② strong version for $(C(x), \frac{d}{dx})$

<u>Task:</u> Given $f \in C(x)$, find (if possible) an elementary extension E of $C(x)$ and $g \in E$ st $g' := \frac{d}{dx} = f$.

<u>Note:</u> Because of Alg 1 (Hermite reduction) it suffices to solve the problem for $h = \frac{p}{q} \in C(x)$ with $\deg p < \deg q$ and q squarefree (recall: ~~Alg~~ given $f \in C(x)$, Alg 1 computes $g, h = \frac{p}{q} \in C(x)$ with $f = g' + h$, q sqf, $\deg p < \deg q$; f is elementary integrable $\Leftrightarrow$ h is).

<u>Brutal method:</u>

Write $h = \sum_{k=1}^{n} \frac{c_k}{x - u_k}$ for $u_k, c_k \in \overline{C}$.

Then $g = \sum_{k=1}^{n} c_k \log(x - u_k)$ does the job.

Therefore:

<u>Thm 3</u> For all $f \in C(x)$ there exists an elementary extension E of $C(x)$ and $g \in E$ with $g' = f$.

Problem: A complete partial fraction decomposition may introduce unnecessary algebraic extensions of the constant field.

Ex:

(1) $$h = \frac{1}{x^3+x} = \frac{1}{x} - \frac{1/2}{x-\sqrt{-1}} - \frac{1/2}{x+\sqrt{-1}}$$

$$= \Big(\underbrace{\log x - \tfrac{1}{2}\log(x-i) - \tfrac{1}{2}\log(x+i)}_{\in \mathbb{Q}(i)(x,\, \log x,\, \log(x-i),\, \log(x+i))}\Big)'$$

but also

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

$$= \Big(\underbrace{\log x - \tfrac{1}{2}\log(x^2+1)}_{\in \mathbb{Q}(x)(\log x,\, \log(x^2+1))}\Big)'.$$

(2) On the other hand,

$$h = \frac{1}{x^2-2} = \frac{1/2\sqrt{2}}{x-\sqrt{2}} - \frac{1/2\sqrt{2}}{x+\sqrt{2}}$$

$$= \Big(\frac{1}{2\sqrt{2}}\log(x-\sqrt{2}) - \frac{1}{2\sqrt{2}}\log(x+\sqrt{2})\Big)'$$

and there is no way of avoiding ~~an extensio~~ algebraic numbers in this case.

<u>Def:</u> Let $f \in C(x)$ and let

$$f = p + \sum_{i=1}^{n} \sum_{j=1}^{d_i} \frac{c_{ij}}{(x-u_i)^j}$$

be the partial fraction decomposition of f in $\bar{C}(x)$. Then $u_1, \dots, u_n \in \bar{C}$ are called the poles of f and

$$\mathrm{res}_{u_i} f := c_{i1}$$

is called the residue of f at u_i.
(If $u \in C$ is not a pole of f, $\mathrm{res}_u f := 0$).

<u>Observe:</u> Partial fractions with the same residue can be integrated into a single logarithm:

$$\frac{c}{x-u} + \frac{c}{x-v} = c \cdot \underbrace{\log((x-u)(x-v))'}$$

$$= \frac{1 \cdot (x-v) + (x-u) \cdot 1}{(x-u)(x-v)}$$

$$= \frac{1}{x-u} + \frac{1}{x-v}.$$

<u>idea:</u> group partial fractions according to the residues.

<u>Lemma</u> Let $h = \frac{p}{q} \in C(x)$ with q (monic) sqf, $\deg p < \deg q$, and let $u \in \overline{C}$ be a pole of h. Then $\mathrm{res}_u h = \frac{p(u)}{q'(u)}$.

<u>Proof</u>. Consider the PFD $h \overset{(1)}{=} \sum_{k=1}^{n} \frac{c_k}{x-u_k}$ of h in $\overline{C}(x)$. Say $u = u_1$. Then $q = \prod_{k=1}^{n}(x-u_k)$. Multiply both sides of (1) by $x-u_1$ an then set $x = u_1$ to obtain

$$\frac{p(u_1)}{\prod_{k=2}^{n}(u_1-u_k)} = c_1 .$$

It remains to see that $q'(u_1) = \prod_{k=2}^{n}(u_1-u_k)$. Indeed, $q' = \sum_{k=1}^{n} \prod_{i \neq k} (x-u_i)$ and setting $x = u_1$ turns all the products to zero, except for the first. ∎

Claim ~~Lemma~~ Let $h = \frac{p}{q} \in C(x)$ with q sqf, $\deg p < \deg q$, and let $u_1, \dots, u_n \in \bar{C}$ be all the poles of h with residue $c \in \bar{C}$.

Then
$$(x-u_1)(x-u_2)\cdots(x-u_n) = \gcd(q, p - cq') \in C(c)[x].$$

Proof: By the previous lemma, we have
$$x - u_i \mid q \quad \text{and} \quad x - u_i \mid p - cq'$$
for every i. Also, if $u \in \bar{C}$ is a pole of h with residue $\tilde{c} \neq c$ then
$$\cancel{p - cq' =} \quad \frac{p}{q'} = \tilde{c} \bmod x - u,$$
so $x - u \nmid p - cq'$. Finally $lc(lhs) = lc(rhs)$. ∎

At this point, it follows that
$$h = \frac{p}{q} = \sum_{k=1}^{n} c_k \frac{v_k'}{v_k}$$
where $c_1 \dots c_n \in \bar{C}$ are the residues of h and $v_k = \gcd(q, p - c_k q') \in C(c_k)[x]$ $(k = 1 \dots n)$

Q1: Can we find the residues of h without computing a PFD?

Q2: Can we ~~find a representation~~ solve the problem with a smaller constant field $\mathbb{H}$ than $C(c_1 \dots c_n)$?

ad 1 $c \in \bar{C}$ is a residue

$\iff \exists u \in \bar{C}: \; q(u) = 0$ and $c = \frac{p(u)}{q'(u)}$

$\iff \exists u: (x-u \mid q$ and $x-u \mid p - cq')$

$\iff \gcd(q, p - cq')$ is nontrivial

$\iff \text{Resultant}_x(q, p - cq') = 0$

Hence the nonzero residues of h are precisely the nonzero roots of the polynomial $r(z)$ $\text{Resultant}_x(q, p - cq') \in C[z]$ ("the "Rothstein-Trager resultant").

$$r(z) = p_1(z) \cdots p_m(z)$$

$$\text{return } \sum_{i=1}^{m} \sum_{\gamma : p_i(\gamma) = 0} \gamma \cdot \log(\gcd(q, p - \gamma q'))$$

<u>ad 2</u> No! Let $K \subseteq \overline{\mathbb{C}}$ be any field so that
$$h = \sum_{k=1}^{m} \tilde{c}_k \frac{\tilde{v}_k'}{\tilde{v}_k}$$
for some $\tilde{c}_k \in K$ and $\tilde{v}_k \in K[x]$ $(k = 1..m)$.

Let $\tilde{w}_1, \dots, \tilde{w}_l \in K[x]$ be square free, monic, and pairwise coprime so that for suitable $e_{ij} \in \mathbb{Z}$ we can write
$$\tilde{v}_k = \prod_{j=1}^{l} \tilde{w}_j^{e_{kj}} \quad (k = 1..m).$$

Then, since
$$\frac{(u^n v^m)'}{u^n v^m} = n \frac{u'}{u} + m \frac{v'}{v},$$
$$\begin{aligned} h &= \cancel{\sum_{j=1}^{l} \Big(\sum_{k=1}^{m} \tilde{c}_k e_{kj} \Big)} \\ &= \sum_{k=1}^{m} \tilde{c}_k \sum_{j=1}^{l} e_{kj} \frac{\tilde{w}_j'}{\tilde{w}_j} \\ &= \sum_{j=1}^{l} \Big(\sum_{k=1}^{m} \tilde{c}_k e_{kj} \Big) \cdot \frac{\tilde{w}_j'}{\tilde{w}_j}. \end{aligned}$$

If $u \in \overline{\mathbb{C}}$ is a pole of h then
$$\operatorname{res}_u h = \sum_{j=1}^{l} \Big(\sum_{k=1}^{m} \tilde{c}_k e_{kj} \Big) \underbrace{\operatorname{res}_u \frac{\tilde{w}_j'}{\tilde{w}_j}}_{= \begin{cases} 1 & \text{if } \tilde{w}_j(u) = 0 \\ 0 & \text{else} \end{cases}}$$
by the lemma.

so $\mathrm{res}_u h = \sum_{k=1}^{m} \tilde{c}_k e_{kj}$ for some j.

But then $\mathrm{res}_u h \in K$, and so, since u was arbitrary $C(c_1, \dots, c_n) \subseteq K$.

In summary, we have shown:

<u>Th 4</u> Let $h = \frac{p}{q} \in C(x)$ with $\deg p < \deg q$

q sqf. Then:

(1) The nonzero roots $c_1, \dots, c_n \in \overline{K}$ of

$\mathrm{Resultant}_x(q, p - z q') \in K[z]$

are precisely the nonzero residues of h

(2) If $v_k := \gcd(q, p - c_k q') \in C(c_k)[x]$ $(k = 1..n)$ then

$$h = \sum_{k=1}^{n} c_k \frac{v_k'}{v_k}$$

(3) If $K \subseteq \overline{C}$ and $\tilde{c}_1 \dots \tilde{c}_m \in K$, $\tilde{v}_1, \dots, \tilde{v}_m \in K(x)$ are such that

$$h = \sum_{k=1}^{m} \tilde{c}_k \frac{\tilde{v}_k'}{\tilde{v}_k}$$

then $C(c_1 \dots c_n) \subseteq K$.