Chains of minimal generating sets in inseparable fields

Werner William Shoultz

Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/rtd
Part of the Mathematics Commons

Recommended Citation
Shoultz, Werner William, "Chains of minimal generating sets in inseparable fields " (1968). Retrospective Theses and Dissertations. 3514. https://lib.dr.iastate.edu/rtd/3514

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
SHOULTZ, Werner William, 1936-  
CHAINS OF MINIMAL GENERATING SETS OF  
INSEPARABLE Felds.  
Iowa State University, Ph.D., 1968  
Mathematics  

University Microfilms, Inc., Ann Arbor, Michigan
CHAINS OF MINIMAL GENERATING SETS OF INSEPARABLE FIELDS

by

Werner William Shoultz

A Dissertation Submitted to the
Graduate Faculty in Partial Fulfillment of
The Requirements for the Degree of
DOCTOR OF PHILOSOPHY

Major Subject: Mathematics

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

Head of Major Department

Signature was redacted for privacy.

Dean of Graduate College

Iowa State University
Of Science and Technology
Ames, Iowa

1968
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. RELATIVE CANONICAL CHAINS APPLIED TO ARBITRARY EXTENSIONS</td>
<td>4</td>
</tr>
<tr>
<td>III. THE RELATIVE CANONICAL CHAIN APPLIED TO PURELY INSEPARABLE EXTENSIONS</td>
<td>18</td>
</tr>
<tr>
<td>IV. EXAMPLE</td>
<td>39</td>
</tr>
<tr>
<td>V. REFERENCES</td>
<td>41</td>
</tr>
<tr>
<td>VI. ACKNOWLEDGMENTS</td>
<td>42</td>
</tr>
</tbody>
</table>
I. INTRODUCTION

In this dissertation all fields are of characteristic $p$, a prime number. When we are studying the properties of a field $L$ relative to a subfield $K$, we will use the symbol $L|K$.

$L|K$ is called a separable extension if and only if $L|K$ preserves $p$-independence. This property is equivalent to $L \otimes K^{1/p}$ being a field.

If $L$ is any field extension of $K$, then there is a not necessarily unique intermediate field $F|K$, which is separable, such that if $B$ is a relative $p$-base for $F|K$, then $F|K(B)$ is separable and relatively perfect, and $L|F$ is purely inseparable [1]. In the tower $L \supset F \supset K(B) \supset K$, the most difficult structure occurs between $F$ and $K(B)$ when $F$ is transcendental. This dissertation will deal mainly with the structure of $L$ over $F$.

In 1949 Gunter Pickert [7] published an extensive paper on inseparable field extensions. One of his principal theorems on finite degree extensions may be stated as follows: If $F|K$ is purely inseparable of finite multiplicity $m$, then there is an ordering of the
generators, namely \(a_1, a_2, \ldots, a_m\), so that the following
conditions hold for \(i = 1, \ldots, m\):

I. \(a_i = a_i \in K(a_1, \ldots, a_{i-1})\), where \(q_i = p^{e_i}\) and
   \(e_i > 0\).

II. \(a_i^{p-1} \in K(a_1, \ldots, a_{i-1})\).

III. \(c_1 \geq c_2 \geq \cdots \geq c_m\).

Conversely, if \(L|K\) is generated by the \(m\) elements
\(a_1, \ldots, a_m\), satisfying the first two conditions above, then
the exponents \(e_1, \ldots, e_m\) are invariants of the extension.

In 1950, Pickert [6] gave an improved proof of the above
theorem using the invariant chain of fields.

\[
L \supseteq K(L^p) \supseteq K(L^{p^2}) \supseteq \cdots .
\]

This chain was used by Dieudonné [1] to analyze general
separable extensions and to improve investigations of
Saunders MacLane [5].

Chapter II of this dissertation applies this chain with
the only restriction on \(L\) and \(K\) being that they are of
characteristic \(p\). A very general set of numerical
invariants is derived.

In Chapter III we first apply the results of Chapter II
to the case where \( L \mid K \) is purely inseparable and each field
\[ K(L^P) \mid K \] has an m.g.s. \[ M^P \]. As a consequence we derive
not only the known bounded exponent case (which is a
generalization of Pickert's and is due to Hamann and Mordeson
[3]), but also certain unpublished unbounded cases due to
Vinogradov and Mordeson. In addition, we construct classes of
fields of unbounded exponent to which the theory applies,
generalize several finite exponent results and discuss the
relation between relative \( p \)-bases and minimal generating
sets.
II. RELATIVE CANONICAL CHAINS APPLIED TO ARBITRARY EXTENSIONS

A. Preliminary Considerations

$L|K$ is called a purely inseparable extension if for every element $a$ of $L$ there is a least non-negative integer $c_a$ such that $a^{p^{c_a}}$ is in $K$. We will denote by $M^{p_i}$ the set of the elements of $M$ raised to the $p^i$-th power, where $M$ is a subset of $L$. If there is a least integer $e$ such that $L^{p^e} \subseteq K$, $L|K$ is said to be of finite exponent $e$.

For an arbitrary extension $L|K$, if $X$ is a subset of $L$ such that for all $x \in X$, $x \in L^p(X - x)$, where $X - x = X \setminus \{x\}$, $X$ is called $p$-independent (in $L$). If in addition, $L = L^p(X)$, $X$ is called a $p$-base. If $Y$ is a subset of $L$ such that for all $y \in Y$, $y \in K(L^p)(Y - y)$, $Y$ is called relatively $p$-independent (in $L|K$). If $L = K(L^p)(Y)$, then $Y$ is called a relative $p$-base for $L|K$. A set $M$ is said to be a minimal generating set or simply an m.g.s. for $L|K$ if $L = K(M)$ and for any $m \in M$, $m \in K(M - m)$. It can be shown [9] that $p$-bases and relative $p$-bases for $L|K$ always exist and the cardinalities of each
are invariants for $L|K$.

We will use $F(X,x)$ to denote the field obtained by the adjunction of the set $X \cup \{x\}$ to a field $F$. If $y$ is an element of $L$ such that $y \in K(L^p)(X,x)$ but $y \notin K(L^p)(X)$, then $x \notin K(L^p)(X,y)$. This critical property is called "the exchange property". The exchange property also holds as follows: if $y$ is an element of $L$ such that $y \in L^p(X,x)$ but $y \notin L^p(X)$, then $x \in L^p(X,y)$. We note that if $y \in K(X,x)$ but $y \notin K(X)$, we can not conclude that $x \in K(X,y)$.

We say that a set $X$ generates $F|G$ if $F = G(X)$. A simple application of Zorn's lemma shows that if $X$ is a relatively $p$-independent set for $L|K$ and $X \cup Y$ generates $L|K(L^p)$, then there is a subset $Y'$ of $Y$ such that $X \cup Y'$ is a relative $p$-base for $L|K$. This is true in particular when $X = \emptyset$.

For any extension $L|K$ and a chain of subsets of $L$,

$$M_0 \supseteq M_1 \supseteq \cdots \supseteq M_i \supseteq M_{i+1} \supseteq \cdots,$$

such that $M_i^p$ is a relative $p$-base for $K(L^p)|K$, we define the ordered set
\[ \mathcal{N}(L|K) = \{ M_0, M_1, M_2, \ldots \} \]

and call \( \mathcal{N}(L|K) \) a relative canonical chain for \( L|K \).

From the ordered set \( \mathcal{N}(L|K) \) we define the ordered set \( \{ B_1, B_2, \ldots \} \) where \( B_i = M_{i-1} - M_i \) for \( i = 1, 2, 3, \ldots \). We denote this set by the symbol \( \mathcal{B}(\mathcal{N}, L|K) \), and call this ordered set a "relative canonical system" for \( L|K \). Given \( \mathcal{B}(\mathcal{N}, L|K) \), the ordered set \( \{ |B_1|, |B_2|, \ldots \} \) is called "the set of characters" of \( \mathcal{B}(\mathcal{N}, L|K) \). The number \( |B_i| \) is called "the \( i \)-th character of \( \mathcal{B}(\mathcal{N}, L|K) \)". More simply, the elements of the set of characters of \( \mathcal{B}(\mathcal{N}, L|K) \) are referred to as "the characters" (of \( \mathcal{B}(\mathcal{N}, L|K) \)).

We define

\[ \mathcal{M}(L|K) = \{ \mathcal{N}(L|K) : \mathcal{N}(L|K) \text{ is a relative canonical chain for } L|K \} \]

Similarly for an extension \( L|K \) and a chain of sets

\[ M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \text{ such that for all } i, \]

\[ M_i^p \text{ is an m.g.s. for } K(L^p_i)|K, \]
we define the ordered set

\[ \{ M_0, M_1, M_2, \ldots \} = \tilde{\eta}(L|K) \]

and call this ordered set a "total canonical chain" for \( L|K \). Similarly we define \( \tilde{B}(\tilde{\eta}, L|K) \) and call this set a "total canonical system" for \( L|K \). The "total characters" are defined analogously.

If every element of \( M(L|K) \) is a total canonical chain we say that \( M(L|K) \) is "total". If no element of \( M(L|K) \) is a total canonical chain we say that \( M(L|K) \) is "nil". In the event that some elements of \( M(L|K) \) are total canonical chains and some are not, we say that \( M(L|K) \) is "mixed". Finally, we define:

\[ \tilde{\mathcal{M}}(L|K) = \{ \tilde{\eta}(L|K) \mid \tilde{\eta}(L|K) \text{ is a total canonical chain} \}. \]

Given any extension \( L|K \) a relative canonical chain always exists. For if \( M_i^L \) is a relative p-base for \( K(L^P_i)|K \) then \( M_i^L \) generates \( K(L^P_i)|K \) and hence we can find a
subset $M_{i+1}$ of $M_i$ such that $M_{i+1}^p$ is a relative $p$-base for $K(L^p_i)$|K.

The following propositions will be needed to prove our main theorems:

**Proposition 1.** Suppose $L = K(M)$ and $L|K$ is purely inseparable. Then $M$ is an m.g.s. for $L|K$ if and only if $M$ is a relative $p$-base for $L|K$ [2].

**Proposition 2.** If $L|K$ is of finite exponent $e$, then $M$ is a relative $p$-base for $L|K$ if and only if $M$ is an m.g.s. for $L|K$ [8].

**Proposition 3.** If $B$ is a $p$-independent subset of $L$ and $C$ is a subset of $L$ which is an m.g.s. for $L^p(B,C)|L^p(B)$, then $B \cup C$ is a $p$-base for $L^p(B,C)$ [8].

**Proposition 4.** If $B \cup C$ is a $p$-independent subset of $L$, then for all $i$, $i = 1, 2, \ldots$, $B \cup C^{1/p^i}$ is a $p$-independent subset of $L(C^{1/p^i})$ [7].

**Proposition 5.** If $B$ is a relative $p$-base for $L|K$ and $G$ is a subset of $K$ which is $p$-independent in $L$, and $L^p(G) = L^p(K)$, then $B \cup G$ is a $p$-base for $L$.

These propositions complete the preparation for
Theorem 1 and Theorem 2. Theorem 2 is a converse for Theorem 1.

B. The Relative Canonical Chain

Theorem 1. Let $L|K$ be an arbitrary extension of characteristic $p$. Then there exists a relative canonical chain $\mathcal{H}(L|K)$ and its associated relative canonical system $\mathcal{B}(\mathcal{H},L|K)$ such that for $i = 1, 2, \ldots$, the following conditions hold:

1.) $B_i \subseteq K(L^p_i ) (B_{i+1}^p, B_{i+2}^p, \ldots)$, where $B_j \in \mathcal{B}(\mathcal{H},L|K)$, $j = 1, 2, \ldots$.

2.) If $b \in B_i - B'_i$, where $B_i \subseteq B'$, $b$ has exponent $i+1$ over $K(L^p_i ) (B_{i+1}^p, B_{i+2}^p, \ldots)$.

3.) The characters of $\mathcal{B}(\mathcal{H},L|K)$ are invariants of $L|K$.

Proof. The existence of a relative canonical chain has already been established. We have $K(L^p_i ) = K(K(L^p_{i-1} ))^p$, thus

$$K((K(L^p_i ) (B_{i-l}^p, M_{i-l}^p ))^p = K(L^p_i ) (B_{i+l}^p, M_{i+l}^p)$$

$$= K(L^p_i ) (M_i^p ) .$$
Hence 1.) is established. $M_{i-1}^p$ is p-independent in $K(L^p_i)$; for assume the contrary. Then for some $m, m \in M_i$, 

$m^p \in k(L^p_{i+1})(M_{i-1}^i - m)^p$, which implies that 

$m^p \in k(L^p_i)(M_{i-1}^i - m)^p$, contradicting the hypothesis 

that $M_{i-1}^p$ is a relative p-base of $K(L^p_i)$. Now suppose 

that $B_i \subseteq B_i, b \in (B_i - B_i^i)$. The set $(M_{i-1}^i - b)^p \cup b^p$ is p-independent in $K(L^p_i)$, and thus by Proposition 4, 

$(M_{i-1}^i - b)^p \cup b^p$ is p-independent in $K(L^p_i)(M_{i-1}^i - b)$. 

Hence $b^p \in k(L^p_{i+1})(M_{i-1}^i - b)^p$, so 

$b^p \in k(L^p_{i+1})(M_{i-1}^i - b)$. This last result, together 

with Part 1 of this Theorem, implies $b$ has exponent $i$ 

over $K(L^p_i)(B_{i+1}^i, B_{i+2}^i, \cdots)$.

$(K(L^p_i))^p(M_{i-1}^i)^p = (K(L^p_i)(M_{i-1}^i))^{i-1}$, an 

expression independent of the choice of $M_{i-1}^i$. Since 

$k(L^p_i) = (k(L^p_i))^p(K)$, we may select $G', G' \subseteq K$, as an 
m.g.s. for $K(L^p_i)$ over $(k(L^p_i))^p$. By Proposition 3, 

$M_{i-1}^i \cup G'$ is a p-base for $K(L^p_i)$. $G'$ is p-independent 
in $K(L^p_i)$, so one may select $G, G' \subseteq G \subseteq K$, such that
\[(K(L^P_i))^P(K) = (K(L^P_i))^P(G),\] with \(G\) \(p\)-independent in \(K(L^P_i)\). Since \(M^P_i\) is a relative \(p\)-base for \(K(L^P_i)\), Proposition 5 implies that \(G \cup M^P_i\) is a \(p\)-base for \(K(L^P_i)\).

Now

\[
K(L^P_i) = (K(L^P_i))^P(G',M^P_i)(M_{i-1} - M_i)^P_i
= (K(L^P_i))^P(G',M^P_i)(B_i^P)
= (K(L^P_i))^P(G',M^P_i)(G - G').
\]

Hence \(B_i^P\) and \(G - G'\) are m.g.s. of \(K(L^P_i)\) over the same base field, \((K(L^P_i))^P(G',M^P_i)\), and since \(K(L^P_i)\) is of exponent 1 over this base field, Proposition 2 implies that \(\text{Card}(B_i^P) = \text{Card}(B_i) = \text{Card}(G - G')\). Since \(G - G'\) is chosen independently of \(L|K\), \(|B_i|\) is an invariant of \(L|K\).

**Theorem 2.** Suppose \(L|K\) is a field extension of characteristic \(p\). Suppose there are sets \(B_i, i = 1,2,\ldots\), such that \(B_i^P \subseteq K(L^P_i)(B_{i+1}^P,B_{i+2}^P,\ldots)\), and 

\(L = K(L^P)(B_1,B_2,\ldots)\). Suppose also that if \(B_i^* \subseteq B_i\), and
b \in (B_i - B_i')$, then $b$ has exponent $i$ over $K(L^p)^{i+1}(B_{i}', B_{i+1}', B_{i+2}', \cdots)$. Then the sets $M_k = \bigcup_{i=k+1}^{\infty} B_i'$, $k = 0, 1, 2, \cdots$, are such that $M_k^p$ is a relative $p$-base for $K(L^p)^k$ over $K$. The ordered set $\{B_1', B_2', \cdots\}$ is a relative canonical system.

Proof: $K(L^p)^k = K(K(L^p)(M_0))^p = K(L^p)^{k+1}(M_k^p)$. If

$$B_n^p \subseteq K(L^p)^{k+1}(M_k^p),$$

for all $n$, $k > n > j$, then since

$$B_j^p \subseteq K(L^p)^{j+1}(B_{j+1}', B_{j+2}', \cdots),$$

$$B_j^p \subseteq K(L^p)^{k-j}(B_{j+1}', B_{j+2}', \cdots),$$

$$B_j^p \subseteq K(L^p)^{k+1}(M_k^p).$$

Since $B_k^p \subseteq K(L^p)^{k+1}(M_k^p)$,

$$K(L^p)^{k+1}(M_0^p) \subseteq K(L^p)^{k+1}(M_k^p).$$
Hence $K(L^p_k) = K(L^p_k)(M^p_k)$.

Now suppose that $M^p_k$ is not a relative p-base. Hence there is a $b \in B_r$, $r \geq k + 1$, so that

$$b^p \in K(L^p_k)(M^p_k - b^p),$$

with $r$ chosen minimal with respect to this property. Now if

$$b^p \in K(L^p_k)(B^p_r - b^p, B^p_{r+1}, B^p_{r+2}, \cdots),$$

upon taking $p^{r-k-1}$ powers, we certainly have

$$b^{p^{r-1}} \in K(L^p_r)(B^p_r - B^p_r, B^p_{r+1}, B^p_{r+2}, \cdots).$$

But

$$K(L^p_r) = K(L^p_r)(B^p_{r+1}, B^p_{r+2}, \cdots),$$

so $b^{p^{r-1}} \in K(L^p_r)(B_r - b, B_{r+1}, \cdots)$, contrary to the hypothesis of the theorem.

Hence, if $b^p \in K(L^p_k)(M^p_k - b^p)$, there are non-empty finite subsets $B^*_1, \ldots, B^*_n$ of $B_1, \ldots, B_n$. 
respectively, where \( k + 1 \leq i_1 < \cdots < i_n < r \), such that

\[
\begin{align*}
&b^p_k \in K(L^p) (B_i^p)_{i_1} - b^p_k, B_i^p, \ldots, \\
&B_i^p, B_r - b^p_k, B_r, \ldots,
\end{align*}
\]

but

\[
\begin{align*}
&b^p_k \notin K(L^p) (B_i^p)_{i_1} - b^p_k, B_i^p, \ldots, \\
&B_i^p, B_r - b^p_k, B_r, \ldots.
\end{align*}
\]

By the interchange axiom,

\[
\begin{align*}
&b^p_k \in K(L^p) (B_i^p)_{i_1} - b^p_k, B_i^p, \ldots, B_i^p, B_r, B_r, \ldots.
\end{align*}
\]

Hence \( b^p_k \in K(L^p) (M^p)_{k_1} - b^p_k \). But \( b^* \in B^* \) and \( i_1 < r \), contradicting the choice of \( r \). Hence \( M^p_k \) is a relative \( p \)-base of \( K(L^p) \).

Since the characters of \( \mathcal{B}(\mathcal{N}, L|K) \) are invariants of \( L|K \), they will be referred to as the characters of \( L|K \).

If $L'$ is a subfield of $L$ such that $L \supset L' \supset K$, $L'$ is called an intermediate field for $L|K$. If in addition $L' = K(L^P)$, $L'$ is called a relatively perfect intermediate field for $L|K$. If for some integer $r$, $K(L^P)$ is a relatively perfect intermediate field for $L|K$, then for any integer $s$, $s \geq r$, $K(L^P) = K(L^P)$. In the event that this does not happen the field $K = \bigcap_{i=1}^{\infty} K(L^P)$ is a natural field to study, if $L|K$ is purely inseparable. In this case if the set $M^i$, which is a relative $p$-base for $K(L^P)|K$, is also an m.g.s. for $K(L^P)|K$, then $M^i$ is also an m.g.s. for $K(L^P)|K$. In fact, since $K(L^P) = K(L^P)$, one could repeat the entire analysis with $K$ replacing $K$ everywhere.

If $K$ is not a relatively perfect intermediate field for $L|K$, one may consider the relative canonical chain for $K|K$. An open question is whether there is any connection between the invariants of $L|K$ and $K|K$. In any case, these additional invariants do not characterize $L$ within isomorphism or even lattice isomorphism, as the finite
degree extensions show.

Since the analysis of $L|K$ by relative canonical chains must end when a relatively perfect intermediate field is reached, it is of interest to know whether maximal intermediate fields exist. In fact we have the following proposition:

Proposition 6. There is a maximum relatively perfect intermediate field for $L|K$.

Proof: Let $A = \{L_\alpha | L_\alpha \text{ is a relatively perfect intermediate field for } L|K\}$, and order $A$ by inclusion. Let $\{L_\beta\}$ be a chain in $A$. Then $\cup\{L_\beta\}$ is relatively perfect, for

$$K(\cup\{L_\beta\})^p = K(\cup\{L_\beta^p\}) \supseteq \cup\{K(L_\beta^p)\} = \cup\{L_\beta^p\}.$$  

Hence an application of Zorn's lemma gives a maximal element $L_1$ of $A$. That $L_1$ is actually a maximum element is obvious if one can show that the composite of two relatively perfect fields is relatively perfect. Let $(L_1,L_2)$ denote the smallest subfield of $L$ containing $L_1$ and $L_2$. We say that $(L_1,L_2)$ is the composite of $L_1$ and
L_2 in L. If L_1 and L_2 are relatively perfect intermediate fields then

\[ K((L_1,L_2)^P) = K((L_1^P,L_2^P)) = (K(L_1^P),K(L_2^P)) = (L_1,L_2). \]

We note that \( K(L_1^P) = K(L_2^{e+1}) \) if and only if \( M_0^e \subseteq K^n \).
III. THE RELATIVE CANONICAL CHAIN APPLIED TO
PURELY INSEPARABLE EXTENSIONS

A. The Characterization and Invariants of a
Total Canonical Chain.

In the following theorems $M_i$ will denote the
appropriate member of a total canonical chain and
$B_i (= M_{i-1} - M_i)$ will denote the appropriate member of the
associated total canonical system.

Theorem 1. Suppose $L|K$ is purely inseparable. If there
exists a total canonical chain $\tilde{\eta}(K|L)$, then the sets $B_i$
of $\tilde{\eta}(\tilde{\eta}, L|K)$ satisfy the conditions:

1. $\bigcup_{i=1}^{\infty} B_i = M_0$.
2. $B_i^{p_i} \subseteq K(B_{i+1}^{p_i}, B_{i+2}^{p_i}, \ldots)$.
3. For all $B_i' \subseteq B_i$, if $b \in B_i - B_i'$, $b$ has
   exponent $i$ over $K(B_i', B_{i+1}, B_{i+2}, \ldots)$.

Proof: Since $M_1 \supseteq M_{i+1}$ for all $i$,

$$\bigcup_{i=1}^{\infty} B_i = \bigcup_{i=1}^{\infty} (M_{i-1} - M_i) = M_0 - \bigcap_{i=1}^{\infty} M_i.$$
But \( \cap M_i = \emptyset \). For assume that \( x \in \cap M_i \). Since \( L|K \) is purely inseparable there is an integer \( e \) such that \( x^e \in K \), hence \( x \in M_e \). Since \( e \) is purely inseparable there is an integer \( e \) such that \( x^e \in K \) and \( x \in M_e \) implies that \( x^e \in M_e \), a contradiction. This completes the proof of 1.

By definition, \( K(L_i^e) = K(y_i^e) = K(M_i^e) \) and \( K(L_i^e) = K(L_i^e)^p \). Hence

\[
K(M_i^e) = K(B_i^e, M_i^e) = K(M_i^e).
\]

This completes the proof of 2.

Proposition 1, Chapter II, implies that \( M_i^e \) is a relative \( p \)-base for \( K(L_i^e)|K \). Condition 3 of this theorem then follows from 2 of this theorem and condition 2 of Theorem 1 of Chapter II.

It is clear the total characters are characters and are therefore invariants of \( L|K \).

Theorem 2. If \( L|K \) is purely inseparable and there exists a collection of disjoint sets \( B_i, i = 1,2,\ldots \) of subsets such that
1. \( L = \mathbb{K}(B_1, B_2, \cdots) \).

2. \( B_i^p \subseteq \mathbb{K}(B_{i+1}^p, B_{i+2}^p, \cdots) \) for \( i = 1, 2, \cdots \).

3. For all \( B'_i \subseteq B_i \), if \( b \in B_i - B'_i \), the exponent of \( b \) over \( \mathbb{K}(B'_i, B_{i+1}, B_{i+2}, \cdots) \) is \( i \).

Then \( \{B_1, B_2, \cdots\} \) is a total canonical system.

Proof: We define \( M_k = \bigcup_{i=k}^{n} B_{i+1}^p \mathbb{K}(L^p) = \mathbb{K}(M_0^p) \), for \( k \)

if \( B_n^p \subseteq \mathbb{K}(M_k^p) \) for all \( n, k \geq n > j \), then since \( B_j^p \subseteq \mathbb{K}(B_{j+1}^p, B_{j+2}^p, \cdots), B_j^p \subseteq \mathbb{K}(B_{j+1}^p, B_{j+2}^p, \cdots) \subseteq \mathbb{K}(M_k^p) \).

Since \( B_k^p \subseteq \mathbb{K}(M_k^p) \), \( \mathbb{K}(L^p) = \mathbb{K}(M_0^p) = \mathbb{K}(M_k^p) \).

Thus \( M_k^p \) is an m.g.s. for \( \mathbb{K}(L^p) | \mathbb{K} \) if \( M_k^p \) is a relative \( p \)-base for \( \mathbb{K}(L^p) | \mathbb{K} \). But \( M_k^p \) is a relative \( p \)-base for \( \mathbb{K}(L^p) | \mathbb{K} \) by Theorem 2 of Chapter II.

B. Existence of Total Canonical Chains

Our first result is elementary.

**Proposition 1.** If \( L | \mathbb{K} \) is purely inseparable then...
\( \tilde{\mathcal{M}}(L|K) \subseteq \mathcal{M}(L|K) \). That is, every total canonical chain is a relative canonical chain.

**Proof:** If \( L|K \) is purely inseparable clearly \( K(L^P_r)|K \) is purely inseparable, for any positive integer \( r \). If \( M^P_r \) is an m.g.s. for \( K(L^P_r)|K \), Proposition 1 of Chapter I implies that \( M^P_r \) is a relative \( p \)-base for \( K(L^P_r)|K \).

The above proposition tells us where to search for m.g.s.'s for a purely inseparable extension \( L|K \).

The next proposition is immediately implied by Proposition 2 of Chapter II.

**Proposition 2.** If \( L|K \) is of finite exponent \( e \) then
\[
\tilde{\mathcal{M}}(L|K) = \mathcal{M}(L|K), \quad \mathcal{M}(L|K) \neq \emptyset.
\]

We note in passing that the proposition may be interpreted as implying the existence of a total canonical system whose elements satisfy the conditions of Theorem 1 of this chapter. The \( i \)-th character is the empty set if \( i > e \). Theorem 2 of this chapter characterizes the total canonical systems.

**Proposition 3.** If \( L|K \) is purely inseparable and \( (L|K) \) is a relative canonical chain such that \( M^0 \) is an m.g.s.
for $L|K$ and the characters of $L|K$ are all finite, then $\mathcal{N}(L|K)$ is a total canonical chain.

Proof: Suppose that $M_i^{P_i}$ is an m.g.s. for $K(L^{P_i})|K$. Since $|B_{i+1}|$ is finite there is an integer $e_i+1$ such that $B_{i+1}^{e_i+1} \subseteq K$. Since

$$K(L^{P_i}) = K(B_{i+1}^{P_i} \cup M_i^{P_i})$$

when $s > i$, setting $s > \max(e_i+1,i+1)$ gives

$$K(L^{P_i^s}) = K(L^{P_i})^{i+1} \subseteq K(M_i^{P_i})^{i+1}.$$ 

Proposition 4. If $L|K$ is purely inseparable and $\mathcal{N}(L|K)$ is a relative canonical chain such that $M_0$ is an m.g.s. for $L|K$ and $B_i$ is of finite exponent over $K(M_i)$ then $\mathcal{N}(L|K)$ is a total canonical chain.

Proof: The proof is similar to the proof of Proposition 3.

If $\{L_\alpha\}, \alpha \in I$ is a collection of intermediate fields of $L|K$, $\bigcup L_\alpha$ denotes the smallest subfield of $L$ which contains $\bigcup L_\alpha$. Similarly $L_1 * L_2$ denotes the subfield.
of $L$ generated by $L_1$ and $L_2$.

**Theorem 3.** Let $L|K$ be purely inseparable, which is generated by a set of subfields $\{L_\alpha|K\}$, $\alpha \in I$, such that for all $\beta, \beta \in I$, $L_\beta$ is linearly disjoint from $\bigcap_{\alpha \in I-\beta} L_\alpha$.

Suppose that for all $\alpha$, $L_\alpha$ has the property that $M^{p_i}_{\alpha,i}$ is an m.g.s. for $K(L^{p_i}_\alpha)|K$, with $M^{\alpha,i}_\alpha \supseteq M^{\alpha,i+1}_\alpha$.

Then $L$ has a total canonical chain $\{M_0, M_1, M_2, \ldots\}$.

**Proof:** Define $M_i = \bigcup_{\alpha \in I} M^{\alpha,i}_\alpha$.

$$L = \prod_{\alpha \in I} L_\alpha = \prod_{\alpha \in I} K(M^{\alpha,0}_\alpha) \subseteq K(M_0) \subseteq L.$$  

Hence $L = K(M_0)$. We also have

$$K(L^{p_i}) = K(\prod_{\alpha \in I} L_\alpha^{p_i}) = \prod_{\alpha \in I} K(L^{p_i}_\alpha) = \prod_{\alpha \in I} K(M^{\alpha,i}_\alpha) \subseteq K(M^{p_i}_i) \subseteq K(L^{p_i}).$$

Hence

$$K(L^{p_i}) = \prod_{\alpha \in I} K(M^{\alpha,i}_\alpha) = K(M^{p_i}_i).$$
Now \( M_0 \) is an m.g.s. for \( L \) over \( K \). For assume \( m \in K(M_0 - m) \). Therefore \( m \in M_\beta,0 \) for some \( \beta \in \mathbb{I} \), and

\[
m \in K(M_\beta,0 - m,M_\beta_1,0,M_\beta_2,0, \ldots, M_\beta_n,0)
\]

\[
= K(M_\beta,0 - m) \cup K(M_\beta,0) \subseteq K(M_\beta,0 - m) \cup \prod_{\alpha \in \mathbb{I} - \beta} L_\alpha.
\]

But this is a contradiction. For since \( m \in K(M_\beta,0 - m) \), one has a linear basis \( B_{\beta,0} \) of \( K(M_\beta,0 - m) \) over \( K \) and \( B_{\beta,0} \cup \{m\} \) is therefore linearly independent over \( K \), hence over \( \prod_{\alpha \in \mathbb{I} - \beta} L_\alpha \). But \( m \cdot 1 = \sum_{i=1}^{i=n} k_i b_i \cdot 1 \). so

\[
m \cdot 1 - \sum_{i=1}^{i=n} b_i k_i \cdot 1 = 0,
\]

a non-trivial linear combination of linearly independent elements over the field \( \prod_{\alpha \in \mathbb{I} - \beta} L_\alpha \).

Next we consider \( K(L_\beta^p) \). \( K(L_\beta^p) \) is linearly disjoint from \( \prod_{\alpha \in \mathbb{I} - \beta} K(L_\alpha^p) \) since \( L_\beta \) is linearly disjoint from \( \prod_{\alpha \in \mathbb{I} - \beta} L_\alpha \). The remainder of the proof is identical to the proof above.

Suppose \( L' \mid K \) is an intermediate field of \( L \mid K \). If every relatively \( p \)-independent subset of \( L' \mid K \) remains
relatively \( p \)-independent in \( L \mid K \), we say \( L \mid K \) is a relative \( p \)-independence preserving extension of \( L' \mid K \).

**Theorem 4.** Suppose \( L \mid K \) is purely inseparable and \( \{L_\alpha \mid K : \alpha \in I \} \) is a chain of intermediate fields of \( L \mid K \), each of which has the property that every \( L_\alpha \mid K \) is of finite exponent. Suppose that \( L \mid K \) is a relative \( p \)-independence preserving extension of \( L_\alpha \mid K \) for all \( \alpha \in I \) and \( \{L_\alpha \mid K : \alpha \in I \} \) is well-ordered by inclusion such that for all limiting ordinals \( \gamma \in I \), \( \bigcup_{\alpha < \gamma} L_\alpha = L_\gamma \), and \( L = \bigcup_{\alpha \in I} L_\alpha \). Then \( L \) has a total canonical chain.

**Proof:** If \( L_\alpha \subseteq L_\beta \), in particular when \( L_\beta \) is the successor of \( L_\alpha \), if \( M_\alpha \) is an m.g.s. for \( L_\alpha \mid K \), then since \( M_\alpha \) is a relative \( p \)-base for \( L_\alpha \), \( M_\alpha \) is relatively \( p \)-independent in \( L_\beta \), and hence may be extended to a relative \( p \)-base \( M_\beta \) for \( L_\beta \mid K \). Thus we have an m.g.s. \( M_\beta \) for \( L_\beta \mid K \), with \( M_\beta \supseteq M_\alpha \).

We define \( I' = I \cup \nu \), where \( \nu > \alpha \) for all \( \alpha \in I \), if \( I \) has no last element. \( \nu \) is then a limiting ordinal; if \( I \) has a last element \( \mu \), let \( \nu = \mu \). We may define \( L = L_\nu \). Let \( \rho_\beta, \alpha = \{M_\alpha^{\beta, \rho} : M_\alpha^{\beta, \rho} \text{ is an m.g.s. for } L_\alpha \mid K \text{ for } \alpha \leq \beta; \text{ if } \gamma < \delta, M_\gamma^{\beta, \rho} \subset M_\delta^{\beta, \rho} \} \). Let \( \epsilon \) be a limit
ordinal such that for all $\beta < \epsilon$, there is a chain $C_{\beta, \rho}$.

Let $\mathcal{D}_\epsilon = \{C_{\beta, \rho} : \beta < \epsilon\}$, partially ordered by natural inclusion. Let $C_J$ be a maximal chain in $\mathcal{D}_\epsilon$, with $J$ indexing the chains $C_{\alpha, \rho}$ in the chain $C_J$, with $\alpha \in J$ and $J \subset I$. Let $J' = \{\alpha : \alpha \in I', \alpha$ is an upper bound for $J\}$. $J'$ is non-empty and has a first element $\delta$, with $\delta \leq \epsilon$. $(\cup C_J) \cup (\cup \cup C_J)$ is a $C_{\delta, \rho}$ for $L_\delta$. If $\delta \neq \epsilon$, $C_J \cup C_{\delta, \rho}$ is a chain in $\mathcal{D}_\epsilon$, larger than $C_J$. It is clear $C_J$ does not have a last element, since $\epsilon$ is a limit ordinal and if $C_J$ had a last element, $C_J$ could be enlarged.

By transfinite induction, for all $\alpha \in I'$, there is a corresponding $C_{\alpha, \rho}$. In particular there is a $C_{\nu, \rho}$.

$K(L_\alpha^P)$ is generated over $K$ by $M_\alpha^P$, for $M_\alpha \in C_{\nu, \rho}$.

In the same manner as before, we may show there is a chain $C_{\nu, \rho}$ of subsets of $C_{\nu, \rho}$ such that $C_{\nu, \rho}$ is a chain of m.g.s.'s for $\{K(L_\alpha^P) : \alpha \in I'\}$.

That the constructions in Theorem 3 and 4 give distinct classes of fields can be seen even in the finite degree case. There exists an example of a field with two generators which is not a tensor product. Let $K = P(\mu, \nu)$, where $P$ is a perfect field of characteristic $p$ and
L = K(\mu^{1/p^2},(\mu^{1/p} + v)^{1/p})$. $L|K$ is not a tensor product of two simple extensions of $K$.

C. The Sandwich Theorem

**Theorem 5.** Suppose $L|K$ is of finite exponent, while $M$ is an arbitrary extension of $K$. Then there is a total canonical chain

$$(L|K) = \{M_0', \ldots, M_{r-1}', M_r\},$$

with $M_r = \emptyset$, and a total canonical chain

$$(M(L)|M) = \{M_0', \ldots, M_{r'-1}', M_{r'}\},$$

with $M_{r'} = \emptyset$, such that $M_{k_j} \subseteq M_{k_j} \subseteq M_{k_j+1}$ for $j \in \{0,1,\ldots,r-1\}$, where $0 \leq k_j < k_j + 1 \leq r$. $k_j$ may equal $k_i$ for $i \neq j$, and $k_j \geq j$.

Proof: Let $\mathcal{D}_{r-1,r'-1} = \{I_\alpha^{\mathcal{P}_{r-1}}|I_\alpha\}$ is a subset of $L$ such that $I_\alpha^{\mathcal{P}_{r-1}}$ is relatively $p$-independent in $K(L^{\mathcal{P}_{r-1}})|K$ and $I_\alpha^{\mathcal{P}_{r'-1}}$ is relatively $p$-independent in $M(M(L))^{\mathcal{P}_{r'-1}}|M$.

$\mathcal{D}_{r-1,r'-1}$ is clearly an inductive set and hence there is a
maximal member, $I_{r-1, r'-1}$. Suppose that $I_{r-1, r'-1}$ is not a relative $p$-base for either $K^{p_{r-1}}_L$ or $M^{p_{r'-1}}_{ML}$. This is true if and only if there are elements $a$ and $c$, both belonging to $L$, such that

$$a^{p_{r-1}} \notin K^{p_{r}}_{L^{p_{r}}}(I_{r-1, r'-1})^{p_{r-1}}$$

and

$$c^{p_{r'-1}} \notin M^{p_{r'}}_{ML}(I_{r-1, r'-1})^{p_{r'-1}}.$$

If either $a^{p_{r'-1}} \in M^{p_{r'}}(L^{p_{r'}})(r-1, r'-1)^{p_{r'-1}}$ or

$$c^{p_{r-1}} \in K^{p_{r}}_{L^{p_{r}}}(I_{r-1, r'-1})^{p_{r-1}},$$

then either $I_{r-1, r'-1} \cup a$ or $I_{r-1, r'-1} \cup c$ is a member of $\mathcal{C}_{r-1, r'-1'}$, larger than $I_{r-1, r'-1}$, contradicting maximality. Hence $a^{p_{r'-1}} \in M^{p_{r'}}(L^{p_{r'}})(I_{r-1, r'-1})^{p_{r'-1}}$ and

$$c^{p_{r-1}} \in K^{p_{r}}_{L^{p_{r}}}(I_{r-1, r'-1})^{p_{r-1}}.$$

If $b$ is a non-zero element of $K$, then
\[(a + bc)^P \subseteq K(L^P)(I_{r-1,r'-1})^P\]

and

\[(a + bc)^P \subseteq M(M(L)^P)(I_{r-1,r'-1})^P\]

In any event, \(I_{r-1,r'-1}^P\) is a relative \(p\)-base for

\[K(L^P)|L\] or \(I_{r-1,r'-1}^P\) is a relative \(p\)-base for

\[M(M(L)^P)|M,\] or both. Next, let

\[\mathcal{L}_{r-s,r'-t} = \{I_\beta : I_\beta \supset I_{r-1,r'-1}; I_\beta^P_{r-s}\text{ is relatively }p\text{-independent in }K(L^P)\text{ and }I_\beta^P_{r'-t}\text{ is relatively }p\text{-independent in }M(M(L)^P)\}.\]

If \(I_{r-1,r'-1}^P\) is a relative \(p\)-base for \(K(L^P)|K, s = 1, \) while \(t\) is the smallest number such that \(B_{r'-t-1} \neq \emptyset.\) An analogous result holds in the other cases, in which either \(t = 1\) and \(s\) is the smallest positive number such that \(B_{r'-s-1} \neq \emptyset,\) or \(t\) is the smallest positive number such that \(B_{r-t-1} \neq \emptyset\) and \(s\) is the smallest number such that \(B_{r-s-1} \neq \emptyset.\) By the same argument used above, \(\mathcal{L}_{r-s,r'-t}\) has a maximal element.
such that either \( I_{r-s,r'-t}^P \) is a relative p-base for \( K(L^P_r)^K \) or \( I_{r-s,r'-t}^P \) is a relative p-base for \( M(M(L)^P_r)^M \), or both.

In this manner we may construct a chain of relative p-bases,

\[
I_{r-1,r'-1} \subseteq I_{r-s,r'-t} \subseteq \cdots \subseteq I_{j,0}
\]

with \( j \geq 0 \). It is easily demonstrated that any relative p-base \( M_u^P \) for \( M(M(L)^P_u)^M \) is relatively p-independent in \( K(L^P_u)^K \). This implies that the final element in the chain is an m.g.s. for \( M(L)^M \), and that \( k_j \geq j \) for all \( j \), which completes the proof.

With \( L \) and \( M \) as in Theorem 5, the cardinality of an m.g.s. for \( M(L)^M \) is not greater than that for \( L^K \). This remark generalizes the finite degree case, as given in Pickert [7].

D. Relative p-Independence Preserving Extensions and Minimal Generating Sets

The following propositions are modest generalizations
of Proposition 3 and Proposition 4 of Chapter II.

**Proposition 5.** If $B$ is a relatively $p$-independent subset of $L|K$ and $C$ is an m.g.s. for $K(L^P)(B,C)|K(L^P)(B)$, then $B \cup C$ is a relatively $p$-independent subset of $L|K$.

**Proposition 6.** If $B \cup C$ is relatively $p$-independent in $L|K$, then for all $i$, $i = 1,2,3,\ldots$, $B \cup C^{1/p^i}$ is a relatively $p$-independent subset of $L(C^{1/p^i})|K$.

**Theorem 6.** Let $L|K$ and $M|K$ be purely inseparable with $L \supseteq M$. Then an m.g.s. $B$ for $M|K$ may be extended to an m.g.s. $B \cup C$ for $L|K$ if and only if $B$ remains relatively $p$-independent in $L$ and $L|M$ has an m.g.s.

**Proof:** Let $B$ be an m.g.s. for $M|K$ and hence a relative $p$-base for $M|K$. Let $C$ be an m.g.s. for $L|M$ and let us suppose that $L|K$ is a relative $p$-independence preserving extension of $M|K$. $L = M(C) = L^P(M)(C)$ with $C$ an m.g.s. for $L|L^P(M)$. $M = K(B) = K(M^P)(B)$; $B$ is relatively $p$-independent in $L|K$ and since $C$ is an m.g.s. for $L^P(M)(C)|L^P(M) \text{ and } K(L^P)(B) = L^P(M)$, $C$ is an m.g.s. for $K(L^P)(B,C)|K(L^P)(B)$. Proposition 5 implies that $B \cup C$ is a relative $p$-base for $L|K$ and since
L = M(C) = K(B)(C) = K(B,C), B \cup C is an m.g.s. for L|K.

Let us suppose that an m.g.s. B for M|K may be extended to an m.g.s. D = B \cup C for L|K. D is relatively p-independent in L|K, hence B is relatively p-independent in L|K. L = K(B,C) = K(B)(C). If c \in C, c \not\in K(B,C - c) = K(B)(C - c) = M(C - c). Thus C is an m.g.s. for L|M.

Theorem 7. Suppose L = M(x) is a purely inseparable extension of K, where M = K(B), with B an m.g.s. for M|K. Then L|K has an m.g.s.

Proof: Let e be the exponent of x over M. If \(x^p \in K(M^p)\), \(x^p\) is a relatively p-independent subset of M. Since B is a relative p-base for M, by the exchange property there is an element b, b \in B, such that B - b \cup x^p is a relative p-base for M. We have, by Proposition 6, that (B - b) \cup x is relatively p-independent in K(M^p)(B - b, x) = M(x) = L. Let t be the exponent of b over K. Then L = K(L^p)(B - b, x) = K(L^p t)(B - b, x).

But L^p t = K^p (B - b)^p (b^p, x^p) \subseteq K(B - b)^p (x^p), so L = K(B - b, x). Hence (B - b) \cup x is an m.g.s. for
On the other hand, suppose $x^e \in K(M^e)$. We will first assume that $e = 1$. The desired m.g.s. will be $B \cup x$. $L = K(B, x)$, so our proof will reduce to showing that $B \cup x$ is relatively $p$-independent in $L | K$.

If $x \in K(L^p)(B \cup x - x)$,

$$x \in K(M^p)(x^p)(B) = K(M^p)(B, x^p) = M(x^p) = M,$$

a contradiction.

We next suppose that $b \in K(L^p)(B - b, x)$. But $b \notin K(L^p)(B - b)$, for $K(L^p)(B - b) = K(M^p)(x^p, B - b) = K(M^p)(B - b)$. By the exchange property, $x \in K(L^p)(B)$.

But $K(L^p)(B) = K(M^p)(x^p, B) = M$. This is a contradiction. Hence, $B \cup x$ is relatively $p$-independent in $L | K$.

We now suppose that the theorem is true whenever an element $y$ has exponent $e$ over $M$, with $e = 1$. Suppose that $x$ has exponent $e = k + 1$ over $M$. Then $y = x^p$ has exponent $e = k$ over $M$, and thus $M(y)$ has an m.g.s. $B'$ over $K$; But $X$ has exponent $1$ over $M(y)$, and so $M(x)|K$ has an m.g.s.

**Corollary 1.** If $L | K$ is a finite degree purely inseparable
Corollary 2. If $L|K$ is purely inseparable and is a finite degree extension of $M|K$, and $M|K$ has an m.g.s., then the cardinality of a m.g.s. for $L|K$ is greater than or equal to the cardinality of an m.g.s. for $M|K$.

This corollary, stated for $L|K$ of finite degree, appears in [7], where it is proved in an entirely different manner.

It is clear that if $M|K$ is of finite exponent, every relative p-base for $M|K$ is an m.g.s.. The converse is unknown; that is, if $M|K$ is a purely inseparable extension such that every relative p-base is a m.g.s., is $M|K$ of finite exponent? If this converse were true, the following theorem would be of no consequence, for it would hold automatically.

Theorem 8. Suppose that $M|K$ is purely inseparable, with the property that every relative p-base is an m.g.s.. If $L|K$ is an extension of $M|K$, of exponent 1 over $M$, then $L|K$ has an m.g.s. provided that $M|K$ does.

Proof: Let $L = M(X)$, with $X$ an m.g.s. for $L|M$. We
will partition $X$ into 2 disjoint subsets, $X'$ and $Y$, so that $X = X' \cup Y$, and $X'^p$ is a maximal relatively $p$-independent subset of $X^p$ in $M|K$. Thus

$Y^p \subseteq K(M^p)(X^p)$. If $B$ is a relative $p$-base for $M|K$, since $M = K(M^p)(X^p,B)$, there is a set $B'$, $B' \subseteq B$, such that $X'^p \cup B'$ is a relative $p$-base for $M|K$ and thus $X'^p \cup B'$ is an m.g.s. for $M|K$. By Proposition 6 $X' \cup B'$ is a relative $p$-base for $M(X')$. Since $M = K(X'^p,B')$, $M(X') = K(X'^p,B')(X') = K(X',B')$. Hence $X' \cup B'$ is an m.g.s. for $M(X')|K$.

$L = M(X',Y) = K(B',X',Y)$, so if $B' \cup X' \cup Y$ is relatively $p$-independent for $L|K$, $B' \cup X' \cup Y$ is an m.g.s. for $L|K$. Set $C = B' \cup X'$. Suppose that for $y \in Y$, $y \in K[M(X' \cup Y)]^p[C,Y - y]$, which is contained in $M(X',Y - y)$, a contradiction. We suppose next that $c \in C$ and $c \in K[M(X' \cup Y)]^p(C - c,Y)$.

But $c \in K[M(X' \cup Y)]^p(C - c)$, for
\( K[M(X' \cup Y)]^P(C - c) \subseteq K(M^P)(X'^P)(C - c) = K[M(X')]^P(C - c), \)

and \( C \) is an m.g.s. for \( M(X') | K \). Hence there is a finite non-empty set \( Y_0, Y_0 \subseteq Y \), such that

\( c \notin K(L^P)(C - c, Y_0), \) but \( c \notin K(L^P)(C - c, Y_0 - Y_0) \), which implies that

\( y_0 \in K[M(X' \cup Y)]^P[C, y_0 - y_0], \)

so \( y_0 \notin M(X', Y_0 - Y_0) \), a contradiction. Thus \( X \cup B' = X' \cup Y \cup B' \) is a relative \( p \)-base for \( L|K \) and hence an m.g.s. for \( L|K \).

A rather simple criterion in which a relative \( p \)-base is not an m.g.s. is given by the following proposition.

**Proposition 7.** For some relative \( p \)-base \( B \) of \( L|K \),

\( L \notin K(B) \) if and only if there exists an intermediate field \( M|K, L \neq M \), such that \( L \) is relatively perfect over \( M \);

that is, \( L = M(L^P) \).

**Proof:** Suppose \( B \) is a relative \( p \)-base for \( L|K \), but \( B \) is not an m.g.s.. It is obvious that \( L \) is relatively perfect over \( K(B) \).

On the other hand, let \( M|K \) be an intermediate field
of \( L:K \) such that \( L = M(L^{P}) \). If \( B \) is any set such that \( M = K(B) \), clearly \( L = K(L^{P})(B) \). Hence there is a subset \( B' \) of \( B \) such that \( B' \) is a relative \( p \)-base for \( L:K \), but since \( L \not\in M \), \( L \not\in K(B') \).

The following proposition gives the connection between derivations and relative \( p \)-independence preserving extensions.

**Proposition 8.** If \( L:K \) is an extension of \( M:K \) and \( L:K \) is a purely inseparable extension, then the following conditions are equivalent.

a. Every relative derivation of \( M:K \) into \( L:K \) can be extended to a relative derivation of \( L:K \) into \( L:K \).

b. \( L:K \) is a relative \( p \)-independence preserving extension of \( M:K \).

c. The elements of any relative \( p \)-base remain relatively \( p \)-independent in \( L:K \).

d. There is a relative \( p \)-base of \( M:K \) which remains relatively \( p \)-independent in \( L:K \).

Proof: The equivalence of a and c is proved in Jacobson [4].
Clearly, condition b implies both condition c and condition d, while condition c implies condition d. A easy generalization of Theorem 7 in [5] shows that condition d implies condition b.
IV. EXAMPLE

Our example is that of a purely inseparable extension $L|K$ for which $\mathfrak{M}(L|K)$ is mixed. Let $K = P(x_1, x_2, \ldots)$, where $P$ is a perfect field of characteristic $p$ a prime and $x_1, x_2, \ldots$ are indeterminants. Let

$$L = K(x_1^{p-1}, x_2^{p-2}, \ldots).$$

It is clear that $M_0 = \{x_1^{p-1}, x_2^{p-2}, \ldots\}$ is an m.g.s. for $L|K$, while $M_i = \{x_{i+1}^{p}, x_{i+2}^{p-1}, \ldots\}$ is such that $M_i^p$ is an m.g.s. for $K(L^p)|K$.

On the other hand

$$\bar{M}_0 = \{(x_1 x_2)^{p-1}, (x_2 x_3)^{p-2}, (x_3 x_4)^{p-3}, \ldots\}$$

is a relative $p$-base for $L|K$ which is not an m.g.s. for $L|K$. For if $x_1^{p-1} \in K(\bar{M}_0)$, there is a natural number $n$ for which

$$x_1^{p-1} \in K((x_0 x_2)^{p-1}, (x_2 x_3)^{p-2}, \ldots, (x_n x_{n+1})^{p-n}),$$
and so

\[
K((x_1 x_2)^{p-1}, (x_2 x_3)^{p-2}, \ldots, (x_n x_{n+1})^{p-n})
\]

\[
\supseteq K(x_1^{p-1}, x_2^{p-1}, \ldots, x_{n+1}^{p-1}),
\]

a contradiction on the cardinalities of m.g.s.'s.

In a similar fashion it is easily demonstrated that

\[
\overline{M}_i = \{(x_{i+1} x_{i+2})^{p-i-1}, (x_{i+2} x_{i+3})^{p-i-2}, \ldots\}
\]

is a set such that \(\overline{M}_i\) is a relative p-base for

\(K(L^p)|K\) but not an m.g.s. for \(K(L^p)|K\). Thus

\(\{\overline{M}_0, \overline{M}_1, \ldots\}\) is a relative canonical chain which is not a total canonical chain.
V. REFERENCES


VI. ACKNOWLEDGMENTS

The author wishes to thank both his major professor, Dr. Bernard Vinograde, and Dr. John Mordeson of The Creighton University for their valuable suggestions and guidance during the preparation of this thesis. Dr. Mordeson's permission to use several unpublished results of his is gratefully acknowledged.