Polynomial Discriminants

B. David Saunders

November 3, 1998

Let $A(x) = a_n x^n + \ldots + a_0$ be a polynomial over R, a UFD. Let $A'(x)$ denote it's formal derivative, $A'(x) = n * a_n x^{n-1} + \ldots + a_1$. the discriminant of A may be defined as $\text{discr}\,(A) = (-1)^{n(n-1)/2} a_n^{-1}\ \text{res}\,(A, A')$. Because a_n is a factor of the first column of the Sylvester matrix, the discriminant is an element of R.

The discrminant of a polynomial is a useful tool inasmuch as it serves to discriminate polynomials with repeated roots from polynomials without such repreated roots. The basic theorem being that the polynomial has repeated roots if and only if the discriminant is zero.

The coefficient ring, an integral domain, has a unique extension field up to isomorphism in which the given polynomial splits and hence we may speak unambiguously of the roots of the polynomial, and thus of the existence or nonexistence of repeated roots. A polynomial without repeated roots is called squarefree.

However it is not necessary to bring the splitting field into discussion for the definition of discriminant, for the definition of squarefreeness, or for the basic relation of the discriminant to squarefreeness. If R is a UFD, then $R[x]$ is a UFD also. An element $A \in S$, a UFD, is *squarefree* if for all $B \in S$, either B is a unit or $B^2 \not| A$.

Theorem: If R is a UFD, and $A(x) \in R[x]$, then
(1) A is squarefree if and only if discr$(A) \neq 0$, and
(2) if $\alpha_1 \ldots \alpha_n$ are the roots of A in a splitting field for A and a is it's leading coefficient, then $\text{discr}\,(A) = a^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$.

Proof: (1) If A has a non-trivial square factor, $A = B^2 C$, then $A' = 2BB' + B^2 C'$. Hence A' shares the factor B with A and $\text{res}\,(A, A') = 0$. Since $\text{discr}\,(A)$ is similar to $\text{res}\,(A, A')$ the discriminant is also zero.

Conversely, if $\text{discr}\,(A) = 0$, then A shares a prime factor with A' and we may write $A = PB$, $A' = P'B + PB'$. Since P divides A', we have that P divides $P'B$, hence P divides B. Finally then it follows that P^2 divides A.

For (2) we observe that $A' = \sum_{i=1}^n \prod_{j \neq i} (x - \alpha_j)$. Then plugging A' in for B in the resultant expansion

$$res(A, B) = a_m^n \prod i = 1^n B(\alpha_i)$$

gives the desired result. The m of the formula is $\deg(a) = n$ in our context and the n of the formula is here $\deg(A') = n - 1$.

Two additional remarks: Consider the generic case, in which a_n and the roots α_i of A are algebraically independent in the splitting field for A. The coefficient ring R is the subring generated by a_n and the elementary symmetric functions in the α_i. Then $a_n \not| \operatorname{discr}(A)$ in R. [Prove this.] For example: Let $A = ax^2 + bx + c$.

$$\operatorname{res}(A, A') = \det \left\{ \begin{array}{ccc} 2a & b & 0 \\ 0 & 2a & b \\ a & b & c \end{array} \right\}$$

and

$$\operatorname{discr}(A) = b^2 - 4ac.$$

The second remark is that a resultant algorithm may be used to compute the discriminant. we have no special faster algorithm for computing the discriminant.

References

[1] Donald E. Knuth The Art of Computer Programming, Vol. 2, 3rd Ed. Addison-Wesley, 1997