Plane algebraic curves in PARI/GP

Nicolas Mascot

Trinity College Dublin

Atelier PARI/GP 2022
January 14, 2022

Goals

Fix a field K of characteristic 0 (think $K = \mathbb{Q}$).

Consider the curve

$$C : f(x, y) = 0$$

where $f(x, y) \in K[x, y]$ is squarefree.

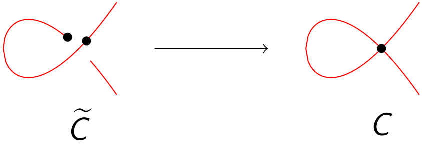
We would like to

- Determine the genus of C,
- Compute Riemann-Roch spaces on C,
- Construct the Jacobian of C,
- ...

Goals

- Determine the genus of C,
- Compute Riemann-Roch spaces on C,
- Construct the Jacobian of C,
- ...

All this actually refers to the desingularisation $\widetilde{C} \to C$ of C.



Local parametrisations

For each point $P = (x_P, y_P)$ of C, local parametrisations

$$x = X(t), y = Y(t)$$

where X, Y are nonconstant formal power series such that $f\big(X(t), Y(t)\big) = 0$ and $X(0) = x_P,\ Y(0) = y_P$.

We assume X and Y are not both series in t^n for any $n \geqslant 2$.

Uniqueness: Hope that Parametrisations at $P \leftrightarrow$ Points of $\widetilde{C}$ above P. But can <u>rescale</u> $t \leftarrow t' = ct + O(t^2)$, $c \neq 0 \dots$

Existence: OK if P is nonsingular: can Newton w.r.t. x or y. But what if P is singular?

Puiseux series

Theorem (Newton–Puiseux)

$\overline{K}\{\{x\}\} = \bigcup_{e\geqslant 1} \overline{K}((x^{1/e}))$ *is algebraically closed.*

View $f(x,y) = f(x)(y) \in K[x][y] \subset K((x))[y]$,
meaning we think of y as an algebraic function of x:

$$\widetilde{C} \longrightarrow C \longrightarrow \mathbb{P}^1_x.$$

Let $n = \deg_y f$.
Then in $\overline{K}\{\{x\}\}$, $f(x)(y)$ has roots $\pi_1, \cdots, \pi_n$
$\rightsquigarrow$ For each $\pi_j = \sum_{n\geqslant n_0} a_n x^{n/e}$,
local parametrisation $x = t^e$, $y = \sum_{n\geqslant n_0} a_n t^n$.

This yields all points above $x = 0$.
For the general case, translate / change variables.

Rationality

Suppose $X(t)$, $Y(t)$ corresponds to $\widetilde{P} \in \widetilde{C}$.

We would like $K(\text{coeffs of } X, Y) = $ the field of definition of $\widetilde{P}$.

⚠ Rescalings $t \leftarrow t' = ct + O(t^2)$ typically destroy this!

If P is nonsingular, we can always have either $X(t) = x_P + t$ or $Y(t) = y_P + t$. But what if P is singular?

If $X(t) = t^e$, $Y(t) = \sum_{n \geqslant n_0} a_n t^n$, can rescale $t \leftarrow \zeta_e t$ $(\zeta_e^e = 1)$

$\rightsquigarrow X(t) = t^e$, $Y(t) = \sum_{n \geqslant n_0} a_n \zeta_e^n t^n$.

Rational parametrisations

Theorem (Duval)

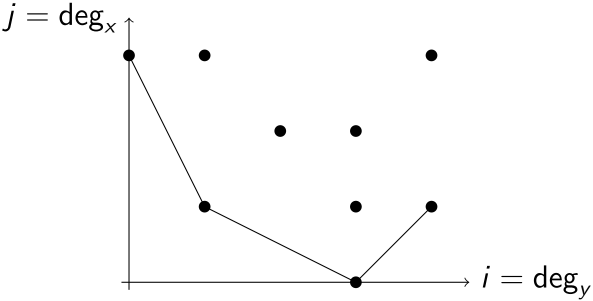
There exists a globally $\mathrm{Gal}(\overline{K}/K)$*-invariant set of parametrisations* $\big(X_j(t), Y_j(t)\big)$*, with* $X_j(t) = b_j t^{e_j}$ *for each* j*, such that the roots of* $f(x)(y) = 0$ *in* $\overline{K}\{\{x\}\}$ *are the* $Y_j\Big(\zeta_{e_j} \sqrt[e_j]{b_j^{-1}} x^{1/e_j}\Big)$ *for* $\zeta_{e_j}^{e_j} = 1$*. In particular,* $\sum_j e_j = n$*.*

Suppose the $\big(X_j(t), Y_j(t)\big)$ for $1 \leqslant j \leqslant g$ form a system of representatives of Galois orbits. For each j, let K_j be $K(b_j, \text{coefs of } Y_j)$, and $f_j = [K_j : K]$. Then $\sum_{i=1}^{g} e_j f_j = n$, and

$$f(x)(y) = \prod_{j=1}^{g} \underbrace{\prod_{\sigma : K_j \hookrightarrow \overline{K}} \underbrace{\prod_{\beta^{e_j} = b_j^{-1}} \big(y - Y_j(\beta x^{1/e_i})\big)}_{\text{irr. factors over } \overline{K}((x))}}_{\text{irr. factors over } K((x))}.$$

Computing the rational parametrisations

Write $f(x)(y) = \sum_{i,j} a_{i,j} x^j y^i$, and draw the Newton polygon of the (i,j) in the support of f.



Let $pi + qj = r$ be a segment, with p, q coprime, $q > 0$. Write

$$f = \underbrace{\sum_{pi+qj=r} a_{i,j} x^j y^i}_{f_0(x,y)} + \underbrace{\sum_{pi+qj>r} a_{i,j} x^j y^i}_{\text{H.O.T.}}.$$

Computing the rational parametrisations

$$f = \underbrace{\sum_{pi+qj=r} a_{i,j} x^j y^i}_{f_0(x,y)} + \underbrace{\sum_{pi+qj>r} a_{i,j} x^j y^i}_{\text{H.O.T.}}.$$

Puiseux approach: Look for roots of valuation p/q, so $y = bx^{p/q} + \text{H.O.T.}$ with $b \in \overline{K}^\times$ determined by $f_0(x,y) = 0$:

$$f_0(x, bx^{p/q}) = \sum_{pi+qj=r} a_{i,j} x^{qj/q} b^i x^{pi/q} = x^{r/q} \sum_{pi+qj=r} a_{i,j} b^i = x^{r/q} B(b).$$

But as p, q coprime, $i = i_0 + qk$, $j = j_0 - pk$ for $k \in \mathbb{Z}$, so $B(b)$ is actually a polynomial in $b^q \rightsquigarrow q$-th roots $\rightsquigarrow$ bad for rationality.

Computing the rational parametrisations

$$f = \underbrace{\sum_{pi+qj=r} a_{i,j} x^j y^i}_{f_0(x,y)} + \underbrace{\sum_{pi+qj>r} a_{i,j} x^j y^i}_{\text{H.O.T.}}.$$

Rational approach: p, q coprime $\rightsquigarrow$ Bézout $up + vq = 1$.
Look for $x = b^{-u} t^q$, $y = b^v t^p + \text{H.O.T.}$, $b \in \overline{K}^\times$. Indeed,

$$f_0(b^{-u} t^q, b^v t^p) = \sum_{pi+qj=r} a_{i,j} b^{-uj} t^{qj} b^{vi} t^{pi}$$

$$= t^r \sum_{pi+qj=r} a_{i,j} b^{v(i_0+qk)-u(j_0-pk)} = t^r b^{vi_0-uj_0} \sum_{pi+qj=r} a_{i,j} b^k = t^r b^{vi_0-uj_0} B(b).$$

Solve $B(b) = 0$, plug in $x = b^{-u} x_1^q$, $y = b^v x_1^p (1 + y_1)$, and iterate until the equation is nonsingular in y.

Practical details

Store and remember the nonsingular equation in y obtained at the end of the recursion
$\rightsquigarrow$ Black box able to give expansions with arbitrary t-adic accuracy.

```
read("Algcurves.gp");
B=Branches0(y^3+2*x^3*y-x^7,t,a)[2][1];
BranchExpand(B,10)
BranchExpand(B,100)
```

Practical details

Useful ingredient to handle successive algebraic extensions:

`AlgExtend` : $(A, F) \longmapsto (B, g, a)$, where

- $A(x) \in K[x]$ irr.,
- $F(x) \in K(\alpha)[x]$ where $A(\alpha) = 0$,

and

- $B(x) \in K[x]$ irr.
- $g(x) \in K[x]$: $g(\beta)$ root of $F(x)$ where $B(\beta) = 0$,
- $a(x) \in K[x]$: $a(\beta)$ root of $A(x)$.

Computing the genus

Write again $f(x,y) = \sum_{i,j} a_{i,j} x^j y^i$.

Theorem (Novocin)

The $\omega_{i,j} = \frac{x^{j-1}y^{i-1}}{\frac{\partial f}{\partial y}} \mathrm{d}x$, $i,j \in \mathbb{N}$, *are holomorphic at the finite nonsingular points. Any holomorphic differential on* C *is a linear combination of the* $\omega_{i,j}$ *for* (i,j) *strictly in the convex hull of the support of* $f(x,y)$.

$\rightsquigarrow$ Strategy: Compute local parametrisations at all the singular points and at the points at infinity. Plug them into the $\omega_{i,j}$, and use linear algebra over K to find the combinations whose polar parts vanish.

We get a K-basis of the space of holomorphic differentials. The genus of the curve is its dimension.

Integral closure (Preparation for Riemann-Roch)

Let $K(C) = \operatorname{Frac} K(x)[y]/f(x,y)$.

The integral closure of $K[x]$ in $K(C)$ is

$$\mathcal{O}_C = \{h(x,y) \in K(C) \mid h \text{ holomorphic above } x \neq \infty\}.$$

Start with the approximation $\mathcal{O} = \bigoplus_{j<n} K[x]y_1^j$,
where $y_1 = lc_y(f)y$.

For all irreducible $U(x) \in K[x]$, $\mathcal{O}$ is U-maximal unless $U^2 \mid \operatorname{disc}_y f(x,y)$.

For such U, compute the parametrisations at the points above $U(x) = 0$, plug them into the $x^i y_1^j / U(x)$ for $i < \deg U$ and $j < n$, and find linear combinations whose polar parts vanish.

Then join the local bases by performing a HNF over $K[x]$.

CrvInit

The GP function `CrvInit` takes $f(x, y)$ and computes the rational parametrisations above the points P such that $x(P) = \infty$ or $x(P)$ is a multiple root of $\Delta(x)$ or P is singular.

```
C=CrvInit(y^3+2*x^3*y-x^7);
CrvPrint(C);


C1=CrvInit(-256*x^56 + 6144*x^55 - 62464*x^54
+ 333824*x^53 - 859648*x^52 - 120832*x^51
+ 7252992*x^50 - 16046080*x^49 - 9891072*x^48
+ 90136576*x^47 - 73076736*x^46 - 237805568*x^45
+ 420485120*x^44 + 341843968*x^43 - 1165840384*x^42
- 192667648*x^41 + 2178936320*x^40 - 238563328*x^39
...
+ 3232*y^6*x^6 + 384*y^6*x^5
-96*y^6*x^4 - 16*y^6*x^3 + 27*y^8);
```

Application: Weierstrass form

$C : y^3 + 2x^3y - x^7 = 0$ has genus $g = 2$, so it is hyperelliptic
$\rightsquigarrow$ has model $H : w^2 = F(u)$.

$\Omega^1(H) = \langle \frac{\mathrm{d}u}{w}, \frac{u\,\mathrm{d}u}{w} \rangle \rightsquigarrow$ our basis of $\Omega^1(C)$ is $\frac{(au+b)\,\mathrm{d}u}{w}, \frac{(cu+d)\,\mathrm{d}u}{w}$
$\rightsquigarrow$ Their quotient is $\frac{au+b}{cu+d}$.

```
C[7] \\ yx/(2x^3+3y^2) dx, x^3/(2x^3+3y^2) dx
u = C[7][1][1]/C[7][1][2]
w = x
factor(MorImg(y^3+2*x^3*y-x^7,u,w))
poldisc(%[2,1],y)
DivPrint(FnDiv(C,u-2/3))
```

Riemann-Roch

Let $D = \sum n_{\widetilde{P}} \widetilde{P}$ formal $\mathbb{Z}$-linear combination of points of $\widetilde{C}$.
The attached Riemann-Roch space is

$$L(D) = \{h \in K(C) \mid \operatorname{ord}_{\widetilde{P}} h \geqslant -n_{\widetilde{P}} \text{ for all } \widetilde{P}\}.$$

This is a finite-dimensional K-vector space. We want a basis.

Represent points $\widetilde{P} \in \widetilde{C}$ either as nonsingular points $P \in C$, or as local parametrisations.

Strategy:

- Find $d(x) \in K[x]$ such that $h(x,y) \in L(D) \Longrightarrow d(x)h(x,y) \in \mathcal{O}_C$.
- Use local parametrisations to find combinations vanishing at appropriate order at relevant points.

Riemann-Roch : Example

```
CrvPrint(C)
RiemannRoch(C,[2,5])
L=RiemannRoch(C,[[-1,1],3;3,1;1,-2])
DivPrint(FnDiv(C,L[1]))
```

Riemann-Roch : Applications

We put a genus 1 curve in Weierstrass form:

```
C1 = CrvInit((x+y+1/x+1/y+1)*x*y);
CrvPrint(C1)
CrvEll(C1,[1,0,0])
```

We find a rational parametrisation of a curve of genus 0:

```
f = x^5+y^4+x^2*y^3;
C0 = CrvInit(f);
CrvPrint(C0)
[X,Y] = CrvRat(C0,1)
substvec(f,[x,y],[X,Y])
```

Jacobians and Galois representations

With Riemann-Roch spaces, we can construct a Makdisi model of the Jacobian J of C.

At the moment, only implemented for models of J over $\mathbb{Z}_q/p^e$, where $q = p^d$ with p a prime of good reduction, $\mathbb{Z}_q$ is the ring of integers of the unramified extension of $\mathbb{Q}_p$ of degree d, and $e \in \mathbb{N}$ is arbitrary.
But no difficulty for models of J over number fields.

p-adic models of J can be used to compute Galois representations occurring in the torsion of J.

```
C=CrvInit(x^5 + y^5 - 6*x^3 + 6*x^2 + x*y - 3*y^2);
CrvPrint(C)
CrvPicTorsGalRep(C,2,13,700)
```

Questions?

Thank you!