Discriminants and Resultants

Antarish Rautela

July 2020

Abstract

This paper will dive into the definitions of discriminants and resultants and explore how they are connected. We then will go into various theorems about discriminants and the tranisition over to theorems about resultants. This paper assumes basic knowledge of ring theory.

1 Discriminant

The discriminant of an algebraic number field is the invariant that shows the size of the ring of integers of the algebraic number field. The discriminant is very useful since it is used in formulas like the functional equation of the Dedekind zeta function of K and the analytic class number formula of K where K is a number field over Q.

The most familiar examples the discriminant of a quadratic polynomial $f(x) = ax^2 + bx + c$. This is $D(f) = b^2 - 4ac$, which vanishes when $f(x)$ has a double root in other words the discriminant equals zero when $f(x)$ has a double root. While when $f(x)$ has no real root the discriminant is less than zero. Another example is the discriminant of the cubic polynomial $ax^3 + bx^2 + cx + d$ which is equal to $a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2$ and this discriminant is equivalent to zero when it has one to two distinct roots and when it's coefficients are irreducible. The discriminant is positive when the roots are distinct are are real numbers and the discriminant is negative when there are two complex conjugate roots and one real root (Fun Fact:A cubic polynomial with real coefficients can have less than one real root). One famous type of cubic polynomials with a special type of discriminant are cubic polynomials that can be expressed as $x^3 + px + q$ which has a discriminant of $-4p^3 - 27q^2$. An interesting thing about cubic polynomials is that when the Galois group of an irreducible cubic polynomial where it's coefficients are rational numbers is a cyclic group of order three then the discriminant of the polynomial is a square of a rational or a number from the number field.

We can consider a polynomial $f(x_l.....x_k)$ of degree $< d$ in k variables. The discriminant, Disc(f), is a polynomial function in the coefficients of f which vanishes when ever f has such a "multiple root." The existence of Disc is not quite trivial; however,it can be shown that Disc(f) exists and is unique up to sign if we

require it to be irreducible and to have relatively prime integer coefficients. For the following theorems and corollaries discussed K is a number field of degree n over Q. Let $\sigma_1, ..., \sigma_n$ be the embeddings of K in C. We write $[a_{ij}]$ for the matrix with a_{ij} in the ith row and jth column, and $[a_{ij}]$ for the determinant of the matrix. We let the discriminant of $(\alpha_1, ..., \alpha_n) \in K$ be $disc(\alpha_1, ..., \alpha_n) = |\sigma_i(\alpha_j)|^2$. We also define $T(a) = \sigma_1(a) + ... + \sigma_n(a)$. We are going to denote discriminant as Disc. The resultant also known as the eliminant of two polynomials is an expression related to the coefficients of the two polynomials. The resultant is only equal to 0 if and only if the two polynomials share a root or in other words have a common factor. The discriminant of a polynomial is the resultant of the polynomial and its derivative. The discriminant of a polynomial over a field is equal to zero if and only if the polynomial has a multiple root in some field.

2 Resultant

The resultant R(A,B) where

$$A(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + ... + a_0$$

and

$$B(x) = b_m x^m + b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + ... + b_0$$

, where neither a_0 or b_0 are equivalent to zero, is defined as $R(A, B) = a_n^m b_n^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$ such that α_i and β_j are the roots of A(x) and B(x), respectively. One quick observation is that if A and B are monic then we have that $\prod_\alpha (B(\alpha)) = \prod_\beta (A(\beta))$. We can see that what as said before that if A(x) and B(x) have a common root then the resultant is equal to zero. Similar to a resultant, a discriminant equals 0 when a function and it's derivative have a common root The resultant of polynomials is denoted by $R(A, B)$ where A and B are two polynomials..

3 Preliminary for the Theorems

Let $f(x) = \sum_{i=0}^{n} (a_i x^i)$ and $g(x) = \sum_{j=0}^{m} (b_j x^j)$ be in K[x] of degree n and m respectively. Let α_i $(1 \leq i \leq n)$ and β_j $(1 \leq j \leq n)$ be roots of $f(x)$ and $g(x)$ in some splitting fields. The resultant of f and g is defined by

$$R(f, g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$$

. We have $f(x) = a_n \prod_{i=1}^{n} (x - \alpha_i)$ and $g(x) = b_m \prod_{j=1}^{m} (x - \beta_j)$ then

$$R(f, g) = a_n^m \prod_{i,j=1}^{n,m} b_m(\alpha_i - \beta_j) = a_n^m \prod_{i=1}^{n} (g(\alpha_i)) = (-1)^{mn} b_m^n \prod_{j=1}^{m} (f(\beta_j)).$$

referring to [1] and [2] $R(f,g)$ is described in terms of determinant of the Sylvester matrix of f and g.

Let $f(x) = \sum_{i=0}^{n}(a_i x^i)$ and $g(x) = \sum_{j=0}^{m}(b_j x^j) \in K[x]$. Then $R(f,g)$ is the determinant of $(n+m)$ x $(n+m)$ Sylvester matrix composed of all coefficients:

$$Syl(f,g) = \begin{bmatrix} a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \\ a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \\ a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \\ a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \\ a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \\ a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \\ a_n & a_{n-1} & a_{n-2} & ... & a_1 & ... & 0 \end{bmatrix}$$

For

f(x) $\in K[x]$ with leading coefficient a_n and roots α_i (1) in a splitting field of K, the discriminant Δ of f is defined by

$$\Delta(f) = a_n^{2n-2} \prod_{1 \le i \le j \le n} (\alpha_i - \alpha_j)^2.$$

Let $f(x) \in K[x]$ be of degree n. Then $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} a_n^{-1} R(f, f')$.

4 Theorem 1

$$Disc(\alpha_1, ..., \alpha_n) = |T(\alpha_i \alpha_j)|$$

5 Proof of Theorem 1

We can use the fact that $|a_{ij}| = |a_{ji}|, |AB| = |A||B|$. Then we have

$$[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + ... + \sigma_n(\alpha_i\alpha_j)] = [T(\alpha_i\alpha_j)]$$

The theorem follows from the previous fact.

6 Corollary 1

$Disc(\alpha_1, ..., \alpha_n) \in Q$, and if the a_i are integrals, then we have $Disc(\alpha_1, ..., \alpha_n) \in Z$.

7 Theorem 2

$Disc(\alpha_1, ..., \alpha_n) = 0$ if and only if $(\alpha_1, ..., \alpha_n)$ are linearly dependent over Q.

8 Proof of Theorem 2

If the α_j are linearly dependant over Q then so are the columns of the matrix $[\sigma_i(\alpha_j)]$ and its determinant will be zero. Conversely if $disc(\alpha_1, ..., \alpha_n) = 0$, then the rows R_i of the matrix $[T(\alpha_i\alpha_j)]$ are linearly dependent. Suppose the α_i are all linearly independent. Then let $a_1, .., a_n$ be rationals, where all of them aren't zero, such that $a_1R_1 + ... + a_nR_n = 0$. Then consider $\alpha = a_1\alpha_1 + ... + a_n\alpha_n \neq 0$. Then we have $T(\alpha\alpha_j) = 0$ for all j. The α_j form a basis for K over Q, and since $\alpha \neq 0$, so do the $\alpha\alpha_j$. But this implies $T(\beta) = 0$ for all $\beta \in K$, a contradiction since there exist elements of nonzero trace (for example $T(1) = n$).

9 Theorem 3

Let $K = Q[\alpha]$ and let $\alpha_1, ..., \alpha_n$ be the conjugates of α over Q. Let f be the minimal polynomial of α. Then $disc(1, \alpha, ..., \alpha^{n-1}) = \prod_{1\leq rs\leq n}(\alpha_r - \alpha_s)^2 = \pm N^K(f'(\alpha))$ where the sign is positive if and only if n=0,1(mod 4).

10 Proof Theorem 3

First we can see $|\sigma_i(\alpha^{j-1})| = |(\sigma_i(\alpha))^{j-1}| = |\alpha_i^{j-1}|$ is a Vandermonde determinant, yielding the first equality. Next we can get $\prod_{rs}(\alpha_r - \alpha_s)^2 = \pm\prod_{r\neq s}(\alpha_r - \alpha_s)$, the plus sign holds if and only if n=0,1(mod 4). Since f' has ration coefficients, we have $N^K(f'(\alpha)) = \prod_{r=1}^n \sigma_r(f'(\alpha)) = \prod_{r=1}^n f'(\sigma_r(\alpha)) = \prod_{r=1}^n f'(\alpha_r)$ Then the second equality holds true from the fact that for all r we have $f'(\alpha_r) = \prod_{s\neq r}(\alpha_r - \alpha_s)$. To get this, we can let $f(x) = (x - \alpha_r)g(x)$. Then by the product rule we get $f'(\alpha_r) = g(\alpha_r)$, and the roots of g are all the roots of f except for α_r. Now,apply the theorem to compute $disc(1, \omega, ..., \omega^{p-2})$ for $\omega = e^{2\pi i/p}$ where p is an odd prime. We have $f(x) = 1 + x + ... + x(p - 1)$. Since $x^p - 1 = (x - 1)f(x)$, we get $px^{p-1} = f(x) + (x - 1)f'(x)$ which then can be used to deduce $f'(\omega) = \frac{p}{\omega(\omega-1)}$. If we take norms of both sides we get $N(f'(\omega)) = \frac{N(p)}{N(\omega)N(\omega-1)} = \frac{p^{p-1}}{N(\omega-1)}$. Since $(1 - \omega)...(1 - \omega^{p-1}) = p$, we get $N(\omega - 1) = N(1 - \omega) = p$ so then $N(f'(\omega)) = p^{p-2}$. We now get that $disc(1, \omega, ..., \omega_n) = \pm p^{p-2}$ for prime p. For $\omega = e^{\frac{2i\pi}{m}}$ for m. Now we let h be the minimal polynomial of ω. Then from $x^m - 1 = f(x)g(x)$ for some $g \in Z[x]$ we get that $m = \omega f'(\omega)g(\omega)$. when we norms of both sides we get $^{\phi(m)} = \pm disc(\omega)N(\omega g(\omega))$ showing that $disc(\omega)|m^{\phi(m)}$.

11 Theorem 4

Let K be a field with characteristic 0 and let f(x), g(x), $f_i(x)$ and $g_i(x) \in K[x]$. Then $R(f...f, g) = R(f, g)^s$ (there are s many fs) and $R(f^s, g^u) = R(f, g)^{su}$ for

$s, u > 0$.

$$R(f\prod_i(f_i), g\prod_j(g_j)) = R(f,g)\prod_j(f,g_j)\prod_i(f_i,g)\prod_{i,j}(f_i,g_j)$$

12 Proof Theorem 4

First write $f(x) = a_n\prod_{i=1}^{n}(x-\alpha_i)$, and $g(x) = b_m\prod_{j=1}^{m}(x-\beta_j)$. Let $h(x) = c_t\prod_{k=1}^{t}(x-\lambda_k)$ where λ_k are the roots of h(x). Then we get that $(fh)(x) = a_nc_t\prod_i^n\prod_k^t(x-\alpha_i)(x-\lambda_k)$ has zeros α_i and λ_k. By letting λ_i be equal to α_i for $1 \le i \le n$ and $\lambda_{n+k} = \lambda_k$ for $1 \le k \le t$, we then get

$$R(fh,g) = (a_nc_t)^m{b_m}^{n+t}\prod_{i(\lambda_i=0,g(_j)=0}(\lambda_i-\beta_j) = {a_n}^m{b_m}^n\prod_{g(_j)=0,i=1}^{n}(\alpha_i-\beta_j)*{c_t}^m{b_m}^t\prod_{g(_j)=0,k=1}^{t}(\lambda_k-\beta_j) = R(f,g)$$

Then $R(f...f,g) = R(f,g)^s$ and $R(f^s,g^u) = R(f,g)^{su}$ for $s,u > 0$.We can use the fact that $R(\prod(f_i,g) = \prod(R(f_i,g))$ to get

$$R(f\prod_i(f_i), g\prod_j(g_j))$$

$$= R(f,g)R(f,\prod_j(g_j))R(\prod_i(f_i),g)R(\prod_i(f_i),\prod_j(g_j))$$

$$= R(f,g)\prod_j(R(f,g_j))\prod_i(f_i,g)\prod_{i,j}(f_i,g_j).$$

This concludes our proof.

13 Theorem 5

Let $f(x)$, $g(x)$, $h(x)$, $f(x) \in K[x]$ and $s,u > 1$. Then $\Delta(\prod_{i=1}^{s}(R(f_i)) = \prod_{i=1}^{s}(\Delta(f_i)(\prod_{1\le i\le j\le s}^{s}(R(f_i,f_j))^2)$ and $\Delta(f^sg^u) = 0$.

14 Proof of Theorem 5

From the above we get

$$R(f, f'g + (fg)') = R(fg, f'g + fg') = R(f, f'g + fg') * R(g, f'g + fg')$$

Since

$$R(f, f'g + fg') = (-1)^{n^2(m-1)}a_n^{n(m-1)}R(f, f'g)$$

and

$$R(g, f'g + fg') = (-1)^{m^2(n-1)}b_m^{m(n-1)}R(g, fg'),$$

it follows

$$R(fg,(fg)') = (-1^{n^2(m-1)}(-1^{m^2(n-1)}a_n^{n(m-1)}b_m^{m(n-1)}R(f,f'g)R(g,fg')$$

$$= (-1^{n^2(m-1)+m^2(n-1)+mn}a_n n(m-1)b_m^{m(n-1)}R(f,f')R(f,g)^2R(g,g'),$$

because $R(f,g) = (-1)^{mn}R(g,f)$. By Theorem 4 and Lemma 1.2,

$$\Delta(fg) = (-1)^{\frac{mn(mn-1)}{2}}a_n^{-1}b_m^{-1}R)fg,(fg)')$$

$$= (-1)^{\frac{mn(mn-1)}{2}}a_n\Delta(f)(-1)\frac{m(1-m)}{2}b_m\Delta(g)R(f,g)^2$$

$$= \Delta(f)\Delta(g)R(f,g)^2.$$

Thus we get $\Delta(f^2) = \Delta(f)\Delta(f)R(f,f)^2 = 0$ for $R(f,f) = 0$. $\Delta(f^t) = \Delta(g^s) = 0$, so $\Delta(f^s g^u) = \Delta(f^s)\Delta(g^u)R(f^s,g^u) = 0$. For any h(x) we get

$$\delta(fgh) = \delta(f)\delta(g)\delta(h)(R(f,g)R(f,h)R(g,h))^2,$$

so $\Delta(\prod_{i=1}^{s}(f_i)) = \prod_{i=1}^{s}(\Delta(f_i)(\prod_{1\le i\le j\le s}(R(f_i,f_j)))^2$ by induction.

References

[1] H. Cohen, Resultants and Discriminants. A Course in Computational Algebraic Number Theory, New York: Springer Verlag, 119-123, 1993.

[2] B. L. van der Waerden, Algebra, Vol 1, New York, 1970. (translate from German edition, 1966)

[3] Choi, Eun-Mi. "Resultant And Discriminant Of Iterate Polynomials." Honam Mathematical Journal, vol. 32, no. 3, 2010, pp. 493–514., doi:10.5831/hmj.2010.32.3.493.

[4] Flood, M. M. "The Resultant Matrix of Two Polynomials." The American Mathematical Monthly, vol. 44, no. 5, 1937, p. 309., doi:10.2307/2301885.