Lecture 12B The Sylvester Resultant Michael Monagan

February 25, 2021 1:52 PM

7.3 The Resultant.

Let $A, B \in R[x] \setminus \{0\}$ where R is a UFD e.g. $R = \mathbb{Z}$

Let $A = a_m x^m + \cdots + a_0$ and $B = b_n x^n + \cdots + b_0$.

Suppose $A = a_m \prod_{i=1}^{m} (x - \alpha_i)$ $B = b_n \prod_{j=1}^{n} (x - \beta_j)$

$\alpha_i \in \mathbb{C}$ $\beta_j \in \mathbb{C}$

Definition. The resultant of A and B wrt x

$$\operatorname{res}(A,B) = a_m^n \cdot b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

Properties. (i) $\operatorname{res}(B,A) = (-1)^{mn} \operatorname{res}(A,B)$.

(ii) $\operatorname{res}(A, BC) = \operatorname{res}(A,B) \cdot \operatorname{res}(A,C)$ (exercise.)

(iii) $\operatorname{res}(\underset{m=0}{a}, B) = a^n \cdot b_n^0 \cdot 1 = a^n = a^{\deg B}$.

Example $A = 2x^3 - x^2 + 2x - 1 = (2x-1)(x^2+1) = 2(x-\frac{1}{2})(x-i)(x+i)$.

$B = 1 \cdot x^2 - 2 = 1 \cdot (x-\sqrt{2})(x+\sqrt{2})$.

$\operatorname{res}(A,B) = 2^2 \cdot 1^3 \cdot (\frac{1}{2}-\sqrt{2})(\frac{1}{2}+\sqrt{2})(i-\sqrt{2})(i+\sqrt{2})(-i-\sqrt{2})(-i+\sqrt{2})$

$= 4 \cdot (\frac{1}{4}-2) \cdot (-1-2) \cdot (-1-2)$

$= (-7)(-3)(-3) = -63 \in \mathbb{Z}$.

Maple `resultant(A, B, x);`

Theorem 1. $\operatorname{res}(A,B) = 0 \iff A$ and B have a common root

$\iff \deg(\gcd(A,B)) > 0$.

Can we compute $\operatorname{res}(A,B)$ without factoring over $\mathbb{C}$?

Definition. Sylvester's matrix $S(A,B)$ is the following $(n+m)\times(n+m)$ matrix over R.

$$S=\begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots \\ \vdots & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots \\ \vdots & & \ddots & & & \ddots & \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{bmatrix} \begin{matrix} \\ \\ \\ \} n \text{ times} \\ \\ \\ \\ \} m \text{ times} \end{matrix}$$

$\det(S) = \pm \det(S^T)$.

Example $A = 2x^3 - x^2 + 2x - 1$ $\quad B = x^2 - 2$

$$S(A,B) = \begin{bmatrix} 2 & -1 & 2 & -1 & 0 \\ 0 & 2 & -1 & 2 & -1 \\ 1 & 0 & -2 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & -2 \end{bmatrix} \qquad \det(S(A,B)) = -63.$$

Theorem 2. $\operatorname{res}(A,B) = \det(S(A,B))$ [Proof CLO Ch 3]

Corollary 1: $\operatorname{res}(A,B) \in R$.

Corollary 2: If $\phi: R \to T$ is a ring morphism and $\phi(a_m) \neq 0$ and $\phi(b_m) \neq 0$ then

$$\operatorname{res}(\phi(A), \phi(B)) = \phi(\operatorname{res}(A,B)).$$

Proof for $m=n=1$. $A = ax+b$, $B = cx+d$.

$$\operatorname{res}(\phi(A),\phi(B)) = \operatorname{res}(\phi(a)x+\phi(b), \phi(c)x+\phi(d)) \quad (\phi(a)\neq 0,\ \phi(c)\neq 0)$$

$$\overset{T2}{=} \det\begin{bmatrix} \phi(a) & \phi(b) \\ \phi(c) & \phi(d) \end{bmatrix} = \phi(a)\cdot\phi(d) - \phi(b)\cdot\phi(c).$$

$$\phi(\operatorname{res}(A,B)) = \phi\left(\det\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) \overset{T2}{=} \phi(\underbrace{ad-bc}_{R}) = \phi(ad) - \phi(bc)$$

$$= \phi(a)\cdot\phi(d) - \phi(b)\cdot\phi(c).$$

Characterization of the unlucky primes.

Characterization of the unlucky primes.

Let $A, B \in \mathbb{Z}[x] \setminus \{0\}$, $A = \in \cdot \bar{A}$, $B = \in \cdot \bar{B}$ and $\gcd(\bar{A}, \bar{B}) = 1$.

Recall p is unlucky if $\deg(\gcd(\phi_p(\bar{A}), \phi_p(\bar{B}))) > 0$.

E.g. $\gcd(\overset{\in}{(x+1)}\overset{\bar{A}}{(x+5)}, \overset{\in}{(x+1)}\overset{\bar{B}}{(x+12)}) = x+1$

$p=7$ is unlucky.

$\deg(\gcd(\phi_p(\bar{A}), \phi_p(\bar{B}))) > 0$

T1. $\Leftrightarrow \operatorname{res}(\phi_p(\bar{A}), \phi_p(\bar{B})) = 0$

C2 $\Leftrightarrow \phi_p(\operatorname{res}(\bar{A}, \bar{B})) = 0$

$\Leftrightarrow p \mid \operatorname{res}(\bar{A}, \bar{B}) \in \mathbb{Z}$ (C1)

provided $\phi_p(lc(\bar{A})) \neq 0$ and $\phi_p(lc(\bar{B})) \neq 0$.

Theorem 3. The unlucky primes are the primes that divide $\operatorname{res}(\bar{A}, \bar{B})$ hence # unlucky primes is finite.

Ex 1. $\bar{A} = 1 \cdot x + 5$, $\bar{B} = 1 \cdot x + 12$.

$\operatorname{res}(\bar{A}, \bar{B}) = \det\left(\begin{bmatrix} 1 & 5 \\ 1 & 12 \end{bmatrix}\right) = 7$.

$7 \nmid lc(\bar{A}) = 1$, $7 \nmid lc(\bar{B}) = 1$.

The only unlucky prime is 7.

Ex 2. $\bar{A} = 2x^3 - x + 2x - 1 = (2x-1)(x^2+1)$

$\bar{B} = 1 \cdot x^2 - 2$.

$\operatorname{res}(\bar{A}, \bar{B}) = -63 = -7 \cdot 3^2$. primes 3, 7.

So 3, 7 are the only unlucky primes.

$p=3$ $\gcd(\phi_3(\bar{A}), \phi_3(\bar{B})) = \gcd((2x-1)(x^2+1), x^2-2) = x^2+1$.

$p=7$ $\gcd(\phi_7(\bar{A}), \phi_7(\bar{B})) = \gcd((2x+6)(x^2+1), x^2+5)$

$= \gcd(2(x+3)(x^2+1), (x+3)(x+4)) = x+3$.