Math. Ann. 180, 220—226 (1969)

On Curves with Separated Variables

MICHAEL D. FRIED and R. E. MACRAE

1. Introduction

In connection with certain other investigations the authors, both singly and jointly, have considered questions relating to algebraic curves in which the special feature that the variables on the curve satisfy an equation of the form $f(x)-g(z)=0$ (f and g are polynomials) has intruded repeatedly. See, for example, [1] and [2]. Primarily the problem is one of finding peculiarities of the divisors of $f(x)-g(z)$. We have collected together in this paper several results in this direction. We prove, for example, in Theorem 2.3 that $f_1(x)-g_1(z)$ divides $f(x)-g(z)$ if and only if there exists a polynomial F such that $f(t)=F(f_1(t))$ and $g(t)=F(g_1(t))$. In Section 4 we define the notion of a minimal separation: $f(x)-g(z)$ is said to be a *minimal separation* for $a(x, z)$ if (i) $a(x, z)$ divides $f(x)-g(z)$ and (ii) whenever $a(x, z)$ divides $F(x)-G(z)$ then $f(x)-g(z)$ divides $F(x)-G(z)$ also. Theorem 4.2 gives a necessary and sufficient condition for the existence of a minimal separation. In Section 3 we are concerned with a description of certain of the normal extensions of a rational function field. Finally, in Section 5, we give a counter example to a possible strengthening of a theorem proved earlier in [2]. All of these results depend in one way or another on the simple and quite useful Lemma 2.1.

2. Separated Polynomials

We begin with a lemma which will be used many times in the results which follow.

Lemma 2.1. *Let k be an arbitrary field and let z be an element of the rational function field $k(x)$. Then z is an element of $k[x]$ if and only if the prime at infinity in $k(x)$ is the only prime that lies over the prime at infinity in $k(z)$. Under these circumstances the prime at infinity is totally ramified.*

Proof. Let us suppose first that z is a polynomial in x but that there is a valuation ring R such that $k \leqq R$, $k(x)$ is the quotient field of R, x is an element of R and R contracts in $k(z)$ to the local ring at infinity (whose maximal ideal is, of course, generated by $1/z$). Thus z is not in R since $1/z$ is certainly not a unit in R. However, z must be in R since z is in $k[x]$ which is contained in R. Hence we have a contradiction. Conversely, the hypothesis clearly implies that z is an element of every valuation ring of $k(x)$ which contains $k[x]$. But the intersection of these rings is exactly $k[x]$. The final assertion of the lemma is clear from the fact that the residue class degree of the prime at infinity is always unity.

The next result is merely a technical lemma that will be of help in Theorem 2.3.

Lemma 2.2. *Let k be an arbitrary field and let $f(t)$, $f_1(t)$, $f_2(t)$, $g(t)$, $g_1(t)$, $g_2(t)$, $H(t)$ and $H_1(t)$ be polynomials in $k[t]$ such that $f(t)=H(f_2(t))$, $g(t)=H(g_2(t))$, $f_1(t)=H_1(f_2(t))$ and $g_1(t)=H_1(g_2(t))$. If $f_1(x)-g_1(z)$ divides $f(x)-g(z)$ in $k[x,z]$ then $H_1(x)-H_1(z)$ divides $H(x)-H(z)$.*

Proof. By hypothesis there is a polynomial $b(x,z)$ in $k[x,z]$ such that $f(x)-g(z)=(f_1(x)-g_1(z))\,b(x,z)$. Moreover, by the division algorithm we can find polynomials $a(x,z)$ and $r(x,z)$ in $k[x,z]$ such that $H(x)-H(z)=(H_1(x)-H_1(z))\,a(x,z)+r(x,z)$ and either $r(x,z)=0$ or the degree of $r(x,z)$ in x is strictly less than the degree of $H_1(x)$. Since x and z are independent indeterminates we have

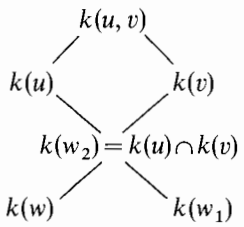
$$f(x)-g(z)=H(f_2(x))-H(g_2(z))=(f_1(x)-g_1(z))\,a(f_2(x),g_2(z))+r(f_2(x),g_2(z))\,.$$

Thus $r(f_2(x),g_2(z))=(f_1(x)-g_1(z))\,(b(x,z)-a(f_2(x),g_2(z))$. Now compare degrees and see that $r(x,z)=0$ and $b(x,z)=a(f_2(x),g_2(z))$.

We may now prove our first main result.

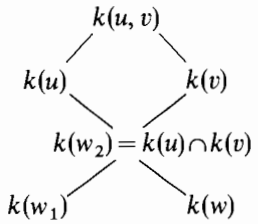
Theorem 2.3. *Let k be an arbitrary field and let $f(t)$, $g(t)$, $f_1(t)$, $g_1(t)$ be polynomials in $k[t]$. Then $f_1(x)-g_1(z)$ divides $f(x)-g(z)$ in $k[x,z]$ if and only if there exists a polynomial $F(t)$ in $k[t]$ such that $f(t)=F(f_1(t))$ and $g(t)=F(g_1(t))$.*

Proof. Suppose first that such a polynomial $F(t)$ exists. Observe that $F(u)-F(v)=(u-v)\,G(u,v)$ for a suitably selected $G(u,v)$ in $k[u,v]$. Now replace u and v by $f_1(x)$ and $g_1(z)$, respectively. Conversely let us suppose that $f_1(x)-g_1(z)$ divides $f(x)-g(z)$. Let $q(x,z)$ be an irreducible factor of $f_1(x)-g_1(z)$ and let $k(u,v)$ be the field of algebraic functions on the curve $q(u,v)=0$. Observe the following lattice of subfields:



where $f(u)=w=g(v)$, $f_1(u)=w_1=g_1(v)$. By Lemma 2.1 there exist polynomials $f_2(t)$ and $g_2(t)$ in $k[t]$ such that $f_2(u)=w_2=g_2(v)$. Moreover, there also exist (by the same lemma) polynomials $H(t)$ and $H_1(t)$ in $k[t]$ such that $w=H(w_2)$ and $w_1=H_1(w_2)$. Thus we see that $f_1(u)=H_1(f_2(u))$, $g_1(v)=H_1(g_2(v))$, $f(u)=H(f_2(u))$ and $g(v)=H(g_2(v))$. Since u and v, considered separately, are indeterminates we may write our hypothesis as $H_1(f_2(x))-H_1(g_2(z))$ divides $H(f_2(x))-H(g_2(z))$. Thus, by Lemma 2.2, $H_1(x)-H_1(z)$ divides $H(x)-H(z)$. If we can now find a polynomial $F(t)$ in $k[t]$ such that $H(t)=F(H_1(t))$, then we are certainly done. We are thus reduced to the case in which $f_1(t)=g_1(t)$

and $f(t)=g(t)$, that is to say the case in which $f_1(x)-f_1(z)$ divides $f(x)-f(z)$. Let p be the characteristic of k and write $f_1(x)=f_2(x^{p^e})$ where $f_2'(x)\neq 0$. Similarly, write $f(x)=f_3(x^{p^d})$ where $f_3'(x)\neq 0$. We claim that $e\leqq d$. If this is not the case let $r=e-d$. Then by Lemma 2.2 we may write $f_2(x^{p^r})-f_2(z^{p^r})$ divides $f_3(x)-f_3(z)$. Since r is positive we see that $x-z$ divides $(f_3(x)-f_3(z))/(x-z)$. Evaluating this last polynomial at $x=z$, we find that $f_3'(x)=0$ which is a contradiction. Let, therefore, $s=d-e$. By another application of Lemma 2.2 we find that $f_2(x)-f_2(z)$ divides $f_3(x^{p^s})-f_3(z^{p^s})$. Now certainly if we can find a polynomial $H(t)$ is $k[t]$ such that $H(f_2(t))=f_3(t^{p^s})$ then we are done. Let us assume from the start, therefore, that $f_1'(t)\neq 0$. We now work by induction on the degree of $f_1(t)$ with degree equal to unity being trivial. For the case of the degree of $f_1(t)$ in excess of one we distinguish two cases. Suppose first that $f_1(x)-f_1(z)$ splits into linear factors (in both x and z) in $k[x,z]$. Then, because $f_1'(t)\neq 0$, $k(t)$ is a galois extension of $k(f_1(t))$. Now the assumption that $f_1(x)-f_1(z)$ divides $f(x)-f(z)$ implies that $f(t)$ is left fixed by every automorphism of $k(t)$ over $k(f_1(t))$ and thus $f(t)$ is an element of $k(f_1(t))$. Moreover an application of Lemma 2.1 shows that $f(t)$ is actually an element of $k[f_1(t)]$. That is to say, $f(t)=H(f_1(t))$ for some $H(t)$ in $k[t]$. Under the remaining case, let $q(x,z)$ be a non-linear irreducible factor of $f_1(x)-f_1(z)$ and let $k(u,v)$ be the field of algebraic functions over the curve $q(u,v)=0$. Consider as before the lattice of subfields:



where $f(u)=w=f(v)$, $f_1(u)=w_1=f_1(v)$. By Lemma 2.1 there exists polynomials $f_2(t)$, $H(t)$, $H_1(t)$ in $k[t]$ such that $f_2(u)=w_2=f_2(v)$, $w=H(w_2)$ and $w_1=H_1(w_2)$. Thus $H_1(f_2(x))-H_1(f_2(z))$ divides $H(f_2(x))-H(f_2(z))$ and thus by Lemma 2.2 $H_1(x)-H_1(z)$ divides $H(x)-H(z)$. The assumption that $q(x,z)$ is non-linear guarantees that the degree of $H_1(t)$ is strictly less than the degree of $f_1(t)$. Thus, by the induction hypothesis, there is a polynomial $F(t)$ in $k[t]$ such that $F(H_1(t))=H(t)$. From this it immediately follows that $F(f_1(t))=f(t)$ and the theorem is completely proved.

3. The Normal Case

We begin with a definition which will facilitate the statement of the theorem in this section.

Definition 3.1. Let k be a field of characteristic p and let $f(x)$ be a polynomial with coefficients in k. We will say that $f(x)$ is *tame of reduced degree m*

if $f(x)=g(x^{p^e})$ where g is a polynomial of degree m with coefficients in k and p is relatively prime to m. If k is of characteristic zero then all polynomials are considered to be tame.

The next result describes certain of the normal extensions of a field of genus zero.

Theorem 3.2. *Let k be an arbitrary field and let $f(x)$ be a tame polynomial of degree n and reduced degree m. If $k(x)$ is a normal (but not necessarily separable) extension of $k(f(x))$ then there exist elements a and b in k such that $f(x)=a(x^{p^e}+b)^m$ where $n=p^e m$. If, moreover, k is perfect then there exist elements a and c in k such that $f(x)=a(x+c)^n$.*

Proof. By hypothesis, $f(x)=g(x^{p^e})$. Let $z=x^{p^e}$. Now set $w=z-d$ and let $h(w)=g(z)$. Since m, the degree of g, is relatively prime to p, we can choose d (in k) in such a way that the coefficient of x^{m-1} in $h(w)$ vanishes. Now $k(w)$ is a galois extension of $k(h(w))$. Moreover, Lemma 2.1 tells us that the prime at infinity is totally ramified. Since m is relatively prime to p, this ramification is tame. Hence $k(w)$ is a cyclic extension of $k(h(w))$. Let S be a generator of the Galois group. It is well-known that S is a linear fractional transformation on $k(w)$. Since S leaves $k(h(w))$ elementwise fixed, Lemma 2.1 implies that the prime at infinity in $k(w)$ remains fixed under S, and thus $S(w)=rw+s$ for some r and s in k. However, this means that $h(w)=h(rw+s)$ and a simple computation shows that s equals zero and r is an m^{th} root of unity. Since S is a generator of the Galois group, r is actually a primitive m^{th} root of unity. Consider now the equation

$$0=a_0+a_1(w-rw)+\cdots+a_j(w^j-r^jw^j)+\cdots=h(w)-h(rw).$$

Factoring out the common powers of w in each term shows that, for each j, $0=a_j(1-r^j)$. Thus, unless $j=m$, a_j vanishes. In other words $h(w)=a_m w^m$. The first assertion of the theorem is now clear. The second assertion follows from the fact that $x^{p^e}-b$ splits completely over k when k is perfect.

4. Minimal Separations

We wish in this section to consider some of the divisors of polynomials of the form $f(x)-g(z)$.

Definition 4.1. Let k be an arbitrary field and let $a(x,z)$ be a non-constant polynomial in $k[x,z]$. A polynomial of the form $f(x)-g(z)$ in $k[x,z]$ will be called a *minimal separation for* $a(x,z)$ if (i) $a(x,z)$ divides $f(x)-g(z)$ and (ii) whenever $a(x,z)$ divides a polynomial of the form $F(x)-G(z)$ in $k[x,z]$ then $f(x)-g(z)$ also divides $F(x)-G(z)$.

We remark that $f(x)-g(z)$ is clearly unique up to multiplication by a non-zero constant from k.

Theorem 4.2. *Let k be an arbitrary field and let $a(x,z)$ be a non-constant polynomial in $k[x,z]$. Then $a(x,z)$ possess a minimal separation if and only if*

there is a polynomial of the form $F(x)-G(z)$ *in* $k[x, z]$ *such that* $a(x, z)$ *divides* $F(x)-G(z)$.

Proof. Part (i) of Definition 4.1 guarantees that if $a(x, z)$ has a minimal separation then it divides a polynomial of the form $F(x)-G(z)$. Conversely, let us suppose that $a(x, z)$ divides $F(x)-G(z)$. If the degree of either $F(x)$ or $G(z)$ is strictly less than one then $a(x, z)$ is clearly its own minimal separation. Let us assume therefore that the degrees of both $F(x)$ and $G(z)$ exceed zero. We note that in this case none of the prime factors of $F(x)-G(z)$ can involve only one of the variables. By virtue of the unique factorization in $k[x, z]$ the same may be said of $a(x, z)$. Let $k[u, v]=k[x, z]/a(x, z)\,k[x, z]$. We claim first that both u and v are transcendental over k. Indeed if $b(u)=0$ then $a(x, z)$ divides $b(x)$. But this would imply that $a(x, z)$ has a prime factor involving only x and we know this to be impossible. Moreover, we claim that the non-zero elements of the subrings $k[u]$ and $k[v]$ are non-divisors of zero in $k[u, v]$. Indeed if $b(u)\,c(u, v)=0$ then $a(x, z)$ divides $b(x)\,c(x, z)$. But $a(x, z)$ must be relatively prime so that $a(x, z)$ divides $c(x, z)$. Thus $c(u, v)=0$. Let, now, S be the multiplicative subset of $k[u, v]$ generated by the non-zero elements of $k[u]$ and $k[v]$ and let $k(u, v)=k[u, v]_S$. We note that $k(u, v)$ contains the rational function fields $k(u)$ and $k(v)$. Let $K=k(u)\cap k(v)$. Since $F(u)-G(v)=0$ we may set $F(u)=W=G(v)$ and note that $k(W)\leqq K$. Thus, by Luroth's theorem, $K=k(w)$. Moreover, by Lemma 2.1, we may choose w so that $f(u)=w=g(v)$ and $W=H(w)$ where f, g and H are polynomials with coefficients in k. We see, therefore, that $a(x, z)$ divides $f(x)-g(z)$ and $f(x)-g(z)$ divides $F(x)-G(z)$. Moreover, the construction of $f(x)-g(z)$ depends only on $a(x, z)$. Thus $f(x)-g(z)$ is the desired minimal separation.

The reader will note that the method of Theorem 4.2 gives an alternate proof of Theorem 2.3.

5. A Counterexample

In an earlier paper [2] the authors gave several proofs of the following result.

Theorem. *Let* k *be an arbitrary field and let* $z=f(x)$ *be a polynomial in* $k[x]$ *such that* $\gcd(\mathrm{char}(k)), \deg(f(x))=1$ *or* $\mathrm{char}(k)=0$. *If* M_1 *and* M_2 *are fields intermediate between* $L=k(x)$ *and* $K=k(f(x))$ *then* $[M_1\cap M_2 : K]=\gcd([M_1 : K], [M_2 : K])$ *and* $[M_1 M_2 : K]=\mathrm{lcm}([M_1 : K], [M_2 : K])$.

We wondered at the time whether the hypothesis that $z=f(x)$ could be weakened to the hypothesis that $z=f(x)/g(x)$, i.e. a rational function in x. The answer to the question is "no" as the following example shows.

Let $k=C$, the field of complex numbers. One knows (see, for example, [3]) that the automorphism group of $C(x)$ over C contains a subgroup G which is isomorphic to the alternating group on 5 letters. Let K be the fixed field for G. There is a point in the Riemann surface for K which lies under 12 points on the

Riemann surface for $C(x)$ and each of these 12 points has ramification index 5 (again see [3]). Now let H be a subgroup of index 5 in G. H is, of course, not normal in G. Let L be its fixed field. Let P denote the distinguished point on the Riemann surface for K which ramifies with index 5. Moreover let $P_1, \ldots, P_g$ be the points which lie over P on the Riemann surface for L. Let $e_1, \ldots, e_g$ be the respective ramification indices of these points. By the general theory $e_1 + \cdots + e_g = 5$. Now let e'_j and g'_j, $j = 1, \ldots, g$ be the ramification and decomposition indices for the points which lie over $P_1, \ldots, P_g$ on the Riemann surface for $C(x)$. Since $C(x)$ is normal over L we know that $e'_1 g'_1 = \cdots = e'_g g'_g = 12$. However $e_1 e'_1 = \cdots = e_g e'_g = 5$. Combining all of these equalities shows that precisely one point on the Riemann surface for L lies over P. Call this point Q. We may now, by Luroth's theorem, find elements w and z in $C(x)$ such that $L = C(w)$ and $K = C(z)$. Moreover we may make the selection in such a way that P and Q are the points at infinity in $C(z)$ and $C(w)$ respectively. By Lemma 2.1 $z = f(w)$. Let now $C(w')$ be one of the distinct conjugates of $C(w)$ in $C(x)$. We may suppose that $f(w') = z$. If we now set $M_1 = C(w)$ and $M_2 = C(w')$, we have our desired counterexample.

By example, we can also show that the assumption in the Theorem that $gcd(\text{char}(k), \deg f(x)) = 1$ cannot be relaxed. At the same time, if we let L be an algebraic closure of k, we show that the lattice of fields between $k(f(x))$ and $k(x)$ is not lattice isomorphic to the lattice of fields between $L(x)$ and $L(f(x))$; unlike the situation when $gcd(\text{char}(k), \deg f(x)) = 1$ holds.

Let $k = \mathbb{Z}/(p)$. Let $g(x) = x^p + ax^{p-1} + \cdots + a^{p-1}x$ where a is a primitive $p+1$-st root of 1. If we let $h(x) = \sum_{i=1}^{p} a_i x^i$ and if we then choose the a_i's so that $h(g(x)) \in k[x]$, then $h(g(x)) = f(x)$ will be decomposable over L, but not over k. If the Theorem were true we would get at most one subfield of degree p over $L(f(x))$ in $L(x)$. However, for each primitive $p+1$-st root of 1 we get a distinct subfield of degree p over $L(f(x))$. In order to choose the coefficients a_i, we notice that

$$f(ax) = \sum a_i (a^p)^i (x^p + x^{p-1} + \cdots + x)^i .$$

If we pick $a_i(a^p)^i = a(-1)^i$, then we will be done if we show that the only exponents with non-zero coefficients in $f(ax)$ are those exponents $\equiv 1 \bmod(p+1)$. However, $f(x) = -(x^p + \cdots + x)(x^p + \cdots + x + 1)^{p-1}$ or $f(x) = -(x)(x^{p+1} - 1)^{p-1}$. This demonstrates our assertion.

We do wish to point out that the following theorem is true.

Theorem. *Let k be an arbitrary field and let $f(x)$ be a polynomial in $k[x]$. If*

$$k(f(x)) = M_1 \subset M_2 \subset \cdots \subset M_r = k(x)$$

and

$$k(f(x)) = N_1 \subset N_2 \subset \cdots \subset N_s = k(x)$$

are two maximal chains in the lattice of fields between $k(x)$ *and* $k(f(x))$, *then* $s = r$ *and the sets of integers*

$$[M_2 : M_1], [M_3 : M_2], \ldots, [M_r : M_{r-1}]$$

and

$$[N_2 : N_1], [N_3 : N_2], \ldots, [N_r : N_{r-1}]$$

are the same (counting multiplicity), although not necessarily in the same order.

The proof of this Theorem is an easy extension of the proof of the Theorem announced at the head of this section, that appears in [2]. Even in the simple situations given by the hypothesis of this Theorem, we still are not able to nicely characterize the lattice of subfields between $k(x)$ and $k(f(x))$ for $f(x) \in k[x]$ when the prime over infinity is wildly ramified.

References

1. Fried, M. D.: Arithmetical properties of value sets of polynomials. To appear, Acta Arithmetica.
2. —, and R. E. MacRae: On the invariance of chains of fields, to appear, Ill. J. of Math.
3. Klein, F.: Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert. Berlin: J. Springer 1927.
4. Schilling, O. F. G.: The theory of valuations. New York: Amer. Math. Soc. Publication 1950.

Professor Michael D. Fried
The Institute for Advanced Study
Princeton, New Jersey, USA

Professor Robert E. MacRae
Department of Mathematics
The University of Colorado
Boulder, Colorado 80302, USA

(Received April 17, 1968)