Lecture 3

Algorithmic Geometry for Function Fields

Summer School UNCG 2016

Florian Hess

Weierstrass Places

First Part

Weierstrass Places

Assume K perfect and let P be a place of degree one of F/K.

The Weierstrass semigroup for P is the additive semisubgroup of $\mathbb{Z}^{\geq 0}$ defined by

$$W(P) = \{-v_P(f) \mid f \in F^\times \text{ with } v_Q(f) \geq 0 \text{ for all } Q \neq P\}$$

Theorem. There is a semisubgroup W of $\mathbb{Z}^{\geq 0}$ such that

$$W = W(P)$$

for almost all P. Moreover, $\#(\mathbb{Z}^{\geq 0} \backslash W(P)) = g$ in general and $\mathbb{Z}^{\geq 0} \backslash W(P) = \{1, \ldots, g\}$ if $\mathrm{char}(F) = 0$.

If $W(P) \neq W$ then P is called Weierstrass place of F/K.

Theorem. There exist Weierstrass places if and only if $g \geq 2$. Their number is between $2g + 2$ and $(g-1)g(g+1)$ for $\mathrm{char}(F) = 0$ and in $O(g^3)$ in general.

Sketch

Let W denote a canonical divisor. The first observation is

$$L(nP) \neq L((n-1)P) \text{ iff } L(W - nP) = L(W - (n-1)P).$$

Thus can/need to study zero and poles of function in $L(W)$ for all P. This can be done using the following tools and objects:

- Higher Derivatives of algebraic functions,
- Wronskian Determinant associated to $L(W)$,
- Invariant divisor.

The Weierstrass places are then the places in the support of this invariant divisor.

Sketch - Essential Idea

Roughly speaking, if $f \in F$ has a zero of order $n \neq 0$ at a place P of degree one, then its i-th derivative $D^{(i)}(f)$ with $i \leq n$ has a zero of order $n - i$ at P.

Let $f_1, \ldots, f_g$ be a basis of $L(W)$ and suppose $P \notin \mathrm{supp}(W)$.

The existence or non-existence of functions in $L(W)$ with prescribed zero orders ε_i at a P can be cast as the linear independece of the vectors

$$(D^{(\varepsilon_i)}(f_1)(P), \ldots, D^{(\varepsilon_i)}(f_g)(P)).$$

Places P where linear independence does not hold are precisely the zeros of the Wronskian determinant

$$\det\left(\left(D^{(\varepsilon_i)}(f_j)\right)_{i,j}\right).$$

Higher Derivatives - Example*

We begin by way of example.

Suppose $f \in \mathbb{C}[x]$. Then also $f \in C[t][x]$ and we can write

$$f = \sum_{i=0}^{\deg(f)} \lambda_i(t)(x-t)^i$$

with $\lambda_i \in C[t]$. The i-th derivative $f^{(i)}$ of f then satisfies

$$f^{(i)}(t) = i! \cdot \lambda_i(t).$$

We wish to generalise this to arbitrary function fields and characteristic.

Note that if $p = \mathrm{char}(F) > 0$ then uninterestingly $f^{(p)}(t) = 0$, so we will take the λ_i as higher derivatives of f.

Local Expansions*

Let P be a place of degree one and π a local uniformizer of P, so $v_p(\pi) = 1$.

For every $f \in F$ and $n \in \mathbb{Z}$ there are uniquely determined $m \in \mathbb{Z}$ and $\lambda_i \in K$ such that

$$v_P\left(f - \sum_{i=m}^{n} \lambda_i \pi^i\right) \geq n + 1.$$

This leads to a K-algebra monomorphism

$$F \to K((t))$$

into the ring of Laurent series over K which maps π to t.

Generic Place*

Let x be a separating element of F/K and $y \in F$ such that $F = K(x, y)$.

Denote $F' = K(x', y')$ an isomorphic copy of F and let FF'/F' be the constant field extension.

There is place P of degree one of FF'/F' which is the unique common zero of $x - x'$ and $y - y'$. Moreover, $x - x'$ is a local uniformizer of P.

This place P is called generic place of F/K.

The generic place is independently of the choice of x and y generated by the set of $f - f'$ for $f \in F$.

Higher Derivatives*

For every $f \in F$ it holds that $v_P(f) \geq 0$. Via local expansions we obtain the monomorphism

$$\phi : F \to F'[[t]],$$

and we define the $D_x^{(i)}(f)$ by

$$\phi(f) = \sum_{i=0}^{\infty} D_x^{(i)}(f)(x - x')^i.$$

Then $D_x^{(i)}(f)$ is called i-th derivative of f with respect to x.

Higher Derivatives and Local Expansions at Places*

A local uniformizer π is also a separating element of F/K.

If $v_P(f) \geq 0$ then $D_\pi^{(i)}(f)(P)$ is the i-th coefficient of the power series expansion of f at P in π.

The element $\pi - \pi' \in FF'$ is also a local uniformizer of the generic place of F/K. Thus the $D_\pi^{(i)}(f)$ can be expressed in terms of the $D_x^{(i)}(f)$ and vice versa.

This is used to define the invariant divisor (under change of x) mentioned above.

Isomorphisms and Automorphisms

Second Part

Isomorphisms

Let $F_{(1)}/K$ and $F_{(2)}/K$ be two function fields over K.

A homomorphism ϕ from $F_{(1)}/K$ to $F_{(2)}/K$ is a K-algebra homomorphism $F_{(1)} \to F_{(2)}$, which is necessarily injective.

If ϕ is surjective it is called an isomorphism.

A homomorphism ϕ is defined by its images in $F_{(2)}$ on generators of $F_{(1)}$ over K.

Theorem. Suppose $F_{(2)}/\phi(F_{(1)})$ is separable and $g_{(1)} \geq 2$. Then ϕ is an isomorphism if and only if $g_{(1)} = g_{(2)}$.

Automorphisms

An isomorphism ϕ of F/K with itself is called an automorphism of F/K. They form a group which is denoted by $\mathrm{Aut}(F/K)$.

Theorem. The automorphism group $\mathrm{Aut}(F/K)$ is finite. If in particular $\mathrm{char}(F) = 0$ then

$$\#\mathrm{Aut}(F/K) \leq 84(g-1).$$

In general, $\#\mathrm{Aut}(F/K)$ is roughly bounded by $16g^4$.

Computation of Isomorphisms

We assume that $g_{(1)} = g_{(2)} \geq 2$ and K is the exact constant field of $F_{(1)}/K$ and $F_{(2)}/K$, for otherwise they are not isomorphic. All this can be checked beforehand.

There are different (better) techniques for $g = 0$ or $g = 1$ and for hyperelliptic function fields.

We compute isomorphisms of complete regular curves C with a distinguished point by computing defining equations for C that are almost uniquely determined.

We assume that K is perfect.

Sketch of Steps of Computation

1. Compute suitable place $P_{(1)}$ of degree one of $F_{(1)}/K$ and a corresponding (small) set of places S of $F_{(2)}/K$ such that any isomorphism would map $P_{(1)}$ inside S.
2. Compute almost unique generators and defining equations for $F_{(1)}/K$ at $P_{(1)}$ and for $F_{(2)}/K$ at $P_{(2)}$ for all $P_{(2)} \in S$.
3. Coefficientwise comparison leads (under some assumptions that always hold if $\mathrm{char}(F)$ is zero or big) to a system of equations in two variables which is easily solved.
4. This yields all isomorphisms $\phi : F_{(1)} \to F_{(2)}$ with $\phi(P_{(1)}) = P_{(2)}$, defined by their images of the computed generators.

The set S can consist of Weierstrass places or places of lowest degree.

Complexity Considerations

Number of Weierstrass places:

- Between $2g+2$ and $(g-1)g(g+1)$ in characteristic zero.
- In general bounded by $O(g^3)$.
- Thus using Weierstrass places $P_{(1)}$ and $P_{(2)}$ can lead to $O(g)$ up to $O(g^3)$ comparisons.

Number of places of degree one for $K = \mathbb{F}_q$:

- Is $q+1+t$ with $|t| \leq 2gq^{1/2}$.
- Thus roughly up to $O(\max\{q, gq^{1/2}\})$ comparisons.

Bound for the number of isomorphisms:

- $84(g-1)$ in $\mathrm{char}(k) = 0$ and roughly $O(g^4)$ for $\mathrm{char}(k) > 0$.

Applications

Testing for isomorphism and the computation of automorphism groups are basic algorithmic problems.

Some applications:

- Tables of function fields and curves.
- Representations of automorphism groups on Riemann-Roch spaces and spaces of differentials.
- Monopole computations in physics.
- ...

Some more details*

If $F_{(1)}$ and $F_{(2)}$ are isomorphic then:

- A place $P_{(1)}$ is mapped to a place $P_{(2)}$.
- We have $\deg(P_{(1)}) = \deg(P_{(2)})$.
- $L(nP_{(1)})$, $L(nP_{(2)})$ and $W(P_{(1)})$, $W(P_{(2)})$ are isomorphic.
- There is a bijection between the sets of Weierstrass places.
- There is a bijection between the sets of places of smallest degree.

The sets of Weierstrass places are finite. If K is finite, the sets of places of smallest degree are also finite.

If $P_{(1)}$ is taken from such a set then there are only finitely many possibilities for its image $P_{(2)}$.

Goal: Turn these necessary conditions for the existence of an isomorphism into a sufficient condition!

Special Generators*

Suppose ϕ is an isomorphism of $F_{(1)}/K$ to $F_{(2)}/K$ such that $P_{(1)}$ is mapped to $P_{(2)}$ and assume $\deg(P_{(\alpha)}) = 1$.

We define some special pole numbers:

- Let $m_0 = 0$ and $m_1 = s > 0$ be minimal in $W(P_{(\alpha)})$.
- Furthermore, let m_i be minimal in $W(P_{(\alpha)})$ such that $m_i \not\equiv m_j \bmod s$ for all $0 < j < i$.
- This yields m_i up to $i = s$, and the m_i are generators of $W(P_{(\alpha)})$.

Special Generators*

We define some corresponding elements of $F_{(\alpha)}$:

- $x_{(\alpha),i} \in L(m_i P_{(\alpha)}) \backslash L((m_i - 1) P_{(\alpha)})$.
- Then
$$1, x_{(\alpha),2}, x_{(\alpha),3}, \dots, x_{(\alpha),s}$$
are a reduced integral basis of $\mathrm{Cl}(K[x_{(\alpha),1}], F_{(\alpha)})$.
- The relation ideal of the $x_{(\alpha),1}, x_{(\alpha),2}, \dots, x_{(\alpha),s}$ is generated by polynomials of the form
$$t_i t_j - \lambda_{(\alpha),i,j,1}(t_1) - \sum_{\nu=2}^{m_1} \lambda_{(\alpha),i,j,\nu}(t_1) t_\nu \quad (2 \le i, j \le s)$$
- In other words, these are the defining polynomials of the corresponding affine regular curve.

Very Special Generators*

Theorem. Assume further that s is coprime to $\mathrm{char}(F)$, if the latter is not zero. Then $F_{(1)}/K$ and $F_{(2)}/K$ are isomorphic and the isomorphism maps $P_{(1)}$ to $P_{(2)}$ if and only if there are

$$x_{(\alpha),1}, \ldots, x_{(\alpha),s}$$

as above and $c, d \in K$ with $c \neq 0$ such that

$$\phi(x_{(1),1}) = c^s x_{(2),1} + d \ \text{ and } \ \phi(x_{(1),i}) = c^s x_{(2),i} \text{ for } i \geq 2 \ .$$

Computing Isomorphisms*

These $x_{(\alpha),i}$ can be computed independently of each other and of ϕ by some rather technical trickery:

- The n-th root of $x_{(\alpha),1}$ is chosen as a local uniformiser $\pi_{(\alpha)}$ at $P_{(\alpha)}$. This is depends only of two parameters c and d.
- The $x_{(\alpha),i}$ are written as Laurent series in $\pi_{(\alpha)}$.
- Using Gaussian elimination, as many as possible coefficients are reduced to zero. This leads to the new $x_{(\alpha),i}$ like in the theorem.
- A coefficientwise comparison of the defining polynomials on slide 20 gives equations for c and d which can easily be solved.

Variations*

There is no $P_{(\alpha)}$ with $\deg(P_{(\alpha)}) = 1$:

- Use constant field extension wrt K_1/K and $K_1 = K(P_{(\alpha)})$.
- Test, whether isomorphisms over K_1 are defined over K.

There is no $P_{(\alpha)}$ with $\deg(P_{(\alpha)}) = 1$ and $\gcd\{s, \mathrm{char}(K)\} = 1$:

- Replace $P_{(\alpha)}$ by suitable $D_{(\alpha)}$ with $\dim(D_{(\alpha)}) = 1$ in the computation of $\pi_{(\alpha)}$.
- Helps sometimes, but not always ...

Working with Different Generators*

Need to compute with isomorphisms. Write generators of one field in the generators of the other field ...

1. $x_{(\alpha),i}$ are represented in generators of $F_{(\alpha)}$, this gives

$$\iota_{(\alpha)} : k(x_{(\alpha),1}, \ldots, x_{(\alpha),s}) \to F_{(\alpha)}.$$

2. Represent generators of $F_{(\alpha)}$ in $K(x_{(\alpha),1}, \ldots, x_{(\alpha),s})$.
   - Gröbner basis approach bad, better use linear algebra.
   - Let $f_{(\alpha)} \in F_{(\alpha)}^{\times}$. Then there is $d \geq 0$ such that $L(rP_{(\alpha)}) \cap fL(rP_{(\alpha)}) \neq \{0\}$. Then $h_1 = f_{(\alpha)} h_2$ with $h_i \in L(rP_{(\alpha)}) \backslash \{0\}$ and h_i is a polynomial in the $x_{(\alpha),i}$.
   - Apply this to generators of $F_{(\alpha)}/K$, gives

$$\iota_{(\alpha)}^{-1} : F_{(\alpha)} \to K(x_{(\alpha),1}, \ldots, x_{(\alpha),s}).$$