ON THE GALOIS THEORY OF PURELY INSEPARABLE FIELD EXTENSIONS

BY MURRAY GERSTENHABER AND AVIGDOR ZAROMP[1,2]

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 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. $[K:k] \geqq n$.
3. *Equality holds iff the k-space V_0 spanned by $\phi_1, \cdots, \phi_n$ is closed under the formation of pth powers, in which case $V_0 \otimes_k K = \text{Der } K/k$.*

Let us call a K-subspace V of 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 Der K/k is spanned by commuting derivations, and

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

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 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

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

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

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

i.e., Φ_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 $m \geqq p^n$, 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 $x_1, \cdots, x_r \in K$ (Sweedler, [5]). We shall describe here those subgroups H which fix the elements of an intermediate field L.

An approximate automorphism Φ_t is **abelian** if the ϕ_i appearing in (1) commute. An **abelian family** is a subgroup A of G in which all ϕ_i appearing in all Φ_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

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

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 Φ_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^{p^n}. If $x_0, x_1, \cdots, x_{n-1}$ are variables and

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

the ith Witt polynomial, then

$$e(t, (x)) = \exp \sum_{i=0}^{n-1} (t^{p^i}/p^i)\, w_i(x)$$

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* $e(t^l, (\theta))$, *where* $(\theta) = (\theta_0, \theta_1, \cdots, \theta_{n-1})$ *is a sequence of (necessarily commuting) k-linear maps of K into itself.*

A sequence $(\theta) = (\theta_0, \theta_1, \cdots, \theta_{n-1})$ 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 θ's is an ordinary derivation. If this is θ_i, then we call θ_i the **leading component** of (θ), and we say that (θ) has degree $n-i$.

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

$$T_a(\theta) = (0, \cdots, 0, a^{p^i}\theta_i, a^{p^{i+1}}\theta_{i+1}, \cdots, a^{p^{n-1}}\theta_{n-1})$$

for all $a \in k^{p^{-i}}$. Then $Pe(t, (\theta)) = e(t, P(\theta))$, $Ve(t, (\theta)) = e(t, V(\theta))$, and $T_a e(t, (\theta)) = e(t, T_a(\theta))$. A set $\mathfrak{L}$ of extended derivations of order $n-1$ is an **abelian family of extended** derivations if all components of all (θ) in $\mathfrak{L}$ commute and if $\mathfrak{L}$ is a group in the Witt addition. We say that $\mathfrak{L}$ is **saturated** if with every (θ), $\mathfrak{L}$ also contains $P(\theta)$, $V(\theta)$, and if for every $\theta \in \mathfrak{L}$ of degree $n-i$, $\mathfrak{L}$ 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* $\mathfrak{L}(A)$ *is saturated. Every saturated abelian family* $\mathfrak{L}$ *of extended derivations is of the form* $\mathfrak{L}(A)$ *for a unique saturated A.*

Since the fixed field L of $\mathfrak{L}(A)$ is the same as that of A, it follows that if $\mathfrak{L}$ 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 $\mathfrak{L}$.

A subset S of a saturated $\mathfrak{L}$ is a **set of generators** if it generates $\mathfrak{L}$ 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 (θ) has degree $n-i$. The set is **standard** if it is a minimal set of generators in which the leading components of the (θ) 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* $\mathfrak{L}$*) 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* $\mathfrak{L}$ *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* $T_a\, e(t, (\theta))$, *where* (θ) *is an extended derivation in* $\mathfrak{L}$ *and a is in* $K^{p^{-i}}$ *whenever the degree of* (θ) *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

1. E. Artin, *Galois theory*, Notre Dame Math. Lectures, no. 2, Univ. of Notre Dame, Notre Dame, Indiana, 1944. MR **5**, 225.

2. N. Jacobson, *Galois theory of purely inseparable fields of exponent one*, Amer. J. Math. 66 (1944), 645–648. MR **6**, 115.

3. ———, *Lectures in abstract algebra*. Vol. III: *Theory of fields and Galois theory*, Van Nostrand, Princeton, N.J., 1964. MR **30** #3087.

4. M. Gerstenhaber, *On the deformation of rings and algebras*. III, Ann. of Math. (2) **88** (1968), 1–34. MR **39** #1521.

5. M. E. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410. MR **36** #6391.

6. A. Zaromp, *On Abelian families of approximate automorphisms of purely inseparable field extensions*, Dissertation, University of Pennsylvania, Philadelphia, Pa., 1968.

UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PENNSYLVANIA 19104