DIFFERENCE POLYNOMIALS AND THEIR GENERALIZATIONS

Saurabh Bhatia*and Sudesh K. Khanduja†

§1. *Introduction.* In 1956, Ehrenfeucht [3] proved that a difference polynomial $f(X) - g(Y)$ in two variables X, Y with complex coefficients is irreducible provided the degrees of f and g are coprime. Angermüller [2] gave a similar irreducibility criterion for a larger class of polynomials with coefficients in any field k, viz. the class of *'generalized difference polynomials'*. Recall that a polynomial $P(X,Y)$ is said to be a generalized difference polynomial (with respect to X) of the type (d,e) if $P(X,Y) = cX^e + \sum\limits_{i=1}^{e} P_i(Y)X^{e-i}$, where $c \in k^*, e \geq 1,\ d = degP_e(Y) \geq 1$ and $degP_i(Y) < di/e$ for $1 \leq i \leq e-1$. It will be shown that contrary to appearances, the property of being a generalized difference polynomial is actually symmetric in X and Y (see Lemma 5.1). It is immediate from the definition that if $P(X,Y)$ is a generalized difference polynomial of the type (d,e), then $d = deg_Y P(X,Y) = degP_e(Y)$.

*This research is supported by CSIR, India vide grant No. 9/135(355)/99/EMR-I

†This research is partially supported by CSIR, India vide grant No. 25(0095)/97/EMR-II

In this paper, we study irreducibility conditions of more general polynomials given by $F(X,Y) = cX^e + \sum_{i=1}^{e} P_i(Y)X^{e-i}$, $c \in k^*$, $e \geq 1$, such that there exists t, $1 \leq t \leq e$ satisfying $deg_Y F(X,Y) = deg P_t(Y) = d$ and $deg P_i(Y) < di/t$ for $i \neq t$, $1 \leq i \leq e$. Such a polynomial $F(X,Y)$ will be referred to as *a quasi-difference polynomial of the type* (d,t) *with respect to* X. In 1990, L. Panaitopol and D. Stefănescu proved that a quasi-difference polynomial of the type (d,t) with d and t coprime is irreducible over $k[X]$ (cf. [5, Theorem 6]). In this direction, we go further and give an irreducibility criterion for a quasi-difference polynomial of the type (d,t) with d and t not necessarily coprime, of which the criterion of Panaitopol and Stefănescu is a special case. Our method of proof is different from the one employed in [2] and [5], and is based on the idea of the proof of the Generalized Eisenstein's Irreducibility Criterion given in [4].

We shall prove:

THEOREM 1.1. *Let* $P(X,Y) = cX^e + P_1(Y)X^{e-1} + ... + P_e(Y)$ *be a quasi-difference polynomial of the type* (d,t) *with respect to* X *over a field* k. *Let* c_0 *denote the coefficient of the monomial* $X^{e-t}Y^d$ *in* $P(X,Y)$ *and* r *the gcd of* d *and* t. *If the polynomial* $X^r + cc_0^{-1}$ *is irreducible over* k, *then* $P(X,Y)$ *is irreducible over* $k[X]$.

THEOREM 1.2. *Let* $P(U,V) = cU^e + \sum_{i=1}^{e} P_i(V)U^{e-i}$ *be a quasi-difference polynomial of the type* (d,t) *with respect to* U *having coefficients in a field* k *in the variables* U, V. *Let* $f(X)$, $g(Y)$ *be non-constant polynomials over* k *with degrees* m, n *and leading coefficients* α, β *respectively. Let* r *denote* $gcd(dn, tm)$ *and* c_0 *be the coefficient of* $U^{e-t}V^d$ *in* $P(U,V)$. *If* $X^r + \dfrac{c\alpha^t}{c_0\beta^d}$ *is irreducible over* k, *then* $P(f(X), g(Y))$ *is irreducible over* $k[X]$.

THEOREM 1.3. *Let* $P(U,V)$ *be a generalized difference polynomial of the type* (d,e) *over a field* k. *Let* c_0 *be the coefficient of the monomial* V^d *in* $P(U,V)$. *Let* $f(X)$ *and* $g(Y)$ *be non-constant polynomials with coefficients in* k *having degrees* m, n *and leading coefficients* α, β *respectively. If* r *denotes* $gcd(dn,\ em)$ *and the polynomial* $X^r + \dfrac{c\alpha^e}{c_0\beta^d}$ *is irreducible over* k, *then* $P(f(X), g(Y))$ *is irreducible in* $k[X,Y]$.

It may be pointed out that the above theorem was proved with different methods by Angermüller when $dn,\ em$ are coprime and $X = (X_1, ..., X_l)$ and $Y = (Y_1, ..., Y_s)$ are independent systems of variables over k (see [2, p.80]).

It is a great pleasure to thank the referee for constructive suggestions to improve the exposition.

§2. *Notations, definitions and preliminary results.* Let v be a valuation of a field K with value group G_v, residue field k_v and valuation ring R_v. For any $\xi \in R_v$, ξ^* will denote the v-residue of ξ, i.e., the image of ξ under the canonical homomorphism from R_v onto k_v. In what follows $K(X)$ will denote a simple transcendental extension of K. If $p(X)$ is a fixed nonzero polynomial of $K[X]$, then each $f(X) \in K[X]$ can be uniquely represented as $f(X) = \sum\limits_{i \geq 0} f_i(X)[p(X)]^i$, where for any i, the polynomial $f_i(X)$ is either zero or has degree less than that of $p(X)$. The above representation will be referred to as the canonical representation of $f(X)$ with respect to $p(X)$. Let $\bar{v}$ be a fixed prolongation of the valuation v defined on K to an algebraic closure $\overline{K}$ of K whose value group will be denoted by $\overline{G}_v$. A pair $(a, \delta) \in \overline{K} \times \overline{G}_v$ will be called minimal (with respect to K and $\bar{v}$) if for every $b \in \overline{K}$, the condition $\bar{v}(a-b) \geq \delta$ implies $[K(a) : K] \leq [K(b) : K]$. The valuation $\bar{w}$ of $\overline{K}(X)$, defined on $\overline{K}[X]$ by $\bar{w}(\sum\limits_i c_i(X-a)^i) = \min\limits_i\{\bar{v}(c_i) + i\delta\}$ will be referred to as the valuation defined by the minimal pair (a, δ). The following theorem is already known (cf. [1, Theorem 2.1], [4, Theorem 2.1]). We omit its proof.

THEOREM A. *Let $\bar{w}$ be the valuation of $\overline{K}(X)$ defined by a minimal pair (a, δ). Let v_1, w be the valuations obtained by restricting $\bar{w}$ to $K(a)$, $K(X)$ respectively with value groups G_{v_1}, G_w and residue fields k_{v_1}, k_w.*
(a) If $p(X)$ is the minimal polynomial of a over K of degree n and $\bar{w}(p(X)) = \gamma$, then for any $f(X) \in K[X]$ having canonical representation $\sum\limits_i f_i(X)[p(X)]^i$

with respect to $p(X)$, we have $w(f(X)) = \min_i(\bar{v}(f_i(a)) + i\gamma)$.

(b) If $g(X) \in K[X]$ is a polynomial of degree less than n, then the $\bar{w}$-residue of $g(X)/g(a)$ equals one.

(c) Let e be the smallest positive integer such that $e\gamma \in G_{v_1}$. If $h(X) \in K[X]$ is a polynomial of degree less than n with $w(h(X)) = e\gamma$, then the w-residue r^* of $r(X) = p(X)^e/h(X)$ is transcendental over k_{v_1} and k_w is canonically isomorphic to $k_{v_1}(r^*)$.

Definition. Let (a, δ) be a minimal pair (with respect to K and $\bar{v}$) and $\bar{w}$, v_1, $p(X)$, n, e, and γ be as in the above theorem. Let $F(Z) \in k_{v_1}[Z]$ be a monic polynomial of degree m in an indeterminate Z. As in [4], a monic polynomial $f(X) \in K[X]$ of degree emn is called a lifting of $F(Z)$ relative to the minimal pair (a, δ) if there exists $h(X) \in K[X]$ of degree less than n satisfying the following conditions:

(i) $\bar{w}(f) = m\bar{w}(h) = me\gamma$;

(ii) the $\bar{w}$-residue $(f/h^m)^*$ of (f/h^m) is $F((p^e/h)^*)$.

We need the following already known theorem (see [4, Theorem 2.2]).

THEOREM B. *Let v be a valuation of a field K and (a, δ) be a minimal pair with respect to the prolongation $\bar{v}$ of v to $\overline{K}$. Let k_{v_1} be the residue field of the valuation v_1 obtained by restricting $\bar{v}$ to $K(a)$. If $F(Z) \neq Z$ is a monic* *irreducible polynomial over* k_{v_1}, *then any lifting of* $F(Z)$ *is irreducible over* K.

§3. *Proof of Theorem 1.1.* We first prove a proposition which will be used in the proof of the theorem and is also of independent interest.

PROPOSITION 3.1. *Let* v *be a valuation of a field* K *with value group the set of rational integers. Let* $g(x) = x^d + a_1x^{d-1} + ... + a_d$ *be a polynomial over* K *such that* $v(a_i)/i > v(a_d)/d$ *for* $1 \leq i \leq d-1$. *Let* r *denote* $gcd(v(a_d), d)$ *and* b *be an element of* K *with* $v(b) = v(a_d)/r$. *Suppose that the polynomial* $Z^r + (a_d/b^r)^*$ *in the indeterminate* Z *is irreducible over the residue field of* v. *Then* $g(x)$ *is irreducible over* K.

Proof. Fix an algebraic closure $\overline{K}$ of K and a prolongation $\bar{v}$ of v to $\overline{K}$. Set $\delta = v(a_d)/d$. Let $\bar{w}$ be the valuation of $\overline{K}(x)$ defined by the minimal pair $(0, \delta)$ and w be its restriction to $K(x)$. The hypothesis $v(a_i)/i > v(a_d)/d$, $1 \leq i \leq d-1$ implies that

$$w(a_ix^{d-i}) = v(a_i) + (d-i)\delta > d\delta = v(a_d) = v(b^r).$$

Therefore by virtue of Theorem A (on taking $a_0 = 1$), we conclude that

$$w(g(x)) = \min_{0\leq i\leq d}(\bar{v}(a_i) + (d-i)\delta) = \bar{v}(a_d)$$

and the w-residue of $(g(x)/b^r)$ is $(x^d/b^r)^* + (a_d/b^r)^*$. If the notations γ, e and h

have the same meaning as in the previous section, then corresponding to the valuation w defined by the minimal pair $(0, \delta)$, we have

$$\gamma = w(x) = \delta = v(a_d)/d.$$

As e is the smallest positive integer such that $e\gamma = ev(a_d)/d$ belongs to the set of rational integers, it follows that in the present situation $e = d/r$. Since $v(b) = v(a_d)/r = e\gamma$, on taking $h = b$, we see that $g(x)$ is a lifting of $Z^r + (a_d/b^r)^*$ with respect to the minimal pair $(0, \delta)$. As $Z^r + (a_d/b^r)^*$ is given to be ireducible over the residue field of v, the proposition follows immediately from Theorem B.

Proof of Theorem 1.1. Since $P(X, Y) = cX^e + P_1(Y)X^{e-1} + ... + P_e(Y)$ has degree d in Y, we can write

$$P(X, Y) = F_0(X)Y^d + F_1(X)Y^{d-1} + ... + F_d(X),\ F_i(X) \in k[X].$$

Observe that

$$deg F_d(X) = e. \tag{1}$$

The property $\max\limits_{1 \le i \le e}\{(deg P_i(Y))/i\} = d/t$ together with the condition $deg P_t(Y) = d$ of a quasi-difference polynomial immediately implies that

$$deg F_0(X) = e - t. \tag{2}$$

The theorem is proved once we show that

$$g(Y) = Y^d + A_1(X)Y^{d-1} + ... + A_d(X) \tag{3}$$

is irreducible over $k(X)$, where $A_i(X) = F_i(X)/F_0(X),\ 1 \leq i \leq d$.

Put $K = k(X)$. Let v be the valuation defined on K by

$$v(f(X)/g(X)) = deg(g(X)) - deg(f(X)).$$

We first show that

$$v(A_i(X))/i > v(A_d(X))/d,\ 1 \leq i \leq d-1. \tag{4}$$

It is clear from (1) and (2) that

$$v(A_d(X)) = degF_0(X) - degF_d(X) = -t.$$

Therefore (4) holds if and only if

$$\frac{e - t - degF_i(X)}{i} > \frac{-t}{d},\ 1 \leq i \leq d-1,$$

i.e., if and only if

$$degF_i(X) < (e-t) + (it/d),\ 1 \leq i \leq d-1. \tag{5}$$

Recall that $F_i(X)$ is the coefficient of Y^{d-i} in $P(X,Y) = cX^e + \sum_{i=1}^{e} P_i(Y)X^{e-i}$. Therefore (5) is proved as soon as we show that if for any j, $degP_j(Y) \geq d-i$, then

$$e - j < (e-t) + (it/d). \tag{6}$$

The inequality (6) is trivially true when $j = t$. If $j \neq t$ and if $degP_j(Y) \geq d-i$, then by virtue of the hypothesis $deg(P_j(Y))/j < d/t$, we have

$$(d-i)/j < d/t. \tag{7}$$

It can be easily checked that the inequality (7) can be rewritten as (6). Thus (4) is proved.

We apply Proposition 3.1 to establish the irreducibility of the polynomial $g(Y)$ given by (3) over $K = k(X)$. Recall that $gcd(d,t) = r$ and c_0 is the leading coefficient of $F_0(X)$ by virtue of the hypothesis. By virtue of (1) and (2), $v(A_d) = -t$. If we take $b = X^{t/r}$, then the v-residue of (A_d/b^r) is $(\dfrac{F_d(X)}{X^t F_0(X)})^*$. Since the leading coefficient of $F_0(X)$, $F_d(X)$ are c_0, c respectively and $v(X^{-1}) > 0$, we conclude that the v-residue of A_d/b^r is c/c_0. As the polynomial $Z^r + cc_0^{-1}$ is given to be irreducible over the residue field k of v, the theorem follows immediately from Proposition 3.1.

§4. *Proof of Theorem 1.2.* The first assertion of the following lemma is already known (cf. [5, Lemma 4]). However for the sake of completeness, we give an elementary and self-contained proof.

LEMMA 4.1. *Let $P(U,V)$ be a quasi-difference polynomial of the type (d,t) with respect to U and let $f(X)$, $g(Y)$ be non-constant polynomials of respective degrees m, n. Then*

(i) P(f(X), g(Y)) is a quasi-difference polynomial of the type (dn, tm) with respect to X.

(ii) If the coefficient of $U^{e-t}V^d$ in $P(U,V)$ is c_0, then the coefficient of

$X^{em-tm}Y^{dn}$ *in* $P(f(X),g(Y))$ *is* $c_0\alpha^{e-t}\beta^d$, *where* $\alpha,\ \beta$ *are respectively the leading coefficients of* $f(X)$ *and* $g(Y)$.

Proof. Write

$$P(U,V) = cU^e + P_1(V)U^{e-1} + ... + P_e(V).$$

We shall denote $P(f(X),g(Y))$ by $q(X,Y)$. Clearly

$$q(X,Y) = c\alpha^e X^{me} + F_1(Y)X^{me-1} + F_2(Y)X^{me-2} + ... + F_{em}(Y).$$

For assertion (i) we need to show that

$$deg_Y q(X,Y) = deg(F_{tm}(Y)) = dn \tag{8}$$

and

$$\frac{degF_j(Y)}{j} < \frac{dn}{tm},\ 1 \le j \le em,\ j \ne tm. \tag{9}$$

It is trivial to verify that $degF_i(Y) \le 0$ for $1 \le i \le m-1$ and $degF_{m+l}(Y) \le degP_1(g(Y))$ for $0 \le l \le m-1$. In fact

$$degF_{im+l}(Y) \le max\{degP_1(g(Y)),...,degP_i(g(Y))\},\ 1 \le i \le e,\ 0 \le l \le m-1. \tag{10}$$

Keeping in view that $deg_V(P(U,V)) = d$, it is clear that $deg_Y(q(X,Y)) = dn$. Since $degP_t(V) = d$ and $degP_j(V) < jd/t < d$ for $j < t$, it follows that $degP_j(g(Y)) < dn$ for $j < t$, $degP_t(g(Y)) = dn$ and the coefficient of

$X^{(e-t)m}Y^{dn}$ is $c_0\alpha^{e-t}\beta^d$. This proves (8) and assertion (ii) of the lemma.

Observe that (9) is trivially true for $j > tm$, because $degF_j(Y) \leq dn$ by virtue of (8). Fix any $j < tm$. By the division algorithm write $j = sm+l,\ 0 \leq l \leq m-1$ so that $s < t$. By (10), we have

$$degF_j(Y) \leq max\{degP_1(g(Y)), ..., degP_s(g(Y))\}. \tag{11}$$

Since $P(U, V)$ is a quasi-difference polynomial, we have

$$degP_i(V) < id/t \text{ for } i \neq t.$$

Therefore (11) implies that

$$degF_j(Y) < sdn/t$$

which gives

$$\frac{degF_j(Y)}{sm} < \frac{dn}{tm}.$$

Keeping in view that $j \geq sm$, (9) follows. This completes the proof of the lemma.

Theorem 1.2 quickly follows from the above lemma and Theorem 1.1.

§5. *Proof of Theorem 1.3.* We first prove an elementary lemma.

LEMMA 5.1. *Let $P(U, V) = cU^e + P_1(V)U^{e-1} + ... + P_e(V)$ be a generalized difference polynomial with respect to U of type (d, e). Then it is also a* *generalized difference polynomial with respect to* V *of type* (e, d).

Proof. Write $P(U,V) = cU^e + P_1(V)U^{e-1} + ... + P_e(V)$ as

$$c'V^d + F_1(U)V^{d-1} + ... + F_d(U).$$

To prove the lemma, we have to show that

$$degF_i(U) < ie/d, \ 0 < i < d. \tag{12}$$

Clearly (12) is proved once we show that whenever j is such that $degP_j(V) \geq d - i$, then

$$e - j < ie/d. \tag{13}$$

By the definition of a generalized difference polynomial, $degP_j(V)/j < d/e, \ 1 \leq j \leq d-1$. Consequently if $degP_j(V) \geq d - i$, we have

$$(d-i)/j < d/e.$$

A simple calculation shows that the last equation is equivalent to (13). This completes the proof of the lemma.

By virtue of the above lemma, $P(U,V)$ is a generalized difference polynomial and hence a quasi-difference polynomial with respect to both U and V. So by Theorem 1.2, $P(f(X), g(Y))$ is irreducible over $k[X]$ as well as over $k[Y]$ and hence is irreducible over k.

REFERENCES

1. V.Alexandru, N. Popescu and A. Zaharescu, A theorem of characterizaton of residual transcendental extension of a valuation, *J. Math. Kyoto Univ.,* 28 (1988), 579-592.

2. G. Angermüller, A generalization of Ehrenfeucht's irreducibility criterion, *J. Number Theory,* 36 (1990), 80-84.

3. A. Ehrenfeucht, Kryterium absolutnej nierozkladalnosci wielomianow, *Prace Math.,* 2 (1958), 167-169.

4. Sudesh K. Khanduja and Jayanti Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika,* 44 (1997), 37-41.

5. L. Panaitopol and D. Stefănescu, On the generalized difference polynomials, *Pacific J. Math.,* Vol 143, No. 2 (1990), 341-348.