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,

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

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

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

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.

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

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.

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 ϕ to the first cyclic factor of the codomain of ϕ.

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

$^{(\dagger)}$: This is for discrete logarithms, so restrictions may apply.

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

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 $N_r > (g-1)2q^{r/2}$. Then $\mathrm{Pic}(F/K)$ is generated by the places of degree $\leq r$ and the places in $\mathrm{supp}(A)$.

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

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 ϕ. We can thus also compute preimages under ϕ 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 $\mathrm{Div}(F/K)/(\langle S \rangle + \mathrm{Princ}(F/K))$.

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 $\mathfrak{n} \geq \mathfrak{m}$.

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.

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

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

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

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

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

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.

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 $\mathrm{char}(F)$.

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.

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

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

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.

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_ℓ 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 ℓ-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 $n = \log_p(q)$.
- Random $q = 2, g = 350$ hyperelliptic curve in 3 days.

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 χ 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!

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.

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

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

Characters and L-series

A character χ 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 χ 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 χ 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 ζ 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,

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

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 $a_1, \ldots, a_m$ can be computed from $N_1(\chi), \ldots, N_m(\chi)$ 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 $N_1(\chi), \ldots, N_m(\chi)$ can be computed from their definition

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

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

Computing one L-series

3. Compute characters χ 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 χ 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 $\mathrm{Pic}_{\mathfrak{m}}(F/K)$.

Computing the Zeta function

Need to choose one ζ for all χ 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!

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.

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

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

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 $[(x, y + 1)]_{\mathfrak{m}}$.