

# Noncommutative Splitting Fields

JAN TREUR

*Potgieterweg 12, 1851 CH Heiloo, The Netherlands*

*Communicated by N. Jacobson*

Received July 10, 1987

## 1. INTRODUCTION

For commutative fields  $K$ ,  $L$  with  $L$  generated over  $K$  by an algebraic element with separable minimal polynomial  $p$  the following facts are well known:

- (1) There exists an extension  $N$  of  $L$  such that  $N/K$  is a Galois extension and  $N$  is generated by zeros of  $p$ .
- (2) This extension  $N$  can be constructed explicitly by repeatedly adding more zeros of  $p$  until  $p$  has a complete set of zeros. In that case  $p$  splits into linear factors; such an  $N$  is called a splitting field for  $p$ .
- (3) This extension  $N$  is unique.

In the noncommutative case also a version of (1) can be proved; see for instance [5, Proposition A.3]. In that case, in general, such an  $N$  is not finitely generated over  $K$ .

What (2) means for the noncommutative case depends on how one defines the phrase "constructing by repeatedly adding zeros of  $p$  until  $p$  has a complete set of zeros." The adding of zeros may be done by forming field coproducts over  $K$  of copies of  $L$ ; however, one can always continue this construction, so there is needed an explicit criterion to determine whether a set of zeros is complete. In this paper we use the notion of "separate zeros" for this, as defined in [6], and we will consider a set of zeros complete if it contains  $\deg(p)$  separate zeros. In this case indeed  $p$  will split in linear factors. More precise definitions will follow below. Using these definitions we will construct noncommutative splitting fields by adding a complete set of zeros; these splitting fields are finitely generated (by at most  $\deg(p)$  zeros). In fact, trying to perform this construction and to define when a set of zeros is complete served as a main motive in developing our theory on separate zeros, as presented in [6]. As a curiosity it appears that in the noncommutative case no criterion on separability of  $p$  is needed; so, for instance we can construct noncommutative fields containing complete

families of separate zeros for inseparable polynomials over commutative fields.

Concerning (3), in this paper no results on uniqueness of these splitting fields in terms of isomorphisms are included. However, some alternative forms of uniqueness may occur.

In this paper by  $K, L, N$  we denote *fields* which may or may not be commutative. As in [6] we denote the *left substitution* of  $\alpha$  by  $\sigma_\alpha: K[X] \rightarrow K$  and  $\mathfrak{Z}(p)$  is the set of *left zeros* of the polynomial  $p$  over  $K$ . By  $q_S$  we denote the *right minimal polynomial* of the subset  $S$  of  $K$  (the generator of the right ideal of polynomials having  $S$  among their left zeros; by using  $q_S$  we will always mean the minimal polynomial with coefficients in a field containing  $S$ ). The set  $S$  is called a *separable set* or a set of *separate elements* or zeros if for every  $\alpha \in S$  and every finite  $F \subset S$  there exists a polynomial vanishing on  $F \setminus \{\alpha\}$  and nonzero on  $\alpha$ . Any maximal separable subset  $B$  of  $S$  is called a *separable basis* of  $S$ . The *degree* of  $S$ , denoted by  $\deg(S)$ , is the number of elements of such  $B$ . The set  $S$  is called *bounded* if  $\deg(S)$  is finite, or, equivalently, if  $S \subset \mathfrak{Z}(p)$  for some nonzero polynomial  $p$ . The element  $\alpha$  is called *dependent on  $S$*  if there exists a finite subset  $F$  of  $S$  such that every polynomial vanishing on  $F$  also vanishes on  $\alpha$ . See [6] for more details.

We call  $L/K$  an (*inner*) *Galois extension* if  $K$  is the field of invariants of some group of (*inner*) automorphisms of  $L$ . The elements  $\theta_1$  and  $\theta_2$  in some extensions of  $K$  are called *uniform over  $K$*  or *of the same  $K$ -type* if  $\theta_1 \rightarrow \theta_2$  induces a  $K$ -isomorphism  $K(\theta_1) \rightarrow K(\theta_2)$ . In [5] we called an extension  $N$  of  $L$  an *inner closure* of  $L/K$  if:

(i) For every  $\theta \in N \setminus K$  there exists a  $\theta' \in N$  of the same  $K$ -type such that  $\theta \neq \theta'$  and the  $K$ -isomorphism  $\theta \rightarrow \theta'$  is induced by an inner  $K$ -automorphism of  $N$  (in other words,  $N$  is inner Galois over  $K$ ).

(ii)  $N$  is generated by  $K$ -copies of  $L$  of the form  $t^{-1}Lt$  for  $t \in Z_N(K)^*$ , (where  $Z_N(K)$  is the centralizer of  $K$  in  $N$ ).

In [5, Appendix] it is proved that every  $L/K$  can be extended to an inner closure. The construction makes use of coproducts of fields.

If  $L_i, i \in I$ , are extensions of  $K$ , we will sometimes form the *field coproduct* of these fields over  $K$ , denoted by  $\circ_K(i \in I) L_i$ . This can be constructed by first taking the *free product of rings*  $*_K(i \in I) L_i$  and then forming its universal field of fractions. For details about this construction we refer to [3, Chap. 4].

From [6] we recall three lemmas. The first one summarizes [6, Lemma 3.1].

LEMMA 1.1. *Let  $L/K$  be a Galois extension and  $G$  a set of automorphisms*

of  $L$  with  $\text{Inv } G = K$ . Let  $\theta \in L$  be right algebraic over  $K$  and take  $S = \{\omega(\theta) \mid \omega \in G\}$ . Then  $q_S$  is the right minimal polynomial of  $\theta$  over  $K$ .

This lemma will be used in this paper only for the case of an inner Galois extension. The next lemma summarizes a special case of [6, Lemma 2.1 and Proposition 2.3].

LEMMA 1.2. Let  $\theta, \eta \in K$  and  $S \subset K$  be given such that  $\eta$  is dependent on  $S \cup \{\theta\}$  but not on  $S$ . Then  $\eta = s^{-1}\theta s$  with  $s = \sigma_\theta(q_S) \sigma_\eta(q_S)^{-1}$ .

Finally, we summarize [6, Lemma 3.4].

LEMMA 1.3. Let  $p \in K[X]$  and  $\theta \in K$  be given. Suppose  $t_i, i \in I$ , are elements of  $K^*$  such that the elements  $\theta_i = t_i^{-1}\theta t_i$  are left zeros of  $p$ . Then the following hold:

(a) If  $e_i \in Z_K(\theta)$  are given with  $t = \sum e_i t_i \neq 0$  then  $t^{-1}\theta t$  is a left zero of  $p$ .

(b) If  $\theta_i, i \in I$ , are separate zeros of  $p$ , then  $t_i, i \in I$ , are left independent over  $Z_K(\theta)$ .

*Remark.* It has been noticed by G. M. Bergman that Lemma 1.3(b) can be made an if-and-only-if statement, as is shown in Lam and Leroy [4, Chap. 4].

## 2. SPLITTING SETS AND SPLITTING FIELDS

DEFINITION. Let  $K \subset N$  be fields,  $p$  a polynomial over  $K$ ,  $S$  a subset of  $\mathfrak{Z}_N(p)$ .

We call  $S$  a *splitting set* for  $p$  (or say  $S$  *splits*  $p$  or  $p$  is *split* by  $S$ ) if  $p = q_S$ .

We say  $p$  *splits over*  $N$  if  $N$  contains a splitting set for  $p$ .

We call  $N$  a *splitting field* for  $p$  if it is generated over  $K$  by some splitting set for  $p$ .

If the set  $S$  is separable we can add in a natural way the modifier *separable* or *separably* to each of the definitions above. The same holds for the modifier *uniform* or *uniformly*.

If  $S$  consists of elements of the form  $\theta_i = \omega_i(\theta)$  for some  $\theta \in N$  and  $K$ -automorphisms  $\omega_i, i \in I$ , of  $N$ , we call  $S$  a *Galois set*; in this case we can speak of  $p$  being "*split by a Galois set*" or  $N$  being "*a transitive splitting field*." If these  $K$ -automorphisms are inner we call  $S$  an *inner (Galois) set*; we can handle this similarly.

This defines a number of notions of a splitting field, namely: splitting field, separable splitting field, uniform splitting field, transitive splitting field, inner transitive splitting field, and various combinations of these. In

the noncommutative case all these do not need to coincide. However, there are some implications between them. Some of these appear in this paper; other remain open questions.

The following results immediately follow from [6].

**LEMMA 2.1.** *For  $K \subset N$ ,  $p \in K[X]$ , and a subset  $S$  of  $N$  the following hold:*

(a)  *$N$  is an inner transitive splitting field implies  $N$  is a transitive splitting field implies  $N$  is a uniform splitting field.*

(b) *If  $p$  is split by a set  $S$ , then  $p$  is also split by any separable basis of  $S$ .*

(c) *If  $S$  is a separable set of zeros of  $p$ , then  $p$  is split by  $S$  if and only if  $\text{card}(S) = \text{deg}(p)$ .*

(d) *If  $S$  splits  $p$ , then every left zero of  $p$  in  $N$  is conjugate to an element of  $S$ .*

(e) *Every field  $N$  that splits a polynomial  $p$  contains as a subfield a splitting field for  $p$ .*

**THEOREM 2.2.** *Let  $L/K$  be a Galois extension. Then the minimal polynomial of any right algebraic element of  $L$  over  $K$  is split in  $L$  by a Galois set.*

Inner closures can be used to prove the existence of splitting fields; in [5, Appendix] it is proved that every  $L/K$  can be embedded in an inner closure. In general inner closures as we construct them (see the reference mentioned above) are not finitely generated over  $K$ . But by choosing a separable inner Galois basis for the set of zeros of  $p$  one can find finitely generated subfields which are splitting fields of  $p$ . The following theorem makes this precise.

**THEOREM 2.3.** *Let  $N$  be an inner closure of  $L/K$ . Then the following hold:*

(a) *The minimal polynomial of any right algebraic element  $\theta \in L$  over  $K$  is split over  $N$  by an inner Galois set containing  $\theta$ .*

(b) *If  $L$  is generated by a single element which is right algebraic over  $K$  with minimal polynomial  $p$ , then  $N$  is an inner transitive splitting field for  $p$ .*

(c) *In the situation of (b),  $N$  contains as a subfield a finitely generated separable transitive splitting field; for the set of generators one can choose any separable inner Galois basis for the set of zeros of  $p$  in  $N$ .*

In general, the subfield as provided by Theorem 2.3(c) is not unique, and its structure is not made explicit by the theorem. But if we analyse more closely the construction used to obtain inner closures in [5, appendix], an

explicit candidate comes forward, namely the field coproduct of a finite number of  $K$ -copies of  $L$ . Indeed it can be proved that this provides a finitely generated splitting field construction, as is established in the next section.

### 3. SPLITTING POLYNOMIALS IN FIELD COPRODUCTS

For a direct construction of a splitting field of a polynomial  $p$  over  $K$  one can think of adding zeros of  $p$  to  $K$  until a separable splitting set is obtained. The construction as used in the commutative case, by repeatedly adding a zero of a remaining irreducible factor of  $p$ , does not work in the noncommutative case, since on dividing  $p$  by a left factor, one is left with a right factor, zeros of which may not be left zeros of  $p$ . However, on the other hand, in the noncommutative case there also are construction tools which are not available in the commutative case, such as the field coproduct construction. This construction can be used to create an arbitrary number of copies of one given zero of  $p$ . We only consider polynomials which are the right minimal polynomial of some element  $\theta$  in an extension  $L$  of  $K$ . For this case indeed we will prove that the procedure sketched above will succeed and produce a separable splitting set for  $p$ . We start in a somewhat more general setting.

In this section  $L_i, i \in I$ , will be field extensions of  $K$  and for every subset  $J$  of  $I$  the field coproduct  $\circ_K(i \in J) L_i$  over  $K$  of these fields  $L_i, i \in J$ , will be denoted by  $P_J$ . We identify these  $P_J$  as subfields of  $P_I$ . A special case is provided by a number of  $K$ -copies of  $L$ . First a lemma on field coproducts.

LEMMA 3.1. *Let  $P = L_1 \circ_K L_2$  be the field coproduct of two extensions  $L_1/K$  and  $L_2/K$ , and  $\theta \in L_2$ . If  $\theta$  is right algebraic over  $L_1$  with minimal polynomial  $p$ , then  $\theta$  is right algebraic over  $K$  with minimal polynomial  $p \in K[X]$ .*

*Proof.* Let  $N$  be an inner closure of  $P/K$ . We show that every  $t^{-1}\theta t$  with  $t \in Z_N(K)^*$  is a left zero of  $p$ . From the universal property of the free product of rings [2, Theorem 3.1] it follows that the  $K$ -homomorphisms

$$x \rightarrow x: L_1 \rightarrow N$$

$$x \rightarrow t^{-1}xt: L_2 \rightarrow N$$

can be extended to a  $K$ -homomorphism

$$\phi: L_1 *_K L_2 \rightarrow N$$

of the free product of rings  $L_1$  and  $L_2$  over  $K$  to  $N$ . Since  $\phi(\theta) = t^{-1}\theta t$  and  $\phi(p) = p$  we conclude that  $t^{-1}\theta t$  is a left zero of  $p$ . From Lemma 1.1 it follows that  $p \in K[X]$ . ■

Lemma 3.1 may be used to establish that elements in different factors of field coproducts over  $K$  are separate, of course under conditions that exclude those cases that trivially contradict such an assertion. The following lemma gives the basic result.

**LEMMA 3.2.** *Let the elements  $\theta_i \in L_i$  ( $i \in I$ ) be given. Suppose that for each  $i$  such that  $\theta_i$  is right algebraic over  $K$ , its minimal polynomial is of degree  $\geq \text{card}(I)$ . Then the  $\theta_i$  are separate.*

*Proof.* Let  $j \in I$  be given; we prove that  $\theta_j$  is separate from the set of zeros  $S = \{\theta_i \mid i \in J\}$ , where  $J = I \setminus \{j\}$ . Note that  $P_I \cong_K P_J \circ_K L_j$ . If  $\theta_j$  was a left zero of  $q_S$ , then by Lemma 3.1 we would have that  $\theta_j$  is right algebraic over  $K$ . If in this case  $p$  is the right minimal polynomial of  $\theta_j$  over  $K$  then  $\deg(p) \leq \deg(q_S) \leq \text{card}(I) - 1$ , a contradiction. We conclude that the  $\theta_i$ ,  $i \in I$ , are separate. ■

As a special case, from Lemma 3.2 it follows that if no  $\theta_i$  is right algebraic over  $K$ , they always form a separable set in  $P_I$ . In the other special case that the  $\theta_i$  have the same minimal right polynomial over  $K$  the following can be said:

**THEOREM 3.3.** *Assume  $p \in K[X]$  and  $\theta_i \in L_i$  all have  $p$  as their right minimal polynomial over  $K$ . Then for every  $J \subset I$  the following hold:*

(a) *If  $\text{card}(J) \leq \deg(p)$  the elements  $\theta_i$ ,  $i \in J$ , are separate left zeros of  $p$ .*

(b) *If  $\text{card}(J) = \deg(p)$  the elements  $\theta_i$ ,  $i \in J$ , form a separable splitting set for  $p$ . In this case  $P_J$  splits  $p$ ; in particular then every left zero of  $p$  in  $P_J$  is conjugate to one of the  $\theta_i$ ,  $i \in J$ , in  $P_J$ .*

(c) *If  $\text{card}(J) > \deg(p)$  the field  $P_J$  splits  $p$ . In this case all left zeros of  $p$  in  $P_J$  are conjugates in  $P_J$ . In particular then all  $\theta_i$ ,  $i \in J$ , and all left zeros of  $p$  in  $L$  are conjugates in  $P_J$ .*

*Proof.* (a) This follows from Lemma 3.2.

(b) If  $\text{card}(J) = \deg(p)$  the elements  $\theta_i$ ,  $i \in J$ , are  $\deg(p)$  separate zeros; applying Lemma 2.1 yields (b).

(c) Let  $i, j \in J$  be given; we prove that  $\theta_i$  and  $\theta_j$  are conjugates. Choose a subset  $J_0$  of  $J$  not containing  $i$  and  $j$  with  $\text{card}(J_0) = \deg(p) - 1$  and take  $B = \{\theta_i \mid i \in J_0\}$ . By (b),  $\theta_j$  is dependent on  $B \cup \{\theta_i\}$  but not on  $B$ . From Lemma 1.2 it follows that  $\theta_i$  and  $\theta_j$  are conjugates. Therefore  $p$  has a separable splitting set consisting of conjugate elements. By Lemma 2.1 all left zeros of  $p$  are conjugates. ■

From Theorem 3.3 it follows that every  $P_j$  with  $\text{card}(J) \geq \text{deg}(p)$  contains splitting fields as subfields. In fact these subfields are coproducts of the fields  $K(\theta_i)$  over  $K$ . So in case the fields  $L_i$  are generated over  $K$  by  $\theta_i$ , this theorem implies that the field coproducts  $P_j$  of  $\text{deg}(p)$  or more factors are splitting fields for  $p$ . We state this in the corollary below. In the special case that all  $L_i$  are  $K$ -copies of one field  $L$ , generated over  $K$  by  $\theta$  with minimal polynomial  $p$ , these copowers are transitive splitting fields for  $p$ . Notice that in Theorem 3.3(c) the inner automorphisms connecting  $\theta_i$  need not be  $K$ -automorphisms; this raises the following question:

QUESTION 3.4. *Under what conditions are copowers of an extension  $L$ , generated over  $K$  by  $\theta$  with minimal polynomial  $p$ , of more than  $\text{deg}(p)$  factors inner transitive splitting fields?*

Two partial positive answers to this question are also included in the corollary below.

COROLLARY 3.5. *Assume the fields  $L_i = K(\theta_i)$  are  $K$ -copies of one field  $L$  and the elements  $\theta_i, i \in I$ , have right minimal polynomial  $p$  over  $K$  and correspond to each other. Assume, moreover  $\text{card}(I) \geq \text{deg}(p)$  and take  $S = \{\theta_i | i \in I\}$ . Then the following hold:*

(a) *The set  $S$  is a Galois splitting set for  $p$ . If  $\text{card}(I) = \text{deg}(p)$  then  $P_I$  is a separable transitive splitting field, generated by  $S$ .*

(b) *If  $\text{card}(I) > \text{deg}(p)$ , and if either  $L$  is commutative or  $[L : K]_r = 2$ , then  $P_I$  is an inner transitive splitting field, generated by  $S$ .*

*Proof.* (a) Since every permutation of  $S$  can be extended to a  $K$ -automorphism of  $P_I$ , in this case  $S$  is a Galois splitting set.

(b) We prove that  $S$  is an inner splitting set in the two cases mentioned in (b). First, if  $L$  is commutative, then  $K$  is a subfield of the center of  $P_I$ . Therefore every two conjugates in  $P_I$  are linked by an inner  $K$ -automorphism of  $P_I$ , so by Theorem 3.3(c) we are done. On the other hand, suppose  $[L : K]_r = 2$ . Note that each  $\theta_j$  satisfies the same commutation rule with respect to  $K$ , given by a homomorphism  $\alpha$  and an  $\alpha$ -derivation  $\delta$  of  $K$ :

$$a\theta_j = \theta_j\alpha a + \delta a \quad \text{for } a \in K.$$

Therefore for any  $j, k \in I$

$$\alpha(\theta_j - \theta_k) = (\theta_j - \theta_k)\alpha a$$

and this implies that for different  $i, j, k \in I$  the element

$$s = (\theta_i - \theta_k)(\theta_j - \theta_k)^{-1}$$

commutes with all elements of  $K$ . Since  $\{\theta_k, \theta_j\}$  is a splitting set for the polynomial  $p$  and  $\theta_i \neq \theta_k$ , by Lemma 1.2 it follows that  $\theta_i = s\theta_j s^{-1}$ , where  $s$  commutes with the elements of  $K$ . This proves (b). ■

G. M. Bergman pointed out to the author that the last sentence of Corollary 3.5 can be strengthened in such a way that left polynomial extensions are also included; this provides a (partial) answer to Question 3.4. This result is an application of a generalized form of Dedekind's lemma on dependence of homomorphisms and it will be included in an extended version of [7].

If  $I$  is a finite set with  $\text{card}(I) = m$ , the fields  $P_i$  considered above are finitely generated, and they only split minimal polynomials of degree  $\leq m$ . If we denote by  $P_\omega$  the coproduct of a countable number of copies of  $L$ , then  $P_\omega$  splits minimal polynomials of all degrees. This  $P_\omega$  is countably generated, and in fact is a Galois extension of  $K$ . However, by [3, Lemma 5.5.4],  $P_\omega$  can be embedded in a field which is generated over  $L$  by one element  $t$ , commuting with the elements of  $K$ . This field can be constructed by adjoining a transcendental element  $t$  to  $K$ , commuting with all elements of  $K$ , and then taking the field coproduct over  $K$  of this field and  $L$ , as follows:  $K(t) \circ_K L$ . The situation occurs that one may obtain from  $K$  and one algebraic element (in  $L$ ) a countable number of algebraic elements over  $K$  of the same  $K$ -type by universally adding just one transcendental element  $t$ . Thus, one could say, polynomials are split by (universally) adding transcendental elements. Note that the term transcendental is used here only in the sense of "not algebraic." The precise statements are in this corollary;

**COROLLARY 3.6.** *Let  $P_\omega$  be the coproduct of a countable number of  $K$ -copies of  $L$ . For every right algebraic element of  $L$  its minimal polynomial splits over  $P_\omega$ . The same holds for the extension  $K(t) \circ_K L$  of  $P_\omega$ .*

Two questions which are related to results in the above section may be raised. The first one concerns the possibility of a generalization of Lemma 3.2.

**QUESTION 3.7.** *Assume for each  $i$  that a separable subset  $S_i$  of  $L_i$  is given and that each member of the union  $S$  of these sets  $S_i$  has degree  $> \text{card}(S)$  over  $K$ . Under what circumstances is  $S$  separable?*

The second question concerns the last line of Corollary 3.6.

**QUESTION 3.8.** *Suppose  $K(\theta)$  and  $K(t)$  are extensions of  $K$  by right algebraic elements, with  $\text{deg}(t) \geq \text{deg}(\theta)$ . Under what conditions will the right minimal polynomial  $p$  of  $\theta$  split in the extension  $K(t) \circ_K K(\theta)$ ?*

4. PREDUALS AND SPLITTING FIELDS IN THE CASE OF  $[L : K]_r < \infty$ 

In the case that  $L/K$  is of finite right degree, all elements of  $L$  are right algebraic over  $K$ , and the degrees of their minimal polynomials are bounded by  $[L : K]_r$ . We may summarize our previous results for this case by saying that "in field coproducts of  $m \geq [L : K]_r$  copies of  $L$  over  $K$  all right minimal polynomials of elements of  $L$  split."

For  $L/K$  with finite right degree there exists another class of extensions  $N$  which split all right minimal polynomials of elements of  $L$ ; this is the class that consists of the  $N$  in which  $L/K$  has a right preduel, as defined in [5]. For convenience we first summarize the definition of a right preduel extension.

If  $K \subset N$ , we denote the *centralizer* of  $K$  in  $N$  by  $Z_N(K)$ . If  $K \subset L \subset N$  are fields with  $[L : K]_r < \infty$  we say  $L/K$  has a *right preduel* in  $N$  or  $Z_N(K)/Z_N(L)$  is a *right preduel* of  $L/K$  in  $N$  if  $[Z_N(K) : Z_N(L)]_1 = [L : K]_r$ . We say  $L/K$  and  $L_1/K_1$  are *dual* in  $N$  if they are preduels of each other. For more details about these notions we refer to [5].

**THEOREM 4.1.** *Suppose  $[L : K]_r < \infty$  and  $L/K$  has a right preduel  $L_1/K_1$  in  $N$ . Then any right minimal polynomial of an element of  $L$  is split over  $N$  by an inner Galois splitting set.*

*Moreover, let  $p$  be the right minimal polynomial of some  $\theta \in L$ . Then any set of uniform separate zeros of  $p$  in  $N$  of the same  $K$ -type as  $\theta$  can be obtained as  $\{t_i^{-1}\theta t_i \mid i \in J\}$ , where  $t_i, i \in I$ , is a left basis of  $L_1/K_1$  and  $J \subset I$ . Any left basis of  $L_1/K_1$  can occur in this way.*

**Proof.** Let  $t_i, i \in I$ , be any left basis of  $L_1/K_1$ . Extend  $N$  to an inner closure  $N_0$  of  $N/K$ ; in that case  $L/K$  has a dual  $L_0/K_0$  in  $N_0$ , as follows from [5, Proposition 1.4]. By Proposition 1.5 of the same reference,  $t_i, i \in I$ , is also a left basis of  $L_0/K_0$ . For any  $i \in I$  take  $\theta_i = t_i^{-1}\theta t_i \in N$  and form  $S = \{\theta_i \mid i \in I\} \subset \mathfrak{Z}(p)$ . From Lemma 1.3(a) it follows that for every  $t \in L_0^*$  the element  $t^{-1}\theta t$  is a left zero of  $q_S$ . Applying Lemma 1.1 yields  $q_S = p$ . Therefore  $S$  is a splitting set for  $p$ . This shows how we can obtain from any left basis of  $L_1/K_1$  an inner Galois splitting set for  $p$ . Conversely, let  $\theta_i, i \in J$ , be any set of separate zeros of  $p$  of the same  $K$ -type as  $\theta$ . By the generalized Skolem–Noether theorem [5, Theorem 2.2] we can find elements  $t_i, i \in J$ , of  $Z_N(K)^*$  such that  $\theta_i = t_i^{-1}\theta t_i$ . From Lemma 1.3(b) it follows that the  $t_i, i \in J$ , are left independent over  $K_1$ . Therefore they can be extended to a left basis  $t_i, i \in I$ , of  $L_1/K_1$ . This finishes the proof. ■

In the special case that  $L/K$  is a right polynomial extension the converse of this theorem also holds, as is proved in [7]. In view of the remarks at the start of this section, this gives rise to the following

QUESTION 4.2. *Under what conditions in general can preduals be obtained in field coproducts of a finite number of  $K$ -copies of  $L$ ?*

As a special case, this question may be considered for polynomial extensions. In fact this depends on Question 3.4. Using Bergman's suggestion as mentioned just below Corollary 3.5, some partial answers will be given in [7]. The following is a related open question:

QUESTION 4.3. *Under what conditions does the converse of Theorem 4.1 hold?*

## 5. FINAL REMARKS AND QUESTIONS

Finally, we shall consider three topics on which we can mainly offer open questions and speculations. The first one is the topic of uniqueness of splitting fields, and the second one is about the noncommutative symmetric expressions arising if one expresses the coefficients of  $q_S$  in terms of its zeros, as given by the separable set  $S$ . This third topic is about characterising minimal polynomials and extending our results to nonminimal polynomials.

Let  $p$  be a polynomial over  $K$  of degree  $m$  which is the minimal polynomial of some element in some extension of  $K$ . Concerning the different forms in which splitting fields may appear, the first step one can take is to restrict to separable splitting fields: these are those splitting fields which are generated by a set of  $m$  separate zeros of  $p$ . Every splitting field contains as a subfield one or more separable splitting fields, as is established by Lemma 2.1. In a separable splitting field, say generated by the separable set  $S$ , the zeros in  $S$  may have different or equal  $K$ -type. Notice that in the coproduct  $P_J$  as treated in Theorem 3.3, in the case  $\text{card}(J) > m$  all zeros of  $p$  are conjugates, but the inner automorphisms connecting them may not be  $K$ -automorphisms. Therefore the  $K$ -types of the zeros may be different.

This suggests indexing separable splitting fields by the  $K$ -types. Let  $T$  be a representative set of nonisomorphic zeros of  $p$ , i.e., every zero of  $p$  in some extension is of the same  $K$ -type of one of the elements of  $T$ . Then every  $m$ -tuple  $\theta_0, \dots, \theta_{m-1}$  of elements of  $T$  gives rise to a *universal kind of splitting field based on these  $K$ -types*, given by  $\circ_K K(\theta_i)$  and denoted by  $U(\theta_0, \dots, \theta_{m-1})$ . This gives rise to the following two questions:

QUESTION 5.1. *Under what conditions are  $U(\theta_0, \dots, \theta_{m-1})$  and  $U(\theta'_0, \dots, \theta'_{m-1})$  isomorphic over  $K$ ? Under what conditions is  $U(\theta_0, \dots, \theta_{m-1})$   $K$ -embeddable in  $U(\theta'_0, \dots, \theta'_{m-1})$ ?*

QUESTION 5.2. *Are these  $U(\theta_0, \dots, \theta_{m-1})$  universal in the sense that every splitting field of  $p$  generated by a separable splitting set of the same  $K$ -type as  $\theta_0, \dots, \theta_{m-1}$  is a  $K$ -specialisation of  $U(\theta_0, \dots, \theta_{m-1})$ ? (See [3, Chap. 4] for definitions of specialisations.)*

Probably the answer on this question is positive, since a field coproduct is the universal field of fractions of the ring coproduct, and this universal property is expressible in terms of specialisations (this was noticed by G. M. Bergman).

Depending on the answers on these questions, there may exist essentially different kinds of splitting fields, dependent on the number of  $K$ -types of zeros of  $p$  in extensions. However, one may also pose the following question:

QUESTION 5.3. *Under what conditions does there exist a universal zero of  $p$ , i.e., an extension  $L_0$  of  $K$  generated by a zero  $\theta^*$  of  $p$  such that any extension  $L$  of  $K$  generated by a zero of  $p$  is a  $K$ -specialisation of  $L_0$ , where the zeros are mapped on each other?*

Under conditions such that the answers to Questions 5.2 and 5.3 are affirmative, this provides *one universal splitting field*, namely  $U(\theta^*, \dots, \theta^*)$ .

Second, we turn to the topic of the expressions by which the coefficients of  $q_S$  can be computed from the zeros in the separable set  $S = \{\theta_0, \dots, \theta_{m-1}\}$ . We recall from [6, Proposition 2.3] the following inductively computable factorisation of  $q_S$ , namely  $q_S = q_m$ , where the  $q_i$  are defined by

$$q_i = (X - \beta_0) \cdots (X - \beta_{i-1}) \tag{1}$$

with

$$\beta_j = s_j^{-1} \theta_j s_j \quad \text{and} \quad s_j = \sigma_{\theta_j}(q_j) \neq 0. \tag{2}$$

The monic right polynomial  $q_m$  may be written as

$$q_m = a_0^{(m)} + \cdots + X^{m-1} a_{m-1}^{(m)} + X^m. \tag{3}$$

Expanding (1) and applying (2) the  $a_i^{(m)}$  may be expressed in the zeros  $\theta_0, \dots, \theta_{m-1}$ . For instance for  $m = 2$  this works out in the following way:

$$\begin{aligned} \beta_0 &= \theta_0, & q_1 &= X - \beta_0 = X - \theta_0, & s_1 &= \theta_1 - \theta_0 \\ \beta_1 &= (\theta_1 - \theta_0)^{-1} \theta_1 (\theta_1 - \theta_0) \\ a_0^{(2)} &= \beta_0 \beta_1 = \theta_0 (\theta_1 - \theta_0)^{-1} \theta_1 (\theta_1 - \theta_0) \\ a_1^{(2)} &= \beta_0 + \beta_1 = \theta_0 + (\theta_1 - \theta_0)^{-1} \theta_1 (\theta_1 - \theta_0). \end{aligned}$$

Since  $q_S$  is invariant under permutations of the zeros  $\theta_0, \dots, \theta_{m-1}$  these  $a_j^{(m)}$  are *symmetric expressions*. Although the form of  $a_0^{(2)}$  and  $a_1^{(2)}$  given above does not look symmetric, one can rewrite them as

$$a_0^{(2)} = (\theta_1^{-1} - \theta_0^{-1})(\theta_1 - \theta_0)$$

$$a_1^{(2)} = -(\theta_1 - \theta_0)^{-1}(\theta_1^2 - \theta_0^2).$$

These are built up from the anti-symmetric expressions  $(\theta_1 - \theta_0)$ ,  $(\theta_1^{-1} - \theta_0^{-1})$ , and  $(\theta_1^2 - \theta_0^2)$ . The following question arises:

**QUESTION 5.4.** *Is it possible to build up the coefficients  $a_j^{(m)}$  from some basic obviously symmetric (or anti-symmetric) expressions?*

To make this more formal we can place it in the setting of the universal field of fractions  $N$  of the free algebra  $\mathbb{Q}\langle X_0, \dots, X_{m-1} \rangle$ . The symmetric group on  $X_0, \dots, X_{m-1}$  induces a group of automorphisms  $G$  of  $N$ . The field of invariants of  $G$  will be called  $K$ . Taking  $\theta_j = X_j$ , the symmetric expressions considered above all lie in  $K$ . The field  $N$  is a separable splitting field for  $q_S \in K[X]$ .

**QUESTION 5.5.** *Is  $K$  finitely generated? If so, is it generated by a finite number of explicitly obtainable basic symmetric expressions? How are these generators related to the coefficients of  $q_S$ ?*

For the case of free powers of rings some results are contained in [1]; however, it is not clear whether these results may be carried over to the case of copowers of fields.

We now come to our last couple of questions.

**QUESTION 5.6.** *Under what conditions will a polynomial  $p$  in  $K[X]$  be the right minimal polynomial of an element in some extension field of  $K$ ?*

Notice that for given  $p$  the answer to the above question is unchanged on extension of base-field: if  $p \in K[X]$  is the right minimal polynomial of some  $\theta \in L$  with  $L$  some extension of  $K$ , then for any extension  $N$  of  $K$ , also  $p$  is the right minimal polynomial of  $\theta$  in  $L \circ_K N$  over  $N$ , as follows from Lemma 4.1. This means the criterion may be checked once and for all in the field generated by the coefficients of  $p$ . This is in contrast with the commutative case.

**QUESTION 5.7.** *Under what conditions will a polynomial  $p$  of  $K[X]$  split in some extension of  $K$ ?*

Notice that the polynomial  $X^2 - 2X + 1$  over the rationals does not split in any extension.

## REFERENCES

1. G. M. BERGMAN AND P. M. COHN, Symmetric elements in free powers of rings, *J. London Math. Soc.* (2) **1** (1969), 525–534.
2. P. M. COHN, On the free product of associative rings. *Math. Z.* **71** (1959), 380–398.
3. P. M. COHN, Skew field constructions, *London Math. Soc. Lecture Note Ser.* **27** (1977).
4. T. Y. LAM AND A. LEROY, Algebraic conjugacy classes and skew polynomial rings, in “Perspectives in Ring Theory, Proceedings of Antwerp Conference,” Reidel, Dordrecht.
5. J. TREUR, On duality for skew field extensions, *J. Algebra* **119** (1988), 1–22.
6. J. TREUR, Separate zeros and Galois extensions of skew fields, *J. Algebra* **120** (1989), 392–405.
7. J. TREUR, Polynomial extensions of skew fields, preprint, 1987; also: Report 8805, Dept. of Math., University of Amsterdam, 1988, *J. Pure Appl. Algebra*, in press.