DYNATOMIC POLYNOMIALS, NECKLACE OPERATORS, AND UNIVERSAL RELATIONS FOR DYNAMICAL UNITS

JOHN R. DOYLE, PAUL FILI, AND TREVOR HYDE

1. INTRODUCTION

Let $f(x) \in K[x]$ be a polynomial with coefficients in a field K. For an integer $k \geq 0$, we denote by $f^k(x)$ the k-fold iterated composition of f with itself. The dth dynatomic polynomial $\Phi_{f,d}(x) \in K[x]$ of f is defined by the product

$$\Phi_{f,d}(x) := \prod_{e|d} (f^{d/e}(x) - x)^{\mu(e)},$$

where μ is the standard number-theoretic Möbius function on $\mathbb{N}$. We refer the reader to [12, §4.1] for background on dynatomic polynomials. For generic $f(x)$, the dth dynatomic polynomial $\Phi_{f,d}(x)$ vanishes at precisely the periodic points of f with primitive period d. In this paper we consider the polynomial equation $\Phi_{f,d}(x) = 1$ and show that it often has f-preperiodic solutions determined by arithmetic properties of d, independent of f. Moreover, these f-preperiodic solutions are detected by cyclotomic factors of the *dth necklace polynomial*:

$$M_d(x) = \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e} \in \mathbb{Q}[x].$$

Our results extend earlier work of Morton and Silverman [8], but our techniques are quite different and apply more broadly.

We begin by recalling some notation and terminology. The *cocore* of a positive integer d is d/d' where d' is the largest squarefree factor of d. If $m \geq 0$ and $n \geq 1$, then the *(m,n)th generalized dynatomic polynomial* $\Phi_{f,m,n}(x)$ of $f(x)$ is defined by $\Phi_{f,0,n}(x) := \Phi_{f,n}(x)$ and

$$\Phi_{f,m,n}(x) := \frac{\Phi_{f,n}(f^m(x))}{\Phi_{f,n}(f^{m-1}(x))}$$

for $m \geq 1$. The roots of $\Phi_{f,m,n}$ for generic f are those preperiodic points which enter into an n-cycle after exactly m iterations under f.

Theorem 1.1 is our main result; it is proved in Section 3.

Theorem 1.1. *Let K be a field, let $f(x) \in K[x]$ be a polynomial of degree at least 2, and let c, d, m, n be integers with $c, m \geq 0$ and $d, n \geq 1$. Suppose that*

(1) either $m > c$ or $n \nmid d$,
(2) the cocore of d is at least $m - \max(c-1, 0)$, and
(3) $x^n - 1$ divides the dth necklace polynomial $M_d(x)$ in $\mathbb{Q}[x]$.

Then $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$.

Alternatively, if $d > 1$, $c - 1 \geq m$, and $n = 1$, then $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$.

Remark 1.2. While we generally discuss polynomials over arbitrary fields, the polynomial M_d will always be considered to be a polynomial over $\mathbb{Q}$; in particular, all statements regarding divisibility or factorizations of M_d should be interpreted in characteristic zero.

1.1. **Dynamical units.** Let K be a number field with ring of integers $\mathcal{O}_K$. Morton and Silverman [8] define *dynamical units* to be algebraic integral units constructed in one of several closely related ways from differences of preperiodic points of a given monic polynomial $f(x) \in \mathcal{O}_K[x]$. If $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$, then for each root $\alpha \in \overline{K}$ of $\Phi_{f,m,n}(x)$,

$$1 = \Phi_{f,d}(\alpha) = \prod_{\beta} (\alpha - \beta), \tag{1.1}$$

where the product ranges over all the roots β of $\Phi_{f,c,d}(x)$ with multiplicity. The differences $\alpha - \beta$ are dynamical units and (1.1) is a multiplicative relation between dynamical units. If the conditions of Theorem 1.1 are satisfied for m, n, c, d, then (1.1) holds for all $f(x)$ with degree at least 2; we view these as *universal relations* for dynamical units. Examples of universal relations for dynamical units have been found by Morton and Silverman [8, Thm. 7.5] and Benedetto [1, Thm. 2]. We give some results on universal relations, and relate them to previous work, in Section 3.2 below.

1.2. **Cyclotomic factors of necklace polynomials.** Of the conditions in Theorem 1.1, (3) is the most subtle. Necklace polynomials $M_d(x)$ have several combinatorial interpretations; for example, if q is a prime power, then $M_d(q)$ is the number of irreducible degree-d monic polynomials in $\mathbb{F}_q[x]$. These interpretations give no indication as to when, if ever, $M_d(x)$ will vanish at all the nth roots of unity. However, as observed in [5], necklace polynomials are generally divisible by many cyclotomic polynomials. Recall that the *nth cyclotomic polynomial* $\Phi_n(x)$ is the $\mathbb{Q}$-minimal polynomial of a primitive nth root of unity.

Example 1.3. $M_{105}(x)$ factors over $\mathbb{Q}$ as

$$\begin{aligned} M_{105}(x) &= \tfrac{1}{105}(x^{105} - x^{35} - x^{21} - x^{15} + x^7 + x^5 + x^3 - x) \\ &= e(x) \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x, \end{aligned} \tag{1.2}$$

where $e(x) \in \mathbb{Q}[x]$ is a degree 92, irreducible, non-cyclotomic polynomial. Since

$$x^n - 1 = \prod_{m|n} \Phi_m(x),$$

the factorization (1.2) implies that $M_{105}(x)$ is divisible by $x^n - 1$ for $n = 1, 2, 3, 4, 6, 8$. Note that $d = 105 = 3 \cdot 5 \cdot 7$ is squarefree, hence the cocore of d is 1. Thus Theorem 1.1 implies that for any polynomial $f(x) \in K[x]$ of degree at least 2, $\Phi_{f,105}(x) - 1$ is divisible by $\Phi_{f,1,n}(x)$ for $n = 1, 2, 3, 4, 6, 8$ and $\Phi_{f,0,n}$ for $n = 2, 4, 6, 8$.

In light of Theorem 1.1 one might naturally ask how often $x^n - 1$ divides $M_d(x)$. Figure 1 suggests that $M_d(x)$ is divisible by several $x^n - 1$ for all $d \geq 1$. Hyde [5] characterized the cyclotomic factors of necklace polynomials in terms of hyperplane arrangements in finite abelian groups. Let $\widehat{\mathcal{U}}_n := \mathrm{Hom}((\mathbb{Z}/(n))^\times, \mathbb{C}^\times)$ denote the group of Dirichlet characters of modulus n. If q is a unit modulo n, then the *hyperplane* $\mathcal{H}_q \subseteq \widehat{\mathcal{U}}_n$ is defined to be the set

$$\mathcal{H}_q := \{\chi \in \widehat{\mathcal{U}}_n : \chi(q) = 1\}.$$

The following theorem gives an alternative to condition (3) in Theorem 1.1 in terms of hyperplanes in the group of Dirichlet characters. We prove Theorem 1.4 in Section 3.3.

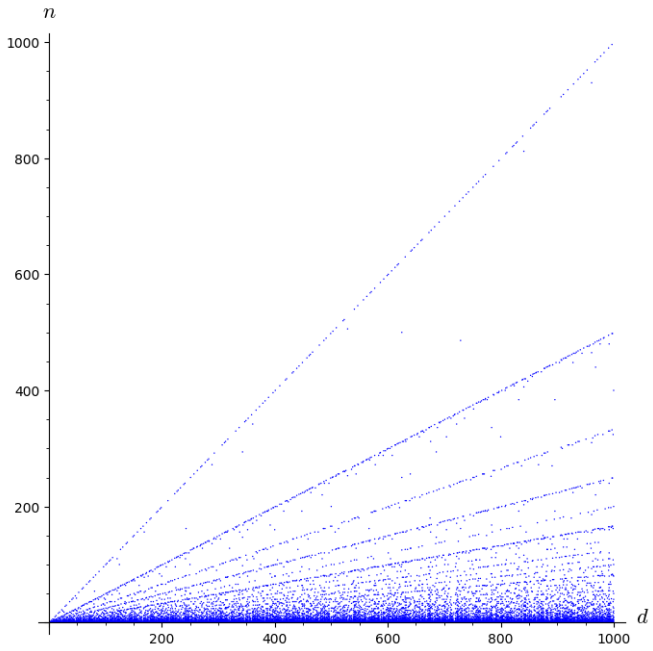

FIGURE 1. Pairs (d, n) with $d, n \leq 1000$ for which $x^n - 1$ divides $M_d(x)$.

Theorem 1.4. *Let $d, n \geq 1$. Then $x^n - 1$ divides $M_d(x)$ if and only if*

$$\widehat{\mathcal{U}}_n \subseteq \bigcup_{\substack{p \mid d \\ p \nmid n}} \mathcal{H}_p.$$

Theorem 1.4 says $x^n - 1$ divides $M_d(x)$ if and only if the finite abelian group $\widehat{\mathcal{U}}_n$ of modulus n Dirichlet characters is covered by an arrangement of "hyperplanes" determined by the prime factors of d. In Example 3.14 we explain how the 5 distinct prime factors of

$$d = 440512358437 = 47^2 \cdot 73 \cdot 79 \cdot 151 \cdot 229$$

correspond to the 5 lines in $(\mathbb{R}/4\mathbb{Z})^2$ in Figure 2, and how the fact that the lines cover all the lattice points translates, via Theorem 1.4, into the fact that $x^{65} - 1$ divides $M_{440512358437}(x)$. Since the cocore of d is 47, Theorem 1.1 implies that

$$\Phi_{f,m,65}(x) \text{ divides } \Phi_{f,440512358437}(x) - 1,$$

for all $f(x) \in K[x]$ with $\deg(f) \geq 2$ and $0 \leq m \leq 47$.

1.3. **Cyclotomic factors of shifted cyclotomic polynomials.** Cyclotomic factors of necklace polynomials are also closely related to cyclotomic factors of shifted cyclotomic polynomials $\Phi_d(x) - 1$. For example, if $d = 105$, then

$$\Phi_{105}(x) - 1 = \widetilde{e}(x) \cdot \Phi_8 \cdot \Phi_6 \cdot \Phi_4 \cdot \Phi_3 \cdot \Phi_2 \cdot \Phi_1 \cdot x,$$

where $\widetilde{e}(x) \in \mathbb{Q}[x]$ is a degree 35, irreducible, non-cyclotomic polynomial. Note that the cyclotomic factors dividing $\Phi_{105}(x) - 1$ are precisely the same as those dividing $M_{105}(x)$. In general, $M_d(x)$ and $\Phi_d(x) - 1$ have most, but not all, cyclotomic factors in common. See [5] for a detailed analysis of the cyclotomic factors in these two sequences.

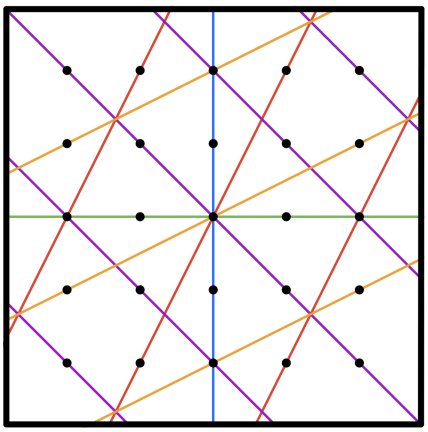

FIGURE 2.

Cyclotomic factors of $\Phi_d(x) - 1$ are also detected by cyclotomic factors of $M_d(x)$ and have an interpretation in terms of multiplicative relations between *cyclotomic units* analogous to the situation with dynamical units discussed above. Thus the cyclotomic factors of necklace polynomials give explicit structural parallels between these two analogous families of units.

1.4. **Necklace operators.** Let $\mathbb{Z}\Psi$ denote the ring generated by formal expressions $[m]$ with $m \in \mathbb{N}$ subject only to the multiplicative relations $[m][n] = [mn]$. The *dth necklace operator* $\varphi_d \in \mathbb{Z}\Psi$ is defined by

$$\varphi_d := \sum_{e|d} \mu(e)[d/e].$$

The cyclotomic factors of $M_d(x)$, cyclotomic factors of $\Phi_d(x) - 1$, and dynatomic factors of $\Phi_{f,d}(x) - 1$ ultimately trace back to the necklace operator φ_d. The polynomials $M_d(x)$, $\Phi_d(x)$ and $\Phi_{f,d}(x)$ may be expressed as images of φ_d with respect to different $\mathbb{Z}\Psi$-module structures. Suppressing the details of the module structures for now, we have

$$\begin{aligned} M_d(x) &= \frac{1}{d}\sum_{e|d} \mu(e)x^{d/e} = \varphi_d(x/d), \\ \Phi_d(x) &= \prod_{e|d}(x^{d/e} - 1)^{\mu(e)} = (x-1)^{\varphi_d}, \\ \Phi_{f,d}(x) &= \prod_{e|d}(f^{d/e}(x) - x)^{\mu(e)} = (f(x) - x)^{\varphi_d}. \end{aligned} \tag{1.3}$$

As the notation suggests, $M_d(x)$ is an image in an additive $\mathbb{Z}\Psi$-module while $\Phi_d(x)$ and $\Phi_{f,d}(x)$ arise from multiplicative $\mathbb{Z}\Psi$-modules. Much of the work that goes into proving Theorem 1.1 involves constructing the appropriate $\mathbb{Z}\Psi$-module in which to realize the above expression of $\Phi_{f,d}(x)$ as an image of φ_d.

All of the cyclotomic and dynatomic factors of the polynomials discussed above, as well as the connection to hyperplane arrangements in the group of Dirichlet characters, ultimately traces back to the following factorization of the necklace operator (in a localization of $\mathbb{Z}\Psi$):

$$\varphi_d = [d]\prod_{p|d}\left(1 - \frac{1}{[p]}\right),$$

where the product is taken over all primes p dividing d.

1.5. **Acknowledgements.** We are happy to thank Patrick Morton and Joe Silverman for feedback on an earlier draft. John Doyle was partially supported by NSF grant DMS-2112697. Trevor Hyde was partially supported by the NSF Postdoctoral Research Fellowship DMS-2002176 and the Jump Trading Mathlab Research Fund.

2. Preliminary results

In this section we prove preliminary results leading up to the proofs of Theorem 1.1 and Theorem 1.4 in Section 3. Our main goal is to make sense of (1.3). We accomplish this by introducing the notions of composition rings and their algebras. In Section 2.4, we prove a statement on the generic separability of (generalized) dynatomic polynomials; this result is folklore in the arithmetic dynamics community but we were unable to find a suitable reference.

2.1. **Composition rings.** Suppose R is a commutative ring and S is a monoid of ring endomorphisms of R with respect to composition. The monoid S generates a (non-unital) subring C_S of the ring of all R-valued functions on R, with pointwise ring operations. Furthermore, C_S has an extra layer of structure coming from the composition operation on S. We abstract this situation into the notion of a composition ring.

Definition 2.1. A *composition ring* C is a (potentially non-unital) commutative ring together with an associative operation $\circ$ such that for all $f, g, h \in C$

(1) $(f+g)\circ h = (f\circ h)+(g\circ h)$,
(2) $(f\cdot g)\circ h = (f\circ h)\cdot(g\circ h)$, and
(3) there exists a two-sided compositional identity $x \in C$.

A morphism $\sigma : C \to D$ of composition rings is a ring homomorphism which respects the composition operator and preserves compositional identities.

All of the composition rings we consider are constructed as follows.

Definition 2.2. Let S be a multiplicative monoid. The *free S-composition ring* $\mathbb{Z}\{S\}$ is the composition ring generated by expressions $[s]$ with $s \in S$ where the composition operation $\circ$ is determined by the following relations: for all $f, g \in \mathbb{Z}\{S\}$ and $s, t \in S$

(*i*) $[s]\circ(f+g) = ([s]\circ f)+([s]\circ g)$,
(*ii*) $[s]\circ(f\cdot g) = ([s]\circ f)\cdot([s]\circ g)$, and
(*iii*) $[s]\circ[t] = [st]$.

Note that the compositional identity is $x := [1]$ where $1 \in S$ is the multiplicative identity.

To see that the composition operation on $\mathbb{Z}\{S\}$ is determined by these properties, first observe that Definition 2.1 (1) and (2) reduce the computation of $f \circ g$ for $f, g \in \mathbb{Z}\{S\}$ to $[s]\circ g$ with $s \in S$. Then Definition 2.2 (*i*) and (*ii*) reduce us further to $[s]\circ[t]$ for $s, t \in S$, and finally (*iii*) tells us that $[s]\circ[t] = [st]$. This reduction is illustrated in the following example.

Example 2.3. Let $S := \langle f, g\rangle$ be the free monoid on two generators. Consider the elements

$$\alpha := 3[f^2][f] + 2[1][g]$$
$$\beta := [f][g] + [fg]$$

of $\mathbb{Z}\{S\}$. Then by Definition 2.1 (1) and (2),

$$\begin{aligned}\alpha\circ\beta &= (3[f^2][f] + 2[1][g])\circ\beta \\ &= 3([f^2]\circ\beta)([f]\circ\beta) + 2([1]\circ\beta)([g]\circ\beta).\end{aligned}$$

Definition 2.2 (*i*) and (*ii*) imply that

$$\begin{aligned}[f^2] \circ \beta &= [f^3][f^2g] + [f^3g],\\ [f] \circ \beta &= [f^2][fg] + [f^2g],\\ [1] \circ \beta &= [f][g] + [fg],\\ [g] \circ \beta &= [gf][g^2] + [gfg].\end{aligned}$$

Thus,

$$\alpha \circ \beta = 3\left([f^3][f^2g] + [f^3g]\right)\left([f^2][fg] + [f^2g]\right) + 2\left([f][g] + [fg]\right)\left([gf][g^2] + [gfg]\right).$$

Remark 2.4. The composition ring $\mathbb{Z}\{S\}$ is closely related to the more familiar monoid ring $\mathbb{Z}[S]$. The latter is the ring generated by $[s]$ for $s \in S$ with multiplication determined by $[s] \cdot [t] = [st]$. The monoid ring $\mathbb{Z}[S]$ embeds into $\mathbb{Z}\{S\}$ as linear combinations of the "degree one" elements with product structure given by $\circ$.

If $\widetilde{\sigma} : S \to T$ is a monoid homomorphism, then there is a unique composition ring homomorphism $\sigma : \mathbb{Z}\{S\} \to \mathbb{Z}\{T\}$ which lifts $\widetilde{\sigma}$. In fact, the map $S \mapsto \mathbb{Z}\{S\}$ gives a functor from monoids to composition rings.

We further restrict our attention to monoids S which are quotients of the free cyclic monoid on one generator $\langle f \rangle$. For each $m, n \in \mathbb{N}$ with $n \geq 1$, let $\mathbb{Z}\{f\} := \mathbb{Z}\{\langle f \rangle\}$ and let

$$\mathbb{Z}_{m,n}\{f\} := \mathbb{Z}\{\langle f : f^{m+n} = f^m \rangle\}.$$

The monoid quotient

$$\langle f \rangle \to \langle f : f^{m+n} = f^m \rangle.$$

induces, by functoriality, a map of composition rings $\mathbb{Z}\{f\} \to \mathbb{Z}_{m,n}\{f\}$. If $\alpha, \beta \in \mathbb{Z}\{f\}$ are elements with the same image in $\mathbb{Z}_{m,n}\{f\}$, then we write

$$\alpha \equiv \beta \bmod \mathbb{Z}_{m,n}\{f\}.$$

2.2. **Ψ-module structure on $\mathbb{Z}\{f\}$.** Let $\mathbb{N}^\circ$ denote the multiplicative monoid of natural numbers and let $\Psi := \mathbb{N}[\mathbb{N}^\circ]$ denote the monoid semiring of $\mathbb{N}^\circ$. That is, Ψ is the semiring additively spanned by formal expressions $[m]$ for $m \in \mathbb{N}$ such that for $m, n \in \mathbb{N}$,

$$[m][n] = [mn].$$

For each $m \in \mathbb{N}$ there is a unique endomorphism $[m]$ of the cyclic semigroup $\langle f \rangle$ expressed in exponential notation as $f^{[m]} := f^m$. This gives, by functoriality, an endomorphism $[m] : \mathbb{Z}\{f\} \to \mathbb{Z}\{f\}$ of composition rings. We extend this action to a multiplicative Ψ-module structure on $\mathbb{Z}\{f\}$.

Example 2.5. If $\psi = 3[5] + 2[4] \in \Psi$, then

$$([f] - [1])^\psi = ([f] - [1])^{3[5]+2[4]} := ([f^5] - [1])^3([f^4] - [1])^2.$$

If $m \geq 0$ and $n \geq 1$ are natural numbers, the semiring quotient $\mathbb{N} \to \mathbb{N}/(m + n = m)$ induces a quotient on multiplicative monoids $\mathbb{N}^\circ \to (\mathbb{N}/(m + n = n))^\circ$. Let $\Psi_{m,n}$ denote the semiring quotient of Ψ induced by this quotient of monoids. If $\psi_1, \psi_2 \in \Psi$ are two elements with the same image under this map, then we write

$$\psi_1 \equiv \psi_2 \ [\mathrm{mod}\ m + n = m],$$

or simply

$$\psi_1 \equiv \psi_2 \ [\mathrm{mod}\ n],$$

when $m = 0$. This notation is meant to suggest that the quotient takes place inside the brackets.

Example 2.6. If $m = 0$ and $n = 3$, then

$$5[1] - 3[2] + 4[5] \equiv 5[1] + [2] \not\equiv 2[1] + [2] \pmod 3.$$

The first congruence holds because $[2] \equiv [5] \pmod 3$. The second congruence does not hold because the congruence does not extend to the coefficients so that $2[1] \not\equiv 5[1] \pmod 3$.

The action of $\mathbb{N}^\circ$ on the cyclic monoid $\langle f : f^{m+n} = f^m \rangle$ factors through the quotient $\mathbb{N}^\circ/(m + n = m)$, hence the multiplicative Ψ-module structure on $\mathbb{Z}_{m,n}\{f\}$ factors through $\Psi_{m,n}$. Lemma 2.7 formally states this observation.

Lemma 2.7. *If $\alpha \in \mathbb{Z}\{f\}$ and $\psi_1, \psi_2 \in \Psi$ are such that $\psi_1 \equiv \psi_2 \pmod{m + n = m}$, then $\alpha^{\psi_1} \equiv \alpha^{\psi_2} \bmod \mathbb{Z}_{m,n}\{f\}$.*

2.3. **Necklace operators.** If R is a semiring, then let $R\Psi := R \otimes_{\mathbb{N}} \Psi$ denote the extension of scalars of Ψ from $\mathbb{N}$ to R.

Definition 2.8. If $d \geq 1$ is a natural number, then the *dth necklace operator* φ_d is

$$\varphi_d := \sum_{e|d} \mu(e)[d/e] \in \mathbb{Z}\Psi,$$

where μ is the usual number theoretic Möbius function.

There is a unique cancellation-free way to write the dth necklace operator as a difference $\varphi_d = \varphi_d^+ - \varphi_d^-$ of elements $\varphi_d^\pm \in \Psi$. Now let $\Phi_{f,d}^\pm \in \mathbb{Z}\{f\}$ be defined by

$$\Phi_{f,d}^\pm = ([f] - [1])^{\varphi_d^\pm}.$$

Note that Ψ and $\Psi_{m,n}$ have no additive torsion, hence embed into $\mathbb{Q}\Psi$ and $\mathbb{Q}\Psi_{m,n}$, respectively. Lemma 2.9 constructs a simple polynomial model of the free $\mathbb{Q}\Psi_{m,n}$-module which allows us to relate the vanishing of φ_d in $\mathbb{Z}\Psi_{m,n}$ to cyclotomic factors of $M_d(x)$. The polynomial ring $\mathbb{Q}[x]$ carries a natural $\mathbb{Q}\Psi$-module structure determined by $[k]g(x) := g(x^k)$ for $g(x) \in \mathbb{Q}[x]$. Here x^k denotes a monomial and not the kth compositional power of the identity function (which would again be the identity.)

Lemma 2.9. *Let $m \geq 0$ and $n \geq 1$. The $\mathbb{Q}\Psi$-module structure on $\mathbb{Q}[x]$ defined by $[k]g(x) := g(x^k)$ descends to $\mathbb{Q}[x]/(x^{m+n} - x^m)$ and factors through $\mathbb{Q}\Psi_{m,n}$. Furthermore,*

$$\mathbb{Q}[x]/(x^{m+n} - x^m) \cong \mathbb{Q}\Psi_{m,n}$$

as $\mathbb{Q}\Psi_{m,n}$-modules.

Proof. Let $M_{m,n} := \mathbb{Q}[x]/(x^{m+n} - x^m)$. To see that the $\mathbb{Q}\Psi$-module structure on $\mathbb{Q}[x]$ descends to $M_{m,n}$ it suffices to check that if $f(x) \equiv g(x) \bmod (x^{m+n} - x^m)$, then $f(x^k) \equiv g(x^k) \bmod (x^{m+n} - x^m)$. This follows from the observation that $x^{mk}(x^{nk} - 1)$ is divisible by $x^m(x^n - 1)$ for all $k \in \mathbb{N}$. The $\mathbb{Q}\Psi$-action on $M_{m,n}$ clearly factors through $\mathbb{Q}\Psi_{m,n}$. Observe that $M_{m,n}$ is cyclic as a $\mathbb{Q}\Psi_{m,n}$-module and is generated by x. Note that both $M_{m,n}$ and $\mathbb{Q}\Psi_{m,n}$ have dimension $m + n$ over $\mathbb{Q}$, hence $M_{m,n}$ is free. □

Definition 2.10. The *core* of a positive integer d is the largest squarefree factor d' of d and the *cocore* of d is d/d'. Note that the core of d is the product of all distinct primes dividing d.

Definition 2.11. The *dth necklace polynomial* $M_d(x) \in \mathbb{Q}[x]$ for $d \geq 1$ is defined by

$$M_d(x) := \frac{1}{d} \sum_{e|d} \mu(e) x^{d/e}.$$

Proposition 2.12. *Let $m, n, d \in \mathbb{N}$ be such that $n, d \geq 1$. If*

(1) the cocore of d is at least m, and
(2) $x^n - 1$ divides $M_d(x)$ in $\mathbb{Q}[x]$,

then $\varphi_d = 0$ in $\mathbb{Z}\Psi_{m,n}$ and

$$\Phi^+_{f,d} \equiv \Phi^-_{f,d} \bmod \mathbb{Z}_{m,n}\{f\}.$$

Proof. Lemma 2.9 implies that $\mathbb{Q}[x]/(x^{m+n} - x^m)$ is a free $\mathbb{Q}\Psi_{m,n}$-module generated by x. Hence $\varphi_d = 0$ in $\mathbb{Z}\Psi_{m,n}$ if and only if $\varphi_d x = 0$ in $\mathbb{Q}[x]/(x^m(x^n - 1))$. Since

$$\varphi_d x = \sum_{e|d} \mu(e)[d/e]x = \sum_{e|d} \mu(e)x^{d/e} = dM_d(x),$$

$\varphi_d = 0$ in $\mathbb{Z}\Psi_{m,n}$ if and only if x^m and $x^n - 1$ both divide $M_d(x)$. Since $\mu(e) = 0$ when e is not squarefree, the exponent of the largest power of x dividing $M_d(x)$ is the cocore of d. Therefore (1) and (2) imply that $\varphi_d = 0$ in $\mathbb{Z}\Psi_{m,n}$.

If $\varphi_d = 0$ in $\mathbb{Z}\Psi_{m,n}$, then $\varphi_d^+ \equiv \varphi_d^- \pmod{m + n = m}$ and, by Lemma 2.7,

$$\Phi^+_{f,d} = ([f] - [1])^{\varphi_d^+} \equiv ([f] - [1])^{\varphi_d^-} = \Phi^-_{f,d} \bmod \mathbb{Z}_{m,n}\{f\}. \qquad \square$$

2.4. **Dynatomic polynomials are generically squarefree.** We step aside from the theory developed in the previous sections to prove a dynamical lemma.

Lemma 2.13. *Let K be a field and let $f(x)$ be the generic degree $k \geq 2$ polynomial over K,*

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0 \in K(a_0, a_1, \ldots, a_k)[x].$$

Then for any $m, n \in \mathbb{N}$ such that $n \geq 1$, $f^{m+n}(x) - f^m(x)$ has non-vanishing discriminant.

Proof. It suffices to prove the claim after specializing some subset of the coefficients of f. We consider two specializations depending the characteristic $p \geq 0$ of K.

First, suppose that $p \nmid k$. Morton [6, Lemma 2] shows that for $f_t(x) := x^k + t$, the polynomial $f_t^n(x) - x$ is separable over $K(t)$ for all $n \geq 1$, and, using similar techniques, the same is shown in [2, Lemma 4.2] for $f_t^{m+n}(x) - f_t^m(x)$ with $m \geq 0$ and $n \geq 1$.

Now suppose that $p \mid k$, and consider the polynomial $f_t(x) := x^k + tx \in K(t)[x]$. Then $f_t'(x) = t$, hence $(f_t^\ell)'(x) = t^\ell$ for all $\ell \geq 1$ by the chain rule. This implies that the polynomial $f_t^{m+n}(x) - f_t^m(x)$ has derivative $t^{m+n} - t^m$, a nonzero constant in $K(t)$. Since its derivative is nowhere vanishing, the polynomial $f_t^{m+n}(x) - f_t^m(x)$ is separable for all $m \geq 0$ and $n \geq 1$. $\square$

Remark 2.14.

(1) In characteristic 0, Lemma 2.13 predates [6]. Indeed, for $a \in \mathbb{C}$ and $f_a(x) = x^k + a$, the polynomial $f_a^{m+n}(x) - f_a^m(x)$ has a multiple root if and only if either f_a has fewer than k^n points of period dividing n, or $m \geq 1$ and the critical point 0 is a root of $f_a^{m+n}(x) - f_a^m(x)$. The set of such $a \in \mathbb{C}$ is contained in the degree-k "Multibrot set" $\mathcal{M}_k$, which is a compact subset of $\mathbb{C}$, hence one can further specialize f_t to any $a \in \mathbb{C} \setminus \mathcal{M}_k$. See also [3]—especially [3, §3]—for related results.
(2) In [2, Lemma 4.2], which we refer to in the proof of Lemma 2.13, it was assumed that K is a finite field, since that was the only case for which the result was needed. However, the proof that $f_t^{m+n}(x) - f_t^m(x)$ is separable over $K(t)$ only requires that the characteristic of K does not divide k.

Definition 2.15. If $f(x) \in K[x]$ is a polynomial, then the *nth dynatomic polynomial* $\Phi_{f,n}(x) \in K[x]$ for $n \geq 1$ is defined by the product

$$\Phi_{f,n}(x) := \prod_{j|n} (f^{n/j}(x) - x)^{\mu(j)}.$$

If $m \geq 0$, then the (m,n)*th generalized dynatomic polynomial* $\Phi_{f,m,n}(x)$ is defined by $\Phi_{f,0,n}(x) := \Phi_{f,n}(x)$ and for $m \geq 1$,

$$\Phi_{f,m,n}(x) := \frac{\Phi_{f,n}(f^m(x))}{\Phi_{f,n}(f^{m-1}(x))}.$$

Despite their appearance, dynatomic polynomials are indeed polynomials and not just rational functions, as was first proven by Morton and Patel [7]. See Silverman [12, Sec. 4.1] for a general introduction to dynatomic polynomials and [12, Thm. 4.5] for a proof that $\Phi_{f,d}(x)$ is a polynomial (and not just a rational function as is apparent from the defining product). As a special case of Hutz [4, Thm. 1] we get that $\Phi_{f,m,n}(x)$ is a polynomial; we may also deduce this quickly from Lemma 2.13.

The following factorization of $f^{m+n}(x) - f^m(x)$ is well-known and is often used without proof. We prove it here for the reader's convenience.

Lemma 2.16. *Let $f(x) \in K[x]$ be a polynomial of degree at least 2, then*

$$f^{m+n}(x) - f^m(x) = \prod_{\substack{i \leq m \\ j|n}} \Phi_{f,i,j}(x).$$

Proof. Recall that the definition of the dynatomic polynomials is equivalent to

$$f^n(x) - x = \prod_{j|n} \Phi_{f,j}(x), \tag{2.1}$$

by Möbius inversion. Pre-composing both sides with $f^m(x)$ and using the telescoping product identity

$$\Phi_{f,j}(f^m(x)) = \frac{\Phi_{f,j}(f^m(x))}{\Phi_{f,j}(f^{m-1}(x))} \frac{\Phi_{f,j}(f^{m-1}(x))}{\Phi_{f,j}(f^{m-2}(x))} \cdots \frac{\Phi_{f,j}(f(x))}{\Phi_{f,j}(x)} \Phi_{f,j}(x) = \prod_{i \leq m} \Phi_{f,i,j}(x),$$

gives us the desired factorization of $f^{m+n}(x) - f^m(x)$. □

Together Lemma 2.13 and Lemma 2.16 imply that the generic generalized dynatomic polynomial $\Phi_{f,m,n}(x)$ is also squarefree.

2.5. **Composition algebras.** Next we introduce the notion of an algebra for a composition ring.

Definition 2.17. Let C be a composition ring. A C*-composition algebra* is a commutative ring R together with an operation $\circ : R \times C \to R$ such that for all $r \in R$ and $g, h \in C$ we have

(1) $r \circ (g \circ h) = (r \circ g) \circ h$,
(2) $r \circ (g + h) = (r \circ g) + (r \circ h)$,
(3) $r \circ (g \cdot h) = (r \circ g) \cdot (r \circ h)$, and
(4) $r \circ x = r$,

where x is the compositional identity in C.

Suppose that a monoid S acts (on the right) by ring endomorphisms on a commutative ring R. If $r \in R$ and $s \in S$, then we denote this action by r^s. By construction there is a unique way to extend this action to a $\mathbb{Z}\{S\}$-composition algebra structure on R so that

$$r \circ [s] = r^s$$

for all $r \in R$ and $s \in S$.

Let K be a field. The polynomial ring $K[x]$ is the free K-algebra on one generator. This implies that for any element f in a K-algebra R, there is a unique map of K-algebras $\sigma_f : K[x] \to R$ such that $\sigma_f(x) = f$. In particular, for each polynomial $f(x) \in K[x]$ there is a K-algebra endomorphism $\sigma_f : K[x] \to K[x]$ such that $g(x)^{\sigma_f} := g(f(x))$ for all $g(x) \in K[x]$. Thus $K[x]$ carries a $K\{f\}$-composition algebra structure where $K\{f\} := K \otimes \mathbb{Z}\{f\}$ and $g(x) \circ f := g(f(x))$.

Example 2.18. We demonstrate these notions with a simple explicit example: If $g(x) \in K[x]$, then

$$g(x) \circ ([f^5] - [1])([f^3] - [1]) = (g(f^5(x)) - g(x))(g(f^3(x)) - g(x)).$$

Definition 2.19. A polynomial $q(x) \in K[x]$ is *f-stable* for $f(x) \in K[x]$ if $q(x)$ divides $q(f(x))$.

If $q(x)$ is f-stable, then the endomorphism $\sigma_f : K[x] \to K[x]$ descends to an endomorphism of the quotient $K[x]/(q(x))$. Note that if $q(x)$ is squarefree, then $q(x)$ divides $q(f(x))$ if and only if f maps the roots of $q(x)$ into themselves. More generally, let $v_\alpha(q(x))$ denote the valuation of $q(x)$ at $x - \alpha$, then $q(x)$ is f-stable if and only if $v_{f(\alpha)}(q(x)) \geq v_\alpha(q(x))$ for all roots α of q.

Lemma 2.20. *Let $f(x) \in K[x]$ be a polynomial and let $m, n \in \mathbb{N}$ such that $n \geq 1$. Then $f^{m+n}(x) - f^m(x)$ is f-stable*

Proof. First suppose $f(x) = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0 \in K(a_0, a_1, \ldots, a_k)[x]$ is the generic degree-k polynomial over K. Lemma 2.13 implies that $f^{m+n}(x) - f^m(x)$ is squarefree. The roots of $f^{m+n}(x) - f^m(x)$ are f-preperiodic hence closed under iteration by f. Therefore $f^{m+n}(x) - f^m(x)$ is f-stable. Stability is preserved under specialization. □

Lemma 2.20 implies that $K[x]/(f^{m+n}(x) - f^m(x))$ inherits a $\mathbb{Z}\{f\}$-composition ring structure from $K[x]$. Furthermore, since $g(f^{m+n}(x)) \equiv g(f^m(x)) \bmod (f^{m+n}(x) - f^m(x))$ for all polynomials $g(x)$, the action of $\mathbb{Z}\{f\}$ factors through $\mathbb{Z}_{m,n}\{f\}$. This is summarized in the following lemma.

Lemma 2.21. *Let $f(x) \in K[x]$, and let the composition ring $\mathbb{Z}\{f\}$ act on $K[x]$ by $g(x) \circ f := g(f(x))$. If $\alpha, \beta \in \mathbb{Z}\{f\}$ are elements such that $\alpha \equiv \beta \bmod \mathbb{Z}_{m,n}\{f\}$, then for all $g(x) \in K[x]$,*

$$g(x) \circ \alpha \equiv g(x) \circ \beta \bmod (f^{m+n}(x) - f^m(x)).$$

3. Results

With everything in place, we now prove the main result.

Theorem 3.1. *Let K be a field, let $f(x) \in K[x]$ be a polynomial of degree at least 2, and let c, d, m, n be integers with $c, m \geq 0$ and $d, n \geq 1$. Suppose that*

(1) either $m > c$ or $n \nmid d$,
(2) the cocore of d is at least $m - \max(c - 1, 0)$, and
(3) $x^n - 1$ divides the dth necklace polynomial $M_d(x)$ in $\mathbb{Q}[x]$.

Then $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$.

Alternatively, if $d > 1$, $c - 1 \geq m$, and $n = 1$, then $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$.

Proof of Theorem 3.1. It suffices to prove the result for $f(x) \in K(a_0, a_1, \ldots, a_k)[x]$ the generic degree $k \geq 2$ polynomial over K. Suppose (1), (2), and (3) hold. We first prove the result assuming $c = 0$. Assumptions (2) and (3) imply that $\Phi^+_{f,d} \equiv \Phi^-_{f,d} \bmod \mathbb{Z}_{m,n}\{f\}$ by Proposition 2.12. If $\Phi^\pm_{f,d}(x) := x \circ \Phi^\pm_{f,d}$, then by Lemma 2.21,

$$\Phi^+_{f,d}(x) \equiv \Phi^-_{f,d}(x) \bmod (f^{m+n}(x) - f^m(x)). \tag{3.1}$$

If $\alpha \in \overline{K(a_0, a_1, \ldots, a_k)}$ is a root of $\Phi_{f,m,n}(x)$, then Lemma 2.16 and (3.1) imply that

$$\Phi^+_{f,d}(\alpha) = \Phi^-_{f,d}(\alpha).$$

If $m > 0$ or $n \nmid d$, then $f^e(\alpha) - \alpha \neq 0$ for any $e \mid d$ by Lemma 2.13 and Lemma 2.16; hence $\Phi^\pm_{f,d}(\alpha) \neq 0$. Observe that

$$\begin{aligned}
\frac{\Phi^+_{f,d}(x)}{\Phi^-_{f,d}(x)} &= x \circ ([f] - [1])^{\varphi^+_d - \varphi^-_d} \\
&= x \circ ([f] - [1])^{\sum_{e \mid d} \mu(e)[d/e]} \\
&= \prod_{e \mid d} (f^{d/e}(x) - x)^{\mu(e)} \\
&= \Phi_{f,d}(x).
\end{aligned}$$

Thus $\Phi_{f,d}(\alpha) = 1$. Since this holds for all roots α and $\Phi_{f,m,n}(x)$ is squarefree by Lemma 2.13, we conclude that $\Phi_{f,m,n}(x)$ divides $\Phi_{f,d}(x) - 1$.

Next suppose $c > 0$ and that the cocore of d is at least $m - c + 1$. The above argument implies that $\Phi_{f,m-c+1,n}(x)$ and $\Phi_{f,m-c,n}(x)$ divide $\Phi_{f,d}(x) - 1$. If α is a root of $\Phi_{f,m,n}(x)$, then $f^{c-i}(\alpha)$ is a root of $\Phi_{f,m-c+i,n}(x)$. Hence $\Phi_{f,d}(f^c(\alpha)) = \Phi_{f,d}(f^{c-1}(\alpha)) = 1$ and

$$\Phi_{f,c,d}(\alpha) = \frac{\Phi_{f,d}(f^c(\alpha))}{\Phi_{f,d}(f^{c-1}(\alpha))} = \frac{1}{1} = 1.$$

Thus $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$ by Lemma 2.13.

Finally assume that $d > 1$, $c - 1 \geq m$, and $n = 1$. If α is a root of $\Phi_{m,1}(x)$, then $c - 1 \geq m$ implies that $\beta := f^c(\alpha) = f^{c-1}(\alpha)$. Furthermore, since $d > 1$ and $f(x)$ is generic, $\Phi_{f,d}(\beta) \neq 0$. Hence

$$\Phi_{f,c,d}(\alpha) = \frac{\Phi_{f,d}(f^c(\alpha))}{\Phi_{f,d}(f^{c-1}(\alpha))} = \frac{\Phi_{f,d}(\beta)}{\Phi_{f,d}(\beta)} = 1.$$

This identity holds for all α and $\Phi_{f,m,1}(x)$ is squarefree by Lemma 2.13, therefore $\Phi_{f,m,n}(x)$ divides $\Phi_{f,c,d}(x) - 1$. □

Example 3.2. We show that condition (1) from Theorem 3.1 is *generically* necessary, in the sense that if $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in K(a_0, a_1 \ldots, a_k)[x]$ is the generic polynomial of degree k, and if $n, d \geq 1$ are integers satisfying $n \mid d$, then $\Phi_{f,0,n}(x) = \Phi_{f,n}(x)$ does not divide $\Phi_{f,d}(x) - 1$. If $n = d$, this is immediate so we assume that $n < d$.

Consider the polynomial $f(x) := x^k + a \in K(a)[x]$, where a is an indeterminate. If the characteristic of K does not divide k, then Theorem 2.2, Corollary 3.3, and Proposition 3.4 of [9] combine to show that the resultant $\mathrm{Res}(\Phi_{f,n}(x), \Phi_{f,d}(x))$ with respect to x is a nonconstant polynomial in $K[a]$. Thus there exists $a_0 \in \overline{K}$ such that, for the polynomial $f_0(x) := x^k + a_0$, the dynatomic polynomials $\Phi_{f_0,n}(x)$ and $\Phi_{f_0,d}(x)$ have a common root x_0. (Over $\mathbb{C}$, these values

of c_0 are roots of hyperbolic components of the degree-k multibrot set.) It follows that $\Phi_{f_0,n}(x)$ cannot divide $\Phi_{f_0,d}(x) - 1$, therefore this divisibility relation cannot hold generically.

Next suppose that the characteristic of K divides k. Let $\zeta \in \overline{K}$ be a root of $\Phi_d(x)$, let $f(x) := x^k + \zeta x$, and let α be any root of $\Phi_{f,n}(x)$. Since $f'(x) = \zeta$, the period-n multiplier of α is $(f^n)'(\alpha) = \zeta^n$, a root of $\Phi_{d/n}(x)$. It then follows from [9, Thm. 2.2] that $\mathrm{Res}(\Phi_{f,n}(x), \Phi_{f,d}(x)) = 0$. Therefore $\Phi_{f,n}(x)$ and $\Phi_{f,d}(x)$ have a common root, whence $\Phi_{f,n}(x)$ does not generically divide $\Phi_{f,d}(x) - 1$.

Example 3.3. Condition (1) in Theorem 3.1 is sufficient to guarantee that $\Phi^{\pm}_{f,d}(\alpha) \neq 0$ for any root α of $\Phi_{f,m,n}(x)$. If (1) fails to hold, deciding whether or not $\Phi_{f,m,n}(x)$ divides $\Phi_{f,d}(x) - 1$ is more subtle.

Consider the quadratic polynomial family $f_a(x) = x^2 + a$. One may verify computationally that $\Phi_{f_a,6}(x) - 1$ factors over the function field $\mathbb{Q}(a)$ as

$$\Phi_{f_a,6}(x) - 1 = h_a(x)\Phi_{f_a,1,2}(x)\Phi_{f_a,1,1}(x)$$

where $h_a(x)$ is a degree 50 irreducible non-dynatomic polynomial with coefficients in $\mathbb{Q}(a)$. The cocore of $d = 6$ is 1 and

$$M_6(x) = \tfrac{1}{6}(x^6 - x^3 - x^2 + x) = \tfrac{1}{6}(x^4 + x^2 - x)(x^2 - 1),$$

hence conditions (2) and (3) of Theorem 3.1 hold for $m = 0$ and $n = 2$, and yet $\Phi_{f_a,2}(x)$ does not generically divide $\Phi_{f_a,6}(x) - 1$. On the other hand, if $a = -1$ or $a = -5/4$, then one may check that $\Phi_{f_a,0,2}(x)$ does divide $\Phi_{f,6}(x) - 1$.

If $m = 0$ and $n = 1$, then condition (1) of Theorem 3.1 is never satisfied. However, the following Proposition shows that in certain cases the conclusion of Theorem 3.1 still holds.

Proposition 3.4. *Let $f(x) \in K[x]$ be a polynomial with fixed point $\alpha \in \overline{K}$, let $\lambda := f'(\alpha)$ be the multiplier of α, and let $d \geq 2$ be an integer, then*

$$\Phi_{f,d}(\alpha) = \Phi_d(\lambda).$$

Moreover, if $\lambda = 0$ or if

(1) λ is a primitive nth root of unity,
(2) n is coprime to d, and
(3) $x^n - 1$ divides $M_d(x)$,

then $\Phi_{f,d}(\alpha) = 1$.

Note that $\Phi_{f,d}(\alpha)$ is the dth dynatomic polynomial of $f(x)$ evaluated at a fixed point α and $\Phi_d(\lambda)$ is the dth cyclotomic polynomial evaluated at the multiplier λ of α.

Proof. Since $(f^k)'(\alpha) = \lambda^k$,

$$f^k(x) - x \equiv (\lambda^k - 1)(x - \alpha) \bmod (x - \alpha)^2.$$

First suppose that λ is not a dth root of unity. Then the $(x - \alpha)$-adic valuation of $f^e(x) - x$ is one for each $e \mid d$. Thus

$$\Phi_{f,d}(x) = \prod_{e|d}(f^e(x) - x)^{\mu(d/e)} = \prod_{e|d}\left(\frac{f^e(x) - x}{x - \alpha}\right)^{\mu(d/e)},$$

where the second equality uses the fact that $\sum_{e|d} \mu(d/e) = 0$ for any $d \geq 2$. Evaluating at $x = \alpha$ gives

$$\Phi_{f,d}(\alpha) = \prod_{e|d} (\lambda^e - 1)^{\mu(d/e)} = \Phi_d(\lambda).$$

Fix a degree k and consider the affine algebraic variety

$$V_k := \{(f, \alpha) : \deg(f) \leq k \text{ and } \alpha \text{ is a fixed point of } f\}.$$

The identity $\Phi_{f,d}(\alpha) = \Phi_d(f'(\alpha))$ holds on the Zariski open subset of all pairs (f, α) for which the multiplier $\lambda = f'(\alpha)$ is not a dth root of unity, hence it must hold on all of V_k.

If $\lambda = 0$, then $d \geq 2$ implies that $\Phi_d(0) = 1$, hence $\Phi_{f,d}(\alpha) = 1$. Our assumption that n is coprime to d and that $x^n - 1$ divides $M_d(x)$ implies, by Theorem 3.12, that $\widehat{\mathcal{U}}_n \subseteq \bigcup_{p|d} \mathcal{H}_p$. Therefore $1 = \Phi_d(\lambda) = \Phi_{f,d}(\alpha)$ by [5, Thm. 1.1]. □

Remark 3.5. The identity proved in Proposition 3.4 is implicit in the proof of Theorem 2.2 of Morton and Vivaldi [9]; see the paragraph starting with display line (2.3). Hyde [5, Thm. 1.8(2)] characterizes the pairs (n, d) for which $d \nmid n$ and $\Phi_d(\zeta_n) = 1$. Using this characterization and Proposition 3.4 one may construct special dynamical unit relations from fixed points α with $\lambda = \zeta_n$ which do not hold universally.

For example, one may check that $\Phi_{231}(\zeta_{12}) = 1$ and $x^{12} - 1$ does not divide $M_{231}(x)$. It is not generally the case that $\Phi_{f,231}(\alpha) = 1$ for fixed points α, but this identity does hold if the multiplier of α is a primitive 12th root of unity (e.g. $f(x) = x^2 + \zeta_{12}x$ with $\alpha = 0$.)

3.1. **Dynamical necklace polynomials.** The composition ring $\mathbb{Z}\{f\}$ also carries an additive Ψ-module structure where the natural action $[m] \cdot [f] := [f^m]$ is extended linearly. With respect to this structure we may define *dynamical necklace polynomials* $M_{f,d}(x)$ analogous to the necklace polynomials $M_d(x)$,

$$M_{f,d}(x) := \frac{1}{d} \sum_{e|d} \mu(e) f^{d/e}(x) = (x/d) \circ \varphi_d[f].$$

We are unaware of any natural interpretation, dynamical or otherwise, of the dynamical necklace polynomials $M_{f,d}(x)$. Nevertheless, the methods developed in the previous sections allow us to easily prove the following analog of Theorem 3.1.

Proposition 3.6. *Let K be a field and let $f(x) \in K[x]$ be a polynomial. If*

(1) the cocore of d is at least m, and

(2) $x^n - 1$ divides the dth necklace polynomial $M_d(x)$ in $\mathbb{Q}[x]$,

then $f^{m+n}(x) - f^m(x)$ divides $M_{f,d}(x)$.

Proof. Proposition 2.12 and assumptions (2), (3) imply that $\varphi_d = 0 \bmod \mathbb{Z}\Psi_{m,n}$. Thus $\varphi_d \alpha \equiv 0 \bmod \mathbb{Z}_{m,n}\{f\}$ for any $\alpha \in \mathbb{Z}\{f\}$ by an additive version of Lemma 2.7. Hence by Lemma 2.21,

$$M_{f,d}(x) = (x/d) \circ \varphi_d[f] \equiv (x/d) \circ 0 \bmod (f^{m+n}(x) - f^m(x)).$$

Note that for $r \in R$ an element of any composition algebra,

$$r \circ 0 = r \circ (0 + 0) = (r \circ 0) + (r \circ 0),$$

hence $r \circ 0 = 0$. Thus

$$M_{f,d}(x) \equiv 0 \bmod (f^{m+n}(x) - f^m(x)),$$

which is to say that $f^{m+n}(x) - f^m(x)$ divides $M_{f,d}(x)$. □

3.2. **Dynamical units.** Theorem 3.1 has implications for the construction of dynamical units. Inspired by the theory of cyclotomic and elliptic units, Narkiewicz [10] and later Morton and Silverman [8] initiated the study of *dynamical units*: algebraic units constructed in one of several closely related ways from differences of preperiodic points of a rational map of the projective line. The inspiration comes from the fact that, in the dictionary between dynamical height and the usual Weil height on the torus $\mathbb{G}_m(\overline{\mathbb{Q}})$, the preperiodic points play the same role as that of roots of unity, so the fields generated by these points are naturally thought of as *dynatomic fields* in analogy with the classical theory of cyclotomic fields. We refer the reader to [12, Section 3.11] for further background on dynamical units.

Some families of dynamical units are known. Let K be a number field with ring of integers $\mathcal{O}_K$. Narkiewicz ([10], cf. [8, Thm. 6.3(a)]) proved that if $f \in \mathcal{O}_K[x]$ is a monic polynomial of degree at least 2, $\alpha \in \overline{K}$ is a root of $\Phi_{f,n}(x)$ for some $n \geq 2$, and $i, j \geq 0$ are integers such that $\gcd(i-j, n) = 1$, then

$$\frac{f^i(\alpha) - f^j(\alpha)}{f(\alpha) - \alpha} \in \mathcal{O}_K^\times$$

is a dynamical unit. If $\zeta = \zeta_{p^m}$ denotes a primitive prime power order root of unity, then the reader will note the similarity to cyclotomic units in the maximal totally real subfield $\mathbb{Q}(\zeta)^{\mathrm{tr}}$ of $\mathbb{Q}(\zeta)$ given by

$$\zeta^{(1-a)/2}\frac{1-\zeta^a}{1-\zeta}, \quad \text{where} \quad 1 < a < p^m/2 \text{ and } \gcd(a,p) = 1.$$

It is known that units of this form, together with -1, generate the unit group of $\mathbb{Q}(\zeta)^{\mathrm{tr}}$, and that this group has finite index in the unit group of $\mathbb{Q}(\zeta)$.

Morton and Silverman proved in [8, Thm. 6.3(b)] (see also [8, Prop. 7.4] for a formulation which is closer to our result) that if $f(x) \in \mathcal{O}_K[x]$ is monic of degree at least 2, and $\alpha, \beta \in \overline{K}$ are points of strict period m and n respectively, where $m, n \in \mathbb{N}$ satisfy $m \nmid n$ and $n \nmid m$, then in fact

$$\alpha - \beta \in \mathcal{O}_K^\times$$

is a dynamical unit. Under the same assumptions on $f(x)$, Benedetto proved that if $m \geq 1$ and α is a root of $\Phi_{f,m,n}(x)$ and β is a root of $\Phi_{f,d}(x)$ for some $n, d \geq 1$, then again, $\alpha - \beta \in \mathcal{O}_K^\times$ (see [1, Thm. 3]). Benedetto's result has interesting implications. For example, if $\{\alpha_1, \ldots, \alpha_n\}$ is an n-cycle for $f(x) = x^2 + c$, that is, if $f(\alpha_1) = \alpha_2$, $f(\alpha_2) = \alpha_3$, $\ldots$, $f(\alpha_n) = \alpha_1$, then Benedetto shows [1, Theorem 1] that

$$\prod_{i=1}^{n}(f(\alpha_i) + \alpha_i) = 1,$$

and in particular, that $f(\alpha) + \alpha$ is a dynamical unit. This result is particularly remarkable as, from a dynamical perspective, one would not expect the sum of points to be related to the dynamics of a quadratic map. For a more recent result involving quadratic forms and dynamical units for rational maps, we also refer the reader to the work of Panraksa and Washington [11].

Theorem 3.1 allows us to deduce similar results about dynamical units, extending the results of Morton-Silverman and Benedetto. Note that if $f \in \mathcal{O}_K[x]$ is monic, then $\Phi_{f,m,n}(x) \in \mathcal{O}_K[x]$ is monic as well, and so our preperiodic points are algebraic integers. It follows that if $\Phi_{f,m,n}(x)$ divides $\Phi_{f,d}(x) - 1$, then for each root $\alpha \in \overline{K}$ of $\Phi_{f,m,n}(x)$,

$$1 = \Phi_{f,d}(\alpha) = \prod_{\beta}(\alpha - \beta), \tag{3.2}$$

where the product ranges over all the roots β of $\Phi_{f,d}(x)$ with multiplicity. Since α, β are algebraic integers, (3.2) implies that the differences $\alpha - \beta$ are dynamical units. If the conditions of Theorem 3.1 are satisfied for m, n, d, then (3.2) holds for all $f(x)$ with degree at least 2. We view these as *universal relations* for dynamical units. In the case where the conditions of Theorem 3.1 are met with $m = 0$ and $n \nmid d$, we recover the result of Morton and Silverman quoted above. However, our result also applies in cases where the results of Morton and Silverman, and those of Benedetto, do not apply.

Example 3.7. If $(m, n, c, d) = (1, 2, 1, 3)$, then the conditions of Theorem 3.1 hold. Suppose that K is a number field, $f(x) \in \mathcal{O}_K[x]$ is a monic polynomial of degree at least 2. If $\alpha, \beta \in \overline{K}$ are roots of $\Phi_{f,1,2}(x)$ and $\Phi_{f,1,3}(x)$, respectively, then $\alpha - \beta$ is a dynamical unit. This class of dynamical units is new; the results of Morton-Silverman and Benedetto for differences of preperiodic points both required at least one of the points to be purely periodic, while both points here are *strictly* preperiodic.

Morton and Silverman [8, Prop. 7.4(b)] prove that if all the prime factors of $d > 1$ are congruent to $1 \bmod n$, then $\Phi_{f,n}(x)$ divides $\Phi_{f,d}(x) - 1$. This is a special case of Corollary 3.8.

Corollary 3.8. *Let $d > 1$ and $n \geq 1$ be integers such that $n \nmid d$ and suppose that d is divisible by some prime $p \equiv 1 \bmod n$. Then $\Phi_{f,n}(x)$ divides $\Phi_{f,d}(x) - 1$.*

Proof. Recall that if $d = \prod_p p^{k_p}$ is the prime factorization of d, then φ_d factors as

$$\varphi_d = \prod_p [p^{k_p - 1}]([p] - [1]).$$

Thus if $p \equiv 1 \bmod n$, then $\varphi_d \equiv 0 \pmod n$. The proof of Proposition 2.12 shows that this is equivalent to $x^n - 1$ dividing $M_d(x)$. Conditions (1) and (2) of Theorem 3.1 are trivially satisfied since $m, c = 0$, hence Theorem 3.1 implies that $\Phi_{f,n}(x)$ divides $\Phi_{f,d}(x) - 1$. □

Note that if all the primes dividing d are $1 \bmod n$, as is assumed in [8, Prop. 7.4(b)], then d and n are coprime, hence $n \nmid d$. Thus the Morton-Silverman result follows. In terms of hyperplanes covering the group of Dirichlet characters (see Section 3.3), the case $p \equiv 1 \bmod n$ for some prime $p \mid d$ corresponds to the situation where $\mathcal{H}_p = \widehat{\mathcal{U}_n}$ is the trivial hyperplane.

We can generalize the result of Benedetto in the following fashion:

Proposition 3.9. *Suppose that K is a number field with ring of integers $\mathcal{O}_K$, $f(x) \in \mathcal{O}_K[x]$ is monic of degree at least 2, and $\beta \in \overline{K}$ is a root of $\Phi_{f,d}(x)$ for some $d \geq 2$. Then $\Phi_{f,1,1}(\beta)$ is a dynamical unit satisfying the relation*

$$\prod_{\substack{\beta \\ \Phi_{f,d}(\beta) = 0}} \Phi_{f,1,1}(\beta) = 1 \tag{3.3}$$

where the product is taken over the roots of $\Phi_{f,d}$ with multiplicity.

Proof. We begin by noting that if $m = n = 1$ and $c = 0$ and $d \geq 2$, then the indices meet the conditions (1)-(3) of Theorem 3.1: The first two conditions are obvious, and the third follows from observing that

$$M_d(1) = \frac{1}{d} \sum_{e \mid d} \mu(e) 1^{d/e} = 0$$

for all $d \geq 2$, so $(x-1) \mid M_d(x)$ in $\mathbb{Q}[x]$. Thus Theorem 1.1 guarantees that $\Phi_{f,1,1}(x)$ divides $\Phi_{f,d}(x) - 1$. This means that if α is any root of $\Phi_{f,1,1}(x)$, then

$$\Phi_{f,d}(\alpha) = \prod_{\substack{\beta \\ \Phi_{f,d}(\beta)=0}} (\alpha - \beta) = 1 \tag{3.4}$$

where the roots of β of $\Phi_{f,d}$ are counted with multiplicity. Taking the product of the identities (3.4) as α varies over the roots of $\Phi_{f,1,1}(x)$ with multiplicity gives

$$\mathrm{Res}(\Phi_{f,1,1}, \Phi_{f,d}) = \prod_{\substack{\alpha \\ \Phi_{f,1,1}(\alpha)=0}} \prod_{\substack{\beta \\ \Phi_{f,d}(\beta)=0}} (\alpha - \beta) = 1.$$

This resultant may also be expressed as,

$$\mathrm{Res}(\Phi_{f,1,1}, \Phi_{f,d}) = \prod_{\substack{\beta \\ \Phi_{f,d}(\beta)=0}} \Phi_{f,1,1}(\beta) = 1$$

which gives us the desired result. □

To see why this generalizes Benedetto's result, observe that when $f(x) = x^2 + c$, one can check that

$$\Phi_{f,1,1}(x) = \frac{\Phi_{f,1}(f(x))}{\Phi_{f,1}(x)} = \frac{f^2(x) - f(x)}{f(x) - x} = f(x) + x$$

and we recover the result that $f(\alpha) + \alpha$ is a dynamical unit, although our multiplicative identity differs slightly from that of Benedetto, as it is a product over other points of formal period d (that is, roots of $\Phi_{f,d}(x)$; for a review of the difference between formal and strict period, we refer the reader to [12, §4.1]), rather than the points directly in the cycle of α. We can also easily find further examples of this sort:

Corollary 3.10. *Suppose $K, \mathcal{O}_K$ are as above and $f(x) = x^2 + b_1 x + b_0 \in \mathcal{O}_K[x]$. Then for any $d \geq 2$,*

$$\prod_{\substack{\alpha \\ \Phi_{f,d}(\alpha)=0}} (f(\alpha) + \alpha + b_1) = 1, \tag{3.5}$$

so $f(\alpha) + \alpha + b_1$ is a dynamical unit for any $\alpha \in \overline{K}$ of formal period $d \geq 2$. Likewise, if $f(x) = x^3 + 1 \in \mathbb{Z}[x]$, then

$$\prod_{\substack{\alpha \\ \Phi_{f,d}(\alpha)=0}} (1 + \alpha + \alpha^2 + 2\alpha^3 + \alpha^4 + \alpha^6) = 1. \tag{3.6}$$

Thus if $\alpha \in \overline{K}$ is of formal period $d \geq 2$, then $1 + \alpha + \alpha^2 + 2\alpha^3 + \alpha^4 + \alpha^6$ is a dynamical unit.

3.3. **Cyclotomic factors of necklace polynomials.** As discussed in the introduction, the most subtle condition in Theorem 3.1 is $x^n - 1$ dividing $M_d(x)$. Theorem 3.12 gives an alternative characterization of this divisibility in terms of hyperplane arrangements in finite abelian groups.

Definition 3.11. For $n \geq 1$, let $\mathcal{U}_n := (\mathbb{Z}/(n))^\times$ denote the multiplicative group of units modulo n and let $\widehat{\mathcal{U}}_n := \mathrm{Hom}(\mathcal{U}_n, \mathbb{C}^\times)$ denote the group of Dirichlet characters of modulus n. If $q \in \mathcal{U}_n$, then the *hyperplane* $\mathcal{H}_q \subseteq \widehat{\mathcal{U}}_n$ is the set

$$\mathcal{H}_q := \{\chi \in \widehat{\mathcal{U}}_n : \chi(q) = 1\}.$$

Theorem 3.12. *Let $d, n \geq 1$. Then $x^n - 1$ divides $M_d(x)$ if and only if*

$$\widehat{\mathcal{U}}_n \subseteq \bigcup_{\substack{p \mid d \\ p \nmid n}} \mathcal{H}_p.$$

Proof. As we argued in the proof of Proposition 2.12, Lemma 2.9 implies that $\varphi_d \equiv 0 \pmod{n}$ if and only if $\varphi_d x/d = M_d(x)$ is divisible by $x^n - 1$. Let $\tilde{d}$ be the largest factor of d coprime to n. The group ring $\mathbb{Q}[\mathcal{U}_n]$ naturally embeds into $\mathbb{Q}\Psi_{0,n}$ as the $\mathbb{Q}$-span of $[q]$ for $q \in \mathcal{U}_n$, and $\varphi_{\tilde{d}} \in \mathbb{Q}[\mathcal{U}_n] \subseteq \mathbb{Q}\Psi_{0,n}$. Observe that

$$\varphi_{\tilde{d}} = \sum_{e \mid \tilde{d}} \mu(e)[\tilde{d}/e] = [\tilde{d}] \prod_{p \mid \tilde{d}} (1 - [p]^{-1}) \in \mathbb{Q}[\mathcal{U}_n],$$

where the product is taken over all primes p dividing $\tilde{d}$. Recall that each character $\chi \in \widehat{\mathcal{U}}_n$ extends to a ring homomorphism $\chi : \mathbb{Q}[\mathcal{U}_n] \to \mathbb{C}$. Thus if $\chi \in \widehat{\mathcal{U}}_n$, then

$$\chi(\varphi_{\tilde{d}}) = \chi(\tilde{d}) \prod_{p \mid \tilde{d}} (1 - \overline{\chi(p)}).$$

If $\chi_i \in \widehat{\mathcal{U}}_n$ for $1 \leq i \leq \varphi(n)$ are the distinct characters of $\mathcal{U}_n$, then the map

$$\alpha \in \mathbb{Q}[\mathcal{U}_n] \longmapsto (\chi_1(\alpha), \chi_2(\alpha), \ldots, \chi_{\varphi(n)}(\alpha)) \in \mathbb{C}^{\varphi(n)}$$

is an embedding of rings. Hence $\alpha = 0$ in $\mathbb{Q}[\mathcal{U}_n]$ if and only if $\chi_i(\alpha) = 0$ for all χ_i. Thus $\varphi_{\tilde{d}} = 0$ in $\mathbb{Q}[\mathcal{U}_n]$ if and only if for each $\chi \in \widehat{\mathcal{U}}_n$ there is some prime $p \mid \tilde{d}$ such that $\chi(p) = 1$. This is equivalent to $\widehat{\mathcal{U}}_n \subseteq \bigcup_{p \mid \tilde{d}} \mathcal{H}_p = \bigcup_{p \mid d, p \nmid n} \mathcal{H}_p$.

Hence if $\widehat{\mathcal{U}}_n \subseteq \bigcup_{p \mid \tilde{d}} \mathcal{H}_p$, then

$$dM_d(x) = \varphi_d x = (\varphi_{\tilde{d}} \varphi_{d/\tilde{d}})x = \varphi_{\tilde{d}} \cdot (\varphi_{d/\tilde{d}} x) \equiv 0 \cdot (\varphi_{d/\tilde{d}} x) \equiv 0 \bmod x^n - 1.$$

Conversely, suppose that $x^n - 1$ divides $M_d(x)$. Let $U \subseteq \mathbb{Q}[x]/(x^n - 1)$ denote the $\mathbb{Q}$-subspace spanned by x^j with j coprime to n, and let $S_d(x) := dM_d(x)$. Observe that

$$S_d(x) = \varphi_d x = \varphi_{d/\tilde{d}} S_{\tilde{d}}(x) = \sum_{e \mid d/\tilde{d}} \mu(d/\tilde{d}e) S_{\tilde{d}}(x^e).$$

Since $\tilde{d}$ is the largest factor of d coprime to n, it follows that each $e > 1$ dividing $d/\tilde{d}$ shares a nontrivial common factor with n. Hence the U-component of $S_d(x)$ is $\pm S_{\tilde{d}}(x)$. Hence if $S_d(x) \equiv 0 \bmod x^n - 1$, then it must be the case that $S_{\tilde{d}}(x) \equiv 0 \bmod x^n - 1$. As argued above, this is equivalent to $\widehat{\mathcal{U}}_n \subseteq \bigcup_{p \mid \tilde{d}} \mathcal{H}_p$. □

Remark 3.13. Theorem 3.12 is closely related to [5, Thm. 1.13] but with a slightly different scope. Neither result directly implies the other.

Example 3.14. The following example is adapted from [5, Ex. 2.8]. Let $d = 440512358437 = 47^2 \cdot 73 \cdot 79 \cdot 151 \cdot 229$ and let $n = 65$. The group $\widehat{\mathcal{U}}_{65} \cong (\mathbb{Z}/(65))^\times$ decomposes as $\widehat{\mathcal{U}}_{65} \cong \mathbb{Z}/(4)^2 \times \mathbb{Z}/(3)$. Note that each hyperplane $\mathcal{H}_p \subseteq \widehat{\mathcal{U}}_{65}$ is a subgroup, hence factors as $\mathcal{H}_p \cong \mathcal{H}_p^{(4)} \times \mathcal{H}_p^{(3)}$ with $\mathcal{H}_p^{(4)} \subseteq \mathbb{Z}/(4)^2$ and $\mathcal{H}_p^{(3)} \subseteq \mathbb{Z}/(3)$. In this case, each of the hyperplanes $\mathcal{H}_p$ with $p \mid d$ is trivial in the 3-torsion $\mathcal{H}_p^{(3)} = \mathbb{Z}/(3)$. Thus it suffices to consider the 4-torsion $\mathcal{H}_p^{(4)}$ of each hyperplane $\mathcal{H}_p$.

Identifying the 4-torsion of $\widehat{\mathcal{U}_{65}}$ with the additive group $\mathbb{Z}/(4)^2$, the group $\mathcal{U}_{65} := (\mathbb{Z}/(65))^\times$ of units modulo 65 has a compatible isomorphism $\rho : \mathcal{U}_{65} \to \langle x, y : 4x = 4y = 0\rangle$ with the dual group of $\mathbb{Z}/(4)^2$. With respect to such an isomorphism, (the 4-torsion of) each hyperplane $\mathcal{H}_p$ may be realized as the vanishing set of a homogeneous linear form, hence the hyperplane terminology.

The units 47 and 151 generate a $\mathbb{Z}/(4)^2$ subgroup of $\mathcal{U}_{65}$, so we may choose coordinates ρ such that $x := \rho(47)$ and $y := \rho(151)$. Then the hyperplanes $\mathcal{H}_p$ may be visualized as lines in the "plane" $(\mathbb{R}/4\mathbb{Z})^2$. Each of the five distinct primes dividing d corresponds to a different colored line in the diagram below. For example, since $229 \equiv 47^2 \cdot 151^{-1} \bmod 65$, the (4-torsion of the) hyperplane $\mathcal{H}_{229}$ is the solution set of $2x - y = 0$ in $\mathbb{Z}/(4)^2$. Figure 3 shows the linear forms defining each line with respect to this choice of coordinates.

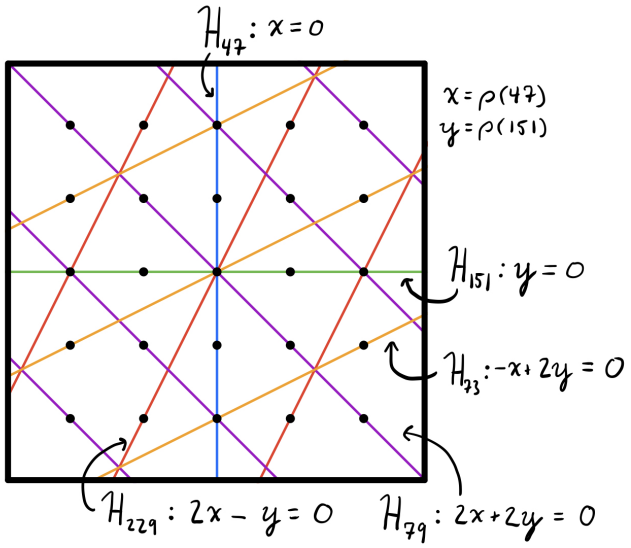

FIGURE 3. The lattice points in $(\mathbb{R}/4\mathbb{Z})^2$ may naturally be identified with $\mathbb{Z}/(4)^2$.

Since the five lines $\mathcal{H}_p$ with $p \mid d$ cover all of $\mathbb{Z}/(4)^2$, it follows that $\widehat{\mathcal{U}_{65}} \subseteq \bigcup_{p|d} \mathcal{H}_p$, with $d = 440512358437$. The cocore of d is 47. Hence Theorem 1.1 implies that for any polynomial $f(x) \in K[x]$ with degree at least 2 and any $m \leq 47$,

$$\Phi_{f,m,65}(x) \text{ divides } \Phi_{f,440512358437}(x) - 1.$$

By drawing other arrangements of lines covering $\mathbb{Z}/(4)^2$ and finding primes in the corresponding congruence classes modulo 65 (which must exist by Dirichlet's theorem on primes in arithmetic progressions) we may construct several other nontrivial examples of d for which $\widehat{\mathcal{U}_{65}} \subseteq \bigcup_{p|d} \mathcal{H}_p$. Three examples are given in Figure 4.

Values of d corresponding to the three arrangements in Figure 4 are, respectively,

$$d_1 = 157 \cdot 181 \cdot 337 \cdot 389$$
$$d_2 = 79 \cdot 181 \cdot 389$$
$$d_3 = 47 \cdot 109 \cdot 151 \cdot 157 \cdot 317 \cdot 337.$$

Each of these d_i are squarefree and coprime to 65, so it follows that

$$\Phi_{f,m,65}(x) \text{ divides } \Phi_{f,d_i}(x) - 1$$

for each $m = 0, 1$ and each d_i.

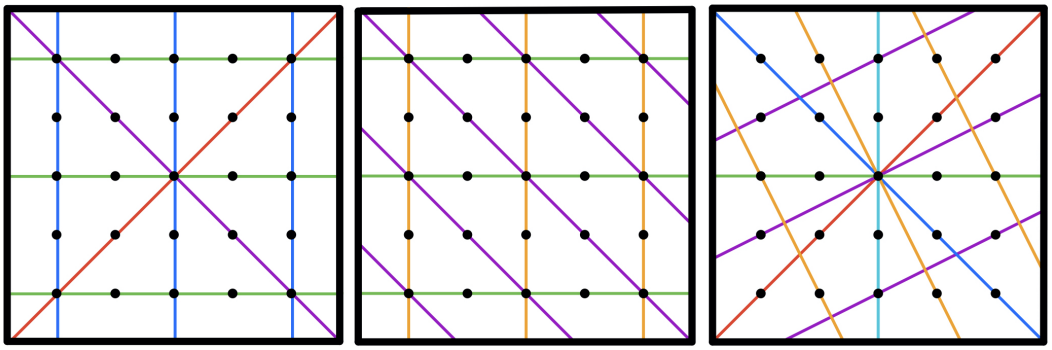

FIGURE 4.

REFERENCES

[1] R. L. Benedetto, An elementary product identity in polynomial dynamics, *Am. Math. Mon.*, **108**, no. 9 (2001), 860–864.

[2] J. R. Doyle and B. Poonen, Gonality of dynatomic curves and strong uniform boundedness of preperiodic points, *Compos. Math.*, **156** (2020), 733–743.

[3] N. Fakhruddin, The algebraic dynamics of generic endomorphisms of $\mathbb{P}^n$, *Algebra Number Theory*, **8** (2014), 587–608.

[4] B. Hutz, Determination of all rational preperiodic points for morphisms of $\mathbb{P}^N$, *Math. Comp.*, **84**, no. 291 (2015), 289–308.

[5] T. Hyde, Cyclotomic factors of necklace polynomials, arXiv:1811.08601, 2020.

[6] P. Morton, On certain algebraic curves related to polynomial maps, *Compos. Math.*, **103**, no. 3 (1996), 319–350.

[7] P. Morton, P. Patel, The Galois theory of periodic points of polynomial maps, *Proc. London Math. Soc. (3)*, vol. 68, no. 2 (1994), 225–263.

[8] P. Morton, J. H. Silverman, Periodic points, multiplicities, and dynamical units, *J. reine angew. Math.*, **461** (1995), 81–122.

[9] P. Morton, F. Vivaldi, Bifurcations and discriminants for polynomial maps, *Nonlinearity*, **8** (1995), 571–584.

[10] W. Narkiewicz, Polynomial cycles in algebraic number fields, *Colloq. Math.*, **58**, no. 1 (1989), 151–155.

[11] C. Panraksa, L. Washington, Arithmetic dynamics and dynamical units, *East-West J. Math.*, **14**, no. 2 (2012), 201–207.

[12] J. H. Silverman, The arithmetic of dynamical systems, *Spring Science & Business Media*, **241** (2007).

DEPARTMENT OF MATHEMATICS, OKLAHOMA STATE UNIVERSITY, STILLWATER, OK 74078
Email address: john.r.doyle@okstate.edu

DEPARTMENT OF MATHEMATICS, OKLAHOMA STATE UNIVERSITY, STILLWATER, OK 74078
Email address: paul.fili@okstate.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO, CHICAGO, IL 60637,
Email address: tghyde@uchicago.edu