SPECIALIZATIONS OF GENERALIZED RIKUNA POLYNOMIALS

CELESTE CASS, JOHN CULLINAN, ALEXANDER RASMUSSEN, AND DARKO TRIFUNOVSKI

Abstract. The generalized Rikuna polynomials are an iterative generalization of Rikuna's generic cyclic polynomials, which themselves generalize Shanks' cubic polynomials. In this paper we study Galois properties of the generalized Rikuna polynomials under specialization.

1. Introduction

The arithmetic of iterated polynomials and rational functions is a vast subject with deep connections to many areas of number theory and algebraic geometry. One of the prototypical examples comes from the arithmetic theory of elliptic curves. Let E be an elliptic curve defined over $\mathbf{Q}$ without complex multiplication, ℓ a rational prime, and $[\ell] : E \longrightarrow E$ the multiplication-by-ℓ isogeny. For all but finitely many ℓ, the ℓ-division fields $\mathbf{Q}(E[\ell])$ have Galois group isomorphic to $\mathrm{GL}_2(\mathbf{Z}/\ell)$. Moreover, the iterates $[\ell]^{(n)} = [\ell^n]$ of $[\ell]$ produce a compatible family of $\mathrm{GL}_2(\mathbf{Z}/\ell^n)$-extensions of $\mathbf{Q}$. These iterated towers not only have small Galois groups, but have restricted ramification: the criterion of Néron, Ogg, and Shafarevich tells us that the only primes ramifying in the tower $\bigcup_n \mathbf{Q}(E[\ell^n])$ are ℓ, and the primes of bad reduction for E. Related to the small Galois group and restricted ramification is that the associated Lattès map $\varphi_\ell(x)$ is postcritically finite. The phenomenon of "small" Galois group, restricted ramification, and postcritically finite towers manifests itself more generally in the m-division fields of abelian varieties defined over global fields.

Another common problem in arithmetic is the behavior of function field extensions under specialization. Given a finite Galois extension $L(t)/K(t)$ of function fields with Galois group $G(t)$, the specialization map $t \mapsto t_0 \in K$ can produce interesting results. On one hand, under suitably general hypotheses, the Hilbert Irreducibility Theorem tells us that for "most" $t_0 \in K$ we have $[L(t) : K(t)] = [L(t_0) : K(t_0)]$ and the extension remains Galois. The set of reducible specializations is *thin* in the sense of Serre [8], and it may be very difficult to determine this set explicitly. Even if $L(t_0)/K(t_0)$ remains Galois upon specialization, the specialized Galois group $G(t_0)$ ("decomposition group" at t_0) may be a proper subgroup of $G(t)$. It may be difficult to determine – or to bound, in the case of infinite extensions – the index of specialization $[G(t) : G(t_0)]$ as $t_0 \in K$ ranges over all irreducible specializations.

In this paper we take up these questions in the context of the *generalized Rikuna polynomials*. These polynomials were introduced in [2] as iterated generalizations of Rikuna's generic cyclic polynomials [7], which are defined in the following way. Let $\ell > 2$ be a positive integer and K a field such that $\zeta_\ell \notin K$, where ζ_ℓ is a primitive ℓth root of unity, but that $\zeta_\ell + \zeta_\ell^{-1} \in K$. Define polynomials $p(x), q(x) \in K[x]$ via

$$p(x) = \frac{\zeta_\ell^{-1}(x-\zeta_\ell)^\ell - \zeta_\ell(x-\zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell} \qquad \text{and} \qquad q(x) = \frac{(x-\zeta_\ell)^\ell - (x-\zeta_\ell^{-1})^\ell}{\zeta_\ell^{-1} - \zeta_\ell},$$

and set $r(x,t) = p(x) - tq(x)$. When $\ell = 3$, these are the cubic polynomials of Shanks [9]. If ℓ is odd, then it was shown in [4] that $r(x,t)$ is *generically cyclic* in the sense that if L/K is a cyclic-ℓ extension, then $L \simeq K[x]/(r(x,t_0))$ for some $t_0 \in K$.

We generalize this construction as follows. Let $\varphi(x) = p(x)/q(x) \in K(x)$ and write $\varphi^{(n)}(x) = p_n(x)/q_n(x)$ for the nth iterated of $\varphi(x)$, written in lowest terms. Define the nth *generalized Rikuna polynomial* to be

$$r_n(x,t) = p_n(x) - tq_n(x) \in K(t)[x],$$

so that $r_1(x,t) = r(x,t)$ as above. In this paper we study the reducibility and Galois-theoretic properties of these polynomials under specialization. We restrict to the following setup. Let ℓ be an odd prime number,

This work was supported by NSF grant DMS-1005028.

and fix a primitive ℓth root of unity $\zeta_\ell \in \overline{\mathbf{Q}}$. Write $\zeta_\ell^+ = \zeta_\ell + \zeta_\ell^{-1}$ and take $K = \mathbf{Q}(\zeta_\ell^+)$. Then K is the maximal real subfield of the ℓth cyclotomic field and is the minimal field of definition for $r(x,t)$ in characteristic 0.

These geometric Galois groups were computed in [2] and it was shown that Gal $r_n(x,t) \simeq \mathbf{Z}/\ell^n \rtimes \mathbf{Z}/\ell^{n-1}$. In particular, these Galois groups are very small, but still non-abelian. In this paper we give certain geometric characterizations of the reducible specializations and of the specializations with smaller Galois group (we call these *exceptional* specializations) and put forth some conjectures for future study. These specialized Galois groups have the interesting property that they give examples of some of the smallest non-abelian transitive subgroups of S_{ℓ^n}. In the case $\ell = 3$ we have $K = \mathbf{Q}$ and this serves as the basis for some conjectures when $\ell > 3$.

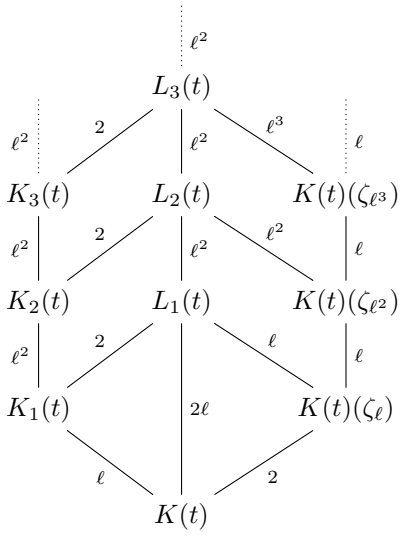
The structure of the paper is as follows. In the next section we recall the results of [2] and give some further properties of the iterated geometric Galois groups. Next, we describe some of the basic dynamical properties of φ. We then take up the questions of specialization. In Section 4 we study the reducible specializations and in Section 5 the irreducible specializations with smaller Galois group.

What remains unclear is whether there is a suitably "geometric" interpretation of the generalized Rikuna polynomials. In the case of Lattès maps, the underlying geometry is that of the elliptic curve. It would be interesting to determine whether the generalized Rikuna polynomials are naturally associated to certain algebraic groups or more general schemes, in a similar fashion to the Lattès maps.

Acknowledgements: We would like to thank Farshid Hajir for helpful discussions and the referee and editors for their suggestions which simplified many of the proofs and improved the exposition of the paper.

2. The Geometric Galois Group

Here we collect the main results of [2] in the context of our setup. Recall that we take ℓ to be an odd prime number and $K = \mathbf{Q}(\zeta_\ell^+)$. Fix a compatible system of primitive ℓ^nth roots of unity such that $\zeta_{\ell^n}^\ell = \zeta_{\ell^{n-1}}$; in other words fix a primitive element of the Tate module $\mathbf{Z}_\ell(1)$. We use this compatible system to construct the following tower of fields:



Here, $K_n(t)$ is the splitting field of the nth generalized Rikuna polynomial $r_n(x,t)$ and $L_n(t) \simeq K_n(t)(\zeta_\ell)$. Note that $[K_1(t) : K(t)] = \ell$ is consistent with Rikuna's original polynomials. In [2], the Galois groups of the $K_n(t)/K(t)$ and the $L_n(t)/K(t)$ were determined by explicitly determining the Galois action on the roots of the $r_n(x,t)$. We briefly recall that action here.

The polynomial $r_n(x,t) \in K(t)[x]$ has degree ℓ^n with roots that are easy to describe. Set $\alpha(t) = \frac{\zeta_\ell - t}{\zeta_\ell^{-1} - t}$ and for each $n \geq 1$ fix a compatible family of ℓ^n-roots $\sqrt[\ell^n]{\alpha(t)}$ of $\alpha(t)$. Then, for each $0 \leq c \leq \ell^n - 1$, the

roots of $r_n(x,t)$ are given by

$$\theta_c^{(n)}(t) := \frac{\zeta_\ell - \zeta_{\ell^n}^c \sqrt[\ell^n]{\alpha(t)}}{1 - \zeta_\ell \zeta_{\ell^n}^c \sqrt[\ell^n]{\alpha(t)}};$$

that is, $r_n(\theta_c^{(n)}(t), t) = 0$ for all $0 \le c \le \ell^n - 1$. We define $L_0(t) = K(t)(\zeta_\ell) = K(t)(\alpha(t))$ so that the fields $L_n(t)$ can be described as $L_n(t) = K(t)(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha(t)})$ for all $n \ge 0$.

For the Galois groups, set $\Gamma_n(t) = \mathrm{Gal}(L_n(t)/K(t))$ and $G_n(t) = \mathrm{Gal}(K_n(t)/K(t))$ so that $G_n(t)$ is a quotient of $\Gamma_n(t)$. It was determined in [2] that these Galois groups are generated as follows:

$$\Gamma_n(t) = \langle \rho_n, \gamma_n \mid \rho_n^{2\ell^{n-1}} = \gamma_n^{\ell^n} = 1,\, \rho_n\gamma_n = \gamma_n^{1-\ell}\rho_n \rangle$$
$$G_n(t) = \langle \sigma_n, \tau_n \mid \sigma_n^{\ell^{n-1}} = \tau_n^{\ell^n} = 1,\, \sigma_n\tau_n = \tau_n^{1-\ell}\sigma_n \rangle,$$

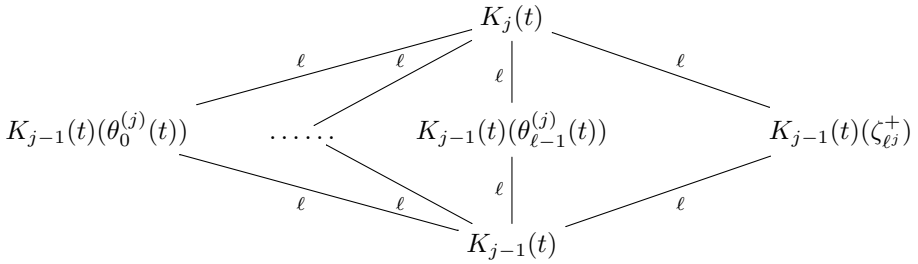
where the individual automorphisms are defined by the following actions:

$$\rho_n : \zeta_{\ell^n} \mapsto \zeta_{\ell^n}^{(\ell-1)^{\ell^{b_n-1}}},\ \sqrt[\ell^n]{\alpha(t)} \mapsto \frac{1}{\sqrt[\ell^n]{\alpha(t)}} \qquad \text{and} \qquad \gamma_n : \zeta_{\ell^n} \mapsto \zeta_{\ell^n},\ \sqrt[\ell^n]{\alpha(t)} \mapsto \zeta_{\ell^n}\sqrt[\ell^n]{\alpha(t)},$$

and σ_n and τ_n are given by restriction. In particular, $\#\Gamma_n(t) = 2 \cdot \ell^{2n-1}$ and $\#G_n(t) = \ell^{2n-1}$ and these groups are clearly non-abelian. The following two properties follow from the main results of [2], but were never made explicit. For completeness we briefly state them here.

Lemma 2.1. *The group $G_n(t)$ admits the filtration $1 \lhd G_1(t) \lhd G_2(t) \lhd \cdots \lhd G_{n-1}(t) \lhd G_n(t)$, where $G_1(t)$ is cyclic of order ℓ and $G_j(t)/G_{j-1}(t) \simeq \mathbf{Z}/\ell \times \mathbf{Z}/\ell$ for all j in the range $2 \le j \le n$.*

Proof. That the sequence is normal follows from the fact that for all j, $G_j(t)$ is the Galois group of $r_j(x,t)$ over $K(t)$. When $j = 1$, it was proved in [7] that the Galois group is cyclic of order ℓ. For $j = 2, \ldots, n$, we appeal to the field diagram:



The extension $K_j(t)/K_{j-1}(t)$ is Galois of degree ℓ^2 and has $\ell + 1$ distinct intermediate extensions; see [2] for details of this construction. □

Let p be a prime. Recall that an *extra-special p-group* is a p-group P such that its center $Z(P)$ has order p and the quotient $P/Z(P)$ is elementary abelian. It is well-known that the order of an extra-special p-group is equal to p^{1+2r}, where $r \in \mathbf{Z}_{\ge 1}$. Moreover, every non-abelian group of order p^3 is extra-special. The groups $G_n(t)$ for $n \ge 2$ are candidates for being extra-special ℓ-groups, but as we will see, only $G_2(t)$ is extra-special.

Proposition 2.2. *The group $G_2(t)$ is extra-special, but for all $n \ge 3$, $G_n(t)$ is not extra-special.*

Proof. Since $G_2(t)$ is a non-abelian group of order ℓ^3 it is automatically extra-special. For all $n \ge 1$, the center $Z_n(t)$ of $G_n(t)$ is cyclic of order ℓ. This is clear for $n = 1$ since $\#G_1(t) = \ell$. When $n \ge 2$, we claim that $\#Z_n(t) = \ell$ and that $K_{n-1}(t)(\zeta_{\ell^n})$ is the fixed-field of $Z_n(t)$. Using the presentation of $G_n(t)$ above, it is not hard to see that $Z_n(t) = \langle \tau^{\ell^{n-1}} \rangle$, hence has order ℓ. By considering the $\ell + 1$ distinct index-ℓ subextensions of $K_n(t)$, only the field $K_{n-1}(t)(\zeta_{\ell^n}^+)$ is Galois over $K(t)$, hence must be the fixed-field of $Z_n(t)$. It remains to show that $G_n(t)/Z_n(t)$ is not elementary abelian for $n \ge 3$. But if it were, then all of its quotients would be abelian, contradicting the fact that $G_{n-1}(t)$ is non-abelian. □

3. Ramification and Dynamics

The discriminant of an irreducible polynomial bounds the number of primes ramifying in the extension generated by that polynomial. Let k be a field and recall that a rational function $f(x) \in k(x)$ is called *postcritically finite* if the forward orbit under f of the critical points of f is a finite set. If k is a number field and $\varphi(x) \in k(x)$ is a postcritically finite rational function, then it was shown in [1, 3] that if k_{n,t_0} is the splitting field of $\varphi^{(n)}(x) - t_0$ (assuming irreducibility), then only finitely many primes of $\mathcal{O}_k$ ramify in the tower $\bigcup_{n\geq 1} k_{n,t_0}$. Take $k = K = \mathbf{Q}(\zeta_\ell^+)$ as above and set $\varphi(x) = p(x)/q(x)$. In [2] it was shown that

$$\text{disc } p_n(x) - tq_n(x) = \ell^{n\ell^n}(\zeta_\ell - \zeta_\ell^{-1})^{(\ell^n-1)(\ell^n-2)}(t^2 - \zeta_\ell^+ t + 1)^{\ell^n-1}. \tag{1}$$

In this way the restricted ramification of the $K_n(t)$ tower is linked to the dynamical properties of $\varphi(x)$.

Under the specialization $t \mapsto t_0$, this formula gives an explicit description of the primes of $\mathcal{O}_K = \mathbf{Z}[\zeta_\ell + \zeta_\ell^{-1}]$ which could ramify in a specialized tower. In Section 5 we study the size of the specialized Galois group in this context. In particular, we are interested in creating *non-abelian* towers with very few primes ramifying. We start with a simple observation.

Lemma 3.1. *If $f(t) = t^2 - \zeta_\ell^+ t + 1$, then $f(t) = f(-t + \zeta_\ell^+)$.*

This observation has the following consequence: since $\mathbf{Q}(\zeta_\ell^+) \subseteq \mathbf{R}$, it inherits a total ordering. The symmetry of Lemma 3.1 then implies that for the purposes of ramification, it suffices to consider specializations $t_0 \geq \zeta_\ell^+/2$.

Lemma 3.2. *For all $t_0 \in K$ the discriminant of $r_n(x, t_0)$ is non-zero. Hence there are no specializations having repeated roots.*

Proof. Note that disc $r_n(x, t_0) = 0$ if and only if $t_0^2 - \zeta_\ell^+ t_0 + 1 = 0$. However, since $\zeta_\ell \notin K$, it follows that disc $r_n(x, t_0) \neq 0$ for any $t_0 \in K$. □

In the special case $\ell = 3$ we have $K = \mathbf{Q}$ and can determine all specializations such that the polynomial discriminant is a power of 3.

Lemma 3.3. *Let $f(t) = t^2 + t + 1$. Then $f(t)$ is a power of 3 if and only if $t \in \{-2, -1, 0, 1\}$.*

Proof. Suppose $t \in \mathbf{Q}$ with $t^2 + t + 1 = 3^n$ and apply the quadratic formula to see that $4 \cdot 3^n - 3$ must be a rational square. When $n \geq 2$ this is impossible because of the power of 3 and when $n = 0$ or 1 we get $t = -2, -1, 0, 1$; if $n < 0$, then the discriminant is negative. □

The dynamics of φ are closely related to the reducibility of $r_n(x, t_0)$ for K-rational values of t_0. For example, if φ has a K-rational fixed point t_0, then $r_n(x, t_0)$ is reducible for all n. Moreover, for all $n \geq 1$ it is clear that $r_n(x, t_0)$ has a linear factor since $\varphi^{(n)}(t_0) = t_0$ means that $x = t_0$ is a solution to $\varphi^{(n)}(x) = t$. Similarly, if t_0 is a K-rational point with period m, then $r_{km}(x, t_0)$ has a linear factor for any positive integer value of k because t_0 is a rational root of $\varphi^{(km)}(x) = t_0$.

Proposition 3.4. *The only K-rational fixed point of φ is $\zeta_\ell^+/2$.*

Proof. Suppose x_0 is a fixed point of φ so that $p(x_0) - x_0 q(x_0) = 0$. Rewriting in terms of the definitions of $p(x)$ and $q(x)$, we get

$$(x_0 - \zeta_\ell)(x_0 - \zeta_\ell^{-1})\left((x_0 - \zeta^{-1})^{\ell-1} - (x_0 - \zeta_\ell)^{\ell-1}\right) = 0.$$

Two of the solutions are ζ_ℓ and ζ_ℓ^{-1}, which do not belong to K. For the remaining factor, we have

$$(x_0 - \zeta^{-1})^{\ell-1} - (x_0 - \zeta_\ell)^{\ell-1} = 0 \Longrightarrow \left(\frac{x_0 - \zeta_\ell}{x_0 - \zeta^{-1}}\right)^{l-1} = 1,$$

which we can write as $\alpha(x_0) = \eta$, where η is an $(\ell-1)$-th root of unity. Since ℓ is odd, two of the roots are 1 and -1. When $\eta = 1$ we get no solutions, while when $\eta = -1$ we get $x_0 = \zeta_\ell^+/2$.

To see that $x_0 = \zeta_\ell^+/2$ is the only solution, suppose η is a non-real $(\ell-1)$-th root of unity. Let k be the least positive integer such that $\eta^k = 1$ and note that k must divide $\ell - 1$ and must be greater than 2. Since

$K(t)(\alpha(t)) = K(t)(\zeta_\ell)$, it follows that $\alpha(x_0) \in K(\zeta_\ell) = \mathbf{Q}(\zeta_\ell)$. Since $x_0 \in K$, we have $\eta \in K$. But ℓ is prime and η is a primitive kth root of unity, where $k \mid \ell - 1$, so this is impossible. □

Due to the deep connections between the complex dynamics of a rational map and the arithmetic it encodes, for the rest of this section we consider $\varphi : \mathbf{P}^1_{\mathbf{C}} \longrightarrow \mathbf{P}^1_{\mathbf{C}}$ as a self-map of the Riemann sphere.

Lemma 3.5. *If z is in the upper (resp. lower) half plane, then $\varphi(z)$ is in the upper (resp. lower) half plane; if $z \in \mathbf{R}$, then so is $\varphi(z)$.*

Proof. For any $z \in \mathbf{C}$, to determine the region of $\mathbf{P}^1_{\mathbf{C}}$ to which $\varphi(z)$ belongs, it suffices to consider

$$\begin{aligned} p(z)\overline{q(z)} &= (\zeta_\ell^{-1}(z-\zeta_\ell)^\ell - \zeta_\ell(z-\zeta_\ell^{-1})^\ell)(\overline{(z-\zeta_\ell)^\ell - (z-\zeta_\ell^{-1})^\ell}) \\ &= \left(\zeta_\ell^{-1}\|(z-\zeta_\ell)^\ell\|^2 + \zeta_\ell\|(z-\zeta_\ell^{-1})^\ell\|^2\right) - \left(\zeta_\ell(z-\zeta_\ell^{-1})^\ell\overline{(z-\zeta_\ell)^\ell} + \zeta_\ell^{-1}(z-\zeta_\ell)^\ell\overline{(z-\zeta_\ell^{-1})^\ell}\right). \end{aligned}$$

The second term in parentheses is real (complex conjugation acts trivially), so we look to the first. If $\operatorname{Im} z > 0$, then $\|(z-\zeta_\ell)\| < \|(z-\zeta_\ell^{-1})\|$, and therefore $\operatorname{Im}\varphi(z) > 0$; similarly if $\operatorname{Im}(z) < 0$, then so is $\operatorname{Im}\varphi(z)$. Finally, if $\operatorname{Im} z = 0$, then $\|(z-\zeta_\ell)\| = \|(z-\zeta_\ell^{-1})\|$, and therefore $\varphi(z)$ is real. □

Proposition 3.6. *Let $\varphi : \mathbf{P}^1_{\mathbf{C}} \longrightarrow \mathbf{P}^1_{\mathbf{C}}$ be as above. Then the Julia set of φ is $\mathbf{R} \cup \{\infty\}$.*

Proof. Partition $\mathbf{P}^1_{\mathbf{C}} = \mathfrak{h}^+ \coprod \mathfrak{h}^- \coprod J$ into the upper half-plane, lower half-plane, and $J := \mathbf{R} \cup \{\infty\}$. By Lemma 3.5, φ is fully (forward and backward) invariant over each of these three subsets. The Julia set is the smallest fully invariant closed set with at least 3 points and so it follows that the Julia set of φ is a subset of J.

It is easy to check that φ has two critical points: $z = \zeta_\ell^{\pm 1}$ (each of which is fixed by φ), and therefore has at most two Fatou domains. It follows that each of $\mathfrak{h}^+$ and $\mathfrak{h}^-$ are contained in different Fatou domains, and since they each contain a fixed critical point, they are components containing an attracting point. Finally, since J is fully invariant under φ it follows that no subset of J can be in the Fatou set and that therefore the Julia set is all of J. □

4. Reducible Specializations

If $k(t)$ is a function field defined over a number field k and $f(x,t) \in k(t)[x]$ is an irreducible polynomial, then the Hilbert Irreducibility Theorem [8, Prop. 3.3.5] states that for all but a thin set of specializations $t_0 \in k$, the polynomial $f(x,t_0) \in k[x]$ is also irreducible. While it is may be difficult to characterize the reducible set explicitly, we can at least say that in the case of the generalized Rikuna polynomials that the reducible set is infinite.

Lemma 4.1. *For each $n \geq 1$, the polynomial $r_n(x,t)$ has infinitely many reducible specializations.*

Proof. Let $x_0 \in K$ with $q_n(x_0) \neq 0$. Since $r_n(x,t)$ is a linear polynomial in t, there exists $t_0 \in K$ for which $r_n(x_0,t_0) = 0$. Thus $r_n(x,t_0)$ has the factor $(x - x_0)$, hence is reducible. Since there are infinitely many choices for $x_0 \in K$ and only finitely many x_0 for which $r_n(x_0,t_0) = 0$ with t_0 fixed, we deduce that there are infinitely many $t_0 \in K$ for which $r_n(x,t_0)$ is reducible. □

We are more interested in the values t_0 which determine the specialization, rather than the parameters x_0 which generate them. Thus, it will be more convenient to focus on only one of the coordinates. To that end, let $\pi : \mathbf{A}^2_K \longrightarrow \mathbf{A}_K$ be the projection-to-t map and define $T_i := \pi(C_i(K))$. Then T_i is precisely the set of K-rational specializations parametrized by C_i (which in turn parameterizes the K-rational linear factors of $r_i(x,t)$).

Due to the iterative nature of our family of polynomials, the specializations in T_i are reducible for r_n even when $i < n$. The natural problem is to determine how $r_n(x,t)$ factors when $t \in T_i$ for $i \leq n$. We start with a simple observation.

Lemma 4.2. *If $r(x,t_0)$ is reducible, then it splits completely into linear factors.*

Proof. The extension $K_1(t)/K(t)$ is cyclic, hence if one root is defined over $K_1(t_0)$, they all are. □

Lemma 4.3. *Let $i \le j \in \mathbf{Z}_{>0}$. Then $T_j \subseteq T_i$.*

Proof. If $t_0 \in T_j$ then there exists an $x_0 \in K$ such that $(x_0, t_0) \in C_j(K)$. Then

$$t_0 = \varphi^{(j)}(x_0) = \varphi^{(i)}\left(\varphi^{(j-i)}(x_0)\right),$$

so that $\left(\varphi^{(j-i)}(x_0), t_0\right) \in C_i(K)$ and hence $t_0 \in T_i$. □

Next we introduce some notation that more accurately describes the factorization of $r_n(x, t_0)$ at reducible specializations $t_0 \in K$.

Definition. We say that $r_n(x, t_0)$ has an $(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m)$-factorization, where $\alpha_i \in \mathbf{Z}_{>0}$, $\alpha_1 \le \cdots \le \alpha_m$, and $\sum_i \alpha_i = \ell^n$ if

$$r_n(x, t_0) = f_1(x) f_2(x) f_3(x) \cdots f_m(x),$$

is a factorization of $r_n(x, t_0)$ into irreducibles with $\deg(f_i) = \alpha_i$.

Using the dominance order $\preceq$, these partitions of ℓ^n form a poset. Any reducible specialization gives rise to a (non-Galois) automorphism group $\mathrm{Aut}(K_n(t_0)/K)$ which is an intransitive subgroup of $\mathrm{Gal}(K_n(t)/K(t))$. Even though $\mathrm{Aut}(K_n(t_0)/K)$ is intransitive, it is still an ℓ-group, hence the α_i describing the factorization type are all powers of ℓ. For example, if $t_0 \in T_1$, then $r_n(x, t_0)$ admits an $(\ell^{n-1}, \ldots, \ell^{n-1})$-factorization. The following more precisely characterizes the allowable factorizations.

Proposition 4.4. *Let $0 \le i \le n-1$ and $t_0 \in T_{n-i}$. Then if $r_n(x, t_0)$ admits an $(\alpha_1, \ldots, \alpha_m)$-factorization, we have*

$$(\alpha_1, \alpha_2, \ldots, \alpha_m) \preceq (\underbrace{\ell^i, \ell^i, \ldots, \ell^i}_{\ell \text{ times}}, \underbrace{\ell^{i+1}, \ell^{i+1}, \ldots, \ell^{i+1}}_{\ell - 1 \text{ times}}, \ldots, \underbrace{\ell^{n-1}, \ell^{n-1}, \ldots, \ell^{n-1}}_{\ell - 1 \text{ times}}).$$

Proof. Let $s = \varphi^{(n-1)}(x)$. Then

$$\begin{aligned}
r_n(x, t_0) &= p_n(x) - t_0 q_n(x) \\
&= q_{n-1}^{\ell}(x)\,[p(s) - t_0 q(s)] \\
&= q_{n-1}^{\ell}(x)\,[(s - y_1)(s - y_2) \cdots (s - y_\ell)] \quad \left(\text{by Lemma 4.2, since } t_0 = \varphi\left(\varphi^{(n-i-1)}(x_0)\right)\right) \\
&= (q_{n-1}(x)s - y_1 q_{n-1}(x))(q_{n-1}(x)s - y_2 q_{n-1}(x)) \cdots (q_{n-1}(x)s - y_\ell q_{n-1}(x)) \\
&= (p_{n-1}(x) - y_1 q_{n-1}(x))(p_{n-1}(x) - y_2 q_{n-1}(x)) \cdots (p_{n-1}(x) - y_\ell q_{n-1}(x)) \quad \left(\text{since } s = \varphi^{(n-1)}(x)\right) \\
&= r_{n-1}(x, y_1) r_{n-1}(x, y_2) \cdots r_{n-1}(x, y_\ell).
\end{aligned}$$

If $i = n-1$ we are done, since the factor has degree ℓ^{n-1}. Otherwise, by Lemma 4.2, since $t_0 = \varphi\left(\varphi^{(n-i-1)}(x_0)\right)$, at least one the y_i must equal $\varphi^{(n-i-1)}(x_0)$ and it follows that one of the r_{n-1} is further reducible. We can repeat this procedure $n - i$ times, each time leaving alone $\ell - 1$ of the polynomials and further factoring one of them, which, since we are reducing the degree by a factor of ℓ at every step, gives us the desired factorization. □

4.1. **Special Case: $\ell = 3$, $n = 2$.** We make a brief digression for the special case $\ell = 3$ and $n = 2$. In this case we can say more precisely which factorizations occur.

Proposition 4.5. *Let $\ell = 3$. Suppose $r_2(x, t_0)$ has a rational root. Then $r_2(x, t_0)$ factors over $\mathbf{Q}$ into the product of three linear polynomials and two irreducible cubics.*

Proof. Writing $t_0 = \varphi^{(2)}(x_0)$ for some $x_0 \in \mathbf{Q}$ yields the factorization

$$\begin{aligned}
\varphi(\varphi(x)) - \varphi(\varphi(x_0)) &= \left(\varphi(x) + \frac{1}{\varphi(x_0) + 1}\right)\left(\varphi(x) + \frac{\varphi(x_0) + 1}{\varphi(x_0)}\right)(\varphi(x) - \varphi(x_0)) \\
&= \left(\varphi(x) + \frac{1}{\varphi(x_0) + 1}\right)\left(\varphi(x) + \frac{\varphi(x_0) + 1}{\varphi(x_0)}\right)\left(x + \frac{1}{x_0 + 1}\right)\left(x + \frac{x_0 + 1}{x_0}\right)(x - x_0).
\end{aligned}$$

We will be done if we can show that the two equations

$$\varphi(x) = -\frac{1}{\varphi(x_0)+1}$$
$$\varphi(x) = -\frac{\varphi(x_0)+1}{\varphi(x_0)}$$

have no rational solutions. Apply the definition of φ to unwind these equations into the following two equations relating x and x_0, respectively:

$$f(x,x_0) := x^3 + \frac{9x_0^2+9x_0}{x_0^3+3x_0^2-1}x^2 + \frac{-3x_0^3+9x_0+3}{x_0^3+3x_0^2-1}x - 1 = 0$$
$$g(x,x_0) := x^3 + \frac{3x_0^3+9x_0^2-3}{x_0^3-3x_0-1}x^2 + \frac{9x_0^2+9x_0}{x_0^3-3x_0-1}x - 1 = 0.$$

We will show that f has no rational roots (the argument for g is similar). Write $x_0 = a/b$ in lowest terms to get

$$f(x,a/b) = 0 \Leftrightarrow (a^3+3ba^2-b^3)x^3 + (9ba^2+9b^2a)x^2 + (-3a^3+9b^2a+3b^3)x + (-a^3-3ba^2+b^3) = 0.$$

It is easy to check that this polynomial is irreducible modulo 5 for all values of a and b, whence $f(x,x_0)$ is irreducible over $\mathbf{Q}$. □

The main consequence of this Proposition is that there are only three possible factorization types for specializations when $\ell = 3$ and $n = 2$, namely:

$$\underbrace{(1,1,1,3,3)}_{T_2} \preceq \underbrace{(3,3,3)}_{T_1} \preceq (9).$$

In particular, there do not exist rational specializations of $r_2(x,t)$ that split completely into linear factors over $\mathbf{Q}$. For higher n and ℓ we expect similar restrictions on the factorizations to hold, though a proof along the same lines is probably not possible, even in the case of $\ell = 5$, for the following reason.

Recall that given an abelian variety A_t defined over the function field $K(t)$ where K is a number field, it is known that for all but finitely many specializations $t_0 \in K$ there is an injection of Mordell-Weil groups

$$A_t(K(t)) \hookrightarrow A_{t_0}(K).$$

Moreover, for all but finitely many good primes $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, there is an injective map of finite groups

$$A_{t_0}(K)_{\text{tors}} \hookrightarrow \overline{A}_{t_0}(\mathbf{F}_\mathfrak{p}),$$

where $\overline{A}_{t_0}$ denotes the reduction modulo $\mathfrak{p}$ of A_{t_0}. In particular, if we consider the hyperelliptic curve $\mathcal{H}$ defined by

$$y^2 = r_n(x,t_0)$$

and embed $\mathcal{H}$ into its Jacobian $\operatorname{Jac}\mathcal{H}$, then the 2-torsion subgroup of $\operatorname{Jac}\mathcal{H}(K)$ is generated by the zeroes of $r_n(x,t_0)$. For a prime of good reduction $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, one could (in theory) compute the number of $\mathbf{F}_\mathfrak{p}$-rational points on $\operatorname{Jac}\mathcal{H} \mod \mathfrak{p}$ and show that this number is odd (our proof of Proposition 4.5 amounts to showing that the elliptic curves $y^2 = f(x,x_0)$ and $y^2 = g(x,x_0)$ have trivial 2-torsion for all $x_0 \in \mathbf{Q}$). While this approach is out of reach currently, we pose the following conjecture based on computations in Magma, Pari, and Sage.

Conjecture 4.6. *Let $0 < i \le n$ and t_0 be a reducible specialization such that $t_0 \in T_i$, but $t_0 \notin T_{i+1}$. Then the factorization type of $r_n(x,t_0)$ is $(\underbrace{\ell^i,\ell^i,\ldots,\ell^i}_{\ell \text{ times}}\underbrace{\ell^{i+1},\ell^{i+1},\ldots,\ell^{i+1}}_{\ell-1 \text{ times}},\ldots,\underbrace{\ell^{n-1}\ell^{n-1}\ldots,\ell^{n-1}}_{\ell-1 \text{ times}})$.*

5. Exceptional Specializations

In this section we study the behavior of the Galois group $G_n(t)$ at the irreducible specializations. While $G_n(t_0)$ is a subgroup of $G_n(t)$ for all $t_0 \in K$ (at reducible specializations it is an intransitive subgroup), it is not immediately clear which specializations give rise to proper subgroups and, as a finer measure, the index $[G_n(t) : G_n(t_0)]$ of specialization. We start with a definition.

Definition. Let $n \geq 1$. With all notation as above, let t_0 be an irreducible specialization of $r_n(x,t)$. We say that $t_0 \in K$ is an *exceptional* specialization if $[G_n(t) : G_n(t_0)] > 1$ and define the *defect* of the specialization $\delta_n(t_0)$ to be

$$\delta_n(t_0) = \log_\ell [G_n(t) : G_n(t_0)].$$

If $\delta_n(t_0) = n-1$, then we say the specialization has *maximal defect*; note that $r_n(x,t_0)$ is an irreducible polynomial of degree ℓ^n, hence the defect cannot exceed $n-1$.

An interesting problem in algebraic number theory is to create high-degree, non-abelian extensions of number fields ramified at very few primes (in particular, those ramified at a single prime). The generalized Rikuna polynomials are one path to creating such extensions. The difficulty lies in finding specializations $t_0 \in \mathbf{Q}(\zeta_\ell^+)$ that simultaneously satisfy: 1) $(t_0^2 - \zeta_\ell^+ t_0 + 1)$ is a unit in $\mathbf{Z}[\zeta_\ell^+]$ (ensuring that only the prime above ℓ is ramified); 2) $r_n(x,t_0)$ is irreducible; and 3) Gal $r_n(x,t_0)$ is non-abelian. If all three conditions are satisfied, then the $r_n(x,t_0)$ give rise to non-abelian ℓ-extensions of $\mathbf{Q}(\zeta_\ell^+)$ ramified only above ℓ. Of course, it is not necessary that $t_0^2 - \zeta_\ell^+ t_0 + 1$ be a unit in order for the extension to be unramified outside ℓ, but it is sufficient.

The irreducible specializations $r_n(x,t_0)$ also have the property that their Galois groups over $\mathbf{Q}(\zeta_\ell^+)$ are some of the smallest transitive ℓ-subgroups of S_{ℓ^n}. Indeed, a Sylow-ℓ subgroup of S_{ℓ^n} is a transitive subgroup of order $\ell^{(\ell^n-1)/(\ell-1)}$, while the Galois group of an irreducible specialization of $r_n(x,t)$ is a transitive subgroup of order dividing ℓ^{2n-1} and divisible by ℓ^n. In what follows in this section we will give computational as well as theoretical evidence for some conjectures on the relation between the defect of the specialization and the primes ramifying in the extension, focusing mainly on the case $\ell = 3$ for examples and motivation. To begin, we show the existence of specializations of maximal defect.

Lemma 5.1. *Let $n \geq 1$. If $t_0 \in \left\{ \dfrac{\zeta_\ell^{-1}\zeta_{2\ell}^c - \zeta_\ell}{\zeta_{2\ell}^c - 1} \mid 1 \leq c \leq 2\ell - 1 \right\}$ is an irreducible specialization of $r_n(x,t)$, then t_0 has maximal defect.*

Proof. The t_0 listed in the statement of the Lemma all belong to $\mathbf{Q}(\zeta_\ell^+)$ and represent the values of t for which $\alpha(t)$ is an ℓth or 2ℓth root of unity (excluding 1). Let t_0 be such an irreducible specialization. Then we have $L_n(t_0) = \mathbf{Q}(\zeta_\ell^+)(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha(t_0)}) \simeq \mathbf{Q}(\zeta_{\ell^{n+1}})$. The irreducibility of $r_n(x,t_0)$ ensures that $K_n(t_0)$ is the *maximal* real subfield of $\mathbf{Q}(\zeta_{\ell^{n+1}})$, namely $K_n(t_0) \simeq \mathbf{Q}(\zeta_{\ell^{n+1}}^+)$ which has degree ℓ^n over $\mathbf{Q}(\zeta_\ell^+)$. Therefore t_0 is a specialization of maximal defect. □

Of the $2\ell - 1$ values of t_0 listed in the Lemma, note that some may be reducible specializations. For instance, if $c = \ell$ then $t_0 = \zeta_\ell^+/2$ is a fixed-point of φ and so $r(\zeta_\ell^+/2, \zeta_\ell^+/2) = 0$, whence $r_n(x, \zeta_\ell^+/2)$ is reducible for all $n \geq 1$. On the other hand, there exist irreducible specializations given by the lemma as well. For example, let $c = 4$ so that $t_0 = 0$. Then $\alpha(0) = \zeta_\ell^2$ so that

$$L_n(0) = \mathbf{Q}(\zeta_\ell^+)(\zeta_{\ell^n}, \sqrt[\ell^n]{\zeta_\ell^2}) \simeq \mathbf{Q}(\zeta_{\ell^{n+1}}).$$

The field inclusion $K_n(0) \subset L_n(0)$ induces the factorization

$$2\ell^n = [L_n(0) : \mathbf{Q}(\zeta_\ell^+)] = [L_n(0) : K_n(0)][K_n(0) : \mathbf{Q}(\zeta_\ell^+)],$$

where Gal $L_n(0)/\mathbf{Q}(\zeta_\ell^+) \simeq \mathbf{Z}/2\ell^n$ and $[L_n(0) : K_n(0)] \geq 2$. But the roots of $r_n(x,0)$ are given by

$$\theta_c^{(n)} = \frac{\zeta_\ell - \zeta_{\ell^n}^c \sqrt[\ell^n]{\zeta_\ell^2}}{1 - \zeta_\ell \zeta_{\ell^n}^c \sqrt[\ell^n]{\zeta_\ell^2}}, \qquad 0 \leq c \leq \ell^n - 1,$$

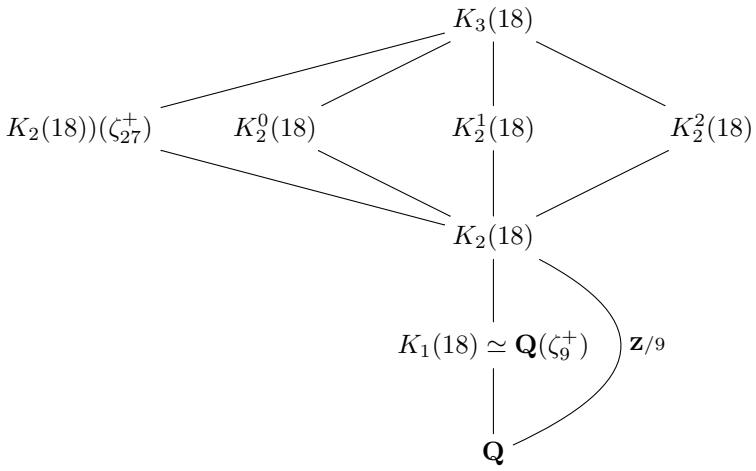
none of which are fixed by the unique subgroup of $\mathbf{Z}/2\ell^n$ of order ℓ. We therefore conclude that the root fields $\mathbf{Q}(\zeta_\ell^+)(\theta_c^{(n)})$ have degree ℓ^n over $\mathbf{Q}(\zeta_\ell^+)$ and, because all are contained in $L_n(0)$, that $K_n(0) \simeq \mathbf{Q}(\zeta_{\ell^{n+1}}^+)$.

It is also useful to exhibit irreducible specializations of positive, non-maximal defect, which we present in the following example.

Example. Let $\ell = 3$. A computer search for integer specializations of t_0 such that $r_3(x, t_0)$ is irreducible and $r_2(x, t_0)$ has Galois group of order 9 returns, among others, $t_0 = 18$. One checks that

- $K_1(18) \simeq \mathbf{Q}(\zeta_9^+)$ (though $\alpha(18)$ is not a 3rd or 6th root of unity);
- $K_2(18) \not\simeq \mathbf{Q}(\zeta_{27}^+)$;
- Gal $r_2(x, 18) \simeq \mathbf{Z}/9$.

The Galois group of $r_3(x, 18)$ is non-abelian of order 81 and the tower of associated subfields has the following shape (for ease of notation, we write $K_{j-1}^i(t_0)$ for $K_{j-1}(t_0)(\theta_i^{(j)}(t_0))$):



Next, apply the discriminant formula $r_n(x, t)$ (equation (1) of Section 3) to the case $\ell = 3$ and $t = 18$ to get

$$\operatorname{disc} r_n(x, 18) = 3^{n3^n + (3^n-1)(3^n-2)/2} \cdot 7^{3(3^n-1)},$$

so the only primes that can ramify in the ring of integers $\mathcal{O}_{K_n(18)}$ are 3 and 7. Thus, the specialization at $t_0 = 18$ produces a non-abelian (once $n \geq 3$) tower of 3-power degree with restricted ramification.

In light of this example, it would be interesting to study the ramification in the specialized towers of positive defect. However, this problem appears to be quite subtle, even in the case $\ell = 3$. For instance, some specializations of maximal defect may be isomorphic to the maximal real subfield of the cyclotomic tower (*e.g.* $t_0 = 0$), while others may not (*e.g.* $K_2(18)$ is not isomorphic to $\mathbf{Q}(\zeta_{27}^+)$). The specializations of positive, non-maximal defect are then interesting examples of non-abelian ℓ-extensions with restricted ramification and should be worthy of future study.

We conclude with an observation on the nature of certain specializations of maximal defect in the case $\ell = 3$. If t_0 is an irreducible specialization of $r_n(x, t)$ with $K_n(t_0) \simeq \mathbf{Q}(\zeta_{3^{n+1}}^+)$, then $r_j(x, t_0)$ is irreducible for all $1 \leq j < n$ and the subfield structure of $\mathbf{Q}(\zeta_{3^{n+1}}^+)$ forces $K_j(t_0) \simeq \mathbf{Q}(\zeta_{3^{j+1}}^+)$ for all $1 \leq j < n$. Therefore, we can give a sufficient condition such that a given specialization t_0 is *not* cyclotomic. In particular, if $K_1(t_0) \not\simeq \mathbf{Q}(\zeta_9^+)$ then $K_n(t_0) \not\simeq \mathbf{Q}(\zeta_{3^{n+1}}^+)$ for all $n \geq 1$. To do this, we will briefly recall Dedekind's criterion, adopting the notation of [6].

Let L be a number field with number ring $\mathcal{O}_L$ and take $x_0 \in \mathcal{O}_L$ so that $L = \mathbf{Q}(x_0)$. Let $\mathcal{O}_f = \mathbf{Z}[x_0] = \mathbf{Z}[x]/(f(x))$, where $f(x)$ is the minimal polynomial of x_0 over $\mathbf{Q}$. Fix a rational prime p and let $\overline{f} = \overline{g_1}^{c_1} \dots \overline{g_r}^{c_r}$ be the reduction of f into irreducible monics modulo p. Group these irreducibles by

exponent: set $e_1 < e_2 < \cdots < e_s$ and let $\overline{f_j}$ be the product of all irreducible factors $\overline{g_i}$ of $\overline{f}$ with $c_i = e_j$; thus

$$\overline{f} = f \pmod p = \overline{g_1}^{c_1} \cdots \overline{g_r}^{c_r} = \overline{f_1}^{e_1} \cdots \overline{f_s}^{e_s}.$$

Choose polynomials $g_i, f_j \in \mathbf{Z}[x]$ with $g_i \equiv \overline{g_i} \pmod p$ and $f_j \equiv \overline{f_j} \pmod p$. Then Dedekind's criterion for $\mathcal{O}_f$ to be isomorphic to $\mathcal{O}_L$ is given by

Theorem 5.2 (Dedekind's criterion)**.** *Let $h = \frac{1}{p}(f_1^{e_1} \dots f_s^{e_s} - f)$. Then $\mathcal{O}_L = \mathcal{O}_f$ if and only if $h \pmod p$ is relatively prime to all factors $\overline{f_j}$ with $e_j > 1$.*

We will apply Dedekind's criterion to the linear shift $r_n(x+t,t)$ of the generalized Rikuna polynomials. We start with a lemma.

Lemma 5.3. *Let $\ell = 3$. For all $n \geq 1$, the polynomial $r_n(x+t,t)$ satisfies the congruence $r_n(x+t,t) \equiv x^{3^n} \pmod{t^2+t+1}$.*

Proof. The proof is by induction where the case $n = 1$ follows from the binomial expansion of $r(x,t)$. If $r_n(x+t,t) \equiv x^{3^n} \pmod{t^2+t+1}$, then write

$$\varphi^{(n)}(x+t) - t \equiv \frac{x^{3^n}}{q_n(x+t)} \pmod{t^2+t+1} \Longrightarrow \varphi^{(n+1)}(x+t) \equiv \varphi\left(\frac{x^{3^n}}{q_n(x+t)}\right) \pmod{t^2+t+1}.$$

A simple computation shows that the right-hand side is congruent to zero modulo t^2+t+1. □

Theorem 5.4. *Let $\ell = 3$. Let $t_0 \in \mathbf{Q}$ be an irreducible specialization of $r_n(x,t)$ such that there exists a prime $p \neq 3$ dividing $t_0^2 + t_0 + 1$ exactly once. Then $K_1(t_0) \not\simeq \mathbf{Q}(\zeta_9^+)$.*

Proof. It suffices to show that a prime p as in the statement of the theorem ramifies in $\mathcal{O}_{K_1(t_0)}$. We use the linear shift as in Lemma 5.3. Suppose $p \neq 3$ divides $t_0^2 + t_0 + 1$ exactly once, and apply the machinery above to our setup. Then $\overline{r} = x^3$ and we choose $h(x) = (r(x+t_0,t_0) - x^3)/p$. It is clear that $\overline{h}(x)$ is coprime to x since $h(0) = r(t_0,t_0) = -(2t_0+1)(t_0^2+t_0+1)$, and if p divides $(t_0^2+t_0+1)$ exactly once, then $p \nmid 2t_0+1$. By Dedekind's criterion, $\mathcal{O}_{K_1(t_0)} \simeq \mathcal{O}_r$ and the prime decomposition of p can thus be read off the factorization modulo p of $r(x+t_0,t_0)$ (it is totally ramified). But the only prime ramifying in $\mathbf{Z}[\zeta_9^+]$ is 3, hence the fields cannot be isomorphic. □

From a computational point of view, it is relatively easy to find such specializations; all we need is a prime $p \neq 3$ dividing $t_0^2 + t_0 + 1$ exactly once. See Appendix A for sample code to check for possible exceptional specializations.

Appendix A. Sample Computations

To get a sense of the paucity of exceptional specializations, the following code was used in the computer-algebra package Sage to test for values of t_0 for which $t_0^2 + t_0 + 1$ is divisible only by primes with exponent greater than or equal to 2. The computations were performed online at `http://www.sagemath.org` and took roughly two hours. The data are displayed in the table below:

```
for a in [-100000000..100000000]:
    for b in [1,100000000]:
        t = a/b
        exps = []
        if not t^2+t+1 == 0:
            n = factor(numerator(QQ(t^2+t+1)))
            for item in list(n):
                if item[1] == 1:
                    exps.append(item[1])

            if exps == []:
                pair = [t, factor(QQ(t^2+t+1))]
                print pair
```

t_0	$t_0^2+t_0+1$	t_0	$t_0^2+t_0+1$
$-5421/6400$	$2^{-16}\cdot 5^{-4}\cdot 7^2\cdot 853^2$	-1	1
$-33/40$	$2^{-6}\cdot 5^{-2}\cdot 37^2$	0	1
$-63/80$	$2^{-8}\cdot 5^{-2}\cdot 73^2$	18	7^3
$-2451/3200$	$2^{-14}\cdot 5^{-4}\cdot 13^2\cdot 223^2$	$88,916$	$7^2\cdot 13^3\cdot 271^2$
$-5/8$	$2^{-6}\cdot 7^2$	$33/800$	$2^{-10}\cdot 5^{-4}\cdot 19^2\cdot 43^2$
$-19,337/32,000$	$2^{-16}\cdot 5^{-6}\cdot 103^2\cdot 271^2$	$21/320$	$2^{-12}\cdot 5^{-2}\cdot 331^2$
$-943/1600$	$2^{-12}\cdot 5^{-4}\cdot 7^2\cdot 199^2$	$19/80$	$2^{-8}\cdot 5^{-2}\cdot 7^2\cdot 13^2$
$-91/160$	$2^{-10}\cdot 5^{-2}\cdot 139^2$	$847/3200$	$2^{-14}\cdot 5^{-4}\cdot 3697^2$
$-69/160$	$2^{-10}\cdot 5^{-2}\cdot 139^2$	$4553/16,000$	$2^{-14}\cdot 5^{-6}\cdot 7^2\cdot 2671^2$
$-657/1600$	$2^{-12}\cdot 5^{-4}\cdot 7^2\cdot 199^2$	$5/16$	$2^{-8}\cdot 19^2$
$-12,663/32,000$	$2^{-16}\cdot 5^{-6}\cdot 103^2\cdot 271^2$	$819/1600$	$2^{-12}\cdot 5^{-4}\cdot 2131^2$
$-3/8$	$2^{-6}\cdot 7^2$	$87/160$	$2^{-10}\cdot 5^{-2}\cdot 7^2\cdot 31^2$
$-749/32,000$	$2^{-14}\cdot 5^{-4}\cdot 13^2\cdot 223^2$	$3/5$	$5^{-2}\cdot 7^2$
$-17/80$	$2^{-8}\cdot 5^{-2}\cdot 73^2$	$26,779/32,000$	$2^{-16}\cdot 5^{-6}\cdot 50,971^2$
$-7/40$	$2^{-6}\cdot 5^{-2}\cdot 37^2$	$7/8$	$2^{-6}\cdot 13^2$
$-979/6400$	$2^{-16}\cdot 5^{-4}\cdot 7^2\cdot 853^2$	$377/400$	$2^{-8}\cdot 5^{-4}\cdot 673^2$
$-88,917$	$7^2\cdot 13^3\cdot 271^2$	$629/640$	$2^{-14}\cdot 5^{-2}\cdot 7^2\cdot 157^2$
-19	7^3		

FIGURE 1. The set of all $t_0 = a/b$ with $-100,000,000 \leq a \leq 100,000,000$ and $1 \leq b \leq 100,000,000$ for which $t_0^2+t_0+1$ is divisible only by primes to powers greater than 1 along with the corresponding factorizations for $t_0^2+t_0+1$.

For these values of t_0 we cannot apply Theorem 7.6 and have to check whether $K_n(t_0)$ is isomorphic to $\mathbf{Q}(\zeta_{3^{n+1}})$ for any n by other means. For these values we find, using the `nfisisom` command implemented in PARI, that the only ones for which $K_1(t_0) \simeq \mathbf{Q}(\zeta_9^+)$ are $t_0 = -19, -1, 0, 18$. Of these, we have seen that $t_0 = -1, 0$ are maximal defect specializations for all n since they specialize to the cyclotomic tower.

REFERENCES

[1] W. Aitken, F. Hajir, C. Maire. Finitely ramified iterated extensions. *Int. Math. Res. Not.*, **14** 855-880 (2005).

[2] Z. Chonoles, J. Cullinan, H. Hausman, A.M. Pacelli, S. Pegado, F. Wei. Arithmetic properties of generalized Rikuna polynomials. *Submitted.* Preprint available at `http://math.bard.edu/cullinan/rikunaweb.pdf`

[3] J. Cullinan, F. Hajir. Ramification in iterated towers for rational functions. *Manuscripta Math.* **137** (2012), no. 3-4, 273286.

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

[5] R.W.K. Odoni. The Galois theory of iterates and composites of polynomials. *Proc. London. Math. Soc.* **(3)**, 51 (1985), 385-414.

[6] P. Schmid. On criteria by Dedekind and Ore for integral ring extensions. *Arch. Math. (Basel)* **84** (2005), no. 4, 304310.

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

[8] J.P. Serre, *Topics in Galois theory. Second edition. With notes by Henri Darmon.* Research Notes in Mathematics, 1. A K Peters, Ltd., Wellesley, MA, 2008

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

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

DEPARTMENT OF MATHEMATICS, BARD COLLEGE, ANNANDALE-ON-HUDSON, NY 12504
E-mail address: `cc2149@bard.edu`

DEPARTMENT OF MATHEMATICS, BARD COLLEGE, ANNANDALE-ON-HUDSON, NY 12504
E-mail address: `cullinan@bard.edu`

DEPARTMENT OF MATHEMATICS, COLBY COLLEGE, WATERVILLE, ME 04901
E-mail address: `ajrasmus@colby.edu`

Department of Mathematics, Reed College, Portland, OR 97202
E-mail address: dtrifuno@reed.edu