Periodic points of a linear transformation

Hua-Chieh Li

Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan, ROC

ARTICLE INFO

Article history:
Received 2 September 2011
Accepted 13 June 2012
Available online 17 July 2012
Submitted by R. Bhatia

AMS classification:
37C25
37P25

Keywords:
Periodic point
Primitive period
Pure periodic point

ABSTRACT

We discuss the structure of periodic points of a linear transformation and find the possible set of the primitive periods of periodic points of a linear transformation.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

A dynamical system is a self map $T : X \rightarrow X$. The dynamics of the system is obtained by iterating the function $T$. We write $T^n$ for the $n$th iterate of $T$, i.e., $T^n(X) = T(T^{n-1}(X))$. (We use this less standard notation to avoid possible confusion with the notation $f^n(x)$, which means raising a polynomial $f(x)$ to the power of $n$.) An element $\alpha \in X$ is called a periodic point of $T$ if $T^n(\alpha) = \alpha$ for some $n \in \mathbb{N}$. For a periodic point $\alpha$, we will say $\alpha$ has period $n$ if $T^n(\alpha) = \alpha$ and the smallest such positive integer $n$ is called the primitive period of $\alpha$. In this paper, we are interested in the relation between the periodic points of a given map $T$. So we will drop the indication of $T$ and use $P_n$ to denote the set of periodic points of $T$ which have period $n$. We also denote the set of periodic points of $T$ which have primitive period $n$ by $\Lambda_n$. Clearly, we have $\Lambda_n \subseteq P_n$ and if $\alpha \in P_n$ then $\alpha \in \Lambda_d$ for some $d \mid n$. By definition it is also clear that if $n \mid m$ then $P_n \subseteq P_m$. In general, there seems no relation between $\Lambda_n$ and $\Lambda_m$ even for $n \mid m$. However, there do exist examples that for $n \mid m$, $\Lambda_n$ is related to $\Lambda_m$. For example, let $T : \mathbb{C} \rightarrow \mathbb{C}$ be defined by $T(x) = x^2$. $\Lambda_n$ is the set of primitive $2^n - 1$th roots of 1 and hence for $n \mid m$, 

E-mail address: li@math.ntnu.edu.tw

0024-3795/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.laa.2012.06.022
elements of $\Lambda_n$ can be generated by raising elements of $\Lambda_m$ to the $1 + 2^n + 2^{2n} + \cdots + 2^{[(m/n) - 1]n}$th power. For the case that $T$ is an automorphism of a formal group over a local field, we can consider $T$ as a map from the maximal ideal of the algebraic closure of $K$ to itself. Let $K(\Lambda_n)$ be the field generated by $\Lambda_n$ over $K$. Then in this case, we have $K(\Lambda_n) \subseteq K(\Lambda_m)$ when $n$ is large enough and divides $m$ (see [5]). For a prime number $p$, let $\mathbb{F}_p$ be the finite field of $p$ elements and let $T(x) = x + x^2$. We can consider $T$ as a map from the algebraic closure of $\mathbb{F}_p$ to itself. In this case, if $q$ is another prime such that $p$ is a primitive root modulo $q^2$, then in [2], Batra and Morton show that $\mathbb{F}_p(\Lambda_{q^r}) \subseteq \mathbb{F}_p(\Lambda_{q^{r+1}})$ for $r \geq 0$.

When $T$ is a linear transformation of a vector space $V$ over a field $K$, it is clear that $P_n$ is a vector space for every $n \in \mathbb{N}$. Let $E_n$ be the vector space generated by $\Lambda_n$. Then since $P_n = \cup_{d|n} \Lambda_d$, we have $P_n = \cup_{d|n} E_d$. Suppose that $K$ is an infinite field. Then since $P_n$ cannot be written as a finite union of its proper subspaces (see [4]), it implies that $P_n = E_d$ for some $d|n$. However, by definition, $E_d \subseteq P_d$ and hence if $\Lambda_n$ is not empty then since $P_d \subseteq P_n$ for $d|n$ and $d \neq n$, we conclude that $P_n = E_n$. In other words, if $\Lambda_n$ is nonempty, then $P_n$ is the vector space generated by $\Lambda_n$. In particular, for $d \mid n$, since $\Lambda_d \subseteq P_d \subseteq P_n$, every periodic point of primitive period $d$ is in the linear span of periodic points of primitive period $n$. This leads us to investigate the relations between periodic points of a linear transformation. In this paper, we concentrate on the structure of periodic points and show that over a finite field $K$, it is also true that $P_n$ is the vector space generated by $\Lambda_n$, providing $\Lambda_n$ is not empty. This gives a generalization of Batra and Morton’s result in [2] mentioned above. We also introduce the concept of periodic points of $P_n$ which help us to determine the set of primitive periods. The set of primitive periods has been studied in [1] for the case that $T$ is a linear transformation on the space $\mathbb{C}^n, \mathbb{R}^n$ and $\mathbb{I}^2$, respectively. For an additive polynomial over a field of positive characteristic, the set of primitive periods is completely studied in [6]. We extend the results in [1] to a more general setting and provide a more conceptual approach for the results in [6].

2. Basic results

In this section, $V$ is a vector space over a field $K$ and $T$ is a $K$-linear transformation from $V$ to $V$. Let $v \in P_n$ be a periodic point of $T$ of period $m$. Then the primitive period of $v$ must divide $m$. Moreover, suppose that $u, v \in V$ are periodic points of $T$ of primitive period $m$ and $n$ respectively. Let $l = \text{lcm}(m, n)$ be the least common multiple of $m$ and $n$. Then since $m \mid l$ and $n \mid l$, we have $T^l(u + v) = T^l(u) + T^l(v) = u + v$ and hence $u + v$ is a periodic point of $T$ of period $l$. We are interested in the primitive period of $u + v$.

Lemma 2.1. Suppose that $u, v \in V$ are periodic points of $T$ of primitive period $md$ and $nd$ respectively, with $\gcd(m, n) = 1$. Then $u + v$ is a periodic point of $T$ of primitive period $md'$, where $d' \mid d$. Moreover, if $d \neq d'$, then $(d/d') \notmid m$ and $(d/d') \notmid n$.

Proof. By the argument above, the primitive period of $u + v$ divides $mdn$. Therefore, we can assume that the primitive period of $u + v$ is $m'n'd'$ where $m' \mid m, n' \mid n$ and $d' \mid d$. Suppose $m' \neq m$. Then $u + v + T^{m'n'd'}(u + v) = T^{m'n'd'}(u) + v$, and hence $T^{m'n'd'}(u) = u$. Since the primitive period of $u$ is $md$, it implies $md \mid m'n'd'$. Thus $(m/m') \mid n$. This contradicts the assumption that $\gcd(m, n) = 1$ and hence we must have $m = m'$. Similarly, we have $n = n'$. This proves $u + v$ is a periodic point of $T$ of primitive period $md'$ for some $d' \mid d$.

Moreover, suppose $d \neq d'$ and $(d/d') \mid m$. Then $md' \mid mnd'$ and hence $u + v + T^{mnd'}(u + v) = T^{mnd'}(u) + v$. Thus $u = T^{mnd'}(u)$ and hence $md \mid mnd'$. Which means $(d/d') \mid n$. Since $d/d'$ divides both $m$ and $n$, this contradicts to the assumption that $\gcd(m, n) = 1$. Therefore, we must have $(d/d') \notmid m$ and similarly $(d/d') \notmid n$. □

Let $u, v$ be periodic points of $T$ and $u \in \Lambda_{md}, v \in \Lambda_{nd}$, where $\gcd(m, n) = 1$. If $d \mid m$ (resp. $d \mid n$), then for any divisor $d'$ of $d$, since $(d/d') \mid m$ (resp. $(d/d') \mid n$), by Lemma 2.1 we conclude that the primitive period of $u + v$ is $mnd$. This proves the following.
Corollary 2.2. Suppose \( u \in \Lambda_m \) and \( v \in \Lambda_n \). Let \( d = \gcd(m, n) \). If \( d \mid m/d \) or \( d \mid n/d \), then the primitive period of \( u + v \) is \( \text{lcm}(m, n) \). In particular, if \( \gcd(m, n) = 1 \), then the primitive period of \( u + v \) is \( mn \).

For the case that the primitive period of \( u \) divides the primitive period of \( v \), we have the following.

Corollary 2.3. Suppose \( u \in \Lambda_m \) and \( v \in \Lambda_n \), where \( m \mid n \) and \( m \neq n \). If the primitive period of \( u + v \) is not \( n \), then the primitive period of \( u + v \) is \( (n/m)\text{m'} \), where \( (m' \mid (m/m') \) \} \} (n/m) \} \} (m/m') \}. In particular, if \( p \) is a prime number and \( u \in \Lambda_{p^r} \) and \( v \in \Lambda_{p^s} \) with \( r < s \), then the primitive period of \( u + v \) is \( p^s \).

Proof. Suppose that the primitive period of \( u + v \) is not \( n \). By Lemma 2.1, the primitive period of \( u + v \) is \( (n/m)\text{m'} \), where \( (m' \mid (m/m') \) \} \} (n/m) \} \} (m/m') \} \} m \). If \( (n/m) \} \} (m/m') \} \} m \) then \( u + v = T^{\text{om}}(u + v) = u + T^{\text{om}}(v) \). Thus \( T^{\text{om}}(v) = v \) and it contradicts to the assumption that \( n \) is the primitive period of \( v \).

For the case \( m = p^r \) and \( n = p^s \), since for any \( m' \mid m \) with \( m' \neq m \), \( m/m' \) is a power of \( p \), we have either \( (m/m') \} \} (n/m) \} \} (m/m') \} \} m \). Therefore, \( m = m' \) and hence the primitive period of \( u + v \) is \( n = p^s \). \( \square \)

3. Structure of periodic points

In this section, we need the assumption that \( V \) is a finite dimensional vector space over \( K \). For investigating further about the primitive period of the summation of two periodic points, we review the primary decomposition theorem (see [3, Chapter IV, Theorem 4.2]).

Theorem 3.1. Let \( T : V \to V \) be a linear transformation of a finite dimensional vector space \( V \) over \( K \). There exist irreducible polynomials \( p_1(x), \ldots, p_s(x) \in K[x] \) and \( T \)-cyclic subspaces \( V_1, \ldots, V_s \) of \( V \) such that \( V = \bigoplus_{i=1}^s V_i \) and for each \( i \) there is a positive integer \( m_i \) such that \( p_i(x) \) is the minimal polynomial of \( T\vert V_i : V_i \to V_i \).

We remark that the prime power polynomials \( p_1^{m_1}(x), \ldots, p_s^{m_s}(x) \) in Theorem 3.1 are not necessary distinct and are called the elementary divisors of \( T \).

Let \( p(x)^m \) be an elementary divisor of \( T \) and let \( W \) be the corresponding \( T \)-cyclic subspace with a generator \( v \). Suppose that \( w = g(T)(v) \in W \) is a periodic point of \( T \). Thus there exists \( n \in \mathbb{N} \) such that \( T^n(w) = w \). In other words, \( p(x)^m \} \} (x^n - 1)g(x) \}. If \( p(x) \} \} x^n - 1 \), then \( p(x) \} \} g(x) \} \} w = 0 \). This says that there exists a nonzero periodic point in \( W \) if and only if \( x \) has finite order in \( K[x]/(p(x)) \) (i.e. there exist \( n \in \mathbb{N} \) such that \( x^n \equiv 1 \pmod{p(x)} \)).

Next we remark that if \( p(x) \) is irreducible and the characteristic of \( K \) is a prime \( p \), then \( p \) cannot divide the order of \( x \) in \( K[x]/(p(x)) \). Otherwise, write the order \( n \) as \( n = pn' \). Then \( x^n - 1 = (x^n - 1)^p \) and hence by the irreducibility of \( p(x) \), \( p(x) \} \} x^n - 1 \) implies \( p(x) \} \} x^n - 1 \). This contradicts to the assumption that \( n \) is the least positive integer such that \( x^n \equiv 1 \pmod{p(x)} \). Now, because the derivative of \( x^n - 1 \) is \( nx^n-1 \) and \( n \) is not divisible by the characteristic of \( K \), it implies that \( x^n - 1 \) has no multiple roots and hence \( x^n - 1 = p(x)h(x) \) where \( p(x) \} \} h(x) \). For any \( r \in \mathbb{N} \), \( x^{rn} = 1 + (p(x)h(x))^r \equiv 1 + rp(x)h(x) \pmod{p^2(x)} \). Therefore, if the characteristic of \( K \) is 0 then there exists no \( s \in \mathbb{N} \) such that \( p_i(x) \} \} x^s - 1 \) for \( s > 1 \). On the other hand, if the characteristic of \( K \) is a prime \( p \), then for \( p \} \} r \) we have \( x^{pr} \} \} x^{rn} - 1 \). Since \( x^{rn} = 1 + (p(x)h(x))^p \), it shows that \( np \) is the order of \( x \) in \( K[x]/(p(x)) \) for \( 2 \leq i \leq p \). Inductively, \( np^k \) is the order of \( x \) in \( K[x]/(p^k(x)) \), for \( p^{k-1} + 1 \leq i \leq p^k \).

Now, we can apply Theorem 3.1 to describe the structure of periodic points of a linear transformation.

Theorem 3.2. Let \( T : V \to V \) be a linear transformation of a finite dimensional vector space \( V \) over \( K \) and let \( P \) be the subspace of periodic points of \( T \). Suppose that \( p_1^{m_1}(x), \ldots, p_r^{m_r}(x), p_{r+1}^{m_{r+1}}(x), \ldots, p_s^{m_s}(x) \) are the elementary divisors of \( T \) where \( x \) has finite order \( n_i \) in \( K[x]/(p_i(x)) \) for \( 1 \leq i \leq r \) and \( x \) does not
has finite order in \( K[x]/(p_i(x)) \) for \( r + 1 \leq j \leq s \). Let \( V_i \) be the \( T \)-cyclic subspace corresponding to the elementary divisor \( p_i^{m_i}(x) \) with generator \( v_i \). We have the following.

1. Suppose the characteristic of \( K \) is 0. Then \( P = \bigoplus_{i=1}^{r} W_i \), where \( W_i \) is the \( T \)-cyclic subspace generated by \( p_i^{m_i-1}(T)(v_i) \). For each \( i \in \{1, \ldots, r\} \), every nonzero element of \( W_i \) is a periodic point of \( T \) of primitive period \( n_i \).

2. Suppose the characteristic of \( K \) is \( p \). Then \( P = \bigoplus_{i=1}^{r} W_i \), where \( W_i = V_i \). For each \( i \in \{1, \ldots, r\} \), \( v_i \) is a periodic point of \( T \) of primitive period \( n_i p_i \), where \( h_i \in \mathbb{N} \) satisfies \( p_i^{h_i-1} + 1 \leq m_i \leq p_i^{h_i} \) for \( m_i \geq 2 \) and \( h_i = 0 \) for \( m_i = 1 \). Moreover, every nonzero element of \( W_i \) is a periodic point of \( T \) of primitive period \( n_i p_i^r \) for some \( 0 \leq t \leq h_i \).

**Proof.** From the discussion above, every nonzero element in \( V_i \) is not a periodic point for \( r + 1 \leq j \leq s \). Therefore, we concentrate on the \( T \)-cyclic subspace \( V_i \) for \( 1 \leq i \leq r \). Suppose that \( w = g(T)(v_i) \in W_i \) is a nonzero periodic point of \( T \) with primitive period \( n \). Then \( n \) is the smallest positive integer such that \( p_i^{m_i}(x) \mid (x^n - 1)g(x) \).

Suppose that the characteristic of \( K \) is 0. By the argument above, \( p_i(x) \mid (x^n - 1) \) but \( p_i^2(x) \nmid (x^n - 1) \) and hence \( p_i^{m_i-1}(x) \mid g(x) \). This shows that the order of \( x \) in \( K[x]/(p_i(x)) \) (i.e. \( n_i \)) divides \( n \) and \( w = h(T) \circ p_i^{m_i-1}(T)(v_i) \) for some \( h(x) \in K[x] \). Thus, every nonzero periodic point in \( V_i \) is an element of the \( T \)-cyclic subspace generated by \( p_i^{m_i-1}(T)(v_i) \) and has primitive period divisible by \( n_i \). Conversely, if \( w = h(T) \circ p_i^{m_i-1}(T)(v_i) \) for some \( h(x) \in K[x] \) then since \( p_i^{m_i}(x) \mid (x^n - 1)h(x)p_i^{m_i-1}(x) \), we have \( T^{on}(w) = w \). In other words, every nonzero element of the \( T \)-cyclic subspace generated by \( p_i^{m_i-1}(T)(v_i) \) is a periodic point of period \( n_i \) and hence it is a periodic point of primitive period \( n_i \).

For the case that the characteristic of \( K \) is \( p \), since the order of \( x \) in \( K[x]/(p_i^{m_i}(x)) \) is \( n_i p_i^{h_i} \), it is clear that \( v_i \) is a periodic point of primitive period \( n_i p_i^{h_i} \). For any nonzero \( w \in W_i \), we have \( w = g \cdot p_i^{m_i}(T)(v_i) \) for some \( g(x) \in K[x] \) with \( p_i(x) \mid g(x) \) and \( 0 \leq k \leq m_i - 1 \). Since \( p_i^{m_i}(x) \mid (x^n - 1)g(x)p_i^k(x) \) if and only if \( p_i^{m_i-k}(x) \mid x^n - 1 \), the primitive period of \( w \) is \( n_i p_i^k \) for some \( 0 \leq t \leq h_i \). □

For simplicity, we call the decomposition \( P = W_1 \oplus \cdots \oplus W_r \) in Theorem 3.2 the primary decomposition of the periodic points of \( T \). For \( w \in P \), write \( w = w_1 + \cdots + w_r \), where \( w_i \in W_i \). If the primitive period of \( w_i \) is \( l_i \), then since \( W_i \) is \( T \)-invariant and \( P \) is a direct sum of \( W_1, \ldots, W_r \), the primitive period of \( w \) is \( \text{lcm}(l_1, \ldots, l_r) \) (see for example [1, Lemma 2]). From this, Theorem 3.2 generalizes [1, Theorem 3, Theorem 4]. For example, for a linear transformation \( T : \mathbb{R}^n \rightarrow \mathbb{R}^n \), every \( T \)-cyclic subspace of the primary decomposition of the periodic points of \( T \) is either of degree 1 or 2 over \( \mathbb{R} \) (because the degree of an irreducible polynomial in \( \mathbb{R}[x] \) is either 1 or 2). Moreover, \( x - 1 \) and \( x + 1 \) are the only possible degree 1 irreducible polynomials \( p(x) \in \mathbb{R}[x] \) such that \( x \) modulo \( p(x) \) has finite order and the nonzero elements in their corresponding \( T \)-cyclic subspace are periodic points of primitive period 1 and 2 respectively. For the case that \( K \) is algebraically closed, since every irreducible polynomial in \( K[x] \) is linear and \( x \) has finite order \( n \) in \( K[x]/(x - \alpha) \) if and only if \( \alpha \) is a primitive root of 1, we have the following.

**Corollary 3.3.** Let \( T : V \rightarrow V \) be a linear transformation of a finite dimensional vector space \( V \) over an algebraically closed field \( K \) and let \( P \) be the subspace of periodic points of \( T \). Suppose that \( (x - \alpha_1)^{m_1}, \ldots, (x - \alpha_r)^{m_r}, (x - \alpha_{r+1})^{m_{r+1}}, \ldots, (x - \alpha_s)^{m_s} \) are the elementary divisors of \( T \) where \( \alpha_i \) is a primitive \( n_i \)th root of 1 for \( 1 \leq i \leq r \) and \( \alpha_j \) is not a root of 1 for \( r + 1 \leq j \leq s \).

1. Suppose the characteristic of \( K \) is 0. Then \( P = \bigoplus_{i=1}^{r} W_i \), where \( W_i \) is a 1-dimensional subspace generated by an eigenvector \( w_i \) with eigenvalue \( \alpha_i \). The set of primitive periods of \( T \) is the smallest subset of \( \mathbb{N} \) containing \( \{n_1, \ldots, n_r\} \) and closed under the least common multiple operation.

2. Suppose the characteristic of \( K \) is \( p \). Then \( P = \bigoplus_{i=1}^{r} W_i \), where \( W_i \) is an \( m_i \)-dimensional \( T \)-cyclic subspace. For each \( i \in \{1, \ldots, r\} \), let \( h_i \in \mathbb{N} \) satisfy \( p_i^{h_i-1} + 1 \leq m_i \leq p_i^{h_i} \) for \( m_i \geq 2 \).
and \( h_i = 0 \) for \( m_i = 1 \). Then the set of primitive periods of \( T \) is the smallest subset of \( \mathbb{N} \) containing \( \{n_r^t \mid 1 \leq i \leq r, \ 0 \leq t \leq h_i \} \) and closed under the least common multiple operation.

Suppose \( u \in \Lambda_2 \) and \( v \in \Lambda_3 \). By Corollary 2.2, the primitive period of \( u + v \) is 6. However, there do exist periodic points which cannot be written as the sum of two periodic points with smaller primitive period. This leads us to the following definition.

**Definition 3.4.** Let \( U_1 = \{0\} \) and for \( m \in \mathbb{N} \) and \( m \geq 2 \), let \( U_m \) be the subspace generated by all the periodic points of \( T \) whose period is a proper divisor of \( m \), i.e. \( U_m = \sum_{d|m, d \neq m} P_d \). If \( w \in P_m \) and \( w \notin U_m \), then we call \( w \) a pure periodic point of \( T \).

For a prime \( p \), Corollary 2.3 tells us that \( U_{p^r} = P_{p^r-1} \) for \( r \in \mathbb{N} \). Therefore, every element in \( \Lambda_{p^r} \) is a pure periodic point. Moreover, if \( w \in \Lambda_{p^r} \) and \( u \in U_{p^r} \), then \( w + u \in \Lambda_{p^r} \) and hence \( w + u \) is also a pure periodic point. This can be generalized as the following.

**Lemma 3.5.** Let \( w \in \Lambda_m \) be a pure periodic point. Then for every \( u \in U_m \), we have \( w + u \in \Lambda_m \) and \( w + u \) is a pure periodic point.

**Proof.** Since \( w, u \in P_m \), it is clear that \( w + u \in P_m \). However, \( w + u \notin U_m \); otherwise \( w + u \in U_m \) and \( u \in U_m \) would imply \( w \in U_m \). This shows \( w + u \notin \Lambda_m \) and hence \( w + u \) is a pure periodic point. □

By Lemma 3.5, we immediately have the following.

**Theorem 3.6.** Let \( T : V \to V \) be a linear transformation of a finite dimensional vector space \( V \) over \( K \). For \( m \in \mathbb{N} \), if there exist pure periodic points of \( T \) of primitive period \( m \), then the subspace \( P_m \) is a group generated by the set of pure periodic points of \( T \) of primitive period \( m \).

**Proof.** If \( u \in U_m \), then for any pure periodic point \( w \in \Lambda_m \), by Lemma 3.5, \( w + u \in \Lambda_m \) is also a pure periodic point. Since \( u = (w + u) - w \), we conclude that \( u \) is contained in the group generated by the set of pure periodic points of primitive period \( m \). □

Consider the primary decomposition of the periodic points of \( T \), \( P = W_1 \oplus \cdots \oplus W_r \). For a periodic point \( w \) of primitive period \( m \), write \( w = w_1 + \cdots + w_r \) with \( w_i \in W_i \). Let \( l_i \) be the primitive period of \( w_i \). If there is \( k \in \{1, \ldots, r\} \) such that \( l_k = m \), then \( w \) is a pure periodic point. In fact, suppose \( w = w' + w'' \). Write \( w' = w'_1 + \cdots + w'_r \) and \( w'' = w''_1 + \cdots + w''_r \), with \( w'_i, w''_i \in W_i \). Then since \( w_k = w'_k + w''_k \), by Theorem 3.2, one of \( w'_k, w''_k \) must have primitive period \( m \). In other words, it is not possible that both \( w' \) and \( w'' \) are in \( U_m \). Conversely, if none of the \( l_i \) is equal to \( m \), then since \( \text{lcm}(l_1, \ldots, l_r) = m \), every \( l_i \) is a proper divisor of \( m \). In other words, \( w_i \in U_m \) and hence \( w \in U_m \). We summarize our discussion as the following.

**Proposition 3.7.** Let \( T : V \to V \) be a linear transformation of a finite dimensional vector space \( V \) over \( K \) and let \( P = W_1 \oplus \cdots \oplus W_r \) be the primary decomposition of the periodic points of \( T \). Suppose that \( w \) is a periodic point of \( T \) of primitive period \( m \) and \( w = w_1 + \cdots + w_r \) with \( w_i \in W_i \). Then \( w \) is a pure periodic point of \( T \) if and only if there exists \( k \in \{1, \ldots, r\} \) such that the primitive period of \( w_k \) is \( m \).

By Proposition 3.7, clearly every nonzero element in \( W_i \) is a pure periodic point. Using the primary decomposition of periodic points of \( T \), every periodic point can be written as a summation of pure periodic points. Knowledge of pure periodic points provides us some information about the primary decomposition of periodic points. In particular, the primitive periods of pure periodic points completely determine the set of primitive periods.

In order to know the existence of pure periodic points of primitive period \( n \), we need to study the dimension of \( P_n/U_n \) over \( K \). For a given \( n \in \mathbb{N} \), denote \( c_n \) the dimension of \( P_n \) over \( K \) and \( r_n \) the dimension of the quotient space \( P_n/U_n \) over \( K \). Let \( \beta_1 \subseteq P_1 \) be a set of \( r_1 = c_1 \) elements such that
Lemma 3.8. Let $T : V \rightarrow V$ be a linear transformation of a finite dimensional vector space $V$ over $K$. For $n \in \mathbb{N}$, let $c_n$ be the dimension of $P_n$ over $K$ and let $r_n$ be the dimension of the quotient space $P_n/U_n$ over $K$. Then $c_n = \sum_{d|n} r_d$ and $r_n = \sum_{d|n} \mu(n/d)c_d$.

In general, there might not exist a pure periodic point of a given primitive period. Next, we show that even if there is no pure periodic point of primitive period $m$, we still can use periodic points of primitive period $m$ to create all the periodic points of period $m$.

Let $f(x) = a_0x^n + \cdots + a_1x + a_0 \in K[x]$. It is clear that if $v \in P_m$, then $f(T)(v) = a_0T^n(v) + \cdots + a_1T(v) + a_0v \in P_m$. Moreover, if $v \in \Lambda_m$, then since $T^n(v) \in \Lambda_m$ for every $i \in \mathbb{N}$, we have that $f(T)(v)$ is in the vector space generated by $\Lambda_m$.

Theorem 3.9. Let $T : V \rightarrow V$ be a linear transformation of a finite dimensional vector space $V$ over $K$. For $m \in \mathbb{N}$, if $\Lambda_m$ is not empty, then the subspace $P_m$ is the vector space generated by $\Lambda_m$.

Proof. We only have to consider the case that $K$ is a (finite) field of characteristic $p$. Consider the primary decomposition $P_m = W_1 + \cdots + W_r$. It is sufficient to show that the generator of every $T$-cyclic subspace $W_i$ is in the vector space generated by $\Lambda_m$.

Let $m' \in \mathbb{N}$ be a generator of a $T$-cyclic subspace $W_i$ and suppose that the primitive period of $m'$ is $m'$ (note that $m' | m$). We write $m' = m''p^t$ where $p \nmid m''$. By Proposition 3.2, the minimal polynomial of $T|_{W_i}$ is $p^t(x) \in K[x]$ where $p(x)$ is an irreducible polynomial in $K[x]$. Moreover, $m''$ is the least positive integer such that $x^{m''} \equiv 1 \pmod{p(x)}$.

We decompose $P_m$ into a direct sum of two subspaces $V_1$ and $V_2$, where $V_1$ (resp. $V_2$) is a direct sum of the $T$-cyclic subspaces $W_j$ such that the minimal polynomial of $T|_{W_j}$ is divisible (resp. not divisible) by $p(x)$. Clearly, $w \in V_1$ and by Proposition 3.2, every nonzero element in $V_1$ has primitive period $m''p^t$ for some $t \in \mathbb{N} \cup \{0\}$.

Let $v$ be a periodic point of primitive period $m$ and suppose that the primitive period of $v+w = u$ is $n$. If $n = m$, then $w = u-v$ with both $u, v \in \Lambda_m$ and we are done. If $n \neq m$, then by Corollary 2.3, $m' | n$. We write $u$ as $u = u' + u''$, where $u' \in V_1$ and $u'' \in V_2$. Let the primitive period of $u'$ and $u''$ be $n'$ and $n''$ respectively. Then since $V_1 \cap V_2 = \{0\}$, we have $\text{lcm}(n', n'') = n$. Moreover, since $m' \nmid n$ and $u' \in V_1$, we have $n' = m''p^t$ for some $t < h$ for the case $h \geq 1$, and $n' = 1$ for the case $h = 0$. In other words, $n' \nmid m'$. Hence the primitive period of $u'-w$ divides $\text{lcm}(n', m') = m'$. Since $v = u-w = (u'-w) + u''$ with $u'-w \in V_1$ and $u'' \in V_2$, we have that $m \mid \text{lcm}(m', n'')$. On the other hand, both $m'$ and $n''$ divide $m'$ and hence $m = \text{lcm}(m', n'')$. Now, let $w' = w + u''$. The primitive period of $w'$ is $\text{lcm}(m', n'')$. In other words, $w' \in \Lambda_m$. Since $u'' \in W_2$, there exists a polynomial $g(x) \in K[x]$ such that $p(x) \mid g(x)$ and $g(T)(u'') = 0$. Hence, there exists a polynomial $h(x) \in K[x]$ such that $h(x)g(x) \equiv 1 \pmod{p^t(x)}$. Because $w = h(T) \circ g(T)(w)$ and $g(T)(w') = g(T)(u'') + g(T)(w) = g(T)(w)$, we have $w = h(T) \circ g(T)(w')$. Thus $w$ is in the vector space generated by $\Lambda_m$. □

4. Periodic points of an additive polynomial on the algebraic closure of a field of characteristic $p$.

Let $K$ be a field of characteristic $p$ and $\overline{K}$ be a fixed algebraic closure of $K$. Let $T(x) = \sum_{i=0}^{n} a_ip^i \in K[x]$ be an additive polynomial. It is clear that $T : \overline{K} \rightarrow \overline{K}$ is a linear transformation over $\mathbb{F}_p$. Though the dimension of $\overline{K}$ over $\mathbb{F}_p$ is not finite, the subspace of periodic points of $T$ of period $m$ is a finite set and hence is finite dimensional over $\mathbb{F}_p$. Therefore results in previous section can be applied.
For a map on an algebraically closed field of characteristic \( p \) defined by a polynomial, the set of its primitive periods is completely studied in [6]. For the case of additive polynomial, the result can be derived from the point of view of Drinfeld modules. However, we can utilize our previous results to get the same result. First we need some information about the multiplicity of periodic points.

**Definition 4.1.** Let \( f(x) \in K[x] \). Let \( \alpha \in \overline{K} \) be a periodic point of \( f(x) \) of period \( m \). Thus \( \alpha \) is a root of \( f^{(m)}(x) - x \). If the multiplicity of \( \alpha \) as a root of \( f^{(m)}(x) - x \) is \( h \), then we call \( \alpha \) a periodic point of \( f(x) \) of period \( m \) with multiplicity \( h \).

We remark first that since there is no primitive \( p \)th root of 1 in \( K \), it implies that \( p \nmid m \). For every \( n \in \mathbb{N} \), denote \( c_n \) the dimension of \( P_n \) over \( \mathbb{F}_p \) and \( r_n \) the dimension of the quotient space \( P_n/U_n \) over \( \mathbb{F}_p \). By Lemma 4.2, \( c_n = nr \) if \( m \nmid n \) and \( c_n = nr - hp^s \) if \( n = mp^s m' \), for some \( s \in \mathbb{N} \cup \{0\} \) and \( p \nmid m' \). Therefore, by Lemma 3.8, if \( m \nmid n \), then since \( c_d = dr \) for all \( d | n \), we have \( r_n = \sum_{d|n} \mu(d)nr/d \). Similarly for \( r_m \), since \( c_m = mr - h \), we have \( r_m = \sum_{d|m} \mu(d)mr/d - h \).

**Lemma 4.3.** Let \( T(x) = \sum_{i=0}^{r} a_i x^p^i \in K[x] \) be an additive polynomial.

1. Suppose \( a_0 \) is not a root of 1. Then every periodic point of \( T \) is simple.
2. Suppose that \( a_0 \) is a primitive mth root of 1 and \( T^{(m)}(x) - x = \sum_{i=0}^{r} b_i x^{p^i} \) with \( b_h \neq 0 \). Then for \( m \nmid n \), every periodic point of \( T \) of period \( n \) is simple. For \( m | n \), if \( n = mp^s m' \) with \( p \nmid m' \), then every periodic point of \( T \) of period \( n \) has multiplicity \( ph^s \).

**Proof.** For every \( n \in \mathbb{N} \), \( T^{(n)}(x) - x \) is also an additive polynomial. Therefore, every root of \( T^{(n)}(x) - x \) is simple if and only if \( a_0^p \) (the coefficient of \( x \) in \( T^{(n)}(x) \)) is not 1. In particular if \( a_0 \) is not a root of 1 or \( a_0 \) is a primitive mth root of 1 but \( m \nmid n \), then every root of \( T^{(n)}(x) - x \) is simple.

When \( a_0 \) is primitive mth root of 1, since by assumption \( T^{(m)}(x) = x + \sum_{i=h}^{r} b_i x^{p^i} \), a simple induction shows that \( T^{(mm')}(x) \equiv x + m' b_h x^{p^h} \pmod{x^{p^{h+1}}} \). Hence when \( p \nmid m' \) the periodic points of period \( m \) and the periodic points of period \( mm' \) have the same multiplicity \( ph^s \). On the other hand, let \( f(x) = T^{(mm')}(x) - x \). Since the characteristic of \( K \) is \( p \), a simple induction shows that \( T^{(mm')p^s}(x) - x = f^{(p^s)}(x) \).

By \( f(x) \equiv m' b_h x^{p^h} \pmod{x^{p^{h+1}}} \), it is clear that the lowest term of \( T^{(mm')p^s}(x) - x \) has degree \( ph^s \). Therefore, every periodic point of \( T \) of period \( mm' p^s \) has multiplicity \( ph^s \). □

It is interesting to know the existence of pure periodic points of specific primitive period. By Lemma 3.8, we have the following.

**Lemma 4.4.** Let \( T(x) = \sum_{i=0}^{r} a_i x^p^i \in K[x] \) be an additive polynomial and suppose that \( a_0 \) is a primitive mth root of 1. Suppose further that \( T^{(m)} = x + \sum_{i=h}^{r} b_i x^{p^i} \) with \( b_h \neq 0 \). Then

\[
\dim_{\mathbb{F}_p}(P_n/U_n) = \begin{cases} 
\sum_{d|m} \mu(d)mr/d - h, & \text{if } n = m; \\
\sum_{d|n} \mu(d)nr/d - h(p^s - p^{s-1}), & \text{if } n = mp^s, s \in \mathbb{N}; \\
\sum_{d|n} \mu(d)nr/d, & \text{otherwise}.
\end{cases}
\]

**Proof.** We remark first that since there is no primitive \( p \)th root of 1 in \( K \), it implies that \( p \nmid m \). For every \( n \in \mathbb{N} \), denote \( c_n \) the dimension of \( P_n \) over \( \mathbb{F}_p \) and \( r_n \) the dimension of the quotient space \( P_n/U_n \) over \( \mathbb{F}_p \). By Lemma 4.2, \( c_n = nr \) if \( m \nmid n \) and \( c_n = nr - hp^s \) if \( n = mp^s m' \), for some \( s \in \mathbb{N} \cup \{0\} \) and \( p \nmid m' \). Therefore, by Lemma 3.8, if \( m \nmid n \), then since \( c_d = dr \) for all \( d | n \), we have \( r_n = \sum_{d|n} \mu(d)nr/d \). Similarly for \( r_m \), since \( c_m = mr - h \), we have \( r_m = \sum_{d|m} \mu(d)mr/d - h \). For the case \( n = mp^s \), since
Next, for the case $p \nmid m$,

$$
\sum_{d \mid mp^s} \mu(d)c_{mp^s/d} = \sum_{d \mid m} \mu(dp^s)c_{m/d} + \sum_{d \mid m} \mu(dp^{s-1})c_{mp^s/d} + \cdots + \sum_{d \mid m} \mu(d)c_{mp^s/d},
$$

and hence

$$
r_n = \sum_{d \mid mp^s} \mu(d)mp^sr/d - \sum_{t=0}^{s} \mu(p^t)p^{s-t}h = \sum_{d \mid n} \mu(d)n/d - h(p^s - p^{s-1}).
$$

Next, for the case $n = mm'$ with $m' > 1$ and $p \nmid m'$, we can write $\sum_{d\mid n} \mu(d)c_{n/d}$ as $\sum_{d\mid mm'} \mu(d)c_{mm'/d} + \sum_{d\mid mm',d\nmid mm'} \mu(d)c_{mm'/d}$. Since $c_{mm'/d} = mm'r/d - h$ for $d \mid m'$ and $c_{mm'/d} = mm'r/d$ for $d \nmid m'$, we conclude that $r_{mm'} = \sum_{d\mid mm'} \mu(d)mm'r/d - \sum_{d\mid m'} \mu(d)h$. It is well known that $\sum_{d\mid m'} \mu(d) = 0$ when $m' \neq 1$, and hence $r_{mm'} = \sum_{d\mid mm'} \mu(d)mm'r/d$. Similarly, for the case $n = mm'p^s$, we have $r_n = \sum_{d\mid n} \mu(d)n/r/d$. □

It is clear that there exists a pure periodic point of primitive period $n$ if and only if the dimension of the quotient space $P_n/U_n$ over $\mathbb{F}_p$ is not zero. Recall that the Euler totient $\phi(n)$ of a positive integer $n$ is defined to be the number of positive integers less than or equal to $n$ that are relatively prime to $n$. It is well known that $\phi(n) = \sum_{d\mid n} \mu(d)n/d$. We have the following.

**Theorem 4.4.** Let $T(x) = \sum_{i=0}^{r} a_ix^{p^i} \in K[x]$ be an additive polynomial and suppose that $a_0$ is a primitive $m$th root of 1. Suppose further that $T^{m} = x + \sum_{i=1}^{m} b_ix^{p^i}$ with $b_i \neq 0$. If $h \neq \phi(m)r$, then there exists a pure periodic point of primitive period $n$ for every $n \in \mathbb{N}$. In the case that $h = \phi(m)r$, there is no pure periodic point of primitive period $n$ if and only if $n$ is $mp^s$, for every $s \in \mathbb{N} \cup \{0\}$.

**Proof.** By Lemma 4.3, for $n$ not of the form $mp^s$ with $s \in \mathbb{N} \cup \{0\}$, the dimension of $P_n/U_n$ is $\phi(n)r$ which is greater than 1 and hence there always exists a pure periodic point of primitive period $n$. For the case that $n = m$, the dimension of $P_m/U_m$ is $\phi(m)r - h$. Therefore, there is a pure periodic point of primitive period $m$ if and only if $h \neq \phi(m)r$. Similarly, for the case $n = mp^s$ with $s \in \mathbb{N}$, the dimension of $P_n/U_n$ is $\phi(mp^s)r - (p^s - p^{s-1})h$ which is equal to $(\phi(m)r - h)(\phi(p^s))$ since $p \nmid m$. Therefore, there is a pure periodic point of primitive period $mp^s$ if and only if $h \neq \phi(m)r$. □

For an additive polynomial $T(x) \in K[x]$, we define the set of primitive periods of $T$ being the set of positive integers $m$ such that $T$ has a periodic point of primitive period $m$ in $K$. For a given additive polynomial, its set of primitive periods can be determined completely.

**Theorem 4.5.** Let $T(x) = \sum_{i=0}^{r} a_ix^{p^i} \in K[x]$ be an additive polynomial. Then for every $m \in \mathbb{N}$, $T$ has a periodic point of primitive period $m$ unless $T(x) = x + \alpha x^{p^l}$ or there is an prime power $l'$ with prime $l \neq p$ such that $a_0$ is a primitive $l'$th root of 1 and $T^{p^l} = x + \sum_{i=1}^{p^l-1} b_ix^{p^i}$ with $b_i \neq 0$ and $h = \phi(m)r$. In the first exceptional case the set of primitive periods of $T$ is $\mathbb{N} \setminus \{p, p^2, \ldots\}$ and in the second exceptional case the set of primitive periods of $T$ is $\mathbb{N} \setminus \{l', l'^2, l'^3, \ldots\}$.

**Proof.** By Theorem 4.4, we only have to consider the case that $T(x) = \sum_{i=0}^{r} a_ix^{p^i} \in K[x]$ where $a_0$ is a primitive $m$th root of 1 and $T^m = x + \sum_{i=1}^{m} b_ix^{p^i}$ with $b_i \neq 0$ and $h = \phi(m)r$. In this case, the set of periodic points of $T$ contains all the positive integers which are not $mp^s$ for some $s \in \mathbb{N} \cup \{0\}$. For other cases, the set of periodic points of $T$ is $\mathbb{N}$.

Suppose first that $m$ is neither 1 nor a prime power. We decompose $m$ as a product of two relatively prime positive integers $a$ and $b$ where $a, b < m$. Since there exist periodic points of primitive period $a$ and $b$, respectively, Lemma 2.1 shows that there is a periodic point of primitive period $ab = m$. Moreover, since $p \nmid m$ and there are periodic points of primitive period $p^s$, for all $s \in \mathbb{N}$, by Lemma 2.1,
there are periodic points of primitive period $mp^s$, for all $s \in \mathbb{N}$. Therefore, the set of primitive periods of $T$ is $\mathbb{N}$.

Next, suppose $m = 1$ and $h = \phi (m) r = r$. This means $T(x) = x + \alpha x^p$ for some $\alpha \in K$. In this case, since $T^t(x) = x + \beta x^{p^t}$ for some $\beta \neq 0$, there is no periodic point of primitive period $p^t$ for every $t \in \mathbb{N}$.

Finally, suppose that $m = l^t$ where $l$ is a prime other than $p$ and $h = \phi (m) r = l^{r-1} (l - 1) r$. Since the degree of $T^r(x) - x$ is $p^r r$ and the degree of $T^{r-1}(x) - x$ is $p^{r-1} r$, the nonexistence of a periodic point of primitive period $l^t$ is equivalent to every root of $T(x) - x = l^t r$ is a root of $T^{r-1}(x) - x$ with multiplicity $p^{r-1} (l-1)$. In other words, $T(x) - x = \beta (T^{r-1}(x) - x) p^{r-1} (l-1)$, for some $\beta \in K$. Since $x^l - 1 = (x^{l-1}) x - 1 = (x^{l-1}) (x - 1) + (x^l - 1)$, it implies $T(x) - x = (T^{r-1}(x) + T^{r-1}(l-2)(x) + \cdots + T^{r-1}(x) + x = \beta x^{p^{r-1}(l-1)}$. Now, we show that in this case, there is no periodic point of primitive period $l^t p^s$ for all $s \in \mathbb{N}$. In fact, the multiplicity of a periodic point of period $l^t p^s$ is $p^{r-1} (l-1) p^s$ and every periodic point of period $l^{r-1} p^s$ is simple. Hence the number of distinct roots of $T(x) - x = p^{r-1} p^s / p^{r-1} (l-1) p^s = p^{r-1} p^s$ which is equal to the number of roots of $T(x) - x$. In other words, every periodic point of period $l^t p^s$ is a periodic point of period $l^{r-1} p^s$ and hence there is no periodic point of primitive period $l^t p^s$ for all $s \in \mathbb{N}$. For other cases, since there exist periodic points of primitive periods $m = l^t$ and $p^s$, respectively, again by Lemma 2.1, there are periodic points of primitive period $mp^s$, for all $s \in \mathbb{N}$ and hence the set of primitive periods of $T$ is $\mathbb{N}$.

5. Conclusion

Pure periodic points provide us information about the primary decomposition of periodic points. In particular, the primitive periods of pure periodic points completely determine the set of primitive periods. In fact, we can construct all the periodic points using pure periodic points.

References