Cyclic p-Extensions of $\mathbb{Z}_p$-Fields

Jordan Schettler

11/9/2011

Outline

Regular and Irregular Primes

- Let p be a rational prime.

Regular and Irregular Primes

- Let p be a rational prime.
- In an 1847 attempt at FLT, Lamé claimed $\mathbb{Z}[\zeta_p]$ was a UFD, or equivalently, the class # of $\mathbb{Q}(\zeta_p)$ is 1.

Regular and Irregular Primes

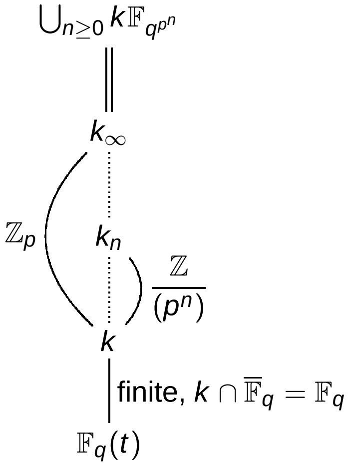
- Let p be a rational prime.
- In an 1847 attempt at FLT, Lamé claimed $\mathbb{Z}[\zeta_p]$ was a UFD, or equivalently, the class # of $\mathbb{Q}(\zeta_p)$ is 1.
- Liouville pointed out that this was false, but Kummer turned Lamé's ideas into a partial proof when p is **regular**, i.e., p does not divide the class # of $\mathbb{Q}(\zeta_p)$.

Regular and Irregular Primes

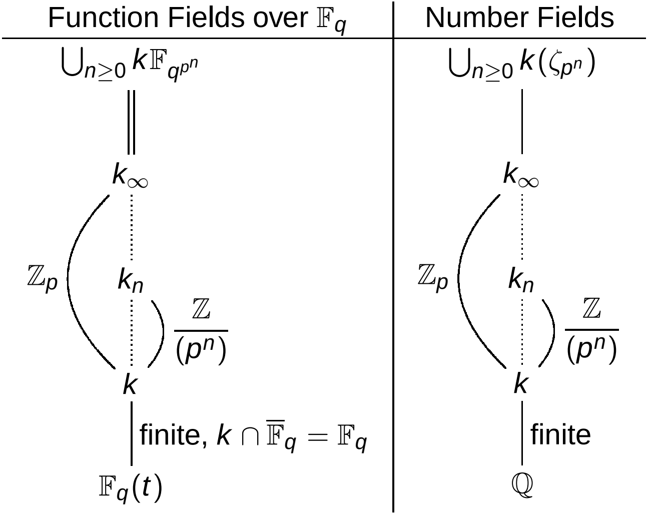
- Let p be a rational prime.
- In an 1847 attempt at FLT, Lamé claimed $\mathbb{Z}[\zeta_p]$ was a UFD, or equivalently, the class # of $\mathbb{Q}(\zeta_p)$ is 1.
- Liouville pointed out that this was false, but Kummer turned Lamé's ideas into a partial proof when p is **regular**, i.e., p does not divide the class # of $\mathbb{Q}(\zeta_p)$.
- Actually, there are infinitely many **irregular** primes p, i.e., p does divide the class # of $\mathbb{Q}(\zeta_p)$.

Constructing $\mathbb{Z}_p$-Extensions

Function Fields over $\mathbb{F}_q$	Number Fields



Constructing $\mathbb{Z}_p$-Extensions



Growth Formulas

Function Fields over $\mathbb{F}_q$	Number Fields
$h_n :=$ class $\#$ of k_n	$h_n :=$ class $\#$ of k_n
$p^{e_n} \| h_n$	$p^{e_n} \| h_n$

Function Fields over $\mathbb{F}_q$	Number Fields
$h_n :=$ class $\#$ of k_n	$h_n :=$ class $\#$ of k_n
$p^{e_n} \| h_n$	$p^{e_n} \| h_n$
Thm (Weil, early 1950s): $\exists \lambda, \nu \in \mathbb{Z}$ s.t. $e_n = \lambda n + \nu$ $\forall n \gg 0$	

Growth Formulas

Function Fields over $\mathbb{F}_q$	Number Fields
$h_n :=$ class $\#$ of k_n	$h_n :=$ class $\#$ of k_n
$p^{e_n} \| h_n$	$p^{e_n} \| h_n$
Thm (Weil, early 1950s)	Thm (Iwasawa, late 1950s)
$\exists \lambda, \nu \in \mathbb{Z}$ s.t.	$\exists \lambda, \mu, \nu \in \mathbb{Z}$ s.t.
$e_n = \lambda n + \nu$	$e_n = \lambda n + \mu p^n + \nu$
$\forall n \gg 0$	$\forall n \gg 0$

Conjecture (Iwasawa)

We have $\mu = 0$ for every cyclotomic $\mathbb{Z}_p$-extension k_∞/k with k a number field.

The μ-Invariant

Conjecture (Iwasawa)

We have $\mu = 0$ for every cyclotomic $\mathbb{Z}_p$-extension k_∞/k with k a number field.

Theorem (Iwasawa, 1973)

There are non-cyclotomic $\mathbb{Z}_p$-extensions with $\mu \neq 0$, but $\mu(k_\infty/k) = 0 \Rightarrow \mu(k'_\infty/k') = 0$ for every p-extension k'/k.

The μ-Invariant

Conjecture (Iwasawa)

We have $\mu = 0$ for every cyclotomic $\mathbb{Z}_p$-extension k_∞/k with k a number field.

Theorem (Iwasawa, 1973)

There are non-cyclotomic $\mathbb{Z}_p$-extensions with $\mu \neq 0$, but $\mu(k_\infty/k) = 0 \Rightarrow \mu(k'_\infty/k') = 0$ for every p-extension k'/k.

Theorem (Ferrero and Washington, 1979)

We have $\mu(k_\infty/k) = 0$ for every abelian number field k.

The λ-Invariant

Function Fields over $\overline{\mathbb{F}}$	$\mathbb{Z}_p$-Fields
K	$K = k_\infty$
finite	finite
$\overline{\mathbb{F}}(t)$	$\mathbb{Q}_\infty$

The λ-Invariant

Function Fields over $\overline{\mathbb{F}}$	$\mathbb{Z}_p$-Fields
K	$K = k_\infty$
finite	finite
$\overline{\mathbb{F}}(t)$	$\mathbb{Q}_\infty$
$\exists$projective curve $X_K/\overline{\mathbb{F}}$: reg, int scheme, fct fld K	$X_K = \text{Spec}(\mathcal{O}_K[1/p])$, dim $= 1$: reg, int scheme, fct fld K

The λ-Invariant

Function Fields over $\overline{\mathbb{F}}$	$\mathbb{Z}_p$-Fields
K | finite | $\overline{\mathbb{F}}(t)$	$K = k_\infty$ | finite | $\mathbb{Q}_\infty$
$\exists$projective curve $X_K/\overline{\mathbb{F}}$: reg, int scheme, fct fld K	$X_K = \mathrm{Spec}(\mathcal{O}_K[1/p])$, dim $= 1$: reg, int scheme, fct fld K
$\mathrm{char}(\mathbb{F}) \neq p \Rightarrow$	$\mu(K/k) = 0 \Rightarrow$
$\mathrm{Pic}(X_K)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2g_K}$	$\mathrm{Pic}(X_K)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_K}$

Formulas

Theorem (Hurwitz Formula, 1890s: function fields over $\overline{\mathbb{F}}$)

$\mathrm{char}(\mathbb{F}) \neq p$, $\mathrm{Gal}(L/K) \cong \mathbb{Z}/(p) \Rightarrow$

$$2g_L = p2g_K - (p-1)2 + \sum_{x \in X_L} (e_x - 1)$$

Formulas

Theorem (Hurwitz Formula, 1890s: function fields over $\overline{\mathbb{F}}$)

$\text{char}(\mathbb{F}) \neq p$, $\text{Gal}(L/K) \cong \mathbb{Z}/(p) \Rightarrow$

$$2g_L = p2g_K - (p-1)2 + \sum_{x \in X_L}(e_x - 1)$$

Theorem (Iwasawa's Formula, 1981: $\mathbb{Z}_p$-fields)

$\mu(K/k) = 0$, $\text{Gal}(L/K) \cong \mathbb{Z}/(p) \Rightarrow$

$$\lambda_L = p\lambda_K - (p-1)\chi_{L/K} + \sum_{x \in X_L}(e_x - 1)$$

where $\chi_{L/K} \in \mathbb{Z}$.

Formulas

Theorem (Hurwitz Formula, 1890s: function fields over $\overline{\mathbb{F}}$)

char$(\mathbb{F}) \neq p$, Gal$(L/K) \cong \mathbb{Z}/(p) \Rightarrow$

$$2g_L = p2g_K - (p-1)2 + \sum_{x \in X_L} (e_x - 1)$$

Theorem (Iwasawa's Formula, 1981: $\mathbb{Z}_p$-fields)

$\mu(K/k) = 0$, Gal$(L/K) \cong \mathbb{Z}/(p) \Rightarrow$

$$\lambda_L = p\lambda_K - (p-1)\chi_{L/K} + \sum_{x \in X_L} (e_x - 1)$$

where $\chi_{L/K} \in \mathbb{Z}$.

Note: $2g_L \equiv 2g_K \pmod{p-1}$ and $\lambda_L \equiv \lambda_K \pmod{p-1}$

Corollary (Ferrero, 1980; Kida, 1979)

$p = 2$: Let $L/K = \mathbb{Q}_\infty(\sqrt{-d})/\mathbb{Q}_\infty$ with $d > 2$ a squarefree integer. Then

$$\lambda_L = -1 + \sum_{x \in X_L} (e_x - 1)$$

Applications of Iwasawa's Formula

Corollary (Ferrero, 1980; Kida, 1979)

$p = 2$: Let $L/K = \mathbb{Q}_\infty(\sqrt{-d})/\mathbb{Q}_\infty$ with $d > 2$ a squarefree integer. Then

$$\lambda_L = -1 + \sum_{x \in X_L} (e_x - 1)$$

Corollary (S., 2010)

The same computation holds if we replace $\mathbb{Q}$ in the above with $k \subseteq \mathbb{Q}(\zeta_{F^2})$ such that $F = [k : \mathbb{Q}] \in \{3, 5, 17, 257\}$.

Corollary (Kida, 1979)

$p > 2$: Let L/K be CM $\mathbb{Z}_p$-fields, $\mathrm{Gal}(L/K) \cong \mathbb{Z}/(p)$. *Then*

$$\lambda_L^- = p\lambda_K^- - (p-1)\delta + \sum{}^-(e_x - 1)$$

where

$$\delta = \chi_{L/K} - \chi_{L^+/K^+} = \begin{cases} 1 & \text{if } \zeta_p \in K \\ 0 & \text{if } \zeta_p \notin K \end{cases}$$

and $\lambda_L^- = \lambda_L - \lambda_{L^+}$, etc., with the assumption $\mu_K^- = 0$.

Let K_n be the function field of the curve over $\mathbb{C}$ given by

$$x^{p^n} + y^{p^n} + z^{p^n} = 0.$$

A Motivating Example

Let K_n be the function field of the curve over $\mathbb{C}$ given by

$$x^{p^n} + y^{p^n} + z^{p^n} = 0.$$

Then K_n/K_{n-1} is cyclic of order p, so

$$2g_{K_n} \equiv 2g_{K_{n-1}} \pmod{p-1}$$

A Motivating Example

Let K_n be the function field of the curve over $\mathbb{C}$ given by

$$x^{p^n} + y^{p^n} + z^{p^n} = 0.$$

Then K_n/K_{n-1} is cyclic of order p, so

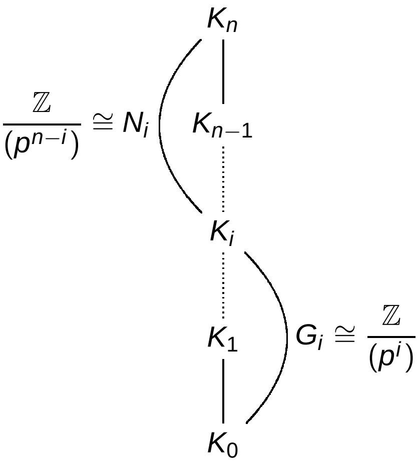
$$2g_{K_n} \equiv 2g_{K_{n-1}} \pmod{p-1}$$

but, in fact, $2g_{K_i} = (p^i - 1)(p^i - 2)$ and

$$(p^n - 1)(p^n - 2) \equiv (p^{n-1} - 1)(p^{n-1} - 2) \pmod{p^{n-1}(p-1)}$$

Hypotheses

Let $K_0 = k_\infty$ with $\mu(K_0/k) = 0$. Consider a tower:



Definitions

Definition

For $G = G_i$ or N_i and M a G-module we define $\chi_G(M)$ by

$$\frac{|H^2(G,M)|}{|H^1(G,M)|} = p^{\chi_G(M)}$$

when these quantities are finite.

Definitions

Definition

For $G = G_i$ or N_i and M a G-module we define $\chi_G(M)$ by

$$\frac{|H^2(G,M)|}{|H^1(G,M)|} = p^{\chi_G(M)}$$

when these quantities are finite.

Definition

$I_{K_i} :=$ invertible fractional ideals of $\mathcal{O}_{K_i}$
$P_{K_i} \leq I_{K_i}$ subgroup of principals
$C_{K_i} := I_{K_i}/P_{K_i}$

Main Result

Theorem (S., 2009)

$$\frac{\lambda_{K_n} - p^n \lambda_{K_0}}{p-1} = p^{n-1}\chi_{G_n}(C_{K_n}) - \sum_{i=1}^{n-1} \varphi(p^i)\chi_{G_i}(C_{K_i})$$

Main Result

Theorem (S., 2009)

$$\frac{\lambda_{K_n} - p^n \lambda_{K_0}}{p-1} = p^{n-1}\chi_{G_n}(C_{K_n}) - \sum_{i=1}^{n-1} \varphi(p^i)\chi_{G_i}(C_{K_i})$$

$$= \frac{p^n}{np-n+1}\chi_{N_0}(C_{K_n}) + \sum_{i=1}^{n-1} \frac{p^i(p-1)\chi_{N_{n-i}}(C_{K_n})}{(ip-i+p)(ip-i+1)}$$

Corollary

$$\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} = p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi_{G_n}(C_{K_n})$$

Congruences

Corollary

$$\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} = p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi_{G_n}(C_{K_n})$$

Corollary

$$\lambda_{K_n} \equiv \lambda_{K_{n-1}} \pmod{\varphi(p^n)}$$

Congruences

Corollary

$$\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} = p^{n-1}(1+n(p-1))\lambda_{K_0} + \varphi(p^n)\chi_{G_n}(C_{K_n})$$

Corollary

$$\lambda_{K_n} \equiv \lambda_{K_{n-1}} \pmod{\varphi(p^n)}$$

$$p \nmid n-1 \Rightarrow \lambda_{K_n} \equiv \sum_{i=1}^{n-1} \frac{p^i(p-1)^2\chi_{N_{n-i}}(C_{K_n})}{(ip-i+p)(ip-i+1)} \pmod{p^n}$$

Vanishing Criterion

Theorem (S., 2011)

Suppose K_n/K_0 is unramified at every infinite place and that $K_0 = k_\infty$ for a number field k s.t. k has exactly one prime above p and $p \nmid$ class # of k. Then

$$\lambda_{K_n} = 0 \Leftrightarrow \mathrm{ord}_p \left| \frac{I_{K_n}^{G_n} P_{K_n}}{I_{K_0} P_{K_n}} \right| = 0.$$

Note: T. Fukuda et al proved the $n = 1$ case in 1997 using Iwasawa's formula.

$\mathbb{Q}_p$-Representations

Theorem (S., 2011)

Let π_{K_n/K_0} be the representation corresponding to the $\mathbb{Q}_p G_n$-module $\mathrm{Hom}_{\mathbb{Z}_p}(C_{K_n}[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then we have the following decomposition:

$$\pi_{K_n/K_0} \cong \lambda_{K_0}\pi_{G_n} \oplus \bigoplus_{i=1}^{n} (\chi_{G_i}(C_{K_i}) - \chi_{G_{i-1}}(C_{K_{i-1}}))\pi_{\varphi(p^i)}$$

where π_{G_n} is the regular representation and π_d is the faithful, irreducible representation of degree $d \in \{\varphi(p), \ldots, \varphi(p^n)\}$.

Note: Comparing degrees of both sides recovers a generalized Iwasawa's formula.