(*February 6, 2024*)

Discriminants and Resultants: multiple and simultaneous zeros

Paul Garrett garrett@umn.edu https://www-users.cse.umn.edu/~garrett/

(All this goes back to mid-1800's, if not earlier!)

---

1. *Discriminants and multiple zeros*

For k a field, and polynomial $f \in k[x]$, the *discriminant* of f is (with no universal notation),

$$\prod_{i \neq j} (\theta_i - \theta_j) \qquad\qquad (\theta_i \text{ the zeros of } f \text{ in } \overline{k})$$

where $\overline{k}$ is an algebraic closure of k. The obvious intentional point is that this is 0 if and only if there is a repeated/multiple zero of f.

Because that expression is invariant under permutations of those zeros, it is expressible in terms of the elementary symmetric polynomials in the θ's, which are (up to signs) the coefficients of f. Beyond the quadratic case, it is tedious to execute the algorithm to obtain that expression of the discriminant. It is barely palatable in the cubic case.

---

2. *Euclidean algorithm for* $\gcd(f, f')$

At the same time, f has a multiple root/factor if and only if $\gcd(f, f')$ is non-trivial, because any repeated factor of f will persist to f'. And conversely. In some extreme cases, it is feasible to formulaically describe the outcome of the Euclidean algorithm applied to f and f'. For example, for $f(x) = x^n + ax + b$:

$$f(x) - \frac{x}{n} \cdot f'(x) \;=\; (x^n + ax + b) - \frac{x}{n}(nx^{n-1} + a) \;=\; ax + b - \frac{x}{n}a \;=\; a(1 - \frac{1}{n})x + b$$

Of course, we don't care about $n = 1$, and we decide now to not care about $a = 0$ (which would be easy to appraise separately). Thus, this linear factor is essentially the same as

$$x + \frac{b}{a(1 - \frac{1}{n})} \;=\; x - \frac{-b}{a(1 - \frac{1}{n})}$$

From the Euclidean algorithm for polynomials over a field, we know that the remainder, upon dividing $g(x)$ by $x - \alpha$, is $g(\alpha)$. Thus, the next step in this slightly larger Euclidean algorithm is

$$f'(x) - [?] \cdot (x - \frac{-b}{a(1 - \frac{1}{n})}) \;=\; f'(\frac{-b}{a(1 - \frac{1}{n})})$$

where we do not care about the *dividend*. This is

$$n \cdot \Big(\frac{-b}{a(1 - \frac{1}{n})}\Big)^{n-1} + a \;=\; (-1)^{n-1} \cdot \Big(a(1 - \frac{1}{n})\Big)^{1-n} \cdot \Big(nb^{n-1} + a \cdot \big(a(\frac{1}{n} - 1)\big)^{n-1}\Big)$$

We can adjust by non-zero constants, to obtain

$$n^n b^{n-1} + (1-n)^{n-1} a^n$$

That is, the latter expression vanishes if and only if f has a repeated factor.

---

3. $\gcd(f, f')$ *is discriminant of* f

[3.1] Claim: For $f(x) = x^n + ax + b$, the expression $n^n b^{n-1} + (1-n)^{n-1} a^n$ obtained above, by applying Euclidean algorithm to f and f', is the discriminant of f.

Proof: The heuristic is about degree considerations, in terms of the zeros of f in an algebraic closure of k. Namely, on one hand, $\prod_{i \neq j}(\theta_i - \theta_j)$ is apparently of degree $n(n-1)$ in the zeros θ_i. On the other hand, $a = \pm s_{n-1}$ and $b = s_n$, the elementary symmetric polynomials in the zeros, which are of degrees $n-1$ and n. Thus, the expression obtained via the Euclidean algorithm is apparently of degree $(n-1)n$, as well.

However, for one thing, if the θ_i are merely *numbers* of some kind, or abstract field elements, this notion of *degree* does not have obvious content. This problem can be overcome by treating the *universal* version of the situation, namely, where k is the fraction field $K(t_1, \ldots, t_n)$ of a polynomial ring $K[t_1, \ldots, t_n]$, and $f \in k[x]$ has zeros t_i. The notion of (total) degree does make sense in $K[t_1, \ldots, t_n]$, so we might want to consider the alleged identity in $K[x, t_1, \ldots, t_n]$, even though we did the computation in a larger ring.

That is, in $K[t_1, \ldots, t_n]$, indeed s_ℓ is of (total) degree ℓ. So a is indeed of degree $n-1$, and b of degree n, so a^n and b^{n-1} are both of degree $n(n-1)$, as the heuristic gives. And the product defining the discriminant, likewise, is of (total) degree $n(n-1)$ in $K[t_1, \ldots, t_n]$.

By unique factorization in polynomial rings over fields, since both expressions vanish (as polynomials in $K[t_1, \ldots, t_n]$) whenever any t_i and t_j are mapped to the same element of any target ring, both are divisible by all $t_i - t_j$. In both cases, by degree arguments, this does not leave any room for further factors of either.

---

4. *Resultants and common zeros*

For field k and $f, g \in k[x]$, the *resultant* $R(f, g)$ of f and g is intended to be a polynomial (with coefficients in k) in the coefficients of f and g whose vanishing is equivalent to f and g having simultaneous zeros. Thus, by the derivation criterion for repeated factors/roots, it should be that, the *discriminant* of a single polynomial f is the *resultant* of f and f'.

Letting α_i and β_j be the zeros (with multiplicities) of f, g in an algebraic closure of k, up to constants, the resultant should be

$$R(f, g) \;=\; \prod_{i,j} (\alpha_i - \beta_j)$$

Since this $R(f, g)$ is invariant under permutations of the α_i, and under permutations of the β_j, by the theory of symmetric functions, it is a polynomial in the elementary symmetric polynomials in the α_i and the β_j. Up to signs, these are the coefficients of f and g. This is *one* proof of the *existence* of the resultant.

However, the basic algorithm to express symmetric polynomials in terms of the elementary ones is qualitatively opaque, and, being completely general, ignores structural features of a given situation.

Another, more structured/intelligible approach: let f be of degree d and g of degree e. Let $P_{<n}$ be the k-vectorspace of polynomials of degrees $< n$. The linear map

$$P_{<e} \oplus P_{<d} \longrightarrow P_{<e+d} \qquad \text{by} \qquad A \oplus B \longrightarrow Af + Bg$$

is a k-linear map from one $(e+d)$-dimensional space to another. It has non-zero kernel exactly when the determinant of the matrix giving the map, in whatever coordinates, is 0.

When the determinant is 0, there are non-zero polynomials A, B, of degrees less than those of g, f (in that order), such that $Af + Bg = 0$. That is, $Af = -Bg$. By unique factorization in $k[x]$, since the degree of B is strictly less than that of f, some factor of f must divide g. So, again, we have *existence* of a resultant, namely, that determinant.

That determinant can be *expressed* formulaically in terms of the natural basis for polynomials consisting of monomials x^i. Letting $T : P_{<e} \oplus P_{<d} \to P_{<e+d}$ be that map, and $f(x) = a_0 + a_1 x + \ldots + a_d x^d$, and $g(x) = b_0 + b_1 x + \ldots + a_d x^d$,

$$\begin{array}{ccccc} T(1 \oplus 0) & = & 1 \cdot f & = & a_0 + a_1 x + \ldots + a_d x^d \\ T(x \oplus 0) & = & x \cdot f & = & a_0 x + a_1 x^2 + \ldots + a_d x^{d+1} \\ \ldots & & & & \\ T(x^{e-1} \oplus 0) & = & x^{e-1} \cdot f & = & a_0 x^{e-1} + a_1 x^e + \ldots + a_d x^{e+d-1} \\ T(0 \oplus 1) & = & 1 \cdot g & = & b_0 + b_1 x + \ldots + b_e x^e \\ T(0 \oplus x) & = & x \cdot g & = & b_0 x + b_1 x^2 + \ldots + b_e x^{e+1} \\ \ldots & & & & \\ T(0 \oplus x^{d-1}) & = & x^{d-1} \cdot g & = & b_0 x^{d-1} + b_1 x^d + \ldots + b_d x^{e+d-1} \end{array}$$

More later! :)

This does lead to a classic algebraic-curve fact, namely, Bézout's theorem, that two plane algebraic curves over $\mathbb{C}$, defined by polynomials f, g, intersect in $(\deg f) \cdot (\deg g)$ points, counting multiplicities and points at infinity.
