Splitting Fields of Generalized Rikuna Polynomials

SMALL REU - Algebraic Number Theory

January 7, 2011

Zev Chonoles, John Cullinan, Hannah Hausman,
Allison M. Pacelli, Sean Pegado, Fan Wei

Our Picture

L to R: John Cullinan, Hannah Hausman, Allison Pacelli, Fan Wei, Sean Pegado, Zev Chonoles

Number Fields

Definition

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

Number Fields

Definition

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

Definition

An **algebraic integer** is a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Number Fields

Definition

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

Definition

An **algebraic integer** is a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Definition

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

Number Fields

Definition

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

Definition

An **algebraic integer** is a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

Definition

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

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

Number Fields

Example

$K = \mathbb{Q}(\sqrt{-6})$

Number Fields

Example

$K = \mathbb{Q}(\sqrt{-6})$

- All elements of K are of the form $a + b\sqrt{-6}$ where $a, b \in \mathbb{Q}$.

Number Fields

Example

$K = \mathbb{Q}(\sqrt{-6})$

- All elements of K are of the form $a + b\sqrt{-6}$ where $a, b \in \mathbb{Q}$.
- The algebraic integers in K are $a + b\sqrt{-6}$ where $a, b \in \mathbb{Z}$.

Number Fields

Example

$K = \mathbb{Q}(\sqrt{-6})$

- All elements of K are of the form $a + b\sqrt{-6}$ where $a, b \in \mathbb{Q}$.
- The algebraic integers in K are $a + b\sqrt{-6}$ where $a, b \in \mathbb{Z}$.
- We write $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

Number Fields

Example

$K = \mathbb{Q}(\sqrt{-6})$

- All elements of K are of the form $a + b\sqrt{-6}$ where $a, b \in \mathbb{Q}$.
- The algebraic integers in K are $a + b\sqrt{-6}$ where $a, b \in \mathbb{Z}$.
- We write $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-6}] & \subset & \mathbb{Q}(\sqrt{-6}) \\ | & & | \\ \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Factorization of Elements of $\mathcal{O}_K$

Remark

In $\mathbb{Z}$, there is unique factorization of integers into primes.

Factorization of Elements of $\mathcal{O}_K$

Remark

In $\mathbb{Z}$, there is unique factorization of integers into primes.

However, in $\mathcal{O}_K$, there is not necessarily unique factorization of algebraic integers into irreducibles.

Factorization of Elements of $\mathcal{O}_K$

Remark

In $\mathbb{Z}$, there is unique factorization of integers into primes.

However, in $\mathcal{O}_K$, there is not necessarily unique factorization of algebraic integers into irreducibles.

Example

Let $K = \mathbb{Q}[\sqrt{-6}]$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

Factorization of Elements of $\mathcal{O}_K$

Remark

In $\mathbb{Z}$, there is unique factorization of integers into primes.

However, in $\mathcal{O}_K$, there is not necessarily unique factorization of algebraic integers into irreducibles.

Example

Let $K = \mathbb{Q}[\sqrt{-6}]$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$.

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

Because -2, 3, and $\sqrt{-6}$ are irreducible in $\mathbb{Z}[\sqrt{-6}]$, these are two distinct factorizations of -6.

Therefore, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ is not a UFD.

Class Group

Definition

Define an equivalence relation $\sim$ on non-zero ideals of $\mathcal{O}_K$ by:

$$I \sim J \text{ if } \alpha I = \beta J \text{ for some non-zero } \alpha, \beta \in \mathcal{O}_K$$

Class Group

Definition

Define an equivalence relation $\sim$ on non-zero ideals of $\mathcal{O}_K$ by:

$$I \sim J \text{ if } \alpha I = \beta J \text{ for some non-zero } \alpha, \beta \in \mathcal{O}_K$$

Theorem

The equivalence classes $[I]$ of $\sim$ form a finite abelian group.

Class Group

Definition

Define an equivalence relation $\sim$ on non-zero ideals of $\mathcal{O}_K$ by:

$$I \sim J \text{ if } \alpha I = \beta J \text{ for some non-zero } \alpha, \beta \in \mathcal{O}_K$$

Theorem

The equivalence classes $[I]$ *of* $\sim$ *form a finite abelian group.*

The group operation is $[I][J] = [IJ]$*, where* IJ *is the usual product of ideals.*

Class Group

Definition

Define an equivalence relation $\sim$ on non-zero ideals of $\mathcal{O}_K$ by:

$$I \sim J \text{ if } \alpha I = \beta J \text{ for some non-zero } \alpha, \beta \in \mathcal{O}_K$$

Theorem

The equivalence classes $[I]$ of $\sim$ form a finite abelian group.

The group operation is $[I][J] = [IJ]$, where IJ is the usual product of ideals.

The identity is the equivalence class of all principal ideals.

Class Group

Definition

Define an equivalence relation $\sim$ on non-zero ideals of $\mathcal{O}_K$ by:

$$I \sim J \text{ if } \alpha I = \beta J \text{ for some non-zero } \alpha, \beta \in \mathcal{O}_K$$

Theorem

The equivalence classes $[I]$ of $\sim$ form a finite abelian group.

The group operation is $[I][J] = [IJ]$, where IJ is the usual product of ideals.

The identity is the equivalence class of all principal ideals.

Definition

This group, denoted Cl_K, is called the **class group** of K.

Class Number

Definition

The **class number**, denoted h_K, is the size of the class group.

Class Number

Definition

The **class number**, denoted h_K, is the size of the class group.

- $\mathcal{O}_K$ has class number 1 if and only if every ideal in $\mathcal{O}_K$ is principal, i.e. $\mathcal{O}_K$ is a PID.

Class Number

Definition

The **class number**, denoted h_K, is the size of the class group.

- $\mathcal{O}_K$ has class number 1 if and only if every ideal in $\mathcal{O}_K$ is principal, i.e. $\mathcal{O}_K$ is a PID.
- $\mathcal{O}_K$ is a UFD if and only if it is a PID.

Class Number

Definition

The **class number**, denoted h_K, is the size of the class group.

- $\mathcal{O}_K$ has class number 1 if and only if every ideal in $\mathcal{O}_K$ is principal, i.e. $\mathcal{O}_K$ is a PID.
- $\mathcal{O}_K$ is a UFD if and only if it is a PID.

Theorem

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

Class Number

Definition

The **class number**, denoted h_K, is the size of the class group.

- $\mathcal{O}_K$ has class number 1 if and only if every ideal in $\mathcal{O}_K$ is principal, i.e. $\mathcal{O}_K$ is a PID.
- $\mathcal{O}_K$ is a UFD if and only if it is a PID.

Theorem

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

Remark

The class number measures the failure of unique factorization in $\mathcal{O}_K$; the larger h_K is, the further $\mathcal{O}_K$ is from being a UFD.

Prime Decomposition

Theorem

For all number fields K, there is unique factorization of ideals into prime ideals in $\mathcal{O}_K$.

Prime Decomposition

Theorem

For all number fields K, there is unique factorization of ideals into prime ideals in $\mathcal{O}_K$.

Let K and L be number fields where L is an extension of K.

Prime Decomposition

Theorem

For all number fields K, there is unique factorization of ideals into prime ideals in $\mathcal{O}_K$.

Let K and L be number fields where L is an extension of K.

$$\begin{array}{ccccc} \mathfrak{p}\mathcal{O}_L & \subset & \mathcal{O}_L & \subset & L \\ | & & | & & | \\ \mathfrak{p} & \subset & \mathcal{O}_K & \subset & K \end{array}$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal in $\mathcal{O}_L$, so it can be uniquely factored into prime ideals in $\mathcal{O}_L$.

Prime Decomposition

Theorem

For all number fields K, there is unique factorization of ideals into prime ideals in $\mathcal{O}_K$.

Let K and L be number fields where L is an extension of K.

$$\begin{array}{ccccc} \mathfrak{q}_1{}^{e_1}\mathfrak{q}_2{}^{e_2}\cdots\mathfrak{q}_r{}^{e_r} & \subset & \mathcal{O}_L & \subset & L \\ | & & | & & | \\ \mathfrak{p} & \subset & \mathcal{O}_K & \subset & K \end{array}$$

Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal in $\mathcal{O}_L$, so it can be uniquely factored into prime ideals in $\mathcal{O}_L$.

Definition

As above, $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1{}^{e_1}\mathfrak{q}_2{}^{e_2}\cdots\mathfrak{q}_r{}^{e_r}$.

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = {\mathfrak{q}_1}^{e_1}{\mathfrak{q}_2}^{e_2}\cdots{\mathfrak{q}_r}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1{}^{e_1}\mathfrak{q}_2{}^{e_2}\cdots\mathfrak{q}_r{}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.
- If $r = [L : K]$, then $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$.

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1{}^{e_1}\mathfrak{q}_2{}^{e_2}\cdots\mathfrak{q}_r{}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.
- If $r = [L : K]$, then $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$.
- If $e_i = 1$ for all i, then $\mathfrak{p}$ is **unramified** in $\mathcal{O}_L$.

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = {\mathfrak{q}_1}^{e_1}{\mathfrak{q}_2}^{e_2}\cdots{\mathfrak{q}_r}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.
- If $r = [L : K]$, then $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$.
- If $e_i = 1$ for all i, then $\mathfrak{p}$ is **unramified** in $\mathcal{O}_L$.
- If $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{[L:K]}$, then $\mathfrak{p}$ is **totally ramified** in $\mathcal{O}_L$.

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = {\mathfrak{q}_1}^{e_1}{\mathfrak{q}_2}^{e_2}\cdots{\mathfrak{q}_r}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.
- If $r = [L : K]$, then $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$.
- If $e_i = 1$ for all i, then $\mathfrak{p}$ is **unramified** in $\mathcal{O}_L$.
- If $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{[L:K]}$, then $\mathfrak{p}$ is **totally ramified** in $\mathcal{O}_L$.

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, so that $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_L = \mathbb{Z}[i]$.

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1{}^{e_1}\mathfrak{q}_2{}^{e_2}\cdots\mathfrak{q}_r{}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.
- If $r = [L : K]$, then $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$.
- If $e_i = 1$ for all i, then $\mathfrak{p}$ is **unramified** in $\mathcal{O}_L$.
- If $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{[L:K]}$, then $\mathfrak{p}$ is **totally ramified** in $\mathcal{O}_L$.

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, so that $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_L = \mathbb{Z}[i]$.

$$\langle 2\rangle\mathcal{O}_L = \langle 1+i\rangle^2 \qquad \langle 3\rangle\mathcal{O}_L = \langle 3\rangle \qquad \langle 5\rangle\mathcal{O}_L = \langle 2+i\rangle\langle 2-i\rangle$$

Splitting, Ramification, Inertia

Definition

As above, $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1{}^{e_1}\mathfrak{q}_2{}^{e_2}\cdots\mathfrak{q}_r{}^{e_r}$.

- If $\mathfrak{p}\mathcal{O}_L$ is prime, then $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$.
- If $r = [L : K]$, then $\mathfrak{p}$ **splits completely** in $\mathcal{O}_L$.
- If $e_i = 1$ for all i, then $\mathfrak{p}$ is **unramified** in $\mathcal{O}_L$.
- If $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^{[L:K]}$, then $\mathfrak{p}$ is **totally ramified** in $\mathcal{O}_L$.

Example

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, so that $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_L = \mathbb{Z}[i]$.

$\langle 2\rangle\mathcal{O}_L = \langle 1+i\rangle^2$	$\langle 3\rangle\mathcal{O}_L = \langle 3\rangle$	$\langle 5\rangle\mathcal{O}_L = \langle 2+i\rangle\langle 2-i\rangle$
(totally ramified)	(inert)	(splits completely)

Galois Theory

Definition

Suppose the polynomial $f \in \mathbb{Q}[x]$ has roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then the **splitting field** of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Definition

Suppose the polynomial $f \in \mathbb{Q}[x]$ has roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then the **splitting field** of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Definition

For any algebraic integer $\alpha \in \mathbb{C}$, we say $\beta \in \mathbb{C}$ is an **algebraic conjugate** of α if there is some irreducible $f \in \mathbb{Q}[x]$ having both α and β as roots.

Galois Theory

Definition

Suppose the polynomial $f \in \mathbb{Q}[x]$ has roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then the **splitting field** of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Definition

For any algebraic integer $\alpha \in \mathbb{C}$, we say $\beta \in \mathbb{C}$ is an **algebraic conjugate** of α if there is some irreducible $f \in \mathbb{Q}[x]$ having both α and β as roots.

Definition

A number field K is **Galois** if $\alpha \in K \Rightarrow$ all conjugates of $\alpha \in K$.

Galois Theory

Definition

Suppose the polynomial $f \in \mathbb{Q}[x]$ has roots $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then the **splitting field** of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

Definition

For any algebraic integer $\alpha \in \mathbb{C}$, we say $\beta \in \mathbb{C}$ is an **algebraic conjugate** of α if there is some irreducible $f \in \mathbb{Q}[x]$ having both α and β as roots.

Definition

A number field K is **Galois** if $\alpha \in K \Rightarrow$ all conjugates of $\alpha \in K$.

Theorem

A number field K is Galois if and only if K is the splitting field of some $f \in \mathbb{Q}[x]$.

Example

$L = \mathbb{Q}(\sqrt[3]{2})$ is not Galois. Because $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2} \in \mathbb{C}$ are the roots of $f = x^3 - 2$, they are algebraic conjugates, but $\zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$ are complex, while $L \subset \mathbb{R}$.

Example

$L = \mathbb{Q}(\sqrt[3]{2})$ is not Galois. Because $\sqrt[3]{2}$, $\zeta\sqrt[3]{2}$, and $\zeta^2\sqrt[3]{2} \in \mathbb{C}$ are the roots of $f = x^3 - 2$, they are algebraic conjugates, but $\zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$ are complex, while $L \subset \mathbb{R}$.

Example

$F = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ is Galois because it is the splitting field of $x^3 - 2$. Note that F contains L.

Galois Theory

Definition

Given a number field K, a bijective homomorphism from K to itself is called an **automorphism** of $K/\mathbb{Q}$.

Galois Theory

Definition

Given a number field K, a bijective homomorphism from K to itself is called an **automorphism** of $K/\mathbb{Q}$.

Theorem

If K is Galois, the automorphisms of $K/\mathbb{Q}$ form a finite group.

Definition

Given a number field K, a bijective homomorphism from K to itself is called an **automorphism** of $K/\mathbb{Q}$.

Theorem

If K is Galois, the automorphisms of $K/\mathbb{Q}$ form a finite group.

The group operation is $\sigma\tau = \sigma \circ \tau$, where $\circ$ is composition.

Galois Theory

Definition

Given a number field K, a bijective homomorphism from K to itself is called an **automorphism** of $K/\mathbb{Q}$.

Theorem

If K is Galois, the automorphisms of $K/\mathbb{Q}$ form a finite group.

The group operation is $\sigma\tau = \sigma \circ \tau$, where $\circ$ is composition.

The identity is the identity homomorphism from K to itself.

Galois Theory

Definition

Given a number field K, a bijective homomorphism from K to itself is called an **automorphism** of $K/\mathbb{Q}$.

Theorem

If K is Galois, the automorphisms of $K/\mathbb{Q}$ form a finite group.

The group operation is $\sigma\tau = \sigma \circ \tau$, where $\circ$ is composition.

The identity is the identity homomorphism from K to itself.

Definition

This group, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the **Galois group** of $K/\mathbb{Q}$.

Galois Theory

Definition

Given a number field K, a bijective homomorphism from K to itself is called an **automorphism** of $K/\mathbb{Q}$.

Theorem

If K is Galois, the automorphisms of $K/\mathbb{Q}$ form a finite group.

The group operation is $\sigma\tau = \sigma \circ \tau$, where $\circ$ is composition.

The identity is the identity homomorphism from K to itself.

Definition

This group, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the **Galois group** of $K/\mathbb{Q}$.

Theorem

If K is Galois, then $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$.

Function Fields

For each prime power $q = p^r$, there is a unique finite field with q elements, denoted $\mathbb{F}_q$.

Function Fields

For each prime power $q = p^r$, there is a unique finite field with q elements, denoted $\mathbb{F}_q$.

Definition

A (global) **function field** K is a finite extension of $\mathbb{F}_q(T)$ where T is a transcendental element over $\mathbb{F}_q$.

Function Fields

For each prime power $q = p^r$, there is a unique finite field with q elements, denoted $\mathbb{F}_q$.

Definition

A (global) **function field** K is a finite extension of $\mathbb{F}_q(T)$ where T is a transcendental element over $\mathbb{F}_q$.

In function fields, the polynomial ring $\mathbb{F}_q[T]$ plays the role of $\mathbb{Z}$.

Function Fields

For each prime power $q = p^r$, there is a unique finite field with q elements, denoted $\mathbb{F}_q$.

Definition

A (global) **function field** K is a finite extension of $\mathbb{F}_q(T)$ where T is a transcendental element over $\mathbb{F}_q$.

In function fields, the polynomial ring $\mathbb{F}_q[T]$ plays the role of $\mathbb{Z}$.

Definition

The **ring of integers** of a function field K, also denoted $\mathcal{O}_K$, is the set of elements of K which are a root of some monic polynomial with coefficients in $\mathbb{F}_q[T]$.

Function Fields

For each prime power $q = p^r$, there is a unique finite field with q elements, denoted $\mathbb{F}_q$.

Definition

A (global) **function field** K is a finite extension of $\mathbb{F}_q(T)$ where T is a transcendental element over $\mathbb{F}_q$.

In function fields, the polynomial ring $\mathbb{F}_q[T]$ plays the role of $\mathbb{Z}$.

Definition

The **ring of integers** of a function field K, also denoted $\mathcal{O}_K$, is the set of elements of K which are a root of some monic polynomial with coefficients in $\mathbb{F}_q[T]$.

$$\begin{array}{ccc} \mathcal{O}_K & \subset & K \\ | & & | \\ \mathbb{F}_q[T] & \subset & \mathbb{F}_q(T) \end{array}$$

Function Fields

Example

$K = \mathbb{F}_q(\sqrt{T+1})$

Function Fields

Example

$K = \mathbb{F}_q(\sqrt{T+1})$

- All elements of K are of the form $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q(T)$.

Function Fields

Example

$K = \mathbb{F}_q(\sqrt{T+1})$

- All elements of K are of the form $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q(T)$.
- The ring of integers in K consists of $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q[T]$.

Example

$K = \mathbb{F}_q(\sqrt{T+1})$

- All elements of K are of the form $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q(T)$.
- The ring of integers in K consists of $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q[T]$.
- We write $\mathcal{O}_K = \mathbb{F}_q[\sqrt{T+1}]$.

Function Fields

Example

$K = \mathbb{F}_q(\sqrt{T+1})$

- All elements of K are of the form $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q(T)$.
- The ring of integers in K consists of $a + b\sqrt{T+1}$ where $a, b \in \mathbb{F}_q[T]$.
- We write $\mathcal{O}_K = \mathbb{F}_q[\sqrt{T+1}]$.

$$\begin{array}{ccc} \mathbb{F}_q[\sqrt{T+1}] & \subset & \mathbb{F}_q(\sqrt{T+1}) \\ | & & | \\ \mathbb{F}_q[T] & \subset & \mathbb{F}_q(T) \end{array}$$

Some Concluding Remarks About Function Fields

Function fields have at least one **prime at infinity.** They “split” and “ramify” in extensions, just like finite primes.

Function fields have at least one **prime at infinity.** They “split” and “ramify” in extensions, just like finite primes.

A function field $K \supseteq \mathbb{F}_q(T)$ can be interpreted as a projective curve over the algebraic closure $\overline{\mathbb{F}_q}$. This curve has a **genus**, which we associate with K.

Some Concluding Remarks About Function Fields

Function fields have at least one **prime at infinity**. They “split” and “ramify” in extensions, just like finite primes.

A function field $K \supseteq \mathbb{F}_q(T)$ can be interpreted as a projective curve over the algebraic closure $\overline{\mathbb{F}_q}$. This curve has a **genus**, which we associate with K.

Many number theory problems are easier in function fields.

Some Concluding Remarks About Function Fields

Function fields have at least one **prime at infinity**. They “split” and “ramify” in extensions, just like finite primes.

A function field $K \supseteq \mathbb{F}_q(T)$ can be interpreted as a projective curve over the algebraic closure $\overline{\mathbb{F}_q}$. This curve has a **genus**, which we associate with K.

Many number theory problems are easier in function fields. Fermat’s Last Theorem can be proven in half a page!

Some Concluding Remarks About Function Fields

Function fields have at least one **prime at infinity**. They "split" and "ramify" in extensions, just like finite primes.

A function field $K \supseteq \mathbb{F}_q(T)$ can be interpreted as a projective curve over the algebraic closure $\overline{\mathbb{F}_q}$. This curve has a **genus**, which we associate with K.

Many number theory problems are easier in function fields. Fermat's Last Theorem can be proven in half a page!

However, looking at the class number of function fields is still very hard.

Some Recent Results

There are infinitely many quadratic function fields over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Ichimura 1999]

Some Recent Results

There are infinitely many quadratic function fields over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Ichimura 1999]

There are infinitely many function fields **of any degree** m over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Pacelli, Rosen]

Some Recent Results

There are infinitely many quadratic function fields over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Ichimura 1999]

There are infinitely many function fields **of any degree** m over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Pacelli, Rosen]

- These fields were explicity constructed using the properties of the *Shanks polynomials*.

The Shanks Polynomials

Definition

The **Shanks polynomials** are a family of cubic polynomials, with a single parameter $u \in \mathbb{Z}$:

$$f(X) = X^3 - 3uX^2 - (3u+3)X - 1.$$

The Shanks Polynomials

Definition

The **Shanks polynomials** are a family of cubic polynomials, with a single parameter $u \in \mathbb{Z}$:

$$f(X) = X^3 - 3uX^2 - (3u+3)X - 1.$$

- These polynomials have several good properties - in fact, their splitting fields are called the *simplest cubic fields*.

The Shanks Polynomials

Definition

The **Shanks polynomials** are a family of cubic polynomials, with a single parameter $u \in \mathbb{Z}$:

$$f(X) = X^3 - 3uX^2 - (3u+3)X - 1.$$

- These polynomials have several good properties - in fact, their splitting fields are called the *simplest cubic fields*.
- They were used by Washington to find infinitely many cubic fields with class number divisible by n.

Some Recent Results

There are infinitely many quadratic function fields over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Ichimura 1999]

There are infinitely many function fields **of any degree** m over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Pacelli, Rosen]

- These fields were explicity constructed using the properties of the *Shanks polynomials*.

Some Recent Results

There are infinitely many quadratic function fields over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Ichimura 1999]

There are infinitely many function fields **of any degree** m over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Pacelli, Rosen]

- These fields were explicity constructed using the properties of the *Shanks polynomials*.

There are infinitely many function fields of any degree m over $\mathbb{F}_q(T)$ with class number indivisible by ℓ, for **any odd prime** ℓ. [SMALL Algebraic Number Theory 2008]

Some Recent Results

There are infinitely many quadratic function fields over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Ichimura 1999]

There are infinitely many function fields **of any degree** m over $\mathbb{F}_q(T)$ with class number indivisible by 3. [Pacelli, Rosen]

- These fields were explicity constructed using the properties of the *Shanks polynomials*.

There are infinitely many function fields of any degree m over $\mathbb{F}_q(T)$ with class number indivisible by ℓ, for **any odd prime** ℓ. [SMALL Algebraic Number Theory 2008]

- These fields were also explicitly constructed, but it required more than just the Shanks polynomials.

The Rikuna Polynomials

The Rikuna polynomials generalize the Shanks polynomials.

The Rikuna Polynomials

The Rikuna polynomials generalize the Shanks polynomials.

For a given ℓ, let ζ_ℓ be an ℓ-th root of unity, and let K be any field with $\zeta_\ell + \zeta_\ell^{-1} \in K$ and $\zeta_\ell \notin K$.

The Rikuna Polynomials

The Rikuna polynomials generalize the Shanks polynomials.

For a given ℓ, let ζ_ℓ be an ℓ-th root of unity, and let K be any field with $\zeta_\ell + \zeta_\ell^{-1} \in K$ and $\zeta_\ell \notin K$.

Definition

Define the polynomials $p, q \in K[x]$ to be

$$p = \frac{\zeta_\ell^{-1}(x - \zeta_\ell)^\ell - \zeta_\ell(x - \zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell}, \quad q = \frac{(x - \zeta_\ell)^\ell - (x - \zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell}.$$

The Rikuna Polynomials

The Rikuna polynomials generalize the Shanks polynomials.

For a given ℓ, let ζ_ℓ be an ℓ-th root of unity, and let K be any field with $\zeta_\ell + \zeta_\ell^{-1} \in K$ and $\zeta_\ell \notin K$.

Definition

Define the polynomials $p, q \in K[x]$ to be

$$p = \frac{\zeta_\ell^{-1}(x - \zeta_\ell)^\ell - \zeta_\ell(x - \zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell}, \quad q = \frac{(x - \zeta_\ell)^\ell - (x - \zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell}.$$

The **Rikuna polynomial** is defined to be

$$r = p - Tq \in K(T)[x].$$

The Rikuna Polynomials

The Rikuna polynomials generalize the Shanks polynomials.

For a given ℓ, let ζ_ℓ be an ℓ-th root of unity, and let K be any field with $\zeta_\ell + \zeta_\ell^{-1} \in K$ and $\zeta_\ell \notin K$.

Definition

Define the polynomials $p, q \in K[x]$ to be

$$p = \frac{\zeta_\ell^{-1}(x-\zeta_\ell)^\ell - \zeta_\ell(x-\zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell}, \quad q = \frac{(x-\zeta_\ell)^\ell - (x-\zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell}.$$

The **Rikuna polynomial** is defined to be

$$r = p - Tq \in K(T)[x].$$

Remark

When $\ell = 3$, the Rikuna polynomial reduces to the Shanks polynomial for $u = T$.

Generalizing Rikuna Polynomials Using Iterations

First, define the rational function $\phi(x) = \frac{p}{q}$.

Generalizing Rikuna Polynomials Using Iterations

First, define the rational function $\phi(x) = \frac{p}{q}$. We can define the polynomials p_m, q_m by writing the m-th iterate of ϕ in lowest terms:

$$\phi^{(m)}(x) = \frac{p_m}{q_m},$$

where $\gcd(p_m, q_m) = 1$.

Generalizing Rikuna Polynomials Using Iterations

First, define the rational function $\phi(x) = \frac{p}{q}$. We can define the polynomials p_m, q_m by writing the m-th iterate of ϕ in lowest terms:

$$\phi^{(m)}(x) = \frac{p_m}{q_m},$$

where $\gcd(p_m, q_m) = 1$.

Definition

The m-th **generalized Rikuna polynomial** is defined to be

$$r_m = p_m - Tq_m \in K(T)[x].$$

This was our main object of study.

Define K_m to be the splitting field of r_m over $K(T)$.

Splitting Fields of Generalized Rikuna Polynomials

Define K_m to be the splitting field of r_m over $K(T)$.

This gives a tower of fields, each containing $K(T)$.

$$\begin{tikzcd}
K_m \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
K(T)
\end{tikzcd}$$

Define K_m to be the splitting field of r_m over $K(T)$.

This gives a tower of fields, each containing $K(T)$.

One thing to study about such towers is the Galois group $\mathrm{Gal}(K_m/K(T))$.

$$\begin{array}{c} K_m \\ | \\ \vdots \\ | \\ K_1 \\ | \\ K(T) \end{array}$$

The Roots of Generalized Rikuna Polynomials

To understand the field K_m, we begin with the roots of the polynomial r_m.

The Roots of Generalized Rikuna Polynomials

To understand the field K_m, we begin with the roots of the polynomial r_m.

The roots of r_m are the solutions to $\phi^{(m)}(x) = T$:

$$r_m = p_m - Tq_m = 0 \iff \phi^{(m)}(x) = \frac{p_m}{q_m} = T$$

The Roots of Generalized Rikuna Polynomials

To understand the field K_m, we begin with the roots of the polynomial r_m.

The roots of r_m are the solutions to $\phi^{(m)}(x) = T$:

$$r_m = p_m - Tq_m = 0 \iff \phi^{(m)}(x) = \frac{p_m}{q_m} = T$$

The iterated nature of the roots gives them the following closed form expression:

The Roots of Generalized Rikuna Polynomials

To understand the field K_m, we begin with the roots of the polynomial r_m.

The roots of r_m are the solutions to $\phi^{(m)}(x) = T$:

$$r_m = p_m - Tq_m = 0 \iff \phi^{(m)}(x) = \frac{p_m}{q_m} = T$$

The iterated nature of the roots gives them the following closed form expression:

Theorem

Define $\alpha(T) = \frac{\zeta_\ell - T}{\zeta_\ell^{-1} - T}$*. For all* $m \geq 1$*, the roots of* r_m *are*

$$\theta_c^{(m)} = \frac{\zeta_\ell - \zeta_{\ell m}^c \sqrt[\ell^m]{\alpha(T)}}{1 - \zeta_\ell \zeta_{\ell m}^c \sqrt[\ell^m]{\alpha(T)}}, \qquad \text{for } 0 \leq c \leq \ell^m - 1.$$

Defining a Useful Field

Instead of finding $\mathrm{Gal}(K_m/K(T))$ directly from these roots, we define an additional tower of fields.

Defining a Useful Field

Instead of finding $\mathrm{Gal}(K_m/K(T))$ directly from these roots, we define an additional tower of fields.

Define the field $L_m = K(T)(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha(T)})$, which contains K_m.

Defining a Useful Field

Instead of finding $\mathrm{Gal}(K_m/K(T))$ directly from these roots, we define an additional tower of fields.

Define the field $L_m = K(T)(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha(T)})$, which contains K_m.

Galois theory tells us how to find $\mathrm{Gal}(K_m/K(T))$ once we know $\mathrm{Gal}(L_m/K(T))$.

Describing $\mathrm{Gal}(L_m/K(T))$

Theorem

Two elements of $\mathrm{Gal}(L_m/K(T))$ *generate the entire group:*

Describing $\mathrm{Gal}(L_m/K(T))$

Theorem

Two elements of $\mathrm{Gal}(L_m/K(T))$ *generate the entire group:*

$$\rho_m : \begin{array}{ccc} \zeta_{\ell m} & \mapsto & \zeta_{\ell m}^{(\ell-1)^{\ell^{v-1}}} \\ \sqrt[\ell m]{\alpha(T)} & \mapsto & \dfrac{1}{\sqrt[\ell m]{\alpha(T)}} \end{array}, \quad \gamma_m : \begin{array}{ccc} \zeta_{\ell m} & \mapsto & \zeta_{\ell m} \\ \sqrt[\ell m]{\alpha(T)} & \mapsto & \zeta_{\ell m} \sqrt[\ell m]{\alpha(T)} \end{array},$$

where $v = \min\{b, m\}$ *and* b *depends only on* K.

Solving for $\mathrm{Gal}(K_m/K(T))$

Having a description of $\mathrm{Gal}(L_m/K(T))$, we find $\mathrm{Gal}(K_m/K(T))$ by restricting automorphisms of L_m to automorphisms of K_m.

Having a description of $\mathrm{Gal}(L_m/K(T))$, we find $\mathrm{Gal}(K_m/K(T))$ by restricting automorphisms of L_m to automorphisms of K_m.

Theorem (SMALL 2010)

For all $m \geq 1$,

$$\mathrm{Gal}(K_m/K(T)) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \rtimes_{\phi_m} \mathbb{Z}/\ell^{m-v}\mathbb{Z},$$

where $\rtimes_{\phi_m}$ is a semi-direct product.

Ramification of Primes of $K(T)$

Ramification of Primes of $K(T)$

Proposition (Cullinan, 2010)

Let $\omega = \zeta_\ell + \zeta_\ell^{-1}$. The discriminant of r_m is given by

$$\operatorname{disc}(r_m) = \pm \ell^{m(\ell^m)} \omega^{(\ell^m - 2)(\ell^m - 1)} (T^2 - \omega T + 1)^{\ell^m - 1}.$$

Ramification of Primes of $K(T)$

Proposition (Cullinan, 2010)

Let $\omega = \zeta_\ell + \zeta_\ell^{-1}$. The discriminant of r_m is given by

$$\mathrm{disc}(r_m) = \pm \ell^{m(\ell^m)} \omega^{(\ell^m-2)(\ell^m-1)} (T^2 - \omega T + 1)^{\ell^m-1}.$$

There are only two primes that can ramify in K_m:

Ramification of Primes of $K(T)$

Proposition (Cullinan, 2010)

Let $\omega = \zeta_\ell + \zeta_\ell^{-1}$. The discriminant of r_m is given by

$$\mathrm{disc}(r_m) = \pm \ell^{m(\ell^m)} \omega^{(\ell^m - 2)(\ell^m - 1)} (T^2 - \omega T + 1)^{\ell^m - 1}.$$

There are only two primes that can ramify in K_m:

- The finite prime $T^2 - \omega T + 1$

Ramification of Primes of $K(T)$

Proposition (Cullinan, 2010)

Let $\omega = \zeta_\ell + \zeta_\ell^{-1}$. The discriminant of r_m is given by

$$\mathrm{disc}(r_m) = \pm \ell^{m(\ell^m)} \omega^{(\ell^m - 2)(\ell^m - 1)} (T^2 - \omega T + 1)^{\ell^m - 1}.$$

There are only two primes that can ramify in K_m:

- The finite prime $T^2 - \omega T + 1$
- The prime at infinity

Ramification of the Finite Prime

Theorem (SMALL 2010)

The prime $T^2 - \omega T + 1$ in $K(T)$ is ramified in K_m.

Theorem (SMALL 2010)

The prime $T^2 - \omega T + 1$ in $K(T)$ is ramified in K_m.

$$
\begin{tikzcd}
 & L_m \arrow[dd, dash, "\ell^m"] \\
K_m \arrow[ur, dash, "2"] \arrow[dd, dash, "\ell^{2m-v}"'] & \\
 & K(T)(\zeta_{\ell^m}) \\
K(T) \arrow[ur, dash, "2\ell^{m-v}"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathfrak{P}_1^{\ell^m}\mathfrak{P}_2^{\ell^m} \arrow[dd, dash] \\
\mathcal{P}^{\ell^m} \arrow[ur, dash] \arrow[dd, dash] & \\
 & \mathfrak{p}_1\mathfrak{p}_2 \\
P \arrow[ur, dash] &
\end{tikzcd}
$$

$$P = T^2 - \omega T + 1, \quad \mathfrak{p}_1 = T - \zeta_\ell, \quad \mathfrak{p}_2 = T - \zeta_\ell^{-1}$$

Ramification of the Prime at Infinity

Theorem (SMALL 2010)

The prime at infinity in $K(T)$ is unramified in K_m.

Theorem (SMALL 2010)

The prime at infinity in $K(T)$ is unramified in K_m.

$$
\begin{tikzcd}
 & L_m \arrow[dd, dash, "\ell^m"] \\
K_m \arrow[ur, dash, "2"] \arrow[dd, dash, "\ell^{2m-v}"'] & \\
 & K(T)(\zeta_{\ell^m}) \\
K(T) \arrow[ur, dash, "2\ell^{m-v}"'] &
\end{tikzcd}
$$

Ramification of the Prime at Infinity

Theorem (SMALL 2010)

The prime at infinity in $K(T)$ is unramified in K_m.

- All primes are unramified in a constant extension, such as $K(T)(\zeta_{\ell^m})/K(T)$.

$$\begin{tikzcd}
 & L_m \arrow[dd, dash, "\ell^m"] \\
K_m \arrow[ur, dash, "2"] \arrow[dd, dash, "\ell^{2m-v}"'] & \\
 & K(T)(\zeta_{\ell^m}) \\
K(T) \arrow[ur, dash, "2\ell^{m-v}"'] &
\end{tikzcd}$$

Ramification of the Prime at Infinity

Theorem (SMALL 2010)

The prime at infinity in $K(T)$ is unramified in K_m.

- All primes are unramified in a constant extension, such as $K(T)(\zeta_{\ell^m})/K(T)$.
- The prime at infinity splits completely in $L_m/K(T)(\zeta_{\ell^m})$.

$$\begin{tikzcd}
 & L_m \arrow[dd, dash, "\ell^m"] \\
K_m \arrow[ur, dash, "2"] \arrow[dd, dash, "\ell^{2m-v}"'] & \\
 & K(T)(\zeta_{\ell^m}) \\
K(T) \arrow[ur, dash, "2\ell^{m-v}"'] &
\end{tikzcd}$$

Theorem (SMALL 2010)

The prime at infinity in $K(T)$ is unramified in K_m.

- All primes are unramified in a constant extension, such as $K(T)(\zeta_{\ell^m})/K(T)$.
- The prime at infinity splits completely in $L_m/K(T)(\zeta_{\ell^m})$.

  Factor the irreducible polynomial from $K(T)(\zeta_{\ell^m})$ to L_m in $K((\frac{1}{T}))(\zeta_{\ell^m})$, the completion of $K(T)(\zeta_{\ell^m})$ with the valuation of the prime of infinity.

$$
\begin{tikzcd}
 & L_m \\
K_m \arrow[ur, dash, "2"] & \\
 & K(T)(\zeta_{\ell^m}) \arrow[uu, dash, "\ell^m"'] \\
K(T) \arrow[uu, dash, "\ell^{2m-v}"] \arrow[ur, dash, "2\ell^{m-v}"'] &
\end{tikzcd}
$$

Riemann-Hurwitz Formula and Genus

The *Riemann-Hurwitz formula* provides a link between the ramification of an extension field and its genus.

Riemann-Hurwitz Formula and Genus

The *Riemann-Hurwitz formula* provides a link between the ramification of an extension field and its genus.

Theorem (Riemann-Hurwitz Formula)

For a finite, separable, geometric extension L/K of function fields, we have:

$$2g_L - 2 \geq [L:K](2g_K - 2) + \sum_{\mathfrak{P}} (e(\mathfrak{P}|P) - 1) \deg_L \mathfrak{P}$$

where the sum is over all primes $\mathfrak{P}$ of L which are ramified in L/K. The inequality is an equality if and only if all ramified primes are tamely ramified.

Riemann-Hurwitz Formula and Genus

The *Riemann-Hurwitz formula* provides a link between the ramification of an extension field and its genus.

Theorem (Riemann-Hurwitz Formula)

For a finite, separable, geometric extension L/K of function fields, we have:

$$2g_L - 2 \geq [L:K](2g_K - 2) + \sum_{\mathfrak{P}} (e(\mathfrak{P}|P) - 1) \deg_L \mathfrak{P}$$

where the sum is over all primes $\mathfrak{P}$ of L which are ramified in L/K. The inequality is an equality if and only if all ramified primes are tamely ramified.

Theorem (SMALL 2010)

For all $m \geq 1$, K_m and L_m have genus 0.

Main Theorem

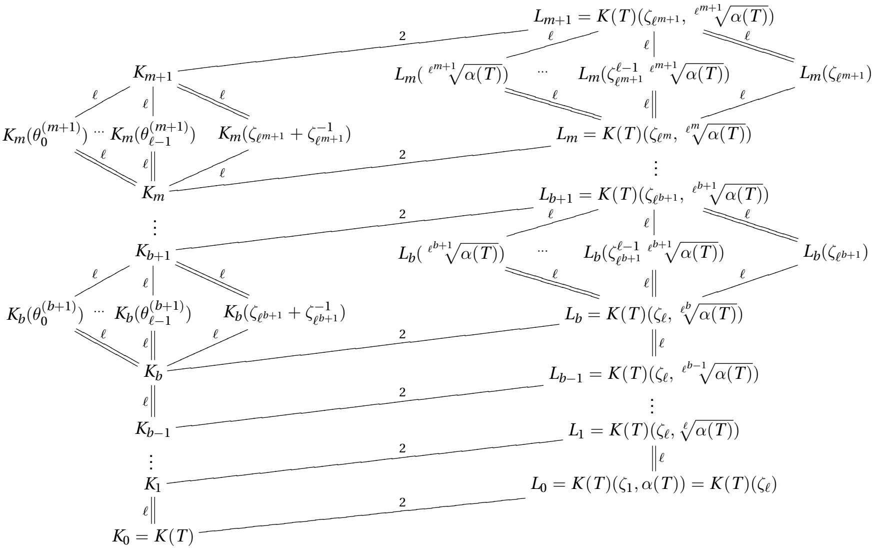
Theorem (SMALL 2010)

Let ℓ be any odd prime and ζ_ℓ be a ℓ-th root of unity. Let K be any perfect field with $\zeta_\ell + \zeta_\ell^{-1} \in K$ and $\zeta_\ell \notin K$.

We can construct explicitly an infinite tower of function fields $K(T) = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots$ such that

- *For all $m \geq 0$, K_{m+1}/K_m is an ℓ-extension.*
- *Exactly one prime of $K(T)$ ramifies in the tower.*
- *For all $m \geq 0$, $h_{K_m} = 1$.*

Towers of K_m and L_m



Ongoing Research, Further Questions

- For any odd integer $\ell \geq 3$,

$$\mathrm{Gal}(K_m/K(T)) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \rtimes \mathbb{Z}/(\ell^m/b_m)\mathbb{Z},$$

where b_m is the size of a certain group of roots of unity in K_m.

Ongoing Research, Further Questions

- For any odd integer $\ell \geq 3$,

$$\mathrm{Gal}(K_m/K(T)) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \rtimes \mathbb{Z}/(\ell^m/b_m)\mathbb{Z},$$

  where b_m is the size of a certain group of roots of unity in K_m. When ℓ is even, the Galois group can be one of four possibilities - which it is depends on the field K.

Ongoing Research, Further Questions

- For any odd integer $\ell \geq 3$,

$$\mathrm{Gal}(K_m/K(T)) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \rtimes \mathbb{Z}/(\ell^m/b_m)\mathbb{Z},$$

  where b_m is the size of a certain group of roots of unity in K_m. When ℓ is even, the Galois group can be one of four possibilities - which it is depends on the field K.

- What can we say about the Galois groups, ramification, genus, and class number when we specialize T to some $\alpha \in K$ (plug in α for T)?

Ongoing Research, Further Questions

- For any odd integer $\ell \geq 3$,

$$\mathrm{Gal}(K_m/K(T)) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \rtimes \mathbb{Z}/(\ell^m/b_m)\mathbb{Z},$$

  where b_m is the size of a certain group of roots of unity in K_m. When ℓ is even, the Galois group can be one of four possibilities - which it is depends on the field K.

- What can we say about the Galois groups, ramification, genus, and class number when we specialize T to some $\alpha \in K$ (plug in α for T)?

- What about polynomials other than Rikuna polynomials, i.e. what if we start with different p and q?

Ongoing Research, Further Questions

- For any odd integer $\ell \geq 3$,

$$\mathrm{Gal}(K_m/K(T)) \simeq \mathbb{Z}/\ell^m\mathbb{Z} \rtimes \mathbb{Z}/(\ell^m/b_m)\mathbb{Z},$$

  where b_m is the size of a certain group of roots of unity in K_m. When ℓ is even, the Galois group can be one of four possibilities - which it is depends on the field K.

- What can we say about the Galois groups, ramification, genus, and class number when we specialize T to some $\alpha \in K$ (plug in α for T)?

- What about polynomials other than Rikuna polynomials, i.e. what if we start with different p and q?

THANK YOU!