Periods of Maps on Irreducible Polynomials over Finite Fields

PATRICK MORTON

Department of Mathematics, Wellesley College, Wellesley, Massachusetts 02181

Communicated by Rudolf Lidl
Received September 11, 1995

1. INTRODUCTION

If $\sigma(x)$ is a polynomial with coefficients in the finite field $\mathbb{F}_q$, then the dynamics of $\sigma$ on the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ are reflected by an induced mapping $\hat{\sigma}$ of $\sigma$ on irreducible polynomials over $\mathbb{F}_q$, defined as follows. If $g$ is a monic irreducible polynomial over $\mathbb{F}_q$ with root $\alpha$, then $\hat{\sigma}(g) = \min \{ h \in \mathbb{F}_q[\alpha] : g(x) | h(\sigma(x)) \}$. Equivalently, $\hat{\sigma}(g) = h$ if and only if $g(x) | h(\sigma(x))$. To this mapping can be associated a directed graph $G_\sigma$ whose vertices are all monic irreducibles over $\mathbb{F}_q$ and whose edges are the pairs $(g, h)$ with $\hat{\sigma}(g) = h$. Periodic orbits of the map $\hat{\sigma}$ correspond to cycles in the graph $G_\sigma$. (See [1], [2], and [10].)

In [1] and [2] this induced mapping and graph were studied for the polynomials $\sigma(x) = x^q + ax$, for nonzero elements $a$ in $\mathbb{F}_q$. The “pre-periodic” structure of the associated graphs was determined in [2] for additive polynomials $\sigma$ over $\mathbb{F}_q$, with very explicit results for the mappings $\sigma(x) = x^p - x$ and $x^p + x$ over $\mathbb{F}_q$. It was also proved in [1] for any polynomial $\sigma$ that the map $\hat{\sigma}$ has infinitely many fixed points and for the special polynomials $\sigma(x) = x^q + ax$ that there are infinitely many irreducibles which are not fixed points of $\hat{\sigma}$.

To complete the determination of the dynamics of the mapping $\hat{\sigma}$ for the polynomials $\sigma(x) = x^q + ax$, it remains to determine the periods of $\hat{\sigma}$ or the lengths of the cycles in $G_\sigma$. In this paper we prove the following theorem. We say an irreducible polynomial $g$ has \textit{primitive} period $n$ with respect to $\hat{\sigma}$ if $\hat{\sigma}^n(g) = g$ but $\hat{\sigma}^m(g) \neq g$ for any positive $m < n$, where $\hat{\sigma}^n$ denotes the $n$th iterate of $\hat{\sigma}$. 

11
Theorem 1. Let \( \sigma(x) = x^q + ax \), for a non-zero \( a \) in \( \mathbb{F}_q \). Then for any integer \( n \geq 1 \) there are infinitely many monic irreducibles in \( \mathbb{F}_q[x] \) which have primitive period \( n \) under the induced mapping \( \sigma \).

Thus \( G_\sigma \) has infinitely many cycles of length \( n \), for any \( n \geq 1 \). The statement of the theorem is equivalent to the assertion that there are infinitely many elements \( \alpha \) of \( \mathbb{F}_q \) for which \( \sigma^n(\alpha) \) is conjugate to \( \alpha \) (over \( \mathbb{F}_q \)) but no \( \sigma^m(\alpha) \) is conjugate to \( \alpha \) (for \( m < n \) (\( \sigma^n \) is the \( n \)th iterate of \( \sigma \)).

To get periodic irreducibles of given period \( n \), prime to \( p \), we first use the Carlitz module (see [3], [4]) to characterize the polynomials which lie in cycles of length \( n \) in terms of the orders of certain elements in \( (\mathbb{F}_q[T]/(D))^* \), for polynomials \( D \) in \( \mathbb{F}_q[T] \), and then we apply Artin’s conjecture in function fields, or rather the extension of Artin’s conjecture given by Lenstra [5, Section 4]. To get irreducibles in cycles of length divisible by \( p \) we use a method given in [1, Section 7] for producing periodic points of \( \sigma \) of period \( p'n \) from periodic points whose periods \( m \) are prime to \( p \).

This result shows dramatically that the dynamics of \( x^q + ax \) on \( \mathbb{F}_q \) is very different from the dynamics of the map \( \phi(x) = x^q \), whose induced mapping fixes every irreducible polynomial. This theorem seems likely to be true for most polynomial maps over \( \mathbb{F}_q \), so we put forward the

Conjecture. For any polynomial \( \sigma(x) \) in \( \mathbb{F}_q[x] \) of degree \( \geq 2 \), which is not equal to \( ax^r + b \) for any \( r \) and \( a,b \) in \( \mathbb{F}_q \), the induced mapping \( \sigma \) on irreducible polynomials has infinitely many periodic points of primitive period \( n \), for any integer \( n \geq 1 \).

It is not hard to see that the periods of \( \sigma \) are bounded when \( \sigma(x) = ax^r + b \) for any \( r \) and \( a,b \) in \( \mathbb{F}_q \), the induced mapping fixes every irreducible polynomial. As noted above, the case \( n = 1 \) of this conjecture was proved in [1].

We also note the following consequence of Theorem 1 for \( p \)-adic orbits of polynomials of the form \( \sigma(x) = x^p + ax \) over \( \mathbb{Q}_p \).

Theorem 2. Let \( \sigma(x) = x^p + ax \), where \( a \) is a unit in the ring of \( p \)-adic integers \( \mathbb{Z}_p \). There are infinitely many periodic orbits of \( \sigma \) in \( \mathbb{Q}_p \) which do not consist entirely of algebraic conjugates over \( \mathbb{Q}_p \). In other words, there are infinitely many periodic points \( \alpha \) of \( \sigma \) in \( \mathbb{Q}_p \) for which \( \alpha \) and \( \sigma(\alpha) \) are not conjugate over \( \mathbb{Q}_p \).

This shows that the conjecture stated in [6, Section 1] for number fields \( K \), to the effect that all but finitely many of the cycles (periodic orbits) of a polynomial map over \( K \) consist entirely of algebraic conjugates over \( K \), is definitely false for \( p \)-adic fields.

I close this Introduction with a question. For the mapping given by \( \sigma(x) = x^q + ax \) over \( \mathbb{F}_q \), let \( A_n = \{ \text{monic irreducibles over } \mathbb{F}_q \text{ with primitive } \} \).
period $n$ wrt $\sigma$. Does $A_n$ have a well-defined natural density (or a Dirichlet density) $d_n$? If the densities $d_n$ exist, then they must tend to 0 as $n \to \infty$, since they sum to some number between 0 and 1. (Theorem 6.2 of [1] suggests that this sum is positive, i.e., a positive density of polynomials lie in cycles of $G_s$; it appears that at least $1/q$ of the irreducible polynomials whose degrees are prime to $p$ lie in cycles, and this is definitely true in the special case $\sigma(x) = x^d - x$.) For which $n$ is $d_n$ largest? Are all $d_n$ positive?

I am grateful to H. W. Lenstra, Jr., for a helpful conversation concerning the argument in Section 4.

2. The Carlitz Module and Iteration

By the results of [1], any periodic polynomial for the induced mapping of $\sigma(x) = x^d + ax$ is a divisor of one of the polynomials

$$\Phi_{n,a}(x) = \prod_{d|n} (\sigma^{d}(x) - x)^{d(n/d)}, \quad (1)$$

whose roots are the essential periodic points of $\sigma$ in $\overline{F}_q$ (in the terminology of [7]). We now introduce the related polynomials $f(x) = x^d + Tx$ and

$$\Phi_n(x, T) = \prod_{d|n} (f^{d}(x) - x)^{d(n/d)}. \quad (2)$$

It is clear that the polynomial $\Phi_{n,a}(x)$ in (1) is the specialization of $\Phi_n(x, T)$ for $T = a$ (cf. [6, Theorem 3.1]). We shall study properties of the irreducible factors of (1) and (2) using the Carlitz module (see [3] and [4]).

Recall that the Carlitz module is defined by

$$C_1(x) = x, \quad C_T(x) = x^d + Tx;$$

$$C_{\lambda A + B}(x) = \lambda C_A(x) + C_B(x), \quad \text{for } A \text{ and } B \text{ in } F_q[T], \text{ and } \lambda \text{ in } F_q;$$

$$C_{AB}(x) = C_A(C_B(x)), \quad \text{for } A \text{ and } B \text{ in } F_q[T].$$

(See [3], Eq. (2.1); the change of sign in the third line of Carlitz’s formula is now standard.) This is a formal module in the same sense that a formal group gives rise to an actual group: there is a natural object (the algebraic closure of $F_q(T)$) which has the structure of an $F_q[T]$-module when its elements are substituted for the variable $x$ in the above assignments. The expression $C_A(x)$ is a polynomial in the two variables $x$ and $T$. For these polynomials Carlitz [3] proved the factorization
where $D$ runs over the monic divisors of $A$ and the polynomials $W_D(x)$ are irreducible over $\mathbb{F}_q[T]$. The polynomials $W_D(x)$ can be considered to be analogues of cyclotomic polynomials, since their roots generate abelian extensions of $\mathbb{F}_q(T)$. Moreover, if $(A, D) = 1$ in $\mathbb{F}_q[T]$, then the polynomial $C_A(x)$ permutes the roots of $W_D(x)$ (see [3, Eq. (3.13)]), and $C_A(\beta) = C_B(\beta)$ for a root $\beta$ of $W_D(x)$ if and only if $W_D(x)$ divides $C_{A-B}(x)$; by (3) this is the case if and only if $D \mid (A-B)$. It follows from this and a degree calculation that

$$\text{Gal}(W_D(x)/\mathbb{F}_q(T)) \cong (\mathbb{F}_q[T]/(D))^\times$$

by the mapping which sends $A$ (mod $D$) to the automorphism $(\beta \mapsto C_A(\beta))$.

For later use we will require the following fact.

**Lemma 1.** Let $D_1$ and $D_2$ be distinct monic polynomials in $\mathbb{F}_q[T]$. Then $\text{Res}(W_{D_1}, W_{D_2})$ is a non-zero constant in $\mathbb{F}_q$ unless $D_1/D_2$ or $D_2/D_1$ is a power of an irreducible polynomial $Q$, in which case this resultant is a power of $Q$.

**Proof.** First we note that $C_A(0) = A(T)$, where the prime denotes the derivative with respect to $x$, a fact which follows easily from the defining formulas. If $D$ is irreducible, it follows from $C_D(x) = W_D(x) = xW_D$ that $W_D(0) = D$, and by induction on $r$ that $W_{D^r}(0) = D$ for any $r \geq 1$. Equation (3) implies further that $W_D(0) = 1$ if $D$ is not a power of an irreducible. Now the resultant $\text{Res}(W_{D_1}, W_{D_2})$ is a product of differences $a - b$, where $a$ is a root of $W_{D_1}$ and $b$ is a root of $W_{D_2}$. The annihilator $D$ of $a - b$ in $\mathbb{F}_q[T]$ divides $\text{lcm}(D_1, D_2)$, and $a - b$ is a root of $W_D(x)$. Further, $D_1 \mid \text{lcm}(D_1, D_2)$ and $D_2 \mid \text{lcm}(D_1, D_2)$. If neither $D_1/D_2$ nor $D_2/D_1$ is a power of an irreducible, it follows that at least two distinct irreducibles divide $D$. Then $W_D(0) = 1$ implies that $a - b$ divides 1 and is therefore a unit in some extension ring of $\mathbb{F}_q[T]$. Hence $\text{Res}(W_{D_1}, W_{D_2})$ must be constant in this case. If $D_1/D_2 = Q$, say, for an irreducible polynomial $Q$, write $D_2 = D_1 \cdot Q$, where $D_1$ is not divisible by $Q$. Then $D_1 \mid \text{lcm}(D_1, D_2)$ implies that $Q''$ divides $D$, for every difference $a - b$. If another irreducible divides $D$ then $a - b$ is a unit, as before. Otherwise $D = Q''$. Moreover, the map $a \rightarrow Q''a$ maps the roots of $W_{D_1}$ onto the roots of $W_{D_2}$, and $b \rightarrow Q''b$ similarly maps the roots of $W_{D_2}$ onto the roots of $W_{D_1}$ (since $Q'$ permutes the roots of $W_{D_2}$). Hence some $a - b$ has annihilator equal to $Q''$. It follows that the only possible irreducible factor of $\text{Res}(W_{D_1}, W_{D_2})$ in $\mathbb{F}_q[T]$ is $Q$ and that $Q$ is definitely an irreducible factor of this resultant: for if we conjugate $a - b$ by automorphisms of the splitting field of $W_{D_1}$, we
must obtain all roots of \( \Phi_{n,a}(x) \) in the form \( a - b \) for suitable \( a \) and \( b \), so that its constant term \( Q \) divides the resultant. This proves the lemma.

A similar argument shows that \( \text{disc}(W_D) \) is a product of powers of the irreducible factors of \( D \). We will also need the following.

**Lemma 2.** (see [3]) For any monic polynomial \( D \) in \( \mathbf{F}_q[T] \) which is relatively prime to \( T - a \) we have \( W_{D(T-a)} = (W_D)^{q^{2m} - 1} \mod (T-a) \).

**Proof.** From the defining formulas it follows easily that 

\[
W_{D(T-a)} = \prod_{B: D(T-a)'} C_B(x)^{\mu(D(T-a)/B)}
\]

\[
= \prod_{B: D} C_B(T-a)^{-1}(x)^{\mu(D(T-a)/B)} \prod_{B: D} C_B(T-a)^{\mu(D/B)}
\]

\[
= \prod_{B: D} C_B(x)^{\mu(D/B)(q^{-1} - q^{2m} - 1)}
\]

\[
= (W_D)^{q^{2m} - 1} \mod (T-a),
\]

where the \( \mu \)-function is defined in the obvious way on polynomials in \( \mathbf{F}_q[T] \).

From the definition of the polynomials \( C_D(x) \) and \( f(x) \) it is clear that \( f(x) = C_T(x) \) and \( f^{m}(x) - x = C_{T^{-1}}(x) \), so that (2) and (3) give

\[
\Phi_{m}(x, T) = \prod_{D \in \mathbb{P}_m} W_D(x),
\]

where \( \mathbb{P}_m \) is the set of primitive divisors of \( T^m - 1 \), those monic polynomials \( D \) for which \( D \mid T^m - 1 \) but \( D \) does not divide \( T^k - 1 \) for \( k < m \). Hence the irreducible factors of \( \Phi_{m,a}(x) \) over \( \mathbf{F}_q \) are identical to irreducible factors of certain specializations of \( W_D(x) \).

3. **Prime Divisors in Extension Fields and the Periodic Points of \( \hat{a} \)**

We shall now derive conditions for a given irreducible factor \( g(x) \) of \( \Phi_{m,a}(x) \) to be a primitive \( n \)-periodic point of \( \hat{a} \).

Suppose that \( g(x) \) divides the specialization of \( W_D(x) \) when \( T = a \). We interpret this using the abelian extension \( K_D \) of \( \mathbf{F}_q(T) \) generated by the roots of \( W_D(x) \). Let \( R \) be the integral closure of \( \mathbf{F}_q[T] \) in \( K_D \). On \( \mathbf{F}_q[T] \) the specialization \( T = a \) is the same as reduction modulo the prime ideal \( (T - a) \). Hence \( g(x) \) is one of the irreducible factors of \( W_D(x) \) (mod
$T - a$). By Lemma 2 it involves no loss of generality to assume that 
$(T(T - a), D) = 1$, though this might require replacing $m$ by a proper 
divisor. For such $D$, the discriminant of $W_D(x)$ is prime to $(T - a)$ (by the 
remark following Lemma 1) and the Dedekind–Kummer theorem ([8, p. 50] or [9, p. 76]) says that the prime ideal divisors of $(T - a)$ in $R$ are in 
$1$–$1$ correspondence with the irreducible factors of $W_D(x)$ (mod $T - a$). Thus

$$P = (g(\beta), T - a)$$

is one of the prime divisors of $T - a$ in $R$. ($W_D(\beta) = 0$.)

I now claim that the behavior of $g(x)$ under the induced mapping $\sigma$ is 
related to the behavior of the prime ideal $P$ under a specific automorphism 
of the Galois group $G_D = \text{Gal}(K_D/F_q(T))$.

To see this, let $Q$ be the ideal $Q = (\sigma g(\beta), T - a)$. Then $\sigma g(\beta) = 0$
(mod $Q$) and $\sigma g(C_T(\beta)) = 0$ (mod $Q'$), where $Q'$ is the image of $Q$
under the automorphism $\tau = (\beta \rightarrow C_T(\beta))$ (a well-defined automorphism by virtue of the assumption that $(D, T) = 1$). On the other hand, $\sigma g(C_T(\beta)) = \sigma g(\sigma(x))$ (mod $T - a$), and $\sigma g(\sigma(x))$ is divisible by $g(x)$, by definition of $\sigma$. We now appeal to Lemma 3.4 of [1], which we state for the convenience
of the reader.

**Lemma 3 (Lemma 3.4 of [1]).** Let $F$ be any field and $\sigma(x)$ be a polynomial 
in $F[x]$. If an irreducible polynomial $u(x)$ in $F[x]$ divides $\Phi_{m,\sigma}(x)$, then for 
any $i \geq 1$ there is a unique irreducible factor $h(x)$ of $\Phi_{m,\sigma}(x)$ for which 
h(x) | $u(\sigma^i(x))$.

Keeping in mind that $g \mid \Phi_{m,\sigma}(x)$ implies $\sigma(g) \mid \Phi_{m,\sigma}(x)$, this lemma says 
that $g(x)$ is the only irreducible factor of $\Phi_{m,\sigma}(x)$ which can also be a factor 
of $\sigma g(\sigma(x))$. Since $\sigma g(\sigma(x))$ does not have multiple roots, it follows from
(5) that $\sigma g(\sigma(x)) = g(x) \cdot h(x)$, where $(h(x), W_D(x)) = 1$ (mod $T - a$).
Hence some linear combination of $\sigma g(C_T(\beta))$, $W_D(x)$ and $T - a$ (with 
coefficients in $F_q[T]$) is equal to $g(x)$ and $h(\beta)$ is invertible (mod $T - a$); 
this implies $Q' = (\sigma g(C_T(\beta)), T - a) = (g(\beta), T - a) = P$ and therefore

$$P^{-1} = (\sigma g(\beta), T - a).$$

Note that $\sigma g(x)$ is also a factor of $W_D(x)$ (mod $T - a$). This can be seen 
as follows: assume that $\sigma g(x) \mid W_E(x)$ (mod $T - a$), so $W_E(x) = \sigma g(x)k(x) + r(T - a)$ for some $r$ in $F_q[x, T]$. We may take $E$ to be a 
primitive divisor of $T^m - 1$ for the same $m$ that $D$ is, by (5). Putting $f(x)$ 
in for $x$ in this equation and using $f(x) = \sigma(x)$ (mod $T - a$) and 
$W_E(f(x)) = W_E(x) \cdot W_{TE}(x)$ (see [3, Eq. (3.14)]) gives

$$W_E(x) \cdot W_{TE}(x) = \sigma g(\sigma(x)) \cdot k(\sigma(x)) + r'(T - a),$$
for another \( r' \) in \( \mathbb{F}_q[x, T] \). Therefore \( g(x) \) divides the left side of this equation (mod \( T - a \)). I claim now that \( \text{Res}(W_{TE}(x), \Phi_m(x, T)) \) is not divisible by \( T - a \), if \( E \) lies in \( P_m \). This follows from (5) and Lemma 1, since the last resultant is a product of resultants of the form \( \text{Res}(W_{TE}(x), W_D(x)) \), for \( D' \) in \( P_m \), and unless \( D' = E \) neither of the quotients \( TE/D' \) or \( D'/TE \) can be the power of an irreducible (especially if \( T - a \) divides \( D' \)). Therefore \( \gcd(W_{TE}(x), \Phi_m(x)) = 1 \) (mod \( T - a \)) and \( g(x) \) divides \( W_E(x) \) (mod \( T - a \)). But \( g(x) \) also divides \( W_D(x) \) (mod \( T - a \)); if \( E \neq D \), then \( (T - a) \) divides the resultant of \( W_D(x) \) and \( W_E(x) \) and Lemma 1 implies that \( E = D \cdot (T - a)^i \), for some \( i \). Now Lemma 2 implies that \( W_D(x) \) and \( W_E(x) \) have the same irreducible factors (mod \( T - a \)), proving the claim.

Thus we may iterate Eq. (7) to obtain

\[
P^{r''} = (\sigma^n g(\beta), T - a).
\] (8)

Because distinct irreducible factors of \( W_D(x) \) (mod \( T - a \)) give rise to distinct prime divisors of \( (T - a) \) in \( R \), we conclude from (8) that \( g(x) \) has primitive period \( n \) with respect to \( \sigma \) if and only if the automorphism \( \tau = (\beta \rightarrow C_T(\beta)) \) has period \( n \) with respect to the decomposition group of the prime ideal \( P \) (since the decomposition group of \( P \) is just the group of automorphisms of \( K_D \) fixing \( P \)).

On the other hand, the decomposition group of \( P \) is generated by the automorphism \( (\beta \rightarrow C_{T-a}(\beta)) \). To see this, recall that this decomposition group is generated by the unique automorphism \( \psi \) of \( K_D/\mathbb{F}_q(T) \) for which \( \psi(a) = a^i \) (mod \( P \)) for all \( a \) in \( K_D \) which are integral for \( P \). Since \( C_{T-a}(x) = x^i + (T - a)x = x^i (\mod T - a) \), we must have \( \psi = (\beta \rightarrow C_{T-a}(\beta)) \).

Putting these arguments together and using the isomorphism (4) gives the following proposition.

**Proposition 1.** Every monic, primitive, irreducible factor \( g(x) \) of \( \Phi_m(x) \) is a factor of \( W_D(x) \) (mod \( T - a \)) for a unique monic, primitive divisor \( D \) of \( T^m - 1 \) in \( \mathbb{F}_q[T] \) for which \( (T(T - a), D) = 1 \). The primitive period \( n \) of the polynomial \( g(x) \) with respect to the map \( \sigma \) is equal to the order of \( T \) with respect to the subgroup of \( (\mathbb{F}_q[T]/(D))^\times \) generated by \( T - a \).

The uniqueness of \( D \) is a consequence of Lemma 1 and the condition \((T(T - a), D) = 1 \). Note that other important parameters of the dynamics are given in terms of the group \( (\mathbb{F}_q[T]/(D))^\times \), as well. The order of \( T \) in this group is \( m \), which is the primitive period of the roots of \( g \) under the map \( \sigma(x) \). The order of \( T - a \) in the group is the degree of \( g \), since this is also the degree of the irreducible factors of \( W_D \) (mod \( T - a \)). (See Theorem 12 in [3].)

**Examples.** We take \( p = q = 2 \) and \( \sigma(x) = x^2 + x \) over \( \mathbb{F}_2 \). Below is a short table of periodic points of \( \sigma \) and their corresponding polynomials \( D \).
In each case listed but the last, \( W_D \) factors (mod \( T + 1 \)) as the product of the irreducibles in the cycle containing \( g \). In the last case \( W_D \) splits into two 2-cycles (mod \( T + 1 \)).

It is possible to prove similar results for more general additive maps of the form \( \sigma(x) = \sum a_i \phi(x) \), where \( \phi(x) = x^d \), but for the sake of brevity we will not go into this.

4. **Existence of Given Periods Prime to** \( p \)

Proposition 1 shows that the set of periods of \( \tilde{\sigma} \) coincides with the set

\[
\{ n: T \text{ has order } n \text{ with respect to } (T - a) \text{ mod } D, \text{ for some } D \text{ s.t. } (T(T - a), D) = 1 \}. \]

In this section we deal with the case \((n, \text{char } F_q) = 1\) by proving

**Proposition 2.** For any integer \( n \geq 1 \) which is relatively prime to \( q \) and any \( a \neq 0 \) in \( F_q \) there exist infinitely many irreducible polynomials \( D \) over \( F_q \) having the property that the order of \( T \) with respect to \( (T - a) \) in \((F_q[T]/(D))^*\) is \( n \).

To prove this proposition we shall attempt to find irreducible polynomials \( D \) for which the following conditions hold:

(i) \( q^{\deg D} = 1 \pmod{n} \);
(ii) \( (T - a) \) has index dividing \( n \) in \((F_q[T]/(D))^*\);
(iii) \( T - a \) is an \( n \)th power in \((F_q[T]/(D))^*\);
(iv) \( T \) is not an \( r \)th power (mod \( D \)) for any \( r \mid n \), \( r \neq 1 \).

Since \((F_q[T]/(D))^*\) is a cyclic group of order \( q^{\deg D} - 1 \), these conditions imply that \( D \) has the required property. Note that (i), (iii), and (iv) can be expressed as Cebotarev conditions for a suitable normal extension of \( F_q(T) \). We may take such a normal extension to be \( F = F_q(T, \ldots) \).
Theorem 4.8 [5, p. 208] says that argument [5, thm. 3.1] shows moreover that the prime ideal \((D(T))\) split completely in the extension \(F_q(\zeta_n, \sqrt[n]{a})/F_q(T)\). Condition (iii) (together with (i)) is equivalent to the condition that the ideal \((D(T))\) split in \(F_q(\zeta_n, \sqrt[n]{a})\), and condition (iv) (together with (i)) is equivalent to the condition that the Frobenius symbol

\[
\left[ \frac{F_q(\zeta_n, \sqrt[n]{a})/F_q(T)}{p} \right]
\]

has order \(n\), where \(p\) is a prime divisor of \((D(T))\) in \(F_q(\zeta_n, \sqrt[n]{a})\). Since \(F_q(\zeta_n, \sqrt[n]{a})\) and \(F_q(\zeta_n, \sqrt{a})\) are linearly disjoint over \(F_q(T, \zeta_n)\), these conditions are compatible, and are satisfied by all the irreducibles \(D\) (prime to \(T(T-a)\)) whose associated Frobenius classes for \(F/F_q(T)\) lie in a certain non-empty set of conjugacy classes \(C\) in Gal\((F/F_q(T))\).

To guarantee the existence of such irreducibles \(D\) we appeal to a result in [5]. In Lenstra’s notation we are interested in the set \(M\) of irreducible \(D\)’s whose Frobenius classes for \(F/F_q(T)\) lie in \(C\) and for which condition (ii) holds (see [5, p. 203] with \(W = (T-a)\)). For any prime \(l \neq p\) (\(p = \text{char } F_q\)) let \(q(l)\) be the smallest power of \(l\) which does not divide \(n\), and define \(L_l\) to be the field \(L_l = F_q(\zeta_n, (T-a)^{q(l)})\). In our case, Lenstra’s Corollary 4.8 [5, p. 208] says that \(M\) is infinite (and then has non-zero Dirichlet density) if and only if \(C\) is not contained in \(\cup_l \text{Gal}(F/L_l)\), the union being over all primes \(l \neq p\) for which \(L_l \subset F\). We will prove \(M\) infinite by showing that the last containment never holds. This is easy, since the ramification indices \(e_f\) of the prime divisors of \(T-a\) in \(F\) are all equal to \(n\), while the ramification indices \(e_l\) of the prime divisors of \(T-a\) in \(L_l\) are all equal to \(q(l)\). Since \(e_l | e_f\) whenever \(L_l \subset F\) and \(q(l)\) does not divide \(n\), by definition, this proves our claim, and with it the proposition. Lenstra’s argument [5, thm. 3.1] shows moreover that

\[
\text{Dirichlet density of } M = \lim_{m \to \infty} \sum_{d|m} \frac{\mu(d)\#(C \cap \text{Gal}(F/F \cap L_d))}{[F \cdot L_d : F_q(T)]} > 0,
\]

where \(L_d\), for square-free \(d\) prime to \(p\), is the compositum of the fields \(L_l\) over the primes \(l\) dividing \(d\), and where \(m\) ranges over square-free integers prime to \(p\).

**Corollary to Proposition 2.** For any integer \(n\) relatively prime to \(p\) (the characteristic of \(F_q\)) there are infinitely irreducible polynomials \(g\) over \(F_q\) which have period \(n\) with respect to the induced mapping \(\sigma\). Such polynomials can be found as irreducible factors of \(W_D \pmod{T-a}\), where \(D\) ranges over the irreducible polynomials guaranteed by Proposition 2.
Proof. We only need to check that different irreducible \( D \)'s yield different \( g \)'s. Since the \( g \)'s are divisors of \( W_D \)'s (mod \( T - a \)), two such \( g \)'s could only be equal if the corresponding \( W_D \)'s had a common root (mod \( T - a \)). But Lemma 1 shows that \( T - a \) does not divide the resultant of different \( W_D \)'s. Q.E.D.

5. Existence of Given Periods Divisible by \( p \)

To produce cycles in \( G_s \) with period divisible \( p'n \), where \( n \) is prime to \( p \), we use Proposition 2 and an idea from [1]. Given an irreducible \( g \) in a cycle of length \( n \), with root \( a \), we take an element \( l \) of degree \( pr \) over \( F_q \) and let \( h \) be the minimal polynomial of the element \( la \). Note that the period \( m \) and degree \( d \) of \( a \) are prime to \( p \) if \( g \) is an irreducible factor of \( WD \) mod \( T^2a \) and \( D \) is one of the polynomials of Proposition 2. Then [1, Theorem 7.2] implies that \( l \) has primitive period \( prm \) and degree over \( F_q \) equal to \( pr \deg g \). We will show that \( h \) lies in a cycle of degree \( p'n \) for suitable \( l \), independent of \( a \) and \( g \). Since there are infinitely many irreducibles \( g \) in cycles of length \( n \), there will be infinitely many corresponding irreducibles \( h \) in cycles of length \( p'n \). We shall prove

Proposition 3. Assume the minimal polynomial \( g \) of the nonzero number \( \alpha \) lies in a cycle of length \( n \) with respect to \( \sigma \), where \( (n, p) = 1 \), and that the minimal period \( m \) of \( \alpha \) is prime to \( p \). If \( \lambda \) is any element of \( \mathbb{F}_{q^p} \) which generates a normal basis over \( \mathbb{F}_q \), then the minimal polynomial \( h \) of \( \lambda \alpha \) lies in a cycle of length \( p'n \).

Let \( \phi(x) = x^p \) be the Frobenius map. Since \( \phi \) is a linear map, the algebraic closure of \( \mathbb{F}_q \) is an \( \mathbb{F}_q[\phi] \) module, and we may consider annihilators of algebraic elements with respect to this module. In particular, if \( \lambda \) generates a normal basis of \( E = \mathbb{F}_{q^p} \) over \( \mathbb{F}_q \), then its annihilator ideal is generated by \((\phi - 1)^p\), since no polynomial \( Q(\phi) \) of degree less than \( p' \) in \( \phi \) can annihilate \( \lambda \). Thus any polynomial \( Q(\phi) \) for which \( Q(\phi) \lambda = 0 \) must be divisible by \((\phi - 1)^p\). This is the main fact we will use in proving the proposition. Conversely, if the annihilator ideal of \( \lambda \) is generated by \((\phi - 1)^p\), then \( \lambda \) generates a normal basis of \( E/\mathbb{F}_q \). This may be used to count allowable \( \lambda \)'s: since they are roots of \((x^{q^p} - x)/(\phi - 1)^{p'}(x)\), there are \( q^p - q^{p-1} = q^{p-1}(q - 1) \) such numbers.

We first show that the period of \( h \) with respect to \( \sigma \) is a power of \( p \) times \( n \). Since \( \sigma^p(\alpha) \) is conjugate to \( \alpha \) and \( \sigma^{p'} \) is a linear map on \( E \) it is clear that \( \sigma^{np'}(\lambda \alpha) = \lambda \sigma^{np'}(\alpha) \) is conjugate to \( \lambda \alpha \). The period of \( h \) must therefore divide \( np' \). On the other hand, the period of \( h \) does not divide \( sp' \) for \( s < n \). For otherwise \( \sigma^{sp'}(\lambda \alpha) = \lambda \sigma^{sp'}(\alpha) \) is conjugate to \( \lambda \alpha \), so that \( \lambda \sigma^{np'} \)
(\alpha) = (\lambda \alpha)^i. Since \lambda and \alpha have relatively prime degrees it follows that 
\lambda^i = b \lambda for some b in F_q, and then that b = 1 (as in the proof of [1, 
Theorem 7.2]). Hence \sigma^{ni}(\alpha) = \alpha^i is conjugate to \alpha, which is impossible 
since n is the primitive period of g with respect to \sigma. This proves that the 
cycle length of h is np^i, for some i \leq r.

For the next step of the proof we first assume that r = 1, so that \lambda has 
degree p over F_q. In this case we just have to prove that \sigma^n(\lambda \alpha) is not 
conjugate to \lambda \alpha. So suppose that \sigma^n(\lambda \alpha) = (\lambda \alpha)^i for some i < p. Using 
\sigma^n = (\phi + a)^n this equation may be written in the form

\[ \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \alpha^k \phi^i(\lambda) = \alpha^i \phi^i(\lambda). \] (9)

Since \lambda has the same annihilator ideal over F_q(\alpha) that it does over F_q, it 
follows that the polynomial

\[ Q(\phi) = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \alpha^k \phi^i - \alpha^i \phi^i \] (10)

must be divisible by (\phi - 1)^p. Setting \phi = 1 gives therefore that Q(1) = 0, or

\[ \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \alpha^k = \alpha^i, \]

which just says that \alpha^i = (\phi + a)^n(\alpha) = \sigma^n(\alpha). Thus (9) may be written 
in the form

\[ \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \alpha^k \phi^i(\lambda) = \sigma^n(\alpha) \phi^i(\lambda). \] (11)

Applying the same argument to the derivative

\[ Q'(\phi) = \sum_{k=0}^{n} k \binom{n}{k} a^{n-k} \alpha^k \phi^{i-1} - i \sigma^n(\alpha) \phi^{i-1} \]

shows that
\[ \sum_{k=0}^{n} k \binom{n}{k} a^{n-k}c^k = i\sigma^n(\alpha). \]

But the left-hand side of the last equation is
\[ \phi \cdot \frac{d}{d\phi} (\phi + a)^n(\alpha) = n\phi(\phi + a)^{n-1}(\alpha), \]
and so we have that \( n\phi(\phi + a)^{n-1}(\alpha) = i\sigma^n(\alpha) \), or
\[ \sigma^{n-1}(\phi(\alpha)) = \frac{i}{n} \sigma^n(\alpha). \]  

(12)

This equation implies that \( i \) is not congruent to 0 or \( n \) (mod \( p \)), since otherwise \( \sigma^{n-1}(\alpha) \) would be 0 or conjugate to \( \alpha \). Since \( \sigma \) and \( \phi \) commute, (12) gives by induction that
\[ \sigma^{n-1}(\phi(\alpha)) = \left( \frac{i}{n} \right)^r \sigma^{nr-1}(\alpha), \quad \text{for } r \geq 1. \]

Now put \( r = p - 1 \). Then we have that \( \sigma^{n-1}(\phi^{p-1}(\alpha)) = \sigma^{n+p-2}(\alpha) \), and applying \( \sigma \) to both sides gives \( \sigma^n(\phi^{p-1}(\alpha)) = \sigma^{n+p-1}(\alpha) \), which we rewrite as \( \sigma^{p-1}(\sigma^n(\alpha)) = \phi^{p-1}(\sigma^n(\alpha)) \). But \( \sigma^n(\alpha) \) is a root of \( g \), so \( \sigma^{n-1}(\alpha) = \phi^{p-1}(\alpha) \) is conjugate to \( \alpha \).

The last fact implies that \( p - 1 \) is a period of \( g \), so \( n \leq p - 1 \). Thus the polynomial \( Q(\phi) \) (see (10)) has degree \( \leq p - 1 \) and leading coefficient \( \frac{i}{n}\sigma^n(\alpha) \) or \( -\phi(\alpha) \) (since \( i \) is not equal to \( n \)), neither of which can be 0. Therefore \( Q(\phi) \) cannot be divisible by \( (\phi - 1)^p \). This contradiction shows that \( h \) lies in a cycle of length \( np \) in \( G_\phi \).

To handle the general case we use the same argument to show that \( h \) does not have period dividing \( np^{r-1} \). Thus we need to show that \( \sigma^{np^{r-1}}(\lambda\alpha) = (\phi^{p^{r-1}} + a^{p^{r-1}})^n(\lambda\alpha) \) is not conjugate to \( \lambda\alpha \) over \( F_q \). But this follows from the case we have just considered \( (r = 1) \), since we may replace the field \( F_q \) by \( F = \mathbb{F}_{q^{p^r}} \), the map \( \sigma \) by \( \tau = \sigma^{p^r-1} = \phi^{p^r-1} + a^{p^{r-1}} \), and \( \phi \) by the Frobenius automorphism \( \phi^{p^{r-1}} \) on \( F \). Then \( \lambda \) has degree \( p \) over \( F \) and annihilator \( (\phi^{p^{r-1}} - 1)^p \); \( g \) is irreducible over \( F \), since its degree is prime to \( p \) (see [1, Theorem 6.2]); and \( g \) has period \( n \) with respect to the induced map of \( \sigma^{p^{r-1}} \), since \( n \) is prime to \( p \). Moreover, if \( \sigma^{np^{r-1}}(\lambda\alpha) \) is conjugate to \( \lambda\alpha \) over \( \mathbb{F}_{q^p} \), then \( \sigma^{np^{r-1}-i}(\lambda\alpha) = \phi^i(\lambda\alpha) \) for some \( i \), and the argument leading to (11) shows that \( \sigma^{np^{r-1}}(\lambda\alpha) = \phi^i(\lambda)^n(\alpha) \). We may iterate this equation \( p \) times to give
\[ \sigma^{np-1}f(\lambda \alpha) = \phi^i(\lambda)\sigma^{np-1}f(\alpha). \]

Since \( \sigma^{np}(\lambda \alpha) = \lambda \sigma^{np}(\alpha) \) we get that \( \phi^i(\lambda) = \lambda \); consequently \( p^{r-1} \mid i \) and \( \phi' \) is a power of the Frobenius map on \( F \), so that \( \sigma^{np-1}(\lambda \alpha) = \phi'(\lambda)\sigma^{np-1}(\alpha) \) is conjugate to \( \lambda \alpha \) over \( F \). (This uses that \( \lambda \) and \( \alpha \) have relatively prime degrees.) Thus the argument for the case \( r = 1 \) applies, and the period of \( h \) with respect to \( \sigma \) cannot divide \( np^{r-1} \). Hence \( h \) has period equal to \( np^r \).

This completes the proof of Proposition 3. Proposition 3 and the corollary to Proposition 2 together imply Theorem 1 of the Introduction.

6. Proof of Theorem 2

Now consider the polynomial \( \sigma(x) = x^p + ax \), where \( a \) is a unit in \( \mathbb{Z}_p \), the ring of \( p \)-adic integers. Let \( m \) be an integer for which \( \Phi_{p^m}(x) \) is divisible (mod \( p \)) by an irreducible polynomial \( \overline{g} \) over \( \mathbb{F}_p \) lying in a cycle of length \( n > 1 \) in \( G_n \), where \( \sigma(x) = x^p + ax \) is the reduced map over \( \mathbb{F}_p \). Furthermore, let \( \overline{g} = \overline{g}_1, \overline{g}_2, \ldots, \overline{g}_n \) be the irreducibles which make up the cycle containing \( \overline{g} \). Then we have a congruence

\[ \Phi_{m,\sigma}(x) = \prod_{i=1}^{n} \overline{g}_i(x)^{e_i} \cdot \overline{h}(x) \quad \text{(mod \( p \)),} \]

in which the polynomials \( \overline{g}_i \) are relatively prime to each other and to \( \overline{h} \). Hensel’s Lemma [8, p. 135] implies a factorization over \( \mathbb{Z}_p \),

\[ \Phi_{m,\sigma}(x) = \prod_{i=1}^{n} g_i(x) \cdot h(x), \]

where \( g_i(x) = \overline{g}_i(x)^{e_i}, h(x) = \overline{h}(x) \) (mod \( p \)). If \( \overline{\sigma}(\overline{g}_i) = \overline{g}_j \), then by Lemma 3 above, \( \gcd(\overline{g}_i(\sigma(x)), \Phi_{m,\sigma}(x)) = \overline{g}_i(x) \) (mod \( p \)) (since \( \overline{g}_i(\sigma(x)) \) has no multiple factors). Using Lemma 3 again, but applied to the irreducible factors of \( g_i(x) \) over \( F = \mathbb{Q}_p \), we see that \( \gcd(g_i(\sigma(x)), \Phi_{m,\sigma}(x)) \) is some product of irreducible polynomials which are relatively prime to \( h(x) \) and to each of the polynomials \( g_k(x) \), with \( k \neq i \). Thus the irreducible factors of \( \gcd(g_i(\sigma(x)), \Phi_{m,\sigma}(x)) \) all divide \( g_i(x) \). Furthermore, for any irreducible factor \( a(x) \) of \( g_i(x) \), \( \sigma(a(x)) \) divides \( g_i(x) \), since \( \sigma(a(x)) \) must divide some \( g_k(x) \), but \( g_k(\sigma(x)) \) is relatively prime to \( g_i(x) \) if \( k \neq j \). It follows that the irreducible factors of \( g_i(x) \) lie in cycles of length \( \equiv n \) in \( G_n \).

This shows that the orbit of a root \( \alpha \) of \( g_i(x) \) under \( \sigma(x) \) in \( \mathbb{Q}_p \) contains roots of each of the polynomials \( g_i(x) \), for \( 2 \leq i \leq n \), and therefore does not consist entirely of algebraic conjugates over \( \mathbb{Q}_p \). Since \( \alpha \) is a periodic
point of $\sigma$ and since $n$ may be chosen arbitrarily, this completes the proof of Theorem 2.

REFERENCES