# Algorithmics of Function Fields

**Slides for Summer School at UNCG 2016**

**Florian Hess**

**Carl von Ossietzky University Oldenburg**

**June 3, 2016**

# Contents

# Index

# List of Symbols

| | | |
|---|---|---|
| $\mathcal{F}(r)$ | Sheaf $\mathcal{F}$ twisted by $r$ | 1.34 (47) |
| $K'$ | Exact constant field of $F/K$ | 1.4 (15) |
| $K(C)$ | Function field of curve $C$ over $K$ | 1.8 (19) |
| $L(D)$ | Riemann-Roch space of divisor $D$ | 1.27 (39) |
| $\mathcal{O}_C(D)$ | Sheaf of fractional ideals of divisor $D$ | 1.31 (44) |
| $L_{F/K}(t)$ | $L$-polynomial of $F/K$ | 2.29 (86) |
| $L(\chi, t)$ | $L$-series of character $\chi$ | 2.33 (90) |
| $\mathfrak{m}_P$ | Maximal ideal of point $P$ | 1.6 (17) |
| $\mu_n$ | Group of roots of unity of order $n$ | 2.23 (80) |
| $N_d(\chi)$ | Character sum of degree $d$ for character $\chi$ | 2.33 (90) |
| $\mathrm{N}_{E/F}$ | Norm of ray class groups of finite abelian extension $E/F$ | 2.19 (76) |
| $N_m$ | Number of places of degree one of constant field extension of $F/K$ of degree $m$ | 2.13 (70) |
| $\mathcal{O}_P$ | Local ring of point $P$ | 1.6 (17) |
| $\mathcal{O}_{C,P}$ | Local ring of point $P$ of curve $C$ | 1.9 (20) |
| $\mathcal{O}_C(U)$ | Subring of regular functions on subset $U$ of curve $C$ | 1.9 (20) |
| $\mathcal{O}_C$ | Structure sheaf of curve $C$ | 1.9 (20) |
| $\mathbb{P}^1$ | One-dimensional projective space | 1.14 (26) |
| $\phi^\#$ | $K$-algebra monomorphism of morphism $\phi$ | 1.12 (24) |
| $\phi_{\mathfrak{m},\mathfrak{n}}$ | Epimorphism $\mathrm{Pic}_\mathfrak{m}(F/K) \to \mathrm{Pic}_\mathfrak{n}(F/K)$ | 2.16 (73) |
| $\mathrm{Pic}(F/K)$ | Class group or Picard group of $F/K$ | 2.3 (60) |
| $\mathrm{Pic}^d(F/K)$ | Set of divisor classes of $F/K$ of degree $d$ | 2.3 (60) |
| $\mathrm{Pic}_\mathfrak{m}(F/K)$ | Ray class group of $F/K$ modulo $\mathfrak{m}$ | 2.16 (73) |
| $\mathrm{Pic}^0_\mathfrak{m}(F/K)$ | Ray class group of degree zero of $F/K$ modulo $\mathfrak{m}$ | 2.16 (73) |
| $\mathrm{Princ}(F/K)$ | Group of principal divisors of $F/K$ | 2.3 (60) |
| $\mathrm{Princ}_\mathfrak{m}(F/K)$ | Group of principal divisors of $F/K$ congruent one modulo $\mathfrak{m}$ | 2.16 (73) |
| $R_\mathfrak{m}$ | Local ring of maximal ideal $\mathfrak{m}$ of $R$ | 20 |
| $\mathrm{Specm}(R)$ | Spectrum of maximal ideals of $R$ | 1.10 (22) |

| | | |
|---|---|---|
| $\mathrm{supp}(P)$ | Support of point $P$, set of places that dominate $P$ | 1.7 (18) |
| $v_P(D)$ | Coefficient of divisor $D$ at $P$ | 1.31 (44) |
| $\zeta_{F/K}$ | Zeta function of $F/K$ | 2.28 (85) |
| $\zeta$ | Root of unity in $\mathbb{C}^\times$ | 2.34 (91) |

# Lecture 1

# Function Fields, Curves and Global sections

Summer School UNCG 2016

Florian Hess

# Introduction

## Function Fields vs. Curves

Function fields vs. regular complete curves:

- Essentially boil down to the same thing - there is an equivalence of categories.
- If base field is $\mathbb{C}$ then there is another equivalence of categories, to compact Riemann surfaces and covering maps.
- So using one term over the other is more a socialogical question about one's mathematical genesis or point of view ...
- Best to know all three ...

Curves can also be singular, this gives some added ways of expressing matters.



A reference for the equivalence of categories is Hartshorne, "Algebraic Geometry", GTM Springer, I.6 or Liu, "Algebraic Geometry and Arithmetic Curves", OGTM, 2002, Proposition 7.3.13.

Equivalence of categories means that up to isomorphism there is a bijection between function fields and regular complete (projective) curves and between their structure preserving maps that preserves identities and compositions. Properties that are invariant under isomorphism can thus be defined and investigated for function fields and curves alike.

Why talk function fields?

- There was an active German school porting algebraic number theory to the function field case around 1930.
- This point of view continues to exist in the literature and research of algebraic number theoretic type, e.g. in books of Eichler, Stichtenoth, Rosen, Villa Salvador, Goss, Thakur, see catch word "'Arithmetic of Function Fields"'.
- Research and implementation of algorithms for number fields have been very active and systematic since say 1990, e.g. Kant/Kash, Pari/GP and Magma. Those number theoretic algorithms were ported successfully to the function field case.
- Hence the name of this summer school.

Why talk curves?

- Usually when the background or tools are more geometric, when singular curves are required, or when the base field is not a finite field or is even not a field ...
- Hasse came from the algebraic number theory side, Weil used algebraic geometry when proving Hasse-Weil.
- Serre gave a geometric development of class field theory.
- The theory of complex multiplication of Deuring started out function field theoretic and was then turned curve theoretic.
- Algorithms for algebraic-geometric codes have mostly been approached via curves.
- In cryptography one talks elliptic and hyperelliptic curves, i.e. curve based cryptography.

So when talk function fields and when curves?

- Depends on the situation and audience ...
- Algebraic geometry usually gives more tools and more ways of expressing matters for function fields than algebraic number theory. If those are required, use curves.
- Curve notation can be overly technical, but is also often better known.
- Function field notation tends to be simpler and can be more to the point, if sufficient for the purpose.

# Function Fields

Let $K$ be a field. An algebraic function field of one variable is a field extension $F/K$ of transcendence degree one.

This means that there is $x \in F$ such that $x$ is transcendental over $K$ and $F/K(x)$ is finite.

The exact constant field of $F/K$ is the algebraic closure $K'$ of $K$ in $F$.

The extension $F/K'$ is also an algebraic function field of one variable, the $x$ from above is still transcendental over $K'$ and $F/K'(x)$ is finite.

In theory one can always assume w.l.o.g. that $K' = K$. In practice one can not or should not.

Algorithmics of Function Fields

1 Function Fields, Curves, Global Sections

Introduction
Function Fields vs. Curves
Function Fields
Curves
Representation and Definition
Representation
Via Affine Curve
Completion
Normalisation
Magma
Global Sections
Outline
Sheaves
Diagonalisation
Global Sections
Grothendiecks Theorem
Riemann-Roch
Special Models
Magma
Exercises

## Separating Elements

The element $x$ is called separating for $F/K$ if $F/K(x)$ is separable. It is a theorem that if $K$ is perfect then there is always a separating element for $F/K$.

Fields of characteristic zero, finite fields and algebraically closed fields are perfect. Any algebraic extension field of a perfect field is perfect.

*Example.* The polynomial $y^2 + x^2 + t \in \mathbb{F}_2(t, x)[y]$ is irreducible and purely inseparable. Thus

$$F = \mathbb{F}_2(t, x)[y]/\langle y^2 + x^2 + t\rangle$$

is a purely inseparable field extension of degree two of $\mathbb{F}_2(t, x)$. Then $F/\mathbb{F}_2(t)$ is an algebraic function field without a separating element.

5 / 44

The existence of a separating element is a special case of the notion of separability for arbitrary field extensions $F/K$. See Fried and Jarden, Field Arithmetic or P. Cohn, Basic Algebra: Groups, Rings and Fields, or Bosch, Algebra (in German). In geometric contexts this is a refined version of Noether normalisation.

For the statements on perfect fields see any textbook on algebraic field extensions, e.g. Lang, Algebra.

We cite some useful theorems in this context. Let $K^{1/p}$ be the $K$ in characteristic zero and the field of all $p$-th roots of elements of $K$ if $p = \mathrm{char}(F) > 0$.

**Theorem.** *A finitely generated field extension $F/K$ has a separating transcendence basis if and only if $F/K$ and $K^{1/p}/K$ are linearly disjoint.*

A finitely generated field extension $F/K$ that satisfies the condition of the theorem it is called regular.

**Theorem.** *Let $A$ be a finitely generated reduced $K$-algebra. Then the follwoing are equivalent:*

1. *$K^{1/p} \otimes_K A$ is reduced.*

2. *$K^{\mathrm{alg}} \otimes_K A$ is reduced.*

3. *$F \otimes_K A$ is reduced for all field extensions $F/K$.*

**Theorem.** *Let $A$ be a finitely generated integral $K$-algebra such that $K^{\mathrm{alg}} \otimes_K A$ is reduced. Then $K^{\mathrm{alg}} \otimes_K A$ is an integral domain if and only if $K$ is algebraically closed in $A$.*

Some references are an old version of the script of Milne on Algebraic Geometry or Zariski and Samuel 1958, III 15, Theorem 40.

# Local rings and Points

We give a "function field" based approach to curves in the spirit of Hartshorne I.6, including singular curves.

Let $F/K$ be an algebraic function field. A subring of $F/K$ is a proper subring $\mathcal{O}$ of $F$ with $K^\times \subseteq \mathcal{O}^\times$ and $\mathrm{Quot}(\mathcal{O}) = F$.

If $\mathcal{O}$ is subring of $F/K$ and a local ring with maximal ideal $\mathfrak{m}$ we call it a point $P$ of $F/K$ with local ring $\mathcal{O}_P = \mathcal{O}$ and maximal ideal $\mathfrak{m}_P = \mathfrak{m}$.

A place of $F/K$ is regarded as point of $F/K$.

## Domination

Let $P$ und $Q$ be points of $F/K$. We say that $P$ is dominated by $Q$ if $\mathcal{O}_P \subseteq \mathcal{O}_Q$ and $\mathfrak{m}_P \subseteq \mathfrak{m}_Q$ holds.

We define $\mathrm{supp}(P)$ as the set of places $Q$ of $F/K$ such that $P$ is dominated by $Q$.

*Theorem.* The sets $\mathrm{supp}(P)$ are non-empty and finite. The residue class fields $\mathcal{O}_P/\mathfrak{m}_P$ are finite over $K$.



*Proof.* See Stichtenoth 1.1.19 for the existence of at most one place $Q$. But there are only finitely many such places: First observe $\mathfrak{m}_P \neq 0$ for otherwise $\mathcal{O}_P$ is a field and then $\mathcal{O}_P = \mathrm{Quot}(\mathcal{O}_P) = F$, hence $\mathcal{O}_P$ is not a proper subring of $F/K$. Since $K^\times \subseteq \mathcal{O}_P^\times$ we also have $(K')^\times \cap \mathcal{O}_P \subseteq \mathcal{O}_P^\times$. Thus any $x \in \mathfrak{m}_P$ with $x \neq 0$ is transcendental over $K$. If $Q$ dominates $P$ then $x \in Q$. Since $x$ has only finitely many zeros by Stichtenoth 1.3.4 the claim follows.

We know $[\mathcal{O}_Q/\mathfrak{m}_Q : K] < \infty$ by Stichtenoth 1.1.15. Let $\phi : \mathcal{O}_P \to \mathcal{O}_Q/\mathfrak{m}_Q$ be the composition of the inclusion and residue class epimorphism. Then $\ker(\phi) = \mathcal{O}_P \cap \mathfrak{m}_Q \supseteq \mathfrak{m}_P$. Since $\mathfrak{m}_P$ is maximal and $\phi$ is the identity on $K$, we have $\ker(\phi) = \mathfrak{m}_P$. Thus $\mathcal{O}_P/\mathfrak{m}_P$ is an intermediate field of $\mathcal{O}_Q/\mathfrak{m}_Q$ and $K$, and hence also finite over $K$. $\square$

A local ring $\mathcal{O}$ with maximal ideal $\mathfrak{m}$ satisfies $\mathcal{O} = \mathcal{O}^\times \cup \mathfrak{m}$ and $\mathcal{O}^\times \cap \mathfrak{m} = \emptyset$. In the relation of domination the cases $\mathcal{O}_P^\times \subsetneq \mathcal{O}_Q^\times$ and $\mathfrak{m}_P = \mathfrak{m}_Q$ as well as $\mathcal{O}_P^\times = \mathcal{O}_Q^\times$ and $\mathfrak{m}_P \subsetneq \mathfrak{m}_Q$ can indeed occur (see exercises).

## Sets of Points and Curves

We will only consider sets $U$ of points of $F/K$ that are

- admissible, i.e. almost all points of $U$ are places.
- separated, i.e. for every place $Q$ of $F/K$ there is at most one $P \in U$ such that $P$ is dominated by $Q$.

Let $U^c$ denote the set of places of $F/K$ that are not contained in $\cup_{P \in U} \mathrm{supp}(P)$. Then $U$ is called cofinite, complete, and affine if $U^c$ is finite, empty and non-empty respectively.

A curve $C$ over $K$ is an admissible separated cofinite set of points of $F/K$.

The function field of $C$ is $K(C) = F$.

A point $P \in C$ is regular if $P$ is a place, otherwise singular. The curve is regular if all points of $C$ are regular.



These definitions capture what is usually called an irreducible algebraic curve over $K$. The definition of sparated amounts to the usual valuational criterion of separatedness. Likewise, the definition of complete amounts to the valuational criterion for properness over $\mathrm{Spec}(K)$.

The maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_P$ is regular if and only $\mathcal{O}_P$ is a discrete valuation ring, and this is case if and only if the $\mathcal{O}_P/\mathfrak{m}_P$-vector space $\mathfrak{m}_P/\mathfrak{m}_P^2$ has dimension one. The latter can usually be checked by the geometrically motivated Jacobian criterion, see Liu "Algebraic Geometry and Arithmetic Curves", OGTM, 2002, Proposition 3.30. A more number theoretic test is the Dedekind criterion, see for example Cohen, "Algorithmic Number Theory", GTM, 1993.

## Subrings

Let $P \in C$ and $U \subseteq C$. We define $\mathcal{O}_{C,P} = \mathcal{O}_P$ and

$$\mathcal{O}_C(U) = \cap_{P \in U} \mathcal{O}_{C,P},$$

where the empty intersection is defined as $F$.

*Theorem.* Suppose $U$ is affine.

1. The rings $\mathcal{O}_C(U)$ are subrings of $F/K$ and the maps

$$P \mapsto \mathcal{O}_C(U) \cap \mathfrak{m}_P \quad \text{and} \quad \mathfrak{m} \mapsto \mathcal{O}_C(U)_{\mathfrak{m}}$$

give mutually inverse bijections from $U$ to the set of non-zero maximal ideals of $\mathcal{O}_C(U)$.

2. Every point in $U$ is regular if and only if $\mathcal{O}_C(U)$ is a Dedekind domain.
3. With $D_U(f) = \{P \in U \,|\, f \notin \mathfrak{m}_P\}$ for $f \in \mathcal{O}_C(U)$,

$$\mathcal{O}_C(D_U(f)) = \mathcal{O}_C(U)[f^{-1}].$$



If $R$ is a subring of $F/K$ and $U \subseteq R$ with $0 \notin U$, we write $R[U^{-1}]$ for the subring of $F/K$ generated by $R$ and the inverses of all elements of $U$. If $\mathfrak{m}$ is a maximal ideal of $R$ we write $R_{\mathfrak{m}} = R[(R\backslash\mathfrak{m})^{-1}]$. If $\mathcal{O}$ is a local subring with maximal ideal, then $\mathcal{O}\backslash\mathfrak{m} = \mathcal{O}^{\times}$, so $\mathcal{O} = \mathcal{O}_{\mathfrak{m}}$.

In more general contexts, $\mathcal{O}_C(\emptyset)$ is defined as the null ring.

**Proposition 1.9.1.** *Let $P$ be a point of $F/K$ and $S_P = \cap_{Q \in \mathrm{supp}(P)} \mathcal{O}_Q$. The conductor*

$$\mathfrak{f}_P = \{x \in S_P \,|\, xS_P \subseteq \mathcal{O}_P\}$$

*of the ring extension $S_P/\mathcal{O}_P$ is a non-zero ideal of $S_P$ with $\mathfrak{f}_P \subseteq \mathcal{O}_P$, and $\mathfrak{f}_P = \mathcal{O}_P$ if $P$ is a place.*

*Proof.* The relevant statement here is the non-zeroness. The proposition can be proven using the finiteness of the integral closure of finitely generated $K$-algebras (see Hartshorne 3.9A). We refer to Rosenlicht, “Equivalence Relations on Algebraic Curves”, Annals of Math. vol. 56, 1952, pp. 169-191. □

**Theorem 1.9.2.** *Let $U$ be an affine subset of $C$. Furthermore, let $P, P_1, \ldots, P_s \in U$ be pairwise distinct and $d_1 \in \mathcal{O}_{C,P_1}, \ldots, d_s \in \mathcal{O}_{C,P_s}$ non-zero. Then there is $d \in \mathcal{O}_{C,P}^{\times}$ such that $d$ is a multiple of $d_i$ in $\mathcal{O}_{C,P_i}$ for all $1 \le i \le s$ and $d \in \mathcal{O}_{C,Q}$ for all $Q \in U$.*

*Proof.* Proposition 1.9.1 shows that every ideal of $S_P$ contained in $\mathfrak{f}_P$ is also contained in $\mathcal{O}_P$. Thus if $x \in F$ and $v_Q(x)$ is sufficiently large for all $Q \in \mathrm{supp}(P)$, then $x \in \mathfrak{f}_P \subseteq \mathfrak{m}_P \subseteq \mathcal{O}_P$.

We may suppose that $P, P_1, \ldots, P_s$ ranges over all points of $U$ that are not places, by choosing additional $d_i = 1$ if neccessary. Since $U$ is affine, the Strong Approximation Theorem in Stichtenoth can be applied and shows that there is $d \in F$ with the following properties: First, $v_Q(d-1)$ is large for all $Q \in \operatorname{supp}(P)$. Second, $v_Q(x/d_i)$ is large for all $Q \in \operatorname{supp}(P_i)$ and $1 \leq i \leq s$, and third $v_Q(x) \geq 0$ for all other $Q \in U$. The inital remark then shows $d - 1 \in \mathfrak{m}_P$, thus $d \in \mathcal{O}_{C,P}^\times$, and $d/d_i \in \mathcal{O}_{C,P_i}$ for all $1 \leq i \leq s$ so $d_i$ divides $d$ in $\mathcal{O}_{C,P_i}$. This proves the theorem. □

*Proof of Theorem of Slide.* 1.: The ideal $\mathcal{O}_C(U) \cap \mathfrak{m}_P$ is maximal, since $\mathcal{O}_C(U)/\mathcal{O}_C(U) \cap \mathfrak{m}_P$ is a $K$-algebra in $\mathcal{O}_P/\mathfrak{m}_P$, which is algebraic over $K$, and hence a field. On the other hand, $\mathcal{O}_C(U)_\mathfrak{m}$ is a local ring and it is clear that $\mathfrak{m}\mathcal{O}_C(U)_\mathfrak{m} \cap \mathcal{O}_C(U) = \mathfrak{m}$, so it remains to show that $\mathcal{O}_C(U)_{\mathcal{O}_C(U) \cap \mathfrak{m}_P} = \mathcal{O}_{C,P}$.

The inclusion $\subseteq$ is obvious. In order to prove $\supseteq$, let $x \in \mathcal{O}_{C,P}$. Then $x \in \mathcal{O}_{C,Q}$ for almost all $Q \in U$, since $x$ has only finitely many poles and almost all $Q \in U$ are places. Denote those finitely many points of $U$ different from $P$ and these $Q$ by $P_1, \ldots, P_s$. Since $\mathcal{O}_{C,P_i}$ is a subring of $F/K$ there are $d_i \in \mathcal{O}_{C,P_i}$ non-zero with $d_i x \in \mathcal{O}_{C,P_i}$ for all $i$.

By Theorem 1.9.2 there is $d \in \mathcal{O}_{C,P}^\times$, which is a multiple of $d_i$ in $\mathcal{O}_{C,P_i}$ and an element of $\mathcal{O}_{C,Q}$ for all $Q$ as above. Then $d, dx \in \mathcal{O}_C(U)$ and $d \notin \mathcal{O}_C(U) \cap \mathfrak{m}_P$. This shows $x = (dx)/d \in \mathcal{O}_C(U)_{\mathcal{O}_C(U) \cap \mathfrak{m}_P}$, as required.

2.: First $\mathcal{O}_{C,P}$ is noetherian and one-dimensional since by the theorem of the next slide it is a localisation of a noetherian and one-dimensional ring. Furthermore, $\mathcal{O}_{C,P}$ is a regular local ring if and only if $\mathcal{O}_{C,P}$ is a discrete valuation ring, see for example Atiyah-Mcdonald, "Commutative Algebra". In combination this gives the usual local criterion for a ring to be a Dedekind ring.

3.: We have $f \notin \mathfrak{m}_P$ for all $P \in D_U(f)$, so $f^{-1} \in \mathcal{O}_{C,P}$ and $f^{-1} \in \mathcal{O}_C(D_U(f))$. Thus $\mathcal{O}_C(D_U(f))[f^{-1}] = \mathcal{O}_C(D_U(f))$. On the other hand, if $f \in \mathfrak{m}_P$ then $\mathcal{O}_{C,P}[f^{-1}] = F$, since this local ring cannot be dominated by a place. The following Lemma 1.9.3 then shows

$$\mathcal{O}_C(U)[f^{-1}] = \mathcal{O}_C(D_U(f))[f^{-1}] \cap (\cap_{P \in U, f \in \mathfrak{m}_P} \mathcal{O}_{C,P}[f^{-1}]) = \mathcal{O}_C(D_U(f)),$$

as was to be proven. □

**Lemma 1.9.3.** *Suppose $R$ and $S$ are subrings of a field $F$ and let $U \subseteq R \cap S$ be multiplicatively closed with $1 \in U$. Then*

$$R[U^{-1}] \cap S[U^{-1}] = (R \cap S)[U^{-1}].$$

*Proof.* Since $R \cap S \subseteq R$ and $R \cap S \subseteq S$ we have $(R \cap S)[U^{-1}] \subseteq R[U^{-1}]$ and $(R \cap S)[U^{-1}] \subseteq S[U^{-1}]$, so $(R \cap S)[U^{-1}] \subseteq R[U^{-1}] \cap S[U^{-1}]$.

Let $x \in R[U^{-1}] \cap S[U^{-1}]$. Then there are $r \in R$, $s \in S$ and $u, v \in U$ such that

$$x = \frac{r}{u} = \frac{s}{v} = \frac{rv}{uv} = \frac{us}{uv}$$

with $rv \in R$, $us \in S$ and $uv \in U$. Since $F$ has no zero divisors we conclude $rv = us$, so $rv = us \in R \cap S$ and $x \in (R \cap S)[U^{-1}]$. □

## Affine Curves

If $R$ is a subring of $F/K$ we define $\mathrm{Specm}(R)$ to be the set of points of $F/K$ defined by $R_\mathfrak{m}$ where $\mathfrak{m}$ ranges over the maximal ideals of $R$.

*Theorem.* The map $C \mapsto \mathcal{O}_C(C)$ gives an inclusion-reversing bijection of the set of *affine curves* $C$ over $K$ with $K(C) = F$ to the set of subrings $R$ of $F/K$ that are *finitely generated* $K$-algebras. Its inverse is given by $R \mapsto \mathrm{Specm}(R)$.

This provides the link to the usual definition of affine curves.



The theorem is basically the reason why one can compute with curves and function fields.

*Proof of Theorem of Slide.* By Theorem 1.9.2 there is transcendental $x \in \mathcal{O}_C(C)$. The integral closure of $K[x]$ in $F$ is $S = \cap_{P \in C, Q \in \mathrm{supp}(P)} \mathcal{O}_{C,Q}$ (see Stichenoth Theorem 3.2.6) which contains $\mathcal{O}_C(C)$. Then $S$ and $\mathcal{O}_C(C)$ are $K[x]$-modules and since $S$ is finite over $K[x]$ by the finiteness of integral closures of finitely generated $K$-algebras, $\mathcal{O}_C(C)$ is also finite over $K[x]$. Thus $\mathcal{O}_C(C)$ is a finitely generated $K$-algebra. The rest is left to the reader. $\square$

Since $\mathcal{O}_C(C)$ is a finitely generated $K$-algebra, it is noetherian. Let $\mathfrak{p} \neq 0$ be a prime ideal of $\mathcal{O}_C(C)$. Then there is a place $P$ such that $\mathcal{O}_P$ dominates $\mathcal{O}_C(C)_\mathfrak{p}$. We obtain the following monomorphisms of $K$-algebras

$$K \to \mathcal{O}_C(C)/\mathfrak{p} \to \mathcal{O}_C(C)_\mathfrak{p}/\mathfrak{p}\mathcal{O}_C(C)_\mathfrak{p} \to \mathcal{O}_P/\mathfrak{m}_P.$$

Since $\mathcal{O}_P/\mathfrak{m}_P$ is algebraic over $K$, $\mathcal{O}_C(C)/\mathfrak{p}$ must be a field. Hence $\mathfrak{p}$ is maximal and $\mathcal{O}_C(C)$ one-dimensional.

## Curves as Topological Spaces*

Let $C$ be a curve over $K$. A subset $U$ of $C$ is called open if $U$ is empty or $C \backslash U$ is finite.

*Theorem.* Let $C$ be a curve over $K$.

1. Then $C$ with its open sets is a topological space.
2 Moreover, it is an irreducible, one-dimensional $T_1$-space and any open subset of $C$ is quasicompact.
3. If $C$ is affine the sets $D_C(f)$ form a basis of the open sets of $C$.



*Proof of the theorem.* 1.: The closed sets are precisely the finite sets of the whole space $C$ or $C$. Finite unions and arbitrary intersections of such sets are again such sets, hence $C$ is a topological space.

2.: If $C$ is the union of two closed sets $S_1$ and $S_2$, then $S_1 = C$ or $S_2 = C$ since $F/K$ and hence $C$ has infinitely many places or points respectively by Stichtenoth 1.3.2. This shows that $C$ is irreducible.

The chains of closed irreducible subsets are thus of the form $C \supsetneq \{P\}$ for $P \in C$, hence the dimension of $C$ is one.

If $P, Q \in C$ are distinct then $\{P\}$ is closed and $U = C \backslash \{P\}$ is open with $Q \in U$. Thus $C$ is a $T_1$-space. Note that it is not a $T_2$-space.

Let $U \subseteq C$ open and let $(U_i)_{i \in I}$ be an open covering. Then $U \backslash U_i$ is finite, hence finitely many $U_i$ suffice to cover $U$. Thus $U$ is quasicompact.

3.: Let $U \subseteq C$ be open, $P \in U$ and $V = C \backslash U$ closed and hence finite. Then by the chinese remainder theorem there exists a non zero $f \in \mathcal{O}_C(V \cup \{Q\})$ contained in every $\mathfrak{m}_P$ for $P \in V$ and not contained in $\mathfrak{m}_Q$. Then $Q \in D_C(f) \subseteq U$. $\square$

## Morphisms

Let $X$ and $Y$ be curves over $K$. A morphism $\phi : X \to Y$ is defined by a $K$-algebra monomorphism $\phi^{\#} : K(Y) \to K(X)$ such that $\phi^{\#}$ restricts for each $P \in X$ to

$$\phi_P^{\#} : \mathcal{O}_{Y,\phi(P)} \to \mathcal{O}_{X,P}.$$

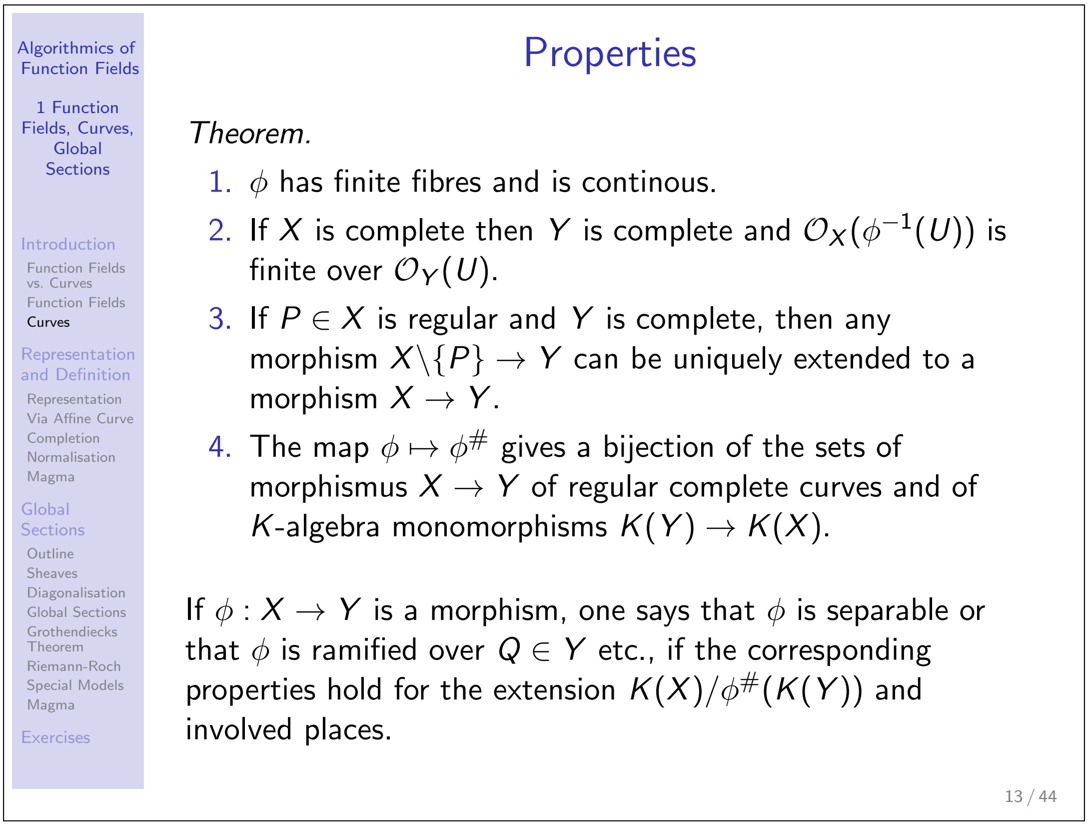
Then $\phi(P) = (\phi_P^{\#})^{-1}(P)$, and if $U \subseteq Y$ we obtain by further restriction

$$\phi^{\#}(U) : \mathcal{O}_Y(U) \to \mathcal{O}_X(\phi^{-1}(U)).$$

The degree of $\phi$ is $\deg(\phi) = [K(X) : \phi^{\#}(K(Y))]$.



In usual terms these morphisms are dominant morphisms. Morphisms which map $X$ to just one point of $Y$ are not covered by our definition.




We extend the notion of domination to arbitrary local rings. Any local $K$-algebra in $F$ is then still dominated by only finitely many places of $F/K$.

*Proof of Theorem of Slide.* 1.: The fibres are finite because there are only finitely many places of $K(X)$ that dominate any given $\mathcal{O}_{Y,P}$, and each such place gives rise to at most one point in the fibre.

Thus the preimage of finite sets under $\phi$ are finite and so preimages of closed sets are closed again, hence $\phi$ is continous.

2.: Let $P$ be a place of $K(Y)$. Then there is a place $Q$ of $K(X)$ dominating it where we regard $K(Y)$ embedded into $K(X)$ according to $\phi$. Since $X$ is complete, there is precisely one point $Q' \in X$ which is dominated by $Q$. Now $\phi(Q') \in Y$ is dominated by $P$, hence $Y$ is complete.

Similar like before, $\mathcal{O}_X(\phi^{-1}(U))$ is contained in the integral closure of $\mathcal{O}_Y(U)$. The integral closure and then $\mathcal{O}_X(\phi^{-1}(U))$ are finite over $\mathcal{O}_Y(U)$.

3. and 4. are left to the reader. □

# Example

Let $F/K$ be the rational function field over $K$.

We define $\mathbb{A}^1$ as the set of places of $F/K$ corresponding to the maximal ideals of $K[x]$, where $x$ is a generator of $F/K$. This is a regular affine curve.

We define $\mathbb{P}^1$ as the set of places of $F/K$. This is a regular complete curve.

There is a bijection between the set of generators of $F/K$ and the set of morphisms $\mathbb{A}^1 \to \mathbb{P}^1$ of degree one.

Algorithmics of Function Fields

1 Function Fields, Curves, Global Sections



## Normalisation

Let $C$ be curve over $K$.

The normalisation $\tilde{C}$ of $C$ is the set of places of $K(C)$ that dominate points of $C$.

There is a morphism $\phi : \tilde{C} \to C$ of degree one, mapping each place to the point of $C$ that it dominates.

The normalisation $\tilde{C}$ of $C$ is a regular curve. If $C$ is complete then $\tilde{C}$ is also complete.

$\mathcal{O}_{\tilde{C}}(\phi^{-1}(U))$ is the integral closure of $\mathcal{O}_C(U)$ in $K(C)$.

Normalisation is thus also desingularisation!

15 / 44

In higher dimensions (not the curve case), normalisation is not sufficient for desingularisation.

# Representation and Definition of Function Fields and Curves

## General Idea

Task: Represent

- (irreducible) complete regular curve $C$ over a field $K$, with
- morphism $\phi : C \to \mathbb{P}^1$ of degree $n$.

This can be done using $K[x]$-algebras that are finitely generated, free modules over $K[x]$ of rank $n$, called $K[x]$-orders.

Advantages and disadvantages:

- Linear algebra over $K[x]$ vs. Gröbner basis computations.
- Many existing algorithms from algebraic number theory, e.g. normalisation, ideal arithmetic, valuations, residue class fields, different etc.

There are of course other approaches and points of view (projective, geometric, Khuri-Makdisi).

# Representation using orders

We embed $K(\mathbb{P}^1)$ via $\phi^*$ into $K(C)$ and choose $x \in K(\mathbb{P}^1)$ to correspond to $\phi$. The pole of $x$ in $\mathbb{P}^1$ is denoted by $\infty$.

Thus have function field $K(C)/K$ and field extension $K(C)/K(x)$ of degree $n$.

Cover $\mathbb{P}^1$ by two affine open subsets $U_0$, $U_\infty$ isomorphic to $\mathbb{A}^1$ with $\mathcal{O}_{\mathbb{P}^1}(U_0) = K[x]$ and $\mathcal{O}_{\mathbb{P}^1}(U_\infty) = K[1/x]$.

Then $V_0 = \phi^{-1}(U_0)$ and $V_\infty = \phi^{-1}(U_\infty)$ are open affines that cover $C$.

# Representation using orders

Write $R_0 = \mathcal{O}_C(V_0)$ and $R_\infty = \mathcal{O}_C(V_\infty)$.

We know that $R_0$ is finite over $K[x] = \mathcal{O}_{\mathbb{P}^1}(U_0)$ and $R_\infty$ is finite over $K[1/x] = \mathcal{O}_{\mathbb{P}^1}(U_\infty)$.

Thus $R_0$ and $R_\infty$ are $K[x]$- and $K[1/x]$-orders of rank $n$.

We can fix bases of $R_0$ and $R_\infty$ of length $n$ whose relation ideals are generated by quadratic polynomials (and form a Gröbner basis).

These bases are related by a transformation matrix in $K(x)^{n\times n}$, which describes the overlap (glueing) of $V_0$ and $V_\infty$.

Algorithmics of Function Fields

1 Function Fields, Curves, Global Sections



## Definition Via Affine Curve

How do we explicitly define such a $C$ as above?

Start with

- (irreducible) affine algebraic curve $C_0$ over a field $K$,
- a finite map $\alpha_0 : C_0 \to \mathbb{A}^1$.

Then complete and normalise!

Representation of $C_0$:

- Coordinate ring $R_0$ of $C_0$ as quotient of polynomial ring by suitable ideal such that $R_0$ is $K[x]$-order.
- Often $\alpha_i = y^i$ with $f(x, y) = 0$ and $f$ irreducible, monic and of degree $n$ in $y$.

*Example.* $f(x, y) = y^2 - x^7 + 1$.

20 / 44

If we start with $C_0$ only, we may in general construct a finite map $C_0 \to \mathbb{A}^1$ by Noether normalisation.

Algorithmics of Function Fields

1 Function Fields, Curves, Global Sections

Introduction
Function Fields vs. Curves
Function Fields
Curves

Representation and Definition
Representation
Via Affine Curve
Completion
Normalisation
Magma

Global Sections
Outline
Sheaves
Diagonalisation
Global Sections
Grothendiecks Theorem
Riemann-Roch
Special Models
Magma

Exercises

## Completion Step

Complete as follows:

- Divide generators of $R_0$ by suitable powers of $x$ such that they become integral over $K[1/x]$ and hence resulting relations are also defined over $K[1/x]$.
- Results in $K[1/x]$-order $R_\infty$.
- Then have $C_0 = \mathrm{Specm}(R_0)$, $C_\infty = \mathrm{Specm}(R_\infty)$ and $\alpha_0 : C_0 \to \mathbb{A}^1$, $\alpha_\infty : C_\infty \to \mathbb{A}^1$.
- Since $R_0$ is integral over $K[x]$, every zero of $x$ dominates a maximal ideal of $R_0$.
- Since $R_\infty$ is integral over $K[1/x]$, every pole of $x$ dominates a maximal ideal of $R_\infty$.
- This combines (glues) to a complete curve $C_{0,\infty} = C_0 \cup C_\infty$ and morphism $\alpha : C_{0,\infty} \to \mathbb{P}^1$.



It is also possible to complete $C_0$ to a projective curve. This usually gives a different completed curve and a priori more than two affine open subsets.

## Completion Step

*Example.*

- $C_0 : y^2 = x^7 - 1$.
- $y/x^4$ is integral over $\mathbb{Q}[1/x]$: $(y/x^4)^2 = 1/x - (1/x)^8$.
- Thus $R_0 = K[x, y]$, $R_\infty = K[1/x, y/x^4]$, and
- $C_{0,\infty} = \mathrm{Specm}(R_0) \cup \mathrm{Specm}(R_\infty)$.
- Is regular in characteristic $\neq 2, 7$.



In weighted homogenous coordinates we get $C_{0,\infty} : y^2 = zx^7 - z^8$.

In comparison, the projective closure of $C_0$ would be the union of the three affine curves $C_0 = \mathrm{Specm}(K[x, y])$, $C_1 = \mathrm{Specm}(K[1/x, y/x])$ and $C_2 = \mathrm{Specm}(K[1/y, x/y])$. The defining equations for $C_1$ and $C_2$ are here $(1/x)^5(y/x)^2 = 1 - (1/x)^7$ and $(1/y)^5 = (x/y)^7 - (1/y)^7$. The homogenous equation is $C_1 \cup C_2 \cup C_3 : z^5y^2 = x^7 - z^7$.

Since $K[x, y]$ is integral over $K[x]$, $C_0$ is only missing maximal ideals dominated by poles of $x$. But no pole of $x$ dominates a maximal ideal of $C_1$, so $C_1 \subseteq C_0$. The poles of $x$ are precisely the poles of $y$. Every such pole dominates the maximal ideal $\langle 1/y, x/y\rangle$ of $K[1/y, x/y]$. The equation shows that this maximal ideal corresponds to a singular point of $C_2$. So the projective closure of $C_0$ is the union of the two affine curves $C_0$ and $C_2$, where $C_2$ is always singular.

Exercise: Can the equations be modified such that all three of $C_0$, $C_1$ and $C_2$ are necessary for completing $C_0$?

## Normalisation Step

Normalise and hence desingularise $C_{0,\infty}$ as follows:

- Compute $\tilde{R}_0 = \mathrm{Cl}(R_0, K(C_0))$, $\tilde{R}_\infty = \mathrm{Cl}(R_\infty, K(C_0))$.
- The normalisations of $C_0$ and $C_\infty$ are $\tilde{C}_0 = \mathrm{Specm}(\tilde{R}_0)$ and $\tilde{C}_\infty = \mathrm{Specm}(\tilde{R}_\infty)$.
- Define $C = \tilde{C}_0 \cup \tilde{C}_\infty$. This gives the regular complete curve $C$ and the normalisation morphism $\beta : C \to C_{0,\infty}$.
- Composing yields the morphism $\phi = \alpha \circ \beta : C \to \mathbb{P}^1$.

Data to be stored: Defining relations for $R_0$, transformation matrices between bases of $R_0$ and $R_\infty$, between bases of $\tilde{R}_0$ and $R_0$, and between bases of $\tilde{R}_\infty$ and $R_\infty$. These matrices are in $K(x)^{n\times n}$ or even $K[x]^{n\times n}$.

## Normalisation Algorithms

There are various normalisation and desingularisation algorithms. Some require $\alpha$ to be separable, $K$ to be perfect or even $\mathrm{char}(K) = 0$.

Some references:

- Zassenhaus (Round2, Round4)
- Grauert-Remmert (Decker, ...)
- van Hoeij
- Montes-Nart
- Chistov: Polynomial time equivalent to factoring discriminant of $f$.

Recent activity:

- J. Bauch: Computation of Integral Bases, 2015.
- Singular Group at Kaiserslautern, 2015.
- What is when the fastest method?

Algorithmics of Function Fields

1 Function Fields, Curves, Global Sections



## Magma

Let $\infty$ denote the pole of $x$ in $\mathbb{P}^1$ and $\mathcal{O}_\infty$ the local ring of $\infty$.

In Magma and its function field package,

- $R_0$ and $R_\infty \mathcal{O}_\infty$ are called finite and infinite (equation) orders, $\tilde{R}_0$ and $\tilde{R}_\infty \mathcal{O}_\infty$ are called finite and infinite maximal orders.
- Places are uniquely represented as maximal ideals in the maximal orders, by explicit generators.
- The poles of $x$ are called places at infinity.
- A host of algorithms from algebraic number theory is quasi readily available, e.g. integral closures, valuations, residue class fields.

These objects are more considered of internal type. One can work with places rather like in Stichtenoth, without knowing those background details.

There is a curve data type in Magma, but it is different from (although equivalent to) that presented here.

25 / 44

One convenient reason for using $\tilde{R}_\infty \mathcal{O}_\infty$ instead of $\tilde{R}_\infty$ is that $\mathrm{Specm}(\tilde{R}_0)$ and $\mathrm{Specm}(\tilde{R}_\infty \mathcal{O}_\infty)$ are disjoint, whereas $\mathrm{Specm}(\tilde{R}_0)$ and $\mathrm{Specm}(\tilde{R}_\infty)$ are not disjoint. The representation of a place as a maximal ideal is thus unique.

# Global Sections,
# Riemann-Roch and an Application

# Outline

Start with function field $F/K$ and divisor $D$ of $F/K$.

Compute the $K$-vector space

$$L(D) = \{f \in F^\times \,|\, \mathrm{div}(f) \geq -D\} \cup \{0\}$$

of global sections of $D$!

Approaches are based on:

- Curves and Brill-Noether method of adjoints
- Integral closures and series expansions
- Sheaves and Grothendiecks theorem

Recent activity:

- J. Bauch: Lattices over Polynomial Rings and Applications to Function Fields, 2014.
- I. Stenger: Computing Riemann-Roch Spaces - a geometric approach, 2014.

## Sheaves

Let $C$ be a curve over $K$ with function field $F$.

Let $M$ an $F$-vector space and $\mathcal{F}_P$ submodules of the $\mathcal{O}_{C,P}$-modules $M$ such that $F\mathcal{F}_p = M$ for all $P \in C$ and each $f \in M$ is contained in almost all $\mathcal{F}_P$. Define

$$\mathcal{F}(U) = \cap_{P \in U} \mathcal{F}_P,$$

where the empty intersection is defined as $M$.

Each $\mathcal{F}(U)$ is a torsion-free $\mathcal{O}_C(U)$-module and $\mathcal{F}$ is called a sheaf of locally torsion-free $\mathcal{O}_C$-modules.

The elements of $\mathcal{F}(U)$ are called sections over $U$, and global sections when $U = C$.

*Example.* $\mathcal{O}_C$ is such a sheaf, or better a sheaf of rings, and is called structure sheaf of $C$.



In addition, the modules $\mathcal{F}_P$ are called stalks of $\mathcal{F}$ at $P$ and their elements germs.

Algorithmics of Function Fields
1 Function Fields, Curves, Global Sections
Introduction
Function Fields vs. Curves
Function Fields
Curves
Representation and Definition
Representation
Via Affine Curve
Completion
Normalisation
Magma
Global Sections
Outline
Sheaves
Diagonalisation
Global Sections
Grothendiecks Theorem
Riemann-Roch
Special Models
Magma
Exercises

## Sheaves

*Theorem.* Let $\mathcal{F}$ be a sheaf of locally torsion-free $\mathcal{O}_C$-modules.

1. We have
$$\mathcal{F}(U) \subseteq \mathcal{F}(V) \quad \text{and} \quad \mathcal{F}(U) = \cap_{i \in I} \mathcal{F}(U_i)$$
for $V \subseteq U$ and for any family $(U_i)_{i \in I}$ with $U = \cup_{i \in I} U_i$.
2. For all $U \subseteq C$ affine, $P \in U$ and $\mathfrak{m}$ the corresponding maximal ideal of $\mathcal{O}_C(U)$,
$$\mathcal{F}(U)_\mathfrak{m} = \mathcal{F}_P.$$
3. For all $U \subseteq C$ affine and $f \in \mathcal{O}_C(U)$,
$$\mathcal{F}(D_U(f)) = \mathcal{F}(U)[f^{-1}].$$



If $R$ is a subring of $F/K$, $A$ an $R$-submodule in the $F$-vector space $M$ and $U \subseteq R$ with $0 \notin U$, we write $A[U^{-1}] = R[U^{-1}] \cdot A$ for the $R[U^{-1}]$-submodule of $M$ generated by $A$. If $\mathfrak{m}$ is a maximal ideal of $R$ we write $A_\mathfrak{m} = A[(R \backslash \mathfrak{m})^{-1}]$. If $R$ is local then $A_\mathfrak{m} = A$.

*Proof of Theorem of Slide.* 1.: This is immediate from the definitions.

2.: It is clear that $\mathcal{F}(U)_\mathfrak{m} \subseteq \mathcal{F}_P$ because $\mathcal{O}_C(U)_\mathfrak{m} \subseteq \mathcal{O}_P$. Let $x \in \mathcal{F}_P$. Then $x \in \mathcal{F}_Q$ for almost all $Q \in U$. Write $P_i$ for those finitely many points of $U$ where $P_i$ ist not regular or $x \notin \mathcal{F}_{P_i}$. There are $d_i \in \mathcal{O}_{C,P_i}$ non-zero with $d_i x \in \mathcal{F}_{P_i}$. By Theorem 1.9.2 here is $d \in \mathcal{O}_C(U) \backslash \mathfrak{m}$ and $dx \in \mathcal{F}(U)$. Then $x = (dx)/d \in \mathcal{F}(U)_\mathfrak{m}$.

3.: We have $f \in \mathcal{O}_C(D_U(f))^\times$, so $\mathcal{O}_C(D_U(f))[f^{-1}] = \mathcal{O}_C(D_U(f))$ and
$$\mathcal{F}(D_U(f))[f^{-1}] = \mathcal{O}_C(D_U(f))[f^{-1}]\mathcal{F}(D_U(f)) = \mathcal{F}(D_U(f)).$$
On the other hand, if $f \in \mathfrak{m}_P$ then
$$\mathcal{F}_P[f^{-1}] = \mathcal{O}_{C,P}[f^{-1}]\mathcal{F}_P = F\mathcal{F}_P = M.$$
The following Lemma 1.29.1 shows
$$\mathcal{F}(U)[f^{-1}] = \mathcal{F}(D_U(f))[f^{-1}] \cap (\cap_{P \in U, f \in \mathfrak{m}_P} \mathcal{F}_P[f^{-1}]) = \mathcal{F}(D_U(f)),$$
as was to be proven. □

**Lemma 1.29.1.** *Suppose $R$ and $S$ are subrings of a field $F$ and let $U \subseteq R \cap S$ be multiplicatively closed with $1 \in U$. Let $M$ be an $R$-submodule and $N$ an $S$-submodule inside a joint $F$-vector space. Then*
$$M[U^{-1}] \cap N[U^{-1}] = (M \cap N)[U^{-1}].$$

*Proof.* Since $M \cap N \subseteq M$ and $M \cap N \subseteq N$ we have $(M \cap N)[U^{-1}] \subseteq M[U^{-1}]$ and $(M \cap N)[U^{-1}] \subseteq N[U^{-1}]$, so $(M \cap N)[U^{-1}] \subseteq M[U^{-1}] \cap N[U^{-1}]$.

Let $x \in M[U^{-1}] \cap N[U^{-1}]$. Then there are $r \in M$, $s \in N$ and $u, v \in U$ such that

$$x = \frac{r}{u} = \frac{s}{v} = \frac{rv}{uv} = \frac{us}{uv}$$

with $rv \in M$, $us \in N$ and $uv \in U$. Since $M$ is an $F$-vector space, we conclude $rv = us$, so $rv = us \in M \cap N$ and $x \in (M \cap N)[U^{-1}]$. $\square$

The theorem shows that $\mathcal{F}$ is quasi-coherent. The converse would also be true.

## Sheaves

A sheaf $\mathcal{F}$ of locally torsion-free $\mathcal{O}_C$-modules is said to be locally finitely generated if all $\mathcal{F}_P$ are finitely generated and if each basis of $M$ is also a basis of $\mathcal{F}_P$ for almost all $P \in C$.

*Theorem.* Let $\mathcal{F}$ be a sheaf of locally torsion-free and finitely generated $\mathcal{O}_C$-modules. Then each $\mathcal{F}(U)$ for $U$ affine is finitely generated.

*Example.* The structure sheaf $\mathcal{O}_C$ is locally torsion-free and finitely generated.



*Proof of Theorem of Slide.* Let $x_1, \dots, x_n$ be an $F$-basis of $M$. Then $x_1, \dots, x_n \in \mathcal{F}_P$ for almost all $P \in U$. By Theorem 1.9.2 there is $d \in \mathcal{O}_C(U)$ non-zero such that $dx_1, \dots, dx_n \in \mathcal{F}(U)$. By assumption, the $dx_1, \dots, dx_n$ are a basis of $\mathcal{F}_P$ for almost all $P \in U$. Denote by $P_1, \dots, P_s$ the missing points in $U$. Each $\mathcal{F}_{P_i}$ is finitely generated, so by Theorem 1.9.2 there is $d_i \in \mathcal{O}_{C,P_i}^\times$ such that the product of the generators of $\mathcal{F}_{P_i}$ and $d_i$ gives generators of $\mathcal{F}_{P_i}$ which are elements of $\mathcal{F}(U)$. Putting all those generators together yields finitely many elements of $\mathcal{F}(U)$ which generate $\mathcal{F}_P$ for all $P \in U$.

Let $N$ be the submodule of $\mathcal{F}(U)$ generated by these finitely many elements. Then

$$N_{\mathfrak{m}_P} = \mathcal{F}_P = \mathcal{F}(U)_{\mathfrak{m}_P},$$

and the $\mathfrak{m}_P$ run through all maximal ideals of $\mathcal{O}_C(U)$. This shows $N = \mathcal{F}(U)$ and hence $\mathcal{F}(U)$ is finitely generated. $\square$

The theorem shows that if $\mathcal{F}$ is locally torsion-free and finitely generated then $\mathcal{F}$ is coherent. The converse is also true here.

## Sheaf of a divisor

Let $C$ denote a regular complete curve with function field $F$ and $D$ a divisor of $C$ resp. $F/K$.

The sheaf $\mathcal{O}_C(D)$ associated to $D$ is defined by

$$\mathcal{O}_C(D)(U) = \{f \in F^\times \mid v_P(f) \geq v_P(-D) \text{ for all } P \in U\} \cup \{0\}.$$

It is a locally torsion-free and finitely generated sheaf of $\mathcal{O}_C$-modules with

$$L(D) = \mathcal{O}_C(D)(C).$$

In other words, the $\mathcal{O}_C(D)(U)$ are non-zero fractional ideals of the Dedekind domains $\mathcal{O}_C(U)$.



Since $\mathcal{O}_{C,P}$ is a discrete valuation ring and hence a principal ideal domain, the $\mathcal{O}_C(D)_P$ are each generated by one element, namely $\pi_P^{-v_P(D)}$ where $\pi_P$ is a generator of $\mathfrak{m}_P$, hence are finitely generated. Moreover, $\mathcal{O}_C(D)_P = \mathcal{O}_{C,P}$ for almost all $P \in C$ and if $x \in F^\times$ then $x \in \mathcal{O}_{C,P}^\times$ for almost all $P \in C$. Thus $x$ is a basis of $\mathcal{O}_C(D)_P$ for almost all $P \in C$ and the conditions are met.

## Representation using two free modules

Since $V_0$ and $V_\infty$ are an open affine cover of $C$, the sheaf $\mathcal{F}$ can be represented by the torsion-free finitely generated modules $\mathcal{F}(V_0)$ of $R_0$ and $\mathcal{F}(V_\infty)$ of $R_\infty$ and

$$\mathcal{F}(C) = \mathcal{F}(V_0) \cap \mathcal{F}(V_\infty).$$

The modules $\mathcal{F}(V_0)$ and $\mathcal{F}(V_\infty)$ are also torsion-free and finitely generated $K[x]$- and $K[1/x]$-modules and thus are free of rank $n \dim_F(M)$ inside the $K(x)$-vector space $M$ of dimension $n \dim_F(M)$. They can thus be explicity described by their bases.

To compute the intersection we need to find all $f \in M$ which can be written as a $K[x]$-linear combination of the basis of $\mathcal{F}(V_0)$ and as a $K[1/x]$-linear combination of the basis of $\mathcal{F}(V_\infty)$ *simultaneously*.

## Diagonalisation

The key proposition is as follows:

*Proposition.* Let $A \in \mathrm{GL}(n, K[x, 1/x])$. Then there are $S \in \mathrm{GL}(n, K[x])$ and $T \in \mathrm{GL}(n, K[1/x])$ such that

$$TAS = (x^{d_i}\delta_{i,j})_{i,j}$$

with $d_1 \geq \cdots \geq d_n$ uniquely determined.

The proof essentially uses

- matrix reduction (Dedekind-Weber, weak Popov form, lattice reduction in function fields),
- or Birkhoff's matrix decomposition.

Thus need to find $\lambda \in K[x]$ such that $x^{-d}\lambda \in K[1/x]$. These are precisely the $\lambda \in K[x]$ with $\deg(\lambda) \leq d$.



For a proof and references see F. Hess, “Computing Riemann-Roch spaces in algebraic function fields and related topics”, J. Symbolic Comp. 33(4): 425-445, 2002.

The proposition appears in Birkhoff apparently in

Birkhoff, G.: A theorem on matrices of analytic functions. Math. Ann., 74, no. 1, 122133 (1913)

Birkhoff, George David (1909), “Singular points of ordinary linear differential equations”, Transactions of the American Mathematical Society 10 (4): 436470,

G. D. Birkhoff, The generalized Riemann problem for linear differential equations and the allied problems for linear difference and q-difference equations, Proc. Amer. Acad. Arts and Sci. 49 (1913), 531-568.

Further references

`https://www.encyclopediaofmath.org/index.php/Birkhoff_factorization`

## Global Sections

Denote by $\mathcal{F}(r)$ the sheaf defined by

$$\mathcal{F}(r)(V_0) = \mathcal{F}(V_0) \text{ and } \mathcal{F}(r)(V_\infty \backslash V_0) = x^r \cdot \mathcal{F}(V_\infty \backslash V_0).$$

*Theorem.* Recall $n = [K(C) : K(x)]$. There exist $K(x)$-linearly independent $f_1, \ldots, f_n \in M$ and uniquely determined $d_1 \geq \cdots \geq d_n$ such that for all $r$:

$$\mathcal{F}(r)(C) = \left\{ \sum_{i=1}^{n} \lambda_i f_i \mid \lambda_i \in K[x] \text{ and } \deg(\lambda_i) \leq d_i + r \right\}.$$

Moreover,

- the $f_1, \ldots, f_n$ are a $K[x]$-basis of $\mathcal{F}(V_0)$ and
- the $x^{d_1} f_1, \ldots, x^{d_n} f_n$ are a $K[1/x]$-basis of $\mathcal{F}(V_\infty)$.

These bases are called reduced.



For the proof with $\mathcal{F} = \mathcal{O}_C(D)$ see F. Hess, "Computing Riemann-Roch spaces in algebraic function fields and related topics", J. Symbolic Comp. 33(4): 425-445, 2002. The case of general $C$ and $\mathcal{F}$ is analogous, or see Grothedieck's theorem.

This shows by the way that the $K$-vector space $\mathcal{F}(C)$ has finite dimension if (and only if) the curve $C$ is complete.

All constituents of the theorem can be computed by Magma, see Magma's intrinsic `ShortBasis`.

## Push Forward of a Sheaf*

Let $\phi : X \to Y$ be a morphism of the curves $X$ and $Y$, and $\mathcal{F}$ a locally torsion-free sheaf of $\mathcal{O}_X$-modules.

We define the push forward $\phi_*(\mathcal{F})$ of $\mathcal{F}$ along $\phi$ via

$$\phi_*(\mathcal{F})(U) = \mathcal{F}(\phi^{-1}(U))$$

for any $U \subseteq Y$.

*Theorem.* Then $\phi_*(\mathcal{F})$ is a locally torsion-free sheaf of $\mathcal{O}_Y$-modules. If $X$ is complete and $\mathcal{F}$ is finitely generated, then $\phi_*(\mathcal{F})$ is also finitely generated.



*Proof.* We have seen that if $X$ is complete then $Y$ is complete and $\mathcal{O}_X(\phi^{-1}(U))$ is finite over $\mathcal{O}_Y(U)$. Since $\mathcal{F}(\phi^{-1}(U))$ is finite over $\mathcal{O}_X(\phi^{-1}(U))$, we thus see that $\mathcal{F}(\phi^{-1}(U))$ is also finite over $\mathcal{O}_Y(U)$. $\square$

## Isomorphisms of Sheaves*

Let $\mathcal{F}$ and $\mathcal{G}$ be sheaves of $\mathcal{O}_C$-modules inside the $F$-vector spaces $M$ and $N$ respectively.

A morphism $f : \mathcal{F} \to \mathcal{G}$ is given by an $F$-linear map $M \to N$ that restricts to $\mathcal{O}_{X,P}$-module homomorphisms

$$f_P : \mathcal{F}_P \to \mathcal{G}_P.$$

It then also restricts to $\mathcal{O}_X(U)$-module homomorphisms

$$f(U) : \mathcal{F}(U) \to \mathcal{G}(U).$$

We say $f$ is an isomorphism if all $f_P$ are isomorphisms. Then all $f(U)$ are also isomorphisms.

# Direct Sum of Sheaves*

Let $\mathcal{F}$ and $\mathcal{G}$ be sheaves of $\mathcal{O}_C$-modules inside the $F$-vector spaces $M$ and $N$ respectively.

We define $\mathcal{F} \oplus \mathcal{G}$ as the sheaf of $\mathcal{O}_C$-modules inside $M \oplus N$ defined by

$$(\mathcal{F} \oplus \mathcal{G})_P = \mathcal{F}_P \oplus \mathcal{G}_P$$

for all $P \in C$. Then also

$$(\mathcal{F} \oplus \mathcal{G})(U) = \mathcal{F}(U) \oplus \mathcal{G}(U)$$

for all $U \subseteq C$.

If $\mathcal{F}$ and $\mathcal{G}$ are locally torsion-free then $\mathcal{F} \oplus \mathcal{G}$ is locally torsion-free. If in addition $\mathcal{F}$ and $\mathcal{G}$ are locally finitely generated then $\mathcal{F} \oplus \mathcal{G}$ is locally finitely generated.

## Grothendiecks Theorem*

Let $C$ be complete and $\phi : C \to \mathbb{P}^1$ a morphism of degree $n$. Let $\mathcal{F}$ be a locally torsion-free and finitely generated sheaf of $\mathcal{O}_C$-modules.

*Grothendieck's Theorem*:

$$\phi_*(\mathcal{F}) \cong \mathcal{O}_{\mathbb{P}^1}(d_1\infty) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(d_n\infty)$$

with $d_1 \geq \cdots \geq d_n$ uniquely determined.

We have indeed computed $\mathcal{F}(C)$ via

$$\begin{aligned}\mathcal{F}(C) &= \phi_*(\mathcal{F})(\mathbb{P}^1)\\ &\cong \mathcal{O}_{\mathbb{P}^1}(d_1\infty)(\mathbb{P}^1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(d_n\infty)(\mathbb{P}^1)\ !\end{aligned}$$



The direct sum decomposition is given by the reduced basis $f_1, \ldots, f_n$, and

$$\mathcal{O}_{\mathbb{P}^1}(d_i\infty)(\mathbb{P}^1) \cong \{\lambda \in K[x] \mid \deg(\lambda) \leq d_i\}.$$

As we can see, the diagonalisation proposition is in fact the key observation in Grothendiecks theorem.

For a reference see A. Grothendieck, “Sur la classification des fibrés holomorphes sur la sphère de Riemann”, Amer. J. Math., 79 (1957) pp. 121-138.

## Relation to Riemann-Roch

$\mathcal{O}_C(C)$ is the algebraic closure of $K$ in $C$. Suppose $K = \mathcal{O}_C(C)$ and let $g$ denote the genus of $C$.

Let $\mathcal{F} = \mathcal{O}_C(D)$. The numbers $d_i$ satisfy

- $d_1 \geq \cdots \geq d_n$.
- $\sum_{i=1}^n d_i = \deg(D) + 1 - g - n$
- $L(D) \neq 0$ iff $d_1 \geq 0$.
- $\deg(D) \geq d_1 \gtrsim (\deg(D) - g)/n$,
- $D$ non-special implies $d_n \geq 0$.
- $d_n \gtrsim (\deg(D) - 2g)/n$.
- $d_1 - d_n \lesssim 2g/n$.
- $\mathcal{O}_C(C) = L(0)$.

The $d_1, \ldots, d_n$ are thus balanced.
If $D = 0$ then $g$ can be computed from $d_1, \ldots, d_n$.



*Proof.* From $\dim(D) \leq \deg(D) + 1$ we obtain $d_1 \leq \deg(D)$.

Choose $s$ such that $\deg(E) < 0$ for $E = D - s\mathrm{div}(x)_\infty$. The invariants of $E$ are $e_i = d_i - s$. Then $e_i < 0$ for all $i$. Choose $r$ minimal such that $\dim(E + r\mathrm{div}(x)_\infty) > 0$. Then $\deg(E) + rn < g + n$ and $e_1 + r \geq 0$. Thus $\deg(D) - sn + rn < g + n$ and $d_1 - s + r \geq 0$. Then $d_1 \geq s - r$ and $\deg(D) - (s - r)n < g + n$. So $s - r > (\deg(D) - g - n)/n$ and $d_1 > (\deg(D) - g - n)/n$.

Similarly for $d_n$ with $g$ replaced by $2g - 1$, so $d_n \gtrsim (\deg(D) - 2g)/n$.

Combination of the previous two statements yields $d_1 - d_n \lesssim 2g/n$.

For the last statement see my RR paper. $\square$

# Application: Special Models

When applied to $\mathcal{I} = \mathcal{O}_C$ the theorem yields

- a specific representation of $C$ and
- also gives an embedding of $C$ in a weighted $n$-dimensional projective space, depending on $\phi$.
- The weights are given by the $-d_i$.

*Example.* $C : y^2 = zx^7 - z^8$ over $\mathbb{Q}$ where $w(x) = w(z) = 1$ and $w(y) = 4$, is regular.

The affine ring $R_0$ of $C$ is generated by $x$ and $n$ additional variables. Relations are at most quadratic in these variables and of degree $O(g/n)$ in $x$.

## Gonality

In practice rather sensitive to $n$.

Thus

- minimize $n$, find $\phi$ of lowest degree. But in general $n = \Theta(g)$.
- substitute variables by powers of others, if possible.

Recent activity:

J. Schicho and D. Sevilla: Effective radical parametrization of trigonal curves, 2011.

M. C. Harrison: Explicit solution by radicals, gonal maps and plane models of algebraic curves of genus 5 or 6, 2013.

## Magma and other Implementations

Probably not exhaustive ...

Global sections:

- via Grothendiecks theorem: Magma
- via saturation of homogenous ideals: Magma, MacCaulay2, Singular.

Maps of minimal degree:

- via Schicho and Sevilla: Magma
- via Harrison: Magma

# Excercises

1. Compute a complete regular curve $C$ in the sense of these slides with function field $\mathbb{Q}(x, y)$, where $y^7 - y^2 = x^2$, and show by the approach presented here that the genus of $C$ is 2.

2. Suppose $C$ is a regular curve and let $U \subseteq C$ be finite. Show that $\mathcal{O}_C(U)$ is a principal ideal domain.

3. Suppose $C$ is a regular curve and let $U \subseteq C$ be affine. Show that every fractional ideal of $\mathcal{O}_C(U)$ can be generated by two elements of $K(C)$.

4. Find a complete curve $C$ over $K$ where $\mathcal{O}_C(C) \neq K$. Verify the latter using Magma.

5. Find a curve $C$ over some $K$ such that there is no separable morphism $C \to \mathbb{P}^1$.

6. Provide examples that in the relation of domination the cases $\mathcal{O}_P^\times \subsetneq \mathcal{O}_Q^\times$ and $\mathfrak{m}_P = \mathfrak{m}_Q$ as well as $\mathcal{O}_P^\times = \mathcal{O}_Q^\times$ and $\mathfrak{m}_P \subsetneq \mathfrak{m}_Q$ can indeed occur.

## Excercises*

For the following excercises let $C$ be a complete curve over $K$.

7. Show that there is a morphism $C \to \mathbb{P}^1$ and a non-zero $K(\mathbb{P}^1)$-linear map $K(C) \to K(\mathbb{P}^1)$.

8. Show that for every sheaf $\mathcal{F}$ of locally torsion-free and finitely generated $\mathcal{O}_C$-modules there is a sheaf $\mathcal{F}^\#$ of locally torsion-free and finitely generated $\mathcal{O}_C$-modules such that if $\phi_*(\mathcal{F}) \cong \oplus_i \mathcal{O}_{\mathbb{P}^1}(d_i)$ then $\phi_*(\mathcal{F}^\#) \cong \oplus_i \mathcal{O}_{\mathbb{P}^1}(-d_i)$.

9. In the situation of excerise 8 show there is a sheaf $\mathcal{F}^*$ of locally torsion-free and finitely generated $\mathcal{O}_C$-modules such that $\phi_*(\mathcal{F}^*) \cong \oplus_i \mathcal{O}_{\mathbb{P}^1}(-d_i - 2)$.

10. Adapt matters if necessary and define a degree $\deg(\mathcal{F})$ of locally torsion-free and finitely generated $\mathcal{O}_C$-modules such that

$$\dim_K(\mathcal{F}(C)) - \dim_K(\mathcal{F}^*(C)) = \deg(\mathcal{F}) + c,$$

where $c$ depends only on $C$ and $\dim_{K(C)} \mathcal{F}(\emptyset)$.



Hint for 10.: Express those quantities for $\mathcal{F}$ in terms of the $d_i$ and compare.

Lecture 2

# Algorithmic Number Theory for Function Fields

Summer School UNCG 2016

Florian Hess

# Class Groups

## First Part

## Notation

Consider complete regular curves $C$ over a field $K$. We can then equivalently work with $F = K(C)$ only.

Notation:

- Group of divisors $\mathrm{Div}(F/K)$.
- Subset of divisors of degree $d$: $\mathrm{Div}^d(F/K)$.
- Subgroup of principal divisors of $\mathrm{Princ}(F/K)$.
- Class group or Picard group: $\mathrm{Pic}(F/K)$.
- Subgroup of class of degree $d$: $\mathrm{Pic}^d(F/K)$.

By definition,

$$\mathrm{Pic}(F/K) = \mathrm{Div}(F/K)/\mathrm{Princ}(F/K),$$
$$\mathrm{Pic}^0(F/K) = \mathrm{Div}^0(F/K)/\mathrm{Princ}(F/K).$$



Since $K$ is assumed to be the exact constant field of $F$, $C$ is geometrically irreducible.

Algorithmics of Function Fields

2 Number Theory



## Some Facts

We have

$$\mathrm{Pic}(F/K) = \mathrm{Pic}^0(F/K) \oplus \langle A \rangle,$$

where $A$ is a divisor of $F/K$ with minimal positive degree.

If $K$ is a finite field are algebraically closed then $\deg(A) = 1$. In the latter case $A$ can be chosen to be a prime divisor.

If $K$ is finitely generated over its prime field then $\mathrm{Pic}^0(F/K)$ is finitely generated.

If $K$ is a finite field then $\mathrm{Pic}^0(F/K)$ is finite. Then usually

$$\#\mathrm{Pic}^0(F/K) \approx (\#K)^g.$$

4 / 40

The “finitely generated” statement is the theorem of Lang-Néron. The “finite” statement is classic, see for example the book of Stichtenoth.

## Computing in the Class Group

Representation of divisors:

- Divisors can be represented as a sum of places with integral coefficients, or as a pair of fractional ideals.
- Addition of divisors either by addition of coefficient vectors or multiplication of ideals.
- Equality by coefficientwise comparison or comparison of Hermite normal forms.

Representation of divisor classes:

- By divisors, which can be "suitably" chosen, for example reduced divisors.
- Comparison via unique divisor class representatives, if they can be computed, or by the test

$$\deg(D) = \deg(E) \text{ and } L(D - E) \neq 0.$$

- This is usally efficient (polynomial time) in terms of operations in $K$.



An efficient algorithm (in theory) is an algorithm that has an (expected) runtime that depends polynomially on the length of the input. If the runtime is measured in operations in $K$ then the length of the input is measured in elements of $K$.

An efficient algorithm in practice is one that works well in implementations. Those both notions need not really coincide.

If $K$ is an infinite field, and worsely not algebraic over a finite field, then the required operations in $K$ often or usually involve elements with large bit length and become prohibitive very quickly, see "coefficient explosion".

## Computing in the Class Group

Reduction of divisors:

- Fix a divisor $A$ of positive degree.
- For every $D$ there is $\tilde{D} \geq 0$ and $f \in F^\times$ such that

$$D = \tilde{D} - rA + \mathrm{div}(f)$$

  and $\deg(\tilde{D}) \leq g + \deg(A) - 1$.
- If $A$ is a prime divisor of degree one and $r$ is minimal then $\tilde{D}$ is uniquely determined.

Class representatives:

- Thus $[D] = [\tilde{D} - rA]$ for every divisor class.
- If $A$ is a prime divisor of degree one then $\tilde{D} - rA$ can be uniquely chosen.



The $\tilde{D}$ is constructed as follows: Choose $r \in \mathbb{Z}$ minimal such that $L(D+rA) \neq 0$. Then for any $f \in L(D+rA)$ we have $D+rA+\mathrm{div}(f) \geq 0$. So we define $\tilde{D} = D+rA+\mathrm{div}(f)$. Replacing $f$ by a non-zero scalar multiple does not change $\tilde{D}$. This shows that $\tilde{D}$ is uniquely determined if $\dim_K(L(D+rA)) = 1$. Otherwise, $\tilde{D}$ is not uniquely determined.

By the Riemann-Roch theorem, $\deg(D+rA) \leq g + \deg(A) - 1$, hence $\tilde{D} = \deg(D + rA) + \mathrm{div}(f)) = \deg(D+rA) \leq g + \deg(A) - 1$.

If $A$ is a prime divisor of degree one then we can always achieve $\dim_K(L(D+rA)) = 1$ by the theorem of Riemann-Roch, so $\tilde{D}$ is uniquely determined.

## Computing in the Class Group

Reduction of divisors:

- The reduced divisor $\tilde{D}$ can be computed by an iterative double-and-add method such that the runtime is polynomial in $g$, $\deg(A)$ and the length of $D$.
- Moreover, $f$ is computed as a product of powers of elements of $F$ and has length polynomial in $g$, $\deg(A)$ and the length of $D$.



An analogous case is computing $\prod_i a_i^{\lambda_i}$ in $\mathbb{Z}/n\mathbb{Z}$. Using the double-and-square strategy combined with intermediate reductions modulo $n$ allows us to compute the product very efficiency, even for large $\lambda_i$.

For a reference see my RR paper.

# Computing in the Class Group

These ideas can be optimised, for example by precomputations, and worked out in great detail.

A (biased) selection of results:

- Cantor: If $F/K$ is hyperelliptic then operations in $\mathrm{Pic}^0(F/K)$ can be reduced to fast polynomial arithmetic in degree $O(g)$, so the runtime is $O^\sim(g)$.
- Makdisi: If $F/K$ is arbitrary then operations in $\mathrm{Pic}^0(F/K)$ can be reduced to fast matrix arithmetic in dimension $O(g)$, so the runtime is $O^\sim(g^\omega)$.
- Hess-Junge: If $F/K$ has a rational subfield of index $n$, where $n = O(g)$ is always possible, then operations in $\mathrm{Pic}^0(F/K)$ can be reduced to fast polynomial matrix arithmetic in dimension $O(n)$ and degree $O(g/n)$, so the runtime is $O^\sim(n^\omega(g/n))$.

## Computing the Class Group

We assume that $K$ is finite! Write $q = \#K$.

Have $\mathrm{Pic}^0(F/K) \cong \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_{2g}\mathbb{Z}$. with $c_i | c_{i+1}$.

Goal:

- Compute the $c_i$.
- Compute images and preimages under a fixed isomorphism

$$\phi : \mathrm{Pic}(F/K) \to \mathbb{Z} \oplus \mathbb{Z}/c_1\mathbb{Z} \times \cdots \times \mathbb{Z}/c_{2g}\mathbb{Z}.$$

Denote by $A$ a fixed divisor of degree one that maps under $\phi$ to the first cyclic factor of the codomain of $\phi$.

## Computing the Class Group

Algorithms that work for any finite abelian group $G$:

- Classic runtime $O((\#G)^{1/2})$.
- Improvements often lead to $O((\#G)^{1/3})$.
- So here roughly $O^\sim(q^{g/2})$ or $O^\sim(q^{g/3})$.

Algorithms that use $G = \mathrm{Pic}^0(F/K)$ usually employ an index calculus strategy:

- If $q$ is small and $g$ is large, the (heuristic) runtime is $q^{(c+o(1))g^{1/2}\log(g)^{1/2}}$, and $q^{(d+o(1))g^{1/3}\log(g)^{2/3}}$ (†) in special families.
- If $q$ is large and $g \geq 2$ fixed, then $O^\sim(q^{2-2/g})$ (†).

(†): This is for discrete logarithms, so restrictions may apply.



Some references for the generic algorithms are Shanks Baby-Step-Giant-Step, Pollard methods and the thesis of Sutherland.

Some references for the index calculus methods are Adleman-Huang, Diem, Enge et. al., Hess, Jacobson, Stein.

(†) : The cases with $q^{(1+o(1))g^{1/3}}$ and $O^\sim(q^{2-2/g})$ are actually for discrete logarithm computations. I think, but am not fully sure, that the runtime also applies to class group computations.

Thus in cryptography one usually takes $q$ large and $g = 1$.

# Index Calculus

Setup:

- Let $S$ denote the set of places of $F/K$ of degree $\leq r$, called factor basis.
- Let $[D_1], \ldots, [D_s]$ denote generators of $\mathrm{Pic}^0/F/K)$.

Relation search:

- Choose random $\lambda_i$ and compute $[\tilde{D} - lA] = \sum_i \lambda_i [D_i]$ with $\tilde{D}$ reduced.
- Factor $\tilde{D}$ over $S$, if possible and obtain

$$\sum_i \lambda_i [D_i] = [\tilde{D} - lA] = -l[A] + \sum_{P \in S} n_P [P].$$

- Store $\lambda_i$ and $n_P$ as rows of a matrix and repeat.

## Index Calculus

Linear algebra:

- If matrix has full rank and sufficiently more rows than columns use a Hermite normal form computation to derive relations between the generators $[D_i]$.
- Use a Smith normal form computation to derive $c_1, \ldots, c_{2g}$ from those relations.

Why does it work?

- There is a good upper bound $d$ on the degrees of the places in the $D_i$.
- The class number can be efficiently approximated and checked against the computed $c_1, \ldots, c_{2g}$.
- There is a reasonable choice of $r$ and a good (heuristic) probability that enough relations are obtained.

Algorithmics of Function Fields

2 Number Theory

Class Groups
Mathematical Background
Computing in the Class Group
Computing the Class Group
Applications

Class Fields
Mathematical Background
Computing Ray Class Groups
Computing Class Fields
Applications

Zeta functions and L-series
Mathematical Background
Computing L-series
Applications

Exercises

## Index Calculus

Let $N_m$ denote the number of places of degree one in the constant field extension of $F$ of degree $m$.

*Theorem.* Suppose $N_d > (g-1)2q^{d/2}$. Then $\mathrm{Pic}(F/K)$ is generated by $A$ and the divisors $D = P - \deg(P)A$, where $P$ ranges through the places of degree less than or equal to $d$.

*Theorem.* Let $h = \#\mathrm{Pic}^0(F/K)$. Then

$$\left|\log\left(\frac{h}{q^g}\right) - \sum_{m=1}^{t} \frac{q^{-m}}{m}(N_m - q^m - 1)\right| \leq \frac{2g}{q^{1/2}-1} \cdot \frac{q^{-t/2}}{t+1}.$$

Since $c_1 \dots c_{2g}$ is an integral multiple of $h$ an approximation of $\log(h/q^g)$ up to an error of $\log(2)/3$ is sufficient.

The total number of places to be considered is $O(g^2)$.

13 / 40

The statements about the probability of obtaining enough relations is rather messy, so we omit those.

## Some Applications

From the relations of the $[D_i]$ it is easy to compute generators of $\mathrm{Pic}^0(F/K)$ corresponding to the cyclic generators of the codomain of $\phi$. We can thus also compute preimages under $\phi$ efficiently.

Images $\phi([D])$ are computed by adding $[D - \deg(D)A]$ to the $[D_i]$ and searching for relations. The runtime is then basically the same like that for computing the $c_1, \ldots, c_{2g}$.

This can directly be used to compute for an arbitrary $S$

- $S$-units $U(S) = \{f \in F^\times \mid \mathrm{supp}(\mathrm{div}(f)) \subseteq S\}$ and
- $S$-class groups $\mathrm{Div}(F/K)/(\langle S \rangle + \mathrm{Princ}(F/K))$.



The computation of $S$-units and $S$-class groups requires the evaluation of the map $\phi$ at the places in $S$, easy manipulations of finitely generated abelian groups and $L(D)$ computations for $D$ a principal divisor.

Note $U(S) \cong \mathbb{Z}^{\#S-1}$, so $U(S)$ is computed by giving a basis in $F^\times$. The basis elements can be efficiently represented as product of powers of small elements, by the divisor reduction: Observe that if $D$ is a principal divisor, then $\tilde{D} = 0$ and $r = 0$.

Note that $\mathcal{O}_S = \cap_{P \notin S} \mathcal{O}_P$ is a Dedekind domain with unit group $\mathcal{O}_S^\times = U(S)$ and ideal class group $\mathrm{Pic}(\mathcal{O}_S) \cong \mathrm{Div}(F/K)/(\langle S \rangle + \mathrm{Princ}(F/K))$.

# Class Fields

Second Part

## Notation

Notation:

- Let $\mathfrak{m}$ denote an effective divisor, called modulus.
- $\mathrm{Div}_{\mathfrak{m}}(F/K)$ group of divisors coprime to $\mathfrak{m}$.
- $F_{\mathfrak{m}}^{\times} = \{f \in F^{\times} \mid v_P(f-1) \geq v_P(\mathfrak{m}) \text{ for all } P\}$ group of elements congruent to one modulo $\mathfrak{m}$.
- $\mathrm{Princ}_{\mathfrak{m}}(F/K) = \{\mathrm{div}(f) \mid f \in F_{\mathfrak{m}}^{\times}\}$, the ray modulo $\mathfrak{m}$.
- $\mathrm{Pic}_{\mathfrak{m}}(F/K) = \mathrm{Div}_{\mathfrak{m}}(F/K) \,/\, \mathrm{Princ}_{\mathfrak{m}}(F/K)$, the ray class group modulo $\mathfrak{m}$.
- $\phi_{\mathfrak{m},\mathfrak{n}} : \mathrm{Pic}_{\mathfrak{m}}(F/K) \to \mathrm{Pic}_{\mathfrak{n}}(F/K)$, $[D]_{\mathfrak{m}} \mapsto [D]_{\mathfrak{n}}$ for $\mathfrak{m} \geq \mathfrak{n}$.

We have $\mathrm{Princ}_{\gcd(\mathfrak{m},\mathfrak{n})}(F/K) = \mathrm{Princ}_{\mathfrak{m}}(F/K) + \mathrm{Princ}_{\mathfrak{n}}(F/K)$.

The $\phi_{\mathfrak{m},\mathfrak{n}}$ are epimorphisms.



Here $\gcd(\mathfrak{m},\mathfrak{n}) = \sum_P \min(v_P(\mathfrak{m}), v_P(\mathfrak{n}))P$. The approximation theorem shows the statements on $\mathrm{Princ}_{\gcd(\mathfrak{m},\mathfrak{n})}(F/K)$ and $\phi_{\mathfrak{m},\mathfrak{n}}$.

References for this section are

- Rosen : "Number theory for function field",
- Artin-Tate: "Class field theory",
- Cassels-Fröhlich : "Algebraic Number Theory",
- Serre : "Algebraic Groups and Class Fields",
- Hess-Massierer : "Tame class field theory for global function fields".

# Artin Map

Let $E/F$ be a finite abelian extension. Let $P$ be place of $F/K$ and write $N(P) = \#\mathcal{O}_P/\mathfrak{m}_P = q^{\deg(P)}$.

If $P$ is unramified in $E/F$ then there is a uniquely determined $\sigma_P \in \mathrm{Gal}(E/F)$ satisfying

$$\sigma_P(x) \equiv x^{N(P)} \bmod \mathfrak{m}_Q$$

for all places $Q$ of $E/K$ above $P$ and all $x \in \mathcal{O}_Q$.

Suppose $E/F$ is unramified outside $\mathrm{supp}(\mathfrak{m})$. The Artin map is defined as

$$A_{E/F} : \mathrm{Div}_{\mathfrak{m}}(F/K) \to \mathrm{Gal}(E/F), \quad D \mapsto \prod_P \sigma_P^{v_P(D)}.$$

## Some Properties of the Artin Map

*Theorem.*

- The Artin map is surjective.
- If the multiplicities of $\mathfrak{m}$ are large enough then

$$\mathrm{Princ}_{\mathfrak{m}}(F/K) \subseteq \ker(A_{E/F}).$$

Any $\mathfrak{m}$ like in the theorem is called a modulus of $E/F$. There is a smallest modulus $\mathfrak{f}(E/F)$ of $E/F$, called conductor of $E/F$. Every place in $\mathfrak{m}$ is ramified in $E/F$.

If $\mathfrak{m}$ is a modulus of $E/F$ then regard

$$A_{E/F} : \mathrm{Pic}_{\mathfrak{m}}(F/K) \to \mathrm{Gal}(E/F).$$

Thus if $H = \ker(A_{E/F})$ then $H$ has finite index in $\mathrm{Pic}_{\mathfrak{m}}(F/K)$ and

$$\mathrm{Gal}(E/F) \cong \mathrm{Pic}_{\mathfrak{m}}(F/K)/H.$$

## Norm Map and Class Fields

Define

$$N_{E/F} : \mathrm{Pic}_{\mathrm{Con}_{E/F}(\mathfrak{m})}(E/K) \to \mathrm{Pic}_{\mathfrak{m}}(F/K)$$

by taking the norm of a representing divisor. Norms of elements of $E^{\times}_{\mathrm{Con}_{E/F}(\mathfrak{m})}$ are elements of $F^{\times}_{\mathfrak{m}}$, so this is well defined.

*Theorem.* If $E/F$ is finite abelian with modulus $\mathfrak{m}$ then

$$\ker(A_{E/F}) = \mathrm{im}(N_{E/F}).$$

We say that $E$ is a class field over $F$ with modulus $\mathfrak{m}$ that belongs to the subgroup $H = \mathrm{im}(N_{E/F}) = \ker(A_{E/F})$ of finite index of $\mathrm{Pic}_{\mathfrak{m}}(F/K)$.

## Existence of Class Fields

*Theorem.*

1. If $H$ is any subgroup of $\mathrm{Pic}_{\mathfrak{m}}(F/K)$ of finite index, then there is a class field $E$ over $F$ with modulus $\mathfrak{m}$ that belongs to $H$, and $E$ is uniquely determined up to $F$-isomorphism.
2. The degree of the exact constant field of $E/K$ over $K$ is equal to $\deg(H)$, the minimal positive degree of divisor classes in $H$.



The Artin map commutes with the epimorphisms $\phi_{\mathfrak{m},\mathfrak{n}}$. It is therefore also possible to combine the groups $\mathrm{Pic}_{\mathfrak{m}}(F/K)$ into the group $\lim_{\mathfrak{m}} \mathrm{Pic}_{\mathfrak{m}}(F/K)$ and let the Artin map take values in the Galois group of a fixed maximal abelian extension of $F$. One then obtains a bijection between subgroups of finite index that contain a ray and finite abelian extensions inside the fixed maximal abelian extension. Also see "idele class groups".

## Computing Ray Class Groups

There is an exact sequence of finitely generated abelian groups

$$0 \to K^\times \to \prod_P (\mathcal{O}_P/\mathfrak{m}_P^{v_P(\mathfrak{m})})^\times \to \mathrm{Pic}_\mathfrak{m}(F/K) \to \mathrm{Pic}(F/K) \to 0.$$

We have:

- Generators and relations can be computed for each object of the sequence other $\mathrm{Pic}_\mathfrak{m}(F/K)$.
- Elements of each object can be represented in chosen generators.
- Images and preimages of the maps of the sequence can also be computed.

Then generators and relations of $\mathrm{Pic}_\mathfrak{m}(F/K)$ can be computed and elements of $\mathrm{Pic}_\mathfrak{m}(F/K)$ can be represented in those generators.



The complexity is dominated by the operations in $\mathrm{Pic}(F/K)$ and the residue class rings $\prod_P(\mathcal{O}_P/\mathfrak{m}_P^{v_P(\mathfrak{m})})^\times$. The latter is dominated by discrete logarithm computations in the residue class fields of the $P$, which are the finite extensions of $\mathbb{F}_q$ of degree $\deg(P)$.

Some references are

- master thesis of Pauli,
- paper by Pauli, Pohst, Hess,
- phd thesis of Roland Auer on the construction of function fields with many rational points,
- second book of Henri Cohen.

## Computing Class Fields

Given $H \leq \mathrm{Pic}_{\mathfrak{m}}(F/K)$ the goal is to compute defining equations for the class field $E$ over $F$ of modulus $\mathfrak{m}$ that belongs to $H$.

*Theorem.* Suppose $H_1, H_2 \subseteq \mathrm{Pic}_{\mathfrak{m}}(F/K)$ with $H_1 \cap H_2 = H$. If $E_1$ belongs to $H_1$ and $E_2$ belongs to $H_2$ then $E = E_1 E_2$ belongs to $H$.

We can choose $H_1$ and $H_2$ such that the index of $H_1$ is coprime to $\mathrm{char}(F)$ and the index of $H_2$ is a power of $\mathrm{char}(F)$.



Some references are

- paper by Fieker on the computation of class fields (for number fields though).
- paper of Hess-Massierer is also helpful.
- second book of Henri Cohen (for number fields though).

## Coprime to Characteristic Case

*Theorem.* Let $F'/F$ finite and $E' = EF'$. Then $E'$ is the class field over $F'$ with modulus $\mathfrak{m}' = \mathrm{Con}_{F'/F}(\mathfrak{m})$ that belongs to $H' = \mathrm{N}_{F'/F}^{-1}(H)$.

Suppose that the index of $H$ is coprime to $\mathrm{char}(F)$ and let $n$ denote the exponent of $\mathrm{Pic}_{\mathfrak{m}}(F/K)/H$.

Let $F' = F(\mu_n)$.

*Theorem.* Every abelian extension of $F'$ of exponent $n$ is a Kummer extension, is thus obtained by adjoining $n$-th roots of suitable Kummer elements of $F'$ to $F'$.

This leads to a rather explicit representation of $E'$.

## Coprime to Characteristic Case

Then it is known and can be done:

- Kummer elements $f_i$ can be computed for the class field $G$ over $F'$ of modulus $\mathfrak{m}'$ that belongs to $n\mathrm{Pic}_{\mathfrak{m}}(F'/K)$, for example by an $S$-units computation in $F'$.
- $H'$ is computed as a preimage of maps of abelian groups.
- $E'$ is the fixed field of $G$ under $A_{G/F'}(H')$, the Kummer elements $g_j$ of $E'$ are accordingly computed as products of the $f_i$ using a generalised Tate-Lichtenbaum pairing.
- $E'/F$ is finite abelian with modulus $m$, and $E$ is the fixed field of $E$ under $A_{E'F}(H)$. Defining equations for $E$ can be computed via explicit Galois theory.



The theorem is not difficult to prove using the following property of the Artin map on divisors: If $\mathrm{res}_{E'/E} : \mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$ denotes the restriction monomorphism then

$$A_{E/F} \circ N_{F'/F} = \mathrm{res}_{E'/E} \circ A_{E'/F'}.$$

For more details see papers by Fieker and Hess-Massierer.

## Power of Characteristic Case

*Theorem.* Every abelian extension of $F'$ of exponent $n$, an $m$-th power of $\mathrm{char}(F)$, is an Artin-Schreier-Witt extension, is thus obtained by adjoining the division points of A-S-W elements in $W_m(F')$ under the A-S-W operator to $F'$.

This leads to a rather explicit but also rather involved representation of $E$. Let $n$ be the exponent of $\mathrm{Pic}_{\mathfrak{m}}(F/K)/H$.

Then it is known and can be done:

- A-S-W elements $f_i$ can be computed for the class field $G$ over $F$ of modulus $\mathfrak{m}$ that belongs to $n\mathrm{Pic}_{\mathfrak{m}}(F/K)$, for example by a Riemann-Roch computation in $F$.
- $E$ is the fixed field of $G$ under $A_{G/F}(H)$, the A-S-W elements $g_j$ of $E$ are accordingly computed as sums of the $f_i$ using a pairing.

## Applications

Construction of function fields with many rational places:

- A place $P$ of $F$ is fully split in $E$ if and only if $P \in H$.
- Let $h_{\mathfrak{n},H} = \#\mathrm{Pic}_{\mathfrak{n}}(F/K)/\phi_{\mathfrak{m},\mathfrak{n}}(H)$. The genus of $E$ satisfies

$$\deg(H)(g_E - 1) = h_{\mathfrak{m},H}\left(g_F - 1 + \frac{\deg(\mathfrak{m})}{2}\right) - \frac{1}{2}\sum_{P|\mathfrak{m}}\left(\sum_{k=1}^{v_P(\mathfrak{m})} h_{\mathfrak{m}-kP,H}\right)\deg(P).$$

Construction of Drinfeld modules:

- Is defined by coefficients which are elements of a specific class field.
- The coefficients satisfy various relations.
- Use those relations to solve for the coefficients over the class field.



Algorithms for the computations of this section have been implemented by Fieker in Magma.

# Zeta functions and $L$-series

Third Part

## Motivation

Study zero sets of polynomial equations over various fields

- Example: $\{(x, y) \in K^2 \mid x^2 + y^2 = 1\}$
- Over finite fields: Count solutions!

Algebraic curves: Polynomial equations have one free variable, the other variables are algebraically dependent.

We will again consider function fields $F/\mathbb{F}_q$ over the exact constant field $\mathbb{F}_q$ instead of curves. Write $N_d$ for the places of degree one of $F/\mathbb{F}_{q^d}$.

The zeta function of $F/K$ is

$$\zeta_{F/K}(t) = \exp\left(\sum_{d=1}^{\infty} N_d \cdot \frac{t^d}{d}\right) = \prod_{P} \frac{1}{1 - t^{\deg(P)}} = \sum_{D \geq 0} t^{\deg(D)}.$$

# Frobenius Operation

There is $L_{F/K}(t) \in \mathbb{Z}[t]$ with $\deg(L_{F/K}(t)) = 2g$ and

$$\zeta_{F/K}(t) = \frac{L_{F/K}(t)}{(1-t)(1-qt)}.$$

This is called the $L$-polynomial of $F/K$.

Moreover, there are $\mathbb{Q}_\ell$-vector spaces $V_\ell$ and $\mathrm{Frob}_{q,\ell} \in \mathrm{Aut}(V_\ell)$ such that

$$L_{F/K}(t) = \det\left(\mathrm{id} - \mathrm{Frob}_{q,\ell} \cdot t \mid V_\ell\right).$$

# Computation of Zeta functions

Possible applications:

- "Cryptography"
- Distribution of the eigenvalues of Frobenius
- ...

Complexity of $\ell$-adic methods:

- Exponential in $g$ and polynomial in $\log(q)$,
- impractical for $g \geq 3$.

Complexity of $p$-adic methods:

- Mostly $O^{\sim}(p^1 g^4 n^3)$ or $O^{\sim}(p^1 g^5 n^3)$ with $n = \log_p(q)$.

# Galois and Abelian Extensions

Let $E/F$ denote a finite Galois extension with Galois group $G$ such that $K$ is the exact constant field of $E$.

The associated product formula for $\zeta_{E/K}(t)$ is

$$\zeta_{E/K}(t) = \prod_{\chi} L(E/F, \chi, t)^{\chi(1)},$$

where $\chi$ runs over the irreducible characters of $G$ and $L(E/F, \chi, t)$ will be defined later (for $G$ abelian).

Can the product be computed more efficiently for large $g_E$?

If $E/F$ is abelian then $E$ is a class field over $F$ belonging to some $H$ and the factors of the product can be described in terms of $H$!

Algorithmics of Function Fields

2 Number Theory

Class Groups
Mathematical Background
Computing in the Class Group
Computing the Class Group
Applications

Class Fields
Mathematical Background
Computing Ray Class Groups
Computing Class Fields
Applications

Zeta functions and L-series
Mathematical Background
Computing L-series
Applications

Exercises

## Ray Class Groups

We have already met ray class groups. Here are some (more) properties.

For a subgroup $H$ of $\mathrm{Pic}_{\mathfrak{m}}(F/K)$ of finite index there is a unique minimal $\mathfrak{f}(H) \leq \mathfrak{m}$ with

$$\mathrm{Pic}_{\mathfrak{f}(H)}(F/K)/\phi_{\mathfrak{m},\mathfrak{f}(H)}(H) \;\cong\; \mathrm{Pic}_{\mathfrak{m}}(F/K)/H.$$

The divisor $\mathfrak{f}(H)$ is the conductor of $H$. It is equal to the conductor of the class field $E$ over $F$ belonging to $H$.

$\mathrm{Pic}_{\mathfrak{m}}(F/K) \cong \mathrm{Pic}^0_{\mathfrak{m}}(F/K) \oplus \mathbb{Z}$.

$$\#\mathrm{Pic}^0_{\mathfrak{m}}(F/K) = \frac{\#\mathrm{Pic}^0(F/K)\cdot\prod_{i=1}^{s}(q^{\deg(P)}-1)q^{\deg(P)(v_P(\mathfrak{m})-1)}}{q-1}.$$

32 / 40

The formula for $\mathrm{Pic}^0_{\mathfrak{m}}(F/K)$ follows from the exact sequence on slide 21.

# Characters and L-series

A character $\chi$ modulo $\mathfrak{m}$ is a homomorphism

$$\chi : \mathrm{Pic}_{\mathfrak{m}}(F/K) \to \mathbb{C}^\times$$

of finite order. The conductor $\mathfrak{f}(\chi)$ of $\chi$ is $\mathfrak{f}(\ker(\chi))$.

The character sum $N_d(\chi)$ of degree $d$ is

$$N_d(\chi) \;=\; \sum_{\deg(P)|d, P \not\leq \mathfrak{f}(\chi)} \deg(P) \cdot \chi([P])^{d/\deg(P)}.$$

The L-series $L(\chi, t) = L(E/F, \chi, t)$ of $\chi$ with $\ker(\chi) \supseteq H$ is

$$L(\chi, t) \;=\; \exp\left(\sum_{d=1}^{\infty} N_d(\chi) \cdot t^d/d\right).$$

We have $\zeta_{F/K}(t) = L(\chi, t)$ for $\chi = \mathrm{id}$.

## L-series

*Theorem.* Assume $\ker(\chi) \neq \mathrm{Pic}_{\mathfrak{m}}(F/K)$. Then

$$L(\chi, t) = \prod_{i=1}^{2g-2+\deg(\mathfrak{f}(\chi))} (1 - \omega_i(\chi)t)$$

with $|\omega_i(\chi)| = q^{1/2}$ and $\zeta$ primitive $\mathrm{ord}(\chi)$-th root of unity, and

$$L(\chi, t) = \varepsilon(\chi) \cdot q^{g-1+\deg(\mathfrak{f}(\chi))/2} \cdot t^{2g-2+\deg(\mathfrak{f}(\chi))} \cdot L(\bar{\chi}, \frac{1}{qt})$$

with $\varepsilon(\chi) \in q^{-\deg(\mathfrak{f}(\chi))/2}\mathbb{Z}[\zeta]$ and $|\varepsilon(\chi)| = 1$. Furthermore,

$$\begin{aligned} \zeta_{E/K}(t) &= \frac{L_{E/K}(t)}{(1-t)(1-qt)} \\ &= \frac{L_{E/K}(t) \cdot \prod_{\mathrm{Pic}_{\mathfrak{m}}(F/K) \supsetneq \ker(\chi) \supseteq H} L(\chi, t)}{(1-t)(1-qt)} \end{aligned}$$



For a reference see the book of Moreno.

# Computing one L-series

Let $L(\chi, t) = \sum_{i=0}^{2g-2+\deg \mathfrak{f}(\chi)} a_i t^i$ with $a_i \in \mathbb{Z}[\zeta]$ and $a_0 = 1$.

1. The coefficients $a_1, \dots, a_m$ can be computed from $N_1(\chi), \dots, N_m(\chi)$ by the definition of $L(\chi, t)$:

$$L(\chi, t) = \sum_{i=0}^{m} a_i t^i \equiv \exp\left(\sum_{d=1}^{m} N_d(\chi) \cdot t^d / d\right) \bmod t^{m+1}.$$

2. The character sums $N_1(\chi), \dots, N_m(\chi)$ can be computed from their definition

$$N_d(\chi) = \sum_{\deg(P) \mid d, P \not\leq \mathfrak{f}(\chi)} \deg(P) \cdot \chi([P])^{d/\deg(P)}$$

by enumerating all places $P$ up to degree $m$ with $P \not\leq \mathfrak{f}(\chi)$.

## Computing one L-series

3. Compute characters $\chi$ modulo $\mathfrak{m}$ with $\ker(\chi) \supseteq H$:
   - Use representations of $\mathrm{Pic}_{\mathfrak{m}}(F/K)$, $H$ and $\mathrm{Pic}_{\mathfrak{m}}(F/K)/H$ in terms of generators and relations.
   - Define $\chi$ on generators of $\mathrm{Pic}_{\mathfrak{m}}(F/K)/H$ and pull back to $\mathrm{Pic}_{\mathfrak{m}}(F/K)$.
   - Compute $\ker(\chi) \supseteq H$ and $\mathfrak{f}(\chi) = \mathfrak{f}(\ker(\chi))$.
   - Write $P$ in the generators of $\mathrm{Pic}_{\mathfrak{f}(\chi)}(F/K)$ to obtain $\chi([P])$.
4. Due to the functional equation there is some redundancy between the coefficients of $L(\chi, t)$. As a consequence it often suffices to take $m$ about half the degree of $L(\chi, t)$.

Best to have a toolbox for finitely generated abelian groups and homomorphisms. Requires algorithms for structure computation of $\mathrm{Pic}_{\mathfrak{m}}(F/K)$ and discrete logarithms in $\mathrm{Pic}_{\mathfrak{m}}(F/K)$.



The required operations for $\mathrm{Pic}_{\mathfrak{m}}(F/K)$ can be reduced to operations in $\mathrm{Pic}(F/K)$ and $\prod_{P \in \mathrm{supp}(\mathfrak{m})} (\mathcal{O}_P/\mathfrak{m}_P^{v_P(\mathfrak{m})})^\times$, see slide 21.

# Computing the Zeta function

Need to choose one $\zeta$ for all $\chi$ on $\mathrm{Pic}_{\mathfrak{m}}(C)$ with $\ker(\chi) \supseteq H$.

Compute $L_{E/K}(t)$ as product over all $L$-series

$$L_{E/K}(t) = L_{F/K}(t) \cdot \prod_{\mathrm{Pic}_{\mathfrak{m}}(F/K) \supsetneq \ker(\chi) \supseteq H} L(\chi, t).$$

Use some optimisations:

- Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Then $L(\sigma \circ \chi, t) = L(\chi, t)^\sigma$. Use Galois redundancy: Compute system of representatives $R$ for $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$-orbits of $(\mathrm{Pic}_{\mathfrak{m}}(F/K)/H)^*$. For each $\chi \in R$ compute $L(\chi, t)$ and derive $L(\sigma \circ \chi, t) = L(\chi, t)^\sigma$.
- Choose some epimorphism $\psi : \mathbb{Z}[\zeta] \to \mathbb{Z}/n\mathbb{Z}$ with $n$ large. Compute product over $\mathbb{Z}/n\mathbb{Z}$ and reconstruct coefficients of $L_{E/K}(t)$ from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$ by choosing the representative of smallest absolute value.

## Complexity

In the following only very rough estimations.

Input size: $F/K, \mathfrak{m}, H$ polynomial in $\log(q)$, $g$, $\deg(\mathfrak{m})$.
Output size: $g_E^2 \log(q)$.

Computing one L-series: $q^{2(g+\deg(\mathfrak{f}(\chi)))}$.

Computing Zeta function:

- L-series product: $g_E^2 \log(q)$.
- Galois redundancy gives big practical, but no asymptotic speed up.

Depending on $H$ have very roughly $\deg(\mathfrak{m}) \lessapprox g_E \lessapprox q^{g+\deg(\mathfrak{m})}$.

So for small $H$ asymptotically optimal!



I have a Magma package for the computations of this section, but it is not yet available in Magma by itself.

## Applications

Galois module structure of $\mathrm{Pic}^0(E/K)$:

- Use $L$-series to compute Stickelberger element in the group ring $\mathbb{Z}[G]$
- Derive information about the structure of $\mathrm{Pic}^0(E/K)$ via Stickelberger ideal and Kolyvagin derivative classes.
- Derive relations of conjugate elements in $\mathrm{Pic}^0(E/K)$ under certain conditions.

This is interesting since no equations for $E/K$ and no expensive class group computation of $\mathrm{Pic}^0(E/K)$ needs to be carried out.



This application is detailed in a paper by Huang-Narayanan.

# Excercises

1. Show that there is an injective map of sets of $\mathrm{Pic}^0(F/K)$ into the set of effective divisors of degree $n$, for any $n \geq n$.

2. Show that $\mathrm{Pic}^0(K(x)/K) = 0$.

3. Show that $\mathrm{Pic}_{\mathfrak{m}}(F/K) \cong \mathrm{Pic}(F/K)$ if and only if $\mathfrak{m}$ is a prime divisor of degree one.

4. Let $\phi : E_1 \to E_2$ be a morphism of elliptic curves. Show that $K(E_1)$ is a class field of $\phi^*(K(E_2))$ belonging to

$$H = \langle\infty\rangle \times \{(\phi(P)) - (\infty) \mid P \in E_1(K)\}.$$

5. If $\chi \neq 1$ is a character for $\mathbb{F}_q(x)/\mathbb{F}_q$ then $\deg(\mathfrak{f}(\chi)) \geq 2$.

6. Let $F = \mathbb{F}_7(x, y)$ with $y^2 = x^5 + 2x + 1$. Compute the genus and number of rational places of the class field of $F/K$ with modulus $\mathfrak{m} = 2\infty + 3(x, y - 1)$ and subgroup $H$ generated by $[(x, y + 1)]_{\mathfrak{m}}$.

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 $\varepsilon_i$ 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 $p = \text{char}(F) > 0$ then uninterestingly $f^{(p)}(t) = 0$, so we will take the $\lambda_i$ as higher derivatives of $f$.

# Local Expansions*

Let $P$ be a place of degree one and $\pi$ 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 $\pi$ to $t$.

Algorithmics of Function Fields

3 Geometry

Weierstrass Places
Mathematical Background
Computation of Weierstrass Placs

Isomorphisms and Automorphisms
Mathematical Background
Computation of Isomorphisms
Applications

## 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 $\pi$ 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 $\pi$.

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

If $\phi$ is surjective it is called an isomorphism.

A homomorphism $\phi$ 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 $\phi$ is an isomorphism if and only if $g_{(1)} = g_{(2)}$.



*Proof of Theorem of Slide.* If $F_{(1)}$ is isomorphic to a proper sub-function field of $F_{(2)}$ and $g_{(1)} \geq 2$, then $g_{(2)} > g_{(1)}$ by the genus formula of Riemann-Hurwitz. □

## Automorphisms

An isomorphism $\phi$ 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 $16g^4$.



The bound for characteristic zero was given by Hurwitz. The bound for positive characteristic was given by Stichtenoth, see “Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik”. Arch. Math., 24:527544, 1973.

# 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.

Algorithmics of Function Fields

3 Geometry

Weierstrass Places

Mathematical Background

Computation of Weierstrass Placs

Isomorphisms and Automorphisms

Mathematical Background

Computation of Isomorphisms

Applications

# 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.

15 / 24

## 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!

Algorithmics of Function Fields

3 Geometry

Weierstrass Places

Mathematical Background

Computation of Weierstrass Placs

Isomorphisms and Automorphisms

Mathematical Background

Computation of Isomorphisms

Applications

## Special Generators*

Suppose $\phi$ 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 $W(P_{(\alpha)})$.

19 / 24

The notation $\alpha$ means that $\alpha = 1$ or $\alpha = 2$, and that any computation need to be carried out in $F_{(1)}$ and $F_{(2)}$ separately. If there is no index $\alpha$, then the computed values need to be the same for $F_{(1)}$ and $F_{(2)}$, otherwise there cannot be an isomorphism.

# 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
  $$1, x_{(\alpha),2}, x_{(\alpha),3}, \ldots, x_{(\alpha),s}$$
  are a reduced integral basis of $\mathrm{Cl}(K[x_{(\alpha),1}], F_{(\alpha)})$.
- The relation ideal of the $x_{(\alpha),1}, x_{(\alpha),2}, \ldots, x_{(\alpha),s}$ is generated by polynomials of the form
  $$t_i t_j - \lambda_{(\alpha),i,j,1}(t_1) - \sum_{\nu=2}^{m_1} \lambda_{(\alpha),i,j,\nu}(t_1) t_\nu \qquad (2 \leq i, j \leq s)$$
- 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 $\phi$ 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

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