2014

ALGEBRAIC PROPERTIES OF FORMAL POWER SERIES COMPOSITION

Thomas S. Brewer
University of Kentucky, tsbrewer84@gmail.com

ALGEBRAIC PROPERTIES OF FORMAL POWER SERIES COMPOSITION

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Thomas Scott Brewer
Lexington, Kentucky

Director: Dr. Edgar Enochs, Professor of Mathematics
Lexington, Kentucky 2014

ABSTRACT OF DISSERTATION

ALGEBRAIC PROPERTIES OF FORMAL POWER SERIES COMPOSITION

The study of formal power series is an area of interest that spans many areas of mathematics. We begin by looking at single-variable formal power series with coefficients from a field. By restricting to those series which are invertible with respect to formal composition we form a group. Our focus on this group focuses on the classification of elements having finite order. The notion of a semi-cyclic group comes up in this context, leading to several interesting results about torsion subgroups of the group. We then expand our focus to the composition of multivariate formal power series, looking at similar questions about classifying elements of finite order. We end by defining a natural automorphism on this group induced by a group action of the symmetric group.

KEYWORDS: formal power series, semi-cyclic groups

Author's signature: Thomas Scott Brewer

Date: December 1, 2014

ALGEBRAIC PROPERTIES OF FORMAL POWER SERIES COMPOSITION

By
Thomas Scott Brewer

Director of Dissertation: Edgar Enochs

Director of Graduate Studies: Peter Perry

Date: December 1, 2014

Dedicated to my wife, Laura, and our children: Ariana, Asher, and Abram.

ACKNOWLEDGMENTS

First, I would like to thank my advisor, Dr. Edgar Enochs, for all of his support during my time at the University of Kentucky. His instruction in the basic algebra sequence provided the foundation for the direction of my research. It would not have been possible to find a more dedicated and knowledgable person to work with. I am greatly indebted for his guidance over the past five years.

I would also like to thank all of the professors who serverd as members of my committee: Dr. Heide Gluesing-Luerssen, Dr. Uwe Nagel, Dr. Paul Eakin, Dr. Cid Srinivasan, and Dr. Connie Wood. Their assistance with this dissertation and is greatly appreciated.

Lastly, I would like to thank all of the professors whose courses I have taken during the last five years. The knowledge gained from their quality instruction was instrumental in building the strong foundation needed to complete this work.

TABLE OF CONTENTS

Acknowledgments iii

Table of Contents iv

Chapter 1 Introduction 1
- 1.1 Motivation 1

Chapter 2 Single-Variable Formal Power Series 3
- 2.1 Preliminaries 3
- 2.2 Composition of Formal Power Series 4
- 2.3 The Group of Invertible Formal Power Series With Respect to Composition 8
- 2.4 Conjugates of Formal Power Series 9
- 2.5 Classifying Series of Finite Order 11

Chapter 3 Semi-Cyclic Groups and an Application to Formal Power Series 15
- 3.1 An Introduction to Semi-Cyclic Groups 15
- 3.2 Preliminaries 15
- 3.3 Proof of Theorem 3.1.1 17
- 3.4 Properties of Semi-cyclic Groups 19
- 3.5 An Application with Formal Power Series 22

Chapter 4 Multivariate Formal Power Series 26
- 4.1 The Group of Invertible Multivariate Series With Respect to Composition 26
- 4.2 Elements Having Finite Order 30
- 4.3 Conjugation of Multivariate Series 32
- 4.4 Classifying Multivariate Series of Finite Order 35

Chapter 5 Group Actions and A Natural Automorphism of I 40
- 5.1 Group Actions of the Symmetric Group on I 40
- 5.2 A Natural Automorphism of I 43
- 5.3 Elements of $F[[x_1, x_2, \dots, x_n]]^n$ Fixed by All Elements of Σ_n 46

Bibliography 49

Vita 50

Chapter 1 Introduction

1.1 Motivation

The study of formal power series is an area of interest that spans many areas of mathematics, for example analysis [2], combinatorics [14], commutative algebra [1], and dynamical systems [9]. This work focuses primarily on the algebraic properties of the ring of formal power series with coefficients from a field. Specifically, we will be looking at various results that arise with respect to formal composition of power series. Related work can be found in [7], [3], [5], [8], [11], and [12]

My interest in this topic can be traced back to a topics course on the subject taught by Edgar Enochs in the spring semester of 2013. The question of which formal power series with integer coefficients produced the single term x when composed with themselves was posed as an extra credit question. After looking at this question, we began looking at which series in $\mathbb{C}[[x]]$ gave x when composed with themselves any finite number of times, and eventually moved on to series with coefficients from an arbitrary field.

We begin this work by looking at single-variable formal power series with coefficients from a field. Elements of $F[[x]]$ that are invertible with respect to formal composition form a group with respect to this operation. We will build toward a classification of elements of finite order. Elements of order 2 were classified Edward Kasner [7] and another classification can be found here [12]. We build on both of these works to offer a new perspective on the topic.

From there we will introduce the concept of a semi-cyclic group, and use this notion to show that torsion subgroups of invertible formal power series of this group are semi-cyclic groups. Furthermore, this result is used to show that torsion subgroups of the same "size" must be conjugate to one another.

Composition of formal power series can also be generalized to multivariate formal power series. In order to have a well-defined generalization of formal composition of formal power series with n variables, we need to consider n-tuples of such objects. Looking at n-tuples of formal power series with n variables, we can define a group with respect to composition in a fashion similar to that which was done with single variable formal power series. Here the question of how to classify series of finite order with respect to composition becomes much more difficult. So, we will impose some restrictions on the degree-one terms of these series in order to arrive at some similar results to those found for single-variable formal power series.

From there we move to defining several group actions of the symmetric group of n objects on the set of n-tuples of formal power series over n variables. One of these group actions in particular, offers a very natural group automorphism on the group of invertible n-tuples of formal power series. Finally, we will end by looking at which n-tuples are fixed by this automorphism.

Chapter 2 Single-Variable Formal Power Series

2.1 Preliminaries

We begin by looking at the ring of formal power series over an arbitrary ring R. For more information on this ring, see [2], [10], and [14]. Given a ring R and an indeterminant x, we consider the set of formal symbols

$$a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n$$

Definition 2.1.1. *We define the sum of $S(x)$ and $T(x)$ to be*

$$\left(\sum_{n=0}^{\infty} s_n x^n\right) + \left(\sum_{n=0}^{\infty} t_n x^n\right) = \sum_{n=0}^{\infty} a_n x^n$$

where

$$a_n = s_n + t_n$$

Definition 2.1.2. *We define the product of $S(x)$ by a scalar λ to be*

$$\lambda \left(\sum_{n=0}^{\infty} s_n x^n\right) = \sum_{n=0}^{\infty} \lambda s_n x^n$$

Definition 2.1.3. *We define the product of $S(x)$ and $T(x)$ to be*

$$\left(\sum_{n=0}^{\infty} s_n x^n\right) \cdot \left(\sum_{m=0}^{\infty} t_m x^m\right) = \sum_{k=0}^{\infty} a_k x^k$$

where

$$a_k = \sum_{n+m=k} s_n t_m$$

If R is a field, then with the above definitions **2.1.1** and **2.1.2**, $R[[x]]$ forms a vector space over R. Multiplication defined in **2.1.3** is associative, so we also have that $R[[x]]$ is a ring. If R is a commutative ring, then so is $R[[x]]$.

One important concept that we will make use of involves the ideal of $R[[x]]$ generated by the series consisting of a single term of the form x^n for some natural number n. We will denote this ideal (x^n). We want to look at elements of $R[[x]]$ modulo this ideal. Let $a_0 + a_1 x + a_2 x^2 + \dots$ be any element of $R[[x]]$. We note that

$$a_0 + a_1 x + a_2 x^2 + \cdots \equiv a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \bmod (x^n)$$

In other words, looking at elements modulo (x^n) allows us to focus only on the terms having degrees $n-1$ and smaller. It is in regard to this notion that we have the following theorem.

Theorem 2.1.4. *Given $S(x) = \sum_{k=0}^{\infty} s_k x^k$ and $T(x) = \sum_{k=0}^{\infty} t_k x^k$ in $R[[x]]$ for some ring R, we have $S(x) = T(x)$ if and only if $S(x) \equiv T(x)$ modulo (x^n) for each $n \geq 0$.*

Proof. If $S(x) = T(x)$, it is trivial that we get congruence modulo (x^n) for each $n \geq 0$. So let us assume that we have $S(x) \equiv T(x)$ modulo (x^n) for each $n \geq 0$. We want to show that, in fact, $S(x) = T(x)$. $S(x) \equiv T(x)$ modulo (x^n) means that $S(x) - T(x) \in (x^n)$. However, this gives that

$$s_0 - t_0 = s_1 - t_1 = \cdots = s_{n-1} - t_{n-1} = 0$$

In other words, $s_i = t_i$ for $i = 1, 2, \ldots, n-1$. Furthermore, if this is true for each natural number n, this gives us that $S(x) = T(x)$. □

The following definition will also prove useful.

Definition 2.1.5. *Given $S(x) = \sum_{k=0}^{\infty} s_k x^k$ in $R[[x]]$, we define the order of $S(x)$ to be the least $n \geq 0$ such that $s_n \neq 0$. If there is no such n, that is if $S(x) = 0$, we define the order to be the symbol ∞.*

We will denote the order of $S(x) \in R[[x]]$ by $\omega(S(x))$ or simply $\omega(S)$.

2.2 Composition of Formal Power Series

Here, for convenience, we suppose R is commutative. We now wish to define the operation of formal composition on the ring $R[[x]]$. We do so as follows:

Definition 2.2.1. *Let $S(x) = \sum_{k=0}^{\infty} s_k x^k$ and $T(x) = \sum_{k=1}^{\infty} t_k x^k$ be elements of $R[[x]]$ with $\omega(T) > 0$. We denote $S(x)$*

$$S(x) = s_0 + s_1 x + s_2 x^2 + \ldots$$

and we similarly denote $T(x)$

$$T(x) = t_1 x + t_2 x^2 + \ldots$$

We define the composition of $S(x)$ composed with $T(x)$, denoted $S \circ T$, to be the formal power series $U(x)$ in $R[[x]]$ such that

$$\begin{aligned} U(x) &= S \circ T \\ &= S(T(x)) \\ &= s_1(T(x)) + s_2(T(x))^2 + \ldots \\ &= s_1(t_1 x + t_2 x^2 + \ldots) + s_2(t_1 x + t_2 x^2 + \ldots)^2 + \ldots \\ &= \textstyle\sum_{n=1}^{\infty} a_n x^n \end{aligned}$$

where

$$a_n = \sum_{k \in \mathbb{N},\ j_1 + \cdots + j_k = n} s_k t_{j_1} t_{j_2} \ldots t_{j_k}$$

Note that if we tried the above procedure with $T(x)$ such that $\omega(T) = 0$, we would have

$$S \circ T = \sum_{k=0}^{\infty} s_k(t_0 + \dots)^k = s_1(t_0 + \dots) + s_2(t_0 + \dots)^2 + \dots$$

In other words,

$$S \circ T \equiv s_1 t_0 + s_2 t_0^2 + s_3 t_0^3 + \dots \text{ modulo } (x)$$

We can see that with many choices of t_0, this value would be undefined. It is for this reason that we restrict to only those elements with order greater than or equal to 1 when we look at composition.

Notice the following properties of composition of formal series.

Proposition 2.2.2. *For S_1, S_2, and T in $R[[x]]$, with $\omega(T) > 0$, we have that*

1. $(S_1 + S_2) \circ T = (S_1 \circ T) + (S_2 \circ T)$
2. $(S_1 \cdot S_2) \circ T = (S_1 \circ T) \cdot (S_2 \circ T)$

Proof. Both of these results follow from the definitions above. Let $S_1(x) = \sum_{n=0}^{\infty} a_n x^n$, $T(x) = \sum_{n=0}^{\infty} b_n x^n$, and $T(x) = \sum_{n=1}^{\infty} t_n x^n$ be elements of $R[[x]]$. Then we have that

$$S_1 + S_2 = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

Thus,

$$(S_1 + S_2) \circ T = \sum_{n=0}^{\infty} c_n x^n$$

where $c_n = \sum_{k \in \mathbb{N}, j_1 + \dots + j_k = n} (a_k + b_k) t_{j_1} t_{j_2} \dots t_{j_k}$

On the other hand,

$$S_1 \circ T = \sum_{n=0}^{\infty} d_n x^n \text{ where } d_n = \sum_{k \in \mathbb{N}, j_1 + \dots + j_k = n} a_k t_{j_1} t_{j_2} \dots t_{j_k}$$

and

$$S_2 \circ T = \sum_{n=0}^{\infty} e_n x^n \text{ where } e_n = \sum_{k \in \mathbb{N}, j_1 + \dots + j_k = n} b_k t_{j_1} t_{j_2} \dots t_{j_k}$$

Notice that $c_n = d_n + e_n$. Hence, $(S_1 \circ T) + (S_2 \circ T)$ is also equal to $\sum_{n=0}^{\infty} c_n x^n$.

For the second part, notice that

$$S_1 \cdot S_2 = \sum_{n=0}^{\infty} c_n x^n \text{ where } c_n = \sum_{n_1 + n_2 = n} a_{n_1} b_{n_2}$$

Thus,

$$(S_1 S_2) \circ T = \sum_{n=0}^{\infty} d_n x^n \text{ where } d_n = \sum_{k \in \mathbb{N},\ j_1 + \dots + j_k = n} \left(\sum_{k_1 + k_2 = k} a_{k_1} b_{k_2} \right) t_{j_1} t_{j_2} \dots t_{j_k}$$

On the other hand

$$S_1 \circ T = \sum_{n=0}^{\infty} d_n x^n \text{ where } d_n = \sum_{k\in\mathbb{N},\ j_1+\cdots+j_k=n} a_k t_{j_1} t_{j_2} \dots t_{j_k}$$

Likewise,

$$S_2 \circ T = \sum_{n=0}^{\infty} e_n x^n \text{ where } e_n = \sum_{k\in\mathbb{N},\ j_1+\cdots+j_k=n} b_k t_{j_1} t_{j_2} \dots t_{j_k}$$

So when we take the product of $S_1 \circ T$ and $S_2 \circ T$, we get

$$\sum_{n=0}^{\infty} f_n x^n \text{ where } f_n = \sum_{n_1+n_2=n} \left(\sum_{k\in\mathbb{N},\ j_1+\cdots+j_k=n_1} a_k t_{j_1} t_{j_2} \dots t_{j_k} \right) \left(\sum_{k\in\mathbb{N},\ j_1+\cdots+j_k=n_2} b_k t_{j_1} t_{j_2} \dots t_{j_k} \right)$$

However, this is the same as

$$\sum_{k\in\mathbb{N},\ j_1+\cdots+j_k=n} \left(\sum_{k_1+k_2=k} a_{k_1} b_{k_2} \right) t_{j_1} t_{j_2} \dots t_{j_k}$$

Thus, $(S_1 \cdot S_2) \circ T = (S_1 \circ T) \cdot (S_2 \circ T)$ □

Proposition 2.2.3. *For a given $T(x) \in R[[x]]$ with $\omega(T) > 0$, the map $\phi : R[[x]] \to R[[x]]$ which sends $S(x) \mapsto S \circ T$ is a homomorphism.*

Proof. This follows from Proposition **2.2.2** □

Proposition 2.2.4. *The single-term element $x \in R[[x]]$ is an identity element with respect to composition.*

Proof. This result is trivial. For any $S(x) = s_0 + s_1 x + s_2 x^2 + \dots$, we clearly see that

$$x \circ (s_0 + s_1 x + s_2 x^2 + \dots) = (s_0 + s_1 x + s_2 x^2 + \dots) \circ x = s_0 + s_1 x + s_2 x^2 + \dots$$

□

Proposition 2.2.5. *Let $S(x) = \sum_{k=0}^{\infty} s_k x^k$, $T(x) = \sum_{k=1}^{\infty} t_k x^k$, and $U(x) = \sum_{k=1}^{\infty} u_k x^k$ be elements of $R[[x]]$ such that $\omega(T(x))$ and $\omega(U(x))$ are greater than zero. Then,*

$$(S \circ T) \circ U = S \circ (T \circ U)$$

In other words, composition of elements of $R[[x]]$ is associative.

Proof. Since $\omega(T(x)) > 0$ and $\omega(U(x)) > 0$ both sides of this equation are defined. First suppose $S(x) = sx^k$ is a monomial. Then $(S \circ T) \circ U = (s(T(x))^k) \circ U = s(T \circ U)^k$ by Proposition **2.2.2**. If S is not a monomial, then we think of S as an (infinite) sum of its monomials. So $S \circ T = \sum_{n=0}^{\infty} s_n (T(x))^n$. It follows that

$$(S \circ T) \circ U = \left(\sum_{n=0}^{\infty} s_n (T(x))^n \right) \circ U = \sum_{n=0}^{\infty} s_n (T \circ U)^n = S \circ (T \circ U)$$

□

Proposition 2.2.6. *Given a commutative ring R, let $S(x) = s_1x + s_2x^2 + \cdots \in R[[x]]$, then $S(x)$ has an inverse $T(x) = t_1x + t_2x^2 + \dots$ in $R[[x]]$ with respect to composition if and only if s_1 is a unit in R.*

Proof. Suppose that $T(x)$ is such an inverse of $S(x)$. Then we have that $S \circ T = x$. Note that

$$S \circ T \equiv s_1t_1x \text{ modulo } (x^2)$$

So we have that $s_1t_1 = 1$. Thus, it follows that s_1 (as well as t_1) is a unit in R.

On the other hand suppose $S(x) = s_1x + s_2x^2 + \cdots \in R[[x]]$ is such that $s_1 \in R$ is a unit. We want to identify coefficients $t_1, t_2, \dots$ such that $T(x) = t_1x + t_2x^2 + \dots$ is an inverse of $S(x)$. We do this inductively by looking at the coefficients of $S \circ T$ for each term.

Note that we have already said that the coefficient of x in $S \circ T$ is s_1t_1. Since we want this to be 1, we let

$$t_1 = s_1^{-1}$$

The coefficient of x^2 is $s_1t_2 + s_2t_1^2$. Since we want this coefficient to be zero, we let

$$t_2 = s_1^{-1}(-s_2t_1^2)$$

We continue in this fashion. Note that for the general case, for some natural number k, the coefficient of x^k will be given by

$$s_1t_k + C(k)$$

where $C(k) \in R$ is a value given by an expression involving only coefficients $t_1, t_2, \dots t_{k-1}$ and coefficients of $S(x)$ itself. if we assume we have already defined coefficients $t_1, t_2, \dots t_{k-1}$, then we just let

$$t_k = s_1^{-1}C(k)$$

in this fashion we define a value for each t_i to arrive at a series $T(x) = t_1x + t_2x^2 + \dots$ for which $S \circ T = x$.

Since t_1 is also a unit in R, this same argument gives us that there exists a series $U(x) \in R[[x]]$ such that $T \circ U = x$. However, we easily see that $U(x) = S(x)$, since

$$S = S \circ x = S \circ T \circ U = x \circ U = U$$

Therefore, we have that $S \circ T = T \circ S = x$.

□

Now we define the subset $I \subset R[[x]]$ to be the set of all $S(x) = s_1x + s_2x^2 + \cdots \in R[[x]]$ such that $\omega(S) = 1$ and s_1 is a unit in R.

Theorem 2.2.7. *The subset $I \subset R[[x]]$ along with the operation of composition forms a group.*

Proof. This follows from the previous three propositions. □

2.3 The Group of Invertible Formal Power Series With Respect to Composition

From now on, we will be looking at the formal power series with coefficients from a field F with characteristic p. Note that p can be either a prime or zero. Also note that all $a \in F$ such that $a \neq 0$ are units. So the group $I \subset F[[x]]$ in this context can be defined to be the set of all $S(x) \in F[[x]]$ such that $\omega(S) = 1$. In this section, it is our goal to determine which elements of I have finite order. The final two theorems of this chapter, Theorem **2.5.1** and Theorem **2.5.4**, will give us two ways of classifying such elements. The first of these results, Theorem **2.5.1**, is known [12]. The second, Theorem **2.5.4**, is closely related but examines the idea of classifying elements of finite order in I in a new way.

At this time we also should clarify a bit of notation. Since we will be composing elements $S(x) \in F[[x]]$ with themselves multiple times, we denote this the following way: For a natural number k, The composition of k copies of $S(x)$ is denoted $(S(x))^{(k)}$ or simply $S^{(k)}$. Along with this, the inverse for a formal power series $S(x) \in F[[x]]$ with respect to composition will be denoted $(S(x))^{(-1)}$ or simply $S^{(-1)}$. We reserve the notation S^k to refer to the usual notion of k copies of $S(x)$ multiplied together.

Now let $S(x) = \epsilon x + s_2x^2 + s_3x^3 + \cdots \in F[[x]]$ be such that $S^{(n)} = x$. We begin by making the following observations:

Proposition 2.3.1. *For $S(x)$ as above, $\epsilon \in F$ is such that $\epsilon^n = 1$.*

Proof. We consider $S^{(n)}$ modulo x^2. Note that

$$\begin{aligned} S^{(n)} &= S(x) \circ S(x) \circ \cdots \circ S(x) \\ &\equiv (\epsilon x) \circ (\epsilon x) \circ \cdots \circ (\epsilon x) (\text{ mod } x^2) \\ &= \epsilon^n x \end{aligned}$$

So we see that if $S^{(n)} = x$, that it must be that $\epsilon^n = 1$. □

Proposition 2.3.2. *If p does not divide n, then $\epsilon = 1$ implies $S(x) = x$.*

Proof. Suppose $S(x) = x + s_2x^2 + s_3x^3 + \ldots$ and $S^{(n)} = x$. Then it must be that $S(x)^{(n)} \equiv x$ (mod x^m) for all $m \in \mathbb{N}$.

Consider $S^{(n)}$ modulo x^3. We see that

$$S^{(n)} = (x + s_2x^2) \circ (x + s_2x^2) \circ \cdots \circ (x + s_2x^2) = x + ns_2x^2$$

Since we assume $S^{(n)} = x$, we must have that $ns_2 = 0$, i.e., $s_2 = 0$.

Now suppose that we have $s_2 = s_3 = \cdots = s_{k-1} = 0$, and consider $S^{(n)}$ modulo x^{k+1}. We have that

$$S^{(n)} = (x + s_kx^k) \circ (x + s_kx^k) \circ \cdots \circ (x + s_kx^k) = x + ns_kx^k$$

Thus, it must be that $s_k = 0$.

By induction, we have that $s_k = 0$ for all k. Hence, $S(x) = x$.

□

So from here on, we address the case that ϵ is a primitive nth root of unity (or ϵ has order n in the multiplicative group F^*), and S is a nth root of x for $n \geq 2$. Consider the following proposition:

Proposition 2.3.3. *If p does not divide n, and $S^{(n)} = x$ where $S(x)$ is of the form $S(x) = \epsilon x + ax^{kn+1} + \ldots$, for some integer k, then $a = 0$.*

Proof. We consider $S^{(n)}$ modulo x^{kn+2}. So we have

$$\begin{aligned} S^{(n)} &= S(x) \circ S(x) \circ \cdots \circ S(x) \\ &\equiv (\epsilon x + ax^{kn+1}) \circ (\epsilon x + ax^{kn+1}) \circ \cdots \circ (\epsilon x + ax^{kn+1}) (\bmod x^{kn+2}) \\ &= \epsilon^n x + n\epsilon^{n-1} a x^{kn+1} \\ &= x + n\epsilon^{n-1} a x^{kn+1} \end{aligned}$$

Now since we assume $S^{(n)} = x$, it must be that $n\epsilon^{n-1}a = 0$. Hence, we have that $a = 0$. □

2.4 Conjugates of Formal Power Series

We now turn our attention to taking conjugates in $F[[x]]$ under composition. Consider the following:

Proposition 2.4.1. *If $S \in F[[x]]$ such that $S^{(n)} = x$, then for any conjugate $R = T^{(-1)} \circ S \circ T$, $R^{(n)} = x$.*

Proof. Note that if $R = T^{(-1)} \circ S \circ T$ for some $T \in F[[x]]$ and $S^{(n)} = x$, we have that

$$\begin{aligned} R^{(n)} &= (T^{(-1)} \circ S \circ T)^{(n)} \\ &= (T^{(-1)} \circ S \circ T) \circ (T^{(-1)} \circ S \circ T) \circ \cdots \circ (T^{(-1)} \circ S \circ T) \\ &= T^{(-1)} \circ S \circ (T \circ T^{(-1)}) \circ S \circ (T \circ T^{(-1)}) \circ \cdots \circ (T \circ T^{(-1)}) \circ S \circ T \\ &= T^{(-1)} \circ S^{(n)} \circ T \\ &= T^{(-1)} \circ x \circ T \\ &= T^{(-1)} \circ T \\ &= x \end{aligned}$$

So we clearly see that if R is conjugate to S, then $R^{(n)} = x$. □

Proposition 2.4.2. *If $T \in F[[x]]$ is of the form $T(x) = x + b_m x^m + \ldots$, where $m \geq 2$, then $T^{(-1)}$ is of the form $T^{(-1)}(x) = x - b_m x^m + \ldots$.*

Proof. Suppose $T^{(-1)}(x) = c_1 x + c_2 x^2 + \ldots$. Then for $k \leq m$, since $T \equiv x (\bmod x^k)$, we have that

$$T^{(-1)} \circ T \equiv T^{(-1)} (\bmod x^k)$$

Hence, we see that $c_1 = 1$ and $c_2 = c_3 = \cdots = c_{m-1} = 0$.

Furthermore, if we consider $T^{(-1)} \circ T$ modulo x^{m+1}, we see that

$$\begin{aligned} T^{(-1)} \circ T &\equiv x + c_m x^m \circ x + b_m x^m (\bmod x^{m+1}) \\ &= x + b_m x^m + c_m x^m \end{aligned}$$

Since we know $T^{(-1)} \circ T = x$, it must be that $c_m = -b_m$.

□

Proposition 2.4.3. *If $S(x) = \epsilon x + a_2 x^2 + a_3 x^3 + \dots$ and $T(x) = x + b_m x^m$, then $T^{(-1)} \circ S \circ T$ is of the form*

$$T^{(-1)} \circ S \circ T = \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + c x^m + \dots$$

for $c = a_m + b_m \epsilon (1 - \epsilon^{m-1})$.

Proof. By the Proposition **2.4.2**, we know that $T^{(-1)}(x) = x - b_m x^m + \dots$. Now note that any polynomial of the form $(x + b_m x^m)^k$ will only have one term of degree less than $m+1$, namely, x^k. In other words, $(x + b_m x^m)^k \equiv x^k \pmod{x^{m+1}}$. So we have

$$\begin{aligned} T^{(-1)} \circ S \circ T &\equiv x - b_m x^m \circ \epsilon x + a_2 x^2 + \dots \circ x + b_m x^m (\bmod x^{m+1}) \\ &\equiv x - b_m x^m \circ \epsilon (x + b_m x^m) + a_2 (x + b_m x^m)^2 + \dots + a_m (x + b_m x^m)^m (\bmod x^{m+1}) \\ &\equiv x - b_m x^m \circ \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + (a_m + \epsilon b_m) x^m (\bmod x^{m+1}) \\ &\equiv \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + (a_m + \epsilon b_m) x^m - b_m \epsilon^m x^m (\bmod x^{m+1}) \\ &\equiv \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + (a_m + \epsilon b_m - b_m \epsilon^m) x^m (\bmod x^{m+1}) \\ &\equiv \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + c x^m (\bmod x^{m+1}), \end{aligned}$$

where $c = (a_m + b_m \epsilon - b_m \epsilon^m)$. □

This proposition also leads to the following corollaries:

Corollary 2.4.4. *If $m-1$ does not divide n, then given any $c \in F$, we can choose b_m such that*

$$T^{(-1)} \circ S \circ T = \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + c x^m + \dots$$

for $S(x) = \epsilon x + a_2 x^2 + a_3 x^3 + \dots$ and $T(x) = x + b_m x^m$.

Proof. From the previous proposition, we see that we can choose

$$b_m = \frac{c - a_m}{\epsilon (1 - \epsilon^{m-1})}$$

to get any desired value for c, as long as $\epsilon^{m-1} \neq 1$. □

Specifically, we may choose b_m so that $c = 0$, i.e.,

$$T^{(-1)} \circ S \circ T = \epsilon x + a_2 x^2 + \dots + a_{m-1} x^{m-1} + 0 x^m + \dots$$

Corollary 2.4.5. *If $S(x) = \epsilon x + a_2x^2 + a_3x^3 + \dots$ where $\epsilon, a_2, a_3, \dots, a_{m-1}$ are given and we allow a_m to vary, and $T(x) = x + b_mx^m$ is given, then the map which sends $a_m \mapsto c$ (c as above)is a bijection.*

Proof. From the previous proposition, we see that for any particular a_m,

$$T^{(-1)} \circ S \circ T = \epsilon x + a_2x^2 + \dots + a_{m-1}x^{m-1} + cx^m + \dots$$

where $c = (a_m + b_m\epsilon - b_m\epsilon^m)$. So $a_m \mapsto c$ is injective.

On the other hand, if we want a given value $c \in F$, we need only let $a_m = c - b_m\epsilon(1 - \epsilon^{m-1})$ to have $a_m \mapsto c$. So this map is also surjective.

□

2.5 Classifying Series of Finite Order

We now come to our main results of the chapter. Again we recall that first of these results is known [12]. However our proof is new and can be used in later work with multivariate formal power series. A proof is nonetheless worth including here as later work with multivariate formal power series will use similar ideas. Also, techniques used up to this point and further used in the proof, assist in our general understanding of the subject matter and, specifically, in proving Theorem **2.5.4** below.

Theorem 2.5.1. *For F a field of characteristic $p \nmid n$, $\epsilon \in F$ such that $|\epsilon| = n$ and $S(x) = \epsilon x + \sum_{i=2}^{\infty} a_ix^i \in F[[x]]$, we have that $S^{(n)} = x$ if and only if S is conjugate to ϵx.*

Proof. Note ϵx is clearly a nth root of x, since we are assuming $|\epsilon| = n$. So if $T^{(-1)} \circ S \circ T = \epsilon x$ for some $T \in F[[x]]$, it follows from Proposition **2.4.1** that $S^{(n)} = x$.

On the other hand, suppose $S^{(n)} = x$. We can use our previous observations to show that S is conjugate to ϵx. By Corollary **2.4.4**, we can choose a b_2 such that if $T_2(x) = x + b_2x^2$, we have that

$$S_2 = T_2^{(-1)} \circ S \circ T_2 = \epsilon x + a'_3x^3 + \dots$$

If $n \neq 2$, then we continue by choosing a b_3 such that if $T_3(x) = x + b_3x^3$, we have

$$S_3 = T_3^{(-1)} \circ S_2 \circ T_3 = \epsilon x + a'_4x^4 + \dots$$

Now we can continue in this fashion until we have

$$S_n = T_n^{(-1)} \circ S_{n-1} \circ T_n = \epsilon x + a'_{n+1}x^{n+1} + \dots$$

However, by construction we have that S_n is a conjugate of S, and we assume that $S^{(n)} = x$. It follows that $S_n^{(n)} = x$. Furthermore, we see that $S_n = \epsilon x + a'_{n+1}x^{n+1} + \dots$, so by Proposition **2.3.3**, we know that it must be that $a_{n+1} = 0$. So we let $S_{n+1} = S_n = \epsilon x + a'_{n+2}x^{n+2} + \dots$, and we can proceed as above by choosing $T_{n+2} = x + b_{n+2}x^{n+2}$, $T_{n+3} = x + b_{n+3}x^{n+3}$, $\ldots$, $T_{2n} = x + b_{2n}x^{2n}$. Then we have

$$S_{2n} = T_{2n}^{(-1)} \circ S_{2n-1} \circ T_{2n} = \epsilon x + a'_{2n+1}x^{2n+1} + \ldots$$

Again by Proposition **2.3.3**, it must be that $a_{2n+1} = 0$. We proceed in this fashion.

So we claim that

$$\ldots T_{2n}^{(-1)} \circ \cdots \circ T_{n+2}^{(-1)} \circ T_n^{(-1)} \circ \cdots \circ T_2^{(-1)} \circ S \circ T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \cdots = \epsilon x$$

We must now turn our attention to showing that $T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \ldots$ and $\ldots T_{2n}^{(-1)} \circ \cdots \circ T_{n+2}^{(-1)} \circ T_n^{(-1)} \circ \cdots \circ T_2^{(-1)}$ are well-defined. So we consider $T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \ldots$ modulo x^m for all $m \in \mathbb{N}$.

Now for any $k \in \mathbb{N}$, note that $T_k = x + b_kx^k \equiv x \pmod{x^m}$, for $k \geq m$. Hence, modulo x^m, we have that the infinite composition $T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \ldots$ is equivalent to the finite composition $T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \ldots T_k$, where k is the largest subscript in our infinite composition that is less than or equal to m. Since this finite composition is well-defined for each value of m, we have that $T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \ldots$ is well-defined.

Similarly, it follows that $\ldots T_{2n}^{(-1)} \circ \cdots \circ T_{n+2}^{(-1)} \circ T_n^{(-1)} \circ \cdots \circ T_2^{(-1)}$ is well-defined.

However, this gives us that

$$\ldots T_{2n}^{(-1)} \circ \cdots \circ T_{n+2}^{(-1)} \circ T_n^{(-1)} \circ \cdots \circ T_2^{(-1)} \circ S \circ T_2 \circ \cdots \circ T_n \circ T_{n+2} \circ \cdots \circ T_{2n} \circ \cdots = \epsilon x$$

□

Here it is worth revisiting some of the first results from section 2.4, namely Proposition **2.3.1** and Proposition **2.3.2**. These results were provided earlier because they are fairly clear an give some early insight into the topic. However, neither are needed to prove the previous theorem, and both follow nicely as corollaries of this theorem. So even though they were presented earlier, we list them again here to emphasize their relation to the previous result.

Corollary 2.5.2. *If $S(x) = \epsilon x + \ldots$ has order n in I, then ϵ has order n in the multiplicative group F^*.*

Proof. This result is actually stronger than Proposition **2.3.1** and follows immediately from the previous theorem. We know that S has finite order if and only if S is conjugate to ϵx. Clearly S and ϵx have the same order, and clearly ϵx has the same order as does ϵ as an element of F^*. □

Corollary 2.5.3. ***(Proposition 2.3.2)****let $S(x) = \epsilon x + \cdots \in I$ be such that $S^{(n)} = x$. If p does not divide n, then $\epsilon = 1$ implies $S(x) = x$.*

Proof. If $S^{(n)} = x$, then S is conjugate to ϵx and will have the same order as ϵx. So if $\epsilon = 1$, $\epsilon x = x$ has order 1. Thus, S has order 1. Hence, $S(x) = x$. □

Here is another way of thinking about elements of I that have finite order.

Theorem 2.5.4. *Given arbitrary $a_2, a_3, \dots a_n, a_{n+2}, \dots, a_{2n}, a_{2n+2}, \dots$ in F, we can choose unique $a_{n+1}, a_{2n+1}, \dots$ so that $S(x) = \epsilon x + a_2x^2 + \dots$ is an n-th root of x.*

Proof. First, let $a_2, a_3, \dots a_n, a_{n+2}, \dots, a_{2n}, a_{2n+2}, \dots$ in F be given. We want to show that we can chose $a_{n+1}, a_{2n+1}, \dots$ so that $S(x) = \epsilon x + a_2x^2 + \dots$ is an n-th root of x. By Theorem **2.5.1**, it suffices to show that there exist $a_{n+1}, a_{2n+1}, \dots \in F$ so that $S(x) = \epsilon x + a_2x^2 + \dots$ is a conjugate of ϵx.

So we begin with ϵx and proceed in a fashion similar to that found in the proof to Theorem **2.5.1**. By Corollary **2.4.4**, we can find a T_2 and $T_2^{(-1)}$ such that

$$T_2^{(-1)} \circ \epsilon x \circ T_2 = \epsilon x + a_2x^2 + \dots$$

Similarly we can choose $T_3, T_4, \dots, T_n \in F[[x]]$ such that

$$T_n^{(-1)} \circ \dots \circ T_3^{(-1)} \circ T_2^{(-1)} \circ \epsilon x \circ T_2 \circ T_3 \circ \dots \circ T_n = \epsilon x + a_2x^2 + a_3x^3 + \dots a_nx^n + \dots$$

We can then choose $T_{n+2}, T_{n+3}, \dots, T_{2n} \in F[[x]]$ so that we have

$$T_{2n}^{(-1)} \circ \dots \circ T_{n+2}^{(-1)} \circ T_n^{(-1)} \circ \dots \circ T_2^{(-1)} \circ \epsilon x \circ T_2 \circ \dots \circ T_n \circ T_{n+2} \circ \dots \circ T_{2n} = \epsilon x + a_2x^2 + a_3x^3 + \dots a_{2n}x^{2n} + \dots$$

Notice that in the above expression $a_2, a_3, \dots a_n, a_{n+2}, a_{n+3}, \dots, a_{2_n}$ are all our previously chosen values, while a_{n+1} is simply some additional value in F.

We continue in this manner, choosing, $T_{2n+2}, T_{2n+3}, \dots, T_{3_n}, \dots$. Then we define

$$T = T_2 \circ \dots \circ T_n \circ T_{n+2} \circ \dots \circ T_{2n} \circ \dots$$

$$T^{(-1)} = \dots T_{2n}^{(-1)} \circ \dots \circ T_{n+2}^{(-1)} \circ T_n^{(-1)} \circ \dots \circ T_2^{(-1)}$$

Notice that this gives us

$$T^{(-1)} \circ \epsilon x \circ T = S(x) = \epsilon x + a_2x^2 + \dots$$

where $a_2, a_3, \dots a_n, a_{n+2}, \dots, a_{2n}, a_{2n+2}, \dots$ are our previously chosen values, and $a_{n+1}, a_{2n+1}, \dots$ are some other values in F. Now since this $S(x)$ is a conjugate of ϵx, we know that $S(x)^{(n)} = x$ by Proposition **2.4.1**. So, we have found a series with our given values $a_2, a_3, \dots a_n, a_{n+2}, \dots, a_{2n}, a_{2n+2}, \dots$ that is an nth root of x in $F[[x]]$.

Now it remains to show that these values of $a_{n+1}, a_{2n+1}, \dots$ are unique. So in addition to $S(x)$ as above, let us define $S'(x) = \epsilon x + a'_2x^2 + a'_3x^3 + \dots$. Suppose that the for all coefficients a_m and a'_m where m is not of the form $kn + 1$, we have that $a_m = a'_m$, i.e., all coefficients of S' are the same as the corresponding coefficients of S except possibly for $a'_{n+1}, a'_{2n+1}, \dots$. Further, suppose that both are nth roots of x, i.e., $S^{(n)} = S'^{(n)} = x$.

Then by Theorem **2.5.1**, we know that S is a conjugate of ϵx. So there are $T, T^{(-1)} \in F[[x]]$ such that $T^{(-1)} \circ S \circ T = \epsilon x$. So we also consider $T^{(-1)} \circ S' \circ T$. Now for $k \leq n$, $S \equiv S' \pmod{x^k}$. So it follows that

$$T^{(-1)} \circ S' \circ T \equiv \epsilon x + \overline{a_{n+1}}\ x^{n+1} \mod x^{n+2}$$

for some $\overline{a_{n+1}} \in F$. However, the fact that $S'^{(n)} = x$ implies $(\epsilon x + \overline{a_{n+1}}\ x^{n+1})^{(n)} \equiv x \pmod{x^{n+2}}$ by Proposition **2.4.1**. This further implies, by Proposition **2.3.3**, that $\overline{a_{n+1}} = 0$. However, by the bijective correspondence seen in Corollary 8, this implies that $a_{n+1} = a'_{n+1}$.

A similar argument gives us that $a_{2n+1} = a'_{2n+1}, a_{3n+1} = a'_{3n+1}, \ldots$. Thus, we see that the choice of coefficients $a_{n+1}, a_{2n+1}, \ldots$ is unique.

□

We conclude this chapter by noting that Theorem **2.5.4** gives a new description of the conjugate class of ϵx in I. If F is the Galois field of order $p > 0$ (p a prime), i.e. $F = GF(p)$, then Klopsch [8] in his thesis described the conjugacy classes of elements of order p in the corresponding group I. There seems to be little known about the conjugacy classes for elements of order p^k ($k \geq 2$) and even whether there exist elements of these orders. We note that the group I in this situation is usually called the Nottingham group.

Chapter 3 Semi-Cyclic Groups and an Application to Formal Power Series

3.1 An Introduction to Semi-Cyclic Groups

In this Chapter we will build toward a result concerning torsion subgroups of I. Specifically, we want to show that any two torsion subgroups of I of the same size are, in fact, conjugate to one another. In order to arrive at this result involving torsion subgroups, we first discuss what we call semi-cyclic groups, and prove the theorem below:

Theorem 3.1.1. *If G is an abelian group, then the following are equivalent:*

1. *$G = \cup_{n=1}^{\infty}(a_n)$, where $(a_1) \subset (a_2) \subset \ldots$ are finite cyclic groups*
2. *Every finitely generated subgroup of G is cyclic of finite order.*
3. *All the elements of G have finite order and for $a, b \in G$, $|(a,b)| = lcm(|a|,|b|)$*
4. *All elements of G are of finite order and for $a, b \in G$, $(b) \subset (a)$ if and only if $|b|$ divides $|a|$.*
5. *All the elements of G have finite order and for $a, b \in G$, $|(a) \cap (b)| = gcd(|a|,|b|)$*
6. *G is the weak direct product of a family of subgroups indexed by the primes p where for each p the factor indexed by p is isomorphic to $\mathbb{Z}/(p^n)$, for $n \geq 0$, or to $\mathbb{Z}(p^\infty)$*

Definition 3.1.2. *Groups that satisfy the conditions of Theorem **3.1.1** we will refer to as semi-cyclic groups.*

As we will see below, it turns out that torsion subgroups of the group I are semi-cyclic groups. Using this fact, it is not difficult to show that any two torsion subgroups of I having the same order are conjugate to one another.

3.2 Preliminaries

In order to accomplish our goal, we must first introduce a few preliminary ideas. First, the following:

Recall that $\mathbb{Z}(p^\infty)$ is the subgroup of $\mathbb{Q}/\mathbb{Z}$ generated by the elements $1/p^n + \mathbb{Z}$, $n \geq 0$. So $\mathbb{Z}(p^\infty)$ is the union of the cylcic groups

$$(1/p + \mathbb{Z}) \subset (1/p^2 + \mathbb{Z}) \subset \ldots$$

of order $p, p^2, \ldots$

Lemma 3.2.1. *If $a, b \in G$ (an abelian group) where a, b are of finite order, there is an element $c \in (a,b)$ whose order is $lcm(|a|,|b|)$*

Proof. Let $|a| = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ and $|b| = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$ where $p_1, p_2, \dots, p_s$ are distinct primes. Then $|a^{p_2^{k_2} \dots p_s^{k_s}}| = p_1^{k_1}$ and $|b^{p_2^{l_2} \dots p_s^{l_s}}| = p_1^{l_1}$. Proceeding in a similar manner we see that in (a) there are elements of order $p_1^{k_1}, p_2^{k_2}, \dots, p_s^{k_s}$ and in (b) there are elements of order $p_1^{l_1}, p_2^{l_2}, \dots, p_s^{l_s}$.

For each i, $1 \leq i \leq s$ we choose an element c_i in (a) or in (b) (so in (a, b)) which has the largest of the two orders $p_i^{k_i}$ or $p_i^{l_i}$. Then $c = c_1 c_2 \dots c_s$ has order $lcm(|a|, |b|)$

□

Lemma 3.2.2. *Let G be an abelian group, and suppose for all $a, b \in G$, we have that $|(a, b)| = lcm(|a|, |b|)$. Then for $a, b \in G$ such that $|a| = |b|$, we have that $(a) = (b)$.*

Proof. We have that $|(a, b)| = lcm(|a|, |b|) = |a| = |b|$. So since $(a) \subset (a, b)$, we have that $(a) = (a, b)$. Similarly, $(b) = (a, b)$. So $(a) = (b)$.

□

Corollary 3.2.3. *Let G be an abelian group, and suppose for all $a, b \in G$, we have that $|(a, b)| = lcm(|a|, |b|)$. Then, if $|b|$ divides $|a|$, then $(b) \subset (a)$.*

Proof. There is a subgroup of (a), say (a'), such that $|(a')| = |b|$ (since $|b|$ divides $|a|$). Hence $|a'| = |b|$. So by the above lemma, $(b) = (a') \subset (a)$.

□

Now, we let A be any torsion abelian group with operation $+$. To say A is torsion just means that every element of A has finite order. For ever prime p let $A_p \subset A$ consist of the elements of A whose order is a power of prime p. Clearly A_p is a subgroup of A.

Lemma 3.2.4. *The sum $\sum_p A_p$ is a direct sum, and $A = \bigoplus_p A_p$.*

Proof. We first argue that the sum $\sum_p A_p$ is direct, or equivalently that $A_p \cap (\sum_{q \neq p} A_q) = 0$ for all p. So suppose, on the contrary, $x \in A_p \cap (\sum_{q \neq p} A_q)$. Since $x \in A_p$, we have $p^k x = 0$ for some $k \geq 0$. Since $x \in \sum_{q \neq p} A_q$, we have $q_1^{k_1} q_2^{k_2} \dots q_s^{k_s} x = 0$ for primes $q_1, q_2, \dots q_s \neq p$. Since $gcd(p^k, (q_1, q_2, \dots q_s)) = 1$, we see that $x = 0$.

Now since $\bigoplus_p A_p \subset A$, it only remains to show that $A \subset \bigoplus_p A_p$. So let $x \in A$ and let $|x| = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, where $p_1, p_2, \dots, p_s$ are distinct primes and $k_1, k_2, \dots, k_s$ are all nonnegative.

Then $gcd(p_2^{k_2} p_3^{k_3} \dots p_s^{k_s}, p_1^{k_1} p_3^{k_3} \dots p_s^{k_s}, \dots, p_1^{k_1} p_2^{k_2} \dots p_{s-1}^{k_{s-1}}) = 1$. So let

$$1 = l_1 p_2^{k_2} p_3^{k_3} \dots p_s^{k_s} + l_2 p_1^{k_1} p_3^{k_3} \dots p_s^{k_s} + \dots + l_s p_1^{k_1} p_2^{k_2} \dots p_{s-1}^{k_{s-1}}$$

Then we have that

$$x = 1x = l_1 p_2^{k_2} p_3^{k_3} \dots p_s^{k_s} x + l_2 p_1^{k_1} p_3^{k_3} \dots p_s^{k_s} x + \dots + l_s p_1^{k_1} p_2^{k_2} \dots p_{s-1}^{k_{s-1}} x$$

However, note that $p_1^{k_1}(l_1 p_2^{k_2} p_3^{k_3} \dots p_s^{k_s} x) = 0$. So, $l_1 p_2^{k_2} p_3^{k_3} \dots p_s^{k_s} x \in A_{p_1}$. Similarly, we have that $l_2 p_1^{k_1} p_3^{k_3} \dots p_s^{k_s} x \in A_{p_2}$, etc.

So, if we denote

$$\begin{aligned}
x_1 &= l_1 p_2^{k_2} p_3^{k_3} \dots p_s^{k_s} x \\
x_2 &= l_2 p_1^{k_1} p_3^{k_3} \dots p_s^{k_s} x \\
\vdots \\
x_s &= l_s p_1^{k_1} p_2^{k_2} \dots p_{s-1}^{k_{s-1}} x
\end{aligned}$$

we have that

$$x = x_1 + x_2 + \dots + x_2 \in A_{p_1} + A_{p_2} + \dots + A_{p_s} \subset \bigoplus_p A_p$$

□

Corollary 3.2.5. *To give a subgroup $B \subset A$ is equivalent to giving a subgroup of A_p for each p.*

Proof. We note that for such an A and a subgroup $B \subset A$, we have $B_p \subset A_p$. Conversely, if $S_p \subset A_p$ is any subgroup and if $B = \sum S_p$, it is easy to argue that $B_p = S_p$.

□

We also note that if $B, C \subset A$ are subgroups, then $(B \cap C)_p = B_p \cap C_p$ and $(B + C)_p = B_p + C_p$ for all p.

Recalling that the sum of cyclic groups of relatively prime finite orders is cyclic and that every subgroup of a cyclic group is cyclic, we easily see that $B \subset A$ is cyclic and if and only if each B_p is cyclic and if $B_p = 0$ for all except a finite number of p.

We are now ready to prove Theorem **3.1.1**.

3.3 Proof of Theorem 3.1.1

Theorem 3.1.1 If G is an abelian group, then the following are equivalent:

1. $G = \cup_{n=1}^{\infty} (a_n)$, where $(a_1) \subset (a_2) \subset \dots$ are finite cyclic groups
2. Every finitely generated subgroup of G is cyclic of finite order.
3. All the elements of G have finite order and for $a, b \in G$, $|(a, b)| = lcm(|a|, |b|)$
4. All elements of G are of finite order and for $a, b \in G$, $(b) \subset (a)$ if and only if $|b|$ divides $|a|$.
5. All the elements of G have finite order and for $a, b \in G$, $|(a) \cap (b)| = gcd(|a|, |b|)$
6. G is the weak direct product of a family of subgroups indexed by the primes p where for each p the factor indexed by p is isomorphic to $\mathbb{Z}/(p^n)$, for $n \geq 0$, or to $\mathbb{Z}(p^\infty)$

Proof. $(1 \Rightarrow 2)$: Every finitely generated subgroup is contained in one of the cyclic groups (a_n), and so as a subgroup of a cyclic group it is cyclic.

$(2 \Rightarrow 3)$: If $c \in (a,b)$, then $c^{lcm(|a|,|b|)} = 1$. But by (2), (a,b) is cyclic. Also there is a $c \in (a,b)$ with $|c| = lcm(|a|,|b|)$. Since by the above lemma $lcm(|a|,|b|)$ is the largest possible order of an element of (a,b). So $(a,b) = (c)$. This gives that $|(a,b)| = |c| = lcm(|a|,|b|)$.

$(3 \Rightarrow 4)$: This follows directly from Corollary **3.2.3**.

$(4 \Rightarrow 5)$: Note that $gcd(|a|,|b|)$ is the largest natural number that divides both $|a|$ and $|b|$, it is the largest possible order of any common subgroup of (a) and (b). Specifically, $(a) \cap (b)$ is such a subgroup. So we have that $|(a) \cap (b)| \leq gcd(|a|,|b|)$. Now since $gcd(|a|,|b|)$ divides $|a|$ and (a) is cyclic, (a) has a cyclic subgroup (a') of order $gcd(|a|,|b|)$. Furthermore, Since $|a'| = gcd(|a|,|b|)$ and $gcd(|a|,|b|)$ divides $|b|$, condition (4) gives us that $(a') \subset (b)$. So we have that $(a') \subset (a) \cap (b)$. Hence, $gcd(|a|,|b|) \leq |(a) \cap (b)|$. Thus, it must be that $|(a) \cap (b)| = gcd(|a|,|b|)$.

$(5 \Rightarrow 6)$: By Lemma **3.2.4** above, we have that $A = \bigoplus_p A_p$. We now want to find out what it means for such an $A = \bigoplus_p A_p$ to satisfy condition (4) in Theorem 1, i.e., all the elements of A have finite order, and for any $a, b \in A$,

$$|(a) \cap (b)| = gcd(|a|,|b|)$$

(recall that we are using the + notation)

First note that our previous remarks about subgroups of A imply that A satisfies condition (5) if and only if each A_p satisfies condition (5). So now we ask what it means for A_p to satisfy condition (5).

Let $x, y \in A_p$ have orders p^k and p^l, respectively. Assume $k \leq l$. By condition (5), with x as a and y as b,

$$|(x) \cap (y)| = gcd(p^k, p^l) = p^k$$

So $(x) \cap (y) \subset (x)$. Furthermore, since these groups have the same order, we have that $(x) \cap (y) = (x)$. Hence, $(x) \subset (y)$.

So now we have that for $x, y \in A_p$, either $(x) \subset (y)$ or $(y) \subset (x)$. So, if A_p has an element x of largest order p^n, we have that $A_p = (x) \cong \mathbb{Z}/(p^n)$.

It remains to argue that if A_p does not have an element of largest order, then $A_p \cong \mathbb{Z}(p^\infty)$. If A_p doesn't have an element of largest order, then for each $n \geq 1$, there is an $x_n \in A_p$ of order p^n. But then

$$(x_1) \subset (x_2) \subset (x_3) \subset \ldots$$

Also, $A_p = \cup_{n=1}^{\infty}(x_n)$, for if $y \in A_p$ has order p^k then $(x_k) = (y)$. Thus, $y \in \cup_{n=1}^{\infty}(x_n)$. Hence $A_p = \cup_{n=1}^{\infty}(x_n)$. Now with this and

$$(x_1) \subset (x_2) \subset (x_3) \subset \ldots$$

we want to argue that we can assume

$$x_1 = px_2, x_2 = px_3, \ldots$$

Noting that $|px_2| = p = |x_1|$, we get that $(x_1) = (px_2)$. So we could replace x_1 with px_2 and get $px_2 = x_1$. We could then similarly replace x_2 with px_3. However, then we might loose the fact that $px_2 = x_1$. So we consider the infinite diagram

$$\begin{array}{ccccccccc}
(x_1) & \subset & (x_2) & \subset & (x_3) & \subset & (x_4) & \subset & \dots \\
\| & & \| & & \| & & \| & & \\
(px_2) & \subset & (x_2) & \subset & (x_3) & \subset & (x_4) & \subset & \dots \\
\| & & \| & & \| & & \| & & \\
(p^2x_3) & \subset & (px_3) & \subset & (x_3) & \subset & (x_4) & \subset & \dots \\
\| & & \| & & \| & & \| & & \\
(p^3x_4) & \subset & (p^2x_4) & \subset & (px_4) & \subset & (x_4) & \subset & \dots \\
\| & & \| & & \| & & \| & & \\
\vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Note that the group (x_1) is finite. So among its elements, $x_1, px_2, p^2x_3, \dots$, at least one of the elements is repeated infinitely often. We call one such element y_1. Now we redraw the above diagram, but only using the rows beginning with $(p^k x_{k+1})$ where $y_1 = p^k x_{k+1}$. Then we repeat the procedure we used to find y_1 with the second column to find a y_2. Clearly, $py_2 = y_1$.

Repeating, we find a $y_3, y_4, \dots$, and we have that $(y_1) \subset (y_2) \subset (y_3) \subset \dots$, with $py_2 = y_1, py_3 = y_2, \dots$.

With this choice it is easy to establish an isomorphism. Note that $(y_1) = (x_1), (y_2) = (x_2), (y_3) = (x_3), \dots$. We define

$$\phi : A_p \to \mathbb{Z}(p^\infty)$$

by

$$\phi(y_n) = \frac{1}{p^n} + \mathbb{Z}$$

So, (again with a change to + notation) we have (5) implies (6).

(6 ⇒ 1): We have that $A = \bigoplus_p A_p$ with each A_p isomorphic to $\mathbb{Z}/(p^n)$ or $\mathbb{Z}(p^\infty)$. Recall that $\mathbb{Z}(p^\infty)$ is the increasing union of a chain of cyclic groups. So then using a zig-zag procedure we can find $x_1, x_2, x_3, \dots \in A$ with (x_n) cyclic for each n and such that

$$(x_1) \subset (x_2) \subset (x_3) \subset \dots$$

This completes our proof.

□

3.4 Properties of Semi-cyclic Groups

We now define what we mean by the order of a semi-cyclic group G.

Definition 3.4.1. *By condition* (6) *of Theorem* ***3.1.1****, G is the weak direct product of a family of subgroups $G_p \subset G$ (p a prime), where $G \cong \mathbb{Z}/(p^n)$ or $G \cong \mathbb{Z}(p^\infty)$ for each p. So we define the order of G to be the formal symbol $\prod_p p^{k_p} = 2^{k_2}3^{k_3}5^{k_5}\dots$ (p ranges over the primes), where each k_p is such that $0 \leq k_p \leq \infty$ and where $k_p = k$ if $G_p \cong \mathbb{Z}/(p^k)$, and where $k_p = \infty$ if $G_p \cong \mathbb{Z}(p^\infty)$.*

Jean-Pierre Serre called these symbols super-natural numbers in his *Galois Cohomology* [13]. He used them originally to define the order of a pro-finite group. However, they are also suitable for defining the order of a semi-cyclic group.

Letting m and n be the supernatural numbers $m = \prod_p p^{k_p}$ and $n = \prod_p p^{l_p}$, Serre says $m|n$ if and only if $k_p \leq l_p$ for each p. With these notions we can establish many claims about semi-cyclic groups that correspond to similar results about cylcic groups.

Proposition 3.4.2. *Every subgroup of a semi-cyclic group is semi-cyclic.*

Proof. note that $\mathbb{Z}/(p^n)$ has a (unique) subgroup of order $\mathbb{Z}/(p^k)$ if and only if $k \leq n$, i.e. if $p^k|p^n$. We have a similar claim for $\mathbb{Z}(p^\infty)$, i.e. it has a (unique) subgroup of order p^k for each k with $0 \leq k \leq \infty$. Noting this, we see that our result follows directly from Corollary **3.2.5** above. □

Proposition 3.4.3. *Any two semi-cyclic groups of order N are isomorphic.*

Proof. This result follows from condition (6) of Theorem **3.1.1**. □

Proposition 3.4.4. *A semi-cyclic group G of order N has a unique (semi-cyclic) subgroup of order M if and only if M divides N.*

Proof. We just showed that any two semi-cyclic groups of order N are isomorphic. Based on this, we can say that if H and G are semi-cyclic groups of order M and N, then also using condition (6) of Theorem 1, it is easy to see that H is isomorphic to a (unique) subgroup of G if and only if $M|N$. □

Proposition 3.4.5. *Quotient groups of semi-cyclic groups are themselves semi-cyclic.*

Proof. Concerning this result, if H and G are semi-cyclic groups such that H is a subgroup of G, then

$$\frac{G}{H} = \frac{\bigoplus G_p}{\bigoplus H_p} = \bigoplus \frac{G_p}{H_p}$$

Clearly, each $\frac{G_p}{H_p}$ will be of the form $\mathbb{Z}/(p^n)$ or $\mathbb{Z}(p^\infty)$. □

In addition to these four propositions, we can also note that for supernatural numbers M and N we can define $gcd(M, N)$ and $lcm(M, N)$ in the obvious fashion. With these notions we can further show the following:

Proposition 3.4.6. *If H and G are semi-cyclic groups of orders m, n respectively, then $H \times G$ is semi-cyclic if and only if $gcd(m, n) = 1$*

Proof. Let G and H be semi-cyclic groups of orders m, n respectively. Then by condition (6) of Theorem **3.1.1**, $G = \prod_p G_p$ and $H = \prod_p H_p$ are the weak direct product of families of subgroups indexed by the primes p where for each p the factors indexed by p are isomorphic to $\mathbb{Z}/(p^n)$, $0 \leq n$ or to $\mathbb{Z}(p^\infty)$. Furthermore, let e_G and e_H denote the respective identities of G and H.

Suppose $gcd(m, n) \neq 1$. Then we have that there is some prime p such that $|G_p| = p^k$ and $|H_p| = p^l$ where neither k nor l are 0. So suppose we have $0 < k \leq l$. Let $g \in G_p$ and $h \in H_p$ with $|g| = p^k$ and $|h| = p^l$. Consider the cyclic subgroups (e_G, h) and (g, e_H). Note that we have $|(e_G, h)| = p^l$, $|(g, e_H)| = p^k$, and

$$|(e_G, h) \cap (g, e_H)| = |(e_G, e_H)| = 1 \neq p^k = gcd(|(e_G, h)|, |(g, e_H)|)$$

So by condition (5) of Theorem **3.1.1**, $G \times H$ is not a semi-cyclic group.

On the other hand, suppose $gcd(m, n) = 1$. Then For each prime p, either $|G_p| = 1$ or $|H_p| = 1$. Then we define a series of cyclic groups indexed by the primes as follows:

$$F_p = \begin{cases} G_p, & \text{if } |H_p| = 1 \\ H_p, & \text{if } |G_p| = 1 \end{cases}$$

This gives us

$$G \times H \cong \prod_p G_p \times \prod_p H_p \cong \prod_p F_p$$

where all above products depict weak direct products. Hence, we see that $G \times H$ is a semi-cyclic group.

□

We make one last observation about a semi-cyclic group of order $\prod_p p^{k_p}$. By condition (1) of Theorem **3.1.1** we know that we can write $G = \cup_{k=1}^{\infty}(a_k)$ where $(a_1) \subset (a_2) \subset (a_3) \subset \dots$ are finite cyclic groups.

Furthermore, if $G = \cup_{k=1}^{\infty}(a_k)$ and $H = \cup_{k=1}^{\infty}(b_k)$ are semi-cyclic groups of the same order n, then $a_1, a_2, \dots$ and $b_1, b_2, \dots$ can be chosen such that $|a_1| = |b_1|$, $|a_2| = |b_2|$, $|a_3| = |b_3|$, $\dots$. This is easily seen if we note that if $n = \prod_p p^{k_p}$ then each of G and H is isomorphic to a common semi-cyclic group K with $K = \cup_{k=1}^{\infty}(c_k)$ (as above). If $\phi : K \to G$ and $\psi : K \to H$ are isomorphisms, we only need to let $\phi(c_k) = a_k$ and $\psi(c_k) = b_k$ and we have our desired values for each a_k and each b_k.

For a basic example, consider any field F and let $U \subset F$ be the set of all units in F. Then U is a group under multiplication. Furthermore, we can easily see that U satisfies condition (4) of Theorem **3.1.1**. If $a, b \in U$ and $|b|$ divides $|a| = k$, then b is a root of the polynomial $x^k - 1$ in $F[x]$. However, we know that $x^k - 1$ has at most k roots, which can all be found in the subgroup (a). Thus, $b \in (a)$ and $(b) \subset (a)$.

3.5 An Application with Formal Power Series

For another example, we return to consider the set of formal power series $F[[x]]$ with coefficients from some field F, along with the operation of composition of series. Here, for convenience, we assume that F has characteristic 0. More specifically, we will once again be looking at our group I of all invertible formal power series with respect to composition.

If we let $G \subset I$ be any torsion subgroup of I, we find that G is a semi-cyclic group. For the rest of this section we assume that F has characteristic 0 and that $G \subset I$ is a torsion subgroup.

Before we proceed, we recall from Chapter 2 that a formal power series S has order n in I if and only if S is conjugate to ϵx, for some $\epsilon \in F$ where ϵ has order n in F^*. Furthermore, given such an S, we can choose $T \in I$ of the form $x + \dots$ such that $T^{(-1)} \circ S \circ T = \epsilon x$. Recall that for such an S, we have $S = \epsilon x + \dots$.

Now for power series $T, S \in I$, if we have that $T^{(-1)} \circ S \circ T = \epsilon x$, then it is easy to see that the degree 1 term of S must be ϵx. So we have that the order of S in I is the same as the order of its degree 1 coefficient in the field F. One specific consequence of this is that the only power series of finite order with degree one coefficient 1 would be the identity itself, $x \in I$.

Lemma 3.5.1. *If $k \geq 1$, the $S \in I$ of the form*

$$S = a_1 x + a_{k+1} x^{k+1} + a_{2k+1} x^{2k+1} + \dots$$

form a subgroup of I.

Proof. If there is an $\epsilon \in F$ with $|\epsilon| = k$, then these S are precisely the S such that $S \circ (\epsilon x) = (\epsilon x) \circ S$. So they form a subgroup of I. If there is no such $\epsilon \in F$, then, since F has characteristic 0, we have an extension $F \subset F'$ such that there is such an $\epsilon \in F'$. So again we see that these S form a subgroup of I.

□

Note that if $S_1, S_2, \dots \in I$ are of this form, where $S_n'(0) = 1$ for each $n \geq 1$ (i.e. $S_n = x + \dots$), and if $S_1 \circ S_2 \circ S_3 \dots$ converges to S, then S is also of this form.

Here, we also recall from the previous chapter that if we let $S = \epsilon x + ax^{k+1} + \dots$, where $k \geq 1$ and $|\epsilon| = n$, then if n does not divide k (i.e. $e^k \neq 1$), there is a (unique) $b \in F$ such that if $T = x + bx^{k+1}$, then $T^{(-1)} \circ S \circ T = \epsilon x + 0x^{k+1} + \dots$. Furthermore, if $|S| = n$ and n divides k, then $a = 0$.

Now we turn our attention back to torsion subgroups of I. let $G \subset I$ be a torsion subgroup. Then

Theorem 3.5.2. *G is abelian.*

Proof. Let $S_1, S_2 \in G$. We want to show S_1 and S_2 commute, i.e., $S_2^{(-1)} \circ S_1 \circ S_2 = S_1$. Let $S_3 = S_2^{(-1)} \circ S_1 \circ S_2$. Suppose $|S_1| = k$. Then it follows that $|S_3| = k$, since S_1 and S_3 are conjugate.

However, since S_1 and S_3 are conjugate, we can write $T^{(-1)} \circ S_3 \circ T = S_1$, for some $T \in F[[x]]$ with the additional property that T, and so $T^{(-1)}$, are of the form $x + \dots$.

So $T^{(-1)} \circ S_3 \circ T \circ S_3^{k-1} = x + \dots$. However, since $T^{(-1)} \circ S_3 \circ T \circ S_3^{k-1} \in G$, we know that $T^{(-1)} \circ S_3 \circ TcircS_3^{k-1}$ has finite order. So, $T^{(-1)} \circ S_3 \circ T \circ S_3^{k-1} = x$. Hence, $T^{(-1)} \circ S_3 \circ T = S_3$. This gives us that

$$S_1 = T^{(-1)} \circ S_3 \circ T = S_3 = S_2^{(-1)} \circ S_1 \circ S_2$$

Therefore, we have that S_1 and S_2 commute.

□

Theorem 3.5.3. *G is a semi-cyclic group.*

Proof. Let $S_1 = \epsilon x + \dots$ and $S_2 = \delta x + \dots$ be elements of G. Then $S_1 \circ S_2 = \epsilon\delta x + \dots$. Here we note that $|S_1| = |\epsilon|$, $|S_2| = |\delta|$, and $|S_1 \circ S_2| = |\epsilon\delta|$. So it follows that $lcm(|S_1|, |S_2|) = lcm(|\epsilon|, |\delta|)$. Further, we know that, in F, $|\epsilon\delta| = lcm(|\epsilon|, |\delta|)$.

Now consider (S_1, S_2). Clearly, $|(S_1, S_2)| \leq lcm(|S_1|, |S_2|)$ Also, $(S_1 \circ S_2) \subset (S_1, S_2)$. So $|(S_1 \circ S_2)|$ divides $|(S_1, S_2)|$. However, we now have that $|(S_1 \circ S_2)| = |\epsilon\delta| = lcm(|\epsilon|, |\delta|) = lcm(|S_1|, |S_2|)$. Thus, $lcm(|S_1|, |S_2|)$ divides $|(S_1, S_2)|$. Thus, $lcm(|S_1|, |S_2|) = |(S_1, S_2)|$. Hence, G is semi-cyclic.

□

This leads us to the following result about torsion subgroups of the group I:

Theorem 3.5.4. *If F is a field of characteristic 0, then two torsion subgroups $G, G' \subset I$ of the same order N (here a supernatural number) are conjugates in I.*

Proof. We let G and G' be two torsion subgroups of I having the same order. Since G and G' are torsion subgroups, we know that they are semi-cyclic. Since G and G' are semi-cyclic with the same order, part 6 of Theorem **3.1.1** gives us that G and G' can be written as the union of chains of finite cyclic subgroups

$$(S_1) \subset (S_2) \subset (S_3) \subset \dots$$

$$(S'_1) \subset (S'_2) \subset (S'_3) \subset \dots$$

where $G = \cup_{n=1}^{\infty}(S_n)$ and $G' = \cup_{n=1}^{\infty}(S'_n)$, and each (S_n) and (S'_n) have the same order. We will denote this value k_n.

To show that G and G' are conjugate, we first show that each are conjugate to a third semi-cyclic subgroup of I, which we will call H and define as follows:

We know that a formal power series S_n has order k_n if and only if it is conjugate to $\epsilon_n x$. Here we note that ϵ_n is the coefficient of the degree 1 term of S_n and also happens to be an element of order k_n in our field F. So we consider the chain of finite cyclic groups

$$(\epsilon_1 x) \subset (\epsilon_2 x) \subset (\epsilon_3 x) \subset \dots$$

where each $\epsilon_n x$ is conjugate to $S_n \in G$. Then we let $H = \cup_{n=1}^{\infty}(\epsilon_n x)$. By construction, H is a semi-cyclic group of the same order as G and G'.

Further, by construction we know that each (S_n) is conjugate to $(\epsilon_n x)$, i.e. $(\epsilon_n x) = T_n^{-1} \circ (S_n) \circ T_n$ for some $T_n \in F[[x]]$. Choosing such a T_1, we consider, $G_1 = Tt_1^{-1} \circ G \circ T_1$. Note that G_1 is the union of the chain

$$(\epsilon_1 x) \subset (S_2^1) \subset (S_3^1) \subset \dots$$

where each (S_n^1) is conjugate to and, thus, has the same order as the original (S_n). Also, note that G_1 is commutative. So, specifically, S_2^1 commutes with $\epsilon_1 x$. This tells us that S_2^1 is of the form

$$S_2^1 = \epsilon_2 x + a_{k_1+1} x^{k_1+1} + a_{2k_1+1} x^{2k_1+1} + \dots$$

Since the only (potentially) non-zero terms of S_2^1 have degree $jk_1 + 1$ for natural numbers j, we can choose T_2, such that $T_2^{(-1)} \circ S_2^1 \circ T_2 = \epsilon_2 x$, to be of the form

$$T_2 = \prod_{j=1}^{\infty} (x + b_{jk_1+1} x^{jk_1+1})$$

Notice that each term $(x + b_{jk_1+1} x^{jk_1+1})$ will commute with $\epsilon_1 x$. Hence, T_2 will commute with $\epsilon_1 x$. So, we can conjugate G_1 by T_2, and doing so will leave $(\epsilon_1 x)$ unchanged. Furthermore, we now have that $G_2 = T_2^{-1} \circ G_1 \circ T_2$ is the union of the chain

$$(\epsilon_1 x) \subset (\epsilon_2 x) \subset (s_3^2) \subset \dots$$

where, again, each (S_n^2) is conjugate to and, thus, has the same order as the original (S_n).

Now since G_2 is commutative, S_3^2 must be of the form

$$S_3^2 = \epsilon_3 x + a_l x^{l+1} + a_{2l+1} x^{2l+1} + \dots$$

where $l = lcm(k_1, k_2)$. Therefore, as above, we can choose T_3 to commute with $\epsilon_1 x$ and $\epsilon_2 x$.

If we continue in this manner, we can find a $T_4, T_5, \dots$ just as we found T_2 and T_3. Then, letting

$$T = T_1 \circ T_2 \circ T_3 \circ \dots$$

we get that

$$T^{-1} \circ G \circ T = H$$

Here we should note that T as defined above is indeed well-defined. To see this, we need only consider the composition $T_1 \circ T_2 \circ T_3 \circ \dots$ modulo x^m for all natural numbers m. Note that from how $T_1, T_2, T_3, \dots$ were chosen, for any specific value of m, there will only be a finite number of $T_1, T_2, T_3, \dots$ that are not congruent to x modulo x^m. Thus, for each specific value of m, the composition

$$T = T_1 \circ T_2 \circ T_3 \circ \dots$$

is well-defined. Hence, T is well defined in general.

So now we have that G is conjugate to $H = \cup_{n=1}^{\infty}(\epsilon_n x)$. By using the same process with G', we get that G' is conjugate to the semi-cyclic group $H' = \cup_{n=1}^{\infty}(\epsilon'_n x)$, where again each $\epsilon'_n x$ has order k_n. However, since both $\epsilon_n x$ and $\epsilon'_n x$ have the same order for each value of n, we have that $(\epsilon_n x) = (\epsilon'_n x)$. Hence, $H = H'$. So we have that G and G' are both conjugate to the same group. Therefore, G and G' are conjugate to one another.

□

Furthermore, we note that Theorem **3.5.4** holds for F of characteristic $p > 0$ with the additional assumption that N is relatively prime to p.

Chapter 4 Multivariate Formal Power Series

4.1 The Group of Invertible Multivariate Series With Respect to Composition

In this chapter, it is our goal to generalize some of the questions and results mentioned in Chapter 2 to multivariate formal power series. In order to do this, we must first define formal composition for multivariate series. In this section, we again let F be a field with characteristic 0 or p for some prime p. If we consider two formal series in n variables, $S, T \in F[[x_1, x_2, \ldots, x_n]]$, we notice that it is unclear how one might go about composing S with T or vice versa. Instead we look, not at individual multivariate series, but at n-tuples of formal power series in n variables. So here, we are looking at elements of the ring $F[[x_1, x_2, \ldots, x_n]]^n$, as opposed to simply $F[[x_1, x_2, \ldots, x_n]]$. If $S = (S_1, S_2, \ldots, S_n)$ and $T = (T_1, T_2, \ldots, T_n)$ are two elements of $F[[x_1, x_2, \ldots, x_n]]^n$, for which each individual series, $S_1, S_2, \ldots, S_n, T_1, T_2, \ldots, T_n$ has no degree 0 coefficient, then we can define the composition, $S \circ T$ to be the following:

Definition 4.1.1.

$$S \circ T = (S_1(T_1, T_2, \ldots, T_n), S_2(T_1, T_2, \ldots, T_n), \ldots, S_n(T_1, T_2, \ldots, T_n))$$

Again, we note here that each individual power series must have no constant term, that is, for each $S_1, S_2, \ldots, S_n, T_1, T_2, \ldots, T_n$, we must have $S_i(0, 0, \ldots, 0) = 0$ and $T_i(0, 0, \ldots, 0) = 0$. This is required for much the same reason we cannot compose two single variable formal power series unless the constant term is zero. Suppose for example $T_1 = 1 + \ldots$ and S_1 (or any individual series S_i of $S = (S_1, S_2, \ldots, S_n)$) had infinitely many terms containing powers of the variable x_1, then we clearly see that taking $S_1(T_1, T_2, \ldots, T_n)$ could lead to a series containing a non-converging infinite sum as the degree 0 coefficient.

At this point, we would like to determine a subset of $F[[x_1, x_2, \ldots, x_n]]^n$ that forms a group with formal composition. However, first we address the property which will prove useful. Similar to what was done in the single-variable case, for an element $S = (S_1, S_2, \ldots, S_n)$ of $F[[x_1, x_2, \ldots, x_n]]^n$, we would like a method of focusing on only finitely many terms of each series S_i of S. More precisely, it will prove useful to focus on only the terms having degree less than k for some natural number k. So consider the ideal J generated by all single terms of degree k for some natural number k with coefficient 1. That is, J is the ideal generated by terms of the form $x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$ for $j_1 + j_2 + \cdots + j_n = k$. We want to examine each S_i modulo J. We will usually refer to this as S_i modulo terms of degree k.

Proposition 4.1.2. *Let $S = (S_1, S_2, \ldots, S_n)$ and $T = (T_1, T_2, \ldots, T_n)$ be two elements of $F[[x_1, x_2, \ldots, x_n]]^n$. We have that $S = T$ if and only if $S_i \equiv T_i$ modulo terms of degree k for all natural numbers k.*

Proof. Let us denote each S_i

$$S_i = \epsilon x_i + \sum_{k=0}^{\infty} \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j_1,j_2,\ldots,j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

and each T_i as

$$T_i = \epsilon x_i + \sum_{k=0}^{\infty} \sum_{j_1+j_2+\cdots+j_n=k} t^i_{(j_1,j_2,\ldots,j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

It is clear that $S = T$ if and only if $S_i = T_i$ for each i. The rest of the proof is similar to the single-variable case. Consider a given value of i. If $S_i = T_i$, it is trivial that we get congruence modulo terms of degree k for each $k \geq 0$. So assume that $S_i \equiv T_i$ modulo terms of degree k for all natural numbers k. $S_i \equiv T_i$ modulo terms of terms of degree k means that $S_i - T_i \in J$, where J is the ideal generated by all terms of degree k with coefficient 1. However, this gives that

$$s_(j_1, j_2, \ldots, j_n) - t_(j_1, j_2, \ldots, j_n) = 0$$

for all values of $j_1, j_2, \ldots, j_n$ for $j_1 + j_2 + \cdots + j_n = l$ and $l = 1, 2, \ldots k-1$. In other words,

$$s_(j_1, j_2, \ldots, j_n) = t_(j_1, j_2, \ldots, j_n)$$

all values of $j_1, j_2, \ldots, j_n$ for $j_1 + j_2 + \cdots + j_n = l$ and $l = 1, 2, \ldots k-1$. Furthermore, if this is true for each natural number k, this gives us that $S_i = T_i$. □

Now we return to trying to determine a subset of $F[[x_1, x_2, \ldots, x_n]]^n$ that forms a group with formal composition. We have already eliminated all elements with non-zero constant terms. We now consider the following properties.

Proposition 4.1.3. *The element $E = (x_1, x_2, \ldots, x_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ is an identity element.*

Proof. This result is trivial. If $S = (S_1, S_2, \ldots, S_n)$ is an element in $F[[x_1, x_2, \ldots, x_n]]^n$, we see that

$$(x_1, x_2, \ldots, x_n) \circ S = S \circ (x_1, x_2, \ldots, x_n) = (S_1, S_2, \ldots, S_n)$$

□

Proposition 4.1.4. *Formal composition of elements of $F[[x_1, x_2, \ldots, x_n]]^n$ having no degree-0 coefficient is associative.*

Proof. This result follows fairly directly from the definition. Let
$S = (S_1(x_1, x_2, \ldots, x_n), S_2(x_1, x_2, \ldots, x_n), \ldots, S_n(x_1, x_2, \ldots, x_n))$,
$T = (T_1(x_1, x_2, \ldots, x_n), T_2(x_1, x_2, \ldots, x_n), \ldots, T_n(x_1, x_2, \ldots, x_n))$, and
$U = (U_1(x_1, x_2, \ldots, x_n), U_2(x_1, x_2, \ldots, x_n) \ldots, U_n(x_1, x_2, \ldots, x_n))$ be elements of $F[[x_1, x_2, \ldots, x_n]]^n$.
Notice that the ith series of $S \circ T$ is

$$S_i(T_1(x_1, x_2, \ldots, x_n), T_2(x_1, x_2, \ldots, x_n), \ldots, T_n(x_1, x_2, \ldots, x_n))$$

Further the ith series of $(S \circ T) \circ U$ is

$$S_i(T_1(U_1, U_2, \ldots, U_n), T_2(U_1, U_2, \ldots, U_n), \ldots, T_n(U_1, U_2, \ldots, U_n))$$

If we instead first take $T \circ U$, we see the ith term of $T \circ U$ is

$$T_i(U_1, U_2, \ldots, U_n)$$

Then taking $S \circ (T \circ U)$ we find that we also arrive at the n-tuple whose ith entry is

$$S_i(T_1(U_1, U_2, \ldots, U_n), T_2(U_1, U_2, \ldots, U_n), \ldots, T_n(U_1, U_2, \ldots, U_n))$$

So we have that our operation is associative. □

Now, in order to form a group with respect to formal composition, we need only identify which elements of $F[[x_1, x_2, \ldots, x_n]]^n$ are invertible with respect to formal composition. However, first we consider the following:

Definition 4.1.5. *If $S = (S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ is such that each S_i is denoted $S_i = s_{i1}x_1 + s_{i2}x_2 + \ldots$, we define the matrix*

$$M_S = \begin{pmatrix} s_{11} & s_{12} & \ldots & s_{1n} \\ s_{21} & s_{22} & \ldots & s_{2n} \\ \vdots & & & \\ s_{n1} & s_{n2} & \ldots & s_{nn} \end{pmatrix}$$

to be the degree-one matrix of S.

Proposition 4.1.6. *An element $S \in F[[x_1, x_2, \ldots, x_n]]^n$ is invertible with respect to formal composition if and only if the degree-one matrix of S is an invertible matrix.*

Proof. Let $S = (S_1, S_2, \ldots, S_n)$ and $T = (T_1, T_2, \ldots, T_n)$ be two elements of $F[[x_1, x_2, \ldots, x_n]]^n$. Further, let each S_i (for $i = 1, 2, \ldots, n$) be denoted $S_i = s_{i1}x_1 + s_{i2}x_2 + \ldots$ and each T_i (for $i = 1, 2, \ldots, n$) be denoted $T_i = t_{i1}x_1 + t_{i2}x_2 + \ldots$.
Then, $S \circ T = (S_1(T_1, T_2, \ldots, T_n), S_2(T_1, T_2, \ldots, T_n), \ldots, S_n(T_1, T_2, \ldots, T_n))$. Focusing on the ith series, S_i, modulo terms of degree 2, we see that

$$\begin{aligned} S_i(T_1, T_2, \ldots, T_n) &= s_{i1}T_1 + s_{i2}T_2 + \cdots + s_{in}T_n \\ &= s_{i1}(t_{11}x_1 + \ldots t_{1n}x_n) + s_{i2}(t_{21}x_1 + \ldots t_{2n}x_n) + \cdots + s_{in}(t_{n1}x_1 + \ldots t_{nn}x_n) \\ &= (s_{i1}t_{11} + s_{i2}t_{21} + \cdots + s_{in}t_{n1})x_1 + \cdots + (s_{i1}t_{1n} + s_{i2}t_{2n} + \cdots + s_{in}t_{nn})x_n \end{aligned}$$

In summary, the coefficient of x_j of the ith series of $S \circ T$, is given by

$$\sum_{k=1}^{n} s_{ik}t_{jk}$$

Now let M_S and M_T denote the degree-one matrices of S and T, respectively. That is,

$$M_S = \begin{pmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ \vdots & & & \\ s_{n1} & s_{n2} & \dots & s_{nn} \end{pmatrix} \qquad T_S = \begin{pmatrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ \vdots & & & \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{pmatrix}$$

Then, we can see that the the coefficient of x_j of the ith series of $S \circ T$, is given by the ijth entry of the product of $M_S M_T^T$, where M_T^T denotes the transpose of M_T.

It follows then that S being invertible (modulo terms of degree 2) is equivalent to there existing a $T \in F[[x_1, x_2, \dots, x_n]]^n$ such that the matrix product $M_S M_T^T$ is the $n \times n$ identity matrix

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \\ \vdots & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}$$

Furthermore, this is true if and only if the determinant of M_S is non-zero [4].

So it suffices to assume that S is congruent to $(x_1, x_2, \dots x_n)$ modulo terms of degree 2. However, suppose $S \neq (x_1, x_2, \dots x_n)$ in general. Then there is some least value k_1 such that each S_i is of the form

$$S_i = \epsilon x_i + \sum_{j_1+j_2+\dots+j_n=k} s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

Now suppose $T^k = (T_1^k, T_2^k, \dots, T_n^k) \in F[[x_1, x_2, \dots, x_n]]^n$ is such that the ith series of T^k is

$$T_i^k = x_i - \sum_{j_1+j_2+\dots+j_n=k} s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

Then, modulo terms of degree $k+1$, the *ith* term of $S \circ T^k$ would be

$$\begin{aligned} S_i(T_1^k, T_2^k, \dots, T_n^k) &= T_i^k + \sum s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \\ &= x_i - \sum s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} + \sum s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \\ &= x_i \end{aligned}$$

We can do this for each value of k for $k \geq 2$. We can then take

$$S \circ T^2 \circ T^3 \circ T^4 \dots$$

Here we note that $T^2 \circ T^3 \circ T^4 \dots = T^2 \circ T^3 \circ T^4 \dots \circ T^k$ modulo terms of degree $k+1$ for all values of k. Hence, $T^2 \circ T^3 \circ T^4 \dots$ is well-defined modulo terms of degree $k+1$ for all values of k. Therefore, $T^2 \circ T^3 \circ T^4 \dots$ is well-defined in general. Furthermore, $S \circ T^2 \circ T^3 \circ T^4 \dots = (x_1, x_2, \dots, x_n)$ modulo terms of degree $k+1$ for all values of k. Therefore, we have that

$$S \circ T^2 \circ T^3 \circ T^4 \dots = (x_1, x_2, \dots, x_n)$$

So by letting $T = T^2 \circ T^3 \circ T^4 \ldots$, we have that $S \circ T = E$. Therefore, T is a right inverse of S, and this completes our proof. □

So we now have all that we need to form a group of elements of $F[[x_1, x_2, \ldots, x_n]]^n$ with formal composition

Definition 4.1.7. *We define the set $I \subset F[[x_1, x_2, \ldots, x_n]]^n$ to be the set of all $S \in F[[x_1, x_2, \ldots, x_n]]^n$ such that the degree-one matrix M_S of S has a non-zero determinant, along with the operation of formal composition.*

Theorem 4.1.8. *The set I along with formal composition is a group*

Proof. This follows from Propositions, 2, 3, and 5. □

4.2 Elements Having Finite Order

We now seek to answer some questions about elements of I with finite order. As one might expect, this question seems to be much more difficult than the single-variable case. So, let us restrict our search to elements $S = (S_1, S_2, \ldots, S_n) \in I$ for which each S_i is of the form

$$S_i = \epsilon_i x_i + \ldots$$

for some $\epsilon_i \in F$. That is, we assume that $S = (\epsilon_1 x_1, \epsilon_2 x_2, \ldots, \epsilon_n x_n)$ modulo terms of degree 2. In this case, we have similar results to the one-dimensional case. So let us assume that S is such that $S^{(m)} = E$. Then we first note that there are only a select few values that ϵ_i could be.

Proposition 4.2.1. *For $S \in F[[x_1, x_2, \ldots, x_n]]^n$ such that $S = (\epsilon_1 x_1, \epsilon_2 x_2, \ldots, \epsilon_n x_n)$ modulo terms of degree 2, let $k_1, k_2, \ldots, k_n$ denote the orders of $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ in the multiplicative group F^*, respectively. If $S^{(m)} = E$, then for $i = 1, 2, \ldots, n$, k_i divides m and, furthermore, the least common multiple of $k_1, k_2, \ldots, k_n$ is equal to m.*

Proof. The fact that k_i divides m for $i = 1, 2, \ldots, n$ is clearly seen by looking at $S^{(m)}$ modulo terms of degree 2. In this case, note that

$$\begin{aligned} S^{(m)} &= (\epsilon_1 x_1, \epsilon_2 x_2, \ldots, \epsilon_n x_n)^{(m)} \\ &= (\epsilon_1^m x_1, \epsilon_2^m x_2, \ldots, \epsilon_n^m x_n) \end{aligned}$$

So if we assume that $S^{(m)} = (x_1, x_2, \ldots, x_n)$, it must be that $\epsilon_i^m = 1$ for $i = 1, 2, \ldots, n$. Furthermore, if we denote the least common multiple of $k_1, k_2, \ldots, k_n$ as k. It is clear that $S^{(k)} = (x_1, x_2, \ldots, x_n)$, since each k_i divides k. □

At this point we restrict S even further, to prove some results about elements of I of finite order. So let $S = (S_1, S_2, \ldots, S_n) \in I$ be such that each $S = (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$ modulo terms of degree 2, i.e., we assume that the value $\epsilon \in F$ is the same for each series. In this case we have the following:

Lemma 4.2.2. *Let $S = (S_1, S_2, \dots, S_n) \in I$ be such that each*

$$S_i = \epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

for some integer k. Then, $S^{(m)}$ is such that the ith series is given by

$$\epsilon^m x_i + \epsilon^{m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)}) \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j_1,j_2,\dots,j_n)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

modulo terms of degree $k+1$.

Before we give the proof of this lemma, we offer the following notational clarification. From this point on, we let (j) denote the n-tuple $(j_1, j_2, \dots, j_n)$. In addition, in order to attempt to keep things from becoming too cluttered, we will often omit the index $j_1 + j_2 + \cdots + j_n = k$ from the summation

$$\sum_{j_1+j_2+\cdots+j_n=k}$$

Proof. We will show this by induction on m. If we suppose that $m = 1$, then the result is trivial.

Now suppose that $S^{(m)}$ is such that the ith series is given by

$$\epsilon^m x_i + \epsilon^{m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)}) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

Consider $S^{(m+1)}$. We note that $S^{(m+1)} = S^{(m)} \circ S$. So (modulo terms of degree $k+1$), the ith series of $S^{(m+1)}$ is given by

$$\begin{aligned}
& \epsilon^m S_i + \epsilon^{m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)}) \sum s^i_{(j)}\ S_1^{j_1} S_2^{j_2} \dots S_n^{j_n} \\
= \ & \epsilon^m(\epsilon x_i + \sum s^i_{(j)}\ x_1^{j_1} \dots x_n^{j_n}) + \epsilon^{m-1}(1 + \epsilon^{k-1} + \cdots + \epsilon^{(m-1)(k-1)}) \sum s^i_{(j)}\ (\epsilon x_1)^{j_1} \dots (\epsilon x_n)^{j_n} \\
= \ & \epsilon^{m+1} x_i + \epsilon^m \sum s^i_{(j)}\ x_1^{j_1} \dots x_n^{j_n} + \epsilon^{m-1}(1 + \epsilon^{k-1} + \cdots + \epsilon^{(m-1)(k-1)}) \sum \epsilon^k s^i_{(j)}\ x_1^{j_1} \dots x_n^{j_n} \\
= \ & \epsilon^{m+1} x_i + (\epsilon^m + \epsilon^{k+m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)})) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \\
= \ & \epsilon^{m+1} x_i + (\epsilon^m + \epsilon^m \epsilon^{k-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)})) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \\
= \ & \epsilon^{m+1} x_i + (\epsilon^m + \epsilon^m(\epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(k-1)})) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \\
= \ & \epsilon^{m+1} x_i + \epsilon^m(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(k-1)}) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}
\end{aligned}$$

Therefore, by induction, our result holds for all integer values of m.

□

Proposition 4.2.3. *Let $S = (S_1, S_2, \dots, S_n) \in I$ be such that each*

$$S_i = \epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

for some integer k. Then, if p does not divide m, $S^{(m)} = E$, and k is congruent to 1 modulo m, we have that each $s^i_{(j_1,j_2,\dots,j_n)} = 0$ for $j_1 + j_2 + \cdots + j_n = k$.

Proof. By the previous lemma, the ith series of $S^{(m)}$ is

$$\epsilon^m x_i + \epsilon^{m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)}) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

modulo terms of degree $k+1$. If $S^{(m)} = E$, it must be that

$$\epsilon^{m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)}) \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} = 0$$

Now if k is congruent to 1 modulo m, we have that

$$\epsilon^{m-1}(1 + \epsilon^{k-1} + \epsilon^{2(k-1)} + \cdots + \epsilon^{(m-1)(k-1)}) \equiv \epsilon^{m-1}(1 + \epsilon^0 + \epsilon^0 + \cdots + \epsilon^0) = m\epsilon^{m-1} \bmod$$

Thus, if p does not divide m, it must be that $s^i_{(j)} = 0$ for all values of $s^i_{(j)}$. □

4.3 Conjugation of Multivariate Series

Now, as we did in the single variable case, we turn our attention to conjugating elements of I.

Proposition 4.3.1. *If $S = (S_1, S_2, \ldots, S_n) \in I$ be such that $S^{(m)} = E$. Then for any conjugate, $T = P^{(-1)} \circ S \circ P$, for any $P \in I$, we have that $T^{(m)} = E$.*

Proof. The proof is identical to the single variable case.

$$\begin{aligned}
T^{(n)} &= (P^{(-1)} \circ S \circ P)^{(m)} \\
&= (P^{(-1)} \circ S \circ P) \circ (P^{(-1)} \circ S \circ P) \circ \cdots \circ (P^{(-1)} \circ S \circ P) \\
&= P^{(-1)} \circ S \circ (P \circ P^{(-1)}) \circ S \circ (P \circ P^{(-1)}) \circ \cdots \circ (P \circ P^{(-1)}) \circ S \circ P \\
&= P^{(-1)} \circ S^{(m)} \circ P \\
&= P^{(-1)} \circ E \circ P \\
&= P^{(-1)} \circ P \\
&= x
\end{aligned}$$

□

Proposition 4.3.2. *Let $P = (P_1, P_2, \ldots, P_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ be such that*

$$P_i = x_i + \sum_{j_1 + j_2 + \cdots + j_n = k} p^i_{(j_1, j_2, \ldots, j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

Then $P^{(-1)} = (P_1^{(-1)}, P_2^{(-1)}, \ldots, P_n^{(-1)})$ exists and is such that

$$P_i^{(-1)} = x_i - \sum p^i_{(j)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

modulo terms of degree $k+1$.

Proof. For $i = 1, 2, \ldots, n$, observe that (modulo terms of degree $k+1$)

$$\begin{aligned} P_i(P_1^{(-1)}, P_2^{(-1)}, \ldots, P_n^{(-1)}), &= P_i^{(-1)} + \sum p^i_{(j)} \; (P_1^{(-1)})^{j_1} (P_2^{(-1)})^{j_2} \ldots (P_n^{(-1)})^{j_n} \\ &= x_i - \sum p^i_{(j)} \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} + \sum p^i_{(j)} \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} \\ &= x_i \end{aligned}$$

Therefore,

$$\begin{aligned} P \circ P^{(-1)} &= (P_1(P_1^{(-1)}, \ldots, P_n^{(-1)}), P_2(P_1^{(-1)}, \ldots, P_n^{(-1)}), \ldots, P_n(P_1^{(-1)}, \ldots, P_n^{(-1)})) \\ &= (x_1, x_2, \ldots, x_n) \end{aligned}$$

We similarly have that $P^{(-1)} \circ P = (x_1, x_2, \ldots, x_n)$. □

Proposition 4.3.3. *Let $S = (S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ be such that each S_i is of the form*

$$S_i = \epsilon x_i + \sum s^i_{(j)} \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

modulo terms of degree $k+1$, where $\epsilon \in F$ has order m in F^*, and if

$$P_i = x_i + \sum p^i_{(j)} \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

and $P = (P_1, P_2, \ldots, P_n)$. Then the ith series of $P^{(-1)} \circ S \circ P$ has the form

$$\epsilon x_i + \sum q^i_{(j)} x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

where

$$q^i_{(j)} = s^i_{(j)} + (\epsilon - \epsilon^k) p^i_{(j)}$$

Proof. We begin by examining the ith entry of the n-tuple $S \circ P$ modulo terms of degree $k+1$. Note that

$$\begin{aligned} S_i(P_1, P_2, \ldots, P_n) &= \epsilon P_i + \sum s^i_{(j)} \; P_1^{j_1} P_2^{j_2} \ldots P_n^{j_n} \\ &= \epsilon x_i + \epsilon \sum p^i_{(j)} \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} + \sum s^i_{(j)} \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} \\ &= \epsilon x_i + \sum (\epsilon p^i_{(j)} + s^i_{(j)}) \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} \end{aligned}$$

To help simplify some notation, we will let $\hat{S}_i = S_i(P_1, P_2, \ldots, P_n)$ and $\hat{S} = (\hat{S}_1, \hat{S}_2, \ldots, \hat{S}_n)$ for $i = 1, 2, \ldots, n$. Hence, $S \circ P = \hat{S} = (\hat{S}_1, \hat{S}_2, \ldots, \hat{S}_n)$.

Now note that, for $i = 1, 2, \ldots, n$

$$\begin{aligned} P_i^{(-1)}(\hat{S}_1, \hat{S}_2, \ldots, \hat{S}_n) &= \hat{S}_i - \sum p^i_{(j)} \; \hat{S}_1^{\,j_1} \hat{S}_2^{\,j_2} \ldots \hat{S}_n^{\,j_n} \\ &= \epsilon x_i + \sum (\epsilon p^i_{(j)} + s^i_{(j)}) \; x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} - \sum p^i_{(j)} \epsilon^{j_1} x_1^{j_1} \epsilon^{j_2} x_2^{j_2} \ldots \epsilon^{j_n} x_n^{j_n} \\ &= \epsilon x_i + \sum (\epsilon p^i_{(j)} + s^i_{(j)} - \epsilon^k p^i_{(j)}) x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n} \end{aligned}$$

So we have that

$$P^{(-1)} \circ S \circ P = P^{(-1)} \circ \hat{S} = Q = (Q_1, Q_2, \ldots Q_n)$$

where each

$$Q_i = \epsilon x_i + \sum (s^i_{(j)} + (\epsilon - \epsilon^k) p^i_{(j)}) x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

□

Corollary 4.3.4. *If k is not congruent to 1 modulo m, then given any values for each $q^i_{(j)}$ in F, we can choose corresponding values for $p^i_{(j)}$ in F such that if*

$$S_i = \epsilon x_i + \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

modulo terms of degree $k+1$, where $\epsilon \in F$ has order m in F^*, and if

$$P_i = x_i + \sum p^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

and $P = (P_1, P_2, \dots, P_n)$, we have that the ith series of $P^{(-1)} \circ S \circ P$ is

$$\epsilon x_i + \sum q^i_{(j)} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

Proof. From the previous proposition, we see that the ith series of $P^{(-1)} \circ S \circ P$ has the form

$$\epsilon x_i + \sum q^i_{(j)} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

where

$$q^i_{(j)} = s^i_{(j)} + (\epsilon - \epsilon^k) p^i_{(j)}$$

Hence, if k is not congruent to 1 modulo m, the expression $(\epsilon - \epsilon^k)$ is non-zero. Thus, we can let

$$p^i_{(j)} = \frac{q^i_{(j)} - s^i_{(j)}}{(\epsilon - \epsilon^k)}$$

Clearly, this gives us our desired result. □

Corollary 4.3.5. *If we let $P = (P_1, P_2, \dots, P_n) \in I$ be such that each P_i has the form*

$$P_i = x_i + \sum p^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

Further let $S = (S_1, S_2, \dots, S_n) \in I$ be such that each

$$S_i = \epsilon x_i + \sum s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

and let $Q = P^{(-1)} \circ S \circ P$ be denoted

$$Q = \epsilon x_i + \sum q^i_{(j)}) x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

If we let P be fixed, then the map that sends each

$$s^i_{(j_1, j_2, \dots, j_n)} \mapsto q^i_{(j_1, j_2, \dots, j_n)})$$

is a bijection.

Proof. Note that for any given values of $s^i_{(j)} \in F$, we can simply choose $q^i_{(j)} = s^i_{(j)} + (\epsilon - \epsilon^k) p^i_{(j)}$ and map $s^i_{(j)}$ to $q^i_{(j)}$. So this map would be injective.

Similarly, for any given values of $q^i_{(j)}$, letting $s^i_{(j)} = q^i_{(j)} - (\epsilon - \epsilon^k) p^i_{(j)}$ will give us that $s^i_{(j)}$ is sent to $q^i_{(j)}$. Hence, this map is surjective.

□

4.4 Classifying Multivariate Series of Finite Order

We now come to a main result that closely resembles one of our earlier results for single-variable series.

Theorem 4.4.1. *Let F be a field of characteristic zero or characteristic p such that p does not divide m. Furthermore, let $\epsilon \in F$ have order m in F^*, and let $S = (S_1, S_2, \ldots, S_n) \in I$ be such that each S_i has the form*

$$S_i = \epsilon x_i + \ldots$$

Then $S^{(m)} = E$ if and only if S is conjugate to $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$.

Proof. First we note that $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$ clearly has order m in $F[[x_1, x_2, \ldots, x_n]]^n$. So it follows from Proposition **4.3.1**. that if S is conjugate to $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$, S will also have order m.

On the other hand, suppose we know that S has order m. Then by Corollary **4.3.4**, we can choose values $\{p^i_{(j)}\}$ for $i = 1, 2, \ldots, n$ and $j_1 + j_2 + \cdots + j_n = 2$ such that if we let $P^2 = (P^2_1, P^2_2, \ldots, P^2_n)$ with

$$P^2_i = x + \sum p^i_{(j)} x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

we will have that

$$(P^2)^{(-1)} \circ S \circ P^2 = S^2 = (S^2_1, S^2_2, \ldots, S^2_n)$$

where each ^2_i has no terms of degree 2. Then, (as long as $m \neq 2$) we can choose values for $\{p^i_{(j)}\}$ for $i = 1, 2, \ldots, n$ and $j_1 + j_2 + \cdots + j_n = 3$ and define P^3 in a similar fashion to that used to define P^2, so that we get that

$$(P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 = S^3 = (S^3_1, S^3_2, \ldots, S^3_n)$$

where S^3_i has no terms of degree 2 or 3. We continue in this manner until we arrive at

$$(P^m)^{(-1)} \circ \cdots \circ (P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 \circ \cdots \circ P^m = S^m = (S^m_1, S^m_2, \ldots, S^m_n)$$

where each S^m_i has no terms of degree $2, 3, \ldots, m$.

So we now have that $S^m = (S^m_1, S^m_2, \ldots, S^m_n)$ is such that for each i,

$$S^m_i = \epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

However, S^m is a conjugate of our original S. Hence, S^m has order m in i. Thus, by Proposition **4.2.3**, it must be the case that each $s^i_{(j)} = 0$ for $j_1 + j_2 + \cdots + j_n = m$. So, we let $P^{m+1} = (P^{m+1})^{(-1)} = x$, and we have that

$$(P^{m+1})^{(-1)} \circ \cdots \circ (P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 \circ \cdots \circ P^{m+1} = S^{m+1} = (S^{m+1}_1, S^{m+1}_2, \ldots, S^{m+1}_n)$$

where each S^{m+1}_i has no terms of degree $2, 3, \ldots, m+1$.

We can continue in this manner, at each stage either

1. choosing coefficients $\{p^i_{(j)}\}$ for $i = 1, 2, \ldots, n$ and $j_1 + j_2 + \cdots + j_n = k$ if k is not congruent to 1 modulo m, to give us

   $$(P^k)^{(-1)} \circ \cdots \circ (P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 \circ \cdots \circ P^k = S^k = (S^k_1, S^k_2, \ldots, S^k_n)$$

   where each S^k_i has no terms of degree $2, 3, \ldots, k$, or

2. if k is congruent to 1 modulo m, we let $P^k = (P^k)^{(-1)} = x$, since Proposition **4.2.3** tells us that it must be the case that

   $$(P^{k-1})^{(-1)} \circ \cdots \circ (P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 \circ \cdots \circ P^{k-1} = S^{k-1} = (S^{k-1}_1, S^{k-1}_2, \ldots, S^{k-1}_n)$$

   where each S^{k-1}_i has no terms of degree $2, 3, \ldots, k$.

Doing this we end up with the following expression

$$\cdots \circ (P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 \circ \cdots = (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \tag{4.4}$$

At this stage, we should discuss why the above is well-defined. Notice that at each stage we chose P^k to be such that the ith series is of the form

$$P^k_i = x + \ldots$$

Hence, by Proposition **4.3.2**, we have that $(P^k)^{(-1)}$ is such that the ith series is of the form

$$(P^k)^{(-1)}_i = x + \ldots$$

Thus, if we look at the left hand side of equation (4) modulo terms of degree $k + 1$, we have

$$(P^k)^{(-1)} \circ \cdots \circ (P^3)^{(-1)} \circ (P^2)^{(-1)} \circ S \circ P^2 \circ P^3 \circ \cdots \circ P^k$$

which is a finite composition, and hence well-defined. This gives us that the infinite composition found in the left hand side of (4) is well-defined modulo terms of degree k for all positive integer values of k. Therefore, it is well-defined in general.

So, we can define the series $P \in I$ to be

$$P = P^2 \circ P^2 \circ \ldots$$

and we have that

$$P^{(-1)} \circ S \circ P = (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$$

Therefore, S is a conjugate of $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$.

□

Corollary 4.4.2. *Let F be a field of characteristic zero or characteristic p such that p does not divide m. Furthermore, let $S = (S_1, S_2, \ldots, S_n) \in I$ be such that each S_i has the form*

$$S_i = \epsilon x_i + \ldots$$

for a given $\epsilon \in F$. Then S having order m in I implies that ϵ has order m in F^*.

Proof. If S has finite order m in I, we have that there is some $P \in I$ such that $P^{(-1)} \circ S \circ P = (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$. Since S and $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$ are conjugates, they have the same order. Clearly $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$ has order m if and only if ϵ has order m in F^*. □

In other words, if we have an $S \in I$ of the above form and we know that S has finite order, we can determine what that order is simply by looking at the degree one coefficient ϵ.

Corollary 4.4.3. *Let F be a field of characteristic zero or characteristic p such that p does not divide m. Furthermore, let $S = (S_1, S_2, \ldots, S_n) \in I$ be such that each S_i has the form*

$$S_i = x_i + \ldots$$

Then S has finite order if and only if $S = (x_1, x_2, \ldots, x_n)$

Proof. We have shown that if S has finite order, it is the same as the coefficient of the degree one term of each series S_i. Since the coefficient of each in this case is 1, the order of S must be 1. Hence $S = (x_1, x_2, \ldots, x_n)$. The other direction is trivial. Clearly $(x_1, x_2, \ldots, x_n)$ has finite order.

□

Also, similar to the single-variable case, we have the equivalent condition below:

Theorem 4.4.4. *Let F be a field of characteristic zero or characteristic p such that p does not divide m. If $S = (S_1, S_2, \ldots, S_n) \in I$ is such that, for each S_i denoted*

$$S_i = \epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j_1,j_2,\ldots,j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

ϵ has order m in F^* and all coefficients of terms with degree $k \neq 1$ modulo m are arbitrarily chosen from F, then there exist unique coefficients for all terms of degree $k = 1$ modulo m for each S_i such that $S^{(m)} = E$.

Proof. Let $S = (S_1, S_2, \ldots, S_n)$ be an element of I, and let us denote each S_i as

$$S_i = \epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=k} s^i_{(j_1,j_2,\ldots,j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

We assume that $\epsilon \in F$ has order m in F^*, and we also assume that $s^i_{(j_1,j_2,\ldots,j_n)}$ are arbitrarily chosen for all i and all $j_1, j_2, \ldots, j_n$ such that $j_1 + j_2 + \cdots + j_n \neq 1$ modulo m. We want to show that there are unique values of $s^i_{(j_1,j_2,\ldots,j_n)}$ for $j_1 + j_2 + \cdots + j_n = 1$ modulo m such that $S^{(m)} = E$.

By Theorem **4.4.1**, it suffices to show that such a S is a conjugate of $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$. So we proceed by beginning with $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$ and showing that we can conjugate to get S. We begin by choosing values for $p^i_{(j_1, j_2, \ldots, j_n)}$ in F for $j_1 + j_2 + \cdots + j_n = 2$ such that if

$$P^2_i = x_i + \sum p^i_{(j)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

and $P^2 = (P^2_1, P^2_2, \ldots, P^2_n)$, we have that the ith series of $(P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2$ is

$$\epsilon x_i + \sum s^i_{(j)} x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

In other words, we have that the degree 2 terms of $(P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2$ match the degree 2 terms of S. Note that this is assuming that $m \neq 1$. However, if $m = 1$, the theorem is trivial.

Then, if $m \neq 3$, we can proceed as above choosing coefficients $p^i_{(j_1, j_2, \ldots, j_n)}$ in F for $j_1 + j_2 + \cdots + j_n = 3$, letting

$$P^3_i = x_i + \sum p^i_{(j)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

and defining $P^3 = (P^3_1, P^3_2, \ldots, P^3_n)$ such that the ith series of $(P^3)^{(-1)} \circ (P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2 \circ P^3$ agrees with S modulo terms of degree 4. That is, $(P^3)^{(-1)} \circ (P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2 \circ P^3$ matches S up through terms of degree 3.

We proceed in this fashion until we have that $(P^m)^{(-1)} \circ \cdots \circ (P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2 \circ \cdots \circ P^m$ is equivalent to S modulo terms of degree $m + 1$. At this point, we know that since $(P^m)^{(-1)} \circ \cdots \circ (P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2 \circ \cdots \circ P^m$ is a conjugate of $(\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n)$, we have that

$$(P^m)^{(-1)} \circ \cdots \circ (P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2 \circ \cdots \circ P^m)^{(m)} = E$$

Since $m + 1 \equiv 1$ modulo m, we cannot find a P^{m+1} in this fashion, so we let $P^{m+1} = x$ and proceed by finding appropriate coefficients to give us $P^{m+2}, P^{m+2}, \ldots, P^{2m}$ so that

$$(P^{2m})^{(-1)} \circ \cdots \circ (P^2)^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P^2 \circ \cdots \circ P^m)^{(2m)}$$

contains all of our chosen coefficients $s^i_{(j_1, j_2, \ldots, j_n)}$ such that $j_1 + j_2 + \cdots + j_n \neq 1$ modulo m up through terms of degree $2m$.

We continue in this manner and then define

$$P = P^2 \circ P^3 \circ \ldots$$

Notice that P modulo terms of degree k for any natural number k is equivalent to

$$P^2 \circ P^3 \circ \cdots \circ P^{k-1}$$

since all P^j for $j \geq k$ are equivalent to x. Hence, P is in fact well-defined and it makes sense to consider conjugation by P.

Furthermore, note that from how we constructed P, $S = P^{(-1)} \circ (\epsilon x_1, \epsilon x_2, \ldots, \epsilon x_n) \circ P$ will contain all of our previously chosen coefficients $s^i_{(j_1,j_2,\ldots,j_n)}$ for all i and all $j_1, j_2, \ldots, j_n$ such that $j_1 + j_2 + \cdots + j_n \neq 1$ modulo m. The coefficients for terms of degree k where $k \equiv 1$ modulo m, which we will also denote $s^i_{(j_1,j_2,\ldots,j_n)}$ for $j_1 + j_2 + \cdots + j_n = k$, are simply some additional values in F.

Therefore, we have $S = (S_1, S_2, \ldots, S_n) \in I$ containing our arbitrarily chosen coefficients $s^i_{(j_1,j_2,\ldots,j_n)}$ where $j_1 + j_2 + \cdots + j_n = k$ for $k \neq 1$ modulo m, such that $S^{(m)} = E$. It only remains to show that the coefficients $s^i_{(j_1,j_2,\ldots,j_n)}$ where $j_1 + j_2 + \cdots + j_n = k$ for $k \equiv 1$ modulo m are unique. So suppose we have S as above such that $S^{(m)} = E$. In addition, let $\bar{S} = (\bar{S}_1, \bar{S}_2, \ldots, \bar{S}_n) \in I$ be such that $\bar{S}^{(m)} = E$ and the ith series of $\bar{S}$ is denoted

$$\bar{S}_i = \epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=k} \bar{s}^i_{(j_1,j_2,\ldots,j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

Also assume that for $j_1 + j_2 + \cdots + j_n = k$ where $k \neq 1$ modulo m, we have that

$$\bar{s}^i_{(j_1,j_2,\ldots,j_n)} = s^i_{(j_1,j_2,\ldots,j_n)}$$

We want to show that when $j_1 + j_2 + \cdots + j_n = k$ for $k \equiv 1$ modulo m, we also have

$$\bar{s}^i_{(j_1,j_2,\ldots,j_n)} = s^i_{(j_1,j_2,\ldots,j_n)}$$

Now we know that there exists a P in I such that $P^{(-1)} \circ S \circ P = E$. It follows that, since S and $\bar{S}$ are equivalent modulo terms of degree $m+1$, that

$$P^{(-1)} \circ \bar{S} \circ P \equiv P^{(-1)} \circ S \circ P = E$$

modulo terms of degree $m+1$. So the i the series of $P^{(-1)} \circ \bar{S} \circ P$ is of the form

$$\epsilon x_i + \sum_{j_1+j_2+\cdots+j_n=m+1} q^i_{(j_1,j_2,\ldots,j_n)}\ x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$$

modulo terms of degree $m+2$, for some values $q^i_{(j_1,j_2,\ldots,j_n)} \in F$. However, since $P^{(-1)} \circ \bar{S} \circ P$ is a conjugate of $\bar{S}$, we know that, like $\bar{S}$, $(P^{(-1)} \circ \bar{S} \circ P)^{(m)} = E$. So, we know that each $q^i_{(j_1,j_2,\ldots,j_n)} = 0$. Thus, we have that conjugating both S and $\bar{S}$ by P yields E modulo terms of degree $m+2$. By Corollary **4.3.5**, this gives us that

$$\bar{s}^i_{(j_1,j_2,\ldots,j_n)} = s^i_{(j_1,j_2,\ldots,j_n)}$$

for $j_1 + j_2 + \cdots + j_n = m+1$.

A similar argument gives us that

$$\bar{s}^i_{(j_1,j_2,\ldots,j_n)} = s^i_{(j_1,j_2,\ldots,j_n)}$$

for all $j_1 + j_2 + \cdots + j_n = k$ when $k \equiv 1$ modulo m. Thus, the coefficients $s^i_{(j_1,j_2,\ldots,j_n)}$ for each i and $k = j_1 + j_2 + \cdots + j_n$ where $k \equiv 1$ modulo m are, in fact, unique. □

Chapter 5 Group Actions and A Natural Automorphism of I

5.1 Group Actions of the Symmetric Group on I

In this chapter, it is our goal to identify a natural automorphism of the group $I \subset F[[x_1, x_2, \ldots, x_n]]^n$. In particular, we seek to identify a kind of permutation automorphism corresponding to elements $\sigma \in \Sigma_n$, where Σ_n denotes the Symmetric group on a set of n elements.

The two most obvious possibilities for such permutation automorphisms would be following:

1. The map that permutes the order of individual series in an n-tuple. That is, if $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$, the map which sends
$$(S_1, S_2, \ldots, S_n) \mapsto (S_{\sigma(1)}, S_{\sigma(2)}, \ldots, S_{\sigma(n)})$$
2. The map that permutes the variables of each individual series in an n-tuple. That is, the map which sends
$$(S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)) \mapsto (S_1(x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \ldots, S_n(x_{\sigma(1)}, \ldots, x_{\sigma(n)}))$$

However, it turns out that neither give an automorphism. For example, consider $(x, y) \in F[[x, y]]^2$ for some field F, and consider $(12) \in S_2$. If we think of (12) permuting the series in (x, y) as in our first possible map, we find that

$$\begin{aligned}(12)((x,y)\circ(x,y)) &= (12)(x,y)\\ &= (y,x)\end{aligned}$$

while, on the other hand,

$$\begin{aligned}(12)(x,y)\circ(12)(x,y) &= (y,x)\circ(y,x)\\ &= (x,y)\end{aligned}$$

If we think of (12) permuting the variable in each series, we get the same result:

$$\begin{aligned}(12)((x,y)\circ(x,y)) &= (12)(x,y)\\ &= (y,x)\end{aligned}$$

while, on the other hand,

$$\begin{aligned}(12)(x,y)\circ(12)(x,y) &= (y,x)\circ(y,x)\\ &= (x,y)\end{aligned}$$

Clearly, our two previous examples do not work. However, it turns out that if we do both, permute the series of the n-tuple and permute the variables of each series, then we do get an automorphism of I. The rest of this sections seeks to establish this fact.

For the following we want to define two actions of the group Σ_n on $F[[x_1, x_2, \ldots, x_n]]^n$. Our first action is as follows:

Definition 5.1.1.

$$\perp : \Sigma_n \times F[[x_1, x_2, \ldots, x_n]]^n \to F[[x_1, x_2, \ldots, x_n]]^n$$

where an element $\sigma \in \Sigma_n$ acts on $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ by permuting $S_1, S_2, \ldots, S_n$ according to σ in the following way: if $\sigma(i) = j$, then replace S_j with S_i.

In other words, $\sigma(S_1, S_2, \ldots, S_n) = (S_{\sigma^{-1}(1)}, S_{\sigma^{-1}(2)}, \ldots, S_{\sigma^{-1}(n)})$.

Note that it is important that, if $\sigma(i) = j$, we replace S_j with S_i and not S_i with S_j. For if we are to consider the map which sends

$$\sigma \times (S_1, S_2, \ldots, S_n) \mapsto (S_{\sigma(1)}, S_{\sigma(2)}, \ldots, S_{\sigma(n)})$$

we find that it is in fact not a group action. Consider the following example

Let $(S_1, S_2, S_3) \in F[[x_1, x_2, x_3]]^3$ for some field F. Then consider $(12) \in S_3$ and $(23) \in S_3$. We see that $(12) \circ (23) = (123)$. So we have that

$$\begin{aligned} (12)((23)(S_1, S_2, S_3)) &= (12)(S_1, S_3, S_2) \\ &= (S_3, S_1, S_2) \end{aligned}$$

On the other hand

$$((12) \circ (23))(S_1, S_2, S_3) = (123)(S_1, S_2, S_3) = (S_2, S_3, S_1)$$

Since $(12)((23)(S_1, S_2, S_3)) \neq ((12) \circ (23))(S_1, S_2, S_3)$, we see that this map is not a group action. Hence, we define our operation $\perp$ as above.

Proposition 5.1.2. *The operation $\perp$, as defined above, is a group action.*

Proof. Let $\sigma, \tau \in \Sigma_n$, and let $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$. Then,

$$\sigma(\tau(S_1, S_2, \ldots, S_n)) = \sigma(S_{\tau^{-1}(1)}, S_{\tau^{-1}(2)}, \ldots, S_{\tau^{-1}(n)})$$

Here we rename $(S_{\tau^{-1}(1)}, S_{\tau^{-1}(2)}, \ldots, S_{\tau^{-1}(n)})$, $(T_1, T_2, \ldots, T_n)$. So we have

$$\begin{aligned} \sigma(\tau(S_1, S_2, \ldots, S_n)) &= \sigma(T_1, T_2, \ldots, T_n) \\ &= (T_{\sigma^{-1}(1)}, T_{\sigma^{-1}(2)}, \ldots, T_{\sigma^{-1}(n)}) \end{aligned}$$

On the other hand, we have that

$$(\sigma\tau)(S_1, S_2, \ldots, S_n) = (S_{(\sigma\tau)^{-1}(1)}, S_{(\sigma\tau)^{-1}(2)}, \ldots S_{(\sigma\tau)^{-1}(n)})$$

Now we need only show that $T_{\sigma^{-1}(k)} = S_{(\sigma\tau)^{-1}(k)}$ for $k = 1, 2, \ldots, n$. So for a given value of k, we let $\sigma^{-1}(k) = j$. We, then, let $\tau^{-1}(j) = i$. So we have that

$$i \overset{\tau}{\mapsto} j \overset{\sigma}{\mapsto} k$$

Thus, it follows that

$$\begin{aligned} T_{\sigma^{-1}(k)} &= T_j \\ &= S_{\tau^{-1}(j)} \\ &= S_i \end{aligned}$$

On the other hand, clearly $S_{(\sigma\tau)^{-1}(k)} = S_i$. Hence, we see that

$$\sigma(\tau(S_1, S_2, \ldots, S_n)) = (\sigma\tau)(S_1, S_2, \ldots, S_n)$$

Furthermore, we clearly see that if $e \in \Sigma_n$ is the identity and $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$, then $e(S_1, S_2, \ldots, S_n) = (S_1, S_2, \ldots, S_n)$.

Therefore, $\perp$ as defined above is a group action.

□

The second action of Σ_n on $F[[x_1, x_2, \ldots, x_n]]^n$ is as follows:

Definition 5.1.3.

$$\top : \Sigma_n \times F[[x_1, x_2, \ldots, x_n]]^n \rightarrow F[[x_1, x_2, \ldots, x_n]]^n$$

where $\sigma \in \Sigma_n$ acts on $(S_1, S_2, \ldots, S_n)$ by permuting the variables $x_1, x_2, \ldots, x_n$ of each S_i according to σ in the following way: if $\sigma(i) = j$, then replace x_i with x_j.

In other words, for a given $(S_1, S_2, \ldots, S_n)$, each $S_i(x_1, x_2, \ldots, x_n)$ is replaced with $S_i(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$.

Proposition 5.1.4. *The operation $\top$, as defined above, is a group action.*

Proof. To arrive at the conclusion that $\top$ is a group action, we first define the action on an individual $S \in F[[x_1, x_2, \ldots, x_n]]$, then use the product action to to obtain our desired result. Thus, it suffices to prove that the operation

$$\top : \Sigma_n \times F[[x_1, x_2, \ldots, x_n]] \rightarrow F[[x_1, x_2, \ldots, x_n]]$$

is indeed a group action.

Let $\sigma, \tau \in \Sigma_n$, and let $S(x_1, x_2, \ldots, x_n) \in F[[x_1, x_2, \ldots, x_n]]$. Then,

$$\begin{aligned} \sigma(\tau S(x_1, x_2, \ldots, x_n)) &= \sigma(S(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)})) \\ &= S(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) \\ &= S(x_{(\sigma\tau)(1)}, x_{(\sigma\tau)(2)}, \ldots, x_{(\sigma\tau)(n)}) \\ &= (\sigma\tau)S(x_1, x_2, \ldots, x_n) \end{aligned}$$

Furthermore, we clearly see that if $e \in \Sigma_n$ is the identity and $S(x_1, x_2, \ldots, x_n) \in F[[x_1, x_2, \ldots, x_n]]$, then $eS(x_1, x_2, \ldots, x_n) = S(x_1, x_2, \ldots, x_n)$.

Therefore, $\top$ as defined above is a group action.

□

Since at this point we have two distinct group actions of Σ_n on $F[[x_1, x_2, \ldots, x_n]]^n$, we will use the following notation. Suppose $\sigma \in \Sigma_n$ and $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$. If we wish to denote that σ acts on $(S_1, S_2, \ldots, S_n)$ via our action $\top$, then we write

$$\sigma\top(S_1, S_2, \ldots, S_n)$$

Similarly, if we wish to denote that σ acts on $(S_1, S_2, \ldots, S_n)$ via our action $\perp$, then we write

$$\sigma\perp(S_1, S_2, \ldots, S_n)$$

Now we turn our attention to the issue of how our two group operations, $\top$ and $\perp$ interact with one another. Specifically, it is fairly easy to see that these two operations will commute. That is, That is, if $\sigma, \tau \in \Sigma_n$ and $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$, then we have that

$$\sigma\perp(\tau\top(S_1, S_2, \ldots, S_n)) = \tau\top(\sigma\perp(S_1, S_2, \ldots, S_n))$$

So, We now introduce a new action defined as follows:

$$\Sigma_n \times F[[x_1, x_2, \ldots, x_n]]^n \xrightarrow{\bullet} F[[x_1, x_2, \ldots, x_n]]^n$$

where $\sigma \in \Sigma_n$ acts on $(S_1, S_2, \ldots, S_n)$ in the following way

$$\sigma \bullet (S_1, S_2, \ldots, S_n) = \sigma\perp(\sigma\top(S_1, S_2, \ldots, S_n))$$

Proposition 5.1.5. *The above operation, $\bullet$, is in fact a group action.*

Proof. Let $\sigma, \tau \in \Sigma_n$, and let $(S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$. Then we have that

$$\begin{aligned}
\sigma \bullet (\tau \bullet (S_1, S_2, \ldots, S_n)) &= \sigma \bullet (\tau\perp(\tau\top(S_1, S_2, \ldots, S_n))) \\
&= \sigma\perp(\sigma\top(\tau\perp(\tau\top(S_1, S_2, \ldots, S_n)))) \\
&= \sigma\perp(\tau\perp(\sigma\top(\tau\top(S_1, S_2, \ldots, S_n)))) \\
&= (\sigma\tau)\perp((\sigma\tau)\top(S_1, S_2, \ldots, S_n)) \\
&= (\sigma\tau) \bullet (S_1, S_2, \ldots, S_n)
\end{aligned}$$

Further, we clearly see that if $e \in \Sigma_n$ is the identity, then

$$e \bullet (S_1, S_2, \ldots, S_n) = e\perp(e\top(S_1, S_2, \ldots, S_n)) = (S_1, S_2, \ldots, S_n)$$

Therefore, $\bullet$ gives us a group action. □

5.2 A Natural Automorphism of I

Now we will seek to show that our previously defined group action, $\bullet$, in fact, defines a group automorphism for I. That is, given $\sigma \in \Sigma_n$, the map defined by

$$(S_1, S_2, \ldots, S_n) \mapsto \sigma \bullet (S_1, S_2, \ldots, S_n)$$

is a group automorphism of I.

So we first note that I is in fact stable under $\bullet$. Let us consider an element $(S_1, S_2, \dots, S_n) \in F[[x_1, x_2, \dots, x_n]]^n$ where each S_k in $(S_1, S_2, \dots, S_n)$ can be denoted

$$S_k = \sum s^k_{(i_1, i_2, \dots, i_n)} x^{i_1} x^{i_2} \dots x^{i_n}$$

It was shown in Proposition **4.1.6** that whether or not an element $(S_1, S_2, \dots, S_n) \in F[[x_1, x_2, \dots, x_n]]^n$ is contained in the group I is dependent only on the degree one terms of each S_k in $(S_1, S_2, \dots, S_n)$. Specifically, $(S_1, S_2, \dots, S_n)$ is contained in I if and only if the degree one matrix

$$\begin{pmatrix} s^1_{(1,0,\dots,0)} & s^2_{(1,0,\dots,0)} & \cdots & s^n_{(1,0,\dots,0)} \\ s^1_{(0,1,0,\dots,0)} & s^2_{(0,1,0,\dots,0)} & \cdots & s^n_{(0,1,0,\dots,0)} \\ \vdots & & & \\ s^1_{(0,\dots,0,1)} & s^2_{(0,\dots,0,1)} & \cdots & s^n_{(0,\dots,0,1)} \end{pmatrix}$$

is invertible. We denote this matrix $M_S = (m_{ij})$. Here we note that m_{ij} is the coefficient of the x_i term of S_j in the n-tuple $(S_1, S_2, \dots, S_n)$.

Now consider a permutation $\sigma \in \Sigma_n$. If we examine now our action $\bullet$ affects the degree one matrix M of an n-tuple $(S_1, S_2, \dots, S_n)$, we find that $\sigma(S_1, S_2, \dots, S_n)$ results in the n-tuple with corresponding degree one matrix

$$P_\sigma M P_\sigma = (m_{\sigma(i)\sigma^{(-1)}(j)})$$

where P_σ is the permutation matrix corresponding to σ.

Since the determinant of $P_\sigma = (-1)^t$ for some natural number t, we can see that the determinant of $P_\sigma M P_\sigma$ is nonzero if and only if the determinant of M is nonzero. Hence, it follows that I is stable under $\bullet$.

Now to show that $\bullet$ defines a group automorphism for I, we first look at the particular case where $\sigma = (ij) \in \Sigma_n$, for $i \neq j$. However, first we introduce some notation. For a given $(ij) \in S_n$ any series $S \in F[[x_1, x_2, \dots, x_n]]$, we will let $S' = (ij) \top S$. Furthermore, for an element of $F[[x_1, x_2, \dots, x_n]]^n$, $(S_1, S_2, \dots, S_n)$, we introduce the shorthand notation $(S) = (S_1, S_2, \dots, S_n)$.

So with this notation, we have that $(ij) \bullet (S) = (S'_1, \dots, S'_j, \dots, S'_i, \dots, S'_n)$.

We now consider the following claim:

Proposition 5.2.1. *If $\sigma \in \Sigma_n$ is of the form $\sigma = (ij)$, where $i \neq j$, then the map*

$$(S_1, S_2, \dots, S_n) \mapsto \sigma \bullet (S_1, S_2, \dots, S_n)$$

is a group automorphism for I.

Proof. Let $\sigma = (ij) \in \Sigma_n$ such that $i \neq j$. In fact, without loss of generality, let us assume $i < j$. In addition, let $(S) = (S_1, S_2, \dots, S_n)$ and $(T) = (T_1, T_2, \dots, T_n)$ be elements of I. We want to show that

$$\sigma \bullet ((S_1, S_2, \dots, S_n) \circ (T_1, T_2, \dots, T_n)) = \sigma \bullet (S_1, S_2, \dots, S_n) \circ \sigma \bullet (T_1, T_2, \dots, T_n)$$

We have that

$$\begin{aligned}
\sigma \bullet (S) \circ \sigma \bullet (T) &= \sigma\top(\sigma\bot(S_1, S_2, \ldots, S_n)) \circ \sigma\bot(\sigma\top(T_1, T_2, \ldots, T_n)) \\
&= \sigma\top(S_1, \ldots, S_j, \ldots, S_i, \ldots, S_n)) \circ \sigma\bot(T_1', T_2', \ldots, T_n') \\
&= (S_1, \ldots, S_j, \ldots, S_i, \ldots, S_n)) \circ (T_1', T_2', \ldots, T_n') \\
&= (S_1(T'), \ldots, S_j(T'), \ldots, S_i(T'), \ldots, S_n(T'))
\end{aligned}$$

On the other hand, we also have that

$$\begin{aligned}
\sigma \bullet ((S) \circ (T)) &= \sigma\top(\sigma\bot(S_1(T), \ldots, S_i(T), \ldots, S_j(T), \ldots, S_n(T)) \\
&= \sigma\top(S_1(T), \ldots, S_j(T), \ldots, S_i(T), \ldots, S_n(T) \\
&= ((S_1(T))', \ldots, (S_j(T))', \ldots, (S_i(T))', \ldots, (S_n(T))')
\end{aligned}$$

Now the coefficient of $x_1^{h_1} x_2^{h_2} \ldots x_n^{h_n}$ in $S_k(T)$ for some $1 \leq k \leq n$, is given by

$$\sum_{k_1 \geq 0,\ k_2 \geq 0,\ \ldots,\ k_n \geq 0} s_{(k_1, k_2, \ldots, k_n)}\ c_{(k_1, k_2, \ldots, k_n)}^{(h_1, h_2, \ldots, h_n)}$$

where $c_{(k_1, k_2, \ldots, k_n)}^{(h_1, h_2, \ldots, h_n)}$ is the coefficient of $x_1^{h_1} x_2^{h_2} \ldots x_n^{h_n}$ for $T_1^{k_1} T_2^{k_2} \ldots T_n^{k_n}$. So the coefficient of $x_1^{h_1} x_2^{h_2} \ldots x_n^{h_n}$ in $(S_k(T))'$ is given by

$$\sum_{k_1 \geq 0,\ k_2 \geq 0,\ \ldots,\ k_n \geq 0} s_{(k_1, k_2, \ldots, k_n)} c_{(k_1, k_2, \ldots, k_n)}^{(h_1, \ldots, h_j, \ldots h_i, \ldots, h_n)}$$

Hence, permuting x_i and x_j in $S_k(T)$ is equivalent to permuting x_i and x_j in $(T_1, T_2, \ldots, T_n)$, then composing with S_k. In other words, $(S_k(T))' = S_k(T')$.

Therefore, we have that

$$\begin{aligned}
\sigma \bullet ((S) \circ (T)) &= ((S_1(T))', \ldots, (S_j(T))', \ldots, (S_i(T))', \ldots, (S_n(T))') \\
&= (S_1(T'), \ldots, S_j(T'), \ldots, S_i(T'), \ldots, S_n(T')) \\
&= (\sigma \bullet (S)) \circ (\sigma \bullet (T))
\end{aligned}$$

Therefore, we have our desired result.

□

Now then, we are ready to address the more general case where σ is any element of Σ_n.

Theorem 5.2.2. *For any $\sigma \in \Sigma_n$, the map*

$$(S_1, S_2, \ldots, S_n) \mapsto \sigma \bullet (S_1, S_2, \ldots, S_n)$$

is a group automorphism for I.

Proof. We have proven the result for the special case that $\sigma = (ij)$, where $i \neq j$. Now for any arbitrary $\sigma \in \Sigma_n$, we can write

$$\sigma = (i_1 j_1) \circ (i_2 j_2) \circ \cdots \circ (i_s j_s)$$

Since we have shown previously that $\bullet$ is a group action, it follows that the map

$$(S_1, S_2, \ldots, S_n) \mapsto \sigma \bullet (S_1, S_2, \ldots, S_n)$$

is a composition of the automorphisms

$$\begin{aligned}(S_1, S_2, \ldots, S_n) &\mapsto (i_1 j_1)(S_1, S_2, \ldots, S_n)\\ (S_1, S_2, \ldots, S_n) &\mapsto (i_2 j_2)(S_1, S_2, \ldots, S_n)\\ &\vdots\\ (S_1, S_2, \ldots, S_n) &\mapsto (i_s j_s)(S_1, S_2, \ldots, S_n)\end{aligned}$$

Therefore, the map

$$(S_1, S_2, \ldots, S_n) \mapsto \sigma \bullet (S_1, S_2, \ldots, S_n)$$

is itself an automorphism of I.

□

5.3 Elements of $F[[x_1, x_2, \ldots, x_n]]^n$ Fixed by All Elements of Σ_n

In this section we focus on the previously defined group action, $\bullet$, of elements of Σ_n acting on $F[[x_1, x_2, \ldots, x_n]]^n$. It is our goal here to give a characterization of all elements $S = (S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ such that $\sigma S = S$ for all $\sigma \in \Sigma_n$. More specifically, we seek to show that there is a bijective correspondence between all such S fixed by all $\sigma \in \Sigma_n$ and individual formal power series $S_1(x_1, x_2, \ldots, x_n)$ that are symmetric with respect to the variables $x_2, x_2, \ldots, x_n$.

To find all such $S = (S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$, it suffices to find all $S \in F[[x_1, x_2, \ldots, x_n]]^n$ such that $\sigma S = S$ for all σ in the set of generators $\{(12), (13), \ldots, (1n)\}$ for the set Σ_n.

For each element $(1k)$ in this set of generators of Σ_n, we need

$$(1k)(S_1, S_2, \ldots, S_n) = (S_1, S_2, \ldots, S_n)$$

In particular, this requires that

$$S_k(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n) = S_1(x_1, x_2, \ldots, x_n)$$

or

$$S_k(x_1, x_2, \ldots, x_n) = S_1(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n)$$

Hence, once we know S_1, we also know what S_k must be for all $k = 2, 3, \ldots, n$.

Now we turn our attention to elements $(ij) \in \Sigma_n$ where neither i nor j are 1 and $i \neq j$. Without loss of generality, let us assume that $i < j$. For such an element $(ij) \in \Sigma_n$, we must of course have

$$S_1(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n) = S_1(x_1, x_2, \ldots, x_n)$$

Since this must be true for all integers $2 \leq i, j \leq n$, we see that $S_1(x_1, x_2, \ldots, x_n)$ must be symmetric in the variables $x_2, x_3, \ldots, x_n$.

Furthermore, going back to the equation above

$$S_k(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n) = S_1(x_1, x_2, \ldots, x_n)$$

we see that S_k must be symmetric in the variables $x_1, x_2, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n$.

This leads us to the following conjecture:

Theorem 5.3.1. *The element $S = (S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ is such that $\sigma S = S$ for all $\sigma \in \Sigma_n$ if and only if S has the following two properties:*

1. *The series $S_1(x_1, x_2, \ldots, x_n)$ is symmetric in the variables $x_2, x_3, \ldots, x_n$.*

2. *For each $k = 2, 3, \ldots, n$, S_k is such that*

$$S_k(x_1, x_2, \ldots, x_n) = S_1(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n)$$

Proof. The fact that S having the two listed properties is a necessary condition is shown in the paragraphs above. So we only concern ourselves here with showing that the two properties are sufficient for S to be fixed by all $\sigma \in \Sigma_n$.

So, assume $S = (S_1, S_2, \ldots, S_n)$ has the two properties above. Let k be an integer greater than 1 and less than or equal to n, and consider the generating element $(1k)$ of the set Σ_n. We seek to show that

$$(1k)(S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)) = (S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n))$$

Before we proceed, let us introduce the following notation: For each $S_i(x_1, x_2, \ldots, x_n)$, let $S_i' = S_i(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n)$. Also, if no variables are listed, we assume that $S_i = S_i(x_1, x_2, \ldots, x_n)$.

Now note that

$$\begin{aligned} & (1k)(S_1(x_1, \ldots, x_n), S_2(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)) \\ = \; & (S_k', S_2', \ldots, S_{k-1}', S_1', S_{k+1}', \ldots, S_n') \end{aligned}$$

Now for every S_j, where j is neither 1 nor k, we know that

$$S_i' = S_i(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n) = S_i(x_1, x_2, \ldots, x_n)$$

since S_i is symmetric in the variables $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.

Furthermore, we know that our assumed properties of S that

$$S_k' = S_k(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n) = S_1(x_1, x_2, \ldots, x_n)$$

and

$$S'_1 = S_1(x_k, x_2, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_n) = S_k(x_1, x_2, \ldots, x_n)$$

Thus, we have that

$$\begin{aligned} & (1k)(S_1(x_1, \ldots, x_n), S_2(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)) \\ = \; & (S'_k, S'_2, \ldots, S'_{k-1}, S'_1, S'_{k+1}, \ldots, S'_n) \\ = \; & (S_1, S_2, \ldots, S_n) \end{aligned}$$

Therefore, we have that $(1k)S = S$ for all generators of Σ_n. It follows that $\sigma S = S$ for all $\sigma \in \Sigma_n$ if and only if S has the two listed properties. □

The above theorem, shows us that we have a bijective correspondence between all formal power series $S_1(x_1, x_2, \ldots, x_n)$ that are symmetric with respect to $x_2, x_3, \ldots, x_n$ and all elements $S = (S_1, S_2, \ldots, S_n) \in F[[x_1, x_2, \ldots, x_n]]^n$ such that $\sigma S = S$ for all $\sigma \in \Sigma_n$.

Bibliography

[1] N Bourbaki, Elements of Mathematics: Commutative Algebra, Chapters 1-7. Springer-Verlag, New York (1989)

[2] H Cartan, Elementary Theory of Analytic Functions of One Or Several Complex Variables. Hermann, Paris (1963)

[3] G Dorfer and H Woracek, Formal Power Series and Some Theorems of J. F. Ritt in Arbitrary Characteristic, Monatshefte fr Mathematik , 127 no. 4, 277-293 (1999)

[4] S Friedberg, A Insel, L Spence, Linear Algebra, 4th ed. Pearson, New York (2002)

[5] S Jean, Conjugacy Classes of Series in Positive Characteristic and Witt Vectors, Journal de Theorie des Nombres de Bordeaux, 21, 263-284 (2009)

[6] D Johnson, The Group of Formal Power Series Under Substitution, Journal of the Australian Mathematical Society, 45, 296-302 (1988)

[7] E Kasner, Infinite Groups Generated by Conformal Transformations of Period Two (Involutions and Symmetries), American Journal of Mathematics, 138 no. 2, 177-184 (1916)

[8] B Klopsch, Automorphisms of the Nottingham Group, Journal of Algebra, 223, 37-56 (2000)

[9] Lubin, Nonarchimedean Dynamical Systems, Compositio Mathematica, 94 no. 3, 321-346 (1994)

[10] H Niven, H Zuckerman, H Montgomery, In Introduction to the Theory of Numbers. Wiley (1991)

[11] A O'Farrell, Compositions of Involutive Power Series, and Reversible Series, Computational Methods and Function Theory, 8 no. 1, 173-193 (2008)

[12] S Scheinberg, Power Series in One Variable, Journal of Mathematical Analysis and Applications, Volume 31, Issue 2, 321-333 (1970)

[13] J-P Serre, Galois Cohomology. Springer-Verlag (1997)

[14] R Stanley, Enumerative Combinatorics Volume 2. Cambridge University Press, New York (1997)

Vita

Thomas Scott Brewer

Education

- **Illinois Wesleyan University**, Bloomington, Illinois
  - B.A., Mathematics, May 2003
- **Eastern Illinois University**, Charleston, Illinois
  - M.A., Mathematics, May 2010

Publications

- *Semi-Cyclic Groups and an Application for Formal Power Series*, submitted to Mathematica Scandinavica

Awards and Fellowships

- Daniel R. Reedy Quality Achievement Fellowship, University of Kentucky, Fall 2010- Spring 2013
- Dulgar Mathematics Scholarship, Eastern Illinois University, Fall 2009
- Dr. Morton B. and Mary F. Harris Family Scholarship, Eastern Illinois University, Spring 2010
- Distinguished Graduate Student Award, Eastern Illinois University, Spring 2010