The residue field of a local algebra

Paul Theodore Rygg
Iowa State University

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

Recommended Citation
Rygg, Paul Theodore, "The residue field of a local algebra" (1959). Retrospective Theses and Dissertations. 2208.
https://lib.dr.iastate.edu/rtd/2208

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.
THE RESIDUE FIELD OF A LOCAL ALGEBRA

by

Paul Theodore Rygg

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
1959
TABLE OF CONTENTS

I. INTRODUCTION .................................................. 1

II. UNSHRINKABLE SETS AND p-INDEPENDENCE IN
PURE INSEPARABLE EXTENSIONS. ................................. 3

   A. Preliminary Considerations .............................. 3
   B. p-Bases and the Sets G, H, and M .................... 10
   C. G p-Independent in F .................................. 21
   D. M* p-Independent in K .................................. 25
   E. Transcendence Bases and p-Bases ...................... 27
   F. Minimum-degree Ordering of M ......................... 29
   G. Examples .................................................. 34

III. IMBEDDING THE RESIDUE FIELD IN THE LOCAL ALGEBRA 36

   A. R a Primary Local Algebra over K .................... 36
   B. R a Complete Local Algebra over K .................... 40

IV. REFERENCES .................................................... 46

V. ACKNOWLEDGMENT ............................................... 47
The problem dealt with in this dissertation is that of finding conditions under which the residue field of a local algebra $R$ over a field $K$ can be imbedded in $R$ in such a way that the imbedded field contains $K$.

If $R$ is an algebra over $K$ we understand that $R$ is a commutative ring with identity containing a subring $K$ that is a field and the identity of $K$ is the identity of $R$. If $R$ is a local algebra we understand that $R$ is a local ring. By a local ring we mean a commutative ring with identity in which the non-units form an ideal, $N$. It is not assumed that $R$ is Noetherian, but only that $\bigcap_{i=1}^{\infty} N^i = (0)$. If there is some positive integer $\lambda$ such that $N^\lambda = (0)$, then $R$ is said to be a primary local ring.

The field $K$, over which $R$ is a local algebra, is assumed to have characteristic $p (\neq 0)$ which is equal to the characteristic of the residue field $R/N$. It is also assumed that $R/N$ is a pure inseparable extension of the image of $K$ under the natural homomorphism $\phi$.

Chapter II is an investigation of the structure of a pure inseparable extension $F$ of a field $K$ with characteristic $p \neq 0$. In this investigation the interrelationships of $p$-bases of $F$ and $K$ and a set of generators of $F|K$ are studied.

Chapter III gives some rather restrictive conditions
under which the field $R/N = F$ has an isomorphic image in $R$
that contains $K$. It is shown that if $R$ is a primary local
algebra, $N^\lambda = (0)$, then $R$ has such a subfield if $F$ has a
finite set of generators over $\varphi(K)$, if $\varphi(K)$ has a $p$-basis
$Y$ such that $Y \cap (F - F^p)$ is $p$-independent in $F$, and if a cer-
tain invariant integer, $e_n$, of $F$ is such that $p^{e_n} \geq \gamma$. Re-
sults of Narita (3) are used in this connection and also in
a brief examination of the case in which $R$ is a complete local
algebra.
II. UNSHRINKABLE SETS AND $p$-INDEPENDENCE IN PURE INSEPARABLE EXTENSIONS

A. Preliminary Considerations

Throughout this dissertation $F$ will denote a field of characteristic $p \neq 0$ that is a pure inseparable extension of a field $K$. For any subset $L$ of $F$ we will denote by $L^p$ the set consisting of the elements of $L$ raised to the $p$-th power. It can be shown that $F^p$ is a field isomorphic to $F$ under the mapping $f \rightarrow f^p$, $f \in F$. It is assumed that $F^p \neq F$, and $F^p \subset K$, $e$ the exponent of $F$ over $K$.

For every element $a$ in $F$ there is then a least non-negative integer $f_a$ such that $a^{p^{f_a}}$ is in $K$. The integer $f_a$ will be referred to as the exponent of $a$ over $K$. The exponent of $a$ over an arbitrary subfield $L$ that contains some power of $a$ is defined analogously.

A finite set of elements $x_1, x_2, \ldots, x_n$ of a subfield $L$ of $F$ is said to be $p$-independent in $L$ if the $p^n$ monomials $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ ($0 \leq i_j < p$) are linearly independent over $L^p$. An arbitrary subset $S$ of $L$ is said to be $p$-independent in $L$ if every finite subset of $L$ is $p$-independent in $L$. A subset $S$ is said to be a $p$-basis of $L$ if $S$ is $p$-independent in $L$ and if $L = L^p(S)$. It can be shown, as in Zariski and Samuel (6), that $p$-bases of $F$ exist and that any two $p$-bases of the same field have the same cardinal number. This number is referred
to as the degree of imperfection of the field. It can be shown, as in Becker and MacLane (1), that if the degree of $F|F^P$ is finite, then $[F:F^P] = p^m$ where the exponent $m$ is the imperfection degree of $F$.

In a discussion of $p$-independence and $p$-bases of a field $F$ it is convenient to define a mapping $\phi$ on subsets of $F$ into subsets of $F$ as follows: if $A$ is any subset of $F$ then $\phi(A) = F^P(A)$. It can easily be shown that the mapping $\phi$ satisfies the following five axioms in which $X$ and $Y$ are subsets of $F$:

1. ($A_1$) If $X \subseteq Y$, then $\phi(X) \subseteq \phi(Y)$.
2. ($A_2$) If $x \in F$ and $X$ a subset of $F$ such that $x \in \phi(X)$, then there exists a finite subset $X' \subseteq X$ such that $x \in \phi(X')$.
3. ($A_3$) For every subset $X$ of $F$ we have $X \subseteq \phi(X)$.
4. ($A_4$) For every subset $X$ of $F$ we have $\phi(\phi(X)) = \phi(X)$.
5. ($A_5$) If $y \in \phi(X, x)$ and $y \notin \phi(X)$, then $x \in \phi(X, y)$.

We will use $L(X, x)$ to denote the field obtained by the adjunction of the set $X \cup \{x\}$ to a field $L$. If $L_1$ and $L_2$ are subsets of $F$ and $L_2 \subseteq L_1$, then $L_1 - L_2$ will be used to denote the complement of $L_2$ in $L_1$; we will also write this as $L_1 \cap c(L_2)$ where $c(L_2)$ denotes the complement of $L_2$ in $F$. In case $L_2 = \{x\}$ we will also write $L_1 - x$ for $L_1 - \{x\}$.

A subset $S$ of $F$ is said to be free with respect to $\phi$ (or simply "free") when for every $x \in S$ it follows that
x \notin \mathcal{Q}(S - x). Using axiom \((A_2)\) it is easy to see that \(S\) is free if and only if every finite subset of \(S\) is free. Zariski and Samuel (6) show that \(S\) is \(p\)-independent in \(F\) if and only if \(S\) is free.

Axiom \((A_5)\) above is referred to as the exchange property. This may be stated in a slightly more general form: Let \(L\) be a subfield of \(F\), \(S\) a subset of \(F\), \(x \in L\), \(y \in F\). If \(y \notin \mathcal{L}^p(S)\) and \(y \in \mathcal{L}^p(S, x)\), then \(x \in \mathcal{L}^p(S, y)\). The proof of axiom \((A_5)\) on page 129 of Zariski and Samuel (6) carries over to a proof of the preceding statement. Another exchange property that will be used frequently in the sequel is given by the following theorem and corollaries.

Theorem 1. If \(x\) and \(y\) are in \(F\), \(y \notin K\), \(y \in \mathbf{K}(x)\), then \(x \in \mathbf{K}(y)\) or \(y \in \mathbf{K}(x^p)\) where \(f\) is the exponent of \(x\) over \(K(y)\).

Proof. From the assumptions we have the equation

\[ b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0 - y = 0, \quad (1) \]

where \(n = p^e - 1\) and \(b_1 \in \mathbf{K}\). The left member of (1) is a polynomial in \(x\) over \(K(y)\). If the degree is less than \(p\), then \(x\) is separable over \(K(y)\) and hence \(x \in K(y)\) since \(x\) is also pure inseparable over \(K(y)\). Let us assume then that the degree is not less than \(p\) and delete from the left member of (1) all proper subsets (not containing \(y\)) of terms whose sum is zero. The resulting equation then has the form
\[ \sum_{\sigma_1 \in S} b_{\sigma_1} x^{\sigma_1} - y = 0, \quad (2) \]

where \( S \) is a subset of \( \{0, 1, \ldots, p^e - 1\} \). Let \( \sigma_1 = p^{t_1} + r_1 \), \( 0 \leq r_1 < p \), and put \( a = x^p \) so \( x^{\sigma_1} = s^{t_1} x^{r_1} \). After we collect like powers of \( x \) equation (2) has the form

\[ \sum_{\alpha_1 \in T} c_{\alpha_1} x^{\alpha_1} - y = 0, \quad (3) \]

where \( T \) is a subset of \( \{0, 1, \ldots, p - 1\} \), and the coefficients, \( c_{\alpha_1} \), are in \( K(x^p) \). If the left member of (3) is not the zero polynomial then \( x \) is separable over \( K(y, x^p) \), which implies that \( x \in K(y, x^p) \). In this case \( K(y, x^p) = K(y, x) \) and therefore \( x \) is separable over \( K(y) \), which implies that \( x \in K(y) \). Assume then that the left member of (3) is the zero polynomial. The term that does not contain \( x \) is

\[ \sum_{\sigma_1 \in S'} b_{\sigma_1} (s) v_1 - y \]

where \( v_1 \) is \( \sigma_1 \) divided by \( p \) and \( S' \) is a subset of \( \{0, p, 2p, \ldots, p^e - p\} \). Since we assumed that no proper subset of the left member of (2) sums to zero we have a contradiction unless \( S' = S \). That is, unless \( y \in K(x^p) \).

If \( x \notin K(y) \) there is then a least positive integer \( r \) such that \( y \in K(x^{p^r}) = K(x^{p^r+p}, x^{p^r}) \) and \( y \notin K(x^{p^{r+1}}) \). If in the preceding argument we replace \( x \) by \( x^{p^r} \) and \( K \) by \( K(x^{p^{r+1}}) \) we
obtain the conclusion \(x^{pr} \in K(x^{pr+1}, y)\) or \(y \in K(x^{pr+1}, x^{pr+1})\). Since \(y \notin K(x^{pr+1})\) by assumption, we have \(x^{pr} \in K(x^{pr+1}, y)\). From this we obtain \(K(x^{pr+1}, y) = K(x^r, y)\) which implies that \(x^{pr}\) is separable over \(K(y)\) and thus \(x^{pr} \in K(y)\) since \(x^{pr}\) is also pure inseparable over \(K(y)\). Obviously \(f \leq r\), so we have the desired result.

Corollary 1. If \(y \notin K\) and \(y \in K(x)\), then \(K(y) = K(x^f)\), where \(f\) is the exponent of \(x\) over \(K(y)\).

Corollary 2. If \(y \in K(x^p) - K(x^{p+1})\), then \(x^p \in K(y) - K(y^p)\).

Proof. Since \(K(x^p, x^{p+1}) = K(x^p), x^p \in K(x^{p+1}, y)\) or \(y \in K(x^{p+1}, x^{p+f})\) where \(f\) is the exponent of \(x^p\) over \(K(x^{p+1}, y)\). Since \(y \notin K(x^{p+1}), x^p \in K(x^{p+1}, y)\). That is, \(K(x^{p+1}, y) = K(x^p, y)\), which implies that \(x^p\) is separable over \(K(y)\). Since \(x^p\) is also pure inseparable over \(K(y)\), \(x^p \in K(y)\). Now \(K(y) \neq K(y^p)\), for otherwise \(y \in K\). Assume that \(x^p \in K(y^p)\). It follows that \(K(x^p) \subseteq K(y^p)\), which gives \(y \in K(y^p)\) and \(K(y) = K(y^p)\). By the usual argument \(y \in K\), which is a contradiction.

To generalize the concept of \(p\)-independent elements we make the following definition in which \(f\) is an arbitrary positive integer. A finite set of elements \(x_1, x_2, \ldots, x_n\) of \(F\) is said to be \(p^f\)-independent in \(F\) if the \(p^n\) monomials \(x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}(0 \leq i_j \leq p^f - 1)\) are linearly independent over \(F^{p^f}\). An arbitrary subset \(S\) of \(F\) is said to be \(p^f\)-independent in \(F\)
if every finite subset of $S$ is $p^f$-independent in $F$. We define a mapping $\sigma$ on the subsets of $F$ as follows: if $S$ is a subset of $S$, $\sigma(S) = F^{p^f}(S)$. A subset $S$ of $F$ is said to be free with respect to $\sigma$ when for every $x \in S$ it follows that $x \notin \sigma(S - x)$. It is easily seen that the mapping $\sigma$ satisfies the first four axioms mentioned previously. If in Theorem 1 we take for $K$ the field $F^{p^f}(S)$ we obtain a weaker version of axiom $(A_5)$. It is natural to ask if a subset $S$ of $F$ is free with respect to $\sigma$ if and only if $S$ is $p^f$-independent in $F$. We will give a partial answer to this question in the following two paragraphs.

Let $T = \{x_1, x_2, \ldots, x_n\}$, $x_1 \in F$. Assume $T$ is not free with respect to $\sigma$. We then have $x_n \in F^{p^f}(x_1, x_2, \ldots, x_{n-1})$, rearranging subscripts if necessary. Since the $x_i$'s are algebraic over $F^{p^f}$ this means that $x_n$ may be written as some polynomial in $x_1, x_2, \ldots, x_{n-1}$ with coefficients in $F^{p^f}$. We have then $x_n - g(x_1, \ldots, x_{n-1}) = 0$ which means that the set $T$ is not $p^f$-independent in $F$. It is easily seen that a subset $S$ is free with respect to $\sigma$ if and only if every finite subset of $S$ is free with respect to $\sigma$. Hence if $S$ is $p^f$-independent, then $S$ is free with respect to $\sigma$.

Let $T$ be the set of the preceding paragraph and assume that $T$ is free with respect to $\sigma$. Assume that

$$\sum_{\alpha \in I} a_\alpha x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} = 0,$$

(4)
where I is a subset of the set of all n-tuples, 
\( \{(i_1, i_2, \ldots, i_n)\} \), in which \( 0 \leq i_j < p^f \). The monomial
\( x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n} \) has the coefficient \( a_\alpha \) where \( \alpha = (i_1, \ldots, i_n) \).

We assume that the coefficients \( a_\alpha \) are in \( F^p \) and we may
assume that \( i_j = 0 \) in some summand for \( j = 1, 2, \ldots, n \).
Also we may assume that no proper subset of the summands has
a sum equal to zero. Let \( g_1 \) denote the exponent of \( x_1 \) over
\( F^p((T - x_1)) \). Put \( a_1 = x_1^{g_1} \) and \( K_1 = F^p(T - x_1), i = 1, 2, \ldots, n \). Let \( k \) be some integer, \( 1 \leq k \leq n \). Every exponent \( i_k \) can be written as \( i_k = p^k t_k + r_k, 0 \leq r_k < p^k \). In
every term of the left member of (4) replace \( x_k^{i_k} \) by \( a_k t_k r_k \).
After collecting terms we have a polynomial in \( x_k \) of degree
less than \( p^k \) with coefficients in \( K_k \). This must be the zero
polynomial since the degree of \( x_k \) over \( K_k \) is \( p^k \). The term
that does not involve \( x_k \) consists of the sum of the terms in
(4) in which the exponent on \( x_k \) is a multiple of \( p^k \). There
is at least one such term since we assumed \( i_j = 0 \) in at least
one term for \( j = 1, 2, \ldots, n \). Since no proper subset of
terms has a sum equal to zero we conclude that \( r_k = 0 \) for
every exponent \( i_k \) of \( x_k \). It follows then that every exponent
of \( x_j \) in (4) is a multiple of \( p^j \), \( j = 1, 2, \ldots, n \). We
have shown that if \( T \) is free with respect to the only possible sets of monomials \( x_1^{i_1}\ldots x_n^{i_n} \) that are not \( p^f \)-independent are those sets of monomials in which \( i_j = p^j t_j \) after dividing
out factors common to all monomials in the set. It is worthy of note that if $g_i = f$ for $i = 1, 2, \ldots, n$, then $T$ is $p^i$-independent when $T$ is free with respect to $\sigma$.

B. $p$-Bases and the Sets $G$, $H$, and $M$

A subset $S$ of $F$ will be said to be unshrinkable with respect to a subfield $L$ of $F$ when $L(S)$ is not contained in $L(S')$ where $S'$ is any proper subset of $S$. In all the considerations that follow $M$ will denote a subset of $F$ such that $F = K(M)$. It has been shown by Becker and MacLane (1) that if $F$ is a finite extension of $K$ the minimum number of generators (the multiplicity) of $F|K$ is $r$, the exponent determined by the degree $[L:L^p(K)] = p^r$.

Unless indication is made to the contrary, it is assumed that $M$ is unshrinkable with respect to $K$. With this restriction on $M$ it is easy to see that $M$ is $p$-independent in $F$. Assume $x \in F^p(M - x), x \in M$. Since $F^p = K^p(M^p)$, we have $x \in K(M - x, x^p)$. Therefore $K(M - x, x^p) = K(M - x, x)$ which implies that $x$ is separable over $K(M - x)$ which in turn implies that $x \in K(M - x)$ since $x$ is pure inseparable over $K(M - x)$. With our restriction on $M$ this is a contradiction so we conclude that $M$ is $p$-independent in $F$. It is clear that in this case no element of $M$ is in $F^p$.

We will assume that $K$ is not contained in $F^p$ and will denote by $J$ the field $K \cap F^p$. Given a $p$-basis $Y$ of $K$ we will
denote by $G$ the elements of $Y$ not in $J$, $H$ will denote the elements of $Y$ in $J$. $Y$ will always denote a $p$-basis of $K$ and $W$ will always denote a $p$-basis of $F$.

Before constructing a $p$-basis of $F$ consisting of $M$ (assuming $M$ is finite) and a subset of a $p$-basis of $K$ we will state and prove several lemmas.

**Lemma 1.** Let $L$ be a subfield of $F$ and let $\mathcal{P}$ be a $p$-basis of $L$. If $a$ is an element of $F$ with positive exponent $f$ over $L$ and $\mathcal{P} \in \mathcal{P}$ such that $a^{\mathcal{P}} \in L^p(\mathcal{P} - \mathcal{P})$, then $\mathcal{P} \notin L^p(\mathcal{P} - \mathcal{P}, a)$.

**Proof.** Let $Z = L^p(\mathcal{P} - \mathcal{P})$ and assume $\mathcal{P} \in Z(a)$. Since $\mathcal{P} \notin Z$ we have $\mathcal{P} \in Z(a^{\mathcal{P}^r})$ and $\mathcal{P} \notin Z(a^{\mathcal{P}^{r+1}})$ for some integer $r$, $0 \leq r < f$. By Corollary 2 of Theorem 1, $a^{\mathcal{P}^r} \in Z(\mathcal{P}^r) = K$, which is a contradiction since $r < f$.

**Lemma 2.** Let $x \in M$. If $x^{\mathcal{P}} \in K^p(M - x)$, then $x^{\mathcal{P}} \in K^p(M - x^p)$.

**Proof.** If $x^{\mathcal{P}} \in K^p(x_1^p, x_2^p, \ldots, x_j^p, x_{j+1}, \ldots, x_s^p)$ and $x^{\mathcal{P}} \notin K^p(x_1^p, x_2^p, \ldots, x_j^p, x_{j+1}^p, x_{j+2}, \ldots, x_s^p)$ where $x_i \in M$, then again by Corollary 2 of Theorem 1 we have $x_{j+1}^p \notin K^p(M - x_{j+1})$. This is a contradiction since $M$ is assumed to be unshrinkable with respect to $K$.

**Corollary.** If $M' \subseteq M - x$ and $f$ is the exponent of $x$ over $K(M')$, then $x^{\mathcal{P}} \notin K^p(M')$.

**Lemma 3.** If $a \in K \cap (F - F^p)$, then $a \notin F^p(M)$.

**Proof.** Since $F^p(M) = K^p(M^p, M) = K^p(M)$ we need only
show a \( \notin K^P(M) \). Assume a \( \in K^P(x_1, \ldots, x_s), x_1 \in M \). Set \( Z^P = K^P(x_1^P, \ldots, x_s^P) \). Since a \( \notin Z^P \) there is an integer \( t \leq s \) such that a \( \notin Z^P(x_1, \ldots, x_{t-1}) \) and a \( \in Z^P(x_1, \ldots, x_t) \). By the exchange property, \( x_t \in Z^P(x_1, \ldots, x_{t-1}, a) \) and thus \( x_t \in K(M - x_t, x_t^P) \). But this implies that \( x_t \) is separable over \( K(M - x_t) \) and therefore \( x_t \in K(M - x_t) \), a contradiction.

**Theorem 2.** If \( M = \{x_1, \ldots, x_n\} \) and \( Y \) is any \( p \)-basis of \( K \), then there exists a \( p \)-basis \( W \) of \( F \) such that \( W = M \cup Y' \) where \( Y' \subseteq Y \).

**Proof.** Let \( K_1 = K(x_1, \ldots, x_1) \), and let \( e_1 \) be the exponent of \( x_1 \) over \( K_{1-1} \), \( a_1 = x_1^{e_1} \), for \( i = 1, 2, \ldots, n \), \( K_0 \) we will understand to be \( K \). We will first show that if \( a_1 \notin Y \), then \( W_1 = \{Y - a_1, x_1\} \) is a \( p \)-basis of \( K_1 \). Clearly \( K_1^P(W_1) = K^P(W_1) = K_1 \). If \( x_1 \notin K^P(Y - a_1) = K(x_1^P) \), then \( x_1 \) is separable over \( K \) and hence in \( K \) since \( x_1 \) is also pure inseparable over \( K \). This is a contradiction since \( M \) is unshrinking. Let \( y \in \{Y - a_1\} \) and assume \( y \notin K^P(W_1 - y) = K^P(W_1 - y) = K^P(Y - y, x_1) \). This is a contradiction by Lemma 1 so \( W_1 \) is \( p \)-independent in \( K_1 \). If \( a_1 \notin Y \) we still have \( a_1 \notin K^P(Y) \), say \( a_1 = \sum k_1^P \ldots y_1^P \ldots y_t^P \). This expression for \( a_1 \) is unique since \( Y \) is \( p \)-independent in \( K \). Therefore \( a_1 \notin K^P(Y - y_1) \) and by the exchange property \( y_1 \notin K^P(Y - y_1, a_1) \). We will next show that \( Y' = \{Y - y_1, a_1\} \) is a \( p \)-basis of \( K \). Clearly \( K^P(Y') = K \). By the choice of \( y_1 \),
$a_1 \notin K^p(Y' - a_1)$. Let $y \in \{Y' - y_1\}$ and assume $y \in K^p(Y' - y)$. Since $y \notin K^p(Y - y_1 - y)$ we have $a_1 \in K^p(Y - y_1)$ by the exchange property. This is a contradiction so we have established that $Y'$ is a p-basis of $K$. Since $Y'$ contains $a_1$ we have already shown that $\{Y' - a_1, x_1\} = \{Y - y_1, x_1\}$ is a p-basis of $K_1$. To continue the proof, assume that

$W_r = \{Y - Y_r\} \cup \{x_1, x_2, \ldots, x_r\}$ is a p-basis of $K_r$ that has been obtained by repeated applications of the construction described for $K_1$. $Y_r$ denotes the subset of $Y$ that the $x_1$'s replaced. If $a_{r+1} \in W_r$ then $W_{r+1} = \{W_r - a_{r+1}, x_{r+1}\}$ is a p-basis of $K_{r+1}$. It is easily seen that $K^p_{r+1}(W_{r+1}) = K^p_r(W_r, x_{r+1}) = K_{r+1}$, since $a_{r+1} \neq x_1$. If $x_{r+1} \in K_{r+1}(W_r - a_{r+1})$, then $x_{r+1} \in K_r(x^p_{r+1})$. This implies that $x_{r+1}$ is separable over $K_r$ and we obtain the contradiction $x_{r+1} \notin K_r$. Let $w \in \{W_r - a_{r+1}\}$ and assume

$w \in K^p_{r+1}(W_{r+1} - w) = K^p_r(W_r - a_{r+1} - w, x_{r+1})$. That is, $w \in K^p_r(W_r - w, x_{r+1})$ which is a contradiction by Lemma 1. If $a_{r+1} \in W_r$ we still have $a_{r+1} \in K^p_r(W_r)$,

$$a_{r+1} = \sum c^p_{i_1} \ldots i_s z^i_1 \ldots z^i_s$$

where the $z^i_1$'s are in $W_r$, the coefficients in $K^p_r$, and this expression is unique. Now at least one of the $z^i_1$'s must be in $Y$ by the Corollary to Lemma 2, denote this element by $y_{r+1}$. We will show that $W'_r = \{W_r - y_{r+1}, a_{r+1}\}$ is a p-basis of $K_r$. 


Since \( a_{r+1} \notin K_r^p (W_r - y_{r+1}) \) we have by the exchange property that \( y_{r+1} \notin K_r^p (W_r - y_{r+1}, a_{r+1}) \). Thus it is clear that 
\[ K_r^p (W_r') = K_r. \]
By the choice of \( y_{r+1} \), \( a_{r+1} \notin K_r^p (W_r' - a_{r+1}) \). Let 
\[ z \in W_r - y_{r+1} \] and assume \( z \in K_r^p (W_r' - z) = K_r^p (W_r - y_{r+1} - z, a_{r+1}) \). Since \( z \notin K_r^p (W_r - y_{r+1} - z) \) we have \( a_{r+1} \notin K_r^p (W_r - y_{r+1}) \), but this is a contradiction so we have established that \( W_r' \) is a \( p \)-basis of \( K_r \). \( W_r' \) contains \( a_{r+1} \) so we may apply the preceding argument and conclude that \( \{ W_r - y_{r+1}, x_{r+1} \} \) is a \( p \)-basis of \( K_{r+1} \). This construction process can be continued to obtain the set \( \{ Y - Y_n \} \cup M \) as a \( p \)-basis for \( K_n = F \).

We next state and prove some facts concerning \( p \)-bases and unshrinkable sets. These will be stated as lemmas, some of which will have application in the proof of the next theorem on the existence of a \( p \)-basis of \( K \) with a subset \( G' \) such that \( M \cup G' \) is a \( p \)-basis of \( F \). In case \( M \) is finite we know that any \( p \)-basis of \( K \) has such a subset by the theorem just proved.

Before proceeding we note that if \( L \) is a subfield containing \( K \) then \( K \cap L^p \) is of course a field and is in fact the \( p \)-th power of another subfield that contains \( K \). This is easily seen by considering the mapping \( k^p \rightarrow k \) for \( k \in K \cap L^p \).

Lemma 4. Assume \( F \supseteq L_2 \supseteq L_1 \supseteq K \) and put \( J_1 = K \cap L_1^p \), \( J_2 = K \cap L_2^p \). There exists a subset \( B^* \) of \( J_2 - J_1 \) such that \( J_2 = J_1 (B^*) \) and \( B^* \) is unshrinkable with respect to \( J_1 \).
Proof: Put $B = J_2 - J_1$ and assume a well-ordering of $B$:

$$B = \{a_1, a_2, \ldots, a_\alpha, \ldots\} = \{a_\sigma\} \sigma \in \mathcal{I}$$

Define $f(a_1) = \{a_1\}$, and assume $f(a_\alpha)$ has been defined for all $\alpha < \alpha_0$, $\alpha_0 \in \mathcal{I}$. Let $\emptyset$ denote the null set. Define

$$f(a_{\alpha_0}) = \emptyset$$

if $a_{\alpha_0} \notin J_1(\bigcup_{\alpha < \alpha_0} f(a_\alpha))$, and

$$f(a_{\alpha_0}) = \{a_{\alpha_0}\}$$

if $a_{\alpha_0} \notin J_1(\bigcup_{\alpha < \alpha_0} f(a_\alpha))$.

By transfinite induction $f(a_\sigma)$ has been defined for all $\sigma \in \mathcal{I}$. Let $B^* = \bigcup_{\mathcal{I}} f(a_\sigma)$. Obviously $J_1(B^*) \subseteq J_2$. Let $a_\alpha \in J_2 - J_1$. If $a_\alpha \in B^*$ then $a_\alpha \in J_1(B^*)$. If $a_\alpha \notin B^*$ then $a_\alpha \in J_1(\bigcup_{\beta < \alpha} f(a_\beta)) \subseteq J_1(B^*)$. Hence $J_1(B^*) = J_2$. Let $a_\beta \in B^*$ and assume $a_\beta \in J_1(B^* - a_\beta)$. We may assume

$$a_\beta \in J_1(a_{\beta_1}, \ldots, a_{\beta_t}), \beta_t = \max \{\beta_i\}_{1=1}^t.$$ If $\beta > \beta_t$ we have a contradiction from the construction of $B^*$. Since $J_1$ is the $p$-th power of a field containing $K$ we have

$$a_{\beta_t} \in J_1(a_{\beta_1}, \ldots, a_{\beta_t-1}, a_{\beta_1})$$

by the exchange property. This also is a contradiction from the construction of $B^*$ and we have established that $B^*$ is unshrinkable with respect to $J_1$.

Lemma 5. If $B$ is a $p$-independent subset of the field $K$ and $C$ is a subset of $K$ that is unshrinkable with respect to $K^p(B)$, then $B \cup C$ is $p$-independent in $K$.

Proof. Let $D = B \cup C$ and assume $d \in K^p(D - d)$, $d \in D$. Then $d \in K^p(b_1, \ldots, b_r, c_1, \ldots, c_s)$, $b_i \in B$, $c_j \in C$. Now $d \notin C$ for $d \in K^p(B, C - d)$ is a contradiction. Assume $d \in B$. 

Since \( d \notin K^p(\mathbf{b}_1, \ldots, \mathbf{b}_r) \) there is an integer \( t \) such that
\[
\begin{align*}
d &\notin K^p(\mathbf{b}_1, \ldots, \mathbf{b}_r, \mathbf{c}_1, \ldots, \mathbf{c}_{t-1}) \\
&\in K^p(\mathbf{b}_1, \ldots, \mathbf{b}_r, \mathbf{c}_1, \ldots, \mathbf{c}_{t-1}, \mathbf{c}_t), \quad t \leq s. \end{align*}
\]
By the exchange property \( c_t \notin K^p(B, C - c_t) \), a contradiction. Hence
\( d \notin K^p(D - d) \) and \( B \cup C \) is \( p \)-independent in \( K \).

Lemma 6. If \( B \) is a subset of \( K \) that is \( p \)-independent in \( K \), then \( B \) can be extended to a \( p \)-basis of \( K \).

Proof. Let \( L = K^p(B) \) and assume we have a well-ordering of the elements of \( K - L \):
\[
\{a_1, a_2, \ldots, a_\alpha, \ldots\} = \{a_\sigma\}_{\sigma \in I}.
\]
Define \( f(a_\sigma), \quad \sigma \in I \), as in the proof of Lemma 4 with \( J_1 \) replaced by \( L \). Let \( C = \bigcup_{\sigma \in I} f(a_\sigma) \) and put \( Y = B \cup C \). Clearly \( K^p(Y) = K \). Let \( a_\alpha \in C \) and assume \( a_\alpha \notin K^p(B, C - a_\alpha) \). Since \( a_\alpha \notin K^p(B) \) we may use the exchange property as in the proof of Lemma 4 to arrive at a contradiction. Hence \( C \) is unshrinking with respect to \( K^p(B) \) and by Lemma 5 \( Y \) is \( p \)-independent in \( K \).

Lemma 7. If \( B \) and \( C \) are disjoint subsets of \( F \) that are \( p \)-independent in \( F \), then \( B \) is unshrinking with respect to \( F^p(C) \) if and only if \( C \) is unshrinking with respect to \( F^p(B) \).

Proof. Assume \( B \) is not unshrinking with respect to \( F^p(C) \), say \( b \in B \) and \( b \notin F^p(C, B - b) \). Now \( b \notin F^p(B - b) \) so there are elements \( c_1 \in C \) such that \( b \in F^p(B - b, c_1, \ldots, c_{r-1}) \) and \( b \in F^p(B - b, c_1, \ldots, c_r) \). By the exchange property
c_r \in F^P(B, c_1, \ldots, c_{r-1}) so C is not unshrinkable with respect to F^P(3). The converse follows by a similar argument.

Theorem 3. There exists a p-basis Y of K with a subset G' such that W = M \cup G' is a p-basis of F.

Proof. Let J = K \cap F^P. By Lemma 4 there exists a subset H of J - K^P such that J = K^P(H) and H is unshrinkable with respect to K^P, that is, H is p-independent in K. Assume a well-ordering of the elements of K - J:

\{ a_1, a_2, \ldots, a_\alpha, \ldots \} = \{ a_\sigma \} \sigma \in I.

Define f(a_\alpha), \alpha \in I, as in the proof of Lemma 4 with J_1 replaced by F^P. Let G' = \bigcup_{\sigma \in I} f(a_\sigma). Using the argument of Lemma 4 we can establish that G' is unshrinkable with respect to F^P. Since J \subset F^P, G' is unshrinkable with respect to K^P(H) and since G' is p-independent in F (therefore certainly in K), G' \cup H is p-independent in K by Lemma 5. If K^P(H, G') is a proper subset of K we can extend H \cup G', by Lemma 6, to a p-basis Y = H \cup G' \cup G'' of K. Put W = M \cup G'. Since F^P(G') contains G'' (by the construction of G') and J it contains K. Hence F^P(W) = K(M) = F. We have noted previously that if M is unshrinkable with respect to K, then M is p-independent in F. Let g \in G' and assume g \in F^P(M, G' - g). Since g \notin F^P(G' - g) there are elements x_1 \in M such that
g \notin F^P(G' - g, x_1, \ldots, x_{r-1}) and
g \in F^P(G' - g, x_1, \ldots, x_{r-1}, x_r).
By the exchange property $x_r \in F^P(G', x_1, \ldots, x_{r-1})$. It follows that $x_r \in K(M - x_r, x_r^P)$ which implies, by a familiar argument, $x_r \in K(M - x_r)$. This is a contradiction so we have established that $G'$ is unshrinkable with respect to $F^P(M)$. By Lemma 5, $M \cup G'$ is p-independent in $F$ and the proof is complete.

We will collect together in the next theorem several facts concerning the sets $G$, $H$, and $M$ that are easily obtained from the preceding material. It is assumed that $Y = G \cup H$ is a $p$-basis of $K$ constructed in such a fashion that $J = K^P(H)$ and the set $H$ was extended to $Y$ as in Lemma 6.

Theorem 4. (1) $K^P(H) \cap K^P(G) = K^P$

(2) $K^P(G) \subseteq K^P \cup \{K \cap c(F^P)\}$

(3) $K \cap c(F^P) \cap F^P(M) = \emptyset$

(4) $F^P(M) \cap K^P(G) = K^P$

Proof. Let $k \in K^P(H) \cap K^P(G)$, $k \notin K^P$. Since $k \notin K^P$ we may assume $k \notin K^P(g_1, \ldots, g_{r-1})$ and $k \in K^P(g_1, \ldots, g_r)$ for some elements $g_i \in G$. This implies $g_r \in K^P(g_1, \ldots, g_{r-1}, k)$; that is, $g_r \in J(G - g_r)$. But this is a contradiction since $G$ was constructed unshrinkable with respect to $J = K^P(H) = K \cap F^P$.

(Equivalently, we may say that $G$ was constructed $p$-independent in $J^P^{-1}$.) Hence $k \in K^P$ and we have established (1). If $k \in K^P(G)$ and $k \notin K^P$ then $k \notin J$ by (1) and consequently $k \in K \cap c(F^P)$. To establish (3) let $k \in K \cap c(F^P)$. By Lemma 3,
k \notin \mathcal{F}^p(M) \text{ so the intersection is empty. Assume } k \in \mathcal{F}^p(M) \cap \mathcal{K}^p(G)\text{ and } k \notin \mathcal{K}^p. \text{ By (1) } k \notin \mathcal{F}^p(H) \text{ and } k \text{ is therefore in } \mathcal{K} \cap c(\mathcal{F}^p). \text{ But in this case } k \notin \mathcal{F}^p(M) \text{ by (3) and the proof is complete.}

If the elements of } K - J \text{ are well-ordered and a set } G \text{ is constructed (by the method of Lemma 4) that is } p\text{-independent in } K, \text{ it is perhaps not the case that if this set } G \text{ is extended to } Y = G \cup H \text{ the set } H \text{ is such that } J = \mathcal{K}^p(H). \text{ We can however make the following observation. If } G \text{ is } p\text{-independent in } \mathcal{J}^{p-1}, \text{ then } \mathcal{K}^p(H) = J. \text{ For if } a \in J - \mathcal{K}^p(H) \text{ we have } a \notin \mathcal{K}^p(H, g_1, \ldots, g_{s-1}) \text{ and } a \in \mathcal{K}^p(H, g_1, \ldots, g_s) \text{ for some } g_i \in G. \text{ This implies } g_s \in \mathcal{K}^p(H, a, g_1, \ldots, g_{s-1}), \text{ but since } \mathcal{K}^p(H, a) \subset J \text{ this is a contradiction if } G \text{ is } p\text{-independent in } \mathcal{J}^{p-1}.

Assume now that } M = \{x_1, \ldots, x_n\} \text{ and let } e_1 \text{ be the exponent of } x_1 \text{ over } K_{1-1} = K(x_1, \ldots, x_{1-1}), f_1 \text{ the exponent of } x_1 \text{ over } K = K_0. \text{ Put } J_1 = K \cap \mathcal{K}^p_1. \text{ By Lemma 4 there exists a subset } H_1 \text{ of } J_1 - J_{1-1} \text{ such that } J_1 = J_{1-1}(H_1) \text{ and } H_1 \text{ is unshrinkable with respect to } J_{1-1}. \text{ Since } J_0 = \mathcal{K}^p, H_1 \text{ is } p\text{-independent in } K; \text{ by Lemma 5, } H_1 \cup H_2 \text{ is also } p\text{-independent in } K. \text{ We see that we may continue this argument and obtain a set } H = \bigcup_{i=1}^n H_i \text{ such that } H \text{ is } p\text{-independent in } K \text{ and } \mathcal{K}^p(H) = J = J_n. \text{ It is perhaps worthy of note that if } H_1 \text{ is empty then } f_1 > e_1. \text{ (That the converse is not true is seen by Example 2, page 34.) From the construction of } H_1 \text{ we}
know that $H_1$ is empty if and only if $J_1 = J_{1-1}$. If $H_1$ is empty, then $a_1^{f_1} \in K_{1-1}$ and consequently $a_1^{f_1-1} \in K_{1-1}$. Hence $e_1 \subseteq f_{1-1}$.

Theorem 8 of Pickert (4) states that any $p$-basis $Y$ of $K$ remains $p$-independent in no inseparable extension of $K$. In the case that $F = K(x_1)$ we can make the following observation: $Y \cap K^p(x_1^p)$ is not empty if and only if $Y \cap c(K^p(x_1^p))$ is $p$-independent in $K(x_1)$. We know from the construction process of Theorem 2 that there is some $y \in Y$ such that $\{Y - y, x_1\}$ is a $p$-basis of $K(x_1)$. If we assume $Y \cap K^p(x_1^p)$ is not empty, then $\{y\} = Y \cap K^p(x_1^p)$ for $\{Y - y\} \cap K^p(x_1^p) = \emptyset$ since $\{Y - y\}$ is $p$-independent in $K(x_1)$. In this case $Y \cap c(K^p(x_1^p)) = \{Y - y\}$. Assume $Y \cap c(K^p(x_1^p))$ is $p$-independent in $K$. If $Y \cap K^p(x_1^p)$ is empty then $Y$ is $p$-independent in $K(x_1)$. But this is a contradiction since $Y$ remains $p$-independent in no inseparable extension of $K$.

Since it is assumed throughout the discussion that $M$ is a subset of $F$ such that $F = K(M)$ and $M$ is unshrinkable with respect to $K$ it is natural to inquire under what conditions is the existence of such a set guaranteed. It is shown in the next theorem that the set $G$ being $p$-independent in $F$ is such a sufficient condition. In the next section we will therefore present a few results concerning the $p$-independence of $G$ in $F$.

Theorem 5. If $K = J(G)$ and $G$ is $p$-independent in $F$, \[ \text{...} \]
then there exists a set $M$ such that $F = K(M)$ and $M$ is unshrinkable with respect to $K$.

Proof. It is shown on page 88 of Pickert (4) that if $B$ is a $p$-basis of $F$, then $F = \mathcal{F}^f(B)$ for any positive integer $f$. Since $G$ is $p$-independent in $F$ it can be extended to a $p$-basis $W$ of $F$. Say $W = G \cup M$. We then have

$$F = \mathcal{F}^p(G, M) = \mathcal{F}^p(G, M) = J(G, M) = K(M),$$

since $F^p \subset J$ and $J(G) = K$. If $F = K(M - x)$, $x \in M$, we have

$$F = K(M - x) = J(G, M - x) = \mathcal{F}^p(G, M - x)$$

which contradicts the assumption that $G \cup M$ is a $p$-basis of $F$. Hence $M$ is unshrinkable with respect to $K$.

C. $G$ $p$-Independent in $F$

In this section we continue to assume that $M$ is unshrinkable with respect to $K$. We assume also that the $p$-basis $Y = G \cup H$ is constructed so that $K^p(H) = J$. This last restriction is not necessary however in the following theorem.

Theorem 6. Let $Y = G \cup H$ be any $p$-basis of $K$. $G$ is $p$-independent in $F$ if and only if $G \cup M$ is a $p$-basis of $F$.

Proof. Assume $G$ is $p$-independent in $F$. $\mathcal{F}^p(G)$ contains $K^p$, $H$, and $G$ and thus contains $K$. Thus $\mathcal{F}^p(G, M)$ contains $K(M) = F$. By an argument employed in the proof of Theorem 3, $G$ is unshrinkable with respect to $\mathcal{F}^p(M)$. $M$ is $p$-independent in $F$ so $G \cup M$ is $p$-independent by Lemma 5. The converse is immediate since every subset of a $p$-independent set is
p-independent.

In the second paragraph following the proof of Theorem 4 it was indicated that in the case of finite $M$ it is possible to construct sets $H_1$ in $J_1 - J_{1-1}$ such that $J = K^P(\bigcup_{i=1}^n H_i)$. The proof of the following theorem will indicate how this might be generalized to a denumerable $M$. The notation used will be that of the paragraph to which reference was just made.

Theorem 7. If $M = \{x_1, x_2, \ldots\}$ and $J_1 - J_{1-1} \neq \emptyset$, $1 \in I = \{1, 2, \ldots\}$, then there exists a $p$-basis $Y = H \cup G$ of $K$ such that $J = K^P(H)$, $K = J(G)$, and $G \cup M$ is a $p$-basis of $F$.

Proof. Let $a \in K$, $a \in K^P(x_1^r)$, $a \notin K^P(x_1^{p+1})$, where $r$ is less than $f_1$, the exponent of $x_1$ over $K$. By Corollary 2 of Theorem 1 we have $x_1^p \notin K$, a contradiction. Hence $J_1 = K^P(a) = K$, a contradiction. Hence $J_1 = K^P(a_1^p)$. Let $H_1$ denote a subset of $J_1 - J_{1-1}$ such that $J_1 = J_{1-1}(H_1)$ and $H_1$ is unshrinkable with respect to $J_{1-1}$, $1 \in I$. We know these sets exist, and by assumption are non-empty, from Lemma 4. Let $H = \bigcup_{1 \in I} H_1$. We note that $\bigcup_{1 \in I} H_1$ contains at least $r$ elements. Let $k \in J = K \cap F^P$.

Since $k \in F^P = K^P(M^P)$, there is some positive integer $t$ such that $k \in K^P(a_1^p, \ldots, a_t^p) = K_t^P$. Therefore $k \in J_t = K \cap K_t^P$. Hence $J = \bigcup_{1 \in I} J_1$. We will next establish that $K^P(\bigcup_{1 \leq r} H_1) = J_r$, $r \in I$. This is true for $r = 1$ by construction of $H_1$. Assume $K^P(\bigcup_{1 \leq r} H_1) = J_{t-1}$. Since $J_t = J_{t-1}(H_t)$ we have
\( J_t = K^P( \bigcup_{1 \leq t} H_1) \) and the induction principle gives the desired result. Let \( a \in J \). Then \( a \in J_t \) for some \( t \) and hence \( a \in K^P( \bigcup_{1 \leq t} H_1) \subset K^P(H) \). Let \( b \in K^P(H) \). Then \( b \in K^P( \bigcup_{1 \leq t} H_1) \) for some \( t \). So \( b \in J_t \subset J \). Hence \( K^P(H) = J \). \( H_1 \) is \( p \)-independent in \( K \) by construction. Assume \( \bigcup_{1 \leq t} H_1 \) is \( p \)-independent in \( K \). Since \( J_{t-1} = K^P( \bigcup_{1 \leq t-1} H_1) \) and \( H_t \) is unshrinkable with respect to \( J_{t-1} \) we have by Lemma 5 that \( \bigcup_{1 \leq t} H_1 \) is \( p \)-independent in \( K \). Let \( y \in H_1 \) and assume \( y \in K^P(H - y) \). Then \( y \in K^P(Z_{1_1}, \ldots, Z_{1_r}) \), \( Z_{1_j} \subset H_{1_j} \), and \( y \notin Z_{1_j} \). If \( t = \max\{s, i_1, \ldots, i_r\} \), then \( y \in K^P( \bigcup_{1 \leq t} H_1 - y) \). But this is a contradiction since \( \bigcup_{1 \leq t} H_1 \) is \( p \)-independent in \( K \). By Lemma 6, \( H \) can be extended to a \( p \)-basis \( Y = H \cup G \) of \( K \) and obviously \( J(G) = K \). From Theorem 2 we know we can construct for every \( K_1 \) a \( p \)-basis \( W_1 = Y_1 \cup M_1 \) where \( M_1 = \{x_1, \ldots, x_i\} \) and \( Y_1 = Y - \{y_1, \ldots, y_i\} \), \( y_1 \in Y \). Let \( W = \bigcap_{i \in I} Y_1 \cup M \). We will show that \( W \) is a \( p \)-basis of \( F \). If \( y_1 \notin G \), then \( W_1 \) contains an element from \( H_1 \subset K_1^P \) since the number of elements of \( H \) in \( K_1^P \) is at least 1 and in this case at most \( i-1 \) elements have been deleted from \( H \). \( W_1 \) contains then an element of \( K_1^P \) which is impossible if \( W_1 \) is a \( p \)-basis of \( K_1 \). Hence \( G \subset W_1 \), \( i \in I \). Since \( F_1^P(W) \) contains \( G, J, \) and \( M \) we have \( F_1^P(W) = K(M) = F \). Assume we have a polynomial \( g \) in elements from \( W \) with coefficients in \( F \) such that
\[
g(a_1, \ldots, a_r, x_{1_1}, \ldots, x_{1_s}) = 0, \quad x_{1_j} \in M \quad \text{and} \quad a_i \in \bigcap_{i \in I} Y_1.
\]
Since $F^P = K^P(M^P)$ the coefficients of $g$ are all from $K^P_t$, for some $t$. If $m = \max\{t, i_1, \ldots, i_s\}$ the above polynomial is a polynomial with coefficients in $K^P_m$ in elements from $W_m$ and is therefore the zero polynomial since $W_m$ is $p$-independent in $K_m$. $W$ is therefore a $p$-basis of $F$. This implies that $\bigcap_{i \in I} X_i = G$ since any other elements would be in $H \subset F^P$. The proof is now complete.

In the case that $M = \{x_1, \ldots, x_n\}$ it is possible to give a condition equivalent to $G$ $p$-independent in $F$. We will state this as a theorem. As before $e_i$ will denote the exponent of $x_i$ over $K_{i-1} = K(x_1, \ldots, x_{i-1})$.

**Theorem 8.** If $M = \{x_1, \ldots, x_n\}$, then $G$ is $p$-independent in $F$ if and only if $x_1^{p e_i} \notin K^P(G, x_1, \ldots, x_{i-1})$ for $i = 1, 2, \ldots, n$.

**Proof.** Assume $a_1 = x_1^{p e_i} \notin K^P(G, x_1, \ldots, x_{i-1})$. It is a consequence of Lemma 2 that $a_1 \notin K^P(x_1, \ldots, x_{i-1})$. We therefore have $a_1 \notin K^P(g_1, \ldots, g_{i-1}, x_1, \ldots, x_{i-1})$ and $a_1 \notin K^P(g_1, \ldots, g_r, x_1, \ldots, x_{i-1})$ for some elements $g_1$ in $G$. Since $g_r \in K$ we may use the exchange property to obtain $g_r \in K^P(G - g_r, x_1, \ldots, x_i)$. If $g_r \notin K^P(G - g_r, x_1^P, x_2^P, \ldots, x_i^P)$ then $x_1 \in K(M - x_1)$, a contradiction. We may continue this argument and obtain $g_r \in K^P(G - g_r, x_1^P, \ldots, x_i^P) \subset F^P(G - g_r)$. Hence $G$ is not $p$-independent in $F$. If $G$ is not $p$-independent in $F$ then $g \in F^P(G - g)$ for some $g \in G$. Therefore $g \in K^P(x_1^P, \ldots, x_r^P, G - g)$.
and \( g \notin K_1^p(x_1^p, \ldots, x_{r-1}^p, G - g) \) for some integer \( r \leq n \) since \( G \) is \( p \)-independent in \( K \). Consequently there is some integer \( q \leq e_r \) such that \( g \in K_1^p(x_1^p, \ldots, x_r^p, G - g) \) and \( g \notin K_1(x_1^p, \ldots, x_r^p, G - g) \). Using Corollary 2 of Theorem 1 we have \( x_r^p \in K_1^p(x_1^p, \ldots, x_{r-1}^p, G - g) \). Hence \( q \geq e_r \) and we conclude \( x_r^p \in K_1(G, x_1, \ldots, x_{r-1}) \).

If \( F \) is a finite extension of \( K \), Theorem 11 of Pickert (4) states that the imperfection degrees of \( F \) and \( K \) are equal. In the case that \( F|K \) is finite and the imperfection degrees are finite we can easily obtain another criterion for the \( p \)-independence of \( G \) in \( F \). We know from the proof of Theorem 3 that there is a subset \( G' \) of \( G \) such that \( G' \cup M \) is a \( p \)-basis of \( F \). For the number of elements in any set \( L \) we will use the notation \( n(L) \). If we assume that \( G \) is \( p \)-independent in \( F \) then \( G \cup M \) is a \( p \)-basis of \( F \) and we have \( n(G) + n(M) = n(G) + n(H) \). Assume now that \( n(M) = n(H) \). Since \( n(G') + n(M) = n(H) + n(G) \) we have then \( n(G') = n(G) \) and \( G \) is \( p \)-independent in \( F \). We have shown that \( G \) is \( p \)-independent in \( F \) if and only if \( n(M) = n(H) \). It follows immediately that if \( H \subseteq G_1 \) and \( H \subseteq G_2 \) are \( p \)-bases of \( K \), then \( G_1 \) is \( p \)-independent in \( F \) if and only if \( G_2 \) is \( p \)-independent in \( F \).

D. \( M^* \) \( p \)-Independent in \( K \)

The set with which this section is concerned is defined as follows: Let \( M \) and let \( f_x \) denote the exponent of \( x \) over
K for all \( x \in M \). \( \overline{M}^* = \{ x^{p^f x} \mid x \in \overline{M} \} \). For convenience in the following discussion let \( M_1 \) denote the set of elements in \( M \) with exponent 1 over \( K \), \( i = 1, 2, \ldots, e \). In terms of these sets, \( M^* = \bigcup_{i=1}^e M_1^p \). It is seen from Lemmas 4 and 5 that there exist sets \( H_i \subseteq M_1^p \) such that \( \bigcup_{i=1}^r H_i \) is \( p \)-independent in \( K \) and \( K^p(\bigcup_{i=1}^r H_i) = K^p(\bigcup_{i=1}^r M_1^p) \). In the case that \( F \) is finite over \( K \) and the degrees of imperfection are finite it is clear that \( M^* \) is \( p \)-dependent in \( K \) if and only if \( n(H_i) < n(M_1) \) for some \( i \). If \( K^p(M^*) = J \) we can obtain a \( p \)-basis \( G \bigcup_{i=1}^e \{ \bigcup_{i=1}^r H_i \} \) of \( K \). If \( G \) is \( p \)-independent in \( F \), then we must have \( n(M) = \Sigma n(H_i) \) in the finite case. This implies \( n(M_1) = n(H_1) \), \( i = 1, 2, \ldots, e \) and we conclude that \( M^* \) is \( p \)-independent in \( K \) under these assumptions.

After the following lemma (which does not assume finite \( M \)) it will be easy to see that if \( M \) is denumerable then \( M^* \) \( p \)-independent in \( K \) implies \( G \) \( p \)-independent in \( F \).

**Lemma 8.** If \( M^* \) is \( p \)-independent in \( K \), then \( x^{p^f x - 1} \notin K(M - x) \) for all \( x \in M \).

**Proof.** Let \( x \in M \) and assume \( x^{p^f x - 1} \notin K(\overline{M}) \) where \( \overline{M} = \{ x_1, x_2, \ldots, x_p \} \). Since \( \overline{M}^* \cup \{ x^{p^f x} \} \) is \( p \)-independent in \( K \), this set can be extended to a \( p \)-basis \( Y \). As in the proof of Theorem 2 we can show that \( \{ Y - \overline{M}^* \} \cup \{ x_1, \ldots, x_p \} \) is a \( p \)-basis of \( K(x_1, \ldots, x_p) = K_p \). (The elements removed from \( Y \) must have been in \( \overline{M}^* \) for otherwise the \( p \)-basis of \( K_p \) would contain an element in \( K_p^D \).) Therefore \( \{ x^{p^f x}, x_1, \ldots, x_p \} \) is
Lemma 8 implies that $J_1 - J_{1-1}$ contains the first power of $x_1$ that is in $K$. In this case $M \cup G$ is a $p$-basis of $F$ by Theorem 7 if $M$ is denumerable. ($J_1 = K \cap K^P_1$, $K_1 = K(x_1, \ldots, x_i), x_i \in M$.)

Theorem 9. If $M^*$ is $p$-independent in $K$ and $M \subseteq M$, then $K \cap K^P(M^p) = K^P(M^*)$.

Proof. Let $a \in K \cap K^P(M^p), a \notin K^P$. Then for some $x_1$'s in $M$ we have $a \in K^P(x_1^p, \ldots, x_r^p)$ and we may assume that none of the $x_1$'s can be deleted. For some integer $q_1 \leq f_{x_1}$ we have $a \in K^P(x_1^{q_1}, x_2^p, \ldots, x_r^p)$ and $a \notin K^P(x_1^{q_1+1}, x_2^p, \ldots, x_r^p)$. By Corollary 2 of Theorem 1 we have $x_1^{q_1} \in K(x_2, \ldots, x_r)$ so $q_1 \geq f_{x_1}$ by Lemma 8. Hence $q_1 = f_{x_1}$. This argument can be repeated to obtain $a \in K^P(M^*)$. Obviously $K^P(M^*) \subseteq K \cap K^P(M^p)$ and the proof is complete.

Corollary. If $M^*$ is $p$-independent in $K$, then $K^P(M^*) = J$.

Proof. Take $\bar{M} = M$ since $J = K \cap F^p = K \cap K^P(M^p)$.

E. Transcendence Bases and $p$-Bases

We will collect together in this section a few easily-obtained observations concerning transcendence bases and $p$-bases. Throughout the discussion $Q$ will denote the maximal perfect subfield of $K$. 
It is easy to see that if $K$ is a pure transcendental extension of $\mathbb{Q}$ with transcendence basis $T$, then $T$ is a $p$-basis of $K$. Clearly $K^p(T) = K$. If $t$ is an element of $K^p(T - t)$, then $t$ is an element of $\mathbb{Q}(T - t, t^p)$ and we have

$$t = \frac{f(t_1, \ldots, t_s, t^p)}{g(t_1', \ldots, t_r', t^p)},$$

which gives the equation

$$t \cdot g(t_1', \ldots, t_r', t^p) - f(t_1, \ldots, t_s, t^p) = 0.$$

Since $t \neq t_1', t \neq t_j'$, the polynomial on the left is not the zero polynomial and we have a contradiction. Hence $t$ is not an element of $K^p(T - t)$ and $T$ is a $p$-basis of $K$.

If a transcendence basis $T$ of $K|\mathbb{Q}$ is $p$-independent in $K$, then $T$ is a separating transcendence basis of $K|\mathbb{Q}$ and is also a $p$-basis of $K$. By the preceding paragraph we know that $T$ is a $p$-basis of $\mathbb{Q}(T)$. $K$ must be a separable extension of $\mathbb{Q}(T)$ since Theorem 8 of Pickert (4) states that a $p$-basis of a field is $p$-independent in no inseparable extension. Theorem 16 of Teichmüller (5) states that a $p$-basis of a field is a $p$-basis of any separable extension of that field, hence $T$ is a $p$-basis of $K$.

It is clear from the above that if $T$ is a separating transcendence basis of $K|\mathbb{Q}$, then $T$ is a $p$-basis of $K$. Thus if $M^*$ is contained in a separating transcendence basis of $K|\mathbb{Q}$, $M^*$ is $p$-independent in $K$. By the Corollary of Theorem 9, $K^p(M^*) = K \cap F^p$ in this case.
If $M$ is a finite set and the degree of imperfection of $K$ is finite (and therefore equal to the degree of imperfection of $F$ by Theorem 11 of Pickert (4)) and $K$ is separably generated over $Q$, it is seen that $W$, a $p$-basis of $F$, and $Y$, a $p$-basis of $K$, are transcendence bases of $F|Q$. For $Y$ is algebraically independent over $Q$ by Theorem 15 of Teichmüller (5) and is therefore a transcendence basis of $K|Q$ since $Y$ and $T$ contain the same number of elements. $W$ is also algebraically independent over $Q$ and must therefore be a transcendence basis of $F|Q$.

F. Minimum-degree ordering of $M$

If $F$ is a finite pure inseparable extension of $K$ and $n$ the minimum number of generators of $F|K$, then any set of $n$ generators can be so ordered, say $x_1, x_2, \ldots, x_n$, such that for $i = 1, 2, \ldots, n$ the following relations hold:

1) $x_i^{q_i} \in K(x_1^{q_1}, \ldots, x_{i-1}^{q_{i-1}})$, $q_i = p^{e_i}$, $e_i > 0$,

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

3) $e_1 \geq e_2 \geq \ldots \geq e_n$.

For a proof of this see Theorem 14 of Pickert (4). Such an ordering of a set of generators will be referred to as a canonical ordering, a set of generators so ordered will be referred to as a canonical set of generators, and the exponents $e_1$ will be referred to as canonical exponents. It is
also established in the above-mentioned theorem that these 
canonical exponents are invariants of $F|K$; that is, the 
canonical exponents of any two canonical sets of generators 
are equal.

Assume now that $M = \{x_1, \ldots, x_n\}$ is an unshrinkable set 
of generators of $F|K$. Let $e_1$ denote the exponent of $x_1$ over 
$K(M - x_1)$, $i = 1, 2, \ldots, n$, and let $e^*_i = \min\{e_1, \ldots, e_n\}$. 
Say $e_{j_1} = e^*_i$ and let $M^{(1)} = \{M - x_1\}$. We now repeat this 
process and select from $M^{(1)}$ an element $x_{j_2}$ with exponent $e_{j_2}$ 
over $K(M^{(1)} - x_{j_2})$ not greater than the exponent of $x_1$ over 
$K(M^{(1)} - x_1)$ for all $x_1 \in M^{(1)}$. Proceeding in this manner 
until $M$ is exhausted we obtain an ordering $x_{j_n}$, $x_{j_{n-1}}$, $\ldots$, $x_{j_1}$ 
of $M$ which we will refer to as a minimum-degree ordering. The 
exponents $e_{j_n}$, $\ldots$, $e_{j_1}$ will be referred to as minimum-degree 
exponents.

Theorem 10. If $M = \{x_1, \ldots, x_n\}$ is an unshrinkable set 
of generators of $F|K$ that has been ordered by minimum-degree, 
$e_1$ the minimum-degree exponent of $x_1$, $i = 1, 2, \ldots, n$, then 

(1) $x_1^{e_1} \epsilon K(x_1^{e_1}, \ldots, x_{i-1}^{e_{i-1}}),$

(2) $x_1^{p_{e_1-1}} \notin K(x_1, \ldots, x_{i-1}),$

(3) $e_1 \geq e_2 \geq \ldots \geq e_n.$

Proof. (2) is an immediate consequence of the definition. Assume $e_1 < e_{i+1}$. This means that the exponent of
$x_1$ over $K(x_1, \ldots, x_{i-1})$ is less than the exponent of $x_{i+1}$ over $K(x_1, \ldots, x_1)$ so the exponent of $x_1$ over $K(x_1, \ldots, x_{i-1}, x_{i+1})$ is less than the exponent of $x_{i+1}$ over $K(x_1, \ldots, x_1)$. But this is impossible in a minimum-degree ordering so $e_{i+1} \leq e_1$. By definition of $e_1$, $x_1^{p_{e_1}} \in K(x_1, \ldots, x_{i-1})$. Assume $x_1^{p_{e_k}} \notin K(x_1, \ldots, x_{i-2})$. There is then an integer $q$ such that $x_1^{p_{e_1}^p} \in K(x_1, \ldots, x_{i-2}, x_1^{-p})$ and $x_1^{p_{e_1}^q} \notin K(x_1, \ldots, x_{i-2}, x_1^{-p})$. This implies $x_1^{p_{e_1}^q} \in K(x_1, \ldots, x_{i-1})$. Since $x_1$ was selected rather than $x_{i-1}$ in the ordering we must have $q \geq e_1$. By repeated applications of this argument we obtain $x_1^{p_{e_1}^q} \in K(x_1^{p_{e_1}^q}, \ldots, x_1^{p_{e_1}^q})$.

**Theorem 11.** A canonical ordering of a finite set of generators of $F|K$ is a minimum-degree ordering and the canonical exponents are minimum-degree exponents.

**Proof.** Let $M = \{b_1, \ldots, b_n\}$ be a canonical set of generators of $F|K$ with canonical exponents $e_1, \ldots, e_n$. Theorem 31 of Pickert (4) states that the $i$-th exponent ($i = 1, 2, \ldots, n$) is the minimum of the first exponents of $F$ over the subfields of $F$ that are $(i-1)$-fold extensions of $K$. Let $a_1, \ldots, a_n$ be a minimum-degree ordering of $M$ with minimum-degree exponents $e_1', \ldots, e_n'$. The exponent of $F$ over $K(a_1, \ldots, a_{n-1})$ is clearly $e_n'$. By the theorem just stated we have $e_n \leq e_n'$. By the minimum-degree ordering we have $e_n' \leq e_n$, hence $e_n = e_n'$. In the minimum-degree ordering
of $M$ we thus could have selected $b_n$ for $a_n$. We will assume $a_n = b_n$. Now $\{b_1, \ldots, b_{n-1}\}$ is a canonical set of generators of $K(b_1, \ldots, b_{n-1})$ over $K$ with canonical exponents $e_1, \ldots, e_{n-1}$. The preceding argument with $F$ replaced by $K(b_1, \ldots, b_{n-1})$ can be used to give $e_{n-1}^i = e_{n-1}$ since $\{b_1, \ldots, b_{n-1}\} = \{a_1, \ldots, a_{n-1}\}$ and the exponent of $K(a_1, \ldots, a_{n-1})$ over $K(a_1, \ldots, a_{n-2})$ is clearly $e_{n-1}^i$. In the minimum-degree ordering of $M$ we thus could have selected $b_{n-1}$ for $a_{n-1}$. Continuing this argument gives $e_1^i = e_1$, $i = 1, \ldots, n$. For each $i$ we can assume $a_i = b_i$ so the given canonical ordering is a minimum-degree ordering.

In the following theorem we again restrict $M$ to be finite, $M = \{x_1, \ldots, x_n\}$, and assume a canonical ordering with $e_1, \ldots, e_n$ the canonical exponents. We will again let $K_1 = K(x_1, \ldots, x_1)$.

**Theorem 12.** If $M$ is finite and $e_n$ the $n$-th canonical exponent of $M$, then $J \subset K^{P(M^e_n)}$.

**Proof.** Let $a \in J = K \cap F^P$. We have then $a \in K^P_n(x^n_P)$.

If $a \notin K^P_{n-1}$ there is a positive integer $t$ such that $a \in K^P_{n-1}(x^{pt}_n)$ and $a \notin K^P_{n-1}(x^{pt+1}_n)$. This implies $x^{pt}_n \in K^P_n(a)$ by Corollary 2 of Theorem 1. Therefore $t \geq e_n$ since $K^P_{n-1}(a) \subset K_{n-1}$. Put $q = p^{e_n}$ and assume $a \in K_{r-1}^P(x^q_r, \ldots, x^q_n)$. If $a \notin K_{r-2}^P(x^q_{r-1}, \ldots, x^q_n)$ then there is some positive integer $t$ such that $a \in K_{r-2}^P(x^{pt}_r, x^q_r, \ldots, x^q_n)$ and
As before, we have 
\[ x_{r-1}^p \in \mathbb{K}_{r-2}^p(a, x_r^q, \ldots, x_n^q) \]. By the previous theorem we can assume that \( M \) has a minimum-degree ordering. Therefore \( t \geq e_n \) since otherwise \( x_{r-1} \) would have been selected instead of \( x_n \) in the ordering process. Hence \( a \in \mathbb{K}_{r-2}^p(x_{r-1}, \ldots, x_n^q) \). We conclude that \( a \in \mathbb{K}^p(x_1^q, \ldots, x_n^q) = \mathbb{K}^p(M^{e_n}) \).

A result which will have an application in the following chapter is contained in the next theorem. We assume a \( p \)-basis \( \gamma = \text{HUG} \) of \( \mathbb{K}, \mathbb{G} \subset \mathbb{C}(\mathbb{F}^p) \) as in the preceding sections. Again we assume a canonical set of generators \( M \) with exponents \( e_1, \ldots, e_n \).

Theorem 13. \( J \subset \mathbb{K}^p_f(M^p, M^{p e_n}) \), \( f \) an arbitrary positive integer.

Proof. Put \( q = p^{e_n} \). From the previous theorem we have \( J \subset \mathbb{K}^p(M^q) \). Since \( \mathbb{H} \subset J \) we have \( \mathbb{H}^p \subset \mathbb{K}^p(M^{pq}) \) and since \( \mathbb{K} = \mathbb{K}^p(\mathbb{H}, \mathbb{G}) \) we also have \( \mathbb{K}^p = \mathbb{K}^p(\mathbb{H}^p, \mathbb{G}^p) \). Therefore \( J \subset \mathbb{K}^p(M^q) = \mathbb{K}^p(M^{pq}, M^q) = \mathbb{K}^p(M^q, M^{pq}) \). Assume \( J \subset \mathbb{K}^p_r(M^p, M^q) \). Since \( \mathbb{K}^p_r = \mathbb{K}^p_{r+1}(\mathbb{H}^p, \mathbb{G}^p) \) and \( \mathbb{H}^p \subset \mathbb{K}^p_{r+1}(M^{pq}) \) we have \( J \subset \mathbb{K}^p_r(M^p, M^q) = \mathbb{K}^p_{r+1}(\mathbb{H}^p, \mathbb{G}^p, M^q) = \mathbb{K}^p_{r+1}(M^{pq}, M^q) \). By the induction principle we have \( J \subset \mathbb{K}^p_f(M^p, M^{p e_n}) \) for any positive integer \( f \).

Corollary. If \( G \) is empty, then \( \mathbb{K} \subset \mathbb{F}^{p e_n} \).
G. Examples

In the following examples \( Q \) will denote any perfect field; \( u, v, w, x, y \) are understood to be algebraically independent indeterminates over \( Q \). We recall that Pickert (4) has shown that if \( F|K \) is finite then \( F \) and \( K \) have imperfection degrees that are equal. Also, Becker and MacLane (1) have shown that the number of minimum generators of \( F|K \) is given by the exponent of \([F:F(K)]\).

Example 1. Let \( K = Q(u, x, y), F = K(a_1, a_2) \) where
\[
a_1 = u^{p-2}, \quad a_2 = (xu^{p-1} + y)^{p-1}.
\]
The set \( \{u, x, y\} \) is a \( p \)-basis of \( K \) since \( K \) is a pure transcendental extension of \( Q \). \( F^p = Q(x^p, y^p, u^{p-1}, xu^{p-1} + y) \) so \( x \in F^p \) if and only if \( y \in F^p \). However, \( F = F^p(y, a_1, a_2) \) so \( y \notin F^p \) since otherwise \( F \) would have imperfection degree less than three. Therefore \( G = \{x, y\} \). \( G \) is not \( p \)-independent in \( F \) for \( x \in F^p(y) \). If \( M = \{a_1, a_2\} \) were not unshrinkable, then the degree of imperfection of \( F \) again would be less than three for a \( p \)-independent in \( F \) subset of \( G \) with an unshrinkable set \( M \) is a \( p \)-basis of \( F \).

Example 2. Let \( K = Q(u, v, w, x, y), F = K(a_1, a_2, a_3) \) where
\[
a_1 = u^{p-2}, \quad a_2 = (u + v^p)^{p-2}, \quad a_3 = (u + v^p + w^p)^{p-2}.
\]
In this example \( M^* = \{u, u + v^p, u + v^p + w^p\} \) so \( K^p(M^*) = K^p(u) \). We see that \( v = a_2^p - a_1^p \) is in \( J_2 - J_1 \), \( w = a_3^p - a_2^p \) is in \( J - J_2 \). \( G = \{x, y\} \) is \( p \)-independent in \( F \) for if we
assume $x \in F^p(y)$ we obtain a contradiction to the algebraic independence of $u, v, w, x, y$ over $Q$. $[F:F^p(K)] = p^3$ so $M = \{a_1, a_2, a_3\}$ is unshrinkable.
III. IMBEDDING THE RESIDUE FIELD IN THE LOCAL ALGEBRA

It is not true that a local algebra $R$ over a field $K$ always contains a field over $K$ isomorphic to the residue field of $R$. For an example and a discussion of the imbedding problem in the context of algebraic geometry the reader is referred to page 46 of Chevalley (2).

A. $R$ a Primary Local Algebra over $K$

Throughout this section it is assumed that $R$ is a primary local algebra over a field $K$ of characteristic $p \neq 0$. The radical will be denoted by $N$, $\lambda$ will denote its index of nilpotency: $N^\lambda = (0)$. The field $R/N$, which we assume also has characteristic $p$, will be denoted by $F$; $\phi$ will be the natural homomorphism of $R$ onto $F$ and we identify $\phi(K)$ with $K$ so $\phi$ is the identity map on $K$. It is also assumed, as in the previous chapter, that $F$ is a pure inseparable extension of $K$ with exponent $e$ over $K$. The symbols $G$, $H$, $M$, $M^*$, etc., will have the same meanings in this chapter as in the preceding. However, we assume that $G$ is $p$-independent in $F$.

Lemma 2 of Narita (3) states that $R$ contains a subfield, $\hat{F}$, isomorphic to $F$ such that $\phi(\hat{F}) = F$. First an isomorphic image of $FP^n$ is found (it is assumed $NP^n = (0)$) in $R$ under the mapping $\psi'(\alpha^n) = a^n$ where $\alpha \in F$ and $a$ is any element in $\phi^{-1}(\alpha)$. For every element $w_t$ of a $p$-basis $W$ of $F$ there is selected arbitrarily an element $c_t$ from $\phi^{-1}(w_t)$. Every
element of \( F \) can be written as a polynomial \( \overline{f} \) in elements from \( W \) with coefficients in \( \mathbb{F}^n \). The mapping
\[
\overline{f}(w_{t_1}, \ldots, w_{t_r}) \mapsto f(c_{t_1}, \ldots, c_{t_r}),
\]
where \( f \) is the polynomial obtained from \( \overline{f} \) by replacing the coefficients of \( \overline{f} \) by their images under \( \psi' \), gives an isomorphic image
\[
\hat{F} = \psi(F) \text{ of } F \text{ in } R.
\]

It is clear from the sketch of Narita's proof that \( R \) contains infinitely many subfields isomorphic to \( F \). It is the purpose of this section to give some conditions that guarantee that \( F \) (as obtained in Narita's proof) contains the given field \( K \).

Let \( p^h \leq \chi \). Since \( F \) is a complete set of representative elements for \( R/N \) it is clear that \( \mathbb{F}^p^h \) is a unique field in \( R \) and is equal to \( R^p^h \). (\( R^p^h \) is the set consisting of all elements of \( R \) raised to the \( p^h \) power.) For if \( r \in R \) then
\[
r = \hat{r} + n \quad \text{where } \hat{r} \in \hat{F} \text{ and } n \in N.
\]
Since \( N^p^h = (0) \), \( r^p^h = \hat{r}^p^h \).

Say \( k \in \mathbb{R}^{p^h} \cap K \), \( k = r^p^h \). Since \( [\phi(r)]^p^h = \phi(r^p^h) = k \), we have \( \mathbb{R}^{p^h} \cap K \subseteq \mathbb{F}^{p^h} \cap K \). If there is some \( \hat{F} \) that contains \( K \) it is necessary that \( \mathbb{F}^{p^h} \cap K \subseteq \mathbb{R}^{p^h} \cap K \). For let \( k \in \mathbb{R}^{p^h} \cap K \), say \( k = r^p^h \), \( f \in F \), and let \( \overline{\phi}^{-1} \) denote the inverse of \( \phi: \hat{F} \longrightarrow F \). Now \( \overline{\phi}^{-1} \) is an isomorphism of \( F \) onto \( \hat{F} \) and is the identity on \( K \), so we have
\[
k = \overline{\phi}^{-1}(k) = \overline{\phi}^{-1}(r^p^h) = \left[ \overline{\phi}^{-1}(r) \right]^p^h = r^p^h.
\]
Hence \( k \in \mathbb{R}^{p^h} \cap K \).

It is also necessary that the ring composite \( [\hat{F}^{p^h}, K] \) of \( K \) and \( \hat{F}^{p^h} \) be a field if \( K \) is contained in some \( \hat{F} \). We
assume in the following that \( \bigcap_{p \neq h} F^p, K \) is a field in \( R \) and \( R^p \cap K = F^p \cap K \).

**Lemma 9.** If \( a \in F \) with exponent \( g \) over \( K \), then there is an element \( b \in \varphi^{-1}(a) \) such that \( b^p = a^p \).

**Proof.** Since \( a^p = k \in K \) there are elements \( r_0 \in R, n_0 \in N \), such that \( r_0^p + n_0 = k \) and \( \varphi(r_0) = a \). Let \( \overline{b} \in \varphi^{-1}(a) \), say \( \overline{b} = r_0 + n_1 \). We have \( a^p = r_0^p + n_0 \) since \( R^p \cap K = F^p \cap K \). \( (r - \overline{b})^p \) is an element of \( N \) and it follows that \( r - \overline{b} \) is in \( N \) since \( N \) is a prime ideal. Put \( r - \overline{b} = n_2 \).

Then \( r = r_0 + n_2 + \overline{b} = r_0 + n_2 + n_1 \) and we have \( r \in \varphi^{-1}(a) \).

**Theorem 14.** If \( G \cup M^* \) contains a \( p \)-basis of \( K \) and \( G \) is \( p \)-independent in \( F \), then there exists an \( F \) containing \( K \).

**Proof.** We know from Theorem 6 that \( G \cup M = \hat{W} \) is a \( p \)-basis of \( F \). For every \( x \) \( M \) we can select an element \( r_x \in \varphi^{-1}(x) \) such that \( x^p x = r_x^p x \) (\( f_x \) is the exponent of \( x \) over \( K \)). \( \varphi^{-1}(G) \) is of course \( G \). With this choice for the elements from \( \varphi^{-1}(w) \) we are assured that \( G \cup M^* \) is in \( \hat{F} \).

If \( t \) is an integer such that \( p^t \geq \lambda \) and \( t \equiv e \), then \( F^p t \) is in \( K \) and we can construct \( \hat{F} \) over \( F^p t \). \( \hat{F} \) in this case contains a \( p \)-basis \( Y \) of \( K \) and also \( K^p t \), there fore \( \hat{F} \) contains \( K = K^p t \).

It was pointed out in the preceding chapter that \( n(H) = n(M) \) is equivalent to \( G \) \( p \)-independent in \( F \), in the case \( F \) is a finite extension and the imperfection degrees are finite.
In this finite case the assumptions of the preceding theorem imply that $M^*$ is $p$-independent in $K$. There are, however, other conditions that guarantee that an $\hat{F}$ resulting from Narita's construction contains $K$.

Theorem 15. If $p^h \geq \lambda$, $G$ $p$-independent in $F$, and $H \subset F^h(G, M^*)$, then there exists a field $\hat{F}$ that contains $K$.

Proof. By assumption, $[\varphi(r)]p^e$ is in $K$ for all $r \in R$. For a given $r \in R$, this implies $(r^e + n) \in K$ for some $n \in N$. Since $n$ is nilpotent $n^q = 0$ for some $q$ and we have $r^e + n \in K$. If $a \in F^h(G, M^*)$, $p^h \geq \lambda$, then $\psi(a) \in \hat{F}^h(G, M^*)$ if we take $G \cup M$ as a $p$-basis for $F$ and select the proper elements from $\varphi^{-1}(M)$ as was done in the preceding proof. Say $\psi(a) = \hat{a}$ and assume $\hat{a}^p^e \in K$. Now $\varphi = \psi^{-1}$ so we have $\varphi(\hat{a}^p^e) = [\varphi(\hat{a})]p^e = a^p^e$. Since $\varphi$ is the identity on $K$, if $a \in K \cap F^h(G, M^*)$ we have $\hat{a}^p^e = a^p^e$. Therefore $(\hat{a} - a)^p^e = 0$ and, since $(\hat{a} - a)$ is an element of the field $[\hat{F}^h, K]$, this implies $\hat{a} = a$. $\psi$ is thus the identity map on $K \cap F^h(G, M^*)$. Since $H \subset F^h(G, M^*)$, $H \cup G$ is in $\hat{F}$. Again, $\hat{F}$ contains a sufficiently high power of $K$ since $F^h$ contains $K \cap F^h$ and $F^e \subset K$ by assumption. Hence $\hat{F}$ contains $K$.

In the case that the multiplicity of $F$ is finite, say $n$, it is possible to give another sufficient condition involving the $n$-th canonical exponent, $e_n$, of $F$.

Theorem 16. If $G$ is $p$-independent in $F$ and $p^{e_n} \geq \lambda$, then there exists an $\hat{F}$ that contains $K$. 
Proof. By Theorem 13, \( J \subseteq K^{p^n}(G^p, K^{p^n}) \) for any positive integer \( f \). In particular, \( J \subseteq K^{p^n}(G^p, K^{p^n}) = F^{p^n}(G^p) \).

Obviously \( H \subseteq F^{p^n}(G, M^*) \) so the preceding theorem gives the desired result.

B. \( R \) a Complete Local Algebra over \( K \)

It is possible to define a topology on a local ring \( R \) by taking the powers \( \{N^m\} \) as a neighborhood system for 0, the neighborhoods of an arbitrary \( x \) in \( R \) being the residue classes \( \{x + N^m\} \). A sequence \( (b_n) \) of elements of \( R \) converges to \( b \) if for any integer \( s > 0 \) we can always find an integer \( n_0(s) \) such that \( (b_n - b) \in N^s \) whenever \( n > n_0(s) \). A sequence \( (b_n) \) is a Cauchy sequence if for any integer \( s > 0 \) there exists a positive integer \( n_0(s) \) such that \( (b_n - b_m) \in N^s \) for \( n > m > n_0(s) \). It can be shown that a sequence \( (b_n) \) is a Cauchy sequence if and only if \( b_n - b_{n-1} \to 0 \) as \( n \to \infty \).

A local ring \( R \) is said to be complete if every Cauchy sequence of elements in \( R \) has a limit in \( R \). We assume in this section that the local algebra \( R \) is complete. It is known that every local ring can be completed; the method used is analogous to the usual method of completing a metric space.

Narita (3) has shown that if \( R \) is a complete local ring having the same characteristic \( p \neq 0 \) as the residue field \( F \), then \( R \) contains a subfield \( \hat{F} \) which is isomorphic to \( F \), such that \( \phi(\hat{F}) = F \). As in the preceding section, \( \phi \) denotes
the natural homomorphism of $R$ onto $F = R/N$. A brief summary of Narita's proof follows.

The local rings $R_i = R/N^i$, $i \in I = \{1, 2, \ldots\}$, are primary and every $R_i$ has a residue field isomorphic to $F$. Let $\theta_1$ be the canonical homomorphism of $R$ onto $R_1$, $\varphi_{1,i+1}$ the canonical homomorphism of $R_{i+1}$ onto $R_i$, and $\varphi_1$ the canonical homomorphism of $R_1$ onto $F$, $i \in I$. By the lemma stated in the preceding section, each ring $R_i$ contains a subfield $F_i^*$ isomorphic to $F$. It is possible to construct $F_{i+1}^*$ in such a way that $\varphi_{1,i+1}(F_{i+1}^*) = F_i^*$. Let $\alpha \in F$ and $\alpha_1$ an element of $\varphi_{1}^{-1}(\alpha) \cap F_i^*$, and let $s_1$ be an element of $\theta_1^{-1}(\alpha_1)$, $i \in I$. The sequence $s_1, s_2, \ldots$ is a Cauchy sequence in $R$ and therefore has a limit $s$ in $R$. The correspondence $\alpha \mapsto s$ of $F$ into $R$ gives a required image, $F$, of $F$ in $R$.

This section is concerned with conditions under which the field $F$, as obtained by Narita's method, contains the given field $K$. To this end we prove first several lemmas. Throughout we will let $K_i = \theta_1(K)$.

**Lemma 10.** For any $r \in R$, 
$$\theta_1(r) = \varphi_{i,i+1} \cdots \varphi_{i+n-2,i+n-1} \left[ \varphi_{i+n-1,i+n} \left[ \theta_{i+n}(r) \right] \right] \cdots.$$  

*Proof.* It is easy to show the assertion valid for $n = 1$. The desired result follows immediately by induction.

**Lemma 11.** If $L$ is a field in $R$ that is a complete set of representative elements for the field $R/N$, then $L$ is
properly contained in no overfield in $\mathbb{R}$.

Proof. Assume $L \subseteq L_1 \subseteq \mathbb{R}$, $L_1$ a field. Since $L$ is a complete set of representative elements for $\mathbb{R}/N$, if $a \in L_1$ and $a \not\in L$ there is an element $b \in L$ and an element $n \in N$ such that $a = b + n$. But this is a contradiction for $L_1$ contains no non-zero nilpotent elements.

Lemma 12. $\hat{F}$ is a complete set of representative elements for $\mathbb{R}/N = F$.

Proof. Let $a \in F$, $a \rightarrow a$, $a \in \hat{F}$. The element $a$ is the limit of a Cauchy sequence $(a_n)$. There exists an integer $n_0$ such that for all $n > n_0$, $(a_n - a) \in N$ and therefore $\theta_1(a_n - a) = 0$. But $\theta_1(a_n) = \phi_n(\theta_1(a_n)) = \alpha$ so we have $\theta_1(a) = \theta_1(a_n) = \alpha$.

Lemma 13. $\hat{F}_1 = \hat{\theta}_1(\hat{F})$ is a complete set of representative elements for $\mathbb{R}_1/N_1$ ($N_1 = N/N^1$).

Proof. Let $b \in \mathbb{R}_1/N_1$, $b = \{(r_0 + n + N^1)\}$. Since $\hat{F}$ is a complete set of representative elements for $\mathbb{R}/N$,

$r_0 \in \{\hat{f}_0 + N\}$ where $\hat{f}_0 \in \hat{F}$. Therefore $b = \{(\hat{f}_0 + n + N^1)\} = \{(\hat{f}_0 + N^1) + \{n + N^1\}\} = \{\theta_1(\hat{f}_0) + N_1\} = \sigma_1(\theta_1(\hat{f}_0))$ where $\sigma_1$ is the natural homomorphism of $\mathbb{R}_1$ onto $\mathbb{R}_1/N_1$.

Lemma 14. $\theta_1(\hat{F}) = F^*_1$.

Proof. We will first show that $\theta_1(\hat{F}) \subseteq F^*_1$. Let $a \in \hat{F}$, $a_n \rightarrow a$ and $(a_n - a) \in N^1$ for $n > n_0(1)$. Hence $\theta_1(a) = \theta_1(a_m)$ for some $m > i$, say $m = i + k$. From the definition of the sequence $a_n$, $\theta_{i+k}(a_{i+k}) \in F^*_1$; and from the construction
of $F^*_1$, $\varphi_{1,1+1}(F^*_1) = F^*_1$, $i \in I$. Applying Lemma 10 we obtain $\varphi_1(s_{1+k}) \in F^*_1$. Now $F^*_1$ is a complete set of representative elements for $R_1/N_1$ by construction. (See Narita's proof concerning primary local rings in the preceding section.) Since $\varphi_1(\hat{F})$ is also a complete set of representative elements of $R_1/N_1$ by Lemma 13, we apply Lemma 11 to obtain $\varphi_1(\hat{F}) = F^*_1$.

Theorem 17. $\hat{F}$ contains $K$ if and only if $F^*_1$ contains $\varphi_1(K) = K_1$, $i \in I = \{1, 2, \ldots\}$.

Proof. Assume $K_1 \subseteq F^*_1$, $i \in I$. Let $k \in K$, say $\alpha = \varphi_1(k)$. To find the image of $\alpha$ in $\hat{F}$ we select an arbitrary element $\alpha_1$ from $\varphi_1^{\perp}(\alpha) \cap F^*_1$ and an element $a_1$ from $\varphi_1^{\perp}(\alpha_1)$, $i \in I$. For $\alpha_1$ we may take the element $\varphi_1(k)$, since $K_1 \subseteq F^*_1$ by assumption, and for $a_1$ take $k$ (or any other element of $\varphi_1^{\perp}(k)$). This sequence obviously converges to $k$ so $K \subseteq \hat{F}$. Since $\varphi_1(\hat{F}) = F^*_1$ the converse is immediate.

Corollary. $\hat{F}$ contains $K$ if and only if there is a field $L \supseteq K$ such that $\varphi_1(L) = F^*_1$, $i \in I$.

Proof. Assume $L \supseteq K$ and $\varphi_1(L) = F^*_1$, $i \in I$. $F^*_1$ contains $K_1$, $i \in I$, so $\hat{F}$ contains $K$. For the converse take $L = \hat{F}$.

In view of the preceding theorem it is natural to search for conditions under which $F^*_1$ contains $K_1$. Our attention is thus directed to the restrictions that were imposed to be certain that Narita's $F$ in the primary case contains $K$. One of these assumptions was that $R^p \cap K = F^p \cap K$ for all non-negative integers $p$. We will next show that this implies
\[ F^p_1 \cap K_1 = R^p_1 \cap K_1 \text{ where } F_1 = R_1 / N_1 = (R / N^1) / (N / K^1). \]

We stipulate here that \( \sigma_1(K_1) \), the image of \( K_1 \) under the natural homomorphism of \( R_1 \) onto \( F_1 \), is identified with \( K_1 \).

Let \( k_1 \in F^p_1 \cap K_1 \), say \( k_1 = r^p_1 \). Now \( k_1 = \sigma_1(r^p_1) = \left[ \sigma_1(r_1) \right]^p_1 \) so \( k_1 \in F^p_1 \). Hence \( R^p_1 \cap K_1 \subseteq F^p_1 \cap K_1 \) without the assumption \( R^p_1 \cap K = F^p_1 \cap K \). Let \( k_1 \in F^p_1 \cap K_1 \), say \( k_1 = r^p_1 \), \( f_1 \in F_1 \), \( k_1 = \sigma_1(k) \), \( k \in K \). Now \( F \) is isomorphic to \( F_1 \) under the mapping \( f = \{ r + N \} \rightarrow \{ r_1 + N_1 \} \) where \( r_1 = \{ r + N^1 \} \). Because of the identification of \( \sigma_1(K) \) with \( K \) and \( \sigma_1(K_1) \) with \( K_1 \), this map reduces to \( \theta_1 \) on \( K \), hence \( k \in F^p_1 \cap K_1 \). By assumption we have \( k = r^p_1 \) for some \( r \in R \).

Thus \( f^p_1 = k_1 = \theta_1(k) = \theta_1(r^p_1) = \left[ \theta_1(r) \right]^p_1 \), so \( k_1 \in R^p_1 \).

In the primary case it was also assumed that the ring composite \( \left[ R^p_{h_1}, K \right] \) is a field. (We recall \( R^p_{h_1} = R^p_{h} \).) Let \( h_1 \) be such that \( p_{h_1} \geq \lambda_1 \) where \( \lambda_1 \) is the index of nilpotency of \( R_1 : N_1 \). It is natural to look for conditions such that the ring composite \( \left[ R^p_{h_1}, K \right] \) is a field in \( R_1 \). We will only show that if \( N \) is a nil ideal and \( R / N \) has an exponent over \( K \), then \( \left[ R^p_{h_1}, K \right] \) is a local ring; therefore \( \left[ R^p_{h_1}, K \right] \), the image of \( \left[ R^p_{h_1}, K \right] \) under \( \theta_1 \), is a local ring.

Put \( D = \left[ R^p_{h_1}, K \right] \) and let \( \overline{N} \) be the set of non-units of \( D \).

Obviously \( \overline{D} \supset \overline{D} \cap N \). Let \( a \in \overline{N} \). We are assuming \( F^p_1 \subseteq K \) so \( (a^{p_{h_1}} + n) \) is in \( K \) for some \( n \in N \). Since \( n^{p_q} = 0 \) for some \( q \) we have \( a^{p_{h_1} + q} \in K \). If \( a \notin N \) then \( a^{p_{h_1} + q} \neq 0 \) and \( a^{-1} = k^{-1} a^{-1} \) is in \( D \). Thus if \( a \in \overline{N} \), then \( a \in \overline{N} \). Therefore \( \overline{N} = D \cap \overline{N} \) and
it is easy to verify that $\overline{N}$ is an ideal in $D$ since $N$ is an ideal and $D$ is a ring.
IV. REFERENCES


V. ACKNOWLEDGMENT

The author wishes to express his gratitude to Dr. Bernard Vinograde for suggesting the present problem and for his generous assistance and instruction in the preparation of this thesis.