

## Separate Zeros and Galois Extensions of Skew Fields

JAN TREUR

*Potgieterweg 12, 1851 CH Heiloo, The Netherlands*

*Communicated by Nathan Jacobson*

Received June 15, 1987

### 1. INTRODUCTION

In the commutative case one has the following characterisation of Galois extensions of finite degree; we call  $L/K$  a Galois extension if  $K$  is the field of invariants of some group of automorphisms  $G$  of  $L$ :  $K = \text{Inv } G$ .

(0)  $L/K$  is a Galois extension if and only if any polynomial  $p$  of degree  $m$  which is the minimal polynomial of an element of  $L$  has  $m$  distinct zeros in  $L$ .

The notions separability and normality are related to this characterisation.

In the case of skew fields polynomials often have infinitely many zeros, so a different way of counting zeros as distinct is needed.

The well-known theorem of Gordon and Motzkin [2] states that a polynomial of degree  $n$  has zeros in at most  $n$  conjugacy classes. This suggests one should count zeros of a polynomial by the conjugacy classes in which they lie. However, in an inner Galois extension, for every minimal polynomial of an element all zeros are conjugates. That should count them as one. In this paper a different, more differentiated way of counting is proposed such that also in the case of an inner Galois extension the zeros of a polynomial  $p$  are counted as  $\deg(p)$ .

In this paper we introduce a relation between zeros, called "separateness," and count zeros by the maximal number of them which are separate. We prove that this notion has the following properties:

(1) Any polynomial of degree  $m$  has at most  $m$  separate zeros.

(2) If  $L/K$  is a Galois extension, then any polynomial  $p$  of degree  $m$  which is the (right) minimal polynomial of an element of  $L$  has  $m$  separate zeros  $\theta_0, \dots, \theta_{m-1}$ .

The zeros in (2) can be taken *uniform* or of *the same  $K$ -type*; that is: for any  $i, j$ ,  $\theta_i \rightarrow \theta_j$  induces a  $K$ -isomorphism  $K(\theta_i) \cong K(\theta_j)$ . The converse of (2)

holds in case  $L/K$  is a *right polynomial extension*, which means: there exists a generator  $\theta$  such that  $1, \theta, \dots, \theta^{n-1}$  is a right basis of  $L/K$ . So for this type of extension a version of (0) holds.

To establish these results we make use of a connection between separate zeros and factorisations of  $p$  into linear factors (Section 2) and of a connection with independent  $K$ -automorphisms of  $L$  (Section 3). The notion "separate zeros" itself is defined using polynomials from  $K[X]$  which vanish on some part of the set of the zeros that are concerned and are nonzero on the others.

Based on the method of counting zeros introduced here, in Section 4 we define the notion of multiplicity of a zero in a given conjugacy class. This enables us to refine the theorem of Gordon and Motzkin mentioned above to a multiplicity rule. In the special case of a Galois extension all multiplicities of one polynomial are proved to be equal (Section 5). We conclude in Section 6 with a characterisation of all polynomials which have a complete conjugacy class among their zeros and with a result which connects left zeros and right zeros in one conjugacy class.

The notion of multiplicity introduced here differs from the one used in [1]. In our case the connection between zeros and linear factors of the polynomial is guaranteed, which is not the case with their definition. The question which is posed at the end of [1] can easily be answered for our notion of multiplicity, but this answer differs from their (partial) answers.

In this paper  $K, L, N$  will denote fields which may or may not be commutative. Given  $\alpha \in K$  we define the *left substitution*  $\sigma_\alpha: K[X] \rightarrow K$  by  $\Sigma X^i a_i \rightarrow \Sigma \alpha^i a_i$  and  $\mathcal{Z}_K(p) = \{\alpha \in K \mid \sigma_\alpha(p) = 0\}$  is the set of *left zeros* of  $p \in K[X]$ . We often omit the prefix left or subscript  $K$ ; in this paper all zeros will be left zeros. If  $S \subset K$ , by  $Z_K(S)$  we denote the *centralizer* of  $S$  in  $K$ . The *center* of  $K$  is denoted by  $Z(K)$ .

By  $C_\alpha$  we denote the *conjugacy class* of  $\alpha$ . The partition of  $K$  into conjugacy classes  $C_i, i \in I$ , induces a partition of any subset  $S$  of  $K$  into  $S \cap C_i, i \in I$ . We use the symbols  $p, q, r$  for polynomials over some field  $K$  and  $a, b, c$  for elements of  $K$  in general. In particular we use  $\alpha, \beta$  for elements of  $K$  which are or may be zeros of some polynomial and  $s, t$  for elements of  $K$  which are used to form conjugates. A homomorphism  $\omega: K \rightarrow K$  is extended to  $K[X]$  by  $\omega(X) = X$ . The following lemma is easy to verify.

**LEMMA 1.1 (Properties of left substitution).** *Let  $\alpha \in K, s \in K^*, p, q \in K[X], \omega: K \rightarrow K$  be a homomorphism. Then the following hold:*

- (a)  $\sigma_\alpha$  is right  $K$ -linear and left  $Z_K(\alpha)$ -linear.
- (b)  $\sigma_\alpha(sp) = s\sigma_{s^{-1}\alpha s}(p)$  and  $\sigma_\alpha(sps^{-1}) = s\sigma_{s^{-1}\alpha s}(p)s^{-1}$ .
- (c)  $\sigma_\alpha(pq) = \sigma_\alpha(\sigma_\alpha(p)q)$ .

- (d) If  $p \in Z_K(\alpha)[X]$  then  $\sigma_\alpha(pq) = \sigma_\alpha(p) \sigma_\alpha(q)$ .
- (e) If  $s = \sigma_\alpha(p) \neq 0$  then  $\sigma_\alpha(pq) = \sigma_\alpha(p) \sigma_{s^{-1}\alpha s}(q)$ .

In particular  $\sigma_\alpha(pq) = 0$  iff  $\sigma_\alpha(p) = 0$  or  $\sigma_{s^{-1}\alpha s}(q) = 0$ .

- (f)  $\omega(\sigma_\alpha(p)) = \sigma_{\omega(\alpha)}(\omega(p))$ .

Assume  $S \subset K$  is a subset and  $I_S$  is the right ideal of  $K[X]$  consisting of all  $q$  with  $\sigma_\alpha(q) = 0$  for all  $\alpha \in S$ . Since  $K[X]$  is a principal ideal ring there is a unique monic  $q_S$  such that  $I_S = q_S K[X]$ . We call this  $q_S$  the *right minimal polynomial* of  $S$ ; in case  $I_S = 0$  we take  $q_S = 0$ . Note that  $q_S \neq 0$  if and only if  $S \subset \mathcal{Z}(p)$  for some nonzero  $p \in K[X]$ . Such an  $S$  is called (*left*) *bounded*. By  $p|q$  we denote the fact that  $p$  is a left factor of  $q$ . We summarize some properties of right minimal polynomials and left zeros:

LEMMA 1.2 (Properties of minimal polynomials and zeros). *Let  $S, T \subset K$ ,  $\alpha \in K$ ,  $p, q \in K[X]$ , and  $\omega: K \rightarrow K$  be a homomorphism. Then the following hold:*

- (a)  $p|q$  implies  $\mathcal{Z}(p) \subset \mathcal{Z}(q)$ .
- (b)  $S \subset T$  implies  $q_S | q_T$ .
- (c)  $S \subset \mathcal{Z}(p)$  if and only if  $q_S | p$ .
- (d)  $S \subset \mathcal{Z}(q_S)$  and  $q_{\mathcal{Z}(p)} | p$ .
- (e)  $q_{\omega S} = \omega(q_S)$ .

The following lemma can easily be derived from Lemmas 1.1 and 1.2, especially by the very useful 1.1(e).

LEMMA 1.3. *Let  $S \subset K$ ,  $\alpha \in K$ ,  $p \in K[X]$  be given and  $t = \sigma_\alpha(q_S)$ .*

- (a)  $\sigma_\alpha(p) = 0$  if and only if  $p = (X - \alpha)p_1$  for some  $p_1 \in K[X]$ .
- (b) If  $t = 0$  then  $q_{S \cup \{\alpha\}} = q_S$ . If  $t \neq 0$  then  $q_{S \cup \{\alpha\}} = q_S(X - t^{-1}\alpha t)$ . So always  $\deg(q_{S \cup \{\alpha\}}) \leq \deg(q_S) + 1$  and equality holds if and only if  $t \neq 0$ .
- (c) If  $S$  is finite then  $S$  is bounded and  $\deg(q_S) \leq \text{card}(S)$ .

*Proof.* (a) If part: Apply Lemma 1.1(d). Only if part: Use the division algorithm in  $K[X]$  to write  $p = (X - \alpha)p_1 + r$ , where  $\deg(r) < 1$ , so  $r \in K$ . Applying Lemma 1.1(a) and (d) yields  $r = 0$ .

(b) If  $t = 0$ , then  $I_S = I_{S \cup \{\alpha\}}$  by (a); therefore  $q_S = q_{S \cup \{\alpha\}}$  in this case. If  $t \neq 0$ , then  $I_{S \cup \{\alpha\}} \neq I_S$ , so  $q_{S \cup \{\alpha\}} \neq q_S$ . Denoting  $q = q_S(X - t^{-1}\alpha t)$ , we can apply Lemma 1.1(e):  $\sigma_\alpha(q) = \sigma_\alpha(q_S) \sigma_{t^{-1}\alpha t}(X - t^{-1}\alpha t) = 0$ . Therefore  $S \cup \{\alpha\} \subset \mathcal{Z}(q)$ , so by 1.2(b) and (c) we have  $q_S | q_{S \cup \{\alpha\}} | q$ . Since  $q_S$  and  $q_{S \cup \{\alpha\}}$  are not equal, this implies  $q_{S \cup \{\alpha\}} = q$ . The remainder of (b) is clear.

(c) Starting with the empty set, apply (b) repeatedly to build up  $S$ . ■

## 2. SEPARATE ZEROS

To generalize the notion of distinct zeros to a more convenient one for the case of skew fields, we have to count several zeros as one. This is made precise in the following:

**DEFINITION.** Let  $\alpha \in K$  and  $S \subset K$  be given. We call  $\alpha$  *dependent on  $S$*  if there is a finite subset  $F \subset S$  such that for every  $p \in K[X]$ ,  $F \subset \mathcal{Z}(p)$  implies  $\alpha \in \mathcal{Z}(p)$ . The set  $S$  is called a *separable set* or a *set of separate elements* if no  $\alpha \in S$  is dependent on  $S \setminus \{\alpha\}$ . If the elements of a separable set are zeros of some polynomial, we call them *separate zeros*.

To study this notion in more detail we make use of the theory of abstract dependence relations, for instance, given by [3, pp. 18–22]. We recall from this reference that an *abstract dependence relation* on a given set  $U$  is a relation which associates with each finite subset  $S$  of  $U$  certain elements of  $U$ , said to be *dependent on  $S$* , such that the following conditions are satisfied:

- D0. Every  $\alpha \in S$  is dependent on  $S$ .
- D1. (Transitivity) If  $\alpha$  is dependent on  $S$  and each  $\beta \in S$  is dependent on  $T$  then  $\alpha$  is dependent on  $T$ .
- D2. (Exchange property) If  $\beta$  is dependent on  $S \cup \{\alpha\}$  but not on  $S$  then  $\alpha$  is dependent on  $S \cup \{\beta\}$ .

For an infinite set  $S$  we call  $\alpha$  *dependent on  $S$*  if  $\alpha$  is dependent on some finite subset of  $S$ .

The following lemma establishes that our notion of dependence defines an abstract dependence relation.

**LEMMA 2.1.** *Let  $\alpha \in K$  and  $S \subset K$ . The following hold:*

- (a) *Dependence as defined above is an abstract dependence relation.*
- (b) *For finite  $S$  the following are equivalent:*
  - (i)  $\alpha$  is dependent on  $S$ .
  - (ii)  $\alpha \in \mathcal{Z}(q_S)$ .
  - (iii)  $q_S = q_{S \cup \{\alpha\}}$ .

*If these are satisfied and  $S_0 \subset S$  is given such that  $\alpha$  is not dependent on  $S_0$  then  $\alpha$  is conjugate to some  $\beta \in S \setminus S_0$ .*

*Proof.* (b)(i)  $\Rightarrow$  (ii) Let  $F$  be the subset of  $S$  given by the definition above; then in particular  $F \subset \mathcal{Z}(q_S)$  implies  $\alpha \in \mathcal{Z}(q_S)$ . By 1.2(d) the condition of this implication is satisfied. Therefore  $\alpha \in \mathcal{Z}(q_S)$ .

(ii)  $\Rightarrow$  (iii) follows from 1.3(b).

(iii)  $\Rightarrow$  (i) Suppose  $q_{S \cup \{\alpha\}} = q_S$ ; take  $F = S$  in the definition above and let  $p$  be given with  $S \subset \mathcal{Z}(p)$ . From 1.2(c) it follows that  $q_{S \cup \{\alpha\}} = q_S | p$  and again by 1.2(c) the other way around we have  $\alpha \in \mathcal{Z}(p)$ . This proves that  $\alpha$  is dependent on  $S$ . The remainder of (b) follows after (a).

(a) We prove the exchange principle. Assume  $\alpha$  is dependent on  $S \cup \{\beta\}$  but not on  $S$ , where  $S$  is finite. Then

$$\deg(q_{S \cup \{\alpha, \beta\}}) = \deg(q_{S \cup \{\beta\}}) \leq \deg(q_S) + 1 = \deg(q_{S \cup \{\alpha\}}).$$

Therefore  $\beta$  is dependent on  $S \cup \{\alpha\}$ .

(b) Finally we prove the remainder of (b), using the above. Take a minimal subset  $F \subset S$  such that  $\alpha$  is dependent on  $F$ . Since  $F \subset S_0$  cannot happen we can choose an element  $\beta \in F \setminus S_0$ ; write  $F = F_0 \cup \{\beta\}$ ; then by the exchange principle  $q_{F_0 \cup \{\alpha\}} = q_{F_0 \cup \{\alpha, \beta\}} = q_{F_0 \cup \{\beta\}} \neq q_{F_0}$ . Now  $t^{-1}\alpha t = s^{-1}\beta s$  for some  $s, t \in K^*$ , as follows from 1.3(b). ■

LEMMA 2.2. *Let  $S \subset K$  have  $n$  elements  $\alpha_0, \dots, \alpha_{n-1}$  and  $q_i = q_{\{\alpha_0, \dots, \alpha_{i-1}\}}$  for each  $i$ . Then the following are equivalent:*

- (i)  $S$  is separable.
- (ii)  $\mathcal{Z}(q_F) \cap S = F$  for every  $F \subset S$ .
- (iii)  $\sigma_{\alpha_i}(q_i) \neq 0$  for every  $i$ .
- (iv)  $\deg(q_S) = \text{card}(S) = n$ .

*Proof.* (i)  $\Rightarrow$  (ii) If  $\alpha \in S \cap \mathcal{Z}(q_F) \setminus F$  then  $F \subset S \setminus \{\alpha\}$ , so  $\alpha \in \mathcal{Z}(q_F) \subset \mathcal{Z}(q_{S \setminus \{\alpha\}})$ .

(ii)  $\Rightarrow$  (iii) Take  $F = \{\alpha_0, \dots, \alpha_{i-1}\}$ .

(iii)  $\Rightarrow$  (iv) From 1.3 it follows that  $\deg(q_{i+1}) = \deg(q_i) + 1$  for each  $i$ .

(iv)  $\Rightarrow$  (i) Use 1.2:  $\deg(q_{S \setminus \{\alpha\}}) \leq \text{card}(S \setminus \{\alpha\}) < \text{card}(S) = \deg(q_S)$ . ■

Notice that Lemma 2.2 implies that every set of two distinct elements is a separable set; this is even the case if these two elements are conjugates.

The theory of abstract dependence relations, for instance, as given in [3, pp. 18–22], enables us to speak of a *separable basis*  $B$  of  $S$  as a maximal separable subset of  $S$ . The cardinality of such a basis is unique; we call it the *degree* of  $S$ , denoted  $\deg(S)$ . Notice that  $\deg(S) < \infty$  if and only if  $S$  is bounded, in which case  $\deg(S) = \deg(q_S)$ .

In case  $S = \mathcal{Z}(p)$  for some polynomial  $p$  over  $K$ , we speak of a *separable basis of  $p$* , for short. Such a basis can be seen as a kind of system of representatives for the zeros of  $p$ . The following proposition gives a connection with factorisations of  $p$  in linear factors.

**PROPOSITION 2.3.** *Let  $p \in K[X]$  with  $\deg(p) = n$ . Then the following hold:*

(a)  *$p$  has at most  $n$  separate zeros; in fact it has  $m = \deg(q_{\mathcal{Z}(p)}) \leq n$  of them.*

(b) *Let a separable basis  $B$  of  $p$  be formed by the elements  $\alpha_0, \dots, \alpha_{m-1}$  and take  $q_i = q_{\{\alpha_0, \dots, \alpha_{i-1}\}}$  for each  $i$ . Then  $\mathcal{Z}(p) = \mathcal{Z}(q_B)$  and  $q_B = q_{\mathcal{Z}(p)}$ . Furthermore, the elements  $\alpha_0, \dots, \alpha_{m-1}$  induce a factorisation of  $p$  into  $p = q_B \cdot r = q_{\mathcal{Z}(p)} \cdot r$ , where  $q_B$  has a complete factorisation in linear factors, computable by  $q_i = (X - \beta_0) \cdots (X - \beta_{i-1})$ , with each  $\beta_j$  a conjugate of  $\alpha_j$  of the form  $s_j^{-1} \alpha_j s_j$  with  $s_j = \sigma_{\alpha_j}(q_j) \neq 0$ . Every left zero  $\alpha$  of  $p$  is conjugate to one of the  $\alpha_i$  by  $\alpha = s s_i^{-1} \alpha_i s_i^{-1}$  with  $s = \sigma_{\alpha}(q_i) \neq 0$ .*

*Proof.* (a) follows from (b).

(b) Using 1.2(b) and (c), from  $B \subset \mathcal{Z}(p)$  it follows that  $q_B | q_{\mathcal{Z}(p)} | p$ ; by 1.2(a) we conclude  $\mathcal{Z}(q_B) \subset \mathcal{Z}(p)$ . Since  $B$  is a separable basis of  $p$ , by 2.1(b) we have  $\mathcal{Z}(p) \subset \mathcal{Z}(q_B)$ . Therefore  $\mathcal{Z}(p) = \mathcal{Z}(q_B)$ . Applying 1.2(c) yields  $q_{\mathcal{Z}(p)} | q_B$ ; combining this with the already established relation  $q_B | q_{\mathcal{Z}(p)}$  we conclude  $q_B = q_{\mathcal{Z}(p)}$ . For the second part of (b) we proceed inductively. By 2.2, for any  $i$ ,  $s_i = \sigma_{\alpha_i}(q_i) \neq 0$ ; now from 1.3(b) it follows that  $q_{i+1} = q_i(X - \beta_i)$ , where  $\beta_i = s_i^{-1} \alpha_i s_i$ . Note that  $q_0 = 1$  and  $q_m = q_B$ . If  $\alpha \in \mathcal{Z}(p)$ , take  $i$  minimal such that  $\alpha \in \mathcal{Z}(q_{i+1})$ . Then by Lemma 1.1(e)  $\beta_i = s^{-1} \alpha s$ . This proves (b). ■

The factorisation given in 2.3(b) will be called the *factorisation induced* by  $\alpha_0, \dots, \alpha_{m-1}$ . Any permutation of these  $\alpha_i$  induces a permuted factorisation. This provides a kind of commutation rule for linear factors in  $p$ . Any partition of the  $\alpha_i$  induces a partition of the factorisation induced. It turns out that separable bases of sets of zeros can be used to construct and manipulate this kind of factorisations. In 4.1 this technique is applied to say more about the zeros of  $p$ .

Notice that Lemma 2.1 implies that a set of zeros in different conjugacy classes is a special case of a separable set; [1] is a paper about that case, and also gives some constructions of factorisations which are not induced by zeros in the above sense (see pp. 514–515). Our notion of separability also handles separate zeros within one conjugacy class; as mentioned earlier, for instance, any two distinct elements in one conjugacy class are separate.

### 3. SEPARATE ZEROS AND AUTOMORPHISMS

In this section we study how Galois extensions are characterised by the existence of separate zeros. First a lemma.

LEMMA 3.1. *Let  $L/K$  be a Galois extension and  $G$  a set of automorphisms with  $\text{Inv } G = K$ . Then the following hold:*

(a) *Let  $S \subset L$  be bounded. If  $S$  is closed under  $G$  then  $q_S \in K[X]$ . In particular every  $\theta \in S$  is right algebraic over  $K$ .*

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

*Proof.* (a) This follows from  $\omega(q_S) = q_{\omega S} = q_S$ .

(b) Note that  $S \subset \mathcal{L}(p)$  where  $p$  is the minimal polynomial of  $\theta$  implies  $q_S \mid p$ . ■

This lemma and Proposition 2.3 imply:

PROPOSITION 3.2. *Let  $L/K$  be a Galois extension and  $G \subset G_{L/K}$  satisfy  $K = \text{Inv } G$ . Assume  $\theta \in L$  has right minimal polynomial  $p$  over  $K$  of degree  $m$  and  $S = \{\omega(\theta) \mid \omega \in G\}$ . Then the following hold:*

(a)  $\deg(S) = \deg(p) = m$ .

(b) *Any separable basis of  $S$  provides  $m$  uniform separate zeros of  $p$  in  $L$ . Every left zero of  $p$  is conjugate to one of the elements of such a basis.*

This proposition gives one side of the characterisation: in a Galois extension there are a maximal number of separate zeros.

In [5, Appendix] we defined the very useful notion of inner closure; it can play a role similar to the notion of normal closure for an extension of commutative fields. We recall the definition of an inner closure. Notice that we call  $\theta, \theta' \in N$  of the same  $K$ -type if  $K \subset N$  and  $\theta \rightarrow \theta'$  gives a  $K$ -isomorphism  $K(\theta) \cong_K K(\theta')$ ; we call  $L'$  a  $K$ -copy of  $L$  if  $L \cong_K L'$ .

DEFINITION. An extension  $N$  of  $K$  is called an *inner (normal) closure* of  $L/K$  if  $K \subset L \subset N$  and

(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  $N$ .

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

Concerning the existence of inner closures: in [5] for any  $L/K$  an inner closure is constructed. Using this we can state and derive the following.

COROLLARY 3.3. *Let  $L/K$  be any extension and assume  $\theta \in L$  has right minimal polynomial  $p$  of degree  $m$  over  $K$ . Then there exists an extension  $N$  of  $L$  such that in  $N$  the polynomial  $p$  has  $m$  uniform separate zeros. One can take for  $N$  any inner closure of  $L/K$ .*

If  $L = K(\theta)$  in 3.3, then an inner closure of  $L/K$  behaves similarly to a splitting field in the commutative case; a difference is that in the noncommutative case no condition of separability on  $p$  is required.

The converse of 3.2 is less easy.

**LEMMA 3.4.** *Let  $p \in K[X]$ ,  $\theta \in K$ , and  $t_i \in K^*$  for  $i = 0, \dots, m - 1$  be given such that  $\theta_i = t_i^{-1}\theta t_i$  are left zeros of  $p$ . Then the following hold:*

- (a) *If  $e_i \in Z_K(\theta)$  and  $t = \sum e_i t_i \neq 0$ , then  $t^{-1}\theta t$  is a left zero of  $p$ .*
- (b) *If  $\theta_0, \dots, \theta_{m-1}$  are separate zeros of  $p$ , then  $t_0, \dots, t_{m-1}$  are left linearly independent over  $Z_K(\theta)$ .*

*Proof.* (a) This follows from a calculation, using 1.1(a), (b):  $\sigma_{t^{-1}\theta t}(p) = t^{-1}\sigma_\theta(tp) = t^{-1}\sum e_i \sigma_\theta(t_i p) = t^{-1}\sum e_i t_i \sigma_{t_i^{-1}\theta_i}(p) = 0$ .

(b) This follows from (a). ■

Now let  $K \subset L \subset N$  be fields. Below, in Proposition 3.5, we will derive from Lemma 3.4 a connection between uniform separate zeros in  $N$  of a polynomial over  $K$  and independent  $K$ -homomorphisms of  $L$  into  $N$ . The proof makes use of Theorem 5.5.1 of Cohn [2, p. 115], which can be stated as follows:

Let  $\omega: L \rightarrow N$  be a  $K$ -homomorphism. Then  $N$  can be embedded in a field  $N_0$  such that there exists a  $t \in N_0^*$  inducing an inner automorphism of  $N_0$  which, restricted to  $L$ , equals  $\omega$ , i.e.,

$$\omega x = t^{-1}xt \quad \text{for all } x \in L.$$

Moreover, the proof uses Lemma 1.2 of [5], which can be stated as:

Let  $t_i, i \in I$ , be elements of  $Z_N(K)$ . The following are equivalent:

- (i) The  $t_i, i \in I$ , are left independent over  $Z_N(L)$ .
- (ii) The  $K$ -homomorphisms  $\omega_i: L \rightarrow N$  given by  $x \rightarrow t_i^{-1}xt_i$  are left linearly independent over  $N$ .

With these preparations we can derive:

**PROPOSITION 3.5.** *Let  $K \subset L \subset N$  be given and  $K_1 = Z_N(L)$ ,  $L_1 = Z_N(K)$ . Assume  $\theta \in L$  has right minimal polynomial  $p$  over  $K$  and  $\theta_0, \dots, \theta_{m-1}$  are uniform separate zeros of  $p$  with  $\theta_0 = \theta$ . Then the following hold:*

(a) *If  $K$ -homomorphisms  $\omega_i: L \rightarrow N$  are given with  $\omega_i(\theta) = \theta_i$  for all  $i$ , then these are left independent over  $N$ .*

(b) *If  $t_i \in L_i^*$  are given with  $t_i^{-1}\theta t_i = \theta_i$  for all  $i$ , then these are left independent over  $K_1$ .*

*Proof.* (b) This follows from 3.4 using  $Z_N(L) \subset Z_N(\theta)$ .

(a) By repeated application of Cohn's theorem as mentioned above we can extend our  $N$  to an  $N_0$  containing  $t_i$  inducing the  $\omega_i$  on  $L$ . By the lemma mentioned above, now (a) follows from (b). ■

A special case arises if in Proposition 3.5 we have  $[L : K]_r = m = \deg(p)$ , i.e., if  $L/K$  is a right polynomial extension as defined in Section 1. If in this case we embed  $N_0$  in an inner closure  $N_1$  of  $N_0/K$ , and we take  $N = N_1$ , then  $L/K$  and  $L_1/K_1$  are dual in  $N$  and the  $t_i$  form a left basis of  $L_1/K_1$ . In cases  $\theta_i \in L$  for all  $i$ , this is a normalizing basis. By duality in that case  $L/K$  is a Galois extension:

**THEOREM 3.6.** *Let  $L/K$  be a right polynomial extension with generator  $\theta$  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 minimal polynomial of an element of  $L$  has  $m$  uniform separate zeros in  $L$ , where  $m = \deg(q)$ .

In [7] as an application of the results presented here it is proved that any right polynomial extension has a dual which is left polynomial extension.

If  $p$  is a polynomial over  $K$  and  $S$  is a set of left zeros of  $p$  in some extension  $L$  of  $K$ , we shall say that  $S$  is a *splitting set* for  $p$  if  $q_S = p$ . In the same spirit one can call  $S$  a *separable splitting set* for  $p$  if  $S$  is a separable basis for  $p$  and  $q_S = p$ . The extension  $L$  can be called a *splitting field* for  $p$  if it is generated over  $K$  by some splitting set for  $p$ . Consider the situation where the polynomial  $p$  is the right minimal polynomial over  $K$  of some  $\theta \in L$  with  $L = K(\theta)$  and  $n$  is the degree of  $p$ . Then Corollary 3.3 states that any inner closure  $N$  of  $L/K$  is a splitting field for  $p$ . In general inner closures, as we construct them, are infinitely generated over  $K$ . In [6] it is shown that there also exist splitting fields that are finitely generated over  $K$ . It is proved that the (free) field product of  $n$  copies of  $L = K(\theta)$  is also a splitting field for  $p$ . Moreover, in this case the splitting field is generated by a separable splitting set of  $n$  uniform zeros of  $p$ . As a related result we establish that in the field product over  $K$  of  $L$  and  $K(t)$  there exists a splitting set for  $p$ . This field product is even generated by the two elements  $\theta$  and  $t$ ; however, it is not a splitting field for  $p$ , since it is not generated by zeros of  $p$  alone.

#### 4. MULTIPLICITIES AND MULTIPLICITY RULE

The central notion of this section is defined by

**DEFINITION.** The *multiplicity* of a subset  $S$  of  $K$  in a conjugacy class  $C$  of  $K$  is given by  $m_C(S) = \deg(S \cap C)$ . The *multiplicity* of a polynomial  $p$

over  $K$  in  $C$  is the multiplicity of  $\mathcal{Z}(p)$  in  $C$ :  $m_C(p) = m_C(\mathcal{Z}(p))$ . If we speak of the multiplicities of  $p$  or  $S$  we mean the nonzero ones.

The following theorem establishes the multiplicity rule as a relation between the sum of the multiplicities and the degree of a polynomial  $p$ .

**THEOREM 4.1 (Multiplicity rule).** *Let the subset  $S$  of  $K$  and the polynomial  $p$  over  $K$  be given and  $C_i$ ,  $i \in I$ , be a partition of  $K$  into conjugacy classes.*

(a) *The set  $S$  is separable if and only if every  $S \cap C_i$  is separable. The subset  $B$  of  $S$  is a separable basis of  $S$  if and only if every  $B \cap C_i$  is a separable basis of  $S \cap C_i$ . The element  $\alpha$  of  $K$  is dependent on  $S$  if and only if  $\alpha$  is dependent on  $S \cap C_\alpha$ .*

(b) *For  $S$  the following multiplicity rule holds:  $\deg(S) = \sum_{i \in I} m_{C_i}(S)$ . For  $p$  the following multiplicity rule holds:  $\deg(q_{\mathcal{Z}(p)}) = \sum_{i \in I} m_{C_i}(p)$ .*

(c) *Any separable basis of  $\mathcal{Z}(p)$  is up to a permutation of the form  $\beta_{11}, \dots, \beta_{1m_1}, \beta_{21}, \dots, \beta_{2m_2}, \dots, \beta_{r1}, \dots, \beta_{rm_r}$ , where  $r$  is the number of conjugacy classes containing zeros of  $p$  and  $m_1, \dots, m_r$  are the multiplicities of  $p$ ; the zeros  $\beta_{ij}$  and  $\beta_{kl}$  are conjugates if and only if  $i = k$ .*

*Proof.* (a) Suppose  $\alpha$  is dependent on  $S$ . By Lemma 2.1  $\alpha$  is dependent on  $S \cap C_\alpha$ . This proves the third statement of (a). The first and second statements of (a) follow directly from the third one.

(b) The first statement of (b) follows (a); the second statement follows from the first using  $\deg(q_{\mathcal{Z}(p)}) = \deg(\mathcal{Z}(p))$ , which follows from Lemma 2.2.

(c) This follows from (a) and (b). ■

This theorem is a refinement of the well-known result of Gordon and Motzkin [4] which states that the zeros of a polynomial of degree  $n$  lie in at most  $n$  conjugacy classes. Using our theorem above, more can be said. For instance, if there exists a conjugacy class  $C$  containing more than one zero of  $p$ , then  $m_C(p) \geq 2$ ; so the zeros lie in strictly less than  $n$  conjugacy classes. In case the zeros lie in exactly  $n$  conjugacy classes,  $p$  has exactly  $n$  zeros. The multiplicity rule also can be used to distinguish some cases if the degree of  $q_{\mathcal{Z}(p)}$  is low: if this degree is 2, there are two possibilities, namely  $m_1 = 1$  and  $m_2 = 1$  or  $m_1 = 2$ ; if the degree is 3, there are three possibilities, namely 1, 1, 1 or 1, 2, or 3. The theorem below will show that in a Galois extension only two of these three possibilities can occur. In the case of degree 4 there are five possibilities, two of which are excluded in a Galois extension.

## 5. MULTIPLICITIES IN GALOIS EXTENSIONS

In the case of a Galois extension the multiplicity rule can be rewritten to a very simple form: the degree of  $p$  is the product of the number of conjugacy classes and one uniform multiplicity. To be more precise:

**THEOREM 5.1.** *Let  $L/K$  be a Galois extension and  $G$  a group of automorphisms with  $\text{Inv } G = K$ . Assume the element  $\theta$  of  $L$  has right minimal polynomial  $p$  over  $K$  and  $r$  is the number of conjugacy classes of  $L$  containing left zeros of  $p$ . Then all multiplicities of  $p$  are equal, say  $m$ . The multiplicity rule takes the form  $\text{deg}(p) = rm$ . The subgroup  $H = \{\omega \in G \mid \omega(\theta) \in C_\theta\}$  of  $G$  satisfies  $[G : H] = r$ .*

*Proof.* It is easily verified that  $H$  is a subgroup of  $G$  containing all inner automorphisms in  $G$ . The partition of  $G$  into left cosets  $\omega H$  of  $H$  induces a partition  $\omega H \theta$  of  $S = \{\omega(\theta) \mid \omega \in G\}$  in different conjugacy classes. Therefore  $[G : H] = r$ . Choose a separable basis  $B$  of  $S \cap C_\theta = H\theta$ . For any  $\omega \in G$  the set  $\omega B$  is a separable basis of  $\omega H \theta$ . By Theorem 4.1 the union of these sets  $\omega B$ , denoted by  $GB$ , is a separable basis of  $S$  of cardinality  $rm$  with  $m = m_{C_\theta}(S)$ . From Proposition 3.2 we know  $\text{deg}(p) = \text{deg}(S)$ . This finishes the proof. ■

In particular this theorem shows us that in a Galois extension the number of conjugacy classes containing zeros of  $p$  is a divisor of the degree of  $p$  for any minimal polynomial  $p$  of an element of  $L$ . The same holds for multiplicities. Therefore as a corollary we have:

**COROLLARY 5.2.** *Let  $L/K$  be a Galois extension and  $p$  the right minimal polynomial over  $K$  of an element of  $L$ . If  $\text{deg}(p)$  is a prime, then there are only two possibilities:*

*Either:  $p$  has exactly  $\text{deg}(p)$  zeros in  $L$ ; these lie in different conjugacy classes.*

*Or: All zeros of  $p$  in  $L$  are conjugates.*

If  $L/K$  is an inner Galois extension then the second possibility is always realized; this is established, for instance, in Proposition 3.2. If in Theorem 5.1 we have  $[G : G \cap \text{Int}(L)] < \infty$  then  $r$  is a divisor of this degree and if also  $[L : K] < \infty$  then  $r$  divides this degree. It is unclear under what conditions  $r = [G : G \cap \text{Int}(L)]$  or, equivalently,  $H = G \cap \text{Int}(L)$ .

## 6. ZEROS IN ONE CONJUGACY CLASS

The multiplicity of a polynomial  $p$  in a conjugacy class  $C$  is not only bounded by  $\text{deg}(p)$ , as expressed in the multiplicity rule, but also by

$\deg(C)$ . In particular if  $\deg(C)$  is finite this can provide restrictions. The following proposition characterises this.

**PROPOSITION 6.1.** *For  $\alpha \in K$  the following are equivalent:*

- (i)  $\deg(C_\alpha) < \infty$ .
- (ii)  $\alpha$  is algebraic over  $Z(K)$ .
- (iii)  $C_\alpha \subset \mathcal{X}(p)$  for some polynomial  $p$  over  $K$  with  $p \neq 0$ .

*If these are satisfied and if  $p_\alpha$  is the minimal polynomial of  $\alpha$  over  $Z(K)$ , then  $p_\alpha = q_{C_\alpha}$ ,  $\mathcal{X}(p_\alpha) = C_\alpha$ ,  $\deg(p_\alpha) = \deg(C_\alpha)$ ,  $m_{C_\alpha}(p) = \deg(C_\alpha)$ , and  $p_\alpha$  is a divisor of  $p$ . The polynomial  $p_\alpha$  has  $\deg(p_\alpha)$  uniform separate zeros in  $K$ .*

*Proof.* (i)  $\Rightarrow$  (ii) The set  $C_\alpha$  is closed under the group  $\text{Int}(K)$  of inner automorphisms and is also bounded. From Lemma 3.1(a) it follows that the polynomial  $q_{C_\alpha}$  has its coefficients in the field  $\text{Inv Int}(K) = Z(K)$ .

(ii)  $\Rightarrow$  (iii) This is immediate.

(iii)  $\Rightarrow$  (i) These are equivalent statements of the fact that  $C_\alpha$  is bounded.

The remainder of this proposition follows from Lemma 3.1(b). ■

The above proposition also determines the polynomials over  $K$  that contain a complete conjugacy class among their zeros. These are the polynomials with highest possible multiplicity in  $C_\alpha$ , namely  $\deg(C_\alpha)$ . This contrasts with [1, Theorem 2B]. This seemingly contradicts our results. The difference lies in the notion of multiplicity as defined by them: in their construction to prove Theorem 2B on pp. 514–515 the connection between zeros and factorisations is lost, whereas we guarantee this connection and employ it. Using our notion of multiplicity we can answer the open question they finish with : whether or not Theorem 2B is true in the case where  $[K : Z(K)]$  is infinite. The answer is embodied by the following proposition.

**PROPOSITION 6.2.** *Let  $p$  be a monic polynomial over  $K$  of degree  $m$  and multiplicity  $m$  in the conjugacy class  $C_\alpha$ . Then the following hold: If  $m + 1 < \deg(C_\alpha)$  then there exist infinitely many monic polynomials  $p'$  over  $K$  such that  $p$  is a left divisor of  $p'$ ,  $\deg(p') = m + 1$  and  $p'$  has multiplicity  $m + 1$  in  $C_\alpha$ . If  $m + 1 = \deg(C_\alpha)$  then there exists a unique  $p'$  as described above, namely  $q_{C_\alpha}$ . If  $m = \deg(C_\alpha)$  then such  $p'$  do not exist.*

*Proof.* If  $m = \deg(C_\alpha)$ , then such a  $p'$  should have a multiplicity  $> \deg(C_\alpha)$  in  $C_\alpha$ ; this is impossible. If  $m = \deg(C_\alpha) - 1$ , then such a  $p'$  should satisfy  $m_{C_\alpha}(p') = \deg(p') = \deg(C_\alpha)$ , so  $p' = q_{\mathcal{X}(p')} = q_{C_\alpha}$ . From  $\mathcal{X}(p) \subset C_\alpha$  it follows that  $p | q_{C_\alpha}$ ; therefore  $p' = q_{C_\alpha}$  satisfies.

We now turn to the case  $m + 1 < \text{deg}(C_\alpha)$ . Choose a separable basis  $B$  of  $\mathcal{Z}(p)$ ; this  $B$  has cardinality  $m$ . From  $m + 2 \leq \text{deg}(C_\alpha)$  it follows that we can extend  $B$  to a separable set  $S = B \cup \{\beta, \gamma\} \subset C_\alpha$ . Say  $\beta = s^{-1}\alpha s$ ,  $\gamma = t^{-1}\alpha t$  for some  $s, t \in K^*$ . Define for  $d \in Z_K(\alpha)$

$$\begin{aligned} t_d &= t + ds, \\ \alpha_d &= t_d^{-1}\alpha t_d, \\ p_d &= q_{B \cup \{\alpha_d\}}. \end{aligned} \tag{1}$$

Then it is clear that  $p = q_B | p_d$ . We prove that  $p_d$  can be taken for  $p'$  and all are different. Suppose  $d, e \in Z_K(\alpha)$  are given with  $d \neq e$ . By (1) we can write  $t_e - t_d = (e - d)s$  so  $s$  can be expressed as a linear combination  $(e - d)^{-1} = (t_e - t_d)$  in  $t_d, t_e$  with coefficients from  $Z_K(\alpha)$ . From Lemma 3.4(a) it follows that  $\beta$  is dependent on  $\{\alpha_d, \alpha_e\}$ . Again by (1) we have  $t = t_d - ds$ ; as above we conclude that  $\gamma$  is also dependent on  $\{\alpha_d, \alpha_e\}$ . It follows that  $\text{deg}(B \cup \{\alpha_d, \alpha_e\}) \geq \text{deg}(B \cup \{\beta, \gamma\}) = m + 2$ . This implies that  $\alpha_d$  is not dependent on  $B$  and  $\mathcal{Z}(p_d) \neq \mathcal{Z}(p_e)$ . Therefore  $p_d \neq p_e$  and  $\text{deg}(p_d) = m + 1$ . So each  $p_d$  can be taken for  $p'$ ; they are all different. Since  $\text{deg}(C_\alpha) \geq 2$  the field  $K$  is not commutative. By [2, Theorem 3] we conclude that  $Z_K(\alpha)$  is infinite; this provides infinitely many possibilities for  $p'$ . ■

This proposition can easily be generalized to the situation that more conjugacy classes are given (using Theorem 4.1), which answers the question of Bray and Whaples mentioned earlier.

We close with the following curious result on left and right zeros in one conjugacy class.

**PROPOSITION 6.3.** *Let  $p$  be the right minimal polynomial of some  $\theta \in L$  over the subfield  $K$  of  $L$ . Assume  $p$  has a right zero  $\alpha$  in  $K$ . Then  $\alpha$  and  $\theta$  are conjugates in  $L$ . In particular all such  $\alpha$  lie in one conjugacy class of  $L$ . The same holds for all such  $\theta$ .*

*Proof.* Since  $\alpha$  is a right zero we can write  $p = q(X - \alpha)$  with  $q$  a polynomial over  $K$ . From the fact that  $p$  is the right minimal polynomial of  $\theta$  we have  $\sigma_\theta(q) \neq 0$ . By Lemma 1.1(e) we get  $\alpha = t^{-1}\theta t$  with  $t = \sigma_\theta(q)$ . ■

The conditions in this proposition may look strange, but this situation can happen easily: take for  $K$  the field of complex numbers and for  $L$  the field of quaternions; then  $\alpha = i, \theta = j$  satisfy the conditions, where  $p = X^2 + 1$ .

*Additional Remarks*

The material presented here was developed during the period from 1980 to 1984. A first draft containing this material was finished in December

1984. This draft has had a very limited distribution; in January 1985 Prof. P. M. Cohn in London received a copy and made some comments on it. A rewritten draft was submitted in June 1986 and accepted, in a revised form, in September 1987.

In May 1988 Prof. G. M. Bergman noticed some overlap of this paper with Prof. T. Y. Lam's paper "A General Theory of Vandermonde Matrices" [*Exp. Math.* **4** (1986), 193–215]. It turns out that Sections 4 and 5 of Lam's paper contain a number of results which correspond to results of Sections 2 and 4 above. In this paper these results are treated in the more general setting of skew polynomial rings. Moreover, Lam gives a characterisation of the dependence relation between zeros  $\alpha_i$  in a field  $K$  by linear dependence of the elements  $(1, \alpha_i, \alpha_i^2, \dots)$  in the linear space  $K^\omega$  (see Prop. 17). More results are presented in [T. Y. Lam and A. Leroy, "Algebraic Conjugacy Classes and Skew Polynomial Rings," Report PAM-391, Center for Pure and Applied Mathematics, University of California (to appear in "Perspectives in Ring Theory," Proc. of Antwerp Conf., Reidel, Dordrecht), 1987].

Prof. G. M. Bergman has also given some suggestions for slight improvements in the presentation of our paper.

#### REFERENCES

1. U. BRAY AND G. WHAPLES, Polynomials with coefficients from a division ring, *Canad. J. Math.* **35** (1983), 509–515.
2. P. M. COHN, "Skew Field Constructions," Cambridge Univ. Press, London/New York, 1977.
3. P. M. COHN, "Algebra," Vol. 2, Wiley, New York, 1977.
4. B. GORDON AND T. S. MOTZKIN, On the zeros of polynomials over division rings, *Trans. Amer. Math. Soc.* **116** (1965), 218–226; **122** (1966), 547.
5. J. TREUR, On duality for skew field extensions, *J. Algebra* **119** (1988), 1–22.
6. J. TREUR, Noncommutative splitting fields, *J. Algebra*, in press.
7. J. TREUR, Polynomial extensions of skew fields, preprint, 1987.