Publications mathématiques de Besançon
Algèbre et théorie des nombres

Z. Chonoles, J. Cullinan, H. Hausman, A.M. Pacelli, S. Pegado, and F. Wei

Arithmetic Properties of Generalized Rikuna Polynomials

2014/1, p. 19-33.

<http://pmb.cedram.org/item?id=PMB_2014____1_19_0>

Publication éditée par le laboratoire de mathématiques de Besançon, UMR 6623 CNRS/UFC

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

ARITHMETIC PROPERTIES OF GENERALIZED RIKUNA POLYNOMIALS

by

Z. Chonoles, J. Cullinan, H. Hausman, A.M. Pacelli, S. Pegado & F. Wei

Abstract. — Fix an integer $\ell \geq 3$. Rikuna introduced a polynomial $r(x,t)$ defined over a function field $K(t)$ whose Galois group is cyclic of order ℓ, where K satisfies some mild hypotheses. In this paper we define the family of *generalized Rikuna polynomials* $\{r_n(x,t)\}_{n\geq 1}$ of degree ℓ^n. The $r_n(x,t)$ are constructed iteratively from the $r(x,t)$. We compute the Galois groups of the $r_n(x,t)$ for odd ℓ over an arbitrary base field and give applications to arithmetic dynamical systems.

Résumé. — Soit $\ell \geq 3$ un nombre entier fixé. Rikuna a défini un polynôme $r(x,t)$ sur un corps de fonctions $K(t)$ dont le groupe de Galois est cyclique d'ordre ℓ, où K satisfait à certaines hypothèses pas très restrictives. Dans cet article, nous définissons la famille des *polynômes de Rikuna généralisés* $\{r_n(x,t)\}_{n\geq 1}$ de degré ℓ^n. Les $r_n(x,t)$ sont construits de manière itérative à partir de $r(x,t)$. Nous calculons les groupes de Galois des $r_n(x,t)$ pour ℓ impair sur un corps de base arbitraire et donnons des applications aux systèmes dynamiques arithmétiques.

1. Introduction

In [**11**], Rikuna introduced a one-parameter family of polynomials with wide-ranging applications to arithmetic. In particular, let $\ell > 2$ be a fixed positive integer (not necessarily prime) and K a field of characteristic coprime to ℓ that does *not* contain a primitive ℓ-th root of unity. Fix an algebraic closure $\overline{K}$ of K and fix a primitive ℓ-th root of unity $\zeta_\ell \in \overline{K}$. Assume further that $\zeta_\ell^+ := \zeta_\ell + \zeta_\ell^{-1} \in K$. Following [**11**], define the polynomials $p(x), q(x) \in K[x]$ by

$$p(x) := \frac{\zeta_\ell^{-1}(x-\zeta_\ell)^\ell - \zeta_\ell(x-\zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1}-\zeta_\ell}$$

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

Let t be an indeterminate over K and define the *degree ℓ Rikuna polynomial* by $r(x,t) = p(x) - t\,q(x) \in K(t)[x]$.

2010 ***Mathematics Subject Classification.*** — 11R32, 11S20.
Key words and phrases. — postcritically finite, Galois group, cyclotomic field.

Rikuna's polynomials have been very well-studied in a number of different guises. For example, when $\ell = 3$, $r(x, s/3)$ is the "simplest cubic" polynomial of Shanks [**13**], which has deep arithmetic implications (see, for example, [**5**], [**8**], and [**12**]). Rikuna originally introduced $r(x,t)$ as a method for creating cyclic Galois extensions of a base field that are not given by Kummer or Artin-Schreier theory (hence the requirement that $\zeta_\ell \notin K$). He proved in [**11**] that for all $\ell \geq 3$, $r(x,t)$ is irreducible over $K(t)$ and has Galois group $\mathbf{Z}/\ell$ over $K(t)$. It was then shown in [**6**] that when ℓ is odd $r(x,t)$ is *generic* in the sense that every $\mathbf{Z}/\ell$-extension of L with $L \supset K$ is obtained as a specialization of $r(x,t)$. When ℓ is even, $r(x,t)$ need not be generic and in [**6**] an algebraic characterization of the non-genericity is given.
When K is a finite field of characteristic coprime to ℓ, the Rikuna polynomials have been used for certain class number constructions. Using the notation above, in [**3**] they consider $\varphi(x) = p(x)/q(x)$ and use a recursive construction to give explicit families of function fields with certain class number indivisibility properties.
Before Rikuna defined the polynomial $r(x,t)$ Shen and Washington introduced in [**14**] and [**15**] an interesting family $\mathcal{P}_n(x,t)$ of polynomials of prime-power degree. There, they take ℓ to be prime and the base field to be $K = \mathbf{Q}(\zeta_\ell^+)$. Then write

$$(x - \zeta_\ell)^{\ell^n} = a_n(x) - \zeta_\ell b_n(x),$$

with $a_n, b_n \in K[x]$. Write $\mathcal{P}_n(x,t) = a_n(x) - (t/\ell^n)\, b_n(x)$ with $t \in \mathcal{O}_K$. The authors call this the ℓ^n-tic polynomial, and it coincides with our "generalized Rikuna polynomial" below (one must replace "t" by "$\ell^n t$", and we consider general $t \in K$). They then determine the splitting fields of the $\mathcal{P}_n(x,t)$, their ramification properties, and the structure of the units. Moreover, they apply Faltings' theorem over K to certain superelliptic curves to show that the number of reducible specializations of their polynomials is finite. In the special case $\ell = 3$, the authors further show in [**15**] that $\mathcal{P}_n(x,t)$ is irreducible for all $t \in \mathbf{Z}$.
In this paper we take a different approach to the polynomials of Rikuna and Shen-Washington by interpreting them in the context of iterated self-maps of $\mathbf{P}^1$. To define them, we follow closely the conventions of [**16**, Ex. 4.9]: if $F, G \in K[X,Y]$ are homogenous polynomials of degree $d \geq 2$ with no common factors, then they give rise to a rational self-map $\varphi = [F,G]$ of $\mathbf{P}^1$. Let $F_0(X,Y) = X$ and $G_0(X,Y) = Y$ and inductively define

$$F_{n+1} = F_n(F(X,Y), G(X,Y)) \qquad \text{and} \qquad G_{n+1} = G_n(F(X,Y), G(X,Y)).$$

Then F_n and G_n have no common factors and the n-th iterate $\varphi^{(n)}$ of φ is given in homogenous coordinates by $\varphi^{(n)} = [F_n, G_n]$.
We now apply this machinery to our setup. Let $P, Q \in K[X,Y]$ be the homogeneous forms of p, q above, respectively. Then P and Q are homogenous of degree ℓ and $\ell - 1$, respectively, and have no common factors (one can show that $\mathrm{Res}(P,Q) = (\zeta_\ell - \zeta_\ell^{-1})^{\ell(\ell-1)} Y^{\ell^2}$). Define $\varphi : \mathbf{P}^1 \to \mathbf{P}^1$ by the pair $[P,Q]$ and the n-th iterate $\varphi^{(n)}$ by $[P_n, Q_n]$, as above. Then $\varphi^{(n)}$ is a rational self-map of $\mathbf{P}^1$ of degree ℓ^n. In affine coordinates we may write $p_n(x) = P_n(x,1)$ and $q_n(x) = Q_n(x,1)$ so that

$$\varphi^{(n)}(x) := \frac{p_n(x)}{q_n(x)}.$$

We define the sequence of *generalized Rikuna polynomials* $\{r_n(x,t) \in K(t)\}_{n \geq 1}$ by

$$r_n(x,t) = p_n(x) - t\, q_n(x),$$

where $r_1(x,t) = r(x,t)$. These polynomials are similar to the ones in [**14**] and [**15**], but we only require that ℓ be odd, not prime, nor do we put any restriction on K except that $\zeta_\ell^+ \in K$ and $\zeta_\ell \notin K$, and we work over the general function field $K(t)$; namely we do not restrict to integral specializations in the special case $K = \mathbf{Q}(\zeta_\ell^+)$. Our main result is the following:

Theorem 1. — *Fix an odd integer $\ell > 2$, let K be a field of characteristic coprime to ℓ, and fix an algebraic closure $\overline{K}$ of K, as well as a primitive ℓ-th root of unity $\zeta_\ell \in \overline{K}$. Suppose further that K does not contain ζ_ℓ but does contain $\zeta_\ell + \zeta_\ell^{-1}$. Let K_n be the splitting field of $r_n(x,t)$ over $K(t)$. Then*

$$\mathrm{Gal}(K_n/K(t)) \simeq \mathbf{Z}/\ell^n \rtimes \mathbf{Z}/(\ell^n/b_n),$$

where b_n is the number of roots of unity in $K(t)(\zeta_\ell)$ of order dividing ℓ^n.

We prove Theorem 1 in Section 3.2 by passing to an auxiliary tower of fields $\{L_n\}$, where $L_n = K_n(\zeta_\ell)$, and determining the Galois group of this tower. Specifically, we show that $\mathrm{Gal}(L_n/K(t))$ has the presentation

$$\mathrm{Gal}(L_n/K(t)) = \langle \rho_n, \gamma_n \mid \rho_n^{2\ell^{n-v_n}} = \gamma_n^{\ell^n} = \mathrm{id},\ \rho_n\gamma_n = \gamma_n^{-(\ell-1)^{\ell^{v_n}-1}}\rho_n \rangle,$$

where v_n is the ℓ-adic valuation of b_n in the statement of the Theorem 1. In particular, we determine $\mathrm{Gal}(K_n/K(t))$ as an explicit quotient of $\mathrm{Gal}(L_n/K(t))$ of index 2. This result builds on that of [**15**] on the Galois groups and shows that the Galois group of $r_n(x,t)$ is relatively small (but non-abelian); recall [**10**, thm. 1] that in characteristic 0, the nth iterate of the generic monic polynomial of degree k is isomorphic to the nth wreath power of S_k. Thus our Galois groups have order ℓ^{2n}/b_n, compared to the maximal size $\ell!^{(\ell^n-1)/(\ell-1)}$. Because we do not assume that K is a number field, our iterative construction has potential applications to class number indivisibility problems in positive characteristic function fields, just as the base function $\varphi(x)$ was used in [**3**].

The $r_n(x,t)$ also have nice applications to arithmetic dynamics. Given a rational self-map F of $\mathbf{P}^1$, one can consider the tower defined as the compositum of the splitting fields of the iterates $F^{(n)}$ of F. For example, when F is the Lattès map associated to an endomorphism Φ of an elliptic curve E, it is a classical result that the tower of splitting fields is finitely-ramified. However, the splitting fields of $K(t)/(F-t)$ may be viewed in the context of the Kummerian fields $K(F^{(-n)}E(K))$, and the arithmetic properties of these fields are much less well-understood.

In the final section of the paper we introduce some of the dynamical properties of the $r_n(x,t)$ in the spirit of [**1**] and [**2**]. In particular, we show that $\varphi(x)$ is postcritically finite and give a simple formula for the discriminant of $r_n(x,t)$. We also raise some questions for future study surrounding the arithmetic of the towers they define.

2. Splitting Fields I – Preliminaries

Fix a positive integer $\ell \geq 3$. In this section we prove some general results on splitting fields associated to the $r_n(x,t)$. We do not distinguish between even and odd ℓ until the next section. We fix once and for all a coherent system $\{\zeta_{\ell^n}\}_{n\geq 1}$ of primitive ℓ^n-th roots of unity; that is, ζ_{ℓ^n} is a primitive ℓ^n-th root of unity and the ℓ-power map sends the level n element to the level $n-1$ element. Recall that $\zeta_\ell \notin K$. We first work out some of the key minimal

polynomials involved in our analysis. Given a field k with algebraic closure $\overline{k}$, we define $\mathrm{Irr}(\pi, k)(x)$ to be the minimal polynomial for $\pi \in \overline{k}$ over k.
Let μ_1 be the group of roots of unity of $K(\zeta_\ell)$. For each $n \geq 1$, let $G_n \subset \mu_1$ be the finite (cyclic) subgroup consisting of elements of order dividing ℓ^n, and let $b_n = \#G_n$. Thus, G_n is generated by a primitive b_n-th root of unity; we fix a generator and write $G_n = \langle \zeta_{b_n} \rangle$. Thus, for all $n \geq 1$, $\zeta_{b_n} \in K(\zeta_\ell)$ and $b_n | \ell^n$. But since $\zeta_\ell \in G_n$ for all n, we have that $\ell | b_n$ for all $n \geq 1$.
Let μ_2 be the group of roots of unity of $K(\zeta_{2\ell})$. For each $n \geq 1$, let $H_n \subset \mu_2$ be the finite (cyclic) subgroup consisting of elements of order dividing ℓ^n, and let $c_n = \#H_n$. A generator of H_n is a primitive c_n-th root of unity, so H_n contains all c_n-th roots of unity, in particular ζ_{c_n}. Thus, for each $n \geq 1$, $\zeta_{c_n} \in K(\zeta_{2\ell})$ and $c_n | \ell^n$. Since $\zeta_\ell \in H_n$ for all $n \geq 1$, we have that $\ell | c_n$ for each $n \geq 1$.

The following lemma, whose proof can be found in [**7**, p. 297], will be needed below.

Lemma 1. — *Let k be a field, $m \geq 2$ an integer, and $a \in k^\times$. Assume that for any prime p with $p \mid m$ we have $a \notin k^p$, and if $4 \mid m$, that $a \notin 4k^4$. Then $x^m - a$ is irreducible in $k[x]$.*

Next we determine three minimal polynomials that will be used extensively in the rest of the paper.

Lemma 2. — *For all integers $\ell > 2$, we have $\mathrm{Irr}(\zeta_\ell, K(t))(x) = x^2 - \zeta_\ell^+ x + 1$. Moreover, if ℓ is odd, or if ℓ is even and $4 | b_n$, then $\mathrm{Irr}(\zeta_{\ell^n}, K(t)(\zeta_\ell))(x) = x^{\ell^n/b_n} - \zeta_{b_n}$. Finally, if ℓ is even and $4 \nmid b_n$, then $\mathrm{Irr}(\zeta_{\ell^n}, K(t)(\zeta_{2\ell}))(x) = x^{\ell^n/c_n} - \zeta_{c_n}$.*

Proof. — Since $\zeta_\ell^+ \in K$ and $\zeta \notin K$, assertion (1) follows. For (2), first note that ζ_{ℓ^n} is a root of the (monic) polynomial $x^{\ell^n/b_n} - \zeta_{b_n} \in K(t)(\zeta)[x]$. Next, for any $d \in \mathbf{Z}_{\geq 0}$, if $\zeta_{db_n} \in K(t)(\zeta_\ell)$, then ζ_{b_n} is a d-th power in $K(t)(\zeta_\ell)$; and if $\zeta_{b_n} = z^d$ for some $z \in K(t)(\zeta_\ell)$, then z is a primitive db_n-th root of unity, so that all db_n-th roots of unity are in $K(t)(\zeta_\ell)$, including ζ_{db_n}. Thus, ζ_{b_n} is a d-th power in $K(t)(\zeta_\ell)$ if and only if $\zeta_{db_n} \in K(t)(\zeta_\ell)$. Therefore, if ζ_{b_n} is a p-th power in $K(t)(\zeta_\ell)$ for some prime p dividing $\frac{\ell^n}{b_n}$, then $\zeta_{pb_n} \in K(t)(\zeta_\ell)$. Because $p \mid \frac{\ell^n}{b_n}$, we have that $pb_n \mid \ell^n$, so that $\zeta_{pb_n} \in G_m$; but the order of ζ_{pb_n} is $pb_n > b_n = \#G_n$, contradiction. Thus, ζ_{b_n} is not a p-th power in $K(t)(\zeta_\ell)$ for any prime p dividing $\frac{\ell^n}{b_n}$, and hence $x^{\ell^n/b_n} - \zeta_{b_n}$ is irreducible.
If ℓ is not odd, we may have $4 \mid (\ell^n/b_n)$, in which case Lemma 1 requires that we also show $\zeta_{b_n} \neq -4z^4$ for all $z \in K(t)(\zeta_\ell)$. We do this when $4 \mid b_n$. Suppose that $4|b_n$, that $4 \mid \ell^n/b_n$, and that $\zeta_{b_n} = -4z^4$ for some $z \in K(t)(\zeta_\ell)$. Then $(2z^2)^2 = -\zeta_{b_n}$, so that $2z^2 = \zeta_4 \zeta_{2b_n}$, or $\zeta_4^3 \zeta_{2b_n}$. Clearly $2z^2 \in K(t)(\zeta_\ell)$, and since $4|b_n$ and $\zeta_{b_n} \in K(t)(\zeta_\ell)$, we have $\zeta_4 \in K(t)(\zeta_\ell)$, whence $\zeta_{2b_n} \in K(t)(\zeta_\ell)$. But since $4 \mid \ell^n/b_n$ we have $4b_n \mid \ell^n$ and thus $2b_n \mid \ell^n$, so that $\zeta_{2b_n} \in G_n$, contradicting the fact that the order of ζ_{2b_n} is $2b_n > b_n = \#G_n$. Thus $x^{\ell^n/b_n} - \zeta_{b_n}$ is irreducible when ℓ is even and $4|b_n$.
For (3), note that $c_1 \mid \ell$ and $\ell | c_1$ so that $c_1 = \ell$. When $n = 1$ it is clear that the minimal polynomial for ζ_ℓ over $K(t)(\zeta_{2\ell})$ is $x - \zeta_\ell$, as claimed. Now consider $n \geq 2$. Since ℓ is even we have that $4|\ell^n$; thus if ζ_4 were an element of $K(t)(\zeta_\ell)$, we would have $\zeta_4 \in G_n$ and thus $4 \mid b_n$. Therefore, our hypothesis implies $\zeta_4 \notin K(t)(\zeta_\ell)$. However, because ℓ is even, we do have that

$4 \mid 2\ell$, and thus $\zeta_4 \in K(t)(\zeta_{2\ell})$. The arguments from (2) now go through exactly as before, with $K(t)(\zeta_\ell)$ replaced by $K(t)(\zeta_{2\ell})$. □

Lemma 3. — *For each $n \geq 2$ the degree of the Galois extension $K(t)(\zeta_{\ell^n})/K(t)$ is*

$$[K(t)(\zeta_{\ell^n}) : K(t)] = \begin{cases} 2\ell^n/b_n & \text{if } \ell \text{ is odd or } \ell \text{ is even with } 4 \mid b_n \\ 4\ell^n/c_n & \text{if } \ell \text{ is even and } 4 \nmid b_n. \end{cases}$$

Remark. Note that $[K(t)(\zeta_\ell) : K(t)] = \deg \operatorname{Irr}(\zeta_\ell, K(t))(x) = 2$.

Proof. — Suppose that ℓ is odd or that ℓ is even and $4 \mid b_n$. Since $K(t)(\zeta_\ell) \subset K(T)(\zeta_{\ell^n})$, we have

$$\begin{aligned} [K(t)(\zeta_{\ell^n}) : K(t)] &= [K(t)(\zeta_{\ell^n}) : K(t)(\zeta_\ell)][K(t)(\zeta_\ell) : K(t)] \\ &= \deg \operatorname{Irr}(\zeta_{\ell^n}, K(t)(\zeta_\ell))(x) \cdot 2 = 2\ell^n/b_n. \end{aligned}$$

On the other hand, if ℓ is even and $4 \nmid b_n$, then $K(t)(\zeta_{2\ell}) \subset K(t)(\zeta_{\ell^n})$ (recall $n \geq 2$). Thus

$$\begin{aligned} [K(t)(\zeta_{\ell^n}) : K(t)] &= [K(t)(\zeta_{\ell^n}) : K(t)(\zeta_{2\ell})][K(t)(\zeta_{2\ell}) : K(t)(\zeta_\ell)][K(t)(\zeta_\ell) : K(t)] \\ &= \deg \operatorname{Irr}(\zeta_{\ell^n}, K(t)(\zeta_{2\ell}))(x) \cdot [K(t)(\zeta_{2\ell}) : K(t)(\zeta_\ell)] \cdot 2 \\ &= 2\ell^n/c_n \cdot [K(t)(\zeta_{2\ell}) : K(t)(\zeta_\ell)]. \end{aligned}$$

Note that $\zeta_{2\ell}$ is a root of $x^2 - \zeta_\ell \in K(t)(\zeta_\ell)[x]$, so that $[K(t)(\zeta_{2\ell}) : K(t)(\zeta_\ell)] \leq 2$. The proof of Lemma 2 shows that $\zeta_4 \notin K(t)(\zeta_\ell)$, but that $\zeta_4 \in K(t)(\zeta_{2\ell})$, so that $[K(t)(\zeta_{2\ell}) : K(t)(\zeta_\ell)] > 1$. Therefore the degree of the field extension $[K(t)(\zeta_{2\ell}) : K(t)(\zeta_\ell)] = 2$, which completes the proof of the lemma. □

For each $n \geq 1$ we know that $\ell \mid b_n$ and that $b_n \mid \ell^n$, so given the prime factorization of ℓ:

$$\ell = 2^{e_0} p_1^{e_1} \cdots p_m^{e_m},$$

the prime factorization of b_n has the form $b_n = 2^{a_0} p_1^{a_1} \cdots p_m^{a_m}$ for some $e_i \leq a_i \leq ne_i$. Also note that because $\ell \mid b_n$, we have $K(t)(\zeta_\ell) \subset K(t)(\zeta_{b_n})$. Moreover, since $\zeta_{b_n} \in K(t)(\zeta_\ell)$ we have the equality of fields $K(t)(\zeta_{b_n}) = K(t)(\zeta_\ell)$.

3. Splitting Fields II – Odd ℓ

In this section and for the rest of the paper we specialize to the case of odd ℓ. We work out the splitting fields of the $r_n(x,t)$ as well as describe an auxiliary tower of fields. We are ultimately interested in the Galois groups of the $r_n(x,t)$ and this auxiliary tower will aid in determining those groups.

Lemma 4. — *Suppose ℓ is odd and recall that ζ_{b_n} is quadratic over $K(t)$ for each $n \geq 1$. Then for each $n \geq 1$ the conjugate of ζ_{b_n} over $K(t)$ is $\zeta_{b_n}^{-1}$. Hence $\zeta_{b_n}^+ \in K(t)$.*

Proof. — Let ψ be the non-trivial automorphism of $K(t)(\zeta_\ell)/K(t)$ so that $\psi(\zeta_\ell) = \zeta_\ell^{-1}$. Let $\zeta_{b_n}^a = \psi(\zeta_{b_n})$ be the conjugate of ζ_{b_n} over $K(t)$. Because ψ^2 is trivial, it must be the case that $a^2 \equiv 1 \pmod{b_n}$, whence $a^2 \equiv 1 \pmod{p_i^{a_i}}$ for all i, where the p_i are the prime divisors of ℓ

as above. By assumption, the p_i are all odd and it then follows that $a \equiv \pm 1 \pmod{p_i^{a_i}}$ for all i. Now,

$$\zeta_\ell^{-1} = \psi(\zeta_\ell) = \psi(\zeta_{b_n}^{b_n/\ell}) = (\zeta_{b_n}^a)^{b_n/\ell} = \zeta_\ell^a,$$

so that $a \equiv -1 \pmod{\ell}$. Thus, $a \equiv -1 \pmod{p_i^{e_i}}$ for all i. Together with $a \equiv \pm 1 \pmod{p_i^{a_i}}$, we must have that $a \equiv -1 \pmod{p_i^{a_i}}$ for all i. By the Chinese Remainder Theorem, we have that $a \equiv -1 \pmod{b_n}$ so that $\psi(\zeta_{b_n}) = \zeta_{b_n}^{-1}$. □

Lemma 5. — *If ℓ is odd, then for each $n \geq 1$, $\mathrm{Irr}(\zeta_{\ell^n}, K(t))(x) = x^{2\ell^n/b_n} - \zeta_{b_n}^+ x^{\ell^n/b_n} + 1$.*

Proof. — Since $\zeta_{b_n}^+ \in K(t)$, we have that $x^{2\ell^n/b_n} - \zeta_{b_n}^+ x^{\ell^n/b_n} + 1 \in K(t)[x]$. This polynomial is monic and ζ_{ℓ^n} is a root. Thus

$$\mathrm{Irr}(\zeta_{\ell^n}, K(t))(x) \mid (x^{2\ell^n/b_n} - \zeta_{b_n}^+ x^{\ell^n/b_n} + 1).$$

However, $\deg \mathrm{Irr}(\zeta_{\ell^n}, K(t))(x) = [K(t)(\zeta_{\ell^n}) : K(t)] = [K(t)(\zeta_{\ell^n}) : K(t)(\zeta_\ell)][K(t)(\zeta_\ell) : K(t)] = 2\ell^n/b_n$, by (1) and (2) of this Lemma. Since $x^{2\ell^n/b_n} - \zeta_{b_n}^+ x^{\ell^n/b_n} + 1$ is monic, it must be the minimal polynomial. □

Corollary 1. — *The extensions $K(t)(\zeta_{\ell^n})/K(t)$ are Galois with degree $2\ell^n/b_n$.*

Define the rational function

$$\alpha(x) = \frac{\zeta_\ell - x}{\zeta_\ell^{-1} - x} \in K(t)(\zeta_\ell)(x).$$

Lemma 6. — *We have the equality of fields $K(t)(\zeta_\ell) = K(t)(\alpha(t))$.*

Proof. — It suffices to show that $\zeta_\ell \in K(t)(\alpha(t))$. But since $\zeta^+ \in K$, we can write

$$\zeta_\ell = \frac{\zeta^+\alpha(t) - t(\alpha(t) - 1)}{\alpha(t) + 1}.$$

Thus, $\zeta_\ell \in K(t)(\alpha(t))$, as desired. □

Define the polynomial

$$A(x) = x^2 - \left(2 + \frac{(\zeta_\ell^+)^2 - 4}{t^2 - \zeta_\ell^+ t + 1}\right) x + 1 \in K(t)[x].$$

Lemma 7. — *The minimal polynomial for $\alpha(t)$ over $K(t)$ is $A(x)$.*

Proof. — Note that $\alpha(t)^{\pm 1}$ are the roots of $A(x)$. Since $[K(t)(\alpha(t)) : K(t)] = [K(t)(\zeta_\ell) : K(t)] = 2$, and $A(x)$ is monic, the lemma follows. □

Next, we characterize the roots of $r_n(x,t)$. Let $\sqrt[\ell]{\alpha(t)} \in \overline{K(t)}$ be an ℓth root of $\alpha(t)$ and for each positive integer d, fix a compatible system of ℓ^dth roots $\sqrt[\ell^d]{\alpha(t)} \in \overline{K(t)}$ of $\alpha(t)$ in the sense that

$$\sqrt[\ell^d]{\alpha(t)}^{\ell} = \sqrt[\ell^{d-1}]{\alpha(t)}.$$

Let K_n be the splitting field of $r_n(x,t)$ over $K(t)$. Because of the cumbersome notation involving the surds, we will set the following notation for the remainder of the paper. Set

$$\beta_n(t) := \sqrt[\ell^n]{\alpha(t)}$$

so that $\{\beta_n(t)\}_{n\geq 1}$ forms a compatible system of ℓ-power roots as well.

Lemma 8. — *For all $n \geq 1$, the minimal polynomial for $\beta_n(t)$ over $K(t)(\zeta_{\ell^n})$ is $x^{\ell^n} - \alpha(t)$.*

Proof. — By Lemma 6, $\alpha(t) \in K(t)(\zeta_{\ell^n})$ for all $n \geq 1$. It is also clear that $x^{\ell^n} - \alpha(t)$ is monic and has $\beta_n(t)$ as a root. Note that $K(t)(\zeta_{\ell^n}) = K(\zeta_{\ell^n})(t)$, so that any element of $K(t)(\zeta_{\ell^n})$ is of the form $\frac{f}{g}$ for relatively prime $f, g \in K(\zeta_{\ell^n})[t]$. Also note that $\alpha(t) = \frac{\zeta_\ell - t}{\zeta_\ell^{-1} - t}$ is in lowest terms, i.e. $\gcd(\zeta_\ell - t, \zeta_\ell^{-1} - t) = 1$; any non-constant $h \in K(\zeta_{\ell^n})[t]$ dividing both $\zeta_\ell - t$ and $\zeta_\ell^{-1} - t$ would divide $(\zeta_\ell - t) - (\zeta_\ell^{-1} - t) = \zeta_\ell - \zeta_\ell^{-1} \in K(\zeta_{\ell^n})$, a contradiction. If $\alpha(t)$ is not an ℓ-th power in $K(t)(\zeta_{\ell^n})$, i.e. $\alpha(t) \notin (K(t)(\zeta_{\ell^n}))^\ell$, then $x^{\ell^n} - \alpha(t)$ is irreducible, by Lemma 1.

Suppose that $\alpha(t) = (\frac{f}{g})^\ell$ for some $\frac{f}{g} \in K(t)(\zeta_{\ell^n})$. Then $f^\ell = \zeta_\ell - t$ and $g^\ell = \zeta_\ell^{-1} - t$, up to multiplication by a unit. But if $\deg(f) = 0$ then $\deg(f^\ell) = 0$, and if $\deg(f) \geq 1$ then $\deg(f^\ell) \geq \ell$, while $\deg(\zeta_\ell - t) = 1$ (likewise with g). Thus $\alpha(t)$ is not an ℓ-th power in $K(t)(\zeta_{\ell^n})$, so that $x^{\ell^n} - \alpha(t)$ is irreducible. □

Proposition 3.1. — *Fix an integer $n \geq 1$. Then the roots of $r_n(x,t)$ are given by*

$$\theta_c^{(n)} = \frac{\zeta_\ell - \zeta_{\ell^n}^c \beta_n(t)}{1 - \zeta_\ell \zeta_{\ell^n}^c \beta_n(t)},$$

for all integers $0 \leq c \leq \ell^n - 1$.

Proof. — When $n = 1$, $z \in \overline{K(t)}$ is a root of $r(x,t)$ if and only if $\phi(z) = t$, which is true if and only if

$$\zeta^{-1}(z-\zeta)^\ell - \zeta(z-\zeta^{-1})^\ell = t((z-\zeta)^\ell - (z-\zeta^{-1})^\ell) \iff \left(\frac{z-\zeta_\ell}{z-\zeta_\ell^{-1}}\right)^\ell = \frac{\zeta_\ell - t}{\zeta_\ell^{-1} - t} = \alpha(t)$$
$$\iff \frac{z-\zeta_\ell}{z-\zeta_\ell^{-1}} = \zeta_\ell^N \beta_1(t)$$

for some $0 \leq N \leq \ell - 1$. Rearranging and reindexing, the ℓ roots of $r(x,t)$ are given by

$$\left\{ \frac{\zeta_\ell - \zeta_\ell^c \beta_1(t)}{1 - \zeta_\ell \zeta_\ell^c \beta_1(t)} \ : \ 0 \leq c \leq \ell - 1 \right\},$$

as claimed.
By induction, $\phi^{(n+1)}(z) = t$ if and only if $\phi(z) = \theta_c^{(n)}$ for some $0 \leq c \leq \ell^n - 1$. For each value of c, $\phi(z) = \theta_c^{(n)}$ if and only if

$$z = \frac{\zeta_\ell - \zeta_\ell^d \beta_1(\theta_c^{(n)})}{1 - \zeta_\ell \zeta_\ell^d \beta_(\theta_c^{(n)}}$$

for some $0 \leq d \leq \ell - 1$. Note that $\alpha(\theta_c^{(n)}) = \zeta_\ell \zeta_{\ell^n}^c \beta_n(t)$, so we may rewrite z as

$$z = \frac{\zeta_\ell - \zeta_{\ell^{n+1}}^{d\ell^n + c + \ell^{n-1}} \beta_{n+1}(t)}{1 - \zeta_\ell \zeta_{\ell^{n+1}}^{d\ell^n + c + \ell^{n-1}} \beta_{n+1}(t)}.$$

Because

$$\{\zeta_{\ell^{n+1}}^{d\ell^n+c+\ell^{n-1}} \ : \ 0 \le d \le \ell-1, 0 \le c \le \ell^{n-1}\} = \{\zeta_{\ell^{n+1}}^{e} \ : \ 0 \le e \le \ell^{m+1}-1\},$$

and because, for each n, the $\theta_c^{(n)}$ are distinct, the the roots of $r_{n+1}(x,t)$ are precisely as claimed. This proves the proposition. □

For each $n \ge 0$, we define K_n to be the splitting field of $r_n(x,t)$ (we define $p_0 = x$ and $q_0 = 1$ so that $r_0(x,t) = x - t$ and $K_0 = K(t)$). Proposition 3.1 shows that for each n, the fields K_n are Galois over $K(t)$ since they are the splitting fields of separable polynomials. Moreover, for each n, we have $K_n \subset K_{n+1}$ because the roots of $\phi^{(n)}(x)$ are the images under ϕ of the roots of $\phi^{(n+1)}(x)$.

3.1. The auxiliary tower $\{L_n\}$. — For each $n \ge 0$ we define the field L_n to be $L_n = K(t)(\zeta_{\ell^n}, \beta_n(t))$. Thus,

$$L_0 = K(t)(\zeta_1, \sqrt[1]{\alpha(t)}) = K(t)(\alpha(t)) = K(t)(\zeta_\ell).$$

In Appendix A, we give a field diagram of the K_n and the L_n towers.

Lemma 9. — *For each $n \ge 0$, $K_n \subset L_n$.*

Proof. — Since $K_0 = K(t) \subset K(t)(\zeta_\ell) = L_0$, it suffices to consider $n > 0$. But for each c with $0 \le c \le \ell^n - 1$, the field L_n contains the elements

$$\theta_c^{(n)} = \frac{\zeta_\ell - \zeta_{\ell^n}^c \beta_n(t)}{1 - \zeta_\ell \zeta_{\ell^n}^c \beta_n(t)},$$

which generate $K_n/K(t)$. This proves the lemma. □

For ease of notation in the subsequent sections, we define the positive integer v_n by $v_n = \nu_\ell(b_n)$, where $\nu_\ell : \mathbf{Z} \longrightarrow \mathbf{Z}_{\ge 0} \cup \{\infty\}$ is the ℓ-adic valuation.

Lemma 10. — *For each $n \ge 0$, the extension $L_n/K(t)$ is Galois with degree $2\ell^{2n-v_n}$.*

Proof. — Because $K(t) \subset K(t)(\zeta_{\ell^n}) \subset L_n$, it follows that

$$[L_n : K(t)] = [L_n : K(t)(\zeta_{\ell^n})][K(t)(\zeta_{\ell^n}) : K(t)] = \ell^n \cdot 2\ell^n / b_n = 2\ell^{2n-v_n}.$$

By Lemma 7, the minimal polynomial for $\alpha(t)$ over $K(t)$ is $A(x)$. Let F be the splitting field of $B(x) = A(x^{\ell^n})$. Note that $z \in \overline{K(t)}$ is a root of B if and only if z^{ℓ^n} is a root of A, *i.e.* $z^{\ell^n} = \alpha(t)^{\pm 1}$. Thus, the roots of B are precisely $\zeta_{\ell^n}^c \beta_n(t)^{\pm 1}$, for $0 \le c \le \ell^n - 1$. Because F contains both $\beta_n(t)$ and $\zeta_{\ell^n}\beta_n(t)$, it contains ζ_{ℓ^n}. Thus $L_n \subset F$. On the other hand, since L_n contains ζ_{ℓ^n} and $\beta_n(t)$, it contains $\zeta_{\ell^n}^c \beta_n(t)^{\pm 1}$. Thus $F = L_n$ and it follows that L_n is Galois over $K(t)$. □

3.2. Galois groups. — In this section we determine the Galois groups of the field extensions $K_n/K(t)$ keeping the convention that ℓ be odd. We begin with an explicit description of the Galois groups of the field extensions $L_n/K(t)$.

Proposition 3.2. — *For all $n \geq 0$, the Galois groups $\mathrm{Gal}(L_n/K(t))$ are generated by the automorphisms ρ_n and γ_n, which are determined by*

$$\rho_n(\zeta_{\ell^n}) = \zeta_{\ell^n}^{(\ell-1)^{\ell^{bn-1}}} \qquad \gamma_n(\zeta_{\ell^n}) = \zeta_{\ell^n}$$
$$\rho_n(\beta_n(t)) = \beta_n(t)^{-1} \qquad \gamma_n(\beta_n(t)) = \zeta_{\ell^n}\beta_n(t).$$

Moreover, they satisfy the relations

$$\rho_n^{2\ell^{n-v_n}} = \gamma_n^{\ell^n} = \mathrm{id}, \qquad \rho_n\gamma_n = \gamma_n^{-(\ell-1)^{\ell^{v_n-1}}}\rho_n.$$

Proof. — The extensions $K(t)(\zeta_{\ell^n})/K(t)$ and $L_n/K(t)$ are Galois, and by Lemma 8 we have

$$[L_n : K(t)(\zeta_{\ell^n})] = \ell^n.$$

Thus, each automorphism of $K(t)(\zeta_{\ell^n})/K(t)$ extends to ℓ^n automorphisms of $L_n/K(t)$. It is easy to check that the mapping

$$\widetilde{\rho_n} : \zeta_{\ell^n} \mapsto \zeta_{\ell^n}^{(\ell-1)^{\ell^{(v_n-1)}}}$$

is an element of $\mathrm{Gal}(K(t)(\zeta_{\ell^n})/K(t))$. Since ℓ is odd, the congruence

$$(\ell-1)^{\ell^{v_n-1}} \equiv (-1)^{\ell^{v_n-1}} \equiv -1 \pmod{\ell}$$

holds, whence

$$\widetilde{\rho_n}(\zeta_\ell) = \widetilde{\rho_n}(\zeta_{\ell^n}^{\ell^{n-1}}) = \widetilde{\rho_n}(\zeta_{\ell^n})^{\ell^{n-1}} = \left(\zeta_{\ell^n}^{(\ell-1)^{\ell^{(v_n-1)}}}\right)^{\ell^{n-1}} = \zeta_\ell^{(\ell-1)^{\ell^{v_n-1}}} = \zeta_\ell^{-1}.$$

Therefore, $\widetilde{\rho_n}$ must act on $\alpha(t)$ as follows:

$$\widetilde{\rho_n}(\alpha(t)) = \widetilde{\rho_n}\left(\frac{\zeta_\ell - t}{\zeta_\ell^{-1} - t}\right) = \frac{\zeta_\ell^{-1} - t}{\zeta_\ell - t} = \alpha(t)^{-1}.$$

It follows that any extension of $\widetilde{\rho_n}$ to an element of $\mathrm{Gal}(L_n/K(t))$ must send $\beta_n(t)$ to $\zeta_{\ell^n}^d\beta_n(t)$, for some $0 \leq d \leq \ell^n - 1$. An extension of any automorphism is determined by its action on $\beta_n(t)$ by definition of the field L_n. We have thus identified all ℓ^n extensions of $\widetilde{\rho_n}$. The ρ_n defined in the statement of the Proposition is indeed an automorphism of $L_n/K(t)$ because it is one of the extensions of $\widetilde{\rho_n}$. By Lemma 8 it is also clear that $\zeta_{\ell^n}\beta_n(t)$ is a conjugate of $\beta_n(t)$ over $K(t)(\zeta_{\ell^n})$, whence the map γ_n defined in the statement of the Proposition is an automorphism of $L/K(t)$. It is clear that the order of γ_n is ℓ^n and the order of ρ_n is $2\ell^{n-v_n}$ because $\rho_n^d = \mathrm{id}$ if and only if

$$\zeta_{\ell^n} = \rho_n^d(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\left((\ell-1)^{\ell^{v_n-1}}\right)^d}, \text{ and}$$
$$\beta_n(t) = \rho_n^d(\beta_n(t)) = \left(\beta_n(t)^{-1}\right)^d,$$

which is the case if and only if

$$1 \equiv \left((\ell-1)^{\ell^{v_n-1}}\right)^d = (\ell-1)^{d\ell^{v_n-1}} \pmod{\ell^n},$$

and d is even. But this is true if and only if $2\ell^{n-v_n} \mid d$, and because $2\ell^{n-v_n}$ is even, it is the least $d \geq 1$ such that $\rho_n^d = \mathrm{id}$.

Because an automorphism of $L_n/K(t)$ is determined by its action on ζ_{ℓ^n} and $\beta_n(t)$, it suffices to check the relation $\rho_n\gamma_n = \gamma_n^{-(\ell-1)^{\ell^{v_n-1}}}\rho_n$ on these two elements. This is a routine computation which we omit. Thus, the subgroup of $\mathrm{Gal}(L_n/K(t))$ generated by ρ_n and γ_n consists of the (possibly non-distinct) automorphisms ρ_n^x, γ_n^y, where $0 \leq x \leq 2\ell^{n-v_n}$ and $0 \leq y \leq \ell^n - 1$. It is also not difficult to show that these automorphisms are all distinct. □

Theorem 2. — *For all $n \geq 0$ the Galois group $\mathrm{Gal}(K_n/K(t))$ is generated by $\sigma_n := \rho_n|_{K_n}$ and $\tau_n := \gamma_n|_{K_n}$. They satisfy the relations*

$$\sigma_n^{\ell^{n-v_n}} = \tau_n^{\ell^n} = \mathrm{id},\ \sigma_n\tau_n = \tau_n^{-(\ell-1)^{\ell^{v_n-1}}}\sigma_n.$$

Granting the theorem for a moment, the description of $\mathrm{Gal}(K_n/K(t))$ in terms of generators and relations lends itself to a description as a semidirect product:

$$\mathrm{Gal}(K_n/K(t)) \simeq \mathbf{Z}/\ell^n\mathbf{Z} \rtimes_{\phi_n} \mathbf{Z}/(\ell^{n-v_n})\mathbf{Z},$$

where $\phi_n : \mathbf{Z}/(\ell^{n-v_n})\mathbf{Z} \longrightarrow \mathrm{Aut}(\mathbf{Z}/\ell^n\mathbf{Z})$ is given by $\phi_n(1) = (1 \mapsto (-1)(\ell-1)^{\ell^{v_n-1}})$. Note that ϕ_n is injective, *i.e.* $(1 \mapsto (-1)(\ell-1)^{\ell^{v_n-1}})$ is always an automorphism of $\mathbf{Z}/\ell^n\mathbf{Z}$ of order ℓ^{n-v_n} because the order of $-(\ell-1)^{\ell^{v_n-1}}$ modulo ℓ^n is ℓ^{n-v_n}.

Proof of Theorem 2. — Basic Galois theory tells us that the quotient map

$$\mathrm{Gal}(L_n/K(t)) \longrightarrow \mathrm{Gal}(K_n/K(t))$$

is given by restriction; thus $\mathrm{Gal}(K_n/K(t))$ is generated by σ_n and τ_n. Because σ_n and τ_n are the restrictions of ρ_n and γ_n, respectively, they satisfy the same relation. Since

$$\rho_n^{\ell^{n-v_n}}(\zeta_{\ell^n}) = \zeta_{\ell^n}^{\left((\ell-1)^{\ell^{v_n-1}}\right)^{\ell^{n-v_n}}} = \zeta_{\ell^n}^{(\ell-1)^{\ell^{n-1}}} = \zeta_{\ell^n}^{-1},\ \text{and}$$
$$\rho_n^{\ell^{n-v_n}}(\beta_n(t)) = (\beta_n(t))^{(-1)^{\ell^{n-v_n}}} = \beta_n(t)^{-1},$$

it follows that $\rho_n(\zeta_\ell) = \zeta_\ell^{-1}$.
Since K_n is the splitting field of $r_n(x,t)$ over $K(t)$, it is generated over $K(t)$ by

$$\theta_c^{(n)} = \frac{\zeta_\ell - \zeta_{\ell^n}^c\beta_n(t)}{1 - \zeta_\ell\zeta_{\ell^n}^c\beta_n(t)},$$

for each $0 \leq c \leq \ell^n - 1$. Note that for each c we have

$$\rho_n^{\ell^{n-v_n}}(\theta_c^{(n)}) = \frac{\rho_n^{\ell^{n-v_n}}(\zeta_\ell) - \rho_n^{\ell^{n-v_n}}(\zeta_{\ell^n}^c\beta_n(t))}{1 - \rho_n^{\ell^{n-v_n}}\left(\zeta_\ell\zeta_{\ell^n}^c\beta_n(t)\right)} = \frac{\zeta_\ell^{-1} - \zeta_{\ell^n}^{-c}\beta_n(t)^{-1}}{1 - \zeta_\ell^{-1}\zeta_{\ell^n}^{-c}\beta_n(t)^{-1}} = \frac{\zeta_{\ell^n}^c\beta_n(t) - \zeta_\ell}{\zeta_\ell\zeta_{\ell^n}^c\beta_n(t) - 1} = \theta_c^{(n)}.$$

Thus, $\rho_n^{\ell^{n-v_n}}$ restricts to the identity on K_n so that $\rho_n^{\ell^{n-v_n}} \in \mathrm{Gal}(L_n/K_n)$. By Proposition 3.2 the order of $\rho_n^{\ell^{n-v_n}}$ in $\mathrm{Gal}(L_n/K(t))$ is 2, hence 2 divides $\#\,\mathrm{Gal}(L_n/K_n) = [L_n : K_n]$. Together

with Lemma 10 we can conclude that $2 \nmid [K_n : K(t)]$ and so it follows that $\zeta_\ell \notin K_n$. Since $\theta_c^{(n)} \in K_n \subset K_n(\zeta_\ell)$ for all $0 \leq c \leq \ell^n - 1$, it must be the case that

$$\theta_c^{(n)} - \zeta_\ell^{-1} = \frac{\zeta_\ell - \zeta_\ell^{-1}}{1 - \zeta_\ell \zeta_{\ell^n}^c \beta_n(t)} \in K_n(\zeta_\ell).$$

But since $\zeta_\ell - \zeta_\ell^{-1} \in K_n(\zeta_\ell)$, we have that $\zeta_{\ell^n}^c \beta_n(t) \in K_n(\zeta_{\ell^n})$ for all $0 \leq c \leq \ell^n - 1$. Therefore both $\beta_n(t)$ and $\zeta_{\ell^n}\beta_n(t)$ are elements of $K_n(\zeta_\ell)$, whence $\zeta_{\ell^n} \in K_n(\zeta_\ell)$. Altogether this results in the inclusion of fields:

$$K_n \subset L_n \subset K_n(\zeta_\ell).$$

Since 2 divides $[L_n : K_n]$ and $[K_n(\zeta_\ell) : K_n] = 2$, we have that $\#\operatorname{Gal}(L_n/K_n) = 2$. We can also conclude that $L_n = K_n(\zeta_\ell)$ and that $\#\operatorname{Gal}(K_n/K(t)) = \ell^{2n-v_n}$.

In light of these observations on the Galois groups, we see there is exactly one non-trivial automorphism of $L_n/K(t)$ that restricts to the identity automorphism on $K_n/K(t)$. We have seen that $\rho_n^{\ell^{n-v_n}}$ has this property, so it must be the only one. Because the order of σ_n is the least $d \geq 1$ such that $\sigma_n^d = \mathrm{id}$, the order of σ_n must be ℓ^{n-v_n}. Finally, since γ_n^y does not equal $\rho_n^{\ell^{n-v_n}}$ for any y, γ_n^y restricts to the identity on K_n if and only if it is the identity on L_n. Thus the order of τ_n is ℓ^n. This completes the proof of the theorem. □

4. Dynamical Properties

In this final section we adopt the notational conventions and context of [**1**]. Let K be a number field and fix a rational self-map φ of $\mathbf{P}^1$ defined over K; in coordinates, we may take $\varphi(x) = g(x)/h(x)$ with $g(x), h(x)$ coprime elements of $\mathcal{O}_K[x]$. Then for $n \geq 1$, the splitting fields of the iterates $\varphi^{(n)}(x) - t$ give rise to tower of splitting fields of the previous iterates. More precisely, we let $\mathcal{F}_n$ be the Galois closure of the field $K(t)/(\varphi^n(x) - t)$ and $\mathcal{F}_\varphi$ the compositum over all n of the splitting fields: $\mathcal{F}_\varphi = \cup_n \mathcal{F}_n$. Fix a compatible system of specialization maps $\sigma_n : \mathcal{O}_{\mathcal{F}_n} \longrightarrow \overline{K}$ and set K_{n,t_0} to be the Galois closure over K of the specialized extension. In this way the compositum K_{φ,t_0} can be viewed as a specialization of the tower $\mathcal{F}_{\varphi,t_0}$.

It is quite difficult to determine the exact primes ramifying in a tower, and the ones which are known tend to use auxilliary information. For example, given an elliptic curve $E/\mathbf{Q}$ without complex multiplication and a rational prime ℓ, the iterates of the Lattès map φ_ℓ give rise to towers ramified above ℓ and the primes of bad reduction for E. A similar example concerns the Chebyshev polynomial $\psi_2(x) = x^2 - 2$. The tower of splitting fields of the iterates of ψ_2 is ramified only above 2. Moreover the Chebyshev polynomials ψ_d arise as the image of projection-to-x for the d-power map on the algebraic group S^1. At the same time, in both examples the associated Galois groups are smaller than one would expect from a "random" tower (the Galois group of a Lattès tower is an open subgroup of $\mathrm{GL}_2(\mathbf{Z}_\ell)$, while the Galois group of the Chebyshev tower is isomorphic to the additive group $\mathbf{Z}_2$ of 2-adic integers). Both of these examples come from the specialization $t = 0$; other specializations would potentially give rise to towers whose Galois groups are less well-understood (though in the case of Lattès maps, if t were the x-coordinate (in Weierstrass form) of a point of infinite order, then more can be said in terms of arboreal representations; see [**4**] for more details).

The common characteristics of these two examples are "small" Galois group, finite ramification, and that φ is postcritically finite; moreover, both arise via endomorphisms of algebraic groups. The $r_n(x,t)$ share some of these characteristics. To give a little more detail, with all notation as above let

$$\mathcal{R}_\varphi := \{\theta \in \overline{K} \ : \ (hg' - gh')(\theta) = 0\} \text{ and } \mathcal{B}_\varphi := \{\varphi(\theta) \ : \ \theta \in \mathcal{R}_\varphi\}$$

be the sets of *ramification points* and *branch points* of φ, respectively. In particular, $\mathcal{R}_\varphi$ consists of the roots of $hg' - gh'$ counted *without* multiplicity. A rational function φ is said to be *postcritically finite* if the forward orbit of the critical points under all iterations is a finite set. In other words, if

$$\mathcal{B}_{\varphi^{(n)}} = \mathcal{B}_\varphi \cup \varphi(\mathcal{B}_\varphi) \cup \cdots \cup \varphi^{(n-1)}(\mathcal{B}_\varphi)$$

is the set of branch points of $\varphi^{(n)}$, then φ is postcritically finite if $\cup_n \mathcal{B}_{\varphi^{(n)}}$ is a finite set.
We can apply this setup to the $r_n(x,t)$. Fix $\ell > 2$ and set $\varphi(x) = p(x)/q(x)$, where $p(x)$ and $q(x)$ are as in the Introduction. Then the following lemma is a simple computation.

Lemma 11. — *Let $\ell > 2$ be an integer and K a field of characteristic coprime to ℓ. Suppose that $\zeta_\ell^+ \in K$, where ζ_ℓ is a primitive ℓth root of unity. Then $\varphi(x) = p(x)/q(x) \in K(x)$ is postcritically finite.*

Proof. — The critical points of φ are ζ_ℓ and ζ_ℓ^{-1}, each of which is fixed by φ. □

In the context where K is a number field, the fact that the φ are postcritically finite means the function field towers are finitely ramified. Moreover, the discriminant formulæ of **[1, 2]** imply that for all $t \in K$, the specialized towers at t are finitely ramified as well. Indeed, applying the results of **[1, 2]** to the present setup, we obtain:

$$\text{disc } r_n(x,t) = \pm \ell^{n(\ell^n)} (\zeta_\ell - \zeta_\ell^{-1})^{(\ell^n-2)(\ell^n-1)} (t^2 - (\zeta_\ell + \zeta_\ell^{-1})t + 1)^{\ell^n - 1}.$$

This bounds the number of primes ramifying at any level of the tower and moreover shows exaclty what the potential ramified primes are. In particular, the primes of $\mathcal{O}_K$ dividing ℓ are ramified in the tower, while those dividing $t^2 - \zeta_\ell^+ t + 1$ may be ramified.
In the special case where ℓ is a prime number and $K = \mathbf{Q}(\zeta_\ell^+)$, we have the factorization $\ell = \mathfrak{l}^{(\ell-1)/2}$ as ideals of $\mathcal{O}_K$. It would be interesting to determine specializations at which only a few primes in addition to $\mathfrak{l}$ ramify in the tower above K. If we set $\ell = 3$, however, and take for example $t = 0, 1$ so that 3 is the only ramified prime, then the tower above $\mathbf{Q}$ specializes to the abelian cyclotomic-3 tower. A delicate problem would be to determine an explicit relationship between the ramified primes and the index of the specialized Galois group inside the geometric Galois group. Finally, it would be interesting to determine, along the lines of the Lattès and Chebyshev towers, whether there is an alternative "geometric" description of the $r_n(x,t)$, which would make the analogy more complete.

Acknowledgements. We would like to express our gratitude to Farshid Hajir and to the referee. The impetus for this paper developed from numerous conversations with Farshid Hajir, while the referee's comments and suggestions greatly improved the exposition of the paper.

References

[1] W. Aitken, F. Hajir, C. Maire. Finitely ramified iterated extensions. *Int. Math. Res. Not.* **2005**, no. 14, 855-880.

[2] J. Cullinan, F. Hajir. Ramification in iterated towers for rational functions. *Manuscripta Math.* **137** (2012), no. 3-4, 273-286.

[3] M. Daub, J. Lang, M. Merling, A. Pacelli, N. Pitiwan, M. Rosen. Function Fields with Class Number Indivisible by a Prime ℓ. *Acta Arith.* **150** (2011), no. 4, 339-359.

[4] R. Jones, J. Rouse. Iterated endomorphisms of abelian algebraic groups. *Proc. Lond. Math. Soc.* **100** (2010), no. 3, 763-794.

[5] Y. Kishi. A family of cyclic cubic polynomials whose roots are systems of fundamental units. *J. Number Theory* **102** (2003), no. 1, 90-106.

[6] T. Komatsu. Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory. *Manuscripta Math.* **114** (2004) 265-279.

[7] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**. Springer-Verlag, New York, 2002.

[8] E. Lehmer. Connection between Gaussian periods and cyclic units. *Math. Comp.* **50** (1988), no. 182, 535-541.

[9] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[10] R.W.K. Odoni. The Galois theory of iterates and composites of polynomials. *Proc. London. Math. Soc.* **51** (1985), no. 3, 385-414.

[11] Y. Rikuna. On simple families of cyclic polynomials. *Proc. Amer. Math. Soc.* **130** (2002), no. 8, 2215-2218

[12] R. Schoof, L. Washington. Quintic polynomials and real cyclotomic fields with large class numbers. *Math. Comp.* **50** (1988), no. 182, 543-556.

[13] D. Shanks. The simplest cubic fields. *Math. Comp.* **28** (1974), 1137-1157

[14] Y.Y. Shen, L.C. Washington. A family of real 2^n-tic fields. *Trans. Amer. Math. Soc.* **345** (1994), no. 1, 413-434.

[15] Y.Y. Shen, L.C. Washington. A family of real p^n-tic fields. *Canad. J. Math.* **47** (1995), no. 3, 655-672.

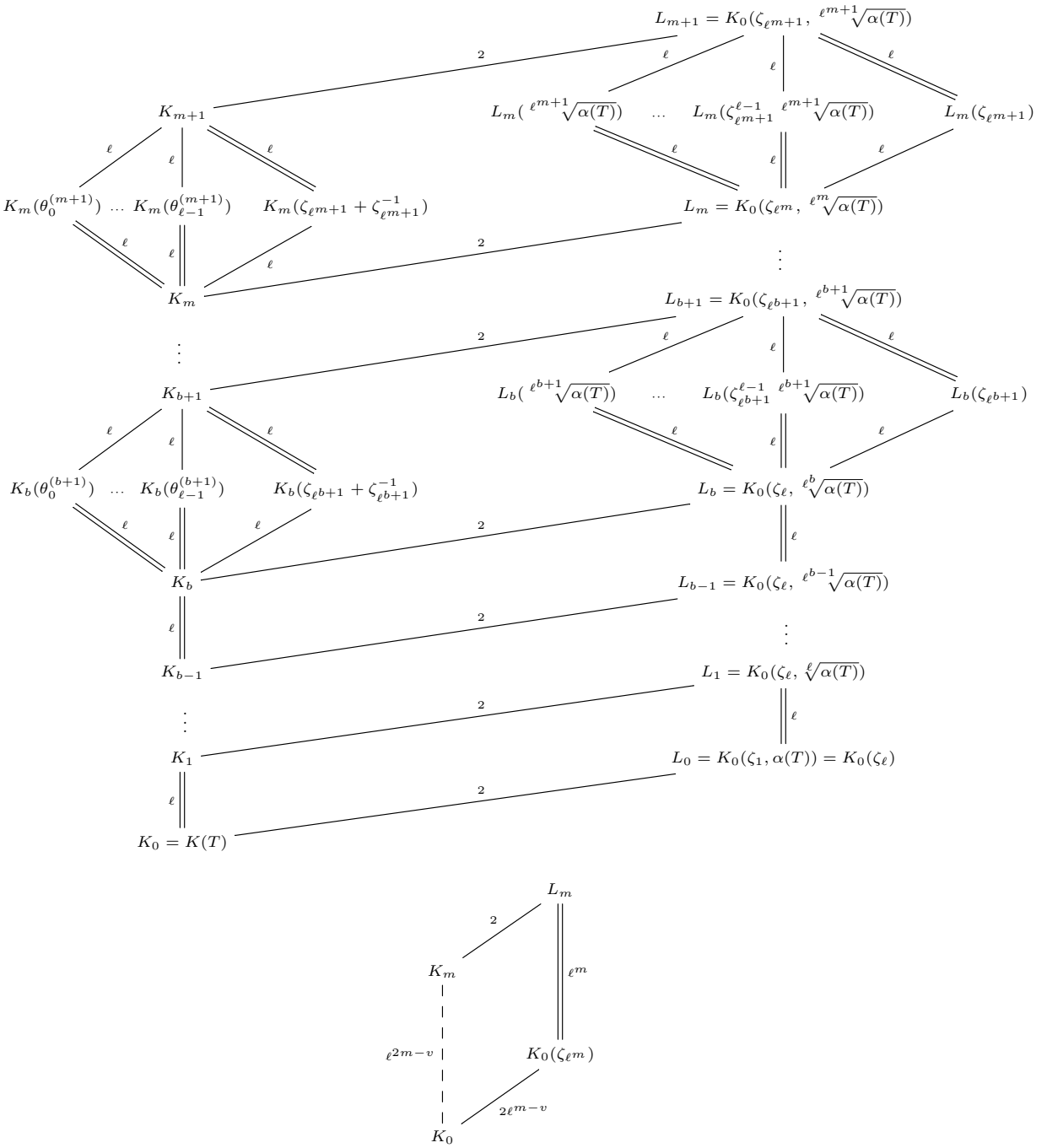
[16] J. Silverman, *The arithmetic of dynamical systems*. Graduate Texts in Mathematics, **241**. Springer, New York, 2007.

Appendix A
Field Diagrams

The following diagram shows the relationship between the towers $\{K_n\}$ and $\{L_n\}$. Define $b \in \mathbf{N} \cup \{\infty\}$ to be

$$b = \sup\{m \in \mathbf{N} : K(\zeta_{\ell^m}) = K(\zeta_\ell)\}.$$

For example, if $K = \mathbf{Q}$ then $b = 1$; if $K = \mathbf{R}$ then $b = \infty$; and if $K = \mathbf{Q}(\zeta_{\ell^2} + \zeta_{\ell^2}^{-1})$ then $K(\zeta_\ell) = K(\zeta_{\ell^2})$ but $K(\zeta_\ell) \subsetneq K(\zeta_{\ell^3})$, so $b = 2$. In terms of the towers, when $n \geq b$, there are $\ell + 1$ intermediate fields between K_n and K_{n+1}. Finally, we make the convention that a single line denotes that all infinite primes are inert, while a double line indicates that all infinite primes split completely.


$L_{m+1} = K_0(\zeta_{\ell^{m+1}}, \sqrt[\ell^{m+1}]{\alpha(T)})$
K_{m+1}
$L_m(\sqrt[\ell^{m+1}]{\alpha(T)})$ ... $L_m(\zeta_{\ell^{m+1}}^{\ell-1}\sqrt[\ell^{m+1}]{\alpha(T)})$
$L_m(\zeta_{\ell^{m+1}})$
$K_m(\theta_0^{(m+1)})$ ... $K_m(\theta_{\ell-1}^{(m+1)})$
$K_m(\zeta_{\ell^{m+1}} + \zeta_{\ell^{m+1}}^{-1})$
$L_m = K_0(\zeta_{\ell^m}, \sqrt[\ell^m]{\alpha(T)})$
K_m
$L_{b+1} = K_0(\zeta_{\ell^{b+1}}, \sqrt[\ell^{b+1}]{\alpha(T)})$
K_{b+1}
$L_b(\sqrt[\ell^{b+1}]{\alpha(T)})$ ... $L_b(\zeta_{\ell^{b+1}}^{\ell-1}\sqrt[\ell^{b+1}]{\alpha(T)})$
$L_b(\zeta_{\ell^{b+1}})$
$K_b(\theta_0^{(b+1)})$ ... $K_b(\theta_{\ell-1}^{(b+1)})$
$K_b(\zeta_{\ell^{b+1}} + \zeta_{\ell^{b+1}}^{-1})$
$L_b = K_0(\zeta_\ell, \sqrt[\ell^b]{\alpha(T)})$
K_b
$L_{b-1} = K_0(\zeta_\ell, \sqrt[\ell^{b-1}]{\alpha(T)})$
K_{b-1}
$L_1 = K_0(\zeta_\ell, \sqrt[\ell]{\alpha(T)})$
K_1
$L_0 = K_0(\zeta_1, \alpha(T)) = K_0(\zeta_\ell)$
$K_0 = K(T)$
2
ℓ

L_m
K_m
$K_0(\zeta_{\ell^m})$
K_0
2
ℓ^m
ℓ^{2m-v}
$2\ell^{m-v}$

6 mai 2013

Z. Chonoles, Department of Mathematics, The University of Chicago, 5734 S. University Avenue Chicago, IL 60637, USA • *E-mail :* chonoles@math.uchicago.edu

J. Cullinan, Department of Mathematics, Bard College, Annandale-On-Hudson, NY 12504, USA
E-mail : cullinan@bard.edu

H. Hausman, Department of Mathematics, Williams College, Williamstown, MA 01267, USA
E-mail : Hannah.E.Hausman@williams.edu

A.M. Pacelli, Department of Mathematics, Williams College, Williamstown, MA 01267, USA
E-mail : apacelli@williams.edu

S. Pegado, Department of Mathematics, Williams College, Williamstown, MA 01267, USA
E-mail : Sean.C.Pegado@williams.edu

F. Wei, Department of Mathematics, Harvard University, One Oxford Street, Cambridge MA 02138, USA
E-mail : fw292@math.harvard.edu