Differential Operators on

Finite Purely Inseparable Extensions

BY

MATTHEW WECHTER
B.A. (Amherst College) 2005
M.S. (University of Illinois at Chicago) 2009

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2013

Chicago, Illinois

Defense Committee:

Henri Gillet, Chair and Advisor
Izzet Coskun, Mathematics, Statistics, and Computer Science
Mihnea Popa, Mathematics, Statistics, and Computer Science
Ramin Takloo-Bighash, Mathematics, Statistics, and Computer Science
Raymond Hoobler, City College and Graduate Center (CUNY)

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

SUMMARY

This thesis explores Galois-type correspondences for finite purely inseparable field extensions. Chapter 1 introduces basic notions of classical Galois theory and purely inseparable field theory. The Jacobson-Bourbaki theorem is presented and proven and then used to prove the Jacobson Galois correspondence regarding purely inseparable extensions of exponent 1.

In Chapter 2, the theory of Hasse-Schmidt derivations is discussed. We explain the connection between higher derivations and special classes of purely inseparable extensions called *modular extensions*. We reinterpret the construction of an array first constructed by Sweedler using modules of differentials to determine whether a field extension if modular, therefore making Sweedler's result independent of any choice of p-bases.

Chapter 3 elaborates further on the theory of Hasse-Schmidt derivations on purely inseparable fields extensions. In particular, this chapter will present constructions of higher derivations using the Artin-Hasse exponential of certain Witt vectors. We correct a theorem originally stated by Gerstenhaber and prove the existence of a many-to-one correspondence between modular subfields of a purely inseparable extension and maximal Witt subgroups of the Witt group generated by Witt vectors of a commutative subring of endomorphisms of the purely inseparable extension.

Chapter 4 approaches modular field extensions from the perspective of the ring of differential operators. Basic definition and facts of differential operators and divided powers algebras are presented. Then we state and prove the necessary and sufficient conditions for a subring of the

SUMMARY (Continued)

ring of differential operators of a finite purely inseparable extension L/K to have a subfield of constants K' such that L/K' is modular.

Chapter 5 presents a result proven by Gerstenhaber which relates intermediate subfields of a finite purely inseparable extension to the ring structure of the graded commutative ring associated to the ring of differential operators by its filtration by orders of differential operators. We then prove the existence of a $1-1$ correspondence between intermediate subfields of a purely inseparable extension of fields of characteristic $p > 0$ with exponent 1 and degree p^2 and certain elements of this associate graded ring of differential operators.

CHAPTER 0

INTRODUCTION

Suppose L/K is a finite Galois field extension. By the Fundamental Theorem of Galois Theory there exists a $1-1$ correspondence between intermediate subfields of L/K and subgroups of the group of automorphisms of L with respect to K, denoted $\mathrm{Aut}_K L$. Any finite field extension L/k has a filtration $k \subseteq K' \subseteq L$ where K'/k is a finite separable extension and L/K is a finite purely inseparable extension. The fixed field of $\mathrm{Aut}_k L$ contains K', so the structure of the field extension L/K' cannot be recovered by studying the automorphisms of L/k. In addition, the automorphism scheme of a finite separable field extension is discrete, while the automorphism scheme of a finite purely inseparable field extension is not discrete, and has positive dimension if the field extension is not trivial.

The Jacobson-Bourbaki Theorem shows that for any field L, there is a $1-1$ correspondence between subfields of L for which L is a finite algebraic extension and finite-dimensional subrings of the ring of endomorphisms of L. Jacobson (14) first studied Galois correspondences on finite purely inseparable extensions, classifying the subrings of endomorphisms for purely inseparable extensions of exponent 1, the simplest type of such an extension. The Lie algebra of derivations for a purely inseparable extension is nontrivial, unlike in the separable case. In addition, since the fields of a purely inseparable extensions are necessarily of characteristic $p > 0$, these Lie algebras have an additional pth power map making them restricted Lie algebras. Jacobson proved that there is a $1-1$ correspondence between restricted sub-Lie algebras and intermediate subfields. In addition, the subring of endomorphisms generated by a restricted sub-Lie algebra of derivations is equal to the ring of endomorphisms of E which are linear with respect to the intermediate subfield.

If L/K is a purely inseparable extension of fields of characteristic $p > 0$, then the derivations of L with respect to K are trivial on KL^p. Thus for any extension of exponent greater than 1, the derivations provide no information on the structure of the extension past the pth powers. Sweedler (24) introduced the notion of a modular extension, one property of which is that the extension decomposes as the tensor product of simple extensions. By looking at the filtration of an extension using successive pth roots (i.e. $K \subseteq K^{p^{-1}} \cap L \subseteq K^{p^{-2}} \cap L \cdots \subseteq L$), he constructed an array whose entries were elements of the p-bases of these successive exponent 1 extensions, and used this array to prove a theorem which provided conditions for when L/K is modular. In Chapter 2, we use the correspondence between a p-basis of an extension and a basis of the module of differentials to construct a basis-free array for the extension using the differentials, and prove

Theorem 30. *Let L and k be fields of characteristic $p > 0$ and suppose L/k is a finite purely inseparable field extension of exponent e. Let $F : L \to L$ be the Frobenius homomorphism. L/k is modular if and only if*

$$\mu \circ \left(\iota_{L_{r-1}} \otimes_{F_r} dF_r\right) : L_{r-1} \otimes_{F_r} \Omega^1_{L_r/L_{r-1}} \to \Omega^1_{L_{r-1}/L_{r-2}}$$

is injective for all r such that $2 \leq r \leq e$, where $L_r = k^{p^{-r}} \cap L$ and F_r is the homomorphism $L_r \to L_{r-1}$ induced by F.

Various attempts have been made to find Galois correspondences which will help parametrize intermediate subfields K' of a purely inseparable extension L/K such that L/K' is modular. Noting that different subgroups of the automorphism scheme of L/K can have the same subfield of constants, Chase (5) proves that a correspondence exists between intermediate fields $K \subseteq L$ and certain closed subgroups of the automorphism scheme of L/K, where the subgroups must be closed under a certain endomorphism of the lattice of subgroups. The historical approach to studying modular field extensions was to study Hasse-Schmidt derivations, or higher derivations, on purely inseparable extensions. If L/K is modular, then K is the fixed field of a set of higher derivations of L. It should be noted that a higher derivation of L/K is a $K[t]/(t^N)$-valued point of the automorphism scheme of L/K for some positive N.

Gerstenhaber (10) attempted to find correspondences between modular subfields of finite purely inseparable extensions and higher derivations by studying the structure of the groups of higher derivations. These groups of Hasse-Schmidt derivations of fixed rank form an inverse system by truncation, and Gerstenhaber studies the inverse limit of this system, which he calls $\mathrm{HDer}_K L$, the group of higher derivations. His contribution to this study comes from constructing higher derivations by applying a modified Artin-Hasse exponential to Witt vectors of endomorphisms of L/K which commute. The Witt vectors whose Artin-Hasse exponentials are higher derivations form a subgroup, and the Artin-Hasse exponential is a group homomorphism from such Witt vectors to the group of higher derivations. However, this homomorphism is injective, so no new information is gained by studying the Witt groups instead of the higher derivations.

In Chapter 3 we correct a theorem of Gerstenhaber and Zaromp to prove there exists a many-to-one correspondence between maximal Witt subgroups with the same fixed field and the full group of higher derivations with that fixed field. The obstruction to making this theorem into a Galois-type correspondence is that the maximal Witt subgroups are closed under actions by K, not L. When L-action is allowed, elements of the subgroups will no longer commute, which negates the usefulness of the Witt group structure. So, there is not a unique maximal Witt group associated to a modular extension L/K which will generate the group of higher derivations of L/K .

If L/K is a finite purely inseparable extension, then the coefficients of a higher derivation on L/K are differential operators on L/K. In fact, every endomorphism of L/K is a differential operator, so $\text{End}_K L = \text{Diff}_K L$. By the Jacobson-Bourbaki Theorem, there is a $1-1$ correspondence between subrings of $\text{End}_K L$ and intermediate subfields K' of L/K such that L/K' is modular. The Jacobson-Bourbaki Theorem gives no information on the structure of these subrings, but in Chapter 4 we identify the subrings of $\text{End}_K L = \text{Diff}_K L$ which correspond to modular extensions.

Theorem 49. *Let L/K be a finite purely inseparable extension of exponent e and set $\mathcal{A}_i = \{D \in \mathit{Diff}_K^{p^i} L : \forall j \leq i,\ D(L^{p^j}) \subseteq L^{p^j}\}$ where $\mathit{Diff}_K^{p^i} L$ consists of the differential operators of L/K of order $\leq p^i$. Then L/K is modular if and only if for all $0 < i \leq e-1$, the multiplication* *homomorphism* $L \otimes_{L^{p^i}} \mathcal{A}_i \to \mathit{Diff}_K^{p^i} L$ *is a surjection. That is, for each* i, $\mathcal{A}_i$ *spans* $\mathit{Diff}_K^{p^i} L$ *as an* L *subspace.*

These $\mathcal{A}_i$ are L^{p^i}-modules, and the symbol of each differential operator of top order in each $\mathcal{A}_i$ is a pth-power divided power in the symbol algebra of differential operators.

If $\{x_1, \ldots, x_n\}$ is a p-basis for a purely inseparable extension L/K of fields of characteristic $p > 0$, then there is an ordering $\{x_{i_1}, \ldots, x_{i_n}\}$ of this set such that if e_j is the exponent of x_{i_j} over $K(x_{i_1}, \ldots, x_{i_{j-1}})$, then e_j is the exponent of $K(x_{i_1}, \ldots, x_{i_j})$ over $K(x_{i_1}, \ldots, x_{i_{j-1}})$ for every j with $2 \leq j \leq n$, and the e_j are a non-increasing sequence. Furthermore, the e_j are independent of the p-basis chosen. Such an ordered p-basis is called a *Pickert generating sequence*. For any i with $1 \leq i < n$, any differential operator D of order N in $\mathrm{Diff}_K K(x_1, \ldots, x_i)$ can be non-uniquely extended to a differential operator $\widetilde{D}$ in $\mathrm{Diff}_K K(x_1, \ldots, x_{i+1})$. Any such extension will be of order M where $M \geq N$. A key step in the proof of the above theorem is the following lemma:

Lemma 48. *Let* K *be a field of characteristic* $p > 0$ *and suppose* L/K *is a finite purely inseparable extension of* K. *Let* $\{x_1, x_2, \ldots, x_n\}$ *be a Pickert generating sequence for* L/K *with corresponding exponent sequence* $e_1 \geq e_2 \geq \cdots \geq e_n$ *and let* D *be a differential operator of order* N *in* $\mathit{Diff}_K K(x_1, \ldots, x_i)$ *for* $i < n$. *Suppose* $\widetilde{D} \in \mathit{Diff}_K K(x_1, \ldots, x_{i+1})$ *is the unique extension of* D *such that* $\widetilde{D}\Big|_{K(x_1,\ldots,x_i)} = D$ *and* $\widetilde{D}(x_{i+1}^j) = 0$ *for all* $0 \leq j < p^{e^{i+1}}$. *Then* $\widetilde{D}$ *is a differential operator of order* N.

Because $K(x_1, \ldots, x_i)$ and $K(x_{i+1})$ are not necessarily linearly disjoint, the statement that the order of $\widetilde{D}$ is equal to the order of D is a nontrivial result. Gerstenhaber (9) calls $\widetilde{D}$ the *normal extension* of D to $K(x_1 \ldots, x_{i+1})$, but he made no attempt to compute the order of this extension.

To each finite purely inseparable extension there corresponds a maximal modular extension:

Corollary 50. *Let L/K be as in the theorem. Let $\mathcal{D}$ be the subalgebra of Diff$_K L$ generated by the $\mathcal{A}_i$. Then $\mathcal{D}$ is the largest subalgebra of Diff$_K L$ such that $L/L^{\mathcal{D}}$ is a modular extension.*

The filtration of the ring of differential operators of a finite purely inseparable extension can reflect the structure of the extension beyond just the modular subfields. If L/K is a finite purely inseparable field extension with K of characteristic $p > 0$, then the top degree subspace $\Gamma(L/K)$ of the "symbol algebra" $\mathrm{Gr}^\bullet \mathrm{Diff}_K L$ is 1-dimensional over L where $\mathrm{Gr}^\bullet \mathrm{Diff}_K L$ is graded by the order of the differential operators. Gerstenhaber calls a nonzero element of this subspace a *fundamental form*, but because the choice of such an element is not canonical, we define $\Gamma(L/K)$ as *the* fundamental form of L/K. It follows that if $K \subseteq K' \subseteq L$, then any nonzero element of $\Gamma(L/K')$ divides any element of $\Gamma(L/K)$ in the divided powers algebra $\Gamma^*(\mathrm{Der}_K L)$. In Chapter 5 we give an explicit construction of the fundamental form for finite purely inseparable extensions, again making use of the lemma above.

Gerstenhaber tried to determine when a factor of $\Gamma(L/K)$ corresponds to an intermediate subfield of L/K. His attempt was not very successful, mainly due to the fact that the pth power of every element of the symbol algebra is 0. However, in a simple case we are able in Theorem 55 to use the Poisson structure of the symbol algebra to determine criteria for when a divisor corresponds to an intermediate subfield in Theorem 55. It is not clear if this method can be extended to other cases.

CHAPTER 1

PURELY INSEPARABLE FIELD THEORY

1.1 Classical Galois Theory

Definition 1. *Let P/k be fields and $\rho \in P$. ρ is **algebraic** over k if there exists a polynomial $f(x) \in k[x]$ such that $f(\rho) = 0$. P is **algebraic over** k or an **algebraic extension of** k if every element of P is algebraic over k. P is **finite** over k if P is finitely-generated as a k-algebra.*

Algebraicity is a transitive property, so that if $k \subseteq E \subseteq P$ are fields such that E is algebraic over k and P is algebraic over E, then P is algebraic over k.

Definition 2. *If P/k are fields and $\rho \in P$ is algebraic over k, then ρ is **separable** if there exists a polynomial $f(x) \in k[x]$ such that $f(\rho) = 0$ and $(f(x), f'(x)) = 1$, where $f'(x)$ is the formal derivative of $f(x)$ with respect to x. P is a **separable extension of** k if every element of P is separable over k. If $f(x) \in k[x]$ is a polynomial and P is the smallest field extension of k containing distinct elements $\{\rho_1, \ldots, \rho_n\} \subset P$ such that $f(x) = (x - \rho_1) \cdots (x - \rho_n)$, then P **splits** $f(x)$.*

Separability is again a transitive property for field extensions. Moreover, if the characteristic of k is 0, then every algebraic element ρ over k is separable (14, I §9).

Definition 3. *A finite field extension P/k is called **normal** or **Galois** if P is a separable splitting field of k.*

Theorem 4 (Fundamental Theorem of Galois Theory)**.** *(14, I, §7) Let P/k be a finite Galois extension, and let Aut_kP denote the group of k-algebra automorphisms of P. There is a one-to-one inclusion-reversing correspondence between intermediate subfields of P/k and subgroups of Aut_kP. That is, for a subgroup $H \subseteq Aut_kP$, the subset $P^H := \{\rho \in P : \forall h \in H, h(\rho) = \rho\}$ is an intermediate field of P/k, and conversely, for $k \subseteq E \subseteq P$, the set of automorphisms of P that are linear with respect to E is a subgroup of Aut_kP. Moreover, if E is Galois over k, then the corresponding subgroup H of Aut_kP is normal, and $Aut_kE \cong (Aut_kP)/H$.*

Classical Galois theory is the study of finite separable extensions and their relation to the group of relative automorphisms of a field extension. If P/k is a field extension, there exists a unique maximal intermediate subfield Σ such that that Σ/k is separable (14, IV, §1). Σ is called the **separable closure** of k in P. Classical Galois theory provides information about Σ/k when Σ/k is a finite extension, but no information about the extension P/Σ. To understand the structure of P/Σ requires studying algebraic extensions which are not separable.

1.2 Purely Inseparable Extensions

Definition 5. *Let P/k be a finite algebraic extension of fields. P/k is* ***purely inseparable*** *if k is the separable closure of k in P. If P/k is an algebraic extension of fields and $\rho \in P$, then ρ is* ***purely inseparable*** *over k if $k(\rho)/k$ is purely inseparable.*

Theorem 6. *(14, I §9 Lemma 2) If k is a field of characteristic $p > 0$, then*

1. *Any algebraic element ρ over k is separable over k if and only if $k(\rho) = k(\rho^{p^i})$ for all positive integers i.*

2. *If ρ is purely inseparable over k, then its monic minimal polynomial has the form $x^{p^e} - \alpha$ for some $\alpha \in k$ and $e \geq 0$.*

3. *If ρ satisfies an equation of the form $x^{p^e} = \alpha$ for some $\alpha \in k$ and $e \geq 0$, then ρ is purely inseparable over k.*

Proof. We omit the proof of the first statement and include proofs of the other statements to demonstrate some computations in characteristic $p > 0$.

2. Let ρ be purely inseparable over k and $g(x) \in k[x]$ its minimal polynomial. $g(x)$ is irreducible in $k[x]$. ρ is not separable, therefore $(g(x), g'(x)) \neq 1$. Hence $g(x)|g'(x)$, and $g'(\rho) = 0$. By the minimal degree of $g(x)$, $g'(x) = 0$, hence $g(x) = x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1x^p + a_0 = h(x^{p^e})$ for some polynomial $h(x) \in k[x]$ and maximal integer e. $h'(x) \neq 0$, otherwise e would not be maximal. Hence ρ^{p^e} is the root of a separable polynomial $h(x) \in k[x]$. Thus $\rho^{p^e} \in k(\rho)$ is separable over k which implies $\rho^{p^e} \in k$ by assumption. So there exists $\alpha \in k$ such that $\rho^{p^e} = \alpha$. That is, ρ is the root of the polynomial $x^{p^e} - \alpha$. $g(x) = h(x^{p^e}) = x^{p^e} - \alpha$, so $x^{p^e} - \alpha$ is the minimal polynomial of ρ over k.

3. Suppose $\rho^{p^e} = \alpha \in k$ for some $e \geq 0$ and $\sigma \in k(\rho)$. Then $\sigma = a_0 + a_1\rho + \cdots + a_m\rho^m$ with $a_i \in k$ and $m < p^e$. Taking the p^eth power, $\sigma^{p^e} = a_0^{p^e} + \cdots + a_m^{p^e}(\rho^{p^e})^m = a_0^{p^e} + a_1^{p^e}\alpha + \cdots + a_m^{p^e}\alpha^m \in k$. If σ is separable over k, then by Property 1, $k(\sigma) = k(\sigma^{p^e}) = k$, so $\sigma \in k$. Therefore ρ is purely inseparable over k by definition.

□

Based on Theorem 6, a finite field extension K/k is purely inseparable if and only if every element of K satisfies an equation of the form $x^{p^e} = \alpha$ for some $\alpha \in k$. Other useful results quickly follow from this theorem.

Corollary 7. *(14, p.48)*

1. *Suppose $k \subseteq E \subseteq K$ are fields such that K/E is a purely inseparable extension and E/k is a purely inseparable extension. Then K/k is purely inseparable.*
2. *If K is a purely inseparable field extension of k, then K is a purely inseparable extension of any intermediate subfield of K/k.*

1.3 Basic Properties of Derivations

Note by Theorem 6 that if K/k is a purely inseparable field extension, then the minimal polynomial of an element of K/k has a unique root. Hence any element of $\mathrm{Aut}_k K$ fixes every element of K. Therefore $\mathrm{Aut}_k K = \{\iota_K\}$, so studying automorphisms of purely inseparable extensions provides no information on their lattices of intermediate subfields. Derivations, however, are useful objects when studying purely inseparable extensions.

Definition 8. *Let A be a commutative ring, B an A-algebra and M a B-module. A* ***derivation*** *from B to M is an A-linear map $d : B \to M$ satisfying the Leibniz property:*

$$\forall b,\, b' \in B,\, d(bb') = bd(b') + d(b')b$$

As is well known, a derivation corresponds to a homomorphism to the dual numbers over the codomain of the derivation:

Lemma 9. *(14, IV, §6) Let A be a ring, B an A-algebra, and C an A-subalgebra of B. The derivations from C to B are in one-to-one correspondence with A-algebra homomorphisms $\psi : C \to B \otimes_A A[x]/(x^2) = B[x]/(x^2)$ satisfying the following property: If π is the projection map from $B[x]/(x^2)$ to B sending a polynomial to the coefficient of its degree 0 term, then $\pi \circ \psi = \iota_C$.*

Proof. Let $D : C \to B$ be an A-derivation. Define a map $s_D : C \to B[x]/(x^2)$ by $s(c) = c + D(c)x$. This is clearly additive, and if c, $c' \in C$, then

$$\begin{aligned} s_D(cc') &= cc' + D(cc')x \\ &= cc' + cD(c')x + D(cc)c'x \\ &= (c + D(c)x)\left(c' + D(c')x\right) \\ &= s_D(c)s_D(c'), \end{aligned}$$

so s is multiplicative as well. In addition, $\pi \circ s = id_C$. Conversely, if $s : C \to B[x]/(x^2)$ is an A-algebra homomorphism, letting $\pi_2 : B[x]/(x^2) \to B$ denote the projection to the coefficient of the degree one term of $B[x]/(x^2)$, it is easy to check that $\pi_2 \circ s$ is a derivation $D : C \to B$, and the homomorphism s_D as constructed above is $\pi_2 \circ s$. □

Recall the following basic notions from commutative algebra (15, §26): Let k be a ring and A a commutative k-algebra. Define the multiplication homomorphism $\mu : A \otimes_k A \to A$, which sends $x \otimes_k y \in A \otimes_k A$ to $xy \in A$. Let $I := \ker \mu$ and $\Omega^1_{A/k} := I/I^2$. Note that for all $a \in A$, $1 \otimes_k a - a \otimes_k 1 \in I$. Let $\overline{1 \otimes_k a - a \otimes_k 1}$ be the image of $1 \otimes_k a - a \otimes_k 1$ in $\Omega^1_{A/k}$. $\Omega^1_{A/k}$ has an A-module structure and can be generated as an A-module by $\{\overline{1 \otimes_k x - x \otimes_k 1}\}_{x \in A}$. $\Omega^1_{A/k}$ is called the **module of differentials of** A/k. Further, there exists a k-linear homomorphism $d : A \to \Omega^1_{A/k}$ such that, for all $a \in A$, $d(a) = \overline{1 \otimes_k a - a \otimes_k 1}$. We adopt standard notation and denote $d(a)$ by da.

d is actually a k-linear derivation from A to $\Omega^1_{A/k}$, and the pair $(\Omega^1_{A/k}, d)$ satisfies the following universal property: If M is an A-module, then for any k-linear derivation $E : A \to M$ there exists a unique A-linear homomorphism $\widetilde{E} : \Omega^1_{A/k} \to M$ such that $E = \widetilde{E} \circ d$. In particular, when $M = A$, then there exists bijection between $\mathrm{Der}_k A$, the set of k-linear derivations of A, and $\mathrm{Hom}_A(\Omega^1_{A/k}, A)$.

Suppose k and k' are fields with A a commutative k-algebra and A' a commutative k'-algebra. Furthermore, assume there exist ring homomorphisms from A to A' and from k to k' such that the diagram

$$\begin{tikzcd}
A \arrow[r, "\phi"] & A' \\
k \arrow[u] \arrow[r] & k' \arrow[u]
\end{tikzcd}$$

commutes. Then there is a natural A-module homomorphism $d\phi : \Omega^1_{A/k} \to \Omega^1_{A'/k'}$ such that for any $a \in A$, $d\phi(da) = d(\phi(a))$.

Just as automorphisms of algebraic extensions must permute the roots of a polynomial, derivations of a field have limitations on how they can extend to algebraic extensions. If k is a field, B and C are k-algebras, and $E : C \to B$ is a k-module homomorphism, then for any

$$f(x_1, x_2, \ldots, x_n) = \sum_{\{i_1, i_2, \ldots, i_n\} \subset \mathbb{N}^n} \alpha_{i_1, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in C[x_1, x_2, \ldots, x_n],$$

define $f^E \in B[x]$ as

$$\sum_{\{i_1,i_2,\ldots,i_n\}\subset\mathbb{N}^n} E(\alpha_{i_1,\ldots,i_n})x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}.$$

Theorem 10. *(14, IV, §6, Theorem 14) Let L/k be an extension of fields and let A be a k-subalgebra of L. Suppose*

$$\xi_1,\ldots,\xi_m,\, \eta_1,\ldots,\eta_m \in L$$

and $D : A \to L$ is a k-derivation. Let I be the ideal of $A[x_1,\ldots,x_m]$ consisting of all polynomials which vanish at the point $(\xi_1,\ldots,\xi_m)$ in the affine m-space over L. If X is a subset of I which generates the ideal, then D can be extended to a derivation $D' : A(\xi_1,\ldots,\xi_m) \to L$ satisfying $D'(\xi_i) = \eta_i$ if and only if for all $g \in X$,

$$g^D(\xi_1,\ldots,\xi_m) + \sum_{i=1}^{m} \frac{\partial g}{\partial x_i}(\xi_1\ldots,\xi_m)\eta_i = 0.$$

Proof. By Theorem 9, D can be extended so that $D(\xi_i) = \eta_i$ for all i if and only if the corresponding k-algebra homomorphism s can be extended to a k-algebra homomorphism $s' : A(\xi_1,\ldots,\xi_m) \to L[t]/(t^2)$ such that $s'(\xi_i) = \xi_i + \eta_i t$. So, it suffices to determine when $g^{s'}(\xi_1 + \eta_1 t,\ldots,\xi_m + \eta_m t) = 0$. If $\mathcal{M}(x_1,\ldots,x_m) = ax_1^{k_1}\cdots x_m^{k_m} \in A[x_1,\ldots,x_m]$ is a monomial, evaluating at the point $(\xi_1,\ldots,\xi_m)$ in affine m-space over L and then applying s' gives $(a + D(a)t)\,(\xi_1 + \eta_1 t)^{k_1}\cdots(\xi_m + \eta_m t)^{k_m}$. Since $t^2 = 0$, this expression simplifies to

$$s'\left(\mathcal{M}(\xi_1,\ldots,\xi_m)\right) = a\xi_1^{k_1}\cdots\xi_m^{k_m} + \left(D(a)\xi_1^{k_1}\cdots\xi_m^{k_m} + \sum_{i=1}^{m} k_i a\xi_1^{k_1}\cdots\xi_i^{k_i-1}\cdots\xi_m^{k_m}\eta_i\right)t. \quad (1.1)$$

Hence

$$s'(\mathcal{M}(\xi_1,\ldots,\xi_m)) = \mathcal{M}(\xi_1,\ldots,\xi_m) + t\left(\mathcal{M}^D(\xi_1,\ldots,\xi_m) + \sum_{i=1}^{m} \frac{\partial \mathcal{M}}{\partial x_i}(\xi_1,\ldots,\xi_m)\eta_i\right). \quad (1.2)$$

Recall that $g(\xi_1,\ldots,\xi_m) = 0$. Since g is a sum of monomials, $g^{s'}(\xi_1 + \eta_1 t,\ldots,\xi_m + \eta_m t) = 0$ if and only if Equation 1.2 equals 0 when $\mathcal{M}$ is replaced by g. □

Given a field extension K/k, Theorem 10 establishes the conditions for which a derivation from k to a K-module L can be extended to a derivation from K to L. In particular, we present three examples of applications of the theorem.

1.3.1 Example 1

Suppose K/k is a purely transcendental field extension of finite transcendence degree. Then there exist then $\xi_1,\ldots,\xi_n \in K$ such that $K = k(\xi_1,\ldots,\xi_n)$. The only element of $k[x_1,\ldots,x_n]$ which vanishes at the point $(\xi_1,\ldots,\xi_n)$ in the affine n-space over K is 0. Hence the ideal of vanishing as described in Theorem 10 is the 0 ideal. Thus for any field K and any element $\eta_1,\ldots,\eta_n \in K$, any derivation $D : k \to K$, extends to a derivation $D' : k(\xi_1,\ldots,\xi_n) \to K$ such that $D(\xi_j) = \eta_j$.

1.3.2 Example 2

Let $D : K \to L$ be a derivation with K and L subfields of a field F, and suppose $\xi \in L$ is separable over K. For any $\eta \in L$, D extends to a derivation $D' : K(\xi) \to L$ such that $D'(\xi) = \eta$ if and only if $f^D(\xi) + f'(\xi)\eta = 0$ where f is the minimal polynomial of ξ over K. Since ξ is separable, $f'(\xi) \neq 0$, so $\eta = -f^D(\xi) \cdot \left(f'(\xi)\right)^{-1}$. Thus there exists a unique extension of a derivation of a field to a derivation of a finite separable extension of that field.

1.3.3 Example 3

Using the notation above, if $\xi \in L$ is purely inseparable over K, by Theorem 6, $f'(\xi) = 0$ where f is the minimal polynomial of ξ over K. Hence for any $\eta \in L$, D can be extended to L so that $D(\xi) = \eta$ if and only if $f^D(\xi) = 0$. By Theorem 6 again, $f(x) = x^{p^e} - \alpha$ for some $\alpha \in K$, hence D can be extended to L if and only if $D(\alpha) = 0$.

Note that of these three examples, purely transcendental field extensions and finite separable field extensions are both examples of *formally smooth extensions* as defined in EGA (11, §17.1.1), while finite purely inseparable extensions are not. If L/K is a finite separable extension and $D : K \to K$ is the 0-derivation (i.e. $D(K) = 0$), then the comments above imply that D extends uniquely to the 0 derivation from L to K. An even stronger statement can be made:

Corollary 11. *(14, IV, §7, p.177) Let $L = K(\xi_1, \ldots, \xi_m)$ be an extension of fields. Then* 0 *is the only K-linear derivation from L to L if and only if L is a separable algebraic extension of K.*

Proof. One direction is already proven by the preceding paragraph. So suppose that L is not separable algebraic over K. Let $\{\xi_1, \ldots, \xi_r\}$ be a transcendency basis for L/K (with r possibly 0). There are two cases to consider. First, suppose L is not separable over $K(\xi_1, \ldots, \xi_r)$ then L is purely inseparable over Σ, where Σ is the separable closure of $K(\xi_1, \ldots, \xi_r)$ in L. Let E be the maximal proper subfield of L containing Σ. For any $\sigma \in L \setminus E$, $L = E(\sigma)$ by maximality. L must be purely inseparable over E by Corollary 7, hence σ has minimal polynomial over E

$x^{p^k} - \beta$ for some $\beta \in E$. By minimality, $x^{p^{k-1}} \notin E$. Define $\rho = \sigma^{p^{k-1}}$, so that $E(\rho) \supset E$. Hence $E(\rho) = L$ and $x^p - \beta$ is the minimal polynomial of ρ over E. By Example 1.3.3, the 0 derivation from E to L can be extended arbitrarily to a derivation from $L = E(\rho)$ to itself. In particular the extension of this derivation need not be 0.

On the other hand, suppose that L is separable over $K(\xi_1, \ldots, \xi_r)$. The ξ_i are algebraically independent over K, hence the 0 derivation from K to $K(\xi_1, \ldots, \xi_n)$ can be arbitrarily extended to a nonzero derivation from $K(\xi_1, \ldots, \xi_r)$ to itself, which then extends uniquely to a non-zero derivation from L to itself by the discussion preceding the corollary. □

Thus, just as classical Galois Theory can distinguish between separable extensions but not purely inseparable extensions, derivations cannot distinguish between separable extensions. In the following section the derivations are shown to distinguish between certain intermediate subfields of purely inseparable extensions.

1.4 The Jacobson-Bourbaki Theorem

Suppose k is a field and A and B are commutative k-algebras. Write $\mathrm{Hom}_k(A, B)$ for the k-vector space of k-linear homomorphisms from A to B. We make $\mathrm{Hom}_k(A, B)$ into a left B-module by, for any $b \in B$ and $\phi \in \mathrm{Hom}_k(A, B)$, then for all $a \in A$, $(b \cdot \phi)(a) = b\phi(a)$.

Lemma 12. *Let E/F and P/F be field extensions and let $Hom_F(E, P)$ be the P-vector space of F-linear homomorphisms from E to P. Then $\dim_F E < \infty$ if and only if $\dim_P Hom_F(E, P) < \infty$. In addition, if $\dim_F E < \infty$, then $\dim_F E = \dim_P Hom_F(E, P)$.*

Proof. See (14, I, §1, Theorem 1). □

If A is an algebra over a ring k, then for all $a \in A$, let $\lambda_a \in \mathrm{End}_k A$ be the endomorphism such that for all $f \in A$, $\lambda_a(f) = af$. Thus there is a ring homomorphism $\lambda : A \to \mathrm{End}_k A$ such that $\lambda(a) = \lambda_a$ for all $a \in A$. When convenient, we denote λ_a by a.

Theorem 13 (Jacobson-Bourbaki Theorem)**.** *(14, p.22 Theorem 2) Let P be a field and $\mathcal{U}$ a subset of the ring of additive endomorphisms of P, End(P). Suppose End(P) has the P-vector space structure as defined in above and suppose $\mathcal{U}$ satisfies the following three properties:*

1. *$\mathcal{U}$ is a subring with unity of End(P).*

2. *$\mathcal{U}$ is a left P-subspace of End(P) (i.e., $\lambda(P) \subset \mathcal{U}$).*

3. $\dim_P \mathcal{U} = n < \infty$.

Define $k = \{a \in P : \forall A \in \mathcal{U},\ \lambda_a A = A\lambda_a\}$. Then the following are true:

A) k is a subfield of P

B) $\dim_k P = n$

C) $\mathcal{U} = End_k(P)$

Proof. A) This is a straightforward computation. The proof is omitted.

B) By property 3, $\mathcal{U}$ is n-dimensional. For every $p \in P$, there exists a homomorphism η from End(P) to P such that, for any $f \in \mathrm{End}(P)$, $\eta(p)(f) = f(p) \in P$. Set η_p as the image of E by η. Let $B^\vee$ be the P-subspace of $\mathcal{U}^\vee := \mathrm{Hom}_P(\mathcal{U}, P)$ spanned by $\eta_\rho|_{\mathcal{U}}$ for every $\rho \in P$. The annihilator of $B^\vee$ is 0, hence $B^\vee = \mathcal{U}^\vee$ since $\mathcal{U}$ is finite-dimensional. There there exist a subset $\{\rho_1, \ldots, \rho_n\} \subset P$ such that $\eta_{\rho_1}, \ldots, \eta_{\rho_n}$ is a P-basis for $\mathcal{U}^\vee$. Let $E_1, \ldots, E_n$ be the dual basis in $\mathcal{U}^{\vee\vee} = \mathrm{Hom}_P(\mathcal{U}^\vee, P) \cong \mathcal{U}$. Thus, $E_i(\rho_j) = 1$ when $i = j$ and 0 otherwise. Since the E_i generate $\mathcal{U}$, $\rho \in k$ if and only if $\lambda_\rho E_i = E_i \lambda_\rho$ for all i. Now, for any $A \in \mathcal{U}$, there exist unique $\{\sigma_1, \ldots, \sigma_n\} \subset P$ with $A = \sum_{i=1}^{n} \lambda_{\sigma_i} E_i$. Hence $A(\rho_j) = \left(\sum_{i=1}^{n} \lambda_{\sigma_i} E_i\right)(\rho_j) = \sigma_j$, so

$$A = \sum_{i-1}^{n} A(\rho_i) \cdot E_i = \sum_{i=1}^{n} \lambda_{A(\rho_i)} E_i \tag{1.3}$$

Claim 14. *Each E_i sends P into k.*

Proof. Let $\sigma \in P$. By properties 1 and 2, $E_m \lambda_\sigma E_j \in \mathcal{U}$ for $1 \leq j$, $m \leq n$. Using Equation 1.3,

$$\begin{aligned} E_m \lambda_\sigma E_j &= \sum_{i=1}^{n} \lambda_{E_m \lambda_\sigma E_j(\rho_i)} E_i \\ &= \lambda_{E_m \lambda_\sigma (1)} E_j \\ &= \lambda_{E_m(\sigma)} E_j \end{aligned}$$

Equivalently, for all $\rho \in P$, $E_m(\sigma \cdot E_j(\rho)) = E_m(\sigma) \cdot E_j(\rho)$. Since σ and $E_j(\rho)$ commute, $E_m\left(E_j(\rho) \cdot \sigma\right) = E_m(\sigma) \cdot E_j(\rho) = E_j(\rho) E_m(\sigma)$. σ is arbitrary, hence $E_m \lambda_{E_j(\rho)} = \lambda_{E_j(\rho)} E_m$ which implies $E_j(\rho) \in k$. □

To finish proving B, we show that $\{\rho_1, \dots, \rho_n\}$ is a basis for P/k. Let $\sigma \in P$ and define $\sigma' = \sigma - \sum_{i=1}^{n} \rho_i E_i(\sigma)$. By the previous claim, $E_j(\sigma) \in k$, so for $1 \leq m \leq n$,

$$\begin{aligned} E_m(\sigma') &= E_m(\sigma) - E_m\left(\sum_{i=1}^{n} \lambda_{E_j(\sigma)}(\rho_i)\right) \\ &= E_m(\sigma) - \sum_{i=1}^{n} \lambda_{E_i(\sigma)} E_m(\rho_i) \\ &= E_m(\sigma) - E_m(\sigma) \text{ by Equation 1.3} \\ &= 0 \end{aligned}$$

Since $\iota_L \in \mathcal{U}$ and $\iota_L = \sum_{i=1}^{n} \lambda_i E_i$ for some $\lambda_i \in P$, the equation above implies $\sigma' = 0$. Hence $\sigma = \sum_{i=1}^{n} \rho_i E_i(\sigma) = \sum_{i=1}^{n} E_i(\sigma)\rho_i$, so σ is a k-linear combination of the ρ_i. Finally, if $\{\alpha_1 \dots, \alpha_n\} \subset k$ with $\sum_{i=1}^{n} \alpha_i \rho_i = 0$, then $\alpha_j = E_j\left(\sum_{i=1}^{n} \alpha_i \rho_i\right) = E_j(0) = 0$. Hence the ρ_i are linearly independent over k.

C) Every $A \in \mathcal{U}$ is k-linear, so $\mathcal{U} \subseteq \mathrm{End}_k(P)$. By B, $\dim_k P = n$, so Lemma 12 shows that $\dim_P \mathrm{End}_k(P) = \dim_k P = n$. $n = \dim_P \mathcal{U}$ as well, so $\mathcal{U} = \mathrm{End}_k(P)$.

□

Let L/K be a finite field extension. By the Jacobson-Bourbaki Theorem, there exists a one-to-one correspondence between intermediate subfields of L/K and finite-dimensional L-subalgebras of $\mathrm{End}_K L$. If L/K is a finite Galois extension with group of automorphisms G, then the homomorphism from the twisted group ring $L[G]$ to $\mathrm{End}_K L$ such that $\sum_{i=0}^{n} l_i g_i$ is sent to $\sum_{i=0}^{n} \lambda_{l_i} g_i$ for all $l_i \in L$ and $g_i \in G$ is a K-algebra isomorphism. Additionally, for any subgroup $H \subset G$, $L[H] \to \mathrm{End}_{K'} L$ is a K'-algebra isomorphism where K' is the fixed field of H. Thus, the Jacobson-Bourbaki Theorem can recover the lattice of subgroups for the Galois group of a finite Galois extension.

1.5 Lie Algebras of Derivations

Definition 15. *Let K be a field of characteristic $p > 0$ and suppose L/K is a finite purely inseparable extension. A **p-basis** for L/K is a minimal generating set for L as a K-algebra. A set $A \subset L$ is **p-independent over K** if A is a subset of a p-basis of L/K.*

It is not hard to show that the cardinality of any p-basis of a finite purely inseparable extension is an invariant of the extension (14, p.180).

If L/K is purely inseparable field extension, then it was shown in Theorem 6 that for any $\alpha \in L$, α has minimal polynomial $x^{p^e} - a$ where $a \in K$. e is called the **exponent of α over K** and denoted $\exp[\alpha : K]$.

Definition 16. *If L/K is a finite purely inseparable field extension, the integer* $\max_{\alpha \in L}\{\exp[\alpha : K]\}$ *is the **exponent of L over K**, denoted* $\exp[L : K]$.

Recall the familiar notion of a Lie algebra in (25, §7.1) for the following definition.

Definition 17. *Let k be a field of characteristic $p > 0$ and A a Lie algebra over k. A is called a **restricted p-Lie algebra** or just a **restricted Lie algebra** if there exists a set map $(-)^{[p]} : A \to A$ such that*

1. *For all $x, y \in A$, $\left[x^{[p]}, y\right] = [x\,[x\,[\cdots[x, y]]\cdots]]$, the pth iterated commutator.*

2. *For all $x \in A$ and $\alpha \in k$, $(\alpha x)^{[p]} = \alpha^p x^{[p]}$.*

3. *For all $x, y \in A$,*

$$(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x, y)$$

where $i \cdot s_i(x, y)$ is the coefficient of λ^{i-1} in the $(p-1)$-fold commutator

$$[\lambda x + y, [\cdots [\lambda x + y, x]] \cdots].$$

Proposition 18. *If k is a field of characteristic $p > 0$ and A is a k-algebra, then the set of derivations from A to A which are linear with respect to k form a restricted p-Lie algebra.*

Proof. If D, E are derivations from A to A, define $D^{[p]} = D^p$ and $[D, E] = D \circ E - E \circ D$. The proof that D^p and $[D, E]$ are derivations as well as the proof that these operators define a restricted p-Lie algebra structure on the derivations of A/k can be found in Jacobson (14, p.174). □

Denote the restricted Lie algebra of derivations from Proposition 18 by $\mathrm{Der}_k A$. Note that this restricted Lie algebra is also an A-submodule of the module of endomorphisms $\mathrm{End}_k A$. If E is a k-algebra, then the set of derivations from A to E which are linear with respect to k will be denoted $\mathrm{Der}_k(A, E)$. $\mathrm{Der}_k(A, E)$ is an E-module, where for any $D \in \mathrm{Der}_k(A, E)$, $a \in A$, and $e \in E$, $(eD)(a) = e \cdot D(a)$.

Let L/K be an extension of fields and $D \in \mathrm{Der}_K L$. Then the subset $L^D = \{a \in L : \lambda_a \circ D = D \circ \lambda_a\}$ is a subfield of L: Noting that $D(1) = 0$, if $a \in L^D$, then $aD\left(\frac{1}{a}\right) + \frac{1}{a}D(a) = D(1) = 0$.

Hence $D\left(\frac{1}{a}\right) = 0$ and $\frac{1}{a} \in L^D$. For any set of derivations $E \subset \mathrm{Der}_K L$, the elements of L which commute with every derivation in E, denoted L^E, is $\bigcap\limits_{D \in E} L^D$, which is also a subfield of L. L^E is called the **subfield of constants of** E.

Suppose E/k and P/k are field extensions of the field k in Proposition 18. For any set of derivations S from E/k to P/k, the subfield of constants of S will always contain $k(E^p)$. Thus if L/K is a finite purely inseparable field extension, then $\mathrm{Der}_K L = \mathrm{Der}_{KL^p} L$ and we may assume that E is purely inseparable of exponent ≤ 1 over the subfield of constants of $\mathrm{Der}_k(E, P)$.

Theorem 19. *Let P be a field of characteristic $p > 0$, and $k \subseteq E \subseteq P$ a filtration of P such that P/k and E/k are finite purely inseparable extensions. If B is a p-basis of E/k and $\delta : B \to P$ is an arbitrary set map, then there exists a unique derivation $D : E/k \to P/k$ such that for all $\epsilon \in B$, $D(\epsilon) = \delta(\epsilon)$.*

Proof. See (14, IV, §7, Theorem 17). □

Corollary 20. *(14, IV, §7, Corollary 1)* $\dim_P$ *Der*$_k(E, P) < \infty$ *if and only if E/k has a finite p-basis B. Additionally, if B is a finite p-basis of E/k, then $|B| = \dim_P$ Der$_k(E, P)$.*

Proof. Let B be a p-basis for E/k and define $\Delta(B, P)$ to be the P-vector space of set maps from B to P. By Theorem 19, each element of $\Delta(B, P)$ lifts to an element $\mathrm{Der}_k(E, P)$. Hence define a map $\mathrm{Der}_k(E, P) \to \Delta(B, P)$ by sending $D \in \mathrm{Der}_k(E, P)$ to $D|_B$. This map is a P-vector space isomorphism by the previous theorem, so $\dim_P \mathrm{Der}_k(E, P) = \dim_P \Delta(B, P)$. If $|B|$ is infinite, then viewing $\Delta(B, P)$ as the dual space to an infinite-dimensional P-vector space with basis B, $\dim_P \Delta(B, P)$ is infinite. If B is finite, then $B = \{\beta_1 \ldots, \beta_n\}$ for some

$\beta_i \in E$, so the maps $\{\delta_i\}_{1\leq i\leq n}$ form a P-basis for $\Delta(B, P)$ where $\delta_i(\beta_j) = 1$ if $i = j$ and 0 otherwise. □

Theorem 21 (Jacobson Galois Theory)**.** *(14, IV, §8, Theorem 19) Let P be a field of characteristic $p > 0$, and let $\mathcal{D}$ be a restricted p-Lie algebra of derivations of P with $\dim_P \mathcal{D} = m < \infty$. The following properties hold:*

1. *If k is the subfield of constants of $\mathcal{D}$, then P is purely inseparable over k, $\exp[P : k] \leq 1$, and $\dim_k P = p^m$.*
2. *If $D \in Der_k P$, then $D \in \mathcal{D}$*
3. *If $\{D_1, \ldots, D_m\}$ is a P-basis for $\mathcal{D}$, then $\{D_1^{k_1} \cdots D_m^{k_m}\}_{0\leq k_i<p}$ is a P-basis for $End_k P$*

Proof. Define $B := \left\{D_1^{k_1} \cdots D_m^{k_m}\right\}_{0\leq k_i<p}$. Let $\mathcal{U}$ be the P-vector subspace of $\mathrm{End}(P)$ generated by elements of B. Then $\dim_P \mathcal{U} < \infty$, and in fact $\dim_P \mathcal{U} \leq p^m$. We seek to show that $\mathcal{U}$ is a ring. Since $D_1^0 \cdots D_m^0 = \mathrm{id}_P$, $1 \in \mathcal{U}$, so it suffices to show that $\mathcal{U}$ is closed under composition. Let $\rho \in P$ and $j \in \mathbb{N}$ such that $1 \leq j \leq m$. Then $D_j\left(\lambda_\rho D_1^{k_1} \cdots D_m^{k_m}\right) = D_j(\rho) \cdot D_1^{k_1} \cdots D_m^{k_m} + \lambda_\rho D_j D_1^{k_1} \cdots D_m^{k_m}$ by Leibniz's Rule. The first term in the sum is in $\mathcal{U}$, so it suffices to prove the following claim.

Claim 22. *Call $N = k_1 + k_2 + \cdots + k_m$ the* order *of $D_1^{k_1} \cdots D_m^{k_m}$. Then $D_j D_1^{k_1} \cdots D_m^{k_m}$ is a P-linear combination of endomorphisms $D_1^{i_1} \cdots D_m^{i_m}$ of order $\leq N + 1$.*

Proof. When $N = 0$, then $D_j 1 = D_j$, an order 1 element of $\mathcal{U}$. Assume every endomorphism $D_j D_1^{l_1} \cdots D_m^{l_m}$ is a P-linear combination of monomials $D_1^{i_1} \cdots D_m^{i_m}$ of order $\leq N$ whenever $l_1 + \cdots + l_m < N$. Proceed by induction:

j=1: For $k_1 < p-1$, $D_j D_1^{k_1} \cdots D_m^{k_m} = D_1^{k_1+1} \cdots D_m^{k_m}$, a monomial of order $N+1$. For $k_1 = p-1$, $D_1 D_1^{k_1} \cdots D_m^{k_m} = D_1^p \cdots D_m^{k_m}$. Since $\mathcal{D}$ is a restricted Lie algebra, it is closed under pth powers, hence $D_1^p = \sum_{i=1}^{m} \mu_i D_i$ where $\mu_i \in P$ for each i. Hence $D_1^p \cdots D_m^{k_m} = \sum_{i=1}^{m} \mu_i D_i D_2^{k_2} \cdots D_m^{k_m}$. Each term of this sum has order $N - k_1 + 1 = N - (p-1) + 1 \leq N < N+1$, so Claim 22 is satisfied when $j = 1$.

We make the following claim: For any $j \leq l$, $D_j D_1^{k_1} \cdots D_m^{k_m}$ is a P-linear combination of elements of B of order $\leq N+1$ when $k_1 + \cdots + k_m = N$. The $l = 1$ case is proven above, which proves the base case for this claim. Assume this statement is true for all $l \leq N$ and proceed by induction. To prove this claim, first note that we are working under the assumption that $N > 0$, so there exists an i such that $k_i > 0$. Let $j = N+1$ and let r be the minimal integer with $k_r > 0$. Then $D_j D_1^{k_1} \cdots D_m^{k_m} = D_j D_r^{k_r} \cdots D_m^{k_m}$. The proof breaks down into multiple cases:

1. $j < r$: Then $D_j D_r^{k_r} \cdots D_m^{k_m}$ is an element of B.

2. j=r: This case was proven in the $j = 1$ discussion above.

3. $j > r$: $\mathcal{D}$ is closed under commutators, so $[D_j, D_r] = D_j D_r - D_r D_j = \sum_{i=1}^{m} \nu_{i,r,j} D_i$ with $\nu_{i,r,j} \in P$. Hence, $D_j D_r^{k_r} \cdots D_m^{k_m} = D_j D_r D_r^{k_r - 1} \cdots D_m^{k_m} = D_r D_j D_r^{k_r-1} \cdots D_m^{k_m} + \sum_{i=1}^{m} \nu_{i,r,j} D_i D_r^{k_r-1} \cdots D_m^{k_m}$. Every term in the last sum is of order N, so by the first inductive hypothesis this sum is a P-linear combination of elements of B of order $\leq N$. By the second inductive hypothesis, $D_r D_j D_r^{k_r-1} \cdots D_m^{k_m}$ can also be written as linear combinations of elements of B of order $\leq N+1$. This finishes the proof of Claim 22.

□

Hence $\mathcal{U}$ is a P-subalgebra of $\mathrm{End}(P)$. Applying the Jacobson-Bourbaki Theorem, if $k \subset P$ is the subfield of constants of $\mathcal{U}$, then $\dim_k P = \dim_P \mathcal{U} \leq p^m$ and $\mathcal{U} = \mathrm{End}_k(P)$. Since the D_i generate $\mathcal{U}$, for any $r \in P$ and $A \in \mathcal{U}$, $\lambda_r A = A\lambda_r$ if and only if for all $1 \leq i \leq m$, $\lambda_r D_i = D_i \lambda_r$. By Leibniz's rule, $D_i \lambda_r = \alpha_{D_i(r)} + \lambda_r D_i$, hence $\lambda_r D_i = D_i \lambda_r$ if and only if $\lambda_{D_i(r)} = 0$, or $D_i(r) = 0$. Thus k is the subfield of constants of $\mathcal{D}$ and by the comments after Proposition 18, P is purely inseparable of exponent ≤ 1 over k. So $\dim_k P = p^{m'}$ where m' is the cardinality of a p-basis of P/k. Hence $m' \leq m$ and $\dim_P \mathrm{Der}_k(P) = m'$ by Corollary 20.

$\mathcal{D} \subset \mathrm{Der}_k(P)$, so $m \leq m'$. Hence $m' = m$ and these vector spaces are equal, proving 1 and 2 of the theorem. Lastly, since $\mathcal{U} = \mathrm{End}_k(P)$ and $\dim_P \mathcal{U} = p^m$, the fact that the elements of B generate $\mathcal{U}$ as a P-vector space and $|B| = p^m$ imply that the elements of B are P-linearly independent, proving 3. □

The previous theorem shows that if P/k is a finite purely inseparable extension of fields of exponent 1, then there is a $1-1$ correspondence between intermediate subfields of P/k and restricted Lie subalgebras of $\mathrm{Der}_k P$. Gerstenhaber (7) simplified Theorem 21 by proving that if $\mathcal{D}$ is a finite-dimensional P-vector subspace of endomorphisms of P which is closed under pth powers, then it is also closed under the Lie bracket.

CHAPTER 2

SWEEDLER'S MODULAR FIELD THEORY

2.1 The Automorphism Scheme of a Field Extension

Suppose K/k is a field extension. The functor $\underline{\mathrm{Aut}}_{K/k}$ from the category of k-algebras to the category of groups, sends a k-algebra T to the group of automorphisms $\mathrm{Aut}_T(K \otimes_k T)$. When K/k is a finite field extension, then this functor is representable (2, Proposition 1) by a k-algebra A, and Spec A is called the **automorphism scheme of** K/k. Note that Spec A is a group scheme, since it represents a group-valued functor.

When K/k is a Galois extension, then the automorphism scheme is discrete and isomorphic to Spec $K \times_k \cdots \times_k$ Spec K where the number of copies of Spec K is equal to the cardinality of the Galois group of K/k. On the other hand, if K/k is a finite purely inseparable extension, then the automorphism scheme will be much larger. For example, suppose $K = k(\alpha)$ where $\exp[\alpha : k] = 1$. Then the automorphism scheme of K/k is Spec $k[t_1, \ldots, t_p]$ (4, Corollary 2.7). It follows that the automorphism scheme of any finite purely inseparable field extension has finite dimension. Hasse-Schmidt derivations on finite purely inseparable extensions, which we describe next, will be shown to be points of the automorphism scheme of the field extension.

2.2 Higher Derivations, Definition and Properties

Definition 23. *(12) Let k be a ring and A a k-subalgebra of a k-algebra B. A **Hasse-Schmidt derivation of rank** $m+1$ **from** A **to** B or **higher derivation of rank** $m+1$ is a sequence* *of additive k-linear homomorphisms in Hom$_k(A, B)$, $\left(\iota_A = D_0^{(m+1)}, D_1^{(m+1)}, \ldots D_m^{(m+1)}\right)$, satisfying the property that $D_i^{(m+1)}(aa') = \sum_{j=0}^{i} D_j^{(m+1)}(a)D_{i-j}^{(m+1)}(a')$ for all $a, a' \in A$. A Hasse-Schmidt derivation from A to B of* ***infinite rank*** *is an infinite sequence of endomorphisms in End$_k(A, B)$, $(\iota_A = E_0, E_1, \ldots)$ such that $E_i(aa') = \sum_{j=0}^{i} E_j(a)E_{i-j}(a')$ for all $a, a' \in A$.*

Suppose $D^{(m+1)} = (\iota_A, D_1, \ldots, D_m)$ is a higher derivation of rank $m+1$ from A to B. Define a map from A to $B[t]/\left(t^{m+1}\right)$ by sending $a \in A$ to $a + D_1(a)t + D_2(a)t^2 + \cdots + D_m(a)t^m$. Note that for $a, a' \in A$,

$$\begin{aligned}
\left(a + D_1(a)t + \cdots + D_m(a)t^m\right)\left(a' + D_1(a')t + \cdots + D_m(a')t^m\right) &= \sum_{i=0}^{m}\sum_{j=0}^{n}\left(D_j(a)D_{i-j}(a')\right)t^i \\
&= \sum_{i=0}^{m} D_i(aa')t^i
\end{aligned}$$

Therefore, a higher derivation of rank $m+1$ is equivalent to a k-linear algebra homomorphism from A to $B[t]/(t^{m+1})$ which is the identity modulo (t). Likewise, a higher derivation of infinite rank from A to B is equivalent to a k-algebra homomorphism from A to $B[[t]]$ which is the identity modulo (t). These k-linear algebra homomorphisms will be called *Hasse-Schmidt homomorphisms* or *higher derivation homomorphisms*.

The minimum $i \neq 0$ such that $D_i \neq 0$, if it exists, is called the **order of** $D^{(m+1)}$. If not such i exists, then $D^{(m+1)}$ is called **trivial**. Note that $D_1^{(m+1)}$ is a derivation from A to B, and derivations from A to B which are linear with respect to k are in $1-1$ correspondence with Hasse-Schmidt derivations from A to B of rank 2.

Let $K \subseteq L$ be fields and $D^{(m)} : K \to L$ a Hasse-Schmidt derivation of rank $m \leq \infty$. It is easy to show that the subset $K^{D^{(m)}} = \{\alpha \in K : D^{(m)}(\alpha) = \alpha\}$ is a subfield of K: $D^{(m)}$ can be viewed as a ring homomorphism from K to $L[t]/(t^m)$ (resp. $L[[t]]$). If a, $b \in K^{D^{(m)}}$, then clearly $a+b$ and ab are in $K^{D^{(m)}}$. Suppose $u \in K^{D^{(m)}}$. $1 = D^{(m)}(1) = D^{(m)}(uu^{-1}) = D^{(m)}(u)D^{(m)}(u^{-1}) = uD^{(m)}(u^{-1})$. Hence $u^{-1} = D^{(m)}(u^{-1})$, so $u^{-1} \in K^{D^{(m)}}$. $K^{D^{(m)}}$ is called the **subfield of constants of** $D^{(m)}$. If $\mathcal{D}$ is a set of higher derivations from K to L, then the intersection of the subfield of constants of every higher derivation in $\mathcal{D}$ is called the **subfield of constants of** $\mathcal{D}$.

Hasse-Schmidt derivations can behave very differently depending on the characteristic of the fields or algebras on which they act. Depending on the algebras, Hasse-Schmidt derivations of certain ranks may not even exist. Some of these differences can be illustrated through two examples.

2.2.1 Example 1

Let $B = k[x]$ where k is a field and suppose x is transcendental over k. The homomorphism $\overline{D} : B \to B[[t]]$ which sends $f(x) \in B$ to $f(x+t) \in B[[t]]$ is a higher derivation homomorphism of infinite rank. This higher derivation is just the classical Taylor series expansion (6, p.3). If the characteristic of k is 0, then $\overline{D}$ can be viewed as the sequence of endomorphisms $\left(1, \frac{d}{dx}, \frac{1}{2!}\left(\frac{d}{dx}\right)^2, \frac{1}{3!}\left(\frac{d}{dx}\right)^3, \ldots\right)$.

2.2.2 Example 2

Let k be a field of characteristic $p > 0$ and $K = k(\rho)$ a purely inseparable extension of exponent e. Then there exists $\alpha \in k$ such that $\rho^{p^e} = \alpha$ and K is isomorphic as a k-algebra to $k[x]/(x^{p^e} - \alpha)$. Let $D : K \to K[t]/(t^{p^e})$ be the additive map such that $D(\rho^i) = (\rho + t)^i$ for all i and $D(a) = a$ for all $a \in k$. D is well-defined as a k-algebra homomorphism (and is therefore a Hasse-Schmidt homomorphism) provided that $D(\rho^{p^e} - \alpha) = 0$. This equation is satisfied because

$$D(\rho^{p^e} - \alpha) = (\rho + t)^{p^e} - \alpha = \rho^{p^e} + t^{p^e} - \alpha = \alpha - \alpha = 0.$$

Furthermore, let $V : K[t]/(t^{p^e}) \to K[t]/(t^{p^{e+1}})$ be the K-algebra homomorphism given by $V(t) = t^p$. Then the composition $V \circ D : K \to K[t]/(t^{p^{e+1}})$ is a higher derivation homomorphism of rank p^{e+1}. Composing D with a finite number of copies of V will result in higher derivations whose rank is larger than the rank of D. However, for finite purely inseparable extensions, higher derivations must be of finite rank, distinguishing them from higher derivations of transcendental extensions.

Theorem 24. *(14, p.194) Let L/k be an algebraic field extension, and K an intermediate subfield. Suppose $D^{(m+1)}$ is a Hasse-Schmidt derivation of rank $m + 1$ and order q from K/k to L/k and suppose Γ is the subfield of constants of $D^{(m+1)}$. If e is the smallest integer such that $p^e > \frac{m}{q}$, then K is purely inseparable of exponent e over Γ.*

Proof. Denote $D^{(m+1)}$ by the sequence of k-linear homomorphisms $(id_K,\, 0,\, \ldots, 0,\, D_q,\, D_{q+1},\, \ldots D_m)$. For any $g \in K$,

$$D^{(m+1)}(g^{p^e}) = (g + D_q(g)t^q + \cdots D_m(g)t^m)^{p^e} = g^{p^e} + D_q(g)t^{p^e q} + \cdots + D_m(g)t^{p^e m}.$$

As $p^e q > m$, $D^{(m+1)}(g^{p^e}) = g^{p^e}$. Hence $g^{p^e} \in \Gamma$ and K is of exponent at most e over Γ. Further, suppose $f \neq \Gamma$ and $D_q(f) \neq 0$. Then $D^{(m+1)}(f) \neq f$. Also, by minimality of e, $D_q(f)^{p^{e-1}} \neq 0$. Hence $D^{(m+1)}(f^{p^{e-1}}) \neq f^{p^{e-1}}$, so $f^{p^{e-1}} \notin \Gamma$. and K is of exponent at least e over Γ. □

Thus for any finite rank Hasse-Schmidt derivation D from a field L to itself, L is purely inseparable of finite exponent over the subfield of constants of D. It follows that if $\mathcal{D}^{(m+1)}$ is a set of Hasse-Schmidt derivations of rank $m+1 < \infty$ from L to itself, then L is again purely inseparable over the intersection of the subfields of constants of the higher derivations in $\mathcal{D}^{(m+1)}$.

Let $(id_L, E_1, \ldots, E_m) = E : L \to L[t]/(t^{m+1})$ be a higher derivation of order $m+1$. E extends to a $k[t]/(t^{m+1})$-linear ring endomorphism $\overline{E}$ of $L[t]/(t^{m+1})$ where $\overline{E}\left(\sum_{i=1}^{m} l_i t^i\right) = \sum_{i=1}^{m} E(l_i)t^i$ for any $l_i \in L$. Since $E(l_i)(\text{mod } t) = l_i$, the constant term of $\overline{E}\left(\sum_{i=1}^{m} l_i t^i\right)$ is l_0, hence $\overline{E}$ is injective. Next, let $\xi = l_0 + l_1 t + \cdots + l_m t^m$. Then $\xi - \overline{E}(l_0) = l'_1 t + l'_2 t^2 + \cdots + l'_m t^m$ for some $l'_i \in L$. Further, $\xi - \overline{E}(l_0) - \overline{E}(l'_1 t) = l''_2 t^2 + l''_3 t^3 + \cdots + l''_m t^m$, and by iteration $\xi - \overline{E}(l_0) - \overline{E}(l'_1 t) - \cdots - \overline{E}(l_n^{(n)} t^n) = l_{n+1}^{(n+1)} t^{n+1} + l_{n+2}^{(n+1)} t^{n+2} + \cdots + l_m^{(n+1)} t^m$. Eventually, $\xi - \overline{E}(l_0 + l'_1 t + \cdots) = 0$, so $\overline{E}$ is surjective.

Hence any higher derivations from L to itself of order $m+1$ which are linear with respect to k extend to a automorphisms of $L[t]/(t^{m+1})$. On the other hand, any automorphism $\overline{E}$

of $L[t]/(t^m)$ satisfying $\overline{E}(a) = a(\text{mod } t)$ corresponds to a higher derivation homomorphism by restriction of $\overline{E}$ to L. In particular, if $\overline{E}(a) = a(\text{mod } t)$, then $\overline{E}^{-1}(a)(\text{mod } t) = a$, so the restriction of $\overline{E}^{-1}$ to L is a higher derivation homomorphism. Thus we have proven the following theorem:

Theorem 25. *Let L/k be a finite purely inseparable field extension. The higher derivations of L of order $m+1$ which are linear with respect to k are in $1-1$ correspondence with the subgroup of automorphisms of $Aut_{k[t]/(t^m)}\left(L[t]/(t^{m+1})\right)$ which are the identity modulo (t).*

The subgroup described in the theorem above will be denoted $\mathbf{HDer}_k^{m+1}L$ and will be called the **group of higher derivations of** L/k **of order** $m+1$. We remark that any higher derivation of order $m+1$ from L to itself is equivalent to a $k[t]/(t^{m+1})$-linear automorphism of $L[t]/(t^{m+1})$. Therefore, by the discussion in Section 2.1, $\text{HDer}_k^{m+1}L = \underline{\text{Aut}}_{L/k}\left(k[t]/(t^{m+1})\right)$.

Based on the above theorem, if A is a ring and B is an A-algebra, any higher derivation of B of rank $m+1$ which is linear with respect to A can be viewed as an element of $\text{End}_{A[t]/(t^m)}B[t]/\left(t^{m+1}\right)$, and the group operation in $\text{HDer}_A^{m+1}B$ is the same as multiplication in this ring.

Proposition 26. *Let A be a commutative ring and B a commutative A-algebra. Suppose $\overline{D} = 1 + D_1t + D_2t^2 + \cdots D_mt^m$ is a Hasse-Schmidt homomorphism in $HDer_A^{m+1}B$. If D_i is the first non-zero endomorphism of B of this higher derivation, then D_i is an A-linear derivation of B.*

Proof. Let b_1, $b_2 \in B$. By definition, $D_i(b_1b_2) = \sum_{j=0}^{i} D_j(b_1)D_{i-j}(b_2)$. Since $D_j = 0$ for $0 < j < i$,

$$D_i(b_1b_2) = D_0(b_1)D_i(b_2) + D_i(b_1)D_0(b_2) = b_1D_i(b_2) + D_i(b_1)b_2.$$

D_i is A-linear and satisfies Leibnitz's rule, hence it is a derivation of B/A. □

Proposition 27. *Let $\overline{D} = (1, D_1, \ldots, D_m)$ and $\overline{E} = (1, E_1, \ldots, E_m)$ be elements of $HDer_A^m B$ such that $D_i = E_i$ for $1 \leq i < m$. Then $D_m - E_m$ is a derivation of B over A.*

Proof. Let b_1, $b_2 \in B$. Then

$$(D_m - E_m)(b_1b_2) = \sum_{i=0}^{m} D_i(b_1)D_{m-i}(b_2) - E_i(b_1)E_{m-i}(b_2).$$

All middle terms will vanish to leave $b_1D_m(b_2) - b_1E_m(b_2) + D_m(b_1)b_2 - E_m(b_1)b_2$ which proves $D_m - E_m$ obeys Leibniz's rule. □

Corollary 28. *Let $\overline{D}$ be a higher derivation of rank m from A to B. Then extensions of $\overline{D}$ to higher derivations of rank $m+1$ from A to B form a torsor under the set of derivations.*

It is not true that any higher derivation of from A to B of rank m lifts to a higher derivation of rank $m+1$. If A is 0-*smooth* (16, p.193), then every higher derivation lifts. However, not every purely inseparable field extension is 0-smooth, so we are not guaranteed a lifting to higher order higher derivations.

We end this section by defining a type of higher derivation which is commonly studied. Let k be a field and A a k-subalgebra of a k-algebra B. An **iterative higher derivation of order** $m+1$, $(\iota_A,\, D_1, \ldots, D_m)$ is a higher derivation such that $D_i \circ D_j = \binom{i+j}{j} D_{i+j}$ for all $i,\, j$. For instance, Example 2.2.1 is an iterative higher derivation.

2.3 Sweedler Diagrams

Sweedler's early work on purely inseparable extensions prompted much of the study of Galois-type correspondences that followed. Let K/k be a finite purely inseparable field extension of exponent e. Then there exists the following filtration of K:

$$k \subset k^{1/p} \cap K \subset k^{1/p^2} \cap K \subset \cdots \subset k^{1/p^{e-1}} \cap K \subset k^{1/p^e} \cap K = K \tag{2.1}$$

To simplify notation, let $k_i := k^{1/p^i}$ and $K_i := k^{1/p^i} \cap K$. Using this filtration, Sweedler (24) describes a procedure to fill out an $e \times e$ grid with elements of K. In the (1, 1)th position of the grid place a p-basis for K/K_{e-1}. Call this set $S_{1,\,1}$. Take the pth powers of the elements of $S_{1,\,1}$. Call this set $S^p_{1,\,1}$. These are elements in K_{e-1}, so let $S_{2,\,1}$ be a maximal subset of $S^p_{1,\,1}$ which is p-independent over K_{e-2}. Finally, let $S_{2,\,2}$ be a subset of K_{e-1} which, when taken in a union with $S_{2,\,1}$, forms a full p-basis for K_{e-1}/K_{e-2}.

In general, suppose the ith row of the grid has been filled with elements of K so that $S_{i,\,1} \cup S_{i,\,2} \cup \cdots \cup S_{i,\,i}$ is a p-basis for K_{e-i+1}/K_{e-i}. Then $S^p_{i,\,1} \cup S^p_{i,\,2} \cup \ldots \cup S^p_{i,\,i}$ is a subset of K_{e-i}. Take a maximal subset of $S^p_{i,\,1} \cup S^p_{i,\,2} \cup \ldots \cup S^p_{i,\,i}$ which is p-independent over K_{e-i-1}. If α^p is an element in this maximal subset and α appears in entry $(i,\, j)$ of the grid, then α^p will be an element of $S_{i+1,\,j}$. In $S_{i+1,\,i+1}$ put elements of K_{e-i} which extend $S_{i+1,\,1} \cup \cdots \cup S_{i+1,\,i}$ to a full p-basis for K_{e-i}/K_{e-i-1}. Once this procedure has been completed for each row of the grid, it will be called a **Sweedler Diagram for** K/k. Note it is certainly not unique because of the various choices of p-bases that are made. The following examples illustrate how to construct these diagrams.

1. Let k_0 be a perfect field of characteristic $p > 0$ with X a transcendental element over k_0. Define $K = k_0(X)$ and $k = k_0(X^{p^e})$. Then $K_i = k_0(X^{p^{e-i}})$. Thus a Sweedler Diagram for K/k has

X
X^p
$\vdots$
$X^{p^{e-1}}$

   for its first column, and the rest of the $e - 1$ columns are empty.

2. Let k_0 be a perfect field of characteristic $p > 0$ with X and Y algebraically independent over k_0. Define $K = k_0(X, Y)$ and let $k = k_0(X^p, Y^{p^2})$. K/k is a degree p^3 extension of exponent 2, and $K_1 = k_0(X, Y^p)$. Hence a Sweedler Diagram for this extension is

Y	
Y^p	X

3. Let k_0 be a perfect field of characteristic $p > 0$ with X, U and Z algebraically independent over k_0. Define $K = k_0(X, U, Z)$ and $k = k_0(X, U^p - XZ^p, Z^{p^2})$. K/k is an

exponent 2 extension, and $K_1 = k_0(X^{1/p},\, U - X^{1/p}Z,\, Z^p) \cap K = k_0(X,\, U^p - XZ^p,\, Z^p) = k_0(X,\, U^p,\, Z^p)$. A Sweedler Diagram for this extension is

U, Z	
Z^p	

4. Let k_0 again be a perfect field of characteristic $p > 0$ with X, U, Z algebraically independent over k_0. Define $K = k_0(X,\, Z,\, U)$ and $k = k_0(X^p,\, U^p - X^pZ^p,\, Z^{p^2})$. K/k is an exponent 2 extension with $K_1 = k_0(X,\, U - XZ,\, Z^p)$. A Sweedler Diagram for K/k is thus

U	
U^p	X, $U - XZ$

5. k_0 is again a perfect field of characteristic $p > 0$ with X, U, Z algebraically independent over k_0. Suppose $\alpha \in k_0(X,\, U,\, Z)$, but $\alpha \notin k_0(X^p,\, U^p,\, Z^p)$. Define $K = k_0(X,\, Z,\, U)$ and $k = k_0(X^p,\, Z^p - \alpha U^{p^2},\, U^{p^3})$. K/k is an exponent 3 extension with $K_1 = k_0(X,\, Z^p - \alpha U^{p^2},\, U^{p^2}) = k_0(X,\, Z^p,\, U^{p^2})$ and $K_2 = k_0(X,\, Z,\, U^p)$. A Sweedler Diagram for K/k is thus

U		
U^p	Z	
U^{p^2}		X

If an element $\alpha \in K$ first appears in $S_{i,\,i}$ of a Sweedler Diagram, then define $c(\alpha) := i$ and $l(\alpha)$ as the number of rows that α or its pth powers appear in the Sweedler Diagram. Since a

Sweedler Diagram is constructed from successive p-bases, it is clear that $S_{1,\,1} \cup S_{2,\,2} \cup \cdots \cup S_{e,\,e}$ is a p-basis for K/k.

There are a few properties of the Sweedler Diagram worth noting. First, any entry $(i,\, j)$ with $j > i$ will be empty. Second, let K/k be a finite purely inseparable field extension of exponent e. Entry $S_{1,\,1}$ will contain a p-basis for K/K_{e-1}. Since $K_{e-1}^p \subseteq K_{e-2}$, then $S_{1,\,1}^p$ generates $K^p \cdot K_{e-2}$ over K_{e-2}. $S_{2,\,1}$ is a maximal p-independent subset of $S_{1,\,1}^p$ over K_{e-2}, hence the elements in $S_{2,\,1}$ form a p-basis of the field extension $K^p \cdot K_{e-2}/K_{e-2}$. By construction, the entries of $S_{2,\,2}$ are elements of K_{e-1} such that $S_{2,\,2} \cup S_{2,\,1}$ is a full p-basis of K_{e-1}/K_{e-2}. $S_{2,\,2}$ will contain no elements of K^p, so the entries of $S_{2,\,2}$ form a p-basis of the field extension $K_{e-1}/K^p \cdot K_{e-2}$.

By the same reasoning, the elements of $S_{3,\,1}$ form a p-basis of $K^{p^2} \cdot K_{e-3}/K_{e-3}$, elements of $S_{3,\,2}$ form a p-basis of $K_{e-1}^p \cdot K_{e-3}/K^{p^2} \cdot K_{e-3}$, and elements of $S_{3,\,3}$ form a p-basis for $K_{e-2}/K_{e-1}^p \cdot K_{e-3}$. When these field extensions are put into an array the pattern becomes clearer:

TABLE I: Field Extensions Represented in the Sweedler Diagram

K/K_{e-1}			
$K^p \cdot K_{e-2}/K_{e-2}$	$K_{e-1}/K^p \cdot K_{e-2}$		
$K^{p^2} \cdot K_{e-3}/K_{e-3}$	$K_{e-1}^p \cdot K_{e-3}/K^{p^2} \cdot K_{e-3}$	$K_{e-2}/K_{e-1}^p \cdot K_{e-3}$	
$K^{p^3} \cdot K_{e-4}/K_{e-4}$	$K_{e-1}^{p^2} \cdot K_{e-4}/K^{p^3} \cdot K_{e-4}$	$K_{e-2}^p \cdot K_{e-4}/K_{e-1}^{p^2} \cdot K_{e-4}$	$K_{e-3}/K_{e-2}^p \cdot K_{e-4}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Hence, when $j > 1$ the elements in entry $S_{i,\,j}$ of the Sweedler Diagram form a p-basis for the extension

$$K_{e-j+1}^{p^{i-j}} \cdot K_{e-i-1} / K_{e-j+2}^{p^{i-j+1}} \cdot K_{e-i}, \tag{2.2}$$

and when $j = 1$ the elements of $S_{i,1}$ form a p-basis for $K^{p^{i-1}} \cdot K_{e-i-1}/K_{e-i}$.

2.4 Modular Field Extensions

Sweedler first proved the following theorem (24, Theorem 1), which relates Hasse-Schmidt derivations to certain intermediate subfields of finite purely inseparable extensions.

Theorem 29. *Let k be a field of characteristic $p > 0$ and suppose K/k is a finite purely inseparable extension of exponent e. Let N be the union of the diagonal entries of a Sweedler Diagram for K/k. The following are equivalent:*

1. $\displaystyle\bigotimes_{x \in N} k(x) \cong K$.
2. *There exist higher derivations of K for which k is the subfield of constants.*
3. *K^{p^i} is linearly disjoint from k for all positive integers i.*
4. *For all $x \in N$, $l(x) = e - c(x) + 1$ recalling that $c(x)$ is the row number of the Sweedler Diagram where x first appears and $l(x)$ is the number of rows of the Sweedler Diagram that an element of the set $\{x, x^p, x^{p^2}, \ldots\}$ appears.*
5. *$\{x^{p^{e-c(x)}} : x \in N\}$ forms a p-basis for $k^{1/p} \cap K$ over k.*

Proof. $\underline{1 \Rightarrow 2}$: Suppose $K \cong k(\xi_1) \otimes \cdots \otimes k(\xi_n)$. Let $K_i = k(\xi_1) \otimes \cdots \otimes \widehat{k(\xi_i)} \otimes \cdots \otimes k(\xi_n)$. Then K is purely inseparable over K_i with p-basis $\{\xi_i\}$. Hence by Example 2 there is a higher derivation of K which vanishes on K_i. Call this higher derivation D_i. The subfield of constants of all the D_i is $K_1 \cap \cdots \cap K_n = k$.

$\underline{2 \Rightarrow 3}$: Let $D = (1, D_1, \ldots, D_m)$ be a higher derivation of K. Since D can be viewed as a ring homomorphism from L to $L[t]/(t^{m+1})$, for $x \in K$, if $p|m$, then $D_m(x^p) = \big(D_{m/p}(x)\big)^p$, and if p does not divide m, then $D_m(x^p)$ must be 0. Therefore $D_m(K^{p^n}) \subseteq K^{p^n}$.

Now, suppose there exists a positive integer n so that k and K^{p^n} are not linearly disjoint. Then there is a minimal length relation $k_1\alpha_1 + \cdots + k_t\alpha_t = 0$ where the elements of $\{k_i\} \subset k$ are linearly independent over $k \cap K^{p^n}$ and $\{\alpha_i\} \subset K^{p^n}$. Divide the relation by α_1 and relabel to get a relation

$$k_1 + k_2\alpha_2 + \cdots k_t\alpha_t = 0. \tag{2.3}$$

By the linear independence of the k_i, there is some $\alpha_i \notin k \cap K^{p^n}$. Relabel the α_i's and k_i's so that $a_2 \notin k \cap K^{p^n}$. Thus by assumption there exists a higher derivation E such that $E(\alpha_2) \neq \alpha_2$. If $E = (\iota_K, E_1, E_2, \ldots, E_m)$ where the E_i are endomorphisms of K, then there exists an integer n such that $E_n(\alpha_2) \neq 0$, and by the preceding paragraph, $E_n(\alpha_2) \in K^{p^n}$. Apply E_n to Equation 2.3 to get

$$0 = E_n(k_1) + E_n(k_2\alpha_2) + \cdots + E_n(k_t\alpha_t) = k_2E_n(\alpha_2) + \cdots + k_tE_n(\alpha_t).$$

The right hand side is a shorter dependence relation on the k_i than Equation 2.3, which contradicts minimality. Hence k and K^{p^n} are linearly disjoint.

$\underline{3 \Rightarrow 4}$: Let $x \in N$. The equality $l(x) = e - c(x) + 1$ is equivalent to the following property: If $x \in N$ and $c(x) \leq i \leq e$, then the ith row of the Sweedler Diagram contains an element from the set $\{x^{p^i}\}_{0 \leq i < \infty}$. Thus it suffices to show that the pth powers of any elements in row i of the Sweedler Diagram will appear in row $i + 1$ of the diagram. Specifically, we show that if S is a subset of $k^{1/p^{i+1}} \cap K$ and the elements of S are p-independent over $k^{1/p^i} \cap K$ then S^p is p-independent over $k^{1/p^{i-1}} \cap K$.

Suppose the previous statement were untrue. Then the set of monomials $M = \left\{ \prod_{x \in S} x^{pe_x} \right\}_{0 \leq e_x < p}$ are linearly dependent over $k^{1/p^{i-1}} \cap K$. Let F denote be the dependence relation on M and $F^{p^{i-1}}$ the p^{i-1}th power of the relation. Then $F^{p^{i-1}}$ is a dependence relation over $k \cap K^{p^{i-1}}$ of elements in the set $M^{p^{i-1}} = \left\{ \prod_{x \in S} x^{p^i e_x} \right\}_{0 \leq e_x < p} \subset K^{p^i}$. Since K^{p^i} and k are linearly disjoint, then there exists a dependence relation of elements of M^{p^i} over $k \cap K^{p^i}$. Call this relation G. Take the p^ith root of G to obtain a dependence relation over $k^{1/p^i} \cap K$ of the monomials $M^{1/p} = \left\{ \prod_{x \in S} x^{e_x} \right\}_{0 \leq e_x < p}$. This contradicts p-independence of S over $k^{1/p^i} \cap K$. Therefore $l(x) = e - c(x) + 1$ for every $x \in N$. The rest of the proof follows easily from the construction of the Sweedler Diagram and basic properties of p-bases. □

Any field extension which satisfies the properties of Theorem 29 is called a **modular extension**. Note that for any finite purely inseparable extension K/k, if F is the subfield of constants of all higher derivations of K/k , then K/F is modular, and F will be the smallest intermediate subfield such that K/F is modular.

2.5 The Shape of a Sweedler Diagram

Based on property 4 of Theorem 29, and using the fact that the cardinality of a p-basis is independent of the choice of basis, we can determine if a field extension is modular based only on how many elements are in each entry of a Sweedler Diagram: For every entry $(i,\, j)$ in the Sweedler Diagram with $i > 1$, if the number of elements in $(i,\, j)$ is greater than or equal to the number of elements in entry $(i-1, j)$, then the field extension is modular. Hence, Examples 1, 2, and 4 of Sweedler Diagrams are modular while examples 3 and 5 are not, since U^p does not appear in row 2 of the diagram in Example 3 and Z^p does not appear in row 3 of the Sweedler Diagram in Example 5.

We expand on this idea of the "shape" of a Sweedler Diagram (i.e. how elements are distributed in the entries of the diagram) to develop another property that is equivalent to the properties in Theorem 29. It is easy to show that $\{x_1, \dots, x_n\}$ is a p-basis for K/k if and only if $\{dx_1, \dots, dx_n\}$ is a K-basis for $\Omega^1_{K/k}$ (16, p.202). Since the elements of the entries in a Sweedler Diagram correspond to the p-bases of the fields show in Table I, by the above fact we can construct another diagram, mirroring the Sweedler Diagram, whose entries are the modules of differentials of the field extensions in Table I. That is, for $j > 1$ the $(i,\, j)$th entry contains the module

$$\Omega^1_{K^{p^{i-j}}_{e-j+1} \cdot K_{e-i-1} / K^{p^{i-j+1}}_{e-j+2} \cdot K_{e-i}}, \tag{2.4}$$

and when $j = 1$ the $(i,\, 1)$th entry contains the module

$$\Omega^1_{K^{p^{i-1}} \cdot K_{e-i-1}/K_{e-i}}.$$

Call this the *diagram of differentials of* K/k. For example, the following table displays the top-left corner of a diagram of differentials:

$\Omega^1_{K/K_{e-1}}$	
$\Omega^1_{K^p \cdot K_{e-2}/K_{e-2}}$	$\Omega^1_{K_{e-1}/K^p \cdot K_{e-2}}$

In the Sweedler Diagram, a subset of the pth powers of elements in entry $(i,\, j)$ are placed into entry $(i+1,\, j)$. One can ask how this translates to the diagram of differentials? Let $F : K \to K$ be the Frobenius homomorphism, so that for all $x \in K$, $F(x) = x^p$. For $2 \leq i \leq e$, the following diagram commutes:

$$\begin{tikzcd}
K_i \arrow[r, "F"] & (K_i)^p \arrow[r] & K_{i-1} \\
K_{i-1} \arrow[u] \arrow[r, "F"] & (K_{i-1})^p \arrow[u] \arrow[r] & K_{i-2} \arrow[u]
\end{tikzcd}$$

where all unlabeled arrows are natural inclusions. These homomorphisms induce a homomorphism of modules of differentials

$$dF : \Omega^1_{K_i/K_{i-1}} \to \Omega^1_{K_{i-1}/K_{i-2}}.$$

Based on the discussion following the proof of Theorem 29, K/k is modular if and only if the pth powers of elements of a p-basis of K_i/K_{i-1} are p-independent over K_{i-2}. More concretely, this means that for each i and any subset $\{x_1, \ldots, x_n\} \subset K_i$ which is a p-basis for K_i/K_{i-1},

K/k is modular if and only if $\{x_1^p, \ldots, x_n^p\}$ is p-independent over K_{i-2}. In terms of differentials, the above statement translates to: K/k is modular if and only if, for every i and any K_i-basis for $\Omega^1_{K_i/K_{i-1}}$, $\{dx_1, \ldots, dx_n\}$, $\{dx_1^p, \ldots dx_n^p\}$ is a K_i-linearly independent subset of $\Omega^1_{K_{i-1}/K_{i-2}}$.

In general, suppose E and F are fields and $\psi : F \to E$ is a nontrivial ring homomorphism. Suppose also that V is a vector space over F and W is a vector space over E. Then W is also a vector space over F. If $h : V \to W$ is an F-module homomorphism, then the image in W of an F-basis of V will be E-linearly independent if and only if the composition map

$$\mu \circ (1_E \otimes_F h) : E \otimes_\psi V \to E \otimes_\psi W \to W$$

is injective. Thus, we have proven the following:

Theorem 30. *Let L and k be fields of characteristic $p > 0$ and suppose L/k is a finite purely inseparable field extension of exponent e. Let $F : L \to L$ be the Frobenius homomorphism. L/k is modular if and only if*

$$\mu \circ \left(\iota_{L_{r-1}} \otimes_{F_r} dF_r\right) : L_{r-1} \otimes_{F_r} \Omega^1_{L_r/L_{r-1}} \to \Omega^1_{L_{r-1}/L_{r-2}}$$

is injective for all r such that $2 \le r \le e$, where $L_r = k^{p^{-r}} \cap L$ and F_r is the homomorphism $L_r \to L_{r-1}$ induced by F.

Heuristically, this homomorphism maps the modules in the rth row of the diagram of differentials onto entries $(r+1, 1)$, $(r+1, 2), \ldots, (r+1, r)$ of the diagram of differentials. The cokernel will then be the module in entry $(r+1,\, r+1)$ of the diagram of differentials. That is,

$$\operatorname{coker}\left(\mu \circ \left(1_{K_{r-1}} \otimes_{F_r} dF_r\right)\right) \cong \Omega^1_{K_{r-1}/K_r^p \cdot K_{r-2}}.$$

Theorem 30 gives an intrinsic way to test if a field extension is modular or not without having to make any choices of p-bases.

The next chapter will further develop the theory of higher derivations, but we finish here by using Example 3 to illustrate how property 2 of Theorem 29, the higher derivation property, fails for non-modular extensions. Recall Example 3, where k_0 is a perfect field of characteristic $p > 0$, $K = k_0(X, U, Z)$, and $k = k_0(X, U^p - XZ^p, Z^{p^2})$. Note that $Z^p \notin k$. Suppose there is a higher derivation $D = (D_0, D_1, \ldots, D_m)$ of K with $K^D \supseteq k$ such that $Z^p \notin K^D$. Then there is an endomorphism $D_n : K \to K$ with $D_n(Z^p) \neq 0$. Using techniques from the proof of Theorem 29, $p|n$ and $D_n(Z^p) = \left(D_{n/p}(Z)\right)^p$. Since D is linear with respect to k, $X \in k$ implies $X\left(D_{n/p}(Z)\right)^p = D_n(XZ^p) = D_n(U^p - (U^p - XZ^p)$. D_n is additive, and $U^p - XZ^p \in k$, hence this last term is equal to $D_n(U^p) = \left(D_{n/p}(U)\right)^p$. Solving for X gives $X = \left(\frac{D_{n/p}(U)}{D_{n/p}(Z)}\right)^p \in K^p$, which is impossible since $X^{1/p} \notin K$. Hence D must be trivial at Z^p, so the field of constants K^D is strictly larger than k. No higher derivation of K/k has k as a field of constants, thus K/k cannot be a modular extension.

CHAPTER 3

GERSTENHABER GALOIS THEORY

3.1 Witt Vectors and the Artin-Hasse Exponential

Fix a prime number p and a sequence of indeterminates $(\theta) = (\theta_0, \theta_1, \ldots)$. The **nth Witt polynomial** is then given by $w_n(\theta) \coloneqq \theta_0^{p^n} + p\theta_1^{p^{n-1}} + \cdots + p^n\theta_n \in \mathbb{Z}[\theta_0, \theta_1, \ldots]$.

Theorem 31. *(22, II, §6,Theorem 6) If $(\theta) = (\theta_0, \theta_1, \ldots)$ and $(\psi) = (\psi_0, \psi_1, \ldots)$ are two sequences of indeterminates, then there exists unique sequences of elements $(\phi) = (\phi_0, \phi_1, \ldots)$ and $(\phi') = (\phi'_0, \phi'_1, \ldots)$ in $\mathbb{Z}[\theta_0, \theta_1, \ldots; \psi_0, \psi_1 \ldots]$ such that $w_i((\phi)) = w_i((\theta)) + w_i((\psi))$ and $w_i((\phi')) = w_i(\theta) \cdot w_i(\psi)$.*

(ϕ) is called the *Witt sum* of (θ) and (ψ) and denoted $(\theta) +_w (\psi)$ and (ϕ') is called the *Witt product* of (θ) and (ψ) and denoted $(\theta) \cdot_w (\psi)$. These are commutative operations. If R is ring, then θ_i and ψ_i can be replaced by elements of R which commute with each other, and we can analogously define the Witt sum and Witt product on sequences of elements of R which commute. Under these operations, this set of sequences is called the **ring of p-Witt vectors with coefficients in R**, denoted $W(R)$(22, [II, §6,Theorem 7).

Given a prime number p, recall the Artin-Hasse exponential of an indeterminate x as

$$\exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots\right).$$

Let (θ) be a sequence of elements in a ring R which commute as before and let t be a formal variable. Gerstenhaber(8) introduces the following modified Artin-Hasse exponential

$$e\left(t,\,(\theta)\right) := \exp\left(\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^i} w_i(\theta)\right). \tag{3.1}$$

Setting $(\theta^p) := (\theta_0^p, \theta_1^p, \ldots)$, note that $e\left(t^p,\,(\theta^p)\right) = \exp \sum_{i=0}^{\infty} \frac{t^{p^{i+1}}}{p^i} w_{i+1}(\theta)$, while

$$(e(t,\,(\theta)))^p = \exp\left(p\left(\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^i} w_i(\theta)\right)\right) = \exp\left(\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^{i-1}} w_i(\theta)\right).$$

Taking the quotient,

$$\exp \sum_{i=0}^{\infty} \frac{t^{p^{i+1}}}{p^i} w_{i+1}(\theta) \Big/ \exp\left(\sum_{i=0}^{\infty} \frac{t^{p^i}}{p^{i-1}} w_i(\theta)\right) = \exp(p\,t\,w_0(\theta)),$$

which is congruent to 1 modulo p. Therefore Dwork's Lemma (8, §3 Lemma 2) the series $e(t,\,(\theta))$ is has p-integral coefficients. Thus $e\left(t,\,(\theta)\right)$ is well-defined modulo p.

3.2 Abelian Families of Higher Derivations

Let L/K be a purely inseparable field extension of exponent e where L and K have characteristic $p > 0$. Also let $G = \mathrm{HDer}_K^{p^e} L$ be the group of higher derivations of rank p^e. By Theorem 24, L is modular over the subfield of constants of G. Let K_0 be the subfield of constants, so that $L = K_0(x_1) \otimes_{K_0} \cdots \otimes_{K_0} K(x_n)$ with $x_i \in L$ and $\exp[x_i : K_0] = e_i$. Expanding on Example 2 from the previous chapter, each group $\mathrm{HDer}_{K_0}^{p^{e_i}} K_0(x_i)$ embeds into $\mathrm{HDer}_{K_0}^{p^e} L$ by mapping t

to $t^{p^{e-e_i}}$. Thus, if $1 + D_1t + \cdots + D_{p^{e_i}-1}t^{p^{e_i}-1} \in \mathrm{HDer}^{p^{e_i}}_{K_0}K_0(x_i)$, then this maps to a higher derivation $E \in \mathrm{HDer}^{p^e}_{K_0}L$ where $E(x_j) = x_j$ for $i \neq j$ and $E(x_i) = x_i + D_1(x_i)t^{p^{e-e_i}} + \cdots$.

If $m < p^e$, and $G' = \mathrm{HDer}^m_{K_0}L$, then every element in G' is the truncation of an element of G. Hence there is an inverse system on the groups of higher derivations of L/K_0. On the other hand, if $m > p^e$, then for every element $G'' \in \mathrm{HDer}^m_{K_0}L$ there exists $H_1, \ldots, H_n \in \mathrm{HDer}^{p^e}_{K_0}L$ such that $G'' = H_{1,l_1} \cdots H_{n,l_n}$, where H_{i,l_i} is the extension of H_i to $\mathrm{HDer}^m_{K_0}L$ by sending t to t^{l_i} for some $l_i > 0$. Hence, restricting our attention to the group $\mathrm{HDer}^{p^e}_K L$ will suffice to understand all higher derivations of L/K. In other words, we will study the inverse limit of the groups of higher derivations instead of the inverse system.

Let $\overline{D} = 1 + D_1t + D_2t^2 + \cdots D_{p^e-1}t^{p^e-1}$ be a higher derivation homomorphism of L/K. $\overline{D}$ is **abelian** if all the D_i commute as endomorphisms of L. A subgroup $H \subseteq \mathrm{HDer}^{p^e}_K L$ is called an **abelian family** if every element is abelian and for any $1 + D_1t + \cdots + D_{p^e-1}t^{p^e-1}$, $1 + E_1t + \cdots E_{p^e-1}t^{p^e-1} \in H$, $D_iE_j = E_jD_i$ for all $0 < i, j < p^e$. Let $a \in L$ and define maps $V : \mathrm{HDer}^{p^e}_K L \to \mathrm{HDer}^{p^e}_K L$ and $T_a : \mathrm{HDer}^{p^e}_K L \to \mathrm{HDer}^{p^e}_K L$, where V sends t to t^p and T_a sends t to at. Hence,

$$V(\overline{D}) = 1 + D_1t^p + D_2t^{2p} + \cdots + D_{p^{e-1}-1}t^{p^e-p}$$

and

$$T_a(\overline{D}) = 1 + aD_1t + a^2D_2t^2 + \cdots + a^{p^e-1}D_{p^e-1}t^{p^e-1}.$$

While V is a group homomorphism, T_a will most of the time not be unless $a \in K$. Additionally, for any abelian family $\mathcal{A}$ and any $D \in \mathcal{A}$, the operation

$$P(\overline{D}) = 1 + D_1^p t + \cdots + D_{p^e-1}^p t^{p^e-1}$$

is a group homomorphism from $\mathcal{A}$ to $\mathrm{HDer}_K^{p^e} L$.

If $(\theta_1, \ldots, \theta_{e-1})$ is a sequence of endomorphisms of L/K which commute with each other, it is not necessarily true that $e\,(t, (\theta))$ is a higher derivation homomorphism. For instance, if X and Y are algebraically independent over $\overline{\mathbb{F}}_p$, suppose $K = \overline{\mathbb{F}}_p(X^{p^2},\, Y^{p^2})$, $L = K(X,\, Y)$. Define $\left(\frac{\partial}{\partial Y}\right)^{[p]}$ as the endomorphism of L which sends X^i to 0 for all i and Y^j to $\binom{p}{j} Y^{j-p}$. If $(\theta) = \left(\frac{\partial}{\partial X}, \left(\frac{\partial}{\partial Y}\right)^{[p]}\right)$, then the coefficient of t in $e\,(t,\, (\theta))$ is $\frac{\partial}{\partial X}$ while the coefficient of t^p is

$$\left(\frac{1}{p} + \frac{1}{p!}\right)\left(\frac{\partial}{\partial X}\right)^p + \left(\frac{\partial}{\partial Y}\right)^{[p]} = \left(\frac{\partial}{\partial Y}\right)^{[p]}.$$

$e\,(t,\, (\theta))$ fails to be a higher derivation homomorphism because the proof of Theorem 29 establishes that if it were, then $\left(\frac{\partial}{\partial Y}\right)^{[p]}(Y^p) = \left(\left(\frac{\partial}{\partial X}\right)(Y)\right)^p$, which is not true. Yet applying Equation 3.1 to some sequences of endomorphisms does result in higher derivation homomorphisms.

Proposition 32. *(8, p. 17) Let L/K be a purely inseparable field extension of exponent e. Any higher derivation $\overline{H} \in HDer_K^{p^e-1} L$ with commuting coefficients is the product of higher derivations of the form $e(t^r,\, (\theta))$ with $r \in \mathbb{Z}_{\geq 1}$ and $(\theta) = (\theta_0,\, \ldots,\theta_{e-1})$ a sequence of endomophisms in $End_K L$ that commute. Furthermore, any abelian family can be generated by such elements.*

The proof of this proposition is omitted, but it follows readily after choosing a basis of $\mathrm{End}_K L$ and applying Proposition 27.

If $(\theta) = (\theta_0, \ldots, \theta_{e-1})$ is a sequence of endomorphisms of L/K which commute with each other such that $e(t,\, (\theta)) \in \mathrm{HDer}_K^{p^e-1} L$, then (θ) is called an **extended derivation**. If (θ) is an extended derivation, then by construction the first nonzero θ_i in the sequence is a derivation in $\mathrm{Der}_K L$.

We next define three operations on extended derivations and use familiar notation to indicate how they relate to operations on abelian higher derivations already defined. If (θ) is an extended derivation with $e(t,\, (\theta)) = 1 + \delta_1 t + \cdots + \delta_{p^e-1} t^{p^e-1}$, then $e(t,\, (\theta^p)) = 1 + \delta_1^p t + \cdots + \delta_{p^e-1}^p t^{p^e-1}$ is also a higher derivation homomorphism. Define $P(\theta) = (\theta_0^p, \ldots, \theta_{e-1}^p)$. Furthermore, define $V(\theta) = (0,\, \theta_0, \ldots, \theta_{e-2})$. Then

$$\begin{aligned} e(t,\, V(\theta)) &= \exp\left(\sum_{i=0}^{e-1} \frac{t^{p^i}}{p^i} w_i\left(V(\theta)\right)\right) \\ &= \exp\left(\sum_{i=1}^{e-1} \frac{t^{p^i}}{p^i} p w_{i-1}(\theta)\right) \\ &= 1 + \delta_1 t^p + \delta_2 t^{2p} + \cdots \delta_{p^{e-1}-1} t^{p^e-p}. \end{aligned}$$

Lastly, note that if (θ) is an extended derivation, then for all $a \in K$, $\left(\theta_0,\, a^p\theta_1, \ldots, a^{p^{e-1}}\theta_{e-1}\right)$ is again a commuting sequence of endomorphisms in $\mathrm{End}_K L$. More generally, if θ_i is the first nonzero endomorphism of (θ), then for $a \in K^{p^{-i}}$, define

$$T_a(\theta) = (0, \ldots, 0,\, \theta_{i-1},\, a^{p^i}\theta_i, \ldots, a^{p^{e-1}}\theta_{e-1}).$$

The image is again a sequence of endomorphisms of L/K which commute. In fact, $T_a(\theta)$ is an extended derivation, since

$$e(t,\, T_a(\theta)) = 1 + a^{p^i}\delta_{p^i}t^{p^i} + a^{2p^i}\delta_{2p^i}t^{2p^i} + \cdots + a^{p^{e-1}}\delta_{p^{e-1}}t^{p^{e-1}} = T_a e(t,\, (\theta)).$$

Thus the action of P, V, and T_a on extended derivations commutes with the action of P, V, and T_a on higher derivations after applying the truncated Artin-Hasse exponential.

Fix a subset $S \subset \mathrm{End}_K L$ which is a K-algebra and whose elements all commute. A Witt group of extended derivations of L/K, denoted H, can be constructed from S by taking all extended derivations whose entries are endomorphisms in S. Since the truncated Artin-Hasse exponential transforms Witt sums of extended derivations into products of higher derivation homomorphisms, the set $\{e\left(t^l,\, (\theta)\right) : (\theta) \in H,\, 0 \leq l \leq p^e - 1\}$ is a subgroup of $\mathrm{HDer}_K^{p^e-1} L$.

Let $\mathcal{L}$ be a set of sequences of elements in $\mathrm{End}_K L$ whose entries all commute and which are each an extended derivation. If $\mathcal{L}$ is a group under Witt addition, then it is called an **abelian family of extended derivations**. Suppose further that for all i, $a \in K^{p^{-i}}$ and $(\theta) \in \mathcal{L}$, $T_a(\theta) \in \mathcal{L}$ if θ_i is the first nonzero endomorphism in the sequence (θ). If $\mathcal{L}$ is closed under P, V, and T_a as described above, then $\mathcal{L}$ is called **saturated**. By Proposition 32, any saturated abelian family of extended derivations generates a group of commuting Hasse-Schmidt derivations which is closed under the operations P, V, and T_a for $a \in K$. If $(\theta) = (\theta_0, \ldots, \theta_{e-1})$ is an extended derivation of L/K, the **fixed field of** (θ) is the fixed field of the set $\{\theta_0,\, \ldots, \theta_{e-1}\} \subset \mathrm{End}_K L$.

The fixed field of a set of extended derivations of L/K is the intersection of the fixed fields of each extended derivation in the set.

3.3 Gerstenhaber's Galois Correspondence

The following theorem is one of the main results from Zaromp's dissertation. The proof is omitted, but we note that the proof involves constructing extended derivations using the property proven in Proposition 27.

Theorem 33. *(26, p.23) Let K be a field of characteristic $p > 0$ and suppose L/K is a finite modular field extension. Let M be an abelian family of extended derivations of L/K such that K is the fixed field of M. If M is a saturated finitely generated Witt group then M is a maximal abelian family of extended derivations.*

The previous theorem can be restated as

Theorem 33.1. *Let K be a field of characteristic $p > 0$ and suppose L/K is a finite modular field extension of exponent e. Let M be an abelian family of higher derivations of L/K such that K is the fixed field of M. If M is closed under P, T_a where T_a acts only on higher derivations of M with order $\geq p^i$ when $a \in K^{p^{-i}}$, and reparametrizations of $L[t]/(t^{p^e})$ which send t to t^r for any positive integer r, then M is a maximal abelian family of higher derivations.*

Note that the group M from the above theorem is only closed under reparametrization by elements of K, not L. As an example, suppose $L = \mathbb{F}_p(X, Y)$ and $K = \mathbb{F}_p(X^p, Y^p)$ where p is a prime. L/K is an extension of exponent 1, so we only need to study subgroups of $G = \mathrm{HDer}_K^p L$. The subgroup $H \subset G$ generated by

$$1 + \frac{d}{dX}t + \frac{1}{2!}\left(\frac{d}{dX}\right)^2 t^2 + \cdots + \frac{1}{(p-1)!}\left(\frac{d}{dX}\right)^{p-1} t^{p-1}$$

has subfield of constants $K' = \mathbb{F}_p(X^p, Y)$. The saturated subgroup generated by $T_a(D)$, $V(D)$, and $P(D)$ for all $D \in H$ and $a \in K'$ has the same subfield of constants, and is a maximal abelian family by Theorem 33.1.

On the other hand, in the same manner construct the subgroup closed under K'-reparametrization, V, and P by the higher derivation

$$1 + X\frac{d}{dX} + X^2\frac{1}{2!}\left(\frac{d}{dX}\right)^2 + \cdots + X^{p-1}\frac{1}{(p-1)!}\left(\frac{d}{dX}\right)^{p-1}.$$

This subgroup again has $\mathbb{F}_p(X^p, Y)$ as its subfield of constants and will again be a maximal saturated abelian family. This subgroup is not equal to the subgroup constructed in the previous paragraph because $\frac{d}{dX}$ and $X\frac{d}{dX}$ do not commute, hence both cannot be elements of an abelian family. Therefore, distinct saturated abelian families of higher derivations closed under V, P and T_a can have the same subfield of constants. Equivalently, distinct saturated abelian families of extended derivations can also have the same subfield of constants.

Based on this theorem, Gerstenhaber claims (10, p.1014) that there is a $1-1$ correspondence between subgroups $\mathrm{HDer}_{K'}^{p^e} L \subset \mathrm{HDer}_K^{p^e} L$ where $K \subseteq K' \subseteq L$ and saturated abelian families of extended derivations. The correspondence sends a saturated abelian family to the subgroup of higher derivations generated by $\{T_a e\,(t,\,(\theta))\}_{a\in L}$. However, this statement is not accurate as published. Consider the following example: Let K_0 be a perfect field of characteristic 3 with X and Y algebraically independent over K_0. Then $L = K_0(X,\,Y)$ is an extension of $K = K_0(X^3,\,Y^3)$ of degree 9 and exponent 1. The higher derivation homomorphism

$$1 + \frac{\partial}{\partial X}t + \left(\frac{1}{2!}\left(\frac{\partial}{\partial X}\right)^2 + \frac{\partial}{\partial Y}\right)t^2 \in \mathrm{HDer}^2_K L \tag{3.2}$$

can be factored as $e\left(t,\,\left(\frac{\partial}{\partial X}\right)\right) e\left(t^2,\,\left(\frac{\partial}{\partial Y}\right)\right)$. Note that the second factor,

$$e\left(t^2,\,\left(\frac{\partial}{\partial Y}\right)\right) = 1 + \frac{d}{dY}t^2,$$

is not a higher derivation homomorphism of the form $T_a e(t,\,(\theta))$ for any (θ) because any nontrivial higher derivation homomorphism of the form $e\,(t,\,(\theta))$ has a nonzero coefficient in the degree 1 term. Thus the higher derivation homomorphism of Equation 3.2 is not included in the $1-1$ correspondence described by Gerstenhaber.

His statement can easily be corrected to the following:

Theorem 34. *Let L/K be a finite purely inseparable extension of exponent e. Suppose $\mathcal{L}$ is a saturated abelian family of extended derivations of the form $(\theta) = (\theta_0, \ldots, \theta_{e-1})$ with fixed field K', and let $\overline{\mathcal{L}}$ denote the subgroup of HDer$^{p^e}_K L$ generated by the higher derivations $T_a e(t^l,\,(\theta))$, where $1 \le l \le p^e - 1$ and $a \in L^{p^{-i}}$ if θ_i is the first nonzero term of (θ). Then $\overline{\mathcal{L}} =$ HDer$^{p^e}_{K'} L$.*

Proof. This theorem was first stated in Zaromp's thesis (26, p. 35), where the proof was promised in a future publication. It was then restated in (10), again without a proof. An analogous theorem is proven by Heerema and Deveney (13, Theorem 4.2) for iterative higher derivations.

The first nonzero term of any element of $\mathcal{L}$ is a derivation in $\text{Der}_{K'}L$. Because $\mathcal{L}$ is saturated, the collection of such derivations is a L^pK' vector space of commuting derivations which is closed under pth powers. We first show that the fixed field of this restricted Lie algebra of derivations is L^pK. Call this restricted L^pK'-Lie algebra D, its fixed field K_0, and suppose m is the cardinality of a p-basis of L/K'. Zaromp proves (26, Theorem 2) that any $K'L^p$-basis of D has cardinality m. He also shows (26, Proposition 1) that any $K'L^p$-linearly independent set of commuting derivations which commute with every term of $\mathcal{L}$ will also be linearly independent over K_0, which is an intermediate field of L/L^pK'. Since D is closed under pth powers, $[L : K_0] = p^m$ (26, Theorem, p.6). But $[L : L^pK'] = p^m$ as well, and since all these extensions are exponent 1, then it is necessary that $L^pK' = K_0$.

Let $\overline{\mathcal{L}}$ be the group of higher derivations defined above. The collection of the first nonzero terms of $\overline{\mathcal{L}}$ is equal to $\text{Der}_{K'}L$ by the argument above. The rest of the proof follows very closely to the proof of Heerema and Deveney (13, Theorem 4.2), and we omit some details. Suppose $\overline{D} = (\iota_L, D_1, \ldots, D_{p^e-1})$ is a higher derivation in $\text{HDer}_{K'}L$ whose first nonzero term is D_i. By Proposition 26, D_i is a derivation in $\text{Der}_{K'}L$. Hence there exists a higher derivation $\overline{E_i} = (\iota_L, E_{i1}, E_{i2}, \ldots, E_{ip^e-1})$ in $\overline{\mathcal{L}}$ such that E_{in} is its first nonzero term and $E_{in} = D_i$ for some n. Thus, $\overline{E_i}^{-1}\overline{D}$ is a higher derivation of order $j > i$. Repeat this process to obtain higher derivations of strictly larger order. Since the ranks of all these higher derivations are p^e, this process terminates after a finite number of steps, and there exist $\overline{E_i}, \overline{E_{i+1}}, \ldots, \overline{E_{p^e-1}} \in \overline{\mathcal{L}}$ such that

$$\overline{E_i}^{-1}\overline{E_{i+1}}^{-1} \cdots \overline{E_{p^e-1}}^{-1}\overline{D} = \overline{\iota_L} \in \mathrm{HDer}_{K'}L.$$

Multiplying both sides by $\overline{E_{p^e-1}} \cdots \overline{E_i}$ proves that $\overline{D} \in \overline{\mathcal{L}}$, hence $\overline{\mathcal{L}} = \mathrm{HDer}_{K'}L$.

□

If K' is an intermediate subfield of L/K with L/K' modular, then there are many subgroups of $\mathrm{HDer}^{p^e}_K L$ whose subfield of constants is K', but $\mathrm{HDer}^{p^e}_{K'} L$ is the maximal such subgroup. This theorem establishes a many-to-one correspondence between saturated abelian families of extended derivations of L/K and subgroups H of $\mathrm{HDer}_K L$ such that H is the maximal subgroup with subfield of constants L^H. Thus, if K is a field, $\mathcal{L}$ is a saturated family of extended derivations of K, and $H = \mathrm{HDer}_{K^{\mathcal{L}}} K$, then $H = \langle \mathcal{L} \rangle$ where $\langle \mathcal{L} \rangle$ is the group of higher derivations, closed under reparametrizations by K, which is generated by $\mathcal{L}$ via the Artin-Hasse exponential. Thus there is a Galois correspondence between modular intermediate subfields of L/K and subgroups $H \subset \mathrm{HDer}_K L$ such that there exists a saturated abelian family of extended derivations $\mathcal{L}$ with $H = \langle \mathcal{L} \rangle$. Call this correspondence **Gerstenhaber Galois theory**.

We note that Gerstenhaber never claimed that there exists a one-to-one correspondence between modular subfields of a finite purely inseparable extension and saturated abelian families of higher derivations. He correctly states that there is a correspondence between collections of saturated abelian families and modular extensions. Even so, Theorem 34 gives a fairly unsatisfactory correspondence, as it does not address the many-to-one correspondence from saturated families of extended derivations to groups of higher derivations explained earlier, nor does it provide a clear structure for the subgroups H.

CHAPTER 4

MODULAR FIELD THEORY AND DIFFERENTIAL OPERATORS

4.1 Differential Operators

Let A be a commutative ring and B a commutative A-algebra. The algebra $B \otimes_A B$ has two B-module structures, induced by maps $d_1 : B \to B \otimes_A B$ and $d_2 : B \to B \otimes_A B$ where, for any $b \in B$, $d_1(b) = b \otimes_A 1$ and $d_2(b) = 1 \otimes_A B$. For any B-module M, the $B \otimes_A B$-module $B \otimes_A B \otimes_B M$ has a B-bimodule structure induced by d_1 and d_2. There is a natural homomorphism $d_2^M : M \to B \otimes_A B \otimes_B M$ which is B-linear with respect to the d_2-induced B-module structure on $B \otimes_A B \otimes_B M$. That is, for all $m \in M$, $d_2^M(m) = 1 \otimes_A 1 \otimes_B m$.

Definition 35. *Let A be a commutative ring with unity, B a commutative A-algebra, and suppose M and N are B-modules. Set $I = \ker(\mu : B \otimes_A B \to B)$ where μ is the multiplication map. An A-linear homomorphism $D : M \to N$ is called a* ***differential operator of order*** *$\leq n$ if $\widetilde{D} = \mu \circ (1_B \otimes_A 1_B \otimes_B D) : \left(B \otimes_A B/I^{n+1}\right) \otimes_B M \to N$ is a B-module homomorphism by the d_1-action on $B \otimes_A B$, and the following diagram commutes:*

$$\begin{tikzcd}
M \arrow[r, "D"] \arrow[d, "d_2^M"] & N \\
B \otimes_A B \otimes_B M \arrow[d, two heads] & \\
\left(B \otimes_A B/I^{n+1}\right) \otimes_B M \arrow[uur, "\widetilde{D}=\mu\circ(1_B\otimes_A 1_B\otimes_B D)"'] &
\end{tikzcd}$$

Letting A, B, and M be defined as above, B embeds in $\mathrm{End}_A B$ by sending $b \in B$ to λ_b as described prior to Theorem 13. As in Chapter 1, we use the notation $b \in \mathrm{End}_A B$ and $\lambda_b \in \mathrm{End}_A B$ interchangeably in this context.

Lemma 36. *Let A be a commutative ring and B a commutative A-algebra. Set $Diff^0_A(B,\, B) \coloneqq B \subset End_A B$. An endomorphism $D \in End_A B$ is an A-linear differential operator of order $\leq n$ from B to B if, for all $b \in B$, $[D,\, b]$ is a differential operator of order $\leq n-1$. That is, if $Diff^n_A(B,\, B)$ denotes the set of such differential operators, then $[Diff^n_A(B,\, B),\, B] \subseteq Diff^{n-1}_A(B,\, B)$.*

Proof. By EGA (11, §16.8) both Definition 35 and the recursive property described in the Lemma induce the formula

$$D(x_0 x_1 \cdots x_n) = \sum_{s=0}^{n} (-1)^{s-1} \sum_{i_1 < i_2 < \ldots i_s} x_{i_1} x_{i_2} \cdots x_{i_s} D\left(x_1 \cdots \widehat{x_{i_1}} \cdots \widehat{x_{i_s}} \cdots x_n\right) \tag{4.1}$$

for any differential operator D of order $\leq n$ and any $\{x_0, \ldots, x_n\} \subset B$. □

Let D and Δ be differential operators from B to B of order $\leq r$ and $\leq s$, respectively. Then noting that

$$[D\Delta,\, b] = D\Delta\lambda_b - \lambda_b D\Delta = D\,[\Delta,\, \lambda_b] + [D,\, \lambda_b]\,\Delta$$

for any $b \in B$, it is easy to prove by induction (17, Corollary 6.1) that $D\Delta$ is a differential operator of order $\leq r + s$.

In addition, using the notation of Definition 35, for any positive integer i, $I^{n+i} \subseteq I^{n+1}$, so if D is a differential operator of order $\leq n$, then $\widetilde{D}$ vanishes on I^{n+i}. Thus D is also a differential operator of order $\leq n+i$. For any nonnegative integer i, let $\mathrm{Diff}^i_A(B,\, B)$ consist of all A-linear differential operators from B to itself of order $\leq i$. Denoting $\mathrm{Diff}_A(B,\, B) = \bigcup\limits_{i=0}^{\infty} \mathrm{Diff}^i_A(B,\, B)$, $\mathrm{Diff}_A(B,\, B)$ is thus a B-algebra with natural filtration $B = \mathrm{Diff}^0_A B \subseteq \mathrm{Diff}^1_A B \subseteq \mathrm{Diff}^2_A B \subseteq \cdots$. Define $\mathrm{Diff}_A B := \mathrm{Diff}_A(B,\, B)$. We say a differential operator has **order** n if n is the smallest integer such that D is a differential operator of order $\leq n$.

Neither Definition 35 nor Lemma 36 present an easy way to construct differential operators. Fortunately higher derivations provide a ready supply.

Proposition 37. *(17, Proposition 5) Let A be a commutative ring and B a commutative A-algebra. Suppose $\overline{D} = 1 + D_1 t + \cdots + D_N t^N \in (End_A B)\,[t]/(t^{N+1})$ (resp. $\overline{D} \in (End_A B)\,[[t]]$). If $\overline{D} \in HDer^{N+1}_A B$ (resp. $\overline{D} \in HDer^{\infty}_A B$), then D_q is a differential operator of B/A of order $\leq q$.*

Proof. The proofs for the finite rank and infinite rank higher derivations are identical, so we only prove the result using the finite-rank notation. In Proposition 26 it was shown that $D_1 \in \mathrm{Der}_A B$. Proceed by induction. For any $x,\, y \in B$, by definition $D_q(xy) = \sum\limits_{m=0}^{q} D_m(x) D_{q-m}(y)$. Hence,

$$D_q(xy) - xD_q(y) - D_q(x)y = \sum_{m=1}^{q-1} D_m(x)D_{q-m}(y),$$

or

$$\left(D_q \circ \lambda_x - xD_q - D_q(x)\right)(y) = \left(\sum_{m=1}^{q-1} D_m(x)D_{q-m}\right)(y).$$

For $m \geq 1$, $D_m(x)D_{q-m}$ is a differential operator of order $\leq q$ by the inductive hypothesis. $D_q(x)$ is a differential operator of order 0, so moving it to the right hand side makes the left hand side equal to $D_q \circ \lambda_x - xD_q = [D_q, x]$. Comparing to the right hand side, this differential operator is of order $\leq q-1$. The proof is then concluded by Lemma 36. □

Let $\mathrm{Gr}^\bullet\mathrm{Diff}_A B$ denote the graded ring associated to the filtration of $\mathrm{Diff}_A B$ by orders of differential operators. Lemma 36 shows that this ring is a commutative B-algebra. Let $\sigma : \mathrm{Diff}_A B \twoheadrightarrow \mathrm{Gr}^\bullet\mathrm{Diff}_A B$ denote the *symbol* map. σ is a surjective map on sets, but it is not a homomorphism, as it will not preserve addition or multiplication. The associated graded algebra has an A-bilinear map

$$\{-,-\} : \mathrm{Gr}^\bullet\mathrm{Diff}_A B \times \mathrm{Gr}^\bullet\mathrm{Diff}_A B \to \mathrm{Gr}^\bullet\mathrm{Diff}_A B$$

called the *Poisson Bracket* where, for $D,\, E \in \mathrm{Diff}_A B$, $\{\sigma(D),\, \sigma(E)\} = \sigma\left([D,\, E]\right)$. Additionally, $Gr^1\mathrm{Diff}_A B = \mathrm{Der}_A B$, and by the universal property of the symmetric algebra generated by $\mathrm{Der}_A B$, there is a B-homomorphism $\mathrm{Sym}^\bullet\mathrm{Der}_A B \to \mathrm{Gr}^\bullet\mathrm{Diff}_A B$.

The homomorphism from the symmetric algebra of the derivations to the algebra $\mathrm{Gr}^\bullet\mathrm{Diff}_A B$ is not too interesting, especially because, as we will see in the next section, $\mathrm{Gr}^\bullet\mathrm{Diff}_A B$ embeds into the divided powers algebra of the derivations of B/A whenever B is a projective A-module. This divided powers algebra has additional structure that makes it nice to work with.

4.2 Divided Powers Rings

Berthelot and Ogus (3) follow Roby's presentation (20) in making the following definition:

Definition 38. *Let A be a commutative ring and $I \subseteq A$ an ideal. I is called an **ideal with divided powers** if there exists a set of maps $\{\gamma_i : I \to A\}_{i\in\mathbb{Z}_{\geq 0}}$ such that for all x, $y \in I$ and i, $j \geq 0$ the following properties hold:*

1. $\gamma_0(x) = 1$, $\gamma_1(x) = x$, *and* $\gamma_i(x) \in I$ *for* $i \geq 2$
2. $\gamma_i(x+y) = \sum_{j=0}^{i} \gamma_j(x)\gamma_{i-j}(y)$
3. $\gamma_i(\lambda x) = \lambda^i \gamma_i(x)$ *for any* $\lambda \in A$
4. $\gamma_i(x)\gamma_j(x) = \dfrac{(i+j)!}{(i!)(j!)}\gamma_{i+j}(x)$
5. $\gamma_i(\gamma_j(x)) = \dfrac{(ij)!}{(i!)(j!)^i}\gamma_{ij}(x)$.

*If I is a an ideal with divided powers as above, then the set (A, I, γ) is called a **ring with divided powers**.*

A homomorphism of rings with divided powers $f : (A, I, \gamma) \to (B\, J, \delta)$ is a ring homomorphism which respects the divided powers structures and satisfies $f(I) \subseteq J$. Note that all the coefficients appearing in Definition 38 are integers, so divided powers structures may exist for rings of any characteristic. Also, if $(A,\, I,\, \gamma)$ is a ring with divided powers and A contains $\mathbb{Q}$, then Property 4 of Definition 38 implies that $\gamma_n(x) = x^n/n!$ for all $x \in I$. If $(A,\, I,\, \gamma)$ is a ring with divided powers and the characteristic of A is a prime p, then for all $x \in I$, $\gamma_n(x) = x^n/n!$ for all $n < p$.

Divided powers are useful in studying differential operators. To see how, we first construct a universal object for divided powers structures. Let A be a commutative ring and M an A-module. Then there exists a commutative A-algebra with divided powers $(\Gamma^*(M),\, \Gamma^+(M),\, \gamma)$ and an A-linear map $\phi :\, M \to \Gamma^*(M)$ with the following universal property (3, Theorem 3.9): For any A-algebra with divided powers $(B,\, J,\, \delta)$ and any A-linear homomorphism $\psi :\, M \to J$, there exists a unique homomorphism of rings with divided powers

$$\overline{\psi} :\, \big(\Gamma^*(M),\, \Gamma^+(M),\, \gamma\big) \to (B,\, J,\, \delta)$$

such that $\overline{\psi} \circ \phi = \psi$. $\Gamma^*(M)$ is a commutative A-algebra, hence by the universal property of the symmetric algebra on M, there exists a canonical homomorphism Sym $M \to \Gamma^*(M)$ which will send $m \in M \subset \text{Sym } M$ to $\phi(m)$.

To construct $\Gamma^*(M)$, first let $G(M)$ denote the free symmetric A-algebra on the set $\{m^{[i]} :\, m \in M,\, i \in \mathbb{Z}_{\geq 0}\}$. Let I be the ideal of $G(M)$ generated by the elements

1. $m^{[0]} - 1$
2. $(\lambda m)^{[i]} - \lambda^i m^{[i]}$
3. $m^{[i]} m^{[j]} - \frac{(i+j)!}{(i!)(j!)} m^{[i+j]}$

4. $(m+n)^{[i]} - \sum_{j=0}^{i} m^{[j]} n^{[i-j]}$

for all $m, n \in M$, $\lambda \in A$ and $i \in \mathbb{Z}_{\geq 0}$. Then $G(M)/I \cong \Gamma^*(M)$, with the third property showing it is a graded algebra. So $\Gamma^*(M) = \bigoplus_{i=0}^{\infty} \Gamma^{[i]}(M)$, where $\Gamma^{[i]}$ is equal to the image of the set $\left\{m^{[i]} : m \in M\right\} \subset G(M)$ in the quotient $G(M)/I$. The construction of I shows that $\Gamma^{[0]}(M) = A$ and $\Gamma^{[1]}(M) = M$ by properties 1 and 3, respectively.

If M is a projective A-module of finite rank, then $\Gamma^*(M^\vee) \cong (\mathrm{Sym}\ M)^\vee$ as graded A-algebras (3, Proposition A10). Let L/K be a field extension, and $\Omega^1_{L/K} = I/I^2$ be the module of differentials as described in Section 2.5. Then $\left(\Omega^1_{L/K}\right)^\vee = \mathrm{Der}_K L$, hence $\Gamma^*(\mathrm{Der}_K L) \cong \left(\mathrm{Sym}\ \Omega^1_{L/K}\right)^\vee$. It is proven in EGA (11, 16.3.1.1) that $\mathrm{Gr}^\bullet\mathrm{Diff}_K L$ injects into $\Gamma^*(\mathrm{Der}_K L)$ by applying $\mathrm{Hom}_K(-, L)$ to the surjective homomorphism $\mathrm{Sym}\ \Omega^1 L/K \to \bigoplus_{i=0}^{\infty} I^k/I^{k+1}$, where I is the kernel of the multiplication homomorphism $L \otimes_K L \to L$. Following this idea, Narváev Macarro (18, Theorem 2.2) explicitly constructs an injective homomorphism $\theta : Gr^\bullet\mathrm{Diff}_K L \to \left(\mathrm{Sym}\ \Omega^1_{L/K}\right)^\vee$ in the following way: For any nonnegative integer n, suppose $D \in \mathrm{Diff}^n_K L$ such that $\sigma(D) \neq 0 \in Gr^n\mathrm{Diff}_K L$ and let $dx_1, \ldots, dx_n \in \Omega^1_{L/K}$. Then

$$\theta\left(\sigma(D)\right)\left(dx_1 \cdots dx_n\right) \coloneqq \left[\left[\cdots\left[\left[D,\, x_n\right],\, x_{n-1}\right], \ldots, x_2\right],\, x_1\right].$$

Using Equation 4.1, it can be shown that θ is well-defined and injective.

If $D \in \mathrm{Diff}_K L$, we will often use the notation $\sigma(D)$ to denote the symbol of D as well as the image of the symbol of D in the divided powers algebra $\Gamma^*\left(\mathrm{Der}_K L\right)$. In addition, we will refer to the image of $\mathrm{Gr}^\bullet\mathrm{Diff}_K L$ in $\Gamma^*\left(\mathrm{Der}_K L\right)$ as the **symbol algebra** of L/K. We remark that every element of $\Gamma^* (\mathrm{Der}_K L)$ is nilpotent of order at most p, hence the pth power of every element in the symbol algebra of L/K is 0.

4.3 Differential Operators on Purely Inseparable Extensions

Proposition 39. *Let L/K be a purely inseparable extension of fields of characteristic $p > 0$. Suppose L/K has finite exponent e and finite degree p^n. Then $Diff_K L = End_K L$.*

Proof. L/K is purely inseparable of finite degree, hence it must have a finite p-basis. If the cardinality of a p-basis is d, then by the discussion in Section 2.5, $\dim_L \Omega^1_{L/K} = d$. So there exist $\alpha_1, \dots \alpha_d \in L$ such that $\{d\alpha_1, \dots, d\alpha_d\}$ is an L-basis for $\Omega^1_{L/K}$. Letting I be the kernel of the multiplication homomorphism $\mu : L \otimes_K L \to L$ as described in Section 2.5, the differential $d\alpha_i$ corresponds to $\overline{1 \otimes_K \alpha_i - \alpha_i \otimes_K 1} \in I/I^2$. Let $d\alpha_{i_1} \cdots d\alpha_{i_n}$ denote the image of

$$(1 \otimes_K \alpha_{i_1} - \alpha_{i_1} \otimes_K 1) \cdots (1 \otimes_K \alpha_{i_n} - \alpha_{i_n} \otimes_K 1)$$

in I. Then $\{d\alpha_{i_1} \cdots d\alpha_{i_n}\}_{0 \le i_j \le d}$ generates I^n as a left L-vector space. If $\exp[\alpha : K] = s$, then $(d\alpha)^{p^s} = 0$ because $(1 \otimes_K \alpha - \alpha \otimes_K 1)^{p^s} = 0$. Hence $I^{p^{(e-1)d+1}} = 0$. By Definition 35 any $D \in \mathrm{Diff}_K^{p^{(e-1)d}} L$ factors through $L \otimes_K L/I^{p^{(e-1)d}+1} = L \otimes_K L/0$ which reduces to the composition $L \to L \otimes_K L \to L$. However, *any* $E \in \mathrm{End}_K L$ can be L-linearized in this way, so $\mathrm{Diff}_K^{p^{(e-1)d}} L = \mathrm{End}_K L$. □

For exponent 1 extensions, this proposition is part of Jacobson's Galois theory, where the fact that the derivations generate the ring of endomorphisms provides a link between the Jacobson-Bourbaki theorem and Jacobson's Galois theory.

In purely inseparable extensions of exponent > 1, any differential operator of order p which is a product of differential operators of lower order will vanish on L^p. Thus, for any purely inseparable extension L/K and any positive integer e, if $L^{p^e} \not\subseteq K$ then there exists an endomorphism of L which does not vanish on L^{p^e}. Thus, some differential operator does not vanish on L^{p^e}, and this differential operator cannot be a product of differential operators of order less than p^e. Hence, the image of the L-vector space $\mathrm{Diff}_K^{p^e} L$ in $\Gamma^{[p^e]}(\mathrm{Der}_K L)$ is not 0.

4.3.1 Example 1

Let k be a perfect field and X transcendental over k. Define $L = k(X)$ and $K = k(X^{p^2})$. Then L/K is purely inseparable of exponent two and degree p^2. Thus the ring of endomorphisms of L/K has dimension p^2 over L. Then

$$\mathrm{Diff}_K L = \bigoplus_{i,j=0}^{p-1} L \left(\frac{d}{dX}\right)^{[i]} \left(\frac{d}{dX}\right)^{[pj]}$$

where $\left(\frac{d}{dX}\right)^{[n]}$ is defined as the endomorphism satisfying

$$\left(\frac{d}{dX}\right)^{[n]} (X^m) = \binom{n}{m} X^{n-m}$$

Note that the image of $\sigma\left(\left(\frac{d}{dX}\right)^{[p]}\right)$ in $\Gamma^{[p]}(\mathrm{Der}_K L)$ is $\left(\frac{d}{dX}\right)^{[p]}$.

4.3.2 Example 2

Consider Example 2 from Section 2.3, where $L = k_0(X, U, Z)$ and $K = k_0(X, U^p - XZ^p, Z^{p^2})$. Furthermore, define $K_0 = k_0(X, U^{p^2}, Z^{p^2})$. L/K_0 is modular, and using notation from the previous example,

$$\mathrm{Diff}_{K_0} L = \bigoplus_{0 \leq i,\, j < p^2} L \partial_U^{[i]} \partial_Z^{[j]}$$

where $\partial_U = \dfrac{\partial}{\partial U}$ and $\partial_Z = \dfrac{\partial}{\partial Z}$. $\mathrm{Diff}_K L$ is a finite-dimensional subring of $\mathrm{Diff}_{K_0} L$. Since $\mathrm{Diff}_{K_0} L$ is already linear with respect to X and Z^{p^2}, in order to explicitly write down $\mathrm{Diff}_K L$ it suffices to compute the differential operators of $\mathrm{Diff}_{K_0} L$ that are linear with respect to $U^p - XZ^p \in K$. Let $\sum\limits_{0 \leq m,\, n < p^2} a_{mn} \partial_U^{[m]} \partial_Z^{[n]} \in \mathrm{Diff}_{K_0} L$, $a_{mn} \in L$. Then

$$\sum_{0 \leq m,\, n < p^2} a_{mn} \partial_U^{[m]} \partial_Z^{[n]} \left(U^p - XZ^p\right) = a_{p0} - X a_{0p}$$

Hence, ∂_U, ∂_Z, and $X\partial_U^{[p]} + \partial_Z^{[p]}$ are elements of $\mathrm{Diff}_K L$ which commute with each other and are clearly linearly independent over L. The L-algebra generated by these elements can be represented as

$$A := \bigoplus_{0 \leq i,\, j,\, k < p} L \partial_U^{[i]} \partial_Z^{[j]} \left(X\partial_U^{[p]} + \partial_Z^{[p]}\right)^k,$$

which has dimension p^3 over L. A must then be the full ring of differential operators of L/K, because p^3 is the largest value $< p^4$ satisfying

$$\dim_L \mathrm{Diff}_K L = [L : K] \,\Big|\, [L : K_0] = p^4.$$

So far in both examples, no information will be lost when passing from the differential operators to the divided powers algebra of derivations. One might hope that just studying the divided powers algebra alone can provide information about whether a purely inseparable extension is modular or not. The next example dispels such hopes.

4.3.3 Example 3

Keeping the same notation as in the previous examples, let $L = k_0(X,\, Z,\, U)$ and $K = k_0(X,\, U^{p^2} - XZ^p,\, Z^{p^2})$. In Example 5 of Section 2.3 the extension L/K was shown to not be modular. As in the previous example, L is modular over $K_0 = k_0(X,\, U^{p^3},\, Z^{p^2})$, and using the same dimension argument, the algebra of $\mathrm{Diff}_{K_0} L$ generated over L by ∂_U, ∂_Z, $\partial_U^{[p]}$, and $X\partial_U^{[p^2]} + \partial_Z^{[p]}$ is equal to the algebra $\mathrm{Diff}_K L$.

Denote the element $X\partial_U^{[p^2]} + \partial_Z^{[p]}$ by D. D is a differential operator of order p^2, and $\sigma(D) = X\partial_U^{[p^2]}$. So, $\sigma\left(\mathrm{Diff}_K L\right)$ is equal to $\sigma\left(\mathrm{Diff}_{K'} L\right)$ where $K' = k_0(X,\, U^{p^3},\, Z^p)$. Thus, unfortunately, two different extensions can have the same symbol algebra. Therefore we need more detailed information to identify whether an extension is modular.

4.4 Pickert Generating Sequences

To better study the differential operators of a purely inseparable field extension, it is worthwhile to determine more properties and invariants of the extension.

Definition 40. *Let L/K be a finite purely inseparable extension of fields of characteristic $p > 0$. A sequence $\{x_1, \ldots, x_n\} \subset L$ is called a* ***Pickert generating sequence*** *if the x_i form a p-basis for L/K and for each i, $\exp[K(x_1, \ldots, x_i) : K] = \exp[x_i : K(x_1, \ldots, x_{i-1})]$.*

Any p-basis of a finite purely inseparable extension can be ordered to make it a Pickert generating sequence. Let e_i denote the exponents in Definition 40. By the definition of exponents, for any $\alpha \in L$, $\exp[\alpha : K(x_1, \ldots, x_{i-1})] \leq e_i$. Hence $e_i \geq \exp[x_{i+1} : K(x_1, \ldots, x_{i-1})]$, and $\exp[x_{i+1} : K(x_1, \ldots, x_{i-1})] \geq \exp[x_{i+1} : K(x_1, \ldots, x_i)] = e_{i+1}$. Thus $e_1 \geq e_2 \geq \cdots \geq e_n$, and

$$\{x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n}\}_{0 \leq r_i < p^{e_i}}$$

is a K-basis for L.

Proposition 41. *(19, §3, Theorem 1) Let L/K be a finite purely inseparable extension of fields of characteristic $p > 0$. Suppose $\{x_1, \ldots, x_n\}$ is a Pickert generating sequence for L/K with corresponding exponent sequence $\{e_i\}$. For each i,*

$$x_i^{p^{e_i}} \in K(x_1^{p^{e_i}}, \ldots, x_{i-1}^{p^{e_i}}).$$

Proof. Set $q_i := p^{e_i}$. If $n = 1$, then $q_1 = \exp[x_1 : K] = \exp[L : K]$ and the proposition is proven. Suppose the proposition is true for all purely inseparable extensions with Pickert generating sequences of length less than i where $i \geq 2$. For any extension L/K with Pickert generating sequence $\{x_1, \ldots, x_i\}$, $\{x_2, \ldots, x_i\}$ is then a Pickert generating sequence for $L/K(x_1)$. Hence, $x_i^{q_i} \in K(x_1)\,(x_2^{q_i}, \ldots, x_i^{q_i})$. $\{x_1^j\}_{0 \leq j < q_i}$ is a vector space basis for $K(x_1)$ over $K(x_1^{q_i})$, so

$$x_i^{q_i} = \sum_{j=0}^{q_i} g_j x_1^j \tag{4.2}$$

where $g_j \in K(x_1^{q_i}, \ldots, x_{i-1}^{q_i})$. It suffices to show that $g_j = 0$ for $j > 0$.

Let $t = q_2/q_i$. Then there is a filtration $K \subseteq K(x_1^{q_2}) \subseteq K(x_1^t) \subseteq K(x_1)$. Raise Equation 4.2 to the power t, so

$$x_i^{q_2} = x_i^{q_i t} = \sum_{j=0}^{q_i} g_j^t x_1^{jt}.$$

Noting that $\{x_1^{jt}\}_{0 \leq j < q_i}$ is a basis for $K(x_1^t)$ over $K(x_1^{q_2})$, it now suffices to show that $x_i^{q_2} \in K(x_1^{q_2})$ and $g_j^t \in K(x_1^{q_2})$ for all j, because then $x_i^{q_2} = g_0^t$, proving that $g_j^t = 0$ for $j > 0$.

$q_2 \geq q_i$, and $K(x_1, x_i)$ is a purely inseparable extension of K with Pickert generating sequence $\{x_1, x_i\}$. By induction, $x_i^{q_2} \in K(x_1^{q_2})$. Also, by definition $g_j \in KL^{q_i}$, so $g_j^t \in KL^{q_2}$. Thus, by the definition of the e_i and the fact that they are not increasing, $KL^{q_2} \subseteq K(x_1)$. Therefore $g_j^t \in K(x_1) \cap K(x_1^{q_2}, x_2^{q_2}, \ldots, x_{i-1}^{q_2}) = K(x_1^{q_2})$ and the proof is done. □

By the above proposition, for each x_i in a Pickert generating sequence, there is a corresponding $g_i \in K(x_1^{q_i}, \dots, x_{i-1}^{q_i})$ such that $x_i^{q_i} = g_i$. These polynomials will be called the **structure equations** for L/K corresponding to the Pickert generating sequence $\{x_1, \dots, x_n\}$, and

$$L \cong K[x_1, \dots, x_n]/(x_1^{q_1} - g_1,\, x_2^{q_2} - g_2, \dots, x_n^{q_n} - g_n)$$

as K-algebras. For each i, the definition of e_i guarantees that q_i is the minimal power of p for which the structure equations have the property described in Proposition 41.

Pickert generating sequences provide another criterion for determining modularity:

Proposition 42. *(19, §5, Theorem 4) Let K be a field of characteristic $p > 0$ and suppose L/K is a finite purely inseparable field extension with Pickert generating sequence $\{x_1, \dots, x_n\}$ and corresponding exponent sequence $e_1 \geq \cdots \geq e_n$. L/K is modular if and only if for all i, $e_i = \exp[x_i : K]$.*

Proof. By construction of the Sweedler diagram, if an extension L/K is modular, then for *any* choice of p-basis $\{x_1, \dots, x_n\}$, $L \cong K(x_1) \otimes_K \cdots \otimes_K K(x_n)$. Suppose $\{y_1, \dots, y_m\}$ is a Pickert generating sequence for L/K and that there exists an i with $e_i < \exp[x_i : K]$. Then there is a structure equation $x^{q_i} = g_i$, with $g_i \notin K$ and the natural multiplication map $K(y_1) \otimes_K K(y_2) \otimes_K \cdots \otimes_K K(y_m) \to L$ has a nontrivial kernel containing the element of the tensor product being sent to $x^{q_i} - g_i \in L$. Hence by Theorem 29, L/K is not modular. Conversely, if $e_i = \exp[x_i : K]$ for each i, then the aforementioned homomorphism is injective, so L/K is modular by Theorem 29. □

The previous proposition makes a connection between the e_i related to a certain Pickert generating sequence and the modularity, or lack thereof, of a finite purely inseparable extension. Modularity is an intrinsic property of a field extension, so it is expected that the e_i will be as well. We next show that the e_i are invariants of a purely inseparable extension. Suppose K is a field with char $K = p > 0$. Let $\{x_1, \ldots, x_n\}$ be a Pickert generating sequence of a purely inseparable extension L/K with corresponding structure equations g_i. Let $\widetilde{K}$ be the field generated over K by the q_ith roots of the coefficients of g_i for all i. Then by Proposition 41, each g_i splits as the q_ith power of a polynomial f_i over $\widetilde{K}$. Define $z_i \coloneqq x_i - f_i(x_1, \ldots, x_{i-1})$ in some algebraic closure of K. Then $\widetilde{K} \otimes_K L$ is generated by $\{x_i\}$ over $\widetilde{K}$, or $\widetilde{K} \otimes_K L = \widetilde{K}\,[x_1, \ldots, x_n]$. Furthermore, by construction $\widetilde{K}[x_1, \ldots, x_n] = \widetilde{K}[z_1, \ldots, z_n]$.

Definition 43. *Let k be a field of and T a finitely-generated k-algebra. If $k[t_1, \ldots, t_r]$ is a polynomial ring over k of transcendence degree $r > 0$, and $T \cong k[t_1, \ldots, t_r]/I$ where $I \subset k[t_1, \ldots, t_r]$ is an ideal generated by $\{t_1^{e_1}, \cdots, t_r^{e_r}\}$ for $e_i > 0$, then T is called a* ***truncated polynomial ring over*** *k.*

Hence, $\widetilde{K}[z_1, \ldots, z_n]$ from above is a truncated polynomial ring, since $z_i^{q_i} = 0$. Note that $\widetilde{K}[x_1, \ldots, x_n]$ is modular over $\widetilde{K}$. To finish laying the groundwork for our stated goal of proving that the exponent sequence of a Pickert generating sequence is intrinsic to the field extension, we establish two technical results of Rasala without proof.

Proposition 44. *(19, §2, Proposition 8) Let R be a commutative ring and A a truncated polynomial ring over R. Suppose $\{u_1, \ldots, u_n\}$ and $\{w_1, \ldots, w_m\}$ are minimal generating sets* *of A/R with e_i the order of u_i and f_j the order of w_j. Then $n = m$ and, up to some relabeling, $e_k = f_k$ for each k.*

Proposition 45. *(19, p.425) If L/K is a finite purely inseparable field extension with Pickert generating sequence $\{x_1, \ldots, x_n\}$, then the field $\widetilde{K}$ defined in the paragraph preceding Definition 43 is the unique smallest field such that $\widetilde{K} \otimes_K L$ is a truncated polynomial ring.*

These two uniqueness propositions provide the final criteria for

Theorem 46. *Let L/K be a finite purely inseparable extension. Then any exponent sequence derived from a Pickert generating sequence is independent of the choice of p-basis.*

Proof. Using the above notation, for any Pickert generating sequence of L/K, the exponent sequence is the same as the exponent sequence of the truncated polynomial ring $\widetilde{K}[z_1 \ldots, z_n]$ over $\widetilde{K}$, where the z_i are constructed as above. By Proposition 44, $\widetilde{K}$ is unique, independent of the choice of p-basis of L/K, and by Proposition 45, the exponent sequence of $\widetilde{K}[z_1, \ldots, z_n]$ is unique. Therefore the exponent sequence of L/K is independent of the choice of p-basis. □

Modularity can be determined from the exponent sequence by Proposition 42, but this determination will still be non-intrinsic since a choice of p-basis is required in the proposition. The structure equations of an extension, however, can be related to behavior of the differential operators, allowing us to construct a test for modularity.

4.5 Differential Operators on Modular Field Extensions

An elementary observation by Sato (21, Theorem 2) characterizes the ring of differential operators of a modular field extension in terms of higher derivations over that extension.

Theorem 47. *Let K/k be a finite purely inseparable field extension. K/k is modular if and only if $\mathit{Diff}_k K$ is generated as a K-algebra by the coefficients of the higher derivations of K/k.*

Proof. The proof of this theorem is very similar to the proof of Theorem 34. Let $\{x_1, \ldots, x_n\}$ be a p-basis for K/k. If this extension is modular, then the higher derivations which send x_i to $x_i + t$ generate the group of higher derivations of K/k (allowing reparameterizations of t). If e_i is the exponent of x_i over k, then these higher derivations can be written as

$$\sum_{i=0}^{p^{e_i}-1} \left(\frac{\partial}{\partial x_i}\right)^{[i]} t^i,$$

the coefficients of which clearly generate $\mathrm{Diff}_k K$.

On the other hand, suppose the coefficients of the higher derivations of K/k generate the ring of differential operators $\mathrm{Diff}_k K$. Let $x \in K \setminus k$. Then there exists a differential operator $D \in \mathrm{Diff}_k K$ such that $D(x) \neq 0$. D is generated by coefficients of higher derivations. Thus there exists a higher derivation $\overline{E}_x = (\iota_K, E_1, \ldots, E_n)$ such that $E_i(x) \neq 0$ for some i. Therefore, the set of higher derivations $\mathcal{E} = \{\overline{E}_x\}_{x \in K \setminus k}$ are trivial on k but are not all trivial on K. Hence k is the subfield of constants of $\mathcal{E}$ and K/k is a modular extension by Theorem 29. □

By Theorem 47, studying the rings of differential operators for modular extensions provides information on the higher derivations of the extension, which in turn is related to the extended derivations that appear in Chapter 3. We seek a more intrinsic property of the differential operators that determines whether a purely inseparable field extension is modular.

Lemma 48. *Let K be a field of characteristic $p > 0$ and suppose L/K is a finite purely inseparable extension of K. Let $\{x_1, x_2, \ldots, x_n\}$ be a Pickert generating sequence for L/K with corresponding exponent sequence $e_1 \geq e_2 \geq \cdots \geq e_n$ and let D be a differential operator of order N in $\mathit{Diff}_K K(x_1, \ldots, x_i)$ for $i < n$. Suppose $\widetilde{D} \in \mathit{Diff}_K K(x_1, \ldots, x_{i+1})$ is the unique extension of D such that $\widetilde{D}\Big|_{K(x_1,\ldots,x_i)} = D$ and $\widetilde{D}(x_{i+1}^j) = 0$ for all $0 \leq j < p^{e_{i+1}}$. Then $\widetilde{D}$ is a differential operator of order N.*

Proof. Set $q_i = p^{e_i}$ and let f_{i+1} be the structure equation for x_{i+1} with respect to the Pickert generating sequence $\{x_1, \ldots, x_n\}$. Thus $x_{i+1}^{q_{i+1}} = f_{i+1}(x_1, \ldots, x_i)$ where, by Proposition 41, the degree of each x_j in f_{i+1} is a multiple of q_{i+1}. Note that $K(x_1, \ldots, x_{i+1}) = \bigoplus_{j=0}^{q_{i+1}-1} K(x_1, \ldots, x_i)x_{i+1}^j$. Therefore, the map $\widetilde{D}$ as defined in the statement of the lemma is a well-defined endomorphism of $K(x_1, \ldots, x_{i+1})$ over K and is unique by the direct sum decomposition of $K(x_1, \ldots, x_{i+1})$. Since $K(x_1, \ldots, x_{i+1})/K$ is a finite purely inseparable extension, every endomorphism is a differential operator. Hence, $\widetilde{D} \in \mathrm{Diff}_K K(x_1, \ldots, x_{i+1})$.

The order of $\widetilde{D}$ is greater than or equal to the order of D as differential operators in $\mathrm{Diff}_K K(x_1, \ldots, x_i)$ and $\mathrm{Diff}_K K(x_1, \ldots, x_{i+1})$, respectively. Thus, it remains to show that the order of $\widetilde{D}$ is N. Suppose M is the order of $\widetilde{D}$. Then there exist $a_1, \ldots, a_M$ such that

$$\left[\left[\cdots\left[\widetilde{D}, a_1\right], a_2\right], \ldots, a_M\right] = z \in K(x_1, \ldots, x_{i+1}) \tag{4.3}$$

where $z \neq 0$. This expression is symmetric in the a_i and is a derivation in each commutator. That is, for any a, $b \in K(x_1, \ldots, x_{i+1})$

$$\begin{aligned}\left[\left[\cdots\left[\widetilde{D},\, a_1\right],\, a_2\right],\ldots, ab\right] &= a\left[\left[\cdots\left[\widetilde{D},\, a_1\right],\, a_2\right],\ldots, b\right] \\ &+ b\left[\left[\cdots\left[\widetilde{D},\, a_1\right],\, a_2\right],\ldots, a\right].\end{aligned}$$

Hence, Equation 4.3 can be decomposed as a sum of commutators such that one of the summands is nonzero. In particular, there exists a nonnegative integer J and $g_1 \ldots g_{M-J} \in K(x_1, x_2, \ldots, x_i)$ such that

$$\left[\left[\left[\cdots\left[\left[\left[\left[\widetilde{D},\, x_{i+1}\right],\, x_{i+1}\right],\ldots, x_{i+1}\right], g_1\right], g_2\right]\ldots,\right], g_{M-J}\right] \neq 0 \tag{4.4}$$

where the number of x_{i+1}'s in this expression is J. By Gerstenhaber (9, Lemma 5.1), q_{i+1} divides J. If $J = cq_{i+1}$ where c is a nonnegative integer, then using a formula proven by Nakai (17, Corollary 11.2), Equation 4.4 simplifies to

$$\left[\left[\left[\cdots\left[\left[\left[\left[\widetilde{D},\, f_{i+1}\right],\, f_{i+1}\right],\ldots, f_{i+1}\right], g_1\right], g_2\right]\ldots,\right], g_{M-J}\right] \in K(x_1, \ldots, x_{i+1})^{\times} \tag{4.5}$$

where the number of f_{i+1}'s in the expression is c. This equation is the commutator of $\widetilde{D}$ with $M - J + c$ elements of $K(x_1, \ldots, x_i)$. Hence, Equation 4.5 equals

$$[[[\cdots[[[[D,\, f_{i+1}],\, f_{i+1}],\ldots, f_{i+1}], g_1], g_2]\ldots,], g_{M-J}] \tag{4.6}$$

Each f_{i+1} is a polynomial of degree at least q_{i+1}, hence the order of $[D,\, f_{i+1}]$ is at most $N - q_{i+1}$. Therefore the order of the differential operator in Equation 4.6 is at most $N - cq_{i+1} - (M - J) = N - M$. The iterative commutator is a differential operator of order 0 by construction, hence $N = M$ and the order of $\widetilde{D}$ equals the order of D.

□

Let A be a ring of characteristic $p > 0$ and B a commutative A-algebra. Define

$$\mathcal{A}_{B/A,\,i} = \{D \in \mathrm{Diff}_A^{p^i} B : \forall j \leq i,\, D(B^{p^j}) \subseteq B^{p^j}\}.$$

Note that $\mathcal{A}_{B/A,\,i}$ is a B^{p^i}-subalgebra of $\mathrm{Diff}_A^{p^i} B$. As an example, let L/K be a modular field extension with a p-basis $\{x_1, \ldots, x_n\}$ such that $\exp[x_i : K] > 1$ for each $1 \leq i \leq n$. $\mathcal{A}_{L/K,\,1}$ consists of all differential operators of order ≤ 1 which map $L^p \to L^p$. Hence $\mathcal{A}_{L/K,\,1} = L^p \bigoplus \mathrm{Der}_K L \bigoplus_{i=1}^{n} L^p \left(\dfrac{d}{dx_i}\right)^{[p]}$. Also, since $\left(\dfrac{d}{dx_i}\right)^{[i]} (L^p) = 0$ for $i < p$,

$$\mathcal{A}_{L/K,\,2} = L^{p^2} \bigoplus_{0 < i_1 + \cdots i_n < p} L \left(\frac{d}{dx_1}\right)^{[i_1]} \cdots \left(\frac{d}{dx_n}\right)^{[i_n]} \bigoplus_{j=1}^{n} L^p \left(\frac{d}{dx_j}\right)^{[p]} \bigoplus_{i=1}^{n} L^{p^2} \left(\frac{d}{dx_i}\right)^{[p^2]}.$$

These subalgebras may be complicated to describe in general, but note that the symbol of $\mathcal{A}_\rangle$ kills all direct summands except for the top degree differential operators. The $\mathcal{A}_i$, not the symbol algebra, are necessary to study differential operators for modular extensions.

Theorem 49. *Let L/K be a finite purely inseparable extension of exponent e. Then L/K is modular if and only if for all $0 < i \leq e-1$, the multiplication homomorphism $L \otimes_{L^{p^i}} \mathcal{A}_i \rightarrow \mathrm{Diff}_K^{p^i} L$ is a surjection. That is, for each i, $\mathcal{A}_{L/K,i}$ spans $\mathrm{Diff}_K^{p^i} L$ as an L subspace.*

Proof. Let $\mathcal{A}_{L/K,i}$ be denoted $\mathcal{A}_i$ in this proof. Suppose L/K is a modular extension. By definition there exist $\{x_1, \ldots x_n\} \subset L$ such that $L \cong \bigotimes_{i=1}^{n} K(x_i)$. Then

$$\mathrm{Diff}_K L \cong \bigotimes_{i=1}^{n} \mathrm{Diff}_K K(x_i). \tag{4.7}$$

Now, if $l_i = \exp\,[x_i : K]$, then $\mathrm{Diff}_K K(x_i)$ is generated as a $K(x_i)$-algebra by $\left\{ \left(\frac{d}{dx_i} \right)^{[p^k]} \right\}_{0 \leq k < l_i}$. Hence, by the isomorphism in Equation 4.7, any $D \in \mathrm{Diff}_K L$ is a linear combination over L of differential operators of the form

$$D_{a_1,\ldots,a_n} := \left(\frac{d}{dx_1} \right)^{[a_1]} \cdots \left(\frac{d}{dx_n} \right)^{[a_n]}$$

where $0 \leq a_i < l_i$. $D_{a_1,\ldots,a_n} \in \mathcal{A}_i$ if and only if $a_1 + \cdots + a_n \leq p^i$. Thus every $D \in \mathrm{Diff}_K^{p^i} L$ is the sum of elements in $\mathcal{A}_i$. Hence $\mathcal{A}_i$ spans $\mathrm{Diff}_K^{p^i} L$.

Now suppose L/K is not a modular extension. We will find elements a, $b \in L$ with $a \in L^{p^i}$ and $b \in L^{p^j}$ and a differential operator $D \in \mathrm{Diff}_K^{p^l} L$, i, $j \leq l$ that satisfy the following properties: D is not the sum of products of differential operators of lower order, $D(a) \in L^{p^i}$, and $D(b) \notin L^{p^j}$. This operator D will then not be spanned by $\mathcal{A}_l$.

By Theorem 46, it is possible to construct a Pickert Generating Sequence $\{x_1, \ldots, x_n\}$ with $e_1 \geq e_2 \geq \cdots \geq e_n$, the intrinsic non-increasing sequence of exponents. Since L/K is not modular, by Proposition 42 there exists an integer i satisfying $\exp[x_i : K(x_1, \ldots, x_{i-1}] \neq \exp[x_i : K]$, and x_i has a structure equation with coefficients which are not in $L^{p^{e_i}}$.

Let $z \coloneqq x_i$ be the first such element in the Pickert Generating sequence to exhibit this property. Set $q = p^{e_i}$ and let $z^q = f(x_1^q, \ldots, x_{i-1}^q)$ be the structure equation of z. Since $z^q \notin K$, f is neither constant nor does the degree of every x_j^q in the polynomial exceed p^{e/e_i}.

The polynomial f must have at least two terms with coefficients which are not qth powers in L. That is, suppose $\alpha x_1^{qa_1} \ldots x_{i-1}^{qa_{i-1}}$ is the only summand of f with $\alpha \in K \setminus L^q$. Then solving the structure equation of z for α, we get

$$\alpha = \frac{z^q - f(x_1^q, \ldots x_{i-1}^q) + \alpha x_1^{qa_1} \ldots x_{i-1}^{qa_{i-1}}}{x_1^{qa_1} \ldots x_{i-1}^{qa_{i-1}}}.$$

The right-hand side is a qth power in L, which contradicts $\alpha \notin L^q$.

Thus, at least two of the coefficients of terms of f are not in L^q. Let $\mathcal{C}$ denote the set of all such monomials of f. $\mathcal{C}$ has at least two elements, so f must have K-independent summands $ax_1^{qa_1} \cdots x_{i-1}^{qa_{i-1}}$ and $bx_1^{qb_1} \cdots x_{i-1}^{qb_{i-1}}$ where a and b are not in L^q and $a_j, b_j < p^{e_j - e_i}$ for all $1 \leq j \leq i-1$. At least one of the x_j must have different degrees in these summands or else they are not linearly independent. Suppose without loss of generality that x_1 is the element with $a_1 \neq b_1$ and that b_1 is the largest such exponent of x_1^q for such an element of $\mathcal{C}$. Define Q as the largest power of p which is $\leq qb_1$. Set

$$f(x_1^q \ldots, x_{i-1}^q) = \sum_{0 \leq j_k < p^{e_k - e_i}} \alpha_{j_1,\ldots,j_{i-1}} x_1^{qj_1} \cdots x_{i-1}^{qj_{i-1}}$$

Now, $\left(\dfrac{d}{dx_1}\right)^{[Q]}$ is a differential operator on $K(x_1, \ldots, x_{i-1}) = \bigotimes_{j=1}^{i-1} K(x_j)$ over K of order Q. By Lemma 48, we can extend $\left(\dfrac{d}{dx_1}\right)^{[Q]}$ to a differential operator $D \in \mathrm{Diff}_K K(x_1, \ldots, x_i)$ of order Q. By induction on i we can extend D in this manner to a differential operator on L. Call $\widetilde{D}$ the extension of $\left(\dfrac{d}{dx_1}\right)^{[Q]}$ to L. Gerstenhaber (9) calls $\widetilde{D}$ the *normal extension of* $\left(\dfrac{d}{dx_1}\right)^{[Q]}$, which is a differential operator of order Q by Lemma 48.

So,

$$\begin{aligned}
\widetilde{D}(z^q) &= D\left(f(x_1^q, \ldots, x_{i-1}^q)\right) \\
&= \left(\frac{d}{dx_1}\right)^{[Q]} \left(\sum_{0 \leq j_k < p^{e_k - e_i}} \alpha_{j_1,\ldots,j_{i-1}} x_1^{qj_1} \cdots x_{i-1}^{qj_{i-1}} \right) \\
&= \sum_{0 \leq j_k < p^{e_k - e_i}} \alpha_{j_1,\ldots,j_{i-1}} \binom{qj_1}{Q} (x_1)^{qj_1 - Q} (x_2^q)^{j_2} \cdots (x_{i-1}^q)^{j_{i-1}}
\end{aligned}$$

This last sum is not zero because, by the choice of x_1, f has at least one nonzero term with the degree of x_1^q greater than 0. Additionally, by the choice of Q, $\binom{qj_1}{Q} \neq 0$ for some j_1 (1, p.577). Likewise, the sum is not a qth power in L, because at least one of the coefficients $\alpha_{j_1,\ldots,j_{i-1}}$ is neither a qth power in L nor the coefficient of a term which vanishes by $\widetilde{D}$. Therefore,

$\widetilde{D}(z^q) \notin L^q$ but $\widetilde{D}(x_1^Q) = 1 \in L^Q$. Since $\left(\dfrac{d}{dx_1}\right)^{[Q]}$ is not the product of differential operators of lower order in $\mathrm{Diff}_K K(x_1, \ldots, x_{i-1})$, then $\widetilde{D}$ is not the product of differential operators of lower order either. Therefore, $\widetilde{D}$ is not in the L-span of $\mathcal{A}_i$ for any i and the theorem is proven. □

An immediate corollary of the theorem is

Corollary 50. *Let L/K be as in the theorem. Let $\mathcal{D}$ be the subalgebra of $\mathrm{Diff}_K L$ generated by the $\mathcal{A}_i$. Then $\mathcal{D}$ is the largest subalgebra of $\mathrm{Diff}_K L$ such that $L/L^{\mathcal{D}}$ is a modular extension.*

Thus L/K has a minimal intermediate subfield E with L/E modular, which is also the the subfield of constants of $\mathrm{HDer}_K L$. We remark that the relationship between Theorem 49 above and the reformulation of the Sweedler Diagram using modules of differentials presented in Theorem 30 from Chapter 2 is unclear.

We finish this chapter by interpreting Example 4.3.3 in light of Theorem 49. Recall $L = k_0(X, U, Z)$, $K = k_0(X, U^{p^2} - XZ^p, Z^{p^2})$ and $K' = k_0(X, U^{p^3}, Z^p)$. $\mathrm{Diff}_K L$ is generated over L by ∂_U, ∂_Z, $\partial_U^{[p]}$, and D where $\sigma(D) = X\partial_U^{[p^2]}$. $\mathrm{Diff}_{K'} L$ is generated over L by ∂_U, ∂_Z, $\partial_U^{[p]}$, and $\partial_U^{[p^2]}$. L/K' is modular, and

$$\begin{aligned}
\mathcal{A}_{L/K',0} &= L \\
\mathcal{A}_{L/K',1} &= L^p \bigoplus_{0<i_1+i_2<p} L\partial_U^{[i_1]}\partial_Z^{[i_2]} \bigoplus L^p\partial_U^{[p]} \\
\mathcal{A}_{L/K',2} &= L^{p^2} \bigoplus_{0<i_1+i_2<p} L\partial_U^{[i_1]}\partial_Z^{[i_2]} \bigoplus L^p\partial_U^{[p]} \bigoplus L^{p^2}\partial_U^{[p^2]}
\end{aligned}$$

Note that $\mathcal{A}_{L/K',2}$ generates $\mathrm{Diff}_{K'} L$ over L.

For L/K,

$$\begin{aligned}
\mathcal{A}_{L/K,\,0} &= L \\
\mathcal{A}_{L/K,\,1} &= L^p \bigoplus_{0<i_1+i_2<p} L\partial_U^{[i_1]}\partial_Z^{[i_2]} \bigoplus L^p\partial_U^{[p]} \\
\mathcal{A}_{L/K,\,2} &= L^{p^2} \bigoplus_{0<i_1+i_2<p} L\partial_U^{[i_1]}\partial_Z^{[i_2]} \bigoplus L^p\partial_U^{[p]}
\end{aligned}$$

The differential operator D is not in any of these subsets of $\mathrm{Diff}_K L$ because $D(Z^p) = 1 \in L^p$ and $D(U^{p^2}) = X \notin L^{p^2}$, demonstrating that L/K is not modular. Note that for L/K, the homomorphism defined in Theorem 49 is surjective for $0 \leq i < 2$, which are the degree for which $\mathcal{A}_{L/K,\,i}$ agrees with $\mathcal{A}_{L/K',\,i}$.

CHAPTER 5

FUNDAMENTAL FORMS

So far our search for Galois correspondences for purely inseparable extensions has focused on finding correspondences to intermediate subfields which are the base fields of modular extensions. The Jacobson-Bourbaki Theorem (Theorem 13) does not pick out modular intermediate subfields in particular, but as we have seen from the previous chapter, the filtration of the ring of differential operators of a purely inseparable extension provides some information on the field extension as well as its lattice of subfields. To each intermediate subfield of E' of E/F, Gerstenhaber (9) associates the top degree subspace of the symbol algebra of E/E'. This subspace will be 1-dimensional, and Gerstenhaber calls a nonzero element of this subspace the *fundamental form*. Because the choice of such an element is not canonical, we will call the entire subspace *the fundamental form* instead.

Gerstenhaber proves that every intermediate subfield of the finite purely inseparable extension E/F corresponds to a factor of a nonzero element of the fundamental form of E/F in the divided powers algebra $\Gamma^* (\mathrm{Der}_F E)$. His goal was to find criteria for when a subspace of the symbol algebra of E/F is the fundamental form of an intermediate subfield. He was mostly unsuccessful in this goal, mainly because every element of the symbol algebra is nilpotent, making the factorization of elements non-unique. In this chapter we will give an explicit construction of the fundamental form for a finite purely inseparable extension. Also, in a simple case, we will present criteria using the Poisson structure on the symbol algebra for when a subspace of the symbol algebra is the fundamental form of an intermediate extension.

5.1 Differential Operators and Symmetric Multiderivations

Let k be a field and A a commutative k-algebra. Define $C^n(A,\, A) := \mathrm{Hom}_k(\underbrace{A \otimes_k \cdots \otimes_k A}_{n},\, A)$. For any $f \in C^n(A,\, A)$ and for all $a_0, \ldots a_n \in A$, define $\Delta : C^n(A,\, A) \to C^{n+1}(A,\, A)$ as

$$\Delta(f)(a_0, \ldots, a_n) = a_0 f(a_2, \ldots a_n) - f(a_0 a_1,\, a_2, \ldots, a_n) + a_1 f(a_0,\, a_2, \ldots, a_n). \tag{5.1}$$

Restrict to the submodule $Y^n \subseteq C^n(A,\, A)$ of maps from $\underbrace{A \otimes_k \cdots \otimes_k A}_{n}$ to A which factor through $\mathrm{Sym}^n_k(A)$. Clearly $\mathrm{End}_k A = Y^1$, and by a basic combinatorial argument (9, p. 167), for any $D \in \mathrm{End}_k A$ and $a_0, \ldots, a_n \in A$,

$$\Delta^n D(a_0,\, a_1, \ldots, a_n) = \sum_{s=0}^{n} (-1)^{s-1} \sum_{i_1 < i_2 < \ldots i_s} a_{i_1} a_{i_2} \cdots a_{i_s} D\left(a_1 \cdots \widehat{a_{i_1}} \cdots \widehat{a_{i_s}} \cdots a_n\right).$$

The right-hand side is symmetric with respect to the a_i, and appears in Equation 4.1 as well as in Nakai (17, p.3), where he proves the above equation equals

$$\left[\left[\cdots [D,\, a_1]\,,\, a_2\right], \cdots, a_n\right](a_0).$$

Hence by Definition 36, $\Delta^n D = 0$ if and only if D is a differential operator of A/k of order $\leq n$. Note also that if n is the minimal integer for which $\Delta^n D = 0$, then $\Delta\left(\Delta^{n-1} D\right) = 0$. Equation 5.1 and the fact that $\Delta^{n-1}D \in Y^n$ imply that $\Delta^{n-1}D$ is a symmetric k-multilinear homomorphism $A^n \to A$ which acts as a derivation in every coordinate. That is, for all $a_j, b_i, c_i \in A$,

$$\Delta^{n-1}D(a_0, \ldots, b_i c_i, \ldots a_n) = b_i \Delta^{n-1}D(a_0, \ldots, c_i, \ldots a_n) + c_i \Delta^{n-1}D(a_0, \ldots, b_i, \ldots a_n).$$

Gerstenhaber calls such a map an $(n+1)$**-symmetric k-multiderivation** and denotes the set of such maps $\mathrm{SDer}_k^{n+1}A$. Note that $\mathrm{SDer}_k^n A$ has a left A-module structure induced from the A-module structure on $C^{n+1}(A,\, A)$.

It is important to notice that an n-symmetric multiderivation of A/k is nothing more an than element of $\left(\mathrm{Sym}^n\left(\Omega^1_{A/k}\right)\right)^\vee$. Thus, if $\mathrm{Der}_k A$ is a finite rank projective A-module, it was noted in Section 4.2 that $\left(\mathrm{Sym}^*\left(\Omega^1_{A/k}\right)\right)^\vee \cong \Gamma^*(\mathrm{Der}_k A)$.

Furthermore, it is an observation of Narváez Macarro (18, p.2992) that $\Gamma^*(\mathrm{Der}_k A)$ is isomorphic to the A-module $\bigoplus_{i=0}^{\infty} \mathrm{SDer}_k^i A$ (setting $\mathrm{SDer}_k^0 A = A$). In fact, $\bigoplus_{i=0}^{\infty} \mathrm{SDer}_k^i A$ has a graded A-algebra structure which makes the module isomorphism an isomorphism of graded A-algebras: Let $f \in \mathrm{SDer}_k^n A$ and $g \in \mathrm{SDer}_k^m A$. Then for any $a_1, \ldots, a_{m+n} \in A$,

$$(f \star g)(a_1, \ldots, a_{m+n}) = \sum_J f(a_J) g(a_{J^c})$$

where J runs over all cardinality m subsets of $\{a_1, \ldots, a_{m+n}\}$ and J^c is the complement of J in $\{a_1, \ldots, a_{m+n}\}$.

The homomorphism $\theta : \mathrm{Gr}^\bullet \mathrm{Diff}_k A \to \Gamma^*(\mathrm{Der}_k A)$ defined in Section 4.2 is an injection, and for any $D \in \mathrm{Diff}_k^n A$, $\theta(\sigma(D)) = \Delta^{n-1}D$ where $\Delta^{n-1}D$ is viewed as an element in $\Gamma^*(\mathrm{Der}_k A)$ by the isomorphism noted above. Thus the following discussion of Gerstenhaber's ideas will adopt the standard notations of divided powers rings instead of symmetric multderivations.

5.2 Fundamental Forms of Purely Inseparable Extensions

Definition 51. *Let k be a field and A a commutative k-algebra. Suppose there exists a minimal positive integer m such that for all $m' > m$, $Gr^{m'} Diff_k A = 0$. If $Gr^m Diff_k A$ is a free A-module of rank 1, then $Gr^m Diff_k A$ is called the* ***fundamental form of*** *A/k and is denoted $\Gamma(A/k)$.*

Let L/K be a purely inseparable extension of fields of characteristc $p > 0$ with exponent e. Suppose a p-basis of L/K contains only one element. Then $L = K(x)$ for some $x \in L$ and $\exp[x : K] = e$. The fundamental form of L/K exists and is simple to construct based on the calculation of the ring of differential operators from Example 4.3.1:

$$\Gamma(L/K) = L \cdot \sigma\left(\left(\frac{d}{dx}\right)^{[p^e-1]}\right).$$

Suppose that L/K is again a finite purely inseparable extension of fields of characteristic $p > 0$, but with a p-basis of cardinality larger than 1. By the framework laid out in the previous example, we use Lemma 48 again to explicitly construct the fundamental form of L/K. Let $\{x_1, \ldots, x_n\}$ be a Pickert generating sequence of L/K with corresponding exponent sequence $e_1 \geq e_2 \geq \cdots \geq e_n$. Consider the filtration of L

$$K \subset K(x_1) \subset K(x_1, x_2) \subset \cdots \subset K(x_1, \ldots, x_n) = L.$$

From above, $\Gamma(K(x_1)/K)$ is the L-vector space generated by the symbol of $D_1 := \left(\frac{d}{dx_1}\right)^{[p^{e_1}-1]}$. Let $\widetilde{D}_1$ be the differential operator in $\mathrm{Diff}_K K(x_1,\, x_2)$ which extends D_1 as described in Lemma 48. Then

$$\Gamma(K(x_1,\, x_2)/K) = L \cdot \sigma\left(\widetilde{D}_1 \left(\frac{\partial}{\partial x_2}\right)^{[p^{e_2}-1]}\right).$$

Generalizing this construction, set $D_i = \left(\dfrac{\partial}{\partial x_i}\right)^{[p^{e_i}-1]} \in \mathrm{Diff}_{K(x_1,\ldots,x_{i-1})} K(x_1, \ldots, x_i)$. Then the normal extension $\widetilde{D}_i \in \mathrm{Diff}_K L$ extends D_i as described in Theorem 49. Therefore

$$\Gamma(L/K) = L \cdot \sigma\left(\widetilde{D}_1 \widetilde{D}_2 \cdots \widetilde{D}_n\right). \tag{5.2}$$

If $D,\, E \in \Gamma^*(\mathrm{Der}_K L)$, then D **divides** E if there exists $G \in \Gamma^*(\mathrm{Der}_K L)$ such that $DG = E$. As discussed in 4.2, every element in $Gr^{\bullet}\mathrm{Diff}_K L$ is nilpotent of order at most p. Thus, a factorization of an element of $Gr^{\bullet}\mathrm{Diff}_K L$ will not necessarily be unique.

Let k be a field of characteristic $p > 0$ and suppose K and L are purely inseparable extensions of k such that $k \subseteq K \subseteq L$. Then $\Gamma^*(\mathrm{Der}_K L) \subseteq \Gamma^*(\mathrm{Der}_k L)$ and the following question arises: How does $\Gamma(L/K)$ relate to $\Gamma(L/k)$?

Theorem 52. *(9, Main Theorem) Let $k \subseteq K \subseteq L$ be fields as described above. Then for all $\gamma \in \Gamma(L/K)$ and $\gamma' \in \Gamma(L/k)$ with $\gamma \neq 0$, γ divides γ'.*

Sketch. We only sketch the proof, noting that it requires the existence of extensions of differential operators like we proved in Lemma 48 and Theorem 49, but does not require knowing the order of the extension. After choosing Pickert generating sequences for L/K and K/k, let B be the dual basis of L/K determined by the generating sequence for L/K and let B' be the dual basis of K/k determined by the generating sequence for K/k. Then there exist $f \in B \subset \mathrm{Diff}_K L$ and $h \in B' \subset \mathrm{Diff}_k K$ such that $\Gamma(L/k) = L \cdot \sigma\left(f\overline{h}\right)$ where $\overline{h}$ is the normal extension of h to $\mathrm{Diff}_k L$. Hence $\sigma(f) \in \Gamma^*(\mathrm{Der}_k L)$ is an element of the fundamental form of L/K, and $\sigma(f)|\Gamma(L/k)$. □

5.3 Examples of Fundamental Forms

Using the results from Chapter 4 regarding rings of differential operators of purely inseparable extensions, it is fairly easy to compute the fundamental form of an extension.

5.3.1 Example 1

Let k_0 be a perfect field of characteristic $p > 0$ and suppose X and Y are algebraically independent over k_0. Suppose $L = k_0(X, Y)$ and $K = k_0(X^p, Y^p)$. Then $\Gamma(L/K) = \left(\frac{\partial}{\partial X}\right)^{[p-1]}\left(\frac{\partial}{\partial Y}\right)^{[p-1]}$. Suppose K' is an intermediate subfield of L/K. If $K' \neq L$ and $K \neq K'$, then L/K' is a purely inseparable extension of degree p and exponent 1. Hence, by Theorem 21, $\mathrm{Der}_{K'} L$ is a p-Lie subalgebra of $\mathrm{Der}_K L$ which must have dimension 1 over L. For some $a, b \in L$, let

$$D = a\frac{\partial}{\partial X} + b\frac{\partial}{\partial Y}$$

be a generator for $\mathrm{Der}_{K'} L$. Then D^{p-1} is a differential operator in $\mathrm{Diff}_{K'} L$ of order $\leq p - 1$, which can be written as a sum

$$\sum_{0\leq i+j\leq p-1} c_{ij}\left(\frac{\partial}{\partial X}\right)^{i}\left(\frac{\partial}{\partial Y}\right)^{j}. \tag{5.3}$$

The L-vector space generated by the symbol of this differential operator is $\Gamma(L/K')$. Thus,

$$L \cdot \left(\sum_{i+j=p-1} c_{ij} \left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^j \right) = \Gamma(L/K').$$

It is straightforward to show that $\displaystyle\sum_{i+j=p-1} c_{ij} \left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^j \Bigg| \Gamma(L/K)$: Since $\dfrac{\partial}{\partial X}$ and $\dfrac{\partial}{\partial Y}$ are nilpotent of order p in $\Gamma^*(\mathrm{Der}_K L)$, for any pair $(m,\, n)$ such that $c_{mn} \neq 0$,

$$\left(\frac{\partial}{\partial X}\right)^{p-1-m} \left(\frac{\partial}{\partial Y}\right)^{p-1-n} \Gamma(L/K') = c_{mn} \left(\frac{\partial}{\partial X}\right)^{p-1} \left(\frac{\partial}{\partial Y}\right)^{p-1} \in \Gamma(L/K).$$

Hence the fundamental form of L/K' divides the fundamental form of L/K. In fact, any element of $\Gamma^*(\mathrm{Der}_K L)$ which is of the form shown in Equation 5.3 will divide $\Gamma(L/K)$, whether it is an element of the fundamental form of an intermediate subfield of L/K or not.

5.3.2 Example 2

Using the notation from Example 4.3.2, $\mathrm{Diff}_K L$ is generated as an L-algebra by ∂_U, ∂_Z, and $X\partial_U^{[p]} + \partial_Z^{[p]}$. Up to scalar multiple, the largest order differential operator of $\mathrm{Diff}_K L$ is $\partial_U^{[p-1]}\partial_Z^{[p-1]} \left(X\partial_U^{[p]} + \partial_Z^{[p]}\right)^{[p-1]}$, which is equal to

$$\partial_U^{[p-1]}\partial_Z^{[p-1]} \left(X^{p-1}\partial_U^{[p^2-p]} + X^{p-2}\partial_U^{[p^2-2p]}\partial_Z^{[p]} + \cdots + \partial_Z^{[p^2-p]}\right).$$

The L-vector space generated by the symbol of this operator is $\Gamma(L/K)$. Letting $K' = k_0(U^p,\, Z^p)$, then $\Gamma(L/K') = L \cdot \left(\partial_U^{[p-1]}\partial_Z^{[p-1]}\right)$, which clearly divides $\Gamma(L/K)$.

5.3.3 Example 3

It is not true that distinct intermediate subfields must have distinct fundamental forms. Let k_0 be a perfect field of characteristic $p > 0$ with X, U, and Z algebraically independent over k_0. Define the fields

$$\begin{aligned} L &= k_0(X,\, U,\, Z) \\ K' &= k_0(X,\, U^{p^3},\, Z^p) \\ K'' &= k_0(X,\, U^{p^2} - XZ^p,\, Z^{p^2}) \\ K_0 &= k_0(X,\, U^{p^3},\, Z^{p^2}). \end{aligned}$$

Suppose $S \subset \operatorname{Diff} L$. Let $L\left\langle S \right\rangle$ denote the L-subalgebra of $\operatorname{Diff} L$ generated by S. Using the notation from the example in 4.3.3,

$$\begin{aligned} \operatorname{Diff}_{K'} L &= L\left\langle \partial_U,\, \partial_Z,\, \partial_U^{[p]},\, \partial_U^{[p^2]} \right\rangle \\ \operatorname{Diff}_{K''} L &= L\left\langle \partial_U,\, \partial_Z,\, \partial_U^{[p]},\, X\partial_U^{[p^2]} + \partial_Z^{[p]} \right\rangle \\ \operatorname{Diff}_{K_0} L &= L\left\langle \partial_U,\, \partial_Z,\, \partial_U^{[p]},\, \partial_Z^{[p]},\, \partial_U^{[p^2]} \right\rangle \end{aligned}$$

Thus $\Gamma(L/K') = \Gamma(L/K'') = L \cdot \left(\partial_U^{[p^2-1]} \partial_Z^{[p-1]}\right)$, which shows different intermediate subfields may have the same fundamental form. In general, factors of a generator of the fundamental form classify families of intermediate fields.

5.3.4 Example 4

In certain cases these families of intermediate fields can be explicitly described. Let k_0 be a perfect field of characteristic $p > 0$ with X and Y algebraically independent over k_0. Define $L = k_0(X, Y)$ and $K = k_0(X^{p^2}, Y^p)$. L/K is a modular field extension of exponent 2 and degree p^3. Suppose $\alpha \in L$ such that $\alpha^p \in K$. Then $K(\alpha)$ is a purely inseparable extension of K of exponent 1 and $L/K(\alpha)$ is purely inseparable of degree p^2. Assume also that $K(\alpha) \neq k_0(X^p)$. Then X is an element of a p-basis for $L/K(\alpha)$. Since $X^p \notin K(\alpha)$ and $X^{p^2} \in K(\alpha)$, then $\exp[X : K(\alpha)] = 2$, hence X generates L over $K(\alpha)$. Thus

$$\Gamma\left(L/K(\alpha)\right) = L \cdot \left(\frac{d}{dX}\right)^{[p^2-1]}, \tag{5.4}$$

where $\dfrac{d}{dX} \in \mathrm{Der}_K L$. Just as in the previous example, there are many intermediate fields with this fundamental form. For instance, $L/K(X^p + Y)$ and $L/K(3X^p + 2Y)$ have the fundamental form above. In general, for any polynomial $f(X^p)$ over K, $L/K(Y + f(X^p))$ will have this fundamental form.

On the other hand, if $K(\alpha) = k_0(X^p)$, then X cannot generate $L/K(\alpha)$. Hence $L/K(\alpha) = K(\alpha)(X, Y)$, which is a modular extension of exponent 1. In this case,

$$\Gamma\left(L/K(\alpha)\right) = L \cdot \left(\frac{\partial}{\partial X}\right)^{[p-1]} \left(\frac{\partial}{\partial Y}\right)^{[p-1]}, \tag{5.5}$$

where $\frac{\partial}{\partial X}, \frac{\partial}{\partial Y} \in \mathrm{Der}_K L$. Thus, the fundamental form in Equation 5.4 corresponds to a family of intermediate subfields which can be explicitly descibed, while the fundamental form in Equation 5.5 corresponds to a unique intermediate subfield

5.4 Fundamental Forms of Exponent 1 and Degree p^2 Extensions

Studying the case of purely inseparable extensions of exponent 1 demonstrates the complications that can arise in devising a Galois correspondence using fundamental forms. Adopt the notation of Example 5.3.1 above. Since every element in $\Gamma^*(\mathrm{Der}_K L)$ is nilpotent, any element of this ring of the form $\sum_{0 \leq i+j \leq p-1} c_{ij} \left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^j$ divides $\Gamma(L/K)$ where $c_{ij} \in L$. The main question we seek to answer is which factors of a generator of $\Gamma(L/K)$ correspond to intermediate subfields by Theorem 52?

Any proper intermediate subfield K' of L/K has the property that L/K' is purely inseparable of exponent 1. Thus, by Theorem 21, $\mathrm{Diff}_{K'} L$ is generated by an element of $\mathrm{Der}_{K'} L \subseteq \mathrm{Der}_K L$.

$\mathrm{Der}_K L$ is an L-vector space of dimension 2, so there exist a, $b \in L$ such that the L-vector space generated by the symbol of $\left(a\frac{\partial}{\partial X} + b\frac{\partial}{\partial Y}\right)^{p-1}$ is the fundamental form $\Gamma(L/K')$, where $\frac{\partial}{\partial X}$ and $\frac{\partial}{\partial Y}$ form an L-basis of $\mathrm{Der}_K L$. If a or b is 0, then the fundamental form is either $L\left(\frac{\partial}{\partial X}\right)^{[p-1]}$ or $L\left(\frac{\partial}{\partial Y}\right)^{[p-1]}$, and we omit these cases for the rest of the discussion. The computation $\left(a\frac{\partial}{\partial X} + b\frac{\partial}{\partial Y}\right)^{[p-1]}$ is straightforward, so that

$$\sigma\left(\left(a\frac{\partial}{\partial X} + b\frac{\partial}{\partial Y}\right)^{p-1}\right) = \sum_{i=0}^{p-1} a^i b^{p-1-i} \left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^{p-1-i}.$$

Therefore, for an element of $\Gamma^*\left(\mathrm{Der}_K L\right)$ to be the generator of a fundamental form of L/K', it is necessary that

$$\Gamma(L/K') = \sum_{i=0}^{p-1} c_i \left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^{p-1-i}$$

satisfying

$$\frac{c_0}{c_1} = \frac{c_1}{c_2} = \cdots = \frac{c_{p-2}}{c_{p-1}}. \tag{5.6}$$

Fixing a basis for $\mathrm{Der}_K L$, view the space of 1-dimensional subspaces of $\mathrm{Der}_K L$ as the projective line $\mathbb{P}^1_L$. Likewise, fixing the same basis, 1-dimensional subspaces of $\mathrm{Gr}^{p-1}\left(\mathrm{Diff}_K L\right)$ are parameterized by points of $\mathbb{P}^p_L$. Therefore, in order for a point $q \in \mathbb{P}^p_L$ to represent the fundamental form of L/K' for some intermediate subfield K', it is necessary that q lies in the $(p-1)$-uple Veronese embedding from $\mathbb{P}^1_L$ to $\mathbb{P}^p_L$ (23, §4.4).

Once a basis of $\mathrm{Der}_K L$ is chosen and it is determined that an element of $\Gamma^*\left(\mathrm{Der}_K L\right)$ is the image of the $(p-1)$st-power of the symbol of a derivation, it then suffices to show that the L-vector space generated by this derivation is closed under pth powers. This sufficiency follows from Theorem 21, since intermediate subfields of L/K are in $1-1$ correspondence with restricted p-Lie subalgebras of $\mathrm{Der}_K L$. Thus, for any intermediate subfield K' of L/K, $\mathrm{Der}_{K'} L$ is a 1-dimensional vector space over L with a basis $\{D\} \subset \mathrm{Der}_K L$ such that $D^p = aD$ for some $a \in L$.

Let $\gamma \in \Gamma^*\left(\mathrm{Der}_K L\right)$. Using the terminology of fundamental forms, if γ divides a generator of $\Gamma(L/K)$ and there exists a derivation $D \in \mathrm{Der}_K L$ with $D^p = aD$ such that $\gamma = \sigma\left(D^{p-1}\right)$

(possibly up to rescaling by an element of L), then there exists an intermediate subfield $K \subseteq K' \subseteq L$ such that $L \cdot \gamma = \Gamma(L/K')$. Our final goal, then, is to describe this p-closure using the element γ. We first require the following lemma:

Lemma 53. *Let k be a field of characteristic $p > 0$ and suppose K/k is a purely inseparable field extension. Suppose $\{X_1, \ldots, X_n\} \subset K$ are p-independent over k and $\partial_i := \dfrac{\partial}{\partial X_i}$. For any $a_1, \ldots, a_n \in K$, if $D = a_1\partial_1 + \cdots a_n\partial_n$, then*

$$(a_1\partial_1 + \cdots a_n\partial_n)^p = D^{p-1}(a_1)\partial_1 + \cdots + D^{p-1}(a_n)\partial_n.$$

Proof. The ∂_i are commuting K-linearly independent derivations such that $\partial_i^p = 0$ for each i. For each $j < p$, it can be verified by induction that $D^j = D^{j-1}(a_1)\partial_1 + \cdots D^{j-1}(a_n)\partial_n + E_j$ where E_j is a sum of differential operators of the form $c\partial_1^{j_1} \cdots \partial_n^{j_n}$ where $c \in K$ and $1 < j_1 + \cdots + j_n \leq j$. Since D^p must be a derivation by Proposition 18 and each ∂_i is nilpotent of order p, then $E_p = 0$ and the lemma is proven. □

Return to the notation preceding the lemma and suppose $D = a\dfrac{\partial}{\partial X} + b\dfrac{\partial}{\partial Y}$ is a derivation of $\mathrm{Der}_K L$ with a, $b \in L$. Then the subspace of $\mathrm{Der}_K L$ generated by D is closed under pth powers if and only if there exists an $\eta \in L$ such that $D^p = \eta D$, or

$$D^{p-1}(a)\frac{\partial}{\partial X} + D^{p-1}(b)\frac{\partial}{\partial Y} = \eta a\frac{\partial}{\partial X} + \eta b\frac{\partial}{\partial Y}. \tag{5.7}$$

$\dfrac{\partial}{\partial X}$ and $\dfrac{\partial}{\partial Y}$ are linearly independent over L, hence Equation 5.7 is satisfied if and only if

$$\frac{D^{p-1}(a)}{a} = \frac{D^{p-1}(b)}{b} \tag{5.8}$$

holds.

Lemma 54. *Let k be a field of characteristic $p > 0$ and K/k a purely inseparable field extension. Suppose $D \in Der_k K$ and denote $D^{[p-i]} = \frac{1}{(p-i)!} D^{p-1}$ for $0 < i \leq p$. Then for any $\alpha \in K$*

$$\left\{\sigma\left(D^{[p-1]}\right), \left\{\sigma\left(D^{[p-1]}\right), \alpha\right\}\right\} = \sigma\left(D^{[p-1]}(\alpha) D^{[p-1]}\right),$$

where the curly brackets denote the Poisson bracket defined at the end of Section 4.1.

Proof. Note that $\sigma\left[D^{[p-1]}, \alpha\right] = \sigma\left(D(\alpha) D^{[p-2]}\right)$. Then

$$\begin{aligned}\sigma\left(\left[D^{[p-1]}, D(\alpha) D^{[p-2]}\right]\right) &= \sigma\left(D^{[p-1]}\left(D(\alpha) D^{[p-2]}\right) - D(\alpha) D^{[p-2]} D^{[p-1]}\right)\\ &= \sigma\left(\sum_{i=1}^{p-1} D^{[i]}\left(D(\alpha)\right) D^{[p-1-i]} D^{[p-2]}\right)\end{aligned}$$

$D^p \in \mathrm{Gr}^1 \mathrm{Diff}_K L$, so $D^{p+i} \in \mathrm{Gr}^i \mathrm{Diff}_K L$ for any integer $0 \leq i < p$. Hence the symbol of the last term above is $D^{[p-2]} D(\alpha) D D^{[p-2]} = (p-1)^2 D^{[p-1]}(\alpha) D^{[p-1]} = D^{[p-1]}(\alpha) D^{[p-1]}$. □

We can now state the full result:

Theorem 55. *Let K be a field of characteristic $p > 0$ and suppose L/K is a purely inseparable extension of exponent 1 and degree p^2. Let $\{X, Y\}$ be a p-basis for L/K and $\left\{\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}\right\}$ the corresponding L-basis for $Der_K L$. Also, for $c_0, \ldots, c_{p-1} \in L$, let*

$$\gamma = c_0 \left(\frac{\partial}{\partial X}\right)^{p-1} + c_1 \left(\frac{\partial}{\partial X}\right)^{p-2} \left(\frac{\partial}{\partial Y}\right) + \cdots c_{p-1} \left(\frac{\partial}{\partial Y}\right)^{p-1}$$

be the corresponding nonzero element of $\Gamma^* \left(Der_K L\right)$. Then there exists a proper intermediate subfield $K \subset K' \subset L$ such that $\gamma \in \Gamma(L/K')$ if and only if one of the following two cases is satisfied:

1. $c_0 = c_1 = \cdots = c_{p-2} = 0$ *or* $c_1 = c_2 = \cdots = c_{p-1} = 0$
2. *All c_i are nonzero,* $\frac{c_0}{c_1} = \cdots = \frac{c_{p-2}}{c_{p-1}}$, *and* $\left\{c_0^{-1}\gamma, \left\{c_0^{-1}\gamma, \frac{c_i}{c_{i+1}}\right\}\right\} = 0$ *for any and all i.*

Proof. The first case of the theorem is obviously true from the discussion regarding Equation 5.6. For the second case, it was shown in the same equation that the quotients $\frac{c_i}{c_{i+1}}$ are equal if and only if γ is a multiple of $D^{p-1} \in \Gamma^* \left(\mathrm{Der}_K L\right)$ for some $D \in \mathrm{Der}_K L$. Call this quotient c. If γ is such a multiple, then $c_0^{-1}\gamma$ is the $(p-1)$st power of the derivation $D' = \frac{\partial}{\partial X} + c\frac{\partial}{\partial Y}$. It has also been established that the submodule of derivations generated by D' is closed under pth powers if and only if

$$\frac{D'^{p-1}(1)}{1} = \frac{D'^{p-1}(c)}{c}.$$

The left-hand side of this equation is 0, hence $D'^{p-1}(c) = 0$. By Equation 5.8, $D'^{p-1}(c) = 0$ is equivalent to the equation

$$\left\{\sigma(D'^{p-1}), \left\{\sigma(D'^{p-1}),\, c\right\}\right\} = 0,$$

which agrees with the statement made in the theorem. Finally, D' is a scalar multiple of D, and if D' is closed under pth powers then D must be as well by the Hochschild formula (16, Theorem 25.5). □

It is difficult to expand the result of Theorem 55 to purely inseparable extensions of exponent greater than 1. Additionally, suppose L/K is a purely inseparable extension of fields of characteristic $p > 0$ and exponent 1 with a p-basis consisting of more than 2 elements. The computations for determining whether a factor of a generator of $\Gamma(L/K)$ generates the fundamental form for an intermediate subfield become much more complicated than the conditions provided in Theorem 55. This is because if a restricted sub-Lie algebra of a purely inseparable extension L/K has dimension over L greater than 1, it is no longer necessary that the pth power of a derivation be a scalar multiple of that same derivation. This subtlety involving the pth powers of differential operators is a major stumbling block to finding nice criteria for when elements of the divided powers algebra of derivations generate fundamental forms for intermediate subfields.

CITED LITERATURE

1. Roger C. Alperin, *p-adic binomial coefficients mod p*, Amer. Math. Monthly **92** (1985), no. 8, 576–578. MR 812101 (86m:11001)

2. Lucile Bégueri, *Schéma d'automorphisms. Application à l'étude d'extensions finies radicielles*, Bull. Sci. Math. (2) **93** (1969), 89–111. MR 0257047 (41 #1701)

3. Pierre Berthelot and Arthur Ogus, *Notes on crystalline cohomology*, Princeton University Press, Princeton, N.J., 1978. MR 0491705 (58 #10908)

4. Stephen U. Chase, *On the automorphism scheme of a purely inseparable field extension*, Ring theory (Proc. Conf., Park City, Utah, 1971), Academic Press, New York, 1972, pp. 75–106. MR 0354629 (50 #7107)

5. ______, *Infinitesimal group scheme actions on finite field extensions*, Amer. J. Math. **98** (1976), no. 2, 441–480.

6. M. Fernández-Lebrón and L. Narváez-Macarro, *Hasse-Schmidt derivations and coefficient fields in positive characteristics*, J. Algebra **265** (2003), no. 1, 200–210. MR 1984906 (2004i:13031)

7. Murray Gerstenhaber, *On the Galois theory of inseparable extensions*, Bull. Amer. Math. Soc. **70** (1964), 561–566. MR 0162794 (29 #98)

8. ______, *On the deformation of rings and algebras. III*, Ann. of Math. (2) **88** (1968), 1–34. MR 0240167 (39 #1521)

9. ______, *The fundamental form of an inseparable extension*, Trans. Amer. Math. Soc. **227** (1977), 165–184. MR 0429861 (55 #2871)

10. Murray Gerstenhaber and Avigdor Zaromp, *On the Galois theory of purely inseparable field extensions*, Bull. Amer. Math. Soc. **76** (1970), 1011–1014.

11. A Grothendieck, *Elements de geometrie algebrique iv*, Publ. Math. IHES **20** (1964), no. 24, 1965.

12. H. Hasse and F.K. Schmidt, *Noch eine begrndung der theorie der hheren differentialquotienten in einem algebraischen funktionenkrper einer unbestimmten. (nach einer brieflichen mitteilung von f.k. schmidt in jena).*, Journal fr die reine und angewandte Mathematik **177** (1937), 215–223 (ger).

13. Nickolas Heerema and James Deveney, *Galois theory for fields K/k finitely generated*, Trans. Amer. Math. Soc. **189** (1974), 263–274. MR 0330124 (48 #8462)

14. Nathan Jacobson, *Lectures in abstract algebra. III*, Springer-Verlag, New York, 1975, Theory of fields and Galois theory, Second corrected printing, Graduate Texts in Mathematics, No. 32.

15. Hideyuki Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980. MR 575344 (82i:13003)

16. ______, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid. MR 1011461 (90i:13001)

17. Yoshikazu Nakai, *High order derivations. I*, Osaka J. Math. **7** (1970), 1–27. MR 0263804 (41 #8404)

18. Luis Narváez Macarro, *Hasse-Schmidt derivations, divided powers and differential smoothness*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 7, 2979–3014.

19. Richard Rasala, *Inseparable splitting theory*, Trans. Amer. Math. Soc. **162** (1971), 411–448.

20. Norbert Roby, *Les algèbres à puissances divisées*, Bull. Sci. Math. (2) **89** (1965), 75–91. MR 0193127 (33 #1348)

21. Shizuka Sato, *On modular extensions*, Proc. Amer. Math. Soc. **109** (1990), no. 3, 621–626. MR 1019282 (91b:13004)

22. Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

23. Igor R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid. MR 1328833 (95m:14001)

24. Moss Eisenberg Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410.

25. Charles A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994. MR 1269324 (95f:18001)

26. Avigdor Zaromp, *On abelian families of approximate automorphisms of purely inseparable field extensions*, ProQuest LLC, Ann Arbor, MI, 1969, Thesis (Ph.D.)–University of Pennsylvania. MR 2618811

VITA

MATT WECHTER

EDUCATION

2013 PhD in Mathematics (August 2013)

- **Thesis:** *Differential Operators on Finite Purely Inseparable Extensions*, University of Illinois at Chicago.
- **Advisor:** Henri Gillet

May 2009 MS in Mathematics from the University of Illinois at Chicago.

May 2005 BA in Mathematics and Physics from Amherst College.

HONORS and DISTINCTIONS

- **Awards and Scholarships**

  2005 Robert H. Breusch Prize in Mathematics at Amherst College

  2005 Cum Laude from Amherst College.

- **Seminars and Colloquia**
  - *Differential Operators on Modular Field Extensions.* University of Illinois at Chicago (February 2013)
  - *Galois Theories and Differential Algebra.* University of Illinois at Chicago (April 2012)

- *Toric Resolution of Singularities and Polytope Constructions.* University of Illinois at Chicago (February 2012)
- *Line Bundles on Toric Varieties.* University of Illinois at Chicago (December 2011)
- *Gromov-Witten Invariants.* University of Illinois at Chicago (March 2011)
- *Descent, Derivations, and the Jacobson-Bourbaki Theorem.* University of Illinois at Chicago (March 2011)
- *Quotients by Finite Group Schemes.* University of Illinois at Chicago (October 2010)
- *Local Structure of the Grassmannian.* University of Illinois at Chicago (August 2010)
- *Galois Descent and Purely Inseparable Fields.* University of Illinois at Chicago (April 2010)
- *Topological Classification of Vector Bundles.* University of Illinois at Chicago (February 2010)
- *Introduction to the Moduli of Curves.* University of Illinois at Chicago (September 2008)
- *The Mordell-Weil Theorem.* University of Illinois at Chicago (December 2007)
- Regular presenter in the Graduate Algebraic Geometry Seminar, Graduate Number Theory Seminar, and Graduate Student Colloquium at the University of Illinois at Chicago.

TEACHING AND MENTORING EXPERIENCE

- **Lecturer**, Multivariable Calculus, (Fall 2012)

- **Teaching Assistant**, Differential Equations (Summer 2012)
- **Workshop Coordinator**, Emerging Scholars Program, Intro to Mathematical Proofs (Spring 2012, Fall 2011)
  - Supervised and coordinated cooperative learning for first proof-based course for undergraduate mathematics majors.
- **Tutor** UIC College Prep, AP Calculus (Spring 2012)
  - Prepared high school seniors for AP Calculus exam for a credited course.
- **Tutor** UIC College Prep, Calculus II (Fall 2011)
  - Tutored advanced high school upperclassman in college calculus.

MATT WECHTER

- **Lecturer**, Summer Enrichment Workshop, College Algebra (Summer 2011)
  - Lectured incoming college freshmen in College Algebra.
  - Provided academic counseling to facilitate transition into college courseloads.
- **Workshop Coordinator**, Emerging Scholars Program, Multivariable Calculus (Spring 2011)
- **Tutor** UIC College Prep, Calculus I (Spring 2011)
- **Workshop Coordinator**, Emerging Scholars Program, Calculus I (Spring 2013, Fall 2010, Fall 2009)
  - Supervised and coordinated cooperative learning of first calculus course for undergraduates.
- **Teaching Assistant**, Calculus I (Fall 2010, Fall 2009)
  - Led regular discussions and administered quizzes and exams for Calculus I.
- **Mentor**, ASCEND Program, Calculus (Summer 2010).
  - Lectured incoming freshmen in college mathematics, including calculus.
  - Supervised student presentations on applications of mathematics
  - Oversaw students in learning Aleks and Mathematica computer packages
- **Workshop Coordinator**, Emerging Scholars Program, Calculus II (Spring 2010)
- **Teaching Assistant**, Calculus II (Spring 2010)
- **Mentor**, ASCEND Program, Calculus (Summer 2009)
- **Workshop Coordinator**, Emerging Scholars Program, Precalculus (Spring 2009, Fall 2008)

- **Teaching Assistant**, Precalculus (Spring 2009, Fall 2008)
- **Mentor**, ASCEND Program, Calculus (Summer 2008)
- **Teaching Assistant**, Business Calculus (Spring 2008)
- **Teaching Assistant**, College Algebra (Spring 2007)
- **Computer Lab Assistant**, Amherst College (2003-2005)
  - Assisted students with homework and computer issues in the Physics computer lab

CONFERENCES ATTENDED

- Differential Schemes and Differential Cohomology, BIRS (June 2012)
- Derived Algebraic Geometry, University of Michigan (May 2012)
- A Celebration of Algebraic Geometry, Harvard University (August 2011)
- Workshop on Differential Algebraic Geometry, CCNY (April 2010)
- Toric Varieties, MSRI (June 2009)
- Research Experience for Undergraduates, Mount Holyoke College (Summer 2004)

PRIOR EMPLOYMENT:

- **Business Analyst,** College Loan Corporation, Washington, DC (August 2005- August 2007)
  - Analyze and correct SQL-based data irregularities for inter- and intra-company reporting.
  - Create SPSS statistical response models for cost-effective mass mailings.