3-12-25 (WEEK 4)

Shun/翔海(@shun4midx)

RESULTANT

DEFINITION

Let R be a commutative ring and $f(x)=a_nx^n+\dots+a_0$, $g(x)=b_mx^m+\dots+b_0 \in R[x]$.
The **resultant** of f and g is the determinant here:

$$R(f,g)=\det A=\begin{array}{c} \left|\begin{matrix} a_n & a_{n-1} & \cdots & a_0 & & \\ & a_n & a_{n-1} & \cdots & a_0 & \\ & & \ddots & & & \\ & & & a_n & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & \\ & \ddots & & & & \\ & & & b_m & \cdots & b_0 \end{matrix}\right| \end{array}\begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} n \text{ rows}\end{array}$$

PROPOSITION 1

$\exists\, r(x), s(x) \in R[x]$ with $\deg r \le m-1$, $\deg s \le n-1$, s.t. $r(x)f(x)+s(x)g(x)=R(f,g)$

Proof

$x^{m-1}f(x)=a_nx^{n+m-1}+a_{n-1}x^{n+m-2}+\dots+a_0x^{m-1}$

$x^{m-2}f(x)=\qquad a_nx^{n+m-2}+\dots+a_1x^{m-1}+a_0x^{m-2}$

$\vdots$

$f(x)=\qquad a_nx^n+\dots\dots+a_0$

$x^{n-1}g(x)=b_mx^{n+m-1}+b_{m-1}x^{n+m-2}+\dots$

$\vdots$

$g(x)=\qquad b_mx^m+\dots\dots+b_0$

Thus,

$$A\begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix}=\begin{pmatrix} x^{m-1}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ \vdots \\ g(x) \end{pmatrix} \Rightarrow \text{By Cramer's Rule, } 1=\frac{1}{\det A}\begin{vmatrix} a_n & & x^{m-1}f(x) \\ \vdots & & \vdots \\ & & f(x) \\ b_m & & x^{n-1}g(x) \\ & & \vdots \\ & & g(x) \end{vmatrix} \Rightarrow R(f,g)=r(x)f(x)+s(x)g(x)$$

COROLLARY

f and g have a common divisor of $\deg \ge 1 \Rightarrow R(f,g)=0$ (Say $h|f$, $h|g \Rightarrow h \mid \underbrace{R(f,g)}_{\exists\, \text{by}}=rf+sg$)

PROPOSITION 2

Let $f(x)=a_n\prod_{i=1}^{n}(x-y_i)=\sum_{i=0}^{n}a_ix^i$, and $g(x)=b_m\prod_{j=1}^{m}(x-z_j)=\sum_{j=0}^{m}b_jx^j \in R(y_1,\dots,y_n,z_1,\dots,z_m)[x]$, where $a_n, b_m \in R$, $a_0/a_n \dots a_{n-1}/a_n$ are elementary symmetric functions in $y_1,\dots,y_n$ (w.r.t. $z_1,\dots,z_m$) up to sign. Then, $R(f,g)=a_n^m b_m^n \prod_{i,j}(y_i-z_j)=\underline{a_n^m\prod_{i=1}^{n}g(y_i)}=(-1)^{mn}b_m^n\prod_{j=1}^{m}f(z_j)$

Proof

- $R(f,g)$ is a homogeneous poly of deg mn in $R[y_1,\dots,y_n,z_1,\dots,z_m]$

$$\begin{vmatrix} a_n & a_{n-1} & \cdots & & \\ & a_n & & & \\ & & a_n & \cdots & \\ b_m & b_{m-1} & \cdots & b_0 & \\ & & & \ddots & b_0 \end{vmatrix}\begin{matrix} \cdot y_i \\ \cdot y_i^2 \\ \vdots \\ \\ \cdot y_i^n \end{matrix} = \begin{vmatrix} \deg 1 & \cdots & \deg n+m \end{vmatrix}$$

Multiply

So, $R(f,g)$ is a homo poly of deg: $\frac{(n+m)(n+m+1)}{2}-\frac{n(n+1)}{2}-\frac{m(m+1)}{2}=mn$ ✓

- $g(y_i) \mid R(f,g)\ \forall i$

$$\begin{vmatrix} a_n & a_{n-1} & a_{n-2} \\ & \ddots & a \\ b_m & b_{m-1} & \\ & b_m & \cdots \end{vmatrix}=\begin{vmatrix} y_i^{m}\cancel{f(y_i)}^{\,0} \\ \vdots \\ y_i\cancel{f(y_i)} \\ \vdots \\ y_i(g(y_i)) \end{vmatrix}=g(y_i)\begin{vmatrix} \quad \end{vmatrix} \Rightarrow g(y_i) \mid y_i^{m+n}R(f,g) \Rightarrow g(y_i) \mid R(f,g)\ \forall i$$

- $\prod_{i,j}(y_i-z_j) \mid R(f,g)$: Since $g(y_i) \mid R(f,g)$, i.e. $\prod_{j=1}^{m}(y_i-z_j) \mid R(f,g)\ \forall i$ and $\prod_j(y_i-z_j)$ and $\prod_j(y_k-z_j)$ have no common factor

Shun/翔海 (@shun4midx)

- Since $\deg \prod_{i,j}(y_i - z_j) = \deg R(f,g) = mn$ in $y_1, \dots, y_n, z_1, \dots, z_m$, and $R(f,g) = c\prod_{i,j}(y_i - z_j)$ for some $c \in R$.
  When we take $y_1 = \dots = y_n = 0$, $z_1 = \dots = z_m = 1$, we get $a_0 = \dots = a_{n-1} = 0$, $b_0 = (-1)^m b_m$
  Thus, $LHS = a_n^m b_0^n = (-1)^{nm} a_n^m b_m^n$
  $RHS = (-1)^{nm} c$

COROLLARY

Let $f, g \in F[x]$ with F being a field and $a_n b_m \neq 0$. Then, $R(f,g) = 0 \Leftrightarrow f$ and g have a root in common

Proof

$\exists$ field $\Omega \supset F$, s.t. $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ and $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$ for $\alpha_j, \beta_j \in \Omega$ and then $R(f,g) = a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j)$

Hence, $R(f,g) = 0 \Leftrightarrow \prod_{i,j}(\alpha_i - \beta_j) = 0 \Leftrightarrow \alpha_i = \beta_j$ for some i, j

FIELD EXTENSION (VERY ROUGH SKETCH)

qwq don't attack me I still dk Galois Theory ._. here's just smth I came up with to explain
ボクは代数学が本当にできないqwq~TT（始めてノートに日本語を使うね~..）

$f(x) \in F[x] \Rightarrow \exists \alpha \in F_1 \supset F$ s.t. $f(\alpha) = 0$

Proof

As $F[x]$ is a UFD, $f(x) = \underbrace{f_1(x)}_{\text{irr}} \cdots \underbrace{f_r(x)}_{\text{irr}}$

Consider $F_1 = \underbrace{F[x]}_{\text{UFD}} / \underbrace{\langle f_1(x) \rangle}_{\text{Max } F[x]}$ which is a field

Let $\alpha = \bar{x}$ in F_1, then $f_1(\alpha) = \overline{f_1(x)} = \bar{0}$ in $F_1 \Rightarrow f(\alpha) = f_1(\alpha) \cdots f_r(\alpha) = 0$ ✓

Furthermore, we can find $\Omega \supset F$, s.t. $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ in $\Omega(x)$:

Let $\alpha \in F_1$ s.t. $f(\alpha) = 0 \Rightarrow f(x) = g(x)(x - \alpha)$ with $g(x) \in F_1[x]$. Here, $\deg g \leq n-1$. By induction, $g(x) = a_n \prod_{j=2}^{n}(x - \alpha_j)$, $\alpha_j \in \Omega \supset F$ ✓

Also, $R(f,g) = 0 \Leftrightarrow f, g$ have a common root $\Longrightarrow$ say $f(\alpha) = 0$, then $\exists$ minimal poly $m_\alpha(x) \mid f(x)$,
$\Leftrightarrow f, g$ have a common factor $\qquad g(\alpha) = 0 \Rightarrow m_\alpha(x) \mid g(x)$ too ✓

DEFINITION

If $f(x) = a_n \prod_{j=1}^{n}(x - \alpha_j)$, $\alpha_j \in \Omega$, then we define the discriminant of f to be $D(f) = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)^2$

PROPOSITION 3

$R(f, \underbrace{f'}_{\text{Derivative}}) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} D(f)$

Proof

$f'(x) = a_n \sum_{l=1}^{n} \prod_{j \neq l}(x - \alpha_j)$

By prop 2, $R(f, f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$ and $f'(\alpha_i) = a_n \prod_{j \neq i}(\alpha_i - \alpha_j)$ $\forall i$ □

COROLLARY

f has a repeated root $\Leftrightarrow D(f) = 0 \Leftrightarrow R(f, f') = 0$

EXAMPLE

$f(x) = x^3 + px + q$, $f'(x) = 3x^2 + p$

Then, $R(f, f') = \begin{vmatrix} 1 & 0 & p & q & \\ & 1 & 0 & p & q \\ 3 & 0 & p & & \\ & 3 & 0 & p & \\ & & 3 & 0 & p \end{vmatrix} = 4p^3 + 27q^2$

EXAMPLE

$f = x^2 + 2xy^2 + y + 1$

Here, repeated roots are when: $D(f) = (2y^2)^2 - 4(1)(y+1) = 0$

QUESTION

How to solve $f(x,y) = 0$ and $g(x,y) = 0$ with $f(x,y), g(x,y) \in \mathbb{C}[x,y]$? (Assuming $f(x) = 0$ is something we can solve)

Shun/羊羽海 (@shun4midx)

STRATEGY

Write $f(x,y)=a_n(y)x^n+\dots+a_0(y)$, $g(x,y)=b_m(y)x^m+\dots+b_0(y)$ with $a_i(y), b_i(y)\in\mathbb{C}[y]$.
By prop 1, $\exists\, r(x,y), s(x,y)\in\mathbb{C}[x,y]$, $\deg_x r\le m-1$, $\deg_x s\le n-1$, s.t. $r(x,y)f(x,y)+s(x,y)g(x,y)=R(f,g,x)\in\mathbb{C}[y]$
If $(a,b)\in\mathbb{C}^2$ with $f(a,b)=0$, $g(a,b)=0$, then $R(f,g)(b)=0$

PROPOSITION 4

Let $f(x,y)=y^n+a_1(x)y^{n-1}+\dots+a_n(x)$, $g(x,y)=y^m+b_1(x)y^{m-1}+\dots+b_m(x)\in\mathbb{C}[x,y]$.
If a gcd of $f(x,y)$ and $g(x,y)$ is 1, then $f(x,y)=0$, $g(x,y)=0$ has only finitely-many solutions

Proof

If not, then $rf+sg=0\Rightarrow rf=-sg\Rightarrow r\mid g$, i.e. $g=r\tilde{r}\Rightarrow f=-s\tilde{r}\Rightarrow \tilde{r}\mid f$ ※

Let $\varphi(x)=R(f,g,y)$. By assumption, $\varphi(x)\not\equiv 0$
$\therefore$ φ has finitely many roots, say $a_1,\dots,a_r$
Then, $\forall i$, $f(a_i,y)=0$, $g(a_i,y)=0$ has only finitely many solutions

EXAMPLE

$$\begin{cases} f(x,y)=x^2+2y^2-3=0 \\ g(x,y)=x^2+xy+y^2-3=0 \end{cases}$$

$$R(f,g,x)=\begin{vmatrix} 1 & 0 & 2y^2-3 & \\ & 1 & 0 & 2y^2-3 \\ 1 & y & y^2-3 & \\ & 1 & y & y^2-3 \end{vmatrix}=3y^4-3y^2=3y^2(y-1)(y+1)\Rightarrow y=0,\pm 1.$$

$y=0\Rightarrow x=\pm\sqrt{3}$
$y=1\Rightarrow x=1$
$y=-1\Rightarrow x=-1$

EXAMPLE

Let $f(x)=x^3+4x^2-x-4$
$R(f,f')=-450$.

Find all prime integers p, s.t. $f(x) \pmod p$ has a repeated root $\Rightarrow p=2,3,5$
$p=2\Rightarrow x=1$
$p=3\Rightarrow x=-1$
$p=5\Rightarrow x=1$