A DISCRIMINANT CRITERIA FOR REDUCIBILITY OF A POLYNOMIAL

BY

M. FRIED** AND S. FRIEDLAND***

*Department of Mathematics, University of California at Irvine, Irvine, CA 92717, USA ;
and **Institute of Mathematics, The Hebrew University of Jerusalem, Jerusalem, Israel

ABSTRACT

Let \( p(w) \) be a polynomial over a domain \( K \). If \( p \) splits to linear factors then the discriminant \( D(p) \) is a square in \( K \). In this paper we state an additional condition on the roots of \( p \) which together with the discriminant condition imply the splitting of \( p \) in case that \( K = \mathbb{C}[z] \) or \( \mathbb{Z} \). Some extensions are also discussed.

1. Introduction

Let \( K \) be a domain (a commutative ring without zero divisors) with unity. As usual denote by \( K[w_1, \ldots, w_t] \) the ring of polynomials in \( t \) variables \( w_1, \ldots, w_t \).

Assume that \( p(w) \) and \( q(w) \) are monic polynomials in \( K[w] \). That is

\[
\begin{align*}
    p(w) &= w^n + a_1 w^{n-1} + \cdots + a_n, \\
    q(w) &= w^m + b_1 w^{m-1} + \cdots + b_m, \\
        a_i, b_j \in K, & \quad i = 1, \ldots, n, \quad j = 1, \ldots, m.
\end{align*}
\]

Let \( \tilde{K} \) be an algebraic closure of \( K \). Thus \( p(w) \) and \( q(w) \) split into linear factors over \( \tilde{K} \):

\[
\begin{align*}
    p(w) &= (w - \lambda_1) \cdots (w - \lambda_n), \\
    q(w) &= (w - \mu_1) \cdots (w - \mu_m).
\end{align*}
\]

The resultant \( R(p, q) \) and the discriminant \( D(p) \) are defined to be

\[
\begin{align*}
    R(p, q) &= \prod_{1 \leq i < j \leq n} (\lambda_i - \lambda_j), \quad D(p) &= \prod_{1 \leq i < j < k \leq n} (\lambda_i - \lambda_j)^2.
\end{align*}
\]

* Visiting Lady Davis Research Professor at the Hebrew University of Jerusalem, Fall Semester, 1984.

** Supported in part by US-Israel Binational Science Foundation grant 3225/84.

Current address: Department of Mathematics, University of Illinois, Chicago, IL 60680, USA.

Received March 11, 1985.
It is well known that $R(p, q)$ and $D(p)$ are polynomials in the corresponding coefficients

$$R(p, q) = R(a_1, \ldots, a_m, b_1, \ldots, b_m), \quad D(p) = D(a_1, \ldots, a_n)$$

[6, Appendix 4, Sec. 9, 10]. That is, $R(p, q)$ and $D(p) \in K$ are well defined for any $p(w), q(w) \in K[w]$. Let $r(w)$ be a monic polynomial in $K[w]$. Suppose furthermore that $r(w)$ can be written as $p(w)q(w)$ with $p, q \in K[w]$ (i.e., $r(w)$ is reducible). Then (3) gives

$$D(p)D(q) = D(p)R(p, q)^3.$$  

Thus, there is a connection between the reducibility of $p$ and the form of $D(p)$. In particular, if $p(w)$ splits in $K$ then $D(p)$ is a square in $K$.

If, however, $D(p)$ is a square in $K$ we then can deduce, in general, the following condition. Let $\Omega_p$ be splitting field of $p(w)$. Denote the group of automorphisms of $\Omega_p$ which fix all the elements in $K$ by $G(\Omega_p, K)$. Since any element of $G(\Omega_p, K)$ acts faithfully on the roots $\lambda_1, \ldots, \lambda_n$ of $p$ we view $G(\Omega_p, K)$ as a subgroup of the symmetric group $S_n$.

Clearly, the condition that $D(p)$ is a square in $K$ is equivalent to the condition

$$\prod_{1 \leq i < j \leq n}(\lambda_i - \lambda_j) \in K.$$  

Thus, any $\sigma \in G(\Omega_p, K)$ must preserve the above product. In particular,

$$G(\Omega_p, K) \subset A_n$$

where $A_n$ is the alternating group of degree $n$.

Motzkin and Taussky [4] considered a condition, sufficient when combined with (5), to guarantee the splitting of $p(w)$ over $K$.

**Theorem 1** (Motzkin–Taussky). Let $p(w)$ be a monic polynomial in $w$ over $K[z, \zeta]$. Assume that $K$ is an algebraically closed field with characteristic not 2. Suppose also that $p(w) = p(w, z, \zeta)$ is a homogeneous polynomial. Then $p(w)$ splits into linear factors over $K[z, \zeta]$ if the following conditions hold:

(i) $D(p)$ is a square in $K[z, \zeta]$; and

(ii) for any fixed values $(z, \zeta) \neq (0, 0)$ the polynomial $p(w, z, \zeta)$ has neither triple roots nor two distinct double roots.

In fact Motzkin and Taussky stated this Theorem 1 for special polynomials

$$p(w, z, \zeta) = \det(wI - zA - \zeta B)$$

where $A$ and $B$ are $n \times n$ matrices with entries in $K$. But their proof applies for any $p(w, z, \zeta)$ satisfying the above condition.
The purpose of this paper is to generalize the Motzkin–Taussky theorem to two distinct cases. First we extend the above result to polynomials \( p(w) \) over the ring \( \mathbb{C}[z] \). Second we give a version of the above theorem for polynomials \( p(w) \) with integer coefficients. In the first case our main tool is the Riemann–Hurwitz formula. The second case is an application of a theorem of Minkowski [5, Theorem 5.4.10] and it responds to a question of H. Furstenberg.

The second author would like to thank Olga Taussky-Todd for her suggestion to extend the Motzkin–Taussky theorem. We dedicate this paper to her.

2. Reducible polynomials in two variables

Let \( K \) be \( \mathbb{C}[z] \), the ring of polynomials over the complex numbers. Assume that \( p = p(w, z) \in \mathbb{C}[w, z] \) is monic with respect to \( w \). Then the discriminant \( D(p) = D(z) \) is a polynomial in \( z \). Call \( p \) nondegenerate if \( D(p) \neq 0 \). Clearly \( p \) is degenerate if and only if \( p \) has a multiple factor. Assume that \( p \) is a nondegenerate monic polynomial of degree \( n \geq 2 \) in \( w \). Then \( \zeta \in \mathbb{C} \) is a zero of \( D(z) \) if and only if the equation

\[
 p(w, z) = 0
\]

has a multiple zero in \( w \) when \( z = \zeta \). If \( \zeta \) is not a zero of \( D(z) \), then (6) has \( n \) distinct roots (branches) \( w_1(z), \ldots, w_n(z) \) which are analytic in the neighborhood of \( \zeta \). It is, however, possible that \( D(\zeta) = 0 \), but (6) has \( n \) analytic branches in a neighborhood of \( \zeta \) (i.e., \( \zeta \) is a singular point of \( p \)). A point \( \zeta \) is a branch point if (6) has fewer than \( n \) analytic roots in the neighborhood of \( \zeta \). Again this implies that \( D(\zeta) = 0 \), and there is a minimal positive integer \( e(\zeta) \) such that the branches of (6) can be written as \( w_i((z - \zeta)^{1/e(\zeta)}) \), \( i = 1, \ldots, n \), where \( w_i(z), \ldots, w_n(z) \) are analytic in a neighborhood of \( z = 0 \). Let \( \mathbb{C}[[((z - \zeta)^{1/e(\zeta)})]] \) be the field of convergent Laurent series in \( (z - \zeta)^{1/e(\zeta)} \). This field has a canonical automorphism, denoted \( \sigma(\zeta) \), that is fixed on the elements of \( \mathbb{C}[[((z - \zeta))]] \). It acts on \( \alpha((z - \zeta)^{1/e(\zeta)}) \) where \( \alpha(z) \) is analytic in a neighborhood of \( z = \zeta \) by mapping it to \( \alpha(e^{2\pi i/e(\zeta)}(z - \zeta)^{1/e(\zeta)}) \). Regard \( \Omega_\zeta \) as a subfield of \( \mathbb{C}[[((z - \zeta)^{1/e(\zeta)})]] \). Since \( \Omega_\zeta \) is a splitting field over \( \mathbb{C}(z) \), and \( \sigma(\zeta) \) is fixed on \( \mathbb{C}(z) \), restriction of \( \sigma(\zeta) \) to \( \Omega_\zeta \) is an automorphism of \( \Omega_\zeta \). We continue to denote it by \( \sigma(\zeta) \).

We now explain the Riemann–Hurwitz formula [1, I. 27]. Just as for \( \zeta \in \mathbb{C} \) there is an element \( \sigma(\zeta) \) corresponding to \( \zeta = \infty \). That is, there is a minimal positive integer \( e(\zeta) \) such that \( w_1(z^{-1/e(\zeta)}), \ldots, w_n(z^{-1/e(\zeta)}) \) are branches of (6) where \( w_1, \ldots, w_n \) are meromorphic (not necessarily analytic) in a neighborhood of \( z = 0 \). For each \( \zeta \) satisfying \( D(\zeta) = 0 \) write \( \sigma(\zeta) \) (regarded as an element of
$S_n$) as a product of disjoint cycles $\beta_1 \cdots \beta_t$, with $\beta_i$ of length $s_i$, $i = 1, \ldots, t$.
Denote the sum $\Sigma_{i=1}^t (s_i - 1)$ by $\text{ind} (\sigma(\zeta))$, and do similarly for the element $\sigma(\infty)$.
Then the Riemann-Hurwitz formula may be stated as follows under the condition that $p(w, z)$ is irreducible:

$$2(\deg_+ (p) + g(p) - 1) = \sum_{\zeta \in \mathbb{C}} \text{ind} (\sigma(\zeta)) + \text{ind} (\sigma(\infty)).$$

where $g(p)$ is a nonnegative integer (the geometric genus of $p$). If $p(w, z)$ is reducible, write it as a product $p_1(w, z) \cdots p_u(w, z)$. Then formula (7) applies to each factor $p_i(w, z)$ separately if we restrict $\sigma(\zeta)$ to act on $\Omega_{p_i}$ (and the zeros of $p_i(w, z)$, $i = 1, \ldots, u$).
In what follows we state Theorems 4.22 and 4.24 of [3] and give alternative short proofs.

**Theorem 2.** Let $\zeta$ be a simple root of $D(z)$. Then $\text{ind} (\sigma(\zeta)) = 1$ and $\zeta$ is a branch point of (6) for which $p(w, \zeta) = 0$ has $n - 1$ distinct roots.

**Proof.** Regard $p(w, z)$ as a polynomial in $w$ with coefficients in $\mathbb{C}[[z - \zeta]] = K$. Over this field it factors as $p_1(w, z) \cdots p_u(w, z)$ where $\deg_+ (p_i), \ldots, \deg_+ (p_u)$ are the lengths of the disjoint cycles of $\sigma(\zeta)$ and all roots of $p_i(w, \zeta)$ are the same, $i = 1, \ldots, u$. Now assume that $\zeta$ is a simple root of $D(z)$. From formula (4) (applied inductively to $p_1, \ldots, p_u$) conclude that $p_i(w, \zeta), \ldots, p_u(w, \zeta)$ have no common roots, and at most one of these has degree exceeding 1. Assume that $p_i(w, \zeta)$ has $s$ multiple roots. We show that $(z - \zeta)^{s-1}$ divides $D(p_i)$. Since $\zeta$ is a simple root of $D(z)$, this gives $s = 2$ and the theorem is done.

Indeed, there is a function $w(z) = a_1 z + a_2 z^2 + \cdots$, analytic in a neighborhood of $z = 0$, such that $w((z - \zeta)^{1/s}), w(e^{2\pi i/s} (z - \zeta)^{1/s}), \ldots, w(e^{2\pi (s-1)i/s} (z - \zeta)^{1/s})$
are exactly the branches of $p_i(w, z) = 0$ in a neighborhood of $z = \zeta$. Therefore

$$D(p_i) = \prod_{0 \leq i < k \leq s - 1} ((a_1 e^{2\pi di/s} (z - \zeta)^{1/s} + \cdots) - (a_1 e^{2\pi ki/s} (z - \zeta)^{1/s} + \cdots))^2.$$  

Clearly this is divisible by $(z - \zeta)^{s-1} = (z - \zeta)^{s-1}$. This concludes the proof from the first paragraph.

**Theorem 3.** Let $\zeta$ be a root of $D(z)$ of even order. Then $\text{ind} (\sigma(\zeta))$ is even. Assume in addition that $\zeta$ is a double root of $D(z)$. Then one of the following holds.

(i) $p(w, \zeta) = 0$ has $n - 1$ distinct roots and all branches of $p(w, z) = 0$ are analytic in a neighborhood of $\zeta$;
(ii) \( p(w, \zeta) = 0 \) has \( n - 2 \) distinct roots and \( \sigma(\zeta) \) consists of one disjoint cycle of length 3; or
(iii) \( p(w, \zeta) = 0 \) has \( n - 2 \) distinct roots and \( \sigma(\zeta) \) consists of 2 disjoint cycles of length 2.

Proof. As we did in the proof of Theorem 2, consider \( p(w, z) \) over \( K = \mathbb{C}[\{z - \zeta\}] \). The condition that \( \zeta \) is a root of \( D(z) \) of even order is equivalent to \( D(z) = ((z - \zeta)^{h(z)})^2 \) where \( h(z) \neq 0 \) and \( h(z) \in K \). That is, \( D(z) \) is a square in \( K \). Therefore \( \sigma(\zeta) \) (the generator of \( G(\Omega_p/K) \)) is in \( A_n \) and \( \text{ind}(\sigma(\zeta)) \) is even. Again write \( p \) as \( p_1 \cdots p_n \), a product of irreducible factors over \( K \) with \( \text{deg}(p_i) = s_i \). For simplicity assume \( s_1 \geq s_2 \geq \cdots \geq s_n \). From the last paragraph of the proof of Theorem 2, \( \text{ind}(\sigma(\zeta)) = \sum_{i=1}^n s_i - 1 = s \leq 2l \) where \( s_1, \ldots, s_n \) are the lengths of the disjoint cycles of \( \sigma(\zeta) \). Now take \( l = 1 \). From (4), 2 times the number of analytic branches added to \( s \) is bounded by 2.

The case \( s = 0 \) implies that \( \sigma(\zeta) \) is the identity and corresponds to (i); and the case \( s = 2 \) corresponds to (ii) or (iii) depending on whether \( \sigma(\zeta) \) is a 3-cycle or a product of two disjoint 2-cycles.

Corollary 4. Let \( p(w, z) \in \mathbb{C}[w, z] \) be monic in \( w \) and of degree \( n \). Assume that \( D(z) \) is not identically zero, and that it has \( \zeta \) as a root of even order. If \( p(w, \zeta) = 0 \) has precisely \( n - 1 \) distinct roots, then all branches of \( p(w, z) = 0 \) are analytic in a neighborhood of \( \zeta \) (i.e., \( \sigma(\zeta) \) is the identity).

Proof. From Theorem 3, \( \text{ind}(\sigma(\zeta)) \) is even and \( n - \text{ind}(\sigma(\zeta)) \) is an upper bound for the number of distinct roots of \( p(w, \zeta) \). Conclude that \( \text{ind}(\sigma(\zeta)) = 0 \). That is, (i) of Theorem 3 holds.

We now generalize Theorem 1.

Theorem 5. Let \( p(w, z) \) be a monic nondegenerate polynomial of degree \( n \) in \( w \). Assume for each \( \zeta \in \mathbb{C} \) that
\[
(9) \quad p(w, \zeta) = 0 \text{ has at least } n - 1 \text{ distinct roots.}
\]
Assume also that \( D(p) \) is a square. Then \( p(w, z) \) splits into linear factors in \( w \).

Proof. For each \( \zeta \in \mathbb{C} \), Corollary 4 implies that \( \sigma(\zeta) \) is the identity. With no loss we may assume that \( p(w, z) \) is irreducible over \( \mathbb{C}(z) \). Apply the Riemann–Hurwitz formula in (7). As \( \text{ind}(\sigma(\zeta)) \leq n - 1 \) and \( g(p) \leq 0 \), we get \( 2(n - 1) \leq n - 1 \). The only possibility is that \( n = 1 \).

Theorem 6. Let \( p(w, z) \in \mathbb{C}[w, z] \) be a monic nondegenerate polynomial of degree \( n \) in \( w \). Assume for each \( \zeta \in \mathbb{C} \) that (9) holds. Suppose that \( D(z) \) has \( m \)
roots of odd order. Let \( p(w, z) = p_1(w, z) \cdots p_u(w, z) \) be the decomposition of \( p \) into irreducible monic factors in \( \mathbb{C}[w, z] \). Then

\[
\sum_{i \in \mathbb{N}} (\deg_n(p_i) - 1) \leq m.
\]

In particular, if \( m + 1 < n \), then \( p(w, z) \) is reducible. Also if \( m \geq 1 \), then there exists \( i \) such that \( \deg(p_i) \geq 2 \). Finally, if \( m = 1 \), then \( p(w, z) \) splits into one irreducible quadric and \( n - 2 \) linear factors in \( w \).

**Proof.** The assumptions (and (4)) imply that the roots of \( D(p_1), \ldots, D(p_u) \) are pairwise distinct, and the number of odd roots add up to \( m \).

Let \( m_i \) be the number of odd roots of \( D(p_i) \), \( i = 1, \ldots, u \). Apply (7) to each \( p_i \) separately, \( i = 1, \ldots, u \) (as in the proof of Theorem 5) to get \( \deg(p_i) - 1 \leq m_i \) with equality if and only if

\[
\deg(p_i) - 1 = \text{ind}(\sigma(\infty)) \quad \text{and} \quad g(p_i) = 0
\]

where \( \sigma(\infty) \) is the \( \sigma(\infty) \) associated to \( p_i \). Theorem 6 results from summing this expression over \( i \). If \( m = 1 \) there must be a factor of degree exceeding 1 for Theorem 2. The remainder of the theorem follows easily.

**Corollary 7.** Let \( p(w, z) \) be an irreducible monic polynomial of degree at least 2 that satisfies (9) and let \( m \) be the number of roots of odd degree of \( D(z) \). Then \( \deg_n(p) \leq m + 1 \) with equality if and only if \( \zeta = \infty \) is totally ramified (\( \sigma(\infty) \) is a \( \deg_n(p) \)-cycle) and there exist nonconstant polynomials \( h, g \in \mathbb{C}[x] \) such that \( p(g(x), h(x)) = 0 \) and \( (\deg(g), \deg(h)) = 1 \).

**Proof.** From (11) the function field \( C(w, z) \) of the curve \( p(w, z) = 0 \) is of genus zero, and therefore \( C(w, z) = C(w') \) for some element \( w' \in C(w, z) \). Thus there exist \( h, g \in C(x) \) such that

\[
h(w') = z \quad \text{and} \quad g(w') = w.
\]

We can adjust \( w' \) by a linear fractional transformation to assume that \( w' = \infty \) is the only value of \( w' \) over \( z = \infty \). Thus \( h(w') \) must be a polynomial. Furthermore, since \( p(w, z) \) is monic in \( w \) the total ramification condition implies that \( w \) is a Laurent series in \( z^{-1/n} \) with \( n = \deg_n(p) \), but not in \( z^{-1/e} \) for any integer smaller than \( n \). The leading coefficient of the Puiseux expansion for \( w \) about \( \infty \) is of the form

\[
w = a_0z^{i/n - i} + a_1z^{j - 1/n - i} + a_2z^{j - 2/n - i} + \cdots
\]

where \((i, j)\) is the integer pair for which \( w'z^j \) has a nonzero coefficient in \( P(w, z) \) and \( j/n - i \) is maximal. Thus this occurs for \( i = 0 \) (because of total ramification)
and the corresponding term is \((0, m)\) with \((n, m) = 1\) and \(\deg_z(p(w, z)) = m\). Conclude therefore that \(C(w, z)\) is also totally ramified over \(w = \infty\). That is, \(g\) is also a polynomial. \(\blacksquare\)

Consider polynomials \(p(w, z) = 0\) that satisfy the conclusion of Corollary 7: \(p(g(x), h(x)) = 0\) for some nonconstant polynomials \(h, g \in C[x]\). Clearly, \(p(w, z) = h(w) - z\) are nonsingular examples, and \(p(w, z) = w^3 + w^2 - z^2\) is a singular example (i.e.,

\[
0 = \frac{\partial p}{\partial w} = 3w^2 + 2w = \frac{\partial p}{\partial z} = 2z
\]

has the solution \((0, 0)\). A complete description of such polynomials (satisfying condition (9)) would be interesting. In the case that the fields \(C(w)\) and \(C(z)\) (inside the function field of \(p(w, z) = 0\)) have nontrivial intersection (more than just \(C\)), then Theorem 3 of [2] shows that \(p(w, z)\) must be a linear change of variables of one of two types of examples: (a) \(w^n - z^n\), \((m, n) = 1\); or (b) \(T_n(w) - T_n(z)\), \((m, n) = 1\), where \(T_n(z)\) is the \(n\)th Chebychev polynomial (i.e., \(T_n(\cos(\theta)) = \cos(n\theta)\)). If \(n > 2\) in case (a), or if \(n \geq 4\) in case (b) then condition (9) no longer holds. Since the condition that \(C(w)\) and \(C(z)\) have nontrivial intersection immediately implies that \(p(w, z)\) divides a variable separated polynomial, we have listed all cases of this occurring above.

3. Splitting of polynomials over the integers

Let \(K = \mathbb{Z}\), as in the introduction, be the ring of integers, \(Q\) the field of rationals. Assume that \(p(w) \in \mathbb{Z}[w]\) is a monic polynomial. Suppose that \(D(p)\) is a nonzero square. In order to deduce that \(p(w)\) splits in \(\mathbb{Z}\) we must assume an analogue of the condition (9) of Theorem 5: For each prime \(q\) which divides \(D(p)\)

\[
(13) \quad p(w) = (w - w(q))^2 g(w)(\text{mod } q),
\]

\(g(w(q)) \neq 0(\text{mod } q), \quad D(g) \neq 0(\text{mod } q).\)

THEOREM 8. Let \(p(w)\) be a monic polynomial with integer coefficients. Assume that \(D(p)\) is a nonzero square and that (13) holds. Then \(p(w)\) splits over the integers.

PROOF. Let \(\Omega_p\) be the splitting field of \(p(w)\) over \(Q\), and let \(\mathcal{O}_p\) be the elements of \(\Omega_p\) that are integral over \(\mathbb{Z}\). For each prime ideal \(\pi\) of \(\mathcal{O}_p\) the inertial group of \(\pi\) is defined as follows:

\[
I(\pi) = \{ \sigma \in G(\Omega_p, Q), \sigma(\pi) = \pi \text{ and the induced map on } \mathcal{O}_p/\pi \text{ is trivial} \}.
\]
Assume that the ideal \( \pi \cap \mathbb{Z} \) is generated by the prime \( q \). Let \( \sigma \in I(\pi) \) be a nontrivial element. Then \( \sigma \) permutes the roots \( \lambda_1, \ldots, \lambda_n \in \mathcal{O}_p \) of \( p(w) \). If \( \sigma(\lambda_i) = \lambda_j \), then

\[
\sigma(\lambda_i) = \lambda_j \equiv \lambda_i \pmod{\pi}
\]

since \( \sigma \) acts trivially on \( \mathcal{O}_p / \pi \). Thus, for \( i \neq j \), \( \lambda_i \pmod{\pi} \) and \( \lambda_j \pmod{\pi} \) give a repeated zero of \( p(w) \mod{q} \). Therefore (13) implies that \( \sigma \) can interchange at most two elements of \( \lambda_1, \ldots, \lambda_n \). If \( \sigma \) moves exactly two elements, then \( \sigma \) is a 2-cycle \( \in S_n - A_n \). However, the assumption that \( D(p) \) is a square implies that

\[
G(\Omega_p, Q) \subset A_n.
\]

Thus \( I(\pi) \) is trivial for each prime ideal \( \pi \). Now, Minkowski’s theorem [5, Theorem 5.4.10] implies that if \( [\Omega_p : Q] > 1 \), then there exists \( \pi \), a prime ideal of \( \mathcal{O}_p \) such that \(|I(\pi)| > 1\). So \([\Omega_p : Q] = 1 : p(w) \) splits in \( Q \).

**REFERENCES**