AN ITERATIVE CONSTRUCTION OF IRREDUCIBLE POLYNOMIALS REDUCIBLE MODULO EVERY PRIME

RAFE JONES

ABSTRACT. We give a method of constructing polynomials of arbitrarily large degree irreducible over a global field F but reducible modulo every finite prime of F. The method consists of finding quadratic $f \in F[x]$ whose iterates have the desired property, and it depends on new criteria ensuring all iterates of f are irreducible. In particular when F is a number field of odd degree, we construct infinitely many families of quadratic f such that every iterate f^n is irreducible over F, but f^n is reducible modulo all primes of F for $n \geq 2$. We also give an example of a quadratic f with coefficients in $\mathbb{Z}$ whose eighth iterate is irreducible modulo some primes, but whose ninth iterate is not. Finally, we study the number of primes $\mathfrak{p}$ for which a given quadratic f defined over a global field has f^n irreducible modulo $\mathfrak{p}$ for all $n \geq 1$.

1. INTRODUCTION

At the end of the 19th century, David Hilbert gave examples of irreducible polynomials $f(x) \in \mathbb{Z}[x]$ that are reducible modulo all primes, namely any irreducible member of the family $x^4+2ax^2+b^2$. In particular, one easily checks that $f(x) = x^4+1$ qualifies, since $f(x+1)$ is Eisenstein with respect to 2. Moreover, $g(x) = x^{2^n}+1$, $n \geq 2$, shares the same properties, since $g(x+1)$ is again Eisenstein and $g(x) = f(x^{2^{n-2}})$ inherits from f a non-trivial factorization modulo any p. In this paper, we give a generalization of this construction, one that yields infinitely many infinite families of irreducible polynomials that are reducible modulo all primes. Specifically, we give criteria that ensure a quadratic polynomial $f(x) \in \mathbb{Z}[x]$ has its nth iterate irreducible over $\mathbb{Q}$ but reducible modulo all primes. The construction works over most global fields, and is based on new results dealing with the irreducibility of iterates of quadratic polynomials. For simplicity, we state here our results over $\mathbb{Q}$ and $k(t)$, where k is a finite field of odd characteristic. We denote by f^n the nth iterate of a polynomial f, and by $\overline{f}$ the coefficient-wise reduction of f modulo a prime.

Theorem 1.1. *Let $n \geq 2$ and let $f(x) = (x-\gamma)^2 + \gamma + m$, where $m \in \mathbb{Z}$ is arbitrary and $\gamma \in \mathbb{Z}$ is chosen as follows. Let $f_0(x) = x^2 + m$, and let $s \in \mathbb{Z}$ be a square with $s > (f_0^{n-1}(0))^2$ and with s odd if either m is even or n is odd, and s even otherwise. Put $\gamma = s - f_0^n(0)$. Then for any $i \geq n$, f^i is irreducible over $\mathbb{Q}$ and $\overline{f^i}$ is reducible for all primes $p \in \mathbb{Z}$.*

The author's research was partially supported by NSF grant DMS-0852826.

For instance, $n = 2$, $m = 0$ and $\gamma = 1$ (coming from $s = 1$) satisfy the hypotheses of the theorem, giving that $f(x) = (x-1)^2+1$ has all iterates beyond the first irreducible but reducible modulo all primes. However, $f^i(x) = (x-1)^{2^i} + 1$, and we recover the example given above. Note that Theorem 1.1 applies to f that do not have all iterates Eisenstein. Take $n = 2$, $m = 1$, and $\gamma = 2$ (this comes from choosing $s = 4$). Then Theorem 1.1 applies to $f(x) = (x-2)^2 + 3$, though no iterate of f is Eisenstein since the x^{2^n-1} coefficient of f^n is a power of two and the constant coefficient is either 0 or 3 modulo 4. Our results also allow for the construction of "primitive" examples where $\overline{f^{n-1}}$ is irreducible for some primes; for example we construct $f \in \mathbb{Z}[x]$ such that $\overline{f^8}$ is irreducible for some primes, but $\overline{f^n}$ is reducible modulo all primes for $n \geq 9$. This also furnishes an example of a polynomial whose first 8 iterates yield maximally large Galois groups, but whose 9th iterate does not. This is in contrast to the case of linear ℓ-adic Galois representations, where maximal size at low levels (typically the first level) implies maximality at all levels. See p. 7 for details.

The broad applicability of Theorem 1.1 stems from Theorem 3.1, which gives a new criterion ensuring irreducibility of the iterates of a quadratic polynomial over a number field. Theorem 3.1 applies to any number field in which the ideal (2) is not a square, and in particular to any number field of odd degree over $\mathbb{Q}$. The more general version of Theorem 1.1, Corollary 3.2, also applies to such fields.

We now turn to $F = k(t)$, where our result is weaker because we have no equivalent of Theorem 3.1.

Theorem 1.2. *Let k be a finite field of odd characteristic, $F = k(t)$, and $\mathcal{O} = k[t]$. Let $n \geq 3$ and let $f(x) = (x-\gamma)^2 + \gamma + m$, where $m \in \mathcal{O}$ has odd degree and $\gamma \in \mathcal{O}$ is chosen as follows. Let $f_0(x) = x^2 + m$, and take $\gamma = m^{2^{n-1}} - f_0^n(0)$. Then f^n is irreducible over F and $\overline{f^n}$ is reducible for all primes $\mathfrak{p} \subset \mathcal{O}$.*

We give an example and make some comments on the case $n = 2$ in Section 4. When f satisfies the hypotheses of Theorem 1.2, f^n has the curious property that it is irreducible over $k(t)$ but for any c in the algebraic closure of k, the specialization of f at $t = c$ is reducible over $k(c)$.

We note that in [6] and [10] it is shown that polynomials similar to those in Hilbert's example exist in any composite degree. These papers adopt a Galois-theoretic viewpoint – one needs to construct a polynomial whose Galois group acts transitively on the polynomial's roots, but contains no full cycles. They rely on non-constructive theorems from inverse Galois theory. Here, we shall not use the Galois-theoretic perspective; for more on the Galois theory of iterates of quadratic polynomials, see e.g. [11, 15].

In Section 2 we give background and basic results on the irreducibility of iterates of a quadratic polynomial. In Section 3 we prove our main results on number fields, including Theorem 1.1 (see Corollary 3.3) and Theorem 3.1. In Section 4 we turn to function fields, including Theorem 1.2 (see Corollary 4.2). Finally, in Section 5 we study the number of primes $\mathfrak{p}$ for which a given quadratic f defined over a global field

has $\overline{f}^n$ irreducible for all $n \geq 1$. The answer should depend on the size and arithmetic of the forward orbit of the critical point of f. We prove this holds when the forward orbit of the critical point either contains a square or is finite, and conjecture that it should be true in the remaining case. We give a heuristic argument in support of the conjecture and examine some examples.

2. Setup and Basic Results

Let F be a field of characteristic $\neq 2$, and let $f \in F[x]$ be a monic, quadratic polynomial. By completing the square, we may write

$$f(x) = (x-\gamma)^2 + \gamma + m. \tag{1}$$

Note that γ is the unique critical point of f.

Definition 2.1. *We call $f \in F[x]$ stable if f^n is irreducible over F for all $n \geq 1$.*

Several recent papers have studied various properties of stable f [2, 3, 4, 5, 7, 11, 17]. The following is one of the fundamental results involving stability, and appears in a slightly different form in [5, Proposition 3] (see also [11, Proposition 4.2]).

Theorem 2.2. *Let f be as in (1), and let $n \geq 1$. Then f^n is irreducible if none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^n(\gamma)$ is a square in F. Moreover, "if" may be replaced by "if and only if" provided that for every finite extension E of F the norm homomorphism $N_{E/F} : E^* \to F^*$ induces an injection $E^*/E^{*2} \to F^*/F^{*2}$.*

We recall a proof: for $n = 1$, we have that f is irreducible if and only if $-f(\gamma)$ is a square in F, since $-f(\gamma) = -(\gamma + m)$. Let $n \geq 2$ and assume inductively that f^{n-1} is irreducible if none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^{n-1}(\gamma)$ is a square in F. Suppose that none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^n(\gamma)$ is a square in F. Then we have f^{n-1} irreducible, and hence separable since $\deg f^{n-1} = 2^{n-1}$ and $\operatorname{char} F \neq 2$. Let β be a root of f^n, and note that $\alpha := f(\beta)$ is a root of f^{n-1}. Clearly $F(\beta) \supseteq F(\alpha)$. Now f^n is irreducible if and only if $[F(\beta) : F] = \deg f^n = 2^n$. However, $[F(\beta) : F] = [F(\beta) : F(\alpha)][F(\alpha) : F] = 2^{n-1}[F(\beta) : F(\alpha)]$, where the last equality follows since f^{n-1} is irreducible. Thus f^n is irreducible if and only if $[F(\beta) : F(\alpha)] = 2$, i.e., if and only if $f(x) - \alpha$ is irreducible over $F(\alpha)$. This is a special case of Capelli's Lemma [8, p. 490]. But $f(x) - \alpha$ is irreducible over $F(\alpha)$ if and only if $-(\gamma + m - \alpha)$ is a square in $F(\alpha)$. One now computes

$$\begin{aligned} N_{F(\alpha)/F}(-(\gamma + m - \alpha)) &= \prod_{f^{n-1}(\alpha)=0} -(\gamma + m - \alpha) \\ &= (-1)^{2^{n-1}} f^{n-1}(\gamma + m) \\ &= f^n(\gamma). \end{aligned} \tag{2}$$

By assumption $f^n(\gamma)$ is not a square in F, implying that $-(\gamma + m - \alpha)$ is not a square in $F(\alpha)$ and proving the irreducibility of f^n. In the case where $N_{F(\alpha)/F}$ induces an injection $F(\alpha)^*/F(\alpha)^{*2} \to F^*/F^{*2}$, then $f^n(\gamma)$ is a square in F if and only if

$-(\gamma+m-\alpha)$ is a square in $F(\alpha)$, i.e., if and only if f^n is irreducible. This proves the theorem.

We note that in general f^n will be irreducible even if $f^n(\gamma)$ is a square. Indeed, in the proof of Theorem 2.2, for $n \geq 2$ we may replace the ground field F by $F_1 := F(\sqrt{-\gamma-m})$, the splitting field of f over F. Then over F_1 we have

$$f^{n-1}(x) = f(f^{n-2}(x)) = \left(f^{n-2}(x) - \gamma + \sqrt{-(\gamma+m)}\right)\left(f^{n-2}(x) - \gamma - \sqrt{-(\gamma+m)}\right).$$

The two polynomials in the last expression are irreducible because f^{n-1} is irreducible over F, implying that $[F(\alpha):F_1] = 2^{n-2}$. Hence (2) becomes

$$\begin{aligned} N_{F(\alpha)/F_1}(-(\gamma+m-\alpha)) &= (-1)^{2^{n-2}}\left(f^{n-2}(\gamma+m) - \gamma \pm \sqrt{-(\gamma+m)}\right) \\ &= (-1)^{2^{n-2}}\left(f^{n-1}(\gamma) - \gamma \pm \sqrt{-(\gamma+m)}\right) \end{aligned}$$

To ease notation, set $\delta = \sqrt{-(\gamma+m)}$, and assume $n \geq 3$. We now have that $N_{F(\alpha)/F_1}(-(\gamma+m-\alpha))$ is a square in F_1 if and only if there are $a, b \in F$ with $(a+b\delta)^2 = f^{n-1}(\gamma) - \gamma \pm \delta$. This gives $a^2 - b^2(\gamma+m) = f^{n-1}(\gamma) - \gamma$ and $2ab = \pm 1$. A straightforward computation shows this happens if and only if one of

$$\frac{1}{2}\left(f^{n-1}(\gamma) - \gamma \pm \sqrt{f^n(\gamma)}\right) \tag{3}$$

is a square in F. When $n = 2$ there is an extra minus sign and the elements in question become $(-f(\gamma) + \gamma \pm \sqrt{f^2(\gamma)})/2$. The point of this computation is that the elements in (3) may well fail to be squares in F even if $f^n(\gamma)$ is a square. This observation lies behind our main results, since $f^n(\gamma)$ being a square ensures reducibility of f^n modulo all primes for which $\overline{\gamma}$ and $\overline{m}$ are defined (see Theorem 2.5). Because it will be useful to us in the sequel, we state as a theorem:

Theorem 2.3. *Let $f(x) = (x-\gamma)^2 + \gamma + m$ for $\gamma, m \in F$, and let $n \geq 2$. Then f^n is irreducible if none of*

$$-f(\gamma), \frac{-f(\gamma) + \gamma \pm \sqrt{f^2(\gamma)}}{2}, \frac{f^2(\gamma) - \gamma \pm \sqrt{f^3(\gamma)}}{2}, \ldots, \frac{f^{n-1}(\gamma) - \gamma \pm \sqrt{f^n(\gamma)}}{2}$$

is a square in F.

Remark. The expressions $f^n(\gamma) - \gamma$ are independent of γ. Indeed, if we set $f_0(x) = x^2 + m$, then it is easy to see that

$$f^n(\gamma) - \gamma = f_0^n(0). \tag{4}$$

We turn our attention now to Dedekind domains. The next proposition illustrates the kind of stability result made possible by Theorems 2.2 and 2.3. It is a mild generalization for quadratic polynomials of a result of Odoni [14, Lemma 2.2], where it is shown that Eisenstein polynomials are stable. In Theorem 3.1 we give a stronger result in the case where $\mathcal{O}$ is the ring of integers in a number field.

Proposition 2.4. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions F, and suppose that there is a prime $\mathfrak{p} \subset \mathcal{O}$ with $v_\mathfrak{p}(m)$ positive and odd and $v_\mathfrak{p}(\gamma) > v_\mathfrak{p}(m)$. Then $f(x) = (x-\gamma)^2 + \gamma + m$ is stable.*

Proof. We use Theorem 2.2. Note that by (4), $f^n(\gamma) = f_0^n(0) + \gamma$ for all $n \geq 1$. Suppose that $v_\mathfrak{p}(m) = c$, which is odd and positive by hypothesis; we claim that $v_\mathfrak{p}(f_0^n(0)) = c$ for all $n \geq 1$. For $n = 1$ the claim is clear since $f_0^1(0) = m$. If $v_\mathfrak{p}(f_0^{n-1}(0)) = c$, then $v_\mathfrak{p}(f_0^n(0)) = v_\mathfrak{p}(f_0^{n-1}(0)^2 + m) = v_\mathfrak{p}(m) = c$, where the middle equality follows because $v_\mathfrak{p}(f_0^{n-1}(0)^2 = 2c > c$. As a side note, one can show similarly that if $v_\mathfrak{p}(f_0^n(0)) = e > 0$ for any n, then $v_\mathfrak{p}(f_0^{nm}(0)) = e$ for all $m \geq 1$, or in the terminology of [11, p. 524] the sequence $\{(f_0^n(0)) : n \geq 1\}$ is a rigid divisibility sequence.

We now have that for all $n \geq 1$, $v_\mathfrak{p}(f^n(\gamma)) = v_\mathfrak{p}(f_0^n(0) + \gamma) = v_\mathfrak{p}(f_0^n(0)) = c$, where the middle equality follows since $v_p(\gamma) > v_\mathfrak{p}(m)$. Hence $f^n(\gamma)$ is not a square in F. □

Suppose now that $\mathcal{O}$ is a Dedekind domain with field of fractions F and that for each $\mathfrak{p} \subset \mathcal{O}$ the residue field $\mathcal{O}/\mathfrak{p}$ is finite. We recall some basic algebraic facts regarding the ring $\mathcal{O}_{(\mathfrak{a})} := S^{-1}\mathcal{O}$, where $S = \mathfrak{a}$, an ideal of $\mathcal{O}$. The prime ideals of $\mathcal{O}_{(\mathfrak{a})}$ are precisely those of the form $\mathfrak{p}\mathcal{O}_{(\mathfrak{a})}$, where $\mathfrak{p} \subset \mathcal{O}$ satisfies $\mathfrak{p} \nmid \mathfrak{a}$. Moreover, for any such $\mathfrak{p}$ we have

$$\mathcal{O}_{(\mathfrak{a})}/\mathfrak{p}\mathcal{O}_{(\mathfrak{a})} \cong \mathcal{O}/\mathfrak{p}. \tag{5}$$

Now let f be as in (1), and fix $c \in \mathcal{O}$ so that $c\gamma m \subset \mathcal{O}$ Let $\mathfrak{a} = (c)$ and $R = \mathcal{O}_{(\mathfrak{a})}$, ensuring that f is defined over R (in fact f may be defined over a smaller ring). Then for each prime $\mathfrak{p} \subset \mathcal{O}$ with $\mathfrak{p} \nmid \mathfrak{a}$, (5) gives a natural ring homomorphism $R \to \mathcal{O}/\mathfrak{p}, x \mapsto \overline{x}$. By application to coefficients we thus get a polynomial $\overline{f} \in (\mathcal{O}/\mathfrak{p})[x]$ and $\overline{f^n} = \overline{f}^n$ follows from homomorphism properties.

Theorem 2.5. *Suppose that $\mathcal{O}$ is a Dedekind domain with field of fractions F and finite residue fields. Let $n \geq 2$, let $s \in F$ be a square, and let $m \in F$ be arbitrary. Put $f_0(x) = x^2 + m$, let $\gamma = s - f_0^n(0)$, and consider $f(x) = (x-\gamma)^2 + \gamma + m$. Then $\overline{f^n}$ is reducible for all primes $\mathfrak{p} \subset \mathcal{O}$ with $\mathfrak{p} \nmid (c)$, where c satisfies $csm \in \mathcal{O}$.*

Proof. We have that γ and m belong to $R := \mathcal{O}_{(c)}$ because $s, m \in R$ and $f_0^n(0)$ is a polynomial in m. Hence $\overline{\gamma}$ and $\overline{m}$ (and in particular $\overline{f}$) are well-defined for all $\mathfrak{p} \nmid (c)$.

For $\mathfrak{p} \subset \mathcal{O}$, the field $F_\mathfrak{p} := \mathcal{O}/\mathfrak{p}$ is finite. For any $\mathfrak{p} \nmid (c)$ with $F_\mathfrak{p}$ of characteristic 2, $\overline{f}$ is reducible and hence so is $\overline{f^n}$. Otherwise $F_\mathfrak{p}$ has odd characteristic, and thus any finite extension E of $F_\mathfrak{p}$ satisfies $E^*/E^{*2} \cong \mathbb{Z}/2\mathbb{Z}$. Because $N_{E/F_\mathfrak{p}}$ is surjective, the induced map $N_{E/F_\mathfrak{p}} : E^*/E^{*2} \to F_\mathfrak{p}^*/F_\mathfrak{p}^{*2}$ is too, and hence is also injective. For $\mathfrak{p} \nmid (c)$, we may now write $\overline{f}(x) = (x-\overline{\gamma})^2 + \overline{\gamma} + \overline{m}$ and apply Theorem 2.2. Using (4) we then have

$$\overline{f}^n(\overline{\gamma}) = \overline{\gamma + (f^n(\gamma) - \gamma)} = \overline{\gamma + f_0^n(0)} = \overline{s}.$$

By Theorem 2.2, $\overline{f^n}$ is reducible. □

3. Results for number fields

We now give a criterion for stability for certain quadratic polynomials over a number field. Denote by $v_{\mathfrak{q}}$ the $\mathfrak{q}$-adic valuation for a prime $\mathfrak{q}$ of $\mathcal{O}$.

Theorem 3.1. *Let F be a number field with ring of integers $\mathcal{O}$, and suppose there is a prime $\mathfrak{q} \subset \mathcal{O}$ with $v_{\mathfrak{q}}(2)$ odd. Let $\gamma, m \in \mathcal{O}$ and $f(x) = (x-\gamma)^2 + \gamma + m$. If $\gamma \not\equiv m \bmod \mathfrak{q}$ and $-(\gamma+m)$ is not a square in F, then f is stable.*

Remark. The condition on the existence of $\mathfrak{q}$ is satisfied if and only if the ideal (2) is not a square in F. In particular, it is satisfied provided that $[F : \mathbb{Q}]$ is odd.

Proof. By Theorem 2.3 it suffices to show that $-f(\gamma)$ and all elements of the form

$$\frac{1}{2}\left(\pm(f^{i-1}(\gamma) - \gamma) \pm \sqrt{f^i(\gamma)}\right), \qquad i \geq 2 \tag{6}$$

are not squares in F. Because $f(\gamma) = \gamma + m$, we have that $-f(\gamma)$ is not a square in F by hypothesis. If for given $i \geq 2$, $f^i(\gamma)$ is not a square in F, then certainly no element of the form (6) for the i in question can be a square in F. If $f^i(\gamma)$ is a square in F, then we argue as follows. Suppose that $\mathfrak{q}$ divides $\pm(f^{i-1}(\gamma) - \gamma) \pm \sqrt{f^i(\gamma)}$, so that $\pm(f^{i-1}(\gamma) - \gamma) \equiv \pm\sqrt{f^i(\gamma)} \bmod \mathfrak{q}$. Squaring and using (4) then gives $f_0^{i-1}(0)^2 \equiv f^i(\gamma) \bmod \mathfrak{q}$. Hence $f_0^i(0) - m \equiv f^i(\gamma) \bmod \mathfrak{q}$, and applying (4) again yields

$$f^i(\gamma) - \gamma - m \equiv f^i(\gamma) \bmod \mathfrak{q}.$$

Because $\mathcal{O}/\mathfrak{q}$ has characteristic two, this implies that $\gamma \equiv m \bmod \mathfrak{q}$, a contradiction.

We now have

$$v_{\mathfrak{q}}\left(\frac{\pm(f^{i-1}(\gamma) - \gamma) \pm \sqrt{f^i(\gamma)}}{2}\right) = v_{\mathfrak{q}}(1/2) = -v_{\mathfrak{q}}(2),$$

and the latter is odd, showing that none of the elements of the form (6) is a square in F. □

Corollary 3.2. *Let F be a number field with ring of integers $\mathcal{O}$, and suppose there is a prime $\mathfrak{q} \subset \mathcal{O}$ with $v_{\mathfrak{q}}(2)$ odd. Let $n \geq 2$, fix $m \in \mathcal{O}$, let $f_0(x) = x^2 + m$, and choose $s \in \mathcal{O}$ to be a square such that $s - (f_0^{n-1}(0))^2 \not\equiv 0 \bmod \mathfrak{q}$ and $-(s - (f_0^{n-1}(0))^2)$ is not a square in F. Then putting $\gamma = s - f_0^n(0)$ and $f(x) = (x-\gamma)^2 + \gamma + m$ we have that for any $i \geq n$, f^i is irreducible over F and $\overline{f^i}$ is reducible for all $\mathfrak{p} \subset \mathcal{O}$.*

Proof. Note that $\gamma + m = s - f_0^n(0) + m = s - (f_0^{n-1}(0))^2$, and so the hypotheses imply that $\gamma + m \not\equiv 0 \bmod \mathfrak{q}$ and $-(\gamma+m)$ is not a square in F. By Theorem 3.1 f is stable, and so in particular f^i is irreducible for all $i \geq n$. On the other hand, since $m, s \in \mathcal{O}$ we may take $c = 1$ in Theorem 2.5, showing that $\overline{f^n}$ is reducible for all $\mathfrak{p} \subset \mathcal{O}$. Then $\overline{f^i} = \overline{f^n} \circ \overline{f^{i-n}}$, which is reducible for all $\mathfrak{p} \subset \mathcal{O}$. □

Remark. For each $m \in \mathcal{O}$ it is possible to find infinitely many values of s satisfying the hypotheses of Corollary 3.2. Indeed, fix a prime $\mathfrak{r}$ of $\mathcal{O}$ not dividing (2) or $(f_0^{n-1}(0))$, and let $x \in \mathfrak{r}/\mathfrak{r}^2$. By the Chinese Remainder Theorem there exist infinitely many $a \in \mathcal{O}$ with $a \equiv f_0^{n-1}(0) + x \bmod \mathfrak{r}^2$ and $a \not\equiv f_0^{n-1}(0) \bmod \mathfrak{q}$. Taking $s = a^2$ satisfies the hypotheses of Corollary 3.2. To see why, note that $a + f_0^{n-1}(0) \equiv 2f_0^{n-1}(0) \not\equiv 0 \bmod \mathfrak{r}$, and so $\mathfrak{r}$ divides $s - f_0^{n-1}(0)^2$ to only the first power, showing it is not a square in F. Also, $a \not\equiv f_0^{n-1}(0) \bmod \mathfrak{q}$ implies $a \not\equiv -f_0^{n-1}(0) \bmod \mathfrak{q}$ since $\mathfrak{q} \mid (2)$, and so $s - f_0^{n-1}(0)^2 \not\equiv 0 \bmod \mathfrak{q}$.

Corollary 3.3. *Fix $n \geq 2$ and $m \in \mathbb{Z}$, and let $s \in \mathbb{Z}$ be a square with s odd if either m is even or n is odd, and s even otherwise. Let $f_0(x) = x^2 + m$, and suppose that $s > (f_0^{n-1}(0))^2$. Then putting $\gamma = s - f_0^n(0)$ and $f(x) = (x-\gamma)^2 + \gamma + m$ we have that for any $i \geq n$, f^i is irreducible over F and $\overline{f^i}$ is reducible for all primes $p \in \mathbb{Z}$.*

Proof. By Corollary 3.2, we only need to show that $s - (f_0^{n-1}(0))^2$ is odd and $-(s - (f_0^{n-1}(0))^2)$ is not a square in $\mathbb{Q}$. The latter is immediate from $s > (f_0^{n-1}(0))^2$, while the former follows from the observation that $f_0^{n-1}(0)$ is even if m is even or n is odd, and odd otherwise. □

For a given m, Corollary 3.3 can be used to find infinitely many γ such that $f(x)$ is stable but $\overline{f^n}$ is reducible modulo all primes for any $n \geq 2$. Indeed, let $n = 2$ and choose s of parity and size satisfying the hypotheses of Corollary 3.3. For instance, when $m = 0$ any odd s will do, though the resulting polynomials $f(x) = (x-s)^2 + s$ have iterates with the closed form $f^n(x) = (x-s)^{2^n} + s$. For a family whose iterates do not have a closed form, let $m = 1$; then $n = 2$ implies we need to take s even with $s > 1$. Setting $s = (2a)^2$ with $a \in \mathbb{Z}, a \geq 1$ gives $\gamma = s - f_0^2(0) = 4a^2 - 2$ and this yields the family

$$f(x) = (x-\gamma)^2 + \gamma + 1 = x^2 + (-8a^2 + 4)x + 16a^4 - 12a^2 + 3, \qquad a \geq 1$$

any member of which is stable but has $\overline{f^n}$ reducible modulo all primes, for any $n \geq 2$.

We can also use Corollary 3.3 to generate "primitive" examples, namely where f is stable, $\overline{f^n}$ is reducible modulo all primes, and $\overline{f^{n-1}}$ is irreducible for some primes. We do so with $n = 9$ and $m = 1$. We have

$$f_0^9(0) = 194727047691529644955970344549384893045279120 5.$$

Set $s = (f_0^8(0) + 1)^2$, which is odd and thus satisfies the hypotheses of Corollary 3.3. We then have

$$\gamma = s - f_0^9(0) = 88255775491812351975604,$$

and thus the 9th iterate of the polynomial

$$f(x) = (x - 88255775491812351975604)^2 + 88255775491812351975605$$

is irreducible over $\mathbb{Q}$ but reducible modulo all primes p. One then checks manually that none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^8(\gamma)$ is a square in $\mathbb{Z}$. Then using quadratic

reciprocity and the Chinese remainder theorem one can find p such that none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots, f^8(\gamma)$ is a square modulo p (indeed such p have positive density in the set of primes). By Theorem 2.2, $\overline{f^8}$ is irreducible for any such p.

Indeed, using [11, Theorem 3.3], one can show that the Galois groups obtained by adjoining the roots of f^i to $\mathbb{Q}$ are as large as possible for $1 \leq i \leq 8$, that is, they are the full tree automorphism group of the height-i tree of preimages of 0 under f. To do so, one needs to find for each $1 \leq i \leq 8$ an odd prime p dividing $f^i(\gamma)$ to odd multiplicity, and not dividing $f^k(\gamma)$ for $1 \leq k < i$. MAGMA quickly verifies this is the case. Clearly the Galois group of f^9 is not as large as possible, since it does not even act transitively on the roots of f^9. This poses a contrast to the case of linear ℓ-adic representations, where surjectivity modulo small powers of ℓ implies surjectivity of the full representation (for $\ell \geq 5$ surjectivity modulo ℓ suffices). The salient difference is that the Frattini subgroup of $G \leq \mathrm{GL}_d(\mathbb{Z}_\ell)$ has finite index in G, while the Frattini subgroup of the automorphism group of the infinite tree of preimages of 0 under f has infinite index. For more on this, see [12, Sections 3 and 5].

4. Results for function fields

When F is a function field over a finite field of odd characteristic, we cannot use the same proof as in Theorem 3.1, since now 2 is a unit. Indeed, there does not appear to be a stability result as general as that of Theorem 3.1 that will allow us to mimic the construction of Corollary 3.2. However, it is still possible to give conditions on m and γ that ensure f^n is irreducible but $\overline{f^n}$ is reducible modulo all finite primes.

In order to do so, we need to use properties of primes at infinity. Let F be a function field over a finite field k of odd characteristic, and let $\mathcal{O}$ be the integral closure of $k(t)$ in F. In contrast with the usage of the previous two sections, we take a prime of F to be slightly more general than simply the prime ideals $\mathfrak{p} \subset \mathcal{O}$. Specifically, a prime of F is a discrete valuation ring $R \subset F$ that contains k and has field of fractions F. Denote the maximal ideal of R by P; we often refer to both P and R as a prime of F. We may extend the valuation on R to a multiplicative function $v_P : F^* \to \mathbb{Z}$, which we call the P-adic valuation. The primes of F consist of the usual prime ideals of $\mathcal{O}$ plus finitely many primes that when restricted to $k(t)$ yield the ring $R = k[1/t]$. We call the former the finite primes and the latter the primes at infinity. For all primes P of F, the P-adic valuation satisfies the strong triangle inequality: for $x, y \in F^*$, $v_P(x+y) \geq \max\{v_P(x), v_P(y)\}$, with equality holding if $v_P(x) \neq v_P(y)$. Moreover, if $x \in \mathcal{O}$ and P is a prime at infinity, then $v_P(x) \leq 0$ and $v_P(x) = 0$ if and only if $x \in k$.

Theorem 4.1. *Let F be a function field over a finite field k of odd characteristic, and let $\mathcal{O}$ be the integral closure of $k(t)$ in F. Suppose that there is an infinite prime Q_1 and a finite prime Q_2 with $v_{Q_1}(m)$ and $v_{Q_2}(m)$ both odd. Let $n \geq 3$, $f_0(x) = x^2 + m$, take $\gamma = m^{2^{n-1}} - f_0^n(0)$, and set $f(x) = (x-\gamma)^2 + \gamma + m$. Then f^n is irreducible over F but $\overline{f^n}$ is reducible for each finite prime of F.*

Proof. Suppose that $v_{Q_2}(m) = c$, which is odd by hypothesis. By the proof of Proposition 2.4, $v_{Q_2}(f_0^i(0)) = c$ for all $i \geq 1$, and hence

$$v_{Q_2}\left(\frac{f^{n-1}(\gamma) - \gamma \pm \sqrt{f^n(\gamma)}}{2}\right) = v_{Q_2}(f_0^{n-1}(0) \pm m^{2^{n-1}}) = c.$$

Hence neither of $(f^{n-1}(\gamma) - \gamma \pm \sqrt{f^n(\gamma)})/2$ is a square in F.

Now note that for $n \geq 3$ we have $f_0^n(0) = m^{2^{n-1}} + 2^{n-2}m^{2^{n-1}-1} + \cdots$, and thus $v_{Q_1}(\gamma) = (2^{n-1} - 1)v_{Q_1}(m)$, which is odd. Moreover, for $i < n$,

$$v_{Q_1}(f_0^i(0)) = (2^{i-1})v_{Q_1}(m) > v_{Q_1}(\gamma),$$

where the final inequality follows since $v_{Q_1}(m)$ is negative and $n \geq 3$ ensures $2^{i-1} < 2^{n-1} - 1$. Because $f^i(\gamma) = f_0^i(0) + \gamma$, it follows that $v_{Q_1}(f^i(\gamma)) = v_{Q_1}(\gamma)$, and hence $f^i(\gamma)$ is not a square in F. Hence by Theorem 2.3, f^n is irreducible over F. On the other hand, since $m^{2^{n-1}}$ and m belong to $\mathcal{O}$, we may take $c = 1$ in Theorem 2.5, giving that $\overline{f^n}$ is reducible modulo all finite primes of F. □

Remark. Unlike Theorems 3.2 and 3.3, the conclusion of Theorem 4.1 doesn't necessarily hold for f^i with $i \geq n$. Clearly $\overline{f^i}$ is reducible modulo all finite primes for $i \geq n$, but the lack of an equivalent of Theorem 3.1 means we can't conclude that f^i is irreducible. Proposition 2.4 can't be used in the setting of Theorem 4.1, since $v_P(\gamma) = v_P(m)$ for all primes P dividing m.

When $F = k(t)$, we can use the product formula to simplify the hypotheses of Theorem 4.1.

Corollary 4.2. *Let k be a finite field of odd characteristic, $F = k(t)$, $\mathcal{O} = k[t]$, and suppose that $m \in \mathcal{O}$ has odd degree. Let $n \geq 3$, $f_0(x) = x^2 + m$, take $\gamma = m^{2^{n-1}} - f_0^n(0)$, and set $f(x) = (x - \gamma)^2 + \gamma + m$. Then f^n is irreducible over F but $\overline{f^n}$ is reducible for each finite prime of F.*

Proof. The product formula gives

$$\sum_P v_P(m) = 0,$$

where the sum runs over all primes P of F. In the present case, there is only one prime Q_1 at infinity, and by hypothesis $v_{Q_1}(m)$ is odd. Hence by the product formula there must be a finite prime Q_2 with $v_{Q_2}(m)$ odd. The Corollary then follows from Theorem 4.1. □

To illustrate Corollary 4.2, let $n = 3$ and $m = t$. Then $\gamma = t^4 - (t^4 + 2t^3 + t^2 + t) = -2t^3 - t^2 - t$. Take

$$f(x) = (x - \gamma)^2 + \gamma + t = x^2 + (4t^3 + 2t^2 + 2t)x + 4t^6 + 4t^5 + 5t^4.$$

Then $f^3(x)$ is irreducible over F but reducible modulo all finite primes of F. In other words, for any c in the algebraic closure of k, the specialization of $f^3(x)$ at $t = c$ is reducible over $k(c)$, even though $f^3(x)$ is irreducible over F.

We note that Theorem 4.1 doesn't apply when $n = 2$, since then $f_0^n(0) = m^2 + m$, which means according to the recipe of Theorem 4.1, $\gamma = -m$. But then $\gamma + m = 0$, and so f is reducible. However, this may be remedied by choosing r with $r/2$ a non-quadratic residue in k and taking $\gamma = (m+r)^2 - m^2 - m$. Then $f^2(\gamma) = \gamma + m^2 + m = (m+r)^2$. Moreover, $-f(\gamma) = -(\gamma + m) = -(2rm + r^2)$. Because $r/2$ is not a quadratic residue, $r \neq 0$, and thus $-(2rm + r^2)$ has odd Q_1-adic valuation, and so is not a square in F. Therefore f is irreducible. Finally, we have

$$\frac{-m + \sqrt{f^2(\gamma))}}{2} = \frac{r}{2},$$

which is not a square in F, showing that f^2 is irreducible by Theorem 2.3. It is worth noting that if we extend the field of constants of F to be $k(\sqrt{r/2})$ then f^2 becomes reducible.

5. THE NUMBER OF STABLE PRIMES

The purpose of this section is to investigate, for given monic, quadratic f defined over a global field F, the number of primes of F for which $\overline{f}$ is stable. For simplicity let us suppose that f is defined over $\mathcal{O}$, which we take to be the ring of integers of F in the number field case and the integral closure of $k[t]$ in the case where F is a function field over the finite field k (of odd characteristic). Then $f(x)$ may be written as $(x-\gamma)^2 + \gamma + m$, with $\gamma \in \frac{1}{2}\mathcal{O}$ and $m \in \frac{1}{4}\mathcal{O}$. In the function field case the reductions $\overline{\gamma}$ and $\overline{m}$ are defined for all primes, while in the number field case they are defined for all primes not lying over 2. For the latter, $\overline{f}$ cannot be stable, as indeed its third iterate must always be reducible [1].

Theorem 5.1. *Let F be a global field, and $f \in F[x]$ monic and quadratic with critical point γ. Let $S = \{-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots\}$.*

1. *If S contains a square, then there is an iterate of f that is reducible modulo all primes.*
2. *If S is finite and does not contain a square, then $\overline{f}$ is stable for a set of primes of density at least $2^{-|S|}$.*

Note that in Theorem 5.1, (1) implies that $\overline{f}$ is stable for no primes, while (2) implies $\overline{f}$ is stable for infinitely many primes. In assertion (2), we use the notion of natural density for sets of primes in number fields and Dirichlet density for sets of primes in function fields. When S is finite, f is known as *post-critically finite* or *critically finite*. In the case $F = \mathbb{Q}$, the positive-density set of primes referenced in (2) is by quadratic reciprocity the union of congruence classes for some fixed modulus.

Proof of Theorem 5.1. Assertion (1) follows easily from Theorem 2.2 and the fact that $\overline{\gamma}$ and $\overline{m}$ are both defined for all primes we need consider.

To prove assertion (2), suppose that S is finite and does not contain a square. Let T be the set of primes $\mathfrak{p}$ such that no element of S is a square in $\mathcal{O}/\mathfrak{p}$. By Theorem 2.2, $\overline{f}$ is stable for all $\mathfrak{p} \in T$. Consider the extension E of F obtained by adjoining to F the square roots of all elements of S. Then E is a Galois extension of F with $\mathrm{Gal}\,(E/F)$ an elementary abelian 2-group. There is a unique Galois element σ with $\sigma(\sqrt{s}) = -\sqrt{s}$ for all $s \in S$, and $\mathfrak{p} \in T$ if and only if $\mathrm{Frob}_{\mathfrak{p}} = \sigma$. By the Chebotarev density theorem (see [13, p. 545] for the number field case, [18, p. 125] for the function field case), the density of $\mathfrak{p}$ with $\mathrm{Frob}_{\mathfrak{p}} = \sigma$ is $1/|\mathrm{Gal}\,(E/F)|$. By Kummer theory $|\mathrm{Gal}\,(E/F)|$ is the order of the subgroup of F^*/F^{*2} generated by S, which is at most $2^{|S|}$. □

Conjecture 5.2. *Let F be a global field, and $f \in F[x]$ monic and quadratic with critical point γ. Let $S = \{-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots\}$. If S is infinite and does not contain a square, then $\overline{f}$ is stable for only finitely many primes.*

Conjecture 5.2 appears difficult to prove. However, the following heuristic suggests that it is true. For $\mathfrak{p} \in \mathcal{O}$, denote by $N_{\mathfrak{p}}$ the the number of elements of $\mathcal{O}/\mathfrak{p} := F_{\mathfrak{p}}$. We need two main assumptions: that the elements of the orbit of $\overline{\gamma}$ behave like a random orbit of a random self-map of $F_{\mathfrak{p}}$ and that the elements of S are close to multiplicatively independent. The orbit of a random point under a random self-map of $F_{\mathfrak{p}}$ has length bounded below by $\sqrt{N_{\mathfrak{p}}}$ [9] (See also [19, Section 6]). Hence $\overline{f}$ is stable for $\mathfrak{p}$ if none of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots f^j(\gamma)$ is a square in $F_{\mathfrak{p}}$, for some $j \geq \sqrt{N_{\mathfrak{p}}}$. As in the proof of Theorem 5.1, the set of primes for which this is true has density $1/r$, where r is the order in F^*/F^{*2} of $\langle S \rangle$. In general, $r = 2^j$. Thus the "probability" that $\overline{f}$ is stable is at most $2^{-\sqrt{N_{\mathfrak{p}}}}$. Assuming independence, this gives that the expected number of primes for which $\overline{f}$ is stable is

$$\sum_{\mathfrak{p}} 2^{-\sqrt{N_{\mathfrak{p}}}}. \tag{7}$$

When F is a number field, let $d = [F : \mathbb{Q}]$, and note that for a given rational prime p, the sum (2) taken over $\mathfrak{p} \mid (p)$ can be at most $d/2^{\sqrt{p}}$, which occurs when (p) splits completely in F. Hence the full sum in (7) is at most $\sum_p d/2^{\sqrt{p}}$, which is less than $d \sum_n 1/2^{\sqrt{n}}$. Separating this last sum into the pieces $i^2 \leq n \leq (i+1)^2 - 1$, we see that it is bounded above by $d \sum_i (2i+1)/2^i$, which converges. A similar argument holds in the function field case.

It would be very interesting to prove Conjecture 5.2 for any single polynomial. We consider for a moment the case of $F = \mathbb{Q}$, $f(x) = x^2 + 1$, and give evidence that Conjecture 5.2 holds in this case. Odoni [16] first observed that $\overline{f}$ is stable for $p = 3$, and also remarked on the central role that the sequence $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots$ plays in the Galois theory of iterates of $f(x)$. His work paved the way for Stoll's proof that the Galois groups of iterates of $f(x)$ are as large as possible [20].

Conjecture 5.3. *Let $F = \mathbb{Q}$ and $f(x) = x^2 + 1$. Then $\overline{f}$ is stable for $p = 3$ and for no other primes.*

Using MAGMA, one computes that the first 20 elements of $-f(\gamma), f^2(\gamma), f^3(\gamma), \ldots$ are all non-squares modulo p for 42 of the $50,847,534$ primes $\leq 10^9$. Apart from 3, each of these primes has $f^n(\gamma)$ a square modulo p for some $n \leq 25$, thereby verifying Conjecture 5.3 for primes $\leq 10^9$. As further evidence, we give the following result, though we first define some terminology. Let $a, f(a), f^2(a), \ldots$ be a finite orbit, and take $f^0(a) = a$. let r be the minimal positive integer with $f^r(a) = f^s(a)$ for some $0 \leq s < r$. Then the *tail* of the orbit is $a, f(a), \ldots f^{s-1}(a)$ when $s > 0$, and is empty otherwise. By the length of the tail, we mean s.

Proposition 5.4. *Let $f(x) = x^2 + 1$, and suppose that $\overline{f}$ is stable for a prime p. Then the orbit of 0 under $\overline{f}$ has tail of length two.*

Proof. To ease notation, let $a_n = \overline{f}^n(0)$ for $n \geq 0$, and note that $a_0 = 0$ and $a_n = a_{n-1}^2 + 1$ for $n \geq 1$. Let r be minimal with $a_r = a_s$ for some $s < r$. If $s = 0$ then $a_r = 0$, and hence $\overline{f}$ is not stable. If $s = 1$ then $a_r = 1$, and hence $a_{r-1} = 0$, so again $\overline{f}$ is not stable. So assume $s \geq 2$. Then $a_{r-1}^2 = a_{s-1}^2$. But by the minimality of r, we must have $a_{r-1} \neq a_{s-1}$. Hence $a_{r-1} = -a_{s-1}$. Note that not all of $a_{s-1}, -a_{s-1}$, and -1 can be non-squares in $\mathbb{Z}/p\mathbb{Z}$. Because $-1 = -a_1$, this shows that a_{s-1}, a_{r-1}, or $-a_1$ is a square in $\mathbb{Z}/p\mathbb{Z}$. If the square is a_{r-1} or $-a_1$, or if $s > 2$, then one of $-a_1, a_2, a_3, \ldots$ is a square, and $\overline{f}$ is not stable by Theorem 2.2. Therefore if $\overline{f}$ is stable then $s = 2$. $\square$

We note that if $s = 2$, then $\overline{f}^r(0) = 2$ for some $r \geq 2$, and indeed $\overline{f}^{r-1}(0) = -1$, since otherwise $\overline{f}^{r-1}(0) = 1 = \overline{f}^1(0)$, contradicting $s = 2$. Thus the only p for which $\overline{f}$ has a chance of being stable are those with $f^n(0) \equiv -1 \bmod p$ for some n. By factoring $f^n(0) + 1$ for $1 \leq n \leq 9$ using MAGMA, one sees that apart from 3, all primes with $f^n(0) \equiv -1 \bmod p$ for $1 \leq n \leq 9$ are congruent to 1 modulo 4, and thus -1 is a square modulo p, so already $\overline{f}(x)$ is reducible. However, there are factors of $f^n(0) + 1$ with $n = 10, 11$ that are congruent to 3 modulo 4.

We note that $f^n(0) + 1$ may be obtained from $f^{n-1}(0) + 1$ by applying $g(x) = (x-1)^2 + 2$. Indeed, $g^n(1) = f^n(0) + 1$, so the only primes for which $x^2 + 1$ has a chance of being stable are those dividing some element of the forward orbit of the critical point of g.

As a final remark, we note that assertion (3) of Conjecture 5.2 implies that the subgroup of F^*/F^{*2} generated by S is infinite, which already is not known in general. This statement does follow in certain special cases where $f^n(\gamma)$ is a rigid divisibility sequence or the orbit of 0 under f is finite. Indeed, in these cases one can prove the stronger assertion that for infinitely many n, there is a prime dividing $f^n(\gamma)$ with odd multiplicity but not dividing $f^i(\gamma)$ for any $i < n$. See [11] for details.

References

[1] O. Ahmadi. A note on stable quadratic polynomials over fields of characteristic two. *ArXiv e-prints*, October 2009.

[2] Nidal Ali. Stabilité des polynômes. *Acta Arith.*, 119(1):53–63, 2005.

[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. To appear, *Proc. Amer. Math. Soc.*

[6] Rolf Brandl. Integer polynomials that are reducible modulo all primes. *Amer. Math. Monthly*, 93(4):286–288, 1986.

[7] 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.

[8] Burton Fein and Murray Schacher. Properties of iterates and composites of polynomials. *J. London Math. Soc. (2)*, 54(3):489–497, 1996.

[9] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics. In *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 329–354. Springer, Berlin, 1990.

[10] Robert Guralnick, Murray M. Schacher, and Jack Sonn. Irreducible polynomials which are locally reducible everywhere. *Proc. Amer. Math. Soc.*, 133(11):3171–3177 (electronic), 2005.

[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 and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[13] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

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

[15] R. W. K. Odoni. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *J. London Math. Soc. (2)*, 32(1):1–11, 1985.

[16] R. W. K. Odoni. Realising wreath products of cyclic groups as Galois groups. *Mathematika*, 35(1):101–113, 1988.

[17] Alina Ostafe and Igor E. Shparlinski. On the length of critical orbits of stable quadratic polynomials. *Proc. Amer. Math. Soc.*, 138(8):2653–2656, 2010.

[18] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[19] Joseph H. Silverman. Variation of periods modulo p in arithmetic dynamics. *New York J. Math.*, 14:601–616, 2008.

[20] Michael Stoll. Galois groups over $\mathbf{Q}$ of some iterated polynomials. *Arch. Math. (Basel)*, 59(3):239–244, 1992.