The Arithmetic of Realizable Sequences

P. B. Moss

A thesis submitted to the School of Mathematics of the
University of East Anglia in partial fulfilment of the
requirements for the degree of Doctor of Philosophy
October 2003

Abstract

In this thesis we consider sequences of non-negative integers which arise from counting the periodic points of a map $T : X \to X$, where X is a non-empty set. Some of the main results obtained are concerned with the counting of the periodic points of an endomorphism of a group, in particular when the group is locally nilpotent, for which class of groups a local-global property is established. The ideas developed are applied to some classical sequences, including the Bernoulli and Euler numbers, which are shown to have certain 'dynamical' properties. We also consider the Lehmer-Pierce construction for sequences of integers, looking at possible generalizations and their associated measures.

Acknowledgements

I would like to thank both Graham and Tom for all their advice, encouragement, energy, enthusiasm, inspiration, suggestions and in general for just being there.

Thanks to Alan Camina for suggesting nilpotent groups, and for the conversations we had.

Thanks to the mathematics staff of the Open University for the MSc course that helped get me thinking again.

Special thanks go to Sally for her support and encouragement.

Thank you to my family, and to all of my friends and colleagues who have listened to me talk mathematics whenever I have had the chance.

Finally, I am very greatly indebted to Gerry McLaren for prompting me to take up research in mathematics once more, and for always being at the end of the phone to discuss the latest problem.

Notation and Conventions

Sets

- $\mathbb{N}$ the natural numbers $\{1, 2, 3, \ldots\}$
- $\mathbb{N}_0$ the non-negative integers: $\{0\} \cup \mathbb{N}$
- $\mathbb{Z}$ the rational integers
- $\mathbb{Q}$ the rational numbers
- $\mathbb{R}$ the real numbers
- $\mathbb{C}$ the complex numbers
- $\mathbb{T}^n$ the additive n-dimensional torus $\mathbb{R}^n/\mathbb{Z}^n$
- $\mathbb{F}_p$ the field of p elements
- $\mathbb{F}_q$ the field of $q = p^n$ elements
- $\mathbb{Z}_n$ the ring of integers modulo n
- $\mathbb{S}^1$ the multiplicative circle group $\{z \in \mathbb{C} : |z| = 1\}$
- $\emptyset$ the empty set

$|X|$ is used for the cardinal of the set X.

Number Theory

- $\gcd(m, n)$ the greatest common divisor of m and n
- $\operatorname{lcm}(m, n)$ the least common multiple of m and n
- $m \mid n$ m divides n
- $p^r \parallel n$ $p^r \mid n$ but $p^{r+1} \nmid n$
- $\lfloor x \rfloor$ the greatest integer less than or equal to x

The Möbius function $\mu : \mathbb{N} \to \mathbb{Z}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ with } p_1, \ldots, p_k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

The Euler φ-function (or Euler totient), $\varphi : \mathbb{N} \to \mathbb{N}$, is defined by

$$\varphi(n) = |\{k \in \mathbb{N} : k \leq n \text{ and } \gcd(k,n) = 1\}|.$$

Sequences

Sequences are written in the form (u_n) with the subscript n being a natural number by default. If the subscript comes from a different set of integers, or if we wish to emphasize the values taken by the subscript, we will write the sequence in the form $(u_n)_{n\in\mathbb{Z}}$, for example.

Groups

Let G denote a group with $a, b \in G$. The binary operation on G will be written additively as $a + b$, and in this case G is always abelian with identity 0 and inverse of a being $-a$. Sometimes we will use multiplicative notation and write ab, the identity element being 1, with the inverse of a being a^{-1}. The default operation is multiplication.

- $o(a)$ the order of the element a
- $a^b = b^{-1}ab$ the conjugate of a by b
- $[a, b] = a^{-1}b^{-1}ab$ the commutator of a and b
- $H \leq G$ $(G \geq H)$ H is a subgroup of G
- $N \trianglelefteq G$ $(G \trianglerighteq N)$ N is a normal subgroup of G
- $X^a = a^{-1}Xa$ the conjugate by a of $X \subseteq G$
- $|G : H|$ the index of the subgroup H in G
- $\mathbf{Z}(G)$ the centre of G
- ι_G the identity automorphism of G

If S is any subset of G, the subgroup of G generated by S is the smallest subgroup of G containing S and is written as $\langle S\rangle$. If S is a finite set then the subgroup $\langle S\rangle$ is said to be finitely generated. If $\mathcal{P}$ represents certain conditions imposed on the set S, we will write $\langle S : \mathcal{P}\rangle$ for the subgroup of G generated by S subject to the conditions $\mathcal{P}$.

Polynomials

If R is a ring, $R[x_1, \ldots, x_n]$ is used to represent the ring of polynomials in $x_1, \ldots, x_n$ over R. Let $F \in R[x]$. We write $\partial(F)$ for the degree of F; if F is the zero polynomial, $\partial(F) = -\infty$. If $G \in R[x_1, \ldots, x_n]$ this is extended to $\partial_{x_k}(G)$ for the degree of G in the variable x_k. The polynomial $F(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is called *primitive* if $\gcd(a_n, \ldots, a_1, a_0) = 1$.

If $H \in \mathbb{C}[x]$, we say that H is a *monic* polynomial if

$$H(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0,\ d \geq 1.$$

In this case, the *companion matrix* to H is

$$\Lambda_H = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{d-1} \end{pmatrix}.$$

General

- $\mathcal{M}_n(R)$ the ring of $n \times n$ matrices over R
- $\log^+ x = \log\max\{1, x\},\ x \in \mathbb{R},\ x \geq 0$
- $\mathrm{diag}(X^\alpha) = \bigcup_{x \in X}\{x\}^\alpha = \{(x, x, \ldots) : x \in X\}$
- $\mathbf{x}^{\mathrm{T}}$ the transpose of the vector $\mathbf{x}$

Contents

CHAPTER 1

Introduction

The primary concerns of this thesis are the arithmetic properties of those integer sequences which count the periodic points of a given map acting on a given set, with particular emphasis being placed on endomorphisms of groups. In this chapter, the basic concepts are introduced: there are no new results, though some proofs may be new.

1.1. Group Theory

The definitions, notations and properties of groups required in the thesis are recalled here. For more detail we refer to the books [**13**], [**24**], [**25**], and for specialized information about p-groups [**14**]. Throughout this section we will use G to denote an arbitrary group with binary operation 'multiplication'. If H is a subgroup of G we write this as $H \leq G$. Following common practice, the symbol 1 (or 0 in the case of an 'additive' group) is used to denote the identity of G, and also to denote the subgroup of G containing the identity only.

1.1.1. Basics. We assume that the notions of group (abelian and non-abelian), subgroup, coset, quotient group, group generators and elementary presentations are all known. We will concentrate here on terminology and notation.

Denote by X any non-empty subset of G and let $g \in G$. We use the notation X^g to represent the set

$$\{g^{-1}xg : x \in X\},$$

and x^g for the element $g^{-1}xg$ when $x \in G$. This operation on the subsets (elements) of G is known as *conjugation*. Two subgroups H_1, H_2

of G are said to be *conjugate* if there exists $g \in G$ such that $H_1^g = H_2$. For a given $H \leq G$, the set of subgroups of G, $\{H^g : g \in G\}$, is called the *conjugacy class* of the subgroup H. If $N \leq G$ is such that $N^g = N$ for all $g \in G$, then N is a *normal* subgroup of G, written as $N \trianglelefteq G$ (or, occasionally, $G \trianglerighteq N$). Thus, N is a normal subgroup of G if N is the only member of the conjugacy class of N. The *normalizer* of a subgroup H of G is

$$N_G(H) = \{g \in G : H^g = H\}.$$

We have $H \trianglelefteq N_G(H)$, and $N_G(H) = G$ if and only if H is a normal subgroup of G. The *centralizer* of a non-empty subset X of G is defined similarly:

$$C_G(X) = \{g \in G : x^g = x \text{ for all } x \in X\}.$$

Given $x, y \in G$, the *commutator* of x and y is defined to be

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^y.$$

If $A, B \leq G$, the subgroup $[A, B]$ of G is

$$[A, B] = \langle [a, b] : a \in A,\ b \in B \rangle.$$

If A and B are normal subgroups of G then $[A, B] = [B, A] \trianglelefteq G$ and $[A, B] \leq A \cap B$.

If L denotes a group and the map $\vartheta : G \to L$ is such that

$$\vartheta(g_1 g_2) = \vartheta(g_1)\vartheta(g_2) \text{ for all } g_1, g_2 \in G,$$

then we call ϑ a *homomorphism* from G to L. When ϑ is also a bijection, it is called an *isomorphism*, and in this case we write $G \cong L$. A homomorphism $\vartheta : G \to G$ is called an *endomorphism* of G. The set of all endomorphisms of G forms a semigroup under the operation of composition of maps. An isomorphism $\alpha : G \to G$ is known as an *automorphism*, and the set of all automorphisms is written as $\mathrm{Aut}(G)$.

This has the structure of a group, with binary operation the composition of maps. When g is a fixed element of G, the map $\psi_g : G \to G$ defined by $\psi_g : x \mapsto x^g$, is easily seen to be an automorphism of G; and any member of $\mathrm{Aut}(G)$ which has this shape is called an *inner automorphism* of G. We note here that if ψ_g is the inner automorphism just defined then $C_G(g) = \{x \in G : \psi_g(x) = x\}$: that is, $C_G(g)$ is the set of *fixed points* of the map $\psi_g : G \to G$.

A subgroup F of G is said to be *fully-invariant* if $\vartheta(F) \subseteq F$ for all endomorphisms ϑ of G, and $K \leq G$ is known as a *characteristic* subgroup of G if $\alpha(K) \subseteq K$ when $\alpha \in \mathrm{Aut}(G)$. It is clear that a fully-invariant subgroup is characteristic, and a characteristic subgroup is normal: examples exist to show that the converse is not true. A weakening of the requirements for a fully-invariant subgroup is: if ϑ is an endomorphism of G, then the subgroup H is called *ϑ-invariant* if $\vartheta(H) \subseteq H$. Thus, $H \leq G$ is fully-invariant if it is ϑ-invariant for all endomorphisms ϑ of G.

We conclude the basic constructions and definitions associated with a group by making precise what it means for a group to have local properties. Thus, if $\mathcal{P}$ is a property relating to the class of groups (for example, being finite) then a group L is said to be *locally* $\mathcal{P}$ if every finitely generated subgroup of L is contained in a subgroup of L having the property $\mathcal{P}$. For example, L is a *locally finite* group if every finitely generated subgroup of L is in fact finite.

1.1.2. Sylow subgroups. If p is a prime and the group P is such that every member of P has order a power of p, then P is called a *p-group*. A subgroup H of G is a *p-subgroup* of G if H, considered as a group in its own right, is a p-group. The *maximal* p-subgroups of G are known as the *Sylow p-subgroups* of G. The following result, which dates back to 1872, establishes the existence of Sylow p-subgroups of a finite group.

Theorem 1.1.1. (Sylow's Theorem) *Let S denote a finite group with $|S| = p^m r$, where p is prime, m is a non-negative integer and r is a positive integer such that $p \nmid r$. Then*

(1) *S has a Sylow p-subgroup of order p^m.*

(2) *If P is a Sylow p-subgroup of S and H is any p-subgroup of S then $H \leq P^x$ for some $x \in S$. In particular, the Sylow p-subgroups of S form a single conjugacy class.*

(3) *Let the number of distinct Sylow p-subgroups of S be denoted by n_p. Then $n_p = |S : N_S(P)|$, where P is any particular Sylow p-subgroup of S; $n_p \mid r$; and $n_p \equiv 1 \pmod{p}$.*

1.1.3. Central Series and Nilpotent Groups.

First we recall the definition of the centre of a group. The *centre* $\mathbf{Z}(G)$ of G is defined by

$$\mathbf{Z}(G) = \{x \in G : g^x = g \text{ for all } g \in G\}.$$

It is easy to see that $\mathbf{Z}(G)$ is a characteristic subgroup of G.

Let $H_0, H_1, \ldots, H_n$ denote normal subgroups of G with $n \geq 1$ and

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G. \tag{1.1}$$

We call (1.1) a *normal series* for G of length n. If the series is such that

$$H_r/H_{r-1} \leq \mathbf{Z}(G/H_{r-1}), \text{ for } r = 1, \ldots, n,$$

then it is called a *central series* for G. It is possible for a group to have a normal series but not a central series: the group S_3, the permutations of three symbols, is an example of such. If a group does possess a central series then it is said to be *nilpotent*. An abelian group A clearly has a central series: $1 \trianglelefteq A$; so all abelian groups are nilpotent. An example of a non-abelian nilpotent group follows.

Example 1.1.2. Let Q_8 denote the quaternion group of order 8,

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},$$

where the usual rules for the multiplication of quaternions apply. We have $\mathbf{Z}(Q_8) = \{1, -1\}$ and $\mathbf{Z}(Q_8/\mathbf{Z}(Q_8)) = Q_8/\mathbf{Z}(Q_8)$. It follows that a central series for Q_8 is $1 \trianglelefteq \mathbf{Z}(Q_8) \trianglelefteq Q_8$, so Q_8 is a non-abelian nilpotent group.

Next we consider the two most important cases of central series for G. The first of these is related to the centre of G and the construction is suggested by Example 1.1.2. The *upper central series* for the G is

$$\zeta_0(G) \trianglelefteq \zeta_1(G) \cdots \trianglelefteq \zeta_\alpha(G) \trianglelefteq \cdots \trianglelefteq G, \tag{1.2}$$

where $\zeta_0(G) = 1$, and for $r \geq 1$,

$$\zeta_r(G)/\zeta_{r-1}(G) = \mathbf{Z}(G/\zeta_{r-1}(G)).$$

Obviously, $\zeta_1(G)$ is the centre of G and it is clear that the subgroups $\zeta_r(G)$ are all characteristic. If G is a nilpotent group then there exists a least non-negative integer c such that $\zeta_c(G) = G$: c is called the *class* of the nilpotent group. An abelian group $A \neq 1$ has class 1.

The *lower central series* for G is

$$\gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \cdots \trianglerighteq \gamma_\beta(G) \trianglerighteq \cdots \trianglerighteq 1, \tag{1.3}$$

where $\gamma_1(G) = G$, and for $r > 1$,

$$\gamma_r(G) = [G, \gamma_{r-1}(G)].$$

If G is nilpotent then there is a positive integer n such that $\gamma_n(G) = 1$. It is known that if G is a nilpotent group of class c, then $\gamma_{c+1}(G) = 1$; and if c is the least non-negative integer such that $\gamma_{c+1}(G) = 1$, then G is of nilpotent class c.

Example 1.1.3. Let G denote the upper triangular matrix group

$$\begin{bmatrix} 1 & \mathbb{Q}/\mathbb{Z} & \mathbb{Q}/\mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{bmatrix}.$$

Here the notation means that the elements of G are matrices of the form

$$\begin{pmatrix} 1 & s & t \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix},$$

where $s, t \in \mathbb{Q}/\mathbb{Z}$ and $z \in \mathbb{Z}$. The group operation is matrix multiplication, with $\mathbb{Z}$ acting on $\mathbb{Q}/\mathbb{Z}$ in the natural way. It is clear that G is an infinite non-abelian group: we will show that is nilpotent, of class 2. First, the set of matrices

$$\begin{bmatrix} 1 & 0 & \mathbb{Q}/\mathbb{Z} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

is a subgroup of G, and it is easy to see that it is in fact the centre, $\mathbf{Z}(G)$, of G. Now let

$$x = \begin{pmatrix} 1 & s_1 & t_1 \\ 0 & 1 & z_1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & s_2 & t_2 \\ 0 & 1 & z_2 \\ 0 & 0 & 1 \end{pmatrix}$$

be any two members of G. Then we obtain

$$[x, y] = \begin{pmatrix} 1 & 0 & z_2 s_1 - z_1 s_2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and so $\gamma_2(G) = [G, G] \trianglelefteq \mathbf{Z}(G)$. It follows that $\gamma_3(G) = 1$, so G is nilpotent of class 2.

We finish with two results concerning nilpotent groups, the first of which guarantees a plentiful supply of such.

Theorem 1.1.4. *Let p denote a prime and P a finite p-group. Then P is nilpotent.*

The proof of this result is a consequence of the fact that the centre of a finite p-group is non-trivial. The next theorem establishes the overall structure of a finite nilpotent group.

Theorem 1.1.5. (Burnside and Wielandt) *Let G denote a finite group. Then G is nilpotent if and only if each Sylow p-subgroup of G is fully-invariant.*

It follows from this and Sylow's Theorem that in a finite nilpotent group the Sylow p-subgroups are unique for each prime, and that the group is the (direct) product of these subgroups.

1.2. Realizable Sequences

A class of sequences is introduced which owes its origins to the theory of dynamical systems. Many of the definitions and results in this section are to be found in [**22**].

An important consideration in many branches of mathematics is that of the set of *periodic points* of a map $T : X \to X$, where both X and T would normally possess some mathematical structure. For example, X may be a compact topological space and T a continuous map, or X may be a group and T an automorphism. Ergodic theory and the study of dynamical systems provide many examples in these categories. We refer to the books [**10**], [**26**] and [**29**] for information relating to systems of this type. A natural question arising from the study of this kind of system is to enquire about the properties of those integer sequences that count the number of periodic points, leading to the following definitions.

Let X denote a non-empty set, and $T : X \to X$ a map; call the pair (X, T) a *system.* The set of *fixed points* of the map T is

$$\mathrm{Fix}(T) = \{x \in X : T(x) = x\}.$$

For each integer $n \geq 1$, the set of *periodic points* of period n for T is

$$\mathrm{Per}_n(T) = \mathrm{Fix}(T^n) = \{x \in X : T^n(x) = x\}.$$

Definition 1.2.1. A sequence (u_n) of non-negative integers is said to be *realizable* if there exists a system (X, T) such that for every $n \geq 1$, $u_n = |\,\mathrm{Per}_n(T)|$.

In [**22**] the expression *exactly realizable* is used for this type of sequence. We will variously use the alternatives: u is a realizable sequence; the sequence u is realized by the system (X, T); (X, T) realizes the sequence u. Although no structure is placed on the system (X, T), it is known that without any loss of generality, X may be assumed to be a compact topological space and $T : X \to X$ a homeomorphism; see [**22**] for the details. Indeed, a recent result of Alistair Windsor, states that without loss of generality, the system (X, T) may be taken to be: X is the 2-torus, $\mathbb{T}^2$, and $T : X \to X$ is a C^∞ diffeomorphism. A simple example of a realizable sequence follows.

Example 1.2.2. The permutation

$$T = (1\,2\,3\,4)(5\,6) \text{ acting on the set } X = \{1, 2, 3, \ldots, 8\}$$

realizes the periodic sequence $(2, 4, 2, 8, 2, 4, 2, 8, \ldots)$.

A further example of a realizable sequence, which we will require later, is given in the next result.

Proposition 1.2.3. *If a is a positive integer then the sequence $(a^n)_{n\geq 1}$ is realizable.*

Proof. Denote by X the set of sequences $\{0, 1, \ldots, a-1\}^{\mathbb{N}}$ and let $T : X \to X$ be the left shift map; that is, if $x = (x_1, x_2, x_3, \ldots) \in X$ then $T : x \mapsto (x_2, x_3, x_4, \ldots)$. Then it is easy to see that the system (X, T) realizes the sequence $(a^n)_{n\geq 1}$. □

The following gives an arithmetic criterion for determining whether or not a given sequence is realizable. For a proof of the result we refer to [**22**] where it is called the *Basic Lemma.*

Lemma 1.2.4. *Let (u_n) denote a sequence of non-negative integers, and define the sequence (u_n^*) by*

$$u_n^* = \sum_{d|n} \mu(n/d) u_d,$$

where μ is the Möbius *function. Then (u_n) is a realizable sequence if and only if the following two conditions hold for all $n \geq 1$,*

(1) $u_n^* \geq 0$

(2) $n \mid u_n^*$.

The two conditions in Lemma 1.2.4 prompt the following definitions. The first we are able to give in a general form, not being restricted to just integer sequences.

Definition 1.2.5. Let $x = (x_n)_{n\geq 1}$ denote a sequence of non-negative real numbers. We say that x has *positivity* if the sequence $x^* = (x_n^*)$ defined by

$$x_n^* = \sum_{d|n} \mu(n/d) x_d, \ \ n = 1, 2, 3, \dots,$$

satisfies the condition $x_n^* \geq 0$ for all $n \geq 1$.

The second definition is not quite so general.

Definition 1.2.6. Let $a = (a_n)_{n\geq 1}$ denote a sequence of integers. We say that a has *divisibility* if for every integer $n \geq 1$,

$$\sum_{d|n} \mu(n/d) a_d \equiv 0 \pmod{n}.$$

Given a sequence $u = (u_n)$ of non-negative integers, to show that it is a realizable sequence we now have two means of *attack* available. The first (and often the easiest) is to find a system (X, T) which realizes the sequence u. The other approach is to utilize Lemma 1.2.4 and show that u has both positivity and divisibility. On the negative side, the following result often gives a very quick way of establishing the fact that a sequence is *not* realizable.

Lemma 1.2.7. *Let p denote a prime and $u = (u_n)$ a sequence of non-negative integers. If u is a realizable sequence then*

$$u_p - u_1 \geq 0 \text{ and } p \mid u_p - u_1.$$

Proof. Since $\mu(p) = -1$ and $\mu(1) = 1$, this follows immediately from Lemma 1.2.4. □

The class of realizable sequences possesses some algebraic structure, as we will now demonstrate. If $u = (u_n)$ and $v = (v_n)$ are any two sequences, then the *sum* and *product* sequences are defined as pointwise operations. That is: $u + v = (u_n + v_n)$ and $uv = (u_n v_n)$.

Proposition 1.2.8. *If $u = (u_n)$ and $v = (v_n)$ are realizable sequences then $u + v$ and uv are both realizable sequences.*

Proof. Let the realizing systems for u and v be (U, T_u) and (V, T_v). Denote by W the *disjoint* union of the sets U, V and define the map $S : W \to W$ by

$$S : x \mapsto \begin{cases} T_u(x) & \text{if } x \in U \\ T_v(x) & \text{if } x \in V, \end{cases}$$

for $x \in W$. The system (W, S) realizes the sum $u + v$. Clearly, the product sequence uv is realized by the system $(U \times V, T_u \times T_v)$. □

The next result basically says that if we have the beginning of a realizable sequence then we can extend it to give a complete realizable sequence. It is included firstly for interest, but mainly to assist in the proof of Lemma 1.2.10.

Lemma 1.2.9. *Let m denote a fixed positive integer and $s_1, \ldots, s_m$ a finite sequence of non-negative integers where for each integer n in the range $1 \leq n \leq m$*

(1) $\sum_{d|n} \mu(n/d)s_d \geq 0$

(2) $\sum_{d|n} \mu(n/d)s_d \equiv 0 \pmod{n}$.

Then there is a realizable sequence (u_n) *with* $u_k = s_k$ *when* $1 \leq k \leq m$.

Proof. Define the sequence of non-negative integers (a_n) by

$$a_n = \begin{cases} \sum_{d|n} \mu(n/d)s_d & \text{if } 1 \leq n \leq m \\ n & \text{if } n > m. \end{cases}$$

We note that by the given conditions, $a_n \geq 0$ and $n \mid a_n$ for all $n \geq 1$. Now set $u_n = \sum_{d|n} a_d$ for $n \geq 1$. Clearly, (u_n) is a sequence of non-negative integers and the Möbius inversion formula gives $u_k = s_k$ when $1 \leq k \leq m$. Finally, Lemma 1.2.4 shows that (u_n) is a realizable sequence because $\sum_{d|n} \mu(n/d)u_d = a_n$ for all $n \geq 1$. □

Next we have a (partial) generalization of Proposition 1.2.8 to sequences of real numbers.

Lemma 1.2.10. *If the sequences* $x = (x_n)$, $y = (y_n)$ *of non-negative real numbers both have positivity, then the sum and product sequences,* $x + y = (x_n + y_n)$ *and* $xy = (x_n y_n)$ *have positivity.*

Proof. The fact that positivity is preserved by the sum $x+y$ is trivial, so we will concentrate on the product sequence. Fix the integer $m \geq 1$ and assume first of all that x and y are both sequences of non-negative rationals. Then, using Lemma 1.2.9, we can find an integer $k \geq 1$ and realizable sequences $(u_n), (v_n)$ so that $u_n = kx_n$, $v_n = ky_n$ when $1 \leq n \leq m$. Next apply Lemma 1.2.8 to see that the sequence $(u_n v_n)$ has positivity. However, when $1 \leq n \leq m$ we have $u_n v_n = k^2 x_n y_n$, so for n in this range

$$0 \leq \sum_{d|n} \mu(n/d)u_d v_d = k^2 \sum_{d|n} \mu(n/d)x_d y_d,$$

from which we get

$$\sum_{d|n} \mu(n/d)x_d y_d \geq 0, \text{ when } 1 \leq n \leq m.$$

Since m was an arbitrary fixed integer it follows that xy has positivity when x and y are non-negative rational sequences with positivity. To complete the proof we just appeal to analysis and the fact that the rationals are dense in the reals. □

We finish this section with a result establishing a simple sufficient condition for a sequence to have positivity.

Lemma 1.2.11. *If $x = (x_n)$ is an increasing sequence of non-negative real numbers which is such that $x_{2n} \geq nx_n$ for all $n \geq 1$, then x has positivity.*

Proof. First note that because x is an increasing sequence, for any integer $n \geq 1$

$$x_{2n+1} \geq x_{2n} \geq nx_n = \lfloor (2n+1)/2 \rfloor x_{\lfloor (2n+1)/2 \rfloor},$$

so we have $x_n \geq \lfloor n/2 \rfloor x_{\lfloor n/2 \rfloor}$ for all $n \geq 2$. It follows from this and the fact that $\mu(n) \geq -1$ when $n \geq 1$,

$$\sum_{d|n} \mu(n/d) x_d \geq x_n - \sum_{\substack{d|n \\ d \neq n}} x_d \geq x_n - \lfloor n/2 \rfloor x_{\lfloor n/2 \rfloor} \geq 0 \text{ if } n \geq 2.$$

Therefore the sequence x has positivity. □

Alternative proofs of Lemmas 1.2.10 and 1.2.11 can be found in the second chapter of [**22**].

1.3. Local Realizability

In many branches of mathematics, it is often possible to throw light on the structure of an object by looking at it *locally.* The survey article [**20**] examines this process, as applied to number theory, in some depth. We introduce the concept of a *locally realizable* sequence in order to simplify (in some cases) the process of showing that a given sequence is realizable.

If a is a positive integer and p a prime, there are integers $k \geq 0$ and $b \geq 1$ such that $a = p^k b$ with $p \nmid b$: p^k is called the *p-part* of the integer a; we write $[a]_p = p^k$ and $\operatorname{ord}_p(a) = k$. Given a sequence (u_n) of non-negative integers, (u_n) is *locally realizable at* p if the sequence $([u_n]_p)_{n\geq 1}$ is realizable. If $u = (u_n)$ is locally realizable at all primes then u is *everywhere locally realizable.*

Proposition 1.3.1. *If the sequence $u = (u_n)$ is everywhere locally realizable then u is realizable.*

Proof. For each prime p there is a non-empty set X_p with a map $T_p : X_p \to X_p$ such that (X_p, T_p) realizes the sequence of p-parts $([u_n]_p)$. Define the set X by $X = \prod_p X_p$, and the map $T : X \to X$ to be the corresponding product $T = \prod_p T_p$. Now we have

$$|\operatorname{Per}_n(T)| = \prod_p |\operatorname{Per}_n(T_p)| = \prod_p [u_n]_p = u_n,$$

and so the system (X, T) realizes the sequence u. □

In general, the converse of Proposition 1.3.1 is not true, as demonstrated by the following example. However, it is true when the sequence is realized by a system (X, ϑ) where X is a locally nilpotent group and ϑ an endomorphism on X: this is proved in Chapter 3.

Example 1.3.2. Consider the symmetric group of order 6,

$$S_3 = \langle a, b : a^3 = 1, b^2 = 1, a^b = a^{-1} \rangle.$$

If $\psi : S_3 \to S_3$ is the inner automorphism, $\psi : x \mapsto x^a$, $x \in S_3$, then the sequence realized by the system (S_3, ψ) is

$$u = (3, 3, 6, 3, 3, 6, \ldots).$$

The 2-part sequence derived from u is $(1, 1, 2, 1, 1, 2, \ldots)$, which is not realizable by Lemma 1.2.7 since $3 \nmid 2 - 1$. Hence u is not everywhere locally realizable.

We will consider this simple example in more depth later.

1.4. Lehmer-Pierce Sequences

In 1933, D.H. Lehmer published a paper [**17**] in which he made use of a construction previously studied by T.A. Pierce [**21**] in 1917. This construction results in a sequence of integers and is defined as follows.

Let $F \in \mathbb{Z}[x]$ denote a monic polynomial with factorization over $\mathbb{C}$,

$$F(x) = (x - \alpha_1) \cdots (x - \alpha_d), \quad d = \partial(F) \geq 1.$$

The *Lehmer-Pierce* sequence $(\Delta_n(F))$ is given by the equation:

$$\Delta_n(F) = \prod_{k=1}^{d} |\alpha_k^n - 1|, \quad n \geq 1. \tag{1.4}$$

It is easy to see that $(\Delta_n(F))$ is a sequence of non-negative integers since $\Delta_n(F)$ is a symmetric function of the zeros of F. What is more, it is a *divisibility* sequence in the sense that if $m \mid n$, then $\Delta_n(F)$ is a multiple of $\Delta_m(F)$. This can be seen from the fact that the polynomial $x^m - 1$ is a factor of the polynomial $x^n - 1$ when $m \mid n$.

Examples 1.4.1. Let $F \in \mathbb{Z}[x]$ be the monic polynomial defined by $F(x) = x^2 - x - 1$. If the zeros of F are α_1, α_2, then using $\alpha_1 + \alpha_2 = 1$ and $\alpha_1\alpha_2 = -1$, we easily obtain

$$(\Delta_n(F)) = (1, 1, 4, 5, 11, 16, 29, 45, 76, 121, 199, 320, 521, 841, 1364 \ldots).$$

Writing $u = (u_n) = (\Delta_n(F))$ we note that at least for the number of terms shown, Lemma 1.2.4 shows that u is a realizable sequence. Also we note that the terms of u satisfy the linear recurrence relation

$$u_{n+4} = u_{n+3} + 2u_{n+2} - u_{n+1} - u_n;\ u_1 = 1, u_2 = 1, u_3 = 4, u_4 = 5.$$

Let $f \in \mathbb{Z}[x]$ denote the polynomial $f(x) = x + 2$. The Lehmer-Pierce sequence $(\Delta_n(f))$, usually known as the Jacobstal-Lucas sequence, is:

$$(|(-2)^n - 1|) = (3, 3, 9, 15, 33, 63, 129, 255, 513, 1023, \ldots).$$

If the polynomial $g \in \mathbb{Z}[x]$ is given by $g(x) = x^2 - 2x + 2$, then the Lehmer-Pierce sequence $(\Delta_n(g))$ is calculated as

$$([(1+i)^n - 1][(1-i)^n - 1]) = (1, 5, 13, 25, 41, 65, 113, 225, 481, 1025, \ldots).$$

When the monic polynomial $F \in \mathbb{Z}[x]$ is such that no zero of F is a root of unity, it is known that the Lehmer-Pierce sequence $(\Delta_n(F))$ is realizable, arising from the action of an endomorphism on an abelian group. This will be shown to be the case in Chapter 4.

CHAPTER 2

New Realizable Sequences

In this chapter, various ways of obtaining new realizable sequences from existing ones are considered. The first section presents some general means of obtaining realizable sequences from an existing realizable sequence. The second section is concerned with the realizability of certain subsequences of a realizable sequence. The main methods of proof employed in this chapter are combinatoric arguments in conjunction with Lemma 1.2.4.

2.1. Generating New Sequences

Given a realizable sequence $u = (u_n)$, by definition there exists a system (X, T) such that $u_n = |\operatorname{Per}_n(T)|$ for all positive integers n. This system (or its implied existence) can be utilized to construct new sequences. For example, we have the following easy result as a way of introduction.

Proposition 2.1.1. *Let m denote a positive integer and $\{k_1, \ldots, k_m\}$ a set of positive integers. If $u = (u_n)$ is a realizable sequence, then the sequence $v = (v_n)$ with terms given by*

$$v_n = u_{k_1 n} u_{k_2 n} \cdots u_{k_m n}, \quad n = 1, 2, 3, \ldots$$

is realizable.

Proof. If the sequence u is realized by the system (X, T) then the sequence v is realized by (W, S) where $W = X^m$ and $S : W \to W$ is the map $T^{k_1} \times T^{k_2} \times \cdots \times T^{k_m}$. □

Corollary 2.1.2. *If m denotes a fixed positive integer and (u_n) a realizable sequence, then the sequence (u_n^m) is realizable.*

Proof. Let $k_1 = k_2 = \cdots = k_m = 1$ in Proposition 2.1.1. □

We now establish results which provide a generalization of Corollary 2.1.2 in that the constant integer m is shown to be replaceable by certain integer polynomial functions of n.

Lemma 2.1.3. *Let (u_n) be a realizable sequence and p a prime. If r and m denote positive integers with $p \nmid m$, then*

$$u_{p^r m} \equiv u_{p^{r-1}m} \pmod{p^r}.$$

Proof. To shorten the proof we will quote a simple result proved in Proposition 2.2.1 of the next section: the sequence $(u_{mn})_{n\geq 1}$ is realizable. Using this and Lemma 1.2.4, we get

$$p^r \mid \sum_{d|p^r} \mu(p^r/d)u_{md},$$

from which the result easily follows. □

Theorem 2.1.4. *If $u = (u_n)$ is a realizable sequence, then the sequence (u_n^n) is also realizable.*

Proof. Define the sequence $v = (v_n)$ by $v_n = u_n^n$ for $n = 1, 2, 3, \ldots$. We will prove that v is a realizable sequence by showing that it possesses both divisibility and positivity. To this end, for each $n \geq 1$, we will write

$$v_n^* = \sum_{d|n} \mu(n/d)v_d = \sum_{d|n} \mu(n/d)u_d^d.$$

Fix the value of the integer n: since $v_1^* = u_1$ we can suppose that $n > 1$.

We begin by establishing that v has divisibility. Let p denote a prime, and r a positive integer where $p^r \parallel n$; put $n = p^r m$, so that

$$v_n^* = \sum_{d|p^r m} \mu(p^r m/d)v_d = \sum_{d|m} \mu(m/d)(v_{p^r d} - v_{p^{r-1}d}).$$

Now,

$$v_{p^r d} - v_{p^{r-1}d} = u_{p^r d}^{p^r d} - u_{p^{r-1}d}^{p^{r-1}d} = (u_{p^r d}^{p^r d} - u_{p^{r-1}d}^{p^r d}) + (u_{p^{r-1}d}^{p^r d} - u_{p^{r-1}d}^{p^{r-1}d}),$$

and examination of each of the bracketed terms in this expression gives, firstly:

$$u_{p^r d}^{p^r d} - u_{p^{r-1}d}^{p^r d} = (u_{p^r d} - u_{p^{r-1}d})K$$

for some integer K, so by Lemma 2.1.3, $p^r \mid u_{p^r d}^{p^r d} - u_{p^{r-1}d}^{p^r d}$. Next we have, on writing $a = u_{p^{r-1}d}^{d}$

$$u_{p^{r-1}d}^{p^r d} - u_{p^{r-1}d}^{p^{r-1}d} = a^{p^{r-1}}(a^{\varphi(p^r)} - 1),$$

where φ is the Euler φ-function. If $p \nmid a$ then by the Euler-Fermat Theorem,

$$u_{p^{r-1}d}^{p^r d} - u_{p^{r-1}d}^{p^{r-1}d} \equiv 0 \pmod{p^r};$$

while if $p \mid a$,

$$p^{p^{r-1}d} \,\Big|\, u_{p^{r-1}d}^{p^r d} - u_{p^{r-1}d}^{p^{r-1}d},$$

from which it is easy to see that we also get

$$u_{p^{r-1}d}^{p^r d} - u_{p^{r-1}d}^{p^{r-1}d} \equiv 0 \pmod{p^r}.$$

By combining these results, $p^r \mid v_n^*$, and it follows immediately that the sequence v has divisibility.

To prove that v has positivity, first we note that by the definition of a realizable sequence, if $d \mid n$ then $u_d \leq u_n$. Hence, if $u_n \leq 1$ then $u_d^d = u_d$ for all $d \mid n$. It follows therefore, that if the sequence u is such that $u_n \leq 1$, then

$$v_n^* = \sum_{d \mid n} \mu(n/d) u_d \geq 0$$

because u has positivity. Now suppose that $u_n > 1$. Then

$$v_n^* = u_n^n + \sum_{\substack{d \mid n \\ d \neq n}} \mu(n/d) u_d^d \geq u_n^n - \sum_{\substack{d \mid n \\ d \neq n}} u_d^d,$$

and so

$$v_n^* \geq u_n^n - \sum_{k=1}^{\lfloor n/2 \rfloor} u_n^k.$$

This gives

$$v_n^* \geq u_n^n - \frac{u_n(u_n^{\lfloor n/2 \rfloor} - 1)}{u_n - 1} \geq u_n^n - u_n^{1+\lfloor n/2 \rfloor} \geq 0,$$

and therefore the sequence v does have positivity. Lemma 1.2.4 completes the proof. □

Corollary 2.1.5. *Let a, k denote fixed non-negative integers, and (u_n) a realizable sequence. Then the sequence $(u_n^{an^k})_{n \geq 1}$ is realizable.*

Proof. If $a = 0$ this is trivial, so we assume $a \geq 1$. Next, the case $k = 0$ follows from Corollary 2.1.2, so we also suppose that $k \geq 1$. The proof is now completed by first noting that the sequence (u_n^a) is realizable by Corollary 2.1.2, and then using Theorem 2.1.4 inductively. □

Corollary 2.1.6. *If h denotes a polynomial from $\mathbb{N}_0[x]$ and (u_n) is a realizable sequence, then the sequence $(u_n^{h(n)})$ is realizable.*

Proof. If h is the zero polynomial this is trivial. Otherwise, suppose that $h(x) = c_d x^d + \cdots + c_0$, where $d \geq 0$, $c_0, \ldots, c_d \geq 0$ and $c_d \neq 0$. Then

$$u_n^{h(n)} = u_n^{c_d n^d} \cdots u_n^{c_1 n} u_n^{c_0},$$

and so, from the previous Corollary, we see that the sequence $(u_n^{h(n)})$ is a product of realizable sequences. Proposition 1.2.8 completes the proof. □

2.2. Realizable Subsequences

In this section we show that the realizability of a sequence extends to certain subsequences. The arguments used are mainly of a combinatoric nature, because in most cases the results seem not to be easily accessible from properties of the realizing systems. However, this is certainly not the case for the first (essentially trivial) result which is well known and is included just for the sake of completeness.

Proposition 2.2.1. *Let $u = (u_n)$ denote a realizable sequence, and let c denote a positive integer. If the subsequence $v = (v_n)$ of u is defined for each integer $n \geq 1$ by $v_n = u_{cn}$, then v is a realizable sequence.*

Proof. This follows immediately from Proposition 2.1.1. □

The aim now is to replace the constant c in Proposition 2.2.1 by a non-constant function of n. Examples quickly demolish the use of elaborate functions – though there may be some remaining. The main result of this section follows, and it shows that we are able to replace c by a simple polynomial multiplier of the form cn^{k-1}. In contrast to Proposition 2.1.1, this does not seem to be readily proved by a construction using the realizing maps. It would appear to be an inherently more subtle result.

Theorem 2.2.2. *Let $u = (u_n)$ denote a realizable sequence, and let k be a positive integer. If the sequence $v = (v_n)$ is defined by*

$$v_n = u_{n^k}, \quad n = 1, 2, 3, \dots,$$

then v is also a realizable sequence.

Proof. Let $n \in \mathbb{N}$ be such that $n > 1$ and let the distinct prime divisors of n be $p_1, \dots, p_r$, so that $n = p_1^{s_1} \cdots p_r^{s_r}$ for some integers $s_1, \dots, s_r \geq 1$. Then,

$$v_n^* = \sum_{d|n} \mu(n/d) v_d = v_n - \sum_{p_i} v_{n/p_i} + \sum_{p_i, p_j} v_{n/p_i p_j} + \cdots + (-1)^r v_{n/p_1 \cdots p_r},$$

where $p_i, p_j, \dots$ are distinct members of the set $\{p_1, \dots, p_r\}$. It follows that

$$v_n^* = u_{n^k} - \sum_{p_i} u_{n^k/p_i^k} + \sum_{p_i, p_j} u_{n^k/p_i^k p_j^k} + \cdots + (-1)^r u_{n^k/p_1^k \cdots p_r^k}. \tag{2.1}$$

Set $b = n^k/p_1^{k-1}\cdots p_r^{k-1}$; then $n \mid b$. Next define the integer E by

$$E = \sum_{\substack{m|n^k \\ b|m}} \sum_{d|m} \mu(m/d)u_d. \tag{2.2}$$

Now, for each $m \mid n^k$ where $b \mid m$, since (u_n) is a realizable sequence, Lemma 1.2.4 implies that

$$\sum_{d|m} \mu(m/d)u_d \geq 0 \text{ and } m \mid \sum_{d|m} \mu(m/d)u_d.$$

It follows that $E \geq 0$ and $n \mid E$, so by Lemma 1.2.4 it is sufficient to establish that $E = v_n^*$.

Let $m \mid n^k$ with $b \mid m$. Then the form of m is

$$m = p_1^{k(s_1-1)+j_1}\cdots p_r^{k(s_r-1)+j_r},$$

where the integers $j_1, \dots, j_r$ satisfy $1 \leq j_1, \dots, j_r \leq k$. Using this and (2.2), express the integer E as

$$E = \sum_{j_1=1}^{k} \cdots \sum_{j_r=1}^{k} \sum_{d|m} \mu(d)u_{m/d}, \tag{2.3}$$

where in this equation $m = p_1^{k(s_1-1)+j_1}\cdots p_r^{k(s_r-1)+j_r}$.

Let $m_1 = m/p_1^{k(s_1-1)+j_1}$: that is, $m_1 = p_2^{k(s_2-1)+j_2}\cdots p_r^{k(s_r-1)+j_r}$. Then

$$\sum_{d|m} \mu(d)u_{m/d} = \sum_{d|m_1} \mu(d)(u_{m/d} - u_{m/p_1 d}),$$

and so, because m_1 is independent of j_1,

$$\sum_{j_1=1}^{k} \sum_{d|m} \mu(d)u_{m/d} = \sum_{d|m_1} \sum_{j_1=1}^{k} \mu(d)(u_{m/d} - u_{m/p_1 d}),$$

which gives

$$\sum_{j_1=1}^{k} \sum_{d|m} \mu(d)u_{m/d} = \sum_{d|m_1} \mu(d)(u_{p_1^{ks_1}m_1/d} - u_{p_1^{k(s_1-1)}m_1/d}).$$

It follows from (2.3) that

$$E=\sum_{j_2=1}^{k}\cdots\sum_{j_r=1}^{k}\sum_{d|m_1}\mu(d)(u_{p_1^{ks_1}m_1/d}-u_{p_1^{ks_1}m_1/p_1^kd}),$$

where $m_1=p_2^{k(s_2-1)+j_2}\cdots p_r^{k(s_r-1)+j_r}$. Repeating the above procedure, first setting $m_2=m_1/p_2^{k(s_2-1)+j_2}$, gives $E=E_1-E_2$ where

$$E_1=\sum_{j_3=1}^{k}\cdots\sum_{j_r=1}^{k}\sum_{d|m_2}\mu(d)(u_{p_1^{ks_1}p_2^{ks_2}m_2/d}-u_{p_1^{ks_1}p_2^{ks_2}m_2/p_2^kd})$$

and

$$E_2=\sum_{j_3=1}^{k}\cdots\sum_{j_r=1}^{k}\sum_{d|m_2}\mu(d)(u_{p_1^{ks_1}p_2^{ks_2}m_2/p_1^kd}-u_{p_1^{ks_1}p_2^{ks_2}m_2/p_1^kp_2^kd}).$$

Continuing in this fashion, comparing each expression obtained with that of (2.1), shows that $E=v_n^*$. □

Corollary 2.2.3. *Let $u=(u_n)$ be a realizable sequence, and let c,k denote fixed positive integers. If the subsequence $v=(v_n)$ of u is defined by*

$$v_n=u_{cn^k},\quad n=1,2,3,\ldots,$$

then v is a realizable sequence.

Proof. This follows from Proposition 2.2.1 and Theorem 2.2.2. □

Corollary 2.2.4. *If a and k denote positive integers, then the sequence $(a^{n^k})_{n\geq1}$ is realizable.*

Proof. By Proposition 1.2.3 the sequence (a^n) is realizable. So the result is an immediate consequence of Theorem 2.2.2. □

Corollary 2.2.5. *Let a denote a positive integer and h a polynomial from $\mathbb{N}_0[x]$. Then the sequence $(a^{h(n)})$ is realizable.*

Proof. If h is the zero polynomial this is trivial. Otherwise, suppose that $h(x)=c_dx^d+\cdots+c_0$, where $d\geq0$, $c_0,\ldots,c_d\geq0$ and $c_d\neq0$. If we put $a_r = a^{c_r}$, $r = 0, \ldots, d$, then

$$a^{h(n)} = a_d^{n^d} \cdots a_1^n a_0,$$

and so, from the previous Corollary, we see that the sequence $(a^{h(n)})$ is a product of realizable sequences. It follows from Proposition 1.2.8, therefore, that $(a^{h(n)})$ is realizable. □

We note that the previous two Corollaries could equally well have come from Theorem 2.1.4.

The *Lucas sequence* $(L_n) = (1, 3, 4, 7, 11, 18, \ldots)$ is shown to be realizable in [**22**]. When $h(n) = n^2 + n$ we get

$$(L_{h(n)})_{n \geq 1} = (3, 18, \ldots), \tag{2.4}$$

and Lemma 1.2.7 with $p = 2$, immediately shows that (2.4) is not a realizable sequence. So Corollary 2.2.5 does not extend to arbitrary realizable sequences.

We end this chapter with a problem, the solution of which would be very interesting, not only in its own right, but also because it could provide information relating to sequences realized by the action of an endomorphism on a group.

Problem 2.2.6. Give non-combinatoric proofs of Theorem 2.1.4 and Theorem 2.2.2, by using constructions based on a realizing system (X, T) for the sequence $u = (u_n)$ in each case.

CHAPTER 3

Periodic Points from Group Endomorphisms

In this chapter, the arithmetic structure of sequences realized by endomorphisms of groups is studied, with particular emphasis being placed on the class of locally nilpotent groups.

3.1. Group Endomorphisms

Certain realizable sequences are known to be realized by systems (X, ψ) where X is a group and $\psi : X \to X$ is an endomorphism: such systems will be called *algebraic systems*. A sequence which is realized by an algebraic system will be said to be *algebraically realizable*. When it is necessary to distinguish between abelian and non-abelian groups, the algebraic systems will be called *abelian systems* or *non-abelian systems*. Being realized in this fashion imparts a considerable amount of structure to the sequence, as we shall demonstrate in this chapter. First we introduce the notion of a divisibility sequence, not to be confused with a sequence having divisibility, introduced in Definition 1.2.6. If $u = (u_n)$ is a sequence of non-zero integers then u is a *divisibility sequence* if for any integers $m, n \geq 1$, $m \mid n$ implies $u_m \mid u_n$. A well known example of a divisibility sequence is the *Fibonacci sequence* $(1, 1, 2, 3, 5, 8, \ldots)$. However, Lemma 1.2.7 proves that this sequence is not realizable. On the other hand, Proposition 3.1.2 below, shows that sequences realized by algebraic systems provide an unlimited supply of divisibility sequences.

Lemma 3.1.1. *Let the sequence $u = (u_n)$ be realized by the algebraic system (X, ψ). Then for each integer $n \geq 1$, $\mathrm{Per}_n(\psi)$ is a finite ψ-invariant subgroup of X.*

Proof. If $x, y \in \operatorname{Per}_n(\psi)$ then $\psi^n(xy) = \psi^n(x)\psi^n(y) = xy$ and so $xy \in \operatorname{Per}_n(\psi)$. Also, $\psi^n(x^{-1}) = (\psi^n(x))^{-1} = x^{-1}$, so $x^{-1} \in \operatorname{Per}_n(\psi)$. It follows that $\operatorname{Per}_n(\psi)$ is a subgroup of X: it is a finite subgroup since by the definition of a realizable sequence, $|\operatorname{Per}_n(\psi)| = u_n < \infty$. Lastly, since $\psi^n(x) = x$, we have $\psi^n(\psi(x)) = \psi(x)$, so $\psi(x) \in \operatorname{Per}_n(\psi)$; hence the subgroup $\operatorname{Per}_n(\psi)$ is ψ-invariant. □

Proposition 3.1.2. *If the sequence u is realized by the algebraic system (X, ψ) then u is a divisibility sequence.*

Proof. Let the integers $m, n \geq 1$ have $m \mid n$, so $n = mk$ for some integer $k \geq 1$. Then if $x \in \operatorname{Per}_m(\psi)$,

$$\psi^n(x) = \psi^{mk}(x) = (\psi^m)^k(x) = x,$$

so $\operatorname{Per}_m(\psi) \leq \operatorname{Per}_n(\psi)$. But $\operatorname{Per}_m(\psi)$, $\operatorname{Per}_n(\psi)$ are finite subgroups of X by Lemma 3.1.1, so Lagrange's Theorem gives $|\operatorname{Per}_m(\psi)| \,\big|\, |\operatorname{Per}_n(\psi)|$, establishing that u is a divisibility sequence. □

For sequences realized by algebraic systems, the following result enables a simplification when dealing with *bounded* sequences, while also providing information relating to other sequences in this class.

Lemma 3.1.3. *Suppose that the sequence $u = (u_n)$ is realized by the algebraic system (W, ϑ). Then u can be realized by an algebraic system (X, α) where X is a countable locally finite group and $\alpha \in \operatorname{Aut}(X)$. Further, if the sequence u is bounded, and m is the least positive integer so that $u_m = \max\{u_n : n \geq 1\}$, the system (X, α) can be selected with $|X| = u_m$, while the automorphism α has $o(\alpha) = m$.*

Proof. Let $X = \bigcup_{n\geq 1} \operatorname{Per}_n(\vartheta)$. If $x, y \in X$, there are positive integers m, n with $x \in \operatorname{Per}_m(\vartheta)$ and $y \in \operatorname{Per}_n(\vartheta)$; put $r = \operatorname{lcm}(m, n)$. Then $\operatorname{Per}_m(\vartheta), \operatorname{Per}_n(\vartheta) \leq \operatorname{Per}_r(\vartheta)$, so $x, y \in \operatorname{Per}_r(\vartheta)$. By Lemma 3.1.1, $\operatorname{Per}_r(\vartheta)$ is a subgroup of W so $xy, x^{-1} \in \operatorname{Per}_r(\vartheta)$. Hence, $xy, x^{-1} \in X$ and therefore X is a subgroup of W. Next, since $\operatorname{Per}_n(\vartheta)$ is ϑ-invariant for each $n \geq 1$, X is ϑ-invariant. Therefore if $\alpha : X \to X$ is given by $\alpha : x \mapsto \vartheta(x)$ for all $x \in X$, α is an endomorphism on X, and it is clear that the system (X, α) realizes the sequence u, with $\mathrm{Per}_n(\alpha) = \mathrm{Per}_n(\vartheta)$.

Let $x_1, \ldots, x_k$ be a finite set of elements from X. There are positive integers $n_1, \ldots, n_k$ so that $x_j \in \mathrm{Per}_{n_j}(\alpha)$, for $j = 1, \ldots, k$. If $s = \mathrm{lcm}(n_1, \ldots, n_k)$ then $x_1, \ldots, x_k \in \mathrm{Per}_s(\alpha)$, so $\langle x_1, \ldots, x_k \rangle \leq \mathrm{Per}_s(\alpha)$, since $\mathrm{Per}_s(\alpha)$ is a group. And because $\mathrm{Per}_s(\alpha)$ is a finite group by Lemma 3.1.1, $|\langle x_1, \ldots, x_k \rangle| < \infty$. Therefore X is locally finite. Now, if $x \in X$ is such that $\alpha(x) = 1$, since $x \in \mathrm{Per}_n(\alpha)$ for some $n > 1$,

$$x = \alpha^n(x) = \alpha^{n-1}(\alpha(x)) = \alpha^{n-1}(1) = 1.$$

It follows that $\ker(\alpha) = 1$, and since it is clear that $\alpha : X \to X$ is onto, α is an automorphism.

Next, let u be bounded and choose m as in the statement of the Lemma. If the integer $n \geq 1$ exists with $\mathrm{Per}_n(\alpha) \nleq \mathrm{Per}_m(\alpha)$ then $\mathrm{Per}_m(\alpha) \subsetneqq \mathrm{Per}_m(\alpha) \cup \mathrm{Per}_n(\alpha)$ which implies $\mathrm{Per}_m(\alpha) \lneqq \mathrm{Per}_r(\alpha)$, where $r = \mathrm{lcm}(m, n)$. But this gives $u_m < u_r$, a contradiction. Hence, $\mathrm{Per}_n(\alpha) \leq \mathrm{Per}_m(\alpha)$ for all $n \geq 1$. So, in this case, $X = \mathrm{Per}_m(\alpha)$ which gives $\alpha^m(x) = x$ for all $x \in X$: therefore, $o(\alpha) = m$.

Lastly, since X is the countable union of *finite* sets, it is clear that the group X is countable. □

Proposition 3.1.2 showed that for a realizable sequence u to be realized by an algebraic system (X, ϑ), it is necessary that u be a divisibility sequence. The next example shows this is *not* a sufficient condition.

Example 3.1.4. The sequence $u = (1, 1, 1, 1, 6, 1, 1, 1, 1, 6, \ldots)$, which satisfies the linear recurrence relation

$$u_{n+5} = u_n,\ n \geq 1;\ u_1 = u_2 = u_3 = u_4 = 1, u_5 = 6,$$

is a realizable divisibility sequence which is not realizable by an algebraic system (X, ϑ).

First, it is clear that u is a divisibility sequence. Next, the permutation $(1\,2\,3\,4\,5)$ acting on the set $\{1, 2, 3, 4, 5, 6\}$ establishes that u is realizable. However, if there is an algebraic system (X, ϑ) which realizes u, Lemma 3.1.3 allows us to assume that $|X| = 6$, ϑ is an automorphism and $\vartheta^5 = \iota_X$. For any $x \in X$ not equal to the identity element, suppose that there are integers m, n such that $0 \leq m < n \leq 4$ and $\vartheta^m(x) = \vartheta^n(x)$. Since ϑ is an automorphism, this gives $\vartheta^{n-m}(x) = x$, so by the structure of the sequence u, $x \in \mathrm{Fix}(\vartheta)$. Therefore x is the identity, a contradiction. Hence $\mathrm{Orb}_\vartheta(x) = \{x, \vartheta(x), \vartheta^2(x), \vartheta^3(x), \vartheta^4(x)\}$, consists of 5 distinct elements, all of the same order. Since this is not possible, the sequence u is not realizable by an algebraic system.

In the next Section, Theorem 3.2.11 provides an arithmetical explanation for the previous example.

3.2. Endomorphisms of Locally Nilpotent Groups

We now introduce a class of algebraic systems which strictly contains the abelian systems. Call (X, ϑ) a *nilpotent system* if X is a *locally nilpotent* group and $\vartheta : X \to X$ an endomorphism. An important property of a locally nilpotent group X follows from Theorem 1.1.5: if F is a *finite* subgroup of X, then the Sylow p-subgroups of F are unique. We make the following definitions in order to simplify terminology.

Definition 3.2.1. The sequence $u = (u_n)$ is *nilpotently realizable* if there is a *nilpotent* system (X, ϑ) which realizes u. Also, if there exists a nilpotent system which realizes the sequence of p-parts of u for some prime p, we say that the sequence u is *locally nilpotently realizable* at p; a sequence which is locally nilpotently realizable at all primes is *everywhere locally nilpotently realizable.*

The following are examples of sequences which are nilpotently realized. The first is realized by an abelian system.

Example 3.2.2. The *Mersenne sequence* $(2^n-1)_{n\geq 1}$ is realized by the action of the endomorphism $\vartheta : x \mapsto x^2$ on the circle group $\mathbb{S}^1$. This sequence (and its close relatives) serves as a test-example for many workers in the theory of dynamical systems.

The next example shows that it is possible to have a sequence which is realized by a nilpotent system, but not by an abelian system.

Example 3.2.3. Let $X = D_8$, the dihedral group of order 8. Since X is a finite p-group (with $p = 2$), X is nilpotent by Theorem 1.1.4. A presentation for X is

$$X = \langle a, b : a^4 = 1,\ b^2 = 1,\ a^b = a^{-1}\rangle.$$

Using this presentation, let $\alpha : X \to X$ be the map given by the following table

x	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\alpha(x)$	1	a	a^2	a^3	ab	a^2b	a^3b	b

It is easy to see that α is an (outer) automorphism and that the sequence realized by the nilpotent system (X, α) is

$$u = (4, 4, 4, 8, 4, 4, 4, 8, \ldots). \tag{3.1}$$

We will show that the sequence u of (3.1) is not realizable by an abelian system. Assume the contrary, so there is an abelian group W and an endomorphism $\psi : W \to W$ such that u is realized by the system (W, ψ). By Lemma 3.1.3, we can assume that $|W| = 8$ and that ψ is an automorphism where

$$\operatorname{Fix}(\psi) = \operatorname{Per}_2(\psi) = \operatorname{Per}_3(\psi),\ |\operatorname{Fix}(\psi)| = 4 \text{ and } \psi^4 = \iota_W.$$

The quotient group $W/\operatorname{Fix}(\psi)$ has order 2: therefore if $x \in W \setminus \operatorname{Fix}(\psi)$,

$$W/\operatorname{Fix}(\psi) = \{0 + \operatorname{Fix}(\psi), x + \operatorname{Fix}(\psi)\}.$$

This implies that $2x \in \operatorname{Fix}(\psi)$, and since $|\operatorname{Fix}(\psi)| = 4$,

$$W \setminus \operatorname{Fix}(\psi) = \{x + f : f \in \operatorname{Fix}(\psi)\}. \tag{3.2}$$

Consider the orbit of x under ψ,

$$\operatorname{Orb}_\psi(x) = \{\psi^n(x) : n = 0, 1, 2, \ldots\}.$$

Since $\psi^4 = \iota_W$, $\operatorname{Orb}_\psi(x) = \{x, \psi(x), \psi^2(x), \psi^3(x)\}$. We claim that the four elements of $\operatorname{Orb}_\psi(x)$ are distinct, and that $\operatorname{Fix}(\psi) \cap \operatorname{Orb}_\psi(x) = \emptyset$. To see this, first suppose that $\psi^n(x) \in \operatorname{Fix}(\psi)$ for some integer n, $0 < n \leq 3$. Then $\psi^{n+1}(x) = \psi^n(x)$, so, because ψ is an automorphism, $\psi(x) = x$ implying $x \in \operatorname{Fix}(\psi)$, a contradiction. Next assume that $\psi^k(x) = \psi^m(x)$ for integers k, m where $0 \leq k < m \leq 3$: put $n = m - k$, so that $0 < n \leq 3$. Since ψ is an automorphism, this gives $\psi^n(x) = x$, contradicting the above. Therefore $\operatorname{Orb}_\psi(x)$ consists of four distinct elements from $W \setminus \operatorname{Fix}(\psi)$. Using this and (3.2) gives $\psi(x) = x + f$ for some $f \in \operatorname{Fix}(\psi)$. Since $2x \in \operatorname{Fix}(\psi)$,

$$2x = \psi(2x) = 2\psi(x) = 2x + 2f,$$

giving $2f = 0$, and since x and $\psi^2(x)$ are distinct members of $\operatorname{Orb}_\psi(x)$,

$$x \neq \psi^2(x) = \psi(x + f) = x + f + f = x.$$

This contradiction establishes that the sequence u is not realizable by an abelian system.

A particular class of sequences plays an important role in the considerations of nilpotently realizable sequences: we single this class out in the following.

Definition 3.2.4. For a fixed prime p, (u_n) is called a *p-sequence* if for all $n \geq 1$, $u_n = p^{k_n}$, where each $k_n \in \mathbb{N}_0$.

Lemma 3.2.5. *Let p denote a prime and suppose that the p-sequence $u = (u_n)$ is realized by the algebraic system (X, α). If*

$$X = \bigcup_{n \geq 1} \mathrm{Per}_n(\alpha),$$

then X is a countable, locally finite p-group. In particular, X is a locally nilpotent group.

Proof. We already know that X is a countable, locally finite group by Lemma 3.1.3. Suppose that $x \in X$ has order not a power of p. Since X is locally finite, this implies that there is a prime $q \neq p$ such that $q \mid o(x)$. Now $x \in \mathrm{Per}_n(\alpha)$ for some $n \geq 1$, so $q \mid |\mathrm{Per}_n(\alpha)|$. Therefore $q \mid u_n$, which contradicts the fact that u is a p-sequence. Hence, X is a p-group.

Any finitely generated subgroup H of X is a finite subgroup because X is locally finite, and since a finite p-group is nilpotent by Theorem 1.1.4, H is a nilpotent subgroup. Therefore, X is locally nilpotent. □

Lemma 3.2.6. *Suppose that the group G is given by the cartesian product*

$$G = \prod_p G_p,$$

where this product is taken over all primes p and each G_p is a locally finite p-group. If the subgroup X of G is locally finite then X is locally nilpotent.

Proof. Let $x = (x_p) \in X$. Since X is locally finite, $o(x) < \infty$: let $k = o(x)$. For each prime p we have $x_p^k = 1$ so $o(x_p) \mid k$. But since $x_p \in G_p$, $o(x_p)$ is a power of p, which implies that $x_p = 1$ for all but a finite number of primes p. Let

$$\mathrm{supp}(x) = \{x_p : x = (x_p) \in X, \, o(x_p) > 1\},$$

so that $\operatorname{supp}(x)$ is a finite (possibly empty) set for all $x \in X$. If $x^{(1)}, \ldots, x^{(m)}$ is a finite set of elements from X, put $S = \bigcup_{r=1}^{m} \operatorname{supp}(x^{(r)})$, and for each prime p define the subgroup X_p of G_p by $X_p = \langle S \cap G_p \rangle$, where we interpret this to mean that $X_p = 1$ if $S \cap G_p = \emptyset$. Since S is a finite set and G_p is a locally finite p-group, X_p is nilpotent. It is clear that we have $\langle x^{(1)}, \ldots, x^{(m)} \rangle = \prod_p X_p$, and because there are only a finite number of non-trivial groups in this product, $\langle x^{(1)}, \ldots, x^{(m)} \rangle$ is nilpotent. Therefore, X is locally nilpotent. □

The next result is a reworking of Proposition 1.3.1.

Proposition 3.2.7. *If the sequence $u = (u_n)$ is everywhere locally nilpotently realizable then u is nilpotently realizable.*

Proof. For each prime p there is a locally nilpotent group X_p with an endomorphism $\vartheta_p : X_p \to X_p$ such that (X_p, ϑ_p) nilpotently realizes the sequence of p-parts $([u_n]_p)_{n \geq 1}$. Without loss of generality we may assume that $X_p = \bigcup_{n \geq 1} \operatorname{Per}_n(\vartheta_p)$. Since the algebraic system (X_p, ϑ_p) realizes a p-sequence, Lemma 3.2.5 gives X_p is a locally finite p-group. Define the group G by $G = \prod_p X_p$, and the endomorphism $\psi : G \to G$ to be the corresponding product $\psi = \prod_p \vartheta_p$. Then as in Proposition 1.3.1, the algebraic system (G, ψ) realizes the sequence u.

Let X denote the subgroup of G, $X = \bigcup_{n \geq 1} \operatorname{Per}_n(\psi)$, and let $\alpha : X \to X$ be given by $\alpha : x \mapsto \psi(x)$, $x \in X$. Then by Lemma 3.1.3, X is a locally finite subgroup of G and so Lemma 3.2.6 implies that X is locally nilpotent. Since we know from Lemma 3.1.3 that u is realized by the nilpotent system (X, α), we have u is nilpotently realizable. □

Lemma 3.2.8. *Let G represent a group and p a prime. If G has a unique Sylow p-subgroup P then any subgroup $H \leq G$ has a unique Sylow p-subgroup given by $P \cap H$.*

Proof. We may clearly assume that G is not a p-group. Suppose that K is any p-subgroup of G. Because of the uniqueness of P we have

$P \trianglelefteq G$ so $P \leq PK \leq G$. But PK is a p-subgroup of G, and therefore by the maximality of Sylow subgroups, and the assumption that G is not a p-group, we get $PK = P$. Hence, $K \leq P$. Now let $H \leq G$; any Sylow p-subgroup of H is contained in P by the argument just given so $H \cap P$ is the unique Sylow p-subgroup of H. □

Theorem 3.2.9. *If the sequence $u = (u_n)$ is realized by the algebraic system (X, α) where the group X has a unique Sylow p-subgroup for some prime p then u is locally nilpotently realizable at p.*

Proof. By Lemmas 3.1.3 and 3.2.8, we can assume $X = \bigcup_{n \geq 1} \mathrm{Per}_n(\alpha)$ so that X is locally finite and $\alpha : X \to X$ an automorphism. If P is the unique Sylow p-subgroup of X then because X is locally finite, any finitely generated subgroup of P is a finite p-group, so is nilpotent. Hence P is locally nilpotent. Further, P is α-invariant so we can restrict the domain of α to P. Let $\beta : P \to P$ be defined by $\beta : x \mapsto \alpha(x)$ for all $x \in P$. Then β is an automorphism on P and we can consider the nilpotent system (P, β): we will show that this system realizes the sequence of p-parts of the sequence u.

For any $n \geq 1$, if $x \in \mathrm{Per}_n(\beta)$ then $x = \beta^n(x) = \alpha^n(x)$, so $x \in \mathrm{Per}_n(\alpha)$. Hence $\mathrm{Per}_n(\beta) \leq \mathrm{Per}_n(\alpha)$ and therefore, by Lagrange's Theorem, $|\mathrm{Per}_n(\beta)| \mid |\mathrm{Per}_n(\alpha)|$. Now, $\mathrm{Per}_n(\beta)$ is a finite subgroup of the p-group P, so $|\mathrm{Per}_n(\beta)|$ is a power of p; therefore $|\mathrm{Per}_n(\beta)| \mid [u_n]_p$. If for some $n \geq 1$, $|\mathrm{Per}_n(\beta)| \neq [u_n]_p$, then $p \mid [u_n]_p / |\mathrm{Per}_n(\beta)|$ so $p \mid |\mathrm{Per}_n(\alpha) : \mathrm{Per}_n(\beta)|$. This implies that $\mathrm{Per}_n(\beta)$ is not a Sylow p-subgroup of $\mathrm{Per}_n(\alpha)$ and so by Lemma 3.2.8, $\mathrm{Per}_n(\beta) \neq P \cap \mathrm{Per}_n(\alpha)$. However, if $x \in P \cap \mathrm{Per}_n(\alpha)$, since $x \in P$, $\alpha^n(x) = \beta^n(x)$ so we get $x \in \mathrm{Per}_n(\beta)$ implying that $\mathrm{Per}_n(\beta) = P \cap \mathrm{Per}_n(\alpha)$. This contradiction means that for all $n \geq 1$, $|\mathrm{Per}_n(\beta)| = [u_n]_p$ and so the system (P, β) nilpotently realizes the sequence $([u_n]_p)_{n \geq 1}$. That is, u is locally nilpotently realizable at p. □

Lemma 3.2.10. *Suppose that G is a locally finite, locally nilpotent group and p a prime. Then G has a unique Sylow p-subgroup consisting of all elements of G with order a power of p.*

Proof. Denote by $\mathcal{P}$ the collection of subgroups of G,

$$\mathcal{P} = \{P_\omega : P_\omega \text{ is a finite } p\text{-subgroup of G}, \ \omega \in \Omega\},$$

where Ω is an indexing set for the collection, and put $H = \bigcup_{\omega\in\Omega} P_\omega$. We will show that H is the required subgroup of G. If $x, y \in H$, we can find $\omega, \nu \in \Omega$ such that $P_\omega, P_\nu \in \mathcal{P}$ and $x \in P_\omega$, $y \in P_\nu$. It follows that $x^{-1} \in P_\omega$ so $x^{-1} \in H$. If either of x or y is the identity element, $xy \in H$. Hence we may suppose that $o(x) = p^r$ and $o(y) = p^s$ for integers $r, s > 0$. Let $K = \langle x, y\rangle$. Then K is a finite nilpotent subgroup of G, and since $x \in K$ implies $p \,\big|\, |K|$, K has a unique Sylow p-subgroup L. This gives $x, y \in L$, from which $K = L$. Now $L \in \mathcal{P}$, so $xy \in H$ and therefore H is a subgroup of G.

To complete the proof we note that if $x \in G$ has order a power of p, then $\langle x\rangle \in \mathcal{P}$, so for any endomorphism ϑ of G, $\vartheta(x) \in H$. □

The main result of this section follows.

Theorem 3.2.11. *Suppose that $u = (u_n)$ is a sequence of positive integers. Then u is nilpotently realizable if and only if u is everywhere locally nilpotently realizable.*

Proof. First assume that the sequence u is realized by the nilpotent system (X, α). By Lemma 3.1.3 we can assume that X is a locally finite group with $\alpha : X \to X$ an automorphism. Let p denote a prime number; then by Lemma 3.2.10, X has a unique Sylow p-subgroup. Therefore, from Theorem 3.2.9, u is locally nilpotently realized at p. This is true for all primes p, so u is everywhere locally nilpotently realizable.

The converse result is proved in Proposition 3.2.7. □

Lemma 3.2.12. *Let p denote a fixed prime and suppose the sequence $u = (u_n)$ is equal to a product of nilpotently realizable p-sequences. Then u is a nilpotently realizable p-sequence.*

Proof. Let u be the product of the p-sequences $\{u^{(\omega)} : \omega \in \Omega\}$. For any $\omega \in \Omega$, suppose the sequence $u^{(\omega)}$ is nilpotently realized by the nilpotent system $(X_\omega, \vartheta_\omega)$. Then by Lemma 3.1.3 we can assume that $X_\omega = \bigcup_{n\geq 1} \mathrm{Per}_n(\vartheta_\omega)$, and it follows from Lemma 3.2.5 that X_ω is a locally finite p-group. Now, if W is the group $W = \prod_{\omega\in\Omega} X_\omega$ and $\psi : W \to W$ the endomorphism $\psi = \prod_{\omega\in\Omega} \vartheta_\omega$, let X denote the subgroup of W given by $X = \bigcup_{n\geq 1} \mathrm{Per}_n(\psi)$, with the map $\alpha : X \to X$ defined by $\alpha : x \mapsto \psi(x)$. Lemma 3.1.3 gives X is locally finite from which we easily obtain X is a p-group. Hence X is locally nilpotent and so, since the system (X, α) realizes u, we have u is nilpotently realizable. □

The following result provides an alternative view on Theorem 3.2.11 in that it is concerned with the factorization of nilpotently realizable sequences.

Theorem 3.2.13. *The sequence $u = (u_n)$ of positive integers is nilpotently realizable if and only if it is the product of nilpotently realizable p-sequences.*

Proof. First suppose that u is nilpotently realizable. Then by Theorem 3.2.11, u is everywhere locally nilpotently realizable. Hence, if for any prime p we write $u^{(p)} = ([u_n]_p)_{n\geq 1}$, then $u^{(p)}$ is nilpotently realizable and since $u_n = \prod_p [u_n]_p$, for $n \geq 1$, the sequence u is the product of the sequences $u^{(p)}$. This completes the proof in one direction.

Now suppose that the converse is true so that u is the product of nilpotently realizable p-sequences for various primes p. For a fixed prime p, if we group together all of the p-sequences in this product, Lemma 3.2.12 implies that this will form a nilpotently realizable p-sequence. It follows that u is everywhere locally nilpotently realizable, so Proposition 3.2.7 gives u is nilpotently realizable. □

3.3. Algebraically Realizable p-Sequences

In view of Lemmas 3.1.3 and 3.2.5, if a p-sequence u is algebraically realized, then u is nilpotently realizable, so for the class of p-sequences we can take the descriptions algebraically realizable and nilpotently realizable as being equivalent. In this section we will look at various types of p-sequence, and establish the algebraic realizability of some general classes. The types considered do not encompass all algebraically realizable p-sequences, but are included just to give a general flavour. We begin, however, with an example which shows that not all realizable p-sequences are algebraically realizable.

Example 3.3.1. The permutation

$$(1\,2\,\cdots\,6) \text{ acting on the set } \{1, 2, \ldots, 9\}$$

realizes the periodic 3-sequence $u = (3, 3, 3, 3, 3, 9, 3, 3, 3, 3, 3, 9, \ldots)$. We will show that u is not realizable by an algebraic system.

Suppose, on the contrary, that the sequence u can be algebraically realized. Then by Lemma 3.1.3, there is a group X of order 9 (which must therefore be abelian) and an automorphism $\alpha : X \to X$ such that the system (X, α) realizes u. If $x \in X \setminus \operatorname{Fix}(\alpha)$ then it is easy to see that the orbit $\operatorname{Orb}_\alpha(x)$ has order 6. However, since we should have $|\operatorname{Orb}_\alpha(x)| \mid |X|$, this gives a contradiction, so the sequence u is not algebraically realizable.

The previous example establishes the fact that the set of all realizable p-sequences strictly contains the set of algebraically realizable p-sequences. Indeed, this example shows that the set of realizable divisibility p-sequences which satisfy a linear relation is not contained in the set of algebraically realizable p-sequences. We will now consider some of the members of this latter set, with the first to be considered, the 'geometric' sequence, being possibly the simplest, arising in a natural way from the shift operation on a group of sequences.

Throughout the rest of this section, for a given prime p we will represent the field $\mathbb{F}_p$ of order p, by the set of integers $\{0, 1, \ldots, p-1\}$, where all operations are carried out mod p.

Proposition 3.3.2. *For prime p, the geometric sequence $(p^n)_{n\geq 1}$ is algebraically realizable.*

Proof. Let G denote the additive group of the field $\mathbb{F}_p$. Then $X = G^{\mathbb{N}}$ is an abelian group in which the group operation is pointwise addition of the sequences mod p. If $\lambda : X \to X$ is defined to be the left shift map, then $\lambda \in \mathrm{Aut}(X)$ and the system (X, λ) algebraically realizes the sequence (p^n). □

Next we consider various types of bounded p-sequences, arising from the actions of the endomorphisms of finite p-groups. Before this, however, we require some results of a technical nature.

Lemma 3.3.3. *Let m, p denote integers, with $m > 1$ and p an odd prime. Then there exists an integer $r > 1$ such that $r^p \equiv 1 \pmod{p^m}$, while $r^n \not\equiv 1 \pmod{p^m}$ when the integer n is in the range $1 \leq n < p$.*

Proof. Denote by $g > 0$ a primitive root modulo p^m. Since $m > 1$, if φ is the Euler φ-function, $j = \varphi(p^m)/p$ is an integer. Let $r > 1$ denote the integer g^j. Then by the definition of a primitive root, $r^p \equiv 1 \pmod{p^m}$, and when $1 \leq n < p$, $r^n \not\equiv 1 \pmod{p^m}$. □

Lemma 3.3.4. *Let m, p denote integers, with $m > 1$ and p an odd prime. If the integer r is such that $1 < r < p^m$, $r^p \equiv 1 \pmod{p^m}$ and $r^n \not\equiv 1 \pmod{p^m}$ for all integers n in the range $1 \leq n < p$, then there* *is a nilpotent group G of order p^{m+1} with the presentation*

$$\left\langle a, b : a^{p^m} = 1,\, b^p = 1,\, a^b = a^r \right\rangle.$$

Proof. First we note that Lemma 3.3.3 guarantees the existence of the integer r. Denote by C the cyclic group $\langle a : a^{p^m} = 1\rangle$, and let the automorphism $\beta : C \to C$ be given by $\beta(a) = a^r$. Then, $\beta^n(a) = a^{r^n}$ for integer $n \geq 0$, so $o(\beta) = p$. If the group G is defined to be the semi-direct product $\langle\beta\rangle \ltimes C$, then it is clear that $|G| = p^{m+1}$, so G is nilpotent by Theorem 1.1.4. Further, by the construction used, the group G obviously has the presentation

$$\left\langle a, b : a^{p^m} = 1,\, b^p = 1,\, a^b = a^r \right\rangle,$$

which completes the proof. □

The next result is a generalization of Example 3.2.3.

Proposition 3.3.5. *Let m denote a fixed positive integer and p a prime. Then the p-sequence $u = (u_n)$ given by*

$$u_n = \begin{cases} p^m & \text{if } p^m \nmid n \\ p^{m+1} & \text{if } p^m \mid n, \end{cases}$$

is algebraically realizable.

Proof. First we will deal with the case $m = 1$. Denote by Z_{p^2} the additive group of the ring $\mathbb{Z}_{p^2}$, and $\gamma : Z_{p^2} \to Z_{p^2}$ the automorphism $\gamma : x \mapsto (p+1)x$, $x \in Z_{p^2}$. Then the abelian system (Z_{p^2}, γ) realizes the sequence u (with $m = 1$).

Next we make the assumption that $m > 1$. As in Example 3.2.3, the sequence u is algebraically realized by a non-abelian system. If $p = 2$, let k denote 2^m, and X the dihedral group D_{2k} of order $2k = 2^{m+1}$, with the presentation

$$\langle c, d : c^k = 1,\, d^2 = 1,\, c^d = c^{-1}\rangle.$$

Since X is a finite 2-group, X is nilpotent by Theorem 1.1.4. The map $\psi : X \to X$, which is such that

$$\psi(c^r) = c^r \text{ and } \psi(c^r d) = c^{r+1}d,$$

for $r = 0, \ldots, k-1$, is an automorphism of X. It is easy to see that the nilpotent system (X, ψ) realizes the sequence u with $p = 2$.

Now assume that the prime p is odd, and let the nilpotent group G of order p^{m+1} be as in Lemma 3.3.4. That is, let

$$G = \left\langle a, b : a^{p^m} = 1,\, b^p = 1,\, a^b = a^r \right\rangle,$$

where the integer r is such that $1 < r < p^m$, $r^p \equiv 1 \pmod{p^m}$ and $r^n \not\equiv 1 \pmod{p^m}$ for all integers n in the range $1 \leq n < p$. Define the automorphism $\alpha : G \to G$ by $\alpha : g \mapsto g^a$ for all $g \in G$. The nilpotent system (G, α) realizes the sequence u when p is odd. □

Next we look at the sequences obtained from cyclic groups of prime power order. To facilitate this we introduce the following notation.

Definition 3.3.6. Let k, m and p denote non-negative integers, with p prime. For each integer $n \geq 1$ we define

$$\xi_n(k, m, p) = \gcd(p^k, [m^n - 1]_p).$$

Using the notation of this definition, it is clear that any sequence of the form $(\xi_n(k, m, p))_{n \geq 1}$ is a bounded and periodic p-sequence. The next result shows how such a sequence can arise.

Proposition 3.3.7. *Let k, p denote positive integers with p prime. If C is a cyclic group of order p^k and $\vartheta : C \to C$ is an endomorphism, then the p-sequence realized by the abelian system (C, ϑ) is of the form*

$$\xi = (\xi_n(k, m, p))_{n \geq 1},$$

where m is an integer with $0 \leq m < p^k$.

Proof. There is no loss of generality by assuming that C is the additive group of the ring $\mathbb{Z}_{p^k}$: thus we can write

$$C = \{0, 1, \ldots, p^k - 1\},$$

where the group operation on C is addition mod p^k. Let m denote the integer $\vartheta(1)$. Clearly, $0 \leq m < p^k$, and for all $x \in C$, $\vartheta(x) = mx$ (reduced mod p^k). Therefore, if n denotes a positive integer, then $x \in \mathrm{Per}_n(\vartheta)$ if and only if

$$(m^n - 1)x = 0 \text{ in } C. \tag{3.3}$$

Now, when $[m^n - 1]_p \leq p^k$, the number of solutions of (3.3) is easily seen to be $[m^n - 1]_p$; while the number of solutions is p^k if $[m^n - 1]_p > p^k$. It follows that $|\,\mathrm{Per}_n(\vartheta)| = \gcd(p^k, [m^n - 1]_p)$, which completes the proof. □

Example 3.3.8. The 2-sequence

$$(8, 8, 8, 8, 8, 8, 8, 16, 8, 8, 8, 8, 8, 8, 8, 16, 8, 8, 8, 8, 8, 8, 8, 16, \ldots)$$

is algebraically realizable by Proposition 3.3.5, while both 2-sequences

$$(\xi_n(4, 3, 2)) = (2, 8, 2, 16, 2, 8, 2, 16, 2, 8, 2, 16, \ldots)$$

and

$$(\xi_n(4, 5, 2)) = (4, 8, 4, 16, 4, 8, 4, 16, 4, 8, 4, 16, \ldots)$$

are algebraically realizable by Proposition 3.3.7.

A periodic p-sequence $u = (u_n)$ is called *simply periodic* if there are integers $k, m \geq 1$ such that $u_{rk} = u_k = p^m$ for $r = 1, 2, 3, \ldots$, and $u_n = 1$ if $k \nmid n$; the value of k is called the *period* of the sequence.

Lemma 3.3.9. *Let $u = (u_n)$ denote a simply periodic p-sequence of period k, where $u_k = p^m$. Then u is a realizable sequence if and only if $k \mid p^m - 1$.*

Proof. If $k = 1$ then this is trivial, since we have a constant sequence; so we will assume that $k > 1$.

For the proof in one direction, suppose that u is a realizable sequence. Then Lemma 1.2.4 gives

$$k \mid \sum_{d|k} \mu(k/d)u_d.$$

However, since $u_n = 1$ for all integers n where $1 \leq n < k$, we have

$$\sum_{d|k} \mu(k/d)u_d = \sum_{d|k} \mu(k/d) + \mu(1)(u_k - 1) = p^m - 1.$$

Combining these two results gives: $k \mid p^m - 1$.

In the opposite direction, assume now that $k \mid p^m - 1$, and write

$$u_n^* = \sum_{d|n} \mu(n/d)u_d, \ n = 1, 2, 3, \dots .$$

When $n = 1$ we trivially have $u_n^* \geq 0$ and $n \mid u_n^*$, so we will assume that $n > 1$. There are two cases to consider: $k \mid n$ and $k \nmid n$, the second of which is easy to dispose of. If $k \nmid n$, then since $u_d = 1$ for all $d \mid n$, we have $u_n^* = 0$ by similar arguments to above, so in this case it is certainly true that $u_n^* \geq 0$ and $n \mid u_n^*$.

On the other hand, if $k \mid n$ then $n = kr$ for some integer $r \geq 1$. This gives

$$u_n^* = \sum_{\substack{d|kr \\ k\nmid d}} \mu(kr/d)u_d + \sum_{c|r} \mu(r/c)u_{ck},$$

and so

$$u_n^* = \sum_{d|kr} \mu(kr/d) + (p^m - 1)\sum_{c|r} \mu(r/c).$$

It follows that,

$$u_n^* = \begin{cases} p^m - 1 & \text{if } n = k \\ 0 & \text{if } n > k. \end{cases}$$

Therefore we have $u_n^* \geq 0$ and $n \mid u_n^*$ for all values of $n \geq 1$, so Lemma 1.2.4 implies that the sequence u is realizable. □

We will show that a realizable simply periodic p-sequence is always algebraically realizable, but before doing this we require the following result.

Lemma 3.3.10. *Let p denote a prime number and m a positive integer, and let X represent the group G^m, where G is the additive group of the field $\mathbb{F}_p$. There exists an automorphism $\alpha : X \to X$ such that for all non-zero $x \in X$ the orbit of x has the property $|\operatorname{Orb}_\alpha(x)| = p^m - 1$.*

Proof. Let $q = p^m$: the additive group of the field of q elements, $\mathbb{F}_q$, is isomorphic to X and has the structure of a vector space of dimension m over the prime subfield $P \cong \mathbb{F}_p$ of $\mathbb{F}_q$. The multiplicative group $\mathbb{F}_q^*$ of non-zero elements of $\mathbb{F}_q$ is cyclic, so there is an element $g \in \mathbb{F}_q^*$ such that $o(g) = q - 1$. The map $A : \mathbb{F}_q \to \mathbb{F}_q$ given by $A : x \mapsto gx$ for each $x \in \mathbb{F}_q$, defines a non-singular linear transformation on the vector space $\mathbb{F}_q$ over P and since $A^n(x) = g^n x$, it is clear that for non-zero $x \in \mathbb{F}_q$ we have $|\operatorname{Orb}_A(x)| = q - 1$. It follows from this that there is an automorphism $\alpha : X \to X$ with $|\operatorname{Orb}_\alpha(x)| = p^m - 1$ when $x \in X$ is non-zero. □

Proposition 3.3.11. *If $u = (u_n)$ denotes a realizable simply periodic p-sequence, then u is an algebraically realizable sequence.*

Proof. Let the period of the sequence u be k, with $u_k = p^m$. Since u is realizable, by Lemma 3.3.9, $k \mid p^m - 1$: put $c = (p^m - 1)/k$. If G represents the additive group of $\mathbb{F}_p$, denote by X the group G^m. Then from Lemma 3.3.10 we know that there exists an automorphism $\alpha : X \to X$ with $|\operatorname{Orb}_\alpha(x)| = p^m - 1$ for $0 \neq x \in X$. If $\beta \in \operatorname{Aut}(X)$ is defined by $\beta = \alpha^c$, then for all non-zero $x \in X$ this gives $|\operatorname{Orb}_\beta(x)| = k$. If $k = 1$, we obtain from this: $\beta(x) = x$ for all $x \in X$, so the system (X, β) algebraically realizes the sequence $(p^m, p^m, p^m, \ldots)$. Assuming that $k > 1$, suppose that $0 \neq x \in \operatorname{Per}_n(\beta)$ where the integer $n \geq 1$ is such that $k \nmid n$. Then $\beta^n(x) = x$, and since $|\operatorname{Orb}_\beta(x)| = k$, $\beta^k(x) = x$.

There are integers a, b with $a \geq 0$, $0 < b < k$ and $n = ak + b$. It follows that $\beta^b(x) = x$ and so $|\operatorname{Orb}_\beta(x)| \leq b < k$, a contradiction. Therefore, the only member of $\operatorname{Per}_n(\beta)$ is the zero element, and so (X, β) algebraically realizes the sequence u. □

Corollary 3.3.12. *Let $u = (u_n)$ denote a simply periodic p-sequence of period k, where $u_k = p^m$. Then u is an algebraically realizable sequence if and only if $k \mid p^m - 1$.*

Proof. This follows from the previous result and Lemma 3.3.9. □

The set of realizable simply periodic p-sequences gives rise to an uncountable class of algebraically realizable p-sequences as we will now demonstrate. We begin by describing a general method for constructing a p-sequence for any prime p; but first we note that given distinct primes p and q then for any integer $r \geq 1$, there is a smallest integer $s = s(p, q, r) \geq 1$ such that $p^s \equiv 1 \pmod{q^r}$. This follows from the Euler-Fermat theorem.

Construction 3.3.13. Let p denote a prime: the sequence $g = (g_n)$ is constructed according to the following rules.

First we set $g_{p^r} = 1$ for $r \in \mathbb{N}_0$. Next, if q is a prime distinct from p we choose either $g_q = 1$ or $g_q = p^s$ where $s \geq 1$ is the least integer such that $p^s \equiv 1 \pmod{q}$. Suppose that we have made selections for $g_q, \ldots, g_{q^k}$ where $k \geq 1$. Then either we set $g_{q^{k+1}} = g_{q^k}$ or we have $g_{q^{k+1}} = g_{q^k} p^t$ where $t \geq 1$ is the smallest integer such that $p^t \equiv 1 \pmod{q^{k+1}}$. Thus we now have g_n defined when n is a non-negative integer power of any prime number.

To complete the construction, suppose that the integer $n > 1$ has prime decomposition $n = q_1^{k_1} \cdots q_r^{k_r}$ where the q_j are distinct primes and each integer $k_j \geq 1$, for $j = 1, \ldots, r$. Then we define $g_n = g_{q_1^{k_1}} \cdots g_{q_r^{k_r}}$.

The sequence g of Construction 3.3.13 is obviously a p-sequence. We will show that it is algebraically realizable by establishing that it is a product of realizable simply periodic p-sequences.

Proposition 3.3.14. *With the notation of* Construction 3.3.13*, the sequence g is algebraically realizable.*

Proof. Fix a prime $q \neq p$. Then the sequence $v^{(q)} = (v_n^{(q)})$, which is defined by: $v_n^{(q)} = g_n$ if n is a multiple of q, and $v_n^{(q)} = 1$ otherwise, is easily seen to be a product of realizable simply periodic sequences. It follows from Lemma 3.2.12 that $v^{(q)}$ is algebraically realizable.

Next we note that

$$g = \prod_{\substack{q \text{ prime} \\ q \neq p}} v^{(q)},$$

where this product is taken over all primes $q \neq p$. A further application of Lemma 3.2.12 allows us to conclude that the sequence g is algebraically realizable. □

The following result shows that there are quite a lot of algebraically realizable p-sequences for any prime p.

Proposition 3.3.15. *For a given prime p, the class of algebraically realizable p-sequences is uncountable.*

Proof. There are an uncountable number of p-sequences of the type given by Construction 3.3.13. This is so because for a given prime $q \neq p$, when constructing the values of $g_q, g_{q^2}, g_{q^3}, \ldots$, we are required to make choices as to whether or not the next term in the sequence is to equal the previous term. Depending on the choice, we can associate the binary digits $\{0, 1\}$: say 0 if the choice was to keep the terms equal, and 1 otherwise. In this manner we associate the sequence $(g_q, g_{q^2}, g_{q^3}, \ldots)$ with the binary expansion of a number in the real closed interval $[0, 1]$; the reverse association is clear. Since the set of real numbers $[0, 1]$ is uncountable, we deduce that the number of sequences constructed by the rules of 3.3.13 must be uncountable. Hence the class of algebraically realizable p-sequences is uncountable. □

It is obvious that not all realizable p-sequences given by products of realizable simply periodic p-sequences arise in the manner of Construction 3.3.13. Indeed, even if we restrict the sequences to those with first term 1, the example

$$(1,1,1,1,1,25,1,1,1,1,1,25,\ldots),$$

of a realizable simply periodic 5-sequence, is easily seen to be distinct from the sequences of Construction 3.3.13.

Before we consider a class of realizable p-sequences which does not arise from simply periodic sequences, we will look at some examples.

Example 3.3.16. Let X represent the group G^2, where G denotes the additive group of the field $\mathbb{F}_{31}$. The endomorphism $\vartheta : X \to X$ is defined by $\vartheta : (a,b) \mapsto (b, 23a+b)$, all calculations being carried out mod 31. The sequence $u = (u_n)$ which is realized by the system (X, ϑ) is given by:

$$u_n = \begin{cases} 1 & \text{if } 5 \nmid n \\ 31 & \text{if } 5 \mid n \text{ but } 155 \nmid n \\ 961 & \text{if } 155 \mid n. \end{cases}$$

It is easy to see that the algebraically realizable 31-sequence u described in this example is *not* a product of simply periodic 31-sequences.

Although the previous example is not *simply* periodic, because it is defined on a finite group, it is periodic. It is interesting to note that the sequence from this example has the form $(\xi_n(2,2,31))$: see Definition 3.3.6. The next example is defined on an infinite abelian group, and is not periodic.

Example 3.3.17. Let $\alpha : \mathbb{T}^3 \to \mathbb{T}^3$ denote the endomorphism given by the action of the matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

on the elements of $\mathbb{T}^3$ represented as column vectors. The sequence $u = (u_n)$ realized by the algebraic system $(\mathbb{T}^3, \alpha)$ is in fact the Lehmer-Pierce sequence for the monic polynomial $F(x) = x^3 - x - 1$, which will be established later. The first twenty terms of the sequence u are

$$(1, 1, 1, 5, 1, 7, 8, 5, 19, 11, 23, 35, 27, 64, 61, 85, 137, 133, 229, 275, \ldots).$$

The p-part sequences derived from u, for various primes p, lead to the next class of algebraically realizable p-sequences. Thus the 2-part sequence derived from u is

$$(1, 1, 1, 1, 1, 1, 8, 1, 1, 1, 1, 1, 1, 64, 1, 1, 1, 1, 1, 1, 8, 1, 1, 1, 1, 1, 1, 512, \ldots),$$

while the 5-part sequence is

$$(1, 1, 1, 5, 1, 1, 1, 5, 1, 1, 1, 5, 1, 1, 1, 5, 1, 1, 1, 25, 1, 1, 1, 125, 1, 1, 1, 5, \ldots).$$

These are clearly not periodic sequences since it can be checked that they are unbounded. The nth term of the 2-part sequence is given by

$$\begin{cases} 2^{3(1+\operatorname{ord}_2(n))} & \text{if } 7 \mid n \\ 1 & \text{if } 7 \nmid n. \end{cases}$$

However, the 5-part sequence is the product of two 5-sequences with one of them having nth term

$$\begin{cases} 5^{1+\operatorname{ord}_5(n)} & \text{if } 4 \mid n \\ 1 & \text{if } 4 \nmid n, \end{cases}$$

and the other being the 5-sequence with nth term given by

$$\begin{cases} 5^{2(1+\mathrm{ord}_5(n))} & \text{if } 24 \mid n \\ 1 & \text{if } 24 \nmid n. \end{cases}$$

The previous examples illustrate the next class of algebraically realizable p-sequences. Before the introduction of this class we require the following.

Lemma 3.3.18. *If m denotes a positive integer and p a prime, let $q = p^m$. Then there exists a matrix $A \in \mathcal{M}_m(\mathbb{Z})$ with the properties*

(1) $\det(A^n - I) \not\equiv 0 \pmod p$ *if $q - 1 \nmid n$,*

(2) $A^{q-1} = I + pB$, *where $B \in \mathcal{M}_m(\mathbb{Z})$ and* $\det(B) \not\equiv 0 \pmod p$.

Here, n is a positive integer and $I \in \mathcal{M}_m(\mathbb{Z})$ is the unit matrix.

Proof. Adapting the proof of Lemma 3.3.10, there exists a matrix $A \in \mathcal{M}_m(\mathbb{F}_p)$ such that $A^n - I$ is non-singular if $q - 1 \nmid n$ and $A^{q-1} = I$. By using the representation $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ we can interpret the matrix A as being a member of the ring $\mathcal{M}_m(\mathbb{Z})$, with powers of the matrix being calculated mod p. Dropping the requirement for reduction mod p, we have a matrix A from $\mathcal{M}_m(\mathbb{Z})$ which satisfies the first property and is such that $A^{q-1} = I + pB$ for some matrix $B \in \mathcal{M}_m(\mathbb{Z})$. We will show that it is possible to select A so that $p \nmid \det(B)$.

From $A^{q-1} = I + pB$ we get $AB = BA$, so $A(I + AB) = (I + AB)A$. Consider the matrix $A' = A + p(I + AB)$. Since $A' \equiv A \pmod p$, A' satisfies the same conditions as the matrix A. However, we have

$$(A')^{q-1} = A^{q-1} + p(q-1)A^{q-2}(I + AB) + p^2 L = I - pA^{q-2} + p^2 K,$$

where $L, K \in \mathcal{M}_m(\mathbb{Z})$. If we set $B' = -A^{q-2} + pK$ then we have $(A')^{q-1} = I + pB'$ and $\det(B') \equiv \det(-A^{q-2}) \not\equiv 0 \pmod p$. Replacing A with A' and B with B' completes the proof. □

The next definition is made in order to simplify subsequent notation.

Definition 3.3.19. Let k, m and p denote fixed positive integers, with p being a prime such that $p \nmid k$. For each integer $n \geq 1$, the integer $\lambda_n(k, m, p)$ is defined by

$$\lambda_n(k,m,p) = \begin{cases} p^{m(1+\mathrm{ord}_p(n))} & \text{if } k \mid n \\ 1 & \text{if } k \nmid n \end{cases}.$$

Theorem 3.3.20. *Let k, m denote positive integers and p an odd prime with $p \nmid k$. If the p-sequence u is defined by*

$$u = (\lambda_n(k,m,p))_{n\geq 1},$$

then u is algebraically realizable if and only if $k \mid p^m - 1$.

Proof. In one direction, the proof is easy: if u is an algebraically realizable sequence then it is certainly realizable, so as in the proof of Lemma 3.3.9, $k \mid p^m - 1$.

Now consider the converse result, so assume that the sequence u is such that $k \mid p^m - 1$. It is not difficult to show that u is a realizable sequence in this case, but our aim is to construct a system which algebraically realizes u.

The set of rational numbers

$$\mathbb{T}_p = \bigcup_{n\geq 1} \{r/p^n : r = 0, 1, \ldots, p^n - 1\}$$

has the structure of an abelian group under the operation of addition mod 1. Using this we denote by X the abelian group $\mathbb{T}_p^m$. From Lemma 3.3.18, there exists a matrix $A \in \mathcal{M}_m(\mathbb{Z})$ with the properties: $\det(A^n - I) \not\equiv 0 \pmod{p}$ if $p^m - 1 \nmid n$ and $A^{p^m-1} = I + pB$ where $p \nmid \det(B)$. Let $c = (p^m - 1)/k$ and denote by $\alpha : X \to X$ the endomorphism $\alpha : x \mapsto A^c x$ for all $x \in X$. For the purposes of this definition we assume that x is a column vector. The abelian system (X, α) will be shown to realize u.

If $x \in \mathrm{Per}_n(\alpha)$ where $k \nmid n$, then $(A^{cn} - I)x = 0$, so since $p^m - 1 \nmid cn$, $\det(A^{cn} - I) \not\equiv 0 \pmod{p}$. Therefore there is a matrix $C \in \mathcal{M}_m(\mathbb{Z})$

such that $(I + pC)x = 0$. It follows that $x = 0$ so that $|\operatorname{Per}_n(\alpha)| = 1$ when $k \nmid n$.

Next, if $k \mid n$, write $n = p^s kr$ for some integers $s \geq 0$ and $r \geq 1$, where $p \nmid r$. From $A^{p^m-1} = I + pB$ we get

$$A^{cn} = A^{(p^m-1)p^s r} = (I + pB)^{p^s r} = I + p^{s+1} rB + \cdots = I + p^{s+1} D,$$

where $D \in \mathcal{M}_m(\mathbb{Z})$ and $\det(D) \not\equiv 0 \pmod{p}$ since $p \nmid \det(B)$.[1] Hence, if $x \in \operatorname{Per}_n(\alpha)$ we have $p^{s+1} Dx = 0$ and since $p \nmid \det(D)$ this implies that $p^{s+1} x = 0$. It follows from this that $|\operatorname{Per}_n(\alpha)| = p^{m(s+1)}$; that is, $|\operatorname{Per}_n(\alpha)| = p^{m(1+\operatorname{ord}_p(n))}$, and so the abelian system (X, α) algebraically realizes the sequence u. □

Corollary 3.3.21. *If p denotes an odd prime, then the sequence (ϖ_n) where $\varpi_n = p^{1+\operatorname{ord}_p(n)}$ for $n \geq 1$, is algebraically realizable.*

Proof. This follows from Theorem 3.3.20 since $p^{1+\operatorname{ord}_p(n)} = \lambda_n(1, 1, p)$ for all $n \in \mathbb{N}$. □

By an application of the results of this section and Theorem 2.2.2 of Chapter 2, we get the following general result.

Proposition 3.3.22. *Let p denote an odd prime and r, s positive integers. Then the p-sequence with nth term $p^{r+s\operatorname{ord}_p(n)}$ is realizable.*

Proof. Let $u = (u_n)$ be the sequence given by $u_n = p^{r+\operatorname{ord}_p(n)}$. Since we can write this as $u_n = p^{r-1} p^{1+\operatorname{ord}_p(n)}$, it follows from Lemma 3.3.9 and Corollary 3.3.21 that the sequence u is algebraically realizable. Denote by $v = (v_n)$ the sequence where $v_n = u_{n^s}$; then by Theorem 2.2.2, v is realizable, and since $v_n = p^{r+s\operatorname{ord}_p(n)}$, the result follows. □

The methods used in the proof of Theorem 3.3.20 do not work for the prime 2. However, it is relatively easy to prove a result which is similar to Corollary 3.3.21.

[1] It is essential here that p is odd

Let $X_{(2)}$ denote the following subgroup of the multiplicative circle group $\mathbb{S}^1 = \{x \in \mathbb{C} : |x| = 1\}$:

$$\{x \in \mathbb{S}^1 : x^{2^r} = 1 \text{ for some } r \geq 1\} = \bigcup_{r \geq 1} \{e^{2k\pi i/2^r} : 0 \leq k \leq 2^r - 1\}.$$

For any $x \in X_{(2)}$, let $\rho(x) = x^5$. It is easy to see that $\rho : X_{(2)} \to X_{(2)}$ is an endomorphism. The sequence realized by the algebraic system $(X_{(2)}, \rho)$ will be shown to be $(2^{2+\operatorname{ord}_2(n)})$.

Lemma 3.3.23. *Let r denote a non-negative integer. For any odd integer $m \geq 1$ we have $2^{r+2} \mid 5^{2^r m} - 1$, while $2^{r+3} \nmid 5^{2^r m} - 1$.*

Proof. From $5^{2^r m} = (1 + 2^2)^{2^r m}$, a simple application of the binomial theorem gives

$$5^{2^r m} = 1 + 2^{r+2} m + 2^{r+3} K,$$

for some integer $K \geq 0$, and the result follows from this. □

Proposition 3.3.24. *The 2-sequence $(2^{2+\operatorname{ord}_2(n)})_{n \geq 1}$ is algebraically realized by the system $(X_{(2)}, \rho)$.*

Proof. If $x \in \operatorname{Per}_n(\rho)$, where the integer $n \geq 1$ is fixed, then by the definition of the map ρ, $x \in X_{(2)}$ and $x^{5^n - 1} = 1$. We can express n in the form $n = 2^r m$ where the integers r, m are such that $r \geq 0$ and $m \geq 1$ is odd. It follows from Lemma 3.3.23 that $5^n - 1 = 2^{r+2} s$ where $s \geq 1$ is an odd integer. Since $x \in X_{(2)}$, this implies that $x = e^{2k\pi i/2^{r+2}}$ for $0 \leq k < 2^{r+2} - 1$. It follows that $|\operatorname{Per}_n(\rho)| = 2^{r+2} = 2^{2+\operatorname{ord}_2(n)}$. □

Corollary 3.3.25. *Let r denote a fixed integer where $r \geq 2$. Then the 2-sequence $(2^{r+\operatorname{ord}_2(n)})$ is algebraically realizable.*

Proof. This follows from Lemma 3.3.9 and Proposition 3.3.24. □

We finish this section by extending Corollary 3.3.21 to the case where $p = 2$. This requires new techniques, and these will be developed in the following.

Lemma 3.3.26. *Let $(G_1, \alpha_1), (G_2, \alpha_2), (G_3, \alpha_3), \ldots$ denote a chain of algebraic systems, where the groups $G_1, G_2, G_3 \ldots$ are such that*

$$G_1 \lneqq G_2 \lneqq G_3 \lneqq \cdots ,$$

and for each integer $n \geq 1$, the endomorphisms α_n, α_{n+1} satisfy

$$\alpha_{n+1}(x) = \alpha_n(x), \ \textit{for all } x \in G_n.$$

Then $G = \bigcup_{n\geq 1} G_n$ is a group and there is a natural *endomorphism $\alpha : G \to G$ such that $\alpha(x) = \alpha_n(x)$ whenever $x \in G_n$.*

Proof. It is obvious that $G = \bigcup_{n\geq 1} G_n$ is a group. Define the map $\alpha : G \to G$ by $\alpha : x \mapsto \alpha_n(x)$ if $x \in G_n$. This is a well-defined map since if $x \in G_m$ and $x \in G_n$, where $m < n$, then $\alpha_n(x) = \alpha_{n-1}(x) = \cdots = \alpha_m(x)$. Also, for any $x, y \in G$, there is an integer $n \geq 1$ such that $x, y \in G_n$. Therefore $\alpha(xy) = \alpha_n(xy) = \alpha_n(x)\alpha_n(y) = \alpha(x)\alpha(y)$, so that α is an endomorphism of G which by definition has the stated property. □

Our aim is to prove that the 2-sequence $(\lambda_n(1, 1, 2))$ is algebraically realizable. Before doing this, it is necessary to construct certain 2-groups and automorphisms of them. Let Z_2 denote the additive group $\{0, 1\}$ of the field $\mathbb{F}_2$, and $0 \leq Z_2$ the zero group; we define the groups $\mathcal{H}_n$ for $n = 1, 2, 3, \ldots$ by:

$$\mathcal{H}_n = \begin{cases} Z_2 & \text{if } n = 2^k, \text{ where } k \in \mathbb{N}_0 \\ 0 & \text{otherwise.} \end{cases}$$

The groups $\mathcal{H}_n$ are now put together to form an ascending chain of abelian 2-groups. Denote by $\mathcal{K}_n$ the group of order 2^n given by

$$\mathcal{K}_n = \prod_{k=1}^{2^{n-1}} \mathcal{H}_k, \quad n = 1, 2, 3, \ldots .$$

Next, the groups $\mathcal{X}_n$ are defined for $n \geq 1$ by

$$\mathcal{X}_n = \mathcal{K}_n \times \left(\prod_{k=2^{n-1}+1}^{\infty} 0 \right).$$

It is clear from the definitions, that the (additive abelian) groups $\mathcal{X}_n$ satisfy: $\mathcal{X}_n \cong Z_2^n$, $|\mathcal{X}_n| = 2^n$, and $\mathcal{X}_1 \gneqq \mathcal{X}_2 \gneqq \mathcal{X}_3 \gneqq \cdots$.

Now, for each integer $n \geq 1$, denote by $A_n \in \mathcal{M}_{2^{n-1}}(\mathbb{F}_2)$, the *upper triangular* matrix

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

so that

$$A_1 = (1), \quad A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \cdots.$$

Each of the matrices A_n give rise in a natural way to an automorphism $\mathcal{F}_n : \mathcal{K}_n \rightarrow \mathcal{K}_n$ where $\mathcal{F}_n : x \mapsto A_n x$ for all $x \in \mathcal{K}_n$.

Next, extend A_n to the matrix $\mathcal{A}_n$ of size $(\infty \times \infty)$ by means of the block diagonal matrix

$$\mathcal{A}_n = \begin{pmatrix} A_n & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \cdots \\ \boldsymbol{0} & 1 & 0 & 0 & \cdots \\ \boldsymbol{0} & 0 & 1 & 0 & \cdots \\ \boldsymbol{0} & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Using the matrix $\mathcal{A}_n$, we now define an automorphism $\mathcal{T}_n : \mathcal{X}_n \rightarrow \mathcal{X}_n$ (the natural extension of $\mathcal{F}_n : \mathcal{K}_n \rightarrow \mathcal{K}_n$) by $\mathcal{T}_n : x \mapsto \mathcal{A}_n x$ for all $x \in \mathcal{X}_n$. This gives the chain of abelian systems

$$(\mathcal{X}_1, \mathcal{T}_1), (\mathcal{X}_2, \mathcal{T}_2), (\mathcal{X}_3, \mathcal{T}_3), \ldots$$

and it is clear that for each $n \geq 1$,

$$\mathcal{T}_{n+1}(x) = \mathcal{T}_n(x), \text{ for all } x \in \mathcal{X}_n.$$

Hence, the requirements of Lemma 3.3.26 are all satisfied, so we can define the abelian group $\mathcal{X}$ to be $\bigcup_{n\geq 1}\mathcal{X}_n$, and the endomorphism $\tau : \mathcal{X} \to \mathcal{X}$ by $\tau(x) = \mathcal{T}_n(x)$ when $x \in \mathcal{X}_n$; it is easy to see that τ is in fact an automorphism of the group $\mathcal{X}$. The abelian system $(\mathcal{X}, \tau)$ will be used below to establish the algebraic realizability of the 2-sequence $(\lambda_n(1, 1, 2))$, but before doing this we consider an example, and then determine some facts about the systems $(\mathcal{K}_m, \mathcal{F}_m)$.

Example 3.3.27. The 2-sequences realized by the abelian systems $(\mathcal{K}_1, \mathcal{F}_1)$, $(\mathcal{K}_2, \mathcal{F}_2)$ and $(\mathcal{K}_3, \mathcal{F}_3)$ are

$$(2, 2, 2, 2 \ldots),\ (2, 4, 2, 4, \ldots) \text{ and } (2, 4, 2, 8, 2, 4, 2, 8, \ldots)$$

respectively. We note that each of these sequences is an approximation (in some sense) to the sequence $(\lambda_n(1, 1, 2)) = (2, 4, 2, 8, 2, 4, 2, 16, \ldots)$; and that for $m = 1, 2$, the sequence realized by the system $(\mathcal{K}_{m+1}, \mathcal{F}_{m+1})$ first differs from that realized by $(\mathcal{K}_m, \mathcal{F}_m)$ at the 2^mth term.

Lemma 3.3.28. *Let m denote a positive integer, and $u^{(m)} = (u_n^{(m)})_{n\geq 1}$ represent the sequence realized by the system $(\mathcal{K}_m, \mathcal{F}_m)$. Then for all integer $n \geq 1$*

$$u_n^{(m+1)} = \begin{cases} u_n^{(m)} & \text{if } 2^m \nmid n \\ 2u_n^{(m)} & \text{if } 2^m \mid n. \end{cases}$$

Proof. We will assume that $m \geq 3$, since Example 3.3.27 deals with smaller values of m. Note first of all that $o(\mathcal{F}_{m+1}) = 2^m$: this is easy to see from the form of the matrix A_{m+1} over the field $\mathbb{F}_2$. Next, using block matrix notation, we can write

$$A_{m+1} = \begin{pmatrix} A_m & B_m \\ \mathbf{0} & A_m \end{pmatrix}$$

where $B_m \in \mathcal{M}_{2^{m-1}}(\mathbb{F}_2)$ is the matrix with every entry equal to 1. For any integer $n \geq 1$, define the matrices $C_m^{(n)}$ by: $C_m^{(1)} = B_m$, and for

$n > 1$, $C_m^{(n)} = A_m C_m^{(n-1)} + B_m A_m^{n-1}$. Then

$$A_{m+1}^n = \begin{pmatrix} A_m^n & C_m^{(n)} \\ \boldsymbol{0} & A_m^n \end{pmatrix}.$$

Denote by $x = (x_1, \ldots, x_{2^{m-1}}, x_{2^{m-1}+1}, \ldots, x_{2^m})$ an element of the group $\mathcal{K}_{m+1}$. Then by construction we have $x_{2^{m-1}+1} = \cdots = x_{2^m-1} = 0$, so from the form of the matrix A_{m+1}^n, the number of fixed points of $\mathcal{F}_{m+1}^n$, where the integer n is in the range $1 \le n \le 2^m$, is determined by the number of solutions of the equation $A_m^n \hat{x} = \hat{x}$, $\hat{x} = (x_1, \ldots, x_{2^{m-1}})^{\mathrm{T}}$, along with the possible values of x_{2^m}. That is, the periodic points of $\mathcal{F}_{m+1}$ are determined by the periodic points of $\mathcal{F}_m$ and the term x_{2^m}. A simple induction on m, using $o(\mathcal{F}_{m+1}) = 2^m$, completes the proof. □

Lemma 3.3.29. *If m denotes a positive integer, and $u^{(m)} = (u_n^{(m)})_{n\ge1}$ represents the sequence realized by the system $(\mathcal{K}_m, \mathcal{F}_m)$, then*

$$u^{(m)} = \left(\gcd(2^m, 2^{1+\operatorname{ord}_2(n)})\right)_{n\ge1}.$$

Proof. From Example 3.3.27 we have $u^{(1)} = (2, 2, 2, 2, \ldots)$, so the result is certainly true when $m = 1$. Assume that it is true when $m = k \ge 1$; then by Lemma 3.3.28,

$$u_n^{(k+1)} = \begin{cases} \gcd(2^k, 2^{1+\operatorname{ord}_2(n)}) & \text{if } 2^k \nmid n \\ 2\gcd(2^k, 2^{1+\operatorname{ord}_2(n)}) & \text{if } 2^k \mid n. \end{cases}$$

Now, if $2^k \nmid n$ then $1 + \operatorname{ord}_2(n) \le k$, so that

$$\gcd(2^k, 2^{1+\operatorname{ord}_2(n)}) = \gcd(2^{k+1}, 2^{1+\operatorname{ord}_2(n)}).$$

Alternatively, if $2^k \mid n$ then $1 + \operatorname{ord}_2(n) \ge k + 1$, so

$$2\gcd(2^k, 2^{1+\operatorname{ord}_2(n)}) = 2^{k+1} = \gcd(2^{k+1}, 2^{1+\operatorname{ord}_2(n)}).$$

Therefore, in both possible cases we get

$$u_n^{(k+1)} = \gcd(2^{k+1}, 2^{1+\operatorname{ord}_2(n)}),$$

and induction completes the proof. □

Lemma 3.3.30. *If n denotes a positive integer and $m = \lfloor \log_2 n \rfloor + 1$, then*

$$\operatorname{Per}_n(\mathcal{T}_1) \leq \operatorname{Per}_n(\mathcal{T}_2) \leq \cdots \leq \operatorname{Per}_n(\mathcal{T}_m) = \operatorname{Per}_n(\mathcal{T}_{m+1}) = \cdots .$$

Proof. Let r denote any positive integer and suppose that $x \in \operatorname{Per}_n(\mathcal{T}_r)$. Then since $x \in \mathcal{X}_r$, $\mathcal{T}_{r+1}(x) = \mathcal{T}_r(x)$, and so because $\mathcal{X}_r$ is $\mathcal{T}_r$-invariant, $x \in \operatorname{Per}_n(\mathcal{T}_{r+1})$. Hence $\operatorname{Per}_n(\mathcal{T}_r) \leq \operatorname{Per}_n(\mathcal{T}_{r+1})$, which gives the ascending chain of subgroups of $\mathcal{X}$

$$\operatorname{Per}_n(\mathcal{T}_1) \leq \operatorname{Per}_n(\mathcal{T}_2) \leq \operatorname{Per}_n(\mathcal{T}_3) \leq \cdots .$$

We will prove that this chain eventually stabilizes by showing that $|\operatorname{Per}_n(\mathcal{T}_m)| = |\operatorname{Per}_n(\mathcal{T}_{m+s})|$ where $m = \lfloor \log_2 n \rfloor + 1$ and the integer $s \geq 0$.

By definition, the systems $(\mathcal{K}_j, \mathcal{F}_j)$ and $(\mathcal{X}_j, \mathcal{T}_j)$ are *essentially* the same for all $j \geq 1$, and therefore it is easy to see that

$$|\operatorname{Per}_k(\mathcal{T}_j)| = |\operatorname{Per}_k(\mathcal{F}_j)|, \text{ for } k = 1, 2, 3, \ldots .$$

From Lemma 3.3.29 we have

$$|\operatorname{Per}_k(\mathcal{F}_j)| = \gcd(2^j, 2^{1+\operatorname{ord}_2(k)}),$$

so when $j \geq 1 + \operatorname{ord}_2(k)$ this gives $|\operatorname{Per}_k(\mathcal{T}_j)| = 2^{1+\operatorname{ord}_2(k)}$. It is obvious that $\lfloor \log_2 k \rfloor \geq \operatorname{ord}_2(k)$, so for all $j \geq \lfloor \log_2 k \rfloor + 1$,

$$|\operatorname{Per}_k(\mathcal{T}_j)| = 2^{1+\operatorname{ord}_2(k)}.$$

The result follows from this. □

In the next result, Corollary 3.3.21 is extended to include the case where the prime $p = 2$. We note that Proposition 3.3.24 is a consequence of this new result, but since it was possible to prove it without the effort required for the more general case, we preferred to give the easier demonstration.

Theorem 3.3.31. *The 2-sequence $\upsilon = (2^{1+\mathrm{ord}_2(n)})_{n\geq 1}$ is algebraically realizable.*

Proof. We will show that the sequence υ is algebraically realized by the abelian system $(\mathcal{X}, \tau)$ constructed above.

Let n denote a positive integer and $m = \lfloor \log_2 n \rfloor + 1$. If $x \in \mathrm{Per}_n(\tau)$ then $x \in \mathcal{X}_r$ for some positive integer r, so $x = \tau^n(x) = \mathcal{T}_r^n(x)$. Thus, $x \in \mathrm{Per}_n(\mathcal{T}_r)$, and therefore by Lemma 3.3.30, $x \in \mathrm{Per}_n(\mathcal{T}_m)$: hence $\mathrm{Per}_n(\tau) \leq \mathrm{Per}_n(\mathcal{T}_m)$. Since it is clear that the reverse inclusion holds, we have $\mathrm{Per}_n(\tau) = \mathrm{Per}_n(\mathcal{T}_m)$. Applying Lemma 3.3.29, it follows that $|\mathrm{Per}_n(\tau)| = 2^{1+\mathrm{ord}_2(n)}$, and this completes the proof. □

The result just obtained does not completely extend Theorem 3.3.20 to the case where the prime $p = 2$, so we finish this section with the following problem.

Problem 3.3.32. Extend Theorem 3.3.20 to include the prime $p = 2$.

3.4. Non-Locally Nilpotent Groups

In the final section of this chapter, we will look at a question which can be considered to be a converse to Theorem 3.2.11: if the group G possesses the property that *every* automorphism $\alpha : G \to G$ is such that the sequence realized by the algebraic system (G, α) is everywhere locally realizable, then is G locally nilpotent? This question can be interpreted in the alternative form:

Question 3.4.1. If G denotes a group which is not locally nilpotent, does there exist an automorphism $\alpha : G \to G$ which is such that the sequence realized by the algebraic system (G, α) is not everywhere locally realizable?

We do not have a complete answer to Question 3.4.1, but we do show that several well known infinite classes of finite non-nilpotent groups do exist for which the question has a positive answer.

In a finite nilpotent group, the Sylow p-subgroups are unique, so in the the following result, where by implication the group has more than one Sylow p-subgroup, the group in question is not nilpotent.

Lemma 3.4.2. *Let X denote a finite group and p a prime with the following properties*

1. $p \parallel |X|$
2. *there is an automorphism $\vartheta \in \mathrm{Aut}(X)$ and an integer $n \geq 2$ where $n \nmid p-1$ and $|\vartheta| = n$*
3. *for any Sylow p-subgroup P of X, $\{P, \vartheta(P), \ldots, \vartheta^{n-1}(P)\}$ consists of n distinct Sylow p-subroups of X.*

Then the sequence realized by the algebraic system (X, ϑ) is not locally realizable at the prime p.

Proof. Let the integer r be in the range $0 < r < n$, and assume that $p \mid |\operatorname{Per}_r(\vartheta)|$. Then there is a Sylow p-subgroup P of X such that $P \leq \operatorname{Per}_r(\vartheta)$. This implies that $P = \vartheta^r(P)$ and since $0 < r < n$, this contradicts condition 3. Hence, $p \nmid |\operatorname{Per}_r(\vartheta)|$ for $r = 1, \ldots, n-1$. It follows that the p-part of the sequence realized by the system (X, ϑ) is of the form

$$u = (u_k) = (1, 1, \ldots, 1, p, 1, 1, \ldots, 1, p, \ldots)$$

where p occurs at the $n, 2n, 3n, \ldots$ positions only. If u is a realizable sequence then we know from Lemma 1.2.4 that

$$n \mid \sum_{d|n} u_d \mu(n/d).$$

Now, since $n > 1$ and $u_k = 1$ for $1 \leq k < n$, we obtain

$$\sum_{d|n} u_d \mu(n/d) = \sum_{d|n} \mu(n/d) - 1 + p = p - 1$$

so $n \mid p-1$, contrary to condition 2. Hence u is not a realizable sequence, and therefore the sequence realized by (X, ϑ) is not locally realizable at p. □

Proposition 3.4.3. *Let X denote a non-nilpotent group of order pq, where p and q are distinct primes. Then there is an automorphism $\vartheta \in \mathrm{Aut}(X)$ such that the sequence realized by the system (X, ϑ) is not everywhere locally realizable.*

Proof. Since X is not nilpotent, we may assume that the number of Sylow p-subgroups of X is greater than 1. If we denote this number by n_p, then from Sylow's theorem we have

$$n_p \equiv 1 \pmod{p} \text{ and } n_p \mid pq.$$

It follows that the prime q must be such that $q \equiv 1 \pmod{p}$ and $n_p = q > p$, so we certainly have $q \nmid p - 1$. It is now easy to see from Sylow's theorem, that X has a unique Sylow q-subgroup Q, so that Q is a normal subgroup of X. Therefore, if P is any Sylow p-subgroup of X, we have $X = PQ = QP$. Now Q is cyclic, so we can write $Q = \langle z : z^q = 1 \rangle$ for some $z \in Q$. If we define the inner automorphism $\vartheta \in \mathrm{Aut}(X)$ by $\vartheta : x \mapsto x^z$, then $|\vartheta| = q$, and by using Sylow's theorem and the fact that $X = PQ$, we see that the set

$$\{P, \vartheta(P), \vartheta^2(P), \dots, \vartheta^{q-1}(P)\}$$

consists of the q distinct Sylow p-subgroups of X, whenever P is any fixed Sylow p-subgroup of X. We now have all of the ingredients necessary for Lemma 3.4.2, and this completes the proof. □

Theorem 3.4.4. *Denote by n an odd integer with $n \geq 3$, and let D_{2n} be the dihedral group of order $2n$. Then there is an automorphism $\vartheta \in \mathrm{Aut}(D_{2n})$ such that the sequence realized by the system (D_{2n}, ϑ) is not everywhere locally realizable.*

Proof. A presentation for D_{2n} is

$$D_{2n} = \langle a, b : a^n = 1,\ b^2 = 1,\ a^b = a^{-1} \rangle$$

and using this we obtain: $B = \{1, b\}$ is a Sylow 2-subgroup of D_{2n}. For any integer r, we easily compute $b^{a^r} = a^{-2r}b$, so if we set

$$P_r = B^{a^r} = \{1, a^{-2r}b\}, \text{ for } 0 \leq r < n,$$

the complete set of distinct Sylow 2-subgroups of D_{2n} is

$$\{P_0, P_1, P_2, \ldots, P_{n-1}\}.$$

Denoting by $\vartheta \in \mathrm{Aut}(D_{2n})$ the inner automorphism $\vartheta : x \mapsto x^a$, we have $|\vartheta| = n$, and it follows easily that if P is any Sylow 2-subgroup of X then the set

$$\{P, \vartheta(P), \vartheta^2(P), \ldots, \vartheta^{n-1}(P)\}$$

consists of the n Sylow 2-subgroups of X. Lemma 3.4.2 completes the proof. □

Theorem 3.4.5. *Let n denote an integer with $n \geq 3$, and let S_n be the symmetric group of order $n!$. Then there is an automorphism $\vartheta \in \mathrm{Aut}(S_n)$ such that the sequence realized by the system (S_n, ϑ) is not everywhere locally realizable.*

Proof. The case $n = 3$ is contained in Theorem 3.4.4, since $S_3 \equiv D_6$, and therefore we will assume that $n \geq 4$. In order to make use of Lemma 3.4.2, the first task is to show that there is a prime $p \parallel |S_n|$. To do this we appeal to *Bertrand's Postulate* to establish the existence of an odd prime p with $n/2 < p < n$. Now, because $p < n < 2p$, we easily see that p occurs just once (as a factor of any of the terms) in the list $(1, 2, \ldots, n-1, n)$, and so $p \parallel n!$. Next, since any Sylow p-subgroup of S_n is cyclic and is generated by a cycle of length p, the number n_p of such subgroups is given by

$$n_p = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)}.$$

Because it is clear that $p \nmid n$ while $p - 1 \mid (n-1)\cdots(n-p+1)$, we have: n_p is a multiple of n, so it is certainly true that $n_p > 1$.

Let x denote the permutation $(1\,2\,\cdots\,n) \in S_n$. Then if $\pi \in S_n$ is any cycle of length p, it is easy to see that $\pi^x \neq \pi^r$ for any integer r. Therefore, if $\vartheta \in \mathrm{Aut}(S_n)$ is the inner automorphism given by $\vartheta(\omega) = \omega^x$ for all $\omega \in S_n$, and if P is any Sylow p-subgroup of S_n, the set

$$\{P, \vartheta(P), \vartheta^2(P), \ldots, \vartheta^{n-1}(P)\}$$

consists of n distinct Sylow p-subgroups of S_n. Noting that $|\vartheta| = n$ and $n \nmid p-1$, the proof is completed by Lemma 3.4.2. □

Theorem 3.4.6. *Let n denote an integer with $n \geq 4$, and let A_n be the alternating group of order $n!/2$. Then there is an automorphism $\vartheta \in \mathrm{Aut}(A_n)$ such that the sequence realized by the system (A_n, ϑ) is not everywhere locally realizable.*

Proof. The proof of this is essentially the same as that of the previous Theorem, since the prime p being odd guarantees that the Sylow p-subgroups of S_n are in fact contained in A_n. The only other thing to note is that when n is even, the automorphism ϑ is an outer automorphism of A_n, since in this case $x \notin A_n$. □

CHAPTER 4

Sequences of Lehmer-Pierce Type

A sequence of Lehmer-Pierce type will be shown to be algebraically realizable when no term of the sequence is zero. This is not a new result and it is included for completeness. Possible generalizations of the Lehmer-Pierce construction will be considered, some leading to known results. The main source of reference for this chapter is [**10**].

Throughout this chapter we will write $\varsigma = (\varsigma_n)$ for the sequence of monic polynomials $\varsigma_n(x) = x^n - 1$, and $\mathbb{S}^1_n$ for the finite subgroup of the circle group $\mathbb{S}^1$ defined for each integer $n \geq 1$ by

$$\mathbb{S}^1_n = \{z \in \mathbb{S}^1 : z^n = 1\} = \{e^{2r\pi i/n} : r = 0, 1, \ldots, n-1\}.$$

Finally, $\mathbb{S}^1_\omega$ is used to represent the countable subgroup of $\mathbb{S}^1$: $\bigcup_{n\geq 1} \mathbb{S}^1_n$.

4.1. Integer Matrices and Lehmer-Pierce Sequences

In this section we aim to establish certain results about matrices with integer entries. Many of the definitions and early results apply in a wider context but will be given in a form of more use in later arguments. The books [**4**] and [**8**] detail further information.

Let d denote a positive integer. If $A \in \mathcal{M}_d(\mathbb{C})$, then the *characteristic polynomial* of A, written as $\chi_A \in \mathbb{C}[x]$, is the polynomial of degree d defined by $\chi_A(x) = \det(A - xI)$, where I is the unit matrix in $\mathcal{M}_d(\mathbb{C})$. The *eigenvalues* of the matrix A are the zeros of χ_A. A notion corresponding to the eigenvalues of A, is that of the *eigenvectors* of A: a *non-zero* element $\mathbf{x}$ of the vector space $\mathbb{C}^d$ is called an eigenvector of A if $A\mathbf{x} = \lambda\mathbf{x}$ for some $\lambda \in \mathbb{C}$; in this equation, $\mathbf{x}$ is interpreted as a column vector. It is a standard result of linear algebra that λ is an eigenvalue of A; and further, that η is an eigenvalue of A only if there exists $0 \neq \mathbf{x} \in \mathbb{C}^d$ such that $A\mathbf{x} = \eta\mathbf{x}$.

Lemma 4.1.1. *Let d denote a positive integer and A a matrix from $\mathcal{M}_d(\mathbb{C})$ with eigenvalues $\alpha_1, \ldots, \alpha_d$. Then* $\det(A) = \alpha_1 \cdots \alpha_d$.

Proof. By definition, the eigenvalues of A are the zeros of the characteristic polynomial $\chi_A(x) = \det(A - xI)$. This gives $\det(A) = \chi_A(0)$ and the result now follows from elementary algebra. □

Lemma 4.1.2. *Let d and n denote positive integers. If the matrix $A \in \mathcal{M}_d(\mathbb{C})$ has eigenvalues $\alpha_1, \ldots, \alpha_d$, then the eigenvalues of the matrix A^n are $\alpha_1^n, \ldots, \alpha_d^n$.*

Proof. For some integer r in the range $1 \leq r \leq d$, let $\mathbf{x} \in \mathbb{C}^d$ denote an eigenvector of A corresponding to the eigenvalue α_r. Then $A\mathbf{x} = \alpha_r\mathbf{x}$, and from this we obtain

$$A^n\mathbf{x} = \alpha_r A^{n-1}\mathbf{x} = \alpha_r^2 A^{n-2}\mathbf{x} = \cdots = \alpha_r^n\mathbf{x}.$$

Therefore, $\mathbf{x}$ is an eigenvector of the matrix A^n with associated eigenvalue α_r^n. The result follows from this. □

Keeping with the notation of the proof of Lemma 4.1.2, from the equation $A^n\mathbf{x} = \alpha_r^n\mathbf{x}$ we easily obtain $(A^n - I)\mathbf{x} = (\alpha_r^n - 1)\mathbf{x}$, which leads to the following.

Lemma 4.1.3. *If d and n denote positive integers and the matrix $A \in \mathcal{M}_d(\mathbb{C})$ has eigenvalues $\alpha_1, \ldots, \alpha_d$, then*

$$\det(A^n - I) = (\alpha_1^n - 1) \cdots (\alpha_d^n - 1).$$

Proof. This follows by the argument just given and Lemma 4.1.1. □

The next result establishes a connection between Lehmer-Pierce sequences and integer matrices. Although being very straightforward, it is of great use.

Proposition 4.1.4. *Let d denote a positive integer and A a matrix from $\mathcal{M}_d(\mathbb{Z})$. The Lehmer-Pierce sequence $(\Delta_n(\chi_A))$ which is derived from the characteristic polynomial χ_A of A, has terms given by*

$$\Delta_n(\chi_A) = |\det(A^n - I)| \textit{ for } n = 1, 2, 3, \ldots.$$

Proof. Let $\alpha_1, \ldots, \alpha_d$ denote the zeros of the polynomial χ_A. Then by definition, the terms of the Lehmer-Pierce sequence $(\Delta_n(\chi_A))$ are given by

$$\Delta_n(\chi_A) = \prod_{r=1}^{d} |\alpha_r^n - 1|.$$

The proof is completed by Lemma 4.1.3. □

One of the reasons that Proposition 4.1.4 is so useful, especially when calculating Lehmer-Pierce sequences, is due to the following definition.

Definition 4.1.5. Denote by h a monic polynomial from $\mathbb{C}[x]$ of degree $d \geq 1$. If $h(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, then the *companion matrix* to h is

$$\Lambda_h = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & -a_2 & \ldots & -a_{d-1} \end{pmatrix}.$$

The main property of the matrix Λ_h which we require is the well known fact that the eigenvalues of Λ_h are the zeros of the polynomial h: in fact, $h = (-1)^d \chi_{\Lambda_h}$.

Proposition 4.1.6. *Let h denote a monic polynomial from $\mathbb{Z}[x]$. The Lehmer-Pierce sequence $(\Delta_n(h))$ has terms given by*

$$\Delta_n(h) = |\det(\Lambda_h^n - I)| \textit{ for } n = 1, 2, 3, \ldots.$$

Proof. This follows immediately from Proposition 4.1.4. □

The previous result gives an alternative demonstration of the fact that the terms of a Lehmer-Pierce sequence are integers.

The section is completed by showing that a Lehmer-Pierce sequence which contains no zero terms can be algebraically realized by an abelian system. The proof is based on that given in [**10**], the idea being to use the companion matrix Λ_h of the monic polynomial $h \in \mathbb{Z}[x]$ to construct an endomorphism on an abelian group.

Suppose that C is an abelian group and that n denotes an integer. We can define an endomorphism $\vartheta : C \to C$ by $\vartheta : x \mapsto nx$ for all $x \in C$. If we ask about the order of the subgroup $\ker(\vartheta)$ then in general this question will remain unanswered. However, when $C = \mathbb{T} = \mathbb{R}/\mathbb{Z}$, the additive circle group, it is easy to give an answer. Using the half-open interval representation: $\mathbb{T} = [0, 1)$, with addition carried out mod 1, and writing $m = |n|$, we have $\ker(\vartheta) = \mathbb{T}$ if $m = 0$. And when $m \neq 0$, $|\ker(\vartheta)| = m$ since in this case $\ker(\vartheta) = \{r/m : r = 0, 1, \ldots, m-1\}$. Thus: $|\ker(\vartheta)| = |\mathbb{Z}/n\mathbb{Z}|$.

A natural way to extend this is to consider an endomorphism of the toral group $\mathbb{T}^d$ defined by the action of a matrix $A \in \mathcal{M}_d(\mathbb{Z})$. To make this precise we have the following definition.

Definition 4.1.7. Let d denote a positive integer and A a matrix from $\mathcal{M}_d(\mathbb{Z})$. The endomorphism $\tau_A : \mathbb{T}^d \to \mathbb{T}^d$ is defined by $\tau_A : \mathbf{x} \mapsto A\mathbf{x}$ for all $\mathbf{x} \in \mathbb{T}^d$.

If $A \in \mathcal{M}_d(\mathbb{Z})$, then it is clear that $A\mathbb{Z}^d = \{A\mathbf{x} : \mathbf{x} \in \mathbb{Z}^d\}$ is a subgroup of $\mathbb{Z}^d$; and if A is non-singular then $A^{-1}\mathbb{Z}^d$ is a subgroup of $\mathbb{Q}^d$, containing $\mathbb{Z}^d$. Hence, if $A \in \mathcal{M}_d(\mathbb{Z})$ is non-singular, $\mathbb{Z}^d \leq A^{-1}\mathbb{Z}^d \leq \mathbb{Q}^d$.

Lemma 4.1.8. *Let d denote a positive integer and A a non-singular matrix from $\mathcal{M}_d(\mathbb{Z})$. Then $A^{-1}\mathbb{Z}^d/\mathbb{Z}^d \cong \mathbb{Z}^d/A\mathbb{Z}^d$.*

Proof. Define the map $\psi : \mathbb{Z}^d \to A^{-1}\mathbb{Z}^d/\mathbb{Z}^d$ by $\psi : \mathbf{x} \mapsto A^{-1}\mathbf{x} + \mathbb{Z}^d$ for all $\mathbf{x} \in \mathbb{Z}^d$. Then it is easy to see that ψ is a surjective homomorphism (epimorphism) and $\ker(\psi) = A\mathbb{Z}^d$. The proof is completed by appealing to one of the standard isomorphism theorems from group theory. □

Lemma 4.1.9. *If $A \in \mathcal{M}_d(\mathbb{Z})$ is non-singular then $\ker(\tau_A) \cong \mathbb{Z}^d/A\mathbb{Z}^d$.*

Proof. Let $\mathbf{x} \in \mathbb{R}^d$ be such that $\mathbf{x} + \mathbb{Z}^d \in \ker(\tau_A)$. By the definition of τ_A, $A\mathbf{x} \in \mathbb{Z}^d$, so $\mathbf{x} + \mathbb{Z}^d \in A^{-1}\mathbb{Z}^d/\mathbb{Z}^d$, which gives $\ker(\tau_A) \leq A^{-1}\mathbb{Z}^d/\mathbb{Z}^d$. The reverse inclusion is also easy to establish, so $\ker(\tau_A) = A^{-1}\mathbb{Z}^d/\mathbb{Z}^d$. The result now follows from Lemma 4.1.8. □

Next we have a technical result.

Lemma 4.1.10. *If the matrix $A = (a_{ij}) \in \mathcal{M}_d(\mathbb{Z})$ is non-singular with $n = |\det(A)|$, let $\hat{A} = (\hat{a}_{ij})$ denote the unique matrix in $\mathcal{M}_d(\mathbb{Z}_n)$ which is defined by*

$$\mathrm{Adj}(A) = \hat{A} + nM, \text{ for some } M \in \mathcal{M}_d(\mathbb{Z}).$$

Here, for the sake of the definition, the elements of the ring $\mathbb{Z}_n$ are interpreted as the set of integers $\{0, 1, \ldots, n-1\}$, and we assume that $0 \leq \hat{a}_{ij} < n$ for all $1 \leq i, j \leq d$.

The subgroup $\hat{A}\mathbb{Z}_n^d$ of the additive group $\mathbb{Z}_n^d$ is such that $|\hat{A}\mathbb{Z}_n^d| = n$.

Proof. [*Outline Sketch*] Clearly we may assume that $d \geq 2$. The matrix $\mathrm{Adj}(A)$ is such that all 2×2 minors are divisible by n (see [**11**]). It follows that the determinantal rank of the matrix $\hat{A}$ over the ring $\mathbb{Z}_n$ is at most 1, and so the row rank of $\hat{A}$ is either 0 or 1. However, if the row rank were 0, this would contradict the fact that $\det(\mathrm{Adj}(A)) = \pm n^{d-1}$, so we must have: $\text{row-rank}_{\mathbb{Z}_n}(\hat{A}) = 1$. From this we deduce that the number of distinct elements in $\hat{A}\mathbb{Z}_n^d$ is n. □

Lemma 4.1.11. *If $A \in \mathcal{M}_d(\mathbb{Z})$ is non-singular, $|\mathbb{Z}^d/A\mathbb{Z}^d| = |\det(A)|$.*

Proof. Let $n = |\det(A)|$ and denote by $\tilde{A}$ the adjoint matrix of A. Then from standard linear algebra results, $\tilde{A} \in \mathcal{M}_d(\mathbb{Z})$ is non-singular and $A\tilde{A} = \tilde{A}A = \pm nI$. By a similar argument to that used in the proof of Lemma 4.1.8, $\mathbb{Z}^d/A\mathbb{Z}^d \cong \tilde{A}\mathbb{Z}^d/A\tilde{A}\mathbb{Z}^d$, from which we get: $\mathbb{Z}^d/A\mathbb{Z}^d \cong \tilde{A}\mathbb{Z}^d/n\mathbb{Z}^d$. If we define the matrix $\hat{A} \in \mathcal{M}_d(\mathbb{Z}_n)$ as in Lemma 4.1.10, then it is easy to see that the group $\tilde{A}\mathbb{Z}^d/n\mathbb{Z}^d$ is isomorphic to the subgroup $\hat{A}\mathbb{Z}_n^d$ of the additive group $\mathbb{Z}_n^d$, so a further application of Lemma 4.1.10 completes the proof. □

The main result of this section follows.

Theorem 4.1.12. *Denote by h a monic polynomial from $\mathbb{Z}[x]$ which is such that no zero of h is a root of unity; that is, the set of zeros of h is disjoint from the set $\mathbb{S}^1_\omega$. Then the Lehmer-Pierce sequence $(\Delta_n(h))$ is algebraically realized by an abelian system.*

Proof. The condition that no zero of h is a root of unity is clearly equivalent to the requirement that no term of the sequence $(\Delta_n(h))$ is zero. By Proposition 4.1.6 this implies that the matrix $\Lambda_h^n - I$ is non-singular for each positive integer n. Let $d = \partial(h)$, and for ease of notation, write $A = \Lambda_h \in \mathcal{M}_d(\mathbb{Z})$. We will show that the abelian system $(\mathbb{T}^d, \tau_A)$ realizes the Lehmer-Pierce sequence $(\Delta_n(h))$.

Let n denote a fixed positive integer and suppose $\mathbf{x} \in \mathbb{R}^d$ is such that $\mathbf{x} + \mathbb{Z}^d \in \mathrm{Per}_n(\tau_A)$. Then by the definition of τ_A this is equivalent to $(A^n - I)\mathbf{x} \in \mathbb{Z}^d$. Writing B for the matrix $A^n - I$, the preceding arguments give: $\mathrm{Per}_n(\tau_A) = \ker(\tau_B)$. It follows from Lemma 4.1.9 that $\mathrm{Per}_n(\tau_A) \cong \mathbb{Z}^d/B\mathbb{Z}^d$, so by Lemma 4.1.11, $|\mathrm{Per}_n(\tau_A)| = |\det(B)|$. The proof is completed by Proposition 4.1.6. □

We end this section by defining a special type of realizable sequence.

Definition 4.1.13. The sequence $u = (u_n)$ of positive integers is said to be *Lehmer-Pierce realizable* if there is a monic polynomial $h \in \mathbb{Z}[x]$ such that $u_n = \Delta_n(h)$ for all $n \geq 1$.

Since zero is excluded from the definition of a Lehmer-Pierce realizable sequence, this is in fact a special case of an algebraically realizable sequence, as established above in Theorem 4.1.12.

Example 4.1.14. The sequence $(\upsilon_n) = (1, 3, 1, 15, 31, 27, 127, 255, \ldots)$, which is defined for $n = 1, 2, 3, \ldots$ by

$$\upsilon_n = \begin{cases} 2^n - 1 & \text{if } 3 \nmid n \\ (2^{n/3} - 1)^3 & \text{if } 3 \mid n \end{cases}$$

is Lehmer-Pierce realizable since $\upsilon_n = \Delta_n(f)$, where $f(x) = x^3 - 2$.

4.2. Divisibility Sequences of Polynomials

The sequence of polynomials $\varsigma = (\varsigma_n)$ is such that if the positive integers m, n have $m \mid n$, then there is a polynomial $\kappa \in \mathbb{Z}[x]$ with $\varsigma_n = \kappa\varsigma_m$: in fact we have

$$x^n - 1 = (x^m - 1)(x^{n-m} + x^{n-2m} + \cdots + x^m + 1). \tag{4.1}$$

Extending the notation used for the divisibility of integers, we will write this as $\varsigma_m \mid \varsigma_n$. A sequence (f_n) of non-zero polynomials from the ring $\mathbb{Z}[x]$ will be called a *divisibility sequence of polynomials* if $f_m \mid f_n$ when the integers $m, n \geq 1$ are such that $m \mid n$. The sequence ς also has the property that $1 \leq \partial(\varsigma_n) < \partial(\varsigma_{n+1})$ for all $n \geq 1$. We will call a sequence (f_n) from $\mathbb{Z}[x]$ a *proper* divisibility sequence of polynomials if: $\partial(f_n) \to \infty$ as $n \to \infty$; $1 \leq \partial(f_n) \leq \partial(f_{n+1})$ for all $n \geq 1$, and when the positive integers m, n are such that $m \mid n$, then $f_m \mid f_n$. Thus the sequence ς is a proper divisibility sequence of polynomials. In this section, we will investigate a generalization of the Lehmer-Pierce construction which utilises divisibility sequences of polynomials.

Given a monic polynomial $h \in \mathbb{Z}[x]$ with zeros $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$, where $d = \partial(h)$, the Lehmer-Pierce sequence $(\Delta_n(h))$ is defined by

$$\Delta_n(h) = \prod_{k=1}^{d} |\alpha_k^n - 1|, \quad n = 1, 2, 3, \ldots.$$

In terms of the polynomial sequence ς, this can be expressed as

$$\Delta_n(h) = \prod_{k=1}^{d} |\varsigma_n(\alpha_k)|, \quad n = 1, 2, 3, \ldots,$$

and it is this formulation of the Lehmer-Pierce sequence which leads to the following generalization.

Definition 4.2.1. Denote by $f = (f_n)$ a sequence of non-zero polynomials from $\mathbb{Z}[x]$. If $h \in \mathbb{Z}[x]$ is a monic polynomial of degree d with zeros $\alpha_1, \ldots, \alpha_d$, then the sequence $(\Delta_n^{(f)}(h))$ is given by

$$\Delta_n^{(f)}(h) = \prod_{k=1}^{d} |f_n(\alpha_k)|, \quad n = 1, 2, 3, \ldots.$$

Using this definition, the standard Lehmer-Pierce sequence becomes $(\Delta_n^{(\varsigma)}(h))$; however, we will keep with the notation previously used when referring to this sequence.

Example 4.2.2. Let $f_n \in \mathbb{Z}[x]$ denote the polynomial $f_n(x) = x^{d_n} - 1$ where d_n is the nth term of the Fibonacci sequence $(1, 1, 2, 3, 5, \ldots)$. Then $f = (f_n)$ is a proper divisibility sequence of polynomials.

Let the polynomial $h \in \mathbb{Z}[x]$ be given by $h(x) = x - 2$. Then using the sequence f from Example 4.2.2 we obtain

$$(\Delta_n^{(f)}(h)) = (1, 1, 3, 7, 31, \ldots),$$

and it is interesting to note that this sequence of integers is not realizable.

Lemma 4.2.3. *Let $h \in \mathbb{Z}[x]$ denote a polynomial with $\partial(h) = d \geq 1$ and factorization over $\mathbb{C}$, $h(x) = a(x-\alpha_1)\cdots(x-\alpha_d)$. If the polynomial $g \in \mathbb{Z}[x_1, \ldots, x_m]$, where the integer $m \geq 1$, then for $t \in \{1, 2, \ldots, m\}$,*

$$\psi_t(g, h) = a^{\partial_{x_t}(g)} \prod_{k=1}^{d} g(x_1, \ldots, x_{t-1}, \alpha_k, x_{t+1}, \ldots, x_m)$$

is a member of the ring $R = \mathbb{Z}[x_1, \ldots, x_{t-1}, x_{t+1}, \ldots, x_m]$. Further,

$$\psi_t(g, h) = a^{\partial_{x_t}(g)} \det(g(x_1, \ldots, x_{t-1}, \Lambda_{h^*}, x_{t+1}, \ldots, x_m))$$

where Λ_{h^*} is the companion matrix to the monic polynomial $h^* = a^{-1}h$.

Proof. Clearly there will be no loss of generality (but a considerable gain in ease of notation) if we assume that $t = m$. It is easy to see that, by grouping terms appropriately, $\psi_m(g,h)$ can be put in the form

$$\psi_m(g,h) = a^{\partial_{x_m}(g)} \sum_j r_j s_j,$$

where each $r_j \in R = \mathbb{Z}[x_1, \ldots, x_{m-1}]$ and the $s_j \in \mathbb{Z}[\alpha_1, \ldots, \alpha_d]$ are symmetric expressions in the zeros $\alpha_1, \ldots, \alpha_d$ of h. It follows from this, and elementary algebraic number theory, (see [**27**]) that $a^{\partial_{x_m}(g)} s_j \in \mathbb{Z}$ and so $\psi_m(g,h) \in R$.

Now, we can think of g as being a member of the ring $R[x_m]$, and since the eigenvalues of Λ_{h^*} are $\alpha_1, \ldots, \alpha_d$,

$$\det(g(\Lambda_{h^*})) = g(\alpha_1) \cdots g(\alpha_d),$$

from which the result follows. □

We illustrate the previous result with the following example.

Example 4.2.4. Denote by $g(x_1, x_2, x_3) = 3x_1x_2 - x_1^2x_2x_3 + 2x_1x_3^3$ a polynomial from the ring $\mathbb{Z}[x_1, x_2, x_3]$, and let $h(x) = 2x^2 - x + 2 \in \mathbb{Z}[x]$. If the zeros of h are α and β then in the notation of Lemma 4.2.3,

$$\psi_1(g,h) = 4(-x_2x_3\alpha^2 + (3x_2 + 2x_3^3)\alpha)(-x_2x_3\beta^2 + (3x_2 + 2x_3^3)\beta).$$

Expanding this and grouping the terms,

$$\psi_1(g,h) = 4(x_2^2x_3^2\alpha^2\beta^2 - x_2x_3(3x_2 + 2x_3^3)(\alpha^2\beta + \alpha\beta^2) + (3x_2 + 2x_3^3)^2\alpha\beta)$$

from which, on using $\alpha + \beta = 1/2$ and $\alpha\beta = 1$,

$$\psi_1(g,h) = 2(2x_3^2 - 3x_3 + 18)x_2^2 - 4x_3^3(x_3 - 12)x_2 + 16x_3^6 \in \mathbb{Z}[x_2, x_3].$$

Alternatively, the companion matrix to $h^* = 2^{-1}h$ is

$$\Lambda_{h^*} = \begin{pmatrix} 0 & 1 \\ -1 & 1/2 \end{pmatrix},$$

so that $g(x_1, x_2, \Lambda_{h^*}) = 2x_1\Lambda_{h^*}^3 - x_1^2x_2\Lambda_{h^*} + 3x_1x_2I$, where I denotes the 2×2 identity matrix. Hence,

$$g(x_1, x_2, \Lambda_{h^*}) = \frac{1}{4}x_1 \begin{pmatrix} 12x_2 - 4 & -4x_1x_2 - 6 \\ 4x_1x_2 + 6 & -2x_1x_2 + 12x_2 - 7 \end{pmatrix},$$

and from Lemma 4.2.3,

$$\psi_3(g, h) = \frac{1}{2}x_1^2 \begin{vmatrix} 12x_2 - 4 & -4x_1x_2 - 6 \\ 4x_1x_2 + 6 & -2x_1x_2 + 12x_2 - 7 \end{vmatrix}.$$

Expanding this determinant,

$$\psi_3(g, h) = 8x_2^2x_1^4 - 4x_2(3x_2 - 7)x_1^3 + 2(36x_2^2 - 33x_2 + 16)x_1^2 \in \mathbb{Z}[x_1, x_2].$$

Proposition 4.2.5. *Let $f = (f_n)$ denote a sequence of non-zero polynomials from $\mathbb{Z}[x]$. If $h \in \mathbb{Z}[x]$ is a monic polynomial, then $(\Delta_n^{(f)}(h))$ is a sequence of non-negative integers. Further, if f is a divisibility sequence of polynomials and the integers $m, n \geq 1$ are such that $m \mid n$, then $\Delta_n^{(f)}(h)$ is a multiple of $\Delta_m^{(f)}(h)$, so that in this case $(\Delta_n^{(f)}(h))$ is a divisibility sequence of positive integers if it consists of non-zero terms.*

Proof. For each integer $n \geq 1$, the fact that $\Delta_n^{(f)}(h)$ is a non-negative integer follows from Definition 4.2.1 and Lemma 4.2.3. Next, if f is a divisibility sequence and the integers $m, n \geq 1$ are such that $m \mid n$, then $f_n = gf_m$ for some polynomial $g \in \mathbb{Z}[x]$, so by Definition 4.2.1,

$$\Delta_n^{(f)}(h) = \Delta_m^{(f)}(h) \prod_{k=1}^{d} |g(\alpha_k)|,$$

where h has the factorization over $\mathbb{C}$: $h(x) = (x - \alpha_1) \cdots (x - \alpha_d)$. Now from Lemma 4.2.3, $\prod_{k=1}^{d} |g(\alpha_k)|$ is a non-negative integer, and this fact completes the proof. □

In order to consider a converse result to Proposition 4.2.5, we introduce notation to deal with the individual terms of the integer sequence $(\Delta_n^{(f)}(h))$.

Definition 4.2.6. If $g, h \in \mathbb{Z}[x]$ denote polynomials with $\partial(g) \geq 0$ and h having factorization over $\mathbb{C}$, $h(x) = a_h(x - \alpha_1) \cdots (x - \alpha_d)$, then we define

$$\delta(g, h) = |a_h|^{\partial(g)} \prod_{k=1}^{d} |g(\alpha_k)|.$$

Thus, in the notation of this definition, the individual term $\Delta_n^{(f)}(h)$ from the sequence $(\Delta_n^{(f)}(h))$ of Definition 4.2.1, can be written as: $\delta(f_n, h)$. Note also, that Lemma 4.2.3 guarantees that $\delta(g, h)$ is a non-negative integer.

The following example illustrates why a simple converse to the divisibility conclusion of Proposition 4.2.5 will not work.

Example 4.2.7. Let $g_1, g_2 \in \mathbb{Z}[x]$ denote the polynomials given by $g_1(x) = 2(x^2 + 1)$ and $g_2(x) = x(x + 1)(x^4 - 1)$. Then it is easy to see that $\delta(g_1, h) \mid \delta(g_2, h)$ for all *linear* monic $h \in \mathbb{Z}[x]$. However, $g_1 \nmid g_2$, although it is obvious that g_1 is a factor of g_2 in $\mathbb{Q}[x]$. Note that if $k(x) = x^2 + x + 1$, then $\delta(g_1, k) = 4$ and $\delta(g_2, k) = 3$, so that $\delta(g_1, k) \nmid \delta(g_2, k)$.

Lemma 4.2.8. *Let p denote a prime number, n a non-negative integer, and let $g(x) = g_n x^n + \cdots + g_0$ represent a polynomial from the ring $\mathbb{Z}[x]$, where the coefficients satisfy: $g_n \neq 0$ and $\gcd(p, g_0, \ldots, g_n) = 1$. Then there exists a monic polynomial $h \in \mathbb{Z}[x]$ for which $\delta(g, h) \equiv 1 \pmod{p}$.*

Proof. If $\partial(g) = 0$, then the result follows easily from the Euler-Fermat theorem, so we will assume that $\partial(g) = n > 0$. The condition $\gcd(p, g_0, \ldots, g_n) = 1$ implies that there are polynomials $f, k \in \mathbb{Z}[x]$ so that $g = pf + k$ where k is such that: if $k(x) = k_m x^m + \cdots + k_0$ then $0 \leq k_r \leq p - 1$ for $r = 0, \ldots, m$ and $k_m \neq 0$. If $\partial(k) = 0$, so that $k \equiv k_0 \neq 0$, then we can complete the proof by a simple application of the Euler-Fermat theorem. Assuming that $\partial(k) > 0$, we can find a unique integer a such that $1 \leq a \leq p - 1$ and $ak_m \equiv 1 \pmod{p}$, and by a suitable redefinition of the polynomials f, k we have $ag = pf + k$

where k is monic. Let the monic polynomial $h \in \mathbb{Z}[x]$ be given by $h(x) = k(x) - a$. If the zeros of h are $\alpha_1, \dots, \alpha_m$, we have

$$\delta(ag, h) = \prod_{r=1}^{m} |ag(\alpha_r)| = \prod_{r=1}^{m} |pf(\alpha_r) + k(\alpha_r)| = \prod_{r=1}^{m} |pf(\alpha_r) + a|,$$

the last expression arising from $0 = h(\alpha_r) = k(\alpha_r) - a$ for $1 \leq r \leq m$. It follows that

$$\delta(ag, h) = \prod_{r=1}^{m} |pf(\alpha_r) + a| = |p\psi(\alpha_1, \dots, \alpha_m) + a^m|,$$

where ψ is a symmetric expression in $\alpha_1, \dots, \alpha_m$, with integer coefficients, and so is an integer. Hence,

$$a^m \delta(g, h) = \delta(ag, h) \equiv \pm a^m \pmod{p},$$

and therefore, $\delta(g, h) \equiv \pm 1 \pmod{p}$. If $\delta(g, h) \equiv -1 \pmod{p}$ then $\delta(g, h') \equiv 1 \pmod{p}$ where $h' \equiv h^2$, so replace h with h'. □

We illustrate the method used in the proof of Lemma 4.2.8 in the following example.

Example 4.2.9. Let $g(x) = 3x^4 - 2x^3 + 5x^2 - 8$ and the prime $p = 5$. Then write g in the form $g(x) = 5(-x^3 + x^2 - 2) + 3x^4 + 3x^3 + 2$. Next, $2g(x) = 5(-2x^3 + 2x^2 - 4) + 6x^4 + 6x^3 + 4$ which can be rewritten as $2g(x) = 5(x^4 - x^3 + 2x^2 - 4) + x^4 + x^3 + 4$. Finally, set $h(x) = x^4 + x^3 + 2$ and calculate: $\delta(g, h) = 69976 \equiv 1 \pmod{5}$.

Proposition 4.2.10. *Denote by f, g non-zero polynomials from $\mathbb{Z}[x]$, and suppose that $\delta(f, h) \mid \delta(g, h)$ for every monic $h \in \mathbb{Z}[x]$ where $\delta(f, h) \neq 0$. Then $f \mid g$.*

Proof. Because $\mathbb{Z}[x]$ is a subring of the Euclidean domain $\mathbb{Q}[x]$, we can use the division algorithm in $\mathbb{Q}[x]$ to find polynomials $k, r \in \mathbb{Q}[x]$ such that $g = kf + r$, where $\partial(r) < \partial(f)$. We aim to show that $r \equiv 0$ and then that $k \in \mathbb{Z}[x]$ and we begin by obtaining a contradiction to the assumption that $r \neq 0$.

Fix an integer $N > \max\{|\alpha| : \alpha \in \mathbb{C} \text{ and } f(\alpha) = 0\}$; then for all integers $n \geq N$ we have $f(n) \neq 0$. Therefore, if $h_n(x) = x - n$ for $n \geq N$, we have: $h_n \in \mathbb{Z}[x]$ is monic and $\delta(f, h_n) = |f(n)| \neq 0$. Find an integer $m > 0$ so that $mk, mr \in \mathbb{Z}[x]$. Then

$$m\delta(g, h_n) = |mk(n)f(n) + mr(n)| = \delta(f, h_n)|mk(n) + mr(n)/f(n)|,$$

so since $\delta(f, h_n) \mid \delta(g, h_n)$, and $mk(n), mr(n) \in \mathbb{Z}$, it follows that $f(n) \mid mr(n)$ for all integers $n \geq N$. However, because we are assuming that $0 \leq \partial(r) < \partial(f)$, we have $\lim_{n\to\infty} |mr(n)/f(n)| = 0$ and so there is an integer $N_1 \geq N$ such that for every $n \geq N_1$, $|f(n)| > |mr(n)|$, which clearly contradicts $f(n) \mid mr(n)$ for all integers $n \geq N$. It follows that $r \equiv 0$ and so $g = kf$. We will now show that $k \in \mathbb{Z}[x]$.

There exist integers a and b such that

$$a, b \geq 1, \ \gcd(a, b) = 1 \text{ and } k = \frac{a}{b}w,$$

where the polynomial $w \in \mathbb{Z}[x]$ is primitive. Similarly, there is an integer $c > 0$ such that $f = cv$, with $v \in \mathbb{Z}[x]$ primitive. This gives $bg = acwv$ and it is clear from this that the proof will be complete if we can show that $b = 1$. Assuming that this is not the case, let p be a prime factor of b. Since both w and v are primitive, wv is primitive. Therefore, by Lemma 4.2.8, there is a monic polynomial $h \in \mathbb{Z}[x]$ such that $\delta(wv, h) \equiv 1 \pmod{p}$. If $\partial(h) = d > 0$, then

$$b^d\delta(g, h) = a^d c^d \delta(wv, h).$$

Noting that $\delta(wv, h) = \delta(w, h)\delta(v, h)$, we see that $\delta(v, h) \neq 0$, which implies

$$0 \neq c^d\delta(v, h) = \delta(cv, h) = \delta(f, h).$$

It follows from this that $c^d \mid \delta(g, h)$ since $\delta(f, h) \mid \delta(g, h)$. Therefore

$$\frac{a^d}{b^d}\delta(wv, h) = \frac{\delta(g, h)}{c^d} \in \mathbb{Z},$$

so, since $p \mid b$ and $\delta(wv, h) \equiv 1 \pmod{p}$, this implies that $p \mid a$, which contradicts $\gcd(a, b) = 1$. Hence we must have $b = 1$. □

The following result is the converse to the divisibility sequence statement of Proposition 4.2.5.

Theorem 4.2.11. *Let $f = (f_n)$ denote a sequence of non-zero polynomials from the ring $\mathbb{Z}[x]$. If for any monic polynomial $h \in \mathbb{Z}[x]$, the integer sequence $(\Delta_n^{(f)}(h))$ is such that $\Delta_n^{(f)}(h)$ is a multiple of $\Delta_m^{(f)}(h)$ when $m \mid n$, then f is a divisibility sequence of polynomials.*

Proof. Given integers $m, n \geq 1$ with $m \mid n$, the conditions imply that $\delta(f_m, h) \mid \delta(f_n, h)$ for every monic $h \in \mathbb{Z}[x]$ where $\delta(f_m, h) \neq 0$. By Proposition 4.2.10 we get $f_m \mid f_n$, and so f is a divisibility sequence of polynomials. □

From here to the end of the section we will concentrate on divisibility sequences of polynomials $f = (f_n)$ and their *associated* Lehmer-Pierce type integer sequences $(\Delta_n^{(f)}(h))$ of Definition 4.2.1. The main task will be to construct algebraically realizable sequences by this means, though as an aside the techniques will indicate methods for the production of integer divisibility sequences of quite complex structure.

A natural way of constructing polynomial divisibility sequences is to analyze the sequence ς in order to determine possible routines. So the first question to consider is: why does $\varsigma_m \mid \varsigma_n$ when $m \mid n$? An obvious answer is: because of (4.1), but this does not readily provide routines which can be generalized. However, a closer look at this equation does in fact suggest some methods.

If we denote the complex number $e^{2\pi i/n}$ by ϱ_n, then for any positive integer n we have the factorization

$$\varsigma_n(x) = \prod_{k=1}^{n} (x - \varrho_n^k).$$

Now if m denotes a positive integer such that $m \mid n$,

$$\varsigma_m(x) = \prod_{k=1}^{m}(x - \varrho_n^{kn/m}),$$

which not only explains why $\varsigma_m \mid \varsigma_n$, but on noting that

$$\mathbb{S}^1_n = \{\varrho_n^k : 1 \leq k \leq n\} \text{ and } \mathbb{S}^1_m = \{\varrho_n^{kn/m} : 1 \leq k \leq m\},$$

gives the alternative formulation:

$$\varsigma_n(x) = \prod_{\sigma \in \mathbb{S}^1_n}(x - \sigma) \text{ and } \varsigma_m(x) = \prod_{\sigma \in \mathbb{S}^1_m}(x - \sigma).$$

Since the subgroups $\mathbb{S}^1_m, \mathbb{S}^1_n$ of $\mathbb{S}^1_\omega$ have $\mathbb{S}^1_m \leq \mathbb{S}^1_n$ when $m \mid n$, this also indicates why $\varsigma_m \mid \varsigma_n$, with Lagrange's Theorem providing a partial converse. It is this second method of construction which we will utilize because it suggests further generalizations, a possible candidate being to replace the groups $\mathbb{S}^1_n$ with the torsion subgroups associated with a particular elliptic curve. We will not pursue this here, but note that it does lead to divisibility sequences (both integer and polynomial) which have very interesting structures.

If $g \in \mathbb{Z}[x, y]$ denotes the simple polynomial $g(x, y) = x - y$, then for any $n \in \mathbb{N}$,

$$\varsigma_n(t) = \prod_{\sigma \in \mathbb{S}^1_n} g(t, \sigma),$$

from which we are led to the next definition.

Definition 4.2.12. Let $g \in \mathbb{Z}[x, y]$ denote a polynomial with the following properties:

(1) $\partial_x(g) \geq 1$
(2) $\partial_t(g(t, \sigma)) = \partial_x(g)$ for all $\sigma \in \mathbb{S}^1_\omega$.

Then for each integer $n \geq 1$, the polynomial $\varsigma_n^{(g)}$ is defined by

$$\varsigma_n^{(g)}(t) = \prod_{\sigma \in \mathbb{S}^1_n} g(t, \sigma).$$

The reason the two conditions are imposed on g in this definition is to ensure that for all $n \geq 1$, $\varsigma_n^{(g)}(t)$ is never a *constant* function of the variable t. Although this is not a strictly necessary restriction, it simplifies matters considerably and we will assume the conditions to be in place whenever the notation $\varsigma_n^{(g)}$ is used. We will, however, revert to our customary notation of ς_n for this polynomial when $g(x, y) \equiv x - y$.

Example 4.2.13. If $g \in \mathbb{Z}[x, y]$ denotes $g(x, y) = (2 - y)x - y$, then the sequence of polynomials $(\varsigma_n^{(g)}(t))_{n \geq 1}$ is

$$(t - 1, 3t^2 - 2t - 1, 7t^3 - 11t^2 + 5t - 1, 15t^4 - 4t^3 - 6t^2 - 4t - 1, \ldots).$$

Proposition 4.2.14. *For each integer $n \geq 1$, the polynomial $\varsigma_n^{(g)}$ of Definition 4.2.12 is a member of the ring $\mathbb{Z}[t]$. Further, the sequence $(\varsigma_n^{(g)})_{n \geq 1}$ is a proper divisibility sequence of polynomials.*

Proof. The fact that $\varsigma_n^{(g)} \in \mathbb{Z}[t]$ is an immediate consequence of Lemma 4.2.3. And because of the restrictions placed upon the polynomial $g \in \mathbb{Z}[x, y]$, it is easy to see that $\partial(\varsigma_n^{(g)}) = n\partial_x(g)$, so that $1 \leq \partial(\varsigma_n^{(g)}) < \partial(\varsigma_{n+1}^{(g)})$ for all $n \geq 1$. Finally, since $\mathbb{S}_m^1 \leq \mathbb{S}_n^1$ when $m \mid n$, the sequence $(\varsigma_n^{(g)})$ is a divisibility sequence of polynomials. □

The next example will help illustrate the theory to follow. It shows how from a polynomial $g \in \mathbb{Z}[x, y]$, subject to certain conditions, and a monic polynomial $h \in \mathbb{Z}[x]$, we can obtain an algebraically realizable sequence of integers by using the polynomial sequence $(\varsigma_n^{(g)})$.

Example 4.2.15. Let $g \in \mathbb{Z}[x, y]$ denote $g(x, y) = 12x^2 + 6xy + y^2$ and $h \in \mathbb{Z}[x]$ the monic polynomial $h(x) = x^2 - x - 1$. If the zeros of h are α and β, denote by $\tilde{g}_h$ the polynomial given by: $\tilde{g}_h(t) = g(\alpha, t)g(\beta, t)$. Then we calculate

$$\tilde{g}_h(t) = t^4 + 6t^3 - 72t + 144 \in \mathbb{Z}[t].$$

It is easy to see that the set of zeros of the monic polynomial $\tilde{g}_h$ is disjoint from the set $\mathbb{S}^1_\omega$, so by Theorem 4.1.12 the sequence of integers

$$(\Delta_n(\tilde{g}_h)) = (79, 16669, 3017089, 451879921, 64312113889, \dots) \tag{4.2}$$

is algebraically realizable.

Next we calculate the sequence of polynomials $\hat{g} = (\varsigma_n^{(g)}(t))$ as:

$$(12t^2 + 6t + 1, 144t^4 - 12t^2 + 1, 1728t^6 + 1, 20736t^8 + 144t^4 + 1, \dots).$$

And finally we obtain the Lehmer-Pierce type integer sequence

$$(\Delta_n^{(\hat{g})}(h)) = (79, 16669, 3017089, 451879921, 64312113889, \dots),$$

which is identical with the sequence calculated above in (4.2), and so is algebraically realizable.

First we note some things about the previous example – apart from the increasing complications in the notation. Lemma 4.2.3 guarantees that the function $\tilde{g}_h$ is a member of the ring $\mathbb{Z}[t]$. So provided the pair (g, h) are such that $\tilde{g}_h$ is a monic polynomial with a set of zeros which is disjoint from the group $\mathbb{S}^1_\omega$, then Theorem 4.1.12 establishes the fact that the Lehmer-Pierce sequence $(\Delta_n(\tilde{g}_h))$ is algebraically realizable.

Next, the equivalence between the two sequences $(\Delta_n(\tilde{g}_h))$ and $(\Delta_n^{(\hat{g})}(h))$ will be shown to be a property of the various constructions we have made. Thus we see that Example 4.2.15 results in an algebraically realizable sequence of integers mainly because of the choice of the two polynomials $g \in \mathbb{Z}[x, y]$ and $h \in \mathbb{Z}[x]$.

We finish this section with a result in which the number of conditions imposed can certainly be reduced: however, to do so would require a different approach to the Lehmer-Pierce construction – in particular, one in which the polynomial does not have to be monic. Although this approach is not a great deal more difficult – with the first steps in this direction being already supplied by Lemma 4.2.3 and Definition 4.2.6, it does increase the complexity of the notation, and to avoid this we have sacrificed some generality.

Theorem 4.2.16. *Let $h \in \mathbb{Z}[x]$ denote a monic polynomial with zeros $\alpha_1, \ldots, \alpha_d$, where $d = \partial(h)$. For* any *$g \in \mathbb{Z}[x, y]$, we write $\tilde{g}_h \in \mathbb{Z}[t]$ to denote the polynomial*

$$\tilde{g}_h(t) = \prod_{r=1}^{d} g(\alpha_r, t).$$

Suppose the polynomial $g \in \mathbb{Z}[x, y]$ is such that the following conditions hold:

(1) $\partial_x(g) \geq 1$

(2) $\partial_t(g(t, \sigma)) = \partial_x(g)$ *for all* $\sigma \in \mathbb{S}^1_\omega$

(3) $\tilde{g}_h$ *is a monic polynomial*

(4) $\{\beta \in \mathbb{C} : \tilde{g}_h(\beta) = 0\} \cap \mathbb{S}^1_\omega = \emptyset$.

If $\hat{g}$ denotes the sequence of polynomials $(\varsigma_n^{(g)})$, then the integer sequence $(\Delta_n^{(\hat{g})}(h))$ is algebraically realizable.

Proof. By the first two conditions imposed on g and Proposition 4.2.14, the sequence $\hat{g}$ is a proper divisibility sequence of polynomials in $\mathbb{Z}[t]$, so the integer sequence $(\Delta_n^{(\hat{g})}(h))$ is well-defined. Whereas conditions (3) and (4) alongside Theorem 4.1.12 imply that $(\Delta_n(\tilde{g}_h))$ is an algebraically realizable sequence of integers. Therefore, to complete the proof, it is sufficient to show that the two integer sequences are the same.

Denote by n a fixed positive integer. If the zeros of the polynomial $\tilde{g}_h \in \mathbb{Z}[t]$ are $\beta_1, \ldots, \beta_c$ where $c = \partial(\tilde{g}_h)$, then

$$\Delta_n(\tilde{g}_h) = \prod_{k=1}^{c} |\beta_k^n - 1|$$

by the definition of the Lehmer-Pierce sequence. Now, by using

$$\beta_k^n - 1 = \prod_{\sigma \in \mathbb{S}^1_n} (\beta_k - \sigma),$$

we get

$$\Delta_n(\tilde{g}_h) = \left| \prod_{\sigma \in \mathbb{S}_n^1} \prod_{k=1}^{c} (\sigma - \beta_k) \right| = \prod_{\sigma \in \mathbb{S}_n^1} |\tilde{g}_h(\sigma)|.$$

It follows from this and the definition of the polynomial $\tilde{g}_h$, that

$$\Delta_n(\tilde{g}_h) = \prod_{\sigma \in \mathbb{S}_n^1} \prod_{r=1}^{d} |g(\alpha_r, \sigma)|,$$

and so by Definition 4.2.12,

$$\Delta_n(\tilde{g}_h) = \prod_{r=1}^{d} |\varsigma_n^{(g)}(\alpha_r)|.$$

Therefore, $\Delta_n(\tilde{g}_h) = \Delta_n^{(\hat{g})}(h)$ using Definition 4.2.1, and this completes the proof. □

Problem 4.2.17. Find further classes of divisibility sequences of polynomials for which the associated Lehmer-Pierce type integer sequences are (algebraically) realizable.

4.3. Generalizations and Measures

In this section we will consider a possible generalization of the standard Lehmer-Pierce sequence to multi-dimensional polynomials. We will also briefly look at the important topic of the *Mahler Measure* of a sequence. First, however, we prove a simple *reciprocal* property for the quantity $\delta(g, h)$ of Definition 4.2.6.

Proposition 4.3.1. *If g, h denote polynomials from $\mathbb{Z}[x]$ with degrees $\partial(g), \partial(h) \geq 1$, then $\delta(g, h) = \delta(h, g)$.*

Proof. Let the factorizations of g, h over $\mathbb{C}$ be

$$g(x) = a_g(x - \alpha_1) \cdots (x - \alpha_m) \text{ and } h(x) = b_h(x - \beta_1) \cdots (x - \beta_n).$$

Then from Definition 4.2.6,

$$\begin{aligned}
\delta(g,h) &= |b_h|^m \prod_{j=1}^{n} |g(\beta_j)| \\
&= |b_h|^m \prod_{j=1}^{n} \left(|a_g| \prod_{k=1}^{m} |\beta_j - \alpha_k| \right) \\
&= |a_g|^n \prod_{k=1}^{m} \left(|b_h| \prod_{j=1}^{n} |\alpha_k - \beta_j| \right) \\
&= |a_g|^n \prod_{k=1}^{m} |h(\alpha_k)| \\
&= \delta(h,g),
\end{aligned}$$

which completes the proof. □

Now, if $h \in \mathbb{Z}[x]$ is a monic polynomial, the nth term of the Lehmer-Pierce sequence $(\Delta_n(h))$ is equal to $\delta(\varsigma_n, h)$, so Proposition 4.3.1 gives $\Delta_n(h) = \delta(h, \varsigma_n)$. Therefore we have the formulation

$$\Delta_n(h) = \prod_{\sigma \in \mathbb{S}^1_n} |h(\sigma)|, \tag{4.3}$$

and since Proposition 4.3.1 does not require the polynomial h to be monic, (4.3) could be used as the starting point for the definition of the Lehmer-Pierce sequence associated with an *arbitrary* non-zero polynomial $h \in \mathbb{Z}[x]$. If this procedure is adopted, then results similar to those above can be established, and in particular the following is true.

Theorem 4.3.2. *Let $h \in \mathbb{Z}[x]$ denote a non-zero polynomial which is such that*

$$\{\alpha \in \mathbb{C} : h(\alpha) = 0\} \cap \mathbb{S}^1_\omega = \emptyset.$$

If the Lehmer-Pierce sequence $\Delta(h) = (\Delta_n(h))$ is defined by (4.3), then $\Delta(h)$ is algebraically realized by an abelian system.

Proof. For the proof of this result we refer to [**10**]. □

Let m, n denote positive integers. We will write $\mathbb{T}_n^m$ for the group $(\mathbb{S}_n^1)^m$. Using (4.3), a natural extension of the Lehmer-Pierce construction to multi-dimensional polynomials is suggested.

Definition 4.3.3. Let $f \in \mathbb{Z}[x_1, \dots, x_m]$ denote a non-zero polynomial. The sequence $(\Delta_n(f))_{n\geq 1}$ is defined by

$$\Delta_n(f) = \prod_{(\sigma_1,\dots,\sigma_m)\in\mathbb{T}_n^m} |f(\sigma_1, \dots, \sigma_m)|, \quad n = 1, 2, 3, \dots.$$

We note that if $m = 1$ then this reduces to the standard Lehmer-Pierce sequence of integers when f is monic, or to the extension of the sequence suggested above, otherwise. Obviously, other generalizations of this sequence are suggested by (4.3): for example, taking each σ_j in the above formula from $\mathbb{S}_{n_j}^1$ where the point $(n_1, \dots, n_m)$ is specified in some way. Or the σ_j could be the zeros of some sequence of monic polynomials. We will not pursue this, though it is of interest.

Proposition 4.3.4. *If $f \in \mathbb{Z}[x_1, \dots, x_m]$ denotes a non-zero polynomial, then $(\Delta_n(f))_{n\geq 1}$ is a sequence of non-negative integers.*

Proof. This follows inductively from Lemma 4.2.3. □

Example 4.3.5. If $f(x, y) = 2x + y^{12} - 4 \in \mathbb{Z}[x, y]$ then the sequence $(\Delta_n(f))$ is calculated as:

$$(1, 25, 6859, 17850625, 932232699865951, 86482825840140625, \dots).$$

Apart from special cases, the terms of the sequence $(\Delta_n(f))$ grow quite fast. Indeed, for the above example we have

$$\Delta_9(f) = 35323608464050136636624299250570641585970401128 31.$$

A cursory look at this sequence suggests that it is realizable, and this is indeed the case.

Theorem 4.3.6. *If $f \in \mathbb{Z}[x_1, \ldots, x_m]$ denotes a non-zero polynomial, then the sequence $(\Delta_n(f))$ can be algebraically realized by an abelian system provided that no term of the sequence is zero.*

Proof. Refer to [**10**] – a special case, and [**18**] for the general case. □

Example 4.3.7. Denote by $f \in \mathbb{Z}[x, y, z]$ the polynomial given by

$$f(x, y, z) = (x - 2z)(1 - y^2) + 7,$$

and for $m = 1, 2, 3$, let $\hat{f}_n^{(m)}$ denote the polynomial

$$\hat{f}_n^{(m)}(t) = \prod_{\sigma \in \mathbb{S}_n^1} \prod_{\varrho \in \mathbb{S}_n^1} f(\mathbf{w}), \quad n = 1, 2, 3, \ldots,$$

where

$$\mathbf{w} = \begin{cases} (t, \sigma, \varrho), & \text{m=1} \\ (\sigma, t, \varrho), & \text{m=2} \\ (\sigma, \varrho, t), & \text{m=3.} \end{cases}$$

Lemma 4.2.3 guarantees that $\hat{f}_n^{(m)} \in \mathbb{Z}[t]$ for $m = 1, 2, 3$, $n \geq 1$, and we calculate:

$$\begin{aligned} (\hat{f}_n^{(1)}(t)) &= (7, 2401, 9261t^6 + 194481t^5 + \cdots, \ldots) \\ (\hat{f}_n^{(2)}(t)) &= (t^2 + 6, 9t^8 - 36t^6 - 436t^4 + 994t^2 + 1920, \ldots) \\ (\hat{f}_n^{(3)}(t)) &= (7, 2401, 592704t^6 - 6223392t^5 + \cdots, \ldots). \end{aligned}$$

Further calculation gives the generalized Lehmer-Pierce sequence associated with the polynomial f by Definition 4.3.3:

$$(7, 5764801, 618206354824938698990008, \ldots). \tag{4.4}$$

We note that the sequences $(\delta(\hat{f}_n^{(1)}, \varsigma_n))$, $(\delta(\hat{f}_n^{(2)}, \varsigma_n))$ and $(\delta(\hat{f}_n^{(3)}, \varsigma_n))$ are all equal to the sequence (4.4).

The next result is based upon Example 4.3.7.

Proposition 4.3.8. *Denote by $f \in \mathbb{Z}[x_1, \ldots, x_m]$ a non-zero polynomial, and for $k = 1, \ldots, m$, $n \geq 1$, let $\hat{f}_n^{(k)}$ denote the polynomial*

$$\hat{f}_n^{(k)}(t) = \prod_{(\sigma_1,\ldots,\sigma_{k-1})\in\mathbb{T}_n^{k-1}} \prod_{(\varrho_{k+1},\ldots,\varrho_m)\in\mathbb{T}_n^{m-k}} f(\sigma_1, \ldots, \sigma_{k-1}, t, \varrho_{k+1}, \ldots, \varrho_m).$$

Then $\hat{f}_n^{(k)} \in \mathbb{Z}[t]$ and,

$$(\Delta_n(f)) = (\delta(\hat{f}_n^{(k)}, \varsigma_n))_{n\geq 1},\ k = 1, \ldots, m.$$

If for a fixed value of j in the range $1 \leq j \leq m$, the sequence of polynomials $(\hat{f}_n^{(j)})_{n\geq 1}$ is such that

$$\mathbb{S}^1_\omega \cap \left(\bigcup_{n\geq 1} \{\alpha \in \mathbb{C} : \hat{f}_n^{(j)}(\alpha) = 0\} \right) = \emptyset,$$

then

$$\mathbb{S}^1_\omega \cap \left(\bigcup_{n\geq 1} \{\alpha \in \mathbb{C} : \hat{f}_n^{(k)}(\alpha) = 0\} \right) = \emptyset \textit{ for } k = 1, \ldots, m. \tag{4.5}$$

Given that (4.5) holds, the sequence $(\Delta_n(f))$ is algebraically realizable and for $k = 1, \ldots, m$, $(\hat{f}_n^{(k)})_{n\geq 1}$ is a divisibility sequence of polynomials.

Proof. The fact that $\hat{f}_n^{(k)} \in \mathbb{Z}[t]$, is a consequence of Lemma 4.2.3; and $(\Delta_n(f)) = (\delta(\hat{f}_n^{(k)}, \varsigma_n))$ follows directly from the definition of $\Delta_n(f)$. If for some fixed j in the range $1 \leq j \leq m$ we have

$$\mathbb{S}^1_\omega \cap \left(\bigcup_{n\geq 1} \{\alpha \in \mathbb{C} : \hat{f}_n^{(j)}(\alpha) = 0\} \right) = \emptyset,$$

then the sequence $(\Delta_n(f))$ has no zero terms, so

$$\mathbb{S}^1_\omega \cap \left(\bigcup_{n\geq 1} \{\alpha \in \mathbb{C} : \hat{f}_n^{(k)}(\alpha) = 0\} \right) = \emptyset \text{ for } k = 1, \ldots, m.$$

By Theorem 4.3.6, $(\Delta_n(f))$ is an algebraically realizable sequence if it has no zero terms, and this follows if (4.5) holds. Finally, it is clear that when (4.5) holds, $(\hat{f}_n^{(k)})_{n\geq 1}$ is a divisibility sequence of polynomials since for any positive integers a, b, c, if $a \mid b$ then $\mathbb{T}_a^c \leq \mathbb{T}_b^c$. □

In the notation of the previous result, since $\delta(\hat{f}_n^{(k)}, \varsigma_n) = \Delta_n(\hat{f}_n^{(k)})$, we see that the sequence $(\Delta_n(f))$ of Definition 4.3.3 is a definite generalization of the original Lehmer-Pierce sequence, and could lead to a new definition using a divisibility sequence of polynomials (h_n) in place of the original fixed monic polynomial h.

We will finish this section with a brief look at the Mahler measure of a Lehmer-Pierce sequence. This is a (logarithmic) measure of the rate of growth of the sequence. First some technical results, using the notation of Proposition 4.3.8.

Lemma 4.3.9. *Let $f \in \mathbb{Z}[x_1, \ldots, x_m]$ be a non-zero polynomial. Then for each integer $n \geq 1$, $\partial(\hat{f}_n^{(k)}) \leq n^{m-1}\partial_{x_k}(F)$. If the leading coefficient of $\hat{f}_n^{(k)}$ is $b_n^{(k)}$, then there exists a positive integer c, dependent only upon the polynomial f, such that $|b_n^{(k)}| \leq c^{n^{m-1}}$ for all $n \geq 1$.*

Proof. It is easy to see from the definition of the polynomial $\hat{f}_n^{(k)}$ that $\partial(\hat{f}_n^{(k)}) \leq n^{m-1}\partial_{x_k}(f)$ for every $n \geq 1$. For the remainder of the proof, since the result is clear if $\hat{f}_n^{(k)} \equiv 0$, we will assume that $\hat{f}_n^{(k)}$ is not the zero polynomial. Further, in order to make the notation easier, we will assume that $k = 1$. Thus we will show that for $\hat{f}_n^{(1)}(t) = a_n t^s + \cdots + a_0^{(n)}$, where $s = s(n) = \partial(\hat{f}_n^{(1)})$, there exists a positive integer constant c such that $|a_n| \leq c^{n^{m-1}}$ for all $n \geq 1$.

We can express the polynomial f in the form

$$f(x_1, x_2, \ldots, x_m) = g_d(x_2, \ldots, x_m)x_1^d + \cdots + g_0(x_2, \ldots, x_m),$$

where $g_r \in \mathbb{Z}[x_2, \ldots, x_m],\ r = 0, \ldots, d$. Here we have $d = \partial_{x_1}(f) \geq 0$. Consider a non-zero polynomial g_r for some r in the range $0 \leq r \leq d$. This polynomial is of the form

$$g_r(x_2, \ldots, x_m) = \sum_{j_2, \ldots, j_m} h_{j_2 \cdots j_m} x_2^{j_2} \cdots x_m^{j_m},$$

where $j_2, \ldots, j_m$ are non-negative integers and each $h_{j_2 \cdots j_m} \in \mathbb{Z}$. We define the positive integer q_r by

$$q_r = \sum_{j_2, \ldots, j_m} |h_{j_2 \cdots j_m}|.$$

Next, if for any r in the range $0 \leq r \leq d$ we have $g_r = 0$, then we put $q_r = 1$. Thus we now have a complete set $\{q_0, \ldots, q_d\}$ of positive integers. Let the positive integer $c = \max\{q_0, \ldots, q_d\}$. We note that c does not depend on n, but only on the polynomial f. Now, given any integers $j_2, \ldots, j_m$ in the range $0 \leq j_2, \ldots, j_m \leq n-1$, the polynomial $f(t, \varrho^{j_2}, \ldots, \varrho^{j_m}) \in \mathbb{C}[t]$, where $\varrho = \exp(2\pi i/n)$, is non-zero since $\hat{f}_n^{(1)} \neq 0$. Let the leading coefficient of $f(t, \varrho^{j_2}, \ldots, \varrho^{j_m})$ be $b_{j_2 \cdots j_m}$. Then the leading coefficient a_n of $\hat{f}_n^{(1)}$ is given by,

$$a_n = \prod_{j_2=0}^{n-1} \cdots \prod_{j_m=0}^{n-1} b_{j_2 \cdots j_m}.$$

By the definition of the constant c, since $|\varrho| = 1$, we clearly have $|b_{j_2 \cdots j_m}| \leq c$ for all possible choices of $j_2, \ldots, j_m$. It follows that

$$|a_n| \leq \prod_{j_2=0}^{n-1} \cdots \prod_{j_m=0}^{n-1} c.$$

This gives $|a_n| \leq c^{n^{m-1}}$ and completes the proof. □

We now consider the sequence $(\log^+ \Delta_n(f))_{n \geq 1}$, where the polynomial $f \in \mathbb{Z}[x_1, \ldots, x_m]$ and the notation $\log^+ x = \log \max\{1, x\},\ x \in \mathbb{R}$ is used. The terms of this sequence will be shown have order $O(n^m)$ in the case where there are no zero terms in the Lehmer-Pierce sequence $(\Delta_n(f))$, so that the sequence $(\log^+ \Delta_n(f)/n^m)$ is bounded. This will enable us to define a logarithmic measure of the polynomial f in terms of the integer sequence $(\Delta_n(f))$.

Lemma 4.3.10. *Let $f \in \mathbb{Z}[x_1, \ldots, x_m]$ denote a polynomial which is such that the sequence $(\Delta_n(f))$ has no zero terms. Then for all $n \geq 1$, $\log^+ \Delta_n(f) = O(n^m)$.*

Proof. If k denotes an integer with $1 \leq k \leq m$, then Proposition 4.3.8 gives $\Delta_n(f) = \delta_n(\hat{f}_n^{(k)}, \varsigma_n)$. Fix k and $n \geq 1$, and let the polynomial $\hat{f}_n^{(k)}$ factorize over $\mathbb{C}$ as:

$$\hat{f}_n^{(k)}(t) = a_d(t-\alpha_1)\cdots(t-\alpha_d),\ d = \partial(\hat{f}_n^{(k)}).$$

Using Proposition 4.3.1,

$$\Delta_n(f) = \delta(\varsigma_n, \hat{f}_n^{(k)}) = |a_d|^n \prod_{j=1}^{d} |\alpha_j^n - 1|.$$

It follows that

$$\log^+ \Delta_n(f) = n \log^+ |a_d| + \sum_{j=1}^{d} \log^+ |\alpha_j^n - 1|.$$

Now, from Lemma 4.3.9 we know that $d \leq n^{m-1} b_k$ where $b_k = \partial_{x_k}(f)$, and there exists a constant $c \geq 1$ such that $|a_d| \leq c^{n^{m-1}}$. This implies that $\log^+ |a_d| \leq \log c^{n^{m-1}} = n^{m-1} \log c$, so $n \log^+ |a_d| \leq n^m \log c$, which gives $n \log^+ |a_d| = O(n^m)$.

In [**10**] the authors use Baker's theorem (see [**7**]) to obtain the following estimate, where β denotes an algebraic number which does not belong to $\mathbb{S}^1_\omega$:

$$\log^+ |\beta^n - 1| = \begin{cases} O(n), & \text{if } |\beta| \neq 1 \\ O(\log n), & \text{if } |\beta| = 1. \end{cases}$$

It follows that

$$\sum_{j=1}^{d} \log^+ |\alpha_j^n - 1| = O(dn),$$

and so since $d \leq n^{m-1} b_k$,

$$\sum_{j=1}^{d} \log^+ |\alpha_j^n - 1| = O(n^m).$$

Thus we have $\log^+ \Delta_n(f) = O(n^m) + O(n^m) = O(n^m)$. □

It follows from Lemma 4.3.10 that the sequence $(\log^+ \Delta_n(f)/n^m)$ is bounded above, so the next definition makes sense.

Definition 4.3.11. If $f \in \mathbb{Z}[x_1, \ldots, x_m]$ denotes a non-zero polynomial, then the logarithmic *Mahler measure* of f, written as $m(f)$, is defined by

$$m(f) = \limsup_{n\to\infty} \frac{\log^+ \Delta_n(f)}{n^m}.$$

Example 4.3.12. Let $f \in \mathbb{Z}[x, y]$ denote $f(x, y) = x - y + 3$. Then for a fixed integer $n \geq 1$ we calculate:

$$\hat{f}_n^{(1)}(t) = \prod_{\sigma\in\mathbb{S}_n^1} f(t, \sigma) = \prod_{\sigma\in\mathbb{S}_n^1} ((t + 3) - \sigma) = (t + 3)^n - 1.$$

By Proposition 4.3.8,

$$\Delta_n(f) = \prod_{\sigma\in\mathbb{S}_n^1} ((\sigma + 3)^n - 1),$$

which gives the approximation $m(f) = 1.0986122886681096914$ (this is equal to $\log 3$) from the 100th term of the sequence $(\Delta_n(f))$.

The usual definition of the Mahler measure of a non-zero polynomial $f \in \mathbb{Z}[x_1, \ldots, x_m]$ is the multiple integral

$$m(f) = \int_0^1 \cdots \int_0^1 \log |f(e^{2\pi i t_1}, \ldots, e^{2\pi i t_m})| \mathrm{d}t_1 \ldots \mathrm{d}t_m.$$

It is easy to check that the value calculated in Example 4.3.12 agrees with the value of this integral, and it is possible by using more detailed analysis to show that the measure of Definition 4.3.11 is equivalent to the usual definition of the measure for a large class of polynomials. We will not take this further, but instead pose the question: Is it possible to generalize Definition 4.3.11 in some way to give a (meaningful) measure for an algebraically realizable sequence of integers? In the case of a sequence $u = (u_n)$ realized on an infinite minimal (in the sense of Lemma 3.1.3) abelian system (X, ϑ), perhaps something like:

$$m(u) = \limsup_{n\to\infty} \frac{\log u_n}{n^r},$$

where r is the rank of the abelian group X.

CHAPTER 5

Periodic Points and Arithmetic

5.1. Introduction

In this chapter, we will look at the sequences of Bernoulli and Euler numbers from a *dynamical* point of view. We will require the use of several classical results (for example, theorems of von Staudt-Clausen and Kummer) and this begs the question: can the procedure be reversed so that the classical results are obtained from dynamical considerations? We do not attempt to answer this question, but suggest that the results obtained indicate that it may have a positive solution.

5.2. The Euler Numbers

The sequence of *Euler Numbers* $(E_n)_{n\geq 0}$ is defined by the equation

$$\frac{2}{e^t+e^{-t}}=\sum_{n=0}^{\infty}E_n\frac{t^n}{n!}. \tag{5.1}$$

It is known that each E_n, $n\geq 0$, is an integer. Since the left hand side of (5.1) is an even function of t, $E_n=0$ for all odd n, and for $m\geq 0$, we have $(-1)^m E_{2m}>0$. A congruence due to Kummer [**16**] is: for all $n\geq 1$ and odd prime p,

$$E_{2n+p-1}\equiv E_{2n} \pmod{p}.$$

It follows easily that if the integers m,n are such that $1\leq n\leq m$ and $2m\equiv 2n \pmod{p-1}$ then $E_{2m}\equiv E_{2n} \pmod{p}$. Theorem 5.2.3 below extends this congruence. First though, we introduce some notation and related results.

For integers m, n with $m \geq 1$ and $n \geq 0$, we write

$$A_n(m) = \sum_{k=1}^{m} (-1)^{m-k} k^n = m^n - (m-1)^n + \cdots + (-1)^{m-1} 1^n.$$

The next equation is shown to be true in [**28**]. If $p \geq 1$ is odd and $n > 0$ then

$$2^{2n+1} A_{2n}\left(\frac{p-1}{2}\right) = \sum_{k=0}^{2n} \binom{2n}{k} E_k p^{2n-k}. \tag{5.2}$$

We will make use of this equation in the following, with φ being used to denote the Euler φ-function.

Lemma 5.2.1. *Let p denote an odd prime and suppose that the integers $m, n, r \geq 1$ are such that $2m \equiv 2n \pmod{\varphi(p^r)}$. Then*

$$2^{2m+1} A_{2m}(c) \equiv 2^{2n+1} A_{2n}(c) \pmod{p^r},$$

where $c = (p-1)/2$.

Proof. Assume that $m \geq n$ and put $2m = 2n + s\varphi(p^r)$ where $s \geq 0$. Then $2^{2m+1} = 2^{2n+1}(2^{\varphi(p^r)})^s$ and so $2^{2m+1} \equiv 2^{2n+1} \pmod{p^r}$ by the Euler-Fermat Theorem. Next, if $1 \leq k \leq c$, then a second application of the Euler-Fermat Theorem gives $k^{2m} \equiv k^{2n} \pmod{p^r}$. It follows that

$$\begin{aligned} 2^{2m+1} A_{2m}(c) &= 2^{2m+1} \textstyle\sum_{k=1}^{c} (-1)^{c-k} k^{2m} \\ &\equiv 2^{2n+1} \textstyle\sum_{k=1}^{c} (-1)^{c-k} k^{2n} \pmod{p^r}. \end{aligned}$$

That is, $2^{2m+1} A_{2m}(c) \equiv 2^{2n+1} A_{2n}(c) \pmod{p^r}$. □

Lemma 5.2.2. *If m, n, r are such that $1 \leq r \leq 2n-1 \leq 2m-1$, and p denotes an odd prime with $2m \equiv 2n \pmod{\varphi(p^r)}$, then*

$$\sum_{k=0}^{r-1} \binom{2m}{k} E_{2m-k} p^k \equiv \sum_{k=0}^{r-1} \binom{2n}{k} E_{2n-k} p^k \pmod{p^r}.$$

Proof. Using (5.2) with $c = (p-1)/2$ we get

$$2^{2m+1} A_{2m}(c) = \sum_{k=0}^{2m} \binom{2m}{k} E_k p^{2m-k}$$

and

$$2^{2n+1}A_{2n}(c) = \sum_{k=0}^{2n} \binom{2n}{k} E_k p^{2n-k},$$

so Lemma 5.2.1 gives

$$\sum_{k=0}^{2m} \binom{2m}{k} E_k p^{2m-k} \equiv \sum_{k=0}^{2n} \binom{2n}{k} E_k p^{2n-k} \pmod{p^r}.$$

Reducing this expression mod p^r, and adjusting the range of summation, completes the proof. □

We now come to the main result in this section, the generalization of the Kummer congruence stated above.

Theorem 5.2.3. *If $m, n, r \in \mathbb{N}$ are such that $1 \leq r \leq 2n-1 \leq 2m-1$ and p denotes an odd prime with $2m \equiv 2n \pmod{\varphi(p^r)}$ then*

$$E_{2m} \equiv E_{2n} \pmod{p^r}.$$

Proof. If $r = 1$ in Lemma 5.2.2 then we get $E_{2m} \equiv E_{2n} \pmod{p}$ when $2m \equiv 2n \pmod{p-1}$ and $m \geq n \geq 1$. Therefore we will suppose that $r > 1$, and assume that when $1 \leq s < r$,

$$2m \equiv 2n \pmod{\varphi(p^s)} \text{ implies } E_{2m} \equiv E_{2n} \pmod{p^s}.$$

Since $\varphi(p^s) \mid \varphi(p^r)$ when $1 \leq s < r$, this means that we can assume that $E_{2m} \equiv E_{2n} \pmod{p^{r-1}}$ when $2m \equiv 2n \pmod{\varphi(p^r)}$. Now, from Lemma 5.2.2

$$E_{2m} + \sum_{k=1}^{r-1} \binom{2n}{k} (E_{2m-k} - E_{2n-k}) p^k +$$

$$+ \sum_{k=1}^{r-1} \left(\binom{2m}{k} - \binom{2n}{k} \right) E_{2m-k} p^k \equiv E_{2n} \pmod{p^r},$$

and by the assumption made, this reduces to

$$E_{2m} + \sum_{k=1}^{r-1} \left(\binom{2m}{k} - \binom{2n}{k} \right) E_{2m-k} p^k \equiv E_{2n} \pmod{p^r}.$$

Since $2m \equiv 2n \pmod{\varphi(p^r)}$ and $1 \leq k \leq r-1$, a simple consideration of the binomial coefficients gives

$$\binom{2m}{k} \equiv \binom{2n}{k} \pmod{p^{r-k}},$$

so we get $E_{2m} \equiv E_{2n} \pmod{p^r}$. □

Corollary 5.2.4. *Let p denote an odd prime and suppose $b, r \geq 1$ with $p \nmid b$. Then $E_{2p^r b} \equiv E_{2p^{r-1}b} \pmod{p^r}$.*

Proof. The conditions imply $1 \leq r \leq 2p^{r-1}b - 1 < 2p^r b - 1$, and so since $2p^r b \equiv 2p^{r-1}b \pmod{\varphi(p^r)}$, the result follows from Theorem 5.2.3. □

In [**28**] the following result is proved.

Theorem 5.2.5. *If k, n denote non-negative integers, then*

$$E_{2n} \equiv E_{2n+2^k} + 2^k \pmod{2^{k+1}}.$$

Using this result it is possible to extend Corollary 5.2.4 to include the prime 2.

Lemma 5.2.6. *If b, r denote positive integers with b odd, then*

$$E_{2^{r+1}b} \equiv E_{2^r b} \pmod{2^r}.$$

Proof. Using Theorem 5.2.5 gives

$$E_{2^{r+1}b} = E_{(2^{r+1}b-2^r)+2^r} \equiv E_{2^{r+1}b-2^r} + 2^r \pmod{2^{r+1}}.$$

Applying Theorem 5.2.5 again, $E_{2^{r+1}b-2^r} \equiv E_{2^{r+1}b-(2^r)2} + 2^r \pmod{2^{r+1}}$, and so $E_{2^{r+1}b} \equiv E_{2^{r+1}b-(2^r)2} + (2^r)2 \pmod{2^{r+1}}$. Continuing in this fashion we obtain $E_{2^{r+1}b} \equiv E_{2^{r+1}b-2^r b} + 2^r b \pmod{2^{r+1}}$, which gives $E_{2^{r+1}b} \equiv E_{2^r b} + 2^r \pmod{2^{r+1}}$. The result follows from this. □

To end this section, we combine Corollary 5.2.4 and the previous Lemma, to give the next result.

Theorem 5.2.7. *Let p denote a prime and m, r positive integers where m is such that $p \nmid m$. Then*

$$E_{2p^r m} \equiv E_{2p^{r-1}m} \pmod{p^r}.$$

Proof. This follows from Corollary 5.2.4 if p is odd and Lemma 5.2.6 when $p = 2$. □

5.3. Periodic Points and Euler Numbers

The sequence $\varepsilon = (\varepsilon_n)_{n\geq 1}$ is defined by

$$\varepsilon_n = |E_{2n}| = (-1)^n E_{2n},\ n \geq 1,$$

and we write $\varepsilon^* = (\varepsilon^*_n)$ where

$$\varepsilon^*_n = \sum_{d|n} \mu(n/d)\varepsilon_d,\ n \geq 1.$$

We begin by showing that the sequence ε has divisibility.

Proposition 5.3.1. *For every integer $n \geq 1$ we have $n \mid \varepsilon^*_n$.*

Proof. If $n = 1$ this is obvious, so assume that $n > 1$. Let $n = p^r m$ where p is prime, $r \geq 1$ and $p \nmid m$. Then

$$\varepsilon^*_n = \sum_{d|n} \mu(n/d)\varepsilon_d = \sum_{d|m} \mu(m/d)(\varepsilon_{p^r d} - \varepsilon_{p^{r-1}d}).$$

Now by definition,

$$\varepsilon_{p^r d} - \varepsilon_{p^{r-1}d} = (-1)^{p^r d} E_{2p^r d} - (-1)^{p^{r-1}d} E_{2p^{r-1}d}$$

which gives

$$\varepsilon_{p^r d} - \varepsilon_{p^{r-1}d} = (-1)^{p^{r-1}d}((-1)^{p^{r-1}(p-1)d} E_{2p^r d} - E_{2p^{r-1}d}).$$

If p is odd, or if $p = 2$ and $r > 1$, $(-1)^{p^{r-1}(p-1)d} = 1$, so that in either of these cases $\varepsilon_{p^r d} - \varepsilon_{p^{r-1}d} = (-1)^{p^{r-1}d}(E_{2p^r d} - E_{2p^{r-1}d})$. The remaining alternative is $p = 2$ and $r = 1$. In this case, $(-1)^{p^{r-1}(p-1)d} = -1$ so

$$\varepsilon_{2d} - \varepsilon_d = E_{4d} + E_{2d} = (E_{4d} - E_{2d}) + 2E_{2d} \equiv E_{4d} - E_{2d} \pmod 2.$$

We now appeal to Theorem 5.2.7 to obtain $p^r \mid \varepsilon_{p^r d} - \varepsilon_{p^{r-1}d}$ in all possible cases, so $p^r \mid \varepsilon_n^*$. It follows that $n \mid \varepsilon_n^*$. □

Theorem 5.3.2. *The sequence $\varepsilon = (\varepsilon_n)$ is realizable.*[1]

Proof. It is known that (see [**1**], page 807)

$$E_{2n} = (-1)^n \frac{2^{2n+2}(2n)!}{\pi^{2n+1}} \left(1 - \frac{1}{3^{2n+1}} + \frac{1}{5^{2n+1}} - \frac{1}{7^{2n+1}} + \cdots \right),$$

and using this it is easy to show that ε is an increasing sequence and $\varepsilon_{2n} \geq n\varepsilon_n$ for all $n \geq 1$. Since $\varepsilon_1 = 1 \geq 0$, it follows from Lemma 1.2.11 that $\varepsilon_n^* \geq 0$ when $n \geq 1$, and so the sequence ε has positivity. Proposition 5.3.1 established divisibility for ε, hence from Lemma 1.2.4, the sequence ε is realizable. □

5.4. The Bernoulli Numbers

The *Bernoulli Numbers* $(B_n)_{n\geq 0}$ are defined by the relation

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

This sequence of numbers is of great importance in many areas of mathematics, examples of which include algebraic topology [**3**] and the theory of cyclotomic fields [**30**].

It is clear that $(B_n)_{n\geq 0} = (1, -1/2, 1/6, 0, \ldots)$ is a sequence of rational numbers, and since

$$\frac{t}{e^t - 1} + \frac{1}{2}t$$

is an even function of t, $B_{2n+1} = 0$ for $n \geq 1$, while $(-1)^{n+1}B_{2n} > 0$ when $n \geq 1$.

The next three results, due to Adams, von Staudt-Clausen and Kummer, date from the nineteenth century. They provide essential information about the Bernoulli numbers. These are classical theorems

[1] This result has been obtained independently by Juan Arias de Reyna [**6**].

with proofs to be found in many journals. We refer in particular to [**2**], [**12**], [**15**] and [**16**].

Theorem 5.4.1. (Adams) *If p denotes an odd prime and n, r are positive integers with n being such that $p-1 \nmid 2n$, then*

$$p^r \mid n \textit{ implies that } B_{2n} \equiv 0 \pmod{p^r}.$$

Theorem 5.4.2. (von Staudt-Clausen) *The denominator d_n of the Bernoulli number B_{2n} is given by*

$$d_n = \prod_{\substack{p \text{ prime} \\ p-1|2n}} p, \; n \geq 1.$$

Theorem 5.4.3. (Kummer) *Suppose that the integers m, n, r are such that $1 \leq r \leq 2n-1 \leq 2m-1$. Then for any odd prime p where $p-1 \nmid 2n$ and $2m \equiv 2n \pmod{\varphi(p^r)}$,*

$$\frac{B_{2m}}{2m} \equiv \frac{B_{2n}}{2n} \pmod{p^r}.$$

There have been many generalizations of Kummer's theorem since it was first published. The next result relaxes the restriction on the prime p and is a special case of a theorem established in [**31**] by using p-adic analysis.

Theorem 5.4.4. *Let p denote an odd prime and n, r positive integers where $p^r \parallel n$ and $p-1 \mid 2n$. If $k = n/p$ then*

$$(g_p^{2n} - 1)\frac{B_{2n}}{2n} \equiv (g_p^{2k} - 1)\frac{B_{2k}}{2k} \pmod{p^r},$$

where $g_p > 1$ is a primitive root mod p such that $p^2 \nmid g_p^{p-1} - 1$.

A similar result to Theorem 5.4.4 holds for the prime 2. However, in this case, since the result requires an adaptation of the theorem in [**31**], we give a proof.

Theorem 5.4.5. *Let n and r denote positive integers with $2^r \parallel n$. If $k = n/2$ then*

$$(5^n - 1)\frac{B_{2n}}{2n} \equiv (5^k - 1)\frac{B_{2k}}{2k} \pmod{2^r}.$$

Proof. Denote by f the function

$$f(t) = \frac{5}{e^{5t} - 1} - \frac{1}{e^t - 1},$$

and suppose that f has the formal power series expansion

$$f(t) = \sum_{j=0}^{\infty} a_j \frac{t^j}{j!}.$$

In [**31**] it shown that if the integers n, r and k are as in the statement of the theorem, then

$$a_{2n-1} \equiv a_{2k-1} \pmod{2^s} \text{ where } s = \min\{n-1, r+2\}. \tag{5.3}$$

Now we have

$$f(t) = t^{-1}\left(\frac{5t}{e^{5t} - 1} - \frac{t}{e^t - 1}\right) = t^{-1}\sum_{j=0}^{\infty}(5^j - 1)B_j\frac{t^j}{j!},$$

and so (5.3) gives

$$(5^{2n} - 1)\frac{B_{2n}}{2n} \equiv (5^{2k} - 1)\frac{B_{2k}}{2k} \pmod{2^s}, \quad s = \min\{n-1, r+2\}.$$

Noting that for any integer $q \geq 1$ we have $2 \parallel 5^q + 1$, the above gives

$$(5^n - 1)\frac{B_{2n}}{2n} \equiv (5^k - 1)\frac{B_{2k}}{2k} \pmod{2^b},$$

where $b = \min\{n-2, r+1\}$. Since when $r > 1$ it is easy to see that $r \leq \min\{n-2, r+1\}$, the proof will be complete if we can show that the result holds for $r = 1$. However, this case is easily seen to be true, so we are done. □

5.5. Periodic Points and Bernoulli Numbers

In [**9**] the authors prove that the denominators of the sequence $(|B_{2n}|)_{n\geq 1}$ form a realizable sequence, and in an earlier preprint, conjectured that both the denominators and numerators of the sequence $(|B_{2n}/2n|)_{n\geq 1}$ are realizable; we will show that these conjectures hold.

Throughout this section we denote by $\tau = (\tau_n)$ and $\beta = (\beta_n)$ the sequences of positive integers defined by

$$\left|\frac{B_{2n}}{2n}\right| = \frac{\tau_n}{\beta_n},\ n \geq 1,$$

where $\gcd(\tau_n, \beta_n) = 1$ for each value of n. By Theorem 5.4.2, the terms of the sequence β are all even, so we note for later use that τ contains only odd numbers. We begin the section by showing that β is an algebraically realizable sequence.

5.5.1. The Denominator Sequence $\boldsymbol{\beta}$.

Most of the work required to demonstrate the algebraic realizability of the sequence β has already been done, and just needs to be gathered together.

Proposition 5.5.1. *The sequence $w = (w_n)$ which is defined by*

$$w_n = 2 \prod_{\substack{p \text{ prime} \\ p-1|2n}} p^{1+\operatorname{ord}_p(n)},$$

is algebraically realizable.

Proof. The 2-part of w is the sequence $(2^{2+\operatorname{ord}_2(n)})$, and if the prime p is odd, the p-part of w has the form $(\lambda_n((p-1)/2, 1, p))_{n\geq 1}$ – see Definition 3.3.19. Hence by Theorem 3.3.20 and Proposition 3.3.24, w is equal to a product of algebraically realizable sequences and so w is algebraically realizable. □

Proposition 5.5.2. *If n denotes an integer, with $n \geq 1$,*

$$\beta_n = 2 \prod_{\substack{p \text{ prime} \\ p-1|2n}} p^{1+\operatorname{ord}_p(n)}.$$

Proof. We consider the primes 2 and 3 separately. Firstly, by Theorem 5.4.2, the sequence of 2-parts obtained from $(d_n)_{n\geq 1}$ is $(2,2,2,\ldots)$, where d_n is the denominator of the Bernoulli number B_{2n}. Therefore, the 2-part of the sequence β is $(2^{2+\mathrm{ord}_2(n)})_{n\geq 1}$. Similarly, the 3-part of (d_n) is $(3,3,3,\ldots)$, from which the 3-part of β is $(3^{1+\mathrm{ord}_3(n)})_{n\geq 1}$.

Next assume that the prime $p\geq 5$. If n is such that $p-1\mid 2n$ then the p-part of d_n is p by Theorem 5.4.2, so $B_{2n}\not\equiv 0 \pmod p$. It follows that the p-part of β_n in this case is $p^{1+\mathrm{ord}_p(n)}$. Alternatively, if $p-1\nmid 2n$, then Theorem 5.4.1 says that $B_{2n}\equiv 0 \pmod{p^{\mathrm{ord}_p(n)}}$, so we get $\beta_n=1$. Summing this up, if $p\geq 5$

$$[\beta_n]_p=\begin{cases} 1 & p-1\nmid 2n \\ p^{1+\mathrm{ord}_p(n)} & p-1\mid 2n \end{cases}.$$

The result now follows easily. □

Theorem 5.5.3. *The sequence β is algebraically realizable.*

Proof. This is a consequence of Propositions 5.5.1 and 5.5.2. □

5.5.2. The Numerator Sequence $\boldsymbol{\tau}$. To prove that the sequence τ is realizable we will show that τ has both divisibility and positivity. Thus if $\tau^*=(\tau_n^*)$ is the sequence given by

$$\tau_n^*=\sum_{d\mid n}\mu(n/d)\tau_d,\ \ n=1,2,3,\ldots,$$

the following two facts will be established: $n\mid\tau_n^*$ and $\tau_n^*\geq 0$, when $n\geq 1$. We begin with the divisibility property and so we can assume that $n>1$. If $n=p^rm$, where p is prime, $r,m\geq 1$ and $p\nmid m$, we will show that $p^r\mid\tau_n^*$ by considering the separate cases, $p-1\nmid 2n$ and $p-1\mid 2n$. So to start with, suppose n such that $p-1\nmid 2n$. Then p must be an odd prime and we can make use of Theorems 5.4.1, 5.4.2 and 5.4.3. If $k=n/p$ then

$$\frac{B_{2n}}{2n}=(-1)^{n+1}\frac{\tau_n}{\beta_n}\text{ and }\frac{B_{2k}}{2k}=(-1)^{k+1}\frac{\tau_k}{\beta_k},$$

so because $n \equiv k \pmod{\varphi(p^r)}$, Theorem 5.4.3 gives

$$(-1)^{n+1}\frac{\tau_n}{\beta_n} \equiv (-1)^{k+1}\frac{\tau_k}{\beta_k} \pmod{p^r}. \tag{5.4}$$

Now since p is odd, $(-1)^n = (-1)^k$, so (5.4) simplifies to

$$\frac{\tau_n}{\beta_n} \equiv \frac{\tau_k}{\beta_k} \pmod{p^r}. \tag{5.5}$$

Theorem 5.4.2 implies $\beta_n = \delta_n\beta_k$, where the positive integer δ_n is such that $\delta_n \equiv 1 \pmod{p^r}$. Using this and the fact that Theorem 5.4.1 guarantees that $\gcd(p, \beta_n) = 1$, (5.5) gives

$$\tau_n \equiv \delta_n\tau_k \equiv \tau_k \pmod{p^r}.$$

Since

$$\tau_n^* = \sum_{d|m} \mu(m/d)(\tau_{p^r d} - \tau_{p^{r-1}d}),$$

we obtain from the above, $p^r \mid \tau_n^*$ in the case $p - 1 \nmid 2n$.

Next the case $p - 1 \mid 2n$ will be considered.

Lemma 5.5.4. *Let $n = 2^r m$ where m is odd and $r \geq 1$, and put $k = n/2$. Then $(5^n - 1)/2^{r+2}$ and $(5^k - 1)/2^{r+1}$ are odd integers with*

$$\frac{5^n - 1}{2^{r+2}} \equiv \frac{5^k - 1}{2^{r+1}} \pmod{2^r}.$$

Proof. Lemma 3.3.23 implies that both $(5^n - 1)/2^{r+2}$ and $(5^k - 1)/2^{r+1}$ are odd integers, and from

$$\frac{5^n - 1}{2^{r+2}} - \frac{5^k - 1}{2^{r+1}} = \frac{5^k - 1}{2^{r+1}}\left(\frac{5^n - 1}{2(5^k - 1)} - 1\right) = \frac{5^k - 1}{2^{r+1}}\left(\frac{5^k - 1}{2}\right)$$

we obtain

$$\frac{5^n - 1}{2^{r+2}} - \frac{5^k - 1}{2^{r+1}} = 2^r\left(\frac{5^k - 1}{2^{r+1}}\right)^2 \equiv 0 \pmod{2^r},$$

which completes the proof. □

The next result is the equivalent of Lemma 3.3.23, and is just the standard result that g_p is a primitive root mod p^r for all $r \geq 1$.

Lemma 5.5.5. *Let p denote an odd prime and $g_p > 1$ a primitive root mod p which is such that $p^2 \nmid g_p^{p-1} - 1$. If r denotes a non-negative integer and m a positive integer such that $p \nmid m$, then*

$$p^{r+1} \nmid g_p^{(p^r - p^{r-1})m} - 1.$$

Proof. Since $p^2 \nmid g_p^{p-1} - 1$ and g_p is a primitive root mod p, there is an integer $s \geq 1$ with $p \nmid s$ such that $g_p^{p-1} = 1 + sp$. Therefore,

$$g_p^{(p^r - p^{r-1})m} = (1 + sp)^{p^{r-1}m} = 1 + msp^r + tp^{r+1}$$

with $t \in \mathbb{N}_0$. The result follows. □

Lemma 5.5.6. *Let p denote an odd prime and $g_p > 1$ a primitive root mod p which is such that $p^2 \nmid g_p^{p-1} - 1$. If m, r denote positive integers where $p \nmid m$, let $2n = p^r(p-1)m$ and set $k = n/p$. Then $(g_p^{2n} - 1)/p^{r+1}$ and $(g_p^{2k} - 1)/p^r$ are both integers prime to p, and*

$$\frac{g_p^{2n} - 1}{p^{r+1}} \equiv \frac{g_p^{2k} - 1}{p^r} \pmod{p^r}.$$

Proof. It follows from the Euler-Fermat Theorem and Lemma 5.5.5 that $g_p^{2n} - 1 = p^{r+1}c$, where the integer $c \geq 1$ is such that $p \nmid c$. Hence, $(g_p^{2n} - 1)/p^{r+1}$ and $(g_p^{2k} - 1)/p^r$ are both integers prime to p. Now,

$$\frac{g_p^{2n} - 1}{p^{r+1}} - \frac{g_p^{2k} - 1}{p^r} = \frac{g_p^{2k} - 1}{p^r} \left(\frac{g_p^{2n} - 1}{p(g_p^{2k} - 1)} - 1 \right),$$

from which we get

$$\frac{g_p^{2n} - 1}{p^{r+1}} - \frac{g_p^{2k} - 1}{p^r} = \frac{g_p^{2k} - 1}{p^r} \left(\frac{1}{p} \sum_{s=0}^{p-1} g_p^{2ks} - 1 \right).$$

Consideration of the expression in the final set of brackets gives

$$\frac{1}{p} \sum_{s=0}^{p-1} g_p^{2ks} - 1 = \frac{1}{p} \sum_{s=1}^{p-1} (g_p^{2ks} - 1) = \frac{g_p^{2k} - 1}{p} \sum_{s=1}^{p-1} s g_p^{2k(p-1-s)},$$

and so

$$\frac{g_p^{2n} - 1}{p^{r+1}} - \frac{g_p^{2k} - 1}{p^r} = p^{r-1} \left(\frac{g_p^{2k} - 1}{p^r} \right)^2 \sum_{s=1}^{p-1} s g_p^{2k(p-1-s)}.$$

Next, since $p-1 \mid 2k$ and g_p is a primitive root mod p, we have $g_p^{2k(p-1-s)} \equiv 1 \pmod{p}$ when $1 \leq s \leq p-1$. This gives

$$\sum_{s=1}^{p-1} s g_p^{2k(p-1-s)} \equiv \sum_{s=1}^{p-1} s \pmod{p},$$

and therefore there is an integer $b \geq 1$ such that

$$\frac{g_p^{2n}-1}{p^{r+1}} - \frac{g_p^{2k}-1}{p^r} = bp^r \left(\frac{g_p^{2k}-1}{p^r} \right)^2 .$$

The result follows from this. □

Proposition 5.5.7. *Let p denote a prime and suppose the integers $n, r \geq 1$ are such that $p^r \parallel n$ and $p-1 \mid 2n$. Then*

$$\tau_n \equiv \tau_k \pmod{p^r}, \text{ where } k = n/p.$$

Proof. We deal with the cases $p=2$ and p odd separately, though the arguments used are similar. So to begin with suppose that $p=2$ and that $n = 2^r m$ with $m \geq 1$ odd. By Theorem 5.4.5

$$(5^n - 1)\frac{B_{2n}}{2n} \equiv (5^k - 1)\frac{B_{2k}}{2k} \pmod{2^r},$$

so when $r > 1$ this gives

$$(5^n - 1)\frac{\tau_n}{\beta_n} \equiv (5^k - 1)\frac{\tau_k}{\beta_k} \pmod{2^r},$$

and when $r = 1$

$$(5^n - 1)\frac{\tau_n}{\beta_n} \equiv -(5^k - 1)\frac{\tau_k}{\beta_k} \pmod{2}.$$

However, for any integer x, $x \equiv -x \pmod{2}$ so the above implies that for all $r \geq 1$

$$(5^n - 1)\frac{\tau_n}{\beta_n} \equiv (5^k - 1)\frac{\tau_k}{\beta_k} \pmod{2^r}. \tag{5.6}$$

Proposition 5.5.2 implies that there are odd positive integers γ_n, δ_n, with $\delta_n \equiv 1 \pmod{2^r}$, such that $\beta_n = 2^{r+2}\gamma_n\delta_n$ and $\beta_k = 2^{r+1}\gamma_n$.

Using this in (5.6) we get

$$\left(\frac{5^n-1}{2^{r+2}}\right)\frac{\tau_n}{\gamma_n\delta_n} \equiv \left(\frac{5^k-1}{2^{r+1}}\right)\frac{\tau_k}{\gamma_n} \pmod{2^r}.$$

From Lemma 5.5.4, $(5^n-1)/2^{r+2}$ and $(5^k-1)/2^{r+1}$ are odd integers, congruent to each other mod 2^r. It follows, therefore, that

$$\frac{\tau_n}{\gamma_n\delta_n} \equiv \frac{\tau_k}{\gamma_n} \pmod{2^r}.$$

Since γ_n, δ_n are odd, this gives $\tau_n \equiv \delta_n\tau_k \pmod{2^r}$, so by making use of $\delta_n \equiv 1 \pmod{2^r}$, we obtain $\tau_n \equiv \tau_k \pmod{2^r}$.

Now assume that the prime p is odd. Since $p-1 \mid 2n$ we have $2n = p^r(p-1)m$ for some integer $m \geq 1$ such that $p \nmid m$. Using Theorem 5.4.4 we get

$$(g_p^{2n}-1)\frac{B_{2n}}{2n} \equiv (g_p^{2k}-1)\frac{B_{2k}}{2k} \pmod{p^r},$$

where $g_p > 1$ is a primitive root mod p such that $p^2 \nmid g_p^{p-1}-1$. Next, Proposition 5.5.2 gives $\beta_n = p^{r+1}\gamma_n\delta_n$ and $\beta_k = p^r\gamma_n$, where γ_n, δ_n denote positive integers such that $p \nmid \gamma_n$ and $\delta_n \equiv 1 \pmod{p^r}$. This leads to

$$\left(\frac{g_p^{2n}-1}{p^{r+1}}\right)\frac{\tau_n}{\gamma_n\delta_n} \equiv \left(\frac{g_p^{2k}-1}{p^r}\right)\frac{\tau_k}{\gamma_n} \pmod{p^r}.$$

Using Lemma 5.5.6 and similar arguments to above, we obtain from this

$$\tau_n \equiv \delta_n\tau_k \equiv \tau_k \pmod{p^r},$$

and this completes the proof. □

The results obtained above can be combined to give the following.

Theorem 5.5.8. *If n denotes a positive integer, then $n \mid \tau_n^*$.*

Proof. Since we may clearly assume that $n > 1$, there are integers $r, m \geq 1$ and a prime p such that $n = p^r m$ with $p \nmid m$. Denoting by

k the integer n/p, from the above both possibilities $p-1 \nmid 2n$ and $p-1 \mid 2n$ give the result: $p^r \mid \tau_n - \tau_k$. It follows from the equation

$$\tau_n^* = \sum_{d|m} \mu(m/d)(\tau_{p^r d} - \tau_{p^{r-1}d}),$$

that $p^r \mid \tau_n^*$ and so $n \mid \tau_n^*$. □

We have now come to the last stage in showing that the sequence τ is realizable: we will prove that τ has positivity (that is, $\tau_n^* \geq 0$ for all $n \geq 1$).

Theorem 5.5.9. *The sequence τ has positivity.*

Proof. Define the sequence $x = (x_n)$ of positive rational numbers by

$$x_n = \left| \frac{B_{2n}}{2n} \right|, \; n = 1, 2, 3, \ldots .$$

The terms of this sequence are known to be given by the equation

$$x_n = \frac{2(2n-1)!}{(2\pi)^{2n}} \sum_{r=1}^{\infty} \frac{1}{r^{2n}}, \; n \geq 1 . \tag{5.7}$$

This is a standard result relating to the Riemann zeta function: a proof can be found in [**5**]. Using (5.7) it is easy to show that $x_{n+1} \geq x_n$ and $x_{2n} \geq nx_n$ when $n > 2$. Consider the sequence $y = (y_n)$ where $y_1 = y_2 = 0$ and $y_n = x_n$ when $n \geq 3$. Then y is an increasing sequence of non-negative rational numbers and $y_{2n} \geq ny_n$ for all $n \geq 1$. It follows from Lemma 1.2.11 that y has positivity. Now, since the denominator sequence $\beta = (\beta_n)$ is realizable by Theorem 5.5.3, Lemma 1.2.4 implies that β has positivity. It follows from Lemma 1.2.10, therefore, that the sequence βy has positivity. If we write $t = (t_n)$ for the sequence βy then $t = (0, 0, \tau_3, \tau_4, \ldots)$, whereas $\tau = (1, 1, \tau_3, \tau_4, \ldots)$. Suppose that τ does not have positivity. Then there is an integer $n > 1$ such that $\tau_n^* < 0$. Since the terms of the sequence τ are all odd numbers, τ_n^* is even, and because the sequences t and τ differ only in the values of the first two terms and $t_n^* \geq 0$, this implies that $\tau_n^* = -2$. Now for this to be the case n must be even with $\mu(n) = \mu(n/2) = -1$. However, this is easily seen to be impossible, so τ does have positivity. □

We sum the above results up in the following.

Theorem 5.5.10. *The numerator sequence τ is realizable.*

Proof. Theorems 5.5.8 and 5.5.9 show that the sequence τ satisfies the conditions of Lemma 1.2.4, and so τ is a realizable sequence. □

5.6. Local Properties of Bernoulli and Euler Numbers

We end this chapter by considering the sequences β, ε and τ, introduced above, from a *local* viewpoint. First, the sequence β is algebraically realizable by an abelian system, so by Theorem 3.2.11 β is everywhere locally (algebraically) realizable. Indeed, the method of proof employed above was basically to work in the other direction: construct algebraic realizations of the p-part sequences $([\beta_n]_p)$ for each prime p, and so conclude that β is realizable.

The situation is completely different for the sequences ε and τ. It is easy to show, by just inspecting the initial terms of each sequence, that they are not *everywhere* locally realizable. Thus we have

$$\varepsilon = (1, 5, 61, 1385, 50521, 2702765, 199360981, 19391512145, \ldots)$$

and the 61-part of this sequence is

$$([\varepsilon_n]_{61}) = (1, 1, 61, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots)$$

with the next occurrence of 61 being at the 30th term. This is not a realizable sequence since

$$\sum_{d|9} \mu(9/d)[\varepsilon_d]_{61} = 1 - 61 = -60$$

so it does not possess the property of positivity (or divisibility). Similarly, it is easy to check that the 43-part is not realizable. However, the 5-part is the sequence which begins

$$([\varepsilon_n]_5) = (1, 5, 1, 5, 1, 5, 1, 5, 1, 25, 1, 5, 1, 5, 1, 5, 1, 5, 1, 25, 1, 5, 1, 5, 1, 5,$$

$$1, 5, 1, 25, 1, 5, 1, 5, 1, 5, 1, 5, 1, 25, 1, 5, 1, 5, 1, 5, 1, 5, 1, 125, 1, 5, \ldots)$$

and this is of the form $(\lambda_n(2, 1, 5))$, which is an algebraically realizable sequence by Theorem 3.3.20. The 13-part has a similar form: $(\lambda_n(6, 1, 13))$. And, trivially, the 2-part sequence is algebraically realizable since every term of ε is an odd number. So from just an inspection of the terms, it seems that the sequence ε has a fairly complicated local structure.

Problem 5.6.1. Determine the primes p for which the sequence ε is locally realizable at p.

The initial terms of the sequence τ are

$$(1, 1, 1, 1, 1, 691, 1, 3617, 43867, 174611, 77683, 236364091, 657931, \ldots)$$

and a first inspection would suggest that this sequence should also have a complicated local structure, since it clearly has an markedly erratic global one. However, despite this appearance, it is possible to determine (in some sense) the local structure of τ, by using the concept of a *regular* prime – which dates back to Kummer's investigations into the Fermat problem.

Definition 5.6.2. A prime p is called *regular* if $p \nmid B_{2n}$ when the integer n is in the range $1 \leq n \leq (p-3)/2$.

The primes 2 and 3 do not quite fit this definition (except for in a strictly logical sense) but this is of no great consequence, since it follows from Proposition 5.5.2 that,

$$([\tau_n]_p)_{n\geq 1} = (1, 1, 1, 1, 1, 1, \ldots)$$

when $p \in \{2, 3\}$, so the sequence τ is trivially locally realizable at the primes 2 and 3. In fact this simple localization is a property of all regular primes.

Proposition 5.6.3. *Let p denote a regular prime. Then $[\tau_n]_p = 1$ for all $n \in \mathbb{N}$, and so the sequence τ is trivially locally realizable at p.*

Proof. Clearly we may assume that $p \geq 5$. Suppose that there is an integer $n \geq 1$ such that $p \mid \tau_n$: choose the value of n minimal with respect to this property. Then $p \mid B_{2n}/2n$ so from Definition 5.6.2, $2n > p - 3$ and it follows that $p - 1 \leq 2n$. If $p - 1 \mid 2n$, then Proposition 5.5.2 implies that $p \mid \beta_n$, which contradicts $p \mid \tau_n$: hence $p - 1 \nmid 2n$, so if the integer m is defined by $2m = 2n - p + 1$ we have $m \geq 1$. Now, Kummer's theorem gives

$$\frac{B_{2n}}{2n} \equiv \frac{B_{2m}}{2m} \pmod{p},$$

from which we obtain $p \mid B_{2m}/2m$, so that $p \mid \tau_m$, contradicting the minimality of n. This completes the proof. □

Because of the previous result, we only need to consider the local properties of the sequence τ at the *irregular* primes, the first of which are: $\{37, 59, 67, 101, 103, 131, 149, 157, 233, 257, \dots\}$.

Proposition 5.6.4. *Let p denote a prime. The sequence $([\tau_n]_p)_{n\geq 1}$ is non-trivial if and only if p is irregular.*

Proof. If $([\tau_n]_p)_{n\geq 1}$ is not the trivial sequence $(1, 1, 1, \dots)$, then p must be an irregular prime by Proposition 5.6.3.

For the proof in the other direction, suppose that p is an irregular prime. Then there is an integer m such that $1 \leq m \leq (p-3)/2$ with $p \mid B_{2m}$. Since $p > 2m$ this implies that $p \mid \tau_m$, and so the sequence $([\tau_n]_p)_{n\geq 1}$ is non-trivial. □

Lemma 5.6.5. *Let p denote an irregular prime. If k is an integer in the set $\{1, 2, \ldots, (p-3)/2\}$ such that $p \mid \tau_k$, then $p \nmid \tau_m$, where $m = k(p-1)/2$.*

Proof. By Theorem 5.4.2 – the von Staudt-Clausen theorem – since $p - 1 \mid 2m$, the prime p is a factor of the denominator of B_{2m}, so that $p \mid \beta_m$. This immediately gives: $p \nmid \tau_m$. □

Proposition 5.6.6. *If p denotes an irregular prime, then τ localized at p is not realizable.*

Proof. Let k denote an integer in the set $\{1, 2, \ldots, (p-3)/2\}$ such that $p \mid \tau_k$, and put $m = k(p-1)/2$. Then clearly $k \mid m$ and by Lemma 5.6.5, $[\tau_m]_p = 1$, so that $[\tau_k]_p > [\tau_m]_p$. However, if the sequence $([\tau_n]_p)$ is realizable, then $[\tau_k]_p \leq [\tau_m]_p$ since $k \mid m$. This contradiction completes the proof. □

We sum the above up in the final result.

Theorem 5.6.7. *The sequence τ is not locally realizable precisely at the set of irregular primes.*

Proof. This follows from Propositions 5.6.4 and 5.6.6. □

Bibliography

1. M. Abramowitz and I. A. Stegun *Handbook of Mathematical Functions.* Dover Publications, Inc., New York, Ninth Printing, 1970.
2. J. C. Adams. Table of the first sixty-two numbers of Bernoulli *J. Reine Angew. Math., 85:269-272*, 1878.
3. J. F. Adams. On the groups J(X). II. *Topology 3 (1965), 137-171.*
4. W. A. Adkins and S. H. Weintraub. *Algebra An Approach via Module Theory.* GTM 136, Springer-Verlag, New York, 1992.
5. T. M. Apostol. *Introduction to Analytic Number Theory.* UTM, Springer-Verlag, New York, 1976.
6. J. Arias de Reyna. Dynamical zeta functions and Kummer congruences. *Preprint, Universidad de Sevilla*, 2003.
7. A. Baker. Linear forms in the logarithms of algebraic numbers IV. *Mathematika* 15 (1968), 204-216.
8. P. M. Cohn. *Algebra Volume 1.* John Wiley & Sons, Chichester, second edition, 1990.
9. G. Everest, A. J. van der Poorten, Y. Puri and T. Ward. Integer Sequences and Periodic Points. *Journal of Integer Sequences, Vol. 5*, 2002.
10. G. Everest and T. Ward. *Heights of Polynomials and Entropy in Algebraic Dynamics.* Universitext, Springer-Verlag, London, 1999.
11. W. L. Ferrar *Algebra.* Oxford University Press, second edition, 1957.
12. G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* The Clarendon Press Oxford University Press, New York, fifth edition, 1979.
13. M. I. Kargapolov and Ju. I. Merzljakov. *Fundamentals of the Theory of Groups.* GTM 62, Springer-Verlag, New York, 1979.
14. E. I. Khukhro *p-Automorphisms of Finite p-Groups.* LMS Lecture Note Series 246, Cambridge University Press, 1998.
15. N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* GTM 58, Springer-Verlag, New York, 1984.

16. E. E. Kummer. Über eine allgemeine Eigenschaft der rationalen Entwickelungscoëfficienten einer bestimmten Gattung analytischer Functionen. *J. Reine Angew. Math., 41:368-372*, 1851.

17. D. H. Lehmer. Factorisation of certain cyclotomic functions. *Ann. of Math.* 34 (1933), 461-479.

18. D. A. Lind, K. Schmidt and T. Ward. Mahler measure and entropy for commuting automorphisms of compact groups. *Inventiones Math.* 101 (1990), 593-629.

19. K. Mahler. An application of Jensen's formula to polynomials. *Mathematika* 7 (1960), 98-100.

20. B. Mazur. On the passage from local to global in number theory. *Bulletin (New Series) of The American Mathematical Society* 29 (1993), 14-50.

21. T. A. Pierce. Numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$. *Ann. of Math.* 18 (1917), 53-64.

22. Y. Puri. Arithmetic Properties of Periodic Orbits. *PhD thesis, University of East Anglia*, 2000.

23. Y. Puri and T. Ward. Arithmetic and growth of periodic orbits. *Journal of Integer Sequences*, 2001.

24. D. J. S. Robinson. *A Course in the Theory of Groups.* GTM 80, Springer-Verlag, New York, 1982.

25. J. S. Rose. *A Course on Group Theory.* Dover Publications, Inc, New York, 1994.

26. K. Schmidt. *Dynamical Systems of Algebraic Origin.* PM 128, Birkhäuser Verlag, Basel, 1995.

27. I. N. Stewart and D. O. Tall *Algebraic Number Theory.* Chapman and Hall, London, second edition, 1987.

28. S. S. Wagstaff, Jr. Prime divisors of the Bernoulli and Euler numbers. *Proc. of the Millennial Conference on Number Theory, University of Illinois*, 2000.

29. P. Walters. *An Introduction to Ergodic Theory.* GTM 79, Springer-Verlag, New York, 1982.

30. L. C. Washington. *Introduction to Cyclotomic Fields.* GTM 83, Springer-Verlag, New York, 1982.

31. P. T. Young. Congruences for Bernoulli, Euler, and Stirling Numbers. *Journal of Number Theory, 78:204-227*, 1999.