APPLICATIONS OF THE ARTIN-HASSE EXPONENTIAL SERIES AND ITS GENERALIZATIONS TO FINITE ALGEBRA GROUPS

A dissertation submitted to
Kent State University in partial
fulfillment of the requirements for the
degree of Doctor of Philosophy

by

Darci L. Kracht

December, 2011

Dissertation written by

Darci L. Kracht

B.S., Kent State University, 1985

M.A., Kent State University, 1989

Ph.D., Kent State University, 2011

Approved by

Stephen M. Gagola, Jr.,	Chair, Doctoral Dissertation Committee
Donald L. White,	Member, Doctoral Dissertation Committee
Mark L. Lewis ,	Member, Doctoral Dissertation Committee
Paul Farrell,	Member, Doctoral Dissertation Committee
Peter Tandy,	Member, Doctoral Dissertation Committee

Accepted by

Andrew M. Tonge,	Chair, Department of Mathematical Sciences
Timothy Moerland,	Dean, College of Arts and Sciences

TABLE OF CONTENTS

ACKNOWLEDGMENTS

It is a great pleasure to acknowledge some of the many people who have contributed to this dissertation. First, I owe a huge debt of gratitude to my advisor, Steve Gagola. Steve has a remarkable depth and breadth of mathematical knowledge and intuition. I am very lucky he has shared this with me over many years. His undergraduate modern algebra sequence, graduate abstract algebra sequence, and advanced group theory courses are what led me to pursue graduate work in finite group theory. I thank Steve for his unflagging support and patience, even when I took a long hiatus from research.

I thank Don White for teaching my first course in character theory, writing an unparalleled letter of recommendation, mixing one hell of a Caucasian, and especially for keeping his Hattori Hanzo sheathed during my candidacy exam and dissertation defense. I thank Mark Lewis for advice and support, especially when I first began my research on algebra groups. I thank Chuck Gartland for his company in the department on many late evenings and weekends, sharing some great bottles of wine, and for installing some badly needed font files on my computer— I could not have typeset the big box plus in Theorem 2.13 without Chuck's help.

I thank Joe Diestel for my first glimpse into the world of mathematics research during the 1984 Banach Space Conference and for his infectious enthusiasm for all things mathematical. I thank Andrew Tonge for being a great teacher, housemate, friend, and boss. I thank Artem Zvavitch for greasing the wheels of bureaucracy and for managing to reconstruct my lost file when I decided to return to the doctoral program after many years off. I thank Ulrike Vorhauer for a Sunday morning spent helping me to translate and understand an old German number theory paper.

I thank Carl Stitz for the movie trailer. I thank Carol Steiner for her advice ("Don't do it!

Didn't you learn anything from watching me?"). I thank Dan Lewis, Terri Polanski, Laura Dykes, Bev Reed, and many other fellow graduate students, colleagues, and Facebook friends for their encouragement and support.

I thank Dima Ryabogin for his unconventional encouragement ("I don't understand why you never got a Ph.D. All these other stupid people do it.") and frank criticism of my dissertation defense ("The middle part was OK."). I thank Volker Mehrmann for clarifying the shades of meaning in the various German words for "shift" and for the regular weather reports from Berlin. I thank Angie Spalsbury for being my supporter, confidante, and dearest friend as we have traveled the road from student to mathematician and mother together.

I thank my father, Ron Kracht, for posing logic puzzles at the dinner table and, when he helped me with my math homework, for always making me explain the solutions back to him. I thank my mother, Lynne Kracht, for the Cone of Uncertainty and for providing the best role model as wife, mother, and professional woman. It is only now that I realize how difficult it must have been for her to return to college and start a new career with three school-age children. My parents believed in me and taught me to believe in myself.

Finally, I thank my husband, Michael Stacey, and daughter, Claire Stacey, for their limitless patience, love, and support, especially over the past two years, when I have often been absent, distracted, or short of temper. The many sacrifices they have made enabled me to persevere during the most difficult times. They suffered with me through every set-back, and rejoiced with me at every success. I cannot express how grateful I am to be able to share this achievement with them.

CHAPTER 1

INTRODUCTION AND MOTIVATION

In this chapter, we establish the context for the main results of this dissertation. Let F be a field of characteristic p and order q. Let R be a finite-dimensional associative F-algebra and $J = J(R)$ the Jacobson radical of R. (So J is a finite-dimensional, nilpotent, associative F-algebra.) If $G = 1 + J$, then G is a finite p-group. Groups of this form are called *F-algebra groups*, or simply, *algebra groups*. (We will assume this notation throughout this chapter.)

A family of examples is provided by the upper-triangular $n \times n$ matrices over F, for a fixed positive integer n. The Jacobson radical, J, of the algebra of all such matrices is the set of strictly upper-triangular matrices over F. Thus, $G = 1 + J$ is the set of *unipotent upper-triangular matrices*, those with 1's along the main diagonal, often denoted $UT_n(F)$.

The subgroups of $G = 1 + J$ are of the form $1 + X$, where X is a subset of J closed under the operation

$$(x, y) \mapsto x + y + xy. \tag{1.1}$$

In particular, X need not be an algebra. On the other hand, if L is a subalgebra of J, then L is certainly closed under (1.1). In this case, we call $1 + L$ an *algebra subgroup* of G. If $H \leqslant G$ such that $|H \cap K|$ is a q-power for all algebra subgroups K of G, then we say H is a *strong subgroup* of G.

Since algebra subgroups have q-power order and since the collection of algebra subgroups of G is closed under intersection, it follows that algebra subgroups are strong.

However, the converse is not true. For example, the subgroup

$$H = \left\{ \left(\begin{array}{ccc} 1 & \alpha & \binom{\alpha}{2} \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{array} \right) \middle| \, \alpha \in F \right\}$$

is a strong subgroup but not an algebra subgroup of the algebra group $UT_3(F)$ for $p > 2$. Here $\binom{\alpha}{2} = \frac{\alpha(\alpha-1)}{2}$ and, more generally, for k an integer with $0 < k < p$ and $\alpha \in F$,

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$$

denotes the generalized binomial coefficient.

Algebra groups and related notions were introduced by Isaacs (1995) to solve a long-standing problem about the character degrees* of the upper-triangular matrix groups. Strong subgroups played a key role in Isaacs's proof of that result.

In the same paper, Isaacs showed that certain inertia subgroups of characters of algebra groups are strong (Theorems 6.1 and 8.3). An *inertia subgroup* is the stabilizer of a point under the action of the group by conjugation on the set of irreducible characters of a normal subgroup. Of course, a group G also acts on its subgroups by conjugation. Recall that the stabilizer of a subgroup H under this action is known as the normalizer of H, denoted $\mathbf{N}_G(H)$. That is,

$$\mathbf{N}_G(H) = \{g \in G : H^g = H\}.$$

In light of the results of Isaacs about character stabilizers, it is natural to ask if normalizers of algebra subgroups of algebra groups are strong. This is the question considered in Chapter 4. The tools used to answer the question will be power series.

The first of these is the exponential series. If $x \in J$ with $x^p = 0$, then the usual exponential

*A *character* is a type of function from a group to a field, in this case, the field $\mathbb{C}$ of complex numbers. A *character degree* is the value of a certain type of character, called irreducible, at the identity of the group. There is an extensive literature on group characters and character degrees.

series

$$\exp x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

is defined, since it terminates before any division by zero. In fact, if $J^p = 0$, exp defines a bijection $J \to 1 + J$ with inverse $\log\colon 1 + J \to J$ given by the Mercator series

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots,$$

for $x \in J$.

For $x \in J$ with $x^p = 0$ and $\alpha \in F$, define $(1 + x)^\alpha = \exp(\alpha \log(1 + x)) \in G$, or equivalently,

$$(1 + x)^\alpha = 1 + \alpha x + \binom{\alpha}{2} x^2 + \binom{\alpha}{3} x^3 + \cdots.$$

If we define $(1 + x)^F$ by

$$(1 + x)^F = \{(1 + x)^\alpha \colon \alpha \in F\},$$

then $(1 + x)^F$ is a subgroup of G, called an *F-exponent subgroup*. More is true.

Proposition 1.1. *If $x \in J$ with $x^p = 0$, then $(1 + x)^F$ is a subgroup of G containing $1 + x$. If $x \neq 0$, then $(1 + x)^F$ is isomorphic to the additive group of F. Moreover, distinct F-exponent subgroups intersect trivially. Finally, every algebra subgroup of G of exponent p is the union of its distinct F-exponent subgroups.*

Proof. This is Corollary 5.2 of (Isaacs, 1995). □

Notice that if we define $\exp(F\hat{x}) = \{\exp(\alpha\hat{x}) \colon \alpha \in F\}$, then $(1 + x)^F = \exp(F\hat{x})$ for $\hat{x} = \log(1 + x)$, so we may denote F-exponent subgroups by $(1 + x)^F$ or by $\exp(F\hat{x})$, as convenient.

Let H be a subgroup of G of exponent p. We say H is *exponentially closed* if $\exp(Fx) \subseteq H$ whenever $\exp(x) \in H$. Isaacs (1995) called these subgroups *partitioned subgroups* because they are equally partitioned in the sense defined in (Isaacs, 1973). It follows from Proposition

1.1 that F-exponent subgroups and algebra subgroups of exponent p are exponentially closed and that the intersection of exponentially closed subgroups is itself exponentially closed.

The next result is central to §4.1, where we give an affirmative answer to the question about normalizers in the case where $J^p = 0$.

Proposition 1.2. *If G is an algebra group, then every exponentially closed subgroup of G is strong.*

Proof. This is Lemma 5.3 of (Isaacs, 1995). □

The notions of F-exponent and exponentially closed subgroups are of limited use in an algebra group whose exponent exceeds its characteristic. Therefore, we set out to generalize these ideas using different power series. In fact, other power series have been used in similar circumstances. Character degree results analogous to those of Isaacs (1995) but for other classical matrix groups were given by Previtali (1995). He used the power series

$$\sigma(x) = x + \sqrt{1 + x^2} = x + \sum_{k=0}^{\infty} \frac{(-1)^{k-1}}{2^{2k-1}} C_{k-1} x^{2k},$$

where $C_n = \frac{1}{n+1}\binom{2n}{n} \in \mathbb{Z}^\dagger$ is the n-th Catalan number for $n \geqslant 0$ and $C_{-1} = -\frac{1}{2}$. This series is defined in odd characteristic only, but these results were known to be false for $p = 2$, anyway. Previtali obtained his results about character degrees by using this power series to show that certain sections of the groups are strong. Previtali (1999) later used truncated exponential series to prove similar results for sizes of certain conjugacy classes in classical groups.

For our purposes, we wanted a power series, or family of power series, that could be used in any characteristic and in algebra groups of arbitrarily large exponent. The truncated exponential series do not have the properties we need. Fortunately, there is a generalization of the exponential series called the Artin-Hasse exponential series that suits our purpose,

[†] As usual, $\mathbb{Z}$ denotes the set of all integers and $\mathbb{Q}$ denotes the set of all rational numbers.

found in the number theory literature. In Chapter 2, we provide the background material needed to prove that the Artin-Hasse exponential series has the desired properties. This includes some elementary results about the ring of Witt vectors. In Chapter 3, we develop analogs of F-exponent subgroups and exponentially closed subgroups for the Artin-Hasse exponential series. In Chapter 4, we use these tools to show when normalizers of algebra subgroups are strong and when there are counter-examples.

As we have seen, strong subgroups play an important role in the results of Isaacs (1995) and Previtali (1995) about character degrees in classical groups. More recently, André (2010) has obtained similar results in a more general setting by showing that certain fixed-point subgroups are strong. These results as well as our results in Chapter 4 motivate the study of strong subgroups in Chapter 5. Here again, we use power series, but this time the series can be much more general.

CHAPTER 2

WITT VECTORS AND THE ARTIN-HASSE EXPONENTIAL SERIES

In this chapter, we provide the background needed to develop the Artin-Hasse exponential series. In §2.1, we define Witt vectors and prove that they form a ring. In §2.2, we define the p-adic Artin-Hasse exponential series E_p and prove that its coefficients are p-integral.

2.1 Witt vectors

The purpose of this section is to develop needed aspects of the theory of Witt vectors that, though elementary, might not be familiar to the reader. The approach is based in large part on Hazewinkel (2009). While proofs have been elaborated, definitions and statements of results have been streamlined for the present setting. In particular, the current treatment is entirely formula-based. However, the theory can be developed in greater generality and with greater sophistication via category theory. (See, for example, Hazewinkel (2009), Lenstra (2002), and Rabinoff (2007).)

Fix p, a prime. Let $X = (X_0, X_1, X_2, \ldots)$, where the X_i are commuting indeterminates. The *(p-adic) Witt polynomials* are defined to be

$$\begin{aligned}
w_0(X) &= X_0, \\
w_1(X) &= X_0^p + pX_1, \\
w_2(X) &= X_0^{p^2} + pX_1^p + p^2X_2, \\
&\vdots \\
w_n(X) &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^nX_n, \\
&\vdots
\end{aligned}$$

In this context, we define the *weight* of the indeterminate X_i to be p^i and the weight of $X_i^{p^j}$ to be $p^i p^j = p^{i+j}$. The weight of a monomial is the sum of the weights of its indeterminates. A polynomial all of whose monomials have the same weight p^k is said to be *isobaric of weight* p^k. Thus, the n-th Witt polynomial, w_n, is isobaric of weight p^n.

Let A be a commutative ring with identity, equipped with the discrete topology*. Define

$$W(A) = \prod_{i=0}^{\infty} A \quad \text{and (for } l = 0, 1, 2, \ldots) \quad W_l(A) = \prod_{i=0}^{l} A.$$

For each nonnegative integer l, consider the surjective homomorphisms $W_{l+1}(A) \to W_l(A)$ given by

$$(a_0, a_1, \ldots, a_l, a_{l+1}) \mapsto (a_0, a_1, \ldots, a_l),$$

and $W(A) \to W_l(A)$ given by

$$(a_0, a_1, \ldots, a_l, a_{l+1}, \ldots) \mapsto (a_0, a_1, \ldots, a_l).$$

Since these homomorphisms are mutually compatible, there is a natural homomorphism $W(A) \to \varprojlim W_l(A)$, the inverse limit. In fact, this is an isomorphism. Thus, we may view $W(A)$ as being endowed with the inverse limit topology, the coarsest topology in which all these maps are continuous.

The main goal of this section is to put a ring structure on $W(A)$ and each $W_l(A)$ so the Witt polynomials are (continuous) ring homomorphisms from any of these products to A. Since this is possible, $W(A)$ is called the *ring of (p-adic) Witt vectors* and $W_l(A)$ is called the *ring of (p-adic) Witt vectors of length* l.† The i-th component, a_i, of the element $a = (a_0, a_1, a_2, \ldots)$ of $W(A)$ (or $W_l(A)$) is called the *i-th Witt component* of a, while the value $w_n(a) \in A$ is called the *n-th ghost component* of a.

*References to topology will be brief and safely ignored by the reader.

†These rings are sometimes called simply *Witt rings*, but this term usually refers to an entirely different ring. Also, the Witt vectors are actually ring elements, although they look like vectors. If A is an algebra, then so are $W(A)$ and $W_l(A)$, and so the Witt vectors really are vectors in that case.

All Witt vectors considered here are p-adic Witt vectors. Although only finite-length Witt vectors will be needed, it is convenient to develop the theory for Witt vectors of infinite length.

Lemma 2.1. *Let $\psi(X) = \psi(X_0, X_1, \ldots)$ be a polynomial in commuting indeterminates with integer coefficients. Write $\psi(X^p) = \psi(X_0^p, X_1^p, \ldots)$. Then*

(a) $\psi(X^p) \equiv \psi(X)^p \mod p$;

(b) $\psi(X^p)^{p^j} \equiv \psi(X)^{p^{j+1}} \mod p^{j+1}$.

Proof. For the first part, write $\psi(X) = M_0 + M_1 + \cdots + M_{n-1} + M_n$, where $M_0, \ldots, M_n$ are monomials in the X_i. It follows that

$$\begin{aligned}\psi(X)^p &= [(M_0 + M_1 + \cdots + M_{n-1}) + M_n]^p \\ &\equiv (M_0 + M_1 + \cdots + M_{n-1})^p + M_n^p \mod p\end{aligned}$$

since the middle terms are all congruent to zero modulo p by the Binomial Theorem. So by induction,

$$\psi(X)^p \equiv M_0^p + M_1^p + \cdots + M_{n-1}^p + M_n^p \mod p.$$

Now each monomial M is of the form $M = cX_{i_1}^{e_1} X_{i_2}^{e_2} \cdots X_{i_k}^{e_k}$, where $X_{i_j} \in \{X_0, X_1, \ldots\}$, $e_j \in \mathbb{Z}^+$, and c is an integer (by hypothesis). So

$$\begin{aligned}M^p &= c^p X_{i_1}^{pe_1} X_{i_2}^{pe_2} \cdots X_{i_k}^{pe_k} \\ &\equiv c X_{i_1}^{pe_1} X_{i_2}^{pe_2} \cdots X_{i_k}^{pe_k} \mod p\end{aligned}$$

since $c^p \equiv c \mod p$ by Fermat's Little Theorem. Part (a) follows, forming the base step of an inductive argument for the second part.

For the inductive step, assume

$$\psi(X^p)^{p^{j-1}} \equiv \psi(X)^{p^j} \mod p^j.$$

That is, there exists a polynomial $\theta(X)$ with integer coefficients such that

$$\psi(X^p)^{p^{j-1}} = \psi(X)^{p^j} + p^j\theta(X).$$

Therefore,

$$\begin{aligned}
\psi(X^p)^{p^j} &= \left[\psi(X)^{p^j} + p^j\theta(X)\right]^p \\
&= \psi(X)^{p^{j+1}} + p\psi(X)^{p^j}p^j\theta(X) + \cdots + (p^j)^p\theta(X)^p \\
&= \psi(X)^{p^{j+1}} + p^{j+1}\hat{\theta}(X) \\
&\equiv \psi(X)^{p^{j+1}} \mod p^{j+1},
\end{aligned}$$

where $\hat{\theta}(X)$ is a polynomial with integer coefficients. This proves part (b). □

The following theorem is the key to most of the properties of Witt vectors we will need.

Theorem 2.2 ("The miracle of the Witt polynomials")**.** *Let $\phi(U, V)$ be a polynomial over the integers in two commuting indeterminates. Let $X = (X_0, X_1, \ldots)$ and $Y = (Y_0, Y_1, \ldots)$ be commuting indeterminates. Then for $n = 0, 1, \ldots$, there are unique polynomials*

$$\phi_n(X; Y) = \phi_n(X_0, \ldots, X_n; Y_0, \ldots, Y_n)$$

having integer coefficients such that, for all n,

$$w_n(\phi_0(X; Y), \phi_1(X; Y), \ldots, \phi_n(X; Y)) = \phi(w_n(X), w_n(Y)). \tag{2.1}$$

Proof. The miracle is that the coefficients are all integers; existence and uniqueness of the ϕ_n as polynomials over the rational numbers is evident once the notation is sorted out. Indeed, for $n = 0$,

$$\begin{aligned}
w_0(\phi_0(X; Y)) &= \phi(w_0(X_0), w_0(Y_0)), \\
\phi_0(X; Y) &= \phi(X_0, Y_0).
\end{aligned}$$

When $n = 1$,

$$\begin{aligned} w_1(\phi_0(X;Y), \phi_1(X;Y)) &= \phi(w_1(X_0, X_1), w_1(Y_0, Y_1)), \\ \phi_0(X;Y)^p + p\phi_1(X;Y) &= \phi(X_0^p + pX_1, Y_0^p + pY_1), \\ \phi_1(X;Y) &= \frac{1}{p}\left[\phi(X_0^p + pX_1, Y_0^p + pY_1) - \phi_0(X;Y)^p\right]. \end{aligned}$$

Similarly, $\phi_n(X;Y)$ lies in the algebra over $\mathbb{Z}\left[\frac{1}{p}\right] \subseteq \mathbb{Q}$ generated by ϕ and $\phi_0, \ldots, \phi_{n-1}$. Since ϕ is integral, so is ϕ_0. Now suppose $\phi_0, \ldots, \phi_{n-1}$ are all integral. When equation (2.1) is expanded, the term $p^n\phi_n(X;Y)$ on the left-hand side is the only term containing $\phi_n(X;Y)$. Hence, the coefficients of $\phi_n(X;Y)$ are all rational numbers whose denominators divide p^n.

Next, compare

$$w_n(X) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n$$

with

$$\begin{aligned} w_{n-1}(X^p) &= \left(X_0^p\right)^{p^{n-1}} + p\left(X_1^p\right)^{p^{n-2}} + \cdots + p^{n-1}\left(X_{n-1}^p\right)^1 \\ &= X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p \end{aligned}$$

to conclude

$$w_n(X) \equiv w_{n-1}(X^p) \mod p^n.$$

It follows that

$$\phi(w_n(X), w_n(Y)) \equiv \phi(w_{n-1}(X^p), w_{n-1}(Y^p)) \mod p^n. \tag{2.2}$$

Now the left-hand side of (2.2) is

$$\begin{aligned} \phi(w_n(X), w_n(Y)) &= w_n(\phi_0(X;Y), \phi_1(X;Y), \ldots, \phi_{n-1}(X;Y), \phi_n(X;Y)) \\ &= \phi_0(X;Y)^{p^n} + \cdots + p^{n-1}\phi_{n-1}(X;Y)^p + p^n\phi_n(X;Y). \end{aligned}$$

The right-hand side of (2.2) is

$$\begin{aligned}\phi(w_{n-1}(X^p), w_{n-1}(Y^p)) &= w_{n-1}(\phi_0(X^p;Y^p), \phi_1(X^p;Y^p), \ldots, \phi_{n-1}(X^p;Y^p)) \\ &= \phi_0(X^p;Y^p)^{p^{n-1}} + \cdots + p^{n-1}\phi_{n-1}(X^p;Y^p).\end{aligned}$$

By Lemma 2.1, for $0 \leqslant i \leqslant n-1$,

$$\phi_{n-i}(X;Y)^{p^i} \equiv \phi_{n-i}(X^p;Y^p)^{p^{i-1}} \mod p^i$$

and so

$$p^{n-i}\phi_{n-i}(X;Y)^{p^i} \equiv p^{n-i}\phi_{n-i}(X^p;Y^p)^{p^{i-1}} \mod p^n.$$

Thus, the 0-th through $(n-1)$-st terms of the left-hand side of (2.2) are term-for-term congruent to the terms of the right-hand side. There is an additional term on the left-hand side, and so,

$$p^n\phi_n(X;Y) \equiv 0 \mod p^n.$$

Therefore, the coefficients of $\phi_n(X;Y)$ must in fact be integers. □

Note that if $\phi(U,V)$ is homogeneous of degree r and if, as usual, X_i and Y_i have weight p^i (for $0 \leqslant i \leqslant n$), then equation (2.1) implies that $\phi_n(X,Y)$ is isobaric of weight rp^n. Also note that essentially the same proof as above would work if ϕ were a polynomial (or even a formal power series) in any number of commuting indeterminates. Versions for polynomials in one, two, and three indeterminates will be used in the proof of Theorem 2.6 below. Finally, since the ϕ_i are polynomials over $\mathbb{Z}$, they are universal in the sense that the same polynomials will work over any ring A with identity.

Let A be an arbitrary ring with identity. The ring operations in $W(A)$ and $W_l(A)$ will be defined in terms of addition and multiplication polynomials. As usual, $X = (X_0, X_1, \ldots)$ and $Y = (Y_0, Y_1, \ldots)$ denote commuting indeterminates. For $n \in \{0, 1, \ldots\}$, define the *(p-adic)*

Witt addition polynomials $s_n = s_n(X_0, \ldots, X_n; Y_0, \ldots, Y_n)$ and the *(p-adic) Witt multiplication polynomials* $m_n = m_n(X_0, \ldots, X_n; Y_0, \ldots, Y_n)$ by

$$\begin{aligned} w_n(s) &= w_n(X) + w_n(Y) \\ \text{and} \quad w_n(m) &= w_n(X) w_n(Y), \end{aligned} \tag{2.3}$$

where $s = (s_0, s_1, \ldots)$ and $m = (m_0, m_1, \ldots)$. It is not difficult to compute the first few addition polynomials explicitly. Indeed, when $n = 0$,

$$\begin{aligned} w_0(s) &= w_0(X) + w_0(Y), \\ s_0 &= X_0 + Y_0. \end{aligned}$$

For $n = 1$,

$$\begin{aligned} w_1(s) &= w_1(X) + w_1(Y), \\ s_0^p + p s_1 &= X_0^p + p X_1 + Y_0^p + p Y_1, \\ (X_0 + Y_0)^p + p s_1 &= X_0^p + Y_0^p + p(X_1 + Y_1). \end{aligned}$$

Solving for s_1, we obtain

$$\begin{aligned} s_1 &= \frac{X_0^p + Y_0^p - (X_0 + Y_0)^p}{p} + (X_1 + Y_1) \\ &= X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} X_0^{p-i} Y_0^i \,. \end{aligned} \tag{2.4}$$

From this it is apparent that s_0 and s_1, at least, have integer coefficients. Similarly, it is easy to see that m_0 and m_1 are integral by computing them directly from the ghost component equations. However, it is even easier to show that all the s_n and m_n are integral using Theorem 2.2, which we now do.

Corollary 2.3. *The Witt addition and Witt multiplication polynomials exist, are unique, and have integer coefficients. Moreover,* $s_n(X; Y) = s_n(Y; X)$ *and* $m_n(X; Y) = m_n(Y; X)$ *for all*

$X = (X_0, X_1, \ldots)$, $Y = (Y_0, Y_1, \ldots)$, *and* $n \in \{0, 1, \ldots\}$. *Finally,* $s_n(X; Y)$ *is isobaric of weight* p^n *and* $m_n(X; Y)$ *is isobaric of weight* $2p^n$.

Proof. Apply Theorem 2.2 to $\mathcal{S}(U, V) = U + V$ for the addition polynomials and to $\mathcal{M}(U, V) = UV$ for the multiplication polynomials. Since $\mathcal{S}(U, V) = U + V = V + U$ and the s_n are unique, it follows that $s_n(X; Y) = s_n(Y; X)$. Similarly, $\mathcal{M}(U, V) = UV = VU$ implies $m_n(X; Y) = m_n(Y; X)$. The statement about the weights is a consequence of the remark immediately following the proof of Theorem 2.2. □

Now let $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots) \in W(A)$ (or $W_l(A)$). Define *Witt addition* $\boxplus$ and *Witt multiplication* $\boxtimes$ by

$$a \boxplus b = (s_0(a_0; b_0), s_1(a_0, a_1; b_0, b_1), \ldots)$$
$$\text{and} \quad a \boxtimes b = (m_0(a_0; b_0), m_1(a_0, a_1; b_0, b_1), \ldots).$$

These operations are clearly not the usual component-wise operations on the tuples. However, in the special case where the elements a and b have disjoint support (that is, for all i, $a_i = 0$ or $b_i = 0$), $a \boxplus b$ reduces to component-wise addition.

Proposition 2.4. *If* $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots) \in W(A)$ *(or* $W_l(A)$*) have disjoint support, then* $a \boxplus b = (a_0 + b_0, a_1 + b_1, \ldots)$.

Proof. By universality of the Witt addition polynomials, it suffices to prove the lemma for $A = \mathbb{Z}$. Suppose $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots) \in W(\mathbb{Z})$ (or $W_l(\mathbb{Z})$) have disjoint support. For $i \in \{0, 1, \ldots\}$, set

$$c_i = a_i + b_i = \begin{cases} a_i & \text{if } a_i \neq 0; \\ b_i & \text{if } a_i = 0. \end{cases}$$

We wish to show $a \boxplus b = (c_0, c_1, \ldots)$.

Proceed by (strong) induction on the index of the component of the sum. For the base step, note that $s_0(a_0; b_0) = a_0 + b_0$. Next, suppose the first $n - 1$ components of the sum

are $a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1}$, that is, $c_0, c_1, \ldots, c_{n-1}$. Consider the ghost component equation

$$\begin{aligned} w_n(s(a;b)) &= w_n(a) + w_n(b), \qquad (2.5) \\ s_0^{p^n} + \cdots + p^{n-1}s_{n-1}^p + p^n s_n &= \left(a_0^{p^n} + \cdots + p^{n-1}a_{n-1}^p + p^n a_n\right) \\ &\quad + \left(b_0^{p^n} + \cdots + p^{n-1}b_{n-1}^p + p^n b_n\right) \\ &= \left(a_0^{p^n} + b_0^{p^n}\right) + \cdots + \left(p^{n-1}a_{n-1}^p + p^{n-1}b_{n-1}^p\right) \\ &\quad + (p^n a_n + p^n b_n) \\ &= c_0^{p^n} + \cdots + p^{n-1}c_{n-1}^p + p^n c_n. \end{aligned}$$

The last equality holds since, for all i, $p^i a_i^{p^{n-i}} = 0$ or $p^i b_i^{p^{n-i}} = 0$. By the inductive hypothesis, $s_i(a;b) = c_i$ for all $i = 1, \ldots, n-1$. Thus, $p^i s_i^{p^{n-i}} = p^i c_i^{p^{n-i}}$ for all $i = 1, \ldots, n-1$. After canceling these common terms from both sides of equation (2.5), we are left with $p^n s_n = p^n c_n$. That is, $s_n(a;b) = c_n = a_n + b_n$, as desired. □

The following is an immediate corollary.

Corollary 2.5. *The zero for the operation $\boxplus$ is $(0, 0, \ldots)$, the Witt vector all of whose components are 0.*

This is a good place to state Witt's theorem on the structure of $W(A)$.

Theorem 2.6 (Witt)**.** *If p is a prime and A is a commutative ring with identity, then $W(A)$ and $W_l(A)$ with addition $\boxplus$ and multiplication $\boxtimes$ are commutative rings for all $l \in \{0, 1, \ldots\}$. The zero element is $(0, 0, 0, \ldots)$ and the unit element is $(1, 0, 0, \ldots)$. Moreover, for all $n = 0, 1, \ldots$, the Witt polynomial w_n is a ring homomorphism from $W(A)$ (or $W_l(A)$) to A.*

Proof. By universality, it suffices to prove the theorem for $A = \mathbb{Z}$. We will check the ring axioms using ghost component equations and Theorem 2.2. In fact, some of the work has

already been done. Corollary 2.3 shows that both operations are commutative. Corollary 2.5 shows that $(0, 0, 0, \ldots)$ is the zero element.

Next, we will verify that $I = (1, 0, \ldots, 0)$ is the multiplicative identity in $W(A)$. By the definition of the Witt polynomials, $w_n(I) = 1$ for all n. Thus, for all n and all $X = (X_0, X_1, \ldots)$,

$$w_n(m(I; X)) = w_n(I)w_n(X) = 1 \cdot w_n(X) = w_n(X). \tag{2.6}$$

Now the polynomials w_n are certainly not one-to-one, since the value of $w_n(a)$ depends only on the 0-th through n-th components of a. However, for $a, b \in W(\mathbb{Z})$, it is true that $w_n(a) = w_n(b)$ for all n if and only if $a = b$. Therefore, we conclude from equation (2.6) that $m(I; X) = X$ for all X. That is, $I = (1, 0, 0, \ldots)$ is the unit element in $W(A)$.

Each remaining ring axiom can be proved using Theorem 2.2 (or a generalization) and an appropriate polynomial ϕ. The left distributive law will be proved in detail to illustrate the method, while the others will be left to the reader. Note that the right distributive law follows from the left distributive law and commutativity of $\boxtimes$.

For the left distributive law, define $\phi(T, U, V) = T(U + V) = TU + TV$. Recall the polynomials $\mathcal{S}$ and $\mathcal{M}$ defined in the proof of Corollary 2.3. For $i = 0, 1, \ldots$, let $\phi_i(X, Y, Z) = m_i(X; s(Y; Z))$. Then for all n,

$$\begin{aligned}
w_n(\phi_0(X, Y, Z), \ldots, \phi_n(X, Y, Z)) &= w_n(m_0(X; s(Y; Z)), \ldots, m_n(X; s(Y; Z))) \\
&= \mathcal{M}(w_n(X), w_n(s(Y; Z))) \\
&= w_n(X) \cdot w_n(s(Y; Z)) \\
&= w_n(X) \cdot \mathcal{S}(w_n(X), w_n(Y)) \\
&= w_n(X) \cdot [w_n(Y) + w_n(Z)] \\
&= w_n(X)w_n(Y) + w_n(X)w_n(Z).
\end{aligned}$$

Next, for $i = 0, 1, \ldots$, let $\psi_i(X, Y, Z) = s_i(m(X;Y); m(X;Z))$. Then for all n,

$$\begin{aligned} w_n(\psi_0(X,Y,Z), \ldots, \psi_n(X,Y,Z)) &= w_n(s_0(m(X;Y); m(X;Z)), \ldots, s_n(m(X;Y); m(X;Z))) \\ &= \mathcal{S}(w_n(m(X;Y)), w_n(m(X;Z))) \\ &= w_n(m(X;Y)) + w_n(m(X;Z)) \\ &= \mathcal{M}(w_n(X), w_n(Y)) + \mathcal{M}(w_n(X), w_n(Z)) \\ &= w_n(X)w_n(Y) + w_n(X)w_n(Z). \end{aligned}$$

Hence, the sequences $\phi_0, \phi_1, \ldots$ and $\psi_0, \psi_1, \ldots$ both satisfy the three-variable version of equation (2.1) for ϕ. So by uniqueness, $\phi_i = \psi_i$ for all i. That is, $m_i(X; s(Y;Z)) = s_i(m(X;Y); m(X;Z))$ for all i.

Now if $a, b, c \in W(A)$ (or $W_l(A)$), where $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots)$, and $c = (c_0, c_1, \ldots)$, then

$$\begin{aligned} a \boxtimes (b \boxplus c) &= (m_0(a; s(b;c)), m_1(a; s(b;c)), \ldots) \\ &= (s_0(m(a;b); m(a;c)), s_1(m(a;b); m(a;c)), \ldots) \\ &= (a \boxtimes b) \boxplus (a \boxtimes c). \end{aligned}$$

This proves the left distributive law of $\boxtimes$ over $\boxplus$.

The polynomials needed for the remaining axioms are

$$\begin{aligned} &\text{additive inverses} : \phi(U) = -U, \\ &\text{associativity of } \boxplus : \phi(T,U,V) = (T+U)+V = T+(U+V), \\ &\text{associativity of } \boxtimes : \phi(T,U,V) = (TU)V = T(UV). \end{aligned}$$

The statement that the Witt polynomials are ring homomorphisms follows from equations (2.3), which define the addition and multiplication polynomials. □

This completes the main goal of this section. We need one additional tool related to Witt

vectors. The *Verschiebung*[‡] V is defined on $W(A)$ by

$$V(a_0, a_1, \ldots) = (0, a_0, a_1, \ldots)$$

and on $W_l(A)$ by

$$V(a_0, a_1, \ldots, a_{l-2}, a_{l-1}) = (0, a_0, a_1, \ldots, a_{l-2}).$$

The Verschiebung is not generally a ring endomorphism because it is not multiplicative. However, it is additive, as we now show.

Lemma 2.7. *The Verschiebung is a group homomorphism from the additive group of $W(A)$ (or $W_l(A)$) into itself.*

Proof. We will prove this in the universal case $A = \mathbb{Z}$. The result for a general ring A then follows. For $(a_0, a_1, a_2, \ldots) \in W(\mathbb{Z})$ (or $W_l(\mathbb{Z})$), consider the ghost component

$$\begin{aligned} w_n(V(a)) &= w_n(0, a_0, a_1, \ldots) \\ &= 0^{p^n} + p a_0^{p^{n-1}} + p^2 a_1^{p^{n-2}} + \cdots + p^n a_{n-1} \\ &= p\left(a_0^{p^{n-1}} + p a_1^{p^{n-2}} + \cdots + p^{n-1} a_{n-1}\right) \\ &= p w_{n-1}(a). \end{aligned}$$

Thus, for all $a, b \in W(\mathbb{Z})$,

$$\begin{aligned} w_n(V(a \boxplus b)) &= p w_{n-1}(a \boxplus b) \\ &= p(w_{n-1}(a) + w_{n-1}(b)) \\ &= p w_{n-1}(a) + p w_{n-1}(b) \\ &= w_n(V(a)) + w_n(V(b)) \\ &= w_n(V(a) \boxplus V(b)). \end{aligned}$$

Since this is true for all n, we may conclude $V(a \boxplus b)) = V(a) \boxplus V(b)$. □

[‡] "shift"

For $k > 0$, denote by V^k the composition of V with itself k times, which has the effect of shifting each Witt component k positions to the right. Define V^0 to be the identity map. It will be useful to express an arbitrary Witt vector as a sum of Witt vectors having at most one nonzero component. Recall that $W(A)$ is endowed with the inverse limit topology in which an infinite series converges if and only if its terms tend to zero.

Lemma 2.8. *If* $(a_0, a_1, \ldots) \in W(A)$, *then* $(a_0, a_1, \ldots) = \boxplus_{i=0}^{\infty} V^i(a_i, 0, 0, \ldots)$.

Proof. For $m = 0, 1, 2, \ldots$, consider the partial sum $\boxplus_{i=0}^{m} V^i(a_i, 0, 0, \ldots)$. Since the terms of the partial sum have disjoint support, it follows from Proposition 2.4 that, for all $m \geqslant n$, the first n components of $(a_0, a_1, \ldots)$ and $\boxplus_{i=0}^{m} V^i(a_i, 0, 0, \ldots)$ agree. Therefore, the series $\boxplus_{i=0}^{\infty} V^i(a_i, 0, 0, \ldots)$ converges to $(a_0, a_1, \ldots)$. □

2.2 The Artin-Hasse exponential series

In this section, we define the Artin-Hasse exponential series and prove some of its remarkable properties. While the eventual goal is to apply this to an algebra over a finite field of characteristic p, we will work here with formal power series in $\mathbb{Q}[\![X]\!]$. Recall the exponential series $\exp(X) \in \mathbb{Q}[\![X]\!]$ given by

$$\exp(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots.$$

This series satisfies the following familiar identity.

Proposition 2.9 (Exponential Law)**.** *If X and Y are commuting indeterminates, then*

$$\exp(X + Y) = \exp(X) \exp(Y).$$

Indeed, over a field of characteristic zero, exp is the unique solution of the functional equation

$$F(X + Y) = F(X)F(Y) \tag{2.7}$$

for which $F'(0) = 1$. (The standard proof from elementary calculus works here. See the discussion in Mattarei (2006).)

Of course, the coefficients of exp cannot generally be reduced modulo p. For our purposes, we would like an analog of the exponential series whose coefficients are p-integral, that is, rational numbers whose denominators are not divisible by p. Define the *(p-adic) Artin-Hasse exponential series* $E_p(X) \in \mathbb{Q}[\![X]\!]$ by

$$E_p(X) = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \frac{X^{p^3}}{p^3} + \cdots\right).$$

This remarkable series has its roots in a study of reciprocity laws by Artin and Hasse (1928), early in the development of class field theory. It is clear from the definition that E_p is a generalization of exp, but it seems rather unlikely that its coefficients are p-integral. In fact, they are.

Theorem 2.10. *The coefficients of the Artin-Hasse exponential series $E_p(X)$ are p-integral.*

There are several rather different ways to prove this surprising fact. We will give a group-theoretic proof, but first we mention another approach that may yield some additional insight.

This method is to express E_p as an infinite product of infinite series. The ordinary exponential series can be written as

$$\exp(X) = \prod_{n=1}^{\infty} (1 - X^n)^{-\mu(n)/n},$$

where μ is the Möbius function from number theory[§]. Now each factor is of the form

$$(1 - X^n)^{\alpha} = \sum_{i=0}^{\infty} \frac{\alpha(\alpha - 1) \cdots (\alpha - i + 1)}{i!} (-X^n)^i.$$

[§]That is, $\mu(1) = 1$ and for an integer $n > 1$, $\mu(n) = 0$ if n is divisible by a square and otherwise, $\mu(n) = (-1)^k$, where k is the number of distinct prime factors of n.

Since $\binom{\alpha}{i}$ is p-integral whenever α is, the problem factors are those for which the exponents $\alpha = -\mu(n)/n$ are not p-integral, that is, those for which $p \mid n$. If the problem factors are removed, it turns out that

$$\prod_{\substack{n=1 \\ p \nmid n}}^{\infty} (1 - X^n)^{-\mu(n)/n} = \exp\left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \frac{X^{p^3}}{p^3} + \cdots \right).$$

For a fuller treatment, see Koblitz (1984), Rabinoff (2007), and Robert (2000). Robert also gives a proof using the Dieudonné-Dwork criterion from number theory.

Happily, there is also group-theoretic approach, mentioned in Rabinoff (2007). This involves writing the coefficients in the series $E_p(X)$ in terms of numbers of p-elements of symmetric groups. For a positive integer n, denote by S_n the symmetric group on n letters. For a finite group G, denote by $\mathrm{Syl}_p(G)$ the set of all Sylow p-subgroups of G. Then $\left| \bigcup \mathrm{Syl}_p(S_n) \right|$ is the number of p-elements in the symmetric group on n letters.

Lemma 2.11. *For a prime p and indeterminate X,*

$$E_p(X) = 1 + \sum_{n=1}^{\infty} \frac{\left| \bigcup \mathrm{Syl}_p(S_n) \right|}{n!} X^n. \tag{2.8}$$

Proof. By the exponential law,

$$E_p(X) = \exp(X) \exp\left(\frac{X^p}{p}\right) \exp\left(\frac{X^{p^2}}{p^2}\right) \exp\left(\frac{X^{p^3}}{p^3}\right) \cdots.$$

When the right-hand side is expanded and like terms gathered, the coefficient of X^n, for $n \geqslant 1$, is

$$\sum_{n = k_0 + k_1 p + k_2 p^2 + \cdots} \frac{1}{(k_0!)\left(k_1! p^{k_1}\right)\left(k_2! p^{2k_2}\right) \cdots}, \tag{2.9}$$

where $\exp(X)$ contributes in each term factors of the form $\frac{1}{k_0!}$; $\exp\left(X^p/p\right)$ contributes factors of the form $\frac{1}{k_1! p^{k_1}}$; $\exp\left(X^{p^2}/p^2\right)$ contributes factors of the form $\frac{1}{k_2!(p^2)^{k_2}}$; and so on.

Next, we count the p-elements of S_n by conjugacy class. It is well known that elements in S_n are conjugate if and only if they have the same cycle structure. (See, for example,

Proposition 3.3 of Grove (1983).) Consider a p-element $\sigma \in S_n$ having the following cycle structure:

$$\begin{aligned} &k_0 \quad \text{fixed points,} \\ &k_1 \quad p\text{-cycles,} \\ &k_2 \quad p^2\text{-cycles,} \\ &\vdots \end{aligned}$$

To count the elements of S_n that are conjugate to σ, it suffices to count the elements that centralize σ, since $|\mathbf{cl}_{S_n}(\sigma)| = |S_n| / |\mathbf{C}_G(\sigma)|$, where $\mathbf{cl}_{S_n}(\sigma)$ denotes the conjugacy class and $\mathbf{C}_{S_n}(\sigma)$ denotes the centralizer in S_n of σ (Proposition 2.3 of Grove (1983)). Now $\mathbf{C}_{S_n}(\sigma)$ has a normal abelian subgroup that is the direct product of k_i cyclic groups of order p^i, for $i = 0, 1, 2, \ldots$. The factor group of $\mathbf{C}_{S_n}(\sigma)$ by this normal subgroup is isomorphic to the direct product of the symmetric groups on k_i symbols ($i = 0, 1, 2, \ldots$). Hence, $|\mathbf{C}_{S_n}(\sigma)| = (k_0!\, k_1!\, k_2! \cdots)\left(p^{k_1} p^{2k_2} p^{3k_3} \cdots\right)$. This means

$$\begin{aligned} \mathbf{cl}_{S_n}(\sigma) &= \frac{|S_n|}{|\mathbf{C}_{S_n}(\sigma)|} \\ &= \frac{n!}{(k_0!\, k_1!\, k_2! \cdots)\left(p^{k_1} p^{2k_2} p^{3k_3} \cdots\right)} \\ &= \frac{n!}{(k_0!)\left(k_1!\; p^{k_1}\right)\left(k_2!\; p^{2k_2}\right) \cdots}. \end{aligned}$$

Therefore, the number of p-elements in S_n is

$$\left|\bigcup \mathrm{Syl}_p(S_n)\right| = \sum_{n = k_0 + pk_1 + p^2 k_2 + \cdots} \frac{n!}{(k_0!)\left(k_1!\; p^{k_1}\right)\left(k_2!\; p^{2k_2}\right) \cdots}. \tag{2.10}$$

Putting equations (2.9) and (2.10) together, we conclude

$$\begin{aligned} E_p(X) &= 1 + \sum_{n=1}^{\infty} \left[\sum_{n = k_0 + k_1 p + k_2 p^2 + \cdots} \frac{1}{(k_0!)\left(k_1! p^{k_1}\right)\left(k_2! p^{2k_2}\right) \cdots} \right] X^n \\ &= 1 + \sum_{n=1}^{\infty} \left[\sum_{n = k_0 + k_1 p + k_2 p^2 + \cdots} \frac{n!}{(k_0!)\left(k_1! p^{k_1}\right)\left(k_2! p^{2k_2}\right) \cdots} \right] \frac{X^n}{n!} \\ &= 1 + \sum_{n=1}^{\infty} \frac{\left|\bigcup \mathrm{Syl}_p(S_n)\right|}{n!} X^n, \end{aligned}$$

as desired. □

Next, we state without proof a theorem of Frobenius. A very accessible proof is given by Isaacs and Robinson (1992). (In fact, we need only the special case where m is a power of a prime, which is Isaacs and Robinson's Theorem 4.)

Theorem 2.12 (Frobenius)**.** *If G is a finite group and m a positive integer dividing $|G|$, then m divides $|\{x \in G : x^m = 1\}|$.*

This puts in place everything needed to prove Theorem 2.10.

Proof of Theorem 2.10. By Frobenius's Theorem, the highest power of p dividing $|S_n| = n!$ also divides $\left|\bigcup \mathrm{Syl}_p(S_n)\right|$. Therefore, by Lemma 2.11, the coefficients of $E_p(X)$ are p-integral. □

As noted above, we cannot expect the Artin-Hasse exponential series to satisfy the functional equation (2.7). Nevertheless, let us proceed naïvely, computing both sides. To simplify notation, define the formal power series $G_p(X)$, for a prime p, by

$$G_p(X) = X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \cdots .$$

With this notation,

$$E_p(X) = \exp\left(G_p(X)\right).$$

Assume X and Y are commuting indeterminates. First,

$$\begin{aligned} E_p(X)E_p(Y) &= \exp\left(G_p(X)\right)\exp\left(G_p(Y)\right) \\ &= \exp\left(G_p(X) + G_p(Y)\right). \end{aligned}$$

Next,

$$E_p(X+Y) = \exp\left(G_p(X+Y)\right).$$

So we will compare $G_p(X) + G_p(Y)$ to $G_p(X+Y)$. We have

$$\begin{aligned} G_p(X) + G_p(Y) &= \left(X + \frac{X^p}{p} + \frac{X^{p^2}}{p^2} + \cdots\right) + \left(Y + \frac{Y^p}{p} + \frac{Y^{p^2}}{p^2} + \cdots\right) \\ &= X + Y + \frac{X^p}{p} + \frac{Y^p}{p} + \frac{X^{p^2}}{p^2} + \frac{Y^{p^2}}{p^2} + \cdots \\ &= (X+Y) + \frac{X^p + Y^p}{p} + \frac{X^{p^2} + Y^{p^2}}{p^2} + \cdots, \end{aligned}$$

while

$$G_p(X+Y) = (X+Y) + \frac{(X+Y)^p}{p} + \frac{(X+Y)^{p^2}}{p^2} + \cdots.$$

The degree-1 terms are equal, and so

$$E_p(X)E_p(Y) \equiv E_p(X+Y) \mod (X,Y)^p, \tag{2.11}$$

by which we mean that the expressions agree modulo a polynomial in X and Y of degree p or greater. Compute the difference of the terms of degree p to obtain

$$\frac{X^p + Y^p}{p} - \frac{(X+Y)^p}{p} = -\sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X^{p-i}Y^i. \tag{2.12}$$

Denote this expression by $S_1(X,Y)$ and use it to adjust the left-hand side of congruence (2.11) so that both sides agree through their terms of degree p. That is,

$$E_p(X)E_p(Y) \equiv E_p(X+Y)E_p(S_1(X,Y)) \mod (X,Y)^{p^2}.$$

We can repeat this procedure, introducing new factors to adjust for the terms of degree p^2, p^3, and so on. However, note that the expression on the left-hand side of (2.12) looks familiar. It appeared in equation (2.4), the formula for the first Witt addition vector. In fact, $S_1(X,Y)$ is precisely $s_1(X,0;Y,0)$. This is no accident; the pattern holds for the remaining terms if we define $S_k(X,Y) = s_k(X,0,\ldots,0;Y,0,\ldots,0)$ for all $k \geqslant 0$, yielding the following formula of Blache (2005).

Theorem 2.13 (Blache)**.** *If X and Y are commuting indeterminates, then*

$$E_p(X)E_p(Y) = \prod_{k\geqslant 0} E_p(S_k(X,Y)), \tag{2.13}$$

where $S_k(X,Y) = s_k(X,0,\dots,0;Y,0,\dots,0)$ for all $k \geqslant 0$. In particular, S_k is a homogeneous polynomial of degree p^k having integer coefficients.

Proof. By Corollary 2.3, s_k is an isobaric polynomial of weight p^k with integer coefficients. Therefore, $S_k(X,Y) = s_k(X,0,\dots,0;Y,0,\dots,0)$ is a homogeneous polynomial of degree p^k with integer coefficients. For $l \geqslant 0$, suppose $(X,X,\dots,X),(Y,Y,\dots,Y) \in W_{l+1}(\mathbb{Q}[\![X,Y]\!])$. Using Lemmas 2.7 and 2.8, we have

$$\begin{aligned}
(X,X,\dots,X)\boxplus(Y,Y,\dots,Y) &= \left(\boxplus_{k=0}^{l}\left(V^k(X,0,\dots,0)\right)\right)\boxplus\left(\boxplus_{k=0}^{l}\left(V^k(Y,0,\dots,0)\right)\right)\\
&= \boxplus_{k=0}^{l}\left(V^k(X,0,\dots,0)\boxplus V^k(Y,0,\dots,0)\right)\\
&= \boxplus_{k=0}^{l} V^k\left((X,0,\dots,0)\boxplus(Y,0,\dots,0)\right)\\
&= \boxplus_{k=0}^{l} V^k\left(s_0(X;Y),s_1(X,0;Y,0),\dots,s_l(X,0,\dots,0;Y,0,\dots,0)\right)\\
&= \boxplus_{k=0}^{l} V^k\left(S_0(X,Y),S_1(X,Y),\dots,S_l(X,Y)\right)\\
&= \boxplus_{k=0}^{l} V^k\left(\boxplus_{i=0}^{l} V^i(S_i(X,Y),0,\dots,0)\right)\\
&= \boxplus_{k=0}^{l}\boxplus_{i=0}^{l} V^{k+i}\left(S_i(X,Y),0,\dots,0\right)\\
&= \boxplus_{i=0}^{l} V^i\left(\boxplus_{k=0}^{l} V^k(S_i(X,Y),0,\dots,0)\right)\\
&= \boxplus_{i=0}^{l} V^i\left(S_i(X,Y),S_i(X,Y),\dots,S_i(X,Y)\right).
\end{aligned} \tag{2.14}$$

For any $i = 0, \ldots, l$,

$$\begin{aligned} w_l\left(V^i\left(S_i(X,Y), S_i(X,Y), \ldots, S_i(X,Y)\right)\right) &= w_l\left((0, \ldots, 0, S_i(X,Y), \ldots, S_i(X,Y))\right) \\ &= p^i S_i(X,Y)^{p^{l-i}} + p^{i+1} S_i(X,Y)^{p^{l-i-1}} + \cdots + p^l S_i(X,Y) \\ &= p^l \sum_{j=0}^{l-i} \frac{S_i(X,Y)^{p^j}}{p^j}. \end{aligned}$$

Apply w_l to each side of equation (2.14), using the fact that w_l is a ring homomorphism. The left-hand side is

$$\begin{aligned} w_l\left((X, \ldots, X) \boxplus (Y, \ldots, Y)\right) &= w_l\left((X, \ldots, X)\right) + w_l\left((Y, \ldots, Y)\right) \\ &= p^l \sum_{j=0}^{l} \frac{X^{p^j}}{p^j} + p^l \sum_{j=0}^{l} \frac{Y^{p^j}}{p^j} \end{aligned}$$

The right-hand side is

$$\begin{aligned} w_l\left(\boxplus_{i=0}^{l} V^i\left(S_i(X,Y), \ldots, S_i(X,Y)\right)\right) &= \sum_{i=0}^{l} w_l\left(V^i\left(S_i(X,Y), \ldots, S_i(X,Y)\right)\right) \\ &= \sum_{i=0}^{l} \left(p^l \sum_{j=0}^{l-i} \frac{S_i(X,Y)^{p^j}}{p^j}\right). \end{aligned}$$

Dividing both sides by p^l yields

$$\sum_{j=0}^{l} \frac{X^{p^j}}{p^j} + \sum_{j=0}^{l} \frac{Y^{p^j}}{p^j} = \sum_{i=0}^{l} \sum_{j=0}^{l-i} \frac{S_i(X,Y)^{p^j}}{p^j}.$$

It follows that, for all l,

$$G_p(X) + G_p(Y) \equiv \sum_{i=0}^{l} G_p\left(S_i(X,Y)\right) \mod (X,Y)^{p^{l+1}}.$$

Allow l to grow to infinity to obtain

$$G_p(X) + G_p(Y) = \sum_{i=0}^{\infty} G_p\left(S_i(X,Y)\right).$$

Finally, apply exp to each side and use the exponential law to conclude

$$\begin{aligned}
\exp\left(G_p(X) + G_p(Y)\right) &= \exp\left(\sum_{i\geqslant 0} G_p\left(S_i(X,Y)\right)\right), \\
\exp\left(G_p(X)\right)\exp\left(G_p(Y)\right) &= \prod_{i\geqslant 0} \exp\left(G_p\left(S_i(X,Y)\right)\right), \\
E_p(X)E_p(Y) &= \prod_{i\geqslant 0} E_p(S_i(X,Y)),
\end{aligned}$$

as desired. □

CHAPTER 3

SUBGROUPS DEFINED BY THE ARTIN-HASSE EXPONENTIAL SERIES

In this chapter, we return to algebra groups to define analogs of F-exponent subgroups and exponentially closed subgroups for the Artin-Hasse exponential series and to develop some of their properties. We continue the notational conventions of Chapter 1. That is, F is a field of characteristic p and order q; R is a finite-dimensional associative F-algebra; $J = J(R)$ the Jacobson radical of R; and $G = 1 + J$.

3.1 The set $E_p(Fx)$ and the subgroup $\mathcal{E}_p^F(x)$

First, for $x \in J$, define the set

$$E_p(Fx) = \left\{ E_p(\alpha x) : \alpha \in F \right\}.$$

Notice that if $x^p = 0$, then $E_p(Fx) = \exp(Fx)$. However, $E_p(Fx)$ need not be a group in general. We next prove three lemmas that will be used frequently in what follows.

Lemma 3.1. *Distinct sets of the form $E_p(Fx)$ intersect trivially.*

Proof. We first show that E_p is a bijection. Recall that $E_p(x) = \exp(G(x))$ where $G(x) = x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots$. It is well known that a formal power series with constant term 0 has an inverse with respect to function composition if and only if its linear coefficient is invertible. (See Theorem 1 of VI.1.3 of (Robert, 2000).) Therefore, G is invertible with respect to function composition. Since the exponential function is also invertible, their composite is as well. Hence, E_p is a bijection.

Now suppose $x, y \in J$ and $g \in E_p(Fx) \cap E_p(Fy)$ for some $g \neq 1$. Then $g = E_p(\alpha x) = E_p(\beta y)$ for some $\alpha, \beta \in F$ with $\alpha, \beta \neq 0$. Since E_p is injective, this implies $\alpha x = \beta y$, that is, $x = \frac{\beta}{\alpha} y$. We conclude $E_p(Fx) = E_p(Fy)$. □

Lemma 3.2. *If $x \in J$, then the map $F^n \to 1 + J$ given by*

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \mapsto E_p(\alpha_1 x)E_p(\alpha_2 x^2) \cdots E_p(\alpha_n x^n)$$

is one-to-one. It follows that

$$\left|E_p(Fx)E_p(Fx^2) \cdots E_p(Fx^n)\right| = q^n,$$

and more generally,

$$\left|E_p(Fx^{e_1})E_p(Fx^{e_2}) \cdots E_p(Fx^{e_n})\right| = q^n,$$

where $|F| = q$ and $0 < e_1 < e_2 < \cdots < e_n$.

Proof. Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n \in F$ such that

$$E_p(\alpha_1 x)E_p(\alpha_2 x^2) \cdots E_p(\alpha_n x^n) = E_p(\beta_1 x)E_p(\beta_2 x^2) \cdots E_p(\beta_n x^n). \tag{3.1}$$

That is,

$$1 + \alpha_1 x + w_1 = 1 + \beta_1 x + w_2,$$

for some $w_1, w_2 \in x^2 F[x]$. It follows that $\alpha_1 = \beta_1$. Multiplying both sides of equation (3.1) by $E_p(\alpha_1 x)^{-1} = E_p(\beta_1 x)^{-1}$, we obtain

$$E_p(\alpha_2 x^2) \cdots E_p(\alpha_n x^n) = E_p(\beta_2 x^2) \cdots E_p(\beta_n x^n).$$

Repeating the same argument, we conclude $\alpha_2 = \beta_2$, $\alpha_3 = \beta_3$, and so on. The result follows. □

Lemma 3.3. *Let $x \in J$. For all $r \geqslant 1$, if $\alpha_1, \alpha_2, \ldots, \alpha_r \in F$ with $\alpha_1 \neq 0$, then the vector $\alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_r x^r$ generates the same F-algebra as x.*

Proof. Without loss of generality, assume $x^{r+1} = 0$. To enable us to write the powers more easily, we will use double subscripts for the coefficients. Set

$$w = \alpha_{1,1} x + \alpha_{1,2} x^2 + \cdots + \alpha_{1,r-1} x^{r-1} + \alpha_{1,r} x^r,$$

where $\alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{1,r} \in F$ with $\alpha_{1,1} \neq 0$. Since $w \in xF[x]$ (the F-algebra generated by x), we have $wF[w] \subseteq xF[x]$. We now show the reverse inclusion. Consider the triangular system

$$\begin{aligned}
w &= \alpha_{1,1}x + \alpha_{1,2}x^2 + \cdots + \alpha_{1,r-1}x^{r-1} + \alpha_{1,r}x^r, \\
w^2 &= \alpha_{2,2}x^2 + \cdots + \alpha_{2,r-1}x^{r-1} + \alpha_{2,r}x^r, \\
&\vdots \qquad\qquad \ddots \qquad \vdots \qquad\qquad \vdots \\
w^{r-1} &= \alpha_{r-1,r-1}x^{r-1} + \alpha_{r-1,r}x^r, \\
w^r &= \alpha_{r,r}x^r,
\end{aligned}$$

where $\alpha_{i,j} \in F$ for all $1 \leqslant i \leqslant j \leqslant r$. Since $\alpha_{1,1} \neq 0$, we have $\alpha_{i,i} \neq 0$ for all i. From the last row we get $x^r \in wF[w]$. Using the second-to-last row, this implies

$$w^{r-1} - \alpha_{r-1,r}x^r = \alpha_{r-1,r-1}x^{r-1} \in wF[w],$$

and so $x^{r-1} \in wF[w]$. Continue working from the bottom up in this manner to obtain $x^{r-2}, \ldots, x^2, x \in wF[w]$. Therefore, $xF[x] \subseteq wF[w]$, and so equality holds. □

While $\exp(Fx)$ is a subgroup of $1 + J$ whenever it is defined (that is, when $x^p = 0$), the set $E_p(Fx)$ is not generally big enough to be closed under multiplication. We now define a larger set that is. For $x \in J$ with $x^{p^{l+1}} = 0$, define the set $\mathcal{E}_p^F(x)$ by

$$\begin{aligned}
\mathcal{E}_p^F(x) &= E_p(Fx)\, E_p(Fx^p) \cdots E_p\left(Fx^{p^l}\right) \\
&= \left\{ E_p(\alpha_0 x)\, E_p(\alpha_1 x^p) \cdots E_p\left(\alpha_l x^{p^l}\right) : \alpha_0, \ldots, \alpha_l \in F \right\}.
\end{aligned}$$

Our next goal is to show $\mathcal{E}_p^F(x)$ is a strong subgroup of $G = 1 + J$. We begin with a technical lemma about products of elements of the set $E_p\left(Fx^{p^k}\right)$ for a fixed k.

Lemma 3.4. *Suppose $x \in J$ with $x^{p^{l+1}} = 0$. Fix $0 \leqslant k \leqslant l$. For all $r \geqslant 1$, if $\gamma_1, \gamma_2, \ldots, \gamma_r \in F$, then*

$$E_p\left(\gamma_1 x^{p^k}\right) E_p\left(\gamma_2 x^{p^k}\right) \cdots E_p\left(\gamma_r x^{p^k}\right) = E_p\left(\pi x^{p^k}\right) \Theta(x),$$

where $\pi \in F$ and $\Theta(x)$ is a product such that each factor is of the form $E_p\left(\delta x^{p^m}\right)$ for some $m > k$ and $\delta \in F$.

Note that in the factors of $\Theta(x)$, the m varies, but there may be more than one factor for a given value of m. We will call a product such as $\Theta(x)$ a *product of higher p-power-degree factors* when the meaning is clear from the context. It will be evident from the proof that $\pi = \sum \gamma_i$, although we will not need this fact.

Proof. Proceed by induction on r, taking the base case to be $r = 2$. By Blache's formula (Theorem 2.13),

$$E_p\left(\gamma_1 x^{p^k}\right) E_p\left(\gamma_2 x^{p^k}\right) = \prod_{i=0}^{\infty} E_p\left(S_i\left(\gamma_1 x^{p^k}, \gamma_2 x^{p^k}\right)\right),$$

where $S_i(X, Y)$ is a homogeneous polynomial of degree p^i with integer coefficients. Thus, the n-th term of $S_i\left(\gamma_1 x^{p^k}, \gamma_2 x^{p^k}\right)$ is of the form

$$c_n\left(\gamma_1 x^{p^k}\right)^{p^i - n}\left(\gamma_2 x^{p^k}\right)^n = c_n \gamma_1^{p^i-n} \gamma_2^n x^{p^k(p^i-n)} x^{p^k n} = c_n \gamma_1^{p^i-n} \gamma_2^n x^{p^{k+i}},$$

for some integer c_n. Add these to obtain $S_i\left(\gamma_1 x^{p^k}, \gamma_2 x^{p^k}\right) = \pi_{k+i} x^{p^{k+i}}$ for some $\pi_{k+i} \in F$. Hence,

$$\begin{aligned} E_p\left(\gamma_1 x^{p^k}\right) E_p\left(\gamma_2 x^{p^k}\right) &= \prod_{i=0}^{\infty} E_p\left(\pi_{k+i} x^{p^{k+i}}\right) \\ &= \prod_{i=0}^{l-k} E_p\left(\pi_{k+i} x^{p^{k+i}}\right) \qquad (\text{since } x^{p^{l+1}} = 0) \\ &= E_p\left(\pi_k x^{p^k}\right) \prod_{i=1}^{l-k} E_p\left(\pi_{k+i} x^{p^{k+i}}\right), \end{aligned}$$

as desired. This proves the base step of the induction.

Next, suppose the result holds for any product of $r-1$ factors from $E_p\left(Fx^k\right)$. Let $\gamma_1, \ldots, \gamma_r \in F$. By the inductive hypothesis, there exist $\hat{\pi} \in F$ and $\hat{\Theta}(x)$, a product of higher p-power-degree factors, so that

$$E_p\left(\gamma_1 x^{p^k}\right) \cdots E_p\left(\gamma_{r-1} x^{p^k}\right) E_p\left(\gamma_r x^{p^k}\right) = \left(E_p\left(\hat{\pi} x^{p^k}\right) \hat{\Theta}(x)\right) E_p\left(\gamma_r x^{p^k}\right).$$

Rearrange the right-hand side and apply the base step to conclude

$$\begin{aligned} E_p\left(\gamma_1 x^{p^k}\right)\cdots E_p\left(\gamma_{r-1}x^{p^k}\right)E_p\left(\gamma_r x^{p^k}\right) &= \left(E_p\left(\hat{\pi}x^{p^k}\right)E_p\left(\gamma_r x^{p^k}\right)\right)\hat{\Theta}(x) \\ &= E_p\left(\pi x^{p^k}\right)\tilde{\Theta}(x)\hat{\Theta}(x), \end{aligned}$$

for some $\pi \in F$ and product of higher p-power-degree factors $\tilde{\Theta}(x)$. Set $\Theta(x) = \tilde{\Theta}(x)\hat{\Theta}(x)$ to complete the proof. □

Theorem 3.5. *If $x \in J$ with $x^{p^{l+1}} = 0$ but $x^{p^l} \neq 0$, then $\mathcal{E}_p^F(x)$ is a strong subgroup of $G = 1 + J$ of order q^{l+1}.*

Proof. We begin by noting that $\left|\mathcal{E}_p^F(x)\right| = q^{l+1}$ by Lemma 3.2. We next show that $\mathcal{E}_p^F(x)$ is closed under multiplication. Let $g, h \in \mathcal{E}_p^F(x)$ be arbitrary, say

$$\begin{aligned} g &= E_p(\alpha_0 x)\,E_p(\alpha_1 x^p)\cdots E_p\left(\alpha_l x^{p^l}\right) \qquad \text{and} \\ h &= E_p(\beta_0 x)\,E_p(\beta_1 x^p)\cdots E_p\left(\beta_l x^{p^l}\right), \end{aligned}$$

where $\alpha_0, \ldots, \alpha_l, \beta_0, \ldots, \beta_l \in F$. Then we have

$$\begin{aligned} gh &= \left(E_p(\alpha_0 x)\,E_p(\alpha_1 x^p)\cdots E_p\left(\alpha_l x^{p^l}\right)\right)\cdot\left(E_p(\beta_0 x)\,E_p(\beta_1 x^p)\cdots E_p\left(\beta_l x^{p^l}\right)\right) \\ &= \left(E_p(\alpha_0 x)\,E_p(\beta_0 x)\right)\cdot\left(E_p(\alpha_1 x^p)\,E_p(\beta_1 x^p)\right)\cdots\left(E_p\left(\alpha_l x^{p^l}\right)E_p\left(\beta_l x^{p^l}\right)\right). \end{aligned}$$

First apply Lemma 3.4 to the leftmost product $E_p(\alpha_0 x)\,E_p(\beta_0 x)$ to obtain $E_p(\pi_0 x)\,\Theta_0(x)$, where $\pi_0 \in F$ and $\Theta_0(x)$ is a product of higher p-power-degree factors. Now there are at least three factors of the form $E_p(\delta x^p)$. Apply Lemma 3.4 to these to obtain $E_p(\pi_1 x^p)\,\Theta_1(x)$, where $\pi_1 \in F$ and $\Theta_1(x)$ is a product of higher p-power-degree factors. Continue in this fashion from left to right. The process terminates after finitely many steps since $x^{p^{l+1}} = 0$. We then have $\pi_0, \ldots, \pi_l \in F$ for which

$$gh = E_p(\pi_0 x)\,E_p(\pi_1 x^p)\cdots E_p\left(\pi_l x^{p^l}\right) \in \mathcal{E}_p^F(x).$$

Thus, the set $\mathcal{E}_p^F(x)$ is closed under multiplication.

Suppose $g \in \mathcal{E}_p^F(x)$. Since G is a finite group, $g^{-1} = g^n$ for some positive integer n. But since $\mathcal{E}_p^F(x)$ is closed under multiplication, $g^n \in \mathcal{E}_p^F(x)$. Therefore, $\mathcal{E}_p^F(x)$ is a subgroup of G.

Finally, to show $\mathcal{E}_p^F(x)$ is strong, we must show that $\left|\mathcal{E}_p^F(x) \cap K\right|$ is a q-power for all algebra subgroups K of G. Let A be a subalgebra of J such that $\mathcal{E}_p^F(x) \cap 1 + A \neq 1$. If

$$1 \neq g = E_p(\alpha_0 x)\, E_p(\alpha_1 x^p) \cdots E_p\left(\alpha_l x^{p^l}\right) \in 1 + A,$$

then there is some $i \in \{0, \ldots, l\}$ and $w \in x^{p^i+1}F[x]$ such that $g = 1 + \alpha_i x^{p^i} + w$ and $\alpha_i \neq 0$. Choose g so i is minimal. By Lemma 3.3, the F-algebra generated by $\alpha_i x^{p^i} + w$ is $x^{p^i}F[x]$. Thus, $1 + x^{p^i}F[x] \subseteq 1 + A$. Hence,

$$\mathcal{E}_p^F(x) \cap 1 + A = E_p\left(Fx^{p^i}\right) E_p\left(Fx^{p^{i+1}}\right) \cdots E_p\left(Fx^{p^l}\right) = \mathcal{E}_p^F\left(x^{p^i}\right).$$

By Lemma 3.2, $\left|\mathcal{E}_p^F\left(x^{p^i}\right)\right| = q^{l-i+1}$. Therefore, for all algebra subgroups K, either $\left|\mathcal{E}_p^F(x) \cap K\right| = q^{l-i+1}$, for some $0 \leqslant i \leqslant l$, or $\left|\mathcal{E}_p^F(x) \cap K\right| = 1$. That is, $\mathcal{E}_p^F(x)$ is strong. □

3.2 Artin-Hasse-exponentially closed subgroups

Next we define an analog of exponential closure for the Artin-Hasse exponential function. A subset $H \subseteq G$ is said to be *Artin-Hasse-exponentially closed*, abbreviated *AH-closed*, if $E_p(\gamma x) \in H$ for all $\gamma \in F$ whenever $E_p(x) \in H$. First, we make the following easy observation.

Proposition 3.6. *Intersections of AH-closed subgroups are AH-closed.*

Proof. Let $H, K \leqslant G$ be AH-closed. Suppose $g \in H \cap K$, say $g = E_p(x)$. Then $E_p(Fx) \subseteq H$ and $E_p(Fx) \subseteq K$, since both are AH-closed. Therefore, $E_p(Fx) \subseteq H \cap K$, implying $H \cap K$ is AH-closed. □

The next two results show how AH-closed subgroups relate to strong subgroups and to algebra subgroups.

Proposition 3.7. *Algebra subgroups are AH-closed.*

Proof. Let $K = 1 + A$ be an algebra subgroup of G. If $g \in K$, then there is some $x \in A$ such that $g = E_p(x)$. Write $g = E_p(x) = 1 + x + w$, where $w \in x^2F[x]$. By Lemma 3.3, the algebra generated by $\alpha x + \hat{w}$ is the same as the algebra generated by $x + w$ for all $\alpha \in F$ and $\hat{w} \in x^2F[x]$. This means $E_p(x) \in K$ implies $E_p(\alpha x) \in K$ for all $\alpha \in F$. That is, K is AH-closed. □

Proposition 3.8. *AH-closed subgroups are strong.*

Proof. By Propositions 3.7 and 3.6, the intersection of an AH-closed subgroup with an algebra subgroup is itself AH-closed. Therefore, it suffices to show AH-closed subgroups have q-power order. Let H be AH-closed. By Lemma 3.1, $|H| - 1$ is a multiple of $q - 1$. But H is a p-group, say $|H| = p^b$. If $q = p^a$, then this means $(p^a - 1) \mid \left(p^b - 1\right)$. By a well-known result, this occurs only if $a \mid b$. In other words, $p^b = |H|$ is a power of $p^a = q$. □

Unfortunately, $\mathcal{E}_p^F(x)$ is AH-closed only in some cases. For example, if $x^p = 0$, then $\mathcal{E}_p^F(x) = E_p(Fx) = \exp(Fx)$, which is exponentially closed, hence AH-closed. We can say a bit more. First we prove some identities in characteristic zero, where we may use the exponential law freely.

Lemma 3.9. *Let J be a nilpotent algebra over $\mathbb{Q}$. If $x \in J$ with $x^{2p} = 0$, then for all $a, b, c \in \mathbb{Q}$,*

(a) $E_p(ax)\, E_p(bx^p) = E_p\left(ax + bx^p - a^{p-1}bx^{2p-1}\right)$;

(b) $E_p\left(c\left(ax + bx^p - a^{p-1}bx^{2p-1}\right)\right) = E_p(cax)\, E_p(cbx^p)\, E_p\left(\left(c^p - c\right)a^{p-1}bx^{2p-1}\right)$.

Proof. Note that $x^{p^2} = 0$ since $p^2 \geqslant 2p$ for all primes p. For the second identity, we compute

$$\begin{aligned}
&E_p\left(c\left(ax + bx^p - a^{p-1}bx^{2p-1}\right)\right) \\
&\qquad = E_p\left(cax + cbx^p - ca^{p-1}bx^{2p-1}\right) \\
&\qquad = \exp\left(cax + cbx^p - ca^{p-1}bx^{2p-1} + \frac{\left(cax + cbx^p - ca^{p-1}bx^{2p-1}\right)^p}{p}\right) \\
&\qquad = \exp\left(cax + cbx^p - ca^{p-1}bx^{2p-1} + \frac{(cax)^p + p(cax)^{p-1}cbx^p}{p}\right) \\
&\qquad = \exp\left(cax + cbx^p - ca^{p-1}bx^{2p-1} + \frac{(ca)^p x^p}{p} + (ca)^{p-1}cbx^{2p-1}\right) \\
&\qquad = \exp\left(cax + \frac{(ca)^p x^p}{p} + cbx^p - ca^{p-1}bx^{2p-1} + c^p a^{p-1}bx^{2p-1}\right) \\
&\qquad = \exp\left(cax + \frac{(ca)^p x^p}{p} + cbx^p + \left(c^p - c\right)a^{p-1}bx^{2p-1}\right) \\
&\qquad = \exp\left(cax + \frac{(ca)^p x^p}{p}\right)\exp\left(cbx^p\right)\exp\left(\left(c^p - c\right)a^{p-1}bx^{2p-1}\right) \\
&\qquad = E_p\left(cax\right)E_p\left(cbx^p\right)E_p\left(\left(c^p - c\right)a^{p-1}bx^{2p-1}\right).
\end{aligned}$$

The first identity follows from the second by setting $c = 1$. □

Proposition 3.10. *Let J be a nilpotent algebra over a field F of characteristic p. For $x \in J$, the subgroup $\mathcal{E}_p^F(x)$ is AH-closed if $x^{2p-1} = 0$, but counter-examples exist otherwise.*

Proof. We wish to determine whether $E_p(\gamma y) \in \mathcal{E}_p^F(x)$ for an arbitrary element $E_p(y) \in \mathcal{E}_p^F(x)$ and $\gamma \in F$. If $x^{2p} = 0$, then $\mathcal{E}_p^F(x) = E_p(Fx)E_p\left(Fx^p\right)$. Thus, a typical element g of $\mathcal{E}_p^F(x)$ is of the form

$$g = E_p(\alpha x)E_p\left(\beta x^p\right) = E_p\left(\alpha x + \beta x^p - \alpha^{p-1}\beta x^{2p-1}\right),$$

for some $\alpha, \beta \in F$, by identity (a) of Lemma 3.9.

First suppose $x^{2p-1} = 0$. In this case, $g = E_p\left(\alpha x + \beta x^p\right)$. For arbitrary $\gamma \in F$,

$$E_p\left(\gamma\left(\alpha x + \beta x^p\right)\right) = E_p\left(\gamma\alpha x\right)E_p\left(\gamma\beta x^p\right) \in \mathcal{E}_p^F(x),$$

by identity (b) of Lemma 3.9. This proves $\mathcal{E}_p^F(x)$ is AH-closed whenever $x^{2p-1} = 0$.

Now suppose $x^{2p} = 0$ but $x^{2p-1} \neq 0$. Then again by identity (b) of Lemma 3.9, for $\gamma \in F$,

$$E_p\left(\gamma\left(\alpha x + \beta x^p - \alpha^{p-1}\beta x^{2p-1}\right)\right) = E_p\left(\gamma\alpha x\right) E_p\left(\gamma\beta x^p\right) E_p\left(\left(\gamma^p - \gamma\right)\alpha^{p-1}\beta x^{2p-1}\right).$$

By Lemma 3.2, this is not in $\mathcal{E}_p^F(x)$ for arbitrary α and β unless $\gamma^p - \gamma = 0$. Now $\gamma^p - \gamma = 0$ if and only if $\gamma \in \mathbb{F}_p$, where $\mathbb{F}_p$ denotes the field of p elements. This shows $\mathcal{E}_p^F(x)$ is not AH-closed if $x^{2p-1} \neq 0$ and F is larger than $\mathbb{F}_p$. □

CHAPTER 4

NORMALIZERS OF ALGEBRA SUBGROUPS

In this chapter, we determine when normalizers of algebra subgroups are strong. In §4.1, we use the exponential series to prove that normalizers of algebra subgroups are strong when $J^p = 0$. In §4.2, we use the Artin-Hasse exponential series to prove this result when $J^{p+1} = 0$ and to construct counter-examples otherwise. Of course, the result of §4.2 supersedes the result of §4.1, but we include the former to illustrate the method to be generalized.

4.1 When $J^p = 0$: the exponential series

If $J^p = 0$, we can use the ordinary exponential series to show normalizers of algebra subgroups are strong.* Let $H = 1 + S$ be an algebra subgroup of G. (So $\exp S = H$.) We wish to show $\mathbf{N}_G(H)$ is exponentially closed. That is, we wish to show if $\exp(x) \in \mathbf{N}_G(H)$, then $\exp(\alpha x) \in \mathbf{N}_G(H)$ for all $\alpha \in F$.

We put a Lie algebra structure on J by defining the Lie bracket $[\cdot,\cdot]\colon J \times J \to J$ by $[x, y] = xy - yx$ for $x, y \in J$. We adopt the convention that omitted brackets are right-justified, so $[x_1, \ldots, x_{l-1}, x_l]$ is understood to mean $[x_1, [x_2, [\ldots, [x_{l-2}, [x_{l-1}, x_l]] \cdots]$. For $x \in J$, the operator of Lie multiplication by x is denoted $\operatorname{ad} x$. That is, $\operatorname{ad} x(y) = [x, y]$ for $y \in J$. Notice that if $J^p = 0$, then $(\operatorname{ad} x)^{p-1} = 0$. For a subalgebra S of J, denote by $\mathbf{N}_J(S)$ the *Lie normalizer in J of S*, that is, $\mathbf{N}_J(S) = \{y \in J\colon [S, y] \subseteq S\}$. Recall that $\mathbf{N}_J(S)$ is a Lie subalgebra of J, thanks to the Jacobi Identity†.

The following identity is the key to proving the main result of this section.

*The author is grateful to the anonymous referee of a paper on this topic for suggesting the approach taken in this section.

†$[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0$

Lemma 4.1. *If $J^p = 0$, then $y^{(\exp x)^{-1}} = \exp(\operatorname{ad} x)(y)$ for all $x, y \in J$.*

Proof. Suppose $x, y \in J$. Expand the left-hand side to obtain

$$\begin{aligned} y^{(\exp x)^{-1}} &= y^{\exp(-x)} \\ &= \exp(x) y \exp(-x) \\ &= \left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{p-1}}{(p-1)!}\right) y \left(1 - x + \frac{x^2}{2!} - \cdots + \frac{(-1)^{p-1} x^{p-1}}{(p-1)!}\right) \\ &= y + xy - yx + \cdots \\ &= y + [x, y] + \cdots, \end{aligned}$$

where the dots represent terms of degree three or greater (to be specified below). Next expand the right-hand side to obtain

$$\begin{aligned} \exp(\operatorname{ad} x)(y) &= \left(I + \operatorname{ad} x + \frac{(\operatorname{ad} x)^2}{2!} + \cdots + \frac{(\operatorname{ad} x)^{p-2}}{(p-2)!}\right)(y) \\ &= I(y) + \operatorname{ad} x(y) + \frac{(\operatorname{ad} x)^2(y)}{2!} + \cdots + \frac{(\operatorname{ad} x)^{p-2}(y)}{(p-2)!} \\ &= y + [x, y] + \frac{[x, x, y]}{2!} + \cdots + \frac{[x, \cdots, x, y]}{(p-2)!}. \end{aligned}$$

It is easy to see that the left- and right-hand sides agree through the terms of degree two. Let us show by induction that the higher-degree terms agree as well. The terms of degree $n+1$ on the left-hand side are

$$\sum_{\substack{i,j \\ i+j=n}} \frac{x^i}{i!} y \frac{(-1)^j x^j}{j!} = \sum_{j=0}^{n} (-1)^j \frac{x^{n-j} y x^j}{(n-j)!\, j!}.$$

Using the inductive hypothesis, the terms of degree $n+1$ on the right-hand side are

$$\begin{aligned}
\frac{[\overbrace{x,\dots,x}^{n},y]}{(n)!} &= \left[\frac{x}{n}, \frac{[\overbrace{x,\dots,x}^{n-1},y]}{(n-1)!}\right] \\
&= \left[\frac{x}{n}, \sum_{j=0}^{n-1}\frac{(-1)^j x^{n-1-j}yx^j}{(n-1-j)!j!}\right] \\
&= \frac{x}{n}\left(\sum_{j=0}^{n-1}\frac{(-1)^j x^{n-1-j}yx^j}{(n-1-j)!j!}\right) - \left(\sum_{k=0}^{n-1}\frac{(-1)^k x^{n-1-k}yx^k}{(n-1-k)!k!}\right)\frac{x}{n} \\
&= \sum_{j=0}^{n-1}\frac{(-1)^j x^{n-j}yx^j}{n(n-1-j)!j!} - \sum_{k=0}^{n-1}\frac{(-1)^k x^{n-1-k}yx^{k+1}}{n(n-1-k)!k!};
\end{aligned}$$

gathering like terms (when $j = k+1$),

$$\begin{aligned}
&= \frac{(-1)^0 y^n x}{n(n-1)!} + \sum_{j=1}^{n-1}\left(\frac{(-1)^j x^{n-j}yx^j}{n(n-1-j)!j!} - \frac{(-1)^{j-1}x^{n-j}yx^j}{n(n-j)!(j-1)!}\right) - \frac{(-1)^{n-1}xy^n}{n!} \\
&= \frac{y^n x}{n!} + \sum_{j=1}^{n-1}\left(\frac{(-1)^j x^{n-j}yx^j(n-j)}{n(n-j)(n-1-j)!j!} + \frac{(-1)^j x^{n-j}yx^j(j)}{n(n-j)!(j)(j-1)!}\right) + \frac{(-1)^n xy^n}{n!} \\
&= \frac{y^n x}{n!} + \left(\sum_{j=1}^{n-1}\frac{(-1)^j x^{n-j}yx^j(n-j+j)}{n(n-j)!j!}\right) + \frac{(-1)^n xy^n}{n!} \\
&= \frac{y^n x}{n!} + \left(\sum_{j=1}^{n-1}\frac{(-1)^j x^{n-j}yx^j}{(n-j)!j!}\right) + \frac{(-1)^n xy^n}{n!} \\
&= \sum_{j=0}^{n}\frac{(-1)^j x^{n-j}yx^j}{(n-j)!j!},
\end{aligned}$$

as desired. This proves the identity. □

Lemma 4.2. *Suppose $J^p = 0$. If $H = 1+S$ is an algebra subgroup of $1+J$, then $\mathbf{N}_G(H) = \exp \mathbf{N}_J(S)$.*

Proof. We begin by showing $\exp \mathbf{N}_J(S) \subseteq \mathbf{N}_G(H)$. If $x \in \mathbf{N}_J(S)$, then for all $y \in S$, we have $[x,y], [x,x,y], \dots, [\overbrace{x,\dots,x}^{p-2},y] \in S$. Since S is a subspace of J, this implies $\exp(\operatorname{ad} x)(y) \in S$. By Lemma 4.1, this means $y^{(\exp x)^{-1}} \in S$. Therefore, $(1+y)^{(\exp x)^{-1}} \in 1+S$. That is, $\exp x \in \mathbf{N}_G(H)$.

To show the reverse containment, let $y \in S$ and $g \in \mathbf{N}_G(H)$. Write $g = \exp x$ for some $x \in J$. (We wish to show $x \in \mathbf{N}_J(S)$.) Now $\exp(-x) = g^{-1} \in \mathbf{N}_G(H)$, and so $\exp(\operatorname{ad} x)(y) = y^{\exp(-x)} \in S$ (using Lemma 4.1 again). That is, S is stabilized by

$$\exp(\operatorname{ad} x) = I + \operatorname{ad} x + \frac{(\operatorname{ad} x)^2}{2!} + \cdots + \frac{(\operatorname{ad} x)^{p-2}}{(p-2)!}.$$

Consider the nilpotent algebra generated by $\operatorname{ad} x$ in $\operatorname{End}(J)$, the algebra of endomorphisms of J. By Lemma 3.3 , the algebra generated by $\operatorname{ad} x + \frac{(\operatorname{ad} x)^2}{2!} + \cdots + \frac{(\operatorname{ad} x)^{p-2}}{(p-2)!}$ is the same as the algebra generated by $\operatorname{ad} x$. Thus, $\operatorname{ad} x$ stabilizes S, which means $x \in \mathbf{N}_J(S)$. □

Theorem 4.3. *If $J^p = 0$, then normalizers of algebra subgroups are exponentially closed, hence strong.*

Proof. Suppose $H = \exp(S)$ is an algebra subgroup of G. If $g \in \mathbf{N}_G(H)$, then by Lemma 4.2, $g = \exp(x)$ for some $x \in \mathbf{N}_J(S)$. For $\alpha \in F$, $\alpha x \in \mathbf{N}_J(S)$ since $\mathbf{N}_J(S)$ is a Lie algebra. It follows that $\exp(\alpha x) \in \mathbf{N}_G(H)$. Therefore, $\mathbf{N}_G(H)$ is exponentially closed, as desired. □

In fact, Theorem 4.3 will be superseded by Theorem 4.5 below. However, we show the details for the case $J^p = 0$ using the exponential map because we would like to mimic this proof for the general case using the Artin-Hasse exponential map. Unfortunately, we will succeed in generalizing the result only to $J^{p+1} = 0$; our methods will yield counter-examples otherwise.

4.2 When $J^p \neq 0$: the Artin-Hasse exponential series

We wish to define an operator, say $\operatorname{had} x$, that plays the same role for the Artin-Hasse exponential that $\operatorname{ad} x$ plays for the ordinary exponential map when conjugating. Specifically, for $x, y \in J$, we would like $\operatorname{had} x$ to satisfy the following analog of the identity from Lemma 4.1:

$$y^{E_p(x)^{-1}} = E_p(\operatorname{had} x)(y). \tag{4.1}$$

To develop the identities needed to compute had x, we temporarily work in a field of characteristic zero. Computing the left-hand side of equation (4.1), we have

$$\begin{aligned} y^{E_p(x)^{-1}} &= E_p(x)\, y\, E_p(x)^{-1} \\ &= \exp\left(x + \frac{x^p}{p} + \cdots\right) y \exp\left(x + \frac{x^p}{p} + \cdots\right)^{-1} \\ &= \exp\left(\operatorname{ad}\left(x + \frac{x^p}{p} + \cdots\right)\right)(y) \\ &= \exp\left(\operatorname{ad} x + \frac{\operatorname{ad} x^p}{p} + \cdots\right)(y). \end{aligned}$$

Thus, if we define ϑ_x by

$$E_p(\operatorname{ad} x + \vartheta_x) = \exp\left(\operatorname{ad} x + \frac{\operatorname{ad} x^p}{p} + \cdots\right), \tag{4.2}$$

then $\operatorname{had} x = \operatorname{ad} x + \vartheta_x$ is the operator we are looking for. Expanding the left-hand side of equation (4.2) yields

$$\exp\left((\operatorname{ad} x + \vartheta_x) + \frac{(\operatorname{ad} x + \vartheta_x)^p}{p} + \cdots\right) = \exp\left(\operatorname{ad} x + \frac{\operatorname{ad} x^p}{p} + \cdots\right).$$

Since exp is a bijection, this implies

$$(\operatorname{ad} x + \vartheta_x) + \frac{(\operatorname{ad} x + \vartheta_x)^p}{p} + \cdots = \operatorname{ad} x + \frac{\operatorname{ad} x^p}{p} + \cdots. \tag{4.3}$$

(Recall that $\operatorname{char} F = 0$ for now.) Note that ϑ_x has degree p in the sense that $\vartheta_x\left(J^i\right) \subseteq J^{i+p}$ for all i.

Let us now work out exactly what ϑ_x is when $J^{2p} = 0$. In this case, equation (4.3) reduces to

$$\operatorname{ad} x + \vartheta_x + \frac{(\operatorname{ad} x)^p}{p} = \operatorname{ad} x + \frac{\operatorname{ad} x^p}{p}.$$

Solving for ϑ_x, we obtain

$$\vartheta_x = \frac{\operatorname{ad} x^p}{p} - \frac{(\operatorname{ad} x)^p}{p}.$$

Let L_x, R_x denote left and right multiplication by x, respectively. Then $\operatorname{ad} x = L_x - R_x$ and so

$$\begin{aligned}\vartheta_x &= \frac{L_{x^p} - R_{x^p}}{p} - \frac{(L_x - R_x)^p}{p} \\ &= \frac{L_x^p - R_x^p - (L_x - R_x)^p}{p}.\end{aligned}$$

Therefore, if $J^{2p} = 0$,

$$\begin{aligned}\operatorname{had} x &= \operatorname{ad} x + \frac{L_x^p - R_x^p - (L_x - R_x)^p}{p} \\ &= L_x - R_x + \frac{L_x^p - R_x^p - (L_x - R_x)^p}{p}.\end{aligned} \tag{4.4}$$

This expression might look familiar. Indeed, if p is odd, then $(-R_x)^p = -R_x^p$ and so

$$\begin{aligned}\operatorname{had} x &= L_x - R_x + \frac{L_x^p - R_x^p - (L_x - R_x)^p}{p} \\ &= L_x + (-R_x) - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} L_x^{p-i}(-R_x)^i \\ &= s_1\left(L_x, L_x; -R_x, -R_x\right),\end{aligned}$$

where s_1 is the first Witt addition polynomial (equation (2.4)).

On the other hand, if $p = 2$, then formula 4.4 simplifies to

$$\begin{aligned}\operatorname{had} x &= L_x - R_x + \frac{L_x^2 - R_x^2 - (L_x - R_x)^2}{2} \\ &= L_x - R_x + \frac{L_x^2 - R_x^2 - (L_x^2 - 2L_xR_x + R_x^2)}{2} \\ &= L_x - R_x + \frac{2L_xR_x - 2R_x^2}{2} \\ &= L_x - R_x + L_xR_x - R_x^2.\end{aligned}$$

Now if $\alpha \in F$, then for any p,

$$\begin{aligned}
\vartheta_{\alpha x} &= \frac{L_{\alpha x}^p - R_{\alpha x}^p - (L_{\alpha x} - R_{\alpha x})^p}{p} \\
&= \frac{\alpha^p L_x^p - \alpha^p R_x^p - (\alpha L_x - \alpha R_x)^p}{p} \\
&= \frac{\alpha^p L_x^p - \alpha^p R_x^p - \alpha^p (L_x - R_x)^p}{p} \\
&= \alpha^p \left(\frac{L_x^p - R_x^p - (L_x - R_x)^p}{p} \right) \\
&= \alpha^p \vartheta_x.
\end{aligned}$$

While the above computations were carried out in characteristic zero, the resulting identities hold in any characteristic. We summarize in a lemma.

Lemma 4.4. *Suppose J is a finitely generated algebra over a field F of arbitrary characteristic p and that $J^{2p} = 0$.*

(a) If p is an odd prime, then $\operatorname{had} x = L_x - R_x - \sum_{i=1}^{p-1} (-1)^i \frac{1}{p} \binom{p}{i} L_x^{p-i} R_x^i$.

(b) If $p = 2$, then $\operatorname{had} x = L_x - R_x + L_x R_x - R_x^2$.

(c) For any prime p, if $\alpha \in F$, then $\operatorname{had}(\alpha x) = \alpha \operatorname{ad} x + \alpha^p \vartheta_x$.

Recall that identity (4.1), which defines $\operatorname{had} x$, means the element $E_p(x)$ normalizes $1 + S$ if and only if $E_p(\operatorname{ad} x + \vartheta_x)$ stabilizes S. But by Lemma 3.3, $E_p(\operatorname{ad} x + \vartheta_x)$ stabilizes S if and only if $\operatorname{ad} x + \vartheta_x$ stabilizes S. Unfortunately, ϑ_x is not linear in x and this is what can prevent normalizers from being AH-closed, as we now show. The theorem is stated as a result about normalizers of linear subspaces of J, which is a slightly more general setting than normalizers of algebra subgroups. Indeed, if $H = 1 + S$ is an algebra subgroup of $G = 1 + J$, then $\mathbf{N}_G(S) = \mathbf{N}_G(H)$, since $(1 + x)^g = 1 + x^g$ for all $x \in J$ and $g \in G$.

Theorem 4.5. *Let S be a linear subspace of J.*

(a) If $J^{p+1} = 0$, then $N_G(S)$ is AH-closed (hence strong).

(b) If $J^{p+1} \neq 0$, then examples exist for which $|N_G(S)| = p \cdot q^a$, and so $N_G(S)$ need not be strong.

Proof. For part (a), suppose $J^{p+1} = 0$ and S is a subspace of J. Let $E_p(x) \in \mathbf{N}_G(S)$. By the discussion following Lemma 4.4, this occurs if and only if $\operatorname{ad} x + \vartheta_x$ stabilizes S. But since ϑ_x has degree p and $J^{p+1} = 0$, this occurs if and only if $\operatorname{ad} x$ stabilizes S. Let $\alpha \in F$ be arbitrary. We wish to determine whether $E_p(\alpha x) \in \mathbf{N}_G(S)$, so whether $\operatorname{ad}(\alpha x) + \vartheta_{\alpha x} = \operatorname{ad}(\alpha x) = \alpha \operatorname{ad} x$ stabilizes S. But S is a subspace of J, so $\alpha \operatorname{ad} x$ stabilizes S whenever $\operatorname{ad} x$ does. We conclude that $N_G(S)$ is AH-closed, hence strong.

For part (b), we construct a family of counter-examples showing normalizers of linear subspaces need not be strong when $J^{p+1} \neq 0$. If $\mathcal{J}$ is the free F-algebra on two generators, set $J = \mathcal{J}/\mathcal{J}^{p+2}$ and let x and y be the images in J of the two free generators. Since $\mathcal{J}$ is a graded algebra and $\mathcal{J}^{p+2}$ is generated by homogeneous elements, J is graded as well. Specifically, if J_n denotes the additive abelian subgroup of J generated by the homogeneous elements of degree n in x and y, then

$$J = \bigoplus_{n=1}^{p+1} J_n$$

(an internal direct sum) and $J_r J_s \subseteq J_{r+s}$, for all $r, s \in \{1, \ldots, p+1\}$. Let

$$\mathcal{B} = \{y, (\operatorname{ad} x + \vartheta_x)(y), (\operatorname{ad} x + \vartheta_x)^2(y), \ldots, (\operatorname{ad} x + \vartheta_x)^p(y)\},$$

and set $S = \operatorname{span}(\mathcal{B})$. This defines S to be a subspace of J containing y and stabilized by $\operatorname{ad} x + \vartheta_x$. It follows that $E_p(x) \in \mathbf{N}_G(S)$, so in particular, $y^{E_p(x)^{-1}} \in S$. The question is whether $E_p(\alpha x) \in \mathbf{N}_G(S)$ for arbitrary $\alpha \in F$. This happens if and only if $\operatorname{ad}(\alpha x) + \vartheta_{\alpha x}$ stabilizes S.

Therefore, we must determine if $\operatorname{ad}(\alpha x) + \vartheta_{\alpha x} = \alpha \operatorname{ad} x + \alpha^p \vartheta_x$ stabilizes S. For all primes p, $J^{2p} \subseteq J^{p+2} = 0$, and so Lemma 4.4 implies $\operatorname{ad}(\alpha x) + \vartheta_{\alpha x} = \alpha \operatorname{ad} x + \alpha^p \vartheta_x$. Because

$\operatorname{ad} x + \vartheta_x$ stabilizes S, it follows that

$$\alpha^p \left(\operatorname{ad} x + \vartheta_x\right) = \alpha^p \operatorname{ad} x + \alpha^p \vartheta_x$$

does, too. Hence, $\alpha \operatorname{ad} x + \alpha^p \vartheta_x$ stabilizes S if and only if

$$\left(\alpha^p \operatorname{ad} x + \alpha^p \vartheta_x\right) - \left(\alpha \operatorname{ad} x + \alpha^p \vartheta_x\right) = \left(\alpha^p - \alpha\right) \operatorname{ad} x \tag{4.5}$$

does. If $\alpha \notin \mathbb{F}_p$, then $\alpha^p - \alpha \neq 0$, so $\left(\alpha^p - \alpha\right)^{-1} \in F$. In this case, $\alpha \operatorname{ad} x + \alpha^p \vartheta_x$ stabilizes S if and only if

$$\left(\alpha^p - \alpha\right)^{-1} \left(\alpha^p - \alpha\right) \operatorname{ad} x = \operatorname{ad} x$$

does. So the question becomes whether $\operatorname{ad} x(S) \subseteq S$. In particular, is $\operatorname{ad} x(y) = xy - yx$ in S? Suppose so. Then there exist $a_0, a_1, \ldots, a_p \in F$ so that

$$xy - yx = a_0 y + \sum_{n=1}^{p} a_n \left(\operatorname{ad} x + \vartheta_x\right)^n (y). \tag{4.6}$$

Notice that since $J^{p+2} = 0$ and ϑ_x has degree p, $\left(\operatorname{ad} x + \vartheta_x\right)^n = \left(\operatorname{ad} x\right)^n = \left(L_x - R_x\right)^n$ for all $n \geqslant 2$. Therefore, if $n \geqslant 2$,

$$\begin{aligned}
\left(\operatorname{ad} x + \vartheta_x\right)^n (y) &= \left(L_x - R_x\right)^n (y) \\
&= \left(\sum_{i=0}^{n} \binom{n}{i} L_x^{n-i} (-R_x)^i\right) (y) \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} x^{n-i} y x^i,
\end{aligned}$$

which lies in the homogeneous component J_{n+1}. In particular, for $n = p$,

$$\begin{aligned}
\left(\operatorname{ad} x + \vartheta_x\right)^p (y) &= \left(L_x - R_x\right)^p (y) \\
&= \left(L_x^p - R_x^p\right) (y) \\
&= x^p y - y x^p.
\end{aligned}$$

Hence, equation (4.6) becomes

$$\begin{aligned} xy - yx &= a_0 y + a_1 \left(\operatorname{ad} x + \vartheta_x\right)(y) + \sum_{n=2}^{p-1} a_n \left(\operatorname{ad} x\right)^n (y) + a_p \left(\operatorname{ad} x\right)^p (y) \\ &= a_0 y + a_1 \left(xy - yx + \vartheta_x(y)\right) + \sum_{n=2}^{p-1} a_n \left(\operatorname{ad} x\right)^n (y) + a_p \left(x^p y - y x^p\right). \end{aligned}$$

On the one hand, the coefficient of xy on the left-hand side is 1, so a_1, the coefficient of xy on the right-hand side must also be 1. On the other hand, since $xy - yx \in J_2$, the terms on the right-hand side lying in J_{p+1} must sum to zero. That is,

$$a_1 \vartheta_x(y) + a_p \left(x^p y - y x^p\right) = 0. \tag{4.7}$$

We must consider two cases. If p is odd, then by Lemma 4.4 (a), equation (4.7) becomes

$$a_1 \sum_{i=1}^{p-1} (-1)^{i+1} \frac{1}{p} \binom{p}{i} x^{p-i} y x^i + a_p \left(x^p y - y x^p\right) = 0.$$

The coefficient, a_p, of $x^p y$ must be 0, so $a_1 = 0$ also, a contradiction. If $p = 2$, then by Lemma 4.4 (b), equation (4.7) becomes

$$a_1 (xyx - yx^2) + a_2 \left(x^2 y - y x^2\right) = 0.$$

Here again, a_2, the coefficient of $x^2 y$, must be 0, which forces $a_1 = 0$, a contradiction.

In either case, $\operatorname{ad} x(y) = xy - yx$ is not a linear combination of the elements of $\mathcal{B}$. Going back to equation (4.5), we conclude $E_p(\alpha x) \in \mathbf{N}_G(S)$ if and only if $\alpha \in \mathbb{F}_p$. This shows that $\mathbf{N}_G(S)$ is not AH-closed if $F \neq \mathbb{F}_p$.

In fact, we claim $\mathbf{N}_G(S)$ is not strong if $F \neq \mathbb{F}_p$. The set S was constructed so that $y^g \in S$ if and only if $y^g = y$ or else $y^g = (\operatorname{ad} x + \vartheta_x)^n(y)$ for some n. We know $\mathbf{C}_G(S) \subseteq \mathbf{N}_G(S)$ and that $|\mathbf{C}_G(S)| = q^a$, for some a, since it is an F- algebra. In this case, nothing commutes with $(\operatorname{ad} x + \vartheta_x)(y)$ that does not kill it, while y commutes only with powers of itself and elements of J^{p+1}. Therefore, $\mathbf{C}_J(S)$ is the F-algebra generated by y^p and J^{p+1}.

We have shown that $\mathbf{N}_G(S)$ also contains the p elements of the form $E_p(\alpha x)$ for $\alpha \in \mathbb{F}_p$. Therefore, $|\mathbf{N}_G(S)| = q^a p$. If $F \neq \mathbb{F}_p$, this cannot be a strong subgroup, since its order is not a power of q. □

In fact, the proof of part (b) of Theorem 4.5 can be strengthened to show that normalizers of algebra subgroups need not be strong. In this case, the algebra generated by the set $\mathcal{B}$ has the same normalizer as the vector space spanned by $\mathcal{B}$. Let A be the subalgebra of J generated by the set $\mathcal{B}$. Extend $\mathcal{B}$ to a vector space basis $\hat{\mathcal{B}}$ of A, by including all products of elements in $\mathcal{B}$. Then essentially the same argument shows that $N_G(A) = N_G(S)$, which is not strong if $F \neq \mathbb{F}_p$.

CHAPTER 5

STRONG SUBGROUPS

In Chapters 1 and 3, we defined certain strong subgroups in terms of the exponential and Artin-Hasse exponential series. The goal of this chapter is to show that an arbitrary strong subgroup can be described in terms of power series. Perhaps surprisingly, the class of power series that can be used for such a description is quite large. We start in §5.1 with two easy negative results. Part of the purpose here is to illustrate the power-series description of strong subgroups found in §5.2. In §5.3, we present a more thorough treatment of this description in the case where the group is abelian and the power series has an additional property.

5.1 Two counter-examples

In this section, we construct two counter-examples. These constructions will ease us into the more complicated constructions in the main result of this chapter, which appears in §5.2.

First, we construct a family of examples that shows that the collection of strong subgroups of an algebra group need not be closed under intersection. Let $G = 1 + J$ be a finite F-algebra group where F has characteristic $p > 2$ and order $q > p$. Let $x \in J$ with $x^p = 0$ but $x^2 \neq 0$. Suppose $f : F \to F$ is a nonzero additive map with $f(1) = 0$. Define the set H by

$$H = \left\{ (1+x)^{\alpha}(1+x^2)^{f(\alpha)} : \alpha \in F \right\}.$$

It is routine to check that H is an abelian subgroup of G of order q. Also $1 + x \in H$ since $f(1) = 0$.

Now let A be a subalgebra of J with $H \cap (1 + A) \neq 1$. Then there exists some nonzero

$\alpha_0 \in F$ such that

$$(1+x)^{\alpha_0}(1+x^2)^{f(\alpha_0)} \in 1+A.$$

That is,

$$(1+\alpha_0 x+\cdots)(1+f(\alpha_0)x^2+\cdots) \in 1+A.$$

Thus, there exists some $w \in x^2 f[x]$ such that

$$\alpha_0 x + w \in A.$$

However, by Lemma 3.3, $\alpha_0 x + w$ generates the algebra $xF[x]$, which means $xF[x] \subseteq A$. Therefore,

$$H \cap (1+A) = H.$$

We have just shown that, for any algebra subgroup K of G,

$$H \cap K = 1 \text{ or } H \cap K = H;$$

and so

$$|H \cap K| = 1 \text{ or } q.$$

Thus, H is a strong subgroup of G.

Now since $x^p = 0$, we may consider the F-exponent group $(1+x)^F$. This is a strong subgroup of G of order q which is distinct from H since f is not the zero map. However, $1 + x \in (1+x)^F \cap H$. Thus,

$$1 < \left|(1+x)^F \cap H\right| < q.$$

This means that $(1+x)^F \cap H$ is not strong. Therefore, the intersection of strong subgroups need not be strong.

Next, we construct an example which shows that strong subgroups need not be isomorphic to algebra subgroups (even for a different F-algebra). Let $G = 1 + J$ be a finite

F-algebra group where F has odd characteristic p and order q. Let $x \in J$ with $x^{p+1} = 0$ but $x^p \neq 0$. Define the subgroup K by

$$K = \mathcal{E}_p^F(x) = E_p(Fx)E_p(Fx^p).$$

Then K is a strong subgroup of exponent p^2 and order q^2.

Suppose there is an isomorphism $K \to 1 + A$ for some nilpotent F-algebra A. Then $\dim_F(A) = 2$. Since the exponent of $1 + A$ is p^2, there is some element $u \in A$ such that $o(1 + u) = p^2$. It follows that $u, u^2, \ldots, u^p$ are linearly independent. Since p is odd, this contradicts the fact that A has dimension 2. Therefore, the strong subgroup K is not isomorphic to any algebra subgroup.

5.2 A power-series description of strong subgroups

In this section, we prove the main result of this chapter. First, we make some definitions. Assume J is a nilpotent F-algebra with $\dim_F(J) = n$. An *ideal frame* of J is a basis $\{v_1, \ldots, v_n\}$ of J satisfying

$$v_i J, J v_i \subseteq \operatorname{span}\{v_{i+1}, \ldots, v_n\}$$

for all $i = 1, \ldots, n$. Notice that such bases always exist. For example, refine the chain

$$J \supset J^2 \supset \cdots \supset J^{m-1} \supset J^m = 0$$

to a maximal flag

$$J = V_1 \supset V_2 \supset \cdots \supset V_{n-1} \supset V_n \supset 0$$

and choose $v_i \in V_i \setminus V_{i+1}$ for all $i = 1, \ldots, n$. Then $\{v_1, \ldots, v_n\}$ is an ideal frame of J.

Now suppose $G = 1 + J$ is an F-algebra group where $\dim_F(J) = n$. Let $\{v_1, \ldots, v_n\}$ be an ideal frame of J and write $V_i = \operatorname{span}\{v_i, \ldots, v_n\}$. Note that $1 + V_i$ is an algebra subgroup of G and that every element of $1 + V_i$ is of the form $1 + \alpha v_i + w_{i+1}$ for some unique $\alpha \in F$ and $w_{i+1} \in V_{i+1}$. For $i = 1, \ldots, n$, we define maps $*_i : 1 + V_i \to F$ by

$$*_i : 1 + \alpha v_i + w_{i+1} \longmapsto \alpha$$

where $\alpha \in F$ and $w_{i+1} \in V_{i+1}$. Clearly, $*_i$ is onto F and has kernel $1 + V_{i+1}$.

Lemma 5.1. *Let $G = 1 + J$ be a finite F-algebra group where F is a field of order q. If $\dim_F(J) = n$, let $\{v_1, \ldots, v_n\}$ be an ideal frame of J and write $V_i = \operatorname{span}\{v_i, \ldots, v_n\}$. Suppose H is a strong subgroup of G for which $H \nsubseteq (1 + V_2)$. If $H_2 = H \cap (1 + V_2)$, then*

(a) $|H : H_2| = q$;

(b) for all $\alpha \in F$, there exists some $t \in V_2$ such that $1 + \alpha v_1 + t \in H$.

Proof. Since $H \nsubseteq (1 + V_2)$, $|H : H_2| > 1$. But $|H|$ and $|H_2|$ are both powers of q, as H is strong in G and $1 + V_2$ is an algebra subgroup of G. Thus, $|H : H_2| = q^a$ for some $a \geqslant 1$. On the other hand, $|1 + J : 1 + V_2| = q$ which forces $|H : H_2| = q$ as well.

Next, if we restrict the map $*_1 : G \to F$ to H, the kernel of the restriction is H_2. But since $|H : H_2| = q = |F|$, the restriction of $*_1$ to H must be onto F. That is, for all $\alpha \in F$, there exists some $t \in V_2$ such that $1 + \alpha v_1 + t \in H$. □

A power series with constant term 1 is said to be *strict*. In keeping with this metaphor, we make the following definition. A power series $\sigma : J \to 1 + J$ is said to be *stringent* if it is of the form

$$\sigma(x) = 1 + x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots$$

for $x \in J$. That is, σ is stringent provided its linear coefficient and constant term are both 1. Examples of stringent power series include

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

and

$$\begin{aligned} E_p(x) &= \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots\right) \\ &= 1 + \sum_{n=1}^{\infty} \frac{\left|\bigcup \mathrm{Syl}_p(S_n)\right|}{n!} x^n \qquad \text{(by Lemma 2.11)} \\ &= 1 + \frac{\left|\bigcup \mathrm{Syl}_p(S_1)\right|}{1!} x + \sum_{n=2}^{\infty} \frac{\left|\bigcup \mathrm{Syl}_p(S_n)\right|}{n!} x^n \\ &= 1 + x + \sum_{n=2}^{\infty} \frac{\left|\bigcup \mathrm{Syl}_p(S_n)\right|}{n!} x^n. \end{aligned}$$

We next prove some basic properties of stringent power series.

Proposition 5.2. *Stringent power series are invertible.*

Proof. It is well-known that a formal power series over a ring R is invertible if and only if its constant term is invertible in R. Since the constant term of a stringent power series is 1, it is invertible. □

Proposition 5.3. *If σ is stringent and $\alpha \in F$, then $\sigma(\alpha x)^{-1} = 1 - \alpha x + y$, for some $y \in x^2 F[\![x]\!]$.*

Proof. If σ is stringent and $\alpha, \beta \in F$, then

$$\sigma(\alpha x) = 1 + \alpha x + y_\alpha \qquad \text{and} \qquad \sigma(\beta x) = 1 + \beta x + y_\beta,$$

for some $y_\alpha, y_\beta \in x^2 F[\![x]\!]$. Therefore,

$$\begin{aligned} \sigma(\alpha x)\sigma(\beta x) &= (1 + \alpha x + y_\alpha)(1 + \beta x + y_\beta) \\ &= 1 + (\alpha + \beta)x + \hat{y}, \end{aligned}$$

where $\hat{y} \in x^2 F[\![x]\!]$. It follows that $\sigma(\alpha x)\sigma(\beta x) = 1$ if and only if $\beta = -\alpha$ and $y = y_\beta \in x^2 F[\![x]\!]$ is chosen so that $\hat{y} = 0$. □

For a stringent power series, σ, define $\sigma(Fx) = \{\sigma(\alpha x) \,|\alpha \in F\}$. This is a subset, but not necessarily a subgroup, of G.

We next show that for any stringent power series σ, a finite algebra group with a fixed ideal frame is the product, with uniqueness, of some of its subsets of the form $\sigma(Fx)$. Since algebra groups need not be commutative, we will use product notation with the convention that the product is taken in order of the index. That is,

$$\prod_{i=1}^{n} \sigma(Fv_i) = \sigma(Fv_1)\sigma(Fv_2)\cdots\sigma(Fv_n).$$

Lemma 5.4. *Let $G = 1 + J$ be a finite F-algebra group. Suppose $\{v_1, \ldots, v_n\}$ is an ideal frame of J, where $n = \dim_F(J)$. Suppose $\sigma\colon J \to 1 + J$ is a stringent power series. If $V_i = \operatorname{span}\{v_i, \ldots, v_n\}$, then*

(a) $1 + V_i = \sigma(Fv_i)(1 + V_{i+1})$ for all $i = 1, \ldots, n-1$;

(b) every element of G has a unique representation of the form

$$\sigma(\alpha_1 v_1)\sigma(\alpha_2 v_2)\cdots\sigma(\alpha_n v_n)$$

where $\alpha_1, \ldots, \alpha_n \in F$. In particular,

$$G = \prod_{i=1}^{n} \sigma(Fv_i).$$

Proof. For part (a), fix $i \in \{1, \ldots, n\}$ and choose $g \in 1 + V_i$. Then $g = 1 + \alpha v_i + w_{i+1}$ for some $\alpha \in F$ and some $w_{i+1} \in V_{i+1}$. Now

$$\begin{aligned}\sigma(\alpha v_i)^{-1} g &= (1 - \alpha v_i + \cdots)(1 + \alpha v_i + w_{i+1}) \\ &= 1 + 0 v_i + \hat{w}_{i+1}\end{aligned}$$

for some $\hat{w}_{i+1} \in V_{i+1}$. That is, $g = \sigma(\alpha v_i)(1 + \hat{w}_{i+1})$, which implies $1 + V_i \subseteq \sigma(Fv_i)(1 + V_{i+1})$. The reverse inclusion is immediate from the definition of the V_i's and so equality holds.

For part (b), consider an element $g \in G$. Apply the map $*_1$ to g, say $*_1 : g \mapsto \alpha_1$. Then, by part (a), $g = \sigma(\alpha_1 v_1)(1 + w_2)$ for some (unique) $w_2 \in V_2$. Next, apply $*_2$ to $(1 + w_2)$ and

express g uniquely as $g = \sigma(\alpha_1 v_1)\sigma(\alpha_2 v_2)(1 + w_3)$ for some $\alpha_2 \in F$ and $w_3 \in V_3$. Successive application of the remaining maps $*_i$ enables us to write

$$g = \sigma(\alpha_1 v_1)\sigma(\alpha_2 v_2) \cdots \sigma(\alpha_n v_n)$$

where $\alpha_1, \ldots, \alpha_n \in F$ are uniquely determined. It follows that

$$G = \prod_{i=1}^{n} \sigma(F v_i),$$

where the product is taken in order. □

With these preliminaries in place, we are now ready to state our main theorem.

Theorem 5.5. *Suppose F is a field of order q, $G = 1 + J$ is a finite F-algebra group, and $\{v_1, \ldots, v_n\}$ is an ideal frame of J, where $n = \dim_F(J)$. Let $\sigma : J \to 1 + J$ be a stringent power series. If H is a strong subgroup of G, then there exist a partition $I_f \dot\cup I_d = \{1, \ldots, n\}$ and functions $f_{ij} : F \to F$ for all $i \in I_f$ and $j \in I_d$ with $j > i$ such that, for all $\alpha \in F$,*

$$h_i(\alpha) = \sigma(\alpha v_i) \prod_{\substack{j \in I_d \\ j > i}} \sigma\left(f_{ij}(\alpha) v_j\right)$$

is an element of H. Furthermore, every $h \in H$ has a unique representation of the form

$$h = \prod_{i \in I_f} h_i(\alpha_i)$$

where $\alpha_i \in F$. Finally, the set

$$T = \left\{ \prod_{j \in I_d} \sigma\left(\beta_j v_j\right) : \beta_j \in F \right\}$$

is a left transversal for H in G.

Before beginning the proof, let us revisit the first example of §5.1, framing it in the notation of the theorem. Recall that we defined H by

$$H = \left\{ (1 + x)^{\alpha} \left(1 + x^2\right)^{f(\alpha)} : \alpha \in F \right\},$$

where $x^p = 0$, $x^2 \neq 0$, and f is a nonzero additive map with $f(1) = 0$. Suppose also that $x^{p-1} \neq 0$ and that $J = xF[x]$. If we define $v_i = \log\left(1 + x^i\right)$, for $i = 1, 2, \ldots, p-1$ and $\sigma = \exp$, then $\sigma(\alpha v_i) = \exp(\alpha v_i) = \left(1 + x^i\right)^\alpha$ for all $\alpha \in F$. Also note that $\{v_1, v_2, \ldots, v_{p-1}\}$ is an ideal frame of J. Here $I_f = \{1\}$ and $I_d = \{2, \ldots, p-1\}$. (The set I_f consists of the indices of the frame elements occurring in the "free" factors, while I_d consists of the indices occurring in the "dependent" factors.) Set $f_{1,2} = f$ and $f_{1,j} = 0$ for $j = 3, \ldots, p-1$. Then we have

$$\begin{aligned} h_1(\alpha) &= \exp(\alpha v_1) \prod_{\substack{j \in I_d \\ j > 1}} \exp\left(f_{1,j}(\alpha) v_j\right) \\ &= (1+x)^\alpha \left(1 + x^2\right)^{f(\alpha)}. \end{aligned}$$

Thus, every $h \in H$ is of the form

$$h = \prod_{i \in I_f} h_i(\alpha) = h_1(\alpha).$$

Furthermore,

$$T = \left\{ \prod_{j \in I_d} \exp\left(\beta_j v_j\right) : \beta_j \in F \right\} = \left\{ \prod_{j \in I_d} \left(1 + x^j\right)^{\beta_j} : \beta_j \in F \right\}$$

forms a left transversal for H in G.

Note that this example is somewhat specialized. In the general setting, the functions f_{ij} need not be additive, for example. We will consider what happens when the f_{ij} are additive in a special case in §5.3. But first, we prove Theorem 5.5 by induction on the dimension of J.

Proof. Set $V_2 = \operatorname{span}\{v_2, \ldots, v_n\}$. Then $1 + V_2 \trianglelefteq 1 + J$ and $|1 + J : 1 + V_2| = q$. If $H_2 = H \cap (1 + V_2)$, then H_2 is a strong subgroup of the algebra group $1 + V_2$ and the result holds for H_2 by induction. That is, there exist a partition $\hat{I}_f \dot{\cup} \hat{I}_d = \{2, \ldots, n\}$ and functions $f_{ij} : F \to F$ for all $i \in \hat{I}_f$ and $j \in \hat{I}_d$ with $j > i$ that work. In particular,

$$\hat{T} = \left\{ \prod_{j \in \hat{I}_d} \sigma\left(\beta_j v_j\right) : \beta_j \in F \right\}$$

is a left transversal for H_2 in $1 + V_2$.

We must consider two cases.

Case 1: Suppose $H \leqslant 1 + V_2$. This means that $H = H_2$. By Proposition 5.4, the set $\sigma(Fv_1)$ forms a left transversal for $1 + V_2$ in G. Set $I_f = \hat{I}_f$ and $I_d = \{1\} \cup \hat{I}_d$ and define

$$T = \sigma(Fv_1)\hat{T} = \left\{ \prod_{j \in I_d} \sigma(\beta_j v_j) : \beta_j \in F \right\}.$$

Then

$$|T| = q\,|\hat{T}| = q\,|1 + V_2 : H_2| = |G : H|$$

and

$$TH = \sigma(Fv_1)\hat{T}H = \sigma(Fv_1)(1 + V_2) = G.$$

Hence, T is a left transversal for H in G. The description of elements of H as products of $h_i(\alpha_i)$'s remains essentially unchanged from their description as elements of H_2. Therefore, the result holds in this case.

Case 2: Now suppose that $H_2 = H \cap (1 + V_2) \lneqq H$. Since H is strong, $|H : H_2| = q$ by Lemma 5.1. Define $I_d = \hat{I}_d$, which means $T = \hat{T}$, and so $TH_2 = \hat{T}H_2 = 1 + V_2$. Fix $\alpha \in F$. By Lemma 5.1, there exists $h \in H$ such that $*_1 : h \mapsto \alpha$. Of course, $*_1$ also maps $\sigma(\alpha v_1)$ to α and it maps $\sigma(\alpha v_1)^{-1}$ to $-\alpha$. Thus, $*_1 : \sigma(\alpha v_1)^{-1}h \mapsto 0$, which means $\sigma(\alpha v_1)^{-1}h \in 1 + V_2 = TH_2$. Hence, there exist $t_\alpha \in T$ and $h_2 \in H_2$ such that $\sigma(\alpha v_1)^{-1}h = t_\alpha h_2$ or, equivalently,

$$h = \sigma(\alpha v_1)t_\alpha h_2.$$

Indeed, t_α is uniquely determined by α, as we now show. If we choose another element $g \in H$ which $*_1$ maps to α, then g and h are in the same H_2-coset of H and so $g = hk_2$ for

some $k_2 \in H_2$. Therefore,

$$\sigma(\alpha v_1)^{-1} h = t_\alpha h_2,$$

$$\sigma(\alpha v_1)^{-1} h k_2 = t_\alpha h_2 k_2,$$

$$\sigma(\alpha v_1)^{-1} g = t_\alpha g_2,$$

where $g_2 = h_2 k_2 \in H_2$.

In addition, since $t_\alpha \in T$,

$$t_\alpha = \prod_{j \in I_d} \sigma\left(f_{1,j}(\alpha) v_j\right)$$

for some $f_{1,j}(\alpha) \in F$. Thus we have defined the functions $f_{1,j} : F \to F$ for $j \in I_d$.

We now define

$$\begin{aligned} h_1(\alpha) &= \sigma(\alpha v_1) t_\alpha \\ &= \sigma(\alpha v_1) \prod_{j \in I_d} \sigma\left(f_{1,j}(\alpha) v_j\right). \end{aligned}$$

Notice that $h_1(\alpha)$ is uniquely determined by α since the same is true of t_α. Clearly, $h_1(\alpha)$ is sent to α under $*_1$. Also,

$$\begin{aligned} h_1(\alpha) &= \sigma(\alpha v_1) t_\alpha \\ &= \sigma(\alpha v_1) t_\alpha h_2 h_2^{-1} \\ &= h h_2^{-1}, \end{aligned}$$

which implies that $h_1(\alpha)$ is an element of H.

Next, let $h_1(F) = \{h_1(\alpha) | \alpha \in F\}$. Since

$$|h_1(F)| = q = |G : 1 + V_2| = |H : H_2|,$$

$h_1(F)$ forms a left and right transversal for $1 + V_2$ in G and for H_2 in H. (Recall that

$1 + V_2 \trianglelefteq G$ and $H_2 \trianglelefteq H$.) Thus,

$$\begin{aligned} TH &= Th_1(F)H_2 \\ &= TH_2h_1(F) \\ &= \hat{T}H_2h_1(F) \\ &= (1 + V_2)h_1(F) \\ &= G. \end{aligned}$$

Since also

$$|T| = |\hat{T}| = |1 + V_2 : H_2| = |G : H|,$$

T is a left transversal for H in G.

Finally, we define $I_f = \{1\} \cup \hat{I}_f$ and conclude that

$$H = \left\{ \prod_{i \in I_f} h_i(\alpha_i) : \alpha_i \in F \right\},$$

which completes the proof. □

5.3 A special case

We now obtain a stronger result in the special case where $G = 1 + J$ is abelian and $\sigma : J \mapsto 1 + J$ is a stringent power series such that $\sigma(\alpha x)\sigma(\beta x) = \sigma((\alpha + \beta)x)$ for all $x \in J$, $\alpha, \beta \in F$. (When $J^p = 0$, the exponential map has these properties, for example.) It is useful to extend the maps $*_i$ defined in §5.2. Suppose $\{v_1, \ldots, v_n\}$ is an ideal frame of J, where $n = \dim_F(J)$. By Lemma 5.4, every element of G has a unique representation of the form

$$\prod_{k=1}^{n} \sigma(\alpha_k v_k),$$

where $\alpha_k \in F$. Thus, for $i = 1, \ldots, n$, the projection map $\pi_i : G \to F$ given by

$$\prod_{k=1}^{n} \sigma(\alpha_k v_k) \overset{\pi_i}{\longmapsto} \alpha_i$$

is a well-defined extension of $*_i$.

Theorem 5.6. *Let $G = 1 + J$ be a finite, abelian F-algebra group where F has finite order q. Let $\sigma : J \mapsto 1 + J$ be a stringent power series such that $\sigma(\alpha x)\sigma(\beta x) = \sigma((\alpha + \beta)x)$ for all $x \in J$, $\alpha, \beta \in F$. If $\dim_F(J) = n$, suppose $\{v_1, \ldots, v_n\}$ is an ideal frame of J and that $I_f \dot{\cup} I_d$ is a partition of $\{1, \ldots, n\}$. Let $f_{ij} : F \to F$ be a function for all $i \in I_f$ and $j \in I_d$ with $j > i$. Define, for $i \in I_f$, a function $h_i : F \to G$ by*

$$h_i(\alpha) = \sigma(\alpha v_i) \prod_{\substack{j \in I_d \\ j > i}} \sigma(f_{ij}(\alpha) v_j)$$

for $\alpha \in F$. Set $h_i(F) = \{h_i(\alpha) \,|\alpha \in F\}$ and $H = \left\{ \prod_{i \in I_f} h_i(\alpha_i) : \alpha_i \in F \right\}$. Then the following are equivalent:

(a) f_{ij} is additive for all $i \in I_f$ and $j \in I_d$ with $j > i$;

(b) h_i is a homomorphism for all $i \in I_f$;

(c) $h_i(F)$ is a subgroup of G for all $i \in I_f$;

(d) H is a subgroup of G of order q^m where $m = \left|I_f\right|$, and, moreover, $h_i(\alpha) \in H$ for all $i \in I_f$ and $\alpha \in F$;

(e) H is a subgroup of G with $h_i(F) \subseteq H$ for all $i \in I_f$;

(f) H is a subgroup of G with $h_i(0) \in H$ for all $i \in I_f$;

(g) H is a subgroup of G with $h_i(0) = 1$ for all $i \in I_f$.

Proof. First recall that, by Lemma 5.4, each $g \in G$ has a unique representation of the form

$$g = \prod_{i=1}^{n} \sigma(\alpha_i v_i)$$

for $\alpha_i \in F$ where the order of the product does not matter.

(a) $\Leftrightarrow$ (b): Let $i \in I_f$ and $\alpha, \beta \in F$. Then

$$h_i(\alpha)\ h_i(\beta) = \left[\sigma(\alpha v_i) \prod_{\substack{j \in I_d \\ j>i}} \sigma(f_{ij}(\alpha)v_j)\right] \left[\sigma(\beta v_i) \prod_{\substack{j \in I_d \\ j>i}} \sigma(f_{ij}(\beta)v_j)\right]$$

$$= \sigma(\alpha v_i)\ \sigma(\beta v_i) \prod_{\substack{j \in I_d \\ j>i}} \sigma(f_{ij}(\alpha)v_j)\ \sigma(f_{ij}(\beta)v_j)$$

$$= \sigma((\alpha+\beta)v_i) \prod_{\substack{j \in I_d \\ j>i}} \sigma((f_{ij}(\alpha) + f_{ij}(\beta))v_j).$$

Also,

$$h_i(\alpha+\beta) = \sigma((\alpha+\beta)v_i) \prod_{\substack{j \in I_d \\ j>i}} \sigma(f_{ij}(\alpha+\beta)v_j).$$

From these computations and uniqueness of representation in G (Lemma 5.4), it is apparent that the f_{ij}'s are additive if and only if the h_i's are homomorphisms.

(b) $\Rightarrow$ (c): If h_i is a homomorphism, then $h_i(F)$ is a subgroup of G.

(c) $\Rightarrow$ (d): Suppose that $h_i(F)$ is a subgroup of G for all i. By uniqueness of representation, $h_i(\alpha) = h_i(\beta)$ if and only if $\alpha = \beta$. Thus, $|h_i(F)| = q$. Also, since

$$h_i(F) \bigcap \prod_{\substack{k \in I_f \\ k>i}} h_k(F) = \{1\}$$

and H is abelian, we have $H = \prod_{i \in I_f} h_i(F)$ is a group of order q^m, where $m = \left|I_f\right|$. From this, it is also clear that $h_i(\alpha) \in H$ for all $i \in I_f$ and $\alpha \in F$.

(d) $\Rightarrow$ (e): This is immediate.

(e) $\Rightarrow$ (f): This is immediate.

(f) $\Rightarrow$ (g): Suppose H is a subgroup of G with $h_i(0) \in H$ for all $i \in I_f$. Since H is a subgroup,

$1 \in H$ and so there exist $\alpha_i \in F$ such that

$$1 = \prod_{i \in I_f} h_i(\alpha_i).$$

But uniqueness of representation in G forces $\alpha_i = 0$ for all i. Similarly, for $k \in I_f$, $h_k(0) \in H$ means that

$$h_k(0) = \prod_{i \in I_f} h_i(\beta_i)$$

for some $\beta_i \in F$. But then $\beta_i = 0$ for all i. That is,

$$h_k(0) = \prod_{i \in I_f} h_i(0) = 1$$

for all $k \in I_f$, as desired.

(g) $\Rightarrow$ (b): Suppose H is a subgroup of G and that $h_i(0) = 1$ for all $i \in I_f$. Define the map $h : F^{|I_f|} \to G$ by

$$h : (\alpha_i)_{i \in I_f} \longmapsto \prod_{i \in I_f} h_i(\alpha_i).$$

Clearly, the image of h is the set H. To show that h is a homomorphism, let $\alpha_i, \beta_i \in F$ for $i \in I_f$. Since H is a subgroup, there exist $\gamma_i \in F$ such that

$$\begin{aligned} h\left((\alpha_i)_{i \in I_f}\right) \cdot h\left((\beta_i)_{i \in I_f}\right) &= \prod_{i \in I_f} h_i(\alpha_i) \cdot \prod_{i \in I_f} h_i(\beta_i) \\ &= \prod_{i \in I_f} h_i(\gamma_i) \\ &= h\left((\gamma_i)_{i \in I_f}\right). \end{aligned}$$

Apply the i-th projection map π_i to each side of the above equation to conclude that $\gamma_i = \alpha_i + \beta_i$. Hence, h is a homomorphism.

Next, fix $i \in I_f$ and precompose h with the monomorphism $q_i : F \to F^{|I_f|}$, which sends $\alpha \in F$ to $(0, \ldots, \alpha, \ldots, 0)$, the tuple with α in the ith coordinate and 0's elsewhere. So

$$\alpha \overset{q_i}{\longmapsto} (0, \ldots, \alpha, \ldots, 0) \overset{h}{\longmapsto} h_i(\alpha) \prod_{\substack{k \in I_f \\ k \neq i}} h_k(0).$$

However,

$$h_i(\alpha) \prod_{\substack{k \in I_f \\ k \neq i}} h_k(0) = h_i(\alpha)$$

by the assumption that $h_k(0) = 1$ for all k. This says that $h_i = h \circ q_i$, the composite of two homomorphisms. Therefore, h_i is itself a homomorphism of groups.

Thus, the given conditions are equivalent. □

REFERENCES

André, Carlos A.M. 2010. *Irreducible characters of groups associated with finite nilpotent algebras with involution*, Journal of Algebra **324**, 2405-2417.

Artin, Emil and Helmut Hasse. 1928. *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **6**, 146-162.

Blache, Régis. 2005. *A Stickelberger theorem for p-adic Gauss sums*, Acta Arithmetica **118**, 11-26.

Grove, Larry C. 1983. *Algebra*, Pure and Applied Mathematics, vol. 110, Academic Press.

Hazewinkel, Michiel. 2009. *Witt vectors, Part 1*, Handbook of Algebra, Volume 6, pp. 319-472.

Isaacs, I. Martin. 1973. *Equally partitioned groups*, Pacific Journal of Mathematics **49**, 109-116.

_____. 1995. *Characters of groups associated with finite algebras*, Journal of Algebra **177**, 708-730.

Isaacs, I. Martin and Geoffrey R. Robinson. 1992. *On a theorem of Frobenius: solutions of $x^n = 1$ in a finite group*, American Mathematical Monthly **99**, 352-354.

Koblitz, Neal. 1984. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics, vol. 58, Springer-Verlag.

Lenstra, Hendrik. 2002. *Construction of the ring of Witt vectors*, unpublished lecture notes, available at `www.math.berkeley.edu/~hwl/papers/witt.pdf`.

Mattarei, Sandro. 2006. *Exponential functions in prime characteristic*, Aequationes Mathematicae **71**, 311-317.

Previtali, Andrea. 1995. *On a conjecture concerning character degrees of some p-groups*, Archiv der Mathematik **65**, 375-378.

_____. 1999. *Maps behaving like exponentials and maximal unipotent subgroups of groups of Lie type*, Communications in Algebra **27**, 2511-2519.

Rabinoff, Joseph. 2007. *The theory of Witt vectors*, unpublished, available at `www.math.harvard.edu/~rabinoff/misc/witt.pdf`.

Robert, Alain M. 2000. *A Course in p-adic Analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag.