#### PLANE FROBENIUS SANDWICHES OF DEGREE p

#### D. DAIGLE

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. Let k be a field of characteristic p > 0 and A, R polynomial rings in two indeterminates over k. It is shown that, if  $\mathbf{k}[R^p] \subset A \subset R$  (strictly) then there exist  $x, y \in R$  such that  $R = \mathbf{k}[x, y]$  and  $A = \mathbf{k}[x^p, y]$ . (The case where k is algebraically closed was proved by Ganong in 1979.) Another result is obtained in the situation where  $R^{p^n} \subseteq A \subseteq R$ .

One aim of the paper is to prove the following

**Theorem.** Let  $\mathbf{k}$  be a field of characteristic p > 0 and A, R polynomial rings in two indeterminates over  $\mathbf{k}$ . If  $\mathbf{k}[R^p] \subset A \subset R$  (strictly) then there exist  $x, y \in R$  such that  $R = \mathbf{k}[x, y]$  and  $A = \mathbf{k}[x^p, y]$ .

The fact that the result holds when  $\mathbf{k}$  is algebraically closed was proved by Ganong in [4]; we will refer to that fact as *Ganong's theorem*, and will make use of it in our proof. It was also known that Ganong's argument could prove the result under the weaker assumption that  $\mathbf{k}$  is a perfect field, but apparently the general case was not known.

The method used in [4] (namely, the HN-expansions, see [5]) is not available in the general case, because one has to deal with curves with a possibly nonrational place at infinity. The main ingredient in our proof (besides Ganong's theorem) is a result on pairs of polynomials in one indeterminate over an integral domain of positive characteristic (Proposition 1.2), to which the first section is devoted. Section 2 gives two applications of (1.2), the second of which being the proof of the above theorem. The other application (Proposition 2.3) is concerned with the more general "Frobenius sandwich" situation where  $R^{p^n} \subseteq A \subseteq R$ .

We will need some basic facts about automorphisms of k[X, Y] and plane curves with one place at infinity; these can be found in [1, 2] or [5].

# 1. PAIRS OF POLYNOMIALS IN ONE INDETERMINATE

Throughout this section let S be an integral domain containing a field  $\mathbf{k}$ , let T, T<sub>1</sub>, and T<sub>2</sub> be indeterminates, let G be the group of k-automorphisms of  $\mathbf{k}[T_1, T_2]$ , and let E be the set  $(S[T] \times S[T]) \setminus (S \times S)$ . Given  $\theta \in G$  and

Received by the editors July 2, 1991.

<sup>1991</sup> Mathematics Subject Classification. Primary 13F20.

Supported by a grant from NSERC Canada.

 $(x, y) \in E$  we put  $\theta(x, y) = (\alpha(x, y), \beta(x, y)) \in E$ , where  $\alpha = \theta^{-1}(T_1)$ and  $\beta = \theta^{-1}(T_2)$ . This defines a left-action of G on E, and we tacitly refer to this action whenever we speak of an orbit. Note that  $(x, y), (x', y') \in E$ belong to the same orbit if and only if  $(x', y') = (\alpha(x, y), \beta(x, y))$  for some  $\alpha, \beta \in \mathbf{k}[T_1, T_2]$  such that  $\mathbf{k}[\alpha, \beta] = \mathbf{k}[T_1, T_2]$ .

Given  $x \in S[T]$ , the formal derivative dx/dT will be denoted  $\dot{x}$ ; let deg x be the T-degree of x and, in particular, let deg 0 = 0. The *bidegree* of  $(x, y) \in E$  is bideg(x, y) = (deg x, deg y). A pair (m, n) of nonnegative integers is nonprincipal if either mn = 0, or  $m \nmid n$  and  $n \nmid m$ ; otherwise (m, n) is principal.

**Lemma 1.1.** Suppose (x, y),  $(x', y') \in E$  belong to the same orbit, have nonprincipal bidegrees, and satisfy  $\deg x < \deg y$  and  $\deg x' < \deg y'$ . If  $\alpha, \beta \in \mathbf{k}[T_1, T_2]$  are such that  $\mathbf{k}[\alpha, \beta] = \mathbf{k}[T_1, T_2]$  and  $(x', y') = (\alpha(x, y), \beta(x, y))$ , then  $\alpha = aT_1 + b$  and  $\beta = cT_2 + f(T_1)$  for some  $a, c \in \mathbf{k}^* = \mathbf{k} \setminus \{0\}$ ,  $b \in \mathbf{k}$ , and  $f \in \mathbf{k}[T_1]$  such that  $\deg f \deg x < \deg y$ . Consequently,

$$x' = ax + b$$
,  $y' = cy + f(x)$ ,  $bideg(x, y) = bideg(x', y')$ .

*Proof.* This can be found, in one form or another, in the literature (see [2] for instance). At any rate, it is very well known if  $\mathbf{k} = S$ ; we reduce to that case by noting that  $\alpha, \beta \in \mathbf{k}[T_1, T_2]$  also satisfy  $K[\alpha, \beta] = K[T_1, T_2]$ , where K is the field of fractions of S.  $\Box$ 

Call an orbit  $\mathscr{O}$  monic if the leading coefficient of x is in  $\mathbf{k}^*$  whenever  $(x, y) \in \mathscr{O}$  and deg x > 0 (and note that  $(x, y) \in \mathscr{O}$  implies  $(y, x) \in \mathscr{O}$ ). Clearly, every monic orbit contains an element (x, y) with nonprincipal bidegree.

**Proposition 1.2.** Assume that **k** has characteristic p > 0, let  $S_0$  be a **k**-subalgebra of S that contains  $\mathbf{k}[S^p]$ , and let  $\mathcal{O}$  be a monic orbit that contains an element (u, v) such that  $u \in S_0[T^p]$ .

(1) There exists  $(u, v) \in \mathscr{O}$  such that  $u \in S_0[T^p]$  and whose bidegree (m, n) satisfies either (a) (m, n) is nonprincipal, or (b) m > n > 0, n|m, and  $pn \nmid m$ .

(2) Suppose that  $\mathscr{O} \not\subseteq S[T^p] \times S[T^p]$ , that  $(x, y) \in \mathscr{O}$  has nonprincipal bidegree, and that  $\deg x < \deg y$ . Then either  $x \in S_0[T^p]$ , or  $y + f(x) \in S_0[T^p]$  for some  $f \in \mathbf{k}[T_1]$  such that  $\deg f \deg x < \deg x + \deg y$ .

*Remark.* From the special case " $S = \mathbf{k}$ " of this proposition, one may deduce (2.2) of [3] and hence the main theorem of that paper. In the applications contained in the next section, however, S is a polynomial ring in one indeterminate over  $\mathbf{k}$ .

*Proof.* For the first assertion, let  $(u, v) \in \mathcal{O}$  be such that  $u \in S_0[T^p]$ , let (m, n) = bideg(u, v), and assume that neither of conditions (a), (b) holds. Then  $mn \neq 0$  and either m|n or pn|m. Define (u', v') as follows.

If m|n, let d = n/m and note that there exists  $\lambda \in \mathbf{k}^*$  such that  $\deg(v - \lambda u^d) < \deg v$ ; define  $(u', v') = (u, v - \lambda u^d)$ .

If pn|m, let d = m/(pn) and note that there exists  $\lambda \in \mathbf{k}^*$  such that  $\deg(u - \lambda v^{dp}) < \deg u$ ; define  $(u', v') = (u - \lambda v^{dp}, v)$ .

So in each case we obtain  $(u', v') \in \mathscr{O}$  such that  $u' \in S_o[T^p]$  and  $\deg u' + \deg v' < \deg u + \deg v$ . Clearly, this proves the first assertion.

For the second part, choose  $(u, v) \in \mathcal{O}$  such that  $u \in S_0[T^p]$  and whose bidegree (m, n) satisfies one of the conditions (a), (b) of the first part.

Suppose (m, n) is nonprincipal. If m < n then, by (1.1), there exist  $a \in \mathbf{k}^*$  and  $b \in \mathbf{k}$  such that x = au + b, hence  $x \in S_0[T^p]$ . If m > n then u = ay + f(x) for some  $a \in \mathbf{k}^*$  and  $f \in \mathbf{k}[T_1]$ , as in (1.1), so we are done again.

So we may assume that m > n > 0, n|m, and  $pn \nmid m$ . Let d = m/n; then d > 1 and  $p \nmid d$ . Let  $g \in \mathbf{k}[T_1]$  be a polynomial of degree d such that, if we define w = u - g(v), then either  $\deg w = 0$  or  $\deg v \nmid \deg w$ . We claim that  $\deg w > \deg v$ , which implies that  $\operatorname{bideg}(v, w)$  is nonprincipal. To see that, begin with the observation that  $v \notin S[T^p]$ , since  $u \in S_0[T^p]$  and  $\mathscr{O} \nsubseteq S[T^p] \times S[T^p]$ . Hence  $\dot{v} \neq 0$ ,  $\dot{w} = -g'(v)\dot{v}$ , and the derivative  $g' \in \mathbf{k}[T_1]$ has degree d - 1. It follows that

$$\deg w > \deg \dot{w} \ge \deg g'(v) = (d-1)\deg v,$$

and, in particular,  $\deg w > \deg v$ , as claimed.

By (1.1) we obtain bideg(v, w) = bideg(x, y), y = cw + h(v), and v = ax + b, for some  $a, c \in k^*$ ,  $b \in k$ , and  $h \in k[T_1]$ . Setting

$$f(T_1) = cg(aT_1 + b) - h(aT_1 + b) \in \mathbf{k}[T_1]$$

gives  $y + f(x) = cu \in S_0[T^p]$ , and obviously deg  $f \le \max(\deg g, \deg h)$ . Now (1.1) also says that deg  $h \deg x < \deg y$ , and on the other hand, the inequality  $(d-1) \deg v < \deg w$  is equivalent to deg  $g \deg x < \deg x + \deg y$ .  $\Box$ 

### 2. FROBENIUS SANDWICHES

In this section, **k** denotes a field of characteristic p > 0 and  $R = \mathbf{k}^{[2]}$  (for a **k**-algebra A, the notation  $A = \mathbf{k}^{[n]}$  means that A is a polynomial ring in n indeterminates over **k**).

A coordinate system of R is a pair  $(X, Y) \in R \times R$  such that  $R = \mathbf{k}[X, Y]$ ; the set of all coordinate systems of R is denoted  $\Gamma(R)$ . A variable of R is an element u of R such that  $R = \mathbf{k}[u, v]$  for some v. If  $(X, Y) \in \Gamma(R)$  has been chosen then, given  $F \in R$ ,  $\deg_Y F$  and  $lc_Y F$  denote, respectively, the degree and leading coefficient of F, where F is regarded as a polynomial in Y with coefficients in  $\mathbf{k}[X]$  (and similarly for  $\deg_X F$  and  $lc_X F$ ); we also write  $F_X$  and  $F_Y$  for the partial derivatives  $\partial F/\partial X$  and  $\partial F/\partial Y$ .

By a subalgebra of R we mean a subring that contains **k**. Let  $\Sigma(R)$  be the set of subalgebras  $A = \mathbf{k}^{[2]}$  of R such that  $A \supseteq R^{p^n}$  for some  $n \ge 0$ .

**Lemma 2.1.** Suppose  $u \in R$  is a variable of some element of  $\Sigma(R)$ . Then, for each  $(X, Y) \in \Gamma(R)$ , either  $\deg_Y u = 0$  or  $\operatorname{lc}_Y u \in \mathbf{k}^*$ .

*Proof.* Suppose deg<sub>Y</sub> u > 0. There exist  $v \in R$  and an integer  $n \ge 0$  such that  $X^{p^n}$ ,  $Y^{p^n} \in \mathbf{k}[u, v] \subseteq \mathbf{k}[X, Y]$ . Let  $\overline{\mathbf{k}}$  be the algebraic closure of  $\mathbf{k}$ , and let  $u_0$  be the irreducible element of  $\overline{R} = \overline{\mathbf{k}}[X, Y]$  such that  $u = u_0^{p^k}$  for some integer  $k \ge 0$ . Then deg<sub>Y</sub>  $u_0 > 0$  and  $u_0$  is a variable of some element of  $\Sigma(\overline{R})$  (namely,  $\overline{\mathbf{k}}[u_0, v] \in \Sigma(\overline{R})$  since  $X^{p^n}$ ,  $Y^{p^n} \in \mathbf{k}[u, v] \subseteq \overline{\mathbf{k}}[u_0, v]$ ).

In other words, we may assume that  $\mathbf{k} = \overline{\mathbf{k}}$  and that  $u \in R$  is irreducible. Since the above inclusions imply that  $(R/uR)^{p^n} \subseteq \mathbf{k}^{[1]} \subseteq R/uR$ , i.e., that R/uR is purely inseparable over  $\mathbf{k}^{[1]}$ , we conclude that u has one place at infinity (rational, since  $\mathbf{k} = \overline{\mathbf{k}}$ ), and the result follows (see [5, (5.2.1)] for instance).  $\Box$  2.2. Given  $A \in \Sigma(R)$  and  $(X, Y) \in \Gamma(R)$ , we may put ourselves in the context of Proposition 1.2 by letting  $S = \mathbf{k}[X]$ ,  $S_0 = \mathbf{k}[X^p]$ , T = Y, and  $\mathscr{O} = \Gamma(A)$ . Observe that S[T] = R,  $S_0[T^p] = \mathbf{k}[X^p, Y^p] = \mathbf{k}[R^p]$  and that the orbit  $\mathscr{O}$ is monic by the above lemma. Moreover, the condition  $\mathscr{O} \not\subseteq S[T^p] \times S[T^p]$  is equivalent to  $A \not\subseteq \mathbf{k}[X, Y^p]$ . We will use the sentence "apply (1.2) to A, R, and (X, Y)" to indicate that this viewpoint is adopted and that we are making use of (1.2).

**Proposition 2.3.** Let  $A \in \Sigma(R)$ , let  $\overline{\mathbf{k}}$  be the algebraic closure of  $\mathbf{k}$ ,  $\overline{A} = \overline{\mathbf{k}} \otimes_{\mathbf{k}} A$ and  $\overline{R} = \overline{\mathbf{k}} \otimes_{\mathbf{k}} R$ . Then  $\overline{A} \in \Sigma(\overline{R})$  and the following are equivalent:

- (1) some variable of A is in  $\mathbf{k}[R^p]$ ,
- (2) some variable of  $\overline{A}$  is in  $\overline{R}^p$

*Proof.*  $\overline{R} = \overline{k}^{[2]}$  and  $\overline{A} \in \Sigma(\overline{R})$  are easily verified, and (1) clearly implies (2). Assume (2) holds. Since (1) holds trivially if  $A \subseteq k[R^p]$ , let us assume that

 $A \nsubseteq \mathbf{k}[R^p]$ . So we may choose  $(X, Y) \in \Gamma(R)$  such that  $A \nsubseteq \mathbf{k}[X, Y^p]$ . We claim that it suffices to find a variable w of A such that  $w_Y = 0$ . Indeed, let  $t \in A$  be such that  $(w, t) \in \Gamma(A)$ . From  $A \neq R$  (because (2) holds) and  $A \in \Sigma(R)$ , one deduces the nullity of the Jacobian:  $0 = w_X t_Y - w_Y t_X = w_X t_Y$ . Since  $A \nsubseteq \mathbf{k}[X, Y^p]$ , it follows that  $t_Y \neq 0$  and, consequently,  $w_X = 0$ , i.e.,  $w \in \mathbf{k}[R^p]$ .

Choose  $(x, y) \in \Gamma(A)$  such that  $(\deg_Y x, \deg_Y y)$  is nonprincipal and  $\deg_Y x < \deg_Y y$ ; by the previous paragraph, we may assume that  $x_Y \neq 0$ . We will now apply the second part of (1.2) to  $\overline{A}, \overline{R}$ , and  $(X, Y) \in \Gamma(\overline{R})$  (see (2.2)); note that the "k" of (1.2) is  $\overline{k}$  here,  $A \notin k[X, Y^p]$  implies  $\mathscr{O} \notin S[T^p] \times S[T^p]$ and, since (2) holds, some  $(u, v) \in \mathscr{O}$  satisfies  $u \in S_0[T^p] = \overline{R}^p$ . We conclude that  $y + f(x) \in \overline{R}^p$  for some  $f \in \overline{k}[T_1]$ , since the other case  $(x \in \overline{R}^p)$  cannot happen here. Clearly, f may be chosen so that  $p \nmid i$  whenever  $T_1^i$  occurs in f with a nonzero coefficient.

We claim that  $f \in \mathbf{k}[T_1]$ . Begin by observing that

$$0 = \frac{\partial}{\partial Y}(y + f(x)) = y_Y + f'(x)x_Y$$

and  $x_Y \neq 0$  imply that  $f'(x) \in \operatorname{qt} R \cap \overline{R} = R$ , where  $\operatorname{qt} R$  is the field of fractions of R. So the derivative f' is in  $\mathbf{k}[T_1]$ , in view of the following easy fact: If  $g \in \overline{\mathbf{k}}[T_1]$  satisfies  $g(\alpha) \in R$  for some  $\alpha \in R \setminus \mathbf{k}$  then  $g \in \mathbf{k}[T_1]$ . Because of our choice of f, we thus have  $f \in \mathbf{k}[T_1]$ , as claimed. Consequently, y + f(x)is a variable of A and belongs to  $\mathbf{k}[R^p]$ .  $\Box$ 

Proof of the theorem. If  $\overline{\mathbf{k}}$ ,  $\overline{A}$ , and  $\overline{R}$  are defined as in the above proposition, then  $\overline{R}^{p} \subset \overline{A} \subset \overline{R}$  (strictly) so, by Ganong's theorem, some variable of  $\overline{A}$  is in  $\overline{R}^{p}$ . Thus by (2.3) some variable of A is in  $\mathbf{k}[R^{p}]$ .

Choose  $(X, Y) \in \Gamma(R)$  and apply the first part of (1.2) to A, R, and (X, Y). By the previous paragraph,  $\mathscr{O}$  contains an element (u, v) such that  $u \in S_0[T^p] = \mathbf{k}[R^p]$  and, by (1.2), we may arrange that the pair  $(m, n) = (\deg_Y u, \deg_Y v)$  satisfies one of the following:

- (a) (m, n) is nonprincipal; or
- (b) m > n > 0, n|m, and  $pn \nmid m$ .

Note that  $\overline{A} = \overline{\mathbf{k}}[u, v]$  and  $u \in \overline{R}^p$  imply that  $\overline{R} = \overline{\mathbf{k}}[u^{1/p}, v]$ , thus n|(m/p) or (m/p)|n, by the Automorphism Theorem for  $\overline{k}^{[2]}$ . Since these divisibility conditions are incompatible with (b), (m, n) must be nonprincipal.

If mn = 0 then some variable of A is in k[X] and the desired conclusion easily follows. So let us assume that  $mn \neq 0$ .

Since  $n \nmid m$ , we have  $n \nmid (m/p)$ , hence (m/p)|n. Consider the integer d = n/(m/p); then d > 1 and  $p \nmid d$ . We may certainly assume that  $lc_Y v = 1$ ; thus the approximate root  $\rho = App_Y^d(v)$  is defined and belongs to R since v does (see [5, (1.7)]). On the other hand, the conditions

$$\overline{\mathbf{k}}[X, Y] = \overline{\mathbf{k}}[u^{1/p}, v]$$
 and  $\frac{\deg_Y v}{\deg_Y u^{1/p}} = d > 1$ 

(together with well-known properties of coordinate systems) imply that  $\overline{R} = \overline{k}[\rho, v]$ . Thus

$$R = \overline{\mathbf{k}}[\rho, v] \cap R = \mathbf{k}[\rho, v],$$

and it easily follows that  $A = \mathbf{k}[\rho^p, v]$ .  $\Box$ 

#### ACKNOWLEDGMENT

I thank R. Ganong for reading the manuscript and commenting on it.

## References

- 1. S. Abhyankar, *Lectures on expansion techniques in algebraic geometry* (Notes by B. Singh), Tata Lecture Notes, vol. 57, Tata Inst. Fund. Res., Bombay, 1977.
- 2. S. Abhyankar and B. Singh, *Embeddings of certain curves in the affine plane*, Amer. J. Math. **100** (1978), 99-175.
- 3. D. Daigle, A property of polynomial curves over a field of positive characteristic, Proc. Amer. Math. Soc. 109 (1990), 887–894.
- 4. R. Ganong, Plane Frobenius sandwiches, Proc. Amer. Math. Soc. 84 (1982), 474-478.
- 5. K. P. Russell, Hamburger-Noether expansions and approximate roots of polynomials, Manuscripta Math. 31 (1980), 25–95.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF OTTAWA, OTTAWA, CANADA K1N 6N5 *E-mail address*: ddaigle@Acadvm1.uottawa.ca