ON THE GALOIS THEORY OF PURELY INSEPARABLE FIELD EXTENSIONS

BY MURRAY GERSTENHABER AND AVIGDOR ZAROMP1,2

Communicated March 9, 1970

The main purpose of this announcement is to show that those purely inseparable field extensions which behave in a certain sense like normal extensions in fact are of a fundamentally abelian character. Detailed proofs of most results are contained in the second author’s thesis [6].

1. Exponent 1. Throughout \( K \) will be a finite purely inseparable extension of a field \( k \) of characteristic \( p \) and \( \text{Der} K/k \) will denote the \( K \)-space of derivations of \( K \) over \( k \). We consider first the case where \( K/k \) has exponent one. In that case we have

**Theorem 1.** Suppose that \( \phi_1, \cdots, \phi_n \) are commuting derivations of \( K \) over \( k \) which are linearly independent over \( k \). Then

1. They are independent over \( K \).
2. \([K:k]^n \geq n\).
3. Equality holds iff the \( k \)-space \( V_0 \) spanned by \( \phi_1, \cdots, \phi_n \) is closed under the formation of \( p \)th powers, in which case \( V_0 \otimes_k K = \text{Der} K/k \).

Let us call a \( K \)-subspace \( V \) of \( \text{Der} K/k \) **restricted** if \( \phi \in V \) implies \( \phi^p \in V \). From Theorem 1 it is then easy to deduce that:

(i) every restricted subspace of \( \text{Der} K/k \) is spanned by commuting derivations, and

(ii) every restricted \( K \)-subspace \( V \) of \( \text{Der} K/k \) is of the form \( \text{Der} K/L \) for some unique intermediate field \( k \leq L \leq K \).

The latter assertion, an exact analog of the fundamental theorem of the Galois theory for purely inseparable extensions of exponent one, was first proved by Jacobson [2] under the additional hypothesis that \( V \) is a Lie subalgebra of \( \text{Der} K/k \). The stronger form is due to Gerstenhaber [4]. One sees a posteriori that a restricted subspace is necessarily a Lie subalgebra.

The three parts of Theorem 1 are precisely analogous to Theorems 12, 13, and 14 of [1], by means of which Artin demonstrates the usual "fundamental theorem" of the Galois theory.

---

AMS subject classifications. Primary 1360, 1245; Secondary 1240.

Key words and phrases. Inseparable field extensions, higher derivations, approximate automorphisms, Witt polynomials.

1 The authors gratefully acknowledge the support of the NSF through Grant GP-13776 to the University of Pennsylvania.

2 The author’s address is Technical Institute of Alamance, Burlington, North Carolina 27215.
2. Higher exponents. An approximate automorphism of order $m$ ("higher derivation" in the terminology of Jacobson [3]) of $K/k$ is a formal polynomial

$$\Phi_t = 1 + t\phi_1 + t^2\phi_2 + \cdots + t^{m-1}\phi_{m-1}$$

where the $\phi_i$ are $k$-linear maps of $K$ into itself ($1 = \text{id}_K$) such that

$$\Phi_t(ab) = (\Phi_t(a))(\Phi_t(b)) \mod t^m,$$

i.e., $\Phi_t$ is an automorphism of $K[t]/(t^m)$ over $k[t]/(t^m)$. For fixed $m$ these form a group $G_m$, and for every integer $l > 0$ there is a monomorphism $G_m \to G_{lm}$ defined by sending $t$ to $t^l$. This is an isomorphism for $m \geq p^n$, where $n$ is the exponent of $K/k$ [4], so we get $G_{p^n} = G$ and call this "the" group of approximate automorphisms of $K/k$.

An intermediate field $L$ of $K/k$ is the fixed field for a subgroup $H$ of $G$ iff $K$ is modular over $L$, i.e., of the form $L(x_1) \otimes_L \cdots \otimes_L L(x_r)$ for suitable $x_1, \ldots, x_r \in K$ (Sweedler, [5]). We shall describe here those subgroups $H$ which fix the elements of an intermediate field $L$.

An approximate automorphism $\Phi_t$ is abelian if the $\phi_i$ appearing in (1) commute. An abelian family is a subgroup $A$ of $G$ in which all $\phi_i$ appearing in all $\Phi_t$ in $A$ commute with each other. It is a basic fact that if $L$ is the fixed field of some subgroup $H$ of $G$, then it is already the fixed field of some abelian family [4]. If $\Phi_t = 1 + t\phi_1 + t^2\phi_2 + \cdots$ is any approximate automorphism and $a \in K$, then we define maps $T_a$ and $V$ from $G$ into itself by setting

$$T_a\Phi_t = \Phi_t = 1 + at\phi_1 + a^2t^2\phi_2 + \cdots,$$

and

$$V\Phi_t = \Phi_t^p = 1 + t^p\phi_1 + t^{2p}\phi_2 + \cdots.$$

Note that $V$ is an endomorphism of $G$ but $T_a$ generally is not unless $a$ is in $k$. If $\Phi_t$ is abelian, then $P\Phi_t = 1 + t\phi_1^p + t^2\phi_2^p + \cdots$ is also an approximate automorphism; $P$ is an automorphism when restricted to any abelian family.

The exponent of $K/k$ being $n$, all polynomials and power series in $t$ will be understood modulo $t^n$. If $x_0, x_1, \ldots, x_{n-1}$ are variables and

$$w_i(x) = x_0^{p^i} + px_1^{p^{i-1}} + \cdots + p^ix_i, \quad i = 0, \ldots, n - 1,$$

the $i$th Witt polynomial, then

$$e(t, (x)) = \exp \sum_{i=0}^{n-1} \left(\frac{t^i}{p^i}\right) w_i(x)$$
is a polynomial whose coefficients are integral at \( p \), hence meaningful modulo \( p \).

**Theorem 2.** An abelian family is generated by its elements of the form \( e(t, (\theta)) \), where \( (\theta) = (\theta_0, \theta_1, \ldots, \theta_{n-1}) \) is a sequence of (necessarily commuting) \( k \)-linear maps of \( K \) into itself.

A sequence \( (\theta) = (\theta_0, \theta_1, \ldots, \theta_{n-1}) \) of commuting maps of \( K \) into itself such that \( e(t, (\theta)) \) is an approximate automorphism is an extended derivation of order \( n-1 \). It is easy to verify that the first nonzero map amongst the \( \theta \)'s is an ordinary derivation. If this is \( \theta_i \), then we call \( \theta_i \) the leading component of \( (\theta) \), and we say that \( (\theta) \) has degree \( n-i \).

If we have an abelian family \( A \), then the set of all extended derivations \( (\theta) \) such that \( e(t, (\theta)) \) lies in \( A \) will be denoted by \( \mathcal{E}(A) \). Set \( P(\theta) = (\theta_0^p, \theta_1^p, \ldots, \theta_{n-1}^p) \), \( V(\theta) = (0, \theta_0, \ldots, \theta_{n-2}) \). Also, for \( (\theta) \) of the form \( (0, \ldots, 0, \theta_i, \theta_{i+1}, \ldots, \theta_{n-1}) \), we can define

\[
T_a(\theta) = (0, \ldots, 0, a^p\theta_i, a^{p^2}\theta_{i+1}, \ldots, a^{p^{n-1}}\theta_{n-1})
\]

for all \( a \in k^{p^{-i}} \). Then \( P e(t, (\theta)) = e(t, P(\theta)) \), \( V e(t, (\theta)) = e(t, V(\theta)) \), and

\[
T_a e(t, (\theta)) = e(t, T_a(\theta)).
\]

A set \( \mathcal{E} \) of extended derivations of order \( n-1 \) is an abelian family of extended derivations if all components of all \( (\theta) \) in \( \mathcal{E} \) commute and if \( \mathcal{E} \) is a group in the Witt addition. We say that \( \mathcal{E} \) is saturated if with every \( (\theta) \), \( \mathcal{E} \) also contains \( P(\theta) \), \( V(\theta) \), and if for every \( \theta \in \mathcal{E} \) of degree \( n-i \), \( \mathcal{E} \) also contains all \( T_a(\theta) \) with \( a \in k^{p^{-i}} \). We then have

**Theorem 3.** Let \( A \) be an abelian family of extended automorphisms. Then \( A \) is saturated iff \( \mathcal{E}(A) \) is saturated. Every saturated abelian family \( \mathcal{E} \) of extended derivations is of the form \( \mathcal{E}(A) \) for a unique saturated \( A \).

Since the fixed field \( L \) of \( \mathcal{E}(A) \) is the same as that of \( A \), it follows that if \( \mathcal{E} \) is a saturated abelian family of extended derivations then the fields between \( L \) and \( K \) over which \( K \) is modular are in 1-1 correspondence with the saturated subfamilies of \( \mathcal{E} \).

A subset \( S \) of a saturated \( \mathcal{E} \) is a set of generators if it generates \( \mathcal{E} \) using Witt addition and the operators \( V, P \) and \( T_a \), where in \( T_a(\theta) \) we permit \( a \) to be in \( k^{p^{-i}} \) whenever \( (\theta) \) has degree \( n-i \). The set is standard if it is a minimal set of generators in which the leading components of the \( (\theta) \) in \( S \) are all linearly independent over \( k \) which implies that they are such also over \( K \) (Theorem 1). Let \( s_i \) be the number of elements of the standard set \( S \) which are of degree \( n-i \).

**Theorem 4.** If \( L \) is the fixed field of \( S \) (and hence of \( \mathcal{E} \)) then \( K \) is of
the form $L(x_1) \otimes_L \cdots \otimes_L L(x_r)$, where the number of $x$'s having exponent $i$ over $L$ is $s_{n-i}$.

Finally we have

**Theorem 5.** Let $\mathcal{L}$ be a saturated abelian family of extended derivations with fixed field $L$, and $H$ be the subgroup of $G$ generated by all approximate automorphisms of the form $T_{e(t, (\theta))}$, where $(\theta)$ is an extended derivation in $\mathcal{L}$ and $a$ is in $K^{\omega_1}$ whenever the degree of $(\theta)$ is $n-i$. Then $H$ is saturated, i.e., the full subgroup of $G$ consisting of all approximate automorphisms with $L$ as fixed field. Conversely, every saturated $H$ is of this form.

**References**


University of Pennsylvania, Philadelphia, Pennsylvania 19104