isibang/ms/2006/5
March 27th, 2006
http://www.isibang.ac.in/~statmath/eprints

Quadratic factors of $f(X) - g(Y)$ in odd characteristic

Manisha Kulkarni and B. Sury

Indian Statistical Institute, Bangalore Centre
8th Mile Mysore Road, Bangalore, 560059 India

QUADRATIC FACTORS OF $f(X) - g(Y)$ IN ODD CHARACTERISTIC

MANISHA KULKARNI AND B.SURY

ABSTRACT. If $f, g \in K[X]$ where K has odd characteristic, and $f(X)-g(Y)$ has an irreducible quadratic factor in $K[X,Y]$, we show that f and g must have the same degree and can be expressed in terms of Dickson polynomials. This generalizes a theorem of Bilu in characteristic zero.

Introduction.

The motivation for this study comes from a characteristic zero problem in Diophantine equations. That problem is to decide, for given polynomials $f, g \in \mathbf{Z}[X]$, whether there are infinitely many integral solutions for the equation $f(x) = g(y)$. The work of several people, including notably deep work of M.Fried, culminated in a remarkable theorem of Y.Bilu & R.Tichy [3]. The approach to the Bilu-Tichy theorem depends on the classical theorem of Siegel which asserts : *Let $F(X,Y) \in \mathbf{Q}[X,Y]$ be absolutely irreducible. If $F(X,Y) = 0$ has infinitely many integral solutions, then the plane curve $F(X,Y) = 0$ has genus 0 and at the most two points at infinity.* The question as to whether the number of points at infinity for the curve $f(x) = g(y)$ is at most 2, was shown by M.Fried to reduce to two questions, one of which is whether $f(X)-g(Y)$ has a quadratic factor in $\mathbf{Q}[X,Y]$. Y.Bilu [1] solved this problem and we try to generalize this to positive characteristic. Berrondo and Gallardo [2] have considered a special case of the polynomial $f(x) - g(y)$ when characteristic is 2. We confine ourselves to odd characteristic. Even though our result here has no applications to Diophantine equations that we are aware of, it may still be worthwhile to study these problems in positive characteristic as well. The reason is that many of the ideas involved in the (characteristic zero) approach have bearing on other problems in number theory like Kronecker conjugacy which may have formulations in positive characteristic also.

Some notations.

Before stating the theorem, we recall some notations. Let K be any field of positive characteristic p. For any polynomial $P \in K[X]$ and any $c \in \bar{K}$, the *c-type of P* is defined to be the tuple $(e_1, e_2, \cdots, e_r)$ of multiplicities $e_1 \leq e_2 \leq \cdots e_r$ of the irreducible factors of $P(X) - c$ over $\bar{K}$. If P is nonconstant, it is said to be *tame* if p divides neither deg P nor any of the e_i's occurring in the c-type for any c. It should be noted that every nonconstant polynomial of degree $< p$ is tame.

1991 *Mathematics Subject Classification.* 12E05, 12E10.

Key words and phrases. Monodromy group, Dickson polynomial, Dihedral group.

Main theorem.

Let K be a field of odd characteristic p.
Assume :
(i) $f(X) - g(Y) \in K[X,Y]$ has an irreducible quadratic factor $q(X,Y)$, and
(iii) either deg (f) or deg (g) is not a multiple of p.
Then, there exist $\phi, f_1, g_1 \in K[X]$ such that :
(i) $f = \phi \circ f_1, g = \phi \circ g_1$, and
(ii) $q(X,Y) | (f_1(X) - g_1(Y))$, with deg $f_1 =$ deg g_1.
Moreover, if one of f, g is tame, then f_1, g_1 are of the form

$$f_1(X) = D_n(X + \beta, a) \ ,$$

$$g_1(X) = D_n((\alpha X + \gamma)(\zeta + \zeta^{-1}), a)$$

for some $n \in \mathbf{N}, a, \beta, \gamma \in K$, $\alpha \in K^*$.
Finally, in general, if f is not necessarily tame, but neither p nor 4 divides deg f, then one may write $f_1 = P_1 \circ P_2 \cdots \circ P_r$ where each P_i is an indecomposable polynomial in $K[X]$ which is either linear or $D_l(X,1)$ or X^l for some prime $l \neq p$.
Further, in this case g_1 is explicitly expressible in terms of the coefficients of $q(X,Y)$ and those of the polynomials occurring in the decomposition of f_1 above.

Here $D_n(X,a)$ is the Dickson polynomial of degree n defined below, and ζ is a primitive n-th root of unity in $\bar{K}$.
Our proof follows that of Bilu in characteristic 0, but we require some results due to G.Turnwald and P.Müller to carry it through. We have only considered the case when the characteristic p does not divide the egree of f because only under this condition, we have enough understanding of the monodromy group of f to conclude facts like the existence of an n-cycle in it where $n =$ deg f. In the non-tame case, we have assumed that the degree is not a multiple of 4 because we need a certain technical result (quoted as an observation at the end of the proof) on the zeroes of Dickson polynomials. The article [5] is a convenient source for analogues in positive characteristic of several characteristic 0 results.

Dickson polynomials

Let A be any integral domain with quotient field F.
Denote by $\bar{F}$, an algebraic closure of F. We shall be applying the facts on Dickson polynomials only when $A = K$, a field of positive characteristic.
For $a \in A$, and $n \in \mathbf{N}$, the Dickson polynomial $D_n(X,a) \in A[X]$ is the unique polynomial of degree n which satisfies $D_n(z + a/z, a) = z^n + a^n/z^n$.
The existence of $D_n(X,a)$ is easily proved by the recursion

$$D_{n+2}(X,a) = XD_{n+1}(X,a) - aD_n(X,a)$$

and from

$$D_1(X,a) = X, D_2(X,a) = X^2 - 2a.$$

It is also seen then that the coefficients are polynomials in a with (image in A of) integer coefficients.

We note the evident properties :

(i) *If char* $A = p > 0$, *then* $D_{np}(X,a) = D_n(X,a)^p$,
(ii) $D_{mn}(X,a) = D_m(D_n(X,a), a^n)$,
(iii) $D_n(bX, b^2a) = b^n D_n(X,a)$.

The following important property is elementary to prove :

Proposition 1 ([5], proposition 1.7)
Assume that $\bar{F}$ *contains a primitive* n*-th root of unity* ζ *(so char* $F \not| n$*) and that* A *contains* $\zeta + \zeta^{-1}$. *Then, for each* $a \in A$, $D_n(X,a) - D_n(Y,a)$ *factorises in* $A[X,Y]$ *into irreducible factors of degrees* ≤ 2 *as follows:*

$$D_n(X,a) - D_n(Y,a) =$$

$$(X - Y) \prod_{k=1}^{(n-1)/2} (X^2 - (\zeta^k + \zeta^{-k})XY + Y^2 + a(\zeta^k - \zeta^{-k}))$$

or

$$(X^2 - Y^2) \prod_{k=1}^{(n-2)/2} (X^2 - (\zeta^k + \zeta^{-k})XY + Y^2 + a(\zeta^k - \zeta^{-k}))$$

according as to whether n *is odd or even. The quadratic factors are all distinct when* $a \neq 0$.

The following result provides a key link between c-types and the Dickson polynomials. The first part is from [5], lemma 1.11 and the second one is from [3], theorem 5.2.

Proposition 2 .
Assume $f \in F[X]$ *is monic, of degree* $n \geq 3$. *Assume that char* F *does not divide* n. *Then, in either of the following two cases, we must have* $f(X) = D_n(X + b, a) + c$ *for some* $a, b, c \in F$ *and* $a \neq 0$ *:*
(a) *Suppose that, for each* $c \in \bar{F}$ *the c-type of* f *is either* $(1, 1, \cdots, 1)$ *or* $(1, d, d, \cdots, d)$ *for some* d *(depending on* c *but) not divisible by char* F, *or*
(b) *suppose that there are exactly two constants* c_1, c_2 *such that* f *has* c_1*-type* $(1, 1, 2, 2, \cdots, 2)$ *and* c_2*-type* $(2, 2, \cdots, 2)$ *and no other* c *such that* $f(X) - c$ *has multiple roots.*

Arithmetic monodromy groups.

Start with char $K = p > 0$ odd and fix an algebraic closure $\bar{K}$. Let X, t be algebraically independent elements over K. One works with the irreducible, separable polynomial $f(X) - t$ over $K(t)$. Let U_f denote the splitting field of $f(X) - t$ over $K(t)$, Its Galois group is called the arithmetic monodromy group of f over K and is denoted by $\mathrm{Mon}_K(f)$; it is viewed as a permutation group of the roots of $f(X) - t \in K(t)[X]$. The corresponding Galois group when K is replaced by $\bar{K}$ is called the geometric monodromy group and is denoted by $\mathrm{Mon}(f)$. Let $\tilde{K}$ denote the constant subfield of U_f; i.e., the algebraic closure of K in U_f. Then $\tilde{K}$ is Galois over K and the monodromy group $\mathrm{Mon}(f)$ is the normal subgroup of $\mathrm{Mon}_K(f)$ which fixes

$\tilde{K}(t)$. The Galois group $\mathrm{Gal}(\tilde{K}/K)$ can be identified with the quotient. In other words, we have an exact sequence

$$1 \to Mon(f) \to Mon_K(f) \to Gal(\tilde{K}/K) \to 1.$$

Lemma 1. ([5], lemmata 3.3,3.4)
If $c \in \bar{K}$ is such that $f(X)$ has c-type $(e_1, e_2, \cdots, e_r)$ and, if p does not divide $e_1 e_2 \cdots e_r$, then $Mon_K(f)$ contains an element of cycle type $(e_1, e_2, \cdots, e_r)$. Moreover, if $p \not| n$, then $Mon_K(f)$ always contains an n-cycle.

The discussion of a solvable monodromy group for a polynomial in positive characteristic is carried out in [6] using some classical theorems of Galois and Ritt on primitive permutation groups. It is proved by Turnwald in [6] that :

Lemma 2.
Let $f \in K[X]$ have degree $n > 1$ with char $K = p$ not dividing n.
(i) If f has a decomposition $f = f_1 \circ f_2 \circ \cdots f_r$ in $K[X]$, then $Mon_K(f)$ is solvable if, and only if, each $Mon_K(f_i)$ is.
(ii) If f is indecomposable, then $Mon_K(f)$ is a primitive permutation group (that is, stabilisers of points are maximal subgroups).
(iii) If f is indecomposable, and $Mon_K(f)$ is also solvable, one must have $n = 4$ or n must be a prime.

Dihedral groups

Recall that the dihedral group D_n of order $2n$ is the group of symmetries of the regular n-gon; it can be defined by the presentation $< x, y | x^2, (xy)^2, y^n >$.
We have the characterisation :
A finite group which is generated by two involutions x, xy whose product has order n, is isomorphic to D_n.
D_n can be realised as a subgroup of S_n generated by an n-cycle and a product of $[(n-1)/2]$ disjoint transpositions.
A subgroup of S_n which contains an n-cycle and is isomorphic to some D_k, must be isomorphic to D_n (that is, $k = n$). We also note :
(i) *All subgroups of S_n which are isomorphic to D_n are conjugate. Each n-cycle is contained in a unique such subgroup.*
(ii) *A nontrivial element of subgroup of S_n which is isomorphic to D_n must be either a product of ((n/d) number of) disjoint d-cycles for some $d|n$ or a product of $[(n-1)/2]$ disjoint transpositions; that is, the cycle types occurring are of the type $(d, d, \cdots, d)$ or $(1, 2, 2, \cdots, 2)$ (when n is odd) or $(1, 1, 2, 2, \cdots, 2)$ (when n is even).*

A lemma of Bilu.

Bilu proved the following result in characteristic 0 but it works in positive characteristic p not dividing n as well. One may rewrite his proof replacing symbols like cosine and sine etc. by the appropriate expressions in terms of primitive roots of unity.

Lemma 3. ([1])
For $n \geq 3$, $p \not| n$, the absolute monodromy group $Mon(D_n(X,a)) \cong D_n$ if, $a \neq 0$, and is cyclic of order n for $a = 0$.
In particular, if $U_{D_n(X,a)}$ denotes the splitting field of $D_n(X,a) - t$ over $K(t)$, then the degree of the field $\bar{K}U_{D_n(X,a)}$ over $\bar{K}(t)$ is $2n$ or n according as to whether $a \neq 0$ or $a = 0$.
Moreover, the constant subfield in the respective cases, is $K(\zeta + \zeta^{-1})$ and $K(\zeta)$, where ζ is a primitive n-th root of unity in $\bar{K}$.

Proof of main theorem.

We take f monic for convenience, and that $p \not| \deg f$ without loss of generality. The proof will proceed by induction on deg f.

Start with a root $x_0 \in \overline{K(t)}$ of $f(X) - t$.
Let $y_0 \in \overline{K(t)}$ be such that $q(x_0, y_0) = 0$; then $g(y_0) = t$.
Thus, we have two finite extensions $K(x_0), K(y_0)$ of $K(t)$.
Look at $K(x_0) \cap K(y_0)$.
By Luröth's theorem, it is $K(z)$ for some $z \in \overline{K(t)}$ which is integral over $K[t]$. In fact, since

$$K(t) = K(f(x_0)) \subseteq K(x_0) \cap K(y_0) \subseteq K(x_0)$$

and

$$K(t) = K(g(y_0)) \subseteq K(x_0) \cap K(y_0) \subseteq K(y_0),$$

by Luröth's theorem, there exist $f_0, g_0 \in K[X]$ such that

$$z = f_0(x_0) = g_0(y_0)$$

and

$$K(x_0) \cap K(y_0) = K(z).$$

Writing $\phi_0 \in K[X]$ such that $\phi_0(z) = t$, we have

$$f = \phi_0 \circ f_0, g = \phi_0 \circ g_0.$$

Note that $f_0(x_0) - g_0(y_0) = 0$.
Being irreducible, $q(X,Y)$ must divide any polynomial $h(X,Y) \in K[X,Y]$ which satisfies $h(x_0, y_0) = 0$. Therefore, $q(X,Y)$ divides $f_0(X) - g_0(Y)$.
If

$$K(x_0) \cap K(y_0) = K(z) = K(f_0(x_0)) = K(g_0(y_0))$$

is a proper extension of $K(t) = K(f(x_0)) = K(g(y_0))$, then degree of f_0 is less than deg f.
Proceed similarly with f_0, g_0 in place of f, g. Thus, after a finite number of steps, we get polynomials f_1, g_1 such that $q(X,Y)$ divides $f_1(X) - g_1(Y)$, $f = \phi_1 \circ f_1, g = \phi_1 \circ g_1$ for some

$\phi_1 \in K[X]$ and $K(x_0) \cap K(y_0) = K(t)$. From now onwards, we shall assume this and call f_1, g_1 as f, g again. As we shall see, the splitting field U_f will turn out to be the field $K(x_0, y_0)$.

Claims : If $K(x_0) \cap K(y_0) = K(t)$, then
(i) *deg f = deg g.*
(ii) *The coefficients of X^2, Y^2, and XY in $q(X,Y)$ are all non-zero.*
(iii) *The splitting field U_f of $f(X) - t$ over $K(t)$ is $K(x_0, y_0)$. In particular, $Mon_K(f)$, is the Galois group Gal $(U_f/K(t)) \cong D_n$ where deg f = deg $g = n$.*

Proof.

A key observation is that since $q(x_0, y_0) = 0$, the degrees

$$[K(x_0, y_0) : K(x_0)] \ , \ [K(x_0, y_0) : K(x_0)] \leq 2.$$

On the other hand, these degrees cannot be 1; otherwise, x_0 or y_0 would be in $K(x_0) \cap K(y_0) = K(t)$, and therefore the irreducible polynomial $f(X) - t$ must have degree 1, a contradiction. Hence, we have

$$[K(x_0, y_0) : K(x_0)] = [K(x_0, y_0) : K(x_0)] = 2.$$

Thus,

$$[K(x_0, y_0) : K(t)] = [K(x_0, y_0) : K(x_0)][K(x_0) : K(t)] = 2 \ degf,$$

$$[K(x_0, y_0) : K(t)] = [K(x_0, y_0) : K(y_0)][K(y_0) : K(t)] = 2 \ degg.$$

We conclude deg f = deg g which proves claim (i).

To see (ii), write $q(X,Y) = \alpha X^2 + \beta XY + \gamma Y^2 +$ terms of degree ≤ 1.
If $\gamma = 0$, then $q(x_0, Y)$ is linear in Y and then $K(x_0, y_0) = K(x_0)$, a contradiction.
Similarly, we have $\alpha \neq 0$.
Now, if $\beta = 0$, we can write $q(X,Y) = f_0(X) - g_0(Y)$ with deg f_0, deg $g_0 = 2$. Note that $f_0(x_0) = g_0(y_0) \in K(x_0) \cap K(y_0) = K(t)$. Then,

$$deg \ f = [K(x_0) : K(t)] \leq [K(x_0) : K(f_0(x_0))] \leq deg \ f_0 \leq 2$$

which is a contradiction.

For proving (iii), we use the notation U_f for the splitting field of $f(X) - t$ introduced earlier. Now, $K(x_0, y_0)$ is a separable extension of $K(t)$; let us consider its normal closure L in $\overline{K(t)}$.
Then, the subgroup Gal $(L/K(x_0))$ of Gal$(L/K(t))$ leaves invariant the quadratic extension $K(x_0, y_0)$ of $K(x_0)$.
Similarly, the subgroup Gal $(L/K(y_0))$ of Gal$(L/K(t))$ leaves invariant the quadratic extension $K(x_0, y_0)$ of $K(y_0)$.
By the hypothesis that $K(x_0) \cap K(y_0) = K(t)$, these two subgroups generate the whole of Gal $(L/K(t))$, which must itself leave invariant the field $K(x_0, y_0)$.
This means $L = K(x_0, y_0)$ and so $K(x_0, y_0)$ is a Galois extension of $K(t)$.
Therefore, $U_f \subseteq K(x_0, y_0)$.

It suffices to show now that $y_0 \in U_f$.
Now, if we write

$$q(X,Y) = \alpha X^2 + \beta XY + \gamma Y^2 + uX + vY + w$$

then $q(X, y_0) \in K(y_0)[X]$ has two roots x_0 and x_1, say.
Note that $f(x_1) = t$ and so x_1 is also in U_f.
Thus, $x_0 + x_1 \in U_f$.
But,

$$x_0 + x_1 = -(\beta y_0 + u)/\alpha$$

which gives (since $\beta \neq 0$) that $y_0 \in U_f$.
This proves

$$U_f = K(x_0, y_0)$$

and (iii) follows from the characterisation of D_n recalled above, since the nontrivial elements of Gal $(U_f/K(x_0))$ and of Gal $(U_f/K(y_0))$ have order 2, and generate $\mathrm{Mon}_K(f) = Gal(U_f/K(t))$ in view of

$$K(x_0) \cap K(y_0) = K(t).$$

We have also used the fact that $\mathrm{Mon}_K(f)$ contains an n-cycle as $p \not| n$.

Completion of proof when f is tame :

Firstly, we note that if the original polynomial f is tame, then any polynomial f_1 with $f = \phi \circ f_1$ is also tame ([5], remark 4.2), and we are working now with such f_1 as our f.
Using the observation (ii) on dihedral groups, $\mathrm{Mon}_K(f)$ is a subgroup of S_n whose nontrivial elements have the cycle types $(d, d, \cdots, d)$ for some $d|n$ or $(1, 2, 2, \cdots, 2)$ or $(1, 1, 2, 2, \cdots, 2)$.
As f is tame, lemma 1 tells us that the only possible c-types of f for any $c \in \bar{K}$ are either $(d, d, \cdots, d)$ for some $d|n$ or $(1, 2, 2, \cdots, 2)$ or $(1, 1, 2, 2, \cdots, 2)$.
Let us separately consider the cases when the degree n of f is odd and when it is even.
First, consider the case when n is odd.
If there is some c with the c-type $(d, d, \cdots, d)$ with $1 < d \leq n$, then $f(X) - c = \prod_{i=1}^{l}(X - \alpha_i)^d$ implies that there are $l(d-1)$ roots of f' by this c. As $ld = n$, we have $n(d(c)-1)/d(c) \geq 2n/3$ roots for f' from this c as $d(c) \geq 3$. If we had two such different c's, then we would have at least $4n/3$ roots for f', an impossibility since $4n/3 > n - 1$.
Further, if this c were the only constant giving a root of f', then we would have $n(d(c) - 1)/d(c) = n - 1$; that is, $n = d(c)$. Hence, $f(X) - c = (X - \alpha)^n = D_n(X - \alpha, 0)$.
Now, suppose that apart from c, there is at least one other constant c' giving a root of f'; then necessarily f has c'-type $(1, 2, 2, \cdots, 2)$.
Writing $f(X) - c' = (X - \beta)\prod_{i=1}^{r}(X - \theta_i)^2$, this c' accounts for $r = (n-1)/2$ roots of f'. Since $2n/3 + (n-1)/2 > n - 1$, this is impossible as well.
Finally, if there is no c such that f has c-type of the form $(d, d, \cdots, d)$ for ay divisor $d > 1$ of n, then there must be exactly two constants c_1, c_2 with f having c_i-type $(1, 2, \cdots, 2)$ for $i = 1, 2$.
By proposition 2 (i), we must have $f(X) = D_n(X + b, a) + c$ for some constants $a, b, c \in K$.
Now, let n be even.

Then, any constant c giving a multiple root for $f(X)-c$ gives type $(d,d,\cdots,d)$ for some divisor $d>1$ of n or type $(1,1,2,\cdots,2)$.

If $f(X)-c_1=\prod_{i=1}^{l}(X-\alpha_i)^{d(c_1)}$, then we get $l(d(c_1)-1)=n(d(c_1)-1)/d(c_1)\geq n/2$ roots for f'. Thus, if we had two such constants c_1,c_2, then we would have $\geq n/2+n/2>n-1$ roots for f', an impossibility.

Suppose there is exactly one c_1 such that f has c_1-type $(d,d,\cdots,d)$ for some divisor $d>1$ of n.

If there are no other constants giving roots for f', then we have $n-1=\deg f'=n(d(c_1)-1)/d(c_1)$; that is, $d(c_1)=n$. So, $f(X)-c_1=(X-\alpha)^n=D_n(X-\alpha,0)$.

Suppose there is some c_0 such that f has c_0-type $(1,1,2,\cdots,2)$. This gives rise to $(n-2)/2$ roots of f'. As c_1 gives $n(d(c_1)-1)/d(c_1)\geq n/2$ roots of f', we must have $d(c_1)=2$ and c_1,c_0 are the only constants giving roots of f'. This time, we can apply proposition 2 (ii) to get that $f(X)=D_n(X+b,a)+c$ for some $a,b,c\in K$.

Finally, if there is no c_1 giving the type $(d,d,\cdots,d)$ for any divisor $d>1$ of n, then we must have $n=4$ and exactly three c's which give the type $(1,1,2)$.

Writing $f(X)-c_i=(X-\alpha_i)(X-\beta_i)(X-\theta_i)^2$ for $i=1,2,3$, we have that all the α's, β's and θ's to be distinct.

Hence $f'(X)=4\prod_{i=1}^{3}(X-\theta_i)$. We claim that this is impossible.

The coefficient of X^3 in $(X-\alpha_1)(X-\beta_1)(X-\theta_1)^2-(X-\alpha_2)(X-\beta_2)(X-\theta_2)^2$ is zero, as this polynomial is a constant c_2-c_1. This gives us

$$\alpha_2+\beta_2-\alpha_1-\beta_1=2\theta_1-2\theta_2\cdots(A)$$

On the other hand, $f'(X)=(f(X)-c_1)'$ gives

$$4(X-\theta_2)(X-\theta_3)=(2X-\alpha_1-\beta_1)(X-\theta_1)+2(X-\alpha_1)(X-\beta_1).$$

The coefficient of X gives

$$2(\theta_2+\theta_3)=\theta_1+\alpha_1+\beta_1.$$

Similarly,

$$2(\theta_1+\theta_3)=\theta_2+\alpha_2+\beta_2.$$

Subtracting, we have

$$2\theta_1-2\theta_2=\alpha_2+\beta_2-\alpha_1-\beta_1+\theta_2-\theta_1\cdots(B)$$

But then (A) and (B) imply $\theta_1=\theta_2$, a contradiction of the assumption that θ's are distinct. Hence this case $n=4$ with exactly three c's of type $(1,1,2)$ cannot arise.

Hence, we have shown in all cases that $f(X)=D_n(X+b,a)+c$ for some $a,b,c\in K$.

We shall show now that $g(X)=\pm D_n(\frac{uX+v}{\zeta^{k(n-1)/2}+1/\zeta^{k(n-1)/2}},a)+c$ for some $k\in\{0,1,\cdots,n-1\}$ with $\zeta^k\neq-1$.

Now, as in the proof of claim (iii), using the notation x_0 and x_1 for the two roots of $q(X,y_0)$, the sum $x_0+x_1=-(\beta y_0+u)/\alpha$ for some $\alpha,\beta\in K^*$.

Since $f(x_0)=f(x_1)=t$, and since $f(X)=D_n(X+b,a)+c$, the polynomial $D_n(X,a)+c-t$ has roots x_0+b,x_1+b.

We now use the observation (made in [1]) that the sum $x_0 + x_1 + 2b$ must be a root of a certain polynomial of the form $D_n(uX + v, a) \pm (c - t)$.
More precisely, the following observation implies that x_0+x_1+2b is a root of $D_n(\frac{X}{\zeta^{k(n-1)/2}+1/\zeta^{k(n-1)/2}}, a) - (t - c)$ for some $k \in \{0, 1, \cdots, n-1\}$ with $\zeta^k \neq -1$.

Observation.
Assume that a primitive n-th root of unity $\zeta \notin K$ and that $\zeta + \zeta^{-1} \in K$ when $a = 0$. If x_0, x_1 are roots of $D_n(X, a) - t$ with $x_0+x_1 \neq 0$, then x_0+x_1 is a root of $D_n(\frac{X}{\zeta^{k(n-1)/2}+1/\zeta^{k(n-1)/2}}, a) - t$ for some
$k \in \{0, 1, \cdots, n-1\}$ with $\zeta^k \neq -1$.
Proof.
If we write $x_0 = z+a/z$ for some z, then the various roots of $D_n(X, a)-t$ are clearly $\zeta^k z+a/\zeta^k z$ for $k \in \{0, 1, \cdots, n-1\}$. We have then $x_1 = \zeta^k z+a/\zeta^k z$ for one of these $k \neq 0$. As $x_0+x_1 \neq 0$, clearly $\zeta^k \neq -1$.
We have

$$x_0 + x_1 = (1 + \zeta^k)z + \frac{a}{z} + \frac{a}{\zeta^k z}$$

$$= (\zeta^{k(n-1)/2} + \frac{1}{\zeta^{k(n-1)/2}})(\frac{z}{\zeta^{k(n-1)/2}} + \frac{a\zeta^{k(n-1)/2}}{z}).$$

Thus,

$$D_n(\frac{z}{\zeta^{k(n-1)/2}} + \frac{a\zeta^{k(n-1)/2}}{z}, a) = z^n + \frac{a^n}{z^n} = D_n(x_0, a) = t.$$

This proves that $x_0 + x_1$ is a root of

$$D_n(\frac{X}{\zeta^{k(n-1)/2} + \frac{1}{\zeta^{k(n-1)/2}}}, a) - t.$$

This completes the proof of the observation.

Getting back to our $f(X) = D_n(X + b) + c$, note that the roots x_0, x_1 of $q(X, y_0)$ are such that $x_0 + x_1 \neq 0$; otherwise, we will have a contradiction as follows. Recall

$$q(X, Y) = \alpha X^2 + \beta XY + \gamma Y^2 + uX + vY + w$$

in $K[X, Y]$ means that $x_0+x_1 = -(\beta y_0+u)/\alpha$ can be zero only if $y_0 \in K$. This being impossible, we do have $x_0 + x_1 \neq 0$ and, in the above observation, we have shown that $x_0 + x_1 + 2b = 2b - (\beta y_0 + u)/\alpha$ is a root of $D_n(\frac{X}{\zeta^{k(n-1)/2}+1/\zeta^{k(n-1)/2}}, a) - (t - c)$.
We rewrite $x_0 + x_1 + 2b = ry_0 + s$ for some $r, s \in K, r \neq 0$.
In other words, y_0 is a root of the irreducible polynomial $D_n(\frac{rX+s}{\zeta^{k(n-1)/2}+1/\zeta^{k(n-1)/2}}, a) - (t - c)$ over $K(t)$.
As $g(X) - t$ is also an irreducible polynomial over $K(t)$ having the same degree and for which y_0 is a root, we must have

$$\lambda g(X) = D_n(\frac{rX + s}{\zeta^{k(n-1)/2} + 1/\zeta^{k(n-1)/2}}, a) - (t - c)$$

for some $\lambda \in K^*$.
Comparing the coefficients of t, (as t, x are algebraically independent over K), one obtains $\lambda = 1$. We have

$$g(X) = D_n(\frac{rX + s}{\zeta^{k(n-1)/2} + 1/\zeta^{k(n-1)/2}}, a) + c.$$

Thus, if we choose $\phi(X) = X + c$, we note that $f(X) = (\phi \circ f_1)(X)$ where $f_1(X) = D_n(X + b, a)$. Further, if $g_1(X) = D_n(\frac{rX+s}{\zeta^{k(n-1)/2}+1/\zeta^{k(n-1)/2}}, a)$, then noting that $g = \phi \circ g_1$ and that $q(X, Y)$ divides $f_1(X) - g_1(Y)$, the theorem is proved in the tame case.

Completion of proof in the general (non-tame) case.

Recall the assumption that 4 does not divide deg f was made in the theorem. We shall use the following remarkable result due to P.Müller ([4], Theorem 4) which is proved using valuation theory :

Proposition 3. ([4])
Let K be of odd characteristic p, and let $P \in K[X]$ have degree a prime $l \neq p$. Suppose $Mon(P)$ is a solvable group. Then, $P(X) = \lambda D_l(X, a) + \mu$ where $a = 0$ or 1.

Recall that the claims in the body of the proof yield the corollary that $\mathrm{Mon}_K(f)$ is solvable. In fact, we know that it is isomorphic to the dihedral group D_n.
By lemma 2 (ii) and (iii), f is a composition of indecomposable polynomials of degrees $1, 4$ or a prime whose monodromy groups are solvable. By our assumption, (since neither 4 nor p divides deg f), in the decomposition of f, each of the indecomposable polynomials has degree 1 or a prime $\neq p$.
Applying the above proposition of Muller, we have that f must have the form

$$f = P_1 \circ P_2 \circ \cdots \circ P_r$$

for polynomials $P_i \in K[X]$ each of which is either linear or equals $D_l(X, 1)$ or X^l for some prime $l \neq p$.
We may write $f(X) = D_l(h(X), a)$ where $a = 0$ or 1 and $h = P_2 \circ P_3 \circ \cdots \circ P_r$ - the situation when P_1 is linear is easily taken care of at the end.
If $h(X) = h_0 + h_1 X + \cdots + h_m X^m$, then $h(x_0), h(x_1)$ are roots of $D_l(X, 1) - t$. Therefore, $h(x_0) + h(x_1)$ is a root of $D_l(\frac{X}{\zeta^{k(l-1)/2}+\zeta^{-k(l-1)/2}}, a) - t$.

Before proceeding with the rest of the proof, we recall that the polynomial $q(X, y_0)$ of degree 2 in X has the two roots x_0 and x_1. We have

$$x_0 + x_1 = ry_0 + s$$

$$x_0 x_1 = uy_0^2 + vy_0 + w$$

for some $r, s, u, v, w \in K$ with $ru \neq 0$.
Using the above expressions for the sum and product of x_0, x_1, one shows by induction on m that $x_0^m + x_1^m$ is a polynomial $P_m(y_0)$ of degree m over K. Thus, it follows that $h(x_0) + h(x_1) =$

$Q_m(y_0)$ where $Q_m \in K[X]$ has degree m.
Therefore,

$$D_l(\frac{Q_m(y_0)}{\zeta^{k(l-1)/2} + \zeta^{-k(l-1)/2}}, a) = t.$$

By the irreducibility of $g(Y) - t$ over $K(t)$, the fact that $q(X,Y)$ divides each polynomial $F(X,Y)$ satisfying $F(x_0, y_0) = 0$ and the fact $g(y_0) = t$, it follows that

$$g(X) = D_l(\frac{Q_m(X)}{\zeta^{k(l-1)/2} + \zeta^{-k(l-1)/2}}, a).$$

Finally, when the decomposition of f starts with a linear polynomial, then evidently one may take ϕ to be linear and $f_1(X), g_1(Y)$ to be the polynomials

$$f_1(X) = D_l(h(X), a),$$
$$g_1(X) = D_l(\frac{Q_m(X)}{\zeta^{k(l-1)/2} + \zeta^{-k(l-1)/2}}, a)$$

for some $k \in \{0, 1, \cdots, l-1\}, a = 0$ or 1.
We note that $Q_m(X)$ can be explicitly determined in terms of the coefficients of $q(X,Y)$ and the polynomials occurring in the decomposition of f.
This completes the proof of the theorem.

Acknowledgements.

We are grateful to the Tata Institute of Fundamental Research, Mumbai for inviting us to the International conference on Diophantine equations in December 2005 to celebrate the 60th birthday of T.N.Shorey where these results were announced. It is a great pleasure to thank Professor A.Schinzel for showing interest in this work and also for informing us of the paper by Berrondo & Gallardo. The first author would like to thank the Indian Statistical Institute, Bangalore for all the facilities it provided during the course of this work.

References

[1] Y. Bilu. Quadratic Factors of $f(x) - g(y)$ Acta Arithmetica, 90 (1999), 341- 355.

[2] F.Berrondo & L.Gallardo. Factors of small degree of some difference polynomials $f(x) - g(t)$ in $F[t][x]$. Publ. Math. Debrecen, Vol. 67 (2005), 305-314.

[3] Y. Bilu and R.F. Tichy. The Diophantine Equation $f(x) = g(y)$. Acta Arithmetica XCV (2000), 261 - 288.

[4] P.Müller. A Weil-bound free proof of Schur's conjecture. Finite Fields Appl. 3 (1997), 25-32.

[5] G.Turnwald. On Schur's conjecture. J.Austral.Math.Soc. 58 (1995), 312-357.

[6] G.Turnwald. Some notes on monodromy groups of polynomials. Dedicated to Professor Andrzej Schinzel on the occasion of his sixtieth birthday.

Poornaprajna Institute of Scientific Research, Davanhalli, Bangalore, India.

Statistics & Mathematics Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore - 560 059, India.
E-mail address: sury@ns.isibang.ac.in
URL: http://www.isibang.ac.in/~sury