PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 116, Number 1, September 1992

LINEAR DISJOINTNESS OF POLYNOMIALS

SHREERAM S. ABHYANKAR

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. It is shown that any two bivariate polynomials can be made linearly disjoint by applying a linear transformation to one of the variables in one of the polynomials. From this it is deduced that the algebraic fundamental group of an affine line is closed relative to direct products.

1. INTRODUCTION

Let k be an algebraically closed field, and let there be given any two nonconstant monic separable polynomials $f(X, Y)$ and $g(X, Y)$ in Y with coefficients in $k(X)$. Then I shall prove:

Disjointness Theorem. *For most a, b in k with $a \neq 0$, the splitting fields of the polynomials $f(X, Y)$ and $g(aX + b, Y)$ over $k(X)$ are linearly disjoint over $k(X)$.*[1]

Let L_k be the affine line over k, and let $\pi_A(L_k)$ be the algebraic fundamental group of L_k, i.e., $\pi_A(L_k)$ is the set of all finite Galois groups of unramified coverings of L_k. Given any two members H and J of $\pi_A(L_k)$, we can find $f(X, Y)$ and $g(X, Y)$ in $k[X, Y]$ such that H and J are the respective Galois groups of the splitting fields of $f(X, Y)$ and $g(X, Y)$ over $k(X)$, and such that no valuation of $k(X)/k$, other than the valuation $X = \infty$, is ramified in these splitting fields. Clearly J is also the Galois group of the splitting field of $g(aX+b, Y)$ over $k(X)$ and no valuation of $k(X)/k$, other than the valuation $X = \infty$, is ramified in the said splitting field. It follows that no valuation of $k(X)/k$, other than the valuation $X = \infty$, is ramified in the splitting field of $f(X, Y)g(aX + b, Y)$ over $k(X)$, and hence the Galois group of the said splitting field belongs to $\pi_A(L_k)$. Finally, if the splitting fields of $f(X, Y)$ and $g(aX + b, Y)$ over $k(X)$ are linearly disjoint over $k(X)$, then Galois group of the splitting field of $f(X, Y)g(aX+b, Y)$ over $k(X)$ is the direct product $H \times J$. Thus the Disjointness Theorem implies the following statement (FG8) for which different (unpublished) proofs were also obtained by Mulay, Sathaye,

Received by the editors February 13, 1991.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12F10, 14H30; Secondary 12F12, 14E22.

This work was partly supported by NSF grant DMS 88-16286.

[1]Here "most" means there exists $0 \neq \phi(X, Y) \in k[X, Y]$ such that our assertion is true for all a, b in k for which $\phi(a, b) \neq 0$.

0002-9939/92 \$1.00 + \$.25 per page

and Serre; for the companion statements (FG1) to (FG7) concerning $\pi_A(L_k)$ see [A]; it may be noted that (FG8) is vacuous in case k is of characteristic zero because then L_k has no nontrivial unramified extension.

(FG8) $\pi_A(L_k)$ *is closed with respect to direct products.*

Turning to the proof of the Disjointness Theorem, in §2, I shall first prove the following lemma and then, in §3 I shall deduce the Theorem from it.

Lemma. *Let K be a finitely generated field extension of k of transcendence degree one, and let $x \in K$ with $x \notin k$. Assume that either the genus of K/k is nonzero or $K/k(x)$ is not purely inseparable. Then for most a, b in k we have $ax+b \notin \{\tau(x) : \tau \in \mathrm{Aut}_k K\}$ where $\mathrm{Aut}_k K$ is the group of all k-automorphisms of K.*

2. Lemma

To prove the lemma, let $v_1, v_2, \ldots, v_m$ be the poles of x in K, i.e., $v_1, v_2, \ldots, v_m$ are the distinct valuations of K/k for which the value of x is negative. Note that then m is a positive integer. Also note that every $\tau \in \mathrm{Aut}_k K$ permutes the set of all valuations of K/k, and if $\tau(x) = ax + b$ with a, b in k then τ must map the set $\{v_1, v_2, \ldots, v_m\}$ onto itself.

It is well known that if the genus of K/k is nonzero then, for any valuation v of K/k, the group of all $\tau \in \mathrm{Aut}_k K$ that map v onto itself is a finite group; for instance see [IT]. It follows that if the genus of K/k is nonzero then the group of all $\tau \in \mathrm{Aut}_k K$ that map the set $\{v_1, v_2, \ldots, v_m\}$ onto itself is a finite group, and hence for most a, b in k we have $ax + b \notin \{\tau(x) : \tau \in \mathrm{Aut}_k K\}$.

Henceforth assume that the genus of K/k is zero, and $K/k(x)$ is not purely inseparable. Now K/k is simple transcendental and, by applying a suitable fractional linear transformation to a given generator of K/k, we can find $t \in K$ such that $K = k(t)$, and the valuation $t = \infty$ of K/k is v_1, but the valuation $t = 0$ of K/k is not in the set $\{v_1, v_2, \ldots, v_m\}$. It follows that $x = r(t)/s(t)$ where $r(t)$ and $s(t)$ are nonzero coprime polynomials in t with coefficients in k such that $s(t)$ is monic and upon letting d and e to be the respective degrees of $r(t)$ and $s(t)$ we have $0 \le e < d$. Now clearly $s(t) = \prod_{i=2}^{m}(t - \beta_i)^{\varepsilon_i}$ where $\varepsilon_2, \varepsilon_3, \ldots, \varepsilon_m$ are positive integers and $\beta_2, \beta_3, \ldots, \beta_m$ are pairwise distinct nonzero elements in k such that $v_i(t - \beta_i) = 1$ for $2 \le i \le m$. Also $r(t) = \alpha_0 t^d + \alpha_1 t^{d-1} + \cdots + \alpha_d$ where $\alpha_0, \alpha_1, \ldots, \alpha_d$ are elements in k with $\alpha_0 \neq 0$.

Let $\tau \in \mathrm{Aut}_k K$ be such that $\tau(x) = ax + b$ for some a, b in k with $a \neq 0$. Then τ must send v_1 to v_j for some j with $1 \le j \le m$. Since every k-automorphism of K sends t to a fractional linear expression in t, we must have $\tau(t) = (\lambda t + \mu)/\nu_j$ where $\nu_j = 1$ or $t - \beta_j$ depending upon whether $j = 1$ or $j > 1$, and where λ and μ are elements in k, at least one of which is nonzero, such that $\lambda t + \mu$ does not divide ν_j in $k[t]$. If $j = 1$ then obviously $\lambda \neq 0$. If $j \neq 1$ then there is a unique j' with $2 \le j' \le m$ such that τ sends $v_{j'}$ to v_1 and hence such that $v_1(\tau(t - \beta_{j'})) = 1$; since

$$\tau(t - \beta_{j'}) = \tau(t) - \beta_{j'} = \frac{(\lambda - \beta_{j'})t + (\mu + \beta_j \beta_{j'})}{t - \beta_j},$$

we get $\lambda = \beta_{j'} \neq 0$. Thus always $\lambda \neq 0$.

Now

$$\tau(x) = ax + b = \frac{ar(t) + bs(t)}{s(t)}$$

where num (= numerator) and den (= denominator) are nonzero coprime members of $k[t]$ such that den is monic and deg(num) $= d > e =$ deg(den), and also

$$\tau(x) = \frac{r(\tau(t))}{s(\tau(t))} = \frac{\nu_j^d r(\tau(t))}{\nu_j^d s(\tau(t))}$$

where nnum (= new numerator) $= \nu_j^d r(\tau(t))$ and nden (= new denominator) $= \nu_j^d s(\tau(t))$ are nonzero members of $k[t]$ such that deg(nnum) $\leq d$. Therefore, upon letting γ to be the leading coefficient of nden we have

$$0 \neq \frac{\text{nnum}}{\text{num}} = \frac{\text{nden}}{\text{den}} = \gamma \in k.$$

Now

$$\text{nden} = \begin{cases} (t - \beta_j)^{d-e}(\mu - \beta_j\beta_{j'})^{\varepsilon_{j'}} \\ \quad \times \prod_{2\leq i\leq m \text{ with } i\neq j'} [(\beta_{j'} - \beta_i)t + (\mu - \beta_j\beta_i)]^{\varepsilon_i} & \text{if } j \neq 1, \\ \prod_{2\leq i\leq m} (\lambda t + \mu - \beta_i)^{\varepsilon_i} & \text{if } j = 1, \end{cases}$$

and hence

$$\gamma = \begin{cases} \gamma_{jj'}(\mu) & \text{if } j \neq 1, \\ \lambda^e & \text{if } j = 1, \end{cases}$$

where for all l, l' with $1 \leq l \leq m$ and $1 \leq l' \leq m$ and for all $\mu' \in k$ we have put

$$\gamma_{ll'}(\mu') = (\mu' - \beta_l\beta_{l'})^{\varepsilon_{l'}} \prod_{2\leq i\leq m \text{ with } i\neq l'} (\beta_{l'} - \beta_i)^{\varepsilon_i}.$$

If $j \neq 1$ then

$$\frac{\sum_{i=0}^d \alpha_i(\beta_{j'}t + \mu)^{d-i}(t - \beta_j)^i}{a\sum_{i=0}^d \alpha_i t^{d-i} + b\prod_{i=2}^m (t - \beta_i)^{\varepsilon_i}} = \frac{\text{nnum}}{\text{num}} = \gamma_{jj'}(\mu),$$

and hence for this case it suffices to note that, given any l, l' with $1 \leq l \leq m$ and $1 \leq l' \leq m$, obviously there exists $0 \neq \phi_{ll'}(X, Y) \in k[X, Y]$ such that $\phi_{ll'}(a', b') = 0$ for all a', b' in k for which $a' \neq 0$ and

$$\frac{\sum_{i=0}^d \alpha_i(\beta_{j'}t + \mu')^{d-i}(t - \beta_j)^i}{a'\sum_{i=0}^d \alpha_i t^{d-i} + b'\prod_{i=2}^m (t - \beta_i)^{\varepsilon_i}} = \gamma_{jj'}(\mu') \quad \text{for some } \mu' \in k.$$

If $j = 1 < m$ then

$$\frac{\lambda^e \prod_{i=2}^m \left[t - \frac{\beta_i - \mu}{\lambda}\right]^{\varepsilon_i}}{\prod_{i=2}^m (t - \beta_i)^{\varepsilon_i}} = \frac{\text{nden}}{\text{den}} = \lambda^e,$$

and hence for some c with $2 \leq c \leq m$ we must have $\beta_2 = (\beta_c - \mu)/\lambda$, i.e., $\mu = \beta_c - \lambda\beta_2$, and therefore

$$\frac{\sum_{i=0}^d \alpha_i(\lambda t + \beta_c - \lambda\beta_2)^{d-i}}{a\sum_{i=0}^d \alpha_i t^{d-i} + b\prod_{i=2}^m (t - \beta_i)^{\varepsilon_i}} = \frac{\text{nnum}}{\text{num}} = \lambda^e;$$

hence in this case it suffices to note that, given any l with $2 \leq l \leq m$, obviously there exists $\phi_l(X, Y) \in k[X, Y]$ such that $\phi_l(a', b') = 0$ for all a', b' in k for which $a' \neq 0$ and

$$\frac{\sum_{i=0}^{d} \alpha_i(\lambda' t + \beta_c - \lambda' \beta_2)^{d-i}}{a' \sum_{i=0}^{d} \alpha_i t^{d-i} + b' \prod_{i=2}^{m}(t - \beta_i)^{\varepsilon_i}} = \lambda'^e \quad \text{for some } 0 \neq \lambda' \in k.$$

Thus if $m \neq 1$ then upon letting

$$\phi(X, Y) = \left[\prod_{l=1}^{m} \phi_l(X, Y)\right] \left[\prod_{l=1}^{m} \prod_{l'=1}^{m} \phi_{ll'}(X, Y)\right],$$

we see that $0 \neq \phi(X, Y) \in k[X, Y]$ is such that $\phi(a', b') = 0$ for all a', b' in k for which $a'x + b' \in \{\tau'(x) : \tau' \in \mathrm{Aut}_k K\}$.

So henceforth assume that $m = 1$. Then we must have $j = 1$ and $e = 0$. If $\operatorname{char} k = 0$ then let $q = 1$, and if $\operatorname{char} k = p \neq 0$ then let q be the largest power of p such that $r(t) = R(t^q)$ for some $R(T) \in k[T]$. Let $\delta = d/q$. Then δ is a positive integer and $r(t) = R(t^q)$ where $R(T) = \sum_{i=1}^{\delta} A_i T^{\delta - i}$ is a polynomial in an indeterminate T with coefficients $A_0, A_1, \ldots, A_\delta$ in k such that $A_0 \neq 0$. Since $K/k(x)$ is not purely inseparable, we must have $\delta \geq 2$. Let $0 \neq \Lambda \in k$ be such that $\Lambda^q = \lambda$, and let $M \in k$ be such that $M^q = \mu$. Then

$$\frac{R(\Lambda t^q + M)}{aR(t^q) + b} = \frac{r(\lambda t + \mu)}{ar(t) + b} = \frac{\text{nnum}}{\text{num}} = 1,$$

and hence

$$R(\Lambda T + M) = aR(T) + b.$$

Equating the coefficients of T^δ on both sides of the above equation we get $\Lambda^\delta = a$, and differentiating both sides with respect to T and letting $R^*(T)$ stand for the T-derivative of $R(T)$ we get

$$(*) \qquad \Lambda R^*(\Lambda T + M) = aR^*(T).$$

By the definition of q we have $R^*(T) \neq 0$, and upon letting $\delta^* = \deg R^*(T)$ we see that δ^* is an integer with $0 \leq \delta^* \leq \delta - 1$, and by equating the coefficients of T^{δ^*} on both sides of the above equation we get $\Lambda^{1+\delta^*} = a$. Therefore $\Lambda^{\delta - 1 - \delta^*} = 1$.

If $\delta \neq 1 + \delta^*$ then obviously there exists $0 \neq \phi(X, Y)$ such that $\phi(a', b') = 0$ for all a', b' in k for which $a' \neq 0$ and

$$R(\Lambda' T + M') = a'R(T) + b', \qquad \Lambda'^\delta = a', \qquad \Lambda'^{\delta - 1 - \delta^*} = 1$$

for some Λ', M' in k, and hence $\phi(a', b') = 0$ for all a', b' in k for which $a'x + b' \in \{\tau'(x) : \tau' \in \mathrm{Aut}_k K\}$.

So henceforth also assume that $\delta = 1 + \delta^*$. Then $\delta^* \geq 1$ and $R^*(T) = B \prod_{i=1}^{h}(T - B_i)^{\delta_i}$ where $h, \delta_1, \delta_2, \ldots, \delta_h$ are positive integers, $0 \neq B \in k$, and $B_1, B_2, \ldots, B_h$ are pairwise distinct elements in k. By $(*)$ we get

$$\prod_{i=1}^{h}(T + M\Lambda^{-1} - B_i\Lambda^{-1})^{\delta_i} = \prod_{i=1}^{h}(T - B_i)^{\delta_i},$$

and hence for some θ with $1 \leq \theta \leq h$ we must have $M\Lambda^{-1} - B_1\Lambda^{-1} = -B_\theta$, i.e., $M = B_1 + \Lambda B_\theta$. Given any l with $1 \leq l \leq h$, obviously there exists

$0 \neq \psi_l(X, Y) \in k[X, Y]$ such that $\psi_l(a', b') = 0$ for all a', b' in k for which $a' \neq 0$ and

$$R(\Lambda' T + M') = a' R(T) + b', \qquad \Lambda'^{\delta} = a', \qquad M' = B_1 + \Lambda' B_l$$

for some Λ', M', and k. Now upon letting

$$\phi(X, Y) = \prod_{l=1}^{h} \psi_l(X, Y)$$

we see that $0 \neq \phi(X, Y) \in k[X, Y]$ is such that $\phi(a', b') = 0$ for all a', b' in k for which $a'x + b' \in \{\tau'(x) : \tau' \in \mathrm{Aut}_k K\}$.

This completes the proof of the lemma. More precisely, we have shown that in all cases there exists $0 \neq \phi(X, Y) \in k[X, Y]$ such that $\phi(a', b') = 0$ for all a', b' in k for which $a'x + b' \in \{\tau'(x) : \tau' \in \mathrm{Aut}_k K\}$. Now let L be any overfield of $k(x)$, and let $\mathrm{Iso}_k(L, K)$ be the set of all k-isomorphisms of L onto K. If τ'', τ^* in $\mathrm{Iso}_k(L, K)$ and a'', b'', a^*, b^* in k are such that $\tau''(x) = a''x + b''$ and $\tau^*(x) = a^*x + b^*$ then upon letting $\tau' = \tau''^{-1}\tau^*$ we have $\tau' \in \mathrm{Aut}_k K$ and $\tau'(x) = a'x + b'$ with $a' = a''^{-1}a^* \in k$ and $b' = a''^{-1}(b^* - b'') \in k$, and moreover, if $0 \neq \phi'(X, Y) \in k[X, Y]$ is such that $\phi'(a', b') = 0$ then upon letting $\phi^*(X, Y) = \phi'(a''^{-1}X, a''^{-1}(Y - b''))$ we get $0 \neq \phi^*(X, Y) \in k[X, Y]$ such that $\phi^*(a^*, b^*) = \phi'(a', b') = 0$. So if $\mathrm{Iso}_k(L, K)$ is empty then taking $\phi^*(X, Y) = 1$, whereas if $\tau''(x) = a''x + b''$ for some τ'' in $\mathrm{Iso}_k(L, K)$ and a'', b'' in k then letting $\phi^*(X, Y) = \phi'(a''^{-1}X, a''^{-1}(Y - b''))$, we get $0 \neq \phi^*(X, Y) \in k[X, Y]$ such that $\phi^*(a^*, b^*) = 0$ for all a^*, b^* in k for which $a^*x + b^* \in \{\tau^*(x) : \tau^* \in \mathrm{Iso}_k(L, K)\}$. Thus we have proved the following

Corollary. *Let K and x be as in the lemma. Then given any overfield L of $k(x)$, there exists $0 \neq \phi^*(X, Y) \in k[X, Y]$ such that $\phi^*(a^*, b^*) = 0$ for all a^*, b^* in k for which $a^*x + b^* \in \{\tau^*(x) : \tau^* \in \mathrm{Iso}_k(L, K)\}$.*

3. Theorem

To prove the Disjointness Theorem, let K and L be any finite separable algebraic field extensions of $k(X)$. Then there are only a finite number of subfields $K_1, K_2, \ldots, K_\rho$ of K that contain $k(X)$ but are different from it. Likewise there are only a finite number of subfields $L_1, L_2, \ldots, L_\sigma$ of L that contain $k(X)$ but are different from it. By the above corollary there exists $0 \neq \phi_{ij}(X, Y) \in k[X, Y]$ such that $\phi_{ij}(a, b) = 0$ for all a, b in k for which $aX + b \in \{\tau(X) : \tau \in \mathrm{Iso}_k(L_i, K_j)\}$. Let $\phi(X, Y) = \prod_{i=1}^{\rho} \prod_{j=1}^{\sigma} \phi_{ij}(X, Y)$. Then $0 \neq \phi(X, Y) \in k[X, Y]$ is such that $\phi(a, b) = 0$ for all a, b in k for which $aX + b \in \{\tau(X) : \tau \in \mathrm{Iso}_k(L_i, K_j)\}$ for some i, j with $1 \leq i \leq \rho$ and $1 \leq j \leq \sigma$.

Now assume that K and L are the respective splitting fields of $f(X, Y)$ and $g(X, Y)$ over $k(X)$ in an algebraic closure W of $k(X)$. For any a, b in k with $a \neq 0$, we clearly have a k-monomorphism $\tau_{a,b} : L \to W$ such that $\tau_{a,b}(X) = aX + b$ and $\tau_{a,b}(L)$ is the splitting field of $g(aX + b, Y)$ over $k(X)$ in W. If K and $\tau_{a,b}(L)$ are not linearly disjoint over $k(X)$ then for some i, j with $1 \leq i \leq \rho$ and $1 \leq j \leq \sigma$ we must have $\tau_{a,b}(L_i) = K \cap L = K_j$, and then $\tau(X) = aX + b$ where $\tau \in \mathrm{Iso}_k(L_i, K_j)$ is given by taking $\tau(z) = \tau_{a,b}(z)$ for all

$z \in L_i$, and hence $\phi(a, b) = 0$. This completes the proof of the Disjointness Theorem.

4. Characteristic zero

Here is an *alternative proof* of the Disjointness Theorem in case $\operatorname{char} k = 0$. Let $f'(X, Y)$ be the product of the distinct irreducible nonconstant monic factors of $f(X, Y)$ in $k(X)[Y]$, and let R be the Y-degree of $f'(X, Y)$; then we can find $0 \neq I \in k[X]$ such that upon letting $F(X, Y) = I^R f'(X, I^{-1}Y)$ we have $F(X, Y) \in k[X, Y]$. Likewise let $g'(X, Y)$ be the product of the distinct irreducible nonconstant monic factors of $g(X, Y)$ in $k(X)[Y]$, and let S be the Y-degree of $g'(X, Y)$; then we can find $0 \neq J \in k[X]$ such that upon letting $G(X, Y) = J^S g'(X, J^{-1}Y)$ we have $G(X, Y) \in k[X, Y]$. Let $D(X)$ and $E(X)$ be the Y-discriminants of $F(X, Y)$ and $G(X, Y)$ respectively. Then $0 \neq D(X) \in k[X]$ and $0 \neq E(X) \in k[X]$, and clearly there exists $0 \neq \phi(X, Y) \in k[X, Y]$ such that $\phi(a, b) = 0$ for all a, b in k for which $a \neq 0$ and $D(X)$ and $E(aX+b)$ have a nonconstant common factor in $k[X]$. Now let a, b be any elements in k with $a \neq 0$ such that $D(X)$ and $E(aX+b)$ have no nonconstant common factor in $k[X]$. Let K and L^* be the respective splitting fields of $f(X, Y)$ and $g(aX+b, Y)$ over $k(X)$ in an algebraic closure W of $k(X)$. Then obviously K and L^* are the respective splitting fields of $F(X, Y)$ and $G(aX+b, Y)$ over $k(X)$ in W. Now no valuation of $k(X)/k$, other than the valuation $X = \infty$, is ramified in $K \cap L^*$ and hence $K \cap L^* = k(X)$. Therefore K and L^* are linearly disjoint over $k(X)$.

References

[A] S. S. Abhyankar, *Wreath products and enlargements of groups* (to appear).

[IT] K. Iwasawa and T. Tamagawa, *On the group of automorphisms of a function field*, J. Math. Soc. Japan **3** (1951), 137–147.

Department of Mathematics, Purdue University, West Lafayette, Indiana 47907