On the Splitting Fields of Generalized Rikuna Polynomials

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

Algebraic Number Theory Group - SMALL 2010 - Williams College

Background

Definition. *A **number field** is a finite extension of $\mathbb{Q}$, the set of rational numbers. A **function field** is a finite extension of $\mathbb{F}_q(T)$, where T is a transcendental element over the finite field $\mathbb{F}_q$.*

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

Number Field	Function Field
$\mathcal{O}_K \subset K$	$\mathcal{O}_K \subset K$
$\vert \quad \vert$	$\vert \quad \vert$
$\mathbb{Z} \subset \mathbb{Q}$	$\mathbb{F}_q[T] \subset \mathbb{F}_q(T)$

Note that $\mathcal{O}_K$ is not always a unique factorization domain (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 $\mathbb{Z}[\sqrt{-6}]$. Therefore, $\mathbb{Z}[\sqrt{-6}]$ is not a UFD.

Theorem 1. *Every proper ideal in $\mathcal{O}_K$ 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 that $\langle -6 \rangle = \langle -2 \rangle \langle 3 \rangle = \langle \sqrt{-6} \rangle^2 = \langle 2, \sqrt{-6} \rangle^2 \langle 3, \sqrt{-6} \rangle^2$.

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

Theorem 2. *Define an equivalence relation on the nonzero ideals of $\mathcal{O}_K$ as follows: $I \sim J$ if $aI = bJ$ for some nonzero $a, b \in \mathcal{O}_K$. The equivalence classes form a finite abelian group, called the **class group**, denoted by Cl_K. The cardinality of the class group is called the **class number**, denoted by h_K.*

What does the class number tell us?

- $\mathcal{O}_K$ is a UFD if and only if $h_K = 1$.
- $h_K = 1$ or 2 if and only if the number of irreducibles in every factorization of any given element in $\mathcal{O}_K$ is the same.
- In general, the class number roughly measures how close $\mathcal{O}_K$ is to being a UFD.

Remark. *All function fields have at least one **prime at infinity**. The prime at infinity "splits" and "ramifies" in extensions, just like the finite primes.*

Remark. *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.*

Abstract

Fix a positive integer ℓ, and let K be any field containing $\zeta_\ell + \zeta_\ell^{-1}$ but not ζ_ℓ. Rikuna discovered a polynomial F_ℓ over the function field $K(T)$ whose Galois group is $\mathbb{Z}/\ell\mathbb{Z}$. Komatsu recently generalized classical Kummer theory to cover cyclic extensions arising from F_ℓ.

In our work, for each $m \geq 1$, we introduce the *m-th generalized Rikuna polynomial* r_m. Let K_m be the splitting field of r_m over $K(T)$. It is known that the tower of K_m's ramifies at finitely many primes of $K(T)$.

We study the tower of K_m's. For any odd $\ell \geq 3$, we show that the Galois group $\mathrm{Gal}(K_m/K(T))$ is a semi-direct product $\mathbb{Z}/\ell^m\mathbb{Z} \rtimes \mathbb{Z}/(\ell^m/b_m)\mathbb{Z}$, where b_m is the order of a certain group of roots of unity in K_m. For even $\ell \geq 3$, the Galois group is one of four possibilities, depending on the field K. When $\ell \geq 3$ is prime, we also show that only one prime of $K(T)$ ramifies in the tower of K_m's, and determine this prime explicitly. Then, using the Riemann-Hurwitz formula, we prove that for all $m \geq 1$, K_m is of genus 0, and therefore has class number 1.

Main Results

Fix an integer $\ell \geq 3$, and let K be a field with $\mathrm{char}(K) \nmid \ell$. Let $\overline{K}$ be the algebraic closure of K. Let ζ_ℓ be a primitive ℓ-th root of unity in $\overline{K}$. We assume that $\omega = \zeta_\ell + \zeta_\ell^{-1} \in K$, but $\zeta_\ell \notin K$. Write $K_0 = K(T)$ for an indeterminate T. Define the rational function

$$\phi(X) = \frac{p}{q} = \frac{\zeta_\ell^{-1}(X - \zeta_\ell)^\ell - \zeta_\ell(X - \zeta_\ell^{-1})^\ell}{(X - \zeta_\ell)^\ell - (X - \zeta_\ell^{-1})^\ell} \in K(X),$$

and denote the m-th iteration of $\phi(X)$ by $\phi^m(X)$. Let $p_m, q_m \in K[X]$ be such that $\phi^m(X) = \frac{p_m}{q_m}$ where $\gcd(p_m, q_m) = 1$.

Then we define the **m-th generalized Rikuna polynomial** to be $r_m = p_m - Tq_m \in K_0[X]$. Let K_m be the splitting field of r_m over K_0. Define $b_m \in \mathbb{N}$ to be

$$b_m = |\{\alpha \in K(\zeta_\ell) \mid \alpha^{\ell^m} = 1\}|.$$

Let $a \in \mathbb{N}$ be such that $\zeta_{b_m}^a$ is the conjugate of ζ_{b_m} in $K(\zeta_\ell)$.

Theorem 3 (SMALL 2010)**.** *When ℓ is odd, for each $m \geq 0$ we have that $\mathrm{Gal}(K_m/K(T))$ is generated by $\sigma_m = \rho_m|_{K_m}$ and $\tau_m = \gamma_m|_{K_m}$, where $\rho_m, \gamma_m \in \mathrm{Gal}(L_m/K(T))$ are defined by*

$$\rho_m : \begin{array}{ccc} \zeta_{\ell^m} & \mapsto & \zeta_{\ell^m}^a \\ \sqrt[\ell^m]{\alpha(T)} & \mapsto & \frac{1}{\sqrt[\ell^m]{\alpha(T)}} \end{array}, \qquad \gamma_m : \begin{array}{ccc} \zeta_{\ell^m} & \mapsto & \zeta_{\ell^m} \\ \sqrt[\ell^m]{\alpha(T)} & \mapsto & \zeta_{\ell^m}\sqrt[\ell^m]{\alpha(T)} \end{array}.$$

They satisfy the relations

$$\sigma_m^{\ell^m/b_m} = \mathrm{id}, \quad \tau_m^{\ell^m} = \mathrm{id}, \quad \sigma_m\tau_m = \tau_m^{-a}\sigma_m.$$

Theorem 4 (SMALL 2010)**.** *When $\ell \geq 3$ is odd,*

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

When ℓ is even, $\mathrm{Gal}(K_m/K(T))$ is a similar semi-direct product with two, three, or four generators, depending on ℓ and K. We omit the details here.

Theorem 5 (SMALL 2010)**.** *When $\ell \geq 3$ is prime and K is a perfect field, we can explicitly construct 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 $m \geq 0$, $h_{K_m} = 1$.*

The Proof

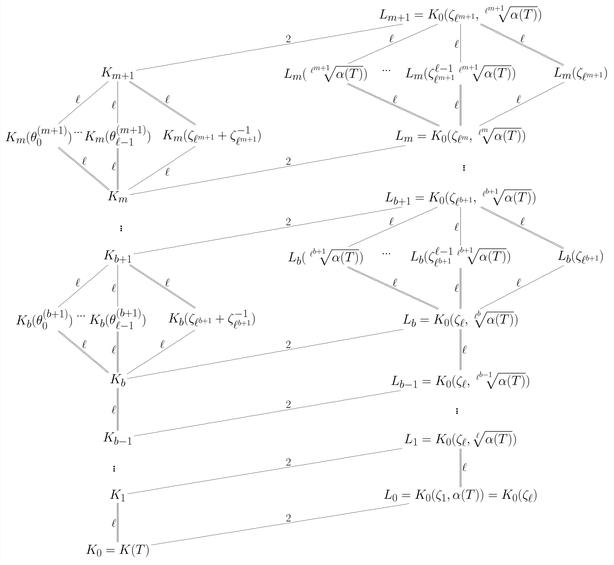
Galois Group of $K_m/K(T)$

To understand the splitting fields K_m, we start with the roots of r_m. The iterated nature of the polynomials gives the roots a closed form:

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

where $\alpha(T) = \frac{\zeta_\ell - T}{\zeta_\ell^{-1} - T}$.

We define $L_m = K(T)(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha(T)})$, an auxiliary field whose Galois group is easier to find. Since $L_m \supseteq K_m$, once the Galois group of L_m is known, we can compute the Galois group of K_m. The following figure shows the relations between L_m and K_m, and some important intermediate fields.



Ramification Behavior and Genus

The discriminant of r_m is

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

where $\omega = \zeta_\ell + \zeta_\ell^{-1}$. The only primes of $K(T)$ that can ramify in K_m are the ones dividing the discriminant, and the prime at infinity.

Theorem 6 (SMALL 2010)**.** *When $\ell \geq 3$ is prime,*

- *The finite prime $T^2 - \omega T + 1$ ramifies in $K_m/K(T)$.*
- *The prime at infinity is unramified in $K_m/K(T)$.*

Applying the

Riemann-Hurwitz Formula. *[1] 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.

we can compute the genus of K_m:

Theorem 7 (SMALL 2010)**.** *When $\ell \geq 3$ is prime, the function field K_m has genus 0, which implies that the class number of K_m is 1.*

Further Questions

- What is the ramification behavior of $K_m/K(T)$, and genus and class number of K_m, for composite $\ell \geq 3$?
- What happens when we specialize T to some $\alpha \in \overline{K}$ (that is, substitute α for T)?
- Will our methods work for other polynomials - e.g., what if we start with different p and q?

References

[1] A. M.Rosen, *Number Theory in Function Fields*, Springer, New York, 2002.

[2] H. Ichimura, *Quadratic function fields whose class numbers are not divisible by three*, Acta Arith. **91** (1999), 181-190.

[3] D. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[4] Y. Rikuna, *On simple families of cyclic polynomials*, Proceedings of the American Mathematical Society. **130** (2002), 2215-2218.

[5] D. Shanks, *The simplest cubic fields*, Math. Comp., 1974

[6] L. Washington, *Class Numbers of the Simplest Cubic Fields*, Math. Comp., 1987