
Purely inseparable field extensions

Author: Meriton Ibraimi
Advisor: Prof. Richard Pink

Abstract

To develop a Galois theory for purely inseparable extensions we use higher derivations and the notion of modular fields. Let L be a finite purely inseparable modular field extension of K, and let M be an intermediate field such that L is also modular over M. If M_0 is the field of constants of all higher derivations on M over K, we prove that every higher derivation on M over K extends to L if and only if $L = M \otimes_{M_0} J$ for some field J.

1 Introduction

From Galois theory we know that the intermediate fields of a finite separable and normal field extension F of a field E are in bijection with the subgroups of the group of automorphisms of F over E. But there is no such correspondence for purely inseparable field extensions, because $\mathrm{Aut}(F/E)$ is trivial. In fact, there is still no theory giving a Galois correspondance for arbitrary purely inseparable field extensions.
Throughout this paper, we consider a finite purely inseparable field extension L of K, where K is a field of characteristic $p > 0$. We denote by $\mathbb{N}$ the set of all integers greater than or equal to 0. We say that L has *exponent* $e \in \mathbb{N}$ over K if for every element $a \in L$, a^{p^e} is in K and e is the smallest integer such that this property holds. A *derivation* D on L is an additive map of L into L such that $D(ab) = D(a)b + aD(b)$. The field of constants of a derivation D is the set of all $a \in L$ such that $D(a) = 0$. It can be shown that this subset of L is really a subfield. The field of constants of a set of derivations on L is the intersection of the fields of constants of each derivation. Since L^p is in the field of constants of any derivation, we see that L has at most exponent one over the field of constants of any set of derivations. It is known that $Der_K(L)$, the space of derivations on L trivial on K, has field of constants $K(L^p)$ and moreover that any intermediate field of $L/K(L^p)$ is the field of constants of a subspace. In the case where $Der_K(L)$ is finite dimensional over K, Jacobson [1] has determined when a subspace of $Der_K(L)$ is equal to the space of all derivations over its field of constants. When the exponent is greater then one it is not sufficient to consider only derivations. We have to use the notion of *higher derivations* (Def. 4.4), which is due to Hasse and Schmidt [2], if we want to develop a Galois Theory for higher exponents. Concepts like linear disjointness (Def. 3.6) and modularity (Def. 4.3) will be needed to state our first main result, Theorem 4.11, which is due to Sweedler [3]. It states that L is modular over K if and only if K is the field of constants of a set of higher derivations of L. It also states that L is modular over K if and only if it is the tensor product of simple extensions of K. So modular extensions are the inseparable equivalent to Galois extensions in the separable case.
In chapter two we recall the definition of inseparable fields and give a theorem showing us how purely inseparable polynomials look like. Chapter three gives a short introduction of tensor products of field extensions. The concept of *linear disjointness* will be formulated and later on frequently used. In section five we will consider $H_K^t(L)$, the set of all rank t higher derivations of L over K. We show that this set is a group with a certain composition. Chapter six is based on a paper of James K. Deveney [4]. Here we show that the only intermediate fields of L over K, which are invariant under all higher derivations in $H_K^t(L)$, are of the form $K(L^{p^r})$ for some $r \in \mathbb{N}$. We also prove that if M is the field of constants of a group of higher derivations of L over K and M_0 is the field of constants of all higher derivations of L over K, then every higher derivation of M over K extends to L if and only if $L = M \otimes_{M_0} J$ for some field J.
I want to thank Professor Richard Pink and his PhD student Mohammad Hadi Hedayatzadeh for their great support while writing this thesis. It has been a grat experience to work with them.

2 Inseparability

Let K be a field of characteristic $p > 0$.

Definition 2.1. *A polynomial $f(X) \in K[X]$ is called purely inseparable if it has exactly one root in an algebraic closure $\bar{K}$.*

Lemma 2.2. *For each purely inseparable polynomial $f(X) \in K[X]$ there exist $m \in \mathbb{N} \setminus \{0\}$ and $a_0 \in K^*$ such that $f(X) = a_0 \cdot (f_\alpha(X))^m$, where f_α is the minimal polynomial over K of the root $\alpha \in \bar{K}$.*

Proof. We proceed by induction on the degree of $f(X)$: Let $k = deg(f)$. For $k = 1$ the assertion is obvious. Let $deg(f) = k+1$ and assume that the assertion is true for all $n \leq k$. We know that $f_\alpha(X)$ divides $f(X)$ in $K[X]$, that is $f(X) = g(X) \cdot f_\alpha(X)$ with $deg(g) \leq k$. But since $f(X)$ is purely inseparable, $g(X)$ must also be purely inseparable and $g(\alpha) = 0$. So by the induction hypothesis, $g(X) = a_0 \cdot (f_\alpha(X))^{m_0}$ for some $m_0 \in \mathbb{N}$, $a_0 \in K^*$. Thus $f(X) = a_0 \cdot (f_\alpha(X))^{m_0+1}$. □

Lemma 2.3. *Let $h(X) \in K[X]$ be a monic, irreducible and purely inseparable polynomial. Then there exist $n \in \mathbb{N}$ and $c \in K$ such that $h(X) = X^{p^n} - c$.*

Proof. Let $r \in \mathbb{N}$ be maximal, such that $h(X) = g(X^{p^r})$ for some $g(X) \in K[X]$. We first show that $g(X)$ is separable by using the fact that $g(X)$ is not separable if and only if $g'(X) = 0$. So let

$$g(X) = \sum_{0 \leq i \leq m} c_i \cdot X^i$$

then

$$g'(X) = \sum_{1 \leq i \leq m} c_i \cdot i \cdot X^{i-1}.$$

We see that $g'(X) = 0$ if and only if $p \mid i$ or $c_i = 0$ for $i = 1, \ldots, m$. Now assume that $g(X)$ is not separable, that is $g'(X) = 0$. Then for the coefficients $c_i \neq 0$ we have $p \mid i$, and so $g(X)$ must be of the form $f(X^p)$ for some $f(X) \in K[X]$. This implies $h(X) = g(X^{p^r}) = f(X^{p^{r+1}})$ which is in contradiction with the maximality of r. So $g(X)$ must be separable. Consequently we have

$$g(X) = \prod_{1 \leq i \leq m} (X - a_i)$$

where $a_i \in \bar{K}$ and $a_i \neq a_j$ for $i \neq j$. Hence

$$h(X) = \prod_{1 \leq i \leq m} (X^{p^r} - a_i).$$

But since $h(X)$ is purely inseparable, m must be equal to 1 and it follows that $h(X) = X^{p^r} - a$. □

Polynomials of the form $X^{p^n}-c$ are purely inseparable, since $X^{p^n}-c = X^{p^n}-\alpha^{p^n} = (X-\alpha)^{p^n}$ for an $\alpha \in \bar{K}$. Using Lemma 2.2 and Lemma 2.3 we obtain the following Theorem:

Theorem 2.4. *A monic polynomial $f(X) \in K[X]$ is purely inseparable if and only if there exist $n \in \mathbb{N}, m \in \mathbb{N}$ and $c \in K$ such that $f(X) = (X^{p^n} - c)^m$.*

Definition 2.5. *Let L be an algebraic field extension of K. An element $\alpha \in K$ is called purely inseparable over K if its minimal polynomial over K is purely inseparable. We call the extension L purely inseparable over K if each $\alpha \in L$ is purely inseparable over K.*

By Theorem 2.4 this is the case if and only if the minimal polynomial is of the form $X^{p^n} - c$ for some $c \in K$.

Lemma 2.6. *L/K is purely inseparable if and only if for each $x \in L$ there exists $n \in \mathbb{N}$ sucht that $x^{p^n} \in K$.*

Proof. "$\Rightarrow$" : This follows immediately from the definition of purely inseparable and Lemma 2.3.
"$\Leftarrow$" : Assume that for each $x \in L$ there exists $n \in \mathbb{N}$ such that $x^{p^n} \in K$. Let $a \in L$ and $n \in \mathbb{N}$ such that $c := a^{p^n} \in K$. Then a is the root of the purely inseparable polynomial $X^{p^n} - c \in K[X]$. But then the minimal polynomial of a has also only one root in $\bar{K}$ and a is purely inseparable over K. □

Definition 2.7. *Let L/K be a purely inseparable field extension. If there exists $e \in \mathbb{N}$, such that $\alpha^{p^e} \in K$ for all $\alpha \in L$, then the smallest such e is called the exponent of L/K. The exponent (over K) of an element $x \in L$ is the smallest integer $e_x \in \mathbb{N}$ such that $x^{p^{e_x}} \in K$.*

Example 2.8. *$\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is a purely inseparable field extension, where t is transcendental over $\mathbb{F}_p$.*

Proof. Let $x \in \mathbb{F}_p(t)$, then

$$x = \frac{\sum\limits_{0 \le i \le p-1} a_i \cdot t^i}{\sum\limits_{0 \le j \le p-1} b_j \cdot t^j}$$

where $a_i, b_j \in \mathbb{F}_p$. Then

$$x^p = \frac{\sum\limits_{0 \le i \le p-1} a_i \cdot t^{p^i}}{\sum\limits_{0 \le j \le p-1} b_j \cdot t^{p^j}} \in \mathbb{F}_p(t^p).$$

So by Lemma 2.6, $\mathbb{F}_p(t)$ is purely inseparable over $\mathbb{F}_p(t^p)$. □

3 Tensor products of field extensions

In this section L, M and T are vector spaces over the field K.

Definition 3.1. *A map $\phi : L \times M \longrightarrow T$ is called* K-bilinear *if $\phi(x, \cdot) : M \to T$ is K-linear $\forall x \in L$ and $\phi(\cdot, y) : L \to T$ is K-linear $\forall\ y \in M$.*

Definition 3.2. *Let $\tau : L \times M \longrightarrow E$ be a K-bilinear map with the following universal property: For each K-bilinear map $\phi : L \times M \longrightarrow E$ into an arbitrary $K-$module E there exists a unique K-linear map $\phi^* : T \to E$ with $\phi = \phi^* \circ \tau$.*
Then the pair (T, τ) is called a tensor product of L and M over K. *We sometimes say that T is the tensor product of L and M (with abuse of language).We also write $L \otimes_K M$ for the tensor product T, when it exists, and $x \otimes y$ for the image of the pair (x, y).*

For the existence of the tensor product and further properties I refer for example to Bosch [5].

Remark 3.3. From the construction of the tensor product it follows that every $z \in L \otimes_K M$ can be written as a finite sum of tensors: $z = \sum_{1 \leq i \leq n} x_i \otimes y_i$.

Remark 3.4. Let M/K be a field extension and V a K-module. Then $V \otimes_K M$ is a M-module. If $\{v_i; i \in I\}$ is a basis of V (resp. linearly independent) over K then $\{v_i \otimes 1; i \in I\}$ is a basis of $V \otimes_K M$ (resp. linearly independent) over M.

Remark 3.5. Let L and M be field extensions of K. Then $L \otimes_K M$ is a K-Algebra with multiplication $x \otimes y \cdot x' \otimes y' = xx' \otimes yy'$.

Definition 3.6. *Now let $L/K, M/K$ be finite field extensions which are contained in a field C. We say that the field extension L/K is* linearly disjoint to *the extension M/K if each set $S \subseteq L$, linearly independent over K, is also linearly independent over M.*

Lemma 3.7. *Let L be a commutative K-Algebra, and $\dim_K(L) < \infty$. Then L is a field if and only if L is an integral domain.*

Proof. "$\Rightarrow$" : Obvious.
"$\Leftarrow$" : It suffices to show that every $x \in L$ has an inverse. For any $x \in L$ we define the map $\phi_x : L \to L$ by sending $L \ni y$ to $x \cdot y$. Obviously, ϕ_x is K-linear. Now if $x \neq 0$ it follows that ϕ_x is injective, since L has no zero divisors. But ϕ_x is also surjective, since L is a finite dimensional vector space over K. So there exists an $l \in L$ such that $x \cdot l = 1$. □

Prop. 3.8. *Let L/K, M/K be finite field extensions. Then $\dim_K(L \otimes_K M) = dim_K L \cdot dim_K M$. In particular, if L and M are finite dimensional over K then $L \otimes_K M$ is also finite over K.*

Proof. Let $\{l_i; i \in I\}$ and $\{m_j; j \in J\}$ be respectively bases of L and M over K. Then the set $\{l_i \otimes m_j; (i,j) \in I \times J\}$ is a basis of $L \otimes_K M$ over K. □

Lemma 3.9. *Let L/K, M/K be finite field extensions contained in a field C, and let $\phi : L \otimes_K M \to C$ be the M-linear map sending $x \otimes y$ to $x \cdot y$. The following statements are equivalent:*

i. L is linearly disjoint over K to M
ii. ϕ is injective
iii. $L \otimes_K M$ is an integral domain

Proof. *i. ⇒ ii.* : Let $\{l_i; i \in I\}$ be a basis of L over K. Then by Remark 3.4 $\{l_i \otimes 1; i \in I\}$ is a basis of $L \otimes_K M$ over M. Let $x \in ker\phi$ and write

$$x = \sum_{i \in I} l_i \otimes m_i \ .$$

Then

$$0 = \phi(x) = \sum_{j \in J} l_j \cdot m_j$$

and since we assumed that L is linearly disjoint over K to M, $m_j = 0$ for $j \in J$, that is $x = 0$.
ii. ⇒ i. : We use the fact that ϕ is injective if and only if linearly independent subsets are mapped to linearly independent subsets. So take any subset $S \subset L$, linearly independent over K. By Remark 3.4 the set $\{s \otimes 1; s \in S\}$ is linearly independent over M, so the set $\{\phi(s \otimes 1) = s; s \in S\} = S$ is linearly independent over M.
ii. ⇒ iii. : Assume ϕ is injective. Then we can consider $L \otimes_K M$ as a K-subalgebra of C, so there can't exist zero divisors in $L \otimes_K M$, since C is a field.
iii. ⇒ ii. : Assume $L \otimes_K M$ is an integral domain. By Remark 3.5, $L \otimes_K M$ is a K-Algebra. By Lemma 3.8 it follows that $\dim(L \otimes_K M) < \infty$, so we can apply Lemma 3.7, so $L \otimes_K M$ is a field. Since $ker\ \phi$ is an ideal in $L \otimes_K M$ and $L \otimes_K M$ is a field and $\phi \neq 0$, $ker\ \phi$ must be the zero ideal, so ϕ is injective. □

Theorem 3.10. *Let L and M be finite field extensions of K, both contained in a field C. Then L is linearly disjoint over K to M if and only if $L \otimes_K M$ is a field.*

Proof. " ⇒ " : If L is linearly disjoint to M we see by Lemma 3.9 that $L \otimes_K M$ is free of zero divisors. Using Lemma 3.8, we see that we can apply Lemma 3.7, thus $L \otimes_K M$ is a field.
" ⇐ " : If $L \otimes_K M$ is a field, then $L \otimes_K M$ is free of zero divisors and by Lemma 3.8 L is linearly disjoint over K to M. □

We see from by Theorem 3.10 that linear disjointness is a symmetric property:

Corollary 3.11. *L is linearly disjoint over K to M if and only if M is linearly disjoint over K to L.*

Using Theorem 3.10 we can extend Definition 3.6 to arbitrary field extensions, which may or may not lie in a common overfield.

Definition 3.12. *For arbitrary finite field extensions L/K and M/K we say that L and M are linearly disjoint if and only if the tensor product $L \otimes_K M$ is a field.*

Here is an example, where $L \otimes_K M$ is not a field:

Example 3.13. *Let $K \subseteq E \subseteq L$ be field extensions of K, with $E = K(\sqrt[p^n]{x})$ and $x \in K \setminus K^p$. Then there exists a K-algebra isomorphism $L \otimes_K E \cong L[T]/(T^{p^n})$.*

Proof. Since $E = K(\sqrt[p^n]{x}) \cong K[X]/(X^{p^n} - x)$, we have $L \otimes_K E \cong L[X]/(X^{p^n} - x)$. But $L[X]/(X^{p^n} - x) \cong L[T]/(T^{p^n})$ since $\sqrt[p^n]{x} \in L$ and the map sending X to $T + \sqrt[p^n]{x}$ is an isomorphism. □

4 Modular field extensions and p-independence

In this section, we assume that L is a finite and purely inseparable extension of the field K, of characteristic $p > 0$.

Definition 4.1. *Consider a purely inseparable extension L of K. We say that an element $x \in L$ is* relatively p-dependent over K on the subset S of L *if $x \in K(L^p)(S)$. Accordingly, we call a subset $S \subset L$* relatively p-independent *if $s \notin K(L^p)(S \setminus \{s\})$ for every $s \in S$. A* relatively p-independent (over K) subset $B \subset L$ such that $L = K(L^p)(B)$, is called a relative *p-basis* of L over K. *If L is of exponent one over K then we call B a* p-base *of L over K.*

One can check in the book of Jacobson [6] that there always exists a p-basis for a purely inseparable extension L over K.

Remark 4.2. Let $B = \{b_1, ..., b_n\}$ be a relative p-basis of L over K. Then $b_i^p \in K(L^p)$ but $b_i \notin K(L^p)(b_1, ..., b_{i-1})$ for $1 \leq i \leq n$. That is $[K(L^p)(b_1, ..., b_i) : K(L^p)(b_1, ..., b_{i-1})] = p$ and so $[K(L^p)(b_1, ..., b_n) : K(L^p)] = p^n$. We see that the set $\left\{b_1^{k_1} \cdot b_2^{k_2} \cdots b_n^{k_n}; 0 \leq k_i \leq p-1\right\}$ forms a basis of L over $K(L^p)$.

Definition 4.3. *L is said to be* modular over K *if and only if K and L^{p^i} are linearly disjoint over $K \cap L^{p^i}$ for $i = 1, 2, ...$.*

Definition 4.4. *A* rank t higher derivation *of a commutatve ring R with 1 is a sequence $d^{(t)} := \{d_0, d_1, ..., d_t\}$ of additive maps from R to R such that*

$$(1) \qquad d_m(a \cdot b) = \sum_{0 \leq i \leq m} d_i(a) \cdot d_{m-i}(b)$$

for all $a, b \in R$, $0 \leq m \leq t$, where $d_0 = I$ is the identity map. A higher derivation of infinite rank is an infinite sequence $d = \{d_0, d_1, d_2, ...\}$ of additive maps of R to R such that (1) holds for all $m \in \mathbb{N}$.
The ring of constants of $d^{(t)}$ is the set $\{a \in F; d_m(a) = 0 \text{ for all } 1 \leq m \leq t\}$ and the ring of constants of a set of higher derivations of R is the intersection of the ring of constants of each one.
For a subring $S \subseteq R$ we say that $d^{(t)}$ is a rank t higher derivation over S, *if for all $m \in \mathbb{N}$ and $a \in S$, $d_m(a) = 0$. We denote by $H_S^t(R)$ the set of all rank t higher derivations of R over S, where $0 \leq t \leq \infty$.*

Lemma 4.5. *Let I be a set of rank t higher derivations on R. Then the subset $S := \{a \in R; \forall d \in I, \forall m \in \mathbb{N} : d_m(a) = 0\}$ is a subring with 1, called* the ring of constants of I. *If R is a field then S is a subfield.*

Proof. One can easily check the first statement. For the second statement we have only to show that $x \in S$ implies $x^{-1} \in S$. Let $d \in I$. Since $1 \in S$ we have $0 = d_m(1) = d_m(x \cdot x^{-1}) = \sum_{0 \leq i \leq m} d_i(x) \cdot d_{m-i}(x^{-1}) = d_m(x^{-1})$, since $x \in S$ and so $d_i(x) = 0$ for $1 \leq i \leq m$. □

Lemma 4.6. *Let $E = K[X]$ be the polynomial algebra in one variable over the field K. Since $\{1, X, X^2, ...\}$ is a basis of E over K, we can define K-linear mappings D_i of $K[X]$ to $K[X]$ by setting $D_i(X^m) = \binom{m}{i} X^{m-i}$, where $m = 0, 1, 2, ...$ and $\binom{m}{i} = 0$ if $i > m$. Then $D = \{D_0, D_1, D_2, ...\}$ is a higher derivation on E of infinite rank. Furthermore, K is the field of constants of D.*

Proof. It is enough to check (1) for the product $X^n X^m$ for all $0 \leq n, m$. By definition we have $D_j(X^{m+n}) = \binom{m+n}{j} X^{m+n-j}$ and $D_i(X^m) \cdot D_{j-i}(X^n) = \binom{m}{i}\binom{n}{j-i} X^{m+n-j}$. Since

$$\sum_{0 \leq i \leq j} \binom{m}{i}\binom{n}{j-i} = \binom{m+n}{j},$$

we have

$$\sum_{0 \leq i \leq j} D_i(X^m) \cdot D_{j-i}(X^n) = D_j(X^{n+m}).$$

This shows that $D = \{D_0 = I, D_1, D_2, ...\}$ is a higher derivation of infinite rank. Since for every non constant $f(X) \in K[X]$ we have $deg D_1(f(X)) = deg(f(X)) - 1$ it is clear from the definition, that K is the field of constants. □

Corollary 4.7. *Let $D = \{D_0, D_1, D_2, ...\}$ be the higher derivation constructed in Lemma 4.6. If $f(X) \in K[X]$ is of the form $f(X) = X^{p^n} - a$ then $D_i(f(X)) = 0$ for every $1 \leq i \leq p^n - 1$.*

Proof. Since $\binom{p^n}{i} = 0$ for every $1 \leq i \leq p^n - 1$, we have $D_i(X^{p^n} - a) = D_i(X^{p^n}) = \binom{p^n}{i} X^{p^n - i} = 0$.

□

Lemma 4.8. *Let $L = K(x)$ and $n \in \mathbb{N}$ be the exponent of x over K. There exists a rank $p^n - 1$ higher derivation $D^{(p^n-1)}$ of L such that K is the field of constants of $D^{(p^n-1)}$.*

Proof. Let $X^{p^n} - a$ be the minimal polynomial of x over K. Let $D = \{D_0, D_1, D_2, ...\}$ be the higher derivation of the polynomial algebra $K[X]$, as defined in Lemma 4.6. Now since D is a higher derivation, every subset $\{D_0, D_1, D_2, ..., D_m\}$, $m \in \mathbb{N}$ is a higher derivation of rank m. Let $D^{(p^n-1)} = \left\{I, D_1, D_2, ..., D^{p^n-1}\right\}$ Then by Corollary 4.7 we have $D_j(X^{p^n} - a) = 0$ for every $1 \leq j \leq p^n - 1$. By property (1) in Definition 4.4 we have for every $f(x) \in K[X]$ and $0 \leq j \leq p^n - 1$:

$$D_j((X^{p^n} - a) \cdot f(X)) = \sum_{0 \leq i \leq j} D_i(X^{p^n} - a) \cdot D_{j-i}(f(X)) = (X^{p^n} - a) \cdot D_j(f(X)).$$

That is, the ideal I generated by the minimal polynomial $X^{p^n} - a$ of x is mapped into itself by every D_j. Consequently, every D_j induces an additive mapping $\widetilde{D}_j$ of $K[X]/I$ to $K[X]/I$. One can check easily that $\widetilde{D}_j$ satisfy (1) of Definition 4.4. Since $K[X]/I \cong K(x) = L$ we have now a higher derivation $D^{(p^n-1)}$ of L such that $D_i(x^m) = \binom{m}{i} x^{m-i}$ for every $0 \leq i, m \leq p^n - 1$. By definition, K is the field of constants. □

Lemma 4.9. *Assume that L/K has exponent n, and let $D^{(t)}$ be a higher derivation of rank t of L. Then:*
i. $D_m(L^{p^i}) \subseteq L^{p^i}$ for all $0 \leq m \leq t$ and $1 \leq i \leq n$
ii. If $x \in L$ is in the field of constants of $D^{(t)}$, then $D_m(x \cdot y) = x \cdot D_m(y)$ for every $y \in L, 0 \leq m \leq t$.

Proof. i. : Note that a rank t higher derivation induces a ring homomorphism $\phi : L \to L[X]/(X^{t+1})$ sending $y \mapsto \sum_{0 \leq m \leq t} D_m(y) \cdot \bar{X}^m$. Since the characteristic of L is $p > 0$ and ϕ is a ring homomorphism we have $\phi(y^p) = \phi(y)^p \in L^p[X^p]$ for every $y \in L$. Then we have

$$\sum_{1 \leq m \leq t} D_m(y^p) \cdot \bar{X}^m = \phi(y^p) = \phi(y)^p = (\sum_{1 \leq m \leq t} D_m(y) \cdot \bar{X}^m)^p$$

$$= \sum_{1 \leq m \leq t} D_m(y)^p \cdot \bar{X}^{mp} = \sum_{1 \leq m \leq [t/p]} D_m(y)^p \cdot \bar{X}^{mp}.$$

Because of this equality we have for $1 \leq m \leq t$, $D_m(y^p) = 0$ if $p \nmid m$ and $D_m(y^p) = D_{m/p}(y)^p$ if $p \mid m$. Hence for every $0 \leq m \leq t$ we have $D_m(L^{p^n}) \subseteq L^{p^n}$.
ii.) : We have $D_m(x \cdot y) = \sum_{0 \leq i \leq m} D_i(x) \cdot D_{m-i}(x) = x \cdot D_m(y)$, since $D_i(x) = 0$ for all $i > 0$. □

Lemma 4.10. *Let $e \in \mathbb{N}$ be the exponent of L over K and $S = \{s_1, ..., s_n\}$ be a p-basis of $K^{p^{-(e-i+1)}} \cap L$ over $K^{p^{-(e-i)}} \cap L$ for $1 \leq i \leq e$. Then S^p is p-independent in $K^{p^{-(e-i)}} \cap L$ over $K^{p^{-(e-i-1)}} \cap L$.*

Proof. Suppose that S^p is not p independent in $K^{p^{-(e-i)}} \cap L$ over $K^{p^{-(e-i-1)}} \cap L$. Then there exists $s \in S$ such that $s^p \in (K^{p^{-(e-i-1)}} \cap L)((K^{p^{-(e-i)}} \cap L)^p)(S^p \setminus \{s^p\}) = (K^{p^{-(e-i-1)}} \cap L)(S^p \setminus \{s^p\})$. Without loss of generality we can assume that $s = s_1$. So

$$s^p = \sum_{0 \leq k_2, ..., k_n \leq p-1} a_{k_2 \cdots k_n} \cdot (s_2^p)^{k_2} \cdots (s_n^p)^{k_n}$$

where $a_{k_2 \cdots k_n} \in K^{p^{-(e-i-1)}} \cap L$. We have $(a^{-p} + b^{-p})^p = (a + b)$ for all $a, b \in L$ and so we have $a^{-p} + b^{-p} = (a + b)^{-p}$. Using this property we have that

$$s = (s^p)^{-p} = \sum_{0 \leq k_2, ..., k_n \leq p-1} (a_{k_2 \cdots k_n})^{-p} \cdot (s_2)^{k_2} \cdots (s_n)^{k_n} \in (K^{p^{-(e-i)}} \cap L)(S \setminus \{s\})$$

which is a contradiction to the p-independence of S. □

Theorem 4.11. *Let L/K be a purely inseparable and finite field extension. The following are equivalent:*
i. L is a tensor product of simple extensions of K
ii. K is the field of constants of a set of higher derivations on L
iii. L is modular over K.

Proof. *i. ⇒ ii.* : Assume that L is a tensor product of simple extensions of K. Since L over K is a finite extension, L must be a finite tensor product of simple extensions $L_1, ..., L_r$ where $r \in \mathbb{N}$, $L_i = K(x_i)$. That is, L is of the form $L = K(x_1, ..., x_r)$, e_i denotes the exponent of x_i for $1 \leq i \leq r$. If we define $K_i = K(x_1, ..., x_{i-1}, x_{i+1}, ..., x_r)$, we have $L = K_i(x_i)$ and $K_1 \cap K_2 \cap ... \cap K_r = K$. So if we construct for each i a higher derivation of L with field of constants K_i as we did in Lemma 7, then we get a set of higher derivations of L with field of constants K.

ii. ⇒ iii. : Suppose that there exists $i \in \mathbb{N}$ such that L^{p^i} and K are not linearly disjoint over $L^{p^i} \cap K$. Then there exists a non-trivial relation $0 = l_1 \cdot a_1 + ... + l_s \cdot a_s$ of minimal length s, with $s \geq 1$, where $\{a_k \in K; 1 \leq k \leq s\}$ is linearly independent over $L^{p^i} \cap K$ and $l_k \in L^{p^i}$. Since the length of the relation is minimal, the set $\{l_k; 1 \leq k \leq s\}$ must be linearly independent over $L^{p^i} \cap K$, in particular $l_k \neq 0$ for $1 \leq k \leq s$. We have also $s > 1$ since if $s = 1$ then we would have a relation $0 = l_1 \cdot a_1$ with l_1 and $a_1 \neq 0$ which is impossible since L is a field. Dividing the relation by l_1, we can assume that $l_1 = 1$. So we have $0 = a_1 + l_2 \cdot a_2 + ... + l_s \cdot a_s$ and since $\{l_k \in K; 1 \leq k \leq s\}$ is linearly independent over $L^{p^i} \cap K$ we have that $l_2 \notin L^{p^i} \cap K$. In particular, l_2 is not in K, the field of constants of our set of higher derivations. So there exists $m > 0$ and $D_m \in D^{(t)}$ such that $D_m(l_2) \neq 0$. Applying D_m to the relation and using Lemma 4.9, *ii)* we obtain a non-trivial relation $0 = D_m(l_2) \cdot a_2 + ... + D_m(l_s) \cdot a_s$, where $D_m(l_k) \in L^{p^i}$, $k = 1, ..., t$ by Lemma 4.9, *i)*. But this relation is shorter than the one at the beginning and so we get a contradiction to the minimality of s.

iii. ⇒ i. : Let e be the exponent of L over K. Notice that we have the following tower of field extensions: $K \subseteq K^{p^{-1}} \cap L \subseteq K^{p^{-2}} \cap L \subseteq ... \subseteq K^{p^{-e}} \cap L = L$. Let S_1

be a p-basis for $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-1)}} \cap L$. From Lemma 4.10 we see that S_1^p is p-independent in $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$. Let S_2 be a completion of S_1^p to a p-basis of $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$ (that is, the disjoint union $S_1^p \amalg S_2$ is a p-basis for $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$). Continue in this manner, such that S_i is a completion to a p-Basis of $K^{p^{-(e-(i-1))}} \cap L$ over $K^{p^{-(e-i)}} \cap L$ of $S_1^{p^{(i-1)}} \cup S_2^{p^{(i-2)}} \cup ... \cup S_{i-1}^p$. The procedure terminates when we arrive at $S_1^{p^{(e-1)}} \cup S_2^{p^{(e-2)}} \cup ... \cup S_e$, which is a p-basis of $K^{p^{-1}} \cap L$ over $K \cap L = K$. Notice that by construction, the set $S_1^{p^{(i-1)}} \cup S_2^{p^{(i-2)}} \cup ... \cup S_{i-1}^p \cup S_i$ is a p-basis for $K^{p^{-(e-(i-1))}} \cap L$ over $K^{p^{-(e-i)}} \cap L$. Consider the p-basis S_1 of $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-1)}} \cap L$: by Remark 4.2 we have that the set

$$\left\{ \prod_{x_1 \in S_1} x_1^{k_{x_1}}; 0 \leq k_{x_1} < p \right\}$$

is a basis for $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-1)}} \cap L$. Since $S_1^p \cup S_2$ is a p-basis for $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$ we have, again by Remark 4.2, that the set

$$\left\{ \prod_{x_1 \in S_1} (x_1^p)^{k_{x_1}} \cdot \prod_{x_2 \in S_2} x_2^{k_{x_2}}; 0 \leq k_{x_1}, k_{x_2} < p \right\}$$

is a basis for $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$. Remembering that, if $\{a_1, ..., a_n\}$ is a basis for $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-1)}} \cap L$ and $\{b_1, ..., b_m\}$ is a basis for $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$ then the set $\{a_i \cdot b_j; 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-2)}} \cap L$ we get: since

$$\left\{ \prod_{x_1 \in S_1} x_1^{k_{x_1}}; 0 \leq k_{x_1} < p \right\}$$

is a basis for $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-1)}} \cap L$ and

$$\left\{ \prod_{x_1 \in S_1} (x_1^p)^{k_{x_1}} \cdot \prod_{x_2 \in S_2} x_2^{k_{x_2}}; 0 \leq k_{x_1} < p, 0 \leq k_{x_2} < p \right\}$$

is a basis for $K^{p^{-(e-1)}} \cap L$ over $K^{p^{-(e-2)}} \cap L$ we have that

$$\left\{ \prod_{x_1 \in S_1} x_1^{k_{x_1}} \cdot \prod_{x_2 \in S_2} x_2^{k_{x_2}}; 0 \leq k_{x_1} < p^2, 0 \leq k_{x_2} < p \right\}$$

is a basis for $L = K^{p^{-e}} \cap L$ over $K^{p^{-(e-2)}} \cap L$. Continueing in this manner we see that

$$\left\{ \prod_{x_1 \in S_1} x_1^{k_{x_1}} \cdot \prod_{x_2 \in S_2} x_2^{k_{x_2}} \cdots \prod_{x_e \in S_e} x_2^{k_{x_e}}; 0 \leq k_{x_1} < p^e, 0 \leq k_{x_2} < p^{e-1}, ..., 0 \leq k_{x_e} < p \right\}$$

is a basis for $L = K^{p^{-e}} \cap L$ over $K \cap L = K$. Note that since $x_i \in S_i \subset K^{p^{-(e-(i-1))}} \cap L$ and S_i is p-independent to S_{i-1}, we have that $e_{x_i} := p^{e-(i-1)}$ is the exponent of x_i

over K. Define $B := S_1 \cup ... \cup S_e$ and note that this is a disjoint union. We get a K-Algebra-homomorphism

$$\phi : \bigotimes_{x \in B} K(x) \to L$$

by sending

$$\bigotimes_{x \in B} x^{k_x} \mapsto \prod_{x \in B} x^{k_x}$$

where $0 \leq k_x < e_x$ and $e_x = p^{e-(i-1)}$ is the exponent of $x \in S_i$. Now since

$$\left\{ \bigotimes_{x \in B} x^{k_x}; 0 \leq k_x < e_x \right\}$$

is a basis for $\bigotimes_{x \in B} K(x)$ over K and, as we have seen,

$$\left\{ \prod_{x \in B} x^{k_x} \cdot; 0 \leq k_x < e_x \right\}$$

is a basis for $L = K^{p^{-e}} \cap L$ over K, we see that ϕ is a K-Algebra-isomprphism. So L is a tensor product of simple extensions of K. □

Example 4.12. Not every finite, purely inseparable extension is modular: Let $k = \mathbb{Z}/p\mathbb{Z}$ and $K = k(X^p, Y^p, Z^{p^2})$ where X, Y, Z are indeterminates. Now, set $L = K(Z, XZ + Y)$ and we see that L is a purely inseparable extension of K of exponent 2. We claim that L is not modular. By Theorem 4.11 it suffices to show that K is not the field of constants of any set of higher derivations of L. Assume that there exists a higher derivation $D^{(t)}$ of L with field of constants K. The element Z^p is not in K and so it is not in the field of constants. Thus for some $1 \leq m \leq t$ we have $D_m(Z^p) \neq 0$. But as mentioned in Lemma 4.9, i) we have that $D_m(Z^p)$ is zero if $p \nmid m$ and $D_{m/p}(Z)^p$ otherwise. So we are in the second case. Now notice that, $X^p \cdot D_{m/p}(Z)^p = X^p \cdot D_m(Z^p) = D_m(X^p \cdot Z^p) = D_m(X^p \cdot Z^p + Y^p) = D_{m/p}(X \cdot Z + Y)^p$ where we have used Lemma 4.9. This implies $X^p = (D_{m/p}(XZ+Y) \cdot D_{m/p}(Z)^{-1})^p$ and $X = (D_{m/p}(XZ + Y) \cdot D_{m/p}(Z)^{-1})$ which contradicts the fact that $X \notin L$. Thus Z^p is in the field of constants of all higher derivations of L over K and L is not modular over K.

Lemma 4.13. *Let L and E be fields such that $L/L \cap E$ is finite and $E/L \cap E$ is algebraic. There exists a unique field extension F/L such that:*
i. F and E are linearly disjoint over $F \cap E$.
ii. F is the smallest field extesnion of L satisfying property i).
iii. $F = L(S)$ for a finite subset S of E.

Proof. Let $B = \{x_i; i \in I\}$ be a finite basis of $L/L \cap E$, and let $C = \{x_j; j \in J\}$ be a maximal subset of B which is linearly independent over E in $L(E)$. Then C is a basis for $L(E)$ over E. Let $D = B \setminus C$. Then for each $x \in D$ we have

$$(*) \qquad x = \sum_{j \in J} a_{x,j} x_j$$

for uniquely determined $a_{x,j} \in E$. Set $S = \{a_{x,j}; x \in D, j \in J\}$ and $F = L(S)$. Note that S is a finite set since D and J are finite. Since C is a basis of $L(E)/E$ we can extend C to a basis $C' := C \cup \{y_k \in L(E); k \in K\}$ (where K is a finite index set) of $L(E)$ over $F \cap E$. Let $A \subseteq F$ be a subset, linearly independent over $F \cap E$. Assume we have a relation $e_1 \cdot a_1 + ... + e_n \cdot a_n = 0$, with $e_i \in E$ and $a_i \in A$. Since $e_i \in L(E)$ we have

$$e_i = \sum_{j \in J} w_{ij} x_j + \sum_{k \in K} w'_{ik} y_k$$

where w_{ij} and w'_{ik} are in $F \cap E$ for all $j \in J, k \in K$ and $1 \leq i \leq n$. Consequently, we have

$$\sum_{1 \leq i \leq n} (\sum_{j \in J} w_{ij} x_j + \sum_{k \in K} w'_{ik} y_k) \cdot a_i = \sum_{j \in J} (\sum_{1 \leq i \leq n} a_i w_{ij}) x_j + \sum_{k \in K} (\sum_{1 \leq i \leq n} a_i w'_{ik}) y_k = 0$$

and since $\{x_j; j \in J\} \cup \{y_k; k \in K\}$ is a basis of $L(E)/F \cap E$, we have that

$$\sum_{1 \leq i \leq n} a_i w_{ij} = 0$$

and

$$\sum_{1 \leq i \leq n} a_i w'_{ik} = 0$$

for all $j \in J$ and $k \in K$. Since A is linearly independent over $F \cap E$ we have that $w_{ij} = 0$ and $w'_{ik} = 0$ for all $j \in J, k \in K$ and $1 \leq i \leq n$. Thus $e_i = 0$ for $1 \leq i \leq n$ and we see that F and E are linearly disjoint over $F \cap E$.
Now suppose M is a field such that M and E are linearly disjoint over $M \cap E$ and $L \subseteq M$. Then $C = \{x_j; j \in J\} \in M$ and since C is linearly independent over E it is also linearly independent over $M \cap E$. For each $x \in D$ we have the identity $(*)$, for unique $\{a_{x,j}; j \in J, x \in D\}$. By the linear disjointness of M and E over $M \cap E$ these relations also hold over $M \cap E$. Hence $\{a_{x,j}; j \in J, x \in D\} \subseteq M \cap E \subseteq M$. Thus $M \supseteq L(S) = F$. □

Lemma 4.14. *Let $E \subseteq K$, and $E \subseteq F \subseteq L$ be four fields having the following poperties:*
(1) *L and F are finite over $F \cap K$,*
(2) *$L = F(K \cap L)$,*
(3) *F and K are linearly disjoint over $F \cap K$.*

Then L and K are linearly disjoint over $L \cap K$.

Proof. Let $\{x_1, ..., x_n\} \subseteq K$ be linearly independent over $L \cap K$. From (2) it follows that F and $K \cap L$ are linearly disjoint over $K \cap F$. By Theorem 3.10, $F \otimes_{F \cap K} (K \cap L)$ is a field and one can see that $F(K \cap L) \cong F \otimes_{F \cap K} (K \cap L)$. Let $\{f_i; i \in I\}$ be a basis of F over $K \cap F$. Since $F(K \cap L) \cong F \otimes_{F \cap K} (K \cap L)$ we see that $\{f_i; i \in I\}$ is a basis of $F(K \cap L)$ over $K \cap L$. Assume

$$\sum_{1 \leq k \leq n} a_k x_k = 0$$

for some $a_k \in L$. Then $a_k = \sum_{i \in I} c_{ki} f_i$ where $c_{ki} \in K \cap L$, hence

$$0 = \sum_{1 \leq k \leq n} \sum_{i \in I} c_{ki} f_i x_k = \sum_{i \in I} f_i (\sum_{1 \leq k \leq n} c_{ki} x_k)$$

Consequently, $\sum_{1 \leq k \leq n} c_{ki} x_k = 0$ and since $\{x_1, ..., x_n\} \subseteq K$ are linearly independent over $L \cap K$ we have that $c_{ki} = 0$ for all $1 \leq k \leq n$ and $i \in I$. Hence $a_k = 0$ for all k and $\{x_1, ..., x_n\}$ is linearly independent over L.

□

Theorem 4.15. *Let L/K be a finite and purely inseparable field extension of exponent e. There exists a unique field extension F of L having the following properties:*
i. F/K is the smallest modular field extenion of K.
ii. F/K is purely inseparable of exponent e.
iii. F/K is finite.

Proof. We construct, by descending induction, fields F_m, $m \leq e$, having the following properties:

(1) $F_m^{p^s}$ and K are linearly disjoint for $s = m, m+1, ...$,
(2) F_m is the unique minimal extension of L having property (1),
(3) F_m/K is purely inseparable,
(4) F_m/K has exponent e,
(5) $[F_m : K] < \infty$.

We start our descending induction at $m = e$ and set $F_e = L$. Since $F_e^{p^s} \subseteq K$ for $s = e, e+1, ...$ we see that property (1) is fulfilled. Obviously L is the minimal extension of itsself having property (1), and the properties (3) and (4) are satisfied by assumption. Since we assumed $[L : K] < \infty$ property (5) is also satisfied.
Suppose now that we have constructed $F_m \supseteq L$ for a $m \leq e$, such that F_m satisfies $(1) - (5)$.
We have to check if we can use Lemma 4.13 on the fields $F_m^{p^{m-1}}$ and K: since F_m/K is finite by (5), clearly $F_m^{p^{m-1}}/K^{p^{m-1}}$ is finite. Since $K^{p^{m-1}} \subseteq K \cap F_m^{p^{m-1}}$ we see that $F_m^{p^{m-1}}/K \cap F_m^{p^{m-1}}$ is finite. We have also that $K/K \cap F_m^{p^{m-1}}$ is algebraic, since every element $\alpha \in K$ is a root of a polynomial $X^{p^{m-1}} - \alpha^{p^{m-1}} \in (K \cap F_m^{p^{m-1}})(X)$. So we can use Lemma 4.13 .
By Lemma 4.13 there exists a unique minimal field $M \supseteq F_m^{p^{m-1}}$ such that M and K are linearly disjoint over their intersection. Let $F_{m-1} = M^{p^{-(m-1)}}$. We show now the conditions $(1) - (5)$ for F_{m-1}.
(1) : Since $F_{m-1}^{p^{m-1}} = M$, we see that $F_{m-1}^{p^{m-1}}$ and K are linearly disjoint over their intersection. So we have to show condition (1) only for $s \geq m$. By Lemma 4.13, $M = F_m^{p^{m-1}}(S)$ for a finite subset S of K. Thus for $s \geq m$, we have $F_{m-1}^{p^s} = M^{p^{s-m+1}} = F_m^{p^s}(S^{p^{s-m+1}})$. Clearly $S^{p^{s-m+1}} \subseteq F_{m-1}^{p^s}$, and since $S \subseteq K$ we have $S^{p^{s-m+1}} \subset F_{m-1}^{p^s} \cap K$,

that is $F_{m-1}^{p^s} = F_m^{p^s}(F_{m-1}^{p^s} \cap K)$. By induction hypothesis, $F_m^{p^s}$ and K are linearly disjoint over their intersection for $s \geq m$. Hence, using Lemma 4.14, we see that $F_{m-1}^{p^s}$ and K are linearly disjoint over their intersection for $s \geq m-1$. Thus F_{m-1} satisfies condition (1).
(3) and (4) : We have seen that $F_{m-1}^{p^s} = F_m^{p^s}(F_{m-1}^{p^s} \cap K)$ for $s \geq m$ and since $e \geq m$ (by assumtion), we have $F_{m-1}^{p^e} = F_m^{p^e}(F_{m-1}^{p^e} \cap K) \subseteq K(F_{m-1}^{p^e} \cap K) = K$. It follows by using Lemma 2.6, that F_{m-1} satisfies (3). As we have seen, the exponent of F_{m-1} is greater than or equal to e and since $F_m \subseteq F_{m-1}$ the exponent is equal to e, hence we have (4).
(5) : By induction hypothesis, $[F_m : K] < \infty$. Since S is a finite subset of K and $F_{m-1} = M^{p^{-(m-1)}} = (F_m^{p^{m-1}}(S))^{p^{-(m-1)}} = F_m(S^{p^{-(m-1)}})$ we see that F_{m-1} is a finite extension of K.
(2) : Suppose E is an extension of L satisfying condition (1). Then $F_m \subseteq E$, since by induction hypothesis, F_m is the minimal field extension satisfying condition (1). Hence $F_m^{p^{m-1}} \subseteq E^{p^{m-1}}$ and by assumption $E^{p^{m-1}}$ is linearly disjoint from K. By Lemma 4.13, $M \subseteq E^{p^{m-1}}$. Thus $F_{m-1} \subseteq E$.

The induction ends when the field F_1 is constructed, which is the desired field. □

5 The group of higher derivations

Thoroughout this section, L will be a finite purely inseparable modular extension of K.

Lemma 5.1. *Let $\phi : L[T]/(T^{t+1}) \longrightarrow L[T]/(T^{t+1})$ be a ring homomorphism, satisfying*
i. $\phi(T) = T$,
ii. $\phi \equiv id \ mod \ (T)$
Then ϕ is an automorphism of $L[T]/(T^{t+1})$.

Proof. Let ϕ be such an homomorphism. Then ϕ is injective: Let $f = \sum_{0 \leq i \leq t} f_i T^i$ be in $L[T]/(T^{t+1})$ such that $\phi(f) = 0$. Let

$$\phi(f_0) = f_0 + \sum_{1 \leq i \leq t} b_i T^i$$

for some $b_i \in L$. Then

$$\phi(f) = f_0 + \sum_{1 \leq i \leq t} (b_i + \phi(f_i))T^i = 0,$$

thus $f_0 = 0$ and since ϕ is a homomorphism, $b_i = 0$ for all $r \geq 1$. Let

$$\phi(f_1) = f_1 + \sum_{2 \leq i \leq t} b_i' T^i$$

for some $b_i' \in L$. Then

$$\phi(f) = \sum_{1 \leq i \leq t} \phi(f_i)T^i = f_1 T + \ terms\ of\ higher\ order = 0,$$

thus we have $f_1 = 0$. Continuing in this manner one can see that $f_i = 0$ for all $0 \leq i \leq t$, hence ϕ is injective.
We show by descending induction that ϕ is surjective. Let $f \in L[T]/(T^{t+1})$ such that the first s coefficients $f_0, ..., f_{s-1}$ of f are equal to zero for some $s \leq t$. Then there exist $g \in L[T]/(T^{t+1})$ such that $\phi(g) = f$:
$\underline{s = m :}$ set $g = f_m T^m$ and obtain

$$\phi(f_m T^m) = \phi(f_m)T^m = (f_m + \sum_{1 \leq i \leq t} c_i T^i)T^m = f_m T^m = f$$

where all equalities are modulo (T^{m+1}).
$\underline{s \to s-1 :}$ Assume that for every $f \in L[T]/(T^{t+1})$ with $f_0 = f_1 = ... = f_{s-1} = 0$ there exists a $g \in L[T]/(T^{t+1})$ such that $\phi(g) = f$. Let $h \in L[T]/(T^{t+1})$ be a polynomial with $h_0 = ... = h_{s-2} = 0$. Define $g_1 = h_{s-1}T^{s-1}$ and $\tilde{f} = h - \phi(g_1)$. Then $\tilde{f}$ has coefficients $\tilde{f}_0 = ... = \tilde{f}_{s-1} = 0$ and by the induction hypothesis there exists a $\tilde{g} \in L[T]/(T^{t+1})$ such that $\phi(\tilde{g}) = \tilde{f}$. Defining $g := g_1 + \tilde{g}$ we see $\phi(g) = \phi(g_1) + \phi(\tilde{g}) = \phi(g_1) + \tilde{f} = \phi(g_1) + h - \phi(g_1) = h$.
The induction is finished when $s = 0$ which states that for an arbitrary $f \in L[T]/(T^{t+1})$ there exists a $g \in L[T]/(T^{t+1})$ such that $\phi(g) = f$. □

Theorem 5.2. *The set $H^t(L)$ of all rank t higher derivations of L is a group with respect to the composition $d \circ e = f$ where $f_k(a) = \sum_{i+j=k} d_j(e_i(a))$.*

Proof. By Lemma 5.1, the set of all ring homomorphisms $\phi : L[T]/(T^{t+1}) \to L[T]/(T^{t+1})$ satisfying (1) and (2) of Lemma 5.1 is equal to the set of all automorphisms satisfying (1) and (2). Let G denote the set of all automorphisms $L[T]/(T^{t+1})$ satisfying (1) and (2). One can easily check that G is a group. We now show that $H^t(L)$ is in bijection with G, hence G induces a group structure on $H^t(L)$: Let $\psi : G \longrightarrow H^t(L)$ be the map sending $\alpha \in G$ to d^α where $d_i^\alpha(x) =$ i-th coefficient of $\alpha(x)$. First we have to check that d^α is a higher derivation of L over K for every $\alpha \in G$. Now since $\alpha \equiv id\ mod\ (T)$ we see that d_0^α is the identity on L. Now let $x, y \in L$, $1 \leq m \leq t$ and $\alpha \in G$. Let

$$\alpha(x) = \sum_{0 \leq i \leq t} x_i T^i,\ \alpha(y) = \sum_{0 \leq j \leq t} y_j T^j$$

and

$$\alpha(xy) = \sum_{0 \leq k \leq t} z_k T^k$$

for some $x_i, y_j, z_k \in L$. Since α is a homomorphism we obtain

$$\sum_{0 \leq k \leq t} z_k T^k = (\sum_{0 \leq i \leq t} x_i T^i) \cdot (\sum_{0 \leq j \leq t} y_j T^j) = \sum_{0 \leq k \leq t} (\sum_{i+j=k} x_i y_j) T^k.$$

From this equality we see that $d^\alpha_m(xy) = \sum_{i+j=m} d^\alpha_i(x)d^\alpha_j(y)T^i$, hence $d^\alpha \in H^t(L)$.
Now we show that ψ is surjective: Let $d \in H^t(L)$. Define a ring endomorphism α of $L[T]/(T^{t+1})$ by setting $\alpha(x) = \sum_{0\le i\le t} d_i(x)T^i$ and $\alpha(T) = T$. Then by Lemma 5.1, α is in G and we have $\psi(\alpha) = d^\alpha = d$. Thus ψ is surjective. Let $\alpha, \beta \in G$ such that $d^\alpha = d^\beta$. Since $\alpha(T) = T = \beta(T)$ it suffices to show that $\alpha(x) = \beta(x)$ for every $x \in L$. But $d^\alpha = d^\beta$ if and only if for every $x \in L$ and all $0 \le i \le t$ the i-th coefficient of $\alpha(x)$ is equal to the i-th coefficient of $\beta(x)$. Hence $\alpha(x) = \beta(x)$. Thus ψ is injective and so ψ is a bijection.
Now we examin the group structure which is induced by G on $H^t(L)$. Let $d, e \in H^t(L)$ and define a composition on $H^t(L)$ as follows: set $\alpha = \psi^{-1}(d) \in G$ and $\beta = \psi^{-1}(e) \in G$. Then $d \circ e := \psi(\alpha \circ \beta) = d^{\alpha\circ\beta}$. Note that for $x \in L$ we have

$$\alpha \circ \beta(x) = \alpha(\sum_{0\le i\le t} b_iT^i) = \sum_{0\le i\le t} \alpha(b_i)T^i$$

$$= \sum_{0\le i\le t} (\sum_{0\le j\le t} a_{ij}T^j)T^i = \sum_{0\le k\le t} (\sum_{i+j=k} a_{ij})T^k$$

for some $a_{ij}, b_j \in L$. Hence $(d \circ e)_k(x) = k$-th coefficient of $\alpha \circ \beta(x) = \sum_{i+j=k} a_{ij}$. Further we have $a_{ij} = (j$-th coefficient of $\alpha(b_i)) = d^\alpha_j(b_i)$ and $b_i = (i$-th coefficient of $\beta(x)) = d^\beta_i(x)$. Hence $(d \circ e)_k(x) = \sum_{i+j=k} d^\alpha_j d^\beta_i(x) = \sum_{i+j=k} d_j e_i(x)$. This is exactly the composition claimed in the theorem. □

Definition 5.3. *A higher derivation $d \in H^\infty_K(L)$ of L is called* iterative of index q, *or simply iterative, if $\binom{i}{j} d_{q\cdot i} = d_{q\cdot j} d_{q\cdot(i-j)}$ for all $j \le i$, and $d_m = 0$ if $q \nmid m$. A rank t higher derivation ($t < \infty$) is iterative if it is the first $t+1$ maps of an infinite iterative higher derivation.*

Remark 5.4. *Let $\alpha \in \mathrm{Aut}\,(L[T]/(T^{t+1}))$ be the corresponding automorphism of some $d \in H^t_K$, d being iterative of index q. Let β be the corresponding automorphism for $e = a \cdot d$, where $a \in L$. Using the definitions, one can check that the i-th coefficient of $\beta(x)$, for some $x \in L$, is equal to zero if $q \nmid i$ and equal to $a^k \cdot \alpha_{qk}$ if $i = q \cdot k$, where $k \in \mathbb{N}$ and α_{qk} is the qk-th coefficient of $\alpha(x)$.*

Lemma 5.5. *If $d \in H^\infty_K(L)$ is iterative of index q, and a is in L, we define $ad := e$ where $e_{q\cdot i} = a^i d_{q\cdot i}$, and $e_j = 0$ if $q \nmid j$. Then ad is in $H^\infty_K(L)$.*

Proof. Let $x, y \in L$. We have to show

$$(*) \quad e_m(xy) = \sum_{0\le j\le m} e_j(x)e_{m-j}(y)$$

for all $m \in \mathbb{N}_0$. If $q \nmid m$ then, by definition, $e_m(xy) = 0$ and the right hand side of $(*)$ is also equal to zero since q cant devide both, j and $m - j$ for $j \ge 0$ and $e_m(y) = 0$

since $q \nmid m$. So let $m = q \cdot i$ for some $i \in \mathbb{N}$. Then we have

$$e_m(xy) = a^i d_m(xy) = a^i \sum_{0 \le j \le m} d_j(x) d_{m-j}(y) = \sum_{0 \le j \le i} d_{qj}(x) d_{m-qj}(y)$$

$$= \sum_{0 \le j \le i} (a^j d_{qj}(x))(a^{i-j} d_{q(i-j)}(y)) = \sum_{0 \le j \le i} e_{qj}(x) e_{m-qj}(y)$$

$$= \sum_{0 \le j \le i} e_j(x) e_{m-j}(y) = e_m(xy).$$

□

Remark 5.6. *Let $d^{(t)} \in H^t(L)$ and α the corresponding automorphism. Then the field of constants is equal to the set $\{x; \alpha(x) = x\}$. As a consequence, the set $H^t_K(L)$ of all rank t higher derivations of L over K is a subgroup of $H^t(L)$, hence it is also a group.*

6 Invariant subfields and extensions of higher derivations

In this section the goal is to state the main theorem of this work. To do that, we have to formulate several lemmas. So for the next lemma, note that a derivation (in the usual sense) is a rank 1 higher derivation.

Lemma 6.1. *Let $\rho_1, ..., \rho_n$ be a set of commuting derivations of L having the following properties:*
i. The set $\left\{\rho_1^{k_1} \cdots \rho_n^{k_n}; 0 \le k_1, ..., k_n \le p-1\right\}$ is linearly independent over L,
ii. $\rho_l^p = 0$ for all $1 \le l \le n$.

Then $[L : K_0] = p^n$, where K_0 is the field of constants of $\rho_1, ..., \rho_n$.

Proof. "$[L : K_0] \ge p^n$" : Suppose to the contrary that $[L : K_0] = m < p^n$. We show that we are led to a contradiction. Let $\omega_1, ..., \omega_m$ be a basis of L over K_0. In the linear equations

$$\sum_{0 \le k_i \le p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(\omega_1) \cdot x_{k_1,...,k_n} = 0$$

$$\sum_{0 \le k_i \le p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(\omega_2) \cdot x_{k_1,...,k_n} = 0$$

$$\vdots$$

$$\sum_{0 \le k_i \le p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(\omega_m) \cdot x_{k_1,...,k_n} = 0$$

there are more unknowns ($= p^n$) than equations ($= m < p^n$) so that there exists a non-trivial solution which, we denote by $\{x_{k_1,...,k_n}; 1 \leq k_i \leq p-1\}$. For any $\alpha \in L$ we can find $a_1, ..., a_m \in K_0$ such that $\alpha = a_1\omega_1 + ... + a_m\omega_m$. We multiply the first equation by a_1, the second by a_2, and so on. Using that $a_i \in K_0$ we obtain

$$\sum_{0 \leq k_i \leq p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(a_1\omega_1) \cdot x_{k_1,...,k_n} = 0$$

$$\sum_{0 \leq k_i \leq p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(a_2\omega_2) \cdot x_{k_1,...,k_n} = 0$$

$$\vdots$$

$$\sum_{0 \leq k_i \leq p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(a_m\omega_m) \cdot x_{k_1,...,k_n} = 0$$

Adding these last equations and using the additivity of derivations we obtain

$$0 = \sum_{0 \leq k_i \leq p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(a_1\omega_1 + ... + a_m\omega_m) \cdot x_{k_1,...,k_n}$$

$$= \sum_{0 \leq k_i \leq p-1} \rho_1^{k_1} \cdots \rho_n^{k_n}(\alpha) \cdot x_{k_1,...,k_n}.$$

Since $\alpha \in L$ was arbitrary we get a contradiction to property (1) of our set of derivations.
"$[L : K_0] = p^n$" : Suppose that $[L : K_0] > p^n$. Then there exist $p^n + 1$ elements $\{\alpha_i; 1 \leq i \leq p^n + 1\}$ which are linearly independent over K_0. In the linear equations

$$\sum_{1 \leq i \leq p^n+1} x_i \cdot \rho_1^0 \cdots \rho_n^0(\alpha_i) = 0$$

$$\vdots$$

$$\sum_{1 \leq i \leq p^n+1} x_i \cdot \rho_1^{k_1} \cdots \rho_n^{k_n}(\alpha_i) = 0$$

$$\vdots$$

$$\sum_{1 \leq i \leq p^n+1} x_i \cdot \rho_1^{p-1} \cdots \rho_n^{p-1}(\alpha_i) = 0$$

(where $0 \leq k_i \leq p-1$) there are more unknowns ($= p^n + 1$) than equations ($= p^n$). So there exists a non-trivial solution. Note that the solution can not lie in K_0, otherwise the first equation would be a dependence relation of the α_i's. Among all these solutions we choose one which has the least number of elements different from 0. We may suppose this solution to be $\beta_1, ..., \beta_r, 0, ..., 0$ where the first r terms are different from 0. Moreover, $r \neq 1$ because $\beta_1\alpha_1 = 0$ implies $\beta_1 = 0$ so $\beta_1, 0, ..., 0$ would be a trivial solution. Also, we may suppose $\beta_r = 1$ since if we multiply the

given solution by β_r^{-1} we obtain a new solution in which the r-th term is 1. Thus we have

$$(*) \sum_{1\le i\le r-1} \beta_i \rho_1^{k_1}\cdots\rho_n^{k_n}(\alpha_i) + \rho_1^{k_1}\cdots\rho_n^{k_n}(\alpha_r) = 0$$

for all $0 \le k_1, ..., k_n \le p-1$. Since $\beta_1, ..., \beta_{r-1}$ cannot all belong to K_0, one of these, say β_1, is in L but not in K_0. So there is a derivation ρ_l such that $\rho_l(\beta_1) \neq 0$. Applying ρ_l to $(*)$ and using ther rule $\rho_l(ab) = \rho_l(a)b + a\rho_l(b)$ we obtain

$$(**) \sum_{1\le i\le r-1} \rho_l(\beta_i)\rho_1^{k_1}\cdots\rho_l^{k_l}\cdot\rho_n^{k_n}(\alpha_i) + \sum_{1\le i\le r-1} \beta_i \rho_1^{k_1}\cdots\rho_l^{k_l+1}\cdots\rho_n^{k_n}(\alpha_i) +$$

$$\rho_1^{k_1}\cdots\rho_l^{k_l+1}\cdots\rho_n^{k_n}(\alpha_i) = 0$$

for all $0 \le k_1, ..., k_l, ..., k_n \le p-1$. If we substract $(**)$ from $(*)$ we obtain

$$\sum_{1\le i\le r-1} \rho_l(\beta_i)\rho_1^{k_1}\cdots\rho_l^{k_l}\cdots\rho_n^{k_n}(\alpha_i) = 0$$

for all $0 \le k_i \le p-1,\ i \neq l$ and $0 \le k_l < p-1$. For $k_l = p-1$ and all $0 \le k_i \le p-1,\ i \neq l$ we obtain in $(**)$

$$\sum_{1\le i\le r-1} \rho_l(\beta_i)\rho_1^{k_1}\cdots\rho_l^{k_l}\cdots\rho_n^{k_n}(\alpha_i) = 0$$

since by property (2) of our derivations $\rho_l^p = 0$. But this is a non-trivial solution to the system having fewer than r elements different from 0, contrary to the choice of r. □

Definition 6.2. *A subset $M = \{m_1, ..., m_r\}$ of L is called a* subbase *of L over K if L is the tensor product (over K) of the simple extensions $K(m_1), ..., K(m_r)$.*

Since L is assumed to be modular over K, it is, by Theorem 4.11, a tensor product of simple extensions of K. So let

$$L = K(x_{1,1}) \otimes ... \otimes K(x_{1,j_1}) \otimes ... \otimes K(x_{n,1}) \otimes ... \otimes K(x_{n,j_n})$$

where $x_{i,e}$ is of exponent i over K.
Let

$$A_L := \left\{d^{i,e_i}; 1 \le i \le n, 1 \le e_i \le j_i\right\}$$

be the set of rank t higher derivations of L defined by

$$d^{i,e_i}_{[t/p^i]+1}(x_{r,s}) = \delta_{((i,e_i),(r,s))},$$

where $[t/p^i]$ is the greatest integer less than or equal to t/p^i. We set

$$d^{i,e_i}_{\alpha}(x_{r,s}) = 0, \quad 1 \le i, r \le n,\ 1 \le e_i \le j_i,\ 1 \le s \le j_r,\ \alpha \neq [t/p^i]+1.$$

One can see that A is a set of commuting derivations, hence

$$d^{i_1,e_{i_1}}_{\alpha} d^{i_2,e_2}_{\beta} = d^{i_2,e_2}_{\beta} d^{i_1,e_{i_1}}_{\alpha}$$

for all $0 \le \alpha, \beta \le t$ and $1 \le i_1, i_2 \le n,\ 1 \le e_{i_1} \le j_{i_1}, 1 \le e_{i_2} \le j_{i_2}$.

Definition 6.3. *The set*

$$\{x_{i,e_i}; 1 \leq i \leq n, 1 \leq e_i \leq j_i\}$$

is called a dual base for A_L.

Lemma 6.4. *Let* d *be a rank* t *higher derivation of* L *over* K. *Then the first non-zero map (of positive index) of* d *is a derivation of* L *over* K.

Proof. Let $d_r,\ r > 0$ be the first non-zero map of d. For $x, y \in L$ we have

$$d_r(xy) = \sum_{0 \leq s \leq r} d_s(x) d_{r-s}(y) = x d_r(y) + d_r(x) y$$

since $d_1 = d_2 = ... = d_{r-1} = 0$. □

Let $d^{i,e}_{z_{i,e}}$ denote the first non-zero map of $d^{i,e}$ of positive subscript $z_{i,e}$ and r be in $\mathbb{N}$. Consider the maps

$$d^{r+1,1}_{z_{r+1,1}p^r}, ..., d^{r+1,j_{r+1}}_{z_{r+1,j_{r+1}}p^r}, ..., d^{n,1}_{z_{n,1}p^r}, ..., d^{n,j_n}_{z_{n,j_n}p^r}.$$

By Lemma 4.9 we have that

$$d^{i,e_i}_{\alpha}(K(L^{p^r})) \subseteq K(L^{p^r})$$

for every $\alpha \geq 0$, thus $d^{i,e_i}|_{K(L^{p^r})}$ is a higher derivation of $K(L^{p^r})$. Since $d^{i,e_i}_{z_{i,e_i}}$ is the first non-zero map of d^{i,e_i} there exist $x \in L$ such that $d^{i,e_i}_{z_{i,e_i}}(x) \neq 0$. We have

$$d^{i,e_i}_{z_{i,e_i}p^r}(x^{p^r}) = (d^{i,e_i}_{z_{i,e_i}}(x))^{p^r}$$

where we have used Lemma 4.9. Thus $d^{i,e_i}_{z_{i,e_i}p^r}|_{K(L^{p^r})}$ is the first non-zero map of $d^{i,e_i}|_{K(L^{p^r})}$ where $r+1 \leq i \leq n,\ 1 \leq e \leq j_i$. By Lemma 6.4, we see that

$$\left\{ d^{i,e_i}_{z_{i,e_i}p^r}|_{K(L^{p^r})}; r+1 \leq i \leq n,\ 1 \leq e \leq j_i \right\}$$

is a set of derivations of $K(L^{p^r})$ over K.
Now we want to check if the set of derivations

$$\left\{ d^{i,e_i}_{z_{i,e_i}p^r}|_{K(L^{p^r})}; r+1 \leq i \leq n,\ 1 \leq e_i \leq j_i \right\}$$

fulfills the conditions *i.* and *ii.* of Lemma 6.1.

Remark 6.5. Every higher derivation $d^{i,e} \in A_L$ is iterative of index $z_{i,e}$.

Lemma 6.6. *Assume there exist* $\left\{ a_{k_{r+1,1},...,k_{n,j_n}} \in K(L^{p^r}); 0 \leq k_{i,j} \leq p-1 \right\}$ *such that*

$$\sum_{0 \leq k_{i,j} \leq p-1} a_{k_{r+1,1},...,k_{n,j_n}} \cdot (d^{r+1,1}_{z_{r+1,1}p^r}|_{K(L^{p^r})})^{k_{r+1,1}} \cdots (d^{n,j_n}_{z_{n,j_n}p^r}|_{K(L^{p^r})})^{k_{n,j_n}}(x) = 0$$

for all $x \in K(L^{p^r})$. *Then* $a_{k_{r+1,1},...,k_{n,j_n}} = 0$ *for all* $0 \leq k_{i,j} \leq p-1$.

Proof. For indices $0 \leq l_{r+1,1}, ..., l_{n,j_n} \leq p-1$ define

$$x_{l_{r+1,1},...,l_{n,j_n}} = (x_{r+1,1}^{p^r})^{l_{r+1,1}} \cdots (x_{n,j_n}^{p^r})^{l_{n,j_n}}.$$

Replacing x by $x_{l_{r+1,1},...,l_{n,j_n}}$ we obtain

$$0 = \sum_{0 \leq k_{i,j} \leq p-1} a_{k_{r+1,1},...,k_{n,j_n}} \cdot (d^{r+1,1}_{z_{r+1,1}p^r}|_{K(L^{p^r})})^{k_{r+1,1}} \cdots (d^{n,j_n}_{z_{n,j_n}p^r}|_{K(L^{p^r})})^{k_{n,j_n}} (x_{l_{r+1,1},...,l_{n,j_n}})$$

$$= a_{l_{r+1,1},...,l_{n,j_n}} \cdot (d^{r+1,1}_{z_{r+1,1}p^r}|_{K(L^{p^r})})^{l_{r+1,1}}((x_{r+1,1}^{p^r})^{l_{r+1,1}}) \cdots (d^{n,j_n}_{z_{n,j_n}p^r}|_{K(L^{p^r})})^{l_{n,j_n}}((x_{n,j_n}^{p^r})^{l_{n,j_n}})$$

$$= a_{l_{r+1,1},...,l_{n,j_n}} \cdot l_{r+1,1}! d^{r+1,1}_{z_{r+1,1}p^r}|_{K(L^{p^r})}((x_{r+1,1}^{p^r})) \cdots l_{n,j_n}! d_{z_{n,j_n}p^r}|_{K(L^{p^r})}((x_{n,j_n}^{p^r}))$$

$$= a_{l_{r+1,1},...,l_{n,j_n}} \cdot l_{r+1,1}! \cdots l_{n,j_n}!$$

Since $0 \leq l_{r+1,1}, ..., l_{n,j_n} \leq p-1$ we have $l_{r+1,1}! \cdots l_{n,j_n}! \neq 0$ and since $K(L^{p^r})$ is a field it follows that $a_{l_{r+1,1},...,l_{n,j_n}} = 0$. Thus varying the indices $l_{r+1,1}, ..., l_{n,j_n}$ if follows that $a_{k_{r+1,1},...,k_{n,j_n}} = 0$ for all $0 \leq k_{i,j} \leq p-1$. □

Lemma 6.7. *We have* $(d^{r+k,e}_{z_{r+k,e}p^r}|_{K(L^{p^r})})^p = 0$ *for all* $1 \leq k \leq n-r$ *and* $1 \leq e \leq j_{r+k}$.

Proof. Note that $K(L^{p^r}) = K(x_{r+1,1}^{p^r}, ..., x_{r+1,j_{r+1}}^{p^r}, ..., x_{n,j_n}^{p^r})$. hence it suffices to show that $(d^{r+k,e}_{z_{r+k,e}p^r}|_{K(L^{p^r})})^p(x_{r+l,s}^{p^r}) = 0$ for all $r+1 \leq k \leq n, 1 \leq e \leq j_{r+k}$ and $r+1 \leq l \leq n,\ 1 \leq s \leq j_{r+l}$. But this is clear since $(d^{r+k,e}_{z_{r+k,e}p^r}|_{K(L^{p^r})})(x_{r+l,s}^{p^r}) = \delta_{(r+k,e),(r+l,s)}$. □

Remark 6.8. By Lemma 6.4 and 6.6, and Lemma 6.7 we can apply Lemma 6.1, thus $[K(L^{p^r}) : K_0] = p^{j_{r+1}+...+j_n}$ where K_0 is the field of constants of $d^{r+1,1}_{z_{r+1,1}p^r}|_{K(L^{p^r})}, ..., d^{n,j_n}_{z_{r+1,1}p^r}|_{K(L^{p^r})}$.

Lemma 6.9. *The set*

$$B := \left\{ d^{r+1,1}_{z_{r+1,1}p^r}|_{K(L^{p^r})}, ..., d^{n,j_n}_{z_{n,j_n}p^r}|_{K(L^{p^r})} \right\}$$

of derivations of $K(L^{p^r})$ *has field of constants* $K(L^{p^{r+1}})$.

Proof. Let K_0 be the field of constants of B.
$\underline{K(L^{p^{r+1}}) \subseteq K_0}$: As in Lemma 6.4 it suffices to show $(d^{r+k,e}_{z_{r+k,e}p^{r+1}}|_{K(L^{p^{r+1}})})(x_{r+l,s}^{p^{r+1}}) = 0$ for all $r+2 \leq k \leq n, 1 \leq e \leq j_{r+k}$ and $r+2 \leq l \leq n,\ 1 \leq s \leq j_{r+l}$. So let $2 \leq k, l \leq n$. Then:

$$d^{r+k,e}_{z_{r+k,e}p^r}|_{K(L^{p^r})}(x_{r+l,s}^{p^{r+1}}) = d^{r+k,e}_{z_{r+k,e}}(x_{r+s,l}^{p})^{p^r} = (px_{r+k,e}^{p^r-1} d^{r+k,e}_{z_{r+k,e}}(x_{r+l,s}))^{p^r} = 0$$

where for the second equality we have used that $d^{r+k,e}_{z_{r+k,e}}$ is a derivation on L.
$\underline{K_0 = K(L^{p^{r+1}})}$: Note that $[K(L^{p^r}) : K(L^{p^{r+1}})] = [K(x_{r+1,1}^{p^r}, ..., x_{r+1,j_{r+1}}^{p^r}, ..., x_{n,j_n}^{p^r}) : K(x_{r+2,1}^{p^{r+1}}, ..., x_{r+2,j_{r+2}}^{p^{r+1}}, ..., x_{n,j_n}^{p^{r+1}})] = p^{j_{r+1}+...+j_n}$ since $x_{r+k,e}^{p^r}$ is of exponent one over $K(L^{p^{r+1}})$ for $1 \leq k \leq n,\ 1 \leq e \leq j_{r+k}$. By Remark 6.8, $[K(L^{p^r}) : K_0] = p^{j_{r+1}+...+j_n}$, thus using that $K(L^{p^{r+1}}) \subseteq K_0$ we obtain $K_0 = K(L^{p^{r+1}})$. □

Definition 6.10. *We say that a subfield $M \subseteq L$ is invariant under $H_K^t(L)$ if for every higher derivation $d \in H_K^t$ the corresponding automorphism $\alpha \in \mathrm{Aut}\,(L[T]/(T^{t+1}))$ satisfies $\alpha(M) \subseteq M$.*

Theorem 6.11. *Let L be a finite purely inseparable extension of K of exponent n. Let M be a subfield of L containing K. Then M is invariant under $H_K^t(L)$ if and only if $M = K(L^{p^r})$ for some nonnegative r.*

Proof. Assume $M = K(L^{p^r})$, and let $d = (d_i) \in H_K^t(L)$. If $x \in M$, then

$$x = \sum_{1 \le i \le s} a_i b_i^{p^r}, \quad d_j(x) = \sum_{1 \le i \le s} a_i d_j(b_i^{p^r})$$

for some $a_i, b_j \in L$. If $p^r \nmid j$, then (using Lemma 4.9) $d_j(x) = 0 \in M$. If $p^r \mid j$ then

$$d_j(x) = \sum_{1 \le i \le t} a_i (d_{j/p^r}(b_i))^{p^r} \in K(L^{p^r}) = M.$$

Since d_j was arbitrary, M is invariant under $H_K^t(L)$.
Conversely, assume M is invariant under $H_K^t(L)$. We can assume $M \subseteq K(L^{p^r})$ and $M \nsubseteq K(L^{p^{r+1}})$, otherwise $M = K(L^{p^n}) = K$ and we are finished. Let $x \in M \setminus K(L^{p^{r+1}})$, and let A be the set of higher derivations which we constructed before. By Lemma 6.7, there exists $d^{i,j} \in A$ such that $d^{i,j}_{z_{i,j}p^r}(x) \neq 0$. Recall that by Remark 6.5, $d^{i,j}$ is iterative of index $z_{i,j}$. Hence by Lemma 5.5, for any $a \in L$, $ad^{i,j}$ has $z_{i,j}p^r$ map $a^{p^r} d^{i,j}_{z_{i,j}p^r}$. Since M is invariant under $H_K^t(L)$, for any $a \in L$, $a^{p^r} d^{i,j}_{z_{i,j}p^r}(x) \in M$. Thus $L^{p^r} \subseteq M$ and thus $M = K(L^{p^r})$. □

For the next theorem we need the following lemmas:

Lemma 6.12. *Let L/M be purely inseparable of exponent e and B a subset of L. Then B is a minimal generating set of L/M if and only if $L = M(B)$ and B is a relative p-base of L over M.*

Proof. If B is a minimal generating set of L/M, then obviously $L = M(B)$ and thus $L = M(L^p, B)$. If B is not p-independent in L/M, then there exists $b \in B$ such that $b \in M(L^p, B \setminus \{b\})$. Thus b is both purely inseparable and separable algebraic over $M(B \setminus \{b\})$, hence $b \in M(B \setminus \{b\})$. This contradicts the fact that B is a minimal generating set over M. Conversely if $L = M(B)$ and B is a p-base of L/M then B is a minimal generating set of L over $M(L^p)$, hence a minmal generating set over M. □

Lemma 6.13. *Let L/M be a purely inseparable field extension of exponent e over M. Let $\{B_1, ..., B_e\}$ be a subbase of L over M. Then B_i is a subbase of L over $M' := M(B_1, ..., B_{i-1}, B_{i+1}, ..., B_e)$ for every $1 \le i \le e$.*

Proof. Since $\prod_{1 \le j \le e} p^{j|B_j|} = [L : M] = [L : M'][M' : M]$, $[L : M'] \le p^{i|B_i|}$ and $[M' : M] \le \prod_{1 \le j_1 \le i-1} p^{j_1|B_{j_1}|} \prod_{i+1 \le j_2 \le e} p^{j_1|B_{j_2}|}$ we see that $[L : M'] = p^{i|B_i|}$. The canonical homomorphism from $\bigotimes_{\substack{M' \\ b_i \in B_i}} M'(b_i)$ to $M'(B_i) = L$ is clearly surjective. Since

$dim_{M'}(\bigotimes_{\substack{M' \\ b_i \in B_i}} M'(b_i))) = p^{i|B_i|}$ and $[L : M'] = p^{i|B_i|}$ we see that $L = \bigotimes_{\substack{M' \\ b_i \in B_i}} M'(b_i)$. □

Lemma 6.14. *Let L/M' be a finite purely inseparable field extension of exponent e over M' such that $[L : M'] = p^{e \cdot r}$ and $B = \{b_1, ..., b_r\}$ a subbase of L over M'. Then for every relative p-base $A = \{a_1, ..., a_s\}$ of L over M' we have:*

(1) $s = r$,
(2) $L \cong M'(a_1) \otimes_{M'} ... \otimes_{M'} M'(a_r)$,

Proof. Notice that since B is a subbase of L over M' it is also a minimal generating set of L over M' and $M'(B) = L$. Hence, by Lemma 6.12, B is also a p-basis of L over M'. From the theory of p-bases we know that different p-bases of the same field extension must have the same cardinality, hence $s = r$. Since $[L : M'] = p^{e \cdot r}$ we have $[M'(b_i) : M'] = p^e$ for every $1 \leq i \leq r$. Using the p-basis exchange theorem we can exchange a_1 with b_1 such that $\{a_1, b_2, ..., b_r\}$ is a p-basis for L over M'. Since $[L : M'] = p^{e \cdot r}$ and $[M'(b_j) : M'] = p^e$ for every $2 \leq j \leq r$ we have that $[M'(a_1) : M'] = p^e$. Thus exchanging a_j with b_j for $2 \leq j \leq r$ we see that $[M'(a_j) : M'] = p^e$ for all $1 \leq j \leq r$. Clearly, the canonical homomorphism from $M'(a_1) \otimes_{M'} ... \otimes_{M'} M'(a_r)$ to $M'(A)$ is surjective, hence by considering the dimension over M' we can see that $M'(A) = M'(a_1) \otimes_{M'} ... \otimes_{M'} M'(a_r)$. Since $[L : M'] = p^{e \cdot r}$ we see that $L = M'(A)$, thus property (2) follows. □

Remark 6.15. *Note that by property (1) and (2) of Lemma 6.14 every $a \in A$ is of exponent e over M'.*

Theorem 6.16. *Let $K \subseteq M \subseteq L$ be fields and assume that L is modular over M of exponent e. The following conditions are equivalent:*
(1) *There exists an intermediate field $K \subseteq J \subseteq L$ such that $L = M \otimes_K J$ and J is modular over K.*
(2) *There exists a subbase $B = B_1 \cup ... \cup B_e$ of L over M such that $B_i^{p^i} \subseteq (L^{p^i} \cap K)((M(B_{i+1}, ..., B_e))^{p^i})$ for all $1 \leq i \leq e$.*

Proof. "(1) ⇒ (2)" : Since $L = M \otimes_K J$, every subbase of J over K is also a subbase of L over M. Since J over K is modular, J has a subbase $\{A_1, ..., A_e\}$ over K. Clearly, $\{A_1, ..., A_e\}$ satisfies (2).

"(2) ⇒ (1)" : Let $\{B_1, ..., B_e\}$ be a subbase of L over M as given in (2). For every $1 \leq i \leq e-1$ let $M_i = M(B_{i+1}, ..., B_e)$ and for $i = e$ we set $M_e = M$.

Claim 1 : $L^{p^i} = (L^{p^i} \cap K)(M_i^{p^i})$ for $i = 1, ..., e$.

Proof. We prove this by induction. For $i = 1$ we have by (2) that $B_1^p \subseteq (L^p \cap K)(M(B_2^p, ..., B_e^p))$. Since $L^p = (M(B_1, ..., B_e))^p = M^p(B_1^p, ..., B_e^p)$ we see by replacing B_1^p by $(L^p \cap K)(M(B_2^p, ..., B_e^p))^p$ that $L^p \subseteq (L^p \cap K)(M^p(B_2^p, ..., B_e^p))$. It

is clear that $L^p \supseteq (L^p \cap K)(M^p(B_2^p, ..., B_e^p))$, hence $L^p = (L^p \cap K)(M_1^p)$. Now assume that for some $i \geq 1$ we have the equality $L^{p^i} = (L^{p^i} \cap K)(M_i^{p^i})$. Then $L^{p^{i+1}} = (L^{p^{i+1}} \cap K^p)(M^{p^{i+1}}(B_{i+1}^{p^{i+1}}, ..., B_e^{p^{i+1}}))$. By (2) we have $B_{i+1}^{p^{i+1}} \subseteq (L^{p^{i+1}} \cap K)(M^{p^{i+1}}(B_{i+2}^{p^{i+1}}, ..., B_e^{p^{i+1}}))$. Since $B_{i+1}^{p^{i+1}} \subseteq (L^{p^{i+1}} \cap K)(M^{p^{i+1}}(B_{i+2}^{p^{i+1}}, ..., B_e^{p^{i+1}}))$ we see that $L^{p^{i+1}} \subseteq (L^{p^{i+1}} \cap K)(M^{p^{i+1}}(B_{i+2}^{p^{i+1}}, ..., B_e^{p^{i+1}})) = (L^{p^{i+1}} \cap K)(M_{i+1}^{p^{i+1}})$. It is again clear that $L^{p^{i+1}} \supseteq (L^{p^{i+1}} \cap K)(M_{i+1}^{p^{i+1}})$, hence $L^{p^{i+1}} = (L^{p^{i+1}} \cap K)(M_{i+1}^{p^{i+1}})$. □

Claim 2 : For every $1 \leq i \leq e$ there exist $A_0, ..., A_{i-1} \subseteq L$ such that :

(1) $L \cong K(A_1) \otimes ... \otimes K(A_{i-1}) \otimes M(B_i, ..., B_e)$,
(2) $\{A_1, ...A_{i-1}, B_i, ..., B_e\}$ is a subbase of L over M,
(3) $a_l \in A_l$ has exponent l over K for all $1 \leq l \leq i$.

Proof. For $i = 1$ we have by assumtion that $\{B_1, ..., B_e\}$ is a subbase of L over M, hence $L = M(B_1, ..., B_e)$. So suppose that $L \cong K(A_1) \otimes ... \otimes K(A_{i-1}) \otimes M(B_i, ..., B_e)$ and $\{A_1, ..., A_{i-1}, B_i, ..., B_e\}$ is a subbase of L over M satisfying $A_l^{p^l} \subseteq K$ for $1 \leq l \leq i-1$. Let $M' := M(A_1, ..., A_{i-1}, B_{i+1}, ..., B_e)$. By induction hypothesis $\{A_1, ...A_{i-1}, B_i, ..., B_e\}$ is a subbase of L over M. So using Lemma 6.13 we see that B_i is a subbasis of L over M'. Notice that by Claim 1 we have $L = M'(L \cap K^{p^{-i}})$. Hence there exists a subset $A_i \subseteq L \cap K^{p^{-i}}$ which is a p-basis of L over M'. Using Lemma 6.14 with $B = B_i$ and $A = A_i$, we see that A_i is a subbase of L over M'. By Corollary 6.15 every $a \in A_i$ has exponent i over M'. We obtain

$$(*) \quad K(A_1) \otimes_K ... \otimes_K K(A_{i-1}) \otimes_K M(B_{i+1}, ..., B_e) \otimes_K \bigotimes_{\substack{K \\ a \in A_i}} K(a)$$

$$= M' \otimes_K \bigotimes_{\substack{K \\ a \in A_i}} K(a)$$

since $K(A_1) \otimes_K ... \otimes_K K(A_{i-1}) \otimes_K M(B_{i+1}, ..., B_e)$ is a field. Note that by property (2) of Lemma 6.14 we have $\bigotimes_{\substack{M' \\ a \in A_i}} M'(a) = L$. Using Corollary 6.15 we see that $dim_{M'}(L) = p^{i \cdot |A_i|}$. Clearly, the canonical homomorphism from $M' \otimes_K \bigotimes_{\substack{K \\ a \in A_i}} K(a)$ to $\bigotimes_{\substack{M' \\ a \in A_i}} M'(a)$ is surjective. Since $A_i^{p^i} \subseteq K$ we have $[K(a) : K] \leq p^i$ for all $a \in A_i$ and hence $dim_{M'}(M' \otimes_K \bigotimes_{\substack{K \\ a \in A_i}} K(a)) \leq p^{i \cdot |A_i|}$. By the surjection mentioned before it follows that $dim_{M'}(M' \otimes_K \bigotimes_{\substack{K \\ a \in A_i}} K(a)) = p^{i \cdot |A_i|}$. This implies that $(*)$ is eqaual to L and that $[K(a) : K] = p^i$ for every $a \in A_i$. Thus property (3) of Claim 2 follows. Consider now the surjective canonical homomorphism from $\bigotimes_{\substack{K \\ a \in A_i}} K(a)$ to $K(A_i)$. Since $dim_K(\bigotimes_{\substack{K \\ a \in A_i}} K(a)) = p^{i|A_i|} = dim_K(K(A_i))$ we see that $K(A_i) = \bigotimes_{\substack{K \\ a \in A_i}} K(a)$. Hence, by replaceing $\bigotimes_{\substack{K \\ a \in A_i}} K(a)$ by $K(A_i)$ in $(*)$, we obtain property (1) of Claim 2. So it remains to show property (2) of Claim 2: Clearly, it suffices

to show that $\bigotimes_{\substack{M\\ a_i\in A_i}} M(a_i) = \bigotimes_{\substack{M\\ b_i\in B_i}} M(b_i)$. Now let $a \in A_i$ and $b \in B_i$. Notice that $[M'(a) : M] = [M'(a) : M'][M' : M] = [M'(b) : M'][M' : M]$ where we have used (2) of Lemma 6.14 in the second equality. So we obtain $[M'(b) : M(b)][M(b) : M] = [M'(b) : M] = [M'(a) : M] = [M'(a) : M(a)][M(a) : M]$ and using that $[M'(b) : M(b)] = [M' : M] = [M'(a) : M(a)]$ we see that $[M(b) : M] = [M(a) : M]$. Hence $\bigotimes_{\substack{M\\ a_i\in A_i}} M(a_i) = \bigotimes_{\substack{M\\ b_i\in B_i}} M(b_i)$. □

By Claim 2 we have $L \cong K(A_1)\otimes ...\otimes K(A_e)\otimes M$, and $\{A_1, ..., A_e\}$ is a subbase of L over M. By construction we have $K(A_i) = \bigotimes_{\substack{K\\ a_i\in A_i}} K(a_i)$ for all $1 \le i \le e$. Taking $J = K(A_1, ..., A_e)$ we see that

$$J = \bigotimes_{\substack{K\\ 1\le i\le e}} K(A_i) = \bigotimes_{\substack{K\\ 1\le i\le e}} \bigotimes_{\substack{K\\ a_i\in A_i}} K(a_i),$$

hence by Theorem 4.11 J is modular over K. □

Lemma 6.17. *Let M be a subfield of L containing K. Assume that M is modular over K and that every rank t higher derivation on M over K can be extended to L. Let $x \in L$ such that $x^{p^i} \in K(M^{p^i})$ for some $i \in \mathbb{N}_0$. Then $x^{p^i} \in (L^{p^i} \cap K)(M^{p^i})$.*

Proof. If $x^{p^i} \in K$, the result is obvious. Hence assume $x^{p^i} \in K(M^{p^r}) \setminus K(M^{p^{r+1}})$ for some $r \ge i$. Let $T := \{x_{i,e_i}; 1 \le i \le e, 1 \le e_i \le j_i\}$ be a subbase of M over K, and let T be a dual base of A_L. Since $\left\{x_{r+1,1}^{p^r}, ..., x_{n,j_n}^{p^r}\right\}$ is a subbase of $K(L^{p^r})$ over K we can write

$$(*) \quad x^{p^i} = \sum_{1\le s\le m} a_s (x_{r+1,1}^{p^r})^{t_{s,r+1,1}} \cdots (x_{n,j_n}^{p^r})^{t_{s,n,j_n}}$$

where $a_s \in K$, $0 \le t_{s,j,e_j} < p^{j-r}$. Since $x^{p^i} \in K(M^{p^r}) \setminus K(M^{p^{r+1}})$, at least one t_{s,j,e_j} is not divisible by p.
To show $x^{p^i} \in (L^{p^i} \cap K)(M^{p^i})$ it suffices to show that each $a_s \in L^{p^i}$, since we have assumed that $r \ge i$. The proof is by induction on m. If $m = 1$, then we see $a_1 \in L^{p^i}$, since we obtain in $(*)$ that $a_1 = x^{p^i}((x_{r+1,1}^{p^r})^{t_{1,r+1,1}} \cdots (x_{n,j_n}^{p^r})^{t_{1,n,j_n}})^{-1} \in L^{p^i}$. Assume the result for $m-1$. By induction it suffices to show $a_s \in L^{p^i}$ for some $1 \le s \le m$. Since every higher derivation on M over K can be extended to a higher derivation on L, and L^{p^i} is invariant under all higher derivations on M by Lemma 4.9, any map in any higher derivation on M over K must map x^{p^i} into L^{p^i}. We will show that some a_s is in L^{p^i} by induction on the total exponent of $(*)$, i.e. $\sum t_{s,\alpha,\beta}$. If the total exponent is 1, then $m = 1$ and the result follows. Since $x^{p^i} \in K(M^{p^r}) \setminus K(M^{p^{r+1}})$, by Lemma 6.9, some $d^{l,e_l}_{z_{l,e_l}p^r}(x^{p^i}) \ne 0$. Applying $d^{l,e_l}_{z_{l,e_l}p^r}$ to $(*)$ yields a nonzero element of L^{p^i} of lower total exponent with nonzero coefficients of the form wa_s, $w \in \mathbb{Z}/p\mathbb{Z}$. If $d^{l,e_l}_{z_{l,e_l}p^r}(x^{p^i}) \notin K$, then by induction some wa_s, hence some a_s, is in L^{p^i} and the result follows. If $d^{l,e_l}_{z_{l,e_l}p^r}(x^{p^i}) \in K$, then since

$$(x_{r+1,1})^{t_{s,r+1,1}} \cdots (x_{n,j_n})^{t_{s,n,j_n}}, \quad 0 \le t_{s,j,e_j} < p^{j-r}$$

is a vector space basis for $K(M^{p^r})$ over K, we have $d^{l,e_l}_{z_{l,e_l}p^r}(x^{p^i}) = a_s$ for some s. Thus once again some a_s is in L^{p^i} and the result follows. □

Lemma 6.18. *Let M be a modular extension of K and A a standard set of generators for $H^t_K(M)$ with dual base $\{x_{i,e_i}; 1 \leq i \leq n,\ 1 \leq e_i \leq j_i\}$. The set of maps*

$$S = \left\{ d^{i,e_i}_{z_{i,e_i}p^{c_i}}; 1 \leq i \leq n, 1 \leq e_i \leq j_i, 0 \leq c_i < min(i,r) \right\}$$

has field of constants $K(M^{p^r})$.

Proof. We do this by induction on r. Let
$S_l := \left\{ d^{i,e_i}_{z_{i,e_i}p^{c_i}}; 1 \leq i \leq n, 1 \leq e_i \leq j_i, 0 \leq c_i < min(i,l) \right\}$. If $r = 1$, then
$S_1 = \left\{ d^{1,1}_{z_{1,1}p^0}, ..., d^{1,j_1}_{z_{1,j_1}p^0} \right\}$ and by Lemma 6.9, S_1 has field of constants $K(M^p)$. Assume the result for a $r \geq 1$. Let D be the set of maps in S_{r+1} which are not in S_r. That is $D = \left\{ d^{i,e_i}_{z_{i,e_i}p^i}; r \leq i \leq n, 1 \leq e_i \leq j_i \right\}$. If we restrict the maps in D to $K(M^{p^r})$ then we see, by Lemma 6.9, that the restricted maps have field of constant $K(M^{p^{r+1}})$. Hence $K(M^{p^{r+1}})$ is contained in the field of constants of D, which we denote by T_0. Let F_{r+1} denote the field of constant of S_{r+1}. Note that since $S_{r+1} = S_r \cup D$, the field of constants of S_{r+1} is the intersection of the fields of constants of S_r and D. By induction hypothesis

$$S_r := S = \left\{ d^{i,e_i}_{z_{i,e_i}p^{c_i}}; r \leq i \leq n, 1 \leq e_i \leq j_i, 0 \leq c_i < min(i,r) \right\}$$

has field of constants $K(M^{p^r})$.Hence $F_{r+1} = K(M^{p^r}) \cap T_0$ and since$K(M^{p^{r+1}}) \subseteq K(M^{p^r})$ we see $F_{r+1} \supseteq K(M^{p^{r+1}})$. Assume now that there exists $x \in F_{r+1} \setminus K(M^{p^{r+1}})$. Then $x \in K(M^{p^r})$ and by Lemma 6.9, there exists $d^{i,j}_{z_{i,j}p^r} \in D$ such that $(d^{i,j}_{z_{i,j}p^r}) \mid_{K(M^{p^r})} (x) \neq 0$. Hence $x \notin F_{r+1}$ which is a contradiction. That is $F_{r+1} = K(M^{p^{r+1}})$.

□

Theorem 6.19. *Let M be an intermediate subfield of L and K, such that L is modular over M and M is modular over K. Then every rank t higher derivation on M over K extends to L if and only if there exists a field J such that $K \subseteq J \subseteq L$, J is modular over K and $L = M \otimes_K J$.*

Proof. If $L = M \otimes_K J$ then every rank t higher derivation on M over K can be extended by acting trivially on J.
Assume now that every rank t higher derivation on M over K can be extended to L. Let $B = B_1 \cup ... \cup B_n$ be a subbase of L over M where $b \in B_i$ is of exponent i over M. We claim $B_r^{p^r} \subseteq K(M^{p^r})$ for each $1 \leq r \leq n$. Let A be a standard set of generators for $H^t_K(M)$ with dual base $\{x_{i,e_i}; 1 \leq i \leq n,\ 1 \leq e_i \leq j_i\}$. By Lemma 6.18, $K(M^{p^r})$ is the field of constants of the set of maps

$$S = \left\{ (d^{i,e_i}_{z_{i,e_i}p^{c_i}}); 1 \leq i \leq n, 1 \leq e_i \leq j_i, 0 \leq c_i < min(i,r) \right\}.$$

Thus it suffices to show each $x^{p^r} \in B_r^{p^r}$ is annihilated by all maps in S. If $p \nmid z_{i,e_i}$, since d^{i,e_i} can be extended to L, we have

$$d^{i,e_i}_{z_{i,e_i}p^{r-1}}(x^{p^r}) = (d^{i,e_i}_{z_{i,e_i}}(x^p))^{p^{r-1}} = 0$$

for all $0 \leq c_i < \min(i,r)$, where we have used Lemma 4.9 for both equalities. If $p \mid z_{i,e_i}$ then consider the higher derivation $e \in H^t_K(M)$ with $e_{(z_{i,e_i}+1)\cdot l} = d_{z_{i,e_i}\cdot l}$ for $(z_{i,e_i}+1)l \leq t$ and $e_j = 0$ if $(z_{i,e_i}+1) \nmid j$, $j \leq t$. We claim $(z_{i,e_i}+1)p^{c_i} \leq t$ if $0 \leq c_i < \min(i,r)$ (unless $t = 1$, in which case the result is obvious). For if not, then $(z_{i,e_i}+1)p^{i-1} > t$, hence $z_{i,e_i} + 1 > t/p^{i-1}$ and $z_{i,e_i} + 1 > t/p^i$ which is a contradiction to the definition of $z_{i,e}$. Since $p \nmid (z_{i,e_i}+1)$ we see $e_{(z_{i,e_i}+1)p^{r-1}}(x^{p^r}) = (e_{(z_{i,e_i}+1)}(x^p))^{p^{r-1}} = 0$ where we have used again Lemma 4.9. Thus we have $0 = e_{(z_{i,e_i}+1)p^{r-1}}(x^{p^r}) = d^{i,e_i}_{z_{i,e_i}p^{r-1}}(x^{p^r})$ by definition of e. Hence $x^{p^r} \in K(M^{p^r})$ and consequently $B_r^{p^r} \subseteq K(M^{p^r})$ for all $1 \leq r \leq n$. By Lemma 6.17,

$$B_r^{p^r} \subseteq (L^{p^r} \cap K)(M^{p^r}) \subseteq (L^{p^r} \cap K)((M(B_{r+1}, ..., B_n))^{p^r}).$$

The result follows immediately from Theorem 6.16. □

Corollary 6.20. *Let M be an intermediate subfield of L and K such that L is modular over M. Let M_0 be the field of constantsof all rank t higher derivations on M over K. Then every rank t higher derivation on M over K extends to L if and only if there exists a field J such that $M_0 \subseteq J \subseteq L$, J is modular over M_0 and $L = M \otimes_{M_0} J$.*

Proof. Note that every rank t higher derivation on M over K is also a rank t higher derivation on M over M_0. By Theorem 4.11, M is modular over M_0 and since $K \subseteq M_0 \subseteq L$, L is also finite dimensional over M_0. Hence we can apply Theorem 6.19 to the chain of fields $M_0 \subseteq M \subseteq L$ and we obtain the result. □

7 References

[1] N. Jacobson, *Galois Theory of purely inseparable fields of exponent one*, Amer. J. Math. 66 (1944), 645 – 648.

[2] H. Hasse and R. Schmidt, *Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten*, J. Reine Angew. Math 17 (1937), 215 – 237.

[3] M. E. Sweedler, *Structure of inseparable extensions*, Ann. Math. (2) 87 (1968), 401 – 410.

[4] J. K. Deveney, *An intermediate theory for a purely inseparable galois theory*, AMS 198 (1973), 287 – 295

[5] Bosch, *Algebra*, 298 – 309

[6] Jacobson, *Abstract Algebra*, Vol.3, Chap. 4.7