

## ON PURELY INSEPARABLE EXTENSIONS $K[X, Y]/K[X', Y']$ AND THEIR GENERATORS

D. DAIGLE

(Communicated by Eric M. Friedlander)

ABSTRACT. Let  $\mathbf{k}$  be a field of characteristic  $p > 0$  and  $R = \mathbf{k}[X, Y]$  a polynomial algebra in two variables. By a  $p$ -generator of  $R$  we mean an element  $u$  of  $R$  for which there exist  $v \in R$  and  $n \geq 0$  such that  $\mathbf{k}[u, v] \supseteq R^{p^n}$ . We also define a  $p$ -line of  $R$  to mean any element  $u$  of  $R$  whose coordinate ring  $R/uR$  is that of a  $p$ -generator. Then we prove that if  $u \in R$  is such that  $u - T$  is a  $p$ -line of  $\mathbf{k}(T)[X, Y]$  (where  $T$  is an indeterminate over  $R$ ), then  $u$  is a  $p$ -generator of  $R$ . This is analogous to the well-known fact that if  $u \in R$  is such that  $u - T$  is a line of  $\mathbf{k}(T)[X, Y]$ , then  $u$  is a variable of  $R$ . We also prove that if  $u$  is a  $p$ -line of  $R$  for which there exist  $\varphi \in \text{qt } R$  and  $n \geq 0$  such that  $\mathbf{k}(u, \varphi) \supseteq R^{p^n}$ , then  $u$  is in fact a  $p$ -generator of  $R$ .

Let  $\mathbf{k}$  be a field of characteristic  $p > 0$  and  $R = \mathbf{k}^{[2]}$  ( $\mathbf{k}^{[n]}$  is a polynomial algebra in  $n$  indeterminates over  $\mathbf{k}$  and  $\mathbf{k}^{(n)}$  is the field of fractions of  $\mathbf{k}^{[n]}$ ). These notations are in effect throughout this paper.

Let  $u \in R$ . Following several authors, we call  $u$  a *line* (of  $R$ ) if  $R/uR = \mathbf{k}^{[1]}$ ; we call  $u$  a *variable* of  $R$  if  $R = \mathbf{k}[u, v]$  for some  $v \in R$ . So a line is an element  $u \in R$  whose coordinate ring  $R/uR$  is that of a variable.

The *conjecture on the classification of lines* asserts that if  $u$  is a line of  $R$ , then there exist  $X, Y \in R$  such that  $R = \mathbf{k}[X, Y]$  and  $u \in \mathbf{k}[X^p, Y]$ . (Note that this conjecture and the seemingly stronger one stated in [6] are equivalent by [2].) This conjecture is expected to be true when  $\mathbf{k}$  is algebraically closed but, as far as we know, nothing has been said about its plausibility when  $\mathbf{k}$  is arbitrary. At any rate, one sees that if this conjecture is true then so is the following:

**Lines Conjecture.** *If  $u$  is a line of  $R$ , then there exist  $v \in R$  and  $n \geq 0$  such that  $\mathbf{k}[u, v] \supseteq R^{p^n}$ .*

Let us call an element  $u$  of  $R$  a  $p$ -generator of  $R$  if there exist  $v \in R$  and  $n \geq 0$  such that  $\mathbf{k}[u, v] \supseteq R^{p^n}$ ; we call  $u \in R$  a  $p$ -line of  $R$  if  $R/uR$  is  $\mathbf{k}$ -isomorphic to  $R/wR$  for some  $p$ -generator  $w$  of  $R$ . The Lines Conjecture, which asserts that every line of  $R$  is a  $p$ -generator of  $R$ , is therefore a special case of

**Question.** *Is every  $p$ -line a  $p$ -generator?*

The first section of this paper studies the behavior of  $p$ -generators with respect to base field extension. The key-result is:

---

Received by the editors June 7, 1994.

1991 *Mathematics Subject Classification.* Primary 13F20.

The author was supported by a grant from NSERC Canada.

**Extension Lemma.** For  $u \in R$ , the following are equivalent:

1.  $u$  is a  $p$ -generator of  $R$ .
2. For all field extensions  $K/\mathbf{k}$ ,  $u$  is a  $p$ -generator of  $K \otimes R$ .
3. For some field extension  $K/\mathbf{k}$ ,  $u$  is a  $p$ -generator of  $K \otimes R$ .

From this, we will deduce that if the Lines Conjecture is true when  $\mathbf{k}$  is algebraically closed, then it is true for arbitrary  $\mathbf{k}$ . We will also prove a similar result related to the question whether all  $p$ -lines are  $p$ -generators. The Extension Lemma is also used in the proofs of the two theorems we will now state; in each case, it allows us to reduce the problem to the case where  $\mathbf{k}$  is algebraically closed.

The first result is an analogue, for  $p$ -lines and  $p$ -generators, of the well-known fact that if  $u \in \mathbf{k}[X, Y]$  is generically a line (i.e.,  $u - T$  is a line of  $\mathbf{k}(T)[X, Y]$ ), then  $u$  is a variable of  $\mathbf{k}[X, Y]$ .<sup>1</sup>

We say that  $u$  is a *generic  $p$ -line* of  $R$  if  $u \in R$  and  $u - T$  is a  $p$ -line of  $\mathbf{k}(T) \otimes R$ , where  $T$  is an indeterminate over  $R$ . The second section gives a proof of:

**Theorem A.** Every generic  $p$ -line of  $R$  is a  $p$ -generator of  $R$ .

Recall that  $u \in R$  is called a *field generator* if there exists  $\varphi \in \text{qt } R$  such that  $\text{qt } R = \mathbf{k}(u, \varphi)$ . It is known that if a field generator is a line, then it is a variable (see 4.9 (ii) of [7]). In the third section we prove an analogue of that fact:

**Theorem B.** Let  $u$  be a  $p$ -line of  $R$  for which there exist  $\varphi \in \text{qt } R$  and  $n \geq 0$  such that  $\mathbf{k}(u, \varphi) \supseteq R^{p^n}$ . Then  $u$  is a  $p$ -generator of  $R$ .

*Notations.* If  $A$  is a ring (i.e., a commutative ring with a unity), then  $A^*$  is its set of units; if  $A$  is an integral domain, then  $\text{qt } A$  is its field of fractions. A *coordinate system* of  $R$  is an ordered pair  $(u, v) \in R \times R$  such that  $R = \mathbf{k}[u, v]$ ; the set of coordinate systems of  $R$  is denoted  $\Gamma(R)$ . Given a polynomial  $F = \sum a_i T^i \in \mathbf{k}[T]$ , where  $a_i \in \mathbf{k}$  and  $T$  is a set of indeterminates, we write  $F^{(p)} = \sum a_i^p T^i$ ; if  $\varphi : \mathbf{k} \rightarrow \mathbf{k}$  is any map, we write  $F^{(\varphi)} = \sum \varphi(a_i) T^i$ . The symbol  $\otimes_A$  means tensor product of  $A$ -algebras and  $\otimes_{\mathbf{k}}$  is abbreviated  $\otimes$ .

## 1. THE EXTENSION LEMMA

**Preliminaries.** The following definitions and facts can be found in [3].

**1.1.** Given  $u \in R$ , let  $\Sigma_u(R)$  denote the collection of subalgebras  $\mathbf{k}[u, v]$  of  $R$  such that  $\mathbf{k}[u, v] \supseteq R^{p^n}$  for some integer  $n \geq 0$ . Thus a  $p$ -generator of  $R$  is an element  $u \in R$  satisfying  $\Sigma_u(R) \neq \emptyset$ . If  $u$  is a  $p$ -generator of  $R$  which does not belong to  $\mathbf{k}[R^p]$ , then  $\Sigma_u(R)$  is totally ordered by inclusion and consequently has a unique maximal member; in that case, we call an element  $v$  of  $R$  an  *$R$ -cogenerator* of  $u$  if  $\mathbf{k}[u, v]$  is the maximal member of  $\Sigma_u(R)$ .

**1.2.** Irreducible  $p$ -generators of  $R$  have one purely inseparable place at infinity.

**1.3.** Every  $p$ -generator of  $R$  factors as  $aw^{p^s}$ , where  $a \in \mathbf{k}^*$ ,  $s \geq 0$  is an integer and  $w$  is an irreducible  $p$ -generator of  $R$ .

**1.4.** Let  $u$  be a  $p$ -generator of  $R$  and  $(X, Y) \in \Gamma(R)$ . If  $\deg_X u > 0$ , then  $u$  is almost monic in  $X$ . On the other hand, if  $\deg_X u \leq 1$  and  $u \notin \mathbf{k}[R^p]$ , then  $u$  is a variable of  $R$ .

<sup>1</sup>The origin of this fact seems to be Theorem 4.4 of [4], but it also appeared at several other places, for instance 2.4.2 of [8].

*Proof of the Extension Lemma.* The implications  $(1 \Rightarrow 2 \Rightarrow 3)$  are trivial. Assume that  $K$  is an extension of  $\mathbf{k}$  such that  $\Sigma_u(\bar{R}) \neq \emptyset$ , where  $\bar{R} = K \otimes R (= K^{[2]})$ .

There exists a subfield  $K_0$  of  $K$  containing  $\mathbf{k}$  such that

$$(1) \quad \text{i) } K_0/\mathbf{k} \text{ is finitely generated, and ii) } \Sigma_u(K_0 \otimes R) \neq \emptyset.$$

To see this, choose  $v \in \bar{R}$  and  $n \geq 0$  such that  $K[u, v] \supseteq \bar{R}^{p^n}$ , and choose  $(X, Y) \in \Gamma(R)$ . Since  $v \in \bar{R} = K[X, Y]$  and  $X^{p^n}, Y^{p^n} \in K[u, v]$  we have  $v = \sum v_{ij} X^i Y^j$ ,  $X^{p^n} = \sum \alpha_{ij} u^i v^j$  and  $Y^{p^n} = \sum \beta_{ij} u^i v^j$  for some  $v_{ij}, \alpha_{ij}, \beta_{ij} \in K$ . Let  $K_0 = \mathbf{k}(v_{ij}, \alpha_{ij}, \beta_{ij})$ . Then  $v \in K_0[X, Y] = K_0 \otimes R$  and  $X^{p^n}, Y^{p^n} \in K_0[u, v]$ , which proves (1).

Let  $s = \sup\{i \geq 0 \mid u \in \mathbf{k}[R^{p^i}]\}$ ,  $R_s = \mathbf{k}[R^{p^s}] = \mathbf{k}^{[2]}$  and  $\bar{R}_s = K[\bar{R}^{p^s}] = K \otimes R_s$ . Then  $u \in R_s$ ,  $u \notin \mathbf{k}[R_s^{p^s}]$  and  $\Sigma_u(\bar{R}_s) \neq \emptyset$  (for if  $v \in \bar{R}$  and  $n \geq 0$  satisfy  $\bar{R}^{p^n} \subseteq K[u, v]$ , then  $v^{p^s} \in \bar{R}_s$  satisfies  $K[u, v^{p^s}] \supseteq \bar{R}_s^{p^n}$ ). Since it suffices to prove that  $\Sigma_u(R_s) \neq \emptyset$ , we may assume that

$$(2) \quad u \notin \mathbf{k}[R^p] \quad (\text{hence } u \notin K[\bar{R}^p]).$$

We will now prove five special cases of the lemma, before proving the general case.

*Case 1.*  $K/\mathbf{k}$  is purely inseparable.

Let  $v \in \bar{R}$  and  $n \geq 0$  be such that  $\bar{R}^{p^n} \subseteq K[u, v]$ , and let  $(X, Y) \in \Gamma(R)$  and  $F, G \in K[T_1, T_2]$  be such that  $X^{p^n} = F(u, v)$  and  $Y^{p^n} = G(u, v)$ . Now for suitable  $s \geq 0$  we have  $v^{p^s} \in R$  and  $F^{(p^s)}, G^{(p^s)} \in \mathbf{k}[T_1, T_2]$ ; since  $X^{p^{n+s}} = F^{(p^s)}(u^{p^s}, v^{p^s}) \in \mathbf{k}[u, v^{p^s}]$  and similarly for  $Y^{p^{n+s}}$ ,  $\Sigma_u(R) \neq \emptyset$ .

*Case 2.*  $K/\mathbf{k}$  is finite and Galois.

Let  $G = \text{Gal}(K/\mathbf{k})$ . Since  $u \notin K[\bar{R}^p]$ ,  $\Sigma_u(\bar{R})$  is totally ordered by inclusion and has a unique maximal member  $A$  (see 1.1). Each  $\theta \in G$  extends uniquely to an  $R$ -automorphism  $\bar{\theta}$  of  $\bar{R}$  and this  $\bar{\theta}$  maps  $A$  onto itself. Indeed,

- if  $A = K[u, v]$ , then  $\bar{\theta}(A) = K[u, \bar{\theta}(v)]$ ,
- if  $\bar{R}^{p^n} \subseteq A$ , then  $\bar{R}^{p^n} = \bar{\theta}(\bar{R}^{p^n}) \subseteq \bar{\theta}(A)$ , so  $\bar{\theta}(A) \in \Sigma_u(\bar{R})$  and therefore  $\bar{\theta}(A) \subseteq A$ ,
- $[\text{qt } \bar{R} : \text{qt } \bar{\theta}(A)] = [\text{qt } \bar{R} : \text{qt } A]$ ,

so  $\bar{\theta}(A) = A$ .

Fix  $(X, Y) \in \Gamma(R)$  and let  $s = \deg_X u$ . We may assume that  $s > 1$ , for otherwise  $u$  is a variable of  $\bar{R}$  by 1.4, hence a variable of  $R$  by a standard argument. Again by 1.4,  $u$  is almost monic in  $X$ . Replacing if necessary  $u$  by  $au + b$  for suitable  $a \in \mathbf{k}^*$  and  $b \in \mathbf{k}$ , we may assume that  $u$  is monic in  $X$  and has no constant term:

$$u = X^s + u_{s-1}X^{s-1} + \dots + u_0 \quad (u_i \in \mathbf{k}[Y] \text{ and } u_0 \in Y\mathbf{k}[Y]).$$

We claim that some  $\bar{R}$ -cogenerator of  $u$  is in  $R$ . This is obvious if some  $\bar{R}$ -cogenerator of  $u$  is in  $K[Y]$ , because in that case  $Y$  itself is an  $\bar{R}$ -cogenerator of  $u$ . So we may assume that every  $\bar{R}$ -cogenerator of  $u$  has positive  $X$ -degree, which implies that  $E \neq \emptyset$ , where we let  $E$  be the set of  $\bar{R}$ -cogenerators  $v$  of  $u$  satisfying:

$$(3) \quad s \nmid \deg_X v, \quad v \text{ is monic in } X \text{ and } v \in (X, Y)\bar{R}.$$

If  $v \in E$  and  $\theta \in G$ , then

$$(4) \quad K[u, v] = A = \bar{\theta}(A) = K[u, \bar{\theta}(v)]$$

so  $\bar{\theta}(v)$  is an  $\bar{R}$ -cogenerator of  $u$ ; since  $v$  and  $\bar{\theta}(v)$  have the same leading term (as elements of  $(K[Y])[X]$ ), we see that  $\bar{\theta}(v) \in E$ . Hence  $G$  acts on  $E$ .

We shall now define a map  $\delta : E \rightarrow \mathbf{N} \cup \{-\infty\}$ . Given  $v \in E$  and  $\theta \in G$ , (4) implies that there exist a unique  $\alpha_{v,\theta} \in K^*$  and a unique  $f_{v,\theta} \in K[T]$  such that

$$(5) \quad \bar{\theta}(v) = \alpha_{v,\theta} v + f_{v,\theta}(u).$$

By (3) we have  $\deg_X f_{v,\theta}(u) \neq \deg_X v = \deg_X \bar{\theta}(v)$ , hence

$$(6) \quad \deg_X f_{v,\theta}(u) < \deg_X v = \deg_X \bar{\theta}(v).$$

Because  $v$  and  $\bar{\theta}(v)$  are monic in  $X$ , (5) and (6) imply that  $\alpha_{v,\theta} = 1$ , hence

$$(7) \quad \bar{\theta}(v) = v + f_{v,\theta}(u).$$

Now  $\delta(v) = \max_{\theta \in G} \deg f_{v,\theta}$  defines a map  $\delta : E \rightarrow \mathbf{N} \cup \{-\infty\}$  and, by Galois theory,  $\delta(v) = -\infty \Leftrightarrow v \in R$ .

Consider  $v \in E \setminus R$ ; then  $d = \delta(v)$  is a positive integer. Write

$$f_{v,\theta} = \sum_{i=1}^d a_i(v,\theta)T^i \quad \text{and} \quad v = \sum v_{ij}X^iY^j,$$

where  $a_i(v,\theta), v_{ij} \in K$ . Since  $\deg_X(u^d) < \deg_X v$  by (6),  $v' = v - v_{sd,0}u^d$  belongs to  $E$ . We claim that  $\delta(v') < \delta(v)$ . Indeed, note that (7) implies

$$(8) \quad \theta(v_{sd,0}) = v_{sd,0} + a_d(v,\theta), \quad \text{for all } \theta \in G,$$

whence  $\bar{\theta}(v') = \bar{\theta}(v) - \theta(v_{sd,0})u^d = v' + f_{v,\theta}(u) - a_d(v,\theta)u^d$  by (7) and (8). So

$$f_{v',\theta} = f_{v,\theta} - a_d(v,\theta)T^d, \quad \text{for all } \theta \in G,$$

and in particular  $\delta(v') < d$ . Hence if we pick  $v \in E$  which minimizes  $\delta(v)$ , we must have  $v \in R$ , which proves the claim.

To complete the proof of Case 2, let  $v$  be an  $\bar{R}$ -cogenerator of  $u$  which belongs to  $R$  and let  $n \geq 0$  be such that  $\bar{R}^{p^n} \subseteq K[u, v]$ . If  $h \in R$ , then  $h^{p^n} \in K[u, v]$  so  $h^{p^n} = F(u, v)$  for some  $F \in K[T_1, T_2]$ . For each  $\theta \in G$  we have  $h^{p^n} = \bar{\theta}(h^{p^n}) = F^{(\theta)}(u, v)$ , whence  $F^{(\theta)} = F$ . By Galois theory,  $F \in \mathbf{k}[T_1, T_2]$ ; this shows that  $R^{p^n} \subseteq \mathbf{k}[u, v]$ .

*Case 3.*  $K/\mathbf{k}$  is finite and separable.

Let  $L$  be a finite extension of  $K$  such that  $L/\mathbf{k}$  is Galois. Since  $\Sigma_u(K \otimes R) \neq \emptyset$  implies  $\Sigma_u(L \otimes R) \neq \emptyset$ , this is an immediate consequence of Case 2.

*Case 4.*  $K/\mathbf{k}$  is algebraic.

By (1), we may assume that  $K/\mathbf{k}$  is finite. Let  $\mathbf{k}_{\text{sep}}$  be the separable closure of  $\mathbf{k}$  in  $K$ , i.e.,

$$\mathbf{k}_{\text{sep}} = \{s \in K \mid s \text{ is separable over } \mathbf{k}\}.$$

Since  $K/\mathbf{k}_{\text{sep}}$  is purely inseparable, Case 1 implies that  $\Sigma_u(\mathbf{k}_{\text{sep}} \otimes R) \neq \emptyset$ ; since  $\mathbf{k}_{\text{sep}}/\mathbf{k}$  is finite and separable, the assertion then follows from Case 3.

*Case 5.*  $K = \mathbf{k}(S)$ ,  $S$  an indeterminate.

Suppose first that  $\mathbf{k}$  is an infinite field. Let  $v \in \bar{R}$  and  $n \geq 0$  be such that  $\bar{R}^{p^n} \subseteq K[u, v]$ . Choose  $(X, Y) \in \Gamma(R)$  and let  $F, G \in K[T_1, T_2]$  be such that  $X^{p^n} = F(u, v)$ ,  $Y^{p^n} = G(u, v)$ . Write  $v = \sum v_{ij}X^iY^j$ ,  $F = \sum \alpha_{ij}T_1^i T_2^j$  and  $G = \sum \beta_{ij}T_1^i T_2^j$ , where  $v_{ij}, \alpha_{ij}$  and  $\beta_{ij}$  all belong to  $K$ . Since  $\mathbf{k}$  is infinite, we may choose  $s \in \mathbf{k}$  such that all  $v_{ij}, \alpha_{ij}$  and  $\beta_{ij}$  are defined at  $S = s$ . Specialization at  $s$

yields  $\bar{v} \in R$ ,  $\bar{F}, \bar{G} \in \mathbf{k}[T_1, T_2]$  such that  $X^{p^n} = \bar{F}(u, \bar{v})$  and  $Y^{p^n} = \bar{G}(u, \bar{v})$ , whence  $\Sigma_u(R) \neq \emptyset$ .

If  $\mathbf{k}$  is a finite field, consider an algebraic closure  $\mathbf{k}'$  of  $\mathbf{k}$  and write  $K' = \mathbf{k}'(S)$ . Since  $\Sigma_u(K \otimes R) \neq \emptyset$  implies  $\Sigma_u(K' \otimes R) \neq \emptyset$ , and since  $\mathbf{k}'$  is an infinite field, the preceding paragraph shows that  $\Sigma_u(\mathbf{k}' \otimes R) \neq \emptyset$ , whence  $\Sigma_u(R) \neq \emptyset$  by Case 4.

We may now complete the proof of the lemma. By (1), we may assume that  $K$  is finitely generated over  $\mathbf{k}$ . Consider a subfield  $K_1$  of  $K$  containing  $\mathbf{k}$  such that  $K_1/\mathbf{k}$  is purely transcendental and  $K/K_1$  is algebraic. Then  $\Sigma_u(K_1 \otimes R) \neq \emptyset$  by Case 4 and  $\Sigma_u(R) \neq \emptyset$  by  $\text{trdeg}_{\mathbf{k}}K$  applications of Case 5.  $\square$

**Corollary 1.5.** *Suppose that, for some field extension  $K/\mathbf{k}$ , the Lines Conjecture holds in  $K^{[2]}$ . Then it holds in  $\mathbf{k}^{[2]}$ .*

**Corollary 1.6.** *Suppose that, for some field extension  $K/\mathbf{k}$ , every  $p$ -line of  $K^{[2]}$  is a  $p$ -generator of  $K^{[2]}$ . Then every  $p$ -line of  $\mathbf{k}^{[2]}$  is a  $p$ -generator of  $\mathbf{k}^{[2]}$ .*

The first corollary follows immediately from the Extension Lemma and the simple observation that every line of  $R$  is a line of  $K \otimes R$ . Similarly, the second one is a consequence of the lemma and of the following fact, which will also be used in the second and third sections.

**Lemma 1.7.** *Let  $K/\mathbf{k}$  be a field extension and write  $\bar{R} = K \otimes R$ . Then every  $p$ -line (respectively, generic  $p$ -line) of  $R$  is a  $p$ -line (respectively, a generic  $p$ -line) of  $\bar{R}$ .*

*Proof.* Suppose that  $u$  is a  $p$ -line of  $R$  and let  $w$  be a  $p$ -generator of  $R$  such that  $R/uR = R/wR$ . Then  $w$  is a  $p$ -generator of  $\bar{R}$  and  $\bar{R}/u\bar{R} = K \otimes (R/uR) = K \otimes (R/wR) = \bar{R}/w\bar{R}$ , so  $u$  is a  $p$ -line of  $\bar{R}$ .

Suppose that  $u$  is a generic  $p$ -line of  $R$ . Applying the first part to the  $p$ -line  $u - T$  of  $\mathbf{k}(T) \otimes R$  and to the extension  $K(T)/\mathbf{k}(T)$ , we get that  $u - T$  is a  $p$ -line of  $K(T) \otimes_{\mathbf{k}(T)} (\mathbf{k}(T) \otimes R) = K(T) \otimes_K \bar{R}$ , i.e.,  $u$  is a generic  $p$ -line of  $\bar{R}$ .  $\square$

## 2. GENERIC $p$ -LINES

The aim of this section is to prove Theorem A. We will need the following result, which can be derived from the proof of Theorem 2.3.1 of [8]:

**2.1.** *Let  $A \subset B$  be integral domains, where  $B$  is finitely generated as an  $A$ -algebra. Suppose that there exists a multiplicatively closed subset  $S$  of  $A$  such that  $S^{-1}B = (S^{-1}A)^{[1]}$ , and that every element of  $S \setminus A^*$  is a finite product of elements  $\pi$  of  $A$  satisfying:*

1.  $\pi$  is a prime element of  $B$ ,
2.  $\pi B \cap A = \pi A$ ,
3.  $A/\pi A$  is algebraically closed in  $B/\pi B$ .

Then  $B = A^{[1]}$ .

The author thanks S.M. Bhatwadekar for having taught him the result in this form; see also Theorem 2.6 of [1]. We will also need some basic properties of  $p$ -lines:

**Lemma 2.2.** *Suppose  $u$  is a  $p$ -line of  $R$  and let  $Q = R/uR$ .*

1. *There exist  $z \in Q$  and  $n \geq 0$  such that  $\mathbf{k}[z] \supseteq Q^{p^n}$ .*
2. *If  $u$  is irreducible in  $R$  and  $\mathbf{k}'$  is the algebraic closure of  $\mathbf{k}$  in  $\text{qt}Q$ , then  $(\mathbf{k}')^{p^n} \subseteq \mathbf{k}$ , where  $n$  is as in (1).*

3.  $u = \lambda u_0^{p^s}$  for some irreducible  $p$ -line  $u_0$  of  $R$ , some  $\lambda \in \mathbf{k}^*$  and  $s \geq 0$ .
4. If  $u \in \mathbf{k}[R^p]$ , then  $u$  is a  $p$ -line of  $\mathbf{k}[R^p]$ .
5. If  $u \notin \mathbf{k}[R^p]$ , then  $u - \theta$  is irreducible in  $R$  for every  $\theta \in \mathbf{k}$ ,  $\text{qt } Q$  is a regular extension of  $\mathbf{k}$  and  $Q^* = \mathbf{k}^*$ .

*Remark 2.3.* If  $u$  is a  $p$ -line of  $R$  not in  $\mathbf{k}[R^p]$ , then  $u$  is irreducible in  $R$  by part (3), so part (1) implies that  $u$  has one purely inseparable place at infinity. Despite the nice properties stated in part (5), that place at infinity is not necessarily rational if  $\mathbf{k}$  is not perfect. If  $\mathbf{k}$  is perfect,  $u$  is easily seen to be a *polynomial curve*, i.e., a rational curve with one rational place at infinity.

*Proof.* There exists a  $p$ -generator  $w_1$  of  $R$  such that  $Q \cong R/w_1R$ . Let  $w_2 \in R$  and  $n \geq 0$  be such that  $\mathbf{k}[w_1, w_2] \supseteq R^{p^n}$ ; then  $n$  and  $z = w_2 + w_1R \in Q$  satisfy (1). Note that  $\mathbf{k}[z] = \mathbf{k}^{[1]}$ .

Since  $(\mathbf{k}')^{p^n}$  is contained in  $\mathbf{k}(z)$  and its elements are algebraic over  $\mathbf{k}$ , (2) holds.

Applying 1.3 to the  $w_1$  of the first paragraph gives  $R/uR \cong R/(w_0^{p^s})R$ , where  $w_0$  is an irreducible  $p$ -generator of  $R$  and  $s \geq 0$  is an integer. Now it easily follows that  $u = \lambda u_0^{p^s}$ , for some  $\lambda \in \mathbf{k}^*$  and  $u_0 \in R$  satisfying  $R/u_0R \cong R/w_0R$ . Hence (3) holds.

To prove (4), suppose that  $u \in \mathbf{k}[R^p]$ . Let  $w_1$  be as before; we claim that  $w_1 \in \mathbf{k}[R^p]$ . To see this, let  $\bar{\mathbf{k}}$  be the algebraic closure of  $\mathbf{k}$  and write  $\bar{R} = \bar{\mathbf{k}} \otimes R$ . Then  $\bar{R}/u\bar{R} \cong \bar{R}/w_1\bar{R}$  and  $u \in \bar{R}^p$ , so the argument of the preceding paragraph shows that  $w_1 \in \bar{R}^p$ , hence  $w_1 \in \mathbf{k}[R^p]$ . Write  $Q = R/uR$ ,  $Q_1 = R/w_1R$  and  $A = \mathbf{k}[R^p]$ ; then  $\mathbf{k}[Q^p] = A/uA$  and  $\mathbf{k}[Q_1^p] = A/w_1A$ . Since any  $\mathbf{k}$ -isomorphism  $Q \rightarrow Q_1$  restricts to a  $\mathbf{k}$ -isomorphism  $\mathbf{k}[Q^p] \rightarrow \mathbf{k}[Q_1^p]$ ,  $A/uA$  is  $\mathbf{k}$ -isomorphic to  $A/w_1A$  and  $u$  is a  $p$ -line of  $A$ .

To prove (5), suppose that  $u \notin \mathbf{k}[R^p]$ . Then, by (3),  $u$  is irreducible in  $R$ , so  $Q$  is a domain.

The fact that  $u \notin \mathbf{k}[R^p]$  implies that  $\text{qt } Q$  is separable over  $\mathbf{k}$ . Indeed, choose  $(X, Y) \in \Gamma(R)$  such that  $u \notin \mathbf{k}[X, Y^p]$  and consider the tower  $\mathbf{k} \subset \mathbf{k}(x) \subseteq \mathbf{k}(x, y) = \text{qt } Q$ , where  $x, y$  are the images of  $X$  and  $Y$  in  $Q$ ; since separability is transitive, it is clear that  $\text{qt } Q$  is separable over  $\mathbf{k}$ .

Let  $\mathbf{k}'$  be the algebraic closure of  $\mathbf{k}$  in  $\text{qt } Q$ . Since  $\mathbf{k}'/\mathbf{k}$  is purely inseparable by (2) and separable by the preceding paragraph,  $\mathbf{k}$  is algebraically closed in  $\text{qt } Q$  and  $\text{qt } Q$  is therefore a regular extension of  $\mathbf{k}$ .

The fact that  $Q^* = \mathbf{k}^*$  follows immediately from part (1) and the fact that  $\mathbf{k}$  is algebraically closed in  $\text{qt } Q$ . Finally, the irreducibility of  $u - \theta$  (when  $\theta \neq 0$ ) is an easy consequence of  $Q^* = \mathbf{k}^*$ . □

**Corollary 2.4.** *If  $u$  is a generic  $p$ -line of  $R$  and  $u \in \mathbf{k}[R^p]$ , then  $u$  is a generic  $p$ -line of  $\mathbf{k}[R^p]$ .*

*Proof.* Choose  $(X, Y) \in \Gamma(R)$ . By the assumptions,  $u - T$  is a  $p$ -line of  $\mathbf{k}(T)[X, Y]$  and  $u - T \in \mathbf{k}(T)[X^p, Y^p]$ . By part (4) of 2.2 it follows that  $u - T$  is a  $p$ -line of  $\mathbf{k}(T)[X^p, Y^p]$ , which means that  $u$  is a generic  $p$ -line of  $\mathbf{k}[X^p, Y^p]$ . □

**Lemma 2.5.** *Suppose that  $\mathbf{k}$  is algebraically closed and that  $u \in R$  satisfies*

1.  $u - \lambda$  is an irreducible element of  $R$ , for all  $\lambda \in \mathbf{k}$ ; and
2. there exist  $v \in R$  and  $n \geq 0$  such that  $\mathbf{k}(u)[v] \supseteq R^{p^n}$ .

*Then  $u$  is a  $p$ -generator of  $R$ . More precisely,  $R \cap \mathbf{k}(u, v) = \mathbf{k}[u]^{[1]}$ .*

*Proof.* Let  $A = \mathbf{k}[u]$  and  $B = R \cap \mathbf{k}(u, v)$ . Then

$$(9) \quad B \text{ is the integral closure of } R^{p^n} \text{ in } \mathbf{k}(u, v)$$

so, in particular,

$$(10) \quad B \text{ is a finitely generated } \mathbf{k}\text{-algebra.}$$

Note that  $B^{p^n} \subseteq R^{p^n} \subseteq \mathbf{k}(u)[v]$  implies that  $\mathbf{k}(u)[B]$  is integral over  $\mathbf{k}(u)[v]$ ; since  $\mathbf{k}(u)[v] \subseteq \mathbf{k}(u)[B] \subseteq \mathbf{k}(u, v)$  and  $\mathbf{k}(u)[v]$  is integrally closed in  $\mathbf{k}(u, v)$ , it follows that  $\mathbf{k}(u)[B] = \mathbf{k}(u)[v]$ , whence

$$(11) \quad S^{-1}B = (S^{-1}A)^{[1]}$$

where  $S = A \setminus \{0\}$ . Note that each element of  $S \setminus A^*$  is a product of factors  $u - \lambda$  with  $\lambda \in \mathbf{k}$ . We claim that for each  $\lambda \in \mathbf{k}$ ,  $\pi = u - \lambda$  satisfies

$$(12) \quad \pi \text{ is a prime element of } B,$$

$$(13) \quad \pi B \cap A = \pi A,$$

$$(14) \quad A/\pi A \text{ is algebraically closed in } B/\pi B.$$

Indeed,  $\pi$  is irreducible in  $R$  by assumption, so  $\pi R \cap B$  is a prime ideal of  $B$  which contains  $\pi B$ . If  $\pi r \in B$  (where  $r \in R$ ), then  $r \in \text{qt } B$  and  $r$  is integral over  $R^{p^n}$ , so  $r \in B$  by (9). This shows that  $\pi R \cap B = \pi B$ , so (12) holds.

Since  $\pi B \cap A$  is a prime ideal of  $A$  and contains  $\pi$ , (13) holds. Finally,  $A/\pi A$  is the algebraically closed field  $\mathbf{k}$ , so (14) holds.

Conditions (10)–(14), together with 2.1, allow us to conclude that  $B = A^{[1]}$ . Hence there exists  $v' \in R$  such that  $B = \mathbf{k}[u, v']$ ; since  $R^{p^n} \subseteq B$ ,  $u$  is a  $p$ -generator of  $R$ . □

*Proof of Theorem A.* Let  $u$  be a generic  $p$ -line of  $R$ .

If  $\bar{\mathbf{k}}$  is the algebraic closure of  $\mathbf{k}$ , then, by 1.7,  $u$  is a generic  $p$ -line of  $\bar{\mathbf{k}} \otimes R$  and, by the Extension Lemma, it suffices to prove that  $u$  is a  $p$ -generator of  $\bar{\mathbf{k}} \otimes R$ . So we may assume that  $\mathbf{k}$  is algebraically closed.

Let  $s \geq 0$  be such that  $u \in R^{p^s}$  but  $u \notin R^{p^{s+1}}$ . By 2.4,  $u$  is a generic  $p$ -line of  $R^{p^s}$ ; since it suffices to show that  $u$  is a  $p$ -generator of  $R^{p^s}$ , we may assume that  $u \notin R^p$ . This implies that the  $p$ -line  $u - T$  of  $\hat{R} = \mathbf{k}(T) \otimes R$  does not belong to  $\mathbf{k}(T)[\hat{R}^p]$ . Applying 2.2 to  $u - T \in \hat{R}$ , we obtain that  $u - T - \theta$  is irreducible in  $\hat{R}$  for all  $\theta \in \mathbf{k}(T)$ ; in particular,

$$(15) \quad u - \lambda \text{ is irreducible in } R, \text{ for all } \lambda \in \mathbf{k}.$$

Identifying the  $\mathbf{k}(T)$ -algebra  $\hat{R}/(u - T)\hat{R}$  with the  $\mathbf{k}(u)$ -algebra  $\mathbf{k}(u)[R]$ , we obtain from the first part of 2.2 that there exist  $v \in \mathbf{k}(u)[R]$  and  $n \geq 0$  such that  $R^{p^n} \subseteq \mathbf{k}(u)[v]$ . We may in fact choose  $v$  in  $R$  so

$$(16) \quad \text{There exist } v \in R \text{ and } n \geq 0 \text{ such that } R^{p^n} \subseteq \mathbf{k}(u)[v].$$

Hence the result follows from 2.5. □

### 3. PROOF OF THEOREM B

Because all valuation rings of  $\mathbf{k}(t)/\mathbf{k}$  are known explicitly, the reader will have no difficulty verifying the following:

**Lemma 3.1.** *Let  $Q$  be a normal  $\mathbf{k}$ -domain with one purely inseparable place at infinity, and such that  $\text{qt } Q = \mathbf{k}(t) = \mathbf{k}^{(1)}$ . If we define  $Q_i = Q \cap \mathbf{k}(t^{p^i})$ , then:*

1. *For each  $i \geq 0$ ,  $Q_i$  is a normal  $\mathbf{k}$ -domain with one purely inseparable place at infinity and satisfies  $\text{qt } Q_i = \mathbf{k}(t^{p^i})$ .*
2. *Define an integer  $j$  by  $[\kappa, \mathbf{k}] = p^j$ , where  $\kappa$  is the residue field of the unique valuation ring of  $\mathbf{k}(t)/\mathbf{k}$  which does not contain  $Q$ . Then  $Q_i = \mathbf{k}^{[1]}$  for all  $i \geq j$ .*

**Proposition 3.2.** *Suppose that  $\mathbf{k}$  is algebraically closed and that  $u \in R$  satisfies*

1.  *$u$  has one place at infinity; and*
2. *there exist  $\varphi \in \text{qt } R$  and  $n \geq 0$  such that  $\mathbf{k}(u, \varphi) \supseteq R^{p^n}$ .*

*Then  $u$  is a  $p$ -generator of  $R$ .*

*Proof.* The assumption that  $u$  has one place at infinity implies

$$(17) \quad u - \lambda \text{ is irreducible in } R, \text{ for all } \lambda \in \mathbf{k},$$

$$(18) \quad u - T \in \mathbf{k}(T) \otimes R \text{ has one purely inseparable place at infinity,}$$

where  $T$  is an indeterminate. Indeed, (18) is part of the Main Theorem of [5] and (17) follows from the fact that  $R/uR$  has trivial units.

Let  $\varphi$  and  $n$  be as in the statement; then the normal ring  $C = R \cap \mathbf{k}(u, \varphi)$  contains  $R^{p^n}$ . We intend to apply 3.1 to the  $\mathbf{k}(u)$ -algebra  $Q = \mathbf{k}(u)[C]$ . This is clearly a normal  $\mathbf{k}(u)$ -domain and, by Lüroth's Theorem and the inclusions  $\mathbf{k}(u) \subset \text{qt } Q \subseteq \mathbf{k}(u, \varphi)$ , we have  $\text{qt } Q = \mathbf{k}(u, t) = \mathbf{k}(u)^{(1)}$  for some  $t \in \text{qt } R$ . Observe that (18) means that the  $\mathbf{k}(u)$ -algebra  $\mathbf{k}(u)[R]$  has one p.i. place at infinity; together with the inclusions  $\mathbf{k}(u)[R^{p^n}] \subseteq Q \subseteq \mathbf{k}(u)[R]$ , this implies that  $Q$  has one p.i. place at infinity.

By 3.1, it therefore follows that  $Q \cap \mathbf{k}(u, t^{p^i}) = \mathbf{k}(u)^{[1]}$  for  $i$  sufficiently large. So  $Q \cap \mathbf{k}(u, t^{p^i}) = \mathbf{k}(u)[v]$  for some  $v \in Q$  and, clearly, we may arrange that  $v \in R$ . Now  $\mathbf{k}(u)[v]$  contains  $R^{p^{n+i}}$ , so we are done by (17) and 2.5.  $\square$

*Proof of Theorem B.* By a straightforward argument involving 1.7 and the Extension Lemma, we may assume that  $\mathbf{k}$  is algebraically closed. Let  $s \geq 0$  be such that  $u \in R^{p^s} \setminus R^{p^{s+1}}$  and write  $R_s = R^{p^s}$ . Observe that  $u$  is a  $p$ -line of  $R_s$  (by part 4 of 2.2) and that  $\mathbf{k}(u, \varphi^{p^s}) \supseteq R_s^{p^n}$ ; since it suffices to prove that  $u$  is a  $p$ -generator of  $R_s$ , we may assume that  $u \notin R^p$ . In particular,  $u$  has one place at infinity (by 2.3), so the result follows from 3.2.  $\square$

## REFERENCES

1. S.M. Bhatwadekar and A.K. Dutta, *Linear planes over a D.V.R.* To appear in J. of Algebra.
2. D. Daigle, *A property of polynomial curves over a field of positive characteristic.* Proc. Amer. Math. Soc. **109** (1990), 887–894. MR **90k**:14030
3. D. Daigle, *Purely inseparable extensions of  $\mathbf{k}[X, Y]$ .* To appear in Proc. Amer. Math. Soc.
4. Paul Eakin and William Heinzer, *A cancellation problem for rings.* Conference on Commutative Algebra, Lecture Notes in Mathematics No 311, Springer-Verlag (1973), 61–77. MR **50**:2157
5. R. Ganong, *On plane curves with one place at infinity.* J. Reine Angew. Math. **307/308** (1979), 173–193. MR **82e**:14036
6. T.T. Moh, *On the classification problem of embedded lines in characteristic  $p$ .* Algebraic Geometry and Commutative Algebra in Honor of Masayoshi NAGATA, Kinokuniya (1987), 267–279. MR **90a**:14004

7. K.P. Russell, *Field generators in two variables*. J. Math. Kyoto Univ. **15** (1975), 555–571. MR **53**:2946
8. K.P. Russell and A. Sathaye, *On finding and cancelling variables in  $\mathbf{k}[X, Y, Z]$* . J. of Algebra **57** (1979), 151–166. MR **80j**:14030

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OTTAWA, OTTAWA, CANADA K1N 6N5  
*E-mail address*: [daniel@zenon.mathstat.uottawa.ca](mailto:daniel@zenon.mathstat.uottawa.ca)