CENTRALISERS OF FORMAL MAPS

ANTHONY G. O’FARRELL

Abstract. We consider the formal maps in any finite dimension $d$ with coefficients in an integral domain $K$ with identity. Those invertible under formal composition form a group $G$. We consider the centraliser $C_g$ of an element $g \in G$ which has infinite order and is tangent to the identity of $G$. If $g$ has infinite order and $K$ is a field of characteristic zero we show that $C_g$ contains an isomorphic copy of the additive group $(K, +)$. If $g$ has infinite order and $K$ has positive characteristic we show that $C_g$ contains an uncountable abelian subgroup. The proofs are quite different in finite characteristic and in characteristic zero, but are connected by so-called sum functions.

1. Introduction

We begin by fixing some terminology and notation.

1.1. Monic monomials. By a monic monomial in $d$ variables we mean an element $x^i := x_1^{i_1} \cdots x_d^{i_d}$, where $x = (x_1, \ldots, x_d)$ and $i \in \mathbb{Z}_+^d$ is a multi-index with nonnegative entries. The degree of the monic monomial $x^i$ is $|i| := i_1 + \cdots + i_d$. Let $S = S_d$ denote the set of all monic monomials in $d$ variables. So $S$ has elements $1, x_1, \ldots, x_d, x_1^2, x_1 x_2, \ldots, x_1^3, x_1 x_2^2$, and so on. If $m = x^i$, then we denote $x^i_j$ by $m_j$. For instance, $(x_1 x_2^2 x_3^3)_2 = x_2^2$.

The set $S$ has the structure of a commutative semigroup with identity, where the product is defined by $x^i \cdot x^j := x^{i+j}$. The semigroup $S$ has cancellation, and if $m$ and $n$ belong to $S$, then we call $m$ a factor of $p = m \cdot n$, we write $m | p$, and write $p/m = n$. Each nonempty subset $A \subset S$ has a highest common factor, which we denote by hcf$(A)$.

1.2. Formal power series. Let $K$ be an integral domain with identity, and $d \in \mathbb{N}$. We form the $K$-algebra $\mathcal{F} := \mathcal{F}_d := K[[x_1, \ldots, x_d]]$
of all formal power series in $d$ variables, with coefficients in $K$. An element $f \in \mathcal{F}$ is a formal sum

$$f = \sum_{m \in S} f_m m,$$

where $f_m \in K$ for each $m \in S$. Addition is done term-by-term, as is scalar multiplication, and multiplication by summing all the coefficients of terms from the factors corresponding to monomials with the same product. More precisely,

$$(f \cdot g)_m = \sum_{p \in S} \sum_{q \in S, pq = m} f_p g_q, \forall m \in S.$$ 

Equivalently,

$$(f \cdot g)_m = \sum_{p \in S, p|m} f_p g_m/p.$$ 

The formal series $1$, which has $1_1 = 1$ and $1_m = 0$ for all other monic monomials $m$, is the multiplicative identity of $\mathcal{F}$.

In the remainder of this section, all summations will be over indices drawn from $S$, so the formula for the product becomes just

$$(f \cdot g)_m = \sum_{p|m} f_p g_m/p.$$ 

The map $f \mapsto f_1$ is a surjective $K$-algebra homomorphism from $\mathcal{F}$ onto $K$.

For $f = \sum_m f_m m \in \mathcal{F}$, we set

$$\text{spt}(f) := \{m \in S : f_m \neq 0\}.$$ 

If $f \neq 0$, then $\text{spt}(f)$ is nonempty, and we define the vertex of $f$ to be the monic monomial

$$v(f) := \text{hcf}(\text{spt}(f)).$$

It is easy to see that

$$v(f)v(g)|v(fg), \forall f, g \in \mathcal{F}.$$

Equality holds in dimension $d = 1$, i.e. the index of the lowest-order nonzero term in $f(x)g(x)$ is the sum of the indices of the lowest-order terms in $f(x)$ and $g(x)$.

**Proposition 1.1.** If $f \in \mathcal{F}$ is nonzero, then there exists $h \in \mathcal{F}$ with $v(h) = 1$ and $f = v(f)h$.

**Proof.** $v(f)$ is a factor of each $m \in \text{spt}(f)$, so we can define

$$h := \sum_{m, f_m \neq 0} f_m \cdot (m/v(f))$$
and we have an \( h \in \mathcal{F} \) and \( f = v(f)h \). The fact that \( v(f) = \text{hcf}\left(\text{spt}(f)\right) \) implies that for each \( j \in \{1, \ldots, d\} \) there exists \( p \in \text{spt}(f) \) with \( f_p \neq 0 \) and \( p_j = v(f)_j \). Thus \( q := p/v(f) \) belongs to \( \text{spt}(h) \) and has \( q_j = 1 \) (i.e. \( q \) ‘does not involve \( x_j \)’). Thus \( v(h) = 1 \). \( \square \)

If \( f = ph \) with \( p \in S \) and \( h \in \mathcal{F} \), then we write \( h = f/p \). Note that \( h \) is uniquely determined by \( f \) and \( p \), because \( h_m = f_m/p \) whenever \( h_m \neq 0 \).

**Proposition 1.2.** \( \mathcal{F}_d \) is an integral domain with identity for each \( d \in \mathbb{N} \).

**Proof.** We use induction on \( d \).

When \( d = 1 \), the result follows from the fact that \( v(fg) = v(f)v(g) \).

Suppose \( \mathcal{F}_d \) is an integral domain, and \( \mathcal{F}_{d+1} \) is not. Choose two nonzero \( f, f' \in \mathcal{F}_{d+1} \), with \( ff' = 0 \). Replacing \( f \) by \( f/v(f) \) and \( f' \) by \( f'/v(f') \), we may assume that \( v(f) = 1 = v(f') \). We may regard monomials in \( d \) variables as monomials in \( d + 1 \) variables that do not involve \( x_{d+1} \), and define

\[
    h := \sum_{m \in S_d} f_m m, \quad h' := \sum_{m \in S_d} f'_m m.
\]

Then

\[
    hh' = \sum_{m \in S_d} (ff')_m m,
\]

the sum of all the terms in \( ff' \) that do not involve \( x_{d+1} \). Thus \( hh' = 0 \), so by hypothesis \( h = 0 \) or \( h' = 0 \). But \( h = 0 \) means \( x_{d+1}|v(f) \), contradicting \( v(f) = 1 \). Similarly, \( h' = 0 \) is impossible. \( \square \)

For any ring \( R \) with identity, we denote by \( R^\times \) the multiplicative group of invertible elements, or units, of \( R \).

We denote by \( \mathcal{M} \) the ideal

\[
    \mathcal{F}x_1 + \cdots + \mathcal{F}x_d = \{ f \in \mathcal{F} : f_1 = 0 \}.
\]

(This ideal is maximal if and only if \( K \) is a field. In that case, \( \mathcal{F} \) is the disjoint union of \( \mathcal{F}^\times \) and \( \mathcal{M} \). If \( K \) is not a field, then \( \mathcal{F} \) is a local ring if and only if \( K \) is local.)

**Proposition 1.3.**

\[
    \mathcal{F}^\times = \{ f \in \mathcal{F} : f_1 \in K^\times \},
\]

so the map \( f \mapsto f_1 \) is a surjective group homomorphism from \( \mathcal{F}^\times \to K^\times \).
Proof. Let $f \in \mathcal{F}$ have $f_1 \in K^\times$. Take $\alpha := (f_1)^{-1} \in K$. Then $\alpha f = 1 + h$, with $h \in \mathcal{M}$, and we may define

$$k := 1 - h + h^2 - h^3 + \cdots \in \mathcal{F},$$

where the sum makes sense because $v(h^r)$ has order at least $r$ for each $r \in \mathbb{N}$. Then $k \alpha f = 1$, so $f \in \mathcal{F}^\times$. This proves that

$$\{f \in \mathcal{F} : f_1 \in K^\times\} \subset \mathcal{F}^\times.$$

The opposite inclusion is clear, because if $f \in \mathcal{F}^\times$, and $h = f^{-1} - 1$, then

$$1 = (fh)_1 = f_1 h_1,$$

so $f_1 \in K^\times$. \qed

1.3. Formal maps. By $\mathcal{M}^d$ we denote (as usual) the Cartesian product $\mathcal{M} \times \cdots \times \mathcal{M}$ of $d$ factors $\mathcal{M}$, so an element $f \in \mathcal{M}^d$ is a $d$-tuple $(f_1, \ldots, f_d)$, with each $f_j \in \mathcal{M}$.

The formal composition $f \circ g$ is defined for $f \in \mathcal{F}$ and $g \in \mathcal{M}^d$, as follows. First, the composition $m \circ g$ of a monomial $m = x^i$ with $g$ is $g_1^i \cdots g_d^i$, where the products and powers use the multiplication of the ring $\mathcal{F}$. Then

$$f \circ g := \sum_m f_m \cdot (m \circ g).$$

The sum makes sense because for a given monomial $p \in S$, the coefficient of $p$ in $m \circ g$ is zero except for a finite number of $m \in S$; in fact it is zero once the degree of $m$ exceeds the degree of $p$. Thus the value

$$(f \circ g)_p = \sum_m f_m \cdot (m \circ g)_p$$

is a finite sum in the ring $K$, and makes sense.

We think of elements of $\mathcal{M}^d$ as formal self-maps of $K^d$ fixing 0. The formal composition $f \circ g$ is defined for $f \in \mathcal{M}^d$ and $g \in \mathcal{M}^d$ by

$$f \circ g := (f_1 \circ g, \ldots, f_d \circ g).$$

With this operation, $\mathcal{M}^d$ becomes a semigroup with identity; the identity is the element

$$\mathbb{1} := (x_1, x_2, \ldots, x_d).$$

We denote the group of invertible elements of this semigroup by $\mathcal{G}$.

For $g \in \mathcal{M}^d$, we define the linear part of $g$ to be the element of $\text{gl}(d, K)$ with $(i, j)$ entry given by

$$L(g)_{ij} := (g_i)_{x_j},$$

i.e. the coefficient of the first-degree monomial $x_j$ in the $i$-th component $g_i$ of $g$. 
The map \( L : \mathcal{M}^d \to \text{gl}(d, K) \) is a semigroup homomorphism, and its restriction \( L := L|\mathcal{G} \) to the invertible maps is a group homomorphism \( L : \mathcal{G} \to \text{GL}(d, K) \).

We say that an element \( g \in \mathcal{M}^d \) is tangent to the identity if \( L(g) = 1 \).

**Proposition 1.4.** Let \( g \in \mathcal{M}^d \). Then \( g \in \mathcal{G} \) if and only if \( L(g) \in \text{GL}(d, K) \).

**Proof.** If \( g \) is invertible in \( \mathcal{M}^d \), then its inverse \( h \) has \( h \circ g = 1 \), and this implies that the matrix product \( L(g)L(h) \) is the identity matrix. Thus \( L(g) \in \text{GL}(d, K) \).

For the converse, suppose \( L(g) \) is an invertible matrix, with inverse \( H \). We can also regard \( L(g) \) as an element of \( \mathcal{G} \), by setting

\[
L(g)_i = \sum_{j=1}^{d} L(g)_{ij} x_j.
\]

If we regard \( H \) in the same way, then \( H \) is the compositional inverse of \( L(g) \), and we can write \( g = L(g) \circ H \circ g \), so it suffices to show that \( H \circ g \) is invertible in \( \mathcal{M}^d \). Now \( H \circ g \) is tangent to the identity, so we just have to show that all \( g' \in \mathcal{M}^d \) of the form

\[
g' = 1 + h,
\]

where \( L(h) = 0 \), are invertible. But it is straightforward to check that such \( g' \) are inverted by

\[
h' := 1 - h + h \circ h - h \circ h \circ h + h \circ h \circ h \circ h + \cdots .
\]

\( \square \)

We remark that a matrix \( T \in \text{gl}(d, K) \) is invertible in \( \text{gl}(d, K) \) if and only if its determinant \( \det(T) \) belongs to \( K^\times \). The condition is necessary because the map \( \det \) sends products in \( \text{gl}(d, K) \) to products in \( K \), and it is sufficient because when \( \det(T) \in K^\times \) we may use the usual adjugate-transpose construction to construct an inverse for \( T \).

In order to avoid confusion, we prefer to use the notation \( g^{\circ k} \) for the \( k \)-times repeated composition. Thus \( g^{\circ 2} = g \circ g \), \( g^{\circ 3} = g \circ g \circ g \), and so on, and the formula used in the foregoing proof becomes

\[
(1 + h)^{\circ -1} = 1 + \sum_{k=1}^{\infty} (-1)^k h^{\circ k}.
\]

1.4. Main Results.

**Theorem 1.** Let \( K \) be a field of characteristic zero, and suppose \( g \in \mathcal{G} \) is tangent to the identity and not equal to the identity. Then there is an injective homomorphism from \((K, +)\) into the centraliser of \( g \) in \( \mathcal{G} \).
Theorem 2. Let $K$ be an integral domain with identity having finite characteristic $c$, and suppose $g \in \mathcal{G}$ is tangent to the identity and not of finite order. Then there is an homomorphism from $(\mathbb{Z}_c, +)$, the additive group of the $c$-adic integers, into the centraliser of $g$ in $\mathcal{G}$, and the image of this homomorphism is uncountable.

Combining these, we have our main conclusion:

Theorem 3 (Main Result). Let $K$ be an integral domain with identity, which is either of finite characteristic or is an uncountable field. Let $d \in \mathbb{N}$, and let $\mathcal{G}$ be the group of formal self-maps of $K^d$ fixing zero. Then each element of $\mathcal{G}$ tangent to the identity has uncountable centraliser in $\mathcal{G}$.

These results are not new in dimension $d = 1$. See [6, 4, 5].

In Theorem 1 it is possible to relax the hypothesis that $K$ be a field. It works on the weaker hypothesis that $K$ be an integral domain of characteristic zero having a certain technical property (called $\rho$-intactness, described in Subsection 2.4 of Section 2 below). For instance, it works for $K = \mathbb{Z}_p$, the ring of $p$-adic integers corresponding to any prime $p$, and for any ring that contains the rational field $\mathbb{Q}$.

1.5. Wider Context. We came to this subject because of our interest in reversibility [6]. We would like to characterise the reversible elements of well-known groups. The power series or formal map groups with real or complex coefficients are usually considered as a preliminary step in approaching groups of diffeomorphisms or biholomorphic maps. We would also hope that progress on the formal map groups will lead to progress on Riordan-style groups, semidirect products of a group of invertibles and a group of automorphisms. The formal maps we study in the present paper are precisely the $K$-algebra automorphisms of the $K$-algebras $\mathcal{F}_d$.

It is standard procedure, in attempting to understand reversibility, to start with centralisers [6]. The results of the present paper are a first step. However, it remains to give a characterisation of the full centraliser of the maps $g$ we consider. It is plausible that in many cases the one-parameter group we identify will be the full centraliser, or will have finite index in the centraliser. We expect this to be the generic situation. However, if the map $g$ is the direct product $(h, k)$ of two similar maps in lower dimensions, then the centraliser of $g$ will have an abelian two-parameter subgroup. We conjecture that whenever the one-parameter group we construct here does not have finite index in the whole centraliser, the map $g$ is conjugate to a product, but this conjecture is unproven to date. We hope that further progress in this
direction might allow us to prove another conjecture, namely that a reversible formal map can always be reversed by a map of finite order.

2. Sum functions

We make no claim to originality for the content of this section and the next. These are included for expository purposes and to set up notation and terminology for later use. The mathematical content must be largely familiar to people who have thought about these matters.

2.1. Let $K$ be an integral domain with identity. We denote the field of fractions of $K$ by $\hat{K}$, and regard $K$ as a subring of $\hat{K}$.

Let $\pi_K$ denote the group homomorphism from $(\mathbb{Z}, +)$ into $(K, +)$ such that $\pi_K(1_{\mathbb{Z}}) = 1_K$. An induction argument shows that it is also a ring homomorphism. We denote the image $\pi_K(\mathbb{Z})$ by $\mathbb{Z}_K$. The ring $\mathbb{Z}_K$ is isomorphic to the quotient ring $\mathbb{Z}/(c)$, where $c$ is the characteristic of $K$. If $c > 0$, then $\mathbb{Z}_K$ is the prime field of $K$. In characteristic zero, we have $\mathbb{Q}_K := \hat{\mathbb{Z}}_K \subset \hat{K}$ (and $\pi_K$ extends to a field isomorphism from $\mathbb{Q}$ onto $\mathbb{Q}_K$), but it may happen that there are elements in $\mathbb{Z}_K$ that are noninvertible in $K$.

The basic sum-functions with respect to $K$ are the $\rho_m = \rho_{m,K} : \mathbb{Z}_+ \to K$, defined inductively for $m \in \mathbb{Z}_+$ by:

$$\rho_0(k) := 1_K, \forall k \in \mathbb{Z}_+,$$

$$\rho_{m+1}(k) := \sum_{r=0}^{k} \rho_m(r), \forall k \in \mathbb{Z}_+.$$

**Definition 1.** A function $f : \mathbb{Z}_+ \to K$ is a sum-function over $K$ if it belongs to the $K$-linear span of the basic sum functions, i.e. there exist $m \in \mathbb{Z}_+$ and $\lambda_0, \ldots, \lambda_m \in K$ such that

$$f(k) = \sum_{i=0}^{m} \lambda_i \cdot \rho_i(k), \forall k \in \mathbb{Z}_+.$$

We denote the set of all sum-functions by $\Sigma_K$, or just $\Sigma$, when the context is clear.

2.2. The case $K = \mathbb{Z}$. It is easy to see that

$$\rho_{m,\mathbb{Z}}(k) = \binom{m + k}{m} = \binom{m + k}{k},$$

whenever $m, k \in \mathbb{Z}_+$. Thus $\rho_{m,\mathbb{Z}}(k) = p(k)$, where $p(t) \in \mathbb{Q}[t]$ is a polynomial over $\mathbb{Q}$, having degree $m$ and leading coefficient $\frac{1}{m!}$. Thus each sum function $f \in \Sigma_{\mathbb{Z}}$ coincides on $\mathbb{Z}_+$ with some polynomial $p(t)$ over $\mathbb{Q}$, and maps $\mathbb{Z}_+$ into $\mathbb{Z}$. Since $p(t)$ agrees with $f(t)$ on the infinite
set $\mathbb{Z}_+$, if follows that $p$ is uniquely determined by $f$. We abuse the notation and denote $p(t)$ by $f(t)$. For instance,

$$p_{m,\mathbb{Z}}(t) = \frac{t(t-1) \cdots (t-m+1)}{m!}.$$ 

According to Pólya’s definition a polynomial $p(t) \in \mathbb{Q}[t]$ is integer-valued if $p(n) \in \mathbb{Z}$ whenever $n \in \mathbb{Z}$.

Proposition 2.1. The sum-functions over $\mathbb{Z}$ are the same as the restrictions to $\mathbb{Z}_+$ of the integer-valued polynomials.

Proof. Given a sum function $f \in \Sigma_{\mathbb{Z}}$, let $f(t) \in \mathbb{Q}[t]$ be the corresponding polynomial. If $f(t)$ has degree $n$, then it is uniquely determined by the values $f(0), f(1), \ldots, f(n)$, and it can be evaluated at each point $x \in \mathbb{Q}$ by Newton’s interpolation formula:

$$f(x) = f(0) + f[0, 1]x + f[0, 1, 2]x(x - 1) + \cdots + f[0, 1, \ldots, n]x(x - 1) \cdots (x - n),$$

where $f[0, 1, \ldots, m]$ denotes the usual divided difference. Observing that $f[0, 1, \ldots, m]$ takes the form of some integer divided by $m!$, and recalling that $m!$ divides any product of $m$ consecutive positive integers, we see that $f(x) \in \mathbb{Z}$ whenever $x$ is a negative integer. Thus $f(t)$ is an integer-valued polynomial.

For the converse, suppose $p(t)$ is an integer-valued polynomial. We wish to see that $p|_{\mathbb{Z}_+}$ is a sum-function.

If $\deg(p) = 0$, then $p = p(0)$ is an integral multiple of $\rho_0$. Proceeding inductively, suppose $m \in \mathbb{N}$ and we are given that each polynomial over $\mathbb{Q}$ of degree less than $m$ that maps $\mathbb{Z}$ into $\mathbb{Z}$ gives a $\mathbb{Z}$-linear combination of $\rho_0, \ldots, \rho_{m-1}$. Fix $p(t) \in \mathbb{Q}[t]$ of degree $m$, and suppose it maps $\mathbb{Z}$ into $\mathbb{Z}$. Then $q(t) := p(t) - p(t - 1)$ belongs to $\mathbb{Q}[t]$, has degree $m - 1$, and maps $\mathbb{Z}$ into $\mathbb{Z}$, so there exist $\lambda_j \in \mathbb{Z}$ such that

$$p(k) - p(k - 1) = \sum_{j=0}^{m-1} \lambda_j \cdot \rho_j(k),$$

whenever $k \in \mathbb{Z}_+$. Thus for $k \in \mathbb{Z}_+$ we have

$$p(k) = \sum_{r=1}^{k} \sum_{j=0}^{m-1} \lambda_j \cdot \rho_j(k) + p(0),$$

$$= \sum_{j=1}^{m} \lambda_{j-1} \cdot \rho_j(k) + p(0)\rho_0(k).$$

So $p$ is a sum-function, a $\mathbb{Z}$-linear combination of $\rho_0, \ldots, \rho_m$. □
In particular, for each polynomial \( p(t) \in \mathbb{Z}[t] \), the restriction \( p|_{\mathbb{Z}_+} \) is a sum-function over \( \mathbb{Z} \).

**Corollary 2.1.** For each \( n \in \mathbb{Z}_+ \), the function \( k \mapsto k^n \) belongs to \( \Sigma_{\mathbb{Z}} \). □

From the proof of Proposition 2.1 we conclude:

**Corollary 2.2.** The basic sum-functions over \( \mathbb{Z} \) form a basis for the \( \mathbb{Z} \)-module (free abelian group) of all integer-valued polynomials. Moreover, for each \( n \in \mathbb{Z}_+ \), the subspace of integer-valued polynomials of degree at most \( n \) is the span of the first \( n+1 \) basic sum-functions. □

Using equation (1), one sees that the coefficient of \( \rho_n \) in the expression of \( t^n \) as an integral combination of basic sum-functions is \( \frac{1}{n!} \).

We define the **degree** of a sum-function over \( \mathbb{Z} \) to be the degree of the corresponding integer-valued polynomial.

**Corollary 2.3.** \( \Sigma_{\mathbb{Z}} \) forms a ring under pointwise operations.

**Proof.** The pointwise product of two integer-valued polynomials is obviously an integer-valued polynomial. Thus \( \Sigma_{\mathbb{Z}} \) is closed under pointwise products, as well as pointwise sums. □

We remark that the proof is easily modified to show that a given polynomial of degree \( n \) (over any field of characteristic zero containing \( \mathbb{Z} \)) maps \( \mathbb{Z} \to \mathbb{Z} \) as soon as it maps any \( n+1 \) consecutive integers into \( \mathbb{Z} \).

### 2.3. General \( K \)

Now consider an arbitrary integral domain \( K \) with identity.

**Proposition 2.2.** (1) \( \Sigma_{K} \) is the \( K \)-linear span of the maps \( k \mapsto \pi_K \left( \binom{m+k}{m} \right) \).

(2) \( \Sigma_{K} \) is also the \( K \)-linear span \( K \cdot (\pi_K \circ \Sigma_{\mathbb{Z}}) \) of the set \( \{ \pi_K \circ (p|_{\mathbb{Z}_+}) : p(t) \text{ is an integer-valued polynomial} \} \).

(3) \( \Sigma_{K} \) contains the set \( K[t] \circ \pi_K \) of all the maps \( k \mapsto p(\pi_K(k)), \ (p(t) \in K[t]) \).

**Proof.** Obviously, \( \rho_{m,K} = \pi_K \circ \rho_{m,\mathbb{Z}} \) so part (1) follows at once from equation (1).

(2) Follows from Proposition 2.1.

(3) Follows from Corollary 2.1. □
Corollary 2.4. The set $\Sigma_K$ of sum-functions is a $K$-algebra of functions from $\mathbb{Z}_+ \to K$, when equipped with pointwise operations of addition, multiplication and scalar multiplication.

Proof. This follows from Corollary 2.3 and part (2) of Proposition 2.2.

From part (1) of Proposition 2.2 we deduce:

Proposition 2.3. The pointwise product of $\rho_m$ and $\rho_n$ is a $\mathbb{Z}_K$-linear combination of $\rho_j$’s, where $j$ ranges from $0$ to $m+n$, and the coefficient of $\rho_{m+n}$ is $\pi_K\left(\binom{m+n}{n}\right)$. □

We note that the latter coefficient may be zero, depending on the characteristic of $K$.

2.4. Characteristic zero. If $K$ has characteristic $0$, then the basic sum-functions are linearly-independent over $\hat{K}$ (when considered as functions from $\mathbb{Z}_+$ into $\hat{K}$), and each element $f$ of $\Sigma_K$ takes the form $p \circ \pi_K$, where $p(t) \in \hat{K}[t]$ is a polynomial over $\hat{K}$, and indeed $p(t)$ has its coefficients in the product ring $K \cdot \mathbb{Q}_K$. The polynomial $p$ is uniquely-determined by $f$, and we denote it by $\hat{f}$.

Indeed, the polynomial $\hat{\rho}_{m,K}$ has degree $m$, and a nontrivial $\hat{K}$-linear relationship between the $\hat{\rho}_{m,K}$ would entail a $\hat{K}$-linear relationship between the $\hat{\rho}_{m,K}$, and that cannot occur between polynomials having distinct degrees.

Hence each $f \in \Sigma_K$ has a unique expression as a $K$-linear combination of basic sum-functions, and we may define the degree of $f$ to be the least $m \geq 0$ such that the coefficient of $\rho_{n,K}$ is zero for all $n > m$. This is then the same as the degree of the polynomial $\hat{f}$.

Proposition 2.4. Let $K$ have characteristic zero, and let $p(t) \in \hat{K}[t]$. If $p(a) \in K$ whenever $a \in K$, then $p \circ \pi_K$ is a sum-function over $K$.

Proof. Suppose $p$ maps $K$ into $K$. If $\deg(p) = 0$, then $p \circ \pi = p(0)\rho_0$ is a sum function of degree $0$. Proceeding inductively, suppose $m \in \mathbb{N}$ and we are given that each polynomial over $\hat{K}$ of degree less than $m$ that maps $K$ into $K$ gives a sum-function. Fix $p(t) \in \hat{K}[t]$ of degree $m$, and suppose it maps $K$ into $K$. Then $q(t) := p(t) - p(t-1)$ belongs to $\hat{K}(t)$, has degree $m-1$, and maps $K$ into $K$, so there exist $\lambda_j \in K$ such that

$$(p \circ \pi)(k) - (p \circ \pi)(k-1) = \sum_{j=0}^{m-1} \lambda_j \cdot \rho_j(k),$$
whenever $k \in \mathbb{Z}_+$. Thus for $k \in \mathbb{Z}_+$ we have

$$(p \circ \pi)(k) = \sum_{r=1}^{k} \sum_{j=0}^{m-1} \lambda_j \cdot \rho_j(k) + p(0),$$

$$= \sum_{j=1}^{m} \lambda_{j-1} \cdot \rho_j(k) + p(0)\rho_0(k).$$

So $p \circ \pi$ is a sum-function. □

A simple-minded converse to Proposition 2.4 would say that if $h$ is a sum-function, then $\hat{h}$ maps $K$ into $\hat{K}$. But this is not true, in general. For instance, taking $K := \mathbb{Z}[y]$ for an indeterminate $y$, the polynomial corresponding to the basic sum-function $\rho_2$ is $\rho_2(t) = \frac{1}{2}t(t+1)$, and yet $\hat{\rho}_2(y) = \frac{1}{2}y(y+1)$ does not belong to $K$. It does not help to assume $K$, or even $(K, +)$, finitely-generated, because the same $\hat{\rho}_2$ does not map the ring of Gaussian integers into itself.

Prompted by this, let us say that an integral domain $K$ is $\rho$-intact if $K$ has characteristic zero and

$$\hat{\rho}_m(a) \in K, \forall a \in K \forall m \in \mathbb{Z}_+.$$

Examples of $\rho$-intact domains are $\mathbb{Z}$, the ring $\mathbb{Z}_p$ of $p$-adic integers corresponding to a prime $p$, and all fields of characteristic zero. It is also easy to see that if $K$ is any integral domain of characteristic zero, then $K\mathbb{Q}_K$ and $\hat{K}$ are $\rho$-intact. (In the case of $K\mathbb{Q}_K$, you could use the fact that the product of each $m$-term arithmetic progression of integers is divisible by $m!$.) Define the $\rho$-intact-envelope of $K$ to be

$$K_\rho := \bigcap \{L : K \subset L, L \text{ is a } \rho\text{-intact subring of } \hat{K}\}.$$

Then $K_\rho$ is $\rho$-intact, and $K \subset K_\rho \subset K\mathbb{Q}_K$. Of course, if $K$ is $\rho$-intact, then $K_\rho = K$.

With this terminology, we have, trivially:

**Proposition 2.5.** If $K$ is a domain of characteristic zero, then $\hat{h}(t) \in (K\mathbb{Q}_K)[t]$ maps $K_\rho$ into $K_\rho$ for each sum-function $h \in \Sigma_K$. □

**Remark.** This account of sum-functions in characteristic zero $K$ could be recast in the language of Elliott [1]. The $\rho$-intact integral domains of characteristic zero are torsion-free examples of binomial rings, a concept useful in group theory that goes back to Philip Hall [2] (or [3]), and has a substantial literature. The $\rho$-intact envelope of a $\hat{K}$ of characteristic zero is the same as the binomial ring $\text{Bin}^U(K)$ of theorem 7 in [1], where the functor $\text{Bin}^U$ from the category of commutative rings
with identity to the category of binomial rings is a left adjoint of the forgetful functor from binomial rings to rings.

2.5. Positive characteristic. In positive characteristic $c$ some sum-functions are not given by polynomials at all. All polynomial functions $P \circ \pi_K$, with $P(t) \in K[t]$ have period $c$, because $\pi_K(k + c) = \pi_K(k)$ for $k \in \mathbb{Z}_+$. But in characteristic 2, for instance, the sequences $(\rho_m(k))_k$ for $m = 0, 1, 2, 3, 4$ begin:

\begin{align*}
1,1,1,1,1,1,1,1, \ldots, \\
1,0,1,0,1,0,1,0, \ldots, \\
1,1,0,0,1,0,0,0, \ldots, \\
1,0,0,0,1,0,0,0, \ldots, \\
1,1,1,1,0,0,0,0, \ldots,
\end{align*}

and have periods 1, 2, 4, 4 and 8, respectively.

In fact, all sum-functions are periodic in finite-characteristic, and more:

**Theorem 4.** Let the integral domain $K$ have characteristic $c > 0$. Then for each $r \in \mathbb{Z}_+$, the set \{\(\rho_m : 0 \leq m < c^r\}\} is a basis for the $K$-module of all functions $f : \mathbb{Z}_+ \to K$ that have period $c^r$.

To be clear, when we say that $f$ has period $n$ we mean that $f(k+n) = f(k)$ for all $k \in \mathbb{Z}_+$. We do not mean that $n$ is the least positive period of $f$.

We will prove this theorem in Section 3.

The theorem has several immediate corollaries:

**Corollary 2.5.** Suppose $K$ has characteristic $c > 0$.
(1) The sum-functions over $K$ are the same as the functions whose least positive period is some power of $c$.
(2) The basic sum-functions form a linearly-independent set over $\hat{K}$.
(3) Each sum-function $h \in \Sigma_K$ has a unique expression

$$h(k) = \sum_{m=0}^{\infty} h_m \rho_m(k), \quad \forall k \in \mathbb{Z}_+,$$

in which each $h_m \in K$ and only a finite number of $h_m$ are nonzero. \(\square\)

This allows us to define the degree of a sum-function as follows:

**Definition 2.** The degree of the sum-function $h = \sum_m h_m \rho_m$ is the largest $m$ having $h_m \neq 0$.

This is consistent with the definitions previously given in the case of rings $K$ of characteristic zero, although it no longer relates to the degree of any associated polynomial.

From Corollary 2.3 we deduce:
Proposition 2.6. If \( h \) and \( h' \) are sum-functions, then
\[
\deg(hh') \leq \deg(h) + \deg(h').
\]
\[\square\]

3. Block-patterns

This section may be skipped by readers who are only interested in domains \( K \) of characteristic zero. Suppose the integral domain \( K \) has characteristic \( c > 0 \). We may regard the values \( \rho_m(k) \in \mathbb{Z}_K \) as forming an infinite matrix, with entries drawn from \( \{0, 1, \ldots, c-1\} \), with rows indexed by \( m = 0, 1, 2, \ldots \) and columns indexed by \( k = 0, 1, 2, \ldots \). We call this the basic sum-function matrix, and denote it by \( B \). It is an element of the matrix ring \( \text{gl}(\mathbb{Z}_+, \mathbb{Z}_K) \), and \( B_{mk} := \rho_m(k) \).

It is a symmetric matrix. The top-left \( c \times c \) block provides a pattern that we call the template, and denote by \( B_1 \). It has the \( c^2 \) entries given by
\[
\rho_m(k) = \binom{m+k}{k} = \frac{(m+k) \cdots (m+1)m}{k!},
\]
where we note that \( k! \) is invertible in \( \mathbb{Z}_K \) when \( 0 \leq k < c \). For instance, the templates in characteristics 3 and 5 are
\[
\begin{pmatrix}
1 & 1 & 1 \\
1 & 2 & 0 \\
1 & 0 & 0 \\
\end{pmatrix}, \quad \begin{pmatrix}
1 & 1 & 1 & 1 & 1 \\
1 & 2 & 3 & 4 & 0 \\
1 & 3 & 1 & 0 & 0 \\
1 & 4 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
\end{pmatrix}
\]
For general \( r \in \mathbb{N} \), we denote the top left \( c^r \times c^r \) block of \( B \) by \( B_r \).

The top left \( c^2 \times c^2 \) block \( B_2 \) falls into \( c^2 \) blocks, each one \( c \times c \), and (as we shall see) the pattern is that the \( (i, j) \)-th \( c \times c \) block is obtained from the template by multiplying each term (modulo \( c \)) by the \( (i, j) \)-th entry in the template! Thus, denoting the template by \( T \), the patterns in characteristics 3 and 5 are:
\[
\begin{pmatrix}
T & T & T \\
T & 2T & T \\
T & 0 & 0 \\
\end{pmatrix}, \quad \begin{pmatrix}
T & T & T & T & T \\
T & 2T & 3T & 4T & 0 \\
T & 3T & T & 0 & 0 \\
T & 4T & 0 & 0 & 0 \\
T & 0 & 0 & 0 & 0 \\
\end{pmatrix}
\]
The block \( B_3 \), is obtained by iterating this procedure: It has \( c^2 \) blocks, each \( c^2 \times c^2 \), and they are obtained from the top left \( c^2 \times c^2 \) block by multiplying it by the appropriate entry in the template. For instance,
you can discern this structure in the following top left section of the characteristic 3 matrix $B$:

$$
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 \\
1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2 \\
1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 0 \\
1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 
\end{pmatrix}
$$

Each number $m \in \mathbb{Z}_+$ has a unique canonical $c$-adic expansion

$$
m = \sum_{r=0}^{\infty} m_r c^r
$$

in powers of (the prime) $c$, where $0 \leq m_r < c$ and only a finite number of $m_r$ are nonzero. Using the $c$-adic expansions of $m$ and $k$, we have a formula for $\rho_m(k)$:

**Proposition 3.1.** If $m, k \in \mathbb{Z}_+$ have the canonical $c$-adic expansions $m = \sum_{r=0}^{\infty} m_r c^r$ and $k = \sum_{r=0}^{\infty} k_r c^r$, then

$$
(1)
$$

$$
(2) \quad \rho_m(k) = \prod_{r=0}^{\infty} \rho_{m_r}(k_r),
$$

(2) In particular, for each $r \geq 1$, $\rho_m(k) = 0$ whenever $m < c^r$, $k < c^r$, and $m + k \geq c^r$. 


Note that all but a finite number of terms in the product are equal to 1. In fact, since \( m_r = 0 \) when \( r > \log_c m \), we may write

\[
\rho_m(k) = \prod_{r=0}^{\lfloor \log_c m \rfloor} \prod_{s=0}^{\lfloor \log_c k \rfloor} \rho_{m_r}(k_s),
\]

where \( \lfloor \cdot \rfloor \) denotes the floor function. This proposition expresses all entries in the \( (\rho_m(k)) \) matrix in terms of the upper left \( c \times c \) template \( B_1 \), and justifies the pattern described at the end of the last subsection.

Part (2) may be summarized by saying that the submatrices \( B_r \) are ‘upper-left triangular’, i.e. have zero entries below the antidiagonal.

**Proof.** It is obvious that formula (2) holds when \( m < c \) and \( k < c \), i.e. for the entries in the template. Both sides of the formula are symmetric in \( m \) and \( k \), so it suffices to prove the case \( k \leq m \geq c \).

We proceed by induction. Suppose \( r \geq 1 \) and (1) and (2) hold whenever \( m < c^r \) and \( k < c^r \). Fix \( m \) and \( k \) with \( c^r \leq m < c^{r+1} \), and \( 0 \leq k \leq m \). Then \( m_r \neq 0 \), and \( m = m_r c^r + m' \) with \( 0 \leq m' < c^r \). Also \( k = k_r c^r + k' \) with \( 0 \leq k' < c^r \).

\( \rho_m(k) \) is the coefficient of \( t^m \) in \( (1 + t)^{m+k} \) (regarded as a polynomial over \( \mathbb{Z}_K \)). In standard notation, we denote this coefficient by \([t^m](1 + t)^{m+k}\). Thus

\[
\rho_m(k) = [t^m] \left( (1 + t)(m_r + k_r)c^r \right)^{m+k}.
\]

Now \( (1 + t)^c = 1 + t^c \) (since \( c = 0 \) in \( K \)), and repeating this we get

\[
(1 + t)(m_r + k_r)c^r = (1 + t^c)^{m_r + k_r}.
\]

From this factor, only the term in \( t^{m_r c^r} \) can contribute to \( \rho_m(k) \) (since \( k' < c^r \)), so

\[
\rho_m(k) = \left( [t^{m_r c^r}](1 + t^c)^{m_r + k_r} \right) \cdot \left( [t^k](1 + t)^{m' + k'} \right).
\]

So

\[
\rho_m(k) = \rho_{m_r}(k_r) \cdot \rho_{m'}(k').
\]

Applying the assumption (1) to \( m' = \sum_{s<r} m_s c^s \) and \( k' = \sum_{s<r} k_s c^s \), we have

\[
\rho_{m'}(k') = \prod_{s<r} \rho_{m_s}(k_s),
\]

so we get formula (2) for the pair \((m, k)\).

Turning to (2), we want to show that \( \rho_m(k) = 0 \) if \( m + k \geq c^{r+1} \). But if \( m + k \geq c^{r+1} \), then \( m_r + c_r \geq c \), and hence \( \rho_{m_r}(c_r) = 0 \) (i.e. the template is upper-left triangular), and hence the formula gives \( \rho_m(k) = 0 \).
This completes the induction step, and the proof.

We now draw some corollaries. First, the $c^r$-th rows of the matrix take a special form:

**Corollary 3.1.** For $r \in \mathbb{Z}^+$, we have $\rho_{c^r}(k) = k_r + 1$.

**Proof.** Formula (2) gives

$$\rho_{c^r}(k) = \rho_1(k_r),$$

since $\rho_0(j) = 1$ for all $j$. But $\rho_1(k) = k + 1$ (modulo $c$).

In particular, the first $c^r$ entries in the $c^r$-th row are all 1. The $c^r + 1$-st entry is 2 (equal to zero, in case $c = 2$).

By symmetry, we have:

**Corollary 3.2.** For $r \in \mathbb{Z}^+$, we have $\rho_m(c^r) = m_r + 1$.

Combining these, we see that the upper-left triangular square submatrix $(B_{mk})$ indexed by $1 \leq m, k < c^r$ is ‘framed’ in $B$ by a square of 1’s, except that that lower right corner of the frame is a 2.

By repeatedly applying the Law of Pascal’s triangle, working up from the $c^r$-th row, we deduce inductively:

**Corollary 3.3.** For each $r \in \mathbb{N}$ all elements on the antidiagonal of $B_r$ are of the form $\pm 1$, and alternate between $+1$ and $-1$.

In other words, for $0 \leq m, k < c^r$, we have

$$\rho_m(c^r - m - 1) = \pm 1.$$ Note that except in characteristic 2, this antidiagonal has an odd number of entries, and in characteristic 2, all the entries are the same.

Thus if we reverse the order of the rows in $B_r$, we get a lower-triangular matrix having invertible elements on the diagonal.

**Corollary 3.4.** $B_r \in \text{GL}(c^r, K)$, so the $K$-linear span of the rows is $K^{c^r}$, and the rows are $K$-linearly-independent.

Next, since $\rho_0(k) = 1$ for all $k$, the formula gives:

**Corollary 3.5.** $\rho_m$ has period $c^r$ whenever $0 \leq m < c^r$.

*Proof of Theorem 4.* The last two corollaries combine to complete the proof of Theorem 4. The $\rho_m$ are periodic, with period $c^r$; they are already $K$-linearly-independent as functions on the first $c^r$ nonnegative integers, and hence a fortiori as functions on $\mathbb{Z}_+$; and their $K$-linear combinations give every $K$-valued function on $\mathbb{Z}_+$ of period $c^r$, because any such function is determined by its values on the subset \{0, 1, \ldots, c^r - 1\}. \qed
4. Iteration of Formal Maps

4.1. Coefficients of iterates. We now consider the iteration of a map $g \in \mathcal{G}$. We define $g^{\circ k}$ for $k \in \mathbb{Z}_+$ by setting $g^{\circ 0} := \mathbb{1}$ and inductively defining $g^{\circ (k+1)} := g \circ g^{\circ k}$.

We also define the backward iterates by $g^{\circ -k} := (g^{\circ (-1)})^k$.

For each $g \in \mathcal{G}$, the map $k \mapsto g^{\circ k}$ is a homomorphism from the additive group $(\mathbb{Z}, +)$ into $\mathcal{G}$:

$$ g^{\circ (k+l)} = g^{\circ k} \circ g^{\circ l}, $$

whenever $k, l \in \mathbb{Z}$.

In the same way, we can define the $k$-th iterate $g^{\circ k}$ of an element $g$ belonging to the semigroup $\mathcal{M}^d$, provided $k \in \mathbb{Z}_+$, but we cannot in general define it for negative integers $k$. For each such $g$, the map $k \mapsto g^{\circ k}$ is a homomorphism from the additive semigroup $(\mathbb{Z}_+, +)$ into the compositional semigroup $(\mathcal{M}^d, \circ)$.

An element $g \in \mathcal{M}^d$ has a series expansion

$$ g = \sum_{m \in S} g_m \cdot m, $$

where $g_m = ((x_1 \circ g)_m, \ldots, (x_d \circ g)_m)$ belongs to $K^d$. We refer to $g_m$ as the $m$-th coefficient of $g$. Note that $g_m$ is a $d$-dimensional vector over $K$. If we group terms of the same degree, by defining

$$ L_k(g) := \sum_{m \in S, \deg m = k} g_m \cdot m, \forall k \in \mathbb{Z}_+, $$

then we get the expansion

$$ g = \sum_{k=1}^{\infty} L_k(g). $$

Here, $L_1(g) = L(g)$ is the linear part of $g$, and in general we refer to $L_k(g)$ as the $k$-th homogeneous term of $g$. This term is a $K^d$-valued homogeneous polynomial of degree $k$ with coefficients in $K$, or, equivalently, it is a $d$-tuple of homogeneous polynomials of degree $k$ over $K$.

**Theorem 5.** Suppose $g \in \mathcal{G}$ is tangent to the identity, and let $m \in S$. Then there is a $d$-tuple of sum-functions $P(t) \in \Sigma_k^d$ (depending on $g$ and $m$) such that $(g^{\circ k})_m = P(k)$ for each $k \in \mathbb{N}$. 

Proof. The \(j\)-th component of the coefficient \((g^k)_m\) is the matrix entry \((x_j \circ g^k)_m\) of \(M(1, g)^k\), so we want to show this is a sum-function of the variable \(k\). Thus it is enough to show that each entry \((n \circ (g^k))_m\) is a sum-function in \(k\) (with coefficients in \(K\)).

Consider the hypothesis \((H_s)\): that the entry \((n \circ (g^k))_m\) is a sum-function in \(k\) of degree less than \(\deg(m)\) whenever \(m, n \in S\) and \(\deg m < s\).

This holds for \(s = 2\), because the only monic monomials of degree 1 are the \(x_j\) \((j = 1, \ldots, d)\), and

\[
(n \circ (g^k))_{x_j} = (n \circ 1)_{x_j} = \begin{cases} 1, & n = x_j, \\ 0, & \text{otherwise}. \end{cases}
\]

Assume that \(s \geq 2\) and \(H_s\) holds. We claim that \(H_{s+1}\) also holds. To prove this, we have to show that for each \(m \in S\) of degree \(s\), and each \(n \in S\), the entry \((n \circ (g^k))_m\) is a sum-function in \(k\) of degree less than \(s\).

Fix \(m \in S\), of degree \(s\).

First, consider the case \(n = x_j\), for some \(j \in \{1, \ldots, d\}\), and let \(\alpha_k := (x_j \circ (g^k))_m\). For \(k \geq 1\), we have

\[
\alpha_{k+1} = (x_j \circ g \circ g^k) = \sum_{p \in S} (x_j \circ g)_p \cdot (p \circ g^k)_m.
\]

If \(\deg(p) = 0\) or \(\deg(p) > s\), then \((p \circ g^k)_m = 0\). If \(\deg(p) = 1\), then \(p = x_i\) for some \(i\), and \((x_j \circ g)_p\) is equal to 1 or 0, depending on whether or not \(i = j\). If \(\deg(p) = s\), then \((p \circ g^k)_m = p_m\) and equals 1 or 0, depending on whether or not \(p = m\). So if we let

\[
T := \{p \in S : 1 < \deg(p) < s\},
\]

and \(\lambda_p := (x_j \circ g)_p\), then

\[
\alpha_{k+1} = \alpha_k + \sum_{p \in T} \lambda_p \cdot (p \circ g^k)_m + \lambda_m.
\]

Fix \(p \in T\). Since the degree of \(p\) is at least 2, we can factor \(p\) as \(x_i \cdot q\) for some \(q \in S\), and then

\[
p \circ g^k = (x_i \circ g^k) \cdot (q \circ g^k),
\]

so

\[
(3) \quad (p \circ g^k)_m = \sum_{r|m} (x_i \circ g^k)_r \cdot (q \circ g^k)_{m/r}.
\]

In this sum, the hypothesis \(H_s\) tells us that the terms are sum-functions in \(k\), except perhaps for the terms \(r = 1\) and \(r = m\). The term with
$r = 1$ is zero (because $(x_i \circ g^\circ k)_1 = 0$), and the term with $r = m$ is also zero, because $(q \circ g^\circ k)_1 = 0$. Thus $(p \circ g^\circ k)_m$ is a sum-function in $k$.

It follows that

$$\alpha_{k+1} = \alpha_k + P(k),$$

where $P$ is a sum-function in $t$. Thus

$$\alpha_k = \sum_{r=1}^{k-1} P(r) + \alpha_1$$

is a sum-function in $k$, of degree at most $\deg(P) + 1$.

It remains to show that the degree of $P$ is less than $\deg(m)$. By the induction hypothesis, the $r$-th term in the sum in Equation (3) is zero or is the product of a sum-function in $k$ of degree less than $\deg(r)$ and a sum-function of degree less than $\deg(m/r)$, so it has degree less than or equal to

$$\deg(r) - 1 + \deg(m/r) - 1 = \deg(m) - 1.$$

Thus $(n \circ g^\circ k)_m$ is a sum-function in $k$ when $n = x_j$.

Now consider a monomial $n \in S$ of degree greater than 1. We can factor $n$ as $x_i \cdot q$ for some $q \in S$ of degree at least 1, and then

$$(n \circ g^\circ k)_m = \sum_{r|m} (x_i \circ g^\circ k)_r \cdot (q \circ g^\circ k)_{m/r}.$$

As before, the terms with $r = 1$ and $r = m$ have a zero factor, hence equal zero. In the nonzero terms, $\deg(r) < s$ and $\deg(m/r) < s$, so by the induction hypothesis each such term is the product of a sum-function in $k$ of degree less than $\deg(r)$ and another of degree less than $s/\deg(r)$. Hence $(n \circ g^\circ k)_m$ is a sum-function in $k$ of degree less than $s$.

Thus $H_{s+1}$ holds.

By induction, $H_s$ holds for all $s$, and the theorem is proven. □

From the proof, we note:

**Corollary 4.1.** Each component of $P(t)$ is a sum-function of degree less than the degree of $m$, and it depends only on the coefficients $g_p$ of the monomials $p \in S$ of degree less than or equal to the degree of $m$. □

In fact, the dependence on the coefficients of $g$ is polynomial.
4.2. Orders and degrees. The order of an element of a group is the least power of the element that equals the identity, or is infinity if there is no such power. If we speak about the order of a formal map \( g \in \mathcal{G} \), this is what we mean. For nonzero power series \( f \in \mathcal{F} \), people sometimes use the term ‘order’ to refer to the least \( k \in \mathbb{Z}_+ \) such that some monomial of degree \( k \) has a nonzero coefficient, what could informally be called the ‘order of vanishing’ of the series. We refer to this number as the lower degree of the series. We take the lower degree of \( 0 \) to be infinity. We extend this to \( d \)-tuples \((f_1, \ldots, f_d) \in \mathcal{F}^d\), by defining the lower degree to be the minimum of the lower degrees of the components \( f_j \). For \( g \in \mathcal{G} \), tangent to \( 1 \), we refer to the lower degree of \( g - 1 \) as the Weierstrass degree of \( g \).

**Proposition 4.1.** Suppose \( K \) has characteristic zero. If \( g \in \mathcal{G} \) is tangent to the identity, and \( g \neq 1 \), then \( g \) has infinite order.

*Proof.* We may write

\[
g = 1 + \sum_{k=r}^{\infty} L_k,
\]

where \( L_k = L_k(g) \) and \( r \geq 2 \) is least with \( L_r \neq 0 \). Then

\[
g^{o2}(x) = 1(g(x)) + L_r(g(x)) + \text{HOT} = 1 + L_r(x) + \text{HOT} + L_r(1) + \text{HOT} = 1 + 2L_r(x).
\]

Continuing inductively, we get

\[
g^{on} = 1 + nL_r + \text{HOT}.
\]

Thus \( g^{on} \neq 1 \) for each \( n \in \mathbb{N} \). \( \square \)

In finite characteristic \( c \), there are maps tangent to the identity that have finite order. For instance, in dimension one, take

\[
g(x) = \frac{x}{1 + x}.
\]

Then one calculates that

\[
g^{kc}(x) = \frac{x}{1 + kx},
\]

so \( g^{oc}(x) = x \), i.e. \( g^{oc} = 1 \). However, the argument in the proof of the proposition shows the following:

**Proposition 4.2.** Suppose \( K \) has characteristic \( c > 0 \). If \( g \in \mathcal{G} \) is tangent to the identity, then either \( g \) has infinite order, or the order of \( g \) is divisible by \( c \). \( \square \)
4.3. **Iterates to nonintegral order.** In this subsection we consider the possibility of defining iterates $g^\lambda$, where $\lambda$ belongs to the ring $K$. This possibility arises mainly in characteristic zero. In the following subsection, we will consider an alternative procedure in positive characteristic.

For $g \in \mathcal{G}$, Theorem 5 tells us that if $g$ is tangent to the identity, then for each monomial $m$, there is a sum-function $P_m(t)$ over $K$ (depending on $g$), of degree less than $\deg m$, such that $(g^ok)_m = P_m(k)$ for all $k \in \mathbb{N}$.

**Theorem 6.** Let $g \in \mathcal{G}$ be tangent to the identity, and fix a monic monomial $m \in S$ of degree $s$. If $s$ is not greater than the cardinality of $\mathbb{Z}_K$, then there exists a unique polynomial $P_m(t) \in \hat{K}[t]$ of degree less than $s$ such that $P_m(k) = (g^ok)_m \forall k \in \mathbb{Z}_+$. 

**Proof.** $P_m(t)$ is a polynomial over the field $\hat{K}$, so it is uniquely determined by its values at $\deg(P_m)+1$ distinct elements of $\hat{K}$. The elements $0_K, 1_K, \ldots, s \cdot 1_K$ are distinct, so the result follows. $\square$

**Corollary 4.2.** If $K$ has characteristic zero, then for each $m \in S$, the polynomial $P_m$ is uniquely determined by $g$.

**Definition 3.** Suppose $K$ has characteristic zero. For $g \in \mathcal{G}$, tangent to the identity, and $\alpha \in K$, we define the $\alpha$-th iterate $g^{\alpha}$ of $g$ by the formula

$$g^{\alpha} := \sum_{m \in S} P_m(\alpha) \cdot m,$$ 

This might be referred to as the formal-formal iterate, because it has to do with formal composition, and the order of iteration is also ‘formal’.

The series $g^{\alpha}$ is a power series over the $\rho$-intact envelope $K_\rho$, as opposed to $K$. We can, if we wish, extend the definition to allow any $\alpha$ belonging to $K_\rho, K\mathbb{Q}_K, \hat{K}$, or any $\rho$-intact domain that contains $K$. In case $\hat{K}$ is the ring of integers, the ring of $p$-adic integers or any field of characteristic zero, the formal-formal iterate $g^{\alpha}$ belongs to the original group $\mathcal{G} = G_K$.

Note that $g^{\pi_K(k)} = g^ok$ for $k \in \mathbb{Z}$.

**Theorem 7.** Suppose $K$ has characteristic zero. Then if $g \in \mathcal{G}$ is tangent to the identity, we have

$$g^{\alpha} \circ g^b = g^{\alpha+b}$$

whenever $a, b \in K$. 
Proof. If a polynomial equation holds at more points than the degree of the polynomial, then it holds identically. The identity
\[ g^{oa} \circ g^{ob} = g^{oa+b} \]
holds for all \( a \in \mathbb{N} \) and \( b \in \mathbb{N} \). As a result, for each \( m \in S \) and each index \( j \in \{1, \ldots, d\} \), we have
\[ (x_j \circ (g^{oa} \circ g^{ob}))_m = (x_j \circ (g^{oa+b}))_m \]
whenever \( a \in \mathbb{N} \) and \( b \in \mathbb{N} \). For fixed \( a \in \mathbb{N} \), this is a polynomial identity in \( b \), so since it holds for all \( b \in \mathbb{N} \), it holds identically for all \( b \in K \). Then, for fixed \( b \in K \) it is a polynomial identity in \( a \), and in the same way it must hold identically for all \( a \in K \). Since this holds for all \( m \in S \), all coefficients agree in the expansion of the two sides of Equation (4), and hence the equation holds for all \( a, b \in K \). \( \square \)

So in characteristic zero, we have the following fact:

**Corollary 4.3.** For each \( a \in K \), \( g^{oa} \) commutes with \( g \), and \( a \mapsto g^{oa} \) is a group homomorphism from the abelian group \((K, +)\) into the centraliser of \( g \) in \( G_{K^\rho} \). \( \square \)

This allows us to give:

**Proof of Theorem 7** The homomorphism \( a \mapsto g^{oa} \) is injective, because \( L_k(g^{oa}) = aL_k(g) \) when \( k \) is the Weierstrass degree of \( g \). \( \square \)

Theorem 7 has other interesting consequences:

**Corollary 4.4.** The coefficients of the compositional inverse \( g^{o-1} \) are given by \( P_m(-1) \). \( \square \)

**Corollary 4.5.** If \( g, h \in G \) are tangent to the identity and commute, then
\[ g^{oa} \circ h^{ob} = h^{ob} \circ g^{oa}, \forall a, b \in K. \] \( \square \)

In particular, if \( K \) is \( \rho \)-intact, then the map
\[ (a, b) \mapsto g^{oa} \circ h^{ob} \]
gives a group homomorphism from \((K^2, +)\) into the centraliser \( C_G(g) \) whenever \( g \) and \( h \) are commuting elements of \( G \) that are tangent to the identity. It is obviously of interest to know when this map is injective, so the following proposition is worth noting:

**Proposition 4.3.** Let \( g, h \in G \) be tangent to the identity. If there exists \( p \in K^\times \) such that \( h^{p} = g \), then \( g^{1/p} = h \), and
\[ \{h^{oa} : a \in K\} = \{g^{oa} : a \in K\}. \]


Thus, if we think of \( \{ h^a : a \in K \} \) as a ‘one-parameter subgroup’ (where the ‘parameter’ runs over \( K \)) of \( \mathcal{G} \), then two one-parameter subgroups in the centraliser of a \( g \) (tangent to but not equal to \( 1 \)) either coincide or give a ‘two-parameter subgroup’.

**Conjecture 1.** We conjecture that if \( K \) is a field of characteristic zero and \( g \in \mathcal{G} \) is tangent to but not equal to the identity, then the centraliser \( C^g \) of \( g \) in \( \mathcal{G} \) is abelian, and is the inner direct product of its torsion subgroup and a finite number of one-parameter groups of iterates \( \{ h^a : a \in K \} \). We expect that, generically the centraliser will be just \( \{ g^a : a \in K \} \), and that the occurrence of a two-parameter subgroup corresponds to the possibility of conjugating \( g \) to a product map, i.e. a formal map of the form \( (h(x_1, \cdots, x_m), k(x_{m+1}, \cdots, x_d)) \), where \( h \in \mathcal{G}_m \) and \( k \in \mathcal{G}_{d-m} \) for some \( m \in \mathbb{N} \) with \( 1 \leq m < d \).

The conjecture holds in dimension \( d = 1 \). 

4.4. \( c \)-adic iterates. Throughout this section, we suppose that \( K \) has positive characteristic \( c \).

There does not appear to be any reasonable way to define iterates \( g^{\lambda} \) for \( \lambda \in K \) in characteristic \( c \), but we can extend the scope of iteration in another way.

We impose the \( M \)-adic valuation topology on \( \mathcal{F} \), i.e. the topology induced by any translation-invariant metric that has
\[
\text{dist}(m \cdot f, 0) = 2^{-\deg m}
\]
whenever \( m \in S \) and \( f \in \mathcal{F}^\times \). Thus a sequence \( (f^{(n)})_n \) of power series over \( K \) converges to zero if and only if
\[
\forall m \in S, \exists N \in \mathbb{N} : n > N \implies (f^{(n)})_m = 0,
\]
i.e. the coefficient of each monomial in the expansion of \( f^{(n)} \) is eventually zero. We use the \( M \)-adic valuation topology on \( \mathcal{F} \) to generate a product topology on \( \mathcal{F}^d \), and restrict it to \( M^d \) and \( \mathcal{G} \). We refer to all these as \( M \)-adic valuation topologies.

**Theorem 8.** Suppose \( g \in \mathcal{G} \) has \( L(g) = 1 \). Then there is a continuous group homomorphism \( z \mapsto g^{oz} \) from \( (\mathbb{Z}_c, +) \) (the additive group of the \( c \)-adic integers) into \( \mathcal{G} \) that extends the iteration map \( k \mapsto g^{ok} \) from \( \mathbb{Z} \).

**Proof.** By Theorem 5, for each monic monomial \( m \in S \), we have a \( d \)-tuple of sum-functions \( P_m(t) \in \Sigma^d \) over \( K \) such that
\[
g^{ok} = \sum_m P_m(k)m, \quad \forall k \in \mathbb{Z}_+.
\]
For each $m$, the component functions of $P_m$ are of degree less than $m$, and hence $P_m$ is periodic of order $c^r$, where $r$ is the ceiling of $\log_c \deg m$, i.e. $P_m(k + c^r) = P_m(k)$ for all $k \in \mathbb{N}$.

Each $z \in \mathbb{Z}_c$ has a $c$-adic expansion $z = \sum_{s=0}^{\infty} z_s p^s$, and we now define

$$P_m(z) := P_m \left( \sum_{s=0}^{r} z_s p^s \right) \in K.$$ 

Observe that, by the periodicity,

$$P_m(z) = P_m \left( \sum_{s=0}^{t} z_s p^s \right)$$

whenever $t > r$, so that it does not matter where we truncate the expansion of $z$: as long as it is far enough out (depending on $m$), we get the same value for $P_m(z)$. Also, if $z \in \mathbb{Z}_0$, then the value of $P_m(z)$ is the same as it was.

Now we define

$$g^oz := \sum_m P_m(z)m.$$ 

Then $z \mapsto g^oz$ extends the iterates map from $\mathbb{Z}$ to $\mathbb{Z}_c$. The extended map is continuous from the $c$-adic valuation topology on $\mathbb{Z}_c$ to the $\mathcal{M}$-adic valuation topology on $\mathcal{G}$, because if $c^r$ divides $z - z'$, then $P_m(z) = P_m(z')$ whenever $\deg m < c^r$.

Since $g^ok \circ g^ok' = g^ok' \circ g^ok$ for all $k, k' \in \mathbb{Z}_0$, and since $\mathbb{N}$ is dense in $\mathbb{Z}_c$, it follows that

$$g^oz \circ g^{oz'} = g^{oz'} \circ g^oz$$

whenever $z, z' \in \mathbb{Z}_c$, so we have a group homomorphism, as asserted.

Finally, if $n \in \mathbb{N}$, then the newly-defined $g^{oz-n}$ — defined using the $c$-adic expansion of $-n$ — is the compositional inverse of $g^{on}$ (by the group homomorphism property), and hence must agree with $(g^{-1})^{on}$ (by the uniqueness of inverses in the group $\mathcal{G}$), so $z \mapsto g^oz$ extends the composition map from all of $\mathbb{Z}$, and not just from $\mathbb{Z}_+$. □

**Corollary 4.6.** If $g \in \mathcal{G}$ is tangent to the identity, then for each $n \in \mathbb{N}$ not divisible by $c$, there exists an $n$-th compositional root $h \in \mathcal{G}$ of $g$, i.e. an element with $h^{on} = g$.

**Proof.** If $n \in \mathbb{N}$ is not divisible by $c$, then $n \in \mathbb{Z}^\times_c$, so $n^{o1/n}$ is an $n$-th compositional root of $g$. □

In particular, if $c \neq 2$, each $g \in \mathcal{G}$ tangent to the identity has a compositional square root. In characteristic 2, we have roots of every odd order.

We can now conclude:
Proof of Theorem 2. If \( g \in G \) is tangent to the identity, and has infinite order, then the map \( k \mapsto g^{ok} \) is injective from \( \mathbb{Z}_+ \) into \( \mathcal{G} \). Since \( g^{or} \to \mathbb{I} \) as \( r \to \infty \), we see that \( \mathbb{I} \) is the limit of a sequence of distinct iterates.

The map \( z \mapsto g^{oz} \) is continuous from the compact space \( \mathbb{Z}_c \) so the one-parameter image subgroup is compact. Since the identity is not isolated, there are no isolated points, so it is a compact metric space without isolated points, and hence has the cardinality of the continuum. \( \Box \)

We don’t see any reason why the map \( z \mapsto g^{oz} \) has to be injective on \( \mathbb{Z}_c \), so we can’t say that the one-parameter subgroup is isomorphic to \((\mathbb{Z}_c, +)\).

4.5. Maps having linear part of finite order. We close with some remarks about the centralisers of formal maps having linear part of finite order.

Let \( K \) be any integral domain. Suppose \( h \in \mathcal{G} \) is such that its linear part \( L := L_1(h) \) is of finite order, say \( s \). Then \( g := h^{os} \) is tangent to the identity, and we may apply the results of the last two subsection to \( g \).

1. If \( h \) itself has finite order, and its order is not a multiple of the characteristic \( c \) of \( K \) (— this includes the case \( c = 0 \)), then \( h \) is conjugate to \( L \) (— compare the argument for lemma 2.1 in [7]) and so \( h \) has order \( s \). Then we can take any \( f \in \mathcal{F} \) with \( f_1 = 1 \) and form

\[
\tilde{f} := \frac{1}{s} \left( f + f \circ L + \cdots + f \circ L^{o(s-1)} \right).
\]

Then \( \tilde{f} \in \mathcal{F}, \tilde{f}_1 = 1 \) and \( \tilde{f} \circ L = \tilde{f} \). So

\[
\tilde{f}(x) := \tilde{f}(x) \cdot \mathbb{I} = (\tilde{f}(x)x_1, \ldots, \tilde{f}(x)x_d)
\]

belongs to \( \mathcal{G} \), is tangent to the identity, and commutes with \( L \). It follows that all \( \tilde{f}^{on} \) commute with \( L \), and then that \( \tilde{f}^\lambda \) also commutes with \( L \) for all \( \lambda \in K \) in characteristic zero or for all \( \lambda \in \mathbb{Z}_c \) in positive characteristic \( c \). Thus \( h \) also has a large centraliser.

2. The case when \( K \) has positive characteristic \( c \) and \( h \in \mathcal{G} \) has a finite order that is a multiple of \( c \) requires further analysis, and we do not pursue it here.

3. Observe that if \( h \) has infinite order, then so does \( g \), and the fact that \( h \) commutes with each \( g^{ok} \) for \( k \in \mathbb{N} \) implies that \( h \) commutes with the
whole one-parameter group (parametrised by $K$ or $\mathbb{Z}_c$, as the case may be) determined by $g$.

4. If $L(h) \neq \mathbb{I}$, then whenever the characteristic does not divide $s$, we have a $g^{1/s} \neq h$, so we get a nontrivial element $h' := h^{s^{-1}}g^{1/s}$ of order $s$. This allows us to factor $h$ in its own centraliser as the product of an element of order $s$ and an element tangent to the identity.

References

[1] J. Elliott, 2006 Binomial rings, integer-valued polynomials, and $\lambda$-rings. *Journal of Pure and Applied Algebra* **207**, 165–185.
[2] P. Hall, 1969 *The Edmonton notes on nilpotent groups*. Queen Mary College Mathematics Notes, London. Mathematics Department, Queen Mary College.
[3] P. Hall, 1988 *Nilpotent groups* (Lectures given at the Canadian Mathematical Congress, Summer Seminar, University of Alberta, 1957), pp. 419–462 in K.W. Gruenberg and J.E. Roseblade (editors), *The collected works of Philip Hall*, Oxford. Oxford University Press.
[4] J. Lubin, 1994 Nonarchimedean dynamical systems. *Compositio Mathematica* **94**, 321–46.
[5] J. Lubin, 2000 Formal flows on the non-Archimedean open unit disk. *Compositio Mathematica* **124**, 123–36.
[6] A. O’Farrell and I. Short, 2015 *Reversibility in dynamics and group theory*. LMS Lecture Notes **416**, Cambridge. Cambridge University Press.
[7] A. O’Farrell and D. Zaitsev, 2014 Formally-reversible maps of $(\mathbb{C}^2, 0)$. *Annali della Scuola Normale Superiore di Pisa, Classe di Scienze* **13**, 371–97.
[8] Wikipedia, 2021 *Integer-valued polynomial*, https://en.wikipedia.org/wiki/Integer-valued_polynomial (accessed 20-3-2022)

Mathematics and Statistics, Maynooth University, Co Kildare, W23 HW31, Ireland

Email address: anthony.ofarrell@mu.ie