Lecture 1 (Shaoshi CHEN) IHP / 2023/11/27

Rational Integration : Hermite Reduction

K a field of characteristic zero (Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$)

$K[x]$ the ring of polynomials in x over K

$K(x)$ the field of rational functions in x over K

1. Factorizations and partial fraction decompositions

Let $P \in K[x]$. Then we can have different factorizations:

Squarefree factorization $P = P_1 P_2^2 \cdots P_m^m$

(i) $\gcd(P_i, P_j) = 1$ for $1 \le i < j \le m$

(ii) $\gcd(P_i, P_i') = 1$ for $1 \le i \le m$, i.e. P_i is squarefree

Irreducible factorization $P = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}$

(i) $\gcd(P_i, P_j) = 1$ for $1 \le i < j \le m$

(ii) P_i's are irreducible polynomials.

Let $f = \frac{P}{Q} \in K(x)$. Then we get a partial fraction decomposition for f with respect to a factorization of Q

$$Q = Q_1 Q_2 \cdots Q_m \quad \text{with} \quad \gcd(Q_i, Q_j) = 1$$

$$\Rightarrow \quad f = \frac{P}{Q} = \sum_{i=1}^{m} \frac{P_i}{Q_i}$$

squarefree PFD: $\quad f = \frac{P}{Q_1 Q_2^2 \cdots Q_m^m} = \sum_{i=1}^{m} \frac{P_i}{Q_i^i}$

Irreducible PFD: $\quad f = \frac{P}{Q_1^{m_1} Q_2^{m_2} \cdots Q_s^{m_s}} = \sum_{i=1}^{s} \frac{P_i}{Q_i^{m_i}}$

2. Integration and decomposition problems in $K(X)$.

Let $'$ be the derivation on $K(x)$ satisfying

(1) $x' = 1$

(2) $(f+g)' = f' + g' \quad \forall f, g \in K(x)$

(3) $(fg)' = f'g + fg'$

Integration problem: Given $f \in K(x)$, decide whether there exists $g \in K(x)$ s.t. $f = g'$.
If such a g exists, we say that f is integrable in $K(x)$.

Decomposition problem: Given $f \in K(x)$, compute $g, r \in K(x)$ such that

$$f = g' + r,$$

where $r = \frac{a}{b}$ satisfying some "minimal" conditions:

(1) $\gcd(a, b) = 1$ (2) $\deg(a) < \deg(b)$ (3) b is squarefree.

Lemma 1 Let $f = \frac{a}{b} \in K(x)$ be satisfying the above three conditions. Then

$$f \text{ is integrable in } K(x) \Leftrightarrow a = 0.$$

Proof. We only need to show "$\Rightarrow$": Suppose that $f = g'$ for some $g \in K(x)$ and $a \neq 0$! Since $\deg(a) < \deg(b)$, g can not be a polynomial in $K[x]$. Thus $g = \frac{P}{Q}$ has at least one pole $\beta \in \overline{K}$ with $Q(\beta) = 0$. Write $g = \frac{P}{(x-\beta)^m \bar{Q}}$ with $\bar{Q}(\beta) \neq 0$, $P(\beta) \neq 0$ and $m \geq 1$.

Then $$f = g' = \frac{-mP\bar{Q} + (x-\beta)(P'\bar{Q} - P\bar{Q}')}{(x-\beta)^{m+1}\bar{Q}^2} = \frac{a}{b}$$

$$\Rightarrow a(x-\beta)^{m+1}\bar{Q}^2 = b(-mP\bar{Q} + (x-\beta)(P'\bar{Q} - P\bar{Q}'))$$

$$\Rightarrow (x-\beta)^{m+1} \mid b$$ contradictes with the assumption that b is squarefree.

Hermite Reduction (Ostrogradsky 1845, Hermite 1872)

We now solve the decomposition problem for rational functions in $K(x)$. by applying GCD computation in $K[x]$.

<u>Step 1</u>

$$f = p + \frac{a}{b} \qquad p, a, b \in K[x]. \text{ with } \gcd(a,b)=1 \text{ and } \deg(a) < \deg(b)$$

$$= q' + \frac{a}{b} \quad \text{for some } q \in K[x].$$

<u>Step 2</u> Let $b = b_1 b_2^2 \cdots b_m^m$ be a squarefree ~~decomposition~~ factorization of b with b_i squarefree and $\gcd(b_i, b_j) = 1 \ \forall i \neq j$

Squarefree partial fraction decomposition:

$$\frac{a}{b} = \sum_{i=1}^{m} \frac{a_i}{b_i^i} \qquad \deg(a_i) < i \deg(b_i)$$

<u>Step 3</u> Integration by part: $A, B \in K[x]$, B squarefree $\deg(A) < m \deg(B)$, $m \geq 2$

$$\frac{A}{B^m} = \frac{UB + VB'}{B^m}$$

$$= \frac{U}{B^{m-1}} + \frac{VB'}{B^m}$$

$$= \frac{U}{B^{m-1}} + \left(\frac{(1-m)^{-1} V}{B^{m-1}}\right)' - \frac{(1-m)^{-1} V'}{B^{m-1}}$$

$$= \left(\frac{(1-m)^{-1} V}{B^{m-1}}\right)' + \frac{U - (1-m)^{-1} V'}{B^{m-1}}$$

Repeating the above process, we get

$$\frac{A}{B^m} = \left(\frac{u}{B^{m-1}}\right)' + \frac{v}{B}, \quad \text{with } u, v \in K[x] \text{ and } \deg u < \deg(B^{m-1}), \ \deg v < \deg(B).$$

Then
$$\frac{a}{b} = \left(\frac{p}{b^-}\right)' + \frac{q}{b^*}$$

where $b^- = \gcd(b, b')$ $\quad b^* = b/b^-$.

$p, q \in K[x]$ with $\deg(p) < \deg(b^-)$ and $\deg(q) < \deg(b^*)$

Thus any rational function $f \in K(x)$ can be decomposed by <u>Hermite Reduction</u> into the form:

$$(*) \quad f = g' + \frac{a}{b}$$

$a, b \in K[x]$ with $\gcd(a,b) = 1$
$\deg(a) < \deg(b)$ and b is squarefree.

<u>Remark</u> ① To compute the form $(*)$, we only need basic operations $(+, -, \cdot, \div)$ in $K[x]$ without any computation in some algebraic extension of K. So Hermite reduction is called a "rational" algorithm for computing additive decompositions of rational functions.

② We can also reduce the decomposition problem to a problem of solving a linear system (Horowitz - Ostrogradsky approach)

$\deg(a) < \deg(b)$
$$\frac{a}{b} = \left(\frac{p}{b^-}\right)' + \frac{q}{b^*}$$
$$p = \sum_{i=0}^{d^- -1} p_i x^i \quad d^- = \deg(b^-)$$
$$q = \sum_{j=0}^{d^* -1} q_j x^j \quad d^* = \deg(b^*)$$

$\Downarrow$

A linear system in the unknowns p_i's and q_j's.

<u>Example</u> ① $f = \dfrac{x^7 - 24x^4 - 4x^2 + 8x - 8}{x^8 + 6x^6 + 12x^4 + 8x^2} \in \mathbb{Q}(x)$

(i) $D = x^8 + 6x^6 + 12x^4 + 8x^2 = x^2(x^2+2)^3$

(ii) $f = \dfrac{x-1}{x^2} + \dfrac{x^4 - 6x^3 - 18x^2 - 12x + 8}{(x^2+2)^3}$

(iii) $$f = \left(\frac{1}{x} + \frac{6x}{(x^2+2)^2} - \frac{x-3}{x^2+2} \right)' + \frac{1}{x}$$

② Horowitz - Ostrogradsky approach

$$f = \left(\frac{p_0+p_1x+p_2x^2+p_3x^3+p_4x^4}{x(x^2+2)^2} \right)' + \frac{q_0+q_1x+q_2x^2}{x(x^2+2)}$$

Solving the linear system yields

$$(p_0, p_1, p_2, p_3, p_4, q_0, q_1, q_2) = (4, 6, 8, 3, 0, 2; 0, 1)$$

Thus $$f = \left(\frac{3x^3+8x^2+6x+4}{x(x^2+2)^2} \right)' + \frac{x^2+2}{x(x^2+2)}$$

$$= \left(\frac{3x^3+8x^2+6x+4}{x(x^2+2)^2} \right)' + \frac{1}{x}$$

Rothstein-Trager.

3. Computing the logarithmic part by resultants.

| $\gcd(a,b)=1$
b squarefree
$\deg(a)<\deg b$ |

$$\frac{a}{b} = \sum_{i=1}^{n} \frac{\alpha_i}{x-\beta_i}$$

$$\Rightarrow \int \frac{a}{b}dx = \sum_{i=1}^{n} \alpha_i \log x-\beta_i$$

Lagrange's formula for residues:

$$\alpha_i = \frac{a(\beta_i)}{b'(\beta_i)}$$

Example $$\frac{1}{x^3+x} = \frac{1}{x} + \frac{-\frac{1}{2}}{x-i} + \frac{-\frac{1}{2}}{x+i}$$

$$\int \frac{1}{x^3+x}dx = \log x - \frac{1}{2}\log(x+i) - \frac{1}{2}\log(x-i)$$

$$= \log x - \frac{1}{2}\log(x^2+1)$$

Lagrange's formula motivates the introducing of Rothstein - Trager resultants: For $f = \frac{a}{b} \in K(X)$

$$R(z) = \operatorname{resultant}_x(b,\ a - z b') \in K[z].$$

Theorem (Rothstein - Trager) [For proof see Bronstein's book « Symbolic Integration »]

$$\int f\,dx = \sum_{\substack{\alpha \in \overline{K} \\ R(\alpha)=0}} \alpha \log(g_\alpha)$$

$$g_\alpha = \gcd(b,\ a - \alpha b') \in K(\alpha)[x]$$

Example 1) $f = \frac{1}{x^3+x} \in \mathbb{Q}(x)$

$$R(z) = \operatorname{resultant}_x(x^3+x,\ 1 - z(3x^2+1))$$

$$= -4z^3 + 3z + 1 = -4(z-1)(z+\tfrac{1}{2})^2$$

$$\Rightarrow \quad \int f\,dx = 1 \cdot \log g_1 + (-\tfrac{1}{2}) \log g_{(-\frac{1}{2})}$$

$$g_1 = \gcd(x^3+x,\ 1-(3x^2+1)) = x$$

$$g_{(-\frac{1}{2})} = \gcd(x^3+x,\ 1+\tfrac{1}{2}(3x^2+1)) = x^2+1$$

$$\Rightarrow \quad \int f\,dx = \log x + (-\tfrac{1}{2}) \log x^2+1$$

2) $f = \frac{1}{x^2-2}$ $\quad R(z) = -8z^2+1 \quad c_1 = \frac{1}{4}\sqrt{2} \quad c_2 = \frac{-1}{4}\sqrt{2}$

$$\Rightarrow \quad \int f\,dx = \tfrac{1}{4}\sqrt{2} \log(x-\sqrt{2}) - \tfrac{1}{4}\sqrt{2} \log(x+\sqrt{2})$$