^2)=0$. We compute as in Example 4.4 that $\delta_P = 2$.

We claim that 2 does not kill U_P. By Lemma 2.2 we need only show that $\hat{M}_P$ does not contain all three of the elements r^2, s^2 and t^2. We will show that $\hat{M}_P$ does not contain r^2. Arguing by contradiction, suppose that $r^2 \in \hat{M}_P$. Then we can write $r^2 = \sum_{i,j} c_{i,j}\alpha^i\beta^j$, where $c_{i,j} \in k$, and the sum is over all pairs of nonnegative integers (i,j) with $i+j \geq 1$. Since $\alpha^2 = r^2+t^2$ is the only such monomial involving r^2, it must be that $c_{2,0} = 1$. And since $\beta = s+t^2$ is the only monomial involving s, we have that $c_{0,1} = 0$. Now, α^2 and β are the only monomials involving t^2, so it must be that $c_{2,0} = -c_{0,1}$. This is a contradiction. Thus, Lemma 4.6 is best possible.

5. The case where $\overline{X}$ is nonsingular

We suppose in this section that X is a proper, reduced, connected curve over k. Recall that we denote by $\overline{X}$ the seminormalization of X, which is the largest curve between X and its normalization that is homeomorphic to X. We further assume here that $\overline{X}$ is nonsingular and that X has at least one singular point. The main result of this section is

Theorem 5.1. *Let X/k be a proper, reduced and connected curve. Let U denote the unipotent part of $J_{X/k}$. Assume that $\overline{X}$ is nonsingular and that X has at least one singular point. Then for any positive integer e, there is a subgroup scheme U' of U such that p^e kills U' and*

$$\dim(U') \geq \sum_{P \text{ singular}} \left(\delta_P - \lceil 2\delta_P/p^e \rceil + 1\right).$$

This result has the following consequences:

Theorem 5.2. *There is a subgroup scheme U' of U such that p^e kills U' and*

$$\dim(U') \geq \dim(U) - \lceil 2\dim(U)/p^e \rceil + 1.$$

Theorem 5.3. *U contains a subgroup scheme which is split and has dimension at least*

$$\dim(U) - \lceil 2\dim(U)/p \rceil + 1.$$

Note that Theorem 5.3 follows from [Ser], Ch. VII, no. 11, Proposition 11 by taking $e = 1$ in Theorem 5.2.

Fix $P \in X$ singular. Then, since $\overline{X}$ is nonsingular, $\hat{\mathcal{R}}_P \cong k[[x_1]]$. Recall that we defined

$$S_{P,1} = \{m \in \mathbb{N} \mid \text{ there is some power series } \sum_{i \geq m} \gamma_i x_1^i \in \hat{M}_P \text{ with } \gamma_m \neq 0\},$$

and $T_{P,1} = (\mathbb{N} \setminus S_{P,1})$, $t_{P,1} = \#T_{P,1}$. Since we have only one x_i, write r for x_1. Accordingly let us shorten our notation: $S_P := S_{P,1}$, $T_P := T_{P,1}$, $t_P := t_{P,1}$. Recall also that $\delta_P = \dim_k(\hat{\mathcal{R}}_P/\hat{\mathcal{O}}_P) = \dim_k(\hat{N}_P/\hat{M}_P)$. Since X is singular at P and $\overline{X}$ is nonsingular at P, we have that $\delta_P > 0$. One easily shows

Proposition 5.4. *$t_P = \delta_P$.*

It follows from Proposition 5.4 and Lemma 2.5 that $\{r^m \mid m \in T_P\}$ is a k-basis for $\hat{\mathcal{R}}_P/\hat{\mathcal{O}}_P$.

Now let us prove Theorem 5.1. Let a be an integer, $a > 1$. Define

$$T_P^a = \{m \in T_P \mid m \geq 2\delta_P/a\},$$

and set $\hat{\mathcal{O}}'_P = \hat{\mathcal{O}}_P[[r^m : m \in T_P^a]]$ (note that if $a \geq 2\delta_P$, then $\hat{\mathcal{O}}'_P = \hat{\mathcal{R}}_P$). Then

$$\hat{\mathcal{O}}_P \subset \hat{\mathcal{O}}'_P \subset \hat{\mathcal{R}}_P = k[[r]],$$

and this new intermediate ring is the completion of the local ring at P of a curve X' that is intermediate between X and $\overline{X}$ (see [Ser], Ch. IV, no. 3, Proposition 2, and recall that X and $\overline{X}$ are homeomorphic). So the map $h\colon \overline{X} \to X$ factors as $\overline{X} \to X' \to X$, and this gives us a factorization of $\psi\colon J_{X/k} \to J_{\overline{X}/k}$ as

$$J_{X/k} \xrightarrow{\rho} J_{X'/k} \to J_{\overline{X}/k}.$$

If we write U' for the kernel of ρ, then U' is a subgroup scheme of $U = \ker(\psi)$, and by an argument like that in the proof of Theorem 2.1, we get a group isomorphism $U'(k) \cong \bigoplus U'_P$, where

$$U'_P = \left(\hat{\mathcal{O}}'_P\right)^* \Big/ \hat{\mathcal{O}}_P^*$$

for each singular point P of X. By Lemmas 2.7 and 2.4, we know that $r^m \in \hat{M}_P$ for all $m \geq 2t_P = 2\delta_P$. Therefore, by the definition of $\hat{\mathcal{O}}'_P$, if $p^e \geq a$, then p^e kills U'_P. Thus p^e kills U' if $p^e \geq a$. Now, just as we calculated the dimension of U via (3), we find that

$$\dim(U') = \sum_{P \in X} \dim_k(\hat{\mathcal{O}}'_P/\hat{\mathcal{O}}_P) = \sum_{P \text{ singular}} \#T_P^a. \tag{5}$$

We prove below that

$$\#T_P^a \geq \delta_P - \lceil 2\delta_P/a \rceil + 1. \tag{6}$$

Then Theorem 5.1 follows from (5) and taking $a = p^e$ in (6). Finally, Theorem 5.2 follows from Theorem 5.1, (3) and the following:

Lemma 5.5. *Let $\beta_1, \ldots, \beta_m \in \mathbb{Q}$. Then*

$$\sum_{i=1}^m (\lceil \beta_i \rceil - 1) \leq \left\lceil \sum_{i=1}^m \beta_i \right\rceil - 1.$$

Proof. We prove the lemma by induction on m. For $m = 1$, the statement is clearly true. Now suppose that it is true for some $m \geq 1$, and let $\beta_1, \ldots, \beta_{m+1} \in \mathbb{Q}$. Then

$$\sum_{i=1}^{m+1} (\lceil \beta_i \rceil - 1) \leq \left\lceil \sum_{i=1}^{m} \beta_i \right\rceil - 1 + \lceil \beta_{m+1} \rceil - 1$$

by the induction hypothesis. Now, $\lceil \beta_{m+1} \rceil - 1 \leq \lfloor \beta_{m+1} \rfloor$, and therefore

$$\sum_{i=1}^{m+1} (\lceil \beta_i \rceil - 1) \leq \left\lceil \sum_{i=1}^{m} \beta_i \right\rceil - 1 + \lfloor \beta_{m+1} \rfloor \leq \left\lceil \sum_{i=1}^{m+1} \beta_i \right\rceil - 1.$$

By induction, then, the lemma is proven. □

Now let us prove (6).

Lemma 5.6. *Let S_P be a semigroup of $\mathbb{N}$ with $S_P \neq \mathbb{N}$ and $\#(\mathbb{N} \setminus S_P) = \delta_P$. Given an integer $a > 1$, define $T_P^a = \{m \in (\mathbb{N} \setminus S_P) \mid m \geq 2\delta_P/a\}$. Then*

$$\#T_P^a \geq \delta_P - \lceil 2\delta_P/a \rceil + 1.$$

Proof. By Lemma 2.7, any semigroup S_P of $\mathbb{N}$ such that $\#(\mathbb{N} \setminus S_P) = \delta_P$ contains all integers greater than or equal to $2\delta_P$. Therefore, among all semigroups of $\mathbb{N}$ with δ_P "holes," clearly $S = \{\delta_P + 1, \delta_P + 2, \ldots\}$ has the minimal number of holes greater than or equal to $2\delta_P/a$, as all its holes are consecutive, starting at 1. By inspection, for this semigroup,

$$\#\{m \in (\mathbb{N} \setminus S) \mid m \geq 2\delta_P/a\} = \delta_P - \lceil 2\delta_P/a \rceil + 1,$$

and Lemma 5.6 is proven. □

6. The case of semigroups with two generators

Now let us consider a special case of the situation in section 5. We retain the notation from there, and make an added assumption about the semigroups S_P. The main result of this section is

Theorem 6.1. *Let X/k be a proper, reduced, connected curve with $\overline{X}$ nonsingular. Denote by U the unipotent part of $J_{X/k}$. Assume that, for each singular point P of X, S_P is generated by two coprime integers. Then for any positive integer e, there is a subgroup scheme U' of U such that p^e kills U' and*

$$\dim(U') \geq \sum_{P \text{ with } p^e < 2\delta_P} \left\lfloor \left(\frac{p^e - 1}{p^e} \right)^2 \cdot \delta_P \right\rfloor + \sum_{P \text{ with } p^e \geq 2\delta_P} \delta_P.$$

We saw earlier (Example 2.11) that S_P is generated by two coprime integers b and c when X is isomorphic in a neighborhood of P to the plane curve $y^b = x^c$ around $(0, 0)$.

We prove Theorem 6.1 in exactly the same way that we proved Theorem 5.1. We did that by constructing, for a given $a > 1$, a subgroup scheme U' of U that was killed by any $p^e \geq a$ and had dimension at least

$$\sum_{P \text{ singular}} \#T_P^a.$$

We prove below, under the added assumption that S_P is generated by two coprime integers, that if $a < 2\delta_P$, then

$$\#T_P^a \geq \left\lfloor \left(\frac{a-1}{a}\right)^2 \cdot \delta_P \right\rfloor. \tag{7}$$

Taking $a = p^e$, then, we obtain Theorem 6.1.

An immediate consequence of Theorem 6.1 is

Theorem 6.2. *U contains a subgroup scheme which is split and has dimension at least*

$$\sum_{P \text{ with } p<2\delta_P} \left\lfloor \left(\frac{p-1}{p}\right)^2 \cdot \delta_P \right\rfloor + \sum_{P \text{ with } p\geq 2\delta_P} \delta_P.$$

Proof. Theorem 6.1 gives a subgroup scheme of U that is killed by p and has the stated dimension. The final assertion follows from [Ser], Ch. VII, no. 11, Proposition 11. □

From this we may obtain a statement independent of p.

Corollary 6.3. *U contains a subgroup scheme which is split and has dimension at least*

$$\sum_P \lfloor \delta_P/4 \rfloor.$$

Proof. Use Theorem 6.2 along with the fact that among all primes p, the minimal value of $\frac{p-1}{p}$ is $1/2$. □

Remark 6.4. Theorem 6.1 is a supplement to Theorem 5.1. We get the lower bound for the dimension in Theorem 6.1 by summing $\left\lfloor \left(\frac{p^e-1}{p^e}\right)^2 \cdot \delta_P \right\rfloor$ over all singular points P of X with $p^e < 2\delta_P$, and we get the bound in Theorem 5.1 by summing $\delta_P - \left\lceil \frac{2\delta_P}{p^e} \right\rceil + 1$ over such P. Now,

$$\left\lfloor \left(\frac{p^e-1}{p^e}\right)^2 \cdot \delta_P \right\rfloor = \left\lfloor \delta_P - \frac{2\delta_P}{p^e} + \frac{\delta_P}{p^{2e}} \right\rfloor = \delta_P - \left\lceil \frac{2\delta_P}{p^e} - \frac{\delta_P}{p^{2e}} \right\rceil.$$

It follows that $\left\lfloor \left(\frac{p^e-1}{p^e}\right)^2 \cdot \delta_P \right\rfloor > \delta_P - \left\lceil \frac{2\delta_P}{p^e} \right\rceil + 1$ if and only if

$$\left\lceil \frac{2\delta_P}{p^e} - \frac{\delta_P}{p^{2e}} \right\rceil < \left\lceil \frac{2\delta_P}{p^e} \right\rceil - 1.$$

This will be the case, for example, when $\delta_P > 2p^{2e}$. Roughly speaking, then, Theorem 6.1 is an improvement on Theorem 5.1 if p^e is small compared to the δ_P's.

Now let us prove (7).

Lemma 6.5. *Let S_P be a semigroup of $\mathbb{N}$ generated by two integers, with $\delta_P = \#(\mathbb{N} \setminus S_P)$ finite. Let a be an integer, $a \geq 1$. Let*

$$T_P^a = \{m \in (\mathbb{N} \setminus S_P) \mid m \geq 2\delta_P/a\}.$$

Then $\#T_P^a \geq \left\lfloor \left(\frac{a-1}{a}\right)^2 \cdot \delta_P \right\rfloor$.

Proof. The lemma is trivially true for $a = 1$, and is also true for $a \geq 2\delta_P$ by Lemma 2.7. Assume $1 < a < 2\delta_P$.

Say that S_P is generated by b and c. Since δ_P is finite, b and c are coprime. Say $b < c$. The lemma is vacuous if $\delta_P = 0$, so assume that $b > 1$. We know that $\delta_P = (b-1)(c-1)/2$. Set $\alpha = \lceil 2\delta_P/a \rceil - 1$. Then

$$\#T_P^a = \delta_P - \alpha + \#\{m \in S_P \mid m \leq \alpha\}.$$

Note that $\alpha \leq 2\delta_P/a < bc/a$, so $\lfloor \alpha/c \rfloor \leq \lfloor b/a \rfloor < b$. It follows that

$$\#\{m \in S_P \mid m \leq \alpha\} = \sum_{k=0}^{\lfloor \alpha/c \rfloor} \left(\left\lfloor \frac{\alpha - kc}{b} \right\rfloor + 1 \right) - 1.$$

Writing $\{\beta\} = \beta - \lfloor \beta \rfloor$ for the fractional part of $\beta \in \mathbb{Q}$, and using that

$$\sum_{k=0}^{\lfloor \alpha/c \rfloor} \left\{ \frac{\alpha - kc}{b} \right\} \leq \sum_{k=1}^{\lfloor \alpha/c \rfloor + 1} \left(\frac{b-k}{b} \right),$$

we obtain

$$\#T_P^a \geq \delta_P - \alpha - 1 + \frac{(\lfloor \alpha/c \rfloor + 1)}{2b} \cdot \left(2(\alpha+1) - \lfloor \alpha/c \rfloor (c-1)\right). \tag{8}$$

Define γ, ϵ by

$$\lfloor \alpha/c \rfloor = \frac{b-1}{a} - \gamma \text{ and } \quad \alpha = \frac{2\delta_P}{a} - \epsilon.$$

Note that $\gamma, \epsilon > 0$ since $\alpha < 2\delta_P/a$. Then (8) becomes

$$\begin{aligned} \#T_P^a \geq{}& \left(\frac{a-1}{a}\right)^2 \cdot \delta_P + (\epsilon - 1) \\ &+ \frac{1}{2b}\left[\frac{2b}{a}(1-\epsilon) + (2(1-\gamma) + 2\gamma\epsilon - \epsilon) \right. \\ &\qquad \left. + \frac{1}{a}\left(\alpha(a-1) + \epsilon - 2\right) + (1-c)(\gamma^2 - \gamma) \right]. \end{aligned} \tag{9}$$

We claim that the expression in brackets in (9) is nonnegative. To see this, we need upper bounds for γ and ϵ. By its definition, it is clear that $\epsilon \leq 1$. Indeed, one can also show that $\gamma \leq 1$. So we have that $0 < \gamma, \epsilon \leq 1$. This implies that each of the four terms inside the brackets in (9) is nonnegative.

Thus we now have

$$\#T_P^a \geq \left(\frac{a-1}{a}\right)^2 \cdot \delta_P + (\epsilon - 1).$$

And since $\epsilon > 0$, this gives our result. ∎

Example 6.6. This example shows that the bound proven in Lemma 6.5 is sharp (in particular, that the floor function is necessary). Take $b = 6$, $c = 7$, $a = 7$. Then $\delta_P = 15$, $\left(\frac{a-1}{a}\right)^2 \cdot \delta_P \approx 11.02$, and

$$\#\{m \in (\mathbb{N} \setminus S_P) \mid m \geq 5\} = 11.$$

7. Rational torsion points on Jacobians

In this section we give an application of Theorem 2.1. Let K be a field complete with respect to a discrete valuation v, with residue field k. Assume that $\mathrm{char}(K) = 0$. Let Z/K be a smooth, proper, geometrically connected curve of genus g with $Z(K) \neq \emptyset$. Let $\mathcal{Z}/\mathcal{O}_K$ be a regular model of Z, where $\mathcal{O}_K$ denotes the ring of integers of K. Let A/K be the Jacobian of Z, $\mathcal{A}/\mathcal{O}_K$ the Néron model of A. Write $\mathcal{A}_k^0$ for the identity component of the special fiber $\mathcal{A}_k$ of $\mathcal{A}$, and $\mathcal{Z}_k$ for the special fiber of $\mathcal{Z}$. Then $\mathcal{A}_k^0 \cong J_{\mathcal{Z}_k/k}$ as k-group schemes (see [BLR], Theorem 9.5/4). So we have the following exact sequences of group schemes over k:

$$0 \to U \times T \to \mathcal{A}_k^0 \cong J_{\mathcal{Z}_k/k} \to B \to 0,$$

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \pi_0(\mathcal{A}_k) \to 0,$$

where $\pi_0(\mathcal{A}_k)$ is the group of components of $\mathcal{A}_k$, and U, T and B are as in section 1.

Theorem 7.1. *Let Z/K be a smooth, proper, geometrically connected curve of genus g with $Z(K) \neq \emptyset$. Let $\mathcal{Z}/\mathcal{O}_K$ be a regular model of Z, with special fiber $\mathcal{Z}_k$. Let A/K be the Jacobian of Z. Suppose that the unipotent part U of $J_{\mathcal{Z}_k/k}$ has dimension g. Suppose further that $\mathcal{Z}_k$ is a reduced curve and that $v(p) < p - 1$. If $p > 2g + 1$, then $A(K)$ has no element of order p^2.*

Proof. Since U has dimension g, $\mathcal{A}_k^0 \cong J_{\mathcal{Z}_k/k} = U$. Since $\mathcal{Z}_k$ is reduced, Theorem 2.1 says that p kills $\mathcal{A}_k^0$. By [Lor], Theorem 2.4, p does not divide $\#\pi_0(\mathcal{A}_k)(k)$. Then from the second exact sequence above, $\mathcal{A}_k(k)$ has no element of order p^2. Now the result follows from the fact that $v(p) < p - 1$ implies that the reduction map $A(K) \to \mathcal{A}_k(k)$ is injective on the torsion subgroup of $A(K)$ (see, for example, the appendix to [Kat]). □

Acknowledgments

The author would like to thank Dino Lorenzini for many stimulating and helpful discussions. The author also wishes to thank Robert Rumely, as well as the referee, for their comments and suggestions.

References

[Bom] E. Bombieri, *Seminormalità e singolarità ordinarie*, Symposia Mathematica XI, Academic Press, New York (1972), 205-210. MR **55:**2884

[BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Springer-Verlag, Berlin, Heidelberg, New York (1990). MR **91i:**14034

[Edi] B. Edixhoven, *On the prime-to-p part of the groups of connected components of Néron models*, Compositio Math. **97** (1995), 29-49. MR **96h:**14066

[Kat] N. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481-502. MR **82d:**14025

[L-O] H. W. Lenstra, Jr. and F. Oort, *Abelian varieties having purely additive reduction*, J. Pure Appl. Alg. **36** (1985), 281-298. MR **86e:**14020

[Lor] D. Lorenzini, *Groups of components of Néron models of Jacobians*, Compositio Math. **73** (1990), 145-160. MR **92d:**14019

[Lor2] D. Lorenzini, *On the group of components of a Néron model*, J. Reine Angew. Math. **445** (1993), 109–160. MR **94k:**11065

[N-W] A. Nijenhuis and H. Wilf, *Representations of integers by linear forms in nonnegative integers*, J. Number Theory **4** (1972), 98-106. MR **44:**5274

[Ser] J.-P. Serre, *Groupes Algébriques et Corps de Classes*, Hermann, Paris (1959). MR **21:**1973

Department of Mathematics, Pennsylvania State University, 218 McAllister Building, University Park, Pennsylvania 16802

Current address: Department of Mathematics, Furman University, Greenville, South Carolina 29613

E-mail address: dpenn@math.furman.edu