Cyclotomic Number Fields and Function Fields

Timothy All

January 29, 2013

Number Field Notation

- $\zeta_m = e^{2\pi i/m}$
- $K_m = \mathbb{Q}(\zeta_m)$
- p a prime
- for $(p, m) = 1$, $\text{ord}_m\, p$ denotes the order of p in $\mathbb{Z}/m\mathbb{Z}^\times$
- $(p, K_m/\mathbb{Q})$ a Frobenius automorphism for p in $\text{Gal}(K_m/\mathbb{Q})$

Explicit Properties of Cyclotomic Number Fields

- $\mathrm{Gal}(K_m/\mathbb{Q}) = \mathbb{Z}/m\mathbb{Z}^\times$
- $\mathbb{Z}[\zeta_m]$ is the ring of integers of K_m
- p ramifies in K_m if and only if $p \mid m$.
- if $(p, m) = 1$, then $(p, K_m/\mathbb{Q}) : \zeta_m \mapsto \zeta_m^p$.
- if $f = \mathrm{ord}_m\, p$, then $p\mathbb{Z}[\zeta_m] = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where $r = \phi(m)/f$ and $[\mathbb{Z}[\zeta_m]/\mathfrak{p}_i : \mathbb{F}_p] = f$.

Function Field Analogy?

	Number fields	**Function fields**
Integers	$\mathbb{Z}$	$A := \mathbb{F}_p[T]$
Fraction Field	$\mathbb{Q}$	$K := \mathbb{F}_p(T)$
Closure	$\mathbb{Q}^{\text{alg}}$	$\overline{K}$, sep. alg. closure of $\mathbb{F}_p(t)$
Action	$m \cdot \alpha := \alpha^m$	?
Cyclotomy	$\mathbb{Q}$ adjoin m-torsion	??

How do we "exponentiate" elements of $\overline{K}$ by polynomials? And what do the torsion modules look like?

Function Field Notation

- $A := \mathbb{F}_p[T]$, $K := \mathbb{F}_p[T]$, and $\overline{K}$ denotes the separable algebraic closure of K
- $K\{\tau\}$ the ring of "twisted" polynomials in τ:

$$\tau a := a^q \tau \quad \forall a \in K$$

- $C : A \to K\{\tau\}$ the $\mathbb{F}_p$-algebra homomorphism defined by

$$T \mapsto T + \tau.$$

  C is called the **Carlitz Module**.
- $C_m := C(m)$.

Examples and the Carlitz Action

Why the wonky commuting relation in $K\{\tau\}$? To mimic function composition:

$$\begin{aligned} C_{T^2} &= (T+\tau)(T+\tau) \\ &= T^2 + (T+T^q)\tau + \tau^2 \end{aligned}$$

$$\begin{aligned} C_{T^2}(x) &= (Tx + x^q) \circ (Tx + x^q) \\ &= T(Tx + x^q) + (Tx + x^q)^q \\ &= T^2 x + (T + T^q)x^q + x^{q^2}. \end{aligned}$$

Now, we define A acting on $\overline{K}$ by

$$m \cdot \lambda := C_m(\lambda).$$

This is called the **Carlitz action**, and it turns out to be the right analogy to exponentiation.

Definitions and Preliminaries

We let

$$\Lambda_m := \{\lambda \in \overline{K} : C_m(\lambda) = 0\}.$$

Then Λ_m is an A-module (with the Carlitz action). The A-module Λ_m is analogous to the $\mathbb{Z}$-module μ_m, the m-th roots of unity. In fact, essentially from the decomposition theorem for modules over a PID, we get that Λ_m is a cyclic A-module:

$$\Lambda_m \simeq A/mA \qquad (\text{vs } \mu_m \simeq \mathbb{Z}/m\mathbb{Z}).$$

We let $K_m = K(\Lambda_m)$. It's now easy to see that we have

$$\mathrm{Gal}(K_m/K) \hookrightarrow \mathrm{GL}(A/mA) \simeq A/mA^\times \qquad (\text{vs } \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq \mathbb{Z}/m\mathbb{Z}^\times).$$

Already we see the analogy with cyclotomic number fields in parenthesis.

Explicit Properties of Cyclotomic Function Fields

Let λ_m be an A-module generator for Λ_m. We have

- $\mathrm{Gal}(K_m/\mathbb{Q}) \simeq A/mA^\times$
- $A[\Lambda_m]$ is the ring of integers of K_m
- an irreducible monic polynomial ℓ ramifies in K_m if and only if $\ell \mid m$.
- if $(\ell, m) = 1$, then $(\ell, K_m/\mathbb{F}_p(T)) : \lambda_m \mapsto C_\ell(\lambda)m)$.
- if $f = \mathrm{ord}_m \ell$, then $\ell A[\Lambda_m] = \mathfrak{l}_1 \cdots \mathfrak{l}_r$ where $r = \phi(m)/f$ and $[A[\Lambda_m]/\mathfrak{l}_i : \mathbb{F}_p[T]/\ell] = f$.

Comparison

Cyclotomic Number fields	Cyclotomic Function fields
p prime, K_m equals $\mathbb{Q}$ adjoined m-exp. torsion	ℓ irr. poly., K_m equals $\mathbb{F}_p(T)$ adjoined m-Carlitz torsion
$\mathrm{Gal}(K_m/\mathbb{Q}) = \mathbb{Z}/m\mathbb{Z}^\times$	$\mathrm{Gal}(K_m/\mathbb{Q}) \simeq A/mA^\times$
$\mathbb{Z}[\zeta_m]$ is the ring of integers of K_m	$A[\Lambda_m]$ is the ring of integers of K_m
p ramifies in K_m if and only if $p \mid m$	ℓ ramifies in K_m if and only if $\ell \mid m$.
if $(p, m) = 1$, then $(p, K_m/\mathbb{Q}) : \zeta_m \mapsto \zeta_m^p$	if $(\ell, m) = 1$, then $(\ell, K_m/\mathbb{F}_p(T)) : \lambda_m \mapsto C_\ell(\lambda_m)$
if $f = \mathrm{ord}_m\, p$, then $p\mathbb{Z}[\zeta_m] = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where $r = \phi(m)/f$ and $[\mathbb{Z}[\zeta_m]/\mathfrak{p}_i : \mathbb{F}_p] = f$	if $f = \mathrm{ord}_m\, \ell$, then $\ell A[\Lambda_m] = \mathfrak{l}_1 \cdots \mathfrak{l}_r$ where $r = \phi(m)/f$ and $[A[\Lambda_m]/\mathfrak{l}_i : \mathbb{F}_p[T]/\ell] = f$.