NEWLY REDUCIBLE POLYNOMIAL ITERATES

PETER ILLIG, RAFE JONES, ELI ORVIS, YUKIHIKO SEGAWA, NICK SPINALE

RÉSUMÉ. Given a field K and n > 1, we say that a polynomial $f \in K[x]$ has newly reducible *n*th iterate over K if f^{n-1} is irreducible over K, but f^n is not (here f^i denotes the *i*th iterate of f). We pose the problem of characterizing, for given d, n > 1, fields K such that there exists $f \in K[x]$ of degree d with newly reducible *n*th iterate, and the similar problem for fields admitting infinitely many such f. We give results in the cases $(d, n) \in \{(2, 2), (2, 3), (3, 2), (4, 2)\}$ as well as for (d, 2) when $d \equiv 2 \mod 4$. In particular, we show that for all these (d, n) pairs, there are infinitely many monic $f \in \mathbb{Z}[x]$ of degree d with newly reducible *n*th iterate over Q. Curiously, the minimal polynomial $x^2 - x - 1$ of the golden ratio is one example of $f \in \mathbb{Z}[x]$ with newly reducible third iterate; very few other examples have small coefficients. Our investigations prompt a number of conjectures and open questions.

1. INTRODUCTION

Although the mathematical study of the golden ratio dates to antiquity, one of its unusual properties appears to have passed the millennia unnoticed : its minimal polynomial $f(x) = x^2 - x - 1$ is irreducible over \mathbb{Q} , as is the second iterate f(f(x)) of this polynomial, but

(1.1)
$$f(f(f(x))) = (x^4 - 3x^3 + 4x - 1)(x^4 - x^3 - 3x^2 + x + 1),$$

where the two quartics are irreducible. The factorization in (1.1) together with the irreducibility over \mathbb{Q} of f(f(x)) is a rare phenomenon : among polynomials $x^2 + ax + b$ with a, b integers satisfying $|a| \leq 100,000$ and $|b| \leq 1,000,000,000$, only 8 others have this property. One might wonder whether there are infinitely many such polynomials. Indeed there are, as we show in Theorem 1.3 below.

More generally, let K be a field and $f \in K[x]$ a polynomial of degree $d \ge 2$. Write $f^n(x)$ for the nth iterate of f. We say that f has a newly reducible nth iterate (over K) for some $n \ge 2$ if f^{n-1} is irreducible over K but f^n is not irreducible over K. We note that the irreducibility of f^{n-1} implies that each of f, f^2, \ldots, f^{n-2} is also irreducible over K. Several recent papers have given conditions ensuring that all iterates of a polynomial remain irreducible (see e.g. [3], [4], [8], [10], [11], [12]). Many fewer have studied newly reducible iterates; a few examples are [6], [9], and [15]. In this paper our main objects of study are the following.

Definition 1.1. Let d, n be integers that are at least two. Define $\mathcal{N}_{d,n}$ (resp. $\mathcal{N}_{d,n}^{\infty}$) to be the class ¹ of all fields K such that there exists at least one (resp. infinitely many) $f \in K[x]$ of degree d with newly reducible nth iterate over K.

When K is a perfect field, the question of whether $K \in \mathcal{N}_{d,n}$ can be phrased as an inverse Galois-type problem : does there exist $f \in K[x]$ such that the absolute Galois group of K acts

²⁰¹⁰ Mathematics Subject Classification. Primary: 37P15. Secondary: 11R09, 37P05, 37P25.

^{1.} Because the collection of all fields is not a set, neither are $\mathcal{N}_{d,n}$ and $\mathcal{N}_{d,n}^{\infty}$. We use them in this article not as objects, but as notational devices. In referring to them we use the usual notation and language of set theory.

transitively on the roots of f^{n-1} but not on the roots of f^n ? Fein and Schacher [9] appear to be the first to have studied newly reducible iterates, and they used results of Odoni to obtain the fundamental result in this area : for all $d, n \geq 2$, $\mathcal{N}_{d,n}$ is non-empty ([9, Corollary 1.3]). Their method relies on knowledge of the Galois groups of iterates of generic polynomials, and then an appeal to the Hilbert irreducibility theorem; the resulting field K depends on the choice of specialization. Our aim is to address at least some cases of the following questions, each of which is unresolved by the methods of [9].

Question 1.2. Let d, n be integers that are at least 2.

- (1) Precisely which fields belong to $\mathcal{N}_{d,n}$ and $\mathcal{N}_{d,n}^{\infty}$?
- (2) For which d, n is $\mathbb{Q} \in \mathcal{N}_{d,n}$? For which d, n is $\mathbb{Q} \in \mathcal{N}_{d,n}^{\infty}$?
- (3) If K is a number field with ring of integers \mathcal{O}_K and $K \in \mathcal{N}_{d,n}^{\infty}$, do there exist infinitely many monic $f \in \mathcal{O}_K[x]$ of degree d with newly reducible nth iterate over K?

The case $K = \mathbb{Q}$ has received significant attention recently. The recent paper [10] of Goksel describes an infinite family of monic quadratic $f \in \mathbb{Z}[x]$ with newly reducible third iterate [10, Lemma 3.9], thereby showing that $\mathbb{Q} \in \mathcal{N}_{2,3}$. The paper [15] gives an infinite family of non-monic cubic $f \in \mathbb{Z}[x]$ with newly reducible second iterate, thus proving $\mathbb{Q} \in \mathcal{N}_{3,2}$, and conjectures that no such family exists among monic cubic $f \in \mathbb{Z}[x]$ [15, Conjecture 4.1].

We summarize our main results. Throughout the article, we sometimes use char(K) to denote the characteristic of a field K.

Theorem 1.3. Let K be an infinite field with $char(K) \neq 2$, and for $n \geq 2$ set $K^n = \{k^n : k \in K\}$.

- (1) We have $K \in \mathcal{N}_{2,2}$ if and only if $K \neq K^2$, and $K \in \mathcal{N}_{2,2}^{\infty}$ if and only if $K \setminus K^2$ is infinite (Proposition 3.2).
- (2) We have K ∈ N_{2,3}[∞] if
 -1 ∉ K² and K has a discrete valuation v with v(5) odd (Proposition 3.6); or
 K is a totally real number field and there is a prime of residue degree 1 lying over (3) (Corollary 3.7).
- (3) We have $K \in \mathcal{N}_{3,2}^{\infty}$ if $char(K) \neq 3$ and $2 \notin K^3$ (Theorem 5.1).
- (4) We have $K \in \mathcal{N}_{4,2}^{\infty}$ if $char(K) \neq 3, 3 \notin K^2$, and $-3 \notin K^4$ (Corollary 6.3).
- (5) We have $K \in \mathcal{N}_{d,2}^{\infty}$ for all $d \equiv 2 \pmod{4}$ if $-1 \notin K^2$ and K has a non-trivial discrete valuation (Corollary 7.2).

In each case, we exhibit an explicit infinite family of polynomials with the desired properties, and if K is a number field the polynomials may be taken to be monic with coefficients in \mathcal{O}_K without loss of generality. For instance, a consequence of Theorem 5.1 is that if

(1.2)
$$f(x) = \left(x + 93312t^9 + 36t^3\right)^3 - 93312t^9$$

for $t \in \mathbb{Z} \setminus \{0\}$, then f has a newly reducible second iterate over \mathbb{Q} . This disproves Conjecture 4.1 of [15], which is based on a search of all polynomials of the form $x^3 + ax^2 + bx + c$, where a, b, c are integers with absolute value at most 500; it is noteworthy that none of the polynomials in (1.2) are of this form.

When K is a finite field of characteristic not equal to 2, all the statements of Theorem 1.3 hold with $\mathcal{N}_{d,n}^{\infty}$ replaced by $\mathcal{N}_{d,n}$, although (5) and the first statement of (2) become vacuous. We

have $\mathbb{F}_2 \notin \mathcal{N}_{2,2}$, since $f(x) = x^2 + x + 1$ is the only irreducible quadratic over \mathbb{F}_2 , and $f^2(x)$ is irreducible over \mathbb{F}_2 . We prove in Proposition 3.4 that $\mathbb{F}_{2^n} \in \mathcal{N}_{2,2}$ for all n > 1 and $\mathbb{F}_{2^n} \in \mathcal{N}_{2,3}$ for all $n \ge 1$. Surprisingly, $\mathbb{F}_{2^n} \notin \mathcal{N}_{2,k}$ for any $k \ge 4$ and any $n \ge 1$, due to a result of Ahmadi et al [2, Theorem 10] (see also [1]) that every $f \in \mathbb{F}_{2^n}[x]$ has $f^3(x)$ reducible.

When K is a general field of characteristic 2, we know of no results addressing whether $K \in \mathcal{N}_{d,n}$ for any d, n, though we give a condition that applies to the case d = n = 2 in Proposition 3.3. This leads us to pose the following question.

Question 1.4. Let p be a prime number and $d \ge p$. Which fields of characteristic p belong to $\mathcal{N}_{d,n}$ for various $n \ge 2$?

The results of Theorem 1.3 prompt the following two conjectures.

Conjecture 1.5. For each $d, n \geq 2$, $\mathcal{N}_{d,n}^{\infty}$ is non-empty.

Conjecture 1.6. Let K be a finite extension of \mathbb{Q} or $\mathbb{F}_p(t)$. Then $K \in \mathcal{N}_{2,3}^{\infty}$ and $K \in \mathcal{N}_{d,2}^{\infty}$ for every $d \geq 2$.

The proofs of the statements in Theorem 1.3 proceed by enumerating all f of a specified form such that $f^n(x)$ is reducible, and then giving conditions under which infinitely many f remain after discarding those with f^m reducible for m < n. In the case where f is quadratic, the specified form is $f(x) = (x - \gamma)^2 + \gamma + m$, so that γ is the critical point of f, and this includes all f. We thus obtain the following result.

Theorem 1.7. Let K be a field of characteristic not equal to 2, and let $f(x) = (x - \gamma)^2 + \gamma + m \in K[x]$. Then f has a newly reducible third iterate over K if and only if the following both hold :

(1) There exist $r, s \in K$ such that

$$\begin{split} \gamma &= \frac{1}{256r^2} (-2r^5s^2 + 9r^4s^4 - 4r^4s^2 - 16r^3s^6 + 32r^3s^4 + 16r^3s^2 + 32r^3 + 14r^2s^8 \\ &\quad - 64r^2s^6 - 8r^2s^4 + 96r^2s^2 + 128r^2 - 6rs^{10} + 48rs^8 - 64rs^6 \\ &\quad - 160rs^4 + 96rs^2 + 128r + s^{12} - 12s^{10} + 40s^8 - 112s^4 - 64s^2), \\ m &= \frac{-r^2 - 2rs^2 - 4r + s^4 - 4s^2 - 4}{8r}. \end{split}$$

$$(2) \text{ None of } \sqrt{-m - \gamma}, \sqrt{-2m + 2\sqrt{m^2 + m + \gamma}}, \sqrt{-2m - 2\sqrt{m^2 + m + \gamma}} \text{ is in } K. \end{split}$$

We note that taking $K = \mathbb{Q}$ and r = s = 1 in Theorem 1.7 gives $\gamma = 1/2$ and m = -7/4. This yields $f(x) = (x - 1/2)^2 + 1/2 - 7/4 = x^2 - x - 1$, and thus we recover the minimal polynomial of the golden ratio, mentioned in the first paragraph. Observe that for this polynomial, $-m - \gamma = 5/4$ and $m^2 + m + \gamma = 29/16$, ensuring that condition (2) in Theorem 1.7 holds.

In general, a convenient way to verify the conditions in part (2) of Theorem 1.7 is to show that neither $-m - \gamma$ nor $m^2 + m + \gamma$ is a square in K. With γ, m as in part (1) of Theorem 1.7, up to squares in K(r, s) we have $-m - \gamma = 2r - s^2 + 4$ and

$$m^{2} + m + \gamma = -2s^{2}r^{3} + (5s^{4} + 4s^{2} + 4)r^{2} + (-4s^{6} + 12s^{4} + 32s^{2} + 16)r + s^{8} - 8s^{6} + 8s^{4} + 32s^{2} + 16r^{2} +$$

In [10, Lemma 3.9], Goksel studies the case m = -1 and gives algebraic characterizations of all γ making $f^2(x)$ and $f^3(x)$ reducible. We recover his results as an outcome of our proof of

Theorem 1.7 (see the discussion following the proof of Theorem 3.5). We use Theorem 1.7 to give another family with non-constant m in Theorem 3.7.

We close this introduction with three additional questions, and an outline of the paper.

Question 1.8. Is $\mathbb{Q} \in \mathcal{N}_{2,4}$?

We have not been able to find any quadratic $f \in \mathbb{Q}[x]$ with newly reducible fourth iterate; we briefly discuss some work on this question in Section 4. We remark that [10, Theorem 1.2] shows that for $m \in \{0, -1, -2\}$ (i.e. when f is post-critically finite), there is no $\gamma \in \mathbb{Z}$ that works.

Question 1.9. Does there exist $f \in \mathbb{Q}[x]$ such that deg f = 3 and f^2 is newly reducible with three distinct factors, each of degree 3?

In the course of our study of cubic polynomials in Section 5 we find infinite families with newly reducible second iterate, but all such families with $f \in \mathbb{Q}[x]$ have $f^2(x)$ that factors as a product of an irreducible sextic and cubic. It would be interesting to find an $f \in \mathbb{Q}[x]$ with second iterate factoring as in Question 1.9. More generally, it would be interesting to study polynomials with newly reducible iterates that have more than two irreducible factors.

To motivate our last question, we remark that the fields in $\mathcal{N}_{d,n}$ constructed in [9] are number fields whose degrees grow very rapidly with n and d.

Question 1.10. Fix $d \ge 2$, and let m_n be the minimal degree of a number field K over which there is $f \in K[x]$ of degree d with newly reducible nth iterate. Is $(m_n)_{n\ge 2}$ unbounded? Does $\lim_{n\to\infty} m_n = \infty$?

In Section 2, we prove under mild hypotheses that if f has a newly reducible nth iterate, then the factorization of f^n must have a certain form. This generalizes some of the results from [5]. These results are particularly useful in the case where f is quadratic, which we study in Section 3, proving Theorem 1.7 and parts (1) and (2) of Theorem 1.3, as well as some results for fields of characteristic 2, such as Proposition 3.4. Section 4 contains brief remarks on Question 1.8. In Section 5, we study cubics with newly reducible second iterate, and prove part (3) of Theorem 1.3. Sections 6 and 7 study polynomials of higher degree with newly reducible second iterate, and contain the proofs of parts (4) and (5) of Theorem 1.3.

Acknowledgements. We thank the anonymous referee for helpful comments. We are also grateful to Carleton College's Towsley Endowment for the Sciences, which partially supported the research of the third author.

2. The form of factors

We begin with some very general results on factorization of iterates, culminating in Theorem 2.5, which gives a generalization of [5, Proposition 2.6] to arbitrary characteristic. The key lemma, Lemma 2.3, can be proven using Capelli's Lemma, as in [5, Proposition 2.6], but we give here a self-contained proof.

Fix an algebraic closure \overline{K} and separable closure K^{sep} of K. Recall that $f \in K[x]$ is separable over K if it has deg f distinct roots in \overline{K} , or equivalently, all roots of f in \overline{K} lie in K^{sep} .

Definition 2.1. Let K be a field and $f \in K[x]$ have degree 2n for some $n \ge 1$. We say that f is symmetrically reducible over K if there exists a monic $g \in K[x]$ with f(x) = Cg(x)g(-x) for some $C \in K$.

Lemma 2.2. Let K be a field, and let $f(x) \in K[x]$ have degree $d \ge 2$. If $f^n(x)$ is newly reducible for some $n \ge 2$, then each irreducible factor of $f^n(x)$ has degree divisible by d^{n-1} .

Démonstration. Let $\alpha \in \overline{K}$ be a root of $f^n(x)$. Then $f(\alpha) \in K(\alpha)$, and so $K(f(\alpha)) \subseteq K(\alpha)$. Hence

(2.1)
$$[K(\alpha):K] = [K(\alpha):K(f(\alpha))][K(f(\alpha)):K] = d^{n-1}[K(\alpha):K(f(\alpha))],$$

where the last equality follows because $f(\alpha)$ is a root of $f^{n-1}(x)$ and f^{n-1} is assumed to be irreducible over K. Now let h be any irreducible factor of f^n , and α a root of h. Then deg $h = [K(\alpha) : K]$ is divisible by d^{n-1} from (2.1).

Lemma 2.3. Let K be a field and let $g, f \in K[x]$ be separable over K. Assume g is irreducible over K, and let $h \in K[x]$ be any non-constant factor of $g \circ f$. Consider the map

(2.2)
$$\Phi: \{ roots \ of \ h \ in \ K^{sep} \} \to \{ roots \ of \ g \ in \ K^{sep} \}$$

defined by $\Phi(\alpha) = f(\alpha)$. Then Φ is a surjective k-to-1 map for some k with $1 \le k \le \deg f$.

Démonstration. First note that a root α of h satisfies $g(f(\alpha)) = 0$, and so $f(\alpha)$ is indeed a root of g, showing that Φ is well-defined. Because h is non-constant, the image of Φ is non-empty.

Let $G_K := \text{Gal}(K^{\text{sep}}/K)$ be the absolute Galois group of K. The key observation is that since f is defined over K, it must commute with the action of G_K on K^{sep} . Hence if α' is a root of g and $f(\alpha) = \alpha'$, then for any $\sigma \in G_K$ we have

(2.3)
$$\sigma(\alpha') = \sigma(f(\alpha)) = f(\sigma(\alpha)).$$

Now let α', β' be roots of g. Because g is irreducible over K, G_K acts transitively on the roots of g, and hence there is some $\sigma \in G_K$ with $\sigma(\alpha') = \beta'$. From (2.3) we have $\beta' = f(\sigma(\alpha))$. If we further assume that α is a root of h, then so must be $\sigma(\alpha)$, since h is defined over K and hence the set of its roots is preserved by G_K . Therefore σ induces a map $\Phi^{-1}(\alpha') \to \Phi^{-1}(\beta')$. This map is injective since σ is an injection from the set of all roots of $g \circ f$ into itself. Similarly, σ^{-1} gives an injection $\Phi^{-1}(\beta') \to \Phi^{-1}(\alpha')$. It follows that $\#\Phi^{-1}(\alpha') = \#\Phi^{-1}(\beta')$, and thus all fibers of Φ have equal cardinality. But Φ has non-empty image, and the lemma is proved.

Lemma 2.4. Let K be a field and $f \in K[x]$. If f is irreducible over K and f' is not identically zero, then all iterates of f are separable over K.

Démonstration. Fix an algebraic closure \overline{K} of K, and recall the well-known fact that $g \in K[x]$ is separable over K if and only if g and g' have no common roots in \overline{K} . We proceed by induction on n, the number of iterations of f. Let n = 1, and suppose there is $\alpha \in \overline{K}$ with $f(\alpha) = f'(\alpha) = 0$. Because f is irreducible over K, we have $[K(\alpha) : K] = \deg f$. But $\deg f' < \deg f$, and so $f'(\alpha) = 0$ forces f' to be identically zero, which is a contradiction.

Assume now that f^n is separable over K for some $n \ge 1$. The chain rule gives

(2.4)
$$(f^{n+1})'(x) = (f^n)'(f(x)) \cdot f'(x)$$

Suppose that $\alpha \in \overline{K}$ satisfies $f^{n+1}(\alpha) = (f^{n+1})'(\alpha) = 0$. From (2.4), we have either $(f^n)'(f(\alpha)) = 0$ or $f'(\alpha) = 0$. In the former case, we also have $0 = f^{n+1}(\alpha) = f^n(f(\alpha))$, contradicting the separability of f^n . In the latter case, we also have $0 = f^{n+1}(\alpha) = f(f^n(\alpha))$, implying that $f^n(\alpha)$ is a root of f with $[K(f^n(\alpha)) : K] \leq [K(\alpha) : K] \leq \deg f' < \deg f$. This contradicts the irreducibility of f.

Theorem 2.5. Let K be a field, let $f(x) = ax^2 + bx + c \in K[x]$ with $a \neq 0$, and assume that f' is non-zero. If $f^n(x)$ is newly reducible over K for some $n \geq 2$, then there is a monic irreducible $h \in K[x]$ of degree 2^{n-1} such that

$$f^{n}(x) = a^{2^{n}-1}h(x)h(-(x + (b/a))).$$

In particular, if K has characteristic not equal to 2, then $f^n(x + \gamma)$ is symmetrically reducible over K, where $\gamma = -b/2a$ is the critical point of f.

Démonstration. Assume that f^n is newly reducible over K for some $n \ge 2$, and observe that by Lemma 2.2 we have $f^n(x) = \ell(f^n)h_1(x)h_2(x)$, where $\ell(f^n)$ is the leading coefficient of f^n , and $h_1, h_2 \in K[x]$ are monic irreducibles of degree 2^{n-1} . An easy induction shows that $\ell(f^n) = a^{2^n-1}$. By Lemma 2.4, both f^{n-1} and f^n are separable over K, and it follows that h_1 and h_2 are separable over K as well. By Lemma 2.3, we have that for i = 1, 2 the maps

$$\Phi_i: \{\text{roots of } h_i \text{ in } K^{\text{sep}}\} \to \{\text{roots of } f^{n-1} \text{ in } K^{\text{sep}}\}$$

defined by $\Phi_i(\alpha) = f(\alpha)$, are bijections. Therefore $\Phi_2^{-1} \circ \Phi_1$ is a bijection from the roots of h_1 to the roots of h_2 . Letting α be a root of h_1 , we have that $\Phi_2^{-1}(\Phi_1(\alpha))$ is a root β of h_2 satisfying $f(\alpha) = f(\beta)$. This gives $a\alpha^2 + b\alpha = a\beta^2 + b\beta$, and because $\alpha \neq \beta$ we further deduce $\beta = -\alpha - \frac{b}{a}$.

Now let $\alpha_1, \ldots, \alpha_{2^{n-1}}$ be the roots of h_1 in K^{sep} and $\beta_1, \ldots, \beta_{2^{n-1}}$ be the roots of h_2 in K^{sep} . We have

$$h_2(x) = \prod_{i=1}^{2^{n-1}} (x - \beta_i) = \prod_{i=1}^{2^{n-1}} (x - (-\alpha_i - (b/a))) = \prod_{i=1}^{2^{n-1}} ((x + (b/a)) + \alpha_i)$$

Because $n \ge 1$, this last expression is the same as $\prod_{i=1}^{2^{n-1}} (-(x+\frac{b}{a})-\alpha_i)$, which is $h_1(-(x+\frac{b}{a}))$. If K has characteristic not equal to 2, then from $f^n(x) = \ell(f^n)h_1(x)h_1(-(x+\frac{b}{a}))$ we have

If K has characteristic not equal to 2, then from $f^n(x) = \ell(f^n)h_1(x)h_1(-(x+\frac{b}{a}))$ we have $f^n(x-\frac{b}{2a}) = \ell(f^n)h_1(x-\frac{b}{2a})h_1(-(x+\frac{b}{2a}))$, whence $f^n(x-\frac{b}{2a}) = \ell(f^n)g(x)g(-x)$ for $g(x) = h_1(x-\frac{b}{2a})$. Thus $f^n(x-\frac{b}{2a})$ is symmetrically reducible over K.

3. QUADRATIC POLYNOMIALS WITH NEWLY REDUCIBLE SECOND AND THIRD ITERATE

A monic quadratic polynomial in K[x] has the form $x^2 + ax + b$, but when K has characteristic not equal to 2 we may write it as $(x - \gamma)^2 + m + \gamma$ with $\gamma = -a/2$ and $m = b + a/2 - a^2/4$. This latter form emphasizes the critical point γ of f, and behaves more simply with respect to iteration. In this section, we prove Theorem 1.7 and give some results in the case where K has characteristic 2.

To prove Theorem 1.7, it is enough, in light of Theorem 2.5, to characterize quadratic polynomials with symmetrically reducible third iterate, and then discard those with a reducible first or second iterate. Clearly f(x) is reducible over K if and only if $\sqrt{-m-\gamma}$ is in K.

We begin by giving a criterion for when $f^2(x + \gamma)$ has symmetrically reducible second iterate.

Lemma 3.1. Let K be a field of characteristic not equal to 2, and let $f(x) = (x - \gamma)^2 + \gamma + m$ for $\gamma, m \in K$. Then $f^2(x + \gamma)$ is symmetrically reducible over K if and only if at least one of

$$\sqrt{-2m \pm 2\sqrt{m^2 + m + \gamma}}$$

is in K.

Démonstration. We have

$$f^{2}(x) = (x - \gamma)^{4} + 2m(x - \gamma)^{2} + m^{2} + m + \gamma.$$

On the other hand, by definition $f^2(x + \gamma)$ is symmetrically reducible over K if and only if $f^2(x + \gamma) = (x^2 + cx + d)(x^2 - cx + d)$ for some $c, d \in K$. Equating coefficients gives

$$(3.1) m^2 + m + \gamma = d^2$$

$$(3.2) 2m = 2d - c^2$$

Clearly (3.1) has a solution $d \in K$ if and only if $\sqrt{m^2 + m + \gamma} \in K$. Substituting $d = \pm \sqrt{m^2 + m + \gamma}$ into (3.2), we see that

$$c = \pm \sqrt{-2m \pm 2\sqrt{m^2 + m + \gamma}}.$$

If one of these choices of c lies in K, then so does the corresponding choice of d, and hence $f^2(x + \gamma)$ is symmetrically reducible over K. On the other hand, if neither of $\sqrt{-2m \pm 2\sqrt{m^2 + m + \gamma}}$ is in K, then there is no $c \in K$ satisfying (3.2), and hence $f^2(x + \gamma)$ is not symmetrically reducible over K.

Proposition 3.2. Let K be a field of characteristic not equal to 2, and let $K^2 = \{k^2 : k \in K\}$. Then $K \in \mathcal{N}_{2,2}$ (resp. $K \in \mathcal{N}_{2,2}^{\infty}$) if and only if $K \neq K^2$ (resp. $K \setminus K^2$ is infinite).

Démonstration. Equations (3.1) and (3.2) imply that for any $a, b \in K$ we can construct f with symmetrically reducible second iterate, simply by taking $m = a - \frac{1}{2}b^2$ and $\gamma = a^2 - m^2 - m$. Taking b = 2 yields the family $f(x) = (x - (3a - 2))^2 + 4a - 4$ for $a \in K$, for which we have

$$f^{2}(x) = \left(x^{2} + (-6a + 2)x + 9a^{2} - 5a\right)\left(x^{2} + (-6a + 6)x + 9a^{2} - 17a + 8\right)$$

Thus f has newly reducible second iterate provided f(x) is irreducible over K, and because K has characteristic not equal to 2, this is equivalent to $1 - a \notin K^2$. Because $x \mapsto 1 - x$ is a bijection on K, it follows that $K \in \mathcal{N}_{2,2}$ (resp. $K \in \mathcal{N}_{2,2}^{\infty}$) if $K \neq K^2$ (resp. $K \setminus K^2$ is infinite). The converse follows from the observation that $K = K^2$ implies that no quadratic polynomial over K is irreducible, and $K \setminus K^2$ finite implies that only finitely many quadratic polynomials over K are irreducible.

When K has characteristic 2, the corresponding result to Lemma 3.1 is more complicated.

Lemma 3.3. Let K be a field of characteristic 2, and let $f(x) = x^2 + ax + b$. Then $f^2(x) = h(x)h(x+a)$ for some $h \in K[x]$ if and only if b = 0, b = a + 1, or

(3.3)
$$x^4 + a^2x^3 + a^3x^2 + a^2(b^2 + ab + b)x + (b^2 + ab + b)^2$$

has a root in K.

Démonstration. We have $f^2(x) = x^4 + (a^2 + a)x^2 + a^2x + (b^2 + ab + b)$. Letting $h(x) = x^2 + cx + d$ and equating coefficients in $f^2(x) = h(x)h(x + a)$ gives

$$a2 + ac + c2 = a2 + a$$
$$a2c + ac2 = a2$$
$$a2d + acd + d2 = b2 + ab + b$$

The first equation gives $ac+c^2+a=0$, which renders the second equation redundant. Multiplying through by a^2d^2 gives $a^2d(acd) + (acd)^2 + a^3d^2 = 0$. From the third equation we have $acd = a^2d + d^2 + b^2 + ab + b$, and substitution yields

$$a^{2}d(a^{2}d + d^{2} + b^{2} + ab + b) + (a^{2}d + d^{2} + b^{2} + ab + b)^{2} + a^{3}d^{2} = 0.$$

Expanding, simplifying, and writing this as a polynomial in d yields

$$d^4 + a^2 d^3 + a^3 d^2 + (a^3 b + a^2 b^2 + a^2 b)d + a^2 b^2 + b^4 + b^2 = 0,$$

which is equivalent to $x^4 + a^2x^3 + a^3x^2 + a^2(b^2 + ab + b)x + (b^2 + ab + b)^2$ having a root in K. When such a root exists, we may solve for c provided that $a \neq 0$ and $d \neq 0$. But a = 0 forces c = 0, and so we obtain c anyway. If d = 0, then we get $b^2 + ab + b = 0$, and so b = 0 or b = a + 1.

Remark. It follows from Theorem 2.5 and Lemma 3.3 that f(x) has a newly reducible second iterate over K if and only if f is irreducible and the polynomial in (3.3) has a root in K. This is because if b = 0 then f(0) = 0, and if b = a + 1 then f(1) = 0, and thus f is reducible in both cases.

We now turn to finite fields of characteristic 2. In particular, one might ask which of the fields \mathbb{F}_{2^n} belong to $\mathcal{N}_{2,k}$ for various $k \geq 2$? When $k \geq 4$, this question has been settled by Ahmadi et al [2, Theorem 10] (see also [1]), and the answer is surprising : none of them. The result [2, Theorem 10] gives that if $f \in \mathbb{F}_{2^n}[x]$ is quadratic, then $f^3(x)$ is reducible over \mathbb{F}_{2^n} .

As for $\mathcal{N}_{2,2}$ and $\mathcal{N}_{2,3}$, observe that $\mathbb{F}_2 \notin \mathcal{N}_{2,2}$, since the unique irreducible quadratic polynomial $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ has $f^2(x)$ irreducible. By adapting the methods of [1], we show the following.

Proposition 3.4. Let $K = \mathbb{F}_{2^n}$. Then $K \in \mathcal{N}_{2,2}$ for all $n \geq 2$ and $K \in \mathcal{N}_{2,3}$ for all $n \geq 1$.

Démonstration. Let $K = \mathbb{F}_{2^n}$, and $f(x) = x^2 + ax + b \in K[x]$, and denote the trace map $K \to \mathbb{F}_2$ by $\operatorname{Tr}_{K/\mathbb{F}_2}$. By a standard result in field theory [14, Corollary 3.6], we have that f is irreducible over K if and only if $a \neq 0$ and $\operatorname{Tr}_{K/\mathbb{F}_2}(b/a^2) = 1$. Assume that this holds. Then by Capelli's Lemma ([1, 7]), $f^2(x)$ is reducible over K if and only if $f(x) - \alpha$ is reducible over $K(\alpha)$, where $f(\alpha) = 0$. Applying [14, Corollary 3.6] again, this is equivalent to $\operatorname{Tr}_{K(\alpha)/\mathbb{F}_2}((b-\alpha)/a^2) = 0$. Properties of the trace now give

$$\operatorname{Tr}_{K(\alpha)/\mathbb{F}_{2}}((b-\alpha)/a^{2}) = \operatorname{Tr}_{K(\alpha)/\mathbb{F}_{2}}(b/a^{2}) - \operatorname{Tr}_{K(\alpha)/\mathbb{F}_{2}}(\alpha/a^{2})$$
$$= 2\operatorname{Tr}_{K/\mathbb{F}_{2}}(b/a^{2}) + \operatorname{Tr}_{K/\mathbb{F}_{2}}(\operatorname{Tr}_{K(\alpha)/K}(\alpha/a^{2}))$$
$$= \operatorname{Tr}_{K/\mathbb{F}_{2}}(a/a^{2}).$$

To show that $K \in \mathcal{N}_{2,2}$, we thus seek $a, b \in K$ with $a \neq 0$, $\operatorname{Tr}_{K/\mathbb{F}_2}(b/a^2) = 1$, and $\operatorname{Tr}_{K/\mathbb{F}_2}(1/a) = 0$. If there are $r, s \in K$ with $r \neq 0$, $\operatorname{Tr}_{K/\mathbb{F}_2}(r) = 0$, and $\operatorname{Tr}_{K/\mathbb{F}_2}(s) = 1$, then we can take a = 1/r and $b = s/r^2$. Now because K is a separable extension of \mathbb{F}_2 , the bilinear form $(x, y) = \operatorname{Tr}_{K/\mathbb{F}_2}(xy)$ is non-degenerate, and taking y = 1 gives that $\operatorname{Tr}_{K/\mathbb{F}_2}$ is a surjective homomorphism from the additive group of K to the additive group of \mathbb{F}_2 . Therefore we can find the desired r, s provided that |K| > 2.

To show that $K \in \mathcal{N}_{2,3}$, we seek $a, b \in K$ with $a \neq 0$ and $\operatorname{Tr}_{K/\mathbb{F}_2}(b/a^2) = \operatorname{Tr}_{K/\mathbb{F}_2}(1/a) = 1$. This ensures that $f^2(x)$ is irreducible over K, and then by [2, Theorem 10] we have that $f^3(x)$ is reducible over K. If we find $r \in K$ with $r \neq 0$ and $\operatorname{Tr}_{K/\mathbb{F}_2}(r) = 1$, then we may take a = b = 1/r. Because $\operatorname{Tr}_{K/\mathbb{F}_2} : K^+ \to \mathbb{F}_2^+$ is a surjective homomorphism, the desired r must exist. \Box The techniques of Proposition 3.4 and [2, Theorem 10] do not apply to general fields of characteristic 2, and it remains an open question which of them belong to $\mathcal{N}_{2,2}$ and $\mathcal{N}_{2,3}$. See Question 1.4.

We now give a characterization of quadratic polynomials f(x) such that $f^3(x + \gamma)$ is symmetrically reducible.

Theorem 3.5. Let K be a field of characteristic not equal to 2, and let $f(x) = (x - \gamma)^2 + \gamma + m \in K[x]$. Then $f^3(x + \gamma)$ is symmetrically reducible over K if and only if $\gamma = -m$ or there exist $r, s \in K$ such that

$$(3.4) \qquad \gamma = \frac{1}{256r^2} \left(-2r^5s^2 + 9r^4s^4 - 4r^4s^2 - 16r^3s^6 + 32r^3s^4 + 16r^3s^2 + 32r^3 + 14r^2s^8 - 64r^2s^6 - 8r^2s^4 + 96r^2s^2 + 128r^2 - 6rs^{10} + 48rs^8 - 64rs^6 - 160rs^4 + 96rs^2 + 128r + s^{12} - 12s^{10} + 40s^8 - 112s^4 - 64s^2 \right)$$

$$(3.5) \qquad m = \frac{-r^2 - 2rs^2 - 4r + s^4 - 4s^2 - 4}{8r}$$

Démonstration. First, if $\gamma = -m$ then $f^3(x+\gamma) = (x^4 - 2\gamma x^2 + \gamma^2 - \gamma)^2$, so $f^3(x+\gamma)$ is symmetrically reducible. Otherwise, suppose that there exist $r, s \in K$ that satisfy (3.4) and (3.5). Note that $r \neq 0$. Then we compute $f^3(x+\gamma)$ and substitute the expressions in r and s for γ and m. This gives

$$f^{3}(x+\gamma) = \frac{h(x)}{64r^{2}} \cdot \frac{h(-x)}{64r^{2}},$$

where

$$\begin{split} h\left(x\right) &= 64r^{2}x^{4} - 64r^{2}sx^{3} + \left(-16r^{3} - 64r^{2} + 16rs^{4} - 64rs^{2} - 64r\right)x^{2} \\ &+ \left(24r^{3}s + 64r^{2}s - 8rs^{5} + 32rs^{3} + 32rs\right)x + \left(r^{4} - 12r^{3}s^{2} + 10r^{2}s^{4} - 24r^{2}s^{2} - 8r^{2} - 4rs^{6} + 16rs^{4} + 16rs^{2} + s^{8} - 8s^{6} + 8s^{4} + 32s^{2} + 16\right). \end{split}$$

Therefore, $f^3(x + \gamma)$ is symmetrically reducible.

Conversely, suppose that $f^3(x + \gamma)$ is symmetrically reducible. Our goal is to show either that $\gamma = -m$ or that (3.4) and (3.5) hold for some $r, s \in K$. We have

$$f^{3}(x+\gamma) = x^{8} + 4mx^{6} + (6m^{2} + 2m)x^{4} + (4m^{3} + 4m^{2})x^{2} + (m^{4} + 2m^{3} + m^{2} + m + \gamma).$$

Since $f^3(x + \gamma)$ is symmetrically reducible, by definition there exist $h_1, h_2 \in K[x]$ such that

$$h_1(x + \gamma) = x^4 + dx^3 + cx^2 + bx + a,$$

$$h_2(x + \gamma) = x^4 - dx^3 + cx^2 - bx + a,$$

and $f^{3}(x + \gamma) = h_{1}(x + \gamma) h_{2}(x + \gamma)$. Equating coefficients gives

- (3.6) $\gamma + m^4 + 2m^3 + m^2 + m = a^2$
- $(3.7) 4m^3 + 4m^2 = 2ac b^2$
- (3.8) $6m^2 + 2m = 2a 2bd + c^2$
- $(3.9) 4m = 2c d^2$

First, we solve (3.8) for a and substitute the resulting value into the other equations. We then solve (3.9) for c, and substitute the resulting value into the other equations. This gives

$$\gamma + m^4 + 2m^3 + m^2 + m = \frac{1}{64} \left(64b^2d^2 - 16bd^5 - 128bd^3m + 128bdm^2 + 128bdm + d^8 + 16d^6m + 48d^4m^2 - 16d^4m - 128d^2m^3 - 128d^2m^2 + 64m^4 + 128m^3 + 64m^2 \right)$$
(3.10)

$$(3.11) 4(m^3+m^2) = \frac{1}{8}(-8b^2+8bd^3+32bdm-d^6-12d^4m-24d^2m^2+8d^2m+32m^3+32m^2)$$

Next we solve (3.11) for b, giving

(3.12)
$$b = \frac{1}{4} \left(2d^3 + 8dm \pm d\beta \right)$$
 where $\beta = \sqrt{2d^4 + 8d^2m + 16m^2 + 16m^2}$

Finally, substituting (3.12) into (3.10) and solving for γ gives

(3.13)
$$\gamma = \pm \beta A + \frac{17}{64}d^8 + \frac{5}{4}md^6 + \frac{11}{4}m^2d^4 + \frac{7}{4}md^4 + 2m^3d^2 + 2m^2d^2 - m$$

where

$$A = \frac{1}{16}d^2 \left(3d^4 + 8d^2m + 8m^2 + 8m \right)$$

Since $b \in K$, (3.12) shows that d = 0 or $\beta \in K$. If d = 0, then (3.13) gives $\gamma = -m$ and we're done. Otherwise, $\beta \in K$. Then (3.12) gives a K-rational point on the surface

(3.14)
$$S: y^2 = 2s^4 + 8s^2m + 16m^2 + 16m.$$

For fixed s, this equation is a conic in y and m, and we can use rational projection to parametrize its K-rational points. The homogeneous form of S can be written

$$\overline{S}: Y^2 = 16M^2 + (8s^2 + 16)MZ + 2s^4Z^2.$$

Note that the rational point $P = [M : Y : Z] = [1 : 4 : 0] \in \mathbb{P}^2(K)$ is on \overline{S} ; this is the point we will project through. Let $r_0 \in K$ be arbitrary. The affine part of the line through r_0 and P is given by $y = 4m + r_0$. To solve for the other intersection point, we substitute into (3.14) to get $(4m + r_0)^2 = 16m^2 + (8s^2 + 16)m + 2s^4$. This equation is linear in m, and we get

$$m = \frac{2s^4 - r_0^2}{8\left(r_0 - s^2 - 2\right)}.$$

Note that $r_0 - s^2 - 2 = 0$ corresponds to the line intersecting the point at infinity with multiplicity 2, so with this projection we don't miss any affine rational points. Taking $r = r_0 - s^2 - 2$ now gives

$$m = m(r,s) = \frac{2s^4 - r^2 - 2rs^2 - 4r - s^4 - 4s^2 - 4}{8r}$$

This is (3.5), so we're halfway done. Since we have $y = 4m + r_0 = 4m + r + s^2 + 2$,

$$y = y(r,s) = \frac{r^2 + s^4 - 4s^2 - 4}{2r}$$

Recall that $y = \beta$ and s = d. Using these in (3.13),

$$\gamma = \pm yA + \frac{17}{64}s^8 + \frac{5}{4}ms^6 + \frac{11}{4}m^2s^4 + \frac{7}{4}ms^4 + 2m^3s^2 + 2m^2s^2 - m.$$

If the plus sign satisfies this equation, it simplifies to

$$\begin{split} \gamma &= \gamma \left(r,s \right) = \frac{1}{256r^2} \left(-2r^5s^2 + 9r^4s^4 - 4r^4s^2 - 16r^3s^6 + 32r^3s^4 + 16r^3s^2 + 32r^3 + 14r^2s^8 \right. \\ &\quad - 64r^2s^6 - 8r^2s^4 + 96r^2s^2 + 128r^2 - 6rs^{10} + 48rs^8 - 64rs^6 \\ &\quad - 160rs^4 + 96rs^2 + 128r + s^{12} - 12s^{10} + 40s^8 - 112s^4 - 64s^2 \right). \end{split}$$

This is (3.4). On the other hand, if we must choose the minus sign, let

$$r' = \frac{-s^4 + 4s^2 + 4}{r}$$
$$s' = s$$

Plugging these in, m(r', s') = m(r, s) and y(r', s') = -y(r, s). So in this case, (3.4) is satisfied by r' and s'.

We make a few observations about Theorem 3.5 and its proof. First, Theorem 1.7 is now proved, as a consequence of Theorem 2.5 and Theorems 3.1 and 3.5. Second, whenever $\gamma = -m$, we have $f(x) = (x - \gamma)^2$, which is obviously reducible. Therefore, Theorem 3.5 shows that all f(x) with newly reducible third iterate have m, γ such that (3.4) and (3.5) are satisfied by some $r, s \in K$.

Third, we emphasize that K-rational points on the surface S described in (3.14) play a crucial role in determining the existence of quadratic polynomials over K with newly reducible third iterate. The fibers of the map $S \to \mathbb{A}^1$ given by projection onto the *m*-coordinate are particularly interesting, and worth dwelling on for a moment. In general, these fibers are elliptic curves, unless m divides the discriminant of $2s^4 + 8s^2m + 16m^2 + 16m$ considered as a polynomial in s. Observe that

$$\operatorname{Disc}(2s^4 + 8s^2m + 16m^2 + 16m) = 2^{21}m^3(m+2)^2(m+1).$$

Hence we obtain a curve of genus zero if and only if $m \in \{0, -1, -2\}$. We remark that for each of these *m*-values, $f(x) = (x - \gamma)^2 + \gamma + m$ is post-critically finite – that is, the forward orbit of γ is finite – and indeed these are the only such *m*-values for $K = \mathbb{Q}$.

When m = 0, we have that S degenerates to $y^2 = 2s^4$, which has no K-rational points unless $\sqrt{2} \in K$. Hence if $\sqrt{2} \notin K$, then $f(x) = (x - \gamma)^2 + \gamma$ has $f^3(x + \gamma)$ symmetrically reducible only if $\gamma = -m$, which implies that f(x) is reducible. If $\sqrt{2} \in K$, then equations (3.6) - (3.9) yield $\gamma = d^8 \left(\frac{17}{64} \pm \frac{3\sqrt{2}}{16}\right)$, and it follows that

$$\sqrt{2\sqrt{\gamma}} = \frac{d^2}{2}(1+\sqrt{2}) \in K.$$

By Lemma 3.1 this shows that $f^2(x)$ is reducible over K. This is in line with [10, Theorem 1.2(i) and Remark 4.3], which give that when $K = \mathbb{Q}$ and m = 0, either $f^2(x)$ is reducible over K, or all iterates of f are irreducible over K.

When m = -2, S degenerates to $y^2 = 2(s^2 - 2)^2$, and again one finds that $f^3(x + \gamma)$ is symmetrically reducible if and only if either f(x) or $f^2(x)$ is reducible.

When m = -1, matters are different, and the following proposition shows we obtain an infinite family of polynomials with newly reducible third iterate for certain K.

Proposition 3.6. Let K be a field of characteristic not equal to 2, and let $f(x) = (x - \gamma)^2 + \gamma - 1$. Then $f^3(x + \gamma)$ is symmetrically reducible if and only if

(3.15)
$$\gamma = 4\left(\frac{(t^2 - 8t + 8)(t^2 + 8)}{(t^2 - 8)^2}\right)^4 + 1 \quad for \ some \ t \in K.$$

Suppose moreover that K is a field with a non-trivial discrete valuation v such that v(5) is odd, and that -1 is not a square in K. Then $f^3(x)$ is newly reducible over K whenever t = 25r in (3.15), for any $r \in K$ with $v(r) \ge 0$. In particular, $K \in \mathcal{N}_{2,3}^{\infty}$.

Démonstration. When m = -1, S degenerates to $y^2 = 2s^2(s^2 - 4)$, whose solutions are given by $s = -2\frac{t^2+8}{t^2-8}$ where t is any element of K. In the notation of the proof of Theorem 3.5 we have s = d, and we now use equations (3.6) - (3.9) to find (3.15).

Observe that for m = -1 we have $-m - \gamma = 1 - \gamma$, and from (3.15) this is not a square in K because -1 is not a square in K. We also have $m^2 + m + \gamma = \gamma$, and so if γ is not a square in K, then Lemma 3.1 gives that $f^2(x)$ is irreducible over K. Now from (3.15) we have that the numerator of γ as a function of t has constant term $c = 5 \cdot 8^8$. Let $v : K^* \to \mathbb{Z}$ be a normalized discrete valuation with v(5) odd. Then v(c) = v(5) + 8v(8), and so v(c) is odd. Taking t = 25r with $v(r) \geq 0$ then shows $v(\gamma)$ is odd, and hence γ cannot be a square in K.

Remark. Proposition 3.6 shows that if K is a number field with ring of integers \mathcal{O}_K , -1 is not a square in K, and the ideal (5) is not the square of an ideal in \mathcal{O}_K , then $K \in \mathcal{N}_{2,3}^{\infty}$. In particular, $\mathbb{Q} \in \mathcal{N}_{2,3}^{\infty}$.

The family appearing in Proposition 3.6 is the same family that appears in Lemma 3.9 of [10], though there it is stated only for integer parameters.

In the preceding discussion, we took m to be constant. It is of interest to give another infinite family with non-constant m-values, which we do in the following corollary to Theorem 3.5.

Corollary 3.7. Let K be a totally real number field and suppose there is a prime \mathfrak{p} of \mathcal{O}_K lying over the ideal (3) with residue degree 1. Let $f(x) = (x - \gamma)^2 + \gamma + m$, where

$$m = -1 - 2k^{2} + k^{4},$$

$$\gamma = 1 + k^{2} \left(-2 + k^{2}\right) \left(-1 - 4k^{2} + 2k^{4}\right) \left(1 - 4k^{2} + 2k^{4}\right)$$

for $k \in \mathcal{O}_K$. If $|k| > \sqrt{2}$ and $\mathfrak{p} \nmid (k)$, then $f^3(x)$ has a newly reducible third iterate over K. In particular, $K \in \mathcal{N}_{2,3}^{\infty}$.

Démonstration. Let r = 2 and s = 2k in Theorem 3.5, and observe that it's sufficient to show that neither of $-m - \gamma$ and $m^2 + m + \gamma$ is a square in K. One calculates $-m - \gamma = -4k^6 (-2 + k^2)^3$. Because $|k| > \sqrt{2}$, we have $-m - \gamma < 0$, and since K is totally real, we have that $-m - \gamma$ is not a square in K. We also have

$$m^{2} + m + \gamma = \left(-1 + k^{2}\right)^{2} \left(1 + 6k^{2} + 13k^{4} - 16k^{6} + 4k^{8}\right)$$

Observe that because \mathfrak{p} has residue degree 1, we have $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/3\mathbb{Z}$. Because $\mathfrak{p} \nmid (k)$ we conclude $k^2 \equiv 1 \pmod{\mathfrak{p}}$, whence

 $1 + 6k^2 + 13k^4 - 16k^6 + 4k^8 \equiv 2 \pmod{\mathfrak{p}},$

proving that $m^2 + m + \gamma$ is not a square in \mathcal{O}_K , and hence not a square in K.

Note that many other infinite families exist; for instance, there is a similar one with r = -2.

4. RATIONAL QUADRATICS WITH NEWLY REDUCIBLE FOURTH ITERATE

In this section we briefly examine the following question.

Question 4.1. Does there exist $f \in \mathbb{Q}[x]$ of degree 2 with newly reducible fourth iterate?

Theorem 2.5 tells us that if $f(x) = (x - \gamma)^2 + m + \gamma$ has a newly reducible fourth iterate, then $f^4(x + \gamma)$ is symmetrically reducible. That is, $f^4(x + \gamma) = h(x)h(-x)$, where

$$h(x) = x^8 + a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

Equating coefficients gives the following system of equations :

$$\begin{split} \gamma + m^8 + 4m^7 + 6m^6 + 6m^5 + 5m^4 + 2m^3 + m^2 + m &= a_0^2 \\ & 8m^7 + 24m^6 + 24m^5 + 16m^4 + 8m^3 = 2a_0a_2 - a_1^2 \\ & 28m^6 + 60m^5 + 36m^4 + 16m^3 + 4m^2 = a_2^2 - 2a_1a_3 + 2a_0a_4 \\ & 56m^5 + 80m^4 + 24m^3 + 8m^2 = -a_3^2 + 2a_2a_4 - 2a_1a_5 + 2a_0a_6 \\ & 70m^4 + 60m^3 + 6m^2 + 2m = a_4^2 + 2a_0 - 2a_3a_5 + 2a_2a_6 - 2a_1a_7 \\ & 56m^3 + 24m^2 = -a_5^2 + 2a_2 + 2a_4a_6 - 2a_3a_7 \\ & 28m^2 + 4m = a_6^2 + 2a_4 - 2a_5a_7 \\ & 8m = 2a_6 - a_7^2 \end{split}$$

This defines a surface, which we denote S_4 , whose rational points correspond to quadratic $f(x) \in \mathbb{Q}[x]$ such that $f^4(x + \gamma)$ is symmetrically reducible over \mathbb{Q} . In particular, this includes all monic quadratic f(x) with newly reducible fourth iterate over \mathbb{Q} . At present, obtaining any information about the rational points on S_4 seems to be quite difficult.

It is interesting to consider the fibers of the map $\pi : S_4 \mapsto \mathbb{A}^1$ given by projection onto the *m*-coordinate. In general these fibers appear to be very high-genus curves, though it is possible that some particular fibers are sufficiently singular that the genus drops significantly. This was the case for the fibers $m \in \{0, -1, -2\}$ for the similar projection map of the curve S in (3.14) that arose from studying f with symmetrically reducible third iterate. Similarly, the fibers $\pi^{-1}(0)$ and $\pi^{-1}(-2)$ are likely to have smaller genera than other fibers; unfortunately, their rational points cannot lead to $f(x) \in \mathbb{Q}[x]$ with newly reducible fourth iterate (see [10, Theorem 4.1 and Remark 4.3]).

The fiber $\pi^{-1}(-1)$, on the other hand, remains a possible location for rational points on S_4 . Lemma 3.10 of [10] shows that *integer* values of γ cannot lead to rational points on this fiber, but the case of non-integer $\gamma \in \mathbb{Q}$ remains open (see Remark 4.3 of [10]).

5. Cubics with Newly Reducible second iterate

In this section we study the question of whether there exist monic irreducible cubic polynomials in K[x] with newly reducible second iterate. Observe that if K does not have characteristic 3, then $f(x) = x^3 + c_2 x^2 + c_1 x + c_0$ can be conjugated to a cubic with no quadratic term : taking $\gamma = -c_2/3$, $a = c_1 - (c_2^2/3) + (c_2/3)$, and $b = c_0 - (c_2^3/27) - (c_2/3)$ gives $f(x) = (x - \gamma)^3 + a(x - \gamma) + b + \gamma$, or equivalently

(5.1)
$$f(x+\gamma) = x^3 + ax + b + \gamma \in K[x]$$

We emphasize that, unlike in the quadratic case, γ is *not* a critical point for f except in the special case that a = 0. It is this special case that is the source of our main result on newly reducible cubics :

Theorem 5.1. Let K be a field of characteristic not equal to 2 or 3, and assume that 2 is not the cube of an element of K. If $f(x) = (x - \gamma)^3 + b + \gamma$, with

(5.2)
$$b = 36t^3 \quad and \quad \gamma = (-2 \cdot 6^6)t^9 - 36t^3, \quad or$$

(5.3)
$$b = -9t^3 \quad and \quad \gamma = 9t^3 + (2 \cdot 3^6)t^9$$

for some non-zero $t \in K$, then f has a newly reducible second iterate.

Démonstration. From Lemma 2.2, we have that if $f^2(x)$ is newly reducible, then $f^2(x) = p_1(x)p_2(x)$, where deg $p_1(x) = 3$, deg $p_2(x) = 6$, and $p_1(x)$ is irreducible. Write

$$f^{2}(x+\gamma) = (x^{3} + a_{2}x^{2} + a_{1}x + a_{0})(x^{6} + b_{5}x^{5} + b_{4}x^{4} + b_{3}x^{3} + b_{2}x^{2} + b_{1}x + b_{0})$$

and equate coefficients to get the system of equations

$$b + b^{3} + \gamma = a_{0}b_{0}$$

$$0 = a_{0}b_{1} + a_{1}b_{0}$$

$$0 = a_{0}b_{2} + a_{1}b_{1} + a_{2}b_{0}$$

$$3b^{2} = a_{0}b_{3} + a_{1}b_{2} + a_{2}b_{1} + b_{0}$$

$$0 = a_{0}b_{4} + a_{1}b_{3} + a_{2}b_{2} + b_{1}$$

$$0 = a_{0}b_{5} + a_{1}b_{4} + a_{2}b_{3} + b_{2}$$

$$3b = a_{0} + a_{1}b_{5} + a_{2}b_{4} + b_{3}$$

$$0 = a_{1} + a_{2}b_{5} + b_{4}$$

$$0 = a_{2} + b_{7}$$

We may solve for b_5, b_4, b_3, b_2, b_1 , and b_0 to obtain

(5.4)
$$b + b^{3} + \gamma = a_{0}^{3} - a_{0}a_{1}^{3} - 6a_{0}^{2}a_{1}a_{2} + 6a_{0}a_{1}^{2}a_{2}^{2} + 4a_{0}^{2}a_{2}^{3} - 5a_{0}a_{1}a_{2}^{4} + a_{0}a_{2}^{6} - 3a_{0}^{2}b + 6a_{0}a_{1}a_{2}b - 3a_{0}a_{2}^{3}b + 3a_{0}b^{2}$$

(5.6)
$$0 = 3a_0a_1^2 + 3a_0^2a_2 - 4a_1^3a_2 - 12a_0a_1a_2^2 + 10a_1^2a_2^3 + 5a_0a_2^4 - 6a_1a_2^5 + a_2^7 - 3a_1^2b - 6a_0a_2b + 9a_1a_2^2b - 3a_2^4b + 3a_2b^2$$

Note that (5.5) is quadratic in a_0 . Taking the discriminant of this equation in a_0 gives (5.7) $9a_2^4b^2 + (36a_1^3a_2 - 42a_1^2a_2^3 + 24a_1a_2^5 - 6a_2^7)b + 12a_1^5 - 3a_1^4a_2^2 - 12a_1^3a_2^4 + 10a_1^2a_2^6 - 4a_1a_2^8 + a_2^{10}$, which in turn is quadratic in *b*. The discriminant of this equation in *b* is

$$+ 144 \left(-9a_1^6 a_2^2 + 24a_1^5 a_2^4 - 25a_1^4 a_2^6 + 14a_1^3 a_2^8 - 5a_1^2 a_2^{10} + a_1 a_2^{12}\right),$$

which has the semi-miraculous factorization

(5.8)
$$12\left(a_1a_2^2\left(a_1-a_2^2\right)\left(9a_1^4-15a_1^3a_2^2+10a_1^2a_2^4-4a_1a_2^6+a_2^8\right)\right).$$

Selecting a_1 and a_2 so that (5.8) vanishes forces (5.7) to be a square, which gives a K-rational solution to (5.5).

One such choice is $a_1 = 0$, which reduces (5.5) to $0 = -3a_0^2a_2^2 - a_0a_2^5 + 3a_0a_2^2b$, giving $a_0 = 0$ or $a_0 = -a_2^3/3 + b$. The former is impossible, since $a_0 = 0$ would imply that the degree three factor of our second iterate was reducible. Substituting $a_0 = -a_2^3/3 + b$ into (5.6) produces another semi-miracle, as the b^2 terms cancel, giving $b = a_2^3/6$. Then (5.4) gives $\gamma = \frac{-a_2^9}{108} - \frac{a_2^3}{6}$. Observe that $b + \gamma = -a_2^9/108$, and it follows from Proposition 6.1 that f(x) is irreducible over K if and only if $a_2^9/108$ is not a cube in K. But this is equivalent to 2 not being a cube in K, which is true by assumption. Hence f has newly reducible second iterate over K. Taking $a_2 = 6t$ clears denominators and gives the family in (5.2).

Taking $a_1 = a_2^2$ also causes (5.8) to vanish, and reduces (5.5) to

$$0 = -2a_0a_2^5 + a_2^8 - 3a_0a_2^2b + 3a_2^5b + 3a_2^2b^2,$$

giving $a_0 = \frac{a_2^8 + 3a_2^5 b + 3a_2^2 b^2}{2a_2^5 + 3a_2^2 b}$. Substituting this into (5.6) yields a cubic rational function in *b* whose numerator fortuitously has a factor of $a_2^3 + 3b$, together with an irreducible quadratic in *b*. Taking $b = -a_2^3/3$ and substituting this into (5.4) yields $\gamma = \frac{1}{27}(9a_2^3 + 2a_2^9)$. Then $b + \gamma = \frac{2}{27}a_2^3$, and we have that *f* is irreducible over *K* since -2 is not a cube in *K*, as in the previous paragraph. Taking $a_2 = 3t$ gives the family in (5.3).

Remark. We can also force (5.8) to vanish by taking $a_2 = 0$, but this produces a family of polynomials f that are all reducible.

We obtain the following immediate corollary of Theorem 5.1.

Corollary 5.2. If K is an infinite field satisfying the hypotheses of Theorem 5.1, then $K \in \mathcal{N}_{3,2}^{\infty}$. In particular, if K is a number field with ring of integers \mathcal{O}_K and 2 is not the cube of an element of K, then there are infinitely many monic $f \in \mathcal{O}_K[x]$ with newly reducible second iterate over K.

We end this section by briefly addressing Question 1.9, which asks whether there exists $f \in \mathbb{Q}[x]$ with f irreducible but $f^2(x)$ a product of three irreducible cubics. The following proposition addresses this.

Proposition 5.3. Let $f(x) \in \mathbb{Q}[x]$ have the form in (5.1), and assume that f^2 is newly reducible with three distinct factors $p_1(x)$, $p_2(x)$, and $p_3(x)$. If β is a root of $p_1(x + \gamma)$, and $f(\beta + \gamma) = \alpha$, then

$$\frac{-\beta \pm \sqrt{-3\beta^2 - 4a}}{2}$$

are roots of $p_2(x+\gamma)$ and $p_3(x+\gamma)$ whose images under $f(x+\gamma)$ are α .

Démonstration. Observe that each of the factors of $f^2(x)$ must have degree 3. By Lemma 2.3, the map

 $\Phi_i : \{ \text{roots of } p_i(x+\gamma) \text{ in } \overline{\mathbb{Q}} \} \to \{ \text{roots of } f(x+\gamma) \text{ in } \overline{\mathbb{Q}} \}$

is surjective and k-to-one for each factor p_i of f^2 . Since each factor has degree equal to the degree of f, Φ_i is one-to-one for each i, and there is one root of each p_i whose image under Φ_i is α . We will show that the roots of $p_2(x + \gamma)$ and $p_3(x + \gamma)$ satisfying this condition are given by (5.9). Let β_2 be such a root, and observe that $\beta^3 + a(\beta) + b + \gamma = \beta_2^3 + a(\beta_2) + b + \gamma$. This gives a quadratic equation for β_2 in terms of β , to which we apply the quadratic formula to obtain $\beta_2 = \frac{-\beta \pm \sqrt{-3\beta^2 - 4a}}{2}$. Notice that when a = 0, we have that the three preimages of a given root of f(x) differ by a multiple of a cubic root of unity. As a consequence, the constant terms of our three factors are equal. We can equate coefficients using this fact to show that there is no monic cubic over $\mathbb{Q}[x]$ with a = 0 whose second iterate factors as three irreducible cubics.

6. QUARTICS WITH NEWLY REDUCIBLE SECOND ITERATE

In this section we will find infinitely many rational quartic polynomials with newly reducible second iterate. We use the following standard fact from field theory to tell when f(x) is irreducible, noting that K^n refers to the set $\{k^n : k \in K\}$.

Proposition 6.1. [13, Theorem 8.1.6] Let K be a field and $f(x) = x^d - c \in K[x]$ for $d \ge 1$. Then f(x) is irreducible over K if and only if $c \notin K^p$ for all primes $p \mid d$ and $c \notin -4K^4$ whenever $4 \mid d$.

Throughout this section, we only consider polynomials of the form $f(x) = (x - \gamma)^4 + m + \gamma$, where $m, \gamma \in \mathbb{Q}$. It turns out that even in this subset of rational quartics, there are infinitely many with newly reducible second iterate.

Theorem 6.2. Let K be a field of characteristic not equal to 2, and suppose that $f(x) = (x - \gamma)^4 + m + \gamma \in K[x]$ is irreducible over K. Then $f^2(x+\gamma)$ factors as $p(x^2)p(-x^2)$ for some $p \in K[x]$ if and only if there exist $r, s \in K$ with $r \neq s^2$ such that $m = \frac{2s^4 - r^2}{8r - 8s^2}$ and

$$\gamma = \frac{-2r^5s^2 + 19r^4s^4 - 72r^3s^6 + 32r^3 + 136r^2s^8 - 32r^2s^2 - 128rs^{10} - 64rs^4 + 48s^{12} + 64s^6}{256\left(r - s^2\right)^2}$$

Démonstration. First, suppose that $m, \gamma, r, s \in K$ are as in the theorem. Writing $r_1 = r - s^2$, one computes that $f^2(x + \gamma) = p(x^2)p(-x^2)$, where

$$p(x) = x^4 - sx^3 + \frac{s^4 - r_1^2}{4r_1}x^2 + \frac{3r_1^2s - s^5}{8r_1}x + \frac{-4r_1s^6 + 10r_1^2s^4 - 12r_1^3s^2 + r_1^4 + s^8}{64r_1^2}.$$

Conversely, suppose that $f(x + \gamma) = p(x^2)p(-x^2)$ for $p(x) = x^4 + dx^3 + cx^2 + bx + a$. Equating coefficients gives us the following system of equations.

$$a^2 = \gamma + m^4 + m$$

(6.2)
$$2ac - b^2 = 4m^3$$

(6.3)
$$2a - 2bd + c^2 = 6m^2$$

(6.4)
$$2c - d^2 = 4m$$

First we solve (6.4) for c and substitute this into the other equations. Then we do the same with (6.3) and b, and then with (6.2) and a. This leaves us with equation (6.1), which becomes

(6.5)
$$\frac{1}{64} \left(3d^4 + 8d^2m \pm 2\sqrt{2}d^2\sqrt{d^4 + 4d^2m + 8m^2} + 8m^2 \right)^2 = \gamma + m^4 + m$$

Note that if d = 0, this equation becomes $m^4 = \gamma + m^4 + m$, so $\gamma + m = 0$. But then $f(x + \gamma) = x^4$ is reducible, which is a contradiction. So $d \neq 0$, and therefore $\sqrt{2(d^4 + 4d^2m + 8m^2)} \in K$. In other words, there is a K-rational solution to

$$S: y^2 = 16m^2 + 8s^2m + 2s^4$$

where s = d. Considering s as a fixed parameter, this is a conic. Now we want to parametrize the K-rational points on S, so we use the homogeneous form of S,

$$\overline{S}: Y^2 = 16M^2 + 8s^2MZ + 2s^4Z^2,$$

and project through the point at infinity [M : Y : Z] = [1 : 4 : 0]. We parametrize our projection line by where it crosses the line m = 0. Then each line is given by y = 4m + r, where $r \in \mathbb{Q}$. Then we solve for the intersection point of this line and S, giving

$$m = m(r,s) = \frac{2s^4 - r^2}{8r - 8s^2}$$
 and $y = y(r,s) = 4m + r = \frac{2s^4 - r^2}{2r - 2s^2} - r.$

Then we solve (6.5) for γ . This gives

$$\gamma = \frac{1}{64} \left(3s^4 + 8s^2m + 8m^2 \pm 2s^2y \right)^2 - m - m^4.$$

Note that there is a plus or minus in front of the term containing y. The plus sign leads to

$$\gamma = \frac{-2r^5s^2 + 19r^4s^4 - 72r^3s^6 + 32r^3 + 136r^2s^8 - 32r^2s^2 - 128rs^{10} - 64rs^4 + 48s^{12} + 64s^6}{256\left(r - s^2\right)^2}$$

as in the statement of the theorem. On the other hand, if we have the minus sign, let $r' = \frac{s^2(2s^2-r)}{s^2-r}$ and s' = s. Plugging these in gives m(r', s') = m(r, s) and y(r', s') = -y(r, s), again giving γ as in the statement of the theorem.

Corollary 6.3. Let K be a field of characteristic not in $\{2,3\}$, and such that 3 is not the square of an element of K, and -3 is not the fourth power of an element of K. Then

$$f(x) = \left(x + 192t^8 - 7t^2\right)^4 - 192t^8$$

has a newly reducible second iterate over K for any $t \in K, t \neq 0$.

Démonstration. Let $t \in K$ with $t \neq 0$, and in the notation of Theorem 6.2 take $r = 48t^2$ and s = 4t. Then from Theorem 6.2 we have that $f(x) = (x - \gamma)^4 + \gamma + m$ has $f^2(x)$ reducible over K, where $\gamma = -192t^8 + 7t^2$ and $m = -7t^2$. We now argue that f(x) is irreducible over K. Observe that

$$-m - \gamma = 192t^8 = (2^6 \cdot 3)t^8$$

If $-m - \gamma = k^2$ for $k \in K$, then 3 is a square in K, while if $4(m + \gamma) = k^4$ for $k \in K$, then -3 is a fourth power in K. Proposition 6.1 now shows that f is irreducible over K.

7. HIGHER-DEGREE POLYNOMIALS WITH NEWLY REDUCIBLE SECOND ITERATE

Theorem 7.1. Let $d \equiv 2 \pmod{4}$, let p_1, \ldots, p_r be the distinct odd primes dividing d, let K be a field, and put $K^n = \{k^n : k \in K\}$. Assume that $-1 \notin K^2$ and $-4k^4 \notin K^{p_i}$ for each $i = 1, \ldots, r$. Then the polynomial $f(x) = (x - 4k^4)^d + 4k^4$ has newly reducible second iterate over K.

Démonstration. We have $f^2(x) = (x - 4k^4)^{d^2} + 4k^4$. Because $4 \mid d^2$, Proposition 6.1 gives that $f^2(x)$ is reducible over K. To show that f(x) is irreducible over K, we note that $4 \nmid d$, and so by Proposition 6.1 it is enough to show that $-4k^4 \notin K^2$ and $-4k^4 \notin K^{p_i}$ for each $i = 1, \ldots, r$. The former follows because $-1 \notin K^2$ and the latter follows by hypothesis.

Corollary 7.2. Let K be a field with a non-trivial discrete valuation. Assume that K has characteristic different from 2, and that $-1 \notin K^2$. Then $K \in \mathcal{N}_{d,2}^{\infty}$ for all $d \equiv 2 \pmod{4}$.

Démonstration. Let $v: K^* \to \mathbb{Z}$ be a (normalized) non-trivial discrete valuation on K. This map is surjective, and taking π with $v(\pi) = 1$, we also have that $v^{-1}(m)$ maps bijectively to $v^{-1}(n)$ via the map $x \mapsto \pi^{m-n}x$. Observe that $2 \in K^*$ because K has characteristic $\neq 2$, and that if $k \in K^n$ for any $n \geq 2$, then $v(k) \in n\mathbb{Z}$. Fix $d \equiv 2 \pmod{4}$, and let p_1, \ldots, p_r be the odd prime divisors of d. By the Chinese Remainder Theorem, the system of congruences

$$x \equiv \frac{1 - 2v(2)}{4} \pmod{p_i}$$

has an infinite solution set $S \subset \mathbb{Z}$. If $v(k) \in S$, then $2v(2) + 4v(k) \equiv 1 \pmod{p_i}$ for all i, and hence $v(-4k^4) \notin p_i\mathbb{Z}$, and thus $-4k^4 \notin K^{p_i}$ for all i. Hence by Theorem 7.1 we have that $f(x) = (x - 4k^4)^d + 4k^4$ has newly reducible second iterate over K.

It remains to argue that $v^{-1}(S)$, and hence S, is infinite. We have already established that $v^{-1}(m)$ and $v^{-1}(n)$ are equinumerous for any $m, n \in \mathbb{Z}$. The only way an infinite union of equinumerous sets can be finite is if all are empty, but this contradicts the surjectivity of v. Thus $v^{-1}(S)$ is infinite.

Références

- [1] O. Ahmadi. A note on stable quadratic polynomials over fields of characteristic two. ArXiv e-prints, October 2009.
- [2] Omran Ahmadi, Florian Luca, Alina Ostafe, and Igor E. Shparlinski. On stable quadratic polynomials. Glasg. Math. J., 54(2):359–369, 2012.
- [3] Mohamed Ayad and Donald L. McQuillan. Irreducibility of the iterates of a quadratic polynomial over a field. Acta Arith., 93(1):87–97, 2000.
- [4] Mohamed Ayad and Donald L. McQuillan. Corrections to: "Irreducibility of the iterates of a quadratic polynomial over a field" [Acta Arith. 93 (2000), no. 1, 87–97]. Acta Arith., 99(1):97, 2001.
- [5] Nigel Boston and Rafe Jones. Settled polynomials over finite fields. Proc. Amer. Math. Soc., 140(6) :1849–1863, 2012.
- [6] Katharine Chamberlin, Emma Colbert, Sharon Frechette, Patrick Hefferman, Rafe Jones, and Sarah Orchard. Newly reducible iterates in families of quadratic polynomials. *Involve*, 5(4):481–495, 2012.
- [7] Stephen D. Cohen. On irreducible polynomials of certain types in finite fields. Proc. Cambridge Philos. Soc., 66:335-344, 1969.
- [8] Lynda Danielson and Burton Fein. On the irreducibility of the iterates of $x^n b$. Proc. Amer. Math. Soc., 130(6) :1589–1596 (electronic), 2002.
- [9] Burton Fein and Murray Schacher. Properties of iterates and composites of polynomials. J. London Math. Soc. (2), 54(3):489-497, 1996.
- [10] Vefa Goksel. Irreducibility of iterates of post-critically finite quadratic polynomials over Q. Rocky Mountain J. Math., 49(7) :2155–2174, 2019.
- [11] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. (2), 78(2):523-544, 2008.
- [12] Rafe Jones. An iterative construction of irreducible polynomials reducible modulo every prime. J. Algebra, 369 :114–128, 2012.
- [13] Gregory Karpilovsky. Topics in Field Theory, volume 155 of North-Holland Mathematics Studies. North-Holland Publishing Co., Amsterdam, 1989. Notas de Matemática [Mathematical Notes], 124.
- [14] Alfred J. Menezes, Ian F. Blake, XuHong Gao, Ronald C. Mullin, Scott A. Vanstone, and Tomik Yaghoobian. Applications of finite fields, volume 199 of The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers, Boston, MA, 1993.
- [15] Jason I. Preszler. An infinite family of cubics with emergent reducibility at depth 1. Quaestiones Mathematicae, 40(1):13–16, 2017.