Lec22D Trager-Rothstein Proof Michael Monagan

April 1, 2021 3:35 PM

residues

Let $$\frac{C}{D} = \frac{C}{1\cdot(x-\beta_1)\cdots(x-\beta_n)} \overset{PF.}{=} \frac{\alpha_1}{x-\beta_1} + \cdots + \frac{\alpha_n}{x-\beta_n}$$

poles

$lc(D)=1$, $\deg C < \deg D$, $\gcd(D,D')=1$

D has no repeated factors $\Rightarrow \beta_i \neq \beta_j$.

Lemma 1. $\alpha_i = C(\beta_i)/D'(\beta_i)$.

Consider $R(z) = res(\overbrace{C(x) - zD'(x)}^{A}, \overbrace{D(x)}^{B}) \in K[z]$

$lc\, D = 1$.

$n = \deg D = \deg B$

$m = \deg A$

$$R(z) = res(A,B) = (-1)^{mn} \cdot \underbrace{b_n^m}_{1} \prod_{i=1}^{n} A(\beta_i) = \pm \prod_{i=1}^{n} A(\beta_i).$$

$$\Rightarrow \quad R(z) = \pm \prod_{i=1}^{n} C(\beta_i) - z D'(\beta_i) \qquad \text{where } D(\beta_i)=0$$

Observe that the roots of $R(z)$ are $z = C(\beta_i)/D'(\beta_i)$.
By Lemma 1 $C(\beta_i)/D'(\beta_i) = \alpha_i$. Do not compute α_i using Lemma 1, instead compute $R(z)$ without factoring $D(x)$.

Lemma 2. Let $v_i = \gcd(C(x) - \alpha_i D'(x), D(x)) \in K(\alpha_i)[x]$.

Then $(x-\beta_j) \mid v_i(x) \iff \alpha_j = \alpha_i$

$[\ \cdots\cdots + \alpha_i \ln(x-\beta_i) + \cdots + \alpha_j \ln(x-\beta_j) + \cdots\cdots\ ]$

Thus if we know the distinct α_i's then we can compute $v_i(x)$'s too without computing the β_i's.

[Ex1. By doing gcd computations in $\mathbb{Q}[x]$ instead of $\mathbb{Q}(i)[x]$.]

$\left[D(x) = 1\cdot(x-\beta_1)\cdots(x-\beta_n) \quad \gcd(D,D')=1 \Rightarrow \beta_i \neq \beta_j \right]$

Lemma 1. $\alpha_i = C(\beta_i)/D'(\beta_i)$

Proof. $\frac{C}{D} = \frac{\alpha_1}{x-\beta_1} + \cdots + \frac{\alpha_n}{x-\beta_n} = \frac{\alpha_i}{x-\beta_i} + \left(\sum_{j\neq i} \frac{\alpha_j}{x-\beta_j} \right)$

$\Rightarrow \quad \frac{C}{D} = \frac{\alpha_i}{x-\beta_i} + \frac{A(x)}{\prod_{j\neq i} x-\beta_j}$ for some $A(x)$.

$\times D \quad \Rightarrow C(x) = \alpha_i \cdot \prod_{j\neq i}(x-\beta_j) + A(x)\cdot(x-\beta_i).$

$\big|_{x=\beta_i} \quad C(\beta_i) = \alpha_i \cdot \prod_{j\neq i} \beta_i - \beta_j + A(\beta_i)\cdot 0$ $= D'(\beta_i)$?

$D(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_n)$

$D'(x) = \left[(x-\beta_i) \cdot \prod_{j\neq i}(x-\beta_j) \right]' = 1 \cdot \prod_{j\neq i}(x-\beta_j) + (x-\beta_i) \cdot \left[\prod_{j\neq i}(x-\beta_j) \right]'$

$D'(\beta_i) = \prod_{j\neq i}(\beta_i - \beta_j) + 0.$

Therefore $C(\beta_i) = \alpha_i \cdot D'(\beta_i) \Longrightarrow \alpha_i = C(\beta_i)/D'(\beta_i).$? $D'(\beta_i) \neq 0.$

Know $D(\beta_i)=0$. Suppose TAC $D'(\beta_i)=0$

$\Rightarrow (x-\beta_i) \mid D(x). \qquad \Rightarrow (x-\beta_i) \mid D'(x).$

$\Rightarrow (x-\beta_i) \mid \gcd(D(x), D'(x))$ a contradiction ($\gcd(D,D')=1$.)

$\Rightarrow D'(\beta_i) \neq 0.$

Lemma 2. $(x-\beta_j) \mid \gcd(C-\alpha_i D', D) \iff \alpha_i = \alpha_j.$

$D = 1\cdot(x-\beta_1)\cdots(x-\beta_n) \quad \gcd(D,D')=1.$

Proof ($\Rightarrow$) $x-\beta_j \mid \gcd(C-\alpha_i D', D)$

$\Rightarrow x-\beta_j \mid D$ and $(x-\beta_j) \mid C(x) - \alpha_i D'(x)$

$\Rightarrow$ $x-\beta_j \mid D$ and $(x-\beta_j) \mid \underline{C(x)-\alpha_i D'(x)}$

$\Rightarrow$ $D(\beta_j)=0$ $\quad\Rightarrow$ $C(\beta_j)-\alpha_i D'(\beta_j)=0$

$\Rightarrow$ $\alpha_i = C(\beta_j)/D'(\beta_j) = \alpha_j$ by Lemma 1

$(\Leftarrow)$ Given $\alpha_i=\alpha_j$

$\Rightarrow$ $\alpha_i=\alpha_j=C(\beta_j)/D'(\beta_j)$ by Lemma 1.

$\Rightarrow$ $C(\beta_j)=\alpha_i \cdot D'(\beta_j)$

$\Rightarrow$ $C(\beta_j)-\alpha_i D'(\beta_j)=0$

$\Rightarrow$ β_j is a root of $C(x)-\alpha_i D'(x)$

$\Rightarrow$ $(x-\beta_j) \mid C(x)-\alpha_i D'(x)$.

But $(x-\beta_j) \mid D(x)$. Hence $(x-\beta_j) \mid \gcd(C(x)-\alpha_i D'(x), D(x))$.