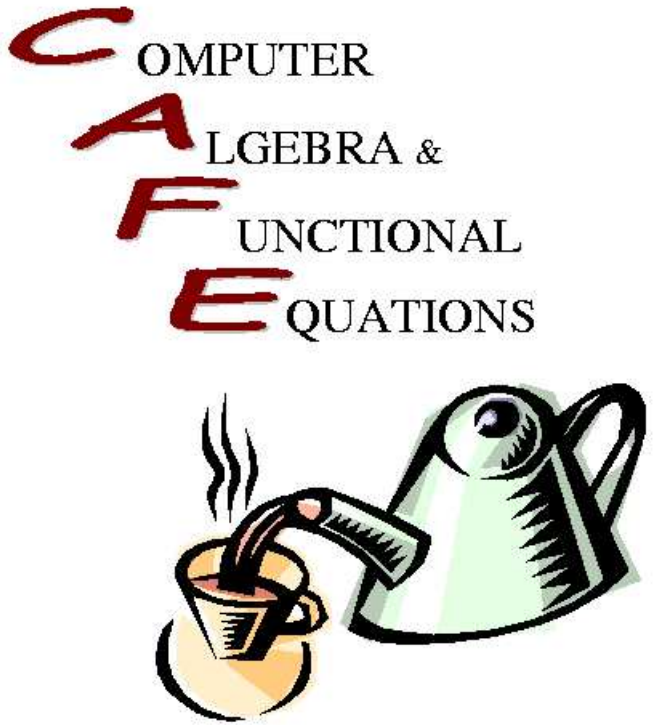
# Regular bases for algebraic function fields

Manuel Bronstein
INRIA (Sophia Antipolis)



## Some problems with algebraic curves and functions

$K$ field of characteristic 0, $P \in K[x, Y]$ squarefree, $n = \deg_Y(P)$.

1. Number of irreducible components of the curve $P(x, Y) = 0$.

2. If $P$ is irreducible over $\overline{K}$, genus of the curve $P(x, Y) = 0$.

3. For a given $f \in K(x, y) = K(x)[Y]/(P)$, is $\int f$ elementary?

Classical geometric algorithms for 1 & 2 (Newton polygon).
Classical algorithms for 3 (Davenport 1981, Trager 1984).
Differential approach for 1 & 2 (Cormier & al. 2002).

## The associated linear differential operator

Any derivation $D$ of $K(x)$ (in particular $d/dx$) extends uniquely to $K(x,y) = K(x)[Y]/(P)$. Since $[K(x,y) : K(x)] = n$, $y, Dy, \ldots, D^n y$ are linearly dependent over $K(x)$, so $L_{D,P}y = 0$ for some linear ordinary differential operator $L_{D,P} \in K(x)[D]$ of order at most $n$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $K(x,y)$ in $\overline{K}(x)$ over $K(x)$. If the $\sigma_i y$ are linearly independent over $\overline{K}$, $L_{D,P}$ is of order exactly $n$ and its solution space is spanned by $\sigma_1 y, \ldots, \sigma_n y$.

$$y^2 - x = 0 \rightarrow 2x\frac{dy}{dx} - y = 0$$

$$z = x + y \rightarrow 2x^2\frac{d^2z}{dx} - x\frac{dz}{dx} + z = 0$$

## Irreducible components

#{irreducible components} $= \dim_K Sol(L_{\frac{d}{dx}}, P) \cap K(x)$

#components $= \#\{\text{orbits of } G\} = \dim_{\overline{K}}\{v \mid Gv = v\}$.

$P = P_1 \dots P_m \to \{\mathrm{Tr}(P_i)\}_{1 \le i \le m}$ is a $\overline{K}$–basis for $\mathrm{Sol}(L_{\frac{d}{dx}}, P) \cap \overline{K}(x)$.

Algorithm for "lifting" a $K$-basis of $Sol(L_{\frac{d}{dx}}, P) \cap K(x)$ to a factorisation of $P$ over $\overline{K}$.

---

#{irreducible components} $= \dim_K \mathrm{Const}_{\frac{d}{dx}}(K(x, y))$

Translates into a differential system of the form $\frac{dZ}{dx} = A(x)Z$ for $c_1(x), \dots, c_n(x)$ such that $c = \sum_{i=0}^{n-1} c_i(x) y^i \in \mathrm{Const}_{\frac{d}{dx}}(K(x, y))$.

$\gcd(P, \alpha - \sum_{i=0}^{n-1} c_i(x) y^i)$ is a non trivial factor of $P$, where $\alpha = \sum_{i=0}^{n-1} c_i(x_0) y_0^i$ for an ordinary point $(x_0, y_0)$ of the curve.

## Computing the genus

$$\begin{aligned} g &= 1-n+\sum_{\mathcal{P}\in\overline{K}\cup\{\infty\}}\ \sum_{\mathcal{Q}\text{ above }\mathcal{P}}\frac{e(\mathcal{Q})-1}{2} \\ &= 1-n+\sum_{\mathcal{P}\in\overline{K}\cup\{\infty\}}\ \sum_{H_{\mathcal{P}}(L_{\frac{d}{dx},P})(\alpha)=0}(\alpha \bmod \mathbb{Z}) \end{aligned}$$

where $H_{\mathcal{P}}(L)$ is the indicial equation of $L$ at $\mathcal{P}$.

Let $\mathcal{Q}$ be above $\mathcal{P}$ with center $t$ and ramification index $e=e(\mathcal{Q})$.

$$y=\sum_{m\geq\mu}\beta_m t^{\frac{m}{e}}=\sum_{j=0}^{e-1}t^{\frac{j}{e}}f_j \text{ where } f_j\in\overline{K}((t))$$

The $e$ conjugates of $y$ are

$$\begin{pmatrix} \tau^1 y \\ \tau^2 y \\ \vdots \\ \tau^e y \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \xi & \cdots & \xi^{e-1} \\ \vdots & \vdots & & \vdots \\ 1 & \xi^{e-1} & \cdots & \xi^{(e-1)(e-1)} \end{pmatrix} \begin{pmatrix} f_0 \\ t^{\frac{1}{e}} f_1 \\ \vdots \\ t^{\frac{e-1}{e}} f_{e-1} \end{pmatrix}$$

where $\xi$ is a primitive $e^{\text{th}}$ root of 1. Therefore, $t^{\frac{j}{e}} f_j$ is a formal series solution of $L_{\frac{d}{dx},P}$ at $\mathcal{P}$, so $H_{\mathcal{P}}(L_{\frac{d}{dx},P})$ has roots $\alpha_0, \ldots, \alpha_{e-1}$ such that $\alpha_j = \frac{j}{e} \pmod{\mathbb{Z}}$.

$$\sum_{j=0}^{e-1} (\alpha_j \bmod \mathbb{Z}) = \sum_{j=0}^{e-1} \frac{j}{e} = \frac{e-1}{2}$$

## Using differential systems

$K(x,y) = K(x)[y]/(P)$ is a vector space of dimension $n$ over $K(x)$. Any derivation $D$ of $K(x)$ extends uniquely to $K(x,y)$. For $w_1, \ldots, w_n$ any basis for $K(x,y)$ over $K(x)$,

$$\begin{pmatrix} Dw_1 \\ \vdots \\ Dw_n \end{pmatrix} = A(x) \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \text{ where } A(x) \text{ has entries in } K(x)$$

$$DU = A(x)U \text{ where } U = \begin{pmatrix} \sigma_1 w_1 & \sigma_2 w_1 & \cdots & \sigma_n w_1 \\ \vdots & \vdots & & \vdots \\ \sigma_1 w_n & \sigma_2 w_n & \cdots & \sigma_n w_n \end{pmatrix}$$

$$c = \sum_{i=1}^{n} c_i(x) w_i \in \mathrm{Const}_D(K(x,y)) \iff D \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = -A(x)^T \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$$

## Using Moser forms

Let $p \in K[x]$ be irreducible. $DZ = AZ$ is in Moser form at $p$ if $pA$ has entries in $\mathcal{O}_p = \{f \in K(x) \text{ st } \nu_p(f) \geq 0\}$.
If $\frac{dZ}{dx} = AZ$ is in Moser form at $p$, then the indicial equation of $\frac{dZ}{dx} = AZ$ at any root $\alpha \in \overline{K}$ of $p$ is $H_p(\lambda) = \det((pA)(\alpha) - \lambda)$.
1) Pick any basis $W$ (e.g. $1, y, \ldots, y^{n-1}$)
2) Compute $A$ st. $\frac{dW}{dx} = AW$
3) For each pole $p \in K[x] \cup \{\infty\}$ of $A$, transform the system into Moser form (Moser 1960, Barkatou 1995) and compute $H_p(\lambda)$.

- Integer roots of $H_p(\lambda) \rightarrow$ bound $\rightarrow$ solutions in $K(x)$
- Adjoint system $\rightarrow$ Const$_{\frac{d}{dx}}(K(x,y)) \rightarrow$ irreducible components
- Rational roots of $H_p(\lambda) \rightarrow$ genus.

## A trivial example

$$y^2 - x = 0 \to \frac{d}{dx}\begin{pmatrix}1\\ y\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & \frac{1}{2x}\end{pmatrix}\begin{pmatrix}1\\ y\end{pmatrix} \qquad \text{is in Moser form}$$

$$H_0(\lambda) = \det\begin{pmatrix}-\lambda & 0\\ 0 & \frac{1}{2}-\lambda\end{pmatrix} = \lambda\left(\lambda - \frac{1}{2}\right) \to \text{ one irreducible component}$$

$$x = 1/z \to zy^2 - 1 = 0 \to \frac{d}{dz}\begin{pmatrix}1\\ y\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & -\frac{1}{2z}\end{pmatrix}\begin{pmatrix}1\\ y\end{pmatrix} \text{ is in Moser form}$$

$$H_\infty(\lambda) = \det\begin{pmatrix}-\lambda & 0\\ 0 & -\frac{1}{2}-\lambda\end{pmatrix} = \lambda\left(\lambda + \frac{1}{2}\right)$$

$$g = 1 - 2 + \frac{1}{2} + \frac{1}{2} = 0$$

## Regular bases

From now on, $D$ is a derivation on $K(x)$ such that both $K$ and $K[x]$ are closed under $D$. Let $p \in K[x]$ be irreducible and define

$$\delta_D(p) = \begin{cases} 1 & \text{if } \gcd(p, Dp) = 1 \\ 0 & \text{if } p \mid Dp \end{cases}$$

A basis $W = (w_1, \ldots, w_n)$ of $K(x, y)$ over $K(x)$ is locally regular at $p$ (w.r.t. $D$) iff
*(i)* each $w_i$ is locally integral at $p$, and
*(ii)* $p^{\delta_D(p)} DW = AW$ for a matrix $A$ with entries in $\mathcal{O}_p$.
$W$ is (globally) regular (w.r.t. $D$) if it is locally regular at all the irreducible $p \in K[t]$.

**Thrm.** For any irreducible $p \in K[x]$, a local integral basis at $p$ is regular at $p$. A global integral basis is globally regular.

## Extending a module

Let $R \subset K(x)$ be a principal ideal domain integrally closed in $K(x)$ and whose fields of fraction is $K(x)$ ($\mathcal{O}_p, \mathcal{O}_\infty, K[x]$).

Let $W = (w_1, \ldots, w_n)$ be any basis of $K(x, y)$ over $K(x)$ and $RW = \sum_{i=1}^{n} Rw_i$ be the module they generate over $R$.

Given $w = \frac{1}{d} \sum_{i=1}^{n} a_i w_i$ where $d, a_1, \ldots, a_n \in K[x]$, the iteration:

- $g_i \leftarrow \gcd(d, a_i) = \alpha d + \beta a_i$
- $u_i \leftarrow \frac{1}{d}\left(g_i w_i + \beta \sum_{j=i+1}^{n} a_j w_j\right)$
- $(a_1, \ldots, a_n) \leftarrow (0, \ldots, 0, \frac{d}{g} a_{i+1}, \ldots, \frac{d}{g} a_n)$

produces a basis $u_1, \ldots, u_n$ of $K(x, y)$ st $RW + Rw = \sum_{i=1}^{n} Ru_i$.

## Constructing a local regular basis at an irreducible $p \in K[x]$

Start with $W = (w_1, \ldots, w_n)$ any basis of $K(x, y)$ over $K(x)$ such that each $w_i$ is locally integral at $p$.
If $W$ is not locally regular at $p$, then for some $i$, there are $b_1, \ldots, b_n \in \mathcal{O}_P$ and $m > 0$ such that

$$p^{m+\delta_D(p)} Dw_i = \sum_{j=1}^{n} b_j w_j$$

and $b_j \notin p\mathcal{O}_p$ for at least one $j$. Let $w = p^{\delta_D(p)} Dw_i$.

$$(i) \quad w \text{ is locally integral at } p$$

$$(ii) \quad w = \frac{1}{p^m} \sum_{j=1}^{n} b_j w_j \notin \mathcal{O}_p W = \sum_{i=1}^{n} \mathcal{O}_p w_i$$

Replace $W$ by $(u_1, \ldots, u_n)$ st $\mathcal{O}_p W + \mathcal{O}_p w = \sum_{i=1}^{n} \mathcal{O}_p u_i$ and repeat.

## Constructing a global regular basis

Start with $W = (w_1, \ldots, w_n)$ any basis of $K(x, y)$ over $K(x)$ such that each $w_i$ is integral over $K[x]$.
If $W$ is not globally regular, then for some $i$, there are there are $q, b_1, \ldots, b_n \in K[x]$ such that $\gcd(q, b_1, \ldots, b_n) = 1$,

$$qDw_i = \sum_{j=1}^{n} b_j w_j \quad \text{and} \quad \deg(\gcd(q, Dq)) > 0$$

Let $q^*$ be the squarefree part of $q$ and $w = \frac{q^*}{\gcd(q^*, Dq^*)} Dw_i$.

$(i)$ $w$ is integral over $K[x]$

$$(ii) \quad w = \frac{q^*}{\gcd(q^*, Dq^*)} \frac{1}{q} \sum_{i=1}^{n} b_i w_i \notin K[x]W = \sum_{i=1}^{n} K[x] w_i$$

Replace $W$ by $(u_1, \ldots, u_n)$ where $K[x]W + K[x]w = \sum_{i=1}^{n} K[x]u_i$ and repeat.

## A degree 10 curve with 26 cusps

$$
\begin{aligned}
1 = {} & 761328152\,x^6 - 5431439286\,x^2y^8 + 2494\,x^2 + 228715574724\,x^6y^4 \\
& + 9127158539954\,x^{10} - 15052058268\,x^6y^2 + 3212722859346\,x^8y^2 \\
& - 134266087241\,x^8 - 202172841\,y^8 - 34263110700\,x^4y^6 - 6697080\,y^6 \\
& - 2042158\,x^4 - 201803238\,y^{10} + 12024807786\,x^4y^4 - 128361096\,x^4y^2 \\
& + 506101284\,x^2y^6 + 47970216\,x^2y^4 + 660492\,x^2y^2 - 474\,y^2 - 84366\,y^4
\end{aligned}
$$

| Method | Time | |
|---|---|---|
| $L_{d/dx}$ | $\infty$ | Roots are linearly dependent over $\overline{\mathbb{Q}}$ |
| $Y' = AY$ | 4'37" | Using AB 2001 instead of Moser reduction |
| regular basis | 4.6" | Y-basis is regular everywhere except at $\infty$ |
| algcurve[genus] | 2.1" | Very simple singularities! |

## Algebraic integration and curves

$$\int \frac{\sqrt{1+\tan(t)^4}+2\tan(t)^5+2\tan(t)^3}{\sqrt{1+\tan(t)^4}\sqrt{t+\sqrt{1+\tan(t)^4}}}\,dt$$

$x=\tan(t)$, $y=\sqrt{t+\sqrt{1+\tan(t)^4}}$, $K=\mathbb{Q}(t)$, $D=\frac{d}{dt}$
$K(x,y)=K(x)[Y]/(Y^4-2\,tY^2-x^4+t^2-1)$, $Dx=1+x^2$.

$$\int \frac{y^2-t+2\,x^5+2\,x^3}{y^3-ty}$$

**Thrm.** If both $K$ and $K[x]$ are closed under $D$, then given any $f\in K(x,y)$, one can compute $g,h\in K(x,y)$ such that $f=Dg+h$ and for any irreducible $p\in K[x]$, if $\gcd(p,Dp)=1$, then $h$ has at most simple poles above the roots of $p$ (Hermite reduction).

## Algebraic Hermite reduction (Trager 1986, MB 1987)

Let $(w_1, \ldots, w_n)$ be an integral basis, and write

$$f = \frac{\sum_{i=1}^{n} A_i w_i}{Q} \text{ where } Q, A_1, \ldots, A_n \in K[x]$$

Compute a split–squarefree factorisation $Q = SQ_1Q_2^2 \ldots Q_{m+1}^{m+1}$ where $S \mid DS$ and $\gcd(Q_i, DQ_i) = 1 = \gcd(Q_i, Q_j)$ for $i \neq j$.
If $m \geq 1$, then let

$$S_i = QD\left(\frac{w_i}{Q_{m+1}^m}\right) \quad \text{for } 1 \leq i \leq n$$

and solve the linear system

$$\sum_{i=1}^{n} g_i S_i = \sum_{i=1}^{n} A_i w_i \quad \text{for } g_1, \ldots, g_n \in \bigcap_{p \mid Q_{m+1}} \mathcal{O}_p \qquad (1)$$

One then proves that there is always a unique solution

$$(g_1, \ldots, g_n) = \left(\frac{G_1}{H}, \ldots, \frac{G_n}{H}\right)$$

where $H, G_1, \ldots, G_n \in K[x]$ and $\gcd(H, Q_{m+1}) = 1$, and that

$$h = f - D\left(\frac{H^{-1} \bmod Q_{m+1}}{Q_{m+1}} \sum_{i=1}^{n} G_i w_i\right) = \frac{\sum_{i=1}^{n} C_i w_i}{\widehat{Q}}$$

where all normal factors of $\widehat{Q}$ appear with multiplicity $\leq m$.

## Lazy Hermite reduction (MB 1998)

Let $W = (w_1, \ldots, w_n)$ be any regular basis, and $f, S_i$ as before.

1. If (1) has a solution $g_1, \ldots, g_n \in \bigcap_{p|Q_{m+1}} \mathcal{O}_p$, then proceed as in the Hermite reduction.

2. Otherwise:

   (a) If $S_1, \ldots, S_n$ are linearly dependent over $K(x)$, then there are $T_1, \ldots, T_n \in K[x]$ such that $\gcd(T_1, \ldots, T_n) = 1$ and $\sum_{i=1}^{n} T_i S_i = 0$. In that case,

   $$w = \frac{Q}{Q_{m+1}^{m+2}} \sum_{i=1}^{n} T_i w_i$$ is integral over $K[x]$ but $w \notin K[x]W$

   Replace $W$ by $(u_1, \ldots, u_n)$ where $K[x]W + K[x]w = \sum_{i=1}^{n} K[x]u_i$ and repeat.

(b) If $S_1, \ldots, S_n$ are linearly independent over $K(x)$, then the unique solution

$$(g_1, \ldots, g_n) = \left(\frac{G_1}{H}, \ldots, \frac{G_n}{H}\right) \in K(x) \qquad \text{of (1)}$$

is not in $\bigcap_{p|Q_{m+1}} \mathcal{O}_p$, so $\deg(G) > 0$ where $G = \gcd(H, Q_{m+1})$. In that case,

$w = \dfrac{Q/G}{GQ_{m+1}^m} \displaystyle\sum_{i=1}^{n} G_i w_i$ is integral over $K[x]$ but $w \notin K[x]W$

Replace $W$ by $(u_1, \ldots, u_n)$ where $K[x]W + K[x]w = \sum_{i=1}^{n} K[x]u_i$ and repeat.

## Example

$$\int \frac{y^3}{x^2}dx \qquad \text{where } y^4 + (x^2+x)y - x^2 = 0$$

$$x(27x^4 + 108x^3 + 418x^2 + 108x + 27)\frac{d}{dx}\begin{pmatrix} 1 \\ y \\ y^2 \\ y^3 \end{pmatrix} = A(x)\begin{pmatrix} 1 \\ y \\ y^2 \\ y^3 \end{pmatrix}$$

where the entries of $A$ are in $\mathbb{Q}[x]$, so $W = (1, y, y^2, y^3)$ is regular.

$$S_i = x^2\frac{d}{dx}\left(\frac{y^i}{x}\right), \qquad S_1, S_2, S_3, S_4 \text{ linearly independent over } \mathbb{Q}(x)$$

The linear system (1) has the unique solution

$$(g_1, g_2, g_3, g_4) = (0, 0, -\frac{2}{x}, \frac{1}{x} + \frac{1}{x^2}) \notin \mathcal{O}_x$$

$G = \gcd(x^2, x) = x$ and

$$w = \frac{1}{x}\Big((x+1)y^3 - 2xy^2\Big) = \Big(1 + \frac{1}{x}\Big)y^3 - 2y^2$$

is integral over $\mathbb{Q}[x]$. W.r.t. the basis $(u_1, u_2, u_3, u_4) = (1, y, y^2, \frac{y^3}{x})$, the integral becomes

$$\int \frac{u_3}{x} dx$$

whose denominator is squarefree.