ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 2, Number 2, Spring 1972

ABELIAN EXTENSIONS OF RINGS OF POSITIVE CHARACTERISTIC

ANDY R. MAGID

The Witt theory of fields of characteristic p gives a structure theorem for extension fields which are Galois with a cyclic Galois group of order p^n. This is essentially an additive theory, and hence can be extended without significant change to commutative rings of positive characteristic. The purpose of the present note is to carry out this extension. More precisely, we show the existence of a commutative algebra E_n, free of rank p^n over the ring A_n of polynomials over the integers in n variables, such that if R is a ring of characteristic p^n, $E_n \otimes R$ is a cyclic Galois $A_n \otimes R$ algebra of rank p^n, and if S is any cyclic Galois R-algebra of rank p^n there is a homomorphism from A_n to R such that $E_n \otimes_{A_n} R$ is isomorphic to S. Except for some minor technical details, the arguments here are the same as in the classical theory for fields.

All our rings and algebras are commutative. Z will denote the integers and p a fixed prime number; A_n denotes the polynomial ring $Z[X_0, \cdots, X_{n-1}]$. We assume the reader is familiar with the construction and basic properties of rings of Witt vectors (see, for example, [2, p. 124]). For a ring R, $W_n(R)$ denotes the Witt vectors of length n over R; elements of $W_n(R)$ are n-tuples $(r_0, \cdots, r_{n-1})$. If R has characteristic p, F denotes the endomorphism of $W_n(R)$ given by raising each component to the pth power. By a Galois extension of a ring R we mean an R-algebra satisfying the conditions of [1, 1.3, p. 4].

Let $m_0, m_1, \cdots$ be the polynomials giving addition of Witt vectors, so that $(a_0, \cdots, a_{n-1}) + (b_0, \cdots, b_{n-1}) = (m_0(a_0, b_0), \cdots, m_{n-1}(a_0, \cdots, b_{n-1}))$. Each m_k is in $Z[X_0, Y_0, \cdots, X_k, Y_k]$, and we can write $m_k = X_k + Y_k + f_k$ where f_k is in $Z[X_0, Y_0, \cdots, X_{k-1}, Y_{k-1}]$. Let g_k be the polynomial $Y_k{}^p - Y_k - (X_k + f_k)$.

Definition 1. Let $E_n = A_n[Y_0, \cdots, Y_{n-1}]/(g_0, \cdots, g_{n-1})$.

This definition is motivated as follows: let $\bar{E}_n = E_n \otimes Z/pZ$ and let $\bar{x}_i, \bar{y}_i$ be the images of X_i, Y_i in $\bar{E}_n$. Let $\bar{x} = (\bar{x}_0, \cdots, \bar{x}_{n-1})$, $\bar{y} = (\bar{y}_0, \cdots, \bar{y}_{n-1})$ in $W_n(\bar{E}_n)$. Then $F(\bar{y}) = \bar{y} + \bar{x}$. If S is any Z/pZ algebra and if z, a in $W_n(S)$ are such that $F(z) = z + a$, there is a

Received by the editors February 1, 1971.
AMS 1970 *subject classifications*. Primary 13B05; Secondary 13K05.

unique map from $\bar{E}_n$ to S such that the induced map from $W_n(\bar{E}_n)$ to $W_n(S)$ sends $\bar{y}$ to z and $\bar{x}$ to a. This universal property will be used below.

We study the separability of E_n, beginning with a lemma:

LEMMA 2. *Let R be a ring and suppose the integer n belongs to the radical of R. Let a be in R and let $P = X^n - X - a$. Then $R[X]/(P)$ is a separable R-algebra (and a free R-module).*

PROOF. The freeness is standard. If m is a maximal ideal of R, the characteristic of R/m divides n, so P has derivative -1 in R/m and hence no multiple roots. By [3, 2.2(4), p. 476], the algebra is separable.

PROPOSITION 3. *Let R be any ring.*

(a) *E_n is free of rank p^n over A_n.*

(b) *If p is in the radical of R, $E_n \otimes R$ is separable over $A_n \otimes R$.*

(c) *If $p = 0$ in R, $E_n \otimes R$ is Galois over $A_n \otimes R$ with a cyclic Galois group.*

PROOF. For each k, $k = 0, 1, \cdots, n$, define B_k inductively as follows: $B_0 = A_n$, $B_{k+1} = B_k[Y_{k-1}]/(\bar{g}_k)$, where $\bar{g}_k$ is the image of g_k in $B_k[Y_{k-1}]$. Then each B_k is free of rank p over B_{k-1}, and $B_n = E_n$. This proves (a); a similar induction, using the lemma, proves (b). To prove (c), it suffices to treat the case $R = Z/pZ$. In the notation after Definition 1, in $W_n(\bar{E}_n)$, $F(\bar{y} + 1) = (\bar{y} + 1) + \bar{x}$, so there is a homomorphism f of $\bar{E}_n$ to $\bar{E}_n$ (leaving $A_n \otimes Z/pZ$ invariant) such that the induced map on $W_n(\bar{E}_n)$ sends $\bar{y}$ to $\bar{y} + 1$. Since $W_n(\bar{E}_n)$ has characteristic p^n, this induced map is an automorphism of $W_n(\bar{E}_n)$ of order p^n, and hence so is f. Let $\bar{A}_n = A_n \otimes Z/pZ$, and let G be the cyclic group generated by f. If $F(G, \bar{E}_n)$ is the ring of all functions from G to $\bar{E}_n$, we have a homomorphism $\bar{E}_n \otimes_{\bar{A}_n} \bar{E}_n \to F(G, \bar{E}_n)$ induced by the constants in one factor and evaluation on the other. The image is a separable subalgebra of a separable, projective algebra and hence a direct summand. To complete the proof, we need only show that there is some homomorphism from $\bar{A}_n$ to Z/pZ such that, after tensoring with this homomorphism, the above map is an isomorphism. This will be done below.

LEMMA 4. *Let R be of characteristic p and let S be a Galois R-algebra with group G. Then $W_n(S)$ is a Galois $W_n(R)$ algebra with group G.*

PROOF. The group G lifts to an isomorphic group of automorphisms of $W_n(S)$ whose fixed ring is $W_n(R)$ (the action is componentwise).

The kernel of the map of $W_n(S)$ to S is generated by p, and $p^n = 0$. Thus if m is a maximal ideal of $W_n(S)$, m/pm is a maximal ideal of S. By [1, 1.3, p. 4], given g in G there is an a in S such that $ga - a$ is not in m/pm. If b in $W_n(S)$ maps to a, $gb - b$ is not in m. By [1, 1.3] again, $W_n(S)$ is Galois over $W_n(R)$.

Using Lemma 4, we can move Galois algebras of characteristic p to Galois algebras of characteristic p^n. As in the theory for fields, this will allow us to apply cohomology.

PROPOSITION 5. *Let S be a Galois R algebra with group G, S^+ the additive group of S. Then $H^1(G, S^+) = 0$.*

PROOF. Let (a_g) be a 1-cocycle. $\mathrm{Hom}_R(S, S)$ is an Azumaya R-algebra and a free S-module on the elements of G. Let D be the S-linear endomorphism of $\mathrm{Hom}_R(S, S)$ defined by $D(g) = a_g g$. The cocycle condition implies D is a derivation, hence inner, so there is an element u in S such that $D(g) = gu - ug = (g(u) - u)g$ for all g in G, and (a_g) is the coboundary of u.

PROPOSITION 6. *Let R have characteristic p and let S be a Galois R-algebra with group G cyclic of order p^n. Then there is a homomorphism from A_n to R such that S is isomorphic to $E_n \otimes_{A_n} R$.*

PROOF. $W_n(S)$ is Galois over $W_n(R)$ with group G, and has characteristic p^n. Let g be a generator of G. By Proposition 5 the cocycle $a_g k = k$ is a coboundary, i.e., there is an element z in $W_n(S)$ such that $g(z) = z + 1$. Let $a = F(z) - z$ (so $F(z) = z + a$), then $g(a) = a$, and hence a is in $W_n(R)$. Let $z = (z_0, \cdots, z_{n-1})$, $a = (a_0, \cdots, a_{n-1})$. We have a homomorphism from A_n to R sending X_i to a_i and a homomorphism from E_n to S extending it and sending the class of Y_i to z_i. The latter gives rise to an R-algebra homomorphism h from $E_n \otimes_{A_n} R$ to S. We consider the induced map on $W_n(E_n \otimes_{A_n} R)$. Let $y \otimes 1 = (y_0 \otimes 1, \cdots, y_{n-1} \otimes 1)$, and let k generate the Galois group of $E_n \otimes_{A_n} R$ over R. Then $k(y \otimes 1) = (y \otimes 1) + 1$, which goes via the induced map to $z + 1 = g(z)$. Thus h is G-linear, and an isomorphism by [1, 3.4, p. 12].

We can complete the proof of Proposition 3 (c). Since there is an extension field S of Z/pZ which is Galois with cyclic Galois group G of order p^n, generated by g, by the proof of Proposition 6 there is a homomorphism from $\bar{E}_n = E_n \otimes_{A_n} Z/pZ$ to S. There is an induced homomorphism from $W_n(\bar{E}_n)$ to $W_n(S)$ sending $\bar{y}$ to z, where $g(z) = z + 1$, and thus the only element of G inducing the identity on the image of this homomorphism is the identity. Thus also the image of $\bar{E}_n$ is a separable subalgebra of S on which no nontrivial element of

G acts trivially. Thus the image equals S; since $\bar{\bar{E}}_n$ and S have the same rank the map is an isomorphism, and $\bar{\bar{E}}_n$ *is Galois over* Z/pZ with group G, so that $\bar{\bar{E}}$ $\bar{\bar{E}}$

$$(\bar{E}_n \otimes_{\bar{A}_n} \bar{E}_n) \otimes_{\bar{A}_n} Z/pZ = \bar{\bar{E}}_n \otimes_{Z/pZ} \bar{E}_n \rightarrow F(G, \bar{E}_n)$$

$$= F(G, E_n) \otimes_{A_n} Z/pZ$$

is an isomorphism.

We now extend Proposition 6 to rings of characteristic p^k. To do this we need to know about the behavior of separable algebras under nilpotent base change. More generally, we have the following:

PROPOSITION 7. *Let I be an ideal in the radical of R such that R is separated and complete in the I-adic topology. Let $R_0 = R/I$, and let S and T be separable, projective R-algebras. Let S_0 and T_0 denote $S \otimes_R R_0$, $T \otimes_R R_0$. Then the map* $\mathrm{Hom}_R(S, T)$ *to* $\mathrm{Hom}_{R_0}(S_0, T_0)$ *sending f to $f \otimes R_0$ is a bijection on algebra homomorphisms.*

PROOF. R_0-algebra homomorphisms from S_0 to T_0 correspond bijectively to T_0 algebra homomorphisms from $S_0 \otimes_{R_0} T_0$ to T_0 which in turn correspond to certain idempotents in $S_0 \otimes_{R_0} T_0$ [1, 1.2, p. 3]. Since under our hypotheses we can uniquely lift idempotents from $S_0 \otimes_{R_0} T_0$ to $S \otimes_R T$, the result follows.

THEOREM 8. *Let R be separated and complete in the I-adic topology, where I is an ideal contained in the radical of R and p belongs to I. Then if S is any Galois R-algebra with Galois group cyclic of order p^n, there is a homomorphism from A_n to R such that S is isomorphic to $E_n \otimes_{A_n} R$.*

PROOF. By Proposition 6, S/IS is isomorphic to $E_n \otimes_{A_n} R/I$ for some homomorphism h from A_n to R/I. We can lift h to a homomorphism h' from A_n to R. Then $E_n \otimes_{A_n} R$ is a separable R-algebra, and $(E_n \otimes_{A_n} R) \otimes_R R/I$ is isomorphic to $S \otimes_R R/I$. Thus, by Proposition 7, $E_n \otimes_{A_n} R$ is isomorphic to S.

The theorem applies in particular when characteristic of R is p^k (take $I = pR$), and describes the cyclic extensions of order a power of p. The cyclic extensions of order prime to p (i.e., whose order is a unit in R) have recently been described when roots of unity are present by a generalized Kummer theory due to Lindsay Childs [4]. Combining his results and ours, one arrives at the complete description of abelian Galois extensions of rings of positive characteristic containing sufficiently many roots of unity.

References

1. S. Chase, D. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings,* Mem. Amer. Math. Soc. No. 52 (1965), 15-33. MR 33 #4118.

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

3. G. Janusz, *Separable algebras over commutative rings,* Trans. Amer. Math. Soc. **122** (1966), 461-479. MR 35 #1585.

4. L. Childs, *Abelian Galois extensions of rings containing roots of unity,* Illinois J. Math. **15** (1971), 273-280.

Columbia University, New York, New York 10027