

POLYNOMIAL EXTENSIONS OF SKEW FIELDS

Jan TREUR

*Faculty of Mathematics and Computer Science, Vrije Universiteit, de Boelelaan 1081,
1081 HV Amsterdam, Netherlands*

Communicated by J. Rhodes

Received 30 November 1988

An extension L/K of skew fields is called a *left polynomial extension* with polynomial generator θ if it has a left basis of the form $1, \theta, \theta^2, \dots, \theta^{n-1}$ for some n . This notion of left polynomial extension is a generalisation of the notion of pseudo-linear extension, known from literature. In this paper we show that any polynomial which is the minimal polynomial over K of some element in an extension of K , occurs as the polynomial related to a polynomial generator of some polynomial extension. We also prove that every left cubic extension is a left polynomial extension. Furthermore we give a characterisation of all left cubic extensions which have right degree 2 and construct an example of such a left cubic extension which is not pseudo-linear and which cannot be obtained as a homomorphic image of some form of a skew polynomial ring. Moreover, we give a classification of all cubic Galois extensions and construct examples of them. It is proved that any quartic central extension of a noncommutative ground field is a polynomial extension. A nontrivial example of a quartic central polynomial extension with noncommutative centralizer is also described. A characterisation is given of a right preduel extension of a right polynomial extension in terms of the existence of certain separate zeros. As a corollary a characterisation is derived for polynomial extensions which are Galois extensions in terms of the existence of separate zeros. Finally it is proved that any right polynomial extension has a dual extension which is left polynomial.

1. Introduction

An extension L/K of skew fields is called a *left polynomial extension* with polynomial generator θ if it has a left basis of the form $1, \theta, \theta^2, \dots, \theta^{n-1}$ for some n . The left minimal polynomial p of θ over K is sometimes referred to as the polynomial related to θ . This notion of left polynomial extension is a generalisation of the notion of pseudo-linear extension, known from literature. In this paper some results on polynomial extensions are presented.

In Section 2 we give a characterisation of all intermediate fields of a polynomial extension in terms of factors of the polynomial related to some polynomial generator. Further we show that any polynomial which is the minimal polynomial over K of some element in an extension of K occurs as the polynomial related to a polynomial generator of some polynomial extension.

In Section 3 we prove that every left cubic extension is a left polynomial extension.

sion. We give a characterisation of all left cubic extensions which have right degree 2 and construct an example of such a left cubic extension which is not pseudo-linear and which cannot be obtained as a homomorphic image of some form of a skew polynomial ring. Further in Section 3 we give a classification of all cubic Galois extensions and construct examples of them.

In Section 4 it is proved that any quartic central extension of a noncommutative ground field is a polynomial extension. This is in contrast with the case of a commutative ground field; in that case there can exist commutative quartic extensions which are not polynomial. A nontrivial example of a quartic central polynomial extension with noncommutative centralizer is also described.

In Section 5 we study the zeros of the polynomial related to some polynomial generator. A characterisation is given of a right preduel of a right polynomial extension in terms of the existence of certain separate zeros. As a corollary a characterisation is derived for polynomial extensions which are Galois extensions in terms of the existence of separate zeros. Further it is proved that for every right polynomial extension L/K of degree n a preduel extension may be constructed by taking the copower of $n+1$ copies of L . Finally it is proved that any right polynomial extension has a dual which is left polynomial. Examples are given of right polynomial extensions for which all duals are left polynomial extensions; also examples are given in which this is not the case.

Since in this paper the main concepts introduced in [10–13] are applied, we have to recall the following definitions. More about them can be found in the references mentioned.

In this paper K, L, N, D will be *fields* which may or may not be commutative. If $S \subset K$ we denote the *centralizer* of S in K by $Z_K(S)$ and the *center* of K by $Z(K)$. By $G_{L/K}$ we denote the *group of K -automorphisms* of L . An extension of fields L/K is a *Galois extension* if K is the field of invariants of some group of K -automorphisms of L . We call L/K an *inner extension* if $Z_L Z_L(K) = K$; L/K is an *outer extension* if $Z_L(K) = Z(L)$. Further L/K is called a *central extension* if $K \cdot Z_L(K) = L$ and a *plain extension* if $Z_L(K) = Z(K)$. In [13] it is shown how any L/K can be decomposed into extensions of these types; a *standard decomposition* is also given there.

A *normalizing element* of L/K is an element $\theta \in L^*$ such that $\theta^{-1}K\theta = K$; a *normalizing basis* is a basis that consists of normalizing elements. The extension L/K is called a *normalizing extension* if such a basis exists. A special kind of normalizing extensions is formed by the *crossed products*; we call L/K a *G -crossed product* if G is a group and there exist a normalizing basis $\theta_i, i \in G$ such that for all $i, j \in G$ we have $\theta_i \theta_j = \mu_{i,j} \theta_{ij}$ for certain $\mu_{i,j} \in K$.

If $K \subset L \subset N$ with $[L : K]_l < \infty$ and $K_1 = Z_N(K), L_1 = Z_N(L)$, we call L_1/K_1 a *left preduel* of L/K (in N) if $[L_1 : K_1]_r = [L : K]_l$; L_1/K_1 is called a *dual* of L/K in N if L/K is also right preduel of L_1/K_1 . A paper about these dual extensions is [10]. We call L_2/K_2 a *double-dual* of L/K if L_2/K_2 and L/K have a common dual L_1/K_1 .

If $S \subset L$ is finite, then there exists a *minimal polynomial* q_S of S in $L[X]$ with the

elements of S among its zeros. If the polynomial p is a *left factor* of the polynomial q , we denote this by $p \mid q$. A finite set $S \subset L$ is called *separable* or a set of *separate* elements or zeros if for every $\alpha \in S$ there exists a polynomial $q \in L[X]$ vanishing on $S \setminus \{\alpha\}$ and nonzero on α . We call θ and η *uniform* over K if $\theta \rightarrow \eta$ induces a K -isomorphism: $K(\theta) \rightarrow K(\eta)$. The field L is called a (*uniform*) *separable splitting field* if it is generated over K by a set of n (uniform) separate zeros of a polynomial $p \in K[X]$ with $\deg(p) = n$. In [11, 12] more can be found about these notions. If $S : K \rightarrow K$ is a homomorphism then $D : K \rightarrow K$ is called an *S-derivation* if $D(xy) = D(x)y + S(x)D(y)$ for all $x, y \in K$.

Constructions to provide examples or counterexamples of field extensions L/K can be carried out by describing explicitly the structure of an extension L of a given ground field K . Especially in the commutative case this strategy has turned out to be useful. In the noncommutative case also sometimes these explicit constructions are given. But more often a more implicit strategy is followed by first constructing the field L and afterwards choosing a subfield K of L as the ground field such that L/K has the desired properties. In this case the ground field has a more relative position. A variant of this implicit strategy is to construct L and K at one time, for instance by taking duals or double-duals of a given extension. To describe these kinds of construction methods the following concept is useful: an extension L_1/K_1 is called an *enlargement* of L/K by K_1 if

$$\begin{array}{c} K_1 \subset L_1 \\ \cup \quad \cup \\ K \subset L \end{array}$$

and $K_1 \cap L = K$ and $L_1 = K_1 \cdot L$.

An enlargement of L/K can have a structure which differs a lot from the structure of L/K . Therefore we call L_1/K_1 a *faithful enlargement* of L/K if most of the structure of L_1/K_1 is isomorphic in some sense to that of L/K , i.e. if the following conditions are satisfied:

- (i) The mapping $D \rightarrow K_1 \cdot D$ is an isomorphism between the lattices of intermediate fields of L/K and those of L_1/K_1 , with inverse $D_1 \rightarrow D_1 \cap L$.
- (ii) Any left basis of L/K is also a left basis of L_1/K_1 .
- (iii) The mapping $\omega \rightarrow \omega \mid L$ is an isomorphism between the groups of K_1 -automorphisms of L_1 and of K -automorphisms of L .
- (iv) There exists a commutative field C such that

$$\begin{aligned} Z(K_1) \cap Z(L_1) &= C \cdot (Z(K) \cap Z(L)), & Z_{L_1}(K_1) &= C \cdot Z_L(K), \\ Z(Z_{L_1}(K_1)) &= C \cdot Z(Z_L(K)), & Z(K_1) &= C \cdot Z(K), & Z(L_1) &= C \cdot Z(L). \end{aligned}$$

Notice that this C is a subfield of $Z(K_1) \cap Z(L_1)$. If these are satisfied by some C , then the field $C_0 = Z(K_1) \cap Z(L_1)$ will also satisfy the conditions.

The faithful enlargement L_1/K_1 of L/K is called a *strictly commutative enlarge-*

ment if $K_1 = C \cdot K$. It is called *strictly noncommutative* if $C \subset Z(K) \cap Z(L)$; in this case $Z_{L_1}(K_1) = Z_L(K)$ and so on.

It is easy to verify that if L_1/K_1 is a faithful enlargement of L/K , then the fields $Z_L Z_L(K)$ and $Z_{L_1} Z_{L_1}(K_1)$ correspond to each other under the mapping of (i) and the same holds for $K \cdot Z_L(K)$ and $K_1 \cdot Z_{L_1}(K_1)$; this can be established as follows:

$$\begin{aligned} K_1 \cdot Z_{L_1}(K_1) &= K_1 \cdot C \cdot Z_L(K) = K_1 \cdot Z_L(K) = K_1 \cdot K \cdot Z_L(K), \\ L \cap Z_{L_1} Z_{L_1}(K) &= L \cap Z_{L_1}(C \cdot Z_L(K)) = L \cap Z_{L_1}(C) \cap Z_{L_1}(Z_L(K)) \\ &= L \cap L_1 \cap Z_{L_1}(Z_L(K)) = Z_L Z_L(K). \end{aligned}$$

In a similar way it can be established that the fields $K \cdot Z(Z_L(K))$ and $K_1 \cdot Z(Z_{L_1}(K_1))$ correspond to each other and the same for $Z_L(Z(Z_L(K)))$ and $Z_{L_1}(Z(Z_{L_1}(K_1)))$. These fields together form the standard decomposition of an extension as given in [13, Theorems 6.1, 6.2]; therefore in faithful enlargements the standard decompositions correspond to each other. In particular a faithful enlargement L_1/K_1 is inner, respectively outer if and only if L/K is, and L_1/K_1 is central, respectively plain if and only if L/K is.

An easy way to construct faithful enlargements is by forming a double-dual L_1/K_1 of a given extension L/K in a field N that contains L (using [10, Duality Theorem 1.6]). This construction technique will be used below a number of times to obtain examples and counterexamples.

2. Polynomial extensions

In this section some properties of polynomial extensions are established. Further we give a survey of a number of more specific classes of extensions which are subsumed by the class of polynomial extensions. We start with the following lemma:

Lemma 2.1. *Let L/K be any extension and $\theta \in L$. Then the following hold:*

(a) *(L/K) is a left polynomial extension with generator θ if and only if L is spanned as a left K -linear space by $\{\theta^i \mid i=0, 1, 2, \dots\}$ and θ is left algebraic over K .*

(b) *Further assume L/K is a left polynomial extension with generator θ and polynomial p of degree n . Then there exist unique additive mappings $S_i: K \rightarrow K$ such that for any $a \in K$ the following commutation rule holds:*

$$\theta a = S_0(a) + S_1(a)\theta + \dots + S_{n-1}(a)\theta^{n-1}.$$

Calculations in L can be made using this commutation rule and the polynomial rule given by:

$$\theta^n = \lambda_0 + \lambda_1\theta + \dots + \lambda_{n-1}\theta^{n-1}$$

where the λ_i are related to p in the sense that $p = -\lambda_0 - \lambda_1 X - \dots - \lambda_{n-1} X^{n-1} + X^n$.

(c) *The mappings S_i given in (b) are left and right linear over $Z(K) \cap Z(L)$; fur-*

ther they satisfy certain relations which express field axioms for L such as associativity. If F is the set of all $a \in K$ which satisfy $S_i(a) = 0$ for all $i \geq 2$, then F is a subfield of K . The mapping $S_1|_F: F \rightarrow K$ is a homomorphism and the mapping $S_0|_F: F \rightarrow K$ is an S_1 -derivation.

(d) Assume that θ is a left polynomial generator as above and moreover, θ satisfies the right pseudo-linear commutation rule $a\theta = \theta S(a) + D(a)$ for all $a \in K$. Then the homomorphism $S_1|_F: F \rightarrow K$ as given in (c) is an isomorphism between F and K with inverse S . In this case θ is a right pseudo-linear polynomial generator of L/K of degree $m \leq n$ and $[K:F]_1 < \infty$. Further the following relation holds for the degrees:

$$n = [L:K]_1 = 1 + [F:K]_1 + \dots + [F:K]_1^{m-1}.$$

Proof. (a), (b), (c). These can be verified in a straightforward way.

(d) Suppose, moreover θ satisfies the right pseudo-linear polynomial commutation rule for $a \in K$ of the form

$$a\theta = D(a) + \theta S(a).$$

On the other hand

$$\theta S(a) = S_0 S(a) + S_1 S(a)\theta + \dots + S_{n-1} S(a)\theta^{n-1}.$$

Combining these two commutation rules provides

$$S_1 S(a) = a, \quad S_i S(a) = 0 \quad \text{for all } i \geq 2.$$

This implies that $F \supset S(K)$ and $S_1|_{S(K)}$ is an isomorphism between $S(K)$ and K with inverse S . In particular $S_1|_{S(K)}$ is surjective; since $S_1|_F$ is a homomorphism, it is injective, which implies $F = S(K)$. Using the right pseudo-linear commutation rule for θ , from the left minimal polynomial p a right polynomial for θ over K can be obtained of degree $m \leq n$. Therefore θ is a right pseudo-linear polynomial generator of L/K . From [3, p. 57] it follows that $[K:F]_1 < \infty$; the relation between the degrees is also given there. \square

In the examples given below the field F as defined in (c) above is often of finite codimension in K ; for instance in Section 3 in both cubic examples $[K:F]_1 = 2$.

In general the relations which are satisfied by the S_i as mentioned in (c) above are rather complicated. For this reason we have not summarized them. But in more specific cases they can get a form which is easier to handle. We will define a number of specific cases.

First we consider possible simplifications of the commutation rule. If $S_i = 0$ for all $i \geq 2$ we call L/K a (left) pseudo-linear polynomial extension; this class of extensions satisfies the commutation rule

$$\theta a = D(a) + S(a)\theta \quad \text{for all } a \in K.$$

Here $S: K \rightarrow K$ is an endomorphism and $D: K \rightarrow K$ an S -derivation. For shortness

Table 1
Subclasses of the class of polynomial extensions

	polynomial	binomial	Δ -binomial
polynomial	polynomial	binomial	Δ -binomial
pseudolinear	pseudolinear polynomial	pseudolinear binomial	pseudolinear Δ -binomial
normalizing	normalizing polynomial	normalizing binomial	normalizing Δ -binomial
Δ -normalizing	Δ -normalizing polynomial	Δ -normalizing binomial	Δ -normalizing Δ -binomial
central	central polynomial	central binomial	central Δ -binomial

sometimes these extensions are called pseudo-linear; they are studied in literature in some depth. A pseudo-linear polynomial extension with $D=0$ is called a *normalizing polynomial extension*, and one with $S=\text{identity}$ is called a *Δ -normalizing polynomial extension*. Finally, L/K is called a *central polynomial extension* if θ commutes with the elements of K , i.e. $D=0$ and $S=\text{identity}$. Thus we can distinguish four subclasses of the class of polynomial extensions by simplifying the commutation rule.

Also the polynomial rule can be simplified. One subclass arising in this way is the class of *binomial extensions*; we call L/K a binomial extension if the polynomial p is a binomial $X^n - \lambda_0$, i.e. $\lambda_i=0$ for $1 \leq i \leq n-1$. We call L/K a *Δ -binomial extension* if the polynomial p is of the form $X^n - X - \lambda_0$, i.e. $\lambda_i=0$ for $2 \leq i \leq n-1$ and $\lambda_1=1$. This provides two subclasses of the class of polynomial extensions.

By combining (intersecting) the subclasses defined above we obtain 15 subclasses, as represented in Table 1.

A number of classes of extensions in this table already plays some role in literature. For instance the following results are known:

- any quadratic extension is a pseudo-linear polynomial extension [3, p. 56];
- the right degree of any left pseudo-linear polynomial extension is greater than or equal to the left degree [3, p. 57];
- every pseudo-linear polynomial extension L/K can be obtained as a homomorphic image of a skew polynomial ring $K[X; S, D]$ [3, p. 56];
- any normalizing polynomial extension can be decomposed into an outer central polynomial extension followed by a plain normalizing binomial extension; the centralizer is commutative and singly generated over the center of the ground field [3, p. 61, Theorem 3.4.2];
- under certain conditions any cyclic Galois extension is either a normalizing binomial extension or a Δ -normalizing Δ -binomial extension (outer case: [1],

generalized case: [10, Section 4]);

- any quadratic Galois extension is either a normalizing binomial extension or a Δ -normalizing Δ -binomial extension [4].

After this survey of more specific classes of polynomial extensions we continue with some properties for the general case. In the proposition below for $\theta \in L$ and $D \subset L$ the left minimal polynomial of θ over D is denoted by $p_{\theta/D}$.

Proposition 2.2. *Let L/K be a right polynomial extension with generator θ and polynomial p . Then the following hold:*

(a) *For any intermediate field D of L/K the extension L/D is a right polynomial extension with generator θ .*

(b) *Denote by Φ the lattice of intermediate fields of L/K and by Ψ the set of left factors of p which have θ as a left zero, i.e. $\Psi = \{q \in L[X] \mid X - \theta \mid q \mid p\}$. The mapping $\phi : D \rightarrow p_{\theta/D}$ of Φ into Ψ is injective and for every $D, E \in \Phi$ we have $D \subset E$ implies $\phi(E) \mid \phi(D)$ and $\deg \phi(E) \mid \deg \phi(D)$. Furthermore $\deg \phi(D) = [L : D]_r$ and D is generated by the coefficients of $p_{\theta/D}$ for all $D \in \Phi$.*

Proof. (a) Since $L = \sum K\theta^i \subset \sum D\theta^i \subset L$ we can apply Lemma 2.1(a).

(b) By (a) we have $\deg \phi(D) = [L : D]_r$. If $D, E \in \Phi$ with $D \subset E$ then the right minimal polynomial $p_{\theta/E}$ of θ over E is a left factor of any polynomial over E with θ as a left zero; in particular this holds for $p_{\theta/D}$. Further $\deg \phi(E) = [L : E]_r \mid [L : D]_r = \deg \phi(D)$. To show that ϕ is injective we define a one-sided inverse of it by $q \rightarrow \langle q \rangle$ where $\langle q \rangle$ is the subfield of L generated by K and the coefficients of q . For any $D \in \Phi$ we have $p_{\theta/D} \in D[X]$, so $\langle p_{\theta/D} \rangle \subset D$. Since $p_{\theta/D}$ is the minimal polynomial of θ over D and $p_{\theta/D} \in \langle p_{\theta/D} \rangle[X]$ we have $\phi(\langle p_{\theta/D} \rangle) = p_{\theta/D}$. Therefore,

$$[L : \langle p_{\theta/D} \rangle]_r = \deg p_{\theta/D} = [L : D]_r$$

which implies $\langle p_{\theta/D} \rangle = D$. This shows that ϕ is injective. \square

The following proposition can be obtained by applying the construction given by Schofield in [8, p. 207, Theorem 13.12]. It asserts that any polynomial which is the minimal polynomial of an element is the polynomial related to some polynomial extension.

Proposition 2.3. *Let p be the left minimal polynomial over K of the element θ in an extension L/K . Then there exists an enlargement L_1/K_1 of $K(\theta)/K$ which is a left polynomial extension with generator θ and polynomial p . The right degree of L_1/K_1 may be prescribed by any finite or infinite cardinal $\leq [K(\theta) : K]_r$. \square*

3. Cubic extensions

In the literature a number of papers on quadratic extensions can be found (sec,

for instance [2, 4, 5, 7]). For any quadratic extension a description can be made in terms of a pseudo-linear generator; this appears useful to establish properties of quadratic extensions. On cubic extensions there is hardly any reference in the literature; in general they cannot be described in terms of a pseudo-linear polynomial generator.

In this section we prove that any cubic extension is a polynomial extension. We describe two examples of them. One is an example of an extension L/K with left degree 3 and right degree 2; this is an example of a polynomial extension which is not pseudo-linear. The other one is an example of an inner Galois extension which, as a polynomial extension, is not normalizing nor Δ -normalizing; this type of extension does not occur in the case of quadratic Galois extensions. We also give a classification of all cubic Galois extensions. Further we give a characterisation of all left cubic extensions which are right quadratic and we obtain a negative result on the issue of representability of a polynomial extension as a homomorphic image of some form of a skew polynomial ring.

Theorem 3.1. *Every (left) cubic extension L/K is a (left) polynomial extension. Moreover, for every $\theta \in L \setminus K$ there exists a $\lambda \in K$ such that $\lambda\theta$ is a left polynomial generator of L/K .*

Proof. Suppose such a λ does not exist; then $(a\theta)^2 \in K + K\theta$ for all $a \in K$. In particular $\theta^2 \in K + K\theta$, which implies $\theta^{-1} \in K + K\theta$. Now for any $a \in K$ we have

$$\begin{aligned} a\theta a\theta &\in K + K\theta, \\ \theta a\theta &\in K + K\theta, \\ \theta a &\in K\theta^{-1} + K \subset K + K\theta. \end{aligned}$$

This implies that $K + K\theta$ is a subfield of L , quadratic over K . This contradicts $[L : K]_1 = 3$. \square

In the above theorem a similar argument can provide an element $\mu \in K$ such that $\theta + \mu$ is a polynomial generator of L/K .

Every pseudo-linear polynomial extension can be constructed using a skew polynomial ring $K[X; S, D]$ (see, for instance [3, p. 58]). One could expect the same holds for polynomial extensions in general, using polynomial rings $K[X; S_0, S_1, \dots, S_{n-1}]$ which satisfy the commutation rule

$$Xa = S_0(a) + S_1(a)X + \dots + S_{n-1}(a)X^{n-1} \quad (*)$$

for $a \in K$. These rings are studied, for instance, in [6, 9]. Although these rings might be used to construct some polynomial extensions, not all can be obtained in this way; this is shown by the following proposition. This also provides an example of a polynomial extension which is not pseudo-linear.

Some five years ago it was still an open problem (originally raised by Artin)

whether or not there exist field extensions with finite but different left and right degree. To determine an example of such an extension, one could try to find an explicit description of an extension with different left and right degree which are the lowest as possible, i.e. left degree 3 and right degree 2. According to Theorem 3.1 such a description can be made using a left polynomial generator which is right pseudo-linear. Moreover, one can try to obtain further simplifications by restricting to left binomial extensions and requiring the coefficients of such a binomial to lie in the prime field, for instance the rationals. Such a line of reasoning provided a characterisation of left cubic extensions which are right quadratic, given in Proposition 3.2(a), and the binomial example given in Proposition 3.2(b) below. This example can be considered in some sense as the most simple example of an extension of finite but different left and right degree. To determine more explicitly the ground field K in this example such that the extension L as described actually exists remains a hard problem. However, since in 1985 Schofield [8, p. 207] provided general construction methods which enabled him to solve Artin's problem, nowadays his methods can be used to prove that such an extension as described in Proposition 3.2(b) actually exists.

Proposition 3.2. *Let L/K be a left cubic extension with polynomial generator θ and let the mappings $S_i: K \rightarrow K$ be defined by*

$$\theta a = S_0(a) + S_1(a)\theta + S_2(a)\theta^2$$

for $a \in K$.

(a) *The following are equivalent:*

(i) $[L : K]_r = 2$.

(ii) *There exists a subfield F of K with $[K : F]_l = 2$ such that $S_1|_F: F \rightarrow K$ is an isomorphism between F and K and $S_2(a) = 0$ if and only if $a \in F$.*

(b) *There exists a field K of characteristic zero, containing an element α with $\alpha^3 = 2$, such that K has a cubic left binomial extension L/K generated by θ satisfying*

$$\theta^3 = 2, \quad \theta\alpha = -\alpha^2 - \theta^2.$$

This binomial extension L/K is outer plain; it has right degree 2 and is not pseudo-linear. The mappings S_i do not satisfy the relations needed to define a skew polynomial ring as in () above.*

Moreover, if F is the subfield of K as described in (a), then the extension K/F has left basis $1, \alpha$ and the following relations can be derived:

$$S_1(a + b\alpha) = S_1(a) \quad \text{for all } a, b \in F,$$

$$S_2(a + b\alpha) = -S_1(b) \quad \text{for all } a, b \in F.$$

This implies that the commutation rule of θ with respect to K can be written as

$$\theta(a + b\alpha) = S_0(a + b\alpha) + S_1(a)\theta - S_1(b)\theta^2 \quad \text{for all } a, b \in F.$$

Proof. (a) (i) \Rightarrow (ii). In this case θ is a right pseudo-linear polynomial generator of L/K . Applying Lemma 2.1(d) yields (ii).

(ii) \Rightarrow (i). Let $\alpha \in K \setminus F$ be given. Since $S_2(\alpha) \neq 0$ we have $\theta\alpha \notin K + K\theta$; therefore $1, \theta, \theta\alpha$ is a left basis of L/K . Now let $x \in L$ be given in the form $x = a + b\theta + c\theta\alpha$ with $a, b, c \in K$. Write $b = S_1(b_1)$, $c = S_1(c_1)$ for $b_1, c_1 \in F$, then $S_2(b_1) = S_2(c_1) = 0$, hence

$$\theta b_1 = S_0(b_1) + b\theta, \quad \theta c_1 = S_0(c_1) + c\theta.$$

This yields

$$\begin{aligned} x &= a + b\theta + c\theta\alpha \\ &= a + \theta b_1 - S_0(b_1) + (\theta c_1 - S_0(c_1))\alpha \\ &\in K + \theta K. \end{aligned}$$

This proves that $1, \theta$ is a right basis of L/K .

(b) Apply Proposition 2.2 to $\mathbb{Q}(\theta)/\mathbb{Q}$ with $\theta = \sqrt[3]{2}$, leading to L/K with left basis $1, \theta, \theta^2$ and right basis $1, \theta$. Since the right minimal polynomial of θ over K is a left factor of $X^3 - 2$ in $K[X]$, by a simple calculation we find it is of the form $X^2 + X\alpha + \alpha^2$ for some $\alpha \in K$ with $\alpha^3 = 2$. We can rewrite this to the commutation rule

$$\theta\alpha = -\alpha^2 - \theta^2$$

for α with respect to θ . Therefore $S_0(\alpha) = -\alpha^2$, $S_1(\alpha) = 0$, $S_2(\alpha) = -1$. Since $[L : K]_r < [L : K]_l$ this L/K cannot be a left pseudolinear extension (see [3, p. 57]). From [13, Theorem 6.1] it follows that the prime extension L/K is either inner or outer and also either central or plain. Both inner extensions and central extensions have equal right and left degree (see [13, Proposition 3.5]), so L/K must be outer plain. We prove that L/K cannot be constructed from a skew polynomial ring defined by S_0, S_1, S_2 . If S_0, S_1, S_2 should define a left polynomial ring by (*), we would have the commutation rule $X\alpha = -\alpha^2 - X^2$ for α . So in this ring we would have $X^2 = -\alpha^2 - X\alpha$, and therefore

$$\begin{aligned} X^3 &= X(-\alpha^2 - X\alpha) \\ &= -X\alpha^2 - X^2\alpha \\ &= -X\alpha^2 - (-\alpha^2 - X\alpha)\alpha \\ &= -X\alpha^2 + \alpha^3 + X\alpha^2 \\ &= 2. \end{aligned}$$

This is a contradiction.

Finally we establish the relations for S_1 and S_2 . Let $b \in F$ be given; then $S_2(b) = 0$, so from associativity it follows that

$$\begin{aligned} \theta(b\alpha) &= (\theta b)\alpha \\ &= (S_0(b) + S_1(b)\theta)\alpha \end{aligned}$$

$$\begin{aligned}
 &= S_0(b)\alpha + S_1(b)(\theta\alpha) \\
 &= S_0(b)\alpha + S_1(b)(-\alpha^2 - \theta^2) \\
 &= S_0(b)\alpha - S_1(b)\alpha^2 - S_1(b)\theta^2.
 \end{aligned}$$

This means that for all $b \in F$

$$S_1(b\alpha) = 0, \quad S_2(b\alpha) = -S_1(b).$$

These imply the relations mentioned in (b). \square

This example shows us that sometimes polynomial relations and commutation rules mix up, and this can have farreaching consequences.

In the remainder of this section we go into the issue of classifying the cubic Galois extensions. The following, more general result is basic for this.

Theorem 3.3. *Suppose p is a prime and L/K is a Galois extension of degree p . Then there are two possibilities:*

- (i) *L/K is an outer Galois extension. In this case L/K is a cyclic Galois extension.*
 - (a) *If $Z(K)$ contains the p th roots of unity, then L/K is a normalizing binomial extension.*
 - (b) *If $\text{char}(K) = p$, then L/K is a Δ -normalizing Δ -binomial extension.*
- (ii) *L/K is an inner Galois extension. In this case L/K is inner plain, that is: $Z(K)/Z(L)$ is an extension of commutative fields of degree p .*
 - (a) *If $Z(K)/Z(L)$ is a (cyclic) Galois extension, then L/K is a normalizing binomial extension.*
 - (b) *If $Z(K)/Z(L)$ is an (purely) inseparable extension, then L/K is a Δ -normalizing Δ -binomial extension.*

Proof. The extension L/K can be decomposed into an outer extension followed by an inner extension (for instance, see [3, p. 52, Corollary] or [13, Theorem 6.1]). Since the degree is a prime this decomposition must be trivial; therefore we only have the possibilities (i) and (ii).

(i) If L/K is outer Galois, then $\text{card}(G_{L/K}) = p$, so L/K is a cyclic Galois extension. The remainder of (i) is Amitsurs well known characterisation of outer cyclic Galois extensions (for instance, see [1] or [10]).

(ii) If L/K is inner, then we can decompose it into an inner central extension followed by an inner plain extension (see [13, Theorem 6.1]). However, inner central extensions have a degree which is a square (see [13, Proposition 6.2]). Therefore this part collapses and L/K is inner plain. From [13, Proposition 3.5] it follows that $Z(K)/Z(L)$ is of degree p . The remainder of (ii) is the dual characterisation given by [10, Corollary 3.5 and Proposition 4.4]. \square

If we take $p=2$ in Theorem 3.3 we recover the classification of quadratic Galois extensions as given by Dieudonné in [4]. In the cubic case there are two types of Galois extensions which do not occur in the quadratic case:

- (i) (c) outer cyclic Galois extensions L/K with $\text{char}(K) \neq p$ such that $Z(K)$ does not contain the p th roots of unity.
- (ii) (c) inner plain Galois extensions L/K such that $Z(K)/Z(L)$ is separable but not Galois.

In the cubic case these possibilities (i)(c) and (ii)(c) give rise to polynomial Galois extensions which are not normalizing nor Δ -normalizing, in contrast with the quadratic case. Examples of cubic Galois extensions of type (i)(c) are already known to occur in the commutative case. We finish this section by describing examples of cubic Galois extensions of type (ii)(c) which are binomial and by proving that any cubic Galois extension of type (ii)(c) can be faithfully enlarged to such a binomial extension.

Proposition 3.4. (a) *For any separable cubic extension of commutative fields L_0/K_0 which is not a Galois extension there exists a cubic inner plain binomial extension L/K with $Z(K)=L_0$ and $Z(L)=K_0$. This L/K is a cubic Galois extension which is not normalizing nor Δ -normalizing; it is described in more details in (c).*

(b) *Any cubic inner plain Galois extension with separable non-Galois $Z(K)/Z(L)$ can be faithfully enlarged to an extension as described in (c).*

(c) *The field K contains a quadratic subfield F such that K/F is an inner plain normalizing binomial extension with generator α . The extension L/K has a binomial generator θ which normalizes F . If $S: F \rightarrow F$ is the endomorphism induced by θ , then θ satisfies with respect to K the following relations for some $\lambda, \mu \in F^*$:*

$$\theta^3 = \mu,$$

$$\theta(a + b\alpha) = S(a)\theta + S(b)\lambda\alpha\theta^2 \quad \text{for } a, b \in F.$$

This binomial generator θ is not a pseudolinear generator. The field $Z(F)$ is the normal closure of $Z(K)/Z(L)$.

Proof. (a) Let N_0 be the normal closure of L_0/K_0 and L/F a dual extension of N_0/K_0 (see [10, Duality Theorem 1.6]). From Proposition 2.1 of the same reference it follows that L/F is inner plain, and from [10, Proposition 1.4] we obtain $Z(F)=N_0$ and $Z(L)=K_0$. By [13, Proposition 3.3], L/F and N_0/K_0 are dual inside L . Now take $K=Z_L(L_0)$; by the duality theorem it follows that L/K and L_0/K_0 are dual in L ; the same holds for K/F and N_0/L_0 . As above it follows that both L/K and K/F are inner plain extensions with $Z(K)=L_0$. The field N_0 is the splitting field of the minimal polynomial of any generator of L_0/K_0 . Since this L_0/K_0 is not a Galois extension, $[N_0: L_0]=2$ and the Galois group G of N_0/K_0 is the symmetric group of 6 elements. So this G is generated by two elements ω, τ of order 3, respectively 2, satisfying $\omega\tau = \tau\omega^2$. The elements of G are represented by $1, \omega, \omega^2, \tau, \tau\omega, \tau\omega^2$. By

duality (see [10, Theorem 3.4]) L/F is a G -crossed product with G -basis say θ_i , $i \in G$ satisfying $\theta_i \theta_j = \mu_{i,j} \theta_{ij}$ for certain $\mu_{i,j} \in F$. If we take $\alpha = \theta_\tau$, $\theta = \theta_\omega$ then these are normalizing F . It is easy to calculate:

$$\begin{aligned} \theta^2 &= \mu_{\omega,\omega} \theta_{\omega^2}, & \alpha\theta &= \mu_{\tau,\omega} \theta_{\tau\omega}, \\ \theta^3 &= \mu_{\omega,\omega} \mu_{\omega^2,\omega} \theta_{\omega^3} = \mu_{\omega,\omega} \mu_{\omega^2,\omega} \in F, & \alpha\theta^2 &= \mu_{\tau,\omega} \mu_{\tau\omega,\omega} \theta_{\tau\omega^2}. \\ \alpha^2 &= \mu_{\tau,\tau} \theta_{\tau^2} = \mu_{\tau,\tau} \in F, \end{aligned}$$

Therefore $1, \theta, \theta^2, \alpha, \alpha\theta, \alpha\theta^2$ is a left basis of L/F . Since $\{1, \tau\}$ is the Galois group of N_0/L_0 , it follows by duality (see [10, Corollary 3.5]) that α is a normalizing binomial generator of K/F . This implies that $1, \theta, \theta^2$ is a left basis of L/K . Finally we establish the commutation rule of θ with respect to $K = F(\alpha)$. From $\omega\tau = \tau\omega^2$ it follows that

$$\begin{aligned} \theta\alpha &= \mu_{\omega,\tau} \theta_{\omega\tau} \\ &= \mu_{\omega,\tau} \theta_{\tau\omega^2} \\ &= \lambda \alpha \theta^2 \quad \text{with } \lambda = \mu_{\omega,\tau} \mu_{\tau\omega,\omega}^{-1} \mu_{\tau,\omega}^{-1} \in F. \end{aligned}$$

This implies the commutation rule for θ .

(b) Let any cubic Galois extension L_1/K_1 of type (ii)(c) be given. By a slight adaptation of the above proof it can be shown that it can be faithfully enlarged to an extension L/K as given by (c). To obtain this L/K , in the proof of (a) take $K_0 = Z(L_1)$, $L_0 = Z(K_1)$ and choose a dual that contains L_1 .

(c) This is given in the proof for (a). \square

Notice that a cubic Galois extension as given in Proposition 3.4(a) is cyclic if and only if L_0/K_0 is chosen binomial. Some further information about the zeros of the polynomials in the Galois extensions considered in this section can be found in Section 5, in particular in Corollary 5.2 below.

4. Polynomial extensions of degree 4

Not every extension of left degree 4 is a polynomial extension; in the commutative case any purely inseparable extension of degree 4 is not a polynomial extension. Besides, the field of quaternions over the reals is a noncommutative extension which is not a polynomial extension. However, these examples share the property that they are central extensions with commutative ground field. It turns out that for noncommutative ground fields things are different. In Proposition 4.1 below it is proved that faithfully enlarging the central extensions mentioned above by any noncommutative field makes them polynomial. One could express this phenomenon by: noncommutativity decreases (linear) dependencies. Viewed in this way it even could

be the case that any quartic extension of a noncommutative field is a polynomial extension. This is left open; in this section we only treat the central case:

Proposition 4.1. *Let K be a noncommutative field. Then any quartic central extension L/K is a polynomial extension. Moreover, there are two cases:*

(i) *L/K is an inner central extension. In case $\text{char}(K) \neq 2$ there exists a left polynomial generator θ of L/K satisfying the following relations:*

$$\theta^4 + \lambda_2 \theta^2 + \lambda_0 = 0 \quad \text{for certain } \lambda_0, \lambda_2 \in K,$$

$$\theta a = S_1(a)\theta + S_3(a)\theta^3 \quad \text{for all } a \in K,$$

for some $S_1, S_3 : K \rightarrow K$. The subfield $F = \{a \in K \mid S_3(a) = 0\}$ of K is of the form $Z_K(t)$ for some $t \in K \setminus Z(K)$ depending on the choice of θ . Any $t \in K \setminus Z(K)$ can be obtained by varying the polynomial generator θ .

(ii) *L/K is an outer central extension. If $Z(L)/Z(K)$ is not purely inseparable, then L/K has a central polynomial generator. If $Z(L)/Z(K)$ is purely inseparable, then L/K has a polynomial generator satisfying the relations described in (i).*

Proof. By [13, Theorem 6.1(b)] we can decompose L/K into an outer central extension D/K followed by an inner central extension L/D . From Theorem 6.2 of the same reference it follows that the degree of L/D is a square. Therefore $D=K$ or $D=L$, so there are two cases:

(i) L/K is inner central. In this case $Z_L(K)$ is a division algebra of degree 4 over its center $Z(K)$. We only go into the details of the case $\text{char}(K) \neq 2$; the case of characteristic 2 is similar but somewhat more complicated. In case $\text{char}(K) \neq 2$ the extension $Z_L(K)/Z(K)$ has two generators i, j such that $i^2 = -\lambda$, $j^2 = -\mu$ for certain $\lambda, \mu \in Z(K)$, $ji = -ij$ and $1, i, j, ij$ is a left and right basis of L over K . Choose $\alpha, \beta \in K$ with $\gamma = \beta\alpha - \alpha\beta \neq 0$ and put $\delta = \alpha^2\lambda + \beta^2\mu$. We take $\theta = \alpha i + \beta j$; the remaining proof is rather straightforward. The powers of θ can be calculated as follows:

$$\theta = \alpha i + \beta j, \quad \theta^3 = -(\alpha\delta + \beta\gamma\mu)i - (\beta\delta - \alpha\gamma\lambda)j,$$

$$\theta^2 = -\delta - \gamma ij, \quad \theta^4 = (\delta^2 - \gamma^2\lambda\mu) + (\gamma\delta + \delta\gamma)ij.$$

It is not hard to conclude that the left minimal polynomial of θ over K is of the form

$$p = X^4 + (\gamma\delta\gamma^{-1} + \delta)X^2 + \gamma\delta\gamma^{-1}\delta + \gamma^2\lambda\mu.$$

So $1, \theta, \theta^2, \theta^3$ is a left basis of L/K . We determine the commutation rule of θ with respect to the elements of K . This commutation rule can be obtained from

$$\theta a = \alpha ai + \beta aj \quad \text{for } a \in K,$$

by expressing i and j in $1, \theta, \theta^2, \theta^3$. This is realized by

$$i = \alpha^{-1}\varepsilon^{-1}(\theta^3 + \varepsilon_2\theta), \quad j = -\beta^{-1}\varepsilon^{-1}(\theta^3 + \varepsilon_1\theta),$$

with $\varepsilon_1 = \alpha\delta\alpha^{-1} + \beta\gamma\alpha^{-1}\mu$, $\varepsilon_2 = \beta\delta\beta^{-1} - \alpha\gamma\beta^{-1}\lambda$ and $\varepsilon = \varepsilon_2 - \varepsilon_1$, which apparently is nonzero. Using these relations one can easily derive that

$$\theta a = S_1(a)\theta + S_3(a)\theta^3 \quad \text{for all } a \in K,$$

where $S_1, S_3 : K \rightarrow K$ are defined by

$$S_1(a) = \alpha a \alpha^{-1} \varepsilon^{-1} \varepsilon_2 - \beta a \beta^{-1} \varepsilon^{-1} \varepsilon_1, \quad S_3(a) = \alpha a \alpha^{-1} \varepsilon^{-1} - \beta a \beta^{-1} \varepsilon^{-1}.$$

Notice that $S_3(a) = 0$ if and only if $a \in Z_K(\alpha^{-1}\beta)$.

(ii) L/K is outer central. In this case $Z(L)$ is a quartic extension of $Z(K)$.

If this extension is separable then it is singly generated. If $Z(L)/Z(K)$ is not separable but not purely inseparable, then there exists an inseparable element i with $i^2 \in Z(K)$ and a separable element j such that i, j generate $Z(L)$ over $Z(K)$. The sum of these two elements is a generator of $Z(L)/Z(K)$. So, if $Z(L)/Z(K)$ is not purely inseparable then in all cases it is singly generated. Any generator of it is a central polynomial generator of L/K (see [13, Proposition 3.5(b)]).

If $Z(L)/Z(K)$ is purely inseparable, then it has two inseparable generators i, j which satisfy the same relations as the quaternion generators in the proof of (i). Therefore, for this case the proof can be taken over completely from (i). \square

Remarks. (a) In part (ii) of the above proof the case that $\text{char}(K) = 2$ and L/K is an outer central extension with purely inseparable $Z(L)/Z(K)$ can be proved exactly by the proof of the inner central case of characteristic $\neq 2$. This coincidence enables one to view purely inseparable extensions of commutative fields as degenerate cases of central inner Galois extensions of noncommutative fields.

(b) The polynomial p in Proposition 4.1(i) can also be obtained by computing the minimal polynomial of the set $\{\theta_0, \theta_1, \theta_2, \theta_3\}$ with

$$\begin{aligned} \theta_0 &= \theta = \alpha i + \beta j, & \theta_2 &= j\theta j^{-1} = -\alpha i + \beta j, \\ \theta_1 &= i\theta i^{-1} = \alpha i - \beta j, & \theta_3 &= ij\theta(ij)^{-1} = -\alpha i - \beta j. \end{aligned}$$

The calculation of their minimal polynomial can be done using [11, Proposition 2.3]; it appears that $\theta_0, \theta_1, \theta_2, \theta_3$ are separate zeros of p .

(c) It is possible to establish that the mappings S_1, S_3 in part (i) of the above proposition do not satisfy the relations needed to define a skew polynomial ring as described by (*) in Section 3. So, as in Proposition 3.2 this extension L is not a homomorphic image of such a polynomial ring.

(d) If the element t in (i) above is algebraic over $Z(K)$, then $[K : F]_1 < \infty$.

(e) In case K is a field of quaternions over $Z(K)$ it can be generated by α, β satisfying $\alpha^2 = -\lambda_0$, $\beta^2 = -\mu_0$, $\beta\alpha = -\alpha\beta$ for some $\lambda_0, \mu_0 \in Z(K)$. In this case the polynomial p from Proposition 4.1(i) simplifies to a polynomial over $Z(K)$:

$$p = X^4 + 2\delta X^2 + \delta^2 - 4\lambda_0\mu_0\lambda\mu,$$

with $\delta = -\lambda_0\lambda - \mu_0\mu \in Z(K)$. In this case also $\varepsilon, \varepsilon_1, \varepsilon_2$ are in $Z(K)$, and in fact $\varepsilon_2 = -\varepsilon_1$. The $Z(K)$ -linear mappings S_1, S_3 can be described by:

$$\begin{aligned}
S_1(1) &= 1, & S_3(1) &= 0, \\
S_1(\alpha) &= 0, & S_3(\alpha) &= 2\varepsilon^{-1}\alpha, \\
S_1(\beta) &= 0, & S_3(\beta) &= -2\varepsilon^{-1}\beta, \\
S_1(\alpha\beta) &= -\alpha\beta, & S_3(\alpha\beta) &= 0.
\end{aligned}$$

So, for instance $\theta\alpha = 2\varepsilon^{-1}\alpha\theta^3$ and $\theta\alpha\beta = -\alpha\beta\theta$. In this case $F = Z(K)(\alpha\beta)$.

(f) Proposition 4.1 also shows us that the centralizer of a polynomial extension need not be singly generated over $Z(K)$. This is in contrast with the case of normalizing polynomial extensions, whose centralizers are commutative fields, singly generated over $Z(K)$, which was mentioned in Section 2.

5. Polynomial extensions, separate zeros and duality

The polynomial p related to a generator θ of a right polynomial extension L/K has at least θ as a left zero; it can have more zeros in L , or in an extension N of L . In this section we study extensions N in which p has n uniform separate zeros, with $n = \deg(p)$. By extending such an N further, in this case we can obtain inner K -automorphisms of N which make these uniform separate zeros conjugates (using [3, Theorem 5.5.1]). Below, it will turn out that in such an N the extension L/K has a right predual. The converse of this connection holds in general, as was established in [12, Theorem 4.1]. Therefore in the case of a polynomial extension we have a remarkable characterisation of predual extensions in terms of separate zeros. Moreover, if L_1/K_1 is a dual of L/K in N , then there is a dual correspondence between the sets of n uniform separate left zeros of p in N and the left bases of L_1/K_1 . As a consequence we prove that every right polynomial extension of degree n has a predual extension in the copower over K of $n+1$ copies of L . Furthermore every right polynomial extension has a dual which is a left polynomial extension.

Notice that in this section we deal with *right* polynomial extensions; we have chosen to present it in this way to be able to deal with left zeros of p and with left linear dependence in the dual extension.

Theorem 5.1. *Let L/K be a right polynomial extension with generator θ and minimal polynomial p of degree n . Assume $K \subset L \subset N$ and $K_1 = Z_N(L)$, $L_1 = Z_N(K)$.*

(a) *The following are equivalent:*

- (i) L_1/K_1 is a right predual of L/K (in N).
- (ii) *There exist n uniform separate left zeros of p in N of the form $t_i^{-1}\theta t_i$ for certain elements t_i , $i=0, \dots, n-1$ of L_1^* .*
- (iii) *There exist n uniform separate left zeros of p in N of the form $t_i^{-1}\eta t_i$ for some $\eta \in N$ and certain elements t_i , $i=0, \dots, n-1$ of L_1^* .*

(iv) For any polynomial $q \in K[X]$ of degree m which is the right minimal polynomial of an element η of $L \setminus K$ there exist m uniform separate zeros in N of the form $t_i^{-1}\eta t_i$ for certain $t_i \in L_1^*$, left independent over K_1 .

(b) Assume L/K and L_1/K_1 are dual in N . Let $\eta \in L$ be given such that there exists a set S of n uniform separate zeros of p in N of the same K -type as η . Then η is a polynomial generator of L/K . In particular this holds if such a set S already exists in L . Moreover, there exists a bijective dual correspondence between left bases of L_1/K_1 and sets of n uniform separate zeros of p in N of the same K -type as η . This dual correspondence is given by

$$t_i, i \in I \rightarrow t_i^{-1}\eta t_i, i \in I.$$

Here the sets of n uniform separate zeros inside L correspond to normalizing bases of L_1/K_1 , if any exist.

Proof. (a) (iii) \Rightarrow (i) In [10, Lemma 1.2] it is established that $[L_1 : K_1]_l \leq [L : K]_r$. From [11, Proposition 3.5] it follows that the elements $t_i, i = 0, \dots, n-1$ are left independent over K_1 . Therefore the degrees are equal; this means that L_1/K_1 is a right preduel extension of L/K .

(i) \Rightarrow (iv) This follows from [12, Theorem 4.1].

(iv) \Rightarrow (ii) \Rightarrow (iii) Trivial.

(b) If such a set S exists, then the minimal polynomial of η has as a factor the minimal polynomial of S (see [11, Lemma 1.2]), which is of degree n by [11, Lemma 2.2]. Therefore p is the minimal polynomial of η ; this implies that η is a polynomial generator of L/K . This proves the first part. The part on the dual correspondence is established in [12, Theorem 4.1]. For the remainder, notice that an element $t \in L_1^*$ normalizes K_1 if and only if it normalizes L (see [10, Lemma 2.3]) if and only if $t^{-1}\eta t \in L$. \square

As a corollary of this theorem we can derive the following characterisation of polynomial Galois extensions which was already stated in [11, Theorem 3.6].

Corollary 5.2. *Let L/K be a right polynomial extension with generator θ and minimal polynomial p of degree n . Then the following are equivalent:*

- (i) L/K is a Galois extension.
- (ii) p has n uniform separate zeros in L .
- (iii) Any polynomial q which is the right minimal polynomial of an element of L has $\deg(q)$ uniform separate zeros in L .

Proof. The proof runs as follows: L/K is a Galois extension if and only if L_1/K_1 is a normalizing extension (see [10, Theorem 3.2]) if and only if p has n uniform separate zeros in L (see Theorem 5.1(b), last line). \square

Theorem 5.1 can be used to construct preduel extensions of a polynomial exten-

sion from uniform splitting fields of the polynomial p , by adjoining t_i that make all θ_i conjugates and centralize K . Especially this construction applies to polynomial Galois extensions.

In [12, Corollary 3.5] it has been established that for a singly generated extension L/K with a generator θ that has minimal polynomial p , the copower P_m over K of $m \geq n$ copies of L is a uniform splitting field for p . In Theorem 3.3 of the same reference it is proved that in case $m > n$ the copies θ_i of θ are conjugates in P_m . However, in general it is not clear whether the θ_i are conjugated by inner K -automorphisms, i.e. that leave the elements of K fixed (see also [12, Question 3.4]). But for the case of polynomial extensions G.M. Bergman pointed out to the author that a generalisation of Dedekind's lemma may be used to prove the following result.

Theorem 5.3. *Let L/K be a right polynomial extension of degree n with generator θ , and let P_m be the copower over K of m copies $K(\theta_i)$, $i = 0, \dots, m-1$ of L , where the θ_i correspond to θ and $\theta_0 = \theta$. If $m > n$ then the following hold:*

(a) *In P_m all θ_i are conjugates by inner K -automorphisms.*

(b) *The extension L/K has a predual in P_m .*

In particular, if for every i it holds $\theta_i = t_i^{-1} \theta t_i$ for certain elements $t_i \in P_m^$ centralizing K , then t_0, \dots, t_{m-1} is a left basis of the predual extension of L/K in P_m .*

Proof. (a) Since $m > n$, the m K -homomorphisms $L \rightarrow L_i$ given by $\theta \rightarrow \theta_i$ are left dependent over P_m (for instance see [10, Lemma 1.1]). From Dedekind's lemma (in the generalised form of [3, Theorem 3.3.1]) it follows that some of these K -homomorphisms are conjugated by inner automorphisms of P_m . By symmetry all of these K -homomorphisms are conjugated by inner automorphisms. In particular, since one of them is the identity, this proves that these K -homomorphisms are induced by inner automorphisms of P_m .

(b) This follows from (a) using Theorem 5.1. \square

This theorem shows us that for a substantial class of extensions, namely polynomial extensions, predual extensions may be constructed by adjoining a finite number of zeros. It turns out that the copower construction automatically provides the inner automorphisms that are needed to get a predual extension.

The question may arise what is the dual notion for the notion of a polynomial extension. It is not easy to dualize the notion in a direct way. However, it will be proved below that every right polynomial extension has at least one dual extension which is left polynomial. In fact, the standard construction of dual extensions as given in [10, Appendix] provides such one. This implies that the notion of a polynomial extension is self-dual in some weak sense.

Theorem 5.4. *Every right polynomial extension has a dual which is left polynomial. Moreover, any right polynomial extension L/K has a right predual in the field coproduct $L \circ_K K(t)$ which is a left polynomial extension with generator t .*

Proof. The subfield of $N_0 = L \circ_K K(t)$ generated by the K -copies $t^{-i}Lt^i$ of L is K -isomorphic to their field coproduct over K (see [3, Lemma 5.5.4]). Let θ be a polynomial generator of L/K and p the related polynomial of degree say n . By [12, Theorem 3.3] the elements $\theta_i = t^{-i}\theta t^i$ for $i = 0, \dots, n-1$ are uniform separate zeros of p . Using Theorem 5.1 we conclude L/K has a right preduel in N_0 with left basis $1, t, \dots, t^{n-1}$. From [10, Duality Theorem 1.6(c)] it follows that for any $N \supset N_0$ such that L/K has a dual in N , this dual also has left basis $1, t, \dots, t^{n-1}$. \square

This theorem implies that a weak form of a duality-principle can be stated. As an illustration, let us try to dualize the statement of Proposition 2.2(a):

– for any intermediate field D of a polynomial extension L/K the extension L/D is also a polynomial extension.

Notice that a strict dualization of this statement provides the statement

– for any intermediate field D of a polynomial extension L/K the extension D/K is also a polynomial extension.

In this form this statement cannot be proved (and probably is not true). However, if L_1/K_1 is a dual of L/K which is left polynomial, then there can be constructed duals L_2/K_2 of L_1/K_1 which are faithful enlargements of L/K . In such a dual L_2/K_2 we can realize the intermediate field D_2 corresponding to D to be polynomial over K_2 . By using this construction repeatedly the weak duality-principle can provide:

– there exists a faithful enlargement L_2/K_2 of L/K such that for any intermediate field D_2 of L_2/K_2 the extension D_2/K_2 is a polynomial extension.

The following proposition shows us there actually exist duals of polynomial extensions which are not polynomial.

Proposition 5.5. *Let L/K be a quartic inner right polynomial extension. Then all duals of L/K are left polynomial, except at most one. The possible exception is $Z_L(K)/Z(L)$, which is the dual of L/K inside L . This possible exception may or may not actually occur as an exception.*

Proof. By duality (see [10, Proposition 2.1]) any dual L_1/K_1 of L/K in some N is a central extension. From Proposition 4.1 it follows that L_1/K_1 is a polynomial extension, except, possibly, in the case K_1 is commutative. In this exceptional case, by duality (see [10, Proposition 1.4(a)]) we have

$$K_1 = Z(K_1) = Z(L)$$

and

$$L_1 = K_1 \cdot Z_{L_1}(K_1) = Z(L) \cdot Z_L(K) = Z_L(K).$$

Finally we point out how to construct examples of extensions L/K which satisfy the conditions of this proposition. Firstly an example in which there is no exception can be obtained by taking a dual extension L/K of a quartic separable extension of commutative fields, using Theorem 5.4. Secondly, an example in which the exception actually occurs can be obtained by taking a dual L/K of the field of quaternions

\mathbb{H}/\mathbb{R} over the reals with K noncommutative. This can be realized by the construction given in [10, Appendix]. By duality this L/K is inner central, so from Proposition 4.1 it follows that it is a polynomial extension. In this case the exceptional $Z_L(K)/Z(L)$ is \mathbb{H}/\mathbb{R} and this is not polynomial. \square

6. Final remarks

Polynomial generators can provide descriptions of extensions which cannot be described by pseudo-linear generators. This paper contains some examples of such extensions and their descriptions by polynomial generators. Especially the examples of cubic extensions given in Propositions 3.2(b) and 3.4 can not easily be described in a different way. The description of extensions by a polynomial generator may open the possibility to study the structure of types of extensions which have not been studied yet since they are hard to handle by other means. Therefore it may be interesting to study the concept of polynomial extension somewhat further. We finish by summing up some open questions on polynomial extensions:

- Which other types of quartic extensions are polynomial, and which are not?
- Do there exist extensions of degree 5 which are not polynomial?
- What kind of polynomial extensions can be obtained as a homomorphic image of some skew polynomial ring?
- Is any L/K with noncommutative K a polynomial extension? Or do there exist counterexamples?
- Can any L/K be faithfully enlarged to a polynomial extension? Or do there exist counterexamples?
- Is it possible to distinguish simplifications of the commutation rule of a polynomial extension which is not pseudo-linear and in this way to determine new kinds of extensions?

For instance consider the commutation rule (a special case of which is in Proposition 3.4)

$$\theta a = S_1(a)\theta + S_2(a)\theta^2.$$

If the degree $n \geq 4$, then by evaluating both sides of $\theta(ab) = (\theta a)b$ the following can be obtained:

- S_1 is an endomorphism of K ;
- S_2 is an (S_1, S_1^2) -derivation;
- $S_2 S_1 = -S_1 S_2$, in particular $S_1(F) \subset F$;
- $S_2^2 = 0$.

If the degree is 3, then $S_2 S_1 = -S_1 S_2$ remains true. A second possibility is to study somewhat closer quartic polynomial extensions satisfying $S_0 = S_2 = 0$ as in Proposition 3.4.

- What are the conditions that characterise $[K : F]_1 < \infty$ with F as in Lemma 2.1?

References

- [1] S.A. Amitsur, Noncommutative cyclic fields, *Duke Math. J.* 21 (1954) 87–105.
- [2] P.M. Cohn, Quadratic extensions of skew fields, *Proc. London Math. Soc.* 11 (1961) 531–556.
- [3] P.M. Cohn, *Skew Field Constructions*, London Mathematical Society Lecture Note Series 27 (Cambridge University Press, Cambridge, 1977).
- [4] J. Dieudonné, Les extensions quadratiques des corps non commutatifs et leurs applications, *Acta Math.* 87 (1952) 175–242.
- [5] A. Doneddu, Sur les extensions quadratiques des corps non commutatifs, *J. Algebra* 18 (1971) 529–540.
- [6] I. Gussarian, Sur une généralisation des polynômes de Ore, *Bull. Sci. Math.* 97 (1973) 89–95.
- [7] N. Jacobson, A note on two dimensional division ring extensions, *Amer. J. Math.* 77 (1955) 593–599.
- [8] A.H. Schofield, *Representations of Rings over Skew Fields*, London Mathematical Society Lecture Note Series 92 (Cambridge University Press, Cambridge, 1985).
- [9] T.H.M. Smits, Skew polynomial rings, *Indag. Math.* 30 (1968) 209–224.
- [10] J. Treur, On duality for skew field extensions, *J. Algebra* 119 (1988) 1–22.
- [11] J. Treur, Separate zeros and Galois extensions of skew fields, *J. Algebra* 120 (1989) 392–405.
- [12] J. Treur, Noncommutative splitting fields, *J. Algebra* 129 (1990) 367–379.
- [13] J. Treur, Founding skew field extensions on their centralizers, Report 87–21, Dept. of Mathematics, University of Amsterdam, 1987.