TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 162, December 1971

INSEPARABLE SPLITTING THEORY

BY
RICHARD RASALA

Abstract. If L is a purely inseparable field extension of K, we show that, for large enough extensions E of K, the E algebra $L \otimes_K E$ splits to become a truncated polynomial algebra. In fact, there is a unique smallest extension E of K which splits L/K and we call this the splitting field $S(L/K)$ of L/K. Now $L \subseteq S(L/K)$ and the extension $S(L/K)$ of K is also purely inseparable. This allows us to repeat the splitting field construction and obtain inductively a tower of fields. We show that the tower stabilizes in a finite number of steps and we study questions such as how soon must the tower stabilize. We also characterize in many ways the case when L is its own splitting field. Finally, we classify all K algebras A which split in a similar way to purely inseparable field extensions.

Introduction. In Chapter 1, we introduce a splitting theory for purely inseparable field extensions. The idea is that if L/K is purely inseparable then for suitable base extensions E of K the algebra $L \otimes_K E$ over E has a very simple form, namely, it is a special case of what we call a simply truncated polynomial algebra. This fits into a pattern long familiar in the theory of separable extensions or the theory of central simple algebras, namely, that after suitable base extensions the initial object reduces to a standard form.

The splitting theory starts from the structure equations of a purely inseparable extension first discovered by Pickert [3]. Let L/K be purely inseparable and let $x_1, \dots, x_r$ be what we call a normal generating sequence for L/K. Set

$$K_i = K[x_1, \dots, x_i] \quad \text{and} \quad q_i = [K_i : K_{i-1}].$$

Then the structure theorem says that

$$x_i^{q_i} \in K[x_1^{q_i}, \dots, x_{i-1}^{q_i}].$$

From this we obtain structure equations of the form

$$x_i^{q_i} = \sum_{\alpha \in I_i} a_{i,\alpha} x^{q_i \alpha}.$$

Here I_i is a suitable multi-index set and $a_{i,\alpha} \in K$. The splitting procedure now works as follows. In some algebraic closure of K, let $d_{i,\alpha}$ be the q_ith root of $a_{i,\alpha}$. Set

$$S(L/K) = K[d_{i,\alpha}], \qquad 1 \leqq i \leqq r \text{ and } \alpha \in I_i.$$

Received by the editors October 21, 1971.

AMS 1970 *subject classifications*. Primary 12F15, 12F05, 13E10, 14B10, 14L20; Secondary 13B10, 14A05, 14B05, 14M10.

Key words and phrases. Field, inseparable field extension, splitting, descent theory, truncated polynomial algebra, finite-dimensional algebra, artin ring, derivation, group scheme, automorphism scheme.

Now let E be a field containing $S(L/K)$ and set $F=L \otimes_K E$. Define elements u_i of F by

$$u_i = x_i - \sum_{\alpha \in I_i} d_{i,\alpha} x^{\alpha}.$$

Then $F=E[u_1, \ldots, u_r]$ and the structure equations for the u_i are simply $u_i^{q_i}=0$. This exhibits the standard form of L/K after base extension.

The field $S(L/K)$ is the unique minimal field extension of K for which splitting occurs so we call $S(L/K)$ the splitting field of L/K. By construction, $S(L/K)$ is purely inseparable over K so we can construct its splitting field. Inductively, we obtain a tower of fields

$$S_n(L/K) = S(S_{n-1}(L/K)/K).$$

The latter part of Chapter 1 is devoted to a study of this tower. One fact we obtain is that the tower stabilizes after a finite number of steps. The field at which the tower stabilizes is the unique minimal field extension of L which is elementary over K. This proves in a simple way a result first shown by Sweedler [5].

In Chapter 2, we generalize the splitting theory to algebras. The basic result is that if a K algebra A splits into a simply truncated polynomial algebra whose exponents of truncation are p powers then A must have generators and structure equations as in the case of inseparable field extensions. We also characterize algebras which split into direct sums of truncated algebras. In particular, we are able to make a unified splitting theory for fields.

In the latter part of Chapter 2, we make some remarks which relate the splitting theory we have developed to other theories, notably, to group schemes.

This paper consists of a revised version of my Harvard Ph.D. thesis of June 1969 together with some additional results which I obtained in the past year. I wish to heartily thank my advisor, Barry Mazur, for many helpful suggestions and much encouragement. I wish to thank William Waterhouse for his interest in this work and for his suggestion that I try to extend the splitting theory of fields to algebras. I also wish to thank the referee for his careful reading of the paper and, in particular, for his discovery of an error I had made in defining the splitting field for an arbitrary splittable algebra. Finally, I wish to thank the NSF for support during my graduate work.

Chapter 1. Splitting Theory for Fields

1. **Notations and basic facts.**

Throughout we assume all fields to be of characteristic $p>0$. In this section, we discuss simple aspects of such fields and algebras over them.

We let K be a field and L be a finite purely inseparable extension of K.

1. *Exponent.* Let A be a K algebra. Set $[A:K]=\dim_K A$. If $[A:K]=p^m$ we call m the exponent of A over K and write $m=e[A:K]$. In particular if $A=K[x]$ we also say that x has exponent m over K and write $m=e[x:K]$. Clearly,

Lemma 1. *For $x \in L$, $e[x:K]$ is the least n such that $x^{p^n} \in K$.*

Let B be an A algebra and assume $[A:K]=p^m$ and $[B:K]=p^n$. We then define $e[B:A]=n-m$. In other words we require $e[B:K]=e[B:A]+e[A:K]$. This rule is consistent if A is a field and $e[B:A]$ is already defined as before.

We define the absolute exponent e_K of K to be $e[K:K^p]$.

Lemma 2. *If E is a finite extension of K then $e_E=e_K$.*

Proof. We know that $[E:K^p]=[E:K]\cdot[K:K^p]=[E:E^p]\cdot[E^p:K^p]$ and, since the map $x \mapsto x^p$ is an isomorphism of E/K to E^p/K^p, we also have $[E:K]=[E^p:K^p]$. Thus $e_E=[E:E^p]=[K:K^p]=e_K$.

2. *Chains of fields in L/K.* We introduce notation for two familiar chains of fields in L/K.

A. *Upper chain.* $L=(L/K)^0 \supseteq (L/K)^1 \supseteq \cdots \supseteq (L/K)^e \supseteq \cdots \supseteq K$.

We define $(L/K)^e=L^{p^e}\cdot K$ and $\delta_e(L/K)=e[(L/K)^{e-1} : (L/K)^e]$.

Proposition 1. *For all $e \geqq 1$, $\delta_e(L/K) \geqq \delta_{e+1}(L/K)$.*

Proof.

$$[L^{p^{e-1}}\cdot K:L^{p^e}\cdot K] = [L^{p^e}\cdot K^p:L^{p^{e+1}}\cdot K^p] \geqq [L^{p^e}\cdot K:L^{p^{e+1}}\cdot K].$$

B. *Lower chain.* $K=(L/K)_0 \subseteq (L/K)_1 \subseteq \cdots \subseteq (L/K)_e \subseteq \cdots \subseteq L$.

We define $(L/K)_e=\{x \in L : e[x:K] \leqq e\}=\{x \in L : x^{p^e} \in K\}$, and $\alpha_e(L/K) =[(L/K)_e:(L/K)_{e-1}]$. We note that the α's do not satisfy inequalities such as the δ's do.

Example 1. Let $L=K[x]$ with $h=e[x:K]$. Let $0<e\leqq h$ and $q=p^e$. Then

$$(L/K)^e = K[x^q] = (L/K)_{h-e}, \qquad \delta_e(L/K) = \alpha_e(L/K) = 1.$$

Example 2. Let P be a field and let a, b, c be algebraically independent over P. Let $K=P(a, b, c)$ and $L=K[z, w]$ where

$$z^{p^2} = a, \qquad w^p = b+cz^p.$$

Then

$(L/K)^1=(L/K)_1=K[z^p]=K[w^p]$,

$\alpha_1(L/K)=1$, $\alpha_2(L/K)=2$, $\alpha_r(L/K)=0$ for $r>2$,

$\delta_1(L/K)=2$, $\delta_2(L/K)=1$, $\delta_r(L/K)=0$ for $r>2$.

The assertion for $(L/K)^1$ is clear. Assume that $(L/K)_1 \neq K[z^p]$. Then there exists $y \in L$ and $y \notin K[z^p]$ such that $y^p \in K$. Call $y^p=d$. Then, by Example 1, $y \notin K[z]$ since $y \in K[z]$ and $y^p \in K \Rightarrow y \in K[z^p]$. Thus $L=K[z, y]$. Hence we can write w as

$$w = \sum r_{i,j,k}z^{i+pj}y^k \quad \text{with } r_{i,j,k} \in K,\ 0 \leqq i, j, k < p.$$

Then

$$b+cz^p = w^p = \sum r^p_{i,j,k}z^{pi+p^2j}y^{pk} = \sum r^p_{i,j,k}a^j\, d^k z^{pi}.$$

By comparison we get $b, c \in K^p[a, d]$ so that $e[K^p[a, b, c]:K^p] \leqq 2$. Then for any field M such that $K^p \subseteq M$ we have $e[M[a, b, c]:M] \leqq 2$. Take $M = P(a^p, b^p, c^p)$. Then $M[a, b, c] = P(a, b, c) = K$. But since a, b, c are algebraically independent over P,

$$e[M[a, b, c]:M] = e[P(a, b, c):P(a^p, b^p, c^p)] = 3.$$

This is a contradiction which shows that $(L/K)_1 = K[z^p]$. The assertions about the α's and δ's follow from the computation of $(L/K)^1$ and $(L/K)_1$.

3. *Height.* The height $h(L/K)$ of L over K is the integer defined by any one of the three equivalent conditions below:

α. Maximum $\{e[x:K] : x \in L\}$.

β. Minimum h such that $(L/K)^h = K$.

γ. Minimum h such that $(L/K)_h = L$.

Remark 1. Other authors have used the word "exponent" for what we call "height". The disadvantage of the old terminology is that if $[L:K] = p^m$ one cannot call m the "exponent of L/K" since the word "exponent" has been used in another sense.

Remark 2. If $h = h(L/K)$ then, for all e, $(L/K)^{h-e} \subseteq (L/K)_e$. We conclude

Proposition 2. *Let* $0 \leqq e \leqq h = h(L/K)$. *Then*

$$\sum_{i=1}^{e} \delta_{h+1-i}(L/K) = e[(L/K)^{h-e}:K] \leqq e[(L/K)_e:K] = \sum_{i=1}^{e} \alpha_i(L/K).$$

We will now seek another inequality similar to the one given in Proposition 2. Let $0 \leqq e \leqq h = h(L/K)$ and let $q = p^e$. We now examine the relationship of the five fields: $(L/K)^e$, $(L/K)_e$, L^q, $L^q \cap K$, K^q. First consider the diagrams:

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & & \\
L^q \arrow[dr, dash] & & (L/K)_e \arrow[dl, dash] \arrow[dr, dash] & \\
 & L^q \cap K \arrow[dr, dash] & & K \arrow[dl, dash] \\
 & & K^q &
\end{tikzcd}$$

Diagram 1

$$\begin{tikzcd}
 & L \arrow[d, dash] & \\
 & (L/K)^e \arrow[dl, dash] \arrow[dr, dash] & \\
L^q \arrow[dr, dash] & & K \arrow[dl, dash] \\
 & L^q \cap K &
\end{tikzcd}$$

Diagram 2

Remark 3. From Diagrams 1 and 2,

$$[L:K] = [L:(L/K)_e] \cdot [(L/K)_e:K] = [L:(L/K)^e] \cdot [(L/K)^e:K].$$

Remark 4. In Diagram 1 the map $x \mapsto x^q$ induces isomorphisms $L \approx L^q$, $(L/K)_e \approx L^q \cap K$, $K \approx K^q$.

Remark 5. In Diagram 2, $(L/K)^e = L^q \cdot K$ so that $[L^q:L^q \cap K] \geqq [(L/K)^e:K]$. Equality holds if and only if L^q and K are linearly disjoint over $L^q \cap K$.

PROPOSITION 3. *Let $0 \leqq e \leqq h = h(L/K)$ and let $q = p^e$. Then*

1. $\sum_{i=1}^{e} \alpha_i(L/K) = e[(L/K)_e : K] \leqq e[L:(L/K)^e] = \sum_{i=1}^{e} \delta_i(L/K)$.

2. *We have equality at the middle of* 1 *if and only if L^q and K are linearly disjoint over $L^q \cap K$.*

Proof. The equalities in 1 are trivial. For the middle inequality we note

$$e[(L/K)_e : K] \leqq e[L:(L/K)^e] \Leftrightarrow [(L/K)_e : K] \leqq [L:(L/K)^e]$$
$$\Leftrightarrow [L:(L/K)_e] \geqq [(L/K)^e : K].$$

The last $\Leftrightarrow$ comes from Remark 3. Moreover, from Remarks 4 and 5, we obtain $[L:(L/K)_e] \geqq [(L/K)^e : K]$. Thus we have 1.

To show 2 note that in the equivalences we can replace all inequalities by equalities. We can then apply Remark 5.

REMARK 6. From Propositions 2 and 3 we obtain

$$\sum_{i=1}^{e} \delta_{h+1-i}(L/K) \leqq \sum_{i=1}^{e} \alpha_i(L/K) \leqq \sum_{i=1}^{e} \delta_i(L/K).$$

PROPOSITION 4. *The following conditions are equivalent:*

1. *For all $q = p^e$, L^q and K are linearly disjoint over $L^q \cap K$.*
2. *For all e, $e[(L/K)_e : K] = e[L:(L/K)^e]$.*
3. *For all i, $\alpha_i(L/K) = \delta_i(L/K)$.*

2. **Definitions.** We continue to let K be a field and L be a finite purely inseparable extension of K.

1. *Normal sequences.* If $x \in L$ we say that x is normal in L/K if $e[x:K] = h(L/K)$ or, equivalently, if $e[x:K] \geqq e[y:K]$ for all $y \in L$.

A normal sequence $x_1, \ldots, x_r$ in L/K is one such that if we let $K_i = K[x_1, \ldots, x_i]$ then, for $1 \leqq i \leqq r$,

α. x_i is normal in L/K_{i-1}.

β. $x_i \notin K_{i-1}$.

If a normal sequence $x_1, \ldots, x_r$ is such that $L = K[x_1, \ldots, x_r]$ we say that $x_1, \ldots, x_r$ is a normal generating sequence or NGS of L/K.

Now let $x_1, \ldots, x_r$ be a normal sequence in L/K. For $1 \leqq i \leqq r$, set $e_i = e[x_i : K_{i-1}]$ and $q_i = p^{e_i}$. Also define $J_i \subseteq \boldsymbol{Z}^r$ by

$$J_i = \{(\alpha_1, \ldots, \alpha_i, 0, \ldots, 0) : 0 \leqq \alpha_k < q_k\}.$$

Then the set $\{x^\alpha\}_{\alpha \in J_i}$ is a K basis for K_i. Also

PROPOSITION 5. $e_1 \geqq e_2 \geqq \cdots \geqq e_r$.

Proof. $e_i = e[x_i : K_{i-1}] \geqq e[x_{i+1} : K_{i-1}] \geqq e[x_{i+1} : K_i] = e_{i+1}$.

PROPOSITION 6. *Let S be a generating set for L/K. Then there exists an NGS for L/K with elements chosen from S.*

Proof. If we have a normal sequence $x_1, \dots, x_s$ with $x_i \in S$ for all i then either $K_s = L$ (and we are done) or $L \neq K_s$. If $L \neq K_s$ then we extend the normal sequence by choosing x_{s+1} so that

α. $x_{s+1} \in S$.

β. x_{s+1} is normal in L/K_s.

This is done by

LEMMA 3. *If S generates L/K and $K \subseteq M \subseteq L$ then there exists $x \in S$ such that x is normal in L/M.*

Proof. If for $e > 0$ and $q = p^e$ we have $S^q \subseteq M$ then $L^q \subseteq M$ since $L = K[S]$. Thus $\operatorname{Max}\{e[x:M] : x \in L\} = \operatorname{Max}\{e[x:M] : x \in S\}$. Thus we can choose $x \in S$ such that $e[x:M] = h(L/M)$, that is, x normal in L/M.

2. *Elementary extensions.* We say that L is elementary over K if there exist elements $x_1, \dots, x_r \in L - K$ such that $L \approx K[x_1] \otimes_K \cdots \otimes_K K[x_r]$. By rearrangement, we can always assume also that $x_1, \dots, x_r$ is an NGS for L/K.

Now let $x_1, \dots, x_r$ be an NGS for an arbitrary extension L/K. We use the notation from 1.

PROPOSITION 7. *The following conditions are equivalent:*

1. *The canonical map $K[x_1] \otimes_K \cdots \otimes_K K[x_r] \to L$ is an isomorphism.*
2. *For $1 \leqq i \leqq r$, $e_i = e[x_i:K]$.*

Proof. The proof is by induction based on the lemma below:

LEMMA 4. *Given a field extension M/K and x algebraic over K then the following conditions are equivalent:*

1. *The canonical map $M \otimes_K K[x] \to M[x]$ is an isomorphism.*
2. $[M[x]:M] = [K[x]:K]$.

We now define the notions "simply truncated polynomial algebra" and "variation" which we use to study field extensions.

3. *Simply truncated polynomial algebras.* Let R be a commutative ring and A be an R algebra. We say that A is a simply truncated polynomial algebra over R if there exist $u_i \in A$, $1 \leqq i \leqq r$, such that

α. $A = R[u_1, \dots, u_r]$.

β. The relations among $u_1, \dots, u_r$ are generated by equations $u_i^{a_i} = 0$ where $a_1 \geqq a_2 \geqq \cdots \geqq a_r > 1$.

For short we say that A is an STP algebra over R. We call the sequence $u_1, \dots, u_r$ a truncating sequence for A. We call a_i the order of u_i and denote it by $o(u_i)$. We say that A is of type $a_1, \dots, a_r$ relative to the truncating sequence $u_1, \dots, u_r$.

PROPOSITION 8. *Let A be an STP algebra over R. Let $u_1, \dots, u_r$ and $w_1, \dots, w_s$ be truncating sequences for A and let $a_i = o(u_i)$ and $b_i = o(w_i)$. Then $r = s$ and, for all i, $a_i = b_i$.*

Proof.

Case 1. *When R is a field E.* Then A is a local ring with maximal ideal $I=(u_1,\dots,u_r)=(w_1,\dots,w_s)$. Define $f_k=\dim_E I^k-\dim_E I^{k+1}$. We will show in effect that the sequence $f_1,f_2,\dots$ determines the structure of A.

We can find an E basis of I^k modulo I^{k+1} in two ways:

1. as $\{u_1^{\alpha_1}\cdot\cdots\cdot u_r^{\alpha_r}\}$ where $\sum\alpha_i=k$ and $0\leqq\alpha_i<a_i$,

2. as $\{w_1^{\beta_1}\cdot\cdots\cdot w_s^{\beta_s}\}$ where $\sum\beta_j=k$ and $0\leqq\beta_j<b_j$.

First apply this to $k=1$. Then $u_1,\dots,u_r$ and $w_1,\dots,w_s$ both form bases of I modulo I^2. Thus $r=s$.

Next suppose that, for some i, $a_i\neq b_i$. Choose t such that $a_t\neq b_t$ but, for $i>t$, $a_i=b_i$. We may assume $a_t>b_t$. Then take $k=b_t$. We will obtain a contradiction.

We first claim that if, for all i, $0\leqq\alpha_i\leqq k-1$, then the conditions given below are equivalent:

1*. $\sum\alpha_i=k$ and, for all i, $0\leqq\alpha_i<a_i$.

2*. $\sum\alpha_i=k$ and, for all i, $0\leqq\alpha_i<b_i$.

Indeed, for $i\leqq t$, the inequality $0\leqq\alpha_i\leqq k-1$ already implies the corresponding inequality in 1* or 2*, while, for $i>t$, we know $a_i=b_i$.

Next, if $\sum\alpha_i=k$ but the condition $0\leqq\alpha_i\leqq k-1$ does not hold for all i, then one $\alpha_i=k$ and all other $\alpha_j=0$. In this case, we get at least t such sequences which satisfy 1* since $a_i>k$ for $i\leqq t$ while we get at most $t-1$ such sequences which satisfy 2* since $b_i\leqq k$ for $i\geqq t$.

These remarks yield two different values for f_k which is of course absurd. Thus, for all i, $a_i=b_i$.

Case 2. *General case.* We reduce to the case of a field by choosing a maximal ideal M in R and considering the STP algebra A/MA over R/MR.

Remark 1. The proposition shows that the number of generators and the type of an STP algebra are independent of the choice of the truncating sequence.

Remark 2. One can extract a method for computing the type sequence of an STP algebra from the proof.

Indeed, suppose $f_1,f_2,\dots$ are known. Then $f_1=r$. Next suppose that a_i has been found for $i>t$. For all k, define

$N_k=$ Number of sequences $\alpha_1,\dots,\alpha_r$ such that

1. $\sum\alpha_i=k$.
2. For $i>t$, $0\leqq\alpha_i<a_i$.
3. For $i\leqq t$, $0\leqq\alpha_i\leqq k-1$.

Then the proof shows that, for $k\geqq a_{t+1}$, $a_t>k\Leftrightarrow f_k-N_k\geqq t$. Thus one can obtain a_t as the least $k\geqq a_{t+1}$ such that $f_k-N_k<t$.

Remark 3. We use the standard multi-index notation in working with STP algebras. If $\alpha=(\alpha_1,\dots,\alpha_r)$ and $\beta=(\beta_1,\dots,\beta_r)$, set

$$\alpha<\beta\Leftrightarrow\text{for all } i,\ \alpha_i<\beta_i,$$

$$\alpha\leqq\beta\Leftrightarrow\text{for all } i,\ \alpha_i\leqq\beta_i.$$

Then, if A has type $a=(a_1,\ldots,a_r)$ and $u=(u_1,\ldots,u_r)$ is a truncating sequence for A, the family of $u^\alpha=u_1^{\alpha_1}\cdot\cdots\cdot u_r^{\alpha_r}$ for $0\leqq\alpha<a$ forms a basis of A over R.

4. *Variations.* We return to the finite purely inseparable extension L/K. Let E be an extension of L and let $A=E[u]$ be an STP algebra of type a over E. Then an E-variation of L/K with values in A is a K algebra hom $\theta\colon L\to A$. We will see in a moment that a variation is a generalization of a derivation.

Write $\theta(z)=\sum_{0\leqq\alpha<a}D_\alpha(z)u^\alpha$. We determine equations which the D_α must satisfy. Each D_α is a K linear map of L into E and the K algebra hom conditions are the following: For all α and all z, $w\in L$,

$$D_\alpha(zw)=\sum_{\beta+\gamma=\alpha}D_\beta(z)D_\gamma(w).$$

In particular, $D_0(zw)=D_0(z)D_0(w)$, so that D_0 is a K isomorphism of L into E and so must be the inclusion map.

We say that $z\in L$ is invariant under θ if equivalently

1. $\theta(z)=z$,
2. for all $\alpha\neq 0$, $D_\alpha(z)=0$,
3. for all α and all $w\in L$, $D_\alpha(zw)=zD_\alpha(w)$.

We let L^θ be the set of invariants of θ. L^θ is a subfield of L containing K. We let $\mathrm{Fix}_E\,(L/K)$ be the intersection of all L^θ as θ ranges over all E-variations of L/K.

We now give some examples.

Example 1. A has one generator u such that $u^2=0$. Then $\theta(z)=z+D(z)u$ with D_1 denoted by D. For z, $w\in L$, we have $D(zw)=D(z)w+zD(w)$. Thus D is a derivation.

Example 2. A has one generator u such that $u^a=0$ and $a>2$. Then the family $\{D_i\}$ for $1\leqq i<a$ is what is called a higher derivation. For z, $w\in L$, we have $D_i(zw)=\sum_{j+k=i}D_j(z)D_k(w)$.

Example 3. Taylor variation. Let $K\subseteq M\subseteq L$ and $L=M[x]$. Set $e=e[x:M]$, $q=p^e$, and $A=L[u]$ with $u^q=0$. Define an L variation of L/K with values in A by setting $\theta(z)=z$ for $z\in M$ and $\theta(x)=x+u$. In general if $a_i\in M$ for $0\leqq i<q$ then

$$\theta\left(\sum_{i=0}^{q-1}a_ix^i\right)=\sum_{i=0}^{q-1}a_i(x+u)^i=\sum_{j=0}^{q-1}\left(\sum_{k=j}^{q-1}a_k\binom{k}{j}x^{k-j}\right)u^j.$$

Thus

$$D_j\left(\sum_{i=0}^{q-1}a_ix^i\right)=\sum_{i=j}^{q-1}a_i\binom{i}{j}x^{i-j}.$$

Thus θ is just the Taylor expansion of $P(x)=\sum a_ix^i$ in terms of $x+u$. Note that $L^\theta=M$.

Example 4. Elementary extensions. Let L be elementary over K and let $x_1,\ldots,x_r$ be an NGS for L/K such that $L\approx K[x_1]\otimes_K\cdots\otimes_K K[x_r]$. Let $e_i=e[x_i:K]$ and $q_i=p^{e_i}$. Let $A=L[u_1,\ldots,u_r]$ with $u_i^{q_i}=0$. Define $\theta\colon L\to A$ by setting $\theta(z)=z$ for $z\in K$ and $\theta(x_i)=x_i+u_i$. We can view θ as a sort of generalized Taylor variation.

If we let θ_i be the Taylor variation defined as in Example 3 by taking $M=K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r]=M_i$ and $x=x_i$, then we have

$$L^\theta = \bigcap_{i=1}^{r} L^{\theta_i} = \bigcap_{i=1}^{r} M_i = K.$$

Also, if $\theta_L \colon L \otimes_K L \to A$ is defined by $\theta_L(x \otimes y)=\theta(x)y$, then θ_L is an isomorphism of L algebras.

3. **Structure theorem.** We continue to let K be a field and L be a finite purely inseparable extension of K. We now give a theorem which leads to elegant structure equations for L/K. A slightly different version of the theorem was discovered by Pickert [3].

THEOREM 1. *Let $x_1, \ldots, x_r$ be a normal sequence in L/K and let $K_i=K[x_1, \ldots, x_i]$. For $1 \leqq i \leqq r$ let $e_i=e[x_i, K_{i-1}]$ and $q_i=p^{e_i}$. Then, for $1 \leqq i \leqq r$,*

$$x_i^{q_i} \in K[x_1^{q_i}, \ldots, x_{i-1}^{q_i}].$$

Proof. We use induction on r.

Case $r=1$. Then $i=1$ and the assertion is $x_1^{q_1} \in K$ which is clear.

Induction step. Assume the assertion for all normal sequences of length less than r. In particular, induction applied to the sequence $x_1, \ldots, x_{r-1}$ yields the assertion for $1 \leqq i < r$. Thus we need only show

$$x_r^{q_r} \in K[x_1^{q_r}, \ldots, x_{r-1}^{q_r}]. \tag{1}$$

Now $x_2, \ldots, x_r$ is a normal sequence in L/K_1 so by induction we also know

$$x_r^{q_r} \in K_1[x_2^{q_r}, \ldots, x_{r-1}^{q_r}]. \tag{2}$$

Since $\{x_1^i\}$ for $0 \leqq i < q_r$ is a basis of K_1 over $K[x_1^{q_r}]$ and since we know (2), we can write

$$x_r^{q_r} = \sum_{0 \leqq i < q_r} A_i x_1^i, \quad \text{with } A_i \in K[x_1^{q_r}, \ldots, x_{r-1}^{q_r}]. \tag{3}$$

Thus we can show (1) if we can show $A_i=0$ for $i>0$. Set $t=q_2/q_r$ and define subfields $K \subseteq M \subseteq N \subseteq K_1$ by

$$M = K[x_1^{q_2}], \qquad N = K[x_1^t].$$

The set $\{x_1^{it}\}$ for $0 \leqq i < q_r$ is a basis of N over M. We now raise the terms in (3) to the power t to obtain

$$x_r^{q_2} = x_r^{q_r t} = \sum_{0 \leqq i < q_r} A_i^t x_1^{it}. \tag{4}$$

Thus if we show that $x_r^{q_2} \in M$ and that, for all i, $A_i^t \in M$, then by the uniqueness of an expression in terms of a basis we get $x_r^{q_2}=A_0^t$ and, for all $i>0$, $A_i=0$, which is what we want to show. Now set $h=e_1=h(L/K)$, $g=e_2=h(L/K_1)$, $f=e_r$. Then note that $p^g=q_2$, $p^f=q_r$, and $p^{g-f}=q_2/q_r=t$. We then assert

1. $x_r^{q_2} \in (L/K)^g$.
2. $A_i^t \in (L/K)^g$.

1 is trivial. For 2, note that $A_i \in (L/K)^f$ so $A_i^t \in (L/K)^{f+g-f}$. Thus it remains only to show that $(L/K)^g \subseteq M$. Now

$$M = (K_1/K)^g = (K_1/K)_{h-g} = K_1 \cap (L/K)_{h-g}.$$

But $(L/K)^g \subseteq (L/K)_{h-g}$ since $h=h(L/K)$ and $(L/K)^g \subseteq (L/K_1)^g \subseteq K_1$ since $g=h(L/K_1)$. Thus $(L/K)^g \subseteq M$ and we are done.

Now let $x_1, \dots, x_r$ be an NGS for L/K. As in §2, part 1, we set

$$K_i = K[x_1, \dots, x_i], \qquad e_i = e[x_i : K_{i-1}], \quad q_i = p^{e_i},$$
$$J_i = \{(\alpha_1, \dots, \alpha_i, 0, \dots, 0) \in \boldsymbol{Z}^r : 0 \leqq \alpha_k < q_k\}.$$

Then the set $\{x^\alpha\}_{\alpha \in J_i}$ is a K basis for K_i. In particular, let $J=J_r$. Then the set $\{x^\alpha\}_{\alpha \in J}$ is a K basis for L. Now let

$$I_i = \{\alpha \in \boldsymbol{Z}^r : q_i\alpha \in J\}.$$

In §4, we will see that $\{x^{q_i\alpha}\}_{\alpha \in I_i}$ forms a K basis for $K[x_1^{q_i}, \dots, x_{i-1}^{q_i}]$. Using Theorem 1 we can write $x_i^{q_i}$ uniquely in terms of this basis with coefficients $a_{i,\alpha} \in K$ for $\alpha \in I_i$,

$$x_i^{q_i} = \sum_{\alpha \in I_i} a_{i,\alpha} x^{q_i\alpha}.$$

We will refer to these equations as the *structure equations*. We remark that these equations generate all the relations among the elements $x_1, \dots, x_r$ since the equations determine a K algebra of dimension $q_1 \cdot \cdots \cdot q_r$ which is exactly the dimension of L/K.

4. Technical results.

We will derive some corollaries of Theorem 1. We will use the notation from the end of §3. Also let $0 \leqq e < h = h(L/K)$. Then set $q=p^e$ and define

$$\gamma_e = \text{Maximum } i \quad \text{such that } e_i > e.$$

COROLLARY 1. $(L/K)^e = K[x_1^q, \dots, x_r^q] = K[x_1^q, \dots, x_{\gamma_e}^q]$.

Proof. The first equality comes from the definition of $(L/K)^e$ and the fact that $x_1, \dots, x_r$ generates L/K. Now let $\gamma_e < i \leqq r$. Then $e_i \leqq e$ so that $q_i | q$. From Theorem 1 we have $x_i^{q_i} \in K[x_1^q, \dots, x_{i-1}^{q_i}]$ so that $x_i^q \in K[x_1^q, \dots, x_{i-1}^q]$ so that $K[x_1^q, \dots, x_i^q] = K[x_1^q, \dots, x_{i-1}^q]$. Descending from $i=r$ to $i=\gamma_e+1$ proves the corollary.

COROLLARY 2. *Let $1 \leqq k \leqq \gamma_e$. Then the elements $x_k^{q\alpha_k}$ with α_k such that $0 \leqq q\alpha_k < q_k$ form a basis of $K[x_1^{q_i}, \dots, x_k^q]$ over $K[x_1^q, \dots, x_{k-1}^q]$.*

Proof. Set $M=K[x_1^q,\dots,x_{k-1}^q]$ and $N=K[x_1^q,\dots,x_k^q]$. Then

1. To show that the powers $(x_k^q)^{\alpha_k}$ with $0\leqq\alpha_k<q_k/q$ span N over M we need $x_k^{q_k}\in M$. By Theorem 1, we know more:

$$x_k^{q_k}\in K[x_1^{q_k},\dots,x_{k-1}^{q_k}].$$

Note, if $k\leqq\gamma_e$, then $e_k>e$, so $q|q_k$.

2. To show that $\{x_k^{q\alpha_k}\}$ for $0\leqq q\alpha_k<q_k$ is independent over M we note that $\{x_k^{\beta_k}\}$ for $0\leqq\beta_k<q_k$ is independent over K_{k-1} and $M\subseteq K_{k-1}$.

Corollary 3. *A K basis of $K[x_1^q,\dots,x_r^q]$ is given by $\{x^{q\alpha}\}$ with α such that $q\alpha\in J$.*

Proof. If $\alpha=(\alpha_1,\dots,\alpha_r)$ then $q\alpha\in J$ amounts to

1. For $1\leqq k\leqq\gamma_e$, $0\leqq q\alpha_k<q_k$.

2. For $\gamma_e<k\leqq r$, $\alpha_k=0$.

Thus Corollary 3 follows from Corollaries 1 and 2.

Remark 1. We are now ready to prove the assertion from the end of §3. To do this take $e=e_i$. Then $q=q_i$ and $\gamma_e<i$. Thus

$$K[x_1^q,\dots,x_r^q]=K[x_1^q,\dots,x_{i-1}^q]=K[x_1^q,\dots,x_{\gamma_e}^q].$$

The basis assertion from the end of §3 follows from Corollary 3.

Remark 2. The next three corollaries show that the sequence of exponents $e_1,\dots,e_r$ depends only on L/K and not on the NGS chosen.

Corollary 4. *The elements $x_1^{q\alpha_1}\cdot\cdots\cdot x_{\gamma_e}^{q\alpha_{\gamma_e}}$ with $0\leqq\alpha_k<p$ form a basis of $(L/K)^e$ over $(L/K)^{e+1}$.*

Corollary 5. $\delta_{e+1}(L/K)=\gamma_e$.

Corollary 6. $e_i>e\Leftrightarrow\gamma_e\geqq i\Leftrightarrow\delta_{e+1}(L/K)\geqq i$.

We have seen in Corollaries 1 and 3 how to find $(L/K)^e=L^q\cdot K$. One can also find L^q and $(L/K)_e$ but the answer is less simple. If $\beta\in J$ we can use the structure equations to write

$$x^{q\beta}=(x^\beta)^q=\sum_{q\alpha\in J}A_{\beta,q,\alpha}x^{q\alpha}.$$

Then if $z=\sum_{\beta\in J}c_\beta x^\beta$ we have

$$z^q=\sum_{\beta\in J}c_\beta^q x^{q\beta}=\sum_{q\alpha\in J}\Bigl(\sum_{\beta\in J}A_{\beta,q,\alpha}c_\beta^q\Bigr)x^{q\alpha}.$$

We obtain immediately

Corollary 7. $z\in(L/K)_e\Leftrightarrow z^q\in K\Leftrightarrow$ *for $\alpha\neq0$ one has*

$$\sum_{\beta\in J}A_{\beta,q,\alpha}c_\beta^q=0.$$

Corollary 8. *Let* $w=\sum_{q\alpha\in J} d_\alpha x^{q\alpha} \in (L/K)^e$. *Then* $w \in L^q \Leftrightarrow$ *for some family* $\{c_\beta\}_{\beta\in J}$ *with* $c_\beta \in K$ *one has*

$$d_\alpha = \sum_{\beta\in J} A_{\beta,q,\alpha} c_\beta^q.$$

Note that the equations in Corollaries 7 and 8 are semilinear relative to the isomorphism $\varphi(x)=x^q$.

The main difficulty in using these corollaries lies in the fact that the coefficients $A_{\beta,q,\alpha}$ are quite hard to write down in terms of the $a_{i,\alpha}$ from the structure equations.

Remark 3. Let A be a K algebra. Let $e \geqq 0$ and set $q=p^e$. One can then define A^q, $(A/K)^e$, $(A/K)_e$:

$$A^q = \{x^q : x \in A\}, \qquad (A/K)^e = A^q \cdot K, \qquad (A/K)_e = \{x \in A : x^q \in K\}.$$

Then A^q is a subring of A and $(A/K)^e$ and $(A/K)_e$ are K algebras. Assume now that $A=K[x_1, \dots, x_r]$ where the defining relations for $x_1, \dots, x_r$ are of the form

$$x_i^{q_i} = \sum_{\alpha\in I_i} a_{i,\alpha} x^{q_i\alpha},$$

with

$$e_1 \geqq e_2 \geqq \cdots \geqq e_r \geqq 1, \qquad q_i = p^{e_i}, \qquad a_{i,\alpha} \in K,$$
$$J = \{(\alpha_1, \dots, \alpha_r) : 0 \leqq \alpha_k < q_k\}, \qquad I_i = \{\alpha : q_i\alpha \in J\}.$$

In this case we will say that A is a special K algebra. When A is a special K algebra then the analogues of Corollaries 1 to 8 hold.

5. **Splitting theorems.** We now examine what happens to L/K under base extension by a field E. We use the notation of §3 and in addition we set

$$F = L \otimes_K E, \qquad z_i = x_i \otimes 1, \qquad E_i = E[z_1, \dots, z_i].$$

We view F as an E algebra via the map $a \mapsto 1 \otimes a$. Over E the z_i satisfy the same structure equations as the x_i do over K, that is

$$z_i^{q_i} = \sum_{\alpha\in I_i} a_{i,\alpha} z^{q_i\alpha}.$$

Hence in the sense of Remark 3 of §4, F is a special E algebra. Certain of our results will depend only on the fact that F is a special E algebra and we will make note of this as we go along.

We begin with a simple result which tells when F is a field. We will give a better result in Chapter 2, §8.

Theorem 2. *The following conditions are equivalent*:

1. *F is a field.*
2. *For all i, E_i is a field.*
3. *For all i, $z_i^{q_i} \notin E_{i-1}^p$.*

Proof. The proof will use only the fact that F is special over E with structure equations as given above.

$1 \Leftrightarrow 2$. Trivial.

$2 \Leftrightarrow 3$. By induction on r one can assume the equivalence of the following:

$$\text{For all } i < r,\ E_i \text{ is a field} \Leftrightarrow \text{for all } i < r,\ z_i^{q_i} \notin E_{i-1}^p.$$

Then, assuming these equivalent statements hold, we must show

$$E_r \text{ is a field} \Leftrightarrow z_r^{q_r} \notin E_{r-1}^p.$$

Set $a = z_r^{q_r} \in E_{r-1}$. Then $E_r = E_{r-1}[z_r]$ and z_r has $X^{q_r} - a$ as its minimal polynomial over E_{r-1}. Thus

$$E_r \text{ is a field} \Leftrightarrow X^{q_r} - a \text{ is prime in } E_{r-1}[X] \Leftrightarrow a \notin E_{r-1}^p.$$

We are done.

The main result, which we now state, asserts that for large enough fields E, F becomes a simply truncated polynomial algebra over E.

THEOREM 3. *The following conditions are equivalent*:

1. *F is an STP algebra over E.*
2. *F is a subalgebra of an STP algebra over E.*
3. *For all i and all $\alpha \in I_i$, $a_{i,\alpha} \in E^{q_i}$.*
4. *For all $q = p^e$, $L^q \cdot (K \cap E^q)$ and K are linearly disjoint over $K \cap E^q$.*

Proof. Conditions 1, 2, and 3 do not mention the original extension L/K explicitly. These conditions are simply assertions about the algebra extension F/E or about the structure constants $a_{i,\alpha} \in E$ in the defining relations for the generators $z_1, \ldots, z_r$ of F/E:

$$z_i^{q_i} = \sum_{\alpha \in I_i} a_{i,\alpha} z^{q_i \alpha}.$$

In fact, the equivalence of conditions 1, 2, and 3 depends only on the fact that F is a special E algebra with generators $z_1, \ldots, z_r$ and structure constants $a_{i,\alpha}$. We will use only this much in the proof that 1, 2, and 3 are equivalent and then we will return to the original situation and show that 1, 2, and 3 are equivalent to 4.

$1 \Rightarrow 2$. Trivial.

$2 \Rightarrow 3$. Let $F \subseteq A$ with A an STP algebra over E. Let $A = E[u_1, \ldots, u_s]$ with $u_j^{b_j} = 0$. Define $N \subseteq \boldsymbol{Z}^s$ by

$$N = \{(\beta_1, \ldots, \beta_s) : 0 \leqq \beta_j < b_j\}.$$

Then $\{u^\beta\}_{\beta \in N}$ forms an E basis for $E[u]$. For $\alpha \in J$ let $z^\alpha = \sum_{\beta \in N} b_{\alpha,\beta} u^\beta$. Then for $e \geqq 0$ and $q = p^e$ we have

$$z^{q\alpha} = \sum_{\beta \in N} b_{\alpha,\beta}^q u^{q\beta} = \sum_{q\beta \in N} b_{\alpha,\beta}^q u^{q\beta}.$$

Note that if $qB \notin N$ then $u^{q\beta}=0$ so that those terms drop from the equation. Now let $1 \leqq i \leqq r$ and let $c_{i,\beta}$ denote $b_{\alpha,\beta}$ for the multi-index α such that $z^{\alpha}=z_i$. Then

$$z_i = \sum_{\beta \in N} c_{i,\beta} u^{\beta}.$$

We apply the above discussion to the structure equation for z_i:

$$\begin{aligned} z_i^{q_i} &= \sum_{q_i\beta \in N} c_{i,\beta}^{q_i} u^{q_i\beta} = \sum_{\alpha \in I_i} a_{i,\alpha} z^{q_i\alpha} \\ &= \sum_{q_i\beta \in N} \Big(\sum_{\alpha \in I_i} a_{i,\alpha} b_{\alpha,\beta}^{q_i} \Big) u^{q_i\beta}. \end{aligned}$$

Since the elements $u^{q_i\beta}$ with $q_i\beta \in N$ are independent over E we can equate coefficients

$$c_{i,\beta}^{q_i} = \sum_{\alpha \in I_i} a_{i,\alpha} b_{\alpha,\beta}^{q_i}.$$

This is a system of linear equations with coefficients in E^{q_i} which is satisfied by $(a_{i,\alpha})_{\alpha \in I_i}$. Conversely if $(\bar{a}_{i,\alpha})_{\alpha \in I_i}$ is any solution of the system then, by reversing the calculation,

$$z_i^{q_i} = \sum_{\alpha \in I_i} \bar{a}_{i,\alpha} z^{q_i\alpha}.$$

But the elements $z^{q_i\alpha}$ with $\alpha \in I_i$ are independent over E so that we must have $\bar{a}_{i,\alpha}=a_{i,\alpha}$ for all $\alpha \in I_i$. Thus we see that $(a_{i,\alpha})_{\alpha \in I_i}$ is the unique solution in E of a system of linear equations with coefficients in E^{q_i} and this shows that $a_{i,\alpha} \in E^{q_i}$ for all $\alpha \in I_i$.

3 ⇒ 1. For all i and all α, write $a_{i,\alpha}=d_{i,\alpha}^{q_i}$ with $d_{i,\alpha} \in E$. Then let

$$u_i = z_i - \sum_{\alpha \in I_i} d_{i,\alpha} z^{\alpha}.$$

Then $F=E[z_1, \ldots, z_r]=E[u_1, \ldots, u_r]$. Moreover $u_i^{q_i}=0$. There are no other relations on the u_i independent of the relations $u_i^{q_i}=0$ since the relations $u_i^{q_i}=0$ define an E algebra of dimension $q_1 \cdot \cdots \cdot q_r = \dim_E F$.

We now turn to 3 ⇔ 4 in the original situation.

3 ⇔ 4. First $L^q(K \cap E^q) \cdot K = L^q \cdot K = (L/K)^e$.

$$\begin{tikzcd} & (L/K)^e \arrow[dl, dash] \arrow[dr, dash] & \\ L^q(K \cap E^q) \arrow[dr, dash] & & K \arrow[dl, dash] \\ & K \cap E^q & \end{tikzcd}$$

Thus the linear disjointness condition becomes $[(L/K)^e : K] = [L^q(K \cap E^q) : K \cap E^q]$. Now the set $\{x^{q\alpha}\}$ for $q\alpha \in J$ belongs to L^q and forms a basis of $(L/K)^e$ over K. Since this set lies in $L^q(K \cap E^q)$ condition 4 is equivalent to

4*. For all e, the set $\{x^{q\alpha}\}_{q\alpha \in J}$ forms a basis of $L^q(K \cap E^q)$ over $K \cap E^q$.

If 4* is true, then the expression for $x_i^{q_i}$ in the structure equations must have coefficients in $K \cap E^{q_i}$, that is, for all α, $a_{i,\alpha} \in E^{q_i}$. Conversely, assume, for all i and α, $a_{i,\alpha} \in E^{q_i}$. Then we have, for all i,

$$x_i^{q_i} \in (K \cap E^{q_i})[x_1^{q_i}, \ldots, x_{i-1}^{q_i}].$$

Thus, for $e \geqq e_i$ and $q=p^e$, $x_i^q \in (K \cap E^q)[x_1^q, \ldots, x_{i-1}^q]$. Then by the technique of Corollary 1 of §4 we obtain

$$L^q(K \cap E^q) = (K \cap E^q)[x_1^q, \ldots, x_r^q] = (K \cap E^q)[x_1^q, \ldots, x_{\gamma_e}^q].$$

We can then mimic Corollaries 2 and 3 of §4 to obtain 4*. Thus we have $3 \Leftrightarrow 4^*$.

This ends the proof of Theorem 3.

We say that E splits L/K if E satisfies the equivalent conditions of Theorem 3. Thus E splits $L/K \Leftrightarrow L \otimes_K E$ is an STP algebra over E.

We set

$$S(L/K) = K[\sqrt[q_i]{a_{i,\alpha}}], \qquad 1 \leqq i \leqq r \text{ and } \alpha \in I_i.$$

By condition 3 of Theorem 3, E splits $L/K \Leftrightarrow S(L/K) \subseteq E$.

Thus $S(L/K)$ is uniquely determined as the smallest field which splits L/K and so we may call $S(L/K)$ the splitting field of L/K. In particular, $S(L/K)$ is independent of the choice of NGS for L/K.

We remark that when E splits L/K the proof $3 \Rightarrow 1$ gives an explicit truncating sequence for the STP algebra $L \otimes_K E$ over E.

Proposition 9. $L \subseteq S(L/K)$.

Proof. Let $S = S(L/K)$. Then $L \otimes_K S$ is an STP algebra over S. Let m be the maximal ideal of $L \otimes_K S$. Then L is mapped to S via

$$L \longrightarrow L \otimes_K S \longrightarrow (L \otimes_K S)/m \xrightarrow{\approx} S.$$

This map is injective since L is a field. The map is unique since L/K is purely inseparable. Thus $L \subseteq S$.

We now give another splitting theorem which studies the case when $L = S(L/K)$.

Theorem 4. *The following are equivalent to* $L = S(L/K)$:

1. *L is elementary over K.*
2. *K is a fixed field of all Taylor variations of L.*
3. *K is the fixed field of all L-variations of L.*
4. *For all $q=p^e$, L^q and K are linearly disjoint over $L^q \cap K$.*
5. *For all e, $e[L:(L/K)^e] = e[(L/K)_e:K]$.*
6. *For all i, $\delta_i(L/K) = \alpha_i(L/K)$.*
7. *$L \otimes_K L$ is an STP algebra over L.*

8. *Given a normal sequence $x_1, \ldots, x_s$ in L/K such that if $K_s = K[x_1, \ldots, x_s]$ then $L \neq K_s$, then there exists $x_{s+1} \in L - K_s$ with*

α. x_{s+1} normal in L/K_s.

β. $e[x_{s+1}:K_s] = e[x_{s+1}:K]$.

Proof. 1 ⇒ 2. By Example 4 of part 4 of §2.

2 ⇒ 3. Trivial.

3 ⇒ 4. Assume that 3 holds but 4 fails, say for $q = p^e$. Choose a subset $c_1, \ldots, c_t$ of K with the smallest number of elements t such that

α. $c_1, \ldots, c_t$ is independent over $L^q \cap K$.

β. $c_1, \ldots, c_t$ is dependent over L^q.

Then we can find $z_1, \ldots, z_t \in L^q$ with all $z_i \neq 0$ such that $0 = \sum_i z_i c_i$. By dividing by z_t we may assume that $z_t = 1$. By condition α, for some i, $z_i \notin K$. We may assume $z_1 \notin K$.

Consider any L variation $\theta: L \to L[u]$. Write $\theta(x) = \sum_\alpha D_\alpha(x) u^\alpha$. Then

$$\begin{aligned} 0 &= \theta\Big(\sum_i z_i c_i\Big) = \sum_i \theta(z_i)\theta(c_i) = \sum_i \theta(z_i) c_i \\ &= \sum_\alpha \Big(\sum_i D_\alpha(z_i) c_i\Big) u^\alpha. \end{aligned}$$

Thus for all α

$$(*) \qquad 0 = \sum_i D_\alpha(z_i) c_i.$$

Now $\theta(L^q) = (\theta L)^q \subseteq (L[u])^q \subseteq L^q[u]$ so that, for all i and α, $D_\alpha(z_i) \in L^q$. Thus the equations (*) are linear equations for the c_i with coefficients in L^q.

Now, since 3 holds and since $z_1 \notin K$, we can choose θ such that $\theta(z_1) \neq z_1$. Then for some $\beta \neq 0$ we have $D_\beta(z_1) \neq 0$. Of course $D_\beta(z_t) = D_\beta(1) = 0$. Thus from (*)

$$0 = \sum_{i=1}^{t-1} D_\beta(z_i) c_i.$$

Thus $c_1, \ldots, c_{t-1}$ are dependent over L^q contrary to the minimal choice of t.

4 ⇔ 7 ⇔ $L = S(L/K)$. By Proposition 9 and the definition, $L = S(L/K) \Leftrightarrow L$ splits L/K. But L splits L/K if L satisfies the equivalent conditions in Theorem 3. Condition 1 in that theorem is Condition 7 here and Condition 4 in that theorem is Condition 4 here since $L^q(K \cap L^q) = L^q$.

$L = S(L/K)$ ⇒ 8. Extend $x_1, \ldots, x_s$ to any NGS $x_1, \ldots, x_s, y_1, \ldots, y_t$. Let $y = y_1$ and set $e = e[y:K_s] = h(L/K_s)$ and $q = p^e$. We seek $z \in L$ with

$$e = e[z:K_s] \quad \text{and} \quad e = e[z:K].$$

Let I denote the usual index set such that $\{x^\alpha\}$ for $\alpha \in I$ forms a basis of K_s over K. Then the structure equation for y^q has the form

$$y^q = \sum_{q\alpha \in I} b_\alpha x^{q\alpha} \quad \text{with } b_\alpha \in K.$$

Let $c_\alpha = \sqrt[q]{b_\alpha}$. Then since the formation of $S(L/K)$ does not depend on the NGS chosen for L/K and since $x_1, \ldots, x_s, y_1, \ldots, y_t$ is an NGS for L/K we have that $c_\alpha \in S(L/K) = L$. Moreover, since $c_\alpha^q = b_\alpha \in K$, we have that $e[c_\alpha : K] \leqq e$.

We claim that, for some β, $e = e[c_\beta : K_s]$. Then $z = c_\beta$ will give the element we seek because then $e = e[c_\beta : K_s] \leqq e[c_\beta : K] \leqq e$, so that $e = e[c_\beta : K_s]$ and $e = e[c_\beta : K]$. To prove the claim note that

$$\begin{aligned} \text{for all } \alpha,\ e[c_\alpha : K_s] < e &\Leftrightarrow \text{for all } \alpha,\ b_\alpha \in K_s^p \\ &\Leftrightarrow y^q \in K_s^p \Leftrightarrow e[y : K_s] < e. \end{aligned}$$

8 ⇒ 1. Using 8, we can find an NGS $x_1, \ldots, x_r$ for L/K such that, for all i, $e[x_i, K_{i-1}] = e[x_i, K]$. By Proposition 7, we get 1.

4 ⇔ 5 ⇔ 6. Proposition 4.

This ends the proof of Theorem 4.

Remark 1. In [5], Sweedler shows the equivalence of the following parts of Theorem 4: 1, 4, and the version of 3 below:

K is the fixed field of all higher derivations of L into L.

We have adapted his proof for 3 ⇒ 4.

Remark 2. In view of conditions 2 and 3 in Theorem 4 one might hope that one can add to the list of conditions in Theorem 3:

K is the fixed field of all E-variations of L/K.

Alas this condition is weaker than the ones in Theorem 3. For a counterexample see Example 3 below.

We now give three examples of nonelementary extensions. In all examples P denotes a field of characteristic p.

Example 1. Let K and L be as in Example 2 of part 2 of §1, that is, $K = P(a, b, c)$ with a, b, c algebraically independent over P and $L = K[z, w]$ with $z^{p^2} = a$, $w^p = b + cz^p$. We have seen that

$$\begin{aligned} \delta_1(L/K) &= 2, & \alpha_1(L/K) &= 1, \\ \delta_2(L/K) &= 1, & \alpha_2(L/K) &= 2. \end{aligned}$$

By 6 of Theorem 4, L/K is not elementary. It is easy to find the splitting field in this case:

$$S(L/K) = K[\sqrt[p^2]{a}, \sqrt[p]{b}, \sqrt[p]{c}] = K[z, \sqrt[p]{b}, \sqrt[p]{c}].$$

Example 2. We now construct L/K such that $S(L/K)$ is also not elementary over K. Let a, b, c, d be algebraically independent over P and set $K = P(a, b, c, d)$, $L = K[u, v]$, with $u^{p^3} = d$, $v^{p^2} = a + (b^p + c^p a)u^{p^2}$. Then $S(L/K) = K[u, z, w]$ with $z^{p^2} = a$, $w^{p^2} = b^p + c^p a$, that is $w^p = b + cz^p$.

Set $M = K[z, w]$ and $N = K[u, z, w] = S(L/K)$. Then $M \subseteq N$, so by Proposition 10 below, we have $S(M/K) \subseteq S(N/K)$. But $S(M/K) = K[z, \sqrt[p]{b}, \sqrt[p]{c}]$. Thus $S(M/K) \nsubseteq N$ so in particular $N \neq S(N/K)$.

Proposition 10. *If $K\subseteq L\subseteq M$ then $S(L/K)\subseteq S(M/K)$.*

Proof. Let $E=S(M/K)$. Then $L\otimes_K E\subseteq M\otimes_K E$ and $M\otimes_K E$ is an STP algebra over E since E splits M/K. By Theorem 3, $L\otimes_K E$ is also an STP algebra over E so that E splits L/K and $S(L/K)\subseteq E$.

Example 3. We now construct $K\subseteq L\subseteq E$ such that the following conditions hold:

1. E does not split L/K.
2. K is the fixed field of all E-variations of L/K.

Define

$K=P(a, b, c, d)$ with a, b, c, d algebraically independent over P and char $P=3$.

$L=K[z, w]$ with $z^9=a$, $w^3=b+cz^3+dz^6$.

$E=L[x]$ with $x^3=c+2dz^3$.

Proof of 1. $S(L/K)=K[\sqrt[9]{a}, \sqrt[3]{b}, \sqrt[3]{c}, \sqrt[3]{d}]$ so that $e[S(L/K){:}L]=2$. On the other hand, $e[E{:}L]=1$. Thus $S(L/K)\nsubseteq E$ so E does not split L/K.

Proof of 2. We will define a variation $\theta\colon L\to E[u]$ where $u^6=0$. On the generators z and w of L we define θ by $\theta z=z+u$, $\theta w=w+xu$. To show that θ defines a K algebra hom we must show that $(z+u)^9=a$, $(w+xu)^3=b+c(z+u)^3+d(z+u)^6$. The first equation is clear and we compute to verify the second:

$$\begin{aligned}(w+xu)^3 &= w^3+x^3u^3 = b+cz^3+dz^6+(c+2dz^3)u^3,\\ b+c(z+u)^3+d(z+u)^6 &= b+cz^3+cu^3+dz^6+2dz^3u^3+du^6\\ &= b+cz^3+dz^6+(c+2dz^3)u^3.\end{aligned}$$

We have used $u^6=0$.

Next let M be the fixed field of θ. We claim that $M=K$. If not then we assert that $K[z^3]=(L/K)_1\subseteq M$. For the equation, $K[z^3]=(L/K)_1$, we note that $K[z^3]\subseteq(L/K)_1$ and that $(L/K)_1$ cannot have exponent 2 over K for this would imply

$$\begin{aligned}&\alpha_1(L/K) = 2 = \delta_1(L/K), \qquad \alpha_2(L/K) = 1 = \delta_2(L/K),\\ &\alpha_k(L/K) = 0 = \delta_k(L/K), \qquad k \geqq 3,\end{aligned}$$

which would imply that L/K is elementary by Theorem 4 which would contradict the calculation of $S(L/K)$ given above. We now obtain the inclusion $(L/K)_1\subseteq M$ by observing that, since $e[(L/K)_1{:}K]=1$, $(L/K)_1$ is the unique subfield of L of height 1 over K and so must be a subfield of any M such that $K\nsubseteq M\subseteq L$. Finally, however, the inclusion $K[z^3]\subseteq M$ is impossible since θ does not fix z^3:

$$\theta(z^3) = (z+u)^3 = z^3+u^3 \neq z^3.$$

Hence the claim that $M=K$ is true and this proves 2.

6. The ascending chain of splitting fields.

We are led by Example 2 of §5 to define an increasing chain of splitting fields $S_n(L/K)$. We do this by induction:

$$\begin{aligned}S_0(L/K) &= L,\\ S_n(L/K) &= S(S_{n-1}(L/K)/K) \quad \text{for } n \geqq 1,\\ S_\infty(L/K) &= \bigcup_{n\geqq 0} S_n(L/K).\end{aligned}$$

We now study these fields in detail.

LEMMA 5. $h(S(L/K)/K)=h(L/K)$.

Proof. Since $K\subseteq L\subseteq S(L/K)$, we have $h(L/K)\leqq h(S(L/K)/K)$. But $S(L/K)$ is built using q_ith roots of elements of K where $q_i=p^{e_i}$ and $e_i\leqq h(L/K)$. Thus $h(S(L/K)/K)=h(L/K)$.

LEMMA 6. *For* $1\leqq n\leqq\infty$, $h(S_n(L/K))=h(L/K)$.

Proof. For n finite use induction on n and Lemma 5. For $n=\infty$, use the finite case and the fact that a union of fields of height h has height h.

PROPOSITION 11. *Let $K\subseteq L\subseteq E$ and let E be elementary over K. Then $S_\infty(L/K)\subseteq E$.*

Proof. We know that $L=S_0(L/K)\subseteq E$. Assume by induction that $S_n(L/K)\subseteq E$. Then $S_n(L/K)\otimes_K E\subseteq E\otimes_K E$ and $E\otimes_K E$ is an STP algebra over E since E is elementary over K. By Theorem 3, E splits $S_n(L/K)$ so that

$$S_{n+1}(L/K) = S(S_n(L/K)/K) \subseteq E.$$

Thus, for all n, $S_n(L/K)\subseteq E$ so that $S_\infty(L/K)\subseteq E$.

PROPOSITION 12. *There exists a finite extension E of K such that $L\subseteq E$ and E is elementary over K.*

Proof. Choose a p-basis $\{z_\mu\}_{\mu\in M}$ of K over K^p. Note that the index set has cardinality equal to the absolute exponent e_K of K and so may be infinite. Let $h=h(L/K)$ and let $q=p^h$. Also let $w_\mu=\sqrt[q]{z_\mu}$. Then standard facts about p-bases show

1. If N is a finite subset of M with n elements and if we set $E_N=K[w_\mu]$ for $\mu\in N$ then

α. $[E_N:K]=q^n$.

β. E_N is elementary over K. In fact: $E_N\approx\bigotimes_{\mu\in N}K[w_\mu]$.

2. If x is purely inseparable over K and $e[x:K]\leqq h$, then there exists a finite subset N of M such that $x\in E_N$.

Thus, if $L=K[x_1,\dots,x_r]$, choose $N\subseteq M$, N finite, such that $x_i\in E_N$ for all i. Then $L\subseteq E_N$ and E_N is the desired field.

THEOREM 5. 1. *$S_\infty(L/K)$ is a finite extension of K.*

2. *For some $n<\infty$, $S_\infty(L/K)=S_n(L/K)$.*

3. *$S_\infty(L/K)$ is elementary over K and thus is the unique minimal extension E of K such that $L\subseteq E$ and E is elementary over K.*

Proof. 1. Use Propositions 11 and 12.

2. Use 1.

3. If $S_\infty(L/K)=S_n(L/K)$ with $n<\infty$ then $S_\infty(L/K)=S_{n+1}(L/K)$ so that $S_\infty(L/K)$ is its own splitting field and so by Theorem 4 is elementary over K. The rest of 3 follows from Proposition 11.

REMARK. In [5], Sweedler shows

There exists a unique minimal extension E of K
such that $L \subseteq E$ and E is elementary over K.

However, lacking splitting fields, his proof is quite complicated.

7. **Complexity.** In Theorem 5 of §6, we have seen that the ascending chain $\{S_n(L/K)\}$ becomes stable after a finite number of steps. Thus we are led to define the complexity $c(L/K)$ of L/K by

$$c(L/K) = \text{least } n \text{ such that } S_\infty(L/K) = S_n(L/K).$$

We will show

THEOREM 6. $c(L/K)+1 \leqq h(L/K)$.

We will need some preliminaries before we can show the theorem. We will call a pair (M, N) of intermediate fields of L/K a normal pair if

1. $L = M \cdot N$.
2. M is elementary over K.

The degree $d(M, N)$ of the normal pair (M, N) is defined as $h(N/K)$.

EXAMPLE 1. The pair (K, L) is always a normal pair whose degree is the height of L/K.

EXAMPLE 2. If L is elementary over K then the pair (L, K) is a normal pair of degree 0.

LEMMA 7. *Suppose there exists a normal pair for L/K of degree $d > 0$. Then there exists a normal pair (M, N) for L/K of degree d such that*

1. *The exponent sequence $e_1 \geqq \cdots \geqq e_m$ defined by any NGS for M/K is such that $e_m \geqq d$.*
2. *For all $x \in N$, $e[x:M] < d$.*

Proof. Let (P, Q) be a normal pair for L/K of degree d. Write P in the form

$$P = K[x_1] \otimes_K \cdots \otimes_K K[x_s].$$

Let $f_i = e[x_i:K]$. We can assume that $f_1 \geqq \cdots \geqq f_s$. Next let r be the maximum integer k such that $f_k \geqq d$. Then set

$$R = K[x_1, \ldots, x_r], \qquad N = Q[x_{r+1}, \ldots, x_s].$$

Then R is elementary over K, $R \cdot N = Q[x_1, \ldots, x_s] = P \cdot Q = L$, $h(N/K) = h(Q/K) = d$. Thus (R, N) is also a normal pair of degree d. Next choose from N a maximal sequence $y_1, \ldots, y_t$ such that if $R_i = R[y_1, \ldots, y_i]$ then $e[y_i : R_{i-1}] = d$ for $1 \leqq i \leqq t$. Set $M = R_t$. By Proposition 7, M is elementary over K. Thus, (M, N) is also a normal pair of degree d. The exponent sequence of M/K is $f_1, \ldots, f_r, d, \ldots, d$. Hence 1 holds for (M, N). Finally, by the maximal choice of the sequence $y_1, \ldots, y_t$ we have, for all $x \in N$, $e[x:M] < d$. This is 2 and so we are done.

Lemma 8. *Suppose there exists a normal pair for L/K of degree* 1. *Then L is elementary over K.*

Proof. Let (M, N) be chosen as in Lemma 7 with $d=1$. Then, for all $x\in N$, $e[x:M]<1$, so that $x\in M$. Thus, $L=M\cdot N=M$, so L is elementary over K.

Lemma 9. *Suppose there exists a normal pair for L/K of degree $d>0$. Then there exists a normal pair for $S(L/K)$ over K of degree strictly less than d.*

Proof. Let (M, N) be chosen as in Lemma 7. Choose $x_1,\ldots,x_m\in M$ so that

$$M = K[x_1]\otimes_K\cdots\otimes_K K[x_m], \qquad e[x_1:K]\geqq\cdots\geqq e[x_m:K].$$

Next, using the fact that N generates L over M and Proposition 6, choose $x_{m+1},\ldots,x_n\in N$ such that $x_{m+1},\ldots,x_n$ is an NGS for L/M. We first show that $x_1,\ldots,x_n$ is an NGS for L/K. Let

$$K_i = K[x_1,\ldots,x_i], \qquad e_i = e[x_i, K_{i-1}], \qquad q_i = p^{e_i},$$
$$S_i = \{x_i,\ldots,x_n\}, \qquad J = \{(\alpha_1,\ldots,\alpha_n) : 0 \leqq \alpha_k < q_k\}.$$

We must show that $e_i=h(L/K_{i-1})$. For $i>m$, this follows from the fact that $x_{m+1},\ldots,x_n$ is an NGS for L/M. Now let $i\leqq m$. We observe that, since S_i generates L over K_{i-1},

$$h(L/K_{i-1}) = \max_{j\geqq i} e[x_j:K_{i-1}].$$

In finding the maximum, there are two cases to consider:

Case 1. $i\leqq j\leqq m$. Then $e[x_j:K_{i-1}]=e[x_j:K]\leqq e[x_i:K]=e[x_i:K_{i-1}]=e_i$.

Case 2. $j>m$. Then, by 1 of Lemma 7, $e_i\geqq d$. On the other hand, since N has height d over K, we have $e[x_j:K_{i-1}]\leqq e[x_j:K]\leqq d\leqq e_i$. Thus

$$\max_{j\geqq i} e[x_j:K_{i-1}] = e_i.$$

Thus, $x_1,\ldots,x_n$ is an NGS for L/K.

We now examine the structure equations for $x_1,\ldots,x_n$. For $i\leqq m$ we have simply $x_i^{q_i}=a_i\in K$. For $i>m$ we have the usual structure equations

$$x_i^{q_i} = \sum_{q_i\alpha\in J} a_{i,\alpha}x^{q_i\alpha}.$$

Thus, $S(L/K)$ is generated over K by

$$\sqrt[q_i]{a_i} = x_i \quad \text{for } i \leqq m,$$
$$\sqrt[q_i]{a_{i,\alpha}} \qquad \text{for } i > m.$$

Now set $P=K[\sqrt[q_i]{a_{i,\alpha}}]$ for $i>m$. Then $S(L/K)=M\cdot P$ so that (M, P) is a normal pair for $S(L/K)$ over K. Finally, $h(P/K)<d$ since, by 2 of Lemma 7, for $i>m$,

$$e_i = e[x_i:K_{i-1}] \leqq e[x_i:M] < d.$$

Thus, (M, P) is a normal pair for $S(L/K)$ over K of degree strictly less than d.

We will obtain Theorem 6 as a consequence of Example 1 and the more general result below:

THEOREM 7. *Suppose there exists a normal pair for L/K of degree $d>0$. Then $c(L/K)+1\leqq d$.*

Proof. Let $c=d-1$. By repeated use of Lemma 9, $S_c(L/K)$ has a normal pair of degree at most 1. By Lemma 8, $S_c(L/K)$ is elementary over K. Thus, by Theorem 5, $S_\infty(L/K)=S_c(L/K)$ so that $c(L/K)\leqq c$, as desired.

8. **Examples.** We now construct a field K and extensions L_n of K such that one has $c(L_n/K)=n$, $h(L_n/K)=n+1$. This will show that the inequality in Theorem 6 is the best of its kind. Let

P be a base field of characteristic p.

$\{y_{i,j}\}_{0\leqq i\leqq j<\infty}$ be independent transcendentals over P.

$K=P(y_{i,j})_{0\leqq i\leqq j<\infty}$.

We next define elements $x_{k,n}$ for $0\leqq k\leqq n<\infty$ which will be used to construct the fields L_n. We use induction on n. To begin

$$x_{0,0}^{p} = y_{0,0}. \tag{0}$$

Assume that $x_{k,m}$ is defined for $m<n$. Then set

$$x_{0,n}^{p^{n+1}} = y_{0,n}. \tag{1}$$

Also for $1\leqq k\leqq n$ set

$$x_{k,n}^{p^n} = y_{k,n}+(x_{k-1,n-1}^{p^n})\cdot x_{0,n}^{p^n}. \tag{2}$$

We then define $L_n=K[x_{0,n},\dots,x_{n,n}]$. To find the properties of the extensions L_n of K it will also be useful to define $z_{k,n}$ by

$$z_{k,n}^{p^n} = y_{k,n}. \tag{3}$$

From (2) one can show

$$x_{k,n} = z_{k,n}+x_{k-1,n-1}\cdot x_{0,n} \quad \text{for } 1 \leqq k \leqq n. \tag{4}$$

We also define

$$M_n = K[x_{0,n}, z_{1,n},\dots, z_{n,n}], \qquad E_{k,n} = L_{n-k}\cdot\dots\cdot L_n.$$

Fact 1. $h(L_n/K)=n+1$.

Proof. First note that $e[x_{0,n}:K]=n+1$ so $h(L_n/K)\geqq n+1$. To show equality we must show that, for $1\leqq k\leqq n$, $x_{k,n}^{p^{n+1}}\in K$. By induction on n, we can assume that $x_{k-1,n-1}^{p^n}\in K$. Then by (1) and (2),

$$x_{k,n}^{p^{n+1}} = y_{k,n}^{p}+(x_{k-1,n-1}^{p^n})^p\cdot y_{0,n}\in K.$$

We are done.

REMARK. Fact 1 shows that the coefficients $(x^{p^n}_{k-1,n-1})$ in (2) are elements of K.

Fact 2. $L_{n-1}\cdot L_n = L_{n-1}[x_{0,n}, z_{1,n}, \ldots, z_{n,n}] = L_{n-1}\cdot M_n$.

Proof. Use (4).

Fact 3. $e[L_n:K] = n^2+n+1$.

Proof. The inequality $e[L_n:K] \leqq n^2+n+1$ comes from the fact that L_n is constructed by adjoining one p^{n+1}-root and n p^n-roots. On the other hand

$$e[L_n:K] \geqq e[L_{n-1}\cdot L_n:L_{n-1}] = e[L_{n-1}\cdot M_n:L_{n-1}] = n^2+n+1.$$

We are done.

Fact 4. The sequence $x_{0,n}, \ldots, x_{n,n}$ is an NGS for L_n/K. Moreover, equations (0), (1), and (2) give the structure equations for this normal generating sequence.

Proof. Fix n and set $P_i = K[x_{0,n}, \ldots, x_{i,n}]$ for $0 \leqq i \leqq n$. Then, to show both assertions, we must show

α. $e[x_{0,n}:K] = n+1 = h(L/K)$.

β. $e[x_{i,n}:P_{i-1}] = n = h(L/P_{i-1})$ for $1 \leqq i \leqq n$.

Assertion α comes from Fact 1. To show assertion β, we first note that for all j

$$x^{p^n}_{j,n} \in K[x^{p^n}_{0,n}] \subseteq P_0 \subseteq P_{i-1}.$$

Thus

$$n \geqq h(L/P_{i-1}) \geqq e[x_{i,n}:P_{i-1}] = e[P_i:P_{i-1}].$$

But in view of Fact 3, we cannot have $e[P_i:P_{i-1}] < n$ for any i so we obtain assertion β and Fact 4 as well.

Fact 5. $S(L_n/K) = L_{n-1}\cdot M_n$.

Proof. Using the structure equations we find that

$$S(L_n/K) = K[x_{0,n}, z_{1,n}, \ldots, z_{n,n}, x_{0,n-1}, \ldots, x_{n-1,n-1}] = L_{n-1}\cdot M_n.$$

Fact 6. $E_{k,n} = L_{n-k}\cdot M_{n-k+1}\cdot \cdots \cdot M_n$.

Proof. By induction on k, using Fact 2.

Fact 7. $S(E_{k,n}/K) = E_{k+1,n}$.

Proof. Set $F_{k,n} = M_{n-k+1}\cdot \cdots \cdot M_n \cdot K$. Then $F_{k,n}$ is elementary over K and linearly disjoint from L_{n-k} over K. By Proposition 13 below as well as Facts 5 and 6 we obtain

$$S(E_{k,n}/K) = S(L_{n-k}/K)\cdot S(F_{k,n}/K) = L_{n-k-1}\cdot M_{n-k}\cdot F_{k,n} = E_{k+1,n}.$$

Fact 8. $c(L_n/K) = n$.

Proof. The chain $E_{0,n} \subseteq E_{1,n} \subseteq \cdots \subseteq E_{n,n}$ is strictly increasing so that by Fact 7 $c(L_n/K) \geqq n$. But by Theorem 6 and Fact 1 we have $c(L_n/K) \leqq h(L_n/K) - 1 = n$. We are done.

It remains to state and prove Proposition 13.

PROPOSITION 13. *Let P and Q be linearly disjoint extensions of K. Then* $S(P\cdot Q/K) = S(P/K)\cdot S(Q/K)$.

Proof. Set $E=S(P/K)\cdot S(Q/K)$. Then, by Proposition 10, $E\subseteq S(P\cdot Q/K)$. On the other hand since P and Q are linearly disjoint over K, $P\cdot Q\approx P\otimes_K Q$. Thus

$$(P\cdot Q)\otimes_K E \approx (P\otimes_K Q)\otimes_K E \approx (P\otimes_K E)\otimes_E (Q\otimes_K E).$$

The last algebra is the tensor product over E of STP algebras over E since E splits P and Q over K. Thus $(P\cdot Q)\otimes_K E$ is an STP algebra over E and E splits $P\cdot Q$ over K, that is, $S(P\cdot Q/K)\subseteq E$.

Chapter 2. Splitting Theory for Algebras

1. **Splitting questions.** Let A be a K algebra where K is a field of characteristic p. We recall that in Remark 3 of Chapter 1, §4 we said that A is a special K algebra if $A=K[x_1,\dots,x_r]$ where the defining relations for $x_1,\dots,x_r$ are of the form

$$x_i^{q_i} = \sum_{\alpha\in I_i} a_{i,\alpha}x^{q_i\alpha}$$

with

$$e_1 \geqq e_2 \geqq \cdots \geqq e_r \geqq 1 \qquad q_i = p^{e_i}, \qquad a_{i,\alpha}\in K,$$
$$J = \{(\alpha_1,\dots,\alpha_r) : 0 \leqq \alpha_k < q_k\},\quad I_i = \{\alpha : q_i\alpha\in J\}.$$

In this case, we will call $x_1,\dots,x_r$ a normal generating sequence or NGS of type $q=(q_1,\dots,q_r)$ for A over K. We also define

$$d_{i,\alpha} = \sqrt[q_i]{a_{i,\alpha}}, \qquad S(A/K) = K[d_{i,\alpha}], \qquad 1 \leqq i \leqq r \text{ and } \alpha\in I_i.$$

Here we view the elements $d_{i,\alpha}$ as in some fixed algebraic closure C of K and we call $S(A/K)$ the splitting field of A over K.

Remark. An example of a special K algebra is the case when A is defined by setting $a_{i,\alpha}=0$ for all i and α. In this case we call A a special STP algebra over K. In general, if $B=K[u_1,\dots,u_r]$ is an STP algebra over K with truncating sequence $u_1,\dots,u_r$, type $b_1,\dots,b_r$, and dimension $b=b_1\cdot\cdots\cdot b_r$, then B is special over K if and only if each b_i is a power of p or, equivalently, b is a power of p.

Now let A be a special K algebra and let E be an extension of K such that $S(A/K)\subseteq E$. In $A\otimes_K E$ define

$$u_i = x_i\otimes 1 - \sum_{\alpha\in I_i} d_{i,\alpha}x^{\alpha}\otimes 1.$$

Then $A\otimes_K E=E[u_1,\dots,u_r]$ and the defining relations for $u_1,\dots,u_r$ are simply $u_i^{q_i}=0$. Thus, $A\otimes_K E$ is a special STP algebra over E. More generally, we have

Theorem 1. *Let A be a special K algebra and E be an extension of K. Then the following conditions are equivalent*:

1. *$A\otimes_K E$ is a special STP algebra over E.*
2. *$A\otimes_K E$ is a subalgebra of a direct sum of STP algebras over E.*
3. *$S(A/K)\subseteq E$.*

Proof. We have just seen that 3 $\Rightarrow$ 1 and it is obvious that 1 $\Rightarrow$ 2. Moreover, the essential aspects of 2 $\Rightarrow$ 3 have already been done in the proof of Theorem 3 of Chapter 1, §5. An inspection of the proof given there shows that with some minor changes of notation the argument works just as well when $A \otimes_K E$ is a subalgebra of a direct sum of STP algebras as when $A \otimes_K E$ is a subalgebra of one STP algebra.

Theorem 1 justifies calling $S(A/K)$ the splitting field of A over K.

We now give a name to the kind of splitting properties that we have just been studying. Let A be a K algebra. Then

1. We say that A is strongly splittable over K if $A \otimes_K E$ is a special STP algebra over E for some extension E of K.
2. We say that A is splittable over K if $A \otimes_K E$ is a direct sum of special STP algebras over E for some extension E of K.

One of our main results will be

THEOREM 2. *The following conditions are equivalent*:

1. *A is strongly splittable over K.*
2. *A is special over K.*

We will prove Theorem 2 in §4. In §2 we study the structure of any finite-dimensional K algebra. We examine what happens to such an algebra under base change. We will then be able to state a theorem which characterizes splittable algebras and to show that this theorem is a consequence of Theorem 2. In §3 we develop the technical results needed to show Theorem 2.

2. The structure of a finite-dimensional K algebra.

Let A be a finite-dimensional commutative K algebra. We will need to examine the relation between A and a certain subalgebra M of A defined by

$$M = \bigcap_{n \geqq 0} A^{p^n} \cdot K.$$

We begin by studying how A and M factor into direct sums of ideals.

Let $\alpha \in A$. Recall that α is an idempotent if $\alpha \neq 0$ and $\alpha^2 = \alpha$. Set

$$I = \{\alpha \in A : \alpha \text{ is an idempotent}\}.$$

Note that if α is an idempotent in A then $\alpha^k = \alpha$ for all $k \geqq 1$ so that $\alpha \in M$. Thus I is also the set of idempotents in M.

Let S be a subset of I. Then one can show that the following conditions are equivalent:

1. A is a direct sum of the ideals $A \cdot \alpha$ for $\alpha \in S$.
2. M is the direct sum of the ideals $M \cdot \alpha$ for $\alpha \in S$.
3. One has $\sum_{\alpha \in S} \alpha = 1$ and $\alpha\beta = 0$ for $\alpha, \beta \in S$ with $\alpha \neq \beta$.

When these conditions hold we say that S factors A and M. Next it can be shown that every factorization of A or M into a direct sum of ideals arises as above from a subset S of I which factors A and M. Thus, in particular, the factorizations of A and M into direct sums of ideals correspond.

We now explain how to get the best possible factorization of A and M. If $\alpha \in A$ is an idempotent, we say that α is minimal if the five equivalent conditions given below hold:

1. $A \cdot \alpha$ is a local K algebra with unit α.
2. α is the unique idempotent in $A \cdot \alpha$.
3. $M \cdot \alpha$ is a local K algebra with unit α.
4. α is the unique idempotent in $M \cdot \alpha$.
5. It is impossible to write $\alpha = \beta + \gamma$ with $\beta, \gamma \in I$ and $\beta\gamma = 0$.

Set

$$J = \{\alpha \in A : \alpha \text{ is a minimal idempotent}\}.$$

Then J factors A and M and the ideals $A \cdot \alpha$ and $M \cdot \alpha$ for $\alpha \in J$ cannot be factored further as the direct sum of ideals. Moreover J is uniquely determined by these properties and it is in this sense that J gives the best possible factorization of A and M.

The factorization of A and M via J allows one to reduce many questions to the case when A and M are local rings. It should be noted that if α is an idempotent in A then

$$M \cdot \alpha = \bigcap_{n \geqq 0} A^{p^n} \cdot K \cdot \alpha = \bigcap_{n \geqq 0} (A \cdot \alpha)^{p^n} \cdot K.$$

This shows that $M \cdot \alpha$ is constructed from $A \cdot \alpha$ just as M is from A.

THEOREM 3. *M is the unique maximal separable K algebra in A.*

Proof. The family $\{A^{p^n} \cdot K\}_{n \geqq 0}$ forms a descending chain of subspaces of the finite-dimensional K vector space A. Hence this chain must stabilize, say at $n = r$. Thus, for $n \geqq r$, $M = A^{p^n} \cdot K$. We can now show that $M = M^p \cdot K$. Indeed

$$M^p \cdot K = (A^{p^r} \cdot K)^p \cdot K = A^{p^{r+1}} \cdot K = M.$$

From $M = M^p \cdot K$, we see that if $x_1, \ldots, x_t$ is a K basis of M then $x_1^p, \ldots, x_t^p$ is also a K basis of M. In particular, M cannot have nilpotent elements. Indeed, if M did have nilpotent elements, we could find $x \in M$ such that $x \neq 0$ and $x^p = 0$ and then could choose a basis with $x_1 = x$ to get a contradiction.

We now show that M is a separable K algebra. For this it is enough to consider the case when A and M are local. Then, since M has no nilpotent elements and is local, M is a field. Then, from $M = M^p \cdot K$, we see that M is a separable field extension of K which shows that M is a separable K algebra.

Finally, if L is any separable K subalgebra of A, we must show that $L \subseteq M$. Since A is commutative, L is commutative and so L must be the direct sum of separable field extensions of K. Thus $L = L^{p^n} \cdot K$ for all $n \geqq 0$. In particular, for $n = r$,

$$L = L^{p^r} \cdot K \subseteq A^{p^r} \cdot K = M.$$

We are done.

We are now ready to study splitting questions. We begin with the case when A is local. M is then a separable field extension of K. We will aim to show

THEOREM 4. *Assume that A is a local K algebra. Then the following conditions are equivalent:*

1. *A is splittable over the field K.*
2. *A is strongly splittable over the field M.*

We will see that the issue in the theorem is to compare $A \otimes_K E$ with $A \otimes_M E$ for certain extensions E of M. We first show

LEMMA 1. *For all extensions E of M, $A \otimes_M E$ is a local E algebra and its residue field is a purely inseparable extension of E.*

Proof. Let C be an algebraic closure of E. We must show that there exists exactly one E homomorphism φ of $A \otimes_M E$ into C. Now one such homomorphism does exist since $A \otimes_M E$ is finite dimensional and C is algebraically closed. Call this homomorphism φ. We must show φ is unique. Since A generates $A \otimes_M E$ as an E algebra it suffices to show that $\varphi(x)$ is uniquely determined for $x \in A$. Choose r so that $M = A^{p^r} \cdot K$. Then $x^{p^r} \in M$ so that $\varphi(x)^{p^r} = \varphi(x^{p^r}) = x^{p^r}$. Thus $\varphi(x)$ is the unique p^rth root in C of x^{p^r} so $\varphi(x)$ is uniquely determined.

We now choose N to be some least normal extension of K such that $M \subseteq N$ and we let Σ be the set of all K isomorphisms of M into N. If E is an extension of N and $\sigma \in \Sigma$, we denote by E_σ the field E viewed as an extension of M via $M \xrightarrow{\sigma} N \subseteq E$. We let φ: $M \to \bigoplus_{\sigma \in \Sigma} E_\sigma$ be the map induced by the maps σ: $M \to E_\sigma$ and we let Ψ: $M \otimes_K E \to \bigoplus_{\sigma \in \Sigma} E_\sigma$ be the E algebra map induced by φ. Note that φ is the map which defines the M algebra structure on $\bigoplus_{\sigma \in \Sigma} E_\sigma$. This implies that Ψ is also an M algebra map.

LEMMA 2. *Let E be an extension of N. Then*

1. *Ψ is an isomorphism.*
2. *$A \otimes_K E \approx \bigoplus_{\sigma \in \Sigma} A \otimes_M E_\sigma$. This is the unique expression of $A \otimes_K E$ as a direct sum of local rings.*

Proof. 1. This fact is well known so we only sketch the proof. Since N is normal over K, the number of elements in Σ is the degree $[M:K]$. Thus $M \otimes_K E$ and $\bigoplus_{\sigma \in \Sigma} E_\sigma$ have the same dimension over E. Moreover Ψ is surjective by the independence of characters theorem. Hence Ψ is an isomorphism.

2. $A \otimes_K E = A \otimes_M (M \otimes_K E) \approx A \otimes_M (\bigoplus_{\sigma \in \Sigma} E_\sigma) = \bigoplus_{\sigma \in \Sigma} (A \otimes_M E_\sigma)$. The last fact follows from Lemma 1 and the fact that an expression as a direct sum of local rings is always unique.

To apply Lemma 2 to the proof of Theorem 4, we must be able to compare the structure of $A \otimes_M E$ to that of $A \otimes_M E_\sigma$ for $\sigma \in \Sigma$ with $\sigma \neq 1$. We can do this when E is an extension of N such that the condition $(*)$ given below holds

$(*)$ Every K automorphism τ of N extends to an automorphism θ of E.

Note that $(*)$ holds if E is algebraically closed.

Lemma 3. *Let E be an extension of N satisfying* $(*)$. *Then the following conditions are equivalent*:

1. *$A \otimes_K E$ is a direct sum of special STP algebras over E.*
2. *For all $\sigma \in \Sigma$, $A \otimes_M E_\sigma$ is a special STP algebra over E.*
3. *$A \otimes_M E$ is a special STP algebra over E.*

Proof. From Lemma 2 it is clear that $1 \Leftrightarrow 2$ while $2 \Rightarrow 3$ is trivial. Thus we must show $3 \Rightarrow 2$. Let $\sigma \in \Sigma$. Then since N is normal over K we can extend σ to an automorphism τ of N. Using $(*)$, we can then extend τ to an automorphism θ of E.

$$\begin{tikzcd}
E \arrow[rr, "\theta"] & & E \\
N \arrow[u] \arrow[rr, "\tau"] & & N \arrow[u] \\
& M \arrow[ul, "1"] \arrow[ur, "\sigma"'] &
\end{tikzcd}$$

Clearly we can view θ as an M algebra isomorphism of E with E_σ. Thus θ extends to an isomorphism $1 \otimes \theta \colon A \otimes_M E \to A \otimes_M E_\sigma$. This is enough to show that if $A \otimes_M E$ is a special STP algebra over E then so is $A \otimes_M E_\sigma$.

We are now ready for the

Proof of Theorem 4. If an algebra splits over some field F then it splits over all extensions E of F. Thus, to test splitting properties, it is enough to use fields E which contain N and which satisfy $(*)$. Then $1 \Leftrightarrow 3$ of Lemma 3 implies the theorem.

Using Theorems 2 and 4, we can now characterize splittable algebras in general:

Theorem 5. *The following conditions are equivalent*:

1. *A is splittable over K.*
2. *For all minimal idempotents α, $A \cdot \alpha$ is a special algebra over the field $M \cdot \alpha$.*

Proof. Let J be the set of minimal idempotents. Then consider two additional conditions:

3. For all $\alpha \in J$, $A \cdot \alpha$ is strongly splittable over the field $M \cdot \alpha$.
4. For all $\alpha \in J$, $A \cdot \alpha$ is splittable over K.

Then

$2 \Leftrightarrow 3$ follows from Theorem 2.

$3 \Leftrightarrow 4$ follows from Theorem 4.

$4 \Leftrightarrow 1$ follows from $A = \bigoplus_{\alpha \in J} A \cdot \alpha$.

As a consequence of our theory, we also obtain

Theorem 6. *If A is a field extension of K, then A is splittable over K.*

Proof. By Lemma 1, A is purely inseparable over M so, by the theory of Chapter 1, A is strongly splittable over M. Then, by Theorem 4, A is splittable over K.

We conclude by defining the splitting field $S(A/K)$ of A over K when A is splittable. We first study the case when A is local. As in the discussion of Theorem 4, we let

M = the maximal separable subfield of A.

C = any algebraically closed field which contains M.

N = the least normal extension of K in C which contains M.

Σ = the set of all K isomorphisms of M into N.

By Lemma 2, we have a decomposition

$$A \otimes_K N \approx \bigoplus_{\sigma\in\Sigma} A \otimes_M N_\sigma. \tag{1}$$

We set $A_\sigma = A \otimes_M N_\sigma$ and we view A_σ as an N algebra. Suppose E is an extension of N. Then we have

$$A_\sigma \otimes_N E = (A \otimes_M N_\sigma) \otimes_N E = A \otimes_M E_\sigma.$$

Thus, if E is an extension of N, we have a decomposition

$$A \otimes_K E \approx \bigoplus_{\sigma\in\Sigma} A_\sigma \otimes_N E. \tag{2}$$

This decomposition shows that we must study the N algebras A_σ for $\sigma \in \Sigma$. First note that since A is splittable over K we have from Theorems 4 and 2 that A is special over M. Let $x_1, \dots, x_r$ be an NGS for A over M and let $a_{i,\alpha} \in M$ be the structure constants in the defining relations for $x_1, \dots, x_r$. The structure equations then have the usual form:

$$x_i^{q_i} = \sum_{\alpha\in I_i} a_{i,\alpha} x^{q_i\alpha}. \tag{3}$$

We set $d_{i,\alpha} = \sqrt[q_i]{a_{i,\alpha}}$ so that $S(A/M) = M[d_{i,\alpha}]$, $1 \leqq i \leqq r$ and $\alpha \in I_i$. Since $S(A/M)$ is purely inseparable over M, each $\sigma \in \Sigma$ has a unique extension from M to an isomorphism of $S(A/M)$ into C which we will also denote by σ. In this way we identify Σ with the set of all K isomorphisms of $S(A/M)$ into C.

Lemma 4. *Let $\sigma \in \Sigma$. Then*

1. *A_σ is a special N algebra.*

2. *The sequence $x_1 \otimes 1, \dots, x_r \otimes 1$ in A_σ is an NGS of A_σ over N and the structure equations for this NGS are*

$$(x_i \otimes 1)^{q_i} = \sum_{\alpha\in I_i} \sigma(a_{i,\alpha}) \cdot (x \otimes 1)^{q_i\alpha}. \tag{4}$$

In particular, the structure constants relative to this NGS are just the elements $\sigma(a_{i,\alpha}) \in N$ for $1 \leqq i \leqq r$ and $\alpha \in I_i$.

3. $S(A_\sigma/N) = N \cdot \sigma(S(A/M))$.

Proof. The equations (4) follow from the equations (3) and the fact that A_σ is defined as $A \otimes_M N_\sigma$. From the equations (4), we obtain the rest of assertions 1 and 2. To get assertion 3, first note that $\sigma(d_{i,\alpha}) = \sqrt[q_i]{\sigma(a_{i,\alpha})}$. Thus

$$S(A_\sigma/N) = N[\sigma(d_{i,\alpha})] = N\cdot\sigma(S(A/M)).$$

We are done.

We now define the splitting field $S(A/K)$ to be the composite of the fields $S(A_\sigma/N)$ for $\sigma\in\Sigma$.

THEOREM 7. *Let A be local and splittable over K and let E be an extension of K. Then the following conditions are equivalent*:

1. *E splits A over K, that is, $A\otimes_K E$ is a direct sum of special STP algebras over E.*
2. *$A\otimes_K E$ is a subalgebra of a direct sum of STP algebras over E.*
3. *$S(A/K)\subseteq E$.*

Proof. We may assume by choosing C large enough that $E\subseteq C$. Then, if any of the three conditions hold, $M\otimes_K E$ is a direct sum of copies of E so that E splits M and we have $N\subseteq E$. Thus we have the decomposition (2). The equivalence proof is now easy:

1 ⇒ 2. Trivial.

2 ⇒ 3. If 2 holds, then for all $\sigma\in\Sigma$ we have that $A_\sigma\otimes_N E$ is a subalgebra of a direct sum of STP algebras over E. Thus, by Theorem 1, $S(A_\sigma/N)\subseteq E$ for all $\sigma\in\Sigma$, that is, $S(A/K)\subseteq E$.

3 ⇒ 1. If 3 holds, then for all $\sigma\in\Sigma$ we have $S(A_\sigma/N)\subseteq E$ so that $A_\sigma\otimes_N E$ is a special STP algebra over E. Thus we have 1.

We now give a new way to define $S(A/K)$.

THEOREM 8. *Let A be local and splittable over K. Then $S(A/K)$ is the least normal extension of K in C which contains $S(A/M)$.*

Proof. Let T denote the least normal extension of K in C which contains $S(A/M)$. Since $M\subseteq S(A/M)$ we see that $N\subseteq T$. Since Σ is the set of all K isomorphisms of $S(A/M)$ into C we also have

$$T = \text{composite of the fields } \sigma(S(A/M)) \text{ for } \sigma\in\Sigma.$$

Thus

$$T = \text{composite of the fields } N\cdot\sigma(S(A/M)) \text{ for } \sigma\in\Sigma.$$

Hence by Lemma 4

$$\begin{aligned} T &= \text{composite of the fields } S(A_\sigma/N) \text{ for } \sigma\in\Sigma \\ &= S(A/K). \end{aligned}$$

We are done.

We now pass to the general situation when A is any splittable K algebra. We let J be the set of minimal idempotents of A. Then we have as usual:

$$A = \bigoplus_{\alpha\in J} A\cdot\alpha.$$

Here, for all $\alpha \in J$, $A \cdot \alpha$ is local. Thus we are led to define

$$S(A/K) = \text{composite of the fields } S(A \cdot \alpha/K) \text{ for } \alpha \in J.$$

REMARK 1. Theorem 7 is true for any splittable K algebra. As a consequence we have

COROLLARY 1. *The following conditions are equivalent for any K algebra A:*

1. *A is splittable over K.*
2. *$A \otimes_K C$ is a direct sum of special STP algebras over C.*

Proof. $2 \Rightarrow 1$ is clear and $1 \Rightarrow 2$ follows from $S(A/K) \subseteq C$.

As a special case of Theorem 7 we have

COROLLARY 2. *Let A be splittable over K and assume that A is a subalgebra of a direct sum of STP algebras over K. Then A is a direct sum of special STP algebras over K.*

REMARK 2. Theorem 8 generalizes to

THEOREM 8*. *Let A be splittable over K, let M be the maximal separable K subalgebra of A, and let J be the set of minimal idempotents in A. Then $S(A/K)$ is the least normal extension of K in C which contains all of the fields $S(A \cdot \alpha/M \cdot \alpha)$ for $\alpha \in J$.*

As a consequence we have

COROLLARY. *If A is splittable over K, then $S(A/K)$ is normal over K.*

3. **Special sequences.** In this section, we study how generators can be chosen in a special STP algebra.

Let E be a field of characteristic p and $F = E[u_1, \ldots, u_r]$ be a special STP algebra over E of type $q = (q_1, \ldots, q_r)$ where

$$u_i^{q_i} = 0, \qquad q_i = p^{e_i}, \qquad e_1 \geqq \cdots \geqq e_r \geqq 1.$$

Let $M = (u_1, \ldots, u_r)$ be the maximal ideal of F. Then $F = E \oplus M$ and we let $\tau: F \to M$ be the projection map.

Let $1 \leqq s \leqq r$ and $x_1, \ldots, x_s \in F$. We say that $x_1, \ldots, x_s$ is a special sequence relative to $u_1, \ldots, u_r$ if for $1 \leqq i \leqq s$

$$F = E[x_1, \ldots, x_i, u_{i+1}, \ldots, u_r].$$

We motivate this definition by the following example:

EXAMPLE. Let A be a special K algebra with $x_1, \ldots, x_r$ an NGS for A over K of type q. Let $S(A/K) \subseteq E$ and set $F = A \otimes_K E$. Define $u_1, \ldots, u_r$ as in §1. Then $x_1, \ldots, x_r$ is a special sequence relative to $u_1, \ldots, u_r$, since in this case for $1 \leqq i \leqq r$

$$E[x_1, \ldots, x_i] = E[u_1, \ldots, u_i].$$

To study special sequences, we will need some notation. For $1 \leqq i \leqq r$ let

1. J_i be the set of all $\alpha = (\alpha_1, \ldots, \alpha_r)$ such that
   for $1 \leqq k \leqq i$, $0 \leqq \alpha_k < q_k$,
   for $i < k \leqq r$, $\alpha_k = 0$.
2. $\bar{J}_i$ be the set of all $\beta = (\beta_1, \ldots, \beta_r)$ such that
   for $1 \leqq k \leqq i$, $\beta_k = 0$,
   for $i < k \leqq r$, $0 \leqq \beta_k < q_k$.
3. $I_i = \{\alpha : q_i\alpha \in J_{i-1}\}$.

Proposition 1. *Let $x_1, \ldots, x_s$ be a special sequence relative to $u_1, \ldots, u_r$ and let $E_i = E[x_1, \ldots, x_i]$. Then, for $1 \leqq i \leqq s$,*

1. $x_i^{q_i} \in E^{q_i}[x_1^{q_i}, \ldots, x_{i-1}^{q_i}]$.
2. $\dim_E E_i = q_1 \cdot \cdots \cdot q_i$.
3. *The set $\{x^\alpha\}$ for $\alpha \in J_i$ is a basis of E_i over E.*
4. *The set $\{u^\beta\}$ for $\beta \in \bar{J}_i$ is a basis of F over E_i.*
5. *The set $\{x^\alpha u^\beta\}$ for $\alpha \in J_i$ and $\beta \in \bar{J}_i$ is a basis of F over E.*
6. *There exist unique constants $a_{i,\alpha} \in E^{q_i}$ for $\alpha \in I_i$ such that $x_i^{q_i} = \sum_{\alpha \in I_i} a_{i,\alpha} x^{q_i \alpha}$.*

Proof. From our assumption that $x_1, \ldots, x_s$ is a special sequence relative to $u_1, \ldots, u_r$, we obtain for $0 \leqq i \leqq s$

$$F = E_i[u_{i+1}, \ldots, u_r].$$

Thus, F is generated as a module over E_i by $\{u^\beta\}$ for $\beta \in \bar{J}_i$ and this set has $q_{i+1} \cdot \cdots \cdot q_r$ elements. Since $\dim_E F = q_1 \cdot \cdots \cdot q_r$, we have

A. $\dim_E E_i \geqq q_1 \cdot \cdots \cdot q_i$.

B. $\dim_E E_i = q_1 \cdot \cdots \cdot q_i \Leftrightarrow \{u^\beta\}$ for $\beta \in \bar{J}_i$ is a basis of F over E_i.

With this, we are ready to prove our assertions:

1. Let $j = i-1$. Then $F = E_j[u_i, \ldots, u_r]$ so that $x_i = \sum b_\beta u^\beta$ with $b_\beta \in E_j$ for $\beta \in \bar{J}_j$. On taking q_ith powers we obtain

$$x_i^{q_i} = \sum b_\beta^{q_i} u^{q_i \beta} = b_0^{q_i}.$$

Thus $x_i^{q_i} \in E_j^{q_i} = E^{q_i}[x_1^{q_i}, \ldots, x_{i-1}^{q_i}]$.

2. By 1, we have that, for $1 \leqq k \leqq i$, $\dim_E E_k \leqq q_k \cdot \dim_E E_{k-1}$. Thus we get $\dim_E E_i \leqq q_1 \cdot \cdots \cdot q_i$ so that, by A, we obtain 2.

3. The set $\{x^\alpha\}$ for $\alpha \in J_i$ generates E_i as a vector space over E, by 1, and this set has $q_1 \cdot \cdots \cdot q_i$ elements. Then from 2 we get 3.

4. Use 2 and B.

5. Use 3 and 4.

6. Use 1 and 5.

Proposition 2. *If $x_1, \ldots, x_r$ is a special sequence relative to $u_1, \ldots, u_r$ then $x_1, \ldots, x_r$ is a normal generating sequence of F over E.*

Proof. Use 6 of Proposition 1.

PROPOSITION 3. *Let $x_1, \ldots, x_s \in F$ with $s<r$. Let X generate F over E. Assume*

$$F = E[x_1, \ldots, x_s, u_{s+1}, \ldots, u_r].$$

Then for some $x_{s+1} \in X$

$$F = E[x_1, \ldots, x_{s+1}, u_{s+2}, \ldots, u_r].$$

Proof. Set $y_i = \tau x_i \in M$ and $z_i = x_i - \tau x_i \in E$. Since $x_i = z_i + y_i$ and $z_i \in E$, our assumption yields

$$F = E[y_1, \ldots, y_s, u_{s+1}, \ldots, u_r].$$

Now M/M^2 has dimension r over E so $y_1, \ldots, y_s, u_{s+1}, \ldots, u_r$ must be a basis of M mod M^2. Delete u_{s+1} from this list and consider the set $Y = \{\tau x : x \in X\}$. Since X generates F over E as an algebra, Y generates M mod M^2 as a vector space over E. Thus we can find $y_{s+1} \in Y$ such that $y_1, \ldots, y_s, y_{s+1}, u_{s+2}, \ldots, u_r$ forms a basis of M mod M^2 over E. Then any $x_{s+1} \in X$ such that $\tau x_{s+1} = y_{s+1}$ will have the required property.

PROPOSITION 4. *Let X generate F over E. Then there exist $x_i \in X$ for $1 \leqq i \leqq r$ such that $x_1, \ldots, x_r$ is a special sequence relative to $u_1, \ldots, u_r$.*

Proof. Use Proposition 3.

4. **Splitting revisited.** Using Proposition 4 of §3, we will now show Theorem 2 of §1. Recall that we must show that for any K algebra A the following conditions are equivalent:

1. A is strongly splittable over K.
2. A is special over K.

From §1, we know that 2 ⇒ 1. To show 1 ⇒ 2, we must show that if condition 1 holds then A has a normal generating sequence. We can show even more:

THEOREM 9. *Let A be a strongly splittable K algebra and let X be a subset of A which generates A over K. Then there exists an NGS $x_1, \ldots, x_r$ of A over K such that, for all i, $x_i \in X$.*

Proof. We let E be an extension of K such that $F = A \otimes_K E$ is a special STP algebra over E and we use the notation of §3. We view A as within F via the map $a \mapsto a \otimes 1$. Then X generates F over E so, by Proposition 4, we can choose $x_i \in X$ such that $x_1, \ldots, x_r$ is a special sequence relative to $u_1, \ldots, u_r$. Then, by Proposition 2, $x_1, \ldots, x_r$ is an NGS of F over E. We claim that $x_1, \ldots, x_r$ is also an NGS of A over K. To prove the claim we need a simple lemma about tensor products which we state without proof.

LEMMA 5. *Let A and E be K algebras and let $F = A \otimes_K E$. View F as an algebra over E. Let S be a subset of A. Let $K[S]$ and $E[S]$ be the rings generated by S over K and E respectively. Then if $a \in A$, $a \in K[S] \Leftrightarrow a \in E[S]$.*

From the fact that $x_1, \dots, x_r$ is an NGS for F over E we obtain two conditions

$$F = E[x_1, \dots, x_r], \qquad x_i^{q_i} \in E[x_1^{q_i}, \dots, x_{i-1}^{q_i}], \qquad 1 \leqq i \leqq r.$$

Using Lemma 5, we obtain

$$A = K[x_1, \dots, x_r], \qquad x_i^{q_i} \in K[x_1^{q_i}, \dots, x_{i-1}^{q_i}], \qquad 1 \leqq i \leqq r.$$

These conditions imply that $x_1, \dots, x_r$ is an NGS for A over K.

As an illustration of how Theorem 9 can be used, we show

THEOREM 10. *Let R and S be K algebras and let $A = R \otimes_K S$. Then the following conditions are equivalent*:

1. *A is strongly splittable over K.*
2. *R and S are strongly splittable over K.*

Proof. 2 ⇒ 1. This follows from $A \otimes_K E = (R \otimes_K E) \otimes_E (S \otimes_K E)$ and the fact that the tensor product of two special STP algebras is a special STP algebra.

1 ⇒ 2. Let $X = R \cup S$. Then X generates A over K and so, by Theorem 9, we can choose an NGS $x_1, \dots, x_r$ of A over K with $x_i \in X$. Now let $y_1, \dots, y_s$ and $z_1, \dots, z_t$ be the subsequences of $x_1, \dots, x_r$ which lie in R and S respectively. Then, by an argument similar to that in Theorem 9, one checks that $y_1, \dots, y_s$ is an NGS for R over K and $z_1, \dots, z_t$ is an NGS for S over K. Thus R and S are special over K and hence strongly splittable over K.

In the same direction, we also have

THEOREM 11. *Let R and S be K algebras and let $A = R \otimes_K S$. Then the following conditions are equivalent*:

1. *A is splittable over K.*
2. *R and S are splittable over K.*

Proof. By Corollary 1 of Theorem 7 (cf. Remark 1 of §2), we can reduce to the case when K is algebraically closed. Then we can reduce to the case when R and S are local. We then apply Theorem 10.

As a consequence of Theorems 10 and 11, we have

COROLLARY. *Let R and S be K algebras and let $A = R \otimes_K S$. Then the following conditions are equivalent*:

1. *A is a (direct sum of) special STP algebra(s) over K.*
2. *R and S are both (direct sums of) special STP algebras over K.*

5. **Remarks on elementary extensions.** Let L be a finite field extension of K. Then L is splittable over K by Theorem 6. Taking a hint from Theorem 4 of Chapter 1, we say that L is elementary over K if $L = S(L/K)$. Let M be the maximal separable extension of K in L. We now relate the conditions "L is elementary over K" and "L is elementary over M".

THEOREM 12. *The following conditions are equivalent*:

1. *L is elementary over K.*
2. *L is elementary over M and L is normal over K.*

Proof. By Theorem 4 of Chapter 1, L is elementary over M if and only if $L=S(L/M)$. Also, by Theorem 8, the least normal extension of K which contains $S(L/M)$ is precisely $S(L/K)$. Thus

$$L = S(L/K) \Leftrightarrow L = S(L/M) \text{ and } L \text{ is normal over } K.$$

This equivalence is just what we wish to prove.

6. **Remarks on group schemes.** If X is an affine scheme over K, we let $\Gamma(X)$ denote the ring of functions of X, that is, $X=\operatorname{Spec}(A)$ with $A=\Gamma(X)$. We will interpret a well-known fact about group schemes in the language of our splitting theory.

THEOREM 13. *Let G be a finite commutative affine group scheme over K and let $A=\Gamma(G)$. Then A is splittable over K.*

Proof. By Corollary 1 to Theorem 7, we can reduce to the case when K is algebraically closed. Then, by [4, Exposé 11, 4.2], $G=G_s\times G_u$ where G_s is the multiplicative part of G and G_u the unipotent part of G. Now, if $A_s=\Gamma(G_s)$ and $A_u=\Gamma(G_u)$, then $A=A_s\otimes_K A_u$. Thus, by Theorem 11, we need only consider two cases:

Case 1. $G=G_s$. Then $A=A_s$ is a separable algebra over K, hence, splittable.

Case 2. $G=G_u$. Then $A=A_u$ is strongly splittable by [2, p. 152].

By Theorem 13 and the earlier results on splitting, we know the algebraic structure of the ring of functions of any finite commutative affine group scheme. Hopefully, this result will be useful in the study of the structure of group schemes over base fields which are not perfect.

7. **Remarks on automorphism schemes.** If R is a ring of characteristic p and S is a special STP algebra over R, then it is easy to describe the automorphisms of S as an R algebra. This calculation can be used in the following situation:

A is strongly splittable over K,
$S(A/K)\subseteq R$,
$S=A\otimes_K R$.

One gets in this way a strong hold on the automorphism scheme of A over K. In a recent paper [1], Mlle. Bégueri uses this idea to study the automorphism scheme of a purely inseparable extension. We describe one of her results.

Let $K\subseteq L\subseteq M$ be a tower of purely inseparable extensions. We define the automorphism scheme $G_{M/L/K}$ by giving the points of $G_{M/L/K}$ with values in a K algebra R:

$$G_{M/L/K}(R) = \text{automorphisms of } M\otimes_K R \text{ which fix } L\otimes_K R.$$

If $z \in M$, we say that z is invariant under $G_{M/L/K}$ if for all K algebras R the element $z \otimes 1$ in $M \otimes_K R$ is fixed by $G_{M/L/K}(R)$. We set

$$I_{M/L/K} = \{z \in M : z \text{ is invariant under } G_{M/L/K}\}.$$

Then $I_{M/L/K}$ is a field and $L \subseteq I_{M/L/K} \subseteq M$. Proposition 14 of [1] then says

PROPOSITION. *The following conditions are equivalent:*

1. $L = I_{M/L/K}$.
2. *For all* $q = p^e$, $M^q \cdot K$ *and* L *are linearly disjoint over* $M^q \cdot K \cap L$.

REMARK 1. If $K = L$ then condition 2 trivially holds.

REMARK 2. Let $h = h(M/L)$. Then, for $e \geqq h$, $M^q \cdot K \subseteq L$, so condition 2 holds. Thus we may assume $e < h$ in testing condition 2. Suppose for $e < h$ it happens that $K \subseteq M^q$. Then condition 2 becomes

For all $e < h$ and $q = p^e$, M^q and L are linearly disjoint over $M^q \cap L$.

By Theorem 4 of Chapter 1, this condition amounts to saying that M is elementary over L.

These remarks show how to find a tower $K \subseteq L \subseteq M$ such that $L \neq I_{M/L/K}$. Indeed

1. Let L be a field of characteristic p which admits extensions M which are purely inseparable and nonelementary and assume that the absolute exponent e_L of L is finite.

2. Take M to be any nonelementary purely inseparable extension of L.

3. Let $h = h(M/L)$ and let K be any subfield of $L \cap M^{h-1}$ such that $[L:K] < \infty$. For example let $K = L^{h-1}$. Then $K \subseteq L \subseteq M$ is a tower such that $L \neq I_{M/L/K}$.

In particular, the hope that every intermediate field L of a purely inseparable extension M/K could be gotten as the field of invariants of its automorphism scheme is destroyed.

8. **On special algebras which are not split.** Let A be a special K algebra, let $x_1, \ldots, x_r$ be an NGS for A/K, let $a_{i,\alpha} \in K$ be the structure constants for A/K relative to the NGS $x_1, \ldots, x_r$, and write the structure equations in the usual way:

$$x_i^{q_i} = \sum_{\alpha \in I_i} a_{i,\alpha} x^{q_i \alpha}.$$

Until now, our main concern has been to examine the splitting of A. We will now consider the question: When is A a field? We will be able to answer this question using the mixed Jacobians of Zariski [6].

We begin by noting that A is an artin local ring and that if we let m denote its maximal ideal and $L = A/m$ then L is a purely inseparable extension of K. This follows from Lemma 1 of §2 since in our case $M = K$ and we can take $E = K$. Now, we want to know when A is a field, that is, when $m = 0$. By Nakayama's Lemma

$$m = 0 \Leftrightarrow m/m^2 = 0 \Leftrightarrow \dim_L (m/m^2) = 0.$$

Our aim is therefore to test when $\dim_L (m/m^2)=0$. Now, from the defining relations for A, we can construct a matrix J called the mixed Jacobian such that J has coefficients in L and

$$\operatorname{rank}(J)+\dim_L (m/m^2) = r.$$

Thus we have

THEOREM 14. *The following conditions are equivalent*:
1. *A is a field.*
2. *The mixed Jacobian J of A has rank r.*

We now review how to construct J. First, if $P \in K[X_1, \ldots, X_r]$ and $D\colon K \to K$ is a derivation, let DP denote the polynomial gotten from P by applying D to the coefficients of P and leaving the X_i fixed. Next define

$$P_i(X_1, \ldots, X_i) = X_i^{q_i} - \sum_{\alpha \in I_i} a_{i,\alpha} X^{q_i \alpha}.$$

Also, fix a set $\{D_\mu\}_{\mu \in M}$ of derivations which generate the vector space of all derivations of K to K and let z_i be the image of x_i in L. Then one can take as the matrix J

$$(1) \qquad J = |D_\mu P_i(z_1, \ldots, z_i)|_{\mu \in M, 1 \leqq i \leqq r}.$$

We remark that in Zariski's general situation one must also have in J expressions involving derivations of the variables X_i. This is unnecessary in our case since all variables appear with powers of p in the polynomials P_i. We now make some further remarks:

REMARK 1. $D_\mu P_i(z_1, \ldots, z_i) = -\sum_{\alpha \in I_i} (D_\mu a_{i,\alpha}) z^{q_i \alpha}$.

REMARK 2. To apply Theorem 14 to show that A is a field ($2 \Rightarrow 1$) it is enough to find some set M of derivations of K to K such that the matrix J defined by (1) has rank r.

APPLICATION. We can use Theorem 14 to simplify the discussion of the fields L_n in Chapter 1, §8. By induction on n, we define a special K algebra $A_n = K[x_{0,n}, \ldots, x_{n,n}]$ by using (0), (1), and (2) of Chapter 1, §8, as the defining relations. Of course, L_n is residue field of A_n modulo the maximal ideal of A_n. The issue in Facts 3 and 4 is essentially that $A_n = L_n$, that is, that A_n is a field. We will now show this using Theorem 14. By induction, we first show

Fact. For $0 \leqq k \leqq n$,

$$x_{k,n}^{p^{n+1}} \in P(y_{i,j})_{0 \leqq i \leqq j \leqq n}.$$

Next we write down the polynomials P_k corresponding to $x_{k,n}$ for $0 \leqq k \leqq n$:

$$P_0(X_0) = X_0^{p^{n+1}} - y_{0,n},$$
$$P_k(X_0, \ldots, X_k) = X_k^{p^n} - y_{k,n} - (x_{k-1,n-1})^{p^n} \cdot X_0^{p^n} \quad \text{if } k \geqq 1.$$

Note that from the above fact, the coefficient $(x_{k-1,n-1})^{p^n}$ lies in the field $P(y_{i,j})$ for $0 \leqq i \leqq j < n$. Now define a derivation D_μ by

$$\begin{aligned} D_\mu(y_{i,j}) &= 1 \quad \text{if } i = \mu \text{ and } j = n, \\ &= 0 \quad \text{otherwise,} \\ D_\mu &= 0 \quad \text{on } P. \end{aligned}$$

In particular

$$D_\mu((x_{k-1,n-1})^{p^n}) = 0.$$

It follows that the polynomials $D_\mu P_k$ are constant, namely

$$\begin{aligned} D_\mu P_k &= -1 \quad \text{if } \mu = k, \\ &= 0 \quad \text{if } \mu \neq k. \end{aligned}$$

Hence the mixed Jacobian matrix formed from $P_0, \ldots, P_n$ and $D_0, \ldots, D_n$ is simply the negative of the identity matrix. Its rank is $n+1=r$ so we conclude that A_n is a field.

Bibliography

1. L. Bégueri, *Schéma d'automorphismes. Application a l'étude d'extensions finies radicielles*, Bull. Sci. Math. (2) **93** (1965), 89–111.

2. M. Demazure and A. Grothendieck, *Schémas en groupes*, fasc. 2b, Séminaire Géométrie Algébrique, Inst. Hautes Études Sci., Paris, 1965. MR **34** #7519.

3. G. Pickert, *Eine Normalform für endliche rein-inseparable Körpererweiterungen*, Math. Z **53** (1950), 133–135. MR **12**, 316.

4. *Séminaire Heidelberg-Strasbourg*, Groupes Algébriques, 1965/66.

5. M. E. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410; corrigendum, ibid. (2) **89** (1969), 206–207. MR **36** #6391; MR **38** #4451.

6. O. Zariski, *The concept of a simple point of an abstract algebraic variety*, Trans. Amer. Math. Soc. **62** (1947), 1–52. MR **9**, 99. See also: *Séminaire H. Cartan et C. Chevalley* 1955/56, Géométrie Algébrique, Secrétariat mathématique, Paris, 1956. MR **20** #3871.

Northeastern University, Boston, Massachusetts 02115