MM Research Preprints, 126–127
KLMM, AMSS, Academia Sinica
Vol. 26, January 2008

# A Note on Discriminants of Univariate Polynomials

Ruyong Feng† and Ziming Li‡
Key Laboratory of Mathematics Mechanization
AMSS,Academia Sinica, Beijing 100080, China
† ryfeng@amss.ac.cn, ‡ zmli@mmrc.iss.ac.cn

**Abstract.** In this note, we prove an identity on the discriminants of univariate polynomials. It is interesting that this identity was discovered from the problem of differential equations.

In this note, we always let $\mathcal{C}$ be the complex number field and $x, a_{n-1}, \cdots, a_0, b_m, \cdots, b_0$ be an indeterminate over $\mathcal{C}$.

Given a univariate polynomial $f$ in $\mathcal{C}[x]$, the discriminant $\mathrm{D}(f)$ of $f$ is understood to be the resultant of $f$ and $f'$. This resultant is a determinant of size $(2n-1)$. Using matrix and determinant polynomials, we have

$$D(f) = \det(\mathrm{mat}(x^{n-1}f, \ldots, f, x^n f', \ldots, f')).$$

Let $b = b_{n-1}x^{n-1} + \cdots + b_0$ be an arbitrary polynomial in $\mathcal{C}[x]$ with degree $(n-1)$. Let

$$D_i = \det(\mathrm{mat}(x^{n-1}f, \ldots, f, x^n f', \ldots, x^{i+1}f', x^i b, x^{i-1}f', \ldots, f'))$$

for $i = 0, \ldots, n$. Experiments lead to the following conjecture:

$$b_{n-1}\mathrm{D}(f) = \left(\sum_{i=1}^{n} D_i\right). \tag{1}$$

Now we look at (1) in another way. Let $\lambda$ be a new indeterminate. The resultant of $f$ and $(f' + \lambda b)$ can be written as $R(\lambda) = r_n\lambda^n + \cdots + r_1\lambda + r_0$ and, in particular, $r_1 = \sum_{i=1}^{n} D_i$ and $r_0 = \mathrm{D}(f)$. This view hints us that, in order to prove (1), we may (i) show $(r_0 = 0) \Longrightarrow (r_1 = 0)$; and (ii) compare $r_1$ and $r_0$.

**Proposition 0.1** *Let $f(a_{n-1}, \ldots, a_0, x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be with generic coefficients $a_{n-1}, \ldots, a_0$. Then $\mathrm{D}(f)$ as a polynomial in $\mathcal{C}[a_{n-1}, \cdots, a_0]$ is irreducible.*

*Proof:* By the computation of determinant we have

$$\mathrm{D}(f(a_{n-1}, \cdots, a_1, a_0, x)) = n^n a_0^{n-1} + (1-n)^{n-1}a_1^n + E$$

and

$$\bar{D} := \mathrm{D}(f(0, \ldots, 0, a_1, a_0, x)) = n^n a_0^{n-1} + (1-n)^{n-1}a_1^n$$

where $E \in \mathcal{C}[a_{n-1}, \cdots, a_0]$ and $\deg(E, a_0) < (n-1)$, $\deg(E, a_1) < n$. It is easy to see that if $\mathrm{D}(f(a_{n-1}, \cdots, a_1, a_0, x))$ is reducible, then $\bar{D}$ is reducible. Therefore, it suffices to show that $\bar{D}$ is irreducible. Suppose the contrary, then $\bar{D} = AB$ where $A, B \in \mathcal{C}[a_1, a_0]$ with $\deg(A, a_0), \deg(B, a_0) < n-1$. Replacing $a_0$ by $ta_1$ in $\bar{D}$, we have

$$a_1^{n-1}(n^n t^{n-1} + (1-n)^{n-1} a_1) = \bar{A}\bar{B},$$

where both $\deg(\bar{A}, t)$ and $\deg(\bar{B}, t)$ are positive. It follows that

$$F = n^n t^{n-1} + (1-n)^{n-1} a_1$$

is reducible in $\mathcal{C}(a_1)[t]$. Since $a_1$ divides the trailing coefficient but not the leading coefficient of $F$, $F$ is irreducible by Eisenstein's criterion, a contradiction. ∎

Let $f(x)$ be the same as in Proposition 0.1 and $g(x) = b_m x^m + \cdots + b_0$ be a generic polynomial. Let $R(\lambda)$ be the resultant of $f(x)$ and $(f(x)' + \lambda g(x))$ with respect to $x$ where $f(x)' = nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$. Then

$$R(\lambda) = A_n \lambda^n + \cdots + A_1 \lambda + A_0 \tag{2}$$

where $A_i \in \mathcal{C}[a_{n-1}, \cdots, a_0]$. Then we have the following results:

**Proposition 0.2** *Let $R(\lambda)$ be as in (2). We have*

1. *If $m < n-1$, then $A_1 = 0$.*
2. *If $m = n-1$, then $A_1 = b_m A_0$*

*Proof:* Denote $\mathcal{C}(a_{n-1}, \cdots, a_1, b_m, \cdots, b_0)$ by $K$. We regard $A_i$ as univariate polynomials in $K[a_0]$ and denote them by $A_i(a_0)$. It is easy to see that $A_0(a_0) = \mathrm{D}(f)$. Proposition 0.1 asserts that $A_0(a_0)$ has no repeated roots. Assume that $\theta_1, \cdots, \theta_{n-1}$ are the $(n-1)$ distinct roots in $\overline{K}$, the algebraic closure of $K$. Let $i \in \{1, \ldots, n\}$. Suppose that $\alpha_{i,1}, \cdots, \alpha_{i,n}$ are all roots of $f(\theta_i, x) := f(a_{n-1}, \ldots, a_1, \theta_i, x)$, which is in $\overline{K}[x]$. Then at least two of them equal to each other, because $\mathrm{D}(f(\theta_i, x)) = A_0(\theta_i) = 0$. Without loss of generality, assume that they are $\alpha_{i1}$ and $\alpha_{i2}$. Hence

$$(f(\theta_i, x)' + \lambda g)(\alpha_{i,1}) = (f(\theta_i, x)' + \lambda g)(\alpha_{i,2}) = \lambda g(\alpha_{i,1}), \tag{3}$$

since $\alpha_{i1}$ is a root of $f(\theta_i, x)'$ as well. Note that $R(\lambda)$ is in $K[a_0, \lambda]$ and that $R(\theta_i, \lambda)$ is the resultant of $f(\theta_i, x)$ and $f(\theta_i, x)' + \lambda g$ with respect to $x$. Since

$$R(\theta_i, \lambda) = \prod_{j=1}^{n} \left(f(\theta_i, x)' + \lambda g(x)\right)(\alpha_{ij}) = \lambda^2 H(\lambda) \quad \text{for some } H \in \overline{K}[\lambda],$$

by (3), we see that $A_1(\theta_i) = 0$. This is true for each $\theta_i$ for $i = 1 \cdots, n-1$. If $m < n-1$, then $\deg(A_1(a_0), a_0) < n-1$, which implies that $A_1(a_0) = 0$. If $m = n-1$, then $A_0(a_0)$ divides $A_1(a_0)$, because $A_0(a_0)$ is irreducible by Proposition 0.1. A straightforward calculation shows that $A_1(a_0) = b_m n^n a_0^{n-1} + E$ where $E \in \mathcal{C}[a_{n-1}, \cdots, a_0, b_m, \cdots, b_0]$ and $\deg(E, a_0) < n-1$. So we have $A_1(a_0) = b_m A_0(a_0)$. ∎

The second statement in Proposition 0.2 implies (1).