Function Fields with Class Number Indivisible by a prime ℓ

Michael Daub, Jaclyn Lang, Mona Merling, Natee Pitiwan

SMALL 2008

Advisor: Allison Pacelli

Definitions: Number Field & Ring of Integers

Definition

A **number field** is a finite extension of $\mathbb{Q}$.

Definitions: Number Field & Ring of Integers

Definition

A **number field** is a finite extension of $\mathbb{Q}$.

Definition

A complex number is an **algebraic integer** if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Definitions: Number Field & Ring of Integers

Definition

A **number field** is a finite extension of $\mathbb{Q}$.

Definition

A complex number is an **algebraic integer** if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Definition

The **ring of integers** of a number field K, denoted by $\mathcal{O}_K$, is the set of all algebraic integers in K.

Definitions: Number Field & Ring of Integers

Definition

A **number field** is a finite extension of $\mathbb{Q}$.

Definition

A complex number is an **algebraic integer** if it is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Definition

The **ring of integers** of a number field K, denoted by $\mathcal{O}_K$, is the set of all algebraic integers in K.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Is $\mathcal{O}_K$ a Unique Factorization Domain?

Is $\mathcal{O}_K$ a Unique Factorization Domain?

Remark

$\mathcal{O}_K$ is not always a UFD.

Is $\mathcal{O}_K$ a Unique Factorization Domain?

Remark

$\mathcal{O}_K$ is not always a UFD.

Example

Let $K = \mathbb{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, and

$$-2 \cdot 3 = -6 = (\sqrt{-6})^2$$

Is $\mathcal{O}_K$ a Unique Factorization Domain?

Remark

$\mathcal{O}_K$ is not always a UFD.

Example

Let $K = \mathbb{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$, and

$$-2 \cdot 3 = -6 = (\sqrt{-6})^2$$

but 2, 3, and $\sqrt{-6}$ are irreducible in $\mathbb{Z}[\sqrt{-6}]$.

Thus, $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.

Unique Factorization of Ideals

Remark

$\mathcal{O}_K$ is a Dedekind domain for any number field K.

Unique Factorization of Ideals

Remark

$\mathcal{O}_K$ is a Dedekind domain for any number field K.

Theorem

Every proper ideal in a Dedekind domain factors uniquely into a product of prime ideals.

Unique Factorization of Ideals

Remark

$\mathcal{O}_K$ is a Dedekind domain for any number field K.

Theorem

Every proper ideal in a Dedekind domain factors uniquely into a product of prime ideals.

Example

Let $K = \mathbb{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

Unique Factorization of Ideals

Remark

$\mathcal{O}_K$ is a Dedekind domain for any number field K.

Theorem

Every proper ideal in a Dedekind domain factors uniquely into a product of prime ideals.

Example

Let $K = \mathbb{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

$$\langle -2 \rangle = \langle 2, \sqrt{-6} \rangle^2$$
$$\langle 3 \rangle = \langle 3, \sqrt{-6} \rangle^2$$
$$\langle \sqrt{-6} \rangle = \langle 2, \sqrt{-6} \rangle \langle 3, \sqrt{-6} \rangle$$

Unique Factorization of Ideals

Remark

$\mathcal{O}_K$ is a Dedekind domain for any number field K.

Theorem

Every proper ideal in a Dedekind domain factors uniquely into a product of prime ideals.

Example

Let $K = \mathbb{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

$$\langle -2 \rangle = \langle 2, \sqrt{-6} \rangle^2$$
$$\langle 3 \rangle = \langle 3, \sqrt{-6} \rangle^2$$
$$\langle \sqrt{-6} \rangle = \langle 2, \sqrt{-6} \rangle \langle 3, \sqrt{-6} \rangle$$

Note $\langle -6 \rangle = \langle -2 \rangle \langle 3 \rangle = \langle \sqrt{-6} \rangle^2 = \langle 2, \sqrt{-6} \rangle^2 \langle 3, \sqrt{-6} \rangle^2$.

Equivalence Relation

Nonzero ideals $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$.

Class Group & Class Number

Equivalence Relation

Nonzero ideals $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$.

Theorem

The equivalence classes under $\sim$ form a finite abelian group, called the ***class group****, denoted by Cl_K. The size of the class group is called the* ***class number****, denoted by h_K.*

Class Group & Class Number

Equivalence Relation

Nonzero ideals $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$.

Theorem

The equivalence classes under $\sim$ form a finite abelian group, called the ***class group****, denoted by Cl_K. The size of the class group is called the* ***class number****, denoted by h_K.*

- Group operation: $[I] * [J] = [IJ]$.

Equivalence Relation

Nonzero ideals $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$.

Theorem

*The equivalence classes under $\sim$ form a finite abelian group, called the **class group**, denoted by Cl_K. The size of the class group is called the **class number**, denoted by h_K.*

- Group operation: $[I] * [J] = [IJ]$.
- Associativity: $\checkmark$

Class Group & Class Number

Equivalence Relation

Nonzero ideals $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$.

Theorem

The equivalence classes under $\sim$ form a finite abelian group, called the ***class group****, denoted by Cl_K. The size of the class group is called the* ***class number****, denoted by h_K.*

- Group operation: $[I] * [J] = [IJ]$.
- Associativity: ✓
- Identity: the equivalence class of principal ideals.

Class Group & Class Number

Equivalence Relation

Nonzero ideals $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$.

Theorem

The equivalence classes under $\sim$ form a finite abelian group, called the ***class group****, denoted by Cl_K. The size of the class group is called the* ***class number****, denoted by h_K.*

- Group operation: $[I] * [J] = [IJ]$.
- Associativity: ✓
- Identity: the equivalence class of principal ideals.
- Inverses: hard

What does the class number tell us?

What does the class number tell us?

- Since the identity element of Cl_K is the class of principal ideals, then $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain (PID).

What does the class number tell us?

- Since the identity element of Cl_K is the class of principal ideals, then $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain (PID).
- A PID is always a UFD, so $\mathcal{O}_K$ is a UFD if $h_K = 1$.

What does the class number tell us?

- Since the identity element of Cl_K is the class of principal ideals, then $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain (PID).
- A PID is always a UFD, so $\mathcal{O}_K$ is a UFD if $h_K = 1$.

Theorem

For Dedekind domains, UFD $\Leftrightarrow$ PID.

What does the class number tell us?

- Since the identity element of Cl_K is the class of principal ideals, then $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain (PID).
- A PID is always a UFD, so $\mathcal{O}_K$ is a UFD if $h_K = 1$.

Theorem

For Dedekind domains, UFD $\Leftrightarrow$ PID.

- Thus, $\mathcal{O}_K$ is a UFD if and only if $h_K = 1$.

What does the class number tell us?

- Since the identity element of Cl_K is the class of principal ideals, then $h_K = 1$ if and only if $\mathcal{O}_K$ is a principal ideal domain (PID).
- A PID is always a UFD, so $\mathcal{O}_K$ is a UFD if $h_K = 1$.

Theorem

For Dedekind domains, UFD $\Leftrightarrow$ PID.

- Thus, $\mathcal{O}_K$ is a UFD if and only if $h_K = 1$.
- Roughly, the class number measures the closeness of $\mathcal{O}_K$ to being a UFD.

Class Numbers of Quadratic Fields:

d	2	3	5	6	7	10	11	13	14	15	17	19	21
$\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$	1	1	1	1	1	2	1	1	1	2	1	1	1
$\mathrm{Cl}_{\mathbb{Q}(\sqrt{-d})}$	1	1	2	2	1	2	1	2	4	2	4	1	4

Class Numbers of Quadratic Fields:

d	2	3	5	6	7	10	11	13	14	15	17	19	21
$\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$	1	1	1	1	1	2	1	1	1	2	1	1	1
$\mathrm{Cl}_{\mathbb{Q}(\sqrt{-d})}$	1	1	2	2	1	2	1	2	4	2	4	1	4

Theorem

The class number of $\mathbb{Q}(\sqrt{d})$, $d < 0$, *is 1 if and only if* $d = -1, -2, -3, -7, -11, -19, -43, -67$ *or* -163.

Class Numbers of Quadratic Fields:

d	2	3	5	6	7	10	11	13	14	15	17	19	21
$\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$	1	1	1	1	1	2	1	1	1	2	1	1	1
$\mathrm{Cl}_{\mathbb{Q}(\sqrt{-d})}$	1	1	2	2	1	2	1	2	4	2	4	1	4

Theorem

The class number of $\mathbb{Q}(\sqrt{d})$, $d < 0$, is 1 if and only if $d = -1, -2, -3, -7, -11, -19, -43, -67$ or -163.

Open Question

Are there infinitely many real quadratic number fields with class number one?

Definition

A **function field** (in one variable) over a finite field $\mathbb{F}$ is a field K, containing $\mathbb{F}$ and at least one transcendental element T over $\mathbb{F}$, such that $K/\mathbb{F}(T)$ is a finite algebraic extension.

Function Fields

Definition

A **function field** (in one variable) over a finite field $\mathbb{F}$ is a field K, containing $\mathbb{F}$ and at least one transcendental element T over $\mathbb{F}$, such that $K/\mathbb{F}(T)$ is a finite algebraic extension.

- Note that $\mathbb{F}(T)$ is the field of fractions of polynomials in T over $\mathbb{F}$.

Function Fields

Definition

A **function field** (in one variable) over a finite field $\mathbb{F}$ is a field K, containing $\mathbb{F}$ and at least one transcendental element T over $\mathbb{F}$, such that $K/\mathbb{F}(T)$ is a finite algebraic extension.

- Note that $\mathbb{F}(T)$ is the field of fractions of polynomials in T over $\mathbb{F}$.
- We can define the ring of integers of K in the same way as for number fields.

Definition

A **function field** (in one variable) over a finite field $\mathbb{F}$ is a field K, containing $\mathbb{F}$ and at least one transcendental element T over $\mathbb{F}$, such that $K/\mathbb{F}(T)$ is a finite algebraic extension.

- Note that $\mathbb{F}(T)$ is the field of fractions of polynomials in T over $\mathbb{F}$.
- We can define the ring of integers of K in the same way as for number fields.
- The ring of integers of $\mathbb{F}(T)$ is $\mathbb{F}[T]$, the ring of polynomials in T over $\mathbb{F}$.

Number Fields vs. Function Fields

Number Field	Function Field
$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \mid & & \mid \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$	$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ \mid & & \mid \\ \mathbb{F}_q[T] & \subset & \mathbb{F}_q(T) \end{array}$

	$\mathbb{Z}$	$\mathbb{F}_q[T]$
UFD	yes	yes
irreducibles	(infinitely many) primes	(infinitely many) irreducible polynomials
units	$\{\pm 1\}$ (finitely many)	$\mathbb{F}_q^\times$ (finitely many)
residue class	$\lvert\mathbb{Z}/n\mathbb{Z}\rvert = \lvert n\rvert$	$\lvert\mathbb{F}_q[T]/f\,\mathbb{F}_q[T]\rvert = q^{\deg f}$

Cool Things about Function Fields

Cool Things about Function Fields

- The proof of the analogue of Fermat's Last Theorem for function fields takes half a page!

Cool Things about Function Fields

- The proof of the analogue of Fermat's Last Theorem for function fields takes half a page!
- The abc-conjecture has been proven!

Cool Things about Function Fields

- The proof of the analogue of Fermat's Last Theorem for function fields takes half a page!
- The abc-conjecture has been proven!
- Riemann Hypothesis analogue for function fields also proven!

Cool Things about Function Fields

- The proof of the analogue of Fermat's Last Theorem for function fields takes half a page!
- The abc-conjecture has been proven!
- Riemann Hypothesis analogue for function fields also proven!
- Every function field is isomorphic to a non-singular projective curve, so we can compute the genus of the function field.

Cool Things about Function Fields

- The proof of the analogue of Fermat's Last Theorem for function fields takes half a page!
- The abc-conjecture has been proven!
- Riemann Hypothesis analogue for function fields also proven!
- Every function field is isomorphic to a non-singular projective curve, so we can compute the genus of the function field.
- Still, questions on class numbers of function fields are VERY HARD.

The Case $\ell = 3$

Theorem (Pacelli, Rosen)

Let m be any positive integer, $m > 1$ and $3 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 3.

The Case $\ell = 5$

Theorem

Let m be any positive integer, $m > 1$ and $5 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 5.

The Case $\ell = 5$

Theorem

Let m be any positive integer, $m > 1$ and $5 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 5.

Let ζ be a root of the polynomial $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_q[X]$, and assume the following conditions on q are true:

The Case $\ell = 5$

Theorem

Let m be any positive integer, $m > 1$ and $5 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 5.

Let ζ be a root of the polynomial $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_q[X]$, and assume the following conditions on q are true:

- $q \equiv 4 \pmod 5$, $q \nmid m$

The Case $\ell = 5$

Theorem

Let m be any positive integer, $m > 1$ and $5 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 5.

Let ζ be a root of the polynomial $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_q[X]$, and assume the following conditions on q are true:

- $q \equiv 4 \pmod 5$, $q \nmid m$
- there exists $\gamma \in \mathbb{F}_q^\times$ such that $\gamma + 5\zeta$ is not a p-th power in $\mathbb{F}_q(\zeta)$ for all primes p dividing m

The Case $\ell = 5$

Theorem

Let m be any positive integer, $m > 1$ and $5 \nmid m$. There are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by 5.

Let ζ be a root of the polynomial $X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_q[X]$, and assume the following conditions on q are true:

- $q \equiv 4 \pmod 5$, $q \nmid m$
- there exists $\gamma \in \mathbb{F}_q^\times$ such that $\gamma + 5\zeta$ is not a p-th power in $\mathbb{F}_q(\zeta)$ for all primes p dividing m
- if $4|m$, then $\gamma + 5\zeta \notin -4\mathbb{F}_q(\zeta)^4$

Constructing the Fields

The Recursion Relation

Define $X_0 = T$ and

$$X_j = \frac{X_{j-1}^5 - 10X_{j-1}^3 + 10\omega X_{j-1}^2 + 5\omega X_{j-1} - 1}{5X_{j-1}(X_{j-1}^3 - 2\omega X_{j-1}^2 - 2\omega X_{j-1} + 1)},$$

for $j \geq 1$ and $\omega \in \mathbb{F}_q(T)$ such that $\omega^2 + \omega - 1 = 0$.

Constructing the Fields

The Recursion Relation

Define $X_0 = T$ and

$$X_j = \frac{X_{j-1}^5 - 10X_{j-1}^3 + 10\omega X_{j-1}^2 + 5\omega X_{j-1} - 1}{5X_{j-1}(X_{j-1}^3 - 2\omega X_{j-1}^2 - 2\omega X_{j-1} + 1)},$$

for $j \geq 1$ and $\omega \in \mathbb{F}_q(T)$ such that $\omega^2 + \omega - 1 = 0$.

The Field of Degree m

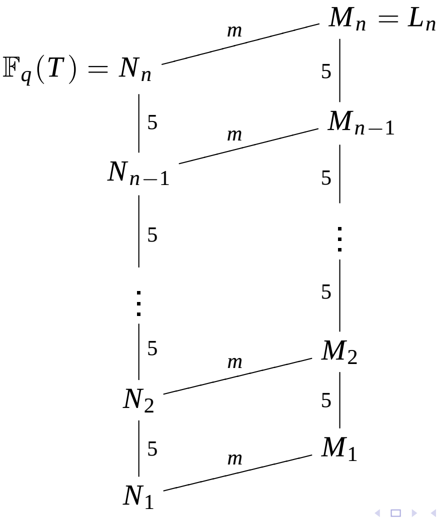
Fix $n \geq 1$. For $1 \leq i \leq n$, define

$$N_i = \mathbb{F}_q(X_{n-i})$$
$$M_i = \mathbb{F}_q(X_{n-i}, \sqrt[m]{5X_n + \gamma}).$$

Let $L_n = \mathbb{F}_q(T)(\sqrt[m]{5X_n + \gamma}) = M_n$.

Field Diagram

$$N_i = \mathbb{F}_q(X_{n-i}) \text{ and } M_i = \mathbb{F}_q(X_{n-i}, \sqrt[m]{5X_n + \gamma})$$



Definition of f_p's

Let p be a divisor of m such that either p is prime or $p = 4$. Define

$$f_p(x) = 5 \sum_{\substack{i=0 \\ i\equiv 0(5)}}^{p} \binom{p}{i} x^{p-i} - \gamma \sum_{\substack{i=0 \\ i\equiv 1(5)}}^{p} \binom{p}{i} x^{p-i} - (5+\gamma\omega) \sum_{\substack{i=0 \\ i\equiv 2(5)}}^{p} \binom{p}{i} x^{p-i}$$

$$+ \omega(\gamma - 5) \sum_{\substack{i=0 \\ i\equiv 3(5)}}^{p} \binom{p}{i} x^{p-i} + (\gamma + 5\omega) \sum_{\substack{i=0 \\ i\equiv 4(5)}}^{p} \binom{p}{i} x^{p-i}$$

$$f_4(x) = x^4 - \frac{4}{5}\gamma x^3 - (\frac{6}{5}\gamma\omega + 6)x^2 + 4\omega(\frac{1}{5}\gamma - 1)x + (\omega + \frac{\gamma}{5})$$

Fact: Each $f_p(x)$ is Eisenstein with respect to the chosen prime $\mathfrak{p} \subset \mathbb{Q}(\omega)$ lying over p, and thus each $f_p(x)$ is irreducible over $\mathbb{Q}(\omega)$.

The Rest of the Proof

- Reduce the problem to showing that $f_p(x)$ has no roots mod q.

The Rest of the Proof

- Reduce the problem to showing that $f_p(x)$ has no roots mod q.

Theorem (Jordan)

Let G be a group acting on a finite set X with cardinality n. If $n \geq 2$ and G acts transitively on X, then there is an element $g \in G$ which acts on X without a fixed point.

The Rest of the Proof

- Reduce the problem to showing that $f_p(x)$ has no roots mod q.

Theorem (Jordan)

Let G be a group acting on a finite set X with cardinality n. If $n \geq 2$ and G acts transitively on X, then there is an element $g \in G$ which acts on X without a fixed point.

Theorem (Frobenius)

Let f be an irreducible polynomial over $\mathbb{Q}(\omega)$ with Galois group G. The density of primes q for which f has no roots mod q exists, and is equal to $1/|G|$ times the number of $\sigma \in G$ with no fixed points.

What about other values of ℓ?

- How can we generalize this result to an arbitrary prime ℓ?

What about other values of ℓ?

- How can we generalize this result to an arbitrary prime ℓ?
- The $\ell = 5$ case relied heavily on creating the chain of cyclic quintic extensions:

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = \mathbb{F}_q(T).$$

What about other values of ℓ?

- How can we generalize this result to an arbitrary prime ℓ?
- The $\ell = 5$ case relied heavily on creating the chain of cyclic quintic extensions:

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = \mathbb{F}_q(T).$$

So, in order to use the same techniques in general, we need a polynomial that generates cyclic extensions of degree ℓ.

What about other values of ℓ?

- How can we generalize this result to an arbitrary prime ℓ?
- The $\ell = 5$ case relied heavily on creating the chain of cyclic quintic extensions:

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = \mathbb{F}_q(T).$$

  So, in order to use the same techniques in general, we need a polynomial that generates cyclic extensions of degree ℓ.
- Rikuna showed that the splitting field of the following polynomial has Galois group $\mathbb{Z}/\ell\mathbb{Z}$ over $k(T)$ for certain fields k:

$$\frac{\zeta^{-1}(X-\zeta)^\ell - \zeta(X-\zeta^{-1})^\ell}{\zeta^{-1}-\zeta} - T\,\frac{(X-\zeta)^\ell - (X-\zeta^{-1})^\ell}{\zeta^{-1}-\zeta}.$$

The General Case

Theorem

Let ℓ be a prime and $m > 1$ be any positive integer such that $\ell \nmid m$. Then there are a positive density of primes (and prime powers) q such that for a given rational function field $\mathbb{F}_q(T)$, there are infinitely many function fields of degree m over $\mathbb{F}_q(T)$ with divisor class number indivisible by ℓ.

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

For a particular q, we need the following conditions satisfied for the theorem to hold:

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

For a particular q, we need the following conditions satisfied for the theorem to hold:

- $\zeta \notin \mathbb{F}_q$, more precisely $g(X)$ has no roots mod q;

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

For a particular q, we need the following conditions satisfied for the theorem to hold:

- $\zeta \notin \mathbb{F}_q$, more precisely $g(X)$ has no roots mod q;
- $\omega \in \mathbb{F}_q$, more precisely $h(X)$ splits completely mod q;

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

For a particular q, we need the following conditions satisfied for the theorem to hold:

- $\zeta \notin \mathbb{F}_q$, more precisely $g(X)$ has no roots mod q;
- $\omega \in \mathbb{F}_q$, more precisely $h(X)$ splits completely mod q;
- $\operatorname{char} \mathbb{F}_q$ does not divide m;

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

For a particular q, we need the following conditions satisfied for the theorem to hold:

- $\zeta \notin \mathbb{F}_q$, more precisely $g(X)$ has no roots mod q;
- $\omega \in \mathbb{F}_q$, more precisely $h(X)$ splits completely mod q;
- $\operatorname{char} \mathbb{F}_q$ does not divide m;
- There exists $\gamma \in \mathbb{F}_q^\times$ such that $\gamma + \ell\zeta$ is not a p-th power in $\mathbb{F}_q(\zeta)$ for all primes p dividing m;

Conditions on q

Let ζ be a root of $g(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1$ and let $h(X)$ be the minimal polynomial of $\omega = \zeta + \zeta^{-1}$.

For a particular q, we need the following conditions satisfied for the theorem to hold:

- $\zeta \notin \mathbb{F}_q$, more precisely $g(X)$ has no roots mod q;
- $\omega \in \mathbb{F}_q$, more precisely $h(X)$ splits completely mod q;
- $\operatorname{char} \mathbb{F}_q$ does not divide m;
- There exists $\gamma \in \mathbb{F}_q^{\times}$ such that $\gamma + \ell\zeta$ is not a p-th power in $\mathbb{F}_q(\zeta)$ for all primes p dividing m;
- If $4|m$, then $\gamma + \ell\zeta \notin -4\mathbb{F}_q(\zeta)^4$.

Constructing the Fields: Revisited

The Recursion Relation

Define $X_0 = T$ and

$$X_j = \frac{\zeta^{-1}(X_{j-1} - \zeta)^\ell - \zeta(X_{j-1} - \zeta^{-1})^\ell}{(X_{j-1} - \zeta)^\ell - (X_{j-1} - \zeta^{-1})^\ell},$$

for $j \geq 1$.

Constructing the Fields: Revisited

The Recursion Relation

Define $X_0 = T$ and

$$X_j = \frac{\zeta^{-1}(X_{j-1} - \zeta)^\ell - \zeta(X_{j-1} - \zeta^{-1})^\ell}{(X_{j-1} - \zeta)^\ell - (X_{j-1} - \zeta^{-1})^\ell},$$

for $j \geq 1$.

The Field of Degree m

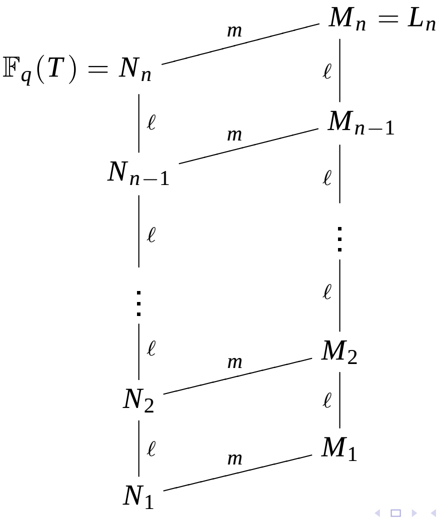
Fix $n \geq 1$. For $1 \leq i \leq n$, define

$$N_i = \mathbb{F}_q(X_{n-i})$$
$$M_i = \mathbb{F}_q(X_{n-i}, \sqrt[m]{\ell X_n + \gamma}).$$

Let $L_n = \mathbb{F}_q(T)(\sqrt[m]{\ell X_n + \gamma}) = M_n$.

Field Diagram

$$N_i = \mathbb{F}_q(X_{n-i}) \text{ and } M_i = \mathbb{F}_q(X_{n-i},\ \sqrt[m]{\ell X_n + \gamma})$$



Proving there are infinitely many q

- Recall: We want $\ell\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$ for all p dividing m and $\ell\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$ if $4 \mid m$.

Proving there are infinitely many q

- Recall: We want $\ell\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$ for all p dividing m and $\ell\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$ if $4 \mid m$.
- For p a prime or $p = 4$, define a polynomial $f_p(X) \in \mathbb{Q}(\omega)[X]$ as follows:

$$f_p(X) = \sum_{j=0}^{\ell-1} \sum_{\substack{i=0 \\ i \equiv j}}^{p} \binom{p}{i} (a_j\gamma + a_{j-1}\ell) X^{p-i}$$

where $a_j = (\zeta^j - \zeta^{-j})/(\zeta - \zeta^{-1})$ and γ is chosen to make f_p Eisenstein for each $p \mid m$.

Proving there are infinitely many q

- Recall: We want $\ell\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$ for all p dividing m and $\ell\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$ if $4 \mid m$.
- For p a prime or $p = 4$, define a polynomial $f_p(X) \in \mathbb{Q}(\omega)[X]$ as follows:

$$f_p(X) = \sum_{j=0}^{\ell-1} \sum_{\substack{i=0 \\ i \equiv j}}^{p} \binom{p}{i} (a_j\gamma + a_{j-1}\ell) X^{p-i}$$

  where $a_j = (\zeta^j - \zeta^{-j})/(\zeta - \zeta^{-1})$ and γ is chosen to make f_p Eisenstein for each $p \mid m$.
- The polynomial f_p was chosen so that if f_p has no roots mod q, then $\ell\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$, and if f_4 has no roots mod q, then $\ell\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$.

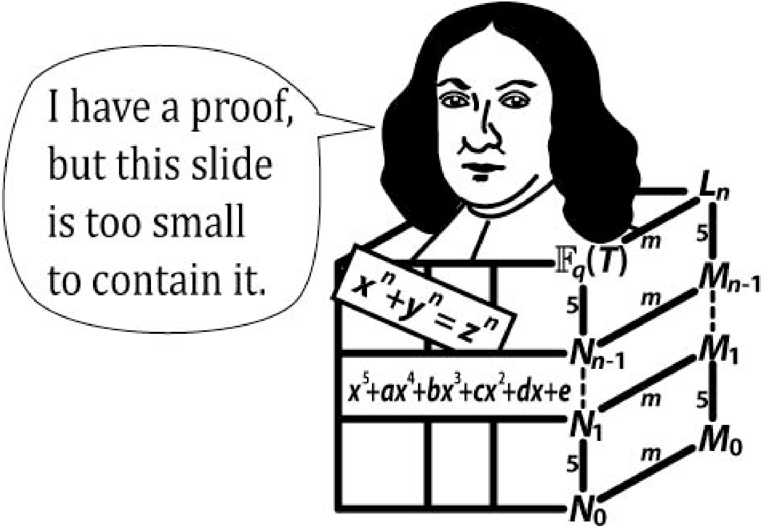
Proving there are infinitely many q

- Recall: We want $\ell\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$ for all p dividing m and $\ell\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$ if $4 \mid m$.
- For p a prime or $p = 4$, define a polynomial $f_p(X) \in \mathbb{Q}(\omega)[X]$ as follows:

$$f_p(X) = \sum_{j=0}^{\ell-1} \sum_{\substack{i=0 \\ i\equiv j}}^{p} \binom{p}{i} (a_j\gamma + a_{j-1}\ell) X^{p-i}$$

  where $a_j = (\zeta^j - \zeta^{-j})/(\zeta - \zeta^{-1})$ and γ is chosen to make f_p Eisenstein for each $p \mid m$.
- The polynomial f_p was chosen so that if f_p has no roots mod q, then $\ell\zeta + \gamma \notin \mathbb{F}_q(\zeta)^p$, and if f_4 has no roots mod q, then $\ell\zeta + \gamma \notin -4\mathbb{F}_q(\zeta)^4$.
- The remainder of the proof is identical to the $\ell = 5$ case.

Thank You


I have a proof, but this slide is too small to contain it.
$x^n + y^n = z^n$
$x^5+ax^4+bx^3+cx^2+dx+e$
$\mathbb{F}_q(T)$
L_n
M_{n-1}
M_1
M_0
N_{n-1}
N_1
N_0
5
m

Analogous Result for Number Fields?

The methods used in the function field case do not generalize to number fields.

Analogous Result for Number Fields?

The methods used in the function field case do not generalize to number fields.

- Function fields have nonzero characteristic, hence we can choose q so that $\mathbb{F}_q$ will have certain useful properties, such as $\omega \in \mathbb{F}_q$ and $\zeta \notin \mathbb{F}_q$. Number fields always have characteristic 0, and the base field is always $\mathbb{Q}$.

Analogous Result for Number Fields?

The methods used in the function field case do not generalize to number fields.

- Function fields have nonzero characteristic, hence we can choose q so that $\mathbb{F}_q$ will have certain useful properties, such as $\omega \in \mathbb{F}_q$ and $\zeta \notin \mathbb{F}_q$. Number fields always have characteristic 0, and the base field is always $\mathbb{Q}$.
- In the function field case, we can construct a chain of fields

$$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = \mathbb{F}_q(T)$$

leading up to the base field $\mathbb{F}_q(T)$. In number fields, the base field $\mathbb{Q}$ has no proper nontrivial subfields.

Analogous Result for Number Fields?

The methods used in the function field case do not generalize to number fields.

- Function fields have nonzero characteristic, hence we can choose q so that $\mathbb{F}_q$ will have certain useful properties, such as $\omega \in \mathbb{F}_q$ and $\zeta \notin \mathbb{F}_q$. Number fields always have characteristic 0, and the base field is always $\mathbb{Q}$.
- In the function field case, we can construct a chain of fields

  $$N_1 \subseteq N_2 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = \mathbb{F}_q(T)$$

  leading up to the base field $\mathbb{F}_q(T)$. In number fields, the base field $\mathbb{Q}$ has no proper nontrivial subfields.
- Tools used in the function field case are unavailable in the number field case, such as the genus of a curve and the Riemann-Hurwitz equation.