Chapter 3

Difference polynomials and their generalizations

3.1 History of the problem and statements of the main results

In 1956, Ehrenfeucht [Ehr] proved that a difference polynomial \( f(x) - g(y) \) in two variables \( x, y \) with complex coefficients is irreducible over the field of complex numbers provided the degrees of \( f \) and \( g \) are coprime. Angermüller [Ang] gave a similar irreducibility criterion for a larger class of polynomials with coefficients in any field \( k \), viz. the class of 'generalized difference polynomials'. A polynomial \( P(x, y) \) is said to be a generalized difference polynomial (with respect to \( x \)) of the type \((d, e)\) if

\[
P(x, y) = c x^e + \sum_{i=1}^{e} P_i(y)x^{e-i}, \quad \text{where } 0 \neq c \in k, \ e \geq 1, \ d = \deg P_e(y) \geq 1 \text{ and }\]

\[
\deg P_i(y) < di/e \text{ for } 1 \leq i \leq e - 1. \]

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 3.5.1). It is immediate from the definition that if \( P(x, y) \) is a generalized difference polynomial of the type \((d, e)\), then \( d = \deg_x P(x, y) = \deg P_e(y) \).

In this chapter, we study irreducibility conditions of more general polynomials.
given by $F(x, y) = c x^e + \sum_{i=1}^{e} P_i(y) x^{e-i}, 0 \neq c \in k, e \geq 1$, such that there exists $t, 1 \leq t \leq e$ satisfying $\deg_y F(x, y) = \deg P_i(y) = d$ and $\deg P_i(y) < \frac{d_i}{t}$ 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 $x$. It may be pointed out that a difference polynomial $f(x) - g(y) = c x^e + c_1 x^{e-1} + ... + (c_e - g(y))$ is a generalized difference polynomial of the type $(d, e)$, where $d \geq 1, e \geq 1$ denote respectively the degrees of $g$ and $f$. Also every generalized difference polynomial of the type $(d, e)$ (with respect to $x$) is a quasi-difference polynomial of the same type, but the converse is not true, e.g., the polynomial $F(x, y) = c x^4 + c_1 x^3 y + c_2 x^2 (y^3 + y) + c_3 x (y^4 + y^3) + c_4 y^4$, with the coefficients $c, c_2$ being non-zero, is a quasi-difference polynomial of the type $(4, 2)$ with respect to $x$, which is not a generalized difference polynomial as $d = 4, e = 4$ and $\deg P_i(y) > \frac{d_i}{e}$ for $i = 2$.

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. [Pa-St, 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 [Ang] and [Pa-St], and is based on the idea of the proof of a generalization of Eisenstein’s Irreducibility Criterion given in [Kh-Sal].

In this chapter, our main aim is to prove:

**THEOREM 3.1.1.** Let $P(x, y) = c x^e + P_1(y) x^{e-1} + ... + P_e(y)$ be a quasi-difference polynomial of the type $(d, t)$ with respect to $x$ over a field $k$. Let $c_0$ denote the leading coefficient of $P_i(y)$ and $r$ the gcd of $d$ and $t$. If the polynomial $x^r + c_0 r^{-1}$ is irreducible over $k$, then $P(x, y)$ is irreducible over $k(x)$.

In fact, pushing our arguments further, we shall prove a result which is more general than the above theorem. Indeed we prove:
THEOREM 3.1.2. 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 $\alpha, \beta$ respectively. Let $r$ denote $\gcd(dn, tm)$ and $c_0$ be the coefficient of $U^{e-t}V^d$ in $P(U, V)$. If $x^r + \frac{\alpha \beta}{c_0}$ is irreducible over $k$, then $P(f(x), g(y))$ is irreducible over $k(x)$.

THEOREM 3.1.3. 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 $\alpha, \beta$ respectively. If $r$ denotes $\gcd(dn, em)$ and the polynomial $x^r + \frac{\alpha \beta}{c_0}$ is irreducible over $k$, then $P(f(x), g(y))$ is irreducible in $k$.

The following corollary, which generalizes irreducibility criterion for difference polynomials due to Tverberg [Tve], is an immediate consequence of the above theorem. Recall that Tverberg proved that a polynomial $P(x) - Q(y)$ over any field $k$ is irreducible provided the degrees of $P$ and $Q$ are coprime.

COROLLARY 3.1.4. Let $P(x)$ and $Q(y)$ be two polynomials with coefficients in a field $k$ having degrees $e, d$ and leading coefficients $c, c_0$ respectively. If $r$ is the $\gcd$ of $d, e$ and if the polynomial $x^r - \frac{c}{c_0}$ is irreducible over $k$, then so is $P(x) - Q(y)$.

It may be pointed out that Theorem 3.1.2 was proved with different methods by Panaitopol and Ştefănescu in the particular case when $r = 1$ (see [Pa-St]). Theorem 3.1.1 extends a recent result of Cohen, Movahhedi and Salinier which has been proved by them for generalized difference polynomials using Newton polygons (see [C-M-S, Theorem 1.7]).

For obtaining the above results, we have used the following theorem which generalizes Eisenstein’s Irreducibility Criterion and thus is of independent interest as well.
THEOREM 3.1.5. (A Generalization of Eisenstein’s Irreducibility Criterion).
Let \( v \) be a valuation of a field \( K \) with value group the set of rational integers. Let 
\[ g(x) = x^d + a_1 x^{d-1} + \ldots + a_d \]
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 \( K \).

Towards the end of the chapter, we give some applications of the above theorems.

3.2 Proof of a generalization of Eisenstein’s Irreducibility Criterion

We now prove Theorem 3.1.5. Fix an algebraic closure \( \overline{K} \) of \( K \) and a prolongation 
\( \tilde{v} \) of \( v \) to \( \overline{K} \). Set \( \delta = v(a_d)/d \). Let \( \tilde{w} \) be the valuation of \( \overline{K}(x) \) corresponding to the 
minimal pair \((0, \delta)\) given by (2.1), 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

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

Therefore by virtue of Theorem 2.2.B (on taking \( a_0 = 1 \)), we conclude that

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

and the \( w \)-residue of \((g(x)/b^r)^* + (a_d/b^r)^*\) is \((x^d/b^r)^* + (a_d/b^r)^*\). If the notations \( \lambda, e \) and \( h \)
have the same meaning as in Theorem 2.1.A, then corresponding to the valuation 
\( w \) defined by the minimal pair \((0, \delta)\), we have

\[ \lambda = w(x) = \delta = v(a_d)/d. \]
As $e$ is the smallest positive integer such that $e\lambda = ev(a_d)/d$ belongs to the set of rational integers, it follows that in the present situation $e = d/r$. Since $v(b) = v(a_d)/r = e\lambda$, on taking $h = b$, we see that $g(x)$ is a lifting of $z'' + (a_d/b')^*$ with respect to the minimal pair $(0, \delta)$. As $z'' + (a_d/b')^*$ is given to be irreducible over the residue field of $v$, the irreducibility of $g(x)$ over $K$ follows from the fact that lifting of an irreducible polynomial is irreducible (cf. [Kh-Sa1, Theorem 2.2]).

3.3 Proof of Theorem 3.1.1

Since $P(x, y) = c x^e + P_1(y)x^{e-1} + \ldots + P_e(y)$ has degree $d$ in $y$, we can write

$$P(x, y) = F_0(x)y^d + F_1(x)y^{d-1} + \ldots + F_d(x), \quad F_i(x) \in k[x].$$

Observe that

$\deg F_d(x) = e. \quad (3.1)$

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

$\deg F_0(x) = e - t. \quad (3.2)$

The theorem is proved once we show that

$$g(y) = y^d + A_1(x)y^{d-1} + \ldots + A_d(x) \quad (3.3)$$

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
\[ \frac{v(A_i(x))}{i} > \frac{v(A_d(x))}{d}, \quad 1 \leq i \leq d - 1. \tag{3.4} \]

It is clear from (3.1) and (3.2) that
\[ v(A_d(x)) = \deg F_0(x) - \deg F_d(x) = -t. \]

Therefore (3.4) holds if and only if
\[ \frac{e - t - \deg F_i(x)}{i} > \frac{-t}{d}, \quad 1 \leq i \leq d - 1, \]
i.e., if and only if,
\[ \deg F_i(x) < (e - t) + \left( \frac{it}{d} \right), \quad 1 \leq i \leq d - 1. \tag{3.5} \]

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 (3.5) is proved as soon as we show that if for any \( j \), \( \deg P_j(y) \geq d - i \), then
\[ e - j < (e - t) + \left( \frac{it}{d} \right). \tag{3.6} \]

The inequality (3.6) is trivially true when \( j = t \). If \( j \neq t \) and if \( \deg P_j(y) \geq d - i \), then by virtue of the hypothesis \( \deg(P_j(y))/j < d/t \), we have
\[ (d - i)/j < d/t. \tag{3.7} \]

It can be easily checked that the inequality (3.7) can be rewritten as (3.6). Thus (3.4) is proved.

We apply Theorem 3.1.5 to establish the irreducibility of the polynomial \( g(y) \) given by (3.3) 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 (3.1) and (3.2), \( v(A_d) = -t. \)
If we take $b = x^{t/r}$, then the $v$-residue of $(A_d/b^r)$ is $\left(\frac{F_d(x)}{x^tF_0(x)}\right)^*$. Since by hypothesis the leading coefficient of $F_0(x)$, $F_d(x)$ are $c_0$, respectively and $v(x^{-1}) > 0$, we conclude that the $v$-residue of $A_d/b^r$ is $c/c_0$. As the polynomial $z^t + cc_0^{-1}$ is given to be irreducible over the residue field $k$ of $v$, the theorem follows immediately from Theorem 3.1.5.

REMARK 3.3.1. Our method of proof shows that if $P(x, y)$ satisfies the hypothesis of the above theorem, then $P(x, y)$ is indeed irreducible over $k((x))$, i.e., the field of Laurent series in $x$.

3.4 Proof of Theorem 3.1.2

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

LEMMA 3.4.1. 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 $U^mV^n$ in $P(U, V)$ is $c_0$, then the coefficient of $x^{en-tn}y^{dn}$ in $P(f(x), g(y))$ is $c_0\alpha^{en-tn}\beta^d$, 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

\[
q(x, y) = cae^{x^{me}} + F_1(y)x^{me-1} + F_2(y)x^{me-2} + \ldots + F_{em}(y).
\]

For assertion (i) we need to show that

\[
\deg_y q(x, y) = \deg(F_{tm}(y)) = dn
\]

and

\[
\frac{\deg F_j(y)}{j} < \frac{dn}{tm}, \quad 1 \leq j \leq em, \quad j \neq tm.
\]

It is trivial to verify that \( \deg F_i(y) \leq 0 \) for \( 1 \leq i \leq m - 1 \) and \( \deg F_{m+t}(y) \leq \deg P_l(g(y)) \) for \( 0 \leq l \leq m - 1 \). In fact

\[
\deg F_{m+t}(y) \leq \max\{\deg P_1(g(y)), \ldots, \deg P_t(g(y))\}, \quad 1 \leq i \leq e, \quad 0 \leq l \leq m - 1. \quad (3.10)
\]

Keeping in view that \( \deg_v(P(U, V)) = d \), it is clear that \( \deg_y(q(x, y)) = dn \). Since \( \deg P_l(V) = d \) and \( \deg P_j(V) < jd/t < d \) for \( j < t \), it follows that \( \deg F_j(g(y)) < dn \) for \( j < t \), \( \deg P_t(g(y)) = dn \) and the coefficient of \( x^{(e-t)m}y^{dn} \) is \( c_0\alpha^{e-t}d^d \). This proves (3.8) and assertion (ii) of the lemma.

Observe that (3.9) is trivially true for \( j > tm \), because \( \deg F_j(y) \leq dn \) by virtue of (3.8). Fix any \( j < tm \). By the division algorithm write \( j = sm + l, \quad 0 \leq l \leq m - 1 \) so that \( s < t \). By (3.10), we have

\[
\deg F_j(y) \leq \max\{\deg P_1(g(y)), \ldots, \deg P_s(g(y))\}. \quad (3.11)
\]

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

\[
\deg P_i(V) < id/t \text{ for } i \neq t.
\]
Therefore (3.11) implies that

\[ \deg F_j(y) < sdn/t \]

which gives

\[ \frac{\deg F_j(y)}{sm} < \frac{dn}{tm}. \]

Keeping in view that \( j > sm \), (3.9) follows. This completes the proof of the lemma.

Theorem 3.1.2 quickly follows from the above lemma and Theorem 3.1.1.

3.5 Proof of Theorem 3.1.3 and some examples

We first prove an elementary lemma.

**LEMMA 3.5.1.** Let \( P(U, V) = cU^e + P_1(V)U^{e-1} + \ldots + P_e(V) \) 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 \( P(U, V) = cU^e + P_1(V)U^{e-1} + \ldots + P_e(V) \) as

\[ cV^d + F_1(U)V^{d-1} + \ldots + F_d(U). \]

To prove the lemma, we have to show that

\[ \deg F_i(U) < ie/d, \; 0 < i < d. \] (3.12)

Clearly (3.12) is proved once we show that whenever \( j \) is such that \( \deg P_j(V) \geq d-i \), then

\[ e - j < ie/d. \] (3.13)

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

\[
\frac{d - i}{j} < \frac{d}{e}.
\]

A simple calculation shows that the last equation is equivalent to (3.13). 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 3.1.2, \( P(f(x), g(y)) \) is irreducible over \( k(x) \) as well as over \( k(y) \) and hence is irreducible over \( k \). This proves the theorem.

We now give some applications of the results of this chapter.

EXAMPLE 3.5.2. The polynomial \( F(x, y) = cx^4 + c_1x^3y + c_2x(y^4 + y) + c_3x(y^4 + y^3) + c_4y^4 \) is irreducible over the field of real numbers for all values of \( c_1, c_3 \) and all non-zero values of \( c, c_4 \). To verify this, note that \( F(x, y) \) is a quasi-difference polynomial of the type \((4, 2)\) (with respect to \( x \)). With notations as in Theorem 3.1.1, here \( r = 2 \) and \( c_0 = c \). Irreducibility of \( F(x, y) \) over \( \mathbb{R}(x) \) follows from Theorem 3.1.1, because the polynomial \( x^2 + 1 \) is irreducible over \( \mathbb{R} \). Indeed \( F(x, y) \) is irreducible over \( \mathbb{R} \) because \( c_4 \neq 0 \).

EXAMPLE 3.5.3. Let \( n, m \) be positive integers with gcd \( 2^i \) for some integer \( i \geq 0 \). Let \( u_1, \ldots, u_s \) be positive integers (not necessarily distinct and none of which exceeds \( n - 1 \)) and \( v_1, \ldots, v_s \) be non-negative integers (not necessarily distinct) such that \( \frac{u_j}{u_i} < \frac{m}{n} \) for \( 1 \leq j \leq s \). Then the polynomial \( F(x, y) = x^n + \sum_{j=1}^{s} c_jx^{n-u_j}y^{v_j} + y^m \) is irreducible over \( \mathbb{Q} \) for all rational numbers \( c_1, \ldots, c_s \). To prove this, observe that \( F(x, y) \) is a generalized difference polynomial of the type \((m, n)\) (with respect to \( x \)). Its irreducibility over \( \mathbb{Q} \) follows from Theorem 3.1.3 (on taking \( f(x) = x, g(y) = y \)) once we verify that the polynomial \( q(x) = x^2 + 1 \) is irreducible over \( \mathbb{Q} \). To verify
the above assertion, it is enough to note that

\[
q(x + 1) = (x + 1)^{2^t} + 1
= x^{2^t} + 2^t x^{2^t - 1} + \ldots + 2
\]

is an Eisenstein polynomial with respect to the prime 2.