ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 223–230

ON SKEW FIELD COPRODUCTS WITH A FINITE EXTENSION

BY

P. M. COHN

Department of Mathematics, University College London
Gower Street, London WC1E 6BT, England
e-mail: pmc@math.ucl.ac.uk

To the memory of Shimshon Amitsur

ABSTRACT

It is shown that the field coproduct of any skew field E with a binomial (commutative) field extension F/k over k can be expressed as a cyclic extension of a skew field K (the E-socle), itself the field coproduct of $[F\colon k]$ copies of E over k. Qua vector space the coproduct may also be expressed as a tensor product of E and K over k.

1. Introduction

The field coproduct of skew fields (cf. [4] and §2 below) is a useful construction, which however is sometimes difficult to manipulate owing to the lack of a convenient normal form for its elements. Our object here is to examine its structure when one of the factors is a commutative binomial field extension F/k. Since we are dealing with skew fields throughout, we shall usually speak simply of fields and only sometimes add "skew" for emphasis. Let us recall that for any two fields F and E with a common subfield k their ring coproduct $F *_k E$ is a fir (= free ideal ring) and as such has a universal skew field of fractions U, which will be denoted by $F \circ_k E$ or $F \circ E$ and called the **field coproduct** of F and E over k. We shall be concerned with the case where E is any skew field with k in its centre. Our main result (Theorem 3.2) is to show that there is a subfield K (itself a coproduct) such that

$$(1) \qquad U = F \circ_k E = F \otimes_k K,$$

Received January 30, 1995 and in revised form December 21, 1995

as (F, K)-bimodule, in particular $[U\colon K] = [F\colon k]$.

Thus the coproduct U of F with E can be represented as a tensor product of F with another subfield K, but it must be emphasized that the multiplication is not that induced by that of the factors; thus it should perhaps be described as a "skew tensor product". Such a representation as a skew tensor product also exists for the centralizer of F in U; this is derived in §4 from a general decomposition theorem for a field by the centralizer of a finite extension of its centre (Proposition 4.1). In §5 we examine the case of finite Galois extensions and in Proposition 5.1 obtain conditions on the coproduct for the extension to be cyclic.

ACKNOWLEDGEMENT: My thanks are due to a referee, whose repeated careful readings led to the removal of a number of errors and obscurities.

2. Notation and terminology

As already mentioned, by a **field** we understand a not necessarily commutative division ring; sometimes the prefix "skew" is added for emphasis. All our fields will be k-algebras, where k is a certain commutative base field, fixed once and for all.

We briefly recall one or two other facts that will be needed later. A matrix A is said to be **full** if it is square and cannot be written as $A = PQ$, where Q has fewer rows than A. A homomorphism of rings which keeps full matrices full is called **honest**.

If K, L are any fields with a common subfield E, then their ring coproduct $R = K *_E L$ over E may be defined essentially as a pushout. We recall from [4], Theorem 5.3.9, p. 222 that R is a fir and hence has a universal field of fractions, written U or also $U(R)$. More specifically we shall call it the **field coproduct** of K and L over E and write it as $K \circ_E L$. Its elements are obtained by formally inverting all full matrices over R and taking their entries.

The free k-algebra on any set X, $k\langle X\rangle$, is also a fir. More generally, if E is any field (and k-algebra), then the tensor E-ring on X, $E *_k k\langle X\rangle$, defined as the E-ring generated by X with defining relations $ax = xa (a \in k)$, is again a fir, and so has a universal field of fractions, which is written $E_k \langle\!\langle X \rangle\!\rangle$. In fact we have a natural isomorphism (cf. [4], Prop. 5.4.3, p. 225):

$$E_k \langle\!\langle X \rangle\!\rangle \cong E \circ_k k \langle\!\langle X \rangle\!\rangle .$$

3. Coproducts with a finite extension

Let E be any field and denote by K the field coproduct of countably many copies of E (over k), indexed by Z. Then K has an automorphism σ called the **shift automorphism**, which consists in replacing each element of the i-th factor E by the corresponding element in the $(i+1)$-st, for all $i \in Z$. There is a corresponding construction for a field coproduct of n factors E over k, for any $n \in N$, with shift automorphism of period n. Returning to our countable coproduct K, we can form the skew polynomial ring $K[u;\sigma]$ and its field of fractions $L = K(u;\sigma)$ (cf. e.g. [4], Ch.2). Since L is generated by u and one copy of E over k, it must be a specialization of the field coproduct $k(u) \circ_k E$, where $k(u)$ is the rational function field in a central indeterminate u. In fact it is not hard to see (cf. [4], Lemma 5.5.6, p. 235) that we have an isomorphism

$$K(u;\sigma) \cong k(u) \circ_k E = E_k \langle\!\langle u \rangle\!\rangle.$$

We consider the analogue when $k(u)$ is replaced by a binomial extension. Thus we take $F = k(a)$, where the minimal polynomial of a over k is

$$p(x) = x^n - \lambda, \qquad \text{where } \lambda \in k. \tag{1}$$

It turns out that in this case the field coproduct can be expressed as a residue-class ring of a skew polynomial ring:

THEOREM 3.1: *Let E be any field which is a k-algebra, and $F = k(a)$ a commutative binomial extension of k, where a has the minimal polynomial p over k given by* (1). *Then*

$$E \circ_k F = K[u;\sigma]/(p), \tag{2}$$

where K is the field coproduct over k of n copies of E, with shift automorphism σ of order n.

Proof: Let P be the ring coproduct of n copies of E over k, with shift automorphism σ, and in the skew polynomial ring $P[u;\sigma]$ write $p = u^n - \lambda$. It is clear that p is in the centre of this ring; we claim that

$$E *_k F \cong P[u;\sigma]/(p). \tag{3}$$

Let us denote the n copies of E in P by $E_0, E_1, \ldots, E_{n-1}$, where $E_i = u^{-i}E_0u^i$. Then we have a homomorphism

$$\alpha\colon E *_k F \longrightarrow P[u;\sigma]/(p),$$

obtained by mapping a to $\overline{u}$, the image of u in the quotient on the right, and E to E_0. To construct a map in the opposite direction we note that every element of $E * F$ can be written as a polynomial in a, of degree at most $n-1$, with coefficients that are expressions in the elements of E, $a^{-1}Ea, \ldots, a^{1-n}Ea^{n-1}$. Thus we can map $P[u;\sigma]$ to $E * F$ by letting $u \mapsto a$ and $E_i \to a^{-i}Ea^i$; since $u^n - \lambda \mapsto \alpha^n - \lambda = 0$, we find that $p(u)$ maps to 0, so we obtain indeed a homomorphism β from $P[u;\sigma]/(p)$ to $E * F$ and this is easily seen to be inverse to α; thus (3) is established.

We now have the following diagram, where K is the universal field of fractions of P. Clearly σ extends to an automorphism of K, again written σ.

$$\begin{array}{ccc} E *_k F & \longrightarrow & P[u;\sigma]/(p) \\ \downarrow & & \downarrow \\ E \circ_k F & & K[u;\sigma]/(p) \end{array} \tag{4}$$

It is also clear that the centre of P is k, and by Theorem 4.4 of [5], k is also the centre of K; thus $K[u;\sigma]/(p)$ is a ring containing K, of finite dimension n as K-space, where n is the degree of p. But $E \circ F$ arises by inverting all full matrices of $E * F$, while $K[u;\sigma]/(p)$ is obtained by inverting certain full matrices over $P[u;\sigma]/(p) = E * F$, viz. those with all entries in P. We observe that any full matrix over P remains full over $P[u;\sigma]/(p)$, because it is inverted over $K[u;\sigma]/(p)$. Hence we can pass from $K[u;\sigma]/(p)$ to $E \circ F$ by inverting certain full matrices, and in particular, since $E * F$ is embedded in $E \circ F$, it follows that $K[u;\sigma]/(p)$ is embedded in $E \circ F$. Hence $K[u;\sigma]/(p)$ has no zero-divisors, so $K[u;\sigma]/(p) = L$ is a field. Since the vertical arrows in (4) are epimorphisms, we conclude that

$$E \circ_k F \cong K[u;\sigma]/(p),$$

and the proof is complete. ∎

The conclusion of Theorem 3.1 can be expressed as an exact sequence

$$0 \longrightarrow (p) \longrightarrow K[u;\sigma] \longrightarrow E \circ_k F \longrightarrow 0. \tag{5}$$

A comparison with the sequence

$$0 \longrightarrow (p) \longrightarrow k[u] \longrightarrow F \longrightarrow 0 \tag{6}$$

shows that (5), as a sequence of vector spaces, is obtained from (6) by operating with $\otimes K$. We can sum up this result as

THEOREM 3.2: *If k, E, F and p are as in Theorem 3.1, then*

$$E \circ_k F \cong F \otimes_k K,$$

where $K = E_0 \circ E_1 \circ \cdots \circ E_{n-1}$ and $a^{-1}E_i a = E_{i+1}$ $(i = 0, 1, \ldots, n-1, E_n = E_0)$, and the tensor product on the right is understood as a vector space.

We shall refer to K as the E-**socle** in $E \circ F$. Without giving a general definition we can look on this concept as an aid to clarifying the structure of the field coproduct. Thus Theorem 3.2 may be expressed by saying that a field coproduct of E over k by a binomial extension F of degree n over k can be written as a vector space which is a tensor product of F by a field K, itself the field coproduct of n copies of E (the "E-socle") with multiplication defined by the shift automorphism σ such that σ^n is the identity. This construction is reminiscent of the formation of a wreath product of groups, with the socle in the role of the normal subgroup, but of course the socle by no means admits all inner automorphisms, as is shown by the Cartan–Brauer–Hua theorem.

More generally there is an analogue of Theorem 3.2 where k is not necessarily central in E and the shift automorphism σ^n is the inner automorphism induced by the constant term of p.

4. The centralizer of F in the coproduct

Let U be any field with centre k and let F be a commutative subfield of U which is a finite extension of k. If C denotes the centralizer of F in U, then by a theorem of Brauer (cf. [3], Th. 7.1.9, p. 263) we have $[U\colon C] = [F\colon k] = n$, say. Suppose that F/k is separable, generated by $a \in F$ with minimal polynomial p, then by [2], Cor. 5.7.4, p. 194,

$$F \otimes_k F \cong E_1 \times \cdots \times E_r, \tag{1}$$

where the E_i are fields corresponding to the irreducible factors over F of p; in particular, $E_1 = F$ corresponds to the linear factor $x - a$. More explicitly, let us write $L = a \otimes 1, R = 1 \otimes a$; then by interpreting L as left and R as right multiplication on U by a, we may regard U as $F \otimes F$-module, i.e. as an F-bimodule. We have $LR = RL$, $p(L) = p(R) = 0$, and if $q(x, y)$ is defined as a polynomial in the commuting variables x and y by the equation

$$p(x) - p(y) = (x - y)q(x, y), \tag{2}$$

then $d = L - R$, $e = q(L, R)$ are k-linear operators of U into itself such that by (2),

$$de = ed = 0. \tag{3}$$

Since $p(x)$ is separable over k, $(x - a)$ and $q(x, a)$ have no common factor in x, so there exist $f, g \in F[x] = k[a, x]$ such that

$$(x - a)f + q(x, a)g = 1.$$

If we rewrite this as an equation in x and y over k, we obtain

$$(x - y)f + q(x, y)g = 1 + p(y)r(x, y),$$

for a polynomial r, and hence, on writing $f_1 = f(L, R)$, $g_1 = g(L, R)$, we find

$$df_1 + eg_1 = 1. \tag{4}$$

By (3), (4) we have im $e = \ker d = C$, say and im $d = \ker e = G$. Here C and G are k-subspaces of U, in fact C is by definition just the centralizer of a and so is a subfield of U. Moreover, $CG + GC \subseteq G$, for if $u \in C$, $v \in G$, then $v = az - za$ for some $z \in U$, hence $uv = uaz - uza = auz - uza \in G$ and similarly $vu \in G$. We summarize these findings as

Proposition 4.1: *Let F/k be a finite separable field extension of degree n, say $F = k(a)$, and let U be a skew field containing F, with centre k. Denote left and right multiplication by a on U by L, R respectively and put $d = L - R$, $e = q(L, R)$, where q acting on C is defined by (2) in terms of the minimal polynomial p for a over k. Then $C = \ker d = \operatorname{im} e$ is the centralizer of F in U and $G = \ker e = \operatorname{im} d$ is a C-space of (left or right) dimension $n - 1$ over C, such that*

$$U = C \oplus G. \tag{5}$$

The representation (5) follows from (3) and (4) and, since $[U: C] = n$, we deduce that $[G: C] = n - 1$.

Suppose now that $U = E \circ_k F$ is a field coproduct of a field E with a binomial extension F/k; then by Theorem 3.1 we have $U \cong F \otimes K$, where K is the E-socle. If we put $C_1 = C \cap K$, $G_1 = G \cap K$, then replacing $d = L - R$ by $D = L^{-1}d = 1 - L^{-1}R$, we have an operator admitted by K, and the reasoning that led to (5) shows that $K = C_1 \oplus G_1$, hence

$$U = (F \otimes C_1) \oplus (F \otimes G_1).$$

A comparison with (5) shows that $C = F \otimes C_1$ and from the definition of C_1 as the centralizer of F in K we see that in this equation the multiplication is that induced by the tensor product structure. Thus we obtain

THEOREM 4.2: *Let $U = E \circ_k F$ be the field coproduct of a skew field E which is a k-algebra and a commutative binomial extension F/k. Then U can be expressed as $U = F \otimes K$, where K is the E-socle as before and, writing C_1 for the centralizer of F in K, we can express the centralizer C of F in U as*

$$C = F \otimes C_1.$$

5. Galois extensions

Suppose now that F/k is a (finite commutative) Galois extension with group Γ and E is any field (and k-algebra); then Γ acts on $U = E \circ_k F$ through the second factor. In detail, each $\sigma \in \Gamma$ extends to an automorphism of $E * F$ which is the identity on E and hence extends to an automorphism of U over E, again denoted by σ. In this way Γ acts on U; if the fixed field is denoted by U_0, then $[U: U_0] = |\Gamma|$, by Theorem 3.3.7 of [4] (note that Γ consists entirely of outer automorphisms of U). We claim that

$$U = F \otimes U_0,$$

as k-spaces (ignoring the multiplication). For we can use a well-known argument to show that F and U_0 are linearly disjoint over k: if $u_1, \dots, u_r \in U_0$ are linearly independent over k but $\sum a_i u_i = 0$ for some $a_i \in F$, not all 0, we may assume that $a_1 = 1$ and r is chosen minimal. Then $a_2, \dots, a_r$ cannot all lie in k, so there exists $\alpha \in \Gamma$ which does not fix them all; now $\sum_2^r (a_i - a_i^\alpha) u_i = 0$ is a shorter non-trivial relation, which is a contradiction. Thus $FU_0 = F \otimes U_0$ in U; moreover, $[U: U_0] = |\Gamma| = [F: k] = [F \otimes U_0: U_0]$, and this shows that $U = F \otimes U_0$, as claimed.

In the special case when F/k is a binomial extension, it is easily seen (and will be shown below) that U_0 is the E-socle. In fact this situation arises whenever U_0 admits conjugation by a generator of F:

PROPOSITION 5.1: *Let F/k be a commutative Galois extension of degree n, where k contains a primitive n-th root of 1, let E be any skew field which is a k-algebra and put $U = E \circ_k F$. Denote by U_0 the fixed field of* $\mathrm{Gal}(F/k)$ *acting on U; then U_0 admits conjugation by a generator of F if and only if F/k is a cyclic extension, and then U_0 is the E-socle in a suitable representation.*

Proof: Let a be a generator of F/k and suppose that for any $x \in E$, $a^{-1}xa \in U_0$; thus if $\sigma \in \Gamma = \mathrm{Gal}(F/k)$, we have $a^{-\sigma}xa^{\sigma} = a^{-1}xa$, i.e.

$$xa^{\sigma}a^{-1} = a^{\sigma}a^{-1}x \quad \text{for all } x \in E.$$

Hence $\lambda = a^{\sigma}a^{-1}$ centralizes E and so lies in k; therefore $a^{\sigma} = \lambda a$. If σ has order r, then $a = a^{\sigma^r} = \lambda^r a$ and so $\lambda^r = 1$. Let m be the LCM of the orders of the elements of Γ and put $b = a^m$; then $b^{\sigma} = \lambda^m a^m = b$. This holds for each $\sigma \in \Gamma$, hence $b \in k$ and so a satisfies the equation $x^m - b = 0$. It follows that $m = n$ and F/k is cyclic.

Conversely, assume F/k to be cyclic, generated by $a \in F$ satisfying $x^n - c = 0$ and let ω be a primitive nth root of 1. Then the conjugates of a are $a, \omega a, \omega^2 a, \ldots, \omega^{n-1}a$, and if K is the field generated by $E, a^{-1}Ea, \ldots, a^{1-n}Ea^{n-1}$, then K is the E-socle in U and is also the fixed field. This completes the proof. ∎

References

[1] P. M. Cohn, *Free Rings and Their Relations*, LMS Monographs, 2nd edn., No. 19, Academic Press, London & New York, 1985.

[2] P. M. Cohn, *Algebra 2*, 2nd edn., J. Wiley & Sons, Chichester, 1989.

[3] P. M. Cohn, *Algebra 3*, 2nd edn., J. Wiley & Sons, Chichester, 1990.

[4] P. M. Cohn, *Skew fields, Theory of general division rings*, in *Encyclopedia of Mathematics and its Applications*, Vol. 57, Cambridge University Press, 1995.

[5] P. M. Cohn, *The universal field of fractions of a semifir III, Centralizers and normalizers*, Proceedings of the London Mathematical Society (3) **50** (1985), 95–113.