Generalized Jacobi Polynomials

T. Shaska

Oakland University

January 18, 2019

Abstract

In this talk we will explore the group addition in Jacobian varieties. First we will describe addition geometrically in low genus curves (i.e. conics, elliptic curves, genus two curves) and then give an interpretation of addition for all hyperelliptic curves via Jacobi polynomials and Mumford's representation. Furthermore, we will explore how Jacobi polynomials could be generalized for all superelliptic curves. The talk is intended to a general audience.

Outline

Preliminaries

Let k be a field of characteristic zero and $\bar{k}$ its algebraic closure. For the purposes of this talk we can think of k as a number field or even more conveniently as $\mathbb{Q}$.

Given an irreducible algebraic curve $\mathcal{C}$ defined over k with affine equation

$$\mathcal{C} : f(x, y) = 0.$$

One of the most celebrated problems in mathematics is to determine the **set of k-rational points of** $\mathcal{C}$, which we will denote by $\mathcal{C}(k)$.

For small genus curves ($g = 1, 2$) the set of such points $\mathcal{C}(k)$ (when it is non-empty) forms an Abelian group.

For higher genus ($g \geq 2$) $\mathcal{C}(k)$ is not a group, but it is embedded into an Abelian group $\mathcal{J}_k(\mathcal{C})$, called the **Jacobian variety** of $\mathcal{C}$.

Our main goal is to understand the operation in this group using elementary geometric arguments.

Conics

A **conic section** is geometrically obtained by the intersection of a double cone with a plane. The general equation of a conic is

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{1}$$

where a, b, c are not at the same time 0. This equation can be written in terms of matrices as

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} d & e \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + f = 0.$$

From linear algebra we know that how to determine the shape of the graph. The symmetric matrix is called the **corresponding matrix**

$$M = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

The **discriminant** is defined as

$$\Delta = b^2 - 4ac.$$

Notice that

$$\Delta = -4 \det M.$$

We have:

Lemma

The shape of the graph is determined as

1. *If $\Delta > 0$, then the graph is a hyperbola*
2. *If $\Delta < 0$, then the graph is an ellipse*
3. *If $\Delta = 0$, then the graph is a parabola*

Conics as groups

What about rational points? It turns out that if we have one rational point we can get as many as we want.

Lemma

A conic $\mathcal{C}$ has a k-rational point if and only if its discriminant is a square in k.

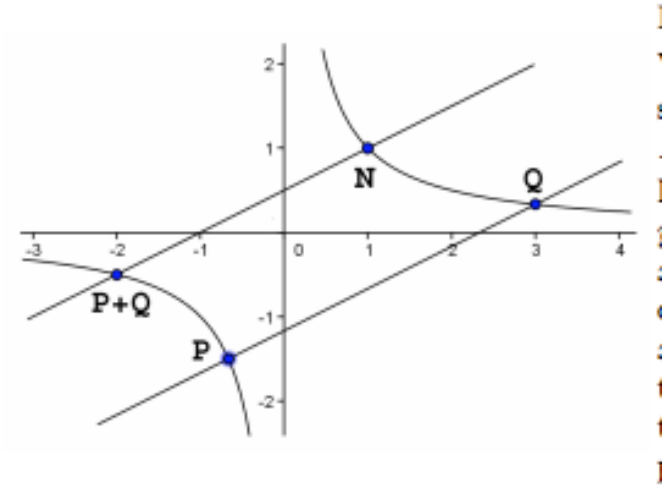


Figure: Addition in a conic

Lemma

Assume that exists $\mathcal{O} \in \mathcal{C}(\mathbb{Q})$. Then,

- *Fix $\mathcal{O}$ in $\mathcal{C}$. This will be the group identity.*
- *For every two points P and Q in $\mathcal{C}$, from $\mathcal{O}$ draw the paralel line with PQ. This line intersects the conic $\mathcal{C}$ in another point $R \in \mathcal{C}(\mathbb{Q})$.*
- *Define $P \oplus Q := R$.*

Then, $(\mathcal{C}(\mathbb{Q}), \oplus)$ is an Abelian group.

Corollary

Given the conic $\mathcal{C}$ with equation

$$ax^2 + bxy + cy^2 + dx + ey = 0,$$

and the point $\mathcal{O}(0,0)$ on it. For every two points $P(\alpha_1, \beta_1)$ and $Q(\alpha_2, \beta_2)$ the formula to compute the coordinates of $P \oplus Q$ is given by

$$P \oplus Q = \left(-\frac{e\lambda + d}{c\lambda^2 + b\lambda + a}, \lambda \left(-\frac{e\lambda + d}{c\lambda^2 + b\lambda + a} \right) \right),$$

where

$$\lambda = \begin{cases} \dfrac{\beta_2 - \beta_1}{\alpha_2 - \alpha_1}, & \text{kur } P \neq Q \\ -\dfrac{2\,a\beta_1 + b\beta_1 + d}{b\alpha_1 + 2\,c\beta_1 + c}, & \text{if } P = Q \end{cases}$$

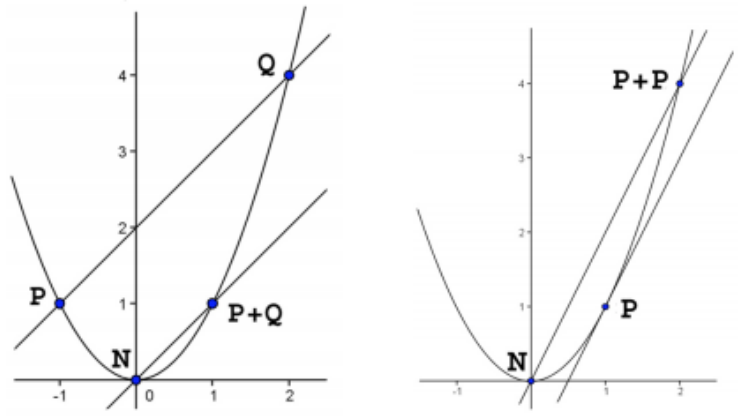


Figure: Addition with $\mathcal{O} = (0,0)$ is the identity

Elliptic curves

A genus 1 curve defined over a field k has equation

$$\mathcal{C}: \quad y^2 = f(x),$$

where deg$f = 3, 4$. (Recall that $\mathrm{char}\ k \neq 2$) We take $\mathcal{O} = \infty$. Then we can define a group structure as follows:
1) For any two points P, Q, construct the line l going through P and Q.
2) From Bezout's theorem, l will intersect $\mathcal{C}$ in a third point R. Take as $P \oplus Q$ the symmetrical of R with respect to the x-axis.

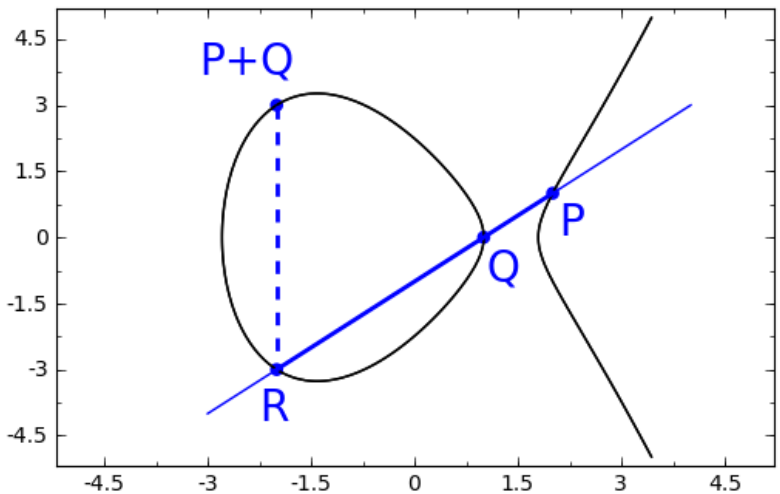


Figure: example caption

A genus 1 curve with a group structure is called an **elliptic curve**.

Higher genus curves.

Let $\mathcal{C}$ be a curve defined over k. Hence there is $n \in \mathbb{N}$ and a homogeneous *prime* ideal $I_{\mathcal{C}} \subset k[X_0, \ldots, X_n]$ such that, with $R = k[X_0, \ldots, X_n]/I_{\mathcal{C}}$, we have

1. $\mathcal{C}$ is the scheme consisting of the topological space $\mathrm{Proj}(R)$ and the sheaf of holomorphic functions given on open subsets U of $\mathrm{Proj}(R)$ by the localization with respect to the functions in R not vanishing on U.
2. The dimension of $\mathcal{C}$ is one, i.e. for every non-empty affine open subset $U \subset \mathrm{Proj}(R)$ the ring of holomorphic functions R_U on U is a ring with Krull dimension 1.
3. $\mathcal{C}$ is regular, i.e. the localization of R with respect to every maximal ideal M in R is a discrete valuation ring R_M of rank 1. The equivalence class of the valuations attached to R_M is the **place** $\mathfrak{p}$ of $\mathcal{C}$, in this class the valuation with value group $\mathbb{Z}$ is denoted by w_M. Alternatively we use the notation $R_{\mathfrak{p}}$ and $w_{\mathfrak{p}}$. A place $\mathfrak{p}$ of $\mathcal{C}$ is also called **prime divisor** of $\mathcal{C}$.
4. (Absolute irreducibility) $I_{\mathcal{C}} \cdot \bar{k}[X_0, \ldots, X_n]$ is a prime ideal in $\bar{k}[X_0, \ldots, X_n]$. This is equivalent with: k is algebraically closed in $\mathrm{Quot}(R)$.

As important consequence we note that for all open $\emptyset \neq U \neq \mathcal{C}$ the ring R_U is a *Dedekind domain*; see (Frey and Shaska, 2019) for details.

Prime Divisors and Points

The set of all places $\mathfrak{p}$ of $\mathcal{C}$ is denoted by $\Sigma_{\mathcal{C}}(k)$. *Completeness* of proj. varieties yields:

Proposition

There is a one-to-one correspondence between $\Sigma_{\mathcal{C}}(k)$ and the equivalence classes of valuations of $k(\mathcal{C})$, which are trivial on k.

Let $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ be a prime divisor with corresponding maximal ideal $M_{\mathfrak{p}}$ and valuation ring $R_{\mathfrak{p}}$. We have a homomorphism

$$r_{\mathfrak{p}} : R_{\mathfrak{p}} \to R_p/M_{\mathfrak{p}} =: L$$

where L is a finite algebraic extension of k. The **degree** of the prime divisor $\mathfrak{p}$ is $\deg(\mathfrak{p}) := [L : k]$.

Lemma

The set $\Sigma^1_{\mathcal{C}}(k)$ of prime divisors of $\mathcal{C}$ of degree 1 is in bijective correspondence with the set of k-rational points $\mathcal{C}(k)$ of the curve $\mathcal{C}$.

Now look at $\mathcal{C}_{\bar{k}}$, the curve obtained from $\mathcal{C}$ by constant field extension to the algebraic closure of k. Obviously, every prime divisor of $\mathcal{C}_{\bar{k}}$ has degree 1.

Corollary

The set of prime divisors of $\mathcal{C}_{\bar{k}}$ corresponds one-to-one to the points in $\mathcal{C}_{\bar{k}}(\bar{k})$.

Corollary

$\Sigma_{\mathcal{C}}(k)$ corresponds one-to-one to the G_k-orbits of $\mathcal{C}_{\bar{k}}(\bar{k})$.

Divisors and Picard groups

Given a curve $\mathcal{C}/k$, the group of k-rational divisors $\mathrm{Div}_{\mathcal{C}}(k)$ is defined as follows.

$$\mathrm{Div}_{\mathcal{C}}(k) = \bigoplus_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} \mathbb{Z}\cdot\mathfrak{p},$$

i.e. $\mathrm{Div}_{\mathcal{C}}(k)$ is the free abelian group with base $\Sigma_{\mathcal{C}}(k)$. Hence a **divisor** D of $\mathcal{C}$ is

$$D = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}\, P$$

where $z_{\mathfrak{p}} \in \mathbb{Z}$ and $z_{\mathfrak{p}} = 0$ for all but finitely many prime divisors $\mathfrak{p}$. The degree of D is

$$\deg(D) := \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}.$$

The map

$$D \mapsto \deg(D)$$

is a homomorphism from $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathbb{Z}$. Its kernel is the subgroup $\mathrm{Div}_{\mathcal{C}}(k)^0$ of divisors of degree 0.

Example

Let $f \in k(\mathcal{C})^*$ be a meromorphic function on $\mathcal{C}$. For $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we have defined the normalized valuation $w_{\mathfrak{p}}$. The divisor of f is defined as

$$(f) = \sum_{\Sigma_{\mathcal{C}}(k)} w_{\mathfrak{p}} \cdot \mathfrak{p}.$$

It is not difficult to verify that (f) is a divisor, and that its degree is 0, see (Stichtenoth, 2009). *Moreover $(f \cdot g) = (f) + (g)$ for functions f, g, and $(f^{-1}) = -(f)$. The completeness of $\mathcal{C}$ implies that $(f) = 0$ if and only if $f \in k^*$, and so (f) determines f up to scalars $\neq 0$.*

Thus, the set of principal divisors $\mathrm{PDiv}_{\mathcal{C}}(k)$ consisting of all divisors (f) with $f \in k(\mathcal{C})^*$ is a subgroup of $\mathrm{Div}^0_{\mathcal{C}}(k)$. The group of divisor classes of $\mathcal{C}$ is defined by

$$\mathrm{Pic}_{\mathcal{C}}(k) := \mathrm{Div}_{\mathcal{C}}(k)/\,\mathrm{PDiv}_{\mathcal{C}}(k)$$

and is called the **divisor class group** of $\mathcal{C}$. The group of divisor classes of degree 0 of $\mathcal{C}$ is defined by

$$\mathrm{Pic}^0_{\mathcal{C}}(k) := \mathrm{Div}^0_{\mathcal{C}}(k)/\,\mathrm{PDiv}_{\mathcal{C}}(k)$$

and is called the **Picard group** (of degree 0) of $\mathcal{C}$.

The Picard Functor

Let L be a finite algebraic extension of k and $\mathcal{C}_L$ the curve obtained from $\mathcal{C}$ by constant field extension. Then places of $k(\mathcal{C})$ can be extended to places of $L(\mathcal{C}_L)$. By the conorm map we get an injection of $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathrm{Div}_{\mathcal{C}_L}(L)$. The well known formulas for the extensions of places yield that

$$\mathrm{conorm}_{L/k}(\mathrm{Div}^0_{\mathcal{C}}(k)) \subset \mathrm{Div}^0_{\mathcal{C}_L}(L)$$

and that principal divisors are mapped to principal divisors. Hence we get a homomorphism

$$\mathrm{conorm}_{L/k} : \mathrm{Pic}^{\,0}_{\mathcal{C}}(k) \to \mathrm{Pic}^{\,0}_{\mathcal{C}_L}(L)$$

and therefore a functor

$$\mathrm{Pic}^{\,0} : L \mapsto \mathrm{Pic}^{\,0}_{\mathcal{C}_L}(L)$$

from the category of algebraic extension fields of k to the category of abelian groups. Coming "from above" we have a Galois theoretical description of this functor. Clearly, 5

$$\mathrm{Div}_{\mathcal{C}_L}(L) = \mathrm{Div}_{\mathcal{C}_{\bar{k}}}(\bar{k})^{G_L}$$

and the same is true for functions. With a little bit of more work one sees that an analogue result is true for $\mathrm{PDiv}_{\mathcal{C}_L}(L)$ and for $\mathrm{Pic}^{\,0}_{\mathcal{C}_L}(L)$.

Theorem

For any curve $\mathcal{C}_k$ and any extension L/k with $k \subset L \subset \bar{k}$ the functor

$$L \mapsto Pic^0_{\mathcal{C}_L}(L)$$

is the same as the functor

$$L \mapsto Pic^0_{\mathcal{C}_{\bar{k}}}(\bar{k})^{G_L}.$$

In particular, we have

$$Pic^0_{\mathcal{C}_{\bar{k}}}(\bar{k}) = \bigcup_{k \subset L \subset \bar{k}} Pic^0_{\mathcal{C}_L}(L),$$

where inclusions are obtained via conorm maps.

Remark

For a finite extension L/k we also have the norm map of places of $\mathcal{C}_L$ to places of $\mathcal{C}_k$ induces a homomorphism from $Pic^0_{\mathcal{C}_L}(L)$ to $Pic^0_{\mathcal{C}}(k)$. In general, this map will be neither injective nor surjective.

It is one of the most important facts for the theory of curves that the functor Pic ^{0} can be represented: There is a variety $\mathcal{J}_{\mathcal{C}}$ defined over k such that for all extension fields L of k we have a functorial equality

$$\mathcal{J}_{\mathcal{C}}(L) = \text{Pic}^0_{\mathcal{C}_L}(L).$$

$J_{\mathcal{C}}$ is the **Jacobian variety** of $\mathcal{C}$.

Properties of Jacobian varieties

From functoriality and universality of the Jacobian it follows that we can introduce coordinates for divisor classes of degree 0 such that the group law in $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$ is given by rational functions defined over k and depending only on $\mathcal{C}$ (and not on L).

Let L/k be a finite algebraic extension. Then the Jacobian variety $\mathcal{J}_{\mathcal{C}_L}$ of $\mathcal{C}_L$ is the scalar extension of $\mathcal{J}_{\mathcal{C}}$ with L, hence a fiber product with projection p to $\mathcal{J}_{\mathcal{C}}$. The norm map is p_*, and the conorm map is p^*.

Proposition

If $f : \mathcal{C} \to \Delta$ is a surjective morphism of curves sending P_0 to Q_0, then there is a uniquely determined surjective homomorphism

$$f_* : \mathcal{J}_{\mathcal{C}} \to J_{\Delta}$$

such that $f_* \circ \phi_{P_0} = \phi_{Q_0}$.

Corollary

Assume that $\mathcal{C}$ is a curve of genus ≥ 2 such that $\mathcal{J}_{\mathcal{C}}$ is a simple abelian variety, and that $\eta : \mathcal{C} \to \Delta$ is a separable cover of degree > 1. Then Δ is the projective line.

Existence of Jacobian varieties

What about the **existence** of Jacobian varieties?

Over the complex numbers the classical theory of curves (key words: Riemann surfaces and the Theorem of Abel-Jacobi) is used to prove the existence of Jacobian varieties already in the 19-th century.

In fact, this notion is historically earlier than the notion "Abelian variety" introduced by A. Weil as most important tool for his proof of the geometric Riemann hypothesis. By the Lefschetz principle the existence of Jacobian varieties follows for algebraically closed fields of characteristic 0.

By the Theorem of Riemann-Roch we have a surjective map from $\Sigma_{\mathcal{C}}^{g}(L)$ to $\mathrm{Pic}_{\mathcal{C}}^{0}(L)$ by sending any positive divisor D of degree g to $D - g \cdot \mathfrak{p}_0$.

We can interpret such positive divisors geometrically. Take the g-fold cartesian product $\mathcal{C}^g$ of the curve $\mathcal{C}$ of genus g and embed it (via Segre's map) into a projective space. On this variety we can permute the factors and so have an action of S_g, the symmetric group with g letters. Define the g-fold symmetric product $\mathcal{C}^{(g)}$ by $\mathcal{C}^g/S_g$. Then we can identify $\mathcal{C}^{(g)}(L)$ with $\Sigma_{\mathcal{C}}^{g}(L)$ and so define a birational map from $\mathcal{C}^{(g)}$ to $\mathcal{J}_{\mathcal{C}}$. Taking an affine part of $\mathcal{C}$ (e.g. found as a regular part of a plane model of $\mathcal{C}$) we get an affine variety which is birational equivalent to $\mathcal{J}_{\mathcal{C}}$.

Cantor's Algorithm

Inspired by the group law on elliptic curves and its geometric interpretation we give an explicit algorithm for the group operations on Jacobian varieties of hyperelliptic curves.

Take a genus $g \geq 2$ hyperelliptic curve $\mathcal{C}$ with a least one rational Weierstrass point given by the affine Weierstrass equation

$$W_{\mathcal{C}} : \; y^2 + h(x)\, y = x^{2g+1} + a_{2g} x^{2g} + \cdots + a_1 x + a_0, \tag{2}$$

over k. We denote the prime divisor corresponding to $P_\infty = (0 : 1 : 0)$ by $\mathfrak{p}_\infty$.
We note that the affine coordinate ring of $W_{\mathcal{C}}$ is

$$\mathcal{O} = k[X, Y]/\langle (Y^2 + h(X)\, Y - (X^{2g+1} + a_{2g} X^{2g} + \cdots + a_1 X + a_0)\rangle$$

So degree d prime divisors $\mathfrak{p}$ of $\mathcal{C}$ correspond to prime ideals $P \neq 0$, $[\mathcal{O}/P : k] = d$.

Let ω be the hyperelliptic involution of $\mathcal{C}$. It operates on $\mathcal{O}$ and on $\mathrm{Spec}(\mathcal{O})$ and fixes exactly the prime ideals which "belong" to Weierstrass points, i.e. split up in such points over $\bar{k}$; see (Frey and Shaska, 2019) for details.

Mumford's representation

Following (Mumford, 2008) we introduce polynomial coordinates for points in $J_{\mathcal{C}}(k)$. The first step is to normalize representations of divisor classes. In each divisor class $c \in \mathrm{Pic}^0(k)$ we find a unique *reduced* divisor

$$D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}\infty$$

with $\sum_{i=1}^{r} n_i \deg(\mathfrak{p}_i) = d \leq g$, $\mathfrak{p}_i \neq \omega(\mathfrak{p}_j$ for $i \neq j$ and $\mathfrak{p}_i \neq \mathfrak{p}_i nfty$. (We use Riemann-Roch and the fact that ω induces $-id_{J_{\mathcal{C}}}$.)

Using the relation between divisors and ideal in coordinate rings we get that $n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r$ corresponds to an ideal $I \subset \mathcal{O}$ of degree d and the property that if the prime ideal P_i is such that both P and $\omega(P)$ divide I then it belongs to a Weierstrass point.
By algebra we get that the ideal I is a free $\mathcal{O}$-module of rank 2 and so

$$I = k[X]u(X) + k[x](v(X) - Y).$$

Fact: $u(X), v(X) \in k[X]$, u monic of degree d, $\deg(v) < d$ and u divides $v^2 + h(X)v - f(X)$.

Moreover, c is uniquely determined by I, I is uniquely determined by (u, v) and so we can *take* (u, v) *as coordinates for c.*

Theorem (Mumford representation)

Let $\mathcal{C}$ be a hyperelliptic curve of genus $g \geq 2$ with affine equation

$$y^2 + h(x)\, y \;=\; f(x),$$

where $h, f \in K[x]$, $\deg f = 2g+1$, $\deg h \leq g$. Every non-trivial group element $c \in \mathrm{Pic}^0_{\mathcal{C}}(k)$ can be represented in a unique way by a pair of polynomials $u, v \in K[x]$, such that

i) *u is a monic*

ii) *$\deg v < \deg u \leq g$*

iii) *$u \mid v^2 + vh - f$*

How to find the polynomials u, v?
We can assume without loss of generality that $k = \bar{k}$ and identify prime divisors $\mathfrak{p}_i$ with points $P_i = (x_i, y_i) \in k \times k$. Take the reduced divisor $D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}_\infty$ now with $r = d \leq g$. Then

$$u(X) = \prod_{i=1}^{r} (X - x_i)^{n_i}.$$

Since $(X - x_i)$ occurs with multiplicity n_i in $u(X)$ we must have for $v(X)$:

$$\left(\frac{d}{dx}\right)^j \Big[v(x)^2 + v(x)\, h(x) - f(x)\Big]_{x=x_i} = 0,$$

and one determines $v(X)$ by solving this system of equations.

Genus 2

Let $\mathcal{C}$ be a genus 2 curve defined over a field k. If $\mathrm{char}\, k \neq 2, 3$ the $\mathcal{C}$ is isomorphic to a curve with equation

$$y^2 = a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0.$$

Thus, infinity is a Weierstrass point of $\mathcal{C}$. Let $\mathcal{O} = \infty$ and $D \in \mathrm{Jac}\,(\mathcal{C})$. Then, in the equivalence class of D we find a **reduced divisor** which is given by

$$D = P_1 + P_2 - 2\mathcal{O}$$

where $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ are points in the curve. For any two divisors $D_1 = P_1 + P_2 - 2\mathcal{O}$ and $D_2 = Q_1 + Q_2 - 2\mathcal{O}$ in the reduced form, we determine the cubic polynomial

$$y = g(x) = b_0 x^3 + b_1 x^2 + b_2 x + b_3,$$

going through the points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $Q_1(x_3, y_3)$, and $Q_2(x_4, y_4)$. This cubic will intersect the curve $\mathcal{C}$ at exactly two other points R_1 and R_2 with coordinates

$$R_1 = (x_5, g(x_5)) \quad \text{and} \quad R_2 = (x_6, g(x_6)),$$

where x_5, x_6 are roots of the quadratic

$$x^2 + \left(\sum_{i=1}^{4} x_i \right) x + \frac{b_3^2 - a_5}{b_0^2 \prod_{i=1}^{4} x_i} = 0.$$

Let us denote by $\overline{R}_1 = (x_5, -g(x_5))$ and $\overline{R}_2 = (x_6, -g(x_6))$. Then,

$$D_1 + D_2 = \overline{R}_1 + \overline{R}_2 - 2\mathcal{O}$$

Curves of genus 2

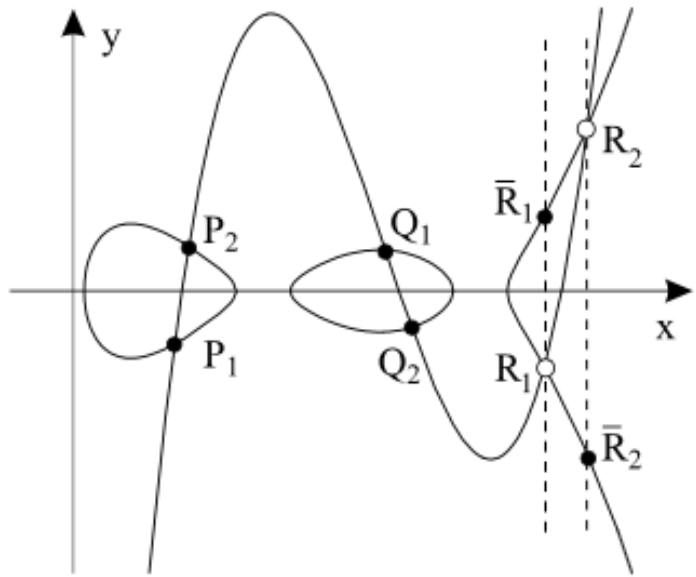


Figure: Addition on Jacobian surfaces

Jacobi polynomials

Let's start with a hyperelliptic curve $\mathcal{C}$ with affine equation

$$y^2 = f(x) = \prod_{i=1}^{2g+1} (x - \alpha_i)$$

defined over a field k. Then $\mathcal{C}$ has a point at infinity and $(x)_\infty = 2 \cdot \infty$ and $(y)_\infty = (2g+1) \cdot \infty$.
Denote by $\mathrm{Div}^d(\mathcal{C})$ the set of degree v divisors in $\mathrm{Div}(\mathcal{C})$ and by $\mathrm{Div}^{+,d}(\mathcal{C})$ the set of positive ones in $\mathrm{Div}^d(\mathcal{C})$. Then $\mathrm{Div}_0^{+,d}(\mathcal{C})$ is the set

$$\mathrm{Div}_0^{+,d}(\mathcal{C}) = \Big\{ D \in \mathrm{Div}^{+,d}(\mathcal{C}) \,|\, \text{ if } \; D = \sum_{i=1}^{d} P_i, \;\; \text{then } \; P_i \neq \infty, \; \text{for all } \; i \\ \text{and } P_i \neq \tau P_j, \;\; \text{for } i \neq j \Big\}$$

where τ is the hyperelliptic involution. Let $D \in \mathrm{Div}_0^{+,d}(\mathcal{C})$ given by

$$D = \sum_{i=1}^{d} \mathfrak{p}_i$$

with $\mathfrak{p}_i = (\lambda_i, u_i)$. By $x(\mathfrak{p}_i)$ we denote the value of x at $\mathfrak{p}_i$. Thus $x(\mathfrak{p}_i) = \lambda_i$ and $y(\mathfrak{p}_i) = u_i$. We follow the idea of Jacobi (Jacobi, 1846) explained in details in (Mumford, 1984) and define

$$U(x) = \prod_{i-1}^{d} (x - \lambda_i) \tag{3}$$

We want to determine a unique polynomial $V(x)$ of degree $< d-1$ such that

$$V(\lambda_i) = u_i, \quad 1 \leq i \leq d.$$

Then we have:

Lemma

The unique polynomial $V(x)$ of degree $\leq d-1$ such that

$$V(\lambda_i) = u_i, \quad 1 \leq i \leq d$$

is given by

$$V(x) = \sum_{i=1}^{d} u_i \frac{\prod_{j \neq i}(x - \lambda_i)}{\prod_{j \neq i}(\lambda_i - \lambda_j)} \tag{4}$$

Moreover,

$$U(x) \mid (f(x) - V(x)^2).$$

Let $W(x)$ be defined as follows

$$W(x) = \frac{1}{U(x)} \left(f(x) - V(x)^2 \right), \tag{5}$$

which from the above is a polynomial. Then we have the following:

Proposition

There is a bijection between $\mathrm{Div}_0^{+,d}(\mathcal{C})$ *and triples* (U, V, W) *such that* U *and* W *are monic and* $degV \leq d - 1$, $degU = d$, $degW = 2g + 1 - d$.

Polynomials $U(x)$, $V(x)$, and $W(x)$ are called **Jacobi polynomials**.

Addition by Interpolation

Another approach to describe addition in the Jacobians of hyperelliptic curves is to use approximation by rational functions; see (Leitenberger, 2005).
For simplicity we assume that $k = \bar{k}$. Let D_1 and D_2 be reduced divisors on Jac ${}_k\mathcal{C}$ given by

$$\begin{aligned} D_1 &= \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_{h_1} - h_1\mathfrak{p}_\infty, \\ D_2 &= \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_{h_2} - h_2\mathfrak{p}_\infty, \end{aligned} \tag{6}$$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ can occur with multiplicities, and $0 \leq h_i \leq g$, $i = 1, 2$. As usual we denote by P_i respectively Q_j the points on $\mathcal{C}$ corresponding to $\mathfrak{p}_i$ and $\mathfrak{q}_j$.
Let $g(X) = \frac{b(X)}{c(X)}$ be the unique rational function going through the points P_i, Q_j. In other words we are determining $b(X)$ and $c(X)$ such that $h_1 + h_2 - 2r$ points P_i, Q_j lie on the curve

$$Y\,c(X) - b(X) \;=\; 0.$$

This rational function is uniquely determined and has the form

$$Y = \frac{b(X)}{c(X)} = \frac{b_0X^p + \ldots b_{p-1}X + b_p}{c_0X^q + c_1X^{q-1} + \cdots + c_q} \tag{7}$$

where

$$p = \frac{h_1 + h_2 + g - 2r - \epsilon}{2}, \quad q = \frac{h_1 + h_2 - g - 2r - 2 + \epsilon}{2},$$

ϵ is the parity of $h_1 + h_2 + g$. By replacing Y from Eq. (7) in Eq. (2) we get a polynomial of degree $\max\{2p, 2q(2g-1)\}$, which gives $h_3 \leq g$ new roots apart from the X-coordinates of P_i, Q_j. Denote the corresponding points on $\mathcal{C}$ by $R_1, \ldots, R_{h_3}$ and $\bar{R}_1, \ldots, \bar{R}_{h_3}$ are the corresponding symmetric points with respect to the $y = 0$ line. Then, we define

$$D_1 + D_2 = \bar{R}_1 + \ldots \bar{R}_{h_3} - h_3\mathcal{O}.$$

For details we refer the reader to (Leitenberger, 2005).

Remark

For $g = 1, 2$ we can take $g(X)$ to be a cubic polynomial.

Exercise

Figure out the formulas for genus 3 hyperelliptic.

Non-hyperelliptic curves

The main question from the above is:

Question
Can the above procedure be extended to non-hyperelliptic curves?

Let $\mathcal{C}$ be a smooth, irreducible, algebraic curve of genus $g \geq 2$, defined over a field K. Let S_d denote the symmetric group of permutations. Then S_d acts on $\mathcal{C}^d$ as follows:

$$\begin{aligned} S_d \times \mathcal{C}^d &\to \mathcal{C}^d \\ (\sigma, (P_1, \ldots, P_d)) &\to (\ldots, P_i^\sigma, \ldots) \end{aligned} \tag{8}$$

We denote the orbit space of this action by $\mathrm{Sym}^d(\mathcal{C})$.
Denote by $\mathrm{Div}^d(\mathcal{C})$ the set of degree v divisors in $\mathrm{Div}(\mathcal{C})$ and by $\mathrm{Div}^{+,d}(\mathcal{C})$ the set of positive ones in $\mathrm{Div}^d(\mathcal{C})$.

Lemma
$\mathrm{Div}^{+\,d}(\mathcal{C}) \cong \mathrm{Sym}^d(\mathcal{C})$.

Let

$$j : \mathcal{C}^d \hookrightarrow \mathbb{P}^{(n+1)d-1}$$

be the Segre embedding. Let $R := \mathbb{C}[\mathcal{C}^d]$ be the homogenous coordinate ring of $\mathcal{C}^d$. Then S_d acts on R by permuting the coordinates. This action preserves the grading. Then j is equivariant under the above action. Hence, the ring of invariants R^{S_d} is finitely generated by homogenous polynomials $f_0, \ldots, f_N$ of degree M. Thus,

$$\mathbb{C}[f_0, \ldots, f_N] \subset \{f \in R^{S_d} \text{ such that } M|\deg f\} \subset R^{S_d}$$

Hence, every element in $\mathbb{C}[f_0, \ldots, f_N]$ we can express it as a vector in $\mathbb{P}^N$ via the basis $\{f_0, \ldots, f_N\}$. Then we have an embedding

$$\mathrm{Sym}^d(\mathcal{C}) \hookrightarrow \mathbb{P}^N$$

with the corresponding following diagram

$$\begin{array}{ccc} \mathcal{C}^d & \xhookrightarrow{\ j\ } & \mathbb{P}^{(n+1)d-1} \\ \downarrow & & \downarrow \\ \mathrm{Sym}^d(\mathcal{C}) & \hookrightarrow & \mathbb{P}^N \end{array}$$

Thus, any divisor $D \in \mathrm{Div}^{+\,d}(\mathcal{C})$ we identify with its correspondent point in $\mathrm{Sym}^d(\mathcal{C})$ and then express it in coordinates in $\mathbb{P}^N$. The variety $\mathrm{Sym}^d(\mathcal{C})$ is smooth because $\mathrm{Sym}^d(\mathcal{C}) \setminus \{\Delta = 0\}$ is biholomorphically to an open set in $\mathbb{C}^d$.

The known result which we will use in our approach is the following:

Theorem
Let $\mathcal{C}$ be a genus $g \geq 2$ curve. The map

$$\phi : \mathrm{Sym}^g(\mathcal{C}) \longrightarrow Jac\,\mathcal{C}$$
$$\sum P_i \longrightarrow \sum P_i - g\infty$$

is surjective. In other words, for every divisor D of degree zero, there exist $P_1, \ldots, P_g$ such that D is linearly equivalent to $\sum_{i=1}^{g} P_i - g\infty$.

See (Mumford, 1984, pg. 3.30). The simplest case of the above construction was suggested by Jacobi and worked out by Mumford in (Mumford, 1984).

So what's the problem?

We still have to figure out those **Jacobi polynomials** which determine $D_1 + D_2$.

The known result which we will use in our approach is the following:

Theorem
Let $\mathcal{C}$ be a genus $g \geq 2$ curve. The map

$$\phi : \mathrm{Sym}^g(\mathcal{C}) \longrightarrow Jac\,\mathcal{C}$$
$$\sum P_i \longrightarrow \sum P_i - g\infty$$

is surjective. In other words, for every divisor D of degree zero, there exist $P_1, \ldots, P_g$ such that D is linearly equivalent to $\sum_{i=1}^{g} P_i - g\infty$.

See (Mumford, 1984, pg. 3.30). The simplest case of the above construction was suggested by Jacobi and worked out by Mumford in (Mumford, 1984).

So what's the problem?

We still have to figure out those **Jacobi polynomials** which determine $D_1 + D_2$.

What about superelliptic curves?

If we want to consider all non-hyperelliptic curves, then for an arbitrary given $g > 2$ we don't know even how the equation of the curve looks like.

So in order to have a general theorem, we want general curves but that we know the general form of the equation.

The answer is **superelliptic curves**.

We explain next.

What about superelliptic curves?

If we want to consider all non-hyperelliptic curves, then for an arbitrary given $g > 2$ we don't know even how the equation of the curve looks like.

So in order to have a general theorem, we want general curves but that we know the general form of the equation.

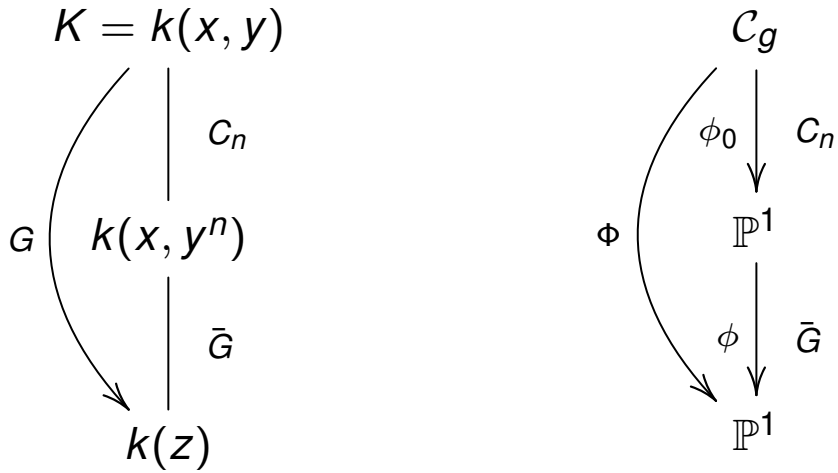
The answer is **superelliptic curves**.

We explain next.

Basics

To generalize the hyperelliptic case we have to consider curves with affine equation $y^n = f(x)$ instead of $y^2 = f(x)$. Hence we need to generalize the *hyperelliptic involution* or the hyperelliptic projection.
A genus $g \geq 2$ smooth, irreducible, algebraic curve $\mathcal{C}$ is called **superelliptic of level n** if there exist an element $\tau \in \mathrm{Aut}(\mathcal{C})$ of order n such that τ is central and the quotient $\mathcal{C}/\langle\tau\rangle$ has genus zero.
Let k be an algebraically closed field of characteristic $p \geq 0$ and $\mathcal{C}_g$ be a genus g cyclic curve given by the equation $y^n = f(x)$ for some $f \in k[x]$. Let $K := k(x, y)$ be the function field of $\mathcal{C}_g$. Then $k(x)$ is degree n genus zero subfield of K. Let $G = \mathrm{Aut}(K/k)$. Since $C_n := Gal(K/k(x)) = \langle\tau\rangle$, with $\tau^n = 1$ such that $\langle\tau\rangle \lhd G$, then group $\bar{G} := G/C_n$ and $\bar{G} \leq PGL_2(k)$. Hence $\bar{G}$ is isomorphic to one of the following: C_m, D_m, A_4, S_4, A_5, *semidirect product of elementary Abelian group with cyclic group*, $PSL(2, q)$ and $PGL(2, q)$, see (Malmendier and Shaska, 2018).

The group $\bar{G}$ acts on $k(x)$ via the natural way. The fixed field is a genus 0 field, say $k(z)$. Thus z is a degree $|\bar{G}|$ rational function in x, say $z = \phi(x)$. We illustrate with the following diagram:



Let $\phi_0 : \mathcal{C}_g \to \mathbb{P}^1$ be the cover which corresponds to the degree n extension $K/k(x)$. Then $\Phi := \phi \circ \phi_0$ has monodromy group $G := \mathrm{Aut}(\mathcal{C}_g)$. From the basic covering theory, the group G is embedded in the group S_l where $l = deg\ \mathbb{P}$. There is an r-tuple $\overline{\sigma} := (\sigma_1, \ldots, \sigma_r)$, where $\sigma_i \in S_l$ such that $\sigma_1, \ldots, \sigma_r$ generate G and $\sigma_1 ... \sigma_r = 1$. The signature of $\mathbb{P}$ is an r-tuple of conjugacy classes $\mathbf{C} := (C_1, ..., C_r)$ in S_l such that C_i is the conjugacy class of σ_i. We use the notation n to denote the conjugacy class of permutations which is cycle of length n. Using the signature of $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ one finds out the signature of $\Phi : \mathcal{C}_g \to \mathbb{P}^1$ for any given g and G.

Let E be the fixed field of G, the Hurwitz genus formula states that

$$2(g_K - 1) = 2(g_E - 1)|G| + deg(\mathfrak{D}_{K/E}) \tag{9}$$

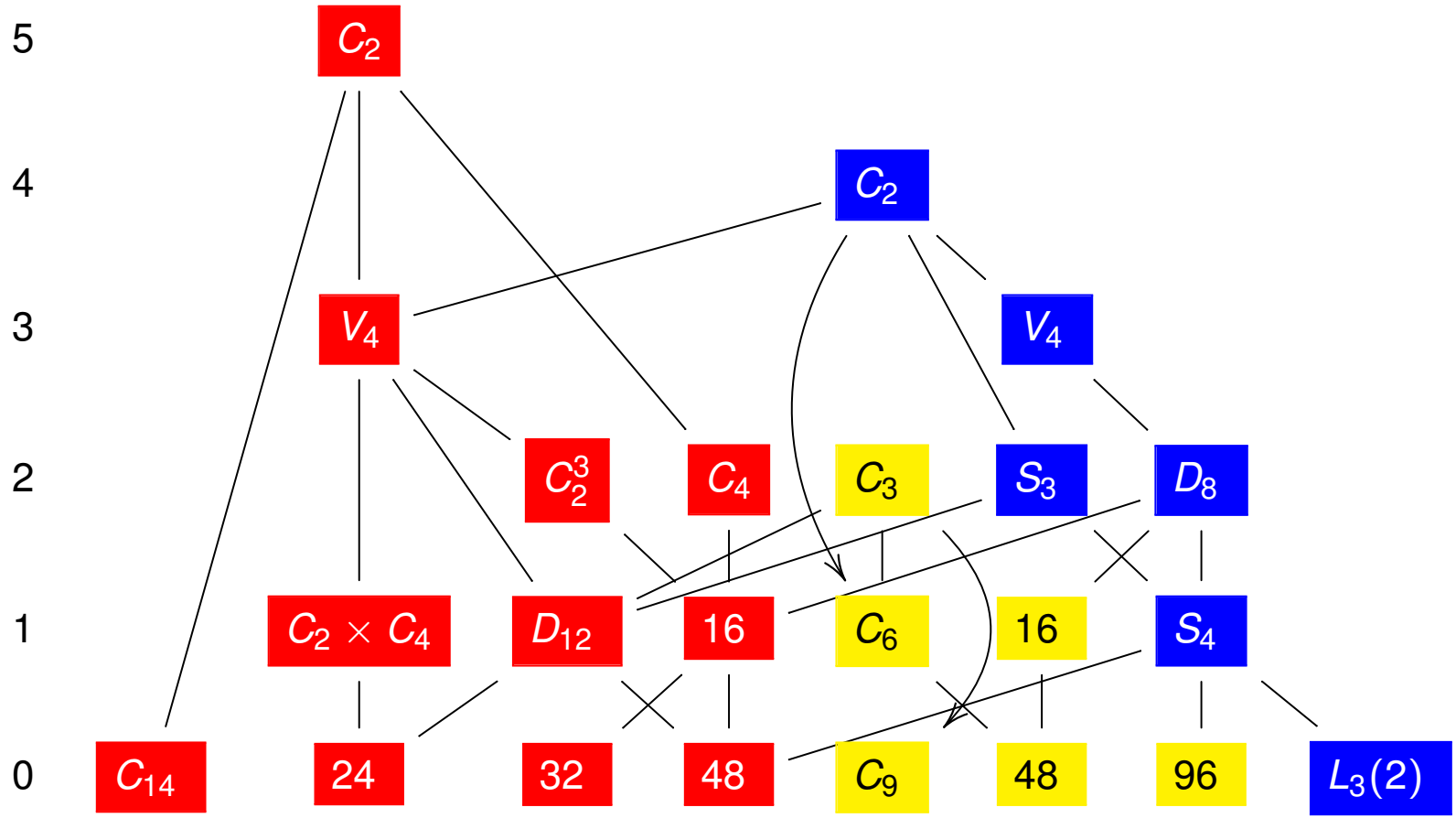
with g_K and g_E the genera of K and E respectively and $\mathfrak{D}_{K/E}$ the different of K/E. Let $\overline{P}_1, \overline{P}_2, ..., \overline{P}_r$ be ramified primes of E. If we set $d_i = deg(\overline{P}_i)$ and let e_i be the ramification index of the $\overline{P}_i$ and let β_i be the exponent of $\overline{P}_i$ in $\mathfrak{D}_{K/E}$. Hence, (1) may be written as

$$2(g_K - 1) = 2(g_E - 1)|G| + |G| \sum_{i=1}^{r} \frac{\beta_i}{e_i} d_i \tag{10}$$

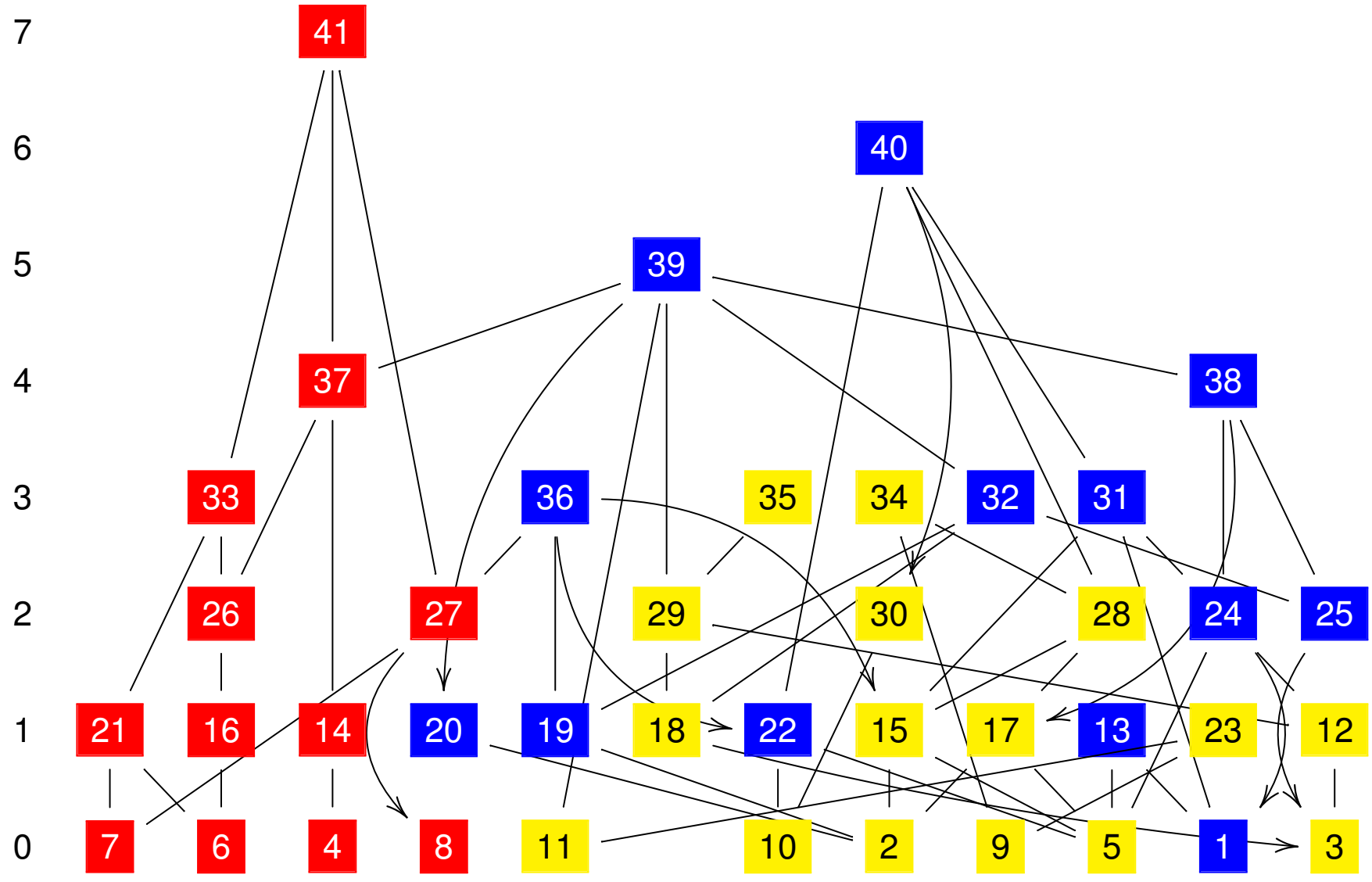
If $\overline{P}_i$ is tamely ramified then $\beta_i = e_i - 1$ or if $\overline{P}_i$ is wildly ramified then $\beta_i = e_i^* q_i + q_i - 2$ with $e_i = e_i^* q_i$, e_i^* relatively prime to p, q_i a power of p and $e_i^* | q_i - 1$. For fixed G, $\mathbf{C}$ the family of covers $\mathbb{P} : \mathcal{C}_g \to \mathbb{P}^1$ is a Hurwitz space $\mathcal{H}(G, \mathbf{C})$. $\mathcal{H}(G, \mathbf{C})$ is an irreducible algebraic variety of dimension $(G, \mathbf{C})$. Using equation (10) and signature $\mathbf{C}$ one can find out the dimension for each G. Next we want to determine the cover $z = \phi(x) : \mathbb{P}^1 \to \mathbb{P}^1$ for all characteristics.

Stratification of the moduli space $\mathcal{M}_g$

Most of the types of curves with extra automorphisms are superelliptic.



The red cases are hyperelliptic loci and the yellow ones are superelliptic (non-hyperelliptic). Notice that from 23 cases only 6 are non-hyperelliptic; see (Magaard et al., 2002).



See (Malmendier and Shaska, 2018).

Other reasons

- Isomorphism classes of superelliptic curves are determined by invariants of binary forms.
- Given invariants of the curves, we can construct an equation of the curve over its field of moduli following techniques as in (Malmendier and Shaska, 2017).
- Important in mathematical physics; see (Clingher et al., 2019) for applications to string theory, etc

Does it work?

The following is preliminary.

Given a superelliptic curve $\mathcal{C}$ with equation

$$\mathcal{C}: \qquad y^n = f(x),$$

such that $\deg f = d$ and two divisors

$$D_1 = \sum_{i=1}^{g} \mathfrak{p}_i - [g]\infty, \quad \text{and} \quad D_2 = \sum_{i=1}^{g} \mathfrak{q}_i - [g]\infty$$

Determine the rational function

$$y = h(x) := \frac{p(x)}{q(x)}$$

such that

$$(p(x))^n = (q(x))^n \cdot f(x)$$

has exactly $3g$ solutions. Thus

$$n \cdot \deg q(x) + d = 3g,$$

or $\deg q(x) = \frac{3g-d}{n}$. A more careful analysis is needed for values of n and d, but it seems to work for all smooth curves.

Determining $h(x)$ as above determines the so called **Jacobi polynomials**.

However, the story is not over. Mumford, Previato, and others have shown that Jacobi polynomials are significant in **differential equations**.

What do the generalized Jacobi polynomials mean in that setting is still mysterious.

This is the scope of investigation in joint work with A. Arsie.

Thank you for your attention!

References

Frey, Gerhard and Tony Shaska. 2019. *Curves, Jacobians, and cryptography*, Contemporary Math. **724**.

Stichtenoth, Henning. 2009. *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin. MR2464941

Mumford, David. 2008. *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

Jacobi, C. G. J. 1846. *Über eine neue Methode zur Integration der hyperelliptischen Differentialgleichungen und über die rationale Form ihrer vollständigen algebraischen Integralgleichungen*, J. Reine Angew. Math. **32**, 220–226. MR1578529

Mumford, David. 1984. *Tata lectures on theta. II*, Progress in Mathematics, vol. 43, Birkhäuser Boston, Inc., Boston, MA. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. MR742776

Leitenberger, Frank. 2005. *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. **46**, no. 1, 125–130. MR2146447

Malmendier, A. and T. Shaska. 2018. *From hyperelliptic to superelliptic curves*, Albanian J. Math. **12**, no. 1, 88–165.

Magaard, K., T. Shaska, S. Shpectorov, and H. Völklein. 2002. *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267**, 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

Malmendier, Andreas and Tony Shaska. 2017. *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13**, Paper No. 089, 17. MR3731039

Clingher, A., A. Malmendier, and T. Shaska. 2019. *Configurations of 6 lines and string dualities*, Comm. Math. Phys. **to appear**.