COMPOSITIO MATHEMATICA

PATRICK MORTON

On certain algebraic curves related to polynomial maps

Compositio Mathematica, tome 103, n° 3 (1996), p. 319-350

<http://www.numdam.org/item?id=CM_1996__103_3_319_0>

Compositio Mathematica **103:** 319–350, 1996.

On certain algebraic curves related to polynomial maps

PATRICK MORTON*
Dept. of Mathematics, Wellesley College, Wellesley, MA 02181, USA, e-mail: pmorton@lucy.wellesley.edu

Received 10 January 1995; accepted in final form 14 August 1995

Abstract. An algebraic/arithmetical proof of irreducibility over the algebraic closure of $\mathbf{Q}$ is given for the polynomial $\Phi_n(x,c)$ whose roots are the periodic points of least period n of the dynamical system $x \to f(x,c)$, where $f(x,c)$ is a polynomial in $\mathbf{Z}[x,c]$ satisfying several conditions, the most important being that the primitive n-bifurcation points, the complex values of c for which two n-orbits coincide, are distinct. A similar condition modulo p implies irreducibility of $\Phi_n(x,c)$ over the algebraic closure of the finite field $\mathbf{F}_p$ having p elements. The genus of the curve $C : \Phi_n(x,c) = 0$ is computed, along with the genus of the curve $\delta_n(x,c) = 0$ defined by the multipliers of period n orbits. The genus of the latter curve is shown to be greater than or asymptotic to $((k-1)/(2k) - 1/n)k^n$, as $n \to \infty$, where $k = \deg_x f$. This fact is used to prove the main result: for the polynomials $f(x,c)$ under consideration, and for large enough n, there are only finitely many cyclic extensions $N = L(\theta)$ of degree n of a given number field L for which $\theta \to f(\theta, a)$, with a in L, is a generating automorphism of Gal (N/L).

Key words: polynomial maps, periodic points, irreducibility

1. Introduction

If F is a field and $f(x) \in F[x]$, then the properties of the polynomial

$$\Phi_n(x) = \prod_{d|n} (f^d(x) - x)^{\mu(n/d)},$$

introduced in [20], [13] and [3] (when $f(x)$ is quadratic; see also [14]), have importance for the dynamical system defined by the map $x \to f(x)$ on the algebraic closure of F. All the periodic points of the map f having minimal period n are roots of $\Phi_n(x)$. In certain exceptional cases some of the roots of $\Phi_n(x)$ can have a minimal period less than n. Because of this, I will use the terminology of [14] and call the roots of $\Phi_n(x)$ the periodic points of f of *essential* period n. The polynomial $\Phi_n(x)$ is analogous to the n-division polynomial on an elliptic curve (see [18, p. 105] and [14]).

If $f(x,c)$ is a polynomial in $F[x,c]$, then the equation $\Phi_n(x) = \Phi_n(x,c) = 0$ defines an algebraic curve. In this paper I use properties of this curve to prove

* Supported by NSF grant DMS-9200575.

a finiteness theorem on the number of cyclic extensions of a given degree over a fixed algebraic number field which can have a generating automorphism of the form $\theta \to f(\theta, a)$, for some primitive element θ and some constant a (in the ground field) depending on the extension, and for polynomials f of a certain form (see Theorems B–E below). In this situation the polynomial $f(x, a)$ is called an automorphism polynomial for the cyclic extension. Like the results of [11] and [12], which consider quadratic polynomials f and cyclic extensions whose degrees are 3 or 4, the underlying idea is to take a noncanonical approach and see what can be said about algebraic number fields which correspond to a given automorphism polynomial. Though the class of polynomials considered is somewhat limited, for technical reasons, the methods are potentially applicable to larger families of polynomials. The main result can be viewed as evidence for an interesting connection between complex dynamics and Galois theory.

In order to prove this finiteness result, it is necessary to know if the polynomial $\Phi_n(x, c)$ is irreducible. For the map $f(x) = x^2 + c$, this has been answered in the affirmative by T. Bousch [3]. Using ideas from complex dynamics, Bousch [3] has shown that $\Phi_n(x, c)$ is indeed irreducible over $\mathbf{C}[c]$ and has computed its Galois group over this field. We note that his results easily imply the truth of conjecture 2(b) of [13] for the case $k = 2$, which states that the Galois group of $\Phi_n(x, c)$ over $\mathbf{Q}[c]$ is isomorphic to the wreath product of the cyclic group $\mathbf{Z}/n\mathbf{Z}$ by the symmetric group S_r, where $r = (\deg \Phi_n(x, c))/n$. (These and more general results have also been obtained by Schleicher and Lau [17], [10], by a different method. See the discussion below.)

In this paper we first consider the question of irreducibility of the polynomials $\Phi_n(x)$ over $\bar{\mathbf{Q}}$ (the algebraic closure of $\mathbf{Q}$) when $f(x) = f(x, c)$ is a homogeneous polynomial of degree $k \geqslant 2$ satisfying several simple conditions. In our generalization we follow the outlines of Bousch's proof, but at several steps replace the analytic or dynamical argument given by Bousch by an algebraic argument. (For $k > 2$ we also need to prove several lemmas that are not necessary in the case $k = 2$ considered in [3].) In this way we are able to isolate the analytic properties required to prove irreducibility to a single, easily computable statement about the factors of the discriminant of $\Phi_n(x)$. We also simplify Bousch's argument by eliminating the use of Zsigmondy's theorem [3]. In addition, the techniques we introduce allow us to prove irreducibility of $\Phi_n(x)$ over the algebraic closure of $\mathbf{F}_p$, for a specific set of primes p depending on f and n (see Section 5).

In order to state the theorem which results from this algebrization of Bousch's argument, we recall the following definitions and facts from [15]. If R is any integral domain and $f(x)$ in $R[x]$ is monic, let α_i be a periodic point of f with essential period n, and define the polynomial $\lambda_i(x)$ by

$$\lambda_i(x) = \prod_{j=0}^{n-1} (x - f^j(\alpha_i)). \tag{1}$$

If $\alpha_i, \ldots, \alpha_r$ are representatives of the orbits of roots of $\Phi_n(x)$, counted with proper multiplicities, then it is clear that

$$\Phi_n(x) = \prod_{i=1}^{r} \lambda_i(x), \tag{2}$$

where r is the number of orbits, and

$$r = \frac{1}{n} \deg \Phi_n(x) = \frac{1}{n} \sum_{d|n} \mu(n/d) k^d, \quad k = \deg f.$$

(These facts are easiest to prove by first assuming that f is a generic polynomial over $\mathbf{Q}$ and then specializing. See [13], Theorem 2.5. I am also grateful to Jacob Sturm (private communication) for his remarks in this regard). As usual, define the multiplier of the orbit containing α_i to be $\omega_n(\alpha_i) = (f^n)'(\alpha_i)$, and let $\delta_n(x)$ denote the polynomial whose roots are the multipliers of the different orbits:

$$\delta_n(x) = \prod_{i=1}^{r} (x - \omega_n(\alpha_i)).$$

The polynomial $\delta_n(x)$ has coefficients in R (see [20] and [13], Sect. 5) and there is a formula for the discriminant of $\Phi_n(x)$ which involves the factors of $\delta_n(1)$.

THEOREM A ([15]) *If $C_m(x)$ denotes the mth cyclotomic polynomial, and the expressions $\Delta_{n,d}$ are defined by means of the formulae*

$$\Delta_{n,d} = \text{Resultant}\,(C_{n/d}(x), \delta_d(x)), \quad \text{for } d|n, d < n$$

and

$$\delta_n(1) = \Delta_{n,n} \prod_{d|n, d<n} \Delta_{n,d}, \tag{3}$$

then $\Delta_{n,d} \in R[c_1, c_2, \ldots, c_k]$, where the c_i are the coefficients of f, and we have

$$\text{disc}\, \Phi_n(x) = \pm \Delta_{n,n}^{n} \prod_{d|n, d<n} \Delta_{n,d}^{n-d}. \tag{3'}$$

Moreover, the delta factors are also given by the expressions:

$$\Delta_{n,d} = \eta_1 \prod_{i=1}^{r} \Phi_d(\alpha_i)^{n/d}, \tag{4}$$

$$\Delta_{n,n} = \eta_2 \prod_{i \neq j} \lambda_j(\alpha_i); \tag{5}$$

here $\eta_1 = \eta_1(d)$ *and* η_2 *lie in the quotient field of* $R[\alpha_1, \ldots, \alpha_r]$ *and* $(\eta_1)^d$ *and* $(\eta_2)^n$ *are units in* $\mathbf{Z}[c_1, \ldots, c_k, \alpha_1, \ldots, \alpha_r]$ *(or* $\mathbf{Z}/p\mathbf{Z}[c_1, \ldots, c_k, \alpha_1, \ldots, \alpha_r]$*, if char* $R = p$*).*

In the case that $f(x) = f(x, c)$ is a polynomial in x and c, the delta factors defined above are polynomials in c. We may now state

THEOREM B *Let* $f(x) = f(x, u)$ *be a homogeneous polynomial in* $\mathbf{Z}[x, u]$ *of degree* $k \geqslant 2$ *satisfying the conditions*:

(i) $f(x, 0) = x^k$;
(ii) $\gcd(\operatorname{disc} f(x, 1), k^n - 1) = 1$;
(iii) $\Delta_{n,n}(u)$*, as a polynomial in* u*, has no multiple roots.*

Then $\Phi_n(x, u)$ is irreducible over $\bar{\mathbf{Q}}$ (or over $\mathbf{C}$).

The hypotheses of Theorem B are easy to verify in particular cases. The theorem is also true for polynomials $f(x, u)$ in $\mathbf{o}[x, u]$, where $\mathbf{o}$ is the ring of integers of an algebraic number field whose intersection with the field $\mathbf{Q}(\zeta_{k^n-1})$ of $(k^n - 1)$th roots of unity is just $\mathbf{Q}$; the proof is the same.

Condition (iii) of Theorem B is a dynamical condition, since it refers to bifurcation points, while condition (ii) is arithmetical. The latter condition plays a fundamental role in the proof of Theorem B, since it implies several facts: that $\Phi_n(x, u)$ splits completely in a suitable Laurent series field; that purported factors of $\Phi_n(x, u)$ have coefficients in $\mathbf{Q}$; that roots of irreducible factors of $\Phi_n(x, u)$ consist of complete orbits under f; and that $\delta_n(1)$ is primitive, as a polynomial in u (its coefficients have gcd equal to 1). An examination of the proof shows that condition (ii) may be replaced by three conditions:

(iia) $f(x, 1)$ has distinct roots [so that $\Phi_n(x, u)$ still splits];
(iib) the splitting field $F^{\sim}$ of $f(x, 1)$ over $\mathbf{Q}$ satisfies $F^{\sim} \cap \mathbf{Q}(\zeta_N) = \mathbf{Q}$, where $N = k^n - 1$ and ζ_N is a primitive Nth root of unity [to imply the facts about purported factors of $\Phi_n(x, u)$, and for the last step in Bousch's argument];
(iic) if p is a prime dividing $\operatorname{disc}(f(x, 1))$, then p does not divide all the coefficients of $\delta_n(1)$ [to get primitivity of $\delta_n(1)$].

Theorem B has the following corollary.

COROLLARY 1 *Let* $f(x) = x^k + c$*, for* $k \geqslant 2$*. If the polynomial* $\delta_n(1) = \delta_n(1, c)$ *has no multiple roots, then* $\Phi_n(x)$ *and* $\delta_n(x)$ *are irreducible over* $\bar{\mathbf{Q}}$*.*

The corollary follows from Theorem B by setting $c = -u^k$. It follows from results of Douady–Hubbard theory concerning the parameter space of the complex map $f(x) = x^k + c$ that $\delta_n(1, c)$ does in fact have simple roots (while we only need that $\Delta_{n,n}(c)$ has simple roots for irreducibility of $\Phi_n(x)$). The roots of $\delta_n(1, c)$ are the bifurcation points of the map f corresponding to period n. They are also the 'roots' of the hyperbolic components of period n, i.e., the images of 1 under certain homeomorphisms from the closed unit disk to the closures of the

hyperbolic components. These roots are distinct because the closures of hyperbolic components are disjoint. (For $k = 2$ see [5]; for $k \geqslant 2$ see [17], Theorem 4.2.3, and [15], Proposition 3.2.) Thus $\Phi_n(x)$ is absolutely irreducible for this family of maps. D. Schleicher and E. Lau have a different proof that $\Phi_n(x)$ is irreducible in this case, which depends on a combinatorial description of M_k, the analogue of the Mandelbrot set for the map $f(x) = x^k + c$ (see [17], [10]). Their argument also allows them to calculate the Galois group of $\Phi_n(x)$. These same results (for $f(x) = x^k + c$) have also been achieved independently by T. Bousch (private communication through D. Schleicher).

An immediate consequence of these remarks is conjecture 2(a) of [13]. (The argument given by Schleicher and Lau also implies conjecture 2(b) of [13].)

COROLLARY 2 *If* $f(x) = x^k + c_1 x^{k-1} + \cdots + c_k$ *is a generic polynomial over* $\mathbf{Q}$, $\Phi_n(x)$ *is irreducible over* $\bar{\mathbf{Q}}[c_1, c_2, \ldots, c_k]$.

The class of polynomials considered in Theorem B may be extended, using the same technique as for Corollary 1. Thus $\Phi_n(x, c)$ is irreducible over $\bar{\mathbf{Q}}$ if $f(x, c) \in \mathbf{Z}[x, c]$, $f(x, u^m)$ is homogeneous in x and u and satisfies conditions (i)–(iii), for some integer $m \geqslant 1$. For ease of reference we list these hypotheses, with (iii) replaced by a stronger condition:

(H) $f(x, u^m)$ is homogeneous in x and u, for some $m \geqslant 1$; $f(x, c)$ satisfies conditions (i)–(ii) of Theorem B (or conditions (iia)–(iic) in place of (ii)), and $\delta_n(1, c)$ has distinct roots.

As in Corollary 1, this condition also implies the irreducibility of $\delta_n(x, c)$. In Section 3 we give a direct computation of the genus of the curves defined by $\Phi_n(x, c) = 0$ and $\delta_n(x, c) = 0$ for the maps $f(x, c)$ satisfying (H). The genus of $\Phi_n(x, c) = 0$ for the map $f(x) = x^2 + c$ was given by Bousch [3], but the computations for other maps and for $\delta_n(x, c) = 0$ are new. These results follow naturally from Theorem A, and make use of the stronger hypothesis that $\delta_n(1, c)$ has no multiple roots.

THEOREM C *Assume* $f(x, c) \in \mathbf{Z}[x, c]$ *satisfies hypothesis (H).*
(a) *The genus of the curve* $\Phi_n(x, c) = 0$ *is given by*

$$g_n = \tfrac{1}{2}(nk - n - m - 1)\nu(n) - \frac{(k-1)}{2} \sum_{d|n, d<n} d\nu(d)\phi(n/d) + 1,$$

where $\nu(n) = \frac{1}{m} \sum_{e|n} \mu(n/e)k^e$ *and* ϕ *is Euler's phi-function.*
(b) *The genus* γ_n *of the curve* $\delta_n(x, c) = 0$ *is given by*

$$\gamma_n = \frac{1}{2}\left(k - 1 - \frac{m}{n}\right)\nu(n) - \frac{e_n}{2} - \frac{k-1}{2} \sum_{d|n, d<n} \nu(d)\phi(n/d) + 1,$$

where

$$e_n = \frac{1}{mn} \sum_{d|(m,n)} \phi(d)^2 \sum_{\substack{r|n, d|r \\ (n/r,d)=1}} \mu(n/r) k^{r/d}.$$

(c) *The genus of* $\delta_n(x,c) = 0$ *satisfies the inequality* $\gamma_n > (\frac{1}{2} - \frac{1}{2k} - \frac{1}{n})k^n + O(nk^{n/2})$, *as* $n \to \infty$, *with an implied constant that depends only on* k.

We note that the terms involving $\nu(n)$ and the Euler ϕ-function in parts (a) and (b) of this theorem result from computing the degrees in c of the discriminant factors $\Delta_{n,d}(c)$ (see the proofs of Theorems 11 and 12).

Part (c) of this theorem implies that the Douady–Hubbard multiplier maps from hyperbolic n-components of the Mandelbrot set to the unit disk (see [4] and [5]) live on Riemann surfaces whose genus goes to infinity with n. It also implies that the genus of the curve $\Phi_n(x,c) = 0$ goes to infinity as $n \to \infty$, and this leads to the following application for the map $f(x) = x^k + c$. (See Section 3.)

THEOREM D *For a fixed* $k \geqslant 2$ *and sufficiently large* n, *there are only finitely many values of* c *in a given algebraic number field* L *for which* $f(x) = x^k + c$ *has an essential* n*-periodic point lying in* L. *The same holds for* $f(x) = x^2 + c$, *for* $n \geqslant 4$.

In [12] it is proved that a map $f(x) = x^2 + c$ with rational c cannot have a rational 4-cycle. It is shown in [8] that such a map can never have a rational 5-cycle. It would be interesting to settle whether or not this map can ever have a rational n-cycle with $n \geqslant 6$ and c in $\mathbf{Q}$. The curve $\Phi_n(x,c) = 0$ does, however, have $\deg_x \Phi_n(x,c)/2$ distinct rational points at infinity, for any n; see Proposition 10. Moreover, this curve has finite rational points over $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p (see [12]); thus for $n = 4$ and $n = 5$ (and probably for $n \geqslant 6$) the equation $\Phi_n(x,c) = 0$ violates the Hasse principle.

The fact that the genus γ_n of $\delta_n(x,c) = 0$ goes to infinity with n leads to our main result.

THEOREM E (see Theorem 14) *Let* $f(x,c)$ *be a polynomial in* $\mathbf{Z}[x,c]$ *satisfying (H), for a certain value of* n. *If* $n \geqslant C(k)$, *a constant depending only on* $k = \deg_x f$, *there are only finitely many cyclic extensions* $N = L(\theta)$ *of a given number field* L *which have degree* n *over* L *and a generating automorphism of the form* $\theta \to f(\theta, a)$, *for some* a *in* L.

COROLLARY 1 *For a given* $k \geqslant 2$ *and* $n \geqslant C(k)$ *there are only finitely many cyclic extensions* $N = L(\theta)$ *of a given number field* L *which have degree* n *over* L *and a generating automorphism of the form* $\theta \to \theta^k + a$, *for some* a *in* L.

COROLLARY 2 *If $n \geqslant 5$, then there are only finitely many cyclic extensions N/L of degree n of a given number field L for which $\theta \to \theta^2 + a$, for some a in L, is a generator of Gal (N/L).*

The last result is a complement to results of [11] and [12] corresponding to the cases $n = 3$ and 4. In those papers the cyclic extensions N/L of a field L (with char $L \neq 2$) are determined which have $[N : L] = 3$ or 4 and a generating automorphism of the form $\theta \to \theta^2 + a$. When char $L = 0$, there are infinitely many such extensions. When $n = 5$, the relevant cyclic extensions of $\mathbf{Q}$ have been determined by Flynn, Poonen and Schaefer [8] (see Section 4).

Theorem E and its corollaries are a consequence of the fact that a cyclic extension N/L of degree n determines a unique L-rational point on the curve $\delta_n(x, c) = 0$.

As noted above, the roots of the multiplier equation $\delta_n(1, c) = 0$ are the 'roots' of hyperbolic components of period n in the parameter space of the complex family $f(x, c) = x^k + c$. Thus, the first corollaries to Theorems B and E show that the nature of these hyperbolic components influences the extent to which the specializations $f(x, a)$ can occur as automorphism polynomials for subfields of $\bar{\mathbf{Q}}$. In this sense complex dynamics has interesting connections to Galois theory.

All of the arguments of this paper are algebraic or arithmetical. The advantage of this approach is that the same techniques can be applied in characteristic p. Thus it is possible to show that p is a prime of good reduction for $\Phi_n(x, c) = 0$ whenever $\delta_n(1, c)$ and $f(x, 1)$ have distinct roots modulo p (Theorem 15). In particular, $\Phi_n(x, c)$ is absolutely irreducible over $\mathbf{F}_p$ for such primes. Dynamically, the condition on $\delta_n(1, c)$ means that the n-bifurcation points of the map f are all distinct modulo p. For $f(x) = x^2 + c$ and small values of n, odd primes at which $\Phi_n(x, c) = 0$ has bad reduction are rare (it always has bad reduction at 2). The first n for which this curve has bad reduction at an odd prime is $n = 5$, and then its only 'bad' primes are $p = 2, p = 5$ and $p = 3701$ (see [8]).

At present I do not have an algebraic/arithmetic proof that $\delta_n(1, c)$ has no multiple roots for the maps $f(x, c) = x^k + c$. It would be of interest to know whether the factors $\Delta_{n,d}(c)$ of the polynomial $\delta_n(1, c)$ are irreducible over $\mathbf{Q}$ in this case (as was conjectured in [15]). In general, is there an interpretation of the polynomials $\Delta_{n,d}(c)$ that would yield an algebraic proof that $\delta_n(1, c)$ has simple roots?

I am very grateful to J. Silverman, J. Sturm, A. Dupre, and B. Poonen for interesting conversations and correspondence, and to D. Schleicher for making me aware of the paper [3]. I am also grateful to B. Poonen for his computation of e_n in Lemma 12 (Section 3).

2. Proof of Theorem B.

We consider a homogeneous polynomial $f(x,u)$ of degree $k \geqslant 2$ in the variables x and u, with coefficients in a given field F, and satisfying the conditions:

$$f(x,0) = x^k \quad \text{and} \quad f(x,1) \text{ has } k \text{ distinct roots over } F. \tag{6}$$

The second condition is equivalent to the statement thst disc $f(x,1)$ is not zero in F, or that $f'(\zeta,1) \neq 0$ for any root ζ of $f(x,1) = 0$, where the prime denotes the derivative with respect to x. To fix notation we set

$$f(x,u) = x^k + c_1 x^{k-1} u + \cdots + c_k u^k. \tag{6'}$$

The first step is to find the roots of $\Phi_n(x)$ in the Laurent series field $L = F^{\sim}((1/u))$, where $F^{\sim}$ is the splitting field of $f(x,1)$ over F. To do this we consider the dynamical system given by the map $z \to f(z,u)$ on the field L. In what follows we denote by ζ a root of $f(x,1) = 0$ and by $f^j(z) = f^j(z,u)$ the jth iterate of $f(z,u)$ in the variable z.

LEMMA 1 *Assume the polynomial f satisfies (6), (6'). For any sequence* $\{\zeta_i, i \geqslant 0\}$ *of roots of* $f(x,1) = 0$, *there is a unique Laurent series z in* $L = F^{\sim}((1/u))$ *of the form*

$$z = u \sum_{m=0}^{\infty} \frac{a_m}{u^{m(k-1)}} = a_0 u + a_1/u^{k-2} + \cdots \tag{7}$$

for which

$$f^j(z,u) = \zeta_j u + O(1), \quad \text{for all } j \geqslant 0, \tag{8}$$

where $O(1)$ *denotes a power series in* $F^{\sim}[[1/u]]$. *If the coefficients of* $f(x,u)$ *lie in the ring R, then the* a_m *are in* $R[1/f'(\zeta_i), i \geqslant 0]$.

Proof. If z is given by (7), a_0 must be ζ_0 in order for (8) to hold for $i = 0$, and then

$$\begin{aligned} f(z) &= u^k \sum_{i=0}^{k} c_i \left(\sum_{m=0}^{\infty} \frac{a_m}{u^{m(k-1)}} \right)^{k-i} \\ &= u^k \left(f(a_0) + \sum_{m=1}^{\infty} \frac{b_m}{u^{m(k-1)}} \right) \\ &= u \left(b_1 + \sum_{m=1}^{\infty} \frac{b_{m+1}}{u^{m(k-1)}} \right) \end{aligned}$$

where

$$b_1 = \sum_{i=0}^{k}(k-i)c_i(a_0)^{k-i-1}a_1 = f'(\zeta_0)a_1$$

and

$$\begin{aligned} b_m &= \sum_{i=0}^{k}(k-i)c_i(a_0)^{k-i-1}a_m + \text{polynomial in } a_0, \ldots, a_{m-1} \\ &= f'(\zeta_0)a_m + \text{polynomial in } a_0, \ldots, a_{m-1}, \end{aligned}$$

for $m \geqslant 2$ ($f'(\zeta_0)$ is shorthand for $f'(\zeta_0, 1)$). Using the assumption that $f'(\zeta_0) \neq 0$, a_1 is determined by $b_1 = \zeta_1$.

If the coefficients $a_0, \ldots, a_{i-1}$ have been determined so that (8) is satisfied for $j \leqslant i-1$, then

$$f^{i-1}(z) = u\left(\zeta_{i-1} + \sum_{m=1}^{\infty}\frac{b_{m,i-1}}{u^{m(k-1)}}\right), \tag{9}$$

with

$$\begin{aligned} b_{m,i-1} &= f'(\zeta_0)f'(\zeta_1)\ldots f'(\zeta_{i-2})a_{m+i-1} \\ &\quad + \text{polynomial in } a_0, \ldots, a_{m+i-2}. \end{aligned} \tag{9'}$$

By the above computation,

$$\begin{aligned} f^i(z) &= u(f'(\zeta_{i-1})f'(\zeta_0)f'(\zeta_1)\ldots f'(\zeta_{i-2})a_i \\ &\quad + \text{polynomial in } a_0, \ldots, a_{i-1}) + O(1), \end{aligned}$$

and so the condition (8) determines the coefficient a_i uniquely. Now it is easily checked that $f^i(z)$ has the form given by (9), (9′) with i-1 replaced by i, and this proves the lemma. □

LEMMA 2 *If f satisfies (6), (6′), then the distinct solutions in $L = F^{\sim}((1/u))$ of $f^n(z) - z = 0$ correspond 1-1 to the sequences $\{\zeta_i, i \geqslant 0\}$ of roots of $f(x, 1) = 0$ which have period n. The roots of $\Phi_n(z) = 0$ correspond 1-1 to the sequences $\{\zeta_i, i \geqslant 0\}$ with minimal period n:*

$$\Phi_n(x) = \prod_s (x - z_s), \tag{10}$$

where s runs over the sequences $s = \{\zeta_i, i \geqslant 0\}$ with minimal period n and z_s is the series corresponding to the sequence s by Lemma 1.

Proof. The lemma is immediate from the uniqueness assertion of Lemma 1 and the fact that

$$f^i(f^n(z)) = \zeta_{i+n}u + O(1) = \zeta_i u + O(1) = f^i(z) + O(1), \quad \text{for } i \geqslant 0,$$

if z corresponds to a sequence $\{\zeta_i, i \geqslant 0\}$ with period n. □

This lemma shows that all of the periodic and pre-periodic points of the map $z \to f(z)$ on the algebraic closure of L are contained in L itself. If w represents the standard valuation on $L = F^{\sim}((1/u))(w(u) = -1)$, the formal Julia set of f may be defined as

$$J_f = \{z \text{ in } L : w(f^i(z)) \text{ is bounded from below, for } i \geqslant 0\}.$$

It can be shown that J_f is the closure of the set of periodic points of f in L, and that the dynamics of f on J_f is canonically isomorphic to symbolic dynamics on the set of all sequences $s = \{\zeta_i, i \geqslant 0\}$ of roots of $f(x, 1) = 0$.

The common hypothesis of the rest of the lemmas of this section, with the exception of Lemmas 4 and 7, will be that f satisfies (6), (6′).

LEMMA 3(a) *If $\Phi_n(x) = A(x)B(x)$ is a factorization of $\Phi_n(x)$ over $\bar{F}$, then $A(x)$ and $B(x)$ have coefficients in $F^{\sim}$, where $F^{\sim}$ is the splitting field of $f(x, 1)$ over F.*

(b) Assume $F = \mathbf{Q}$ and that $f(x, u)$ has coefficients in $\mathbf{Z}$. If $\Phi_n(x) = A(x)B(x)$ over $\bar{\mathbf{Q}}$, the coefficients of A and B lie in the ring $\mathbf{o}$ of algebraic integers of the splitting field $F^{\sim}$ of $f(x, 1)$ over $\mathbf{Q}$.

Proof. By Lemma 2 we have that $A(x)$ is a product of terms $x - z_s$ for s in a certain set of sequences S, if we consider the factorization (10) over the field $\bar{F}((1/u))$. Since $A(x)$ is a polynomial in x and u, all but finitely many of the terms in the Laurent series z_s cancel identically in the product of $x - z_s$ over s in S, and so the coefficients of $A(x)$ are expressions involving only finitely many Laurent series coefficients. This shows that the coefficients of $A(x)$ are in $F^{\sim}$ and proves (a).

To prove (b) we note that the series z_s are all integral over $\mathbf{Z}[u]$, since $f^n(x) - x$ is monic with coefficients in $\mathbf{Z}[u]$. Hence the elementary symmetric functions of the z_s for s in S lie in $F^{\sim}[u]$ and are integral over $\mathbf{Z}[u]$, and are therefore also integral over $\mathbf{o}[u]$. But it is not difficult to check that $\mathbf{o}[u]$ is integrally closed in $F^{\sim}(u)$. (In fact, if $\mathbf{o}$ is any Dedekind ring with quotient field K, then $\mathbf{o}[u]$ is integrally closed in $K(u)$.) Thus the coefficients of A and B lie in $\mathbf{o}$. □

The results we have obtained so far can be looked at in the following way. Let Σ be the splitting field of the polynomial $\Phi_n(x)$ over the field $F(u)$, where F is a prime field. Let p_∞ be the pole divisor of u in $F(u)$. The completion of $F(u)$ at p_∞ is just the field $F((1/u))$, and our results show that the completion of Σ at a

prime divisor $\wp_\infty$ which lies over p_∞ is the Laurent series field $L = F^\sim((1/u))$, *independent of* n. It is also easy to see that $[L{:}F((1/u))] = [F^\sim{:}F]$, where $e = 1$ is the ramification index and $f = [F^\sim{:}F]$ is the inertial degree of $L/F((1/u))$. In particular, there is a natural injection

$$\mathrm{Gal}\,(F^\sim/F) \cong \mathrm{Gal}\,(L/F((1/u))) \to \mathrm{Gal}\,(\Sigma/F(u)).$$

The completion of the field Σ at other prime divisors yields further information about the factorization of $\Phi_n(x)$. Let p_0 be the zero divisor of u in $F(u)$ and let $\wp_0$ be a prime divisor of Σ lying over p_0. The completion $\Sigma_{\wp_0}$ can be determined from the following lemma. For ease of notation let

$$P_n = \{\text{divisors } d \text{ of } k^n - 1 \text{ which don't divide } k^m - 1 \text{ for } m < n\}$$

be the set of primitive divisors of $N = k^n - 1$.

LEMMA 4 *Assume* $f(x,0) = x^k$, *and that char* $F = 0$ *or* p *where* $(p, k^n - 1) = 1$. *For every* d *in* P_n *and every primitive* d*th root of unity* ζ_d *there is a unique series*

$$z = z(\zeta_d) = \zeta_d + \sum_{m=1}^{\infty} a_m u^m$$

in $F(\zeta_d)[[u]]$ *for which* $\Phi_n(z) = 0$, *and we have the factorization*

$$\Phi_n(x) = \prod_{d \in P_n, \zeta_d} (x - z(\zeta_d)) = \prod_{d \in P_n} C_d(x,u), \tag{11}$$

where $C_d(x,u) = \prod_{\zeta_d}(x - z(\zeta_d))$ *has coefficients in* $F[[u]]$. *In case* $F = \mathbf{Q}$, *the polynomial* $C_d(x,u)$ *is irreducible over* $\mathbf{Q}((u))$.

Proof. We find all the solutions of $\Phi_n(z,u) = \Phi_n(z) = 0$ in $F(\zeta_N)((u))$, $(N = k^n - 1)$. Using that $f(x,0) = x^k$ it is easy to see that

$$\Phi_n(x,0) = \prod_{d \in P_n} C_d(x),$$

where $C_d(x)$ is the dth cyclotomic polynomial, so that $\Phi_n(x,0)$ has distinct roots. (There is an extra factor x in $\Phi_n(x,0)$ when $n = 1$. Cf. [13], equation (3.1).) It follows from Hensel's lemma that for each root ζ_d of $C_d(x) = 0$ there is a unique solution

$$z = z(\zeta_d) = \zeta_d + a_1 u + \cdots + a_m u^m + \cdots \tag{12}$$

of $\Phi_n(z,u) = 0$ in the complete field $F(\zeta_d)((u))$. Thus $\Phi_n(x,u)$ splits completely in $F(\zeta_N)((u))$. This proves (11). To show that $C_d(x,u)$ has coefficients in $F((u))$, note that

$$z(\zeta_d) \to z(\zeta_d^i)$$

under the automorphism $\sigma = (\zeta_d \to \zeta_d^i)$ in Gal $(F(\zeta_d)((u))/F((u))) \cong$ Gal $(F(\zeta_d)/F)$. Hence $C_d(x,u)$ has coefficients in the ground field $F((u))$. This also shows $C_d(x,u)$ is irreducible when $F = \mathbf{Q}$, since the roots of unity ζ_d^i are all conjugate over $\mathbf{Q}$. The other assertions are immediate. □

Remarks. (1) The completion $\Sigma_{\wp_0}$ is thus given by $\Sigma_{\wp_0} = F(\zeta_N)((u))$, with residue class field $F(\zeta_N)$, where $N = k^n - 1$. The extension $\Sigma_{\wp_0}/F((u))$ is unramified and

$$\text{Gal}\,(\Sigma_{\wp_0}/F((u))) \cong \text{Gal}\,(F(\zeta_N)/F) \to \text{Gal}(\Sigma/F(u)).$$

(2) For the series $z(\zeta_d)$ in we have

$$f^i(z(\zeta_d)) = \zeta_d^{k^i} + \cdots = z(\zeta_d^{k^i}),$$

so that the action of f on the roots $z(\zeta_d)$ of $\Phi_n(x)$ coincides with the action of the map $(\zeta_d \to \zeta_d^k)$ on $F(\zeta_d)((u))$. When $F = \mathbf{Q}$ it follows that the roots of $C_d(x,u)$ are permuted by the map f and therefore consist of complete orbits.

LEMMA 5 *If $F = \mathbf{Q}$ and $\Phi_n(x) = A(x)B(x)$ over $\bar{\mathbf{Q}}$, the coefficients of A and B lie in $\mathbf{o} \cap \mathbf{Z}[\zeta_N]$, where $N = k^n - 1$. If $F^\sim \cap \mathbf{Q}(\zeta_N) = \mathbf{Q}$, the roots of $A(x)$ and $B(x)$ over $\bar{\mathbf{Q}}(u)$ consist of complete orbits under f.*

Proof. The first assertion follows from Lemma 3(b) and Lemma 4: $A(x)$ and $B(x)$ have coefficients in $\mathbf{o}[u]$ and also in $\mathbf{Q}(\zeta_N)((u))$. If $F^\sim \cap \mathbf{Q}(\zeta_N) = \mathbf{Q}$, then $C_d(x,u)$ is irreducible over $F^\sim((u))$, which implies that the monic polynomial $A(x)$ is a product of certain of the polynomials $C_d(x,u)$. The second assertion now follows from Remark 2 above. □

To complete the next step we need the following lemma.

LEMMA 6 *If $f \in \mathbf{Z}[x,u]$ satisfies (6), (6′) and $\gcd(\text{disc}\, f(x,1), k^n - 1) = 1$, then disc $\Phi_n(x)$, as a polynomial in u, is primitive.*

Proof. Let α_i, for $1 \leqslant i \leqslant r$, denote representatives of the different orbits of roots of $\Phi_n(x)$ under f, and let $\omega(\alpha_i) = \prod_j f'(f^j(\alpha_i))$ denote the multiplier of the ith orbit, corresponding to the periodic sequence $s = \{\zeta_0, \zeta_1, \ldots, \zeta_{n-1}, \ldots\}$, as in Lemma 1. Using the fact that $f'(z,u)$ is homogeneous of degree $k-1$, it is easily checked that

$$\omega(\alpha_i) = f'(\zeta_0,1)f'(\zeta_1,1)\ldots f'(\zeta_{n-1},1)u^{n(k-1)} + \cdots = \xi_i u^{n(k-1)} + \cdots. \quad (13)$$

By the formula

$$\delta_n(x,u) = \prod_i (x - \omega(\alpha_i)) = \prod_i (x - \xi_i u^{n(k-1)} - \cdots), \quad (14)$$

it is clear that the leading coefficient of $\delta_n(1,u)$ is plus or minus a product of terms of the form $f'(\zeta,1)$ and is therefore only divisible by prime factors of disc $f(x,1)$. The same holds for the leading coefficients of the polynomials $\Delta_{n,d}(u)$, by formula (3). On the other hand, the constant term of $\Delta_{n,d}(u)$ is a product of prime divisors of $N = k^n - 1$, by formula (3′), since the substitution $u = 0$ reduces the discriminant of $\Phi_n(x)$ to a product of discriminants and resultants of cyclotomic polynomials $C_d(x)$ over a set of divisors d of N. The assumption gcd (disc $f(x,1), N) = 1$ implies that the $\Delta_{n,d}(u)$ are all primitive in u, so (3′) implies that disc $\Phi_n(x)$ is primitive as well. □

For the rest of this section we assume the condition that gcd (disc $f(x,1), k^n - 1) = 1$. Then $F^{\sim} \cap \mathbf{Q}(\zeta_N) = \mathbf{Q}$ follows automatically, since any primes which ramify in $F^{\sim} \cap \mathbf{Q}(\zeta_N)$ would be common divisors of disc $f(x,1)$ and N. From Lemma 5 the factors $A(x)$ and $B(x)$ in $\Phi_n(x,c) = A(x)B(x)$ each have roots (over $\mathbf{Q}(u)$) consisting of complete orbits under f. By Theorem 5.2 of [13] this factorization corresponds to a factorization of the multiplier polynomial $\delta_n(x,u) = a(x)b(x)$, where

$$a(x) = \prod_{A(\alpha_i)=0} (x - \omega_n(\alpha_i)) \quad \text{and} \quad b(x) = \prod_{B(\alpha_i)=0} (x - \omega_n(\alpha_i)), \tag{15}$$

and the products are taken over representatives α_i from the orbits which make up the roots of A and B respectively. From Lemma 4 we also have

$$A(x) = \prod_{d \in D} C_d(x,u) \quad \text{and} \quad B(x) = \prod_{d \in D'} C_d(x,u), \tag{16}$$

where D and D' are disjoint sets of divisors of $k^n - 1$ and $D \cup D' = P_n$.

LEMMA 7 *Assume $f \in \mathbf{Z}[x,u]$ is monic in x and that $\Phi_n(x) = A(x)B(x)$, where $A(x)$ is irreducible over $\bar{\mathbf{Q}}$. Assume also that the roots of $A(x)$ in an algebraic closure of $\mathbf{Q}(u)$ consist of complete orbits under f. If α_i runs through a set of representatives of these orbits, then for any proper divisor d of n the expression $\prod_i \Phi_d(\alpha_i)^{n/d}$ is a polynomial in $\bar{\mathbf{Q}}[u]$ times a unit η in the integral closure R of $\bar{\mathbf{Q}}[u]$ in $\bar{\mathbf{Q}}(\alpha_1, \ldots, \alpha_i, \ldots, u)$.*

Proof. Since $A(x) = A(x,u)$ is absolutely irreducible, we may work in the algebraic function field $K_1 = \bar{\mathbf{Q}}(\alpha_1, u)$. It is easy to see that this field has the map $\sigma: u \to u, \alpha_1 \to f(\alpha_1)$ as an automorphism of order n with fixed field $K_{1\sigma}$, where $[K_{1\sigma}: \bar{\mathbf{Q}}(u)] = s$, the number of orbits of f which make up the roots of $A(x)$ in an algebraic closure of $\bar{\mathbf{Q}}(u)$. Let P be any prime divisor of K_1 which divides $\Phi_d(\alpha_1)$. Then

$$\alpha_1 \equiv a, u \equiv b (\mathrm{mod}\, P),$$

where $\Phi_d(a,b) = \Phi_n(a,b) = 0$. By Theorem 2.4 of [13] a cannot be a root of any polynomial $\Phi_{d'}(x)$ with $d' \neq d, n$. If G is the decomposition group of P over

$K_{1\sigma}$, then G is generated by $\sigma^{d'}$ for some integer d', and $|G| = n/d' = e$. Since $\sigma^{d'}$ fixes P, we have that $P|(f^{d'}(\alpha_1) - \alpha_1)$ and therefore $P|(f^{d'}(a,b) - a)$, i.e. $f^{d'}(a,b) - a = 0$. This implies that $d|d'$, since a is a primitive d-periodic point of $f(x,b)$. Hence $e|n/d$, and the power of P occurring in $\Phi_d(\alpha_1)^{n/d}$ is a multiple of the ramification index e. On the other hand, the zero-divisor of $\Phi_d(\alpha_1)$ is invariant under σ, since $\Phi_d(f(\alpha_1))/\Phi_d(\alpha_1)$ is a unit in the integral closure of $\bar{\mathbf{Q}}[u]$ in K_1 (see [15], Lemma 2.1 or [14]), so that all the conjugates of P over $K_{1\sigma}$ occur in $\Phi_d(\alpha_1)^{n/d}$ to the same power that P does. It follows that the zero divisor of $\Phi_d(\alpha_1)^{n/d}$ is equal to a divisor of $K_{1\sigma}$, and hence the zero-divisor of $\pi = \prod_i \Phi_d(\alpha_i)^{n/d}$ is equal to a divisor in $\bar{\mathbf{Q}}(u)$, as the maps $\alpha_1 \to \alpha_i$, applied to $K_{1\sigma}$, give rise to all the conjugate extensions of $K_{1\sigma}$ over $\bar{\mathbf{Q}}(u)$ (see [13], Lemma 4.4). Since the individual terms in π are integral over $\bar{\mathbf{Q}}[u]$, there is a polynomial $p(u)$ in $\bar{\mathbf{Q}}[u]$ for which the divisor $(\pi/p(u))$ only involves primes over p_∞ (the pole divisor of u in $\bar{\mathbf{Q}}(u)$). Hence $\eta = \pi/p(u)$ is a unit in R. □

The next lemma contains the crux of the whole argument, and is the only place where the assumption that $\Delta_{n,n}(u)$ has no multiple roots is used.

LEMMA 8 *Assume* $f \in \mathbf{Z}[x,u]$ *satisfies* (6), (6′) *and that* $\Phi_n(x) = A(x)B(x)$ *is a factorization over* $\mathbf{Z}$. *If gcd (disc* $f(x,1), k^n - 1) = 1$ *and the polynomial* $\Delta_{n,n}(u)$ *has no multiple roots, then Res* $(A,B) = \pm 1$.

Proof. Write

$$A(x) = \prod_{i\in I} \lambda_i(x) \quad \text{and} \quad B(x) = \prod_{j\in J} \lambda_j(x),$$

where the $\lambda_i(x)$ are defined by (1) and I and J make up a partition of the integers from 1 to r, and where, without loss of generality, we may assume $A(x)$ to be irreducible over $\bar{\mathbf{Q}}$. We have first that

$$\text{Res}\,(A,B) = \prod_{i\in I, j\in J} \text{Res}\,(\lambda_i(x), \lambda_j(x)) = \eta \prod_{i\in I, j\in J} \lambda_j(\alpha_i)^n, \tag{17}$$

by [15], equation (2.10) (see the computations leading to this equation). Here and in the rest of the proof η represents a unit in the integral closure R of $\mathbf{Q}[u]$ in $\mathbf{Q}(u, \alpha_1, \ldots, \alpha_r)$. In order to relate (17) to $a(1)$ we compute:

$$1 - \omega_n(\alpha_i) = \frac{d}{dx}(x - f^n(x))|_{x=\alpha_i} = -\Phi_n'(\alpha_i) \prod_{d|n, d\neq n} \Phi_d(\alpha_i). \tag{18}$$

Furthermore,

$$\Phi_n'(\alpha_i) = \lambda_i'(\alpha_i) \prod_{j\neq i} \lambda_j(\alpha_i), \tag{19}$$

and

$$\lambda_i'(\alpha_i) = \prod_{k=1}^{n-1}(\alpha_i - f^k(\alpha_i)) = (-1)^{n-1}\prod_{k=1}^{n-1} F_k(\alpha_i),$$

where $F_k(x) = f^k(x) - x$. It can also be shown that

$$\lambda_i'(\alpha_i) = \eta \prod_{d|n,d<n} \Phi_d(\alpha_i)^{(n/d-1)}, \tag{20}$$

by the computations in the proof of [15], Theorem 2.5 (see eqs. (2.5), (2.8), (2.9) of [15]). Putting these formulas together gives

$$a(1) = \prod_{i\in I}(1 - \omega_n(\alpha_i)) = (-1)^{|I|}\prod_{i\in I}\Phi_n'(\alpha_i)\prod_{d|n,d\neq n}\Phi_d(\alpha_i),$$

by (15), hence that

$$\begin{aligned} a(1) &= \eta\prod_{i\in I}\prod_{d|n,d\neq n}\Phi_d(\alpha_i)^{n/d}\prod_{j\neq i}\lambda_j(\alpha_i) \\ &= \eta\prod_{i\in I}\prod_{d|n,d\neq n}\Phi_d(\alpha_i)^{n/d}\cdot\prod_{i,j\in I,j\neq i}\lambda_j(\alpha_i)\cdot\prod_{i\in I,j\in J}\lambda_j(\alpha_i). \end{aligned}$$

Similarly,

$$b(1) = \eta\prod_{j\in J}\prod_{d|n,d\neq n}\Phi_d(\alpha_j)^{n/d}\cdot\prod_{i,j\in J,i\neq j}\lambda_i(\alpha_j)\cdot\prod_{i\in I,j\in J}\lambda_i(\alpha_j).$$

It is easy to see that $\lambda_i(\alpha_j)$ and $\lambda_j(\alpha_i)$ are associates in R (see Lemma 2.3 in [15]), so $a(1)$ and $b(1)$ share the common factor

$$\phi(u) = \prod_{i\in I,j\in J}\lambda_j(\alpha_i). \tag{21}$$

By Lemma 7, the product $\prod_{i\in I}\prod_{d|n,d\neq n}\Phi_d(\alpha_i)^{n/d}$ is a unit times a polynomial in u. Hence the same is true of $\prod_{i,j\in I,j\neq i}\lambda_j(\alpha_i)\cdot\phi(u)$. By (5), we have

$$\Delta_{n,n}(u) = \eta\prod_{i,j\in I,i\neq j}\lambda_i(\alpha_j)\prod_{i,j\in J,i\neq j}\lambda_i(\alpha_j)\cdot\phi(u)^2,$$

so that $\prod_{i,j\in J,i\neq j}\lambda_i(\alpha_j)\cdot\phi(u)$ is also essentially a polynomial in u.

We can now prove Lemma 8. If $\operatorname{Res}(A,B)$ had a complex root u, then by (17) and (21) this would also be a root of $\phi(u)$, and by the above argument, a multiple root of $\Delta_{n,n}(u)$. Hence $\operatorname{Res}(A,B)$ is constant. Moreover, by the formula

$$\operatorname{disc}\Phi_n(x) = \operatorname{disc}A(x)\operatorname{disc}B(x)\operatorname{Res}(A,B)^2$$

and the fact that disc $\Phi_n(x)$ is primitive as a polynomial in u (Lemma 6), the integer $\mathrm{Res}(A, B)$ must be a unit in $\mathbf{Z}$. □

Remark Related to this proof is the following proposition: Assume $\Phi_n(x)$ has coefficients in a unique factorization domain or Dedekind domain R, and that $\Phi_n(x)$ factors as $A(x)B(x)$ over R, where the roots of A and B consist of complete orbits under the polynomial $f \in R[x]$. If $(\Delta_{n,n}, \Delta_{n,d}) = 1$ in R for all proper divisors d of n, then $\mathrm{Res}(A, B) = \eta\rho^n$, where η is a unit in R, $\rho \in R$ and $\rho^2 | \Delta_{n,n}$ in R. The proof, which I omit, uses (17) and an argument similar to the proof of Lemma 7. Thus the expression $\phi(u)$ in (21) is itself a polynomial when $R = \mathbf{Z}[u]$ and $\Delta_{n,n}(u)$ is relatively prime to all the polynomials $\Delta_{n,d}(u)$ (for $d|n$ and $d < n$).

The proof of Theorem B will now follow quickly, using properties of cyclotomic polynomials. The argument is a simplification of the argument given by Bousch [3].

PROOF OF THEOREM B. Assume $\Phi_n(x) = A(x)B(x)$. The hypothesis (disc $f(x, 1), N) = 1$ implies that the condition $F^{\sim} \cap \mathbf{Q}(\zeta_N) = \mathbf{Q}$ of Lemma 5 holds. Hence Lemmas 5–8 are applicable, and the factorizations in (16) and $\mathrm{Res}(A, B) = \pm 1$ imply that $\mathrm{Res}(C_d(x, 0), C_{d'}(x, 0)) = \pm 1$ for any pair (d, d') with d in D and d' in D'. On the other hand, it is well known that $C_d(x)$ and $C_{d'}(x)$ have a resultant which is divisible by p whenever $d|d'$ and d'/d is a power of the prime p. (To see this note that some term $(\zeta_d - \zeta_{d'})$ in the product which defines the resultant equals $\zeta_d(1 - \zeta)$, where $\zeta = \zeta_{p^a}$, and the norm of $(1 - \zeta)$ is a positive power of p.) This shows that if $C_d(x, u)$ divides $A(x)$ and $d|d'$ with d'/d a prime power, then $C_{d'}(x, u)$ also divides A. For any primitive divisor d of N there is certainly a chain of divisors $d_1 = d, d_2, \ldots, d_s = N = k^n - 1$ for which each d_i/d_{i-1} is a prime power, and each d_i is a primitive divisor of N since d is. It follows that $C_N(x, u)$ must divide $A(x)$. But the same argument shows that $C_N(x, u)$ divides $B(x)$, which is impossible by (16). Hence $\Phi_n(x)$ is irreducible over $\bar{\mathbf{Q}}$. □

PROOF OF COROLLARY 1. We prove the corollary for any map $f(x, c)$ satisfying hypothesis (H). Put $c = u^m$. Conditions (i)–(ii) of Theorem B certainly hold for $f(x, u^m)$. Set $\delta(x, u) = \delta_n(x, u^m)$. Formula (13) shows that no multiplier is zero, which implies that $\delta(1, u) = \delta_n(1, u^m)$ has distinct roots. Hence Theorem B implies that $\Phi_n(x, u^m)$ is irreducible over $\bar{\mathbf{Q}}$, which implies that $\Phi_n(x, c)$ is also irreducible. To show that $\delta_n(x, c)$ is irreducible, we first show that it has no multiple factors. By formula (14),

$$\delta(x, u) = \prod_i (x - \omega(\alpha_i)) = \prod_i (x - \xi_i u^{n(k-1)} - \cdots),$$

it is clear that the highest degree monomial in c of $\delta_n(x, c)$ is independent of x, since this monomial is a product of the terms $-\xi_i u^{n(k-1)}$. The same is clearly true of any factor of $\delta_n(x, c)$ over $\bar{\mathbf{Q}}$, and the c-degree of any such factor is positive.

If $\delta_n(x,c)$ had a multiple factor over $\bar{\mathbf{Q}}$, the polynomial $\delta_n(1,c)$ would have a multiple factor as well, contradicting our assumption on $\delta_n(1,c)$. Thus $\delta_n(x,c)$ has no multiple factors over $\mathbf{Q}(c)$, and the irreducibility of $\delta_n(x,c)$ follows from the irreducibility of $\Phi_n(x,c)$ and Theorem 5.5 of [13].

I mention two further applications for quadratic maps. The first concerns the map $f(x,c) = x^2 + c$ and the polynomial $\tau_n(x,c)$ whose roots are the traces of the orbits of essential n-periodic points of f (roots of $\Phi_n(x,c)$), i.e., the expressions $t = \alpha + f(\alpha) + \cdots + f^{n-1}(\alpha)$.

COROLLARY 3 *(to Theorem B) The polynomial $\tau_n(x,c)$ is irreducible over $\bar{\mathbf{Q}}$.*

Proof. Using the fact that $\Phi_n(x,c)$ is irreducible over $\bar{\mathbf{Q}}$, we note first that $\tau_n(x,c)^n$ is the characteristic polynomial of t taken in the extension $\bar{\mathbf{Q}}(\alpha,c)/\bar{\mathbf{Q}}(c)$, where $\Phi_n(\alpha,c) = 0$. (See [13], Theorem 5.3.) Hence $\tau_n(x,c)$ is a power of an irreducible polynomial over $\bar{\mathbf{Q}}$. To show that $\tau_n(x,c)$ does not have multiple roots, consider its roots in the Laurent series field $\bar{\mathbf{Q}}((1/u))$, where $u^2 = -c$. By Lemma 2, these roots have the form

$$\rho = \left(\sum_{i=0}^{n-1} \varepsilon_i\right) u + \sum_{i=0}^{\infty} b_i/u^i,$$

where $\{\varepsilon_i, i \geqslant 0\}$ is a sequence of ± 1's with minimal period n. Now there is only one orbit for which the coefficient of u is n-2, namely, the orbit corresponding to the sign sequence $\{1,1,\ldots,1,-1\}$. Hence the trace of this orbit cannot equal the trace of any other orbit, whence it follows that $\tau_n(x,c)$ has distinct roots and is irreducible over $\bar{\mathbf{Q}}$.

The second application concerns the related map $h(x,a) = x^2 + ax$, which is linearly conjugate to $g(x) = x^2 - \frac{1}{4}a^2 + \frac{1}{2}a = h(x - \frac{1}{2}a, a) + \frac{1}{2}a$. Since $c \to -\frac{1}{4}a^2 + \frac{1}{2}a$ is not linear, it is not immediately clear whether the polynomial $\Phi_{n,h}(x)$ corresponding to $h(x,a)$ is irreducible or not. In fact, $\Phi_{1,h}(x) = x^2 + (a-1)x$ is reducible. However, Theorem B gives

COROLLARY 4 *For $n > 1$, the polynomial $\Phi_{n,h}(x)$ corresponding to $h(x,a) = x^2 + ax$ is irreducible over $\bar{\mathbf{Q}}$.*

Proof. The map $h(x,a)$ satisfies (i) and (ii) of Theorem B, since disc $(h(x,1)) = 1$. Let $\Delta(a)$ be the factor of disc $(\Phi_{n,h}(x))$ referred to in part (iii) of Theorem B. Since the periodic points of $h(x)$ are just the periodic points of $g(x)$, shifted by $-\frac{1}{2}a$, the discriminant of $\Phi_{n,h}(x)$ equals the discriminant of the polynomial $\Phi_{n,g}(x)$ corresponding to $g(x)$, and (5) implies that $\Delta(a) = \Delta_{n,n}(-\frac{1}{4}a^2 + \frac{1}{2}a)$, the $\Delta_{n,n}$-factor for $\Phi_{n,x^2+c}(x,c)$ evaluated at $c = -\frac{1}{4}a^2 + \frac{1}{2}a$. By the discussion following corollary 1 (Section 1), we know $\Delta_{n,n}(c)$ has distinct roots in c. To show that $\Delta_{n,n}(-\frac{1}{4}a^2 + \frac{1}{2}a)$ has distinct roots in a consider its derivative with respect to a:

$$\frac{\mathrm{d}}{\mathrm{d}a}\Delta_{n,n}(-\tfrac{1}{4}a^2 + \tfrac{1}{2}a) = (\Delta_{n,n})'(-\tfrac{1}{4}a^2 + \tfrac{1}{2}a) \cdot (1-a)/2.$$

The only possible multiple root of $\Delta(a)$ is therefore $a = 1$, which corresponds to $c = \frac{1}{4}$. Since $\frac{1}{4}$ is a root of $\Delta_{1,1}(c)$ and no other $\Delta_{n,n}(c)$, this shows that $\Delta(a)$ satisfies the hypothesis of Theorem B, (iii) when $n > 1$. The irreducibility of $\Phi_{n,h}(x)$ follows.

The example $f(x) = x^2 + 7ux + 14u^2$, for which $\Phi_3(x, u)$ is irreducible, but for which $\Delta_{3,3}(u) = 7(u+1)^2$ and disc $f(x, 1) = -7$, shows that neither condition (ii) nor (iii) of Theorem B is a necessary condition for the irreducibility of $\Phi_3(x, u)$. However, this is essentially the only quadratic polynomial $x^2 + aux + bu^2$ with integer coefficients and no multiple factors, for which $\delta_3(1, u)$ has multiple roots. This is because, for the general quadratic,

$$\text{disc}\, \delta_3(1, u) = 2^8 \cdot 3^6 \cdot 7^8 \cdot (9a^4 - 60a^2b + 112b^2)(2a^2 - 7b)(a^2 - 4b)^{12},$$

and this discriminant is equal to 0 (in the case under consideration) only if $b = 2a^2/7$; this implies $7|a$, in which case the substitution $a \to 7a, u \to u/a$ yields the polynomial f above.

3. The genus of the algebraic curves $\Phi_n(x, c) = 0$ and $\delta_n(x, c) = 0$

In this section we left $f(x, c)$ be a polynomial which satisfies hypothesis (H) and we consider the function field

$$K = \bar{\mathbf{Q}}(x, c), \quad \text{where} \quad \Phi_n(x, c) = 0.$$

The assumption that $\delta_n(1, c)$ has distinct roots has important consequences for the arithmetic of K. This field has the automorphism $\sigma = (x \to f(x, c))$ with fixed field K_σ generated by $\omega = \omega(x) = f'(x)f'(f(x)) \dots f'(f^{n-1}(x))$. This follows from $[K{:}K_\sigma] = n = [K{:}\bar{\mathbf{Q}}(\omega, c)]$, where the first equality is a consequence of Galois theory and the second is a consequence of the irreducibility of $\delta_n(x, c)$ over $\bar{\mathbf{Q}}$ and the formula

$$\deg_x \delta_n(x, c) = (\deg_x \Phi_n(x, c))/n.$$

(Note: $\delta_n(\omega, c) = 0$ in K.) Thus $K_\sigma = \bar{\mathbf{Q}}(\omega, c)$. The function field K_σ can also be generated over $\bar{\mathbf{Q}}(c)$ by $t = x + f(x) + \cdots + f^{n-1}(x)$, when the trace polynomial $\tau_n(x, c)$ is irreducible.

Our goal in this section is to compute the genus of the function fields K and K_σ. We may also consider the function fields $K = F(x, c)$ and $K_\sigma = F(\omega, c)$ over any algebraically closed field F (of nonzero characteristic, for example) over which $f(x, 1)$ and $\delta_n(1, c)$ have distinct roots, and over which $\Phi_n(x, c)$ is irreducible. The proof of Corollary 1 to Theorem B shows that $\delta_n(x, c)$ is also irreducible over F. We will see that the same formulas hold for the genus over F that hold over $\bar{\mathbf{Q}}$; this fact will allow us to determine the primes of good reduction for the curve $\Phi_n(x, c) = 0$ (defined over $\mathbf{Q}$), up to an explicit finite set.

We will denote prime divisors in the fields $F(c), K_\sigma$ and K by, $p, \wp$ and P, respectively. We let p_0 and p_∞ denote the zero and pole divisors of c in $F(c)$, while p_b will denote the zero divisor of $(c-b)$, for b constant.

PROPOSITION 9 *Let F be an algebraically closed field over which $\delta_n(1,c)$ has distinct roots, and $\Phi_n(x,c)$ is irreducible.*

(a) The prime divisors P of K which do not divide p_∞ are in 1-1 correspondence with the solutions $(x,c) = (a,b)$ in F of $\Phi_n(x,c) = 0$.

(b) The ring $F[x,c]$ is the integral closure of $F[c]$ in K, with integral basis

$$\{1, x, \ldots, x^{d_n - 1}\}, \quad d_n = \deg_x \Phi_n(x,c).$$

(c) The c-discriminant of K is equal to the discriminant of $\Phi_n(x,c)$ (see Theorem A).

(d) The c-discriminant of K_σ is equal to $\Delta_{n,n}(c)$.

Proof. (a) Certainly every prime divisor of K which does not divide p_∞ defines a unique point $(x,c) = (a,b)$ on the curve defined by $\Phi_n(x,c)$. Conversely, for every solution (a,b) of $\Phi_n(x,c) = 0$ there is at least one prime divisor P of K for which P divides $(x-a, c-b)$. Assume that P and Q are distinct prime divisors, both of which divide $(x-a, c-b)$.

Case 1. Suppose a is a simple root of $\Phi_n(x,b) = 0$. The prime divisors of K lying over p_b correspond to the distinct irreducible factors of $\Phi_n(x,c)$ over the completion $F((c-b))$ of $F(c)$ at p_b (cf. [9], p. 288). By Hensel's lemma there is a factor of $\Phi_n(x,c)$ over $F((c-b))$ which reduces to $(x-a)$ when $c = b$, and this factor is the only one with a as a root (mod p_b). Thus there will be a unique prime divisor P lying over p_b for which $x \equiv a \pmod{P}$.

Case 2. If a is a multiple root of $\Phi_n(x,b) = 0$, then P and Q both divide $1-\omega$, by (18) (with a in place of α_i). Hence $\mathrm{Norm}_{K_\sigma}(P) = \wp_1$ and $\mathrm{Norm}_{K_\sigma}(Q) = \wp_2$ divide $(1-\omega)$. Now the norm to $F(c)$ of $(1-\omega)$ divides $\delta_n(1,c)$, with a square-free zero divisor in $F(c)$, and the norms of $\wp_1$ and $\wp_2$ are both equal to p_b, so $\wp_1$ must equal $\wp_2$. Thus P and Q lie over the same prime divisor of K_σ and are therefore conjugate by some power of σ. If $\sigma^i(P) = Q$, then $Q | (\sigma^i(x) - a)$, and therefore $Q | (x - f^{n-i}(a))$, because $(f^i(x) - a)$ and $(x - f^{n-i}(a))$ are associates in $F[x,c]$ (see [15], Lemma 2.3). This implies $Q | (a - f^{n-i}(a))$ and therefore $a = f^{n-i}(a)$. Suppose that $d < n$ is smallest with the property that $a = f^d(a)$. Then $\Phi_d(a,b) = 0$ and b is a root of $\Delta_{n,d}(c)$ (note $\Delta_{n,d}(c)^d = \mathrm{Res}\,(\Phi_n(x,c), \Phi_d(x,c))$ by a result of [15]). Formulas (18)–(20) show that $P^{n/d}$ divides $1-\omega$, and hence the ramification index of P over $N(P) = \wp_1$ is at least n/d. It follows that there are at most d distinct conjugates of P over K_σ. But there are at least d distinct conjugates because $P | (x-a)$ implies $\sigma^i(P) | (x - f^{d-i}(a))$, and the elements $(x - f^{d-i}(a))$ have no common zero-divisors since the constants $f^{d-i}(a)$ are distinct for $i = 0, \ldots, d-1$. Thus P has exactly d distinct conjugates $\sigma^i(P)$, for $0 \leqslant i \leqslant d-1$, and x is only congruent to a modulo one of them, namely P. This proves part (a).

To prove part (b) it suffices to check the truth of part (c). As in the argument just given, some prime divisor P lying above a divisor p_b for which $\Delta_{n,d}(b) = 0$ and $d < n$ has exactly d distinct conjugates and ramification index n/d over K_σ. Thus the power of $\mathrm{Norm}_{F(c)}P = p_b$ which divides the discriminant of $K/F(c)$ is at least

$$(\mathrm{Norm}_{F(c)}P^{(n/d-1)})^d = p_b^{(n/d-1)d} = p_b^{n-d}.$$

This is exactly the power of $(c - b)$ that divides disc $\Phi_n(x)$. Since disc $K/F(c)$ divides disc $\Phi_n(x)$ (ignoring divisors at ∞) it follows that the exact contribution of p_b to disc $K/F(c)$ is p_b^{n-d}. Moreover, the prime divisors of p_b are unramified in $K_\sigma/F(c)$, since the ramification index of P to $F(c)$ cannot be greater than n/d.

Now consider a prime divisor p_b for which $\Delta_{n,n}(b) = 0$. From (3) (see Sect. 1) and the assumption that $\delta_n(1, c)$ has distinct roots it follows that $\Delta_{n,n}(c)$ and $\Delta_{n,d}(c)$ are relatively prime in c for all proper divisors d of n. Hence a prime P lying above p_b cannot be fixed by any non-trivial power of σ. Thus P is not ramified over K_σ. If $\mathrm{Norm}_{K_\sigma}P = \wp$, and $\wp^e$ exactly divides p_b, then p_b^{e-1} would divide disc $K_\sigma/F(c)$ and $p_b^{(e-1)n}$ would divide disc $K/F(c)$, by the Schachtelungssatz ([9], p. 424 and pp. 448–9). However, Theorem A shows that exactly the nth power of $(c - b)$ divides disc $\Phi_n(x)$, and this implies $e \leqslant 2$. It remains to see that for some prime $\wp$, $\wp^2$ exactly divides p_b. Because $\Delta_{n,n}(b) = 0$ the polynomial $\Phi_n(x)$ has a multiple root, and there are fewer than $d_n = \deg \Phi_n(x)$ essential periodic points of period n. Part (a) shows that some prime divisor P of p_b must be ramified. But we have already shown that P is not ramified in K/K_σ and so $\wp$ must be ramified in $K_\sigma/F(c)$. This proves that

$$p_b = \wp_1^2\wp_2 \cdots \wp_{r-1} \quad \text{in } K_\sigma, \quad \text{if } \Delta_{n,n}(b) = 0,$$

and the exact contribution of p_b to disc $K/F(c)$ is p_b^n.

These considerations show that disc $K/F(c)$ and disc $\Phi_n(x)$ are equal as divisors (except for divisors at ∞), and this implies that the powers of x are an integral basis for the integral closure of $F[c]$ in K.

The argument just given also implies the assertion of (d), since the only possible divisors of the c-discriminant of $K_\sigma/F(c)$ are p_b, where disc $\Phi_n(x, b) = 0$, and we have seen that p_b does not ramify in $K_\sigma/F(c)$ if $\Delta_{n,d}(b) = 0$ for some proper divisor d of n. □

COROLLARY *Under the assumptions of proposition* 9, $\mathrm{disc}_x \delta_n(x, c) = \Delta_{n,n}(c)h(c)^2$, *for some polynomial* $h(c)$.

Remark The dynamical meaning of the last part of this proof is that exactly two orbits of essential n-periodic points coincide at a point b for which $\Delta_{n,n}(b) = 0$, and exactly n/d orbits coincide at a point b for which $\Delta_{n,d}(b) = 0$ and $d < n$.

PROPOSITION 10 *Let F be an algebraically closed field over which $f(x,1)$ has distinct roots, and $\Phi_n(x,c)$ is irreducible. Assume also that the substitution $c = u^m$ renders $f(x,u^m)$ homogeneous in x and u. For the prime p_∞ we have*

$$p_\infty = (P_1 P_2 \dots P_{d/m})^m$$

in K, where the prime divisors P_i are all distinct and $d = d_n = \deg \Phi_n(x)$. All the prime divisors of K lying over p_∞ are rational over the splitting field of $f(x,1)$.

Proof. The prime divisors of K lying over p_∞ are in 1-1 correspondence with the irreducible factors of $\Phi_n(x)$ over $F((1/c))$. I claim these irreducible factors all have degree m. From Lemmas 1 and 2 and the fact that $F((1/u))$ is a Kummer extension of $F((1/c))$, with generating automorphism $\Psi = (u \to \zeta_m u)$ and ζ_m a primitive mth root of 1, it follows that the irreducible factors of $\Phi_n(x)$ over $F((1/c))$ have the form

$$g_s(y) = \prod_{i=0}^{k-1} (y - \Psi^i(z_s)),$$

since each z_s is a primitive element of $F((1/u))$ over $F((1/c))$. This proves the claim. The last assertion follows from the fact that all series z_s are defined over the splitting field of $f(x,1)$. (Note that char $F \nmid m$ by the assumptions on f.) □

We can now prove

THEOREM 11 (Cf. [3] for $f(x) = x^2 + c$ and $k = m = 2$.) *Under the joint hypotheses of Propositions 9 and 10, the discriminant of the extension $K/F(c)$ is*

$$D_n = p_\infty^{d_n - d_n/m} \prod_{d|n, d<n, \Delta_{n,d}(b)=0} p_b^{n-d} \prod_{\Delta_{n,n}(b)=0} p_b^n,$$

where $d_n = \deg_x \Phi_n(x)$. The genus of $K/F(c)$ is

$$g_n = \tfrac{1}{2}(nk - n - m - 1)\nu(n) - \frac{(k-1)}{2} \sum_{d|n, d<n} d\nu(d)\phi(n/d) + 1,$$

where $\nu(n) = (1/m)\sum_{e|n} \mu(n/e)k^e$ and ϕ is Euler's phi-function.

Proof. The formula for the discriminant D_n follows immediately from the proofs of Propositions 9 and 10. To prove the formula for g_n we note from (14), the definition of $\Delta_{n,d}$, and (3) that

$$\deg_c \delta_n(x,c) = (k-1)\nu(n),$$

$$\deg_c \Delta_{n,d}(c) = (k-1)\nu(d)\phi(n/d), \quad \text{for } d|n, d < n,$$

$$\deg_c \Delta_{n,n}(c) = (k-1)\nu(n) - (k-1)\sum_{d|n, d<n} \nu(d)\phi(n/d). \tag{22}$$

Now the Hurwitz genus formula ([9], p. 457 or [19], p. 88) and $d_n = m\nu(n)$ imply that

$$\begin{aligned} g_n &= \tfrac{1}{2}\deg D_n - [K:\bar{\mathbf{Q}}(c)] + 1 \\ &= \frac{1}{2}\left(d_n - \frac{d_n}{m}\right) + \frac{1}{2}\sum_{d|n, d<n} (n-d)\deg \Delta_{n,d}(c) \\ &\quad + \tfrac{1}{2} n \deg \Delta_{n,n}(c) - d_n + 1 \\ &= \tfrac{1}{2}(-m-1)\nu(n) + \frac{1}{2}\sum_{d|n} n \deg \Delta_{n,d}(c) - \frac{1}{2}\sum_{d|n, d<n} d \cdot \deg \Delta_{n,d}(c) + 1 \\ &= \tfrac{1}{2}(nk - n - m - 1)\nu(n) - \frac{(k-1)}{2}\sum_{d|n, d<n} d\nu(d)\phi(n/d) + 1, \end{aligned}$$

as claimed. □

COROLLARY *Let $f(x,c)$ be a polynomial satisfying hypothesis (H) (see Sect. 1). If p is a prime which does not divide disc $(f(x,1))$ or disc $(\delta_n(1,c))$, and if $\Phi_n(x,c)$ is irreducible over $\bar{\mathbf{F}}_p$, then p is a prime of good reduction for the curve $\Phi_n(x,c) = 0$ (over $\mathbf{Q}$).*

In Theorem 13 we deduce a formula for the genus of K_σ. To state the formula we introduce the following notation. Let X_n be the set of all possible 'necklaces' with n beads, colored using the roots of $f(x,1)$, where a necklace is represented by an n-tuple $\{\zeta_1, \zeta_2, \ldots, \zeta_n\}$ of roots of $f(x,1)$ and two n-tuples $\{\zeta_i\}$ and $\{\zeta_i'\}$ represent the same necklace if and only if $\zeta_i = \zeta_{i+j'}$ for all i (mod n) and some fixed j. A *primitive* necklace is a necklace $\{\zeta_1, \zeta_2, \ldots, \zeta_n\}$ whose coloring is not periodic with period $< n$. Let $G = \langle \Psi \rangle$ be the group of mappings on X_n generated by the permutation $\Psi: X_n \to X_n$, where

$$\Psi(\{\zeta_1, \zeta_2, \ldots, \zeta_n\}) = \{\xi\zeta_1, \xi\zeta_2, \ldots, \xi\zeta_n\}, \quad (f(\zeta_i, 1) = 0 \text{ for all } i),$$

and ξ is a primitive mth root of unity. If ε_d is the number of distinct orbits of X_d under G, then $e_n = \Sigma_{d|n}\mu(n/d)\varepsilon_d$ is the number of primitive G-orbits of X_n, i.e., the number of orbits containing primitive necklaces. We have the following formula for e_n, for which I am grateful to Bjorn Poonen (private communication).

LEMMA 12 *If $n > 1$, or if $n = 1$ and 0 is not a root of $f(x, 1) = 0$, then*

$$e_n = \frac{1}{mn} \sum_{d|(m,n)} \phi(d)^2 \sum_{r|n;\, d|r;\, (n/r,d)=1} \mu(n/r) k^{r/d}.$$

Proof. Let X be the set of n-tuples $(x_1, x_2, \ldots, x_n)$ of roots of $f(x, 1)$ which are primitive, when considered as necklaces. Let $G' = \mathbf{Z}/n\mathbf{Z} \times G$. If $\mathbf{Z}/n\mathbf{Z}$ acts on X by rotation, then e_n is number of G'-orbits of X, so that

$$e_n = \frac{1}{mn} \sum_{g \text{ in } G'} \#(\text{fixed points of } g \text{ in } X),$$

by Burnside's lemma (see [1], Ch. 18). Let $g = (a, \xi^j)$, and let d be the order of a in $\mathbf{Z}/n\mathbf{Z}$. If g has fixed point y in X, then $\xi^j \neq 1$ (otherwise y would not be primitive) and $a \neq 0$ (using the assumption that $n > 1$ or 0 is not a root of $f(x, 1) = 0$), unless g is the identity. The same argument applies to powers of g; it follows that the order of $g = d =$ order of ξ^j, and $d|(m, n)$. For each divisor d of (m, n) there are $\phi(d)^2$ elements of G' both of whose coordinates have order d.

Now consider a fixed one of these $\phi(d)^2$ elements, g. Without loss of generality, we may assume that $g = (n/d, \xi^j)$. Let Y_r be the number of n-tuples of roots of $f(x, 1)$ which are fixed by g and which have a period dividing r, when considered as necklaces. Then $|Y_n| = k^{n/d}$, since any fixed point $y = (x_1, x_2, \ldots, x_n)$ of g satisfies $\xi^j x_{i+n/d} = x_i$, and is therefore determined by its first n/d coordinates. Suppose that y has period r (a divisor of n). Then $g^r y = y$ implies that $\xi^{jr} x_{i+rn/d} = x_i$ and $\xi^{jr} = 1$, so $d|r$. We claim that $(n/d, r) = r/d$ as well. Putting $(n/d, r) = e$ and using $g^{r/e} y = y$ implies $\xi^{jr/e} = 1$, so that $d|(r/e)$ and $e|(r/d)$, from which the claim follows. If we now set $ln/d = br + r/d$ for suitable l and b, then l is relatively prime to d, and $g^l y = y$ if and only if $\xi^{jl} x_{i+ln/d} = \xi^{jl} x_{i+r/d} = x_i$, so that y is completely determined by its first r/d coordinates. Thus $|Y_r| = k^{r/d}$, when $d|r$ and $(n/d, r) = r/d$, and $|Y_r| = 0$ otherwise. Applying Möbius inversion to the equation

$$\sum_{m|r} \#(\text{fixed points of } g \text{ in } Y_n \text{ with least period } m) = \chi(r) k^{r/d},$$

where $\chi(r)$ is the characteristic function of the set of integers r with $r|n$, $d|r$ and $(n/d, r) = r/d$, we find that

$$\#(\text{fixed points of } g \text{ in } X) = \sum_{r|n} \mu(n/r) \chi(r) k^{r/d}.$$

This proves the lemma, since $(n/d, r) = r/d$ is equivalent to $(n/r, d) = 1$.

THEOREM 13 *Assume that $f(x, c)$ satisfies the hypotheses of Propositions 9 and 10.*

(a) *The discriminant of the extension* $K_\sigma/F(c)$ *is*

$$\operatorname{Disc} K_\sigma/F(c) = p_\infty^{m\nu(n)/n-e_n} \prod_{\Delta_{n,n}(b)=0} p_b.$$

(b) *The genus of* K_σ *is*

$$\gamma_n = \frac{1}{2}\left(k-1-\frac{m}{n}\right)\nu(n) - \frac{e_n}{2} - \frac{k-1}{2}\sum_{d|n,d<n}\nu(d)\phi(n/d) + 1.$$

(c) *If* $(n,m)=1$, *the genus of* K_σ *is given by*

$$\gamma_n = \tfrac{1}{2}(nk-n-m-1)\frac{\nu(n)}{n} - \frac{k-1}{2}\sum_{d|n,d<n}\nu(d)\phi(n/d) + 1.$$

(d) *As* $n\to\infty, \gamma_n > \left(\frac{1}{2}-\frac{1}{2k}-\frac{1}{n}\right)k^n + O(nk^{n/2})$.

Remark. The result of (b), together with Lemma 12, shows that γ_n depends only on n, k and m and not on the particular polynomial f.

Proof. (a) From the proof of Proposition 9 it is clear that the contribution to disc $K_\sigma/F(c)$ by primes other than p_∞ is exactly Π_b, p_b, the product taken over the values of b for which $\Delta_{n,n}(b)=0$. Thus we need only determine the ramified prime divisors of p_∞. As in the proof of Proposition 10, the prime divisors of p_∞ are in 1-1 correspondence with the irreducible factors of $\delta_n(y,c)$ over $F((1/c))$. Over the field $F((1/u))$ we have

$$\delta_n(y,c) = \prod_{i=1}^{r}(y-\omega_i),$$

where ω_i is the multiplier of the ith orbit. We need to determine the degree of ω_i over $F((1/c))$.

To do this we note that distinct orbits have distinct multipliers, so that ω_i is fixed by a power of the automorphism $\Psi = (u\to\xi u)$ if and only if the corresponding orbit is. Let the orbit whose multiplier is $\omega=\omega_i$ correspond to the periodic sequences $s=\{\zeta_1,\zeta_2,\dots,\zeta_n\}$ of Lemma 2 (where we represent s by its first n terms). Then $\Psi^j(\omega)$ is the multiplier of the orbit corresponding to the sequence $\Psi^j(s)=\{\xi^j\zeta_1,\xi^j\zeta_2,\dots,\xi^j\xi_n\}$. The sequences s and $\Psi^j(s)$ give the same orbit if and only if the finite sequence $\{\xi^j\zeta_1,\xi^j\zeta_2,\dots,\xi^j\zeta_n\}$ is a cyclic permutation of the sequence $\{\zeta_1,\zeta_2,\dots,\zeta_n\}$. Hence, each of the f-orbits of roots of $\Phi_n(x,c)$ determines a well-defined primitive necklace in X_n, i.e., a necklace in which the coloring is not periodic with period less than n, and the number of distinct conjugates of ω_i under $\langle\Psi\rangle$ equals the number of necklaces in the orbit of $\{\zeta_1,\zeta_2,\dots,\zeta_n\}$ under G. It follows that the degree of ω_i over $F((1/c))$ equals $|Gs|$, and the contribution of p_∞ to the discriminant is $\sum_{\text{prim. }G\text{-orbits}}(|Gs|-1) = \#(f\text{-orbits of roots of }\Phi_n(x,c)) - \#(\text{primitive } G\text{-orbits}) = m\nu(n)/n - e_n$, where e_n is given by the lemma. (Note that 0 is not a root of $f(x,1)$ when $n=1$, by the hypothesis that $\Phi_1(x)=f(x)-x$ is irreducible.)

This proves part (a). Now (b) follows as in the proof of Theorem 11. Part (c) follows from Lemma 12 and (b), since $e_n = \nu(n)/n$ when $(n, m) = 1$.

(d) Ignoring the contribution of p_∞ (which is actually absent when $m = 1$) to the genus of $K_\sigma/F(c)$, setting $\nu_1(n) = m\nu(n)/k = \sum_{d|n} \mu(n/d)k^{d-1}$, and using $1 \leqslant m \leqslant k$ and $k\nu_1(n) = [K{:}F(c)]$ gives

$$\begin{aligned}\gamma_n &\geqslant \tfrac{1}{2}\deg \Delta_{n,n}(c) - [K_\sigma{:}F(c)] + 1 \\ &\geqslant \tfrac{1}{2}\nu_1(n)(k-1) - \frac{k\nu_1(n)}{n} - \frac{(k-1)}{2}\sum_{d|n, d<n} k\nu_1(d)\phi(n/d) + 1.\end{aligned}$$

Now we use that $\nu_1(d) \leqslant k^{d-1}$ and

$$\nu_1(n) \geqslant k^{n-1} - k^{n/2-1} - k^{n/2-2} - \cdots - 1 = \frac{k^n - k^{n-1} - k^{n/2} + 1}{k-1},$$

and find that

$$\gamma_n \geqslant \tfrac{1}{2}(k^n - k^{n-1} - k^{n/2} + 1) - \frac{k^n}{n} - \frac{(k-1)}{2}k^{n/2}\sum_{d|n, d<n} \phi(n/d) + 1$$

$$\begin{aligned}&> \left(\frac{1}{2} - \frac{1}{2k} - \frac{1}{n}\right)k^n - \frac{k^{n/2}}{2}(1 + nk - n) + \frac{3}{2}, \\ &= \left(\frac{1}{2} - \frac{1}{2k} - \frac{1}{n}\right)k^n + O(nk^{n/2}),\end{aligned} \tag{23}$$

as $n \to \infty$, for $k \geqslant 2$. This completes the proof. □

COROLLARY *If $k \geqslant 3$ is odd and $f(x) = x^k + c$, then the genus of the function field K_σ defined by $\delta_2(x, c) = 0$ is $((k-3)/2))^2$.*

Proof. Take $n = 2$ and $m = k$ in part (c) of the theorem.

4. Applications to automorphism polynomials

THEOREM 14 *Let $f(x, c)$ be a polynomial in $\mathbf{Z}[x, c]$ satisfying hypothesis* (H), *for some n. If $n \geqslant C(k)$ (a constant depending only on $k = \deg_x f$) there are only finitely many cyclic extensions $N = L(\theta)$ of a given number field L which have degree n over L and a generating automorphism of the form $\theta \to f(\theta, a)$, for some a in L.*

Proof. Every such extension N gives a point (θ, a) on the curve $\Phi_n(x, c) = 0$, because the automorphism $\psi = \theta \to f(\theta, a)$ of N/L has order n and so θ is a periodic point of $f(x, a)$ with primitive period n. Moreover, the multiplier $\omega(\theta)$ of

the orbit containing θ is in L, since it is fixed by ψ. Hence N gives the L-rational point on $(\omega(\theta), a)$ on $\delta_n(x, c) = 0$. For $n \geqslant C(k)$ the genus of K_σ is at least 2, by Theorem 13(d), and Faltings' theorem shows that there are only finitely many solutions $(\omega(\theta), a)$ in L of $\delta_n(x, c) = 0$. Each such point gives at most finitely prime divisors P of the function field K lying over p_a, and therefore only finitely many θ's with $x \equiv \theta \pmod{P}$. This proves the theorem. □

A suitable value for $C(k)$ can be worked out using (23). Any $C(k)$ for which $n \geqslant C(k)$ implies

$$k^{n/2} \geqslant \frac{nk(nk - n + 1)}{(nk - n - 2k)}$$

gives $\gamma_n \geqslant 2$, by (23).

COROLLARY *If $n \geqslant 5$, then there are only finitely many cyclic extensions N/L of degree n of a given number field L for which $\theta \to \theta^2 + a$, for some a in L, is a generator of Gal (N/L).*

Proof. It is easy to check that we can take $C(2) = 11$, since $(n - 4)2^{n/2-1} \geqslant (n^2 + n)$ for $n \geqslant 11$. For $5 \leqslant n \leqslant 10$ we compute γ_n by means of Theorem 13(b) and (c): this gives

$$\gamma_5 = 2, \qquad \gamma_6 = 4, \qquad \gamma_7 = 16,$$

$$\gamma_8 = 32, \qquad \gamma_9 = 79, \qquad \gamma_{10} = 162.$$

Thus $\gamma_n \geqslant 2$ for $n \geqslant 5$, which implies that the conclusion of Theorem 14 holds for all $n \geqslant 5$. □

For $L = \mathbf{Q}$ and $n = 5$ the possible cyclic extensions can be given explicitly. As Flynn, Poonen and Schaefer have shown [8], the finite $\mathbf{Q}$-rational points on $\tau_5(x, c) = 0$ are $(-1, -\frac{4}{3}), (-1, -2), (-\frac{7}{3}, -\frac{16}{9}), (\frac{10}{3}, -\frac{64}{9})$. The c-values $-2, -\frac{16}{9}$ and $-\frac{64}{9}$ correspond to cyclic quintic extensions of $\mathbf{Q}$ of conductors 11, 41 and $5^2 \cdot 11$, respectively (B. Poonen, private communication).

As Bjorn Poonen has pointed out to me, there are infinitely many values of n for which $\tau_n(x, c)$ has a finite rational point. Take $n = \phi(3^r) = 2 \cdot 3^{r-1}$ and note that 2 is a primitive root mod 3^r. If ζ is a primitive 3^rth root of unity, then the automorphism $\zeta \to \zeta^2$ generates the Galois group of $\mathbf{Q}(\zeta)/\mathbf{Q}$. Thus the map $f(x) = x^2$ has an n-cycle in $\mathbf{Q}(\zeta)$ whose trace is rational. Actually, the trace is 0, since the coefficient of the $x^{\phi(m)-1}$ term in the cyclotomic polynomial $C_m(x)$ is $-\mu(m)$. Thus (0,0) is a point on $\tau_n(x, c)$ for infinitely many n.

5. Reduction mod p.

When $\Phi_n(x, c)$ is irreducible, there are only a finite number of primes at which it has bad reduction (see [6], p. 187). The following theorem gives an explicit set of primes outside of which the curve $\Phi_n(x, c) = 0$ has good reduction.

THEOREM 15 *Let f satisfy hypothesis* (H). *If $f(x,1)$ and $\delta_n(1,c)$ have distinct roots over $\mathbf{F}_p$, then $\Phi_n(x,c)$ is irreducible over $\bar{\mathbf{F}}_p$. Thus, if the prime p does not divide disc$(f(x,1))$ or disc$(\delta_n(1,c))$, then the curve $\Phi_n(x,c) = 0$, defined over $\mathbf{Q}$, has good reduction at p.*

The proof requires a lemma. We need the definition of the graph G_f for a polynomial $f(x)$ over a field F: this is the directed graph whose vertices are monic irreducible polynomials over F, in which $g \to h$ if and only if $g(x)|h(f(x))$ (see [2]). The map $g \to h$ is called the induced map of f. In this section we shall use m to denote cycle lengths in G_f; this should cause no confusion with the use of the letter m in hypothesis (H), since the latter will not occur explicitly.

LEMMA 16 Assume that $f(x)$ is a monic polynomial with coefficients in a domain R, and that the irreducible polynomials $g_1, \ldots, g_m$ form a cycle in the graph G_f.

(a) The discriminants disc g_i are all associates in R, and their quotients are squares of units in R.

(b) If $\mathrm{Res}(g_i, g_j)$ is nonzero, then $\mathrm{Res}(g_i, g_j)$ and $\mathrm{Res}(g_{i+r}, g_{j+r})$ are associates in R, for any r.

Proof of (a). Suppose that $g_i \to g_{i+1}$ in the graph G_f. Then $g_i(x)|g_{i+1}(f(x))$; if a is a root of $g_i(x)$, then $f(a)$ is a root of $g_{i+1}(x)$. Thus $R[f(a)]$ is a subring of $R[a]$, which implies that

$$\mathrm{disc}\,\{1, f(a), \ldots, f(a)^{d-1}\} = (\det T)^2\,\mathrm{disc}\,\{1, a, \ldots, a^{d-1}\},$$

where $d = \deg g_i = \deg g_{i+1}$ and T is the transition matrix from the basis $\{1, a, \ldots, a^{d-1}\}$ to the basis $\{1, f(a), \ldots, f(a)^{d-1}\}$. Thus disc g_i divides disc g_{i+1}, for each $i = 1, \ldots, m$; it follows that each of the discriminants disc g_i divides each of the other discriminants, and that the determinants $\det T$ are units in R, proving part (a).

Proof of (b). The map $a \to f(a)$ gives a 1-1 mapping from the roots of g_i to the roots of g_{i+1}, since $f(a) = f(b)$ implies $a = f^n(a) = f^n(b) = b$, for some multiple n of m (see [2], Lemma 3.5). Hence we can write

$$\mathrm{Res}\,(g_{i+r}, g_{j+r}) = \prod_{a,b}(f^r(a) - f^r(b)),$$

where a and b run over the roots of g_i and g_j. It follows from Lemma 2.3 of [15] that $f^r(a) - f^r(b)$ and $a - b$ are associates, and hence that $\mathrm{Res}(g_{i+r}, g_{j+r})$ is an associate of

$$\prod_{a,b}(a - b) = \mathrm{Res}(g_i, g_j). \qquad \square$$

PROOF OF THEOREM 15 Assume that $\Phi_n(x,c)$ is reducible over $\bar{\mathbf{F}}_p$. By Lemma 3 we know that the factors of $\Phi_n(x,c)$ over F are defined over the splitting field $F^{\sim}$ of $f(x,1)$ over $F = \mathbf{F}_p$. Let $A_1(x,c)$ be a monic irreducible factor

of $\Phi_n(x,c)$, and suppose that A_1 belongs to the cycle $A_1, A_2, \ldots, A_m$ of irreducible factors of $\Phi_n(x,c)$ under the induced map of $f(x,c)$. There are two cases in the following argument, according as $\Phi_n(x,c) = A_1(x)\ldots A_m(x)$ or $\Phi_n(x,c) = A_1(x)\ldots A_m(x)B(x)$ for some factor B.

Case 1. $\Phi_n(x,c) = A_1(x)\ldots A_m(x)$. The integer m is a divisor of n and the $A_i(x)$ are irreducible polynomials in $F^{\sim}[x,c]$ which make up a cycle of the graph G_f. Computing the discriminant of $\Phi_n(x,c)$ using this factorization implies by Lemma 16 that

$$\operatorname{disc}\Phi_n(x,c) = \eta(\operatorname{disc}A_1(x))^m \prod_{i=1,m-1} \operatorname{Res}(A_i, A_m)^m,$$

where η is a unit in $F^{\sim}[c]$, i.e. a constant in $F^{\sim}$. Therefore disc $\Phi_n(x,c)$ is essentially an mth power, which implies by formula (3′) and the fact $m|n$ that

$$\prod_{d|n,d\neq n} \Delta_{n,d}(c)^{n-d} = \pm\eta(A(c))^m \tag{24}$$

is an mth power. However, m is relatively prime to $n-1$, which shows that $\Delta_{n,1}(c)$ must either be an mth power itself, or it must have factors in common with $\prod_{d\neq 1,n}\Delta_{n,d}(c)$. Neither case can occur if $m > 1$, since $\operatorname{disc}_c(\delta_n(1,c)) \neq 0$ in F. Thus m must be equal to 1, and $\Phi_n(x,c)$ is irreducible over F.

Case 2. $\Phi_n(x,c) = A_1(x)\ldots A_m(x)B(x)$ for some factor B. In this case we set $A(x,c) = A_1(x)\ldots A_m(x)$, so that $\Phi_n(x,c) = A(x)B(x)$, where the roots of A over $F^{\sim}(c)$ consist of complete orbits. Under the assumption that $\operatorname{disc}_c(\delta_n(1,c)) \neq 0$ in F, the proof of Lemma 8 shows that $\operatorname{Res}(A,B)$ must be a nonzero constant in $F^{\sim}$, since otherwise $\delta_n(1,c) = a(1)\,b(1)$ would have a multiple zero at any root c_0 of $\operatorname{Res}(A,B) = 0$. But the conditions that $\Phi_n(x,c) = A(x)B(x)$ and $\operatorname{Res}(A,B)$ is a nonzero constant in $F^{\sim}$ are exactly the hypotheses of a two-variable version of Hensel's Lemma in a finite extension K_p of $\mathbf{Q}_p$ with residue class field $F^{\sim}$ (cf. [9], p. 161). Hensel's Lemma implies that $\Phi_n(x,c) = \tilde{A}(x)\tilde{B}(x)$ over K_p, where the degrees of the factors in x are the same as $\deg_x A$ and $\deg_x B$. On the other hand, K_p contains the splitting field L of $f(x,1)$ over $\mathbf{Q}$ as a subfield (again by Hensel's Lemma), and Lemma 3 shows that $\tilde{A}(x)$ and $\tilde{B}(x)$ have coefficients in L, implying that $\Phi_n(x,c)$ is reducible over L. But this contradicts the fact that $\Phi_n(x,c)$ is irreducible over $\bar{\mathbf{Q}}$, by Theorem B! Therefore, this case is impossible, and $\Phi_n(x,c)$ is irreducible over F.

The final assertion now follows from the corollary to theorem 11. □

It is possible to prove a result on the irreducibility of $\Phi_n(x,c)$ over $\bar{\mathbf{F}}_p$ with somewhat weaker hypotheses than those in Theorem 15.

PROPOSITION 17 *Let f satisfy the hypotheses* (i) *and* (ii) *of Theorem B (or (iia)–(iic)). Assume that p is a prime which does not divide* $\operatorname{disc}(f(x,1))$ *and which satisfies:*

(a) *p does not divide* $\operatorname{disc}(\Delta_{n,1}(c))$, *so in particular* $(p, n) = 1$;
(b) *there is some irreducible factor of* $\Delta_{n,1}(c)$ *(mod p) which is not a factor of any* $\Delta_{n,d}(c)$ *with* $d \neq 1$;
(c) *p does not divide* $\operatorname{disc}(\Delta_{n,n}(c))$.

Then $\Phi_n(x, c)$ is irreducible over $\bar{\mathbf{F}}_p$.

Remark. The definition of $\Delta_{n,1}(c)$ shows that $\Delta_{n,1}(c)$ has multiple roots (mod p) whenever $p|n$, since the same is true of the cyclotomic polynomial $C_n(x)$.

Proof. We begin as in the proof of Theorem 15, taking $A(x, c)$ to be a monic irreducible factor of $\Phi_n(x, c)$ over $F^{\sim}$ and $\{A_1, A_2, \ldots, A_m\}$ the orbit of irreducible factors of $\Phi_n(x, c)$ containing A_1. Again there are two cases.

Case 1. $\Phi_n(x, c) = A_1(x) \ldots A_m(x)$. The proof of Case 1 in Theorem 15 implies that m must be 1, since conditions (a) and (b) show that some factor of $\Delta_{n,1}(c)$ (mod p) cannot occur to the mth power in disc $\Phi_n(x, c)$.

Case 2. $\Phi_n(x, c) = A_1(x) \ldots A_m(x) B(x)$ for some factor $B(x)$. I claim that conditions (a) and (b) imply that $m = 1$, for some orbit of $\Phi_n(x, c)$. Setting $A(x) = A_1(x) \ldots A_m(x) = \lambda_1(x) \ldots \lambda_s(x)$, and letting $\alpha_1, \alpha_2, \ldots, \alpha_s$ be representatives of the s orbits of roots of A under f, then as in [15], Theorem 2.5 we find that

$$\operatorname{disc} A(x) = \eta \prod_{d|n, d<n} \prod_{i=1}^{s} \Phi_d(\alpha_i)^{n(n/d-1)} \cdot \prod_{i \neq j} \lambda_j(\alpha_i)^n,$$

where η is a unit in $R = F^{\sim}[c, \alpha_1, \alpha_2, \ldots, \alpha_s]$. Replacing the product over i of $\Phi_d(\alpha_i)^n$ by $\operatorname{Res}(\Phi_d(x), A(x))$ times a unit of R ($\Phi_d(\alpha_i)$ and $\Phi_d(f^j(\alpha_i))$ are associates in R) gives the formula

$$\operatorname{disc} A(x) = \eta \prod_{d|n, d<n} \operatorname{Res}(\Phi_d(x), A(x))^{n/d-1} \cdot \prod_{i \neq j} \lambda_j(\alpha_i)^n, \tag{25}$$

where the resultant in the first product is a factor of $\Delta_{n,d}(c)^d$ (see (4)) and the final product is a factor of $\Delta_{n,n}(c)^n$ (see (5)). On the other hand, the same arguments as in Theorem 15, case 1, show that

$$\operatorname{disc} A(x) = \eta'(\operatorname{disc} A_1(x))^m \prod_{i=1, m-1} \operatorname{Res}(A_i, A_m)^m, \tag{26}$$

for some constant η' in $F^{\sim}$. The formulas (25) and (26) hold for any orbit of irreducible factors of $\Phi_n(x)$. We now assume $A(x)$ corresponds to an orbit for which $(c - b)$ divides $\operatorname{Res}(\Phi_1(x), A(x))$ (mod p), where $(c - b)$ is a factor of $\Delta_{n,1}(c)$, but not a factor of any $\Delta_{n,d}(c)$ with $d \neq 1$. Such an orbit exists because the product of all the polynomials $\operatorname{Res}(\Phi_1(x), A(x))$ is $\operatorname{Res}(\Phi_1(x), \Phi_n(x)) = \Delta_{n,1}(c)$ (see [15], Theorem 2.2). By (26), $(c - b)$ occurs to a power in disc $A(x)$ which is

divisible by m; but (25) shows that $(c-b)$ occurs to exactly the power $(n-1)$ in disc $A(x)$ (using (a)). Since $(n-1,m)=1$ this forces $m=1$, so that $A(x)$ is an absolutely irreducible factor of $\Phi_n(x)$.

Because $A(x)$ is absolutely irreducible and $(p,n)=1$, the arguments of Lemma 7 hold over $\bar{\mathbf{F}}_p$ (the crucial point being that there can be at most one divisor d of n for which $\Phi_d(a,b)=0$, by Theorem 2.4 of [13]). Thus we may apply the full argument of Lemma 8, which, together with assumption (c), implies that $\mathrm{Res}(A(x),B(x))$ is a non-zero constant in $F^{\sim}$. The rest of the argument is the same as in Case 2 of Theorem 15, and this completes the proof.

The conditions (a)–(c) in the proposition are somewhat better suited for practical calculations in a particular case than is the stronger condition that p not divide $\mathrm{disc}(\delta_n(1,c))$. Even more work can be saved if it is known that $\delta_n(x,c)$ is irreducible mod p. In this case the following proposition holds.

PROPOSITION 18 *If p is a prime for which $\delta_n(x,c)$ (or $\tau_n(x,c)$) is absolutely irreducible mod p, p does not divide* disc $(\Delta_{n,1}(c))$, *and some irreducible factor of $\Delta_{n,1}(c)$ (mod p) does not divide $\prod_{d\neq 1,n}\Delta_{n,d}(c)$, then $\Phi_n(x,c)$ is absolutely irreducible mod p.*

Proof. Since $\delta_n(x,c)$ is absolutely irreducible mod p, $\Phi_n(x,c)$ can only be the product of the irreducible factors $A_1,\dots,A_m$ in one orbit under f, by Theorem 5.5 of [13]. The argument in Case 1 of Theorem 15 now implies the assertion.

As an example, take $f(x)=x^2+c$ and $n=6$. Then, according to Maple, we have

$$\mathrm{disc}\,\Delta_{6,1}(c) = -2^4\cdot 3,$$

$$\mathrm{Resultant}\,(\Delta_{6,1}(c),\Delta_{6,2}(c)\Delta_{6,3}(c)\Delta_{6,6}(c)) = 2^{126}\cdot 3^{11}\cdot 7^3\cdot 13^4\cdot 211^2\cdot 68700493,$$

$$\mathrm{disc}\,\Delta_{6,6}(c) = 2^{956}\cdot 3^{91}\cdot 5^{25}\cdot 7^{66}\cdot 13^8\cdot 29^3\cdot 61^2\cdot 8029187\cdot \cdot 55218797^3\cdot 47548578843011867^2.$$

(See [15] for the polynomials $\Delta_{6,d}(c)$.) Proposition 17 is applicable for any prime not listed and for the primes 211 and 68700493, since for these two primes $\Delta_{6,1}(c)$ has a linear factor which does not divide the other delta factors ($c+207$ for $p=211$ and $c+15918356$ for $p=68700493$). Proposition 18 applies to all primes other than 2 and 3: this is because

$$\mathrm{Resultant}\,(\Delta_{6,1}(c),\Delta_{6,2}(c)\Delta_{6,3}(c)) = 2^{30}\cdot 3^5\cdot 7\cdot 13;$$

$c+6$ is a factor of $\Delta_{6,1}(c)$(mod 7) which does not divide $\Delta_{6,2}(c)\Delta_{6,3}(c)$;

$c+7$ is a factor of $\Delta_{6,1}(c)$(mod 13) which does not divide $\Delta_{6,2}(c)\Delta_{6,3}(c)$;

and because $\tau_6(x,c)$ is absolutely irreducible over $\mathbf{F}_p$ for any odd prime p, by the method of [12, Sect. 6]. The prime $p=3$ can be handled by the following argument.

Over $\mathbf{F}_3$ we have $\Delta_{6,1}(c) = \Delta_{6,2}(c) = c^2, \Delta_{6,3}(c) = c^2(c+2)$, and (24) implies that m can only equal 3 (the power of $(c+2)$ in (24) is $6-3=3$). Because the roots of the polynomials $A_1(x), A_2(x)$ and $A_3(x)$ come in pairs $\{\alpha, f^3(\alpha)\}$, it follows that $(c+2)$ divides each of their discriminants, since some orbit must collapse to a 3-cycle at any root of $\Delta_{6,3}(c)$. We now set $c=-2$ and factor $\Phi_6(x,-2)$ (mod 3); we find that $A_1(x), A_2(x)$ and $A_3(x)$ must reduce respectively to

$$\begin{aligned} A_1(x,-2) &= (x^{12}+x^{10}+x^9+x^8+2x^3+2x^2+2)(x^3+x^2+x+2)^2, \\ A_2(x,-2) &= (x^{12}+2x^{11}+2x^{10}+2x^9+x^8+2x^7+x^6+2x^4+x^2+2) \\ &\quad (x^3+x^2+x+2)^2, \\ A_3(x,-2) &= (x^3+2x+2)(x^3+x^2+2x+1)(x^3+x^2+x+2)^4, \end{aligned}$$

say, with appropriate numbering. As specializations of the $A_i(x,c)$ these three polynomials must form a 3-cycle under the induced map of $f(x,-2) = x^2-2$ over $\mathbf{F}_3$. However, a calculation on Maple shows that the 12th degree factors of A_1 and A_2 form a 2-cycle, as do the simple cubic factors of A_3, while the cubic x^3+x^2+x+2 is a fixed point. Hence $\Phi_6(x,c)$ cannot factor as $A_1(x)A_2(x)A_3(x)$ over $\mathbf{F}_3$. This shows that $\Phi_6(x,c)$ is absolutely irreducible over $\mathbf{F}_p$ for any odd prime p.

References

1. Armstrong, M. A.: *Groups and Symmetry*, Springer Verlag, New York, 1988.
2. Batra, A. and Morton, P.: Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, I, *Rocky Mountain J. of Math.* 24 (1994), 453–481.
3. Bousch, T.: *Sur Quelques Problèmes de Dynamique Holomorphe*, These, Universite de Paris-Sud, Centre d'Orsay, 1992.
4. Branner, B.: The Mandelbrot set, in *Chaos and Fractals*, R. L. Devaney and L. Keen, eds., AMS Publications, Providence, R.I., 1989, pp. 75–105.
5. Douady, A. and Hubbard, J. H.: *Etude Dynamique des Polynomes Complex, I, II*, Publications Mathematiques d'Orsay, Universite de Paris-Sud, 1984.
6. Eichler, M.: *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser Verlag, Basel, 1963.
7. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* 73 (1983), 349–366.
8. Flynn, V., Poonen, B. and Schaefer, E.: Cycles of quadratic polynomials and rational points on a genus 2 curve, submitted.
9. Hasse, H.: *Zahlentheorie*, Akademie Verlag, Berlin, 1969.
10. Lau, E. and Schleicher, D.: Internal addreses in the Mandelbrot set and irreducibility of polynomials, SUNY Stony Brook, Institute for Mathematical Sciences, Preprint #1994/19.
11. Morton, P.: Characterizing cyclic cubic extensions by automorphism polynomials, J. Number Theory 49 (1994), 183–208.
12. Morton, P.: Arithmetic properties of periodic points of quadratic maps, II, preprint, Wellesley College, 1994.
13. Morton, P. and Patel, P.: The Galois theory of periodic points of polynomial maps, *Proc. London Math. Soc.* (3) 68 (1994), 225–263.
14. Morton, P. and Silverman, J.: Periodic points, multiplicities and dynamical units, *J. reine angew. Math.* 461 (1995), 81–122.

15. Morton, P. and Vivaldi, F.: Bifurcations and discriminants for polynomial maps, Nonlinearity 8 (1995), 571–584.
16. Schleicher, D.: Internal addresses in the Mandelbrot set and irreducibility of polynomials, Ph.D. Dissertion, Cornell University, 1994.
17. Silverman, J. H.: *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
18. Stichtenoth, H.: *Algebraic Function Fields and Codes*, Universitext Series, Springer-Verlag, Berlin, 1993.
19. Vivaldi, F. and Hatjispyros, S.: Galois theory of periodic orbits of polynomial maps, Nonlinearity 5 (1992), 961–978.