Quadratic Factors of $f(X) - g(Y)$

Manisha Kulkarni Peter Müller B. Sury

January 9, 2007

1 Introduction

In [Bil99] Bilu classified the pairs of polynomials f, g over a field of characteristic 0 such that $f(X) - g(Y)$ has an irreducible factor of degree 2. This note extends his results to arbitrary characteristic. Also, the rather specific main result of [BG05] is an immediate consequence of the theorems below.

The strategy is roughly as follows: A straightforward application of Galois theory and Lüroth's Theorem reduces to the following situation: Let x be a transcendental over the base field K, and set $t = f(x)$. Then $K(x)$ has a quadratic extension L, such that $L/K(t)$ is Galois. The Galois group is generated by two involutions, hence it is dihedral. The intermediate field $K(x)$ is the fixed field of one of the involutions.

This reduction appears already in [Bil99], its extension to positive characteristic causes no problems. Let $\bar{K}$ be an algebraic closure of K. To proceed further Bilu applied ramification theoretic arguments to the extension $\bar{K}(x)/\bar{K}(t)$ which rely on Riemann's existence theorem and which don't work in positive characteristic without making quite restrictive assumptions on the characteristic.

Instead, we use a different approach which avoids any use of ramification theoretic arguments: The field L is the function field of the quadratic factor of $f(X) - g(Y)$, thus $\bar{K}L$ is a rational field $\bar{K}(z)$. So $\mathrm{Gal}(\bar{K}(z)/\bar{K}(t))$ is a subgroup of $\mathrm{Gal}(L/K(t))$. Also, the index is at most 2. The group of $\bar{K}$-automorphisms of $\bar{K}(z)$ is $\mathrm{PGL}_2(\bar{K})$ (action via linear fractional transformations of z). Thus we have to determine the cyclic and dihedral subgroups of $\mathrm{PGL}_2(\bar{K})$, and analyze the cases which give pairs f, g such that $f(X) - g(Y)$ has a quadratic factor over K.

The generalization of [Bil99, Theorem 1.2] is

Theorem 1.1. *Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has a factor of degree at most 2. If* *the characteristic p of K is positive, then assume that at least one of the polynomials f, g cannot be written as a polynomial in X^p. Then there are $f_1, g_1, \Phi \in K[X]$ with $f = \Phi \circ f_1$, $g = \Phi \circ g_1$, such that one of the following holds:*

(a) $\deg f_1, \deg g_1 \leq 2$.

(b) $p \neq 2$, $n = \deg f_1 = \deg g_1 \geq 4$ *is a power of* 2, *and there are* $\alpha, \beta, \gamma, a \in K$ *such that* $f_1(X) = D_n(X+\beta, a)$, $g_1(X) = -D_n((\alpha X+\gamma)(\xi+1/\xi), a)$. *Here* ξ *denotes a primitive* $2n$*-th root of unity. Furthermore, if* $a \neq 0$, *then* $\xi^2 + 1/\xi^2 \in K$.

Conversely, in cases (a) and (b) $f(X) - g(Y)$ indeed has a factor of degree at most 2. This is clear for case (a), because $f_1(X) - g_1(Y)$ is such a factor, and follows for case (b) from Lemma 2.8.

If one wants to determine the cases such that $f(X) - g(Y)$ has an irreducible factor of degree 2, then the list becomes longer in positive characteristic. The exact extension of [Bil99, Theorem 1.3] is

Theorem 1.2. *Let $f, g \in K[X]$ be non-constant polynomials over a field K, such that $f(X) - g(Y) \in K[X, Y]$ has a quadratic irreducible factor $q(X, Y)$. If the characteristic p of K is positive, then assume that at least one of the polynomials f, g cannot be written as a polynomial in X^p. Then there are $f_1, g_1, \Phi \in K[X]$ with $f = \Phi \circ f_1$, $g = \Phi \circ g_1$ such that $q(X, Y)$ divides $f_1(X) - g_1(Y)$, and one of the following holds:*

(a) $\max(\deg f_1, \deg g_1) = 2$ *and* $q(X, Y) = f_1(X) - g_1(Y)$.

(b) There are $\alpha, \beta, \gamma, \delta \in K$ *with* $g_1(X) = f_1(\alpha X + \beta)$, *and* $f_1(X) = h(\gamma X + \delta)$, *where* $h(X)$ *is one of the following polynomials.*

  (i) p *does not divide* n, *and* $h(X) = D_n(X, a)$ *for some* $a \in K$. *If* $a \neq 0$, *then* $\zeta + 1/\zeta \in K$ *where* ζ *is a primitive* n*-th root of unity.*

  (ii) $p \geq 3$, *and* $h(X) = X^p - aX$ *for some* $a \in K$.

  (iii) $p \geq 3$, *and* $h(X) = (X^p + aX + b)^2$ *for some* $a, b \in K$.

  (iv) $p \geq 3$, *and* $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2 X$ *for some* $a \in K$.

  (v) $p = 2$, *and* $h(X) = X^4 + (1 + a)X^2 + aX$ *for some* $a \in K$.

(c) n *is even,* p *does not divide* n, *and there are* $\alpha, \beta, \gamma, a \in K$ *such that* $f_1(X) = D_n(X + \beta, a)$, $g_1(X) = -D_n((\alpha X + \gamma)(\xi + 1/\xi), a)$. *Here* ξ *denotes a primitive* $2n$*-th root of unity. Furthermore, if* $a \neq 0$, *then* $\xi^2 + 1/\xi^2 \in K$.

(d) $p \geq 3$, *and there are quadratic polynomials* $u(X), v(X) \in K[X]$, *such that* $f_1(X) = h(u(X))$ *and* $g_1(X) = h(v(X))$ *with* $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$ *for some* $a \in K$.

The theorems exclude the case that f and g are both polynomials in X^p. The following handles this case, a repeated application reduces to the situation of the Theorems above.

Theorem 1.3. *Let* $f, g \in K[X]$ *be non-constant polynomials over a field* K, *such that* $f(X) - g(Y) \in K[X, Y]$ *has an irreducible factor* $q(X, Y)$ *of degree at most* 2. *Suppose that* $f(X) = f_0(X^p)$ *and* $g(X) = g_0(X^p)$, *where* $p > 0$ *is the characteristic of* K. *Then one of the following holds:*

(a) $q(X, Y)$ *divides* $f_0(X) - g_0(Y)$, *or*

(b) $p = 2$, $f(X) = f_0(X^2)$, $g(X) = f_0(aX^2 + b)$ *for some* $a, b \in K$, *and* $q(X, Y) = X^2 - aY^2 - b$.

Remark 1.4. Under suitable conditions on the parameters and the field K, all cases listed in Theorem 1.2 give examples such that $f_1(X) - g_1(Y)$ indeed has an irreducible quadratic factor. The cases of the Dickson polynomials are classically known, see Lemma 2.8 and its proof. We illustrate two examples:

(b)(v). Here $p = 2$ and $h(X) = X^4 + (1 + a)X^2 + aX$. We have $h(X) - h(Y) = (X + Y)(X + Y + 1)(X^2 + X + Y^2 + Y + a)$. If $Z^2 + Z = a$ has no solution in K, then the quadratic factor is irreducible.

(b)(iv). Here $p \geq 3$ and $h(X) = X^p - 2aX^{\frac{p+1}{2}} + a^2X$, and $a \neq 0$ of course. If α is a root of $Z^{p-1} - a$, then so is $-\alpha$. Let T be a set such $T \cup (-T)$ is a disjoint union of the roots of $Z^{p-1} - a$.

We compute

$$\begin{aligned} h(X^2) - h(Y^2) &= (X^2 - Y^2) \prod_{t \in T \cup (-T)} [((X - Y) - t)((X + Y) - t)] \\ &= (X^2 - Y^2) \prod_{t \in T} [((X - Y) - t)((X + Y) - t) \\ &\qquad ((X + Y) + t)((X - Y) + t)] \\ &= (X^2 - Y^2) \prod_{t \in T} ((X^2 - Y^2)^2 - 2t^2(X^2 + Y^2) + t^4). \end{aligned}$$

and therefore

$$h(X) - h(Y) = (X - Y) \prod_{t \in T} ((X - Y)^2 - 2t^2(X + Y) + t^4).$$

The discriminant with respect to X of the quadratic factor belonging to t is $16t^2Y$, so all the quadratic factors are absolutely irreducible.

2 Preparation

Definition 2.1. Let a, b elements of a group G. Then a^b denotes the conjugate $b^{-1}ab$.

Lemma 2.2. *Let G be a finite dihedral group, generated by the involutions a and b. Then a and a suitable conjugate of b generate a Sylow 2-subgroup of G.*

Proof. Set $c = ab$. For $i \in \mathbb{N}$, the order of $<a, b^{c^i}>$ is twice the order of ab^{c^i}. We compute $ab^{c^i} = a(c^{-1})^i bc^i = a(ba)^i b(ab)^i = (ab)^{2i+1} = c^{2i+1}$. Let $2i + 1$ be the largest odd divisor of $|G|$. The claim follows. □

Definition 2.3. For a, b, c, d in a field K with $ad - bc \neq 0$ let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ denote the image of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ in $\mathrm{PGL}_2(K)$.

Lemma 2.4. *Let K be an algebraically closed field of characteristic p, and $\rho \in \mathrm{PGL}_2(K)$ be an element of finite order n. Then one of the following holds:*

(a) p does not divide n, and ρ is conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$, where ζ is a primitive n-th root of unity.

(b) $n = p$, and ρ is conjugate to $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Proof. Let $\hat{\rho} \in \mathrm{GL}_2(K)$ be a preimage of ρ. Without loss of generality we may assume that 1 is an eigenvalue of $\hat{\rho}$. The claim follows from the Jordan normal form of $\hat{\rho}$. □

Lemma 2.5. *Let K be an algebraically closed field of characteristic p, and $G \leq \mathrm{PGL}_2(K)$ be a dihedral group of order $2n \geq 4$, which is generated by the involution τ and the element ρ of order n. Then one of the following holds:*

(a) p does not divide n. There is $\sigma \in \mathrm{PGL}(K)$ such that $\tau^\sigma = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\rho^\sigma = \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$, where ζ is a primitive n-th root of unity.

(b) $n = p \geq 3$. There is $\sigma \in \mathrm{PGL}(K)$ such that $\tau^\sigma = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $\rho^\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

(c) *$n = p = 2$. There is $\sigma \in \mathrm{PGL}(K)$ such that $\tau^\sigma = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ and $\rho^\sigma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ for some $1 \neq b \in K$.*

Proof. By Lemma 2.4 we may assume that ρ has the form given there. From $\rho^\tau = \rho^{-1}$ we obtain the shape of τ:

First assume that p does not divide n, so $\rho = \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}$. Let $\hat{\tau} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ be a preimage of τ. From $\rho^\tau = \rho^{-1}$ we obtain $\rho\tau = \tau\rho^{-1}$, hence

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$$

for some $\lambda \in K$. This gives $(\lambda\zeta - 1)a = 0$, $(\lambda - 1)b = 0$, $(\lambda - 1)c = 0$, and $(\lambda - \zeta)d = 0$. First assume $b = c = 0$. Then ρ and τ commute, so G is abelian, hence $n = 2 \neq p$ and therefore $\zeta = -1$. It follows $\tau = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \rho$, a contradiction.

Thus $b \neq 0$, so $\lambda = 1$. This yields $a = d = 0$, as $\zeta \neq 1$. We obtain $\tau = \begin{bmatrix} 0 & 1 \\ c & 0 \end{bmatrix}$. Choose $\beta \in K$ with $\beta^2 = c$, and set $\delta = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$. The claim follows from $\rho^\delta = \rho$ and $\tau^\delta = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Now assume the second case of Lemma 2.4, that is $p = n$ and $\rho = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Again setting $\hat{\tau} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we obtain

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

for some $\lambda \in K$. This gives $a + c = \lambda a$, $b + d = \lambda(-a + b)$, $c = \lambda c$, and $d = \lambda(-c + d)$. If $c \neq 0$, then $\lambda = 1$, so $c = 0$ by the first equation, a contradiction. Thus $c = 0$, so $a \neq 0$. We may assume $a = 1$, so $d = -1$. This gives the result for $p = n = 2$. If $p \neq 2$, then set $\sigma = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}$ with $\beta = -b/2$. From $\rho^\sigma = \rho$ and $\tau^\sigma = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ we obtain the claim. □

Let z be a transcendental over the field K. The group of K-automorphisms of $K(z)$ is isomorphic to $\mathrm{PGL}_2(K)$, where $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ sends z to $\frac{az+b}{cz+d}$. Note that $K(z) = K(z')$ for $z \in K(z)$ if and only if $z' = \frac{az+b}{cz+d}$ with $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PGL}_2(K)$.

Let $r(z) \in K(z)$ be a rational function. Then the *degree* $\deg r$ of r is the maximum of the degrees of the numerator and denominator of $r(z)$ as a reduced fraction. Note that $\deg r$ is also the degree of the field extension $K(z)/K(r(z))$.

Definition 2.6. For $a \in K$ one defines the nth Dickson polynomial $D_n(X, a)$ (of degree n) implicitly by $D_n(z+a/z, a) = z^n+(a/z)^n$. Note that $D_n(X, 0) = X^n$. Furthermore, from $b^n D_n(z+a/z, a) = b^n(z^n+(a/z)^n) = (bz)^n+(\frac{b^2a}{bz})^n = D_n(bz+\frac{b^2a}{bz}, b^2a) = D_n(b(z+a/z), b^2a)$ one obtains $b^n D_n(X, a) = D_n(bx, b^2a)$, a relation we will use later.

Lemma 2.7. *(a) Let $f(X) = g(h(X))$ with $f \in K[X]$ and $g, h \in K(X)$. Then $f = g \circ h = (g \circ \lambda^{-1}) \circ (\lambda \circ h)$ for a rational function $\lambda \in K(X)$ of degree 1, such that $g \circ \lambda^{-1}$ and $\lambda \circ h$ are polynomials.*

(b) Let $f, g \in K[X]$ be two polynomials such that $f(X) = L(g(R(X)))$ for rational functions $L, R \in K(X)$ of degree 1. Then there are linear polynomials $\ell, r \in K[X]$ with $f(X) = \ell(g(r(X)))$.

Proof. (a) This is well known. For the convenience of the reader, we supply a short proof. Let $\lambda \in K(X)$ be of degree 1 such that $\lambda(h(\infty)) = \infty$. Setting $\bar{g} = g \circ \lambda^{-1}$ and $\bar{h} = \lambda \circ h$ we have $f = \bar{g} \circ \bar{h}$ with $\bar{h}(\infty) = \infty$. Suppose that $\bar{g}$ is not a polynomial. Then there is $\alpha \in \bar{K}$ ($\bar{K}$ denotes an algebraic closure of K) with $\bar{g}(\alpha) = \infty$. Let $\beta \in \bar{K} \cup \{\infty\}$ with $\bar{h}(\beta) = \alpha$). From $\bar{h}(\infty) = \infty$ we obtain $\beta \neq \infty$. Now $f(\beta) = \bar{g}(\bar{h}(\beta)) = \bar{g}(\alpha) = \infty$ yields a contradiction, so $\bar{g}$ is a polynomial. From that it follows that $\bar{h}$ is a polynomial as well.

(b) If L is a polynomial, then R has no poles, so is a polynomial as well.

Suppose now that L is not a polynomial. Then there is $\alpha \in K$ with $L(\alpha) = \infty$. Let $\bar{K}$ be an algebraic closure of K. Choose $\beta \in \bar{K}$ with $g(\beta) = \alpha$. If we can find $\gamma \in \bar{K}$ with $R(\gamma) = \beta$, then we get the contradiction $f(\gamma) = \infty$. The value set of R on $\bar{K}$ is $\bar{K}$ minus the element $R(\infty) \in K$. Thus we are done except for the case that the equation $g(X) = \alpha$ has only the single solution $\beta = R(\infty) \in K$. In this case, however, $g(X) = \alpha + \delta(X - \beta)^n$ with $\delta \in K$. From $L^{-1}(f(R^{-1}(X))) = g(X)$ we analogously either get that L and R are polynomials, or $f(X) = \alpha' + \delta'(X - \beta')^n$ with $\alpha', \delta', \beta' \in K$. The claim follows. □

Lemma 2.8. *Let K be a field of characteristic p, and $n \in \mathbb{N}$ even and not divisible by p (so in particular $p \neq 2$). Let ξ be a primitive $2n$-th root of unity and $a \in K$. Then*

$$D_n(X, a) + D_n(Y, a) = \prod_{1 \le k \le n-1 \ odd} (X^2 - (\xi^k + 1/\xi^k)XY + Y^2 + (\xi^k - 1/\xi^k)^2 a).$$

Proof. This is essentially [Bil99, Prop. 3.1]. The factorizations of $D_m(X,a) - D_m(Y,a)$ are known, see [Tur95, Prop. 1.7]. The claim then follows from that and $D_{2n}(X,a) - D_{2n}(Y,b) = D_n(X,a)^2 - D_n(Y,b)^2 = (D_n(X,a) + D_n(Y,b))(D_n(X,a) - D_n(Y,b))$. □

The following proposition classifies polynomials f over K with a certain Galois theoretic property. To facilitate the notation in the statement and its proof, we introduce a notation: If E is a field extension of K, and $f, h \in K[X]$ are polynomials, then we write $f \sim_E h$ if and only if there are linear polynomials $L, R \in E[X]$ with $f(X) = L(h(R(X)))$. Clearly, $\sim_E$ is an equivalence relation on $K[X]$. In determining the possibilities of f in Proposition 2.10, we first determine certain polynomials $h \in \bar{K}[X]$ with $f \sim_{\bar{K}} h$, and from that we conclude the possibilities for f. The following Lemma illustrates this latter step.

Lemma 2.9. *Let $\bar{K}$ be an algebraic closure of the field K of characteristic p. Suppose that $f \sim_{\bar{K}} X^p - 2X^{(p+1)/2} + X$ for $f \in K[X]$. Then $f \sim_K X^p - 2aX^{(p+1)/2} + a^2X$ for some $a \in K$.*

Proof. There are $\alpha, \beta, \gamma, \delta \in \bar{K}$ with $f(X) = \alpha h(\gamma X + \delta) + \beta \in K[X]$, where $h(X) = X^p - 2X^{(p+1)/2} + X$.

The coefficients of X^p and $X^{(p+1)/2}$ of $f(X)$ are $\alpha\gamma^p \in K$ and $-2\alpha\gamma^{(p+1)/2} \in K$, so $\gamma^{(p-1)/2} \in K$ and $\alpha\gamma \in K$.

Suppose that $p > 3$. Then the coefficient of $X^{(p-1)/2}$ is (up to a factor from K) $\alpha\gamma^{(p-1)/2}\delta \in K$, so $\alpha\delta \in K$ and therefore $\delta/\gamma \in K$. Thus, upon replacing X by $X - \delta/\gamma$, we may assume $\delta = 0$. Then $\beta \in K$, so $\beta = 0$ without loss of generality. Now dividing by $\alpha\gamma^p$ and setting $a = 1/\gamma^{(p-1)/2}$ yields the claim.

In the case $p = 3$ we get from above $\gamma \in K$ and then $\alpha \in K$. Thus we may assume $\alpha = \gamma = 1$. Looking at the coefficient of X, which is $-4\delta + 1$, shows $\delta \in K$, so $\delta = \beta = 0$ without loss of generality. Thus $f(X) = X^3 - 2X^2 + X$. □

Proposition 2.10. *Let K be a field of characteristic p, and $f(X) \in K[X]$ be a polynomial of degree $n \geq 3$ which is not a polynomial in X^p. Let x be a transcendental, and set $t = f(x)$. Suppose that the normal closure of $K(x)/K(t)$ has the form $K(x, y)$ where $F(x, y) = 0$ with $F \in K[X, Y]$ irreducible of total degree 2. Furthermore, suppose that the Galois group of $K(x, y)/K(t)$ is dihedral of order $2n$. Then one of the following holds:*

(a) p does not divide n, and $f \sim_K D_n(X, a)$ for some $a \in K$. If $a \neq 0$, then $\zeta + 1/\zeta \in K$ where ζ is a primitive n-th root of unity.

(b) $n = p \geq 3$, *and* $f \sim_K X^p - aX$ *for some* $a \in K$.

(c) $n = 2p \geq 6$, *and* $f \sim_K (X^p + aX + b)^2$ *for some* $a, b \in K$.

(d) $n = p$, *and* $f \sim_K X^p - 2aX^{\frac{p+1}{2}} + a^2 X$ *for some* $a \in K$.

(e) $n = 4$, $p = 2$, *and* $f \sim_K X^4 + (1 + a)X^2 + aX$ *for some* $a \in K$.

In the cases (b), (d), (e), and (a) for odd n*, the following holds: If* $K(w)$ *is an intermediate field of* $K(x, y)/K(t)$ *with* $[K(x, y) : K(w)] = 2$*, then* $K(w)$ *is conjugate to* $K(x)$.

In case (a) suppose that $f(X) = D_n(X, a)$ *and* $K(w)$ *is not conjugate to* $K(x)$*. Furthermore, suppose that* $t = g(w)$ *for a polynomial* $g(X) \in K[X]$*. Then* $g(X) = -D_n(b(\xi + 1/\xi)X + c, a)$ *for* $b, c \in K$ *and* ξ *a primitive* $2n$*-th root of unity.*

Proof. Let $\hat{K}$ be the algebraic closure of K in $K(x, y)$. Then $K(x) \subseteq \hat{K}(x) \subseteq K(x, y)$, so either $\hat{K} = K$ or $K(x, y) = \hat{K}(x)$.

We start looking at the latter case. Here $\hat{K}(x)/\hat{K}(t)$ is a Galois extension with group C which is a subgroup of $G = \mathrm{Gal}(\hat{K}(x)/K(t))$ of order n. Note that C is either cyclic or dihedral. Let $\sigma \in C$, so $x^\sigma = \frac{ax+b}{cx+d}$ with $a, b, c, d \in \hat{K}$. From $f(\frac{ax+b}{cx+d}) = f(x^\sigma) = f(x)^\sigma = t^\sigma = t = f(x)$ we obtain that $\frac{ax+b}{cx+d}$ is a polynomial, so $x^\sigma = ax + b$.

Suppose that p does not divide n. Then we may assume that the coefficient of X^{n-1} of f vanishes. From $f(ax + b) = f(x)$ we obtain $b = 0$. Thus C is isomorphic to a subgroup of $\hat{K}^\times$, in particular C is cyclic and generated by σ with $x^\sigma = \zeta x$ with ζ a primitive nth root of unity. From $f(x) = f(\zeta x)$ we see that, up to a constant factor, $f(X) = X^n$. This is case (a) with $a = 0$.

From now on it is more convenient to work over an algebraic closure $\bar{K}$ of K. As $\bar{K}(t) \cap K(x, y) = \hat{K}(t)$ (see e.g. [Tur99, Prop. 1.11(c)]), we obtain that $\mathrm{Gal}(\bar{K}(x)/\bar{K}(t)) = C$.

Now suppose that p divides $n = |C|$, but $p \geq 3$. First assume that C is cyclic. From Lemma 2.4 we get $p = n$. Let ρ be a generator of C. Lemma 2.4 shows the following: There is $x' \in \bar{K}(x)$ with $\bar{K}(x) = \bar{K}(x')$, such that $x'^\rho = x' + 1$. So $t' = x'^p - x'$ is fixed under C. We obtain $t' \in \bar{K}(t)$, because $\bar{K}(t)$ is the fixed field of C. From $p = [\bar{K}(x') : \bar{K}(t')]$ we obtain $\bar{K}(t') = \bar{K}(t)$. So there are rational functions $L, R \in \bar{K}(X)$ of degree 1 with $x' = R(x)$ and $t = L(t')$. Then $f(x) = t = L(t') = L(x'^p - x') = L(r(x)^p - R(x))$, so $f = L \circ (X^p - X) \circ R$. By Lemma 2.7 we may assume that L and R are polynomials over $\bar{K}$. Then $f(X) = \alpha(X^p - aX) + \beta$ with $\alpha, \beta, a \in K$. From that we get case (b).

Next assume that C is dihedral of order n. As $p \geq 3$, we get that p divides $n/2$. We apply Lemma 2.5 now. This yields $n = 2p$, and there is x'

with $\bar{K}(x') = \bar{K}(x)$ such that $\bar{K}(t)$ is the fixed field of the automorphisms $x' \mapsto -x'$ and $x' \mapsto x' + 1$. Obviously $t' = (x'^p - x')^2$ is fixed under these automorphisms, and as $[\bar{K}(x') : \bar{K}(t')] = 2p$, we obtain $\bar{K}(t) = \bar{K}(t')$. The claim follows similarly as above.

Now assume that $p = 2$ divides n. Applying Lemmata 2.4 and 2.5, we get that C is the Klein 4 group. We see that $t' = x'(x'+1)(x'+b)(x'+b+1)$ is fixed under the automorphisms sending x' to $x' + 1$ and to $x' + b$. So $t' = h(x')$ with $h(X) = X^4 + (1 + b + b^2)X^2 + (b + b^2)X$. Next we show that $b^2+b \in K$. A suitable substitution $\gamma f(\alpha X+\beta)+\delta$ should give $f(X) \in K[X]$. We obtain $\gamma f(\alpha X + \beta) + \delta = \gamma(f(\alpha X) + f(\beta)) + \delta \in K[X]$. Looking at the coefficients of X^2 and X yields $\alpha \in K$, so $\alpha = 1$ without loss of generality. Looking at X^4 gives $\gamma \in K$, so $\gamma = 1$ without loss. Finally the coefficient of X yields the claim. Thus $f(X) = X^4 + (1 + b + b^2)X^2 + (b + b^2)X \in K[X]$ and $\hat{K} = K(b)$, which gives case (e). In this case assume that w is as in the proposition. Let τ_x and τ_w be the involutions of the dihedral group G of order 8 which fix x and w, respectively. From $K(x, y) = K(x, b) = K(w, b)$ we obtain that $\tau_x, \tau_w \notin C$. This shows that τ_x and τ_w are conjugate in G, so $K(w)$ is conjugate to $K(x)$.

It remains to study the case $K = \hat{K}$, so $\hat{K}(x, y)/\hat{K}(t)$ is Galois with group G. By the Diophantine trick we obtain a rational parametrization of the quadric $F(X, Y) = 0$ over $\bar{K}$ (actually, a suitable quadratic extension over which $F(X, Y) = 0$ has a rational point suffices). In terms of fields that means $\bar{K}(z) = \bar{K}(x, y)$ for some element z.

We apply Lemma 2.5. Up to replacing x and t by x' and t' as above, we get the following possibilities:

(a) p does not divide n, x is fixed under the automorphism sending z to $1/z$, and t is fixed under this automorphism and the one sending z to z/ζ. So we may choose $t = z^n + 1/z^n$, $x = z + 1/z$. But then $t = D_n(x, 1)$. There are linear polynomials $L, R \in \bar{K}[X]$ with $L \circ D_n(X, 1) \circ R = f \in K[X]$, so we get case (a) of the proposition by [Tur95, Lemma 1.9]. For the remaining claims concerning this case, we may assume that $f(X) = D_n(X, a)$. Again set $t = f(x)$, and now choose z with $z + a/z = x$. Then $t = D_n(x, a) = D_n(z + a/z, a) = z^n + (a/z)^n$. The normal closure $K(x, y) = K(x, w)$ of $K(x)/K(t)$ is contained in $K(\zeta, z)$. The elements $x' = \zeta x + \frac{a}{\zeta x}$ and $x'' = \frac{x}{\zeta} + \frac{\zeta a}{x}$ are conjugates of x, so $x, x', x'' \in K(x, y)$. From $x'+x'' = (\zeta+1/\zeta)(x+a/x)$ we obtain $\zeta + 1/\zeta \in K(x, y)$. However, we are in the case that K is algebraically closed in $K(x, y)$, so $\zeta + 1/\zeta \in K$.

Suppose that $K(w)$ is not conjugate to $K(x)$. As extending the coefficients does not change Galois groups, this is equivalent to $\bar{K}(x)$ not being conjugate to $\bar{K}(w)$ in $\bar{K}(x, y) = \bar{K}(z)$. Note that x is fixed under the involution $z \mapsto a/z$. The other involutions in $\mathrm{Gal}(\bar{K}(z)/\bar{K}(t))$ have the form $z \mapsto a\beta/z$, where β is an nth root of unity, or $z \mapsto -z$. The latter involution cannot fix w, because the fixed field would be $\bar{K}(z^2)$, however, $z^n + (a/z)^n$ cannot be written as a polynomial in z^2. Thus suppose that $z \mapsto a\beta/z$ fixes w. If $\beta^{n/2} = 1$, then an easy calculation shows that $\begin{bmatrix} 0 & a \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & \beta a \\ 1 & 0 \end{bmatrix}$ are conjugate in $\mathrm{Gal}(\bar{K}(z)/\bar{K}(t))$, contrary to $\bar{K}(x)$ and $\bar{K}(w)$ not being conjugate. Thus $\beta^{n/2} \neq 1$, hence $\beta^{n/2} = -1$, because $\beta^n = 1$. The element $w' = z + (\beta a)/z$ is fixed under the involution $z \mapsto a\beta/z$, so $\bar{K}(w') = \bar{K}(w)$. Furthermore,

$$t = z^n + (a/z)^n = z^n + (\beta a/z)^n = D_n(z + (\beta a)/z, \beta a) = D_n(w', \beta a),$$

so $g(X) = D_n(uX + v, \beta a)$ for some $u, v \in \bar{K}$. The condition that $g(X)$ has coefficients in K shows that $\frac{v}{u} \in K$, see [Tur95, Lemma 1.9]. Thus, upon replacing X by $X - \frac{v}{u}$, we may assume $v = 0$. The transformation formula in Definition 2.6 gives $g(X) = D_n(uX, \beta a) = \beta^{n/2} D_n(\frac{u}{\sqrt{\beta}}X, a) = -D_n(\frac{1}{\delta}X, a)$ with $\delta \in \bar{K}$. As each conjugate of w has degree 2 over $K(x)$ we obtain that $f(X) - g(Y)$ splits over K in irreducible factors of degree 2. By Lemma 2.8 one of the factors of $f(X) - g(Y) = D_n(X, a) + D_n(\frac{1}{\delta}Y, a)$ is $X^2 - \frac{1}{\delta}(\xi + 1/\xi)XY + \frac{1}{\delta^2}Y^2 - (\xi - 1/\xi)^2 a$. All coefficients of this factor have to be in K, so there is $b_1 \in K$ with $\frac{1}{\delta}(\xi + \frac{1}{\xi}) = b_1$. We obtain $g(X) = -D_n(\frac{b_1}{\xi + 1/\xi}X, a) = -D_n(b(\xi + 1/\xi)X, a)$, where $b = \frac{b_1}{(\xi + 1/\xi)^2} \in K$. The claim follows.

(b) $n = p \geq 3$. From a computation above we obtain $t = (z^p - z)^2$. We may assume that x is fixed under the automorphism sending z to $-z$, so for instance $x = z^2$. Let $h \in \bar{K}(X)$ with $h(x) = t$. That means $h(z^2) = (z^p - z)^2 = z^{2p} - 2z^{p+1} + z^2$, hence $h(X) = X^p - 2X^{\frac{p+1}{2}} + X$. Lemma 2.9 yields the claim.

(c) The case $n = p = 2$ does not arise, because we assumed $n \geq 3$.

The conjugacy of $K(w)$ and $K(x)$ has been shown in the derivation of case (e) above. In the cases (a) (n odd), (b) and (d) it holds as well, because G is dihedral of order $2n$ with n odd, so all involutions in G are conjugate. □

3 Proof of the Theorems

3.1 Proof of Theorem 1.1 and 1.2

Suppose that $f(X)$ is not a polynomial in X^p, so not all exponents of f are divisible by p. Let $q(X, Y)$ be an irreducible divisor of $f(X) - g(Y)$ of degree at most 2. Set $t = f(x)$, where x is a transcendental over K. Clearly both variables X and Y appear in $q(X, Y)$. In an algebraic closure of $K(t)$ choose y with $q(x, y) = 0$. Note that $g(y) = t$. The field $K(x) \cap K(y)$ lies between $K(x)$ and $K(t)$, so by Lüroth's Theorem, $K(x) \cap K(y) = K(u)$ for some u. Writing $t = \Phi(u)$ and $u = f_1(x)$ for rational functions $\Phi, f_1 \in K(X)$, we have $f = \Phi \circ f_1$. By Lemma 2.7(a), we may replace u by u' with $K(u) = K(u')$, such that t is a polynomial in u, and u is a polynomial in x. Thus without loss of generality we may assume that Φ and f_1 are polynomials. From that it follows that u is also a polynomial in y, so $g(X) = \Phi(g_1(X))$ for a polynomial g_1 with $g_1(y) = u$. Note that f_1 is again not a polynomial in X^p. As q is irreducible and $f_1(x) - g_1(y) = u - u = 0$, we get that $q(X, Y)$ divides $f_1(X) - g_1(Y)$. Thus, in order to prove the theorems, we may assume that $f = f_1$ and $g = g_1$, so $K(x) \cap K(y) = K(t)$.

First suppose that the polynomial $q(x, Y)$, considered in the variable Y, is inseparable over $K(x)$. Then the characteristic of K is 2, and (up to a factor) $q(X, Y) = aX^2 + bX + c + Y^2$, hence $y^2 = ax^2 + bx + c$. So $K(y^2) \subseteq K(x) \cap K(y) = K(t)$, therefore $[K(y) : K(t)] \leq 2$. But $[K(x) : K(t)] = [K(x, y) : K(y)][K(y) : K(t)]/[K(x, y) : K(x)] \leq 2$. We obtain $\deg f, \deg g \leq 2$, a situation which gives case (a) in the theorems.

Thus we assume that $K(x, y)/K(x)$ is separable. By the assumption that $f(X)$ is not a polynomial in X^p, we also obtain that $K(x)/K(t)$ is separable. Thus $K(x, y)/K(t)$ is separable. From $K(x) \cap K(y) = K(t)$ we obtain that the fields $K(x)$, $K(y)$, and $K(x, y)$ are pairwise distinct. So $K(x, y)$ is a quadratic extension of $K(x)$ and $K(y)$. Thus $K(x, y)/K(t)$ is a Galois extension, whose Galois group G is generated by involutions τ_x and τ_y, where τ_x and τ_y fix x and y, respectively. In particular, G is a dihedral group.

For $\deg f = \deg g = 2$ we obtain case (a) of the Theorems. Thus assume $n = \deg f = \deg g \geq 3$ from now on.

The possibilities for f are given in Proposition 2.10. In the cases (b), (d), (e), and (a) for odd n, we obtain that $K(x)$ and $K(y)$ are conjugate, yielding the case (a) of Theorem 1.1 and case (b) of Theorem 1.2.

Let us assume case (c) of Proposition 2.10. Here G is a dihedral group of order $4p$. If τ_x and τ_y are conjugate, then we obtain case (a) of Theorem 1.1 and case (b)(iii) of Theorem 1.2. Thus suppose that τ_x and τ_y are not conjugate. By Lemma 2.2 there is a conjugate τ'_y of τ_y such that τ_x and τ'_y generate a group of order 4. Thus $K(x)$ and $K(y')$ have degree 2 over $K(x) \cap K(y')$. So there are $f_0, g_0, h \in K[X]$ with f_0 and g_0 of degree 2 and $f = h \circ f_0$, $g = h \circ g_0$, giving case (a) of Theorem 1.1. Without loss of generality assume that $f(X) = (X^p + aX + b)^2$, and $f_0(X) = X^2$. From $f(-X) = h((-X)^2) = h(X^2) = f(X)$ we obtain $b = 0$, so $f(X) = h(X^2)$

with $h(X) = X^p + 2aX^{\frac{p+1}{2}} + a^2X$. This yields case (d) of Theorem 1.2.

Finally, assume the situation of Proposition 2.10, case (a) for even n. If $K(x)$ and $K(y)$ are conjugate, then we obtain the case (a) of Theorem 1.1 and case (b)(i) of Theorem 1.2. If however $K(x)$ and $K(y)$ are not conjugate, then Proposition 2.10 yields case (c) of Theorem 1.2. In order to obtain case (b) of Theorem 1.1 one applies Lemma 2.2 in order to show that τ_x and a conjugate of τ_y generate a dihedral 2-group and argues as in the previous paragraph.

3.2 Proof of Theorem 1.3

We have $f(X) = u(X)^p$ and $g(X) = v(X)^p$, where the coefficients of u and v are contained in a purely inseparable extension L of K. (This includes the case $K = L$.) In particular, $[L : K]$ is a power of p, so $q(X, Y)$ remains irreducible over L if $p > 2$.

Suppose first that $p > 2$, or that $q(X, Y)$ is irreducible over L if $p = 2$. As each irreducible factor of $f(X) - g(Y) = u(X)^p - v(X)^p = (u(X) - v(Y))^p$ arises at least p times, we obtain that $q(X, Y)^p = q(X^p, Y^p)$ divides $f(X) - g(Y) = f_0(X^p) - g_0(Y^p)$, and the claim follows in this case.

It remains to look at the case that $p = 2$ and $q(X, Y) = q_1(X, Y)q_2(X, Y)$ is a nontrivial factorization over L. If q_1 and q_2 do not differ by a factor, then as above $q_1(X, Y)^2$ and $q_2(X, Y)^2$ divide $u(X)^2 - v(Y)^2$, so $q(X, Y)^2$ divides $u(X)^2 - v(Y)^2$, and we conclude as above.

Thus $q(X, Y) = \delta(\alpha X + Y + \beta)^2$ for some $\alpha, \beta \in L$, $\delta \in K$. Then $q(X, Y) = \delta(aX^2+Y^2+b)$ with $a, b \in K$ divides $f_0(X^2)-g_0(Y^2)$, so $aX+Y+b$ divides $f_0(X) - g_0(Y)$, hence $g_0(X) = f_0(aX + b)$, and the claim follows.

Remark 3.1. The method of the paper is easily extended to the study of degree 2 factors of polynomials of the form $a(X)b(Y) - c(X)d(Y)$, where a, b, c, d are polynomials. For if $q(X, Y)$ is a quadratic factor, x is a transcendental, and y chosen with $q(x, y) = 0$, then $a(x)/c(x) = d(y)/b(y)$, so setting $t = a(x)/c(x) = d(y)/b(y)$ and studying the field extension $K(x, y)/K(t)$ requires only minor extensions of the arguments given in the paper.

References

[BG05] F. Berrondo, L. Gallardo, *Factors of small degree of some difference polynomials $f(x) - g(t)$ in $F[t][x]$*, Publ. Math. Debrecen (2005), **67**(3-4), 305–314.

[Bil99] Y. F. Bilu, *Quadratic factors of $f(x) - g(y)$*, Acta Arith. (1999), **90**(4), 341–355.

[Tur95] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A (1995), **58**, 312–357.

[Tur99] G. Turnwald, *Some notes on monodromy groups of polynomials*, in *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, de Gruyter, Berlin, 1999 pp. 539–552.

Poornaprajna Institute of Scientific Research, Davanhalli, Bangalore, India

Institut für Mathematik, Universität Würzburg, Am Hubland, D-97074 Würzburg, Germany
E-mail: Peter.Mueller@mathematik.uni-wuerzburg.de
URL: www.mathematik.uni-wuerzburg.de/~mueller

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