ON A CLASS OF BINOMIAL EXTENSIONS[1]

BY

P. M. COHN

1. Introduction

Let K be a field (not necessarily commutative) with a subfield k. Then the left and right dimensions of the extension K/k need not be equal, as was shown by an example, in [2], of an extension of right dimension two and left dimension greater than two. It is likely that in this example the left dimension is in fact infinite; this seems difficult to verify directly, but with a little more trouble one can construct an extension which is easily seen to have right dimension two and infinite left dimension.[2]

The object of this note is to give such a construction and to show more generally that for any finite $n > 1$ there exists an extension of right dimension n and infinite left dimension. Moreover, the centre of the extension can be almost any preassigned commutative field (see Theorem 5.1 for a precise statement).

2. Pseudo-linear extensions

Let K be a field and k a subfield; then K may be viewed as right k-space or as left k-space. We denote the corresponding dimensions by $[K:k]_R$ and $[K:k]_L$ respectively. We shall say that K/k is *finite of degree n* if $[K:k]_R = n$ is finite. An extension K/k is called *pseudo-linear*, if K is generated, as a ring, by a single element a over k such that

$$\alpha a = a\alpha_1 + \alpha_2 \qquad (\alpha \in k). \tag{1}$$

If we exclude the trivial case $a \in k$, when $K = k$, then the mappings

$$S : \alpha \to \alpha_1, \qquad D : \alpha \to \alpha_2$$

are uniquely determined and it is easily seen that S is an endomorphism of k, while D is an S-derivation. Moreover, since the kernel of S is an ideal of K not containing 1, it must be zero, i.e., S is necessarily a monomorphism. Note that a quadratic extension (i.e., of degree two) is always pseudo-linear [cf. (2)].

It follows from (1) that K is spanned by the powers of a, as right k-space. If all these powers are linearly independent, then we just have the skew polynomial ring $k[a; S, D]$. Clearly, this is not a field, so the powers of a cannot all be right k-independent over k, i.e., a satisfies an equation with right co-

Received March 8, 1965.

[1] This work was partly supported by a grant from the National Science Foundation.

[2] Such a construction was indicated (without proof) in [2]. For other consequences of this example, see [5].

efficients in k. As in the commutative case one sees that the monic polynomial of least degree with a as zero is uniquely determined and if the degree is n, then $[K:k]_R = n$. The following formula for the left dimension of a pseudo-linear extension generalizes Theorem 3 of [2].

THEOREM 2.1. *Let K/k be a pseudo-linear extension of degree n, with endomorphism S; then*

$$[K:k]_L = 1 + [k:k^S]_L + [k:k^S]_L^2 + \cdots + [k:k^S]_L^{n-1}. \tag{2}$$

In particular

$$[K:k]_L \geq [K:k]_R \tag{3}$$

with equality if and only if S is an automorphism.

Proof. By hypothesis K contains an element a such that $1, a, \cdots, a^{n-1}$ is a right k-basis for K, and

$$\alpha a = a\alpha S + \alpha D \qquad (\alpha \in k).$$

Define $K_0 = k$, $K_i = aK_{i-1} + k$ $(i = 1, 2, \cdots, n-1)$; then

$$k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} = K,$$

and each K_i is clearly a right k-space. It is also a left k-space, because for $i > 0$,

$$\alpha K_i = \alpha a K_{i-1} + ak = a\alpha S K_{i-1} + \alpha D K_{i-1} + ak \subseteq K_i$$

if we assume that K_{i-1} is a left k-space. Thus the result follows by induction.

Let (u_λ) be a left k^S-basis for k; we assert that the set of elements

$$a^i u_{\lambda_{i-1}}^{S^{i-1}} u_{\lambda_{i-2}}^{S^{i-2}} \cdots u_{\lambda_1}^{S} u_{\lambda_0} \tag{4}$$

where $(\lambda_{i-1}, \cdots, \lambda_0)$ ranges over all i-tuples (for fixed i) is a left k-basis for $K_i \pmod{K_{i-1}}$. For, given $\alpha \in k$, we have

$$\alpha = \sum \alpha_{\lambda_0}^{S} u_{\lambda_0} = \sum \alpha_{\lambda_1\lambda_0}^{S^2} u_{\lambda_1}^{S} u_{\lambda_0} = \cdots = \sum \alpha_{\lambda_{i-1}\cdots\lambda_0}^{S^i} u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_0},$$

hence

$$a^i\alpha = \sum a^i \alpha_{\lambda_{i-1}\cdots\lambda_0}^{S^i} u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_0} \equiv \sum \alpha_{\lambda_{i-1}\cdots\lambda_0} a^i u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_0} \pmod{K_{i-1}}$$

which shows that the elements (4) span $K_i \pmod{K_{i-1}}$.

Conversely, if

$$\sum \alpha_{\lambda_{i-1}\cdots\lambda_0} a^i u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_0} \equiv 0 \pmod{K_{i-1}}$$

then

$$\sum a^i \alpha_{\lambda_{i-1}\cdots\lambda_0}^{S^i} u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_0} \equiv 0 \pmod{K_{i-1}};$$

hence

$$\sum \alpha_{\lambda_{i-1}\cdots\lambda_0}^{S^i} u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_0} = 0.$$

Since the u's are left k^S-independent, we have

$$\sum \alpha_{\lambda_{i-1}\cdots\lambda_0}^{S^i} u_{\lambda_{i-1}}^{S^{i-1}} \cdots u_{\lambda_1}^{S} = 0 \qquad \text{for all } \lambda_0,$$

and since S is a monomorphism, we can cancel an application of S. Repeating this process, we find after i steps that $\alpha_{\lambda_{i-1}\cdots\lambda_0} = 0$ for all suffixes, hence the elements (4) are left k-independent. This proves that the dimension of K_i/K_{i-1}, as left k-space is $[k:k^S]_L^i$, the number of elements (4), and now (2) follows by addition. The rest follows because $[k:k^S]_L \geq 1$, with equality if and only if $k^{S'} = k$.

3. A construction for binomial extensions of prime degree

A pseudo-linear extension K/k is said to be *binomial* if it has a generating element a which satisfies a binomial equation over k:

$$x^n - \lambda = 0 \qquad (\lambda \in k). \tag{5}$$

We shall not write down the conditions for an arbitrary equation (5) to determine a binomial extension, but confine our attention to a special case which will be used later.

We recall that if E is any field with endomorphism S and S-derivation D, then the ring $E[x; S, D]$ of skew polynomials, $\sum x^i\alpha_i$, with commutation rule

$$\alpha x = x\alpha S + \alpha D$$

is an integral domain satisfying the right multiple condition of Ore [4], and hence it can be embedded in a field. The least such field is determined up to isomorphism and will be denoted by $E(x; S, D)$.

THEOREM 3.1. *Let p be a prime, E any field with an endomorphism S and assume that E contains a primitive p^{th} root of 1, ω say, which lies in the centre of E and is left fixed by S. Let D be an S-derivation of E such that*

$$DS = \omega SD \tag{6}$$

and put $K = E(t; S, D)$. Then S, D may be extended to K by putting

$$tS = \omega t, \qquad tD = (1 - \omega)t^2 \tag{7}$$

and with these definitions

$$ct = tcS + cD \qquad \text{for all} \quad c \in K. \tag{8}$$

Moreover, $\sigma = S^p$ is an endomorphism of E, and $\delta = D^p$ is a σ-derivation, and if k is the subfield of K generated by t^p over E, then $k = E(t^p; \sigma, \delta)$, and K/k is a binomial extension of degree p.

Proof. Since $\omega^p = 1$, we have $p\omega^{p-1}(\omega D) = 0$; now E has primitive p^{th} roots of 1 and so cannot have characteristic p; hence we may divide by p and conclude that $\omega D = 0$. This shows that ω lies in the centre of K.

In order to show that S, D may be extended to $E[t; S, D]$ so as to satisfy (7), we need only verify (8) for monomials, by linearity. By (7),

$$\begin{aligned}(t^n\alpha)S &= \omega^n t^n\cdot\alpha S,\\ (t^n\alpha)D &= \textstyle\sum_{\nu=1}^n t^{\nu-1}\cdot tD\cdot(t^{n-\nu}\alpha)S + t^n\cdot\alpha D\\ &= t^{n+1}(1-\omega)(1+\omega+\cdots+\omega^{n-1})\alpha S + t^n\cdot\alpha D;\end{aligned}$$

hence $(t^n\alpha)D = (1 - \omega^n)t^{n+1}\cdot\alpha S + t^n\cdot\alpha D$. It follows that

$$\begin{aligned} t(t^n\alpha)S + (t^n\alpha)D &= t^{n+1}\cdot\alpha S\omega^n + (1 - \omega^n)t^{n+1}\alpha S + t^n\alpha D \\ &= t^{n+1}\alpha S + t^n\alpha D \\ &= t^n\alpha t \end{aligned}$$

which checks (8). Thus S is an endomorphism of $E[t; S, D]$; since it is one-one, it can be extended to an endomorphism of the quotient field $E(t; S, D) = \mathrm{K}$ in a unique manner (cf. [6] for the commutative case). Likewise, D is an S-derivation of $E[\mathrm{t}; \mathrm{S}, \mathrm{D}]$, which can be extended to K.

That $\sigma = S^p$ is an endomorphism, is clear. Note that so far we have not used equation (6) or the fact that ω is a primitive p^{th} root of 1. These facts will now be used in showing that $\delta = D^p$ is a σ-derivation. For this purpose we rewrite (8) as an operator equation

$$R = LS + D. \tag{9}$$

Here R, L indicate right and left multiplication by t respectively and S, D indicate application of S, D to the coefficient in E. With this convention, $SL = LS$, and $DL = LD$. Thus

$$R^p = (LS + D)^p = \sum L^i f_i(S, D)$$

where $f_i(S, D)$ represents the sum of all products with i factors S and $p - i$ factors D. We get these terms by first writing down S^iD^{p-i}, and then shifting a factor S past a factor D, one at a time. By (6) each such interchange amounts to multiplication by ω, so that altogether we have

$$f_i(S, D) = S^iD^{p-i}(1 + \omega + \omega^2 + \cdots + \omega^{C_{p,i}-1})$$
$$(C_{p,i} = p!/i!(p - i)!).$$

The coefficient on the right is zero unless $i = 0$ or p, therefore

$$R^p = L^pS^p + D^p. \tag{10}$$

In terms of the action on E this states that

$$\alpha t^p = t^p\alpha\sigma + \alpha\delta \qquad (\alpha \in E);$$

hence the subfield k generated by t^p over E is actually of the form $k(t^p; \sigma, \delta)$.

In order to see under what conditions Theorem 3.1 is applicable, we take a field F with an endomorphism S. Consider the ring $R = F[x]$ of polynomials in x over E (with commutation rule $\alpha x = x\alpha$, $\alpha \in F$), and put

$$f(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

Then fR is a two-sided ideal, and the quotient R/fR is again a field, provided that f is irreducible over F. Clearly this is so if and only if F has characteristic prime to p (possibly zero) and the equation

$$x^p = 1$$

has no solution $\neq 1$ in F. Under these circumstances the quotient $E = R/fR$ is again a field, an extension of F, and moreover S may be extended to E by putting $xS = x$; with this definition $f(x)$ is left fixed, so that S is well defined on E. Thus we can always adjoin a primitive p^{th} root of 1 to F, unless one is present already or F has characteristic p. In the latter case the construction of Theorem 3.1 is modified as follows:

THEOREM 3.2. *Let E be a field of characteristic p, with an endomorphism S and S-derivation D such that*

$$DS = SD.$$

If $K = E(t; S, D)$, S and D may be extended to K by putting

$$tS = t, \qquad tD = 0$$

and with these definitions (8) holds. Moreover, $\sigma = S^p$ is an endomorphism of E and $\delta = D^p$ a σ-derivation, and if k is the subfield of K generated by t^p over E, then $k = E(t^p; \sigma, \delta)$ and K/k is again a binomial extension of degree p.

The first part of the proof is the same as for Theorem 3.1, taking $\omega = 1$. To prove (10) we simply raise both sides of (9) to the p^{th} power and note that now all operators commute: (10) follows because we are in characteristic p.

4. Construction of the example

We begin by constructing, for a given prime p and given commutative field F (containing all p^{th} roots of 1) an extension K/k of degree p and infinite left dimension, with the centre of K equal to F. Later we shall see how to modify the construction so as to obtain extensions of arbitrary (composite) degree.

Let p be a prime and F a commutative field containing all p^{th} roots of 1. For F of characteristic p (or for $p = 2$) this is no restriction; when F has characteristic prime to p, it means that F contains a p^{th} root of 1 other than 1. We denote this by ω, and take $\omega = 1$ in case the characteristic of F is p.

Let A be the free associative algebra over F on a countable free generating set $B = \{a, b_{i\lambda}\}$ where $i = 0, 1, 2, \cdots, \lambda = 0, \pm 1, \pm 2, \cdots$. We totally order B by taking first a and then the $b_{i\lambda}$ in the lexicographical order of suffixes. Let S be the endomorphism of A over F defined by

$$aS = \omega a, \qquad b_{i\lambda} S = b_{i+1,\lambda}. \tag{11}$$

Further, denote by U the set of basic products in B, relative to the ordering just defined. Formally, these are just certain products of elements of B, bracketed in a certain way (cf. [2]). Clearly U is again totally ordered, with a as first element. We denote by U_1 the set of basic products $\neq a$.

It is clear from (11) that S is an order-preserving mapping of B into itself (apart from the scalar factor ω attached to a), so if $[u]$ is a basic product then $[uS]$ is again basic, except for a factor ω^k. We now interpret the basic products in A as follows (cf. [2]). If $u \in B$, then $[u] = u$; if $[u] = [[v][w]]$ is basic of length >1, then $w < v$ and $v \neq a$. In this case put

$$(12) \qquad [[v][w]] = \begin{cases} [v][w] - [w][v] & \text{if } w \neq a, \\ [v]a - a[vS] & \text{if } w = a. \end{cases}$$

It follows that the ascending monomials in the basic products

$$p = u_1 u_2 \cdots u_r \qquad (u_i \in U,\ u_1 \leq \cdots \leq u_r)$$

form a basis of A. We define the *grade* of p as

$$v(p) = \sum [l(u_i) - 1]$$

and in general for $f = \sum p\alpha_p$ $(\alpha_p \in F)$ put

$$v(f) = \min \{v(p) \mid \alpha_p \neq 0\}.$$

It follows as in [2] that this defines a filtration on A, whose associated graded ring gr (A) has the form $R[a; S]$ (skew polynomial ring) where $R = F(U_1)$ is the polynomial ring over F in the elements of U_1 as commuting indeterminates, with the endomorphism S induced from A. Since $R[a; S]$ is an Ore domain, it follows from the embedding theorem in [1] that A can be embedded in a valuated field V, and S extends to an endomorphism of V, again denoted by S. Let D be the inner S-derivation induced by a, i.e.,

$$xD = xa - a \cdot xS \qquad \text{for all } x \in V.$$

Then $xSD = xSa - a \cdot xS^2$, $xDS = xS \cdot aS - aS \cdot xS^2$, whence

$$DS = \omega SD.$$

Denote by K the subfield of V generated by B over F, then K admits S and D and its centre is F. Further, if k is the subfield of K generated by a^p and U_1 over F, then k again admits S and D. We shall show that $[K:k]_R = p$, $[K:k]_L = \infty$. Since K/k is a pseudolinear extension, the first assertion will follow if we can show that $a \notin k$, and the second follows by Theorem 2.1 once we have shown that $[k:k^S]_L = \infty$.

(i) The proof that $a \notin \bar{k}$ is precisely as in [2] and will not be repeated here.

(ii) To prove that $[k:k^S]_L = \infty$, it is enough to show that the elements $b_{0\lambda}$ are left k^S-independent; in fact we shall show that they are left K^S-independent. To see this we first observe that K^S is the subfield of V generated by a, $b_{i\lambda}$ $(i > 0)$ over F. Now if there is a relation

$$(13) \qquad \sum c_\lambda b_{0\lambda} = 0 \qquad (c_\lambda \in K^S)$$

with coefficients not all zero, say $c_0 \neq 0$, then we can express b_{00} in terms of a and the $b_{i\lambda} \neq b_{00}$ over F. Let W be the closed subfield of V generated by a and the $b_{i\lambda} \neq b_{00}$ over F. The construction of V by the embedding theorem shows that W is just the valuated field of fractions of the free associative algebra on a and the $b_{i\lambda} \neq b_{00}$ over F, using the same definitions (11) and (12).

Thus there are no special relations in W, due to the presence of b_{00} in V. Since a and the $b_{i\lambda}$ (including b_{00}) form a free generating set of A, it follows that $b_{00} \notin W$, and this contradicts the existence of a non-trivial relation (13). Hence the $b_{0\lambda}$ are left k^S-independent and it follows that $[k:k^S]_L = \infty$.

5. Extensions of arbitrary degree

With the help of the example constructed in Section 4 it is easy to obtain extensions of any finite degree and infinite left dimension.

Let $n > 1$ be given and let F be any field. If the characteristic of F is prime to n, assume also that F contains a root of $x^n = 1$ other than 1. Then it follows that F contains a primitive p^{th} root of 1, say ω, where $p \mid n$. If the characteristic of F divides n, we set $\omega = 1$. In either case, by the results of Section 4, there exists an extension K/k in which K has centre F and $[K:k]_R = p$, $[K:k]_L = \infty$.

Now any permutation of the second suffix of the $b_{i\lambda}$ is an automorphism of A which extends to an outer automorphism of K, and it is clear that the group of these automorphisms acts faithfully on k. Thus k has outer automorphisms of any finite order. Write $n = pn_1$ and let α be any outer automorphism of A of order n_1. The fixed field k_0 then satisfies $[k:k_0]_L = [k:k_0]_R = n_1$ (cf. [3] p. 163) and hence

$$[K:k_0]_R = pn_1 = n, \qquad [K:k_0]_L = \infty .$$

This completes the proof of

THEOREM 5.1. *Let n be any integer greater than one, and F any field such that if* char *F is prime to n, then F contains a root of $x^n = 1$ other than* 1. *Then there exists a skew field K with centre F, and a subfield k of K such that*

$$[K:k]_R = n, \qquad [K:k]_L = \infty .$$

REFERENCES

1. P. M. COHN, *On the embedding of rings in skew fields*, Proc. London Math. Soc. (3), vol. 11 (1961), pp. 511–530.
2. ———, *Quadratic extensions of skew fields*, Proc. London Math. Soc. (3), vol. 11 (1961), pp. 531–556.
3. N. JACOBSON, *Structure of rings*, Providence, R. I. 1956.
4. O. ORE, *Linear equations in non-commutative fields*, Ann. of Math. (2), vol. 32 (1931), pp. 463–477.
5. A. ROSENBERG AND D. ZELINSKY, *Finiteness of the injective hull*, Math. Zeitschrift, vol. 70 (1959), pp. 372–380.
6. O. ZARISKI AND P. SAMUEL, *Commutative algebra I*, Princeton, Van Nostrand, 1958.

UNIVERSITY OF CHICAGO,
CHICAGO, ILLINOIS
QUEEN MARY COLLEGE,
UNIVERSITY OF LONDON