



**HAL**  
open science

## A generalisation of Amitsur's A-polynomials

Adam Owen, Susanne Pumplün

► **To cite this version:**

Adam Owen, Susanne Pumplün. A generalisation of Amitsur's A-polynomials. Communications in Mathematics, 2021, Volume 29 (2021), Issue 2 (Special Issue: 3rd International Workshop on Nonassociative Algebras in Málaga) (2), pp.281 - 289. 10.2478/cm-2021-0025 . hal-03665015

**HAL Id: hal-03665015**

**<https://hal.science/hal-03665015v1>**

Submitted on 11 May 2022

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

## A generalisation of Amitsur’s A-polynomials

Adam Owen, Susanne Pumplün

**Abstract.** We find examples of polynomials  $f \in D[t; \sigma, \delta]$  whose eigenring  $\mathcal{E}(f)$  is a central simple algebra over the field  $F = C \cap \text{Fix}(\sigma) \cap \text{Const}(\delta)$ .

### Introduction

Let  $K$  be a field of characteristic 0 and  $R = K[t; \delta]$  be the ring of differential polynomials with coefficients in  $K$ . In order to derive results on the structure of the left  $R$ -modules  $R/Rf$ , Amitsur studied spaces of linear differential operators via differential transformations [2], [3], [4]. He observed that every central simple algebra  $B$  over a field  $F$  of characteristic 0 that is split by an algebraically closed field extension  $K$  of  $F$ , is isomorphic to the eigenspace of some polynomial  $f \in K[t; \delta]$ , for a suitable derivation  $\delta$  of  $K$ . This identification of a central simple algebra  $B$  with a suitable differential polynomial  $f \in K[t; \delta]$  he called *A-polynomial* also holds when  $K$  has prime characteristic  $p$  [2, Section 10], [18].

Let  $D$  be a central division algebra of degree  $d$  over  $C$ ,  $\sigma$  an endomorphism of  $D$  and  $\delta$  a left  $\sigma$ -derivation of  $D$ . Our aim is to provide a partial answer to the following generalisation of Amitsur’s investigation:

*“For which polynomials  $f$  in a skew polynomial ring  $D[t; \sigma, \delta]$  is the eigenring  $\mathcal{E}(f)$  a central simple algebra over its subfield  $F = C \cap \text{Fix}(\sigma) \cap \text{Const}(\delta)$ ?”*

After the preliminaries in Section 1, we investigate two different setups, always assuming that  $f$  has degree  $m \geq 1$  and that the minimal left divisor of  $f$  is square-free. We look at generalised A-polynomials in  $D[t; \sigma]$  in Section 2, where  $\sigma$  is an automorphism of  $D$  with  $\sigma^n = \iota_u$  for some  $u \in D^\times$ . Then  $f$  is a generalised A-polynomial in  $R$  if and only if  $f$  right divides  $u^{-1}t^n - a$  for some  $a \in F$  (Theorem 2). If  $n$  is prime and not equal to  $d$ , then  $f$  is a generalised A-polynomial in  $R$  if

---

2020 MSC: Primary: 17A35; Secondary: 17A60, 17A36, 16S36

Key words: Skew polynomial ring, reducible skew polynomials, eigenspace, nonassociative algebra, semisimple Artinian ring.

Affiliation:

School of Mathematical Sciences, University of Nottingham, University Park,  
 Nottingham NG7 2RD, United Kingdom

E-mail: adam.owen@nottingham.ac.uk; susanne.pumpluen@nottingham.ac.uk

and only if one of the following holds: (i) There exists some  $a \in F^\times$  such that  $ua \neq \prod_{j=1}^n \sigma^{n-j}(b)$  for every  $b \in D$ , and  $f(t) = t^n - ua$ . In this case  $f$  is an irreducible polynomial in  $R$ . (ii)  $m \leq n$  and there exist  $c_1, c_2, \dots, c_{m-1}, b \in D^\times$ , such that  $u^{-1} \prod_{j=0}^{n-1} \sigma^{n-j}(b) \in F^\times$ , and  $f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(b))(t - \Omega_1(b))$ . (Theorem 3). In particular,  $f$  is a generalised A-polynomial in  $R = K[t; \sigma]$ ,  $K$  a field, if and only if  $f$  right divides  $t^n - a$  in  $R$  (Theorem 4). If moreover  $n$  is prime then  $f$  is a generalised A-polynomial in  $R = K[t; \sigma]$ , if and only if one of the following holds: (i) There exists some  $a \in F^\times$  such that  $a \neq N_{K/F}(b)$  for any  $b \in K$ , and  $f(t) = t^n - a$ . In this case  $f$  is irreducible. (ii)  $m \leq n$  and there exist some constants  $c_1, c_2, \dots, c_{m-1}, b \in K^\times$ , such that  $f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(b))(t - \Omega_1(b))$  (Corollary 1).

In Section 3, we study generalised A-polynomials in  $D[t; \delta]$ , where  $C$  has prime characteristic  $p$  and  $\delta$  is an algebraic derivation of  $D$  with minimum polynomial  $g(t) \in F[t]$  of degree  $p^e$  such that  $g(\delta) = \delta_c$  for some nonzero  $c \in D$ . Then  $f$  is a generalised A-polynomial in  $D[t; \delta]$  if and only if  $f$  right divides  $g(t) - (b + c)$  for some  $b \in F$ . In particular,  $\deg(f) \leq p^e$  (Theorem 6). In the special case that  $g(t) = t^p - at$ ,  $f$  is a generalised A-polynomial in  $R$  if and only if one of the following holds: (i)  $f(t) = h(t) = t^p - at - (b + c)$ , and  $V_p(\alpha) - a\alpha - (b + c) \neq 0$  for all  $\alpha \in D$ . In this case  $f$  is irreducible in  $R$ . (ii)  $h(t) = t^p - at - (b + c)$  for some  $a, b \in F$ ,  $m \leq p$  and  $f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(\alpha))(t - \Omega_1(\alpha))$  for some  $c_1, c_2, \dots, c_{m-1} \alpha \in D^\times$ , such that  $V_p(\alpha) - a\alpha - (b + c) = 0$  (Theorem 7).

The results are part of the first author’s PhD thesis written under the supervision of the second author.

## 1 Preliminaries

### 1.1 Skew Polynomial Rings ([12], [13], [15], [16])

Let  $D$  be a unital associative division algebra over its center  $C$ ,  $\sigma$  an endomorphism of  $D$ , and  $\delta$  a left  $\sigma$ -derivation of  $D$ , i.e.  $\delta$  is an additive map on  $D$  satisfying  $\delta(xy) = \sigma(x)\delta(y) + \delta(x)y$  for all  $x, y \in D$ . For  $u \in D^\times$ ,  $\iota_u(a) = uau^{-1}$  is called an *inner automorphism* of  $D$ . If there exists  $n \in \mathbb{Z}^+$  such that  $\sigma^n = \iota_u$  for some  $u \in D^\times$ , and  $\sigma^i$  is not an inner derivation for  $1 \leq i < n$ , then  $\sigma$  is said to have *finite inner order*  $n$ . For  $c \in D$ , the derivation  $\delta_c(a) = [c, a] = ca - ac$  for all  $a \in D$  is called an *inner derivation*. The *skew polynomial ring*  $R = D[t; \sigma, \delta]$  is the set of skew polynomials  $a_m t^m + a_{m-1} t^{m-1} + \dots + a_1 t + a_0$  with  $a_i \in D$ , endowed with term-wise addition and multiplication defined by  $ta = \sigma(a)t + \delta(a)$  for all  $a \in D$ .  $R$  is a unital associative ring. If  $\delta = 0$ , we write  $R = D[t; \sigma]$ . If  $\sigma = \text{id}_D$ , we write  $R = D[t; \delta]$ .

For  $f(t) = a_m t^m + a_{m-1} t^{m-1} + \dots + a_1 t + a_0$  with  $a_m \neq 0$ , the *degree* of  $f$ , denoted by  $\deg(f)$ , is  $m$ , and by convention  $\deg(0) = -\infty$ . If  $a_m = 1$ , we call  $f$  *monic*. We have  $\deg(fg) = \deg(f) + \deg(g)$  and  $\deg(f + g) \leq \max(\deg(f), \deg(g))$  for all  $f, g \in R$ . A polynomial  $f \in R$  is called *reducible* if  $f = gh$  for some  $g, h \in R$  such that  $\deg(g), \deg(h) < \deg(f)$ , otherwise we call  $f$  *irreducible*. A polynomial

$f \in R$  is called *right (resp. left) invariant* if  $fR \subseteq Rf$  (resp.  $Rf \subseteq fR$ ), i.e.  $Rf$  (resp.  $fR$ ) is a two-sided ideal of  $R$ . We call  $f$  *invariant* if it is both right and left invariant. Two skew polynomials  $f, g \in R$  are *similar*, written  $f \sim g$ , if  $R/Rf \cong R/Rg$ .

$R$  is a left principal ideal domain. The *left idealiser*  $\mathcal{I}(f) = \{g \in R : fg \in Rf\}$  of  $f \in R$  is the largest subring of  $R$  within which  $Rf$  is a two-sided ideal. We define the *eigenring* of  $f$  as  $\mathcal{E}(f) = \mathcal{I}(f)/Rf = \{g \in R : \deg(g) < m \text{ and } fg \in Rf\}$ . A nonzero  $f \in R$  is said to be *bounded* if there exists another nonzero skew polynomial  $f^* \in R$ , called a *bound* of  $f$ , such that  $Rf^*$  is the unique largest two-sided ideal of  $R$  contained in the left ideal  $Rf$ . Equivalently, a nonzero polynomial in  $f \in R$  is said to be bounded if there exists a right invariant polynomial  $f^* \in R$ , which is called a bound of  $f$ , such that  $Rf^* = \text{Ann}_R(R/Rf) \neq \{0\}$ . The annihilator  $\text{Ann}_R(R/Rf)$  of the left  $R$ -module  $R/Rf$  is a two-sided ideal of  $R$ . When  $f$  is bounded and of positive degree, the nontrivial zero divisors in the eigenspace of  $f$  are in one-to-one correspondence with proper right factors of  $f$  in  $R$ : If  $f$  is bounded and  $\sigma \in \text{Aut}(D)$ , then  $f$  is irreducible if and only if  $\mathcal{E}(f)$  has no non-trivial zero divisors. Each non-trivial zero divisor  $q$  of  $f$  in  $\mathcal{E}(f)$  gives a proper factor  $\text{gcd}(q, f)$  of  $f$  [10, Lemma 3, Proposition 4].

If  $D$  has finite dimension as an algebra over its center  $C$ , then  $R = D[t; \sigma, \delta]$  is either a twisted polynomial ring or a differential polynomial ring [13, Theorem 1.1.21].

### 1.2 Generalized A-polynomials

Unless stated otherwise, from now on let  $D$  be a unital associative division ring with center  $C$ ,  $\sigma \in \text{End}(D)$ ,  $\delta$  a left  $\sigma$ -derivation of  $D$ , and let  $F = C \cap \text{Fix}(\sigma) \cap \text{Const}(\delta)$ . We are interested in the question:

“For  $f \in R = D[t; \sigma, \delta]$  when is  $\mathcal{E}(f)$  a central simple algebra over the field  $F$ ?”

We call  $f \in R$  a *generalised A-polynomial* if  $\mathcal{E}(f)$  is a central simple algebra over  $F$ . For each  $v \in D^\times$ , we define a map  $\Omega_v : D \rightarrow D$  by  $\Omega_v(\alpha) = \sigma(v)\alpha v^{-1} + \delta(v)v^{-1}$ .

**Lemma 1.** [2, Lemma 2 for  $\sigma = \text{id}$ ] *Let  $\alpha, \beta \in D$ . Then  $(t - \alpha) \sim (t - \beta)$  in  $D[t; \sigma, \delta]$  if and only if  $\Omega_v(\alpha) = \beta$  for some  $v \in D^\times$ .*

*Proof.*  $(t - \alpha) \sim (t - \beta)$  is equivalent to the existence of  $v, w \in D^\times$  such that  $w(t - \alpha) = (t - \beta)v$  [14, pg. 33], i.e. there exists  $v, w \in D^\times$  such that  $w(t - \alpha) = \sigma(v)t + \delta(v) - \beta v$ . This is the case if and only if  $w = \sigma(v)$  and  $w\alpha = \sigma(v)\alpha + \beta v - \delta(v)$ . The result follows immediately.  $\square$

### 2 Generalised A-polynomials in $D[t; \sigma]$

Let  $D$  be a central division algebra over  $C$  of degree  $d$  and  $\sigma$  an automorphism of  $D$  of finite inner order  $n$ , with  $\sigma^n = \iota_u$  for some  $u \in D^\times$ . Let  $R = D[t; \sigma]$ . Then  $R$  has center  $F[u^{-1}t^n] \cong F[x]$ . We define the *minimal central left multiple* of  $f$  in  $R$  to be the unique polynomial of minimal degree  $h \in C(R) = F[u^{-1}t^n]$  such that  $h = gf$  for some  $g \in R$ , and such that  $h(t) = \hat{h}(u^{-1}t^n)$  for some monic  $\hat{h}(x) \in F[x]$ .

If the greatest common right divisor  $(f, t)_r$  of  $f$  and  $t$  is one, then  $f^* \in C(R)$  [10, Lemma 2.11]), and the minimal central left multiple of  $f$  equals  $f^*$  up to a scalar multiple in  $D^\times$ . For the remainder of this section we therefore assume that  $f \in R$  is a monic polynomial of degree  $m \geq 1$  such that  $(f, t)_r = 1$ . Then  $f^* \in C(R)$ . Define  $E_{\hat{h}} = F[x]/(\hat{h}(x))$ .  $E_{\hat{h}} = F[x]/(\hat{h}(x))$  is a field if and only if  $\hat{h}(x) \in F[x]$  is irreducible.

Since  $F[x]$  is a unique factorisation domain, we have

$$\hat{h}(x) = \hat{\pi}_1^{e_1}(x)\hat{\pi}_2(x)^{e_2} \cdots \hat{\pi}_z(x)^{e_z}$$

for some irreducible polynomials  $\hat{\pi}_1, \hat{\pi}_2, \dots, \hat{\pi}_z \in F[x]$  such that  $\hat{\pi}_i \neq \hat{\pi}_j$  for  $i \neq j$ , and some exponents  $e_1, e_2, \dots, e_z \in \mathbb{N}$ . Henceforth we assume that  $e_1 = e_2 = \cdots = e_z = 1$ , i.e. that  $\hat{h}$  is square-free. By the Chinese Remainder Theorem for commutative rings [9, §5]  $E_{\hat{h}} \cong E_{\hat{\pi}_1} \oplus E_{\hat{\pi}_2} \oplus \cdots \oplus E_{\hat{\pi}_z}$ , where  $E_{\hat{\pi}_i} = F[x]/(\hat{\pi}_i(x))$  for each  $i$ .  $\mathcal{E}(f)$  is a semisimple algebra over its center  $E_{\hat{h}}$  [17]. Thus  $\mathcal{E}(f)$  has center  $F$  if and only if  $z = 1$  and  $E_{\hat{\pi}_1} = F$ , i.e. if and only if  $\hat{h}$  is a degree 1 polynomial in  $F[x]$ . Hence under the global assumption that  $\hat{h}$  is square-free, we see that for  $f$  to be a generalised A-polynomial it is necessary that  $\hat{h}$  be irreducible. So assume that  $\hat{h}$  is irreducible. Then the eigenspace of  $f$  is a central simple algebra over the field  $E_{\hat{h}}$ :

**Theorem 1.** [17] *Suppose that  $\hat{h}(x)$  is irreducible in  $F[x]$ . Then  $f = f_1 f_2 \cdots f_l$  where  $f_1, f_2, \dots, f_l$  are irreducible polynomials in  $R$  such that  $f_i \sim f_j$  for all  $i, j$ . Moreover,*

$$\mathcal{E}(f) \cong M_\ell(\mathcal{E}(f_i))$$

is a central simple algebra of degree  $s = \frac{\ell dn}{k}$  over the field  $E_{\hat{h}}$  where  $k$  is the number of irreducible factors of  $h(t) \in R$ . In particular,  $\deg(\hat{h}) = \deg(h)/n = \frac{dm}{s}$  and  $[\mathcal{E}(f) : F] = mds$ .

**Theorem 2.** *Suppose that  $\hat{h}(x)$  is irreducible in  $F[x]$ . Then  $f$  is a generalised A-polynomial in  $R$  if and only if  $\hat{h}(x) = x - a$  for some  $a \in F$  if and only if  $f$  right divides  $u^{-1}t^n - a$  for some  $a \in F$ . In particular, if  $f$  is a generalised A-polynomial, then  $m \leq n$ .*

*Proof.* Suppose that  $f$  is a generalised A-polynomial in  $R$ . By the paragraph preceding Theorem 1, for  $f$  to be a generalised A-polynomial it is necessary that  $\hat{h}(x) = x - a$  for some  $a \in F$ . Conversely if  $\hat{h}(x) = x - a \in F[x]$ , then  $E_{\hat{h}} = F[x]/(x - a) = F$ . Hence  $\mathcal{E}(f)$  is a central simple algebra over  $F$  by Theorem 1, i.e.  $f$  is a generalised A-polynomial. It is easy to see that  $\hat{h}(x) = x - a$  is equivalent to  $f$  being a right divisor of  $u^{-1}t^n - a$  by definition of the minimal central left multiple. Moreover, if  $f$  right divides  $u^{-1}t^n - a$ , then  $\deg(f) \leq n$ . □

For  $n$  prime we are able to provide a more concrete description of  $f$ :

**Theorem 3.** *Suppose that  $\hat{h}(x)$  is irreducible in  $F[x]$ . Suppose that  $n$  is prime and not equal to  $d$ . Then  $f$  is a generalised A-polynomial in  $R$  if and only if one of the following holds:*

1. There exists some  $a \in F^\times$  such that  $ua \neq \prod_{j=1}^n \sigma^{n-j}(b)$  for every  $b \in D$ , and  $f(t) = t^n - ua$ . In this case  $f$  is an irreducible polynomial in  $R$ .
2.  $m \leq n$  and there exist  $c_1, c_2, \dots, c_{m-1}, b \in D^\times$ , such that

$$u^{-1} \prod_{j=0}^{n-1} \sigma^{n-j}(b) \in F^\times, \quad \text{and} \quad f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(b))(t - \Omega_1(b)).$$

*Proof.* By Theorem 2,  $f$  is a generalised A-polynomial in  $R$  if and only if  $f$  right divides  $u^{-1}t^n - a$  for some  $a \in F^\times$ . So suppose that  $f$  is a generalised A-polynomial in  $R$ , then there exists some  $a \in F^\times$  and some nonzero  $g \in R$  such that

$$u^{-1}t^n - a = gf. \tag{1}$$

In the notation of Theorem 1,  $\ell dn = ks$  and since  $f$  is a generalised A-polynomial  $\deg(\hat{h}) = \frac{dm}{s} = 1$ , i.e.  $dm = s$ . Combining these yields  $\frac{n}{k} = \frac{m}{\ell} \in \mathbb{N}$ . That is  $k$  must divide  $n$ , and so we must have that  $k = 1$  or  $k = n$  as  $n$  is prime. We analyse the cases  $k = 1$  and  $k = n$  separately.

First suppose that  $k = 1$ , then  $h(t)$  is irreducible. Therefore Equation (1) becomes  $u^{-1}t^n - a = gf(t)$  for some  $a \in F^\times$  and some  $g \in D^\times$ . This yields  $g = u^{-1}$  and  $f(t) = t^n - ua$  for some  $a \in F^\times$ . Suppose that  $f$  were reducible, then  $f$  would be the product of  $n$  linear factors as  $n$  is prime, hence  $f$  is irreducible if and only if  $ua \neq \prod_{j=1}^n \sigma^{n-j}(b)$  for any  $b \in D$ , by [7, Corollary 3.4].

On the other hand, if  $k = n$ , then  $h(t)$  is equal to a product of  $n$  linear factors in  $R$ , all of which are similar. Also, since  $\frac{n}{k} = \frac{m}{\ell}$  and  $n = k$ , we have  $m = \ell \leq n$ . Hence  $f$  is the product of  $m \leq n$  linear factors in  $R$ , all of which are similar to each other.

So there exist constants  $b_1, b_2, \dots, b_m \in D^\times$  such that  $(t - b_i) \sim (t - b_j)$  for all  $i, j \in \{1, 2, \dots, m\}$ , and  $f(t) = \prod_{i=1}^m (t - b_i)$ . In particular  $(t - b_i) \sim (t - b_m)$  for all  $i \neq m$ , which is true if and only if there exist constants  $c_1, c_2, \dots, c_{m-1}, c_m \in D^\times$  such that  $b_i = \Omega_{c_i}(b_m)$  for all  $i$  by Lemma 1. Hence setting  $b = b_m$  and  $c_m = 1$  yields  $f(t) = \prod_{i=1}^m (t - \Omega_{c_i}(b))$ . Finally, we note that  $(t - b)|_r(t^n - ua)$  for some  $a \in F^\times$  if and only if  $u^{-1} \prod_{j=0}^{n-1} \sigma^{n-j}(b) = a \in F^\times$ , by [7, Corollary 3.4]. □

If  $e_i > 1$  for at least one  $i$ , then it is not clear to the authors when  $\mathcal{E}(f)$  is a central simple algebra over the field  $F$ .

### 2.1 Generalised A-polynomials in $K[t; \sigma]$

Throughout this section we suppose that  $R = K[t; \sigma]$  with  $K$  a field, and that  $\sigma$  is an automorphism of  $K$  of finite order  $n$  with fixed field  $F$ . Now the center of  $R$  is  $F[t^n] \cong F[x]$ . Let  $f \in R$  be of degree  $m \geq 1$  and satisfy  $(f, t)_r = 1$ , and suppose that  $f$  has minimal central left multiple  $h(t) = \hat{h}(t^n)$ ,  $\hat{h} \in F[x]$  an irreducible monic polynomial. Again, we consider only those  $f \in R$  where  $\hat{h} \in F[x]$  is square-free.

**Theorem 4.**  *$f$  is a generalised  $A$ -polynomial in  $R$  if and only if  $\hat{h}(x) = x - a$  for some  $a \in F[x]$  if and only if  $f$  right divides  $t^n - a$  in  $R$ .*

This follows from Theorem 2. If  $n$  is prime, then the following is an immediate corollary to both Theorem 2 and Theorem 3:

**Corollary 1.** *Let  $n$  be prime. Then  $f$  is a generalised  $A$ -polynomial in  $R$  if and only if one of the following holds:*

1. *There exists some  $a \in F^\times$  such that  $a \neq N_{K/F}(b)$  for any  $b \in K$ , and  $f(t) = t^n - a$ . In this case  $f$  is an irreducible polynomial in  $R$ .*
2.  *$m \leq n$  and there exist some constants  $c_1, c_2, \dots, c_{m-1}, b \in K^\times$ , such that*

$$f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(b))(t - \Omega_1(b)).$$

*Proof.* The proof is identical to the proof of Theorem 3 with  $d = u = 1$ . The condition that  $\prod_{j=0}^{n-1} \sigma^j(b)$  lies in  $F^\times$  is always satisfied, since  $\prod_{j=0}^{n-1} \sigma^j(b) = N_{K/F}(b) \in F^\times$  for all  $b \neq 0$ . □

In particular, let  $K = \mathbb{F}_{q^n}$ , where  $q = p^e$  for some prime  $p$  and exponent  $e \geq 1$ , and where  $\sigma : K \rightarrow K, a \mapsto a^q$  is the Frobenius automorphism of order  $n$ , with fixed field  $F = \mathbb{F}_q$ . Here the only central division algebra over  $\mathbb{F}_q$  is  $\mathbb{F}_q$  itself. The following result is therefore an easy consequence of Theorems 1 and 2:

**Corollary 2.** *Suppose that  $f \in \mathbb{F}_{q^n}[t, \sigma]$  satisfies  $(f, t)_r = 1$ , and has minimal central left multiple  $h(t) = \hat{h}(t^n)$  for some irreducible polynomial  $\hat{h} \in \mathbb{F}_q[x]$ . Then  $f$  is an  $A$ -polynomial if and only if  $m \leq n$  and there exist some constants  $c_1, c_2, \dots, c_{m-1}, b \in \mathbb{F}_{q^n}^\times$ , such that  $f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(b))(t - \Omega_1(b))$ . In particular,  $f$  is a reducible polynomial in  $\mathbb{F}_{q^n}[t, \sigma]$ , unless  $m = 1$ .*

The result follows identically to the  $n = k$  case in the proof of Theorem 3.

### 3 Generalised $A$ -polynomials in $D[t; \delta]$

From now on let  $R = D[t; \delta]$  where  $D$  is a central division algebra of degree  $d$  over  $C$ . Assume that  $C$  has prime characteristic  $p$ , and that  $\delta$  is an algebraic derivation of  $D$  with minimum polynomial  $g(t) = t^{p^e} + \gamma_1 t^{p^{e-1}} + \dots + \gamma_e t \in F[t]$ , such that  $g(\delta)(a) = [c, a] = ca - ac$  for some nonzero  $c \in D$  and for all  $a \in D$ . Here,  $F = C \cap \text{Const}(\delta)$  ( $D = K$  is a field is included here as special case). Then  $R$  has center  $F[g(t) - c] \cong F[x]$ . For every  $f \in R$ , the *minimal central left multiple* of  $f$  in  $R$  is the unique polynomial of minimal degree  $h \in C(R) = F[x]$  such that  $h = gf$  for some  $g \in R$ , and such that  $h(t) = \hat{h}(g(t) - c)$  for some monic  $\hat{h}(x) \in F[x]$ . All  $f \in R = D[t; \delta]$  have a unique minimal central left multiple, which is a bound of  $f$ .

Again we can restrict our investigation to the case  $\hat{h}$  is square-free in  $F[x]$ , and note that it is necessary that  $\hat{h}$  be irreducible in  $F[x]$  for  $f$  to be a generalised  $A$ -polynomial in  $R$ .

**Theorem 5.** [17] Suppose that  $\hat{h}(x)$  is irreducible in  $F[x]$ . Then  $f = f_1 f_2 \cdots f_l$  where  $f_1, f_2, \dots, f_l$  are irreducible polynomials in  $R$  such that  $f_i \sim f_j$  for all  $i, j$ . Moreover,

$$\mathcal{E}(f) \cong M_\ell(\mathcal{E}(f_i))$$

is a central simple algebra of degree  $s = \frac{\ell d p^e}{k}$  over the field  $E_{\hat{h}}$  where  $k$  is the number of irreducible factors of  $h \in R$ . In particular  $\deg(\hat{h}) = \deg(h)/p^e = \frac{dm}{s}$  and  $[\mathcal{E}(f) : F] = mds$ .

We obtain the following:

**Theorem 6.** Suppose that  $\hat{h}(x)$  is irreducible in  $F[x]$ . Then  $f$  is a generalised A-polynomial in  $R$  if and only if  $f$  right divides  $g(t) - (b + c)$  for some  $b \in F$ . In particular,  $\deg(f) \leq p^e$ .

*Proof.* Suppose that  $f$  is a generalised A-polynomial in  $R$ . For  $f$  to be a generalised A-polynomial it is necessary that  $\hat{h}(x) = x - b$  for some  $b \in F$ . Conversely if  $\hat{h}(x) = x - b \in F[x]$ , then  $E_{\hat{h}} = F[x]/(x - b) = F$ . Hence  $\mathcal{E}(f)$  is a central simple algebra over  $F$  by Theorem 5, i.e.  $f$  is a generalised A-polynomial. It is easy to see that  $\hat{h}(x) = x - b$  is equivalent to  $f$  being a right divisor of  $g(t) - (b + c)$  by definition of the minimal central left multiple. Moreover, if  $f$  right divides  $g(t) - (b + c)$ , then  $\deg(f) \leq \deg(g(t) - (b + c)) = p^e$ .  $\square$

In  $D[t; \delta]$ , we have  $(t - b)^p = t^p - V_p(b)$ ,  $V_p(b) = b^p + \delta^{p-1}(b) + \nabla_b$  for all  $b \in D$ , where  $\nabla_b$  is a sum of commutators of  $b, \delta(b), \delta^2(b), \dots, \delta^{p-2}(b)$  [13, pg. 17–18]. In particular, if  $D$  is commutative, then  $\nabla_b = 0$  and  $V_p(b) = b^p + \delta^{p-1}(b)$  for all  $b \in D$ . Using the identities  $t^p = (t - b)^p + V_p(b)$  and  $t = (t - b) + b$  for all  $b \in D$ , we arrive at:

**Lemma 2.** [13, Proposition 1.3.25 (for  $e = 1$ )] Let  $f(t) = t^p - a_1 t - a_0 \in D[t; \delta]$  and  $b \in D$ . Then  $(t - b) \mid_r f(t)$  if and only if  $V_p(b) - a_1 b - a_0 = 0$ .

If  $e = 1$  (i.e.  $\delta$  is an algebraic derivation of  $D$  of degree  $p$ ), we can determine necessary and sufficient conditions for  $f$  to be an A-polynomial in  $R$ :

**Theorem 7.** Let  $\delta$  be an algebraic derivation of  $D$  of degree  $p$  with minimum polynomial  $g(t) = t^p - at$  such that  $g(\delta) = \delta_c$  for some  $c \in D$ . Suppose that  $\hat{h}(x)$  is irreducible in  $F[x]$ . Then  $f$  is a generalised A-polynomial in  $R$  if and only if one of the following holds:

1.  $f(t) = h(t) = t^p - at - (b + c)$ , and  $V_p(\alpha) - a\alpha - (b + c) \neq 0$  for all  $\alpha \in D$ . In this case  $f$  is irreducible in  $R$ .
2.  $h(t) = t^p - at - (b + c)$  for some  $a, b \in F$ ,  $m \leq p$  and

$$f(t) = \prod_{i=1}^{m-1} (t - \Omega_{c_i}(\alpha))(t - \Omega_1(\alpha))$$

for some  $c_1, c_2, \dots, c_{m-1} \alpha \in D^\times$ , such that  $V_p(\alpha) - a\alpha - (b + c) = 0$ .



*Proof.* By Theorem 6,  $f$  is a generalised A-polynomial in  $R$  if and only if  $f$  right divides  $t^p - at - (b + c)$  for some  $b \in F$ . So suppose that  $f$  is a generalised A-polynomial in  $R$ , then there exists some  $b \in F$  and some nonzero  $f' \in R$  such that

$$t^p - at - (b + c) = f'f \tag{2}$$

In the notation of Theorem 5,  $\ell dp = ks$  and since  $f$  is a generalised A-polynomial,  $\deg(\hat{h}) = \frac{dm}{s} = 1$ , i.e.  $dm = s$ . Combining these yields  $\frac{p}{k} = \frac{m}{\ell} \in \mathbb{N}$ . That is  $k$  must divide  $p$ , and so we must have that  $k = 1$  or  $k = p$  as  $p$  is prime.

First suppose that  $k = 1$ , then  $h(t)$  is irreducible in  $R$ . Therefore Equation (2) becomes  $t^p - at - (b + c) = f'f$  for some  $b \in F^\times$  and some  $f' \in D^\times$ . This yields  $f' = 1$  and  $f(t) = t^p - at - (b + c)$ . Suppose that  $f$  were reducible, then  $f$  would be the product of  $p$  linear factors as  $p$  is prime, hence  $f$  is irreducible if and only if  $V_p(\alpha) - a\alpha - (b + c) \neq 0$  for any  $\alpha \in D$ , by Lemma 2.

On the other hand, if  $k = p$ , then  $h(t)$  is equal to a product of  $p$  linear factors in  $R$ , all of which are similar to one another. Also, since  $\frac{p}{k} = \frac{m}{\ell}$  and  $p = k$ , we have  $m = \ell \leq p$ . Hence  $f$  is the product of  $m \leq p$  linear factors in  $R$ , all of which are mutually similar to each other.

So there exist constants  $\alpha_1, \alpha_2, \dots, \alpha_m \in D^\times$  such that  $f(t) = \prod_{i=1}^m (t - \alpha_i)$ , and  $(t - \alpha_i) \sim (t - \alpha_j)$  for all  $i, j \in \{1, 2, \dots, m\}$ . In particular  $(t - \alpha_i) \sim (t - \alpha_m)$  for all  $i \neq m$ , which is true if and only if there exist constants  $c_1, c_2, \dots, c_{m-1}, c_m \in D^\times$  such that  $\alpha_i = \Omega_{c_i}(\alpha_m)$  for all  $i$  by Lemma 1. Hence setting  $\alpha = \alpha_m$  and  $c_m = 1$  yields  $f(t) = \prod_{i=1}^m (t - \Omega_{c_i}(\alpha))$ . Finally, we note that  $(t - \alpha)$  right divides  $t^p - at - (b + c)$  if and only if  $V_p(\alpha) - a\alpha - (b + c) = 0$  by Lemma 2. □

**Remark 1.** Suppose on the other hand that  $C$  has characteristic 0 and  $\delta$  is the inner derivation  $\delta_c$ . Then  $R$  has center  $C[t - c] \cong C[x]$ . i.e.  $F = C$ . In this case the A-polynomials are trivial: if  $\hat{h}(x)$  is irreducible in  $C[x]$  then  $f$  is a generalised A-polynomial in  $R$  if and only if  $f(t) = (t - c) + a$  for some  $a \in C$ . In this case,  $\mathcal{E}(f) = D$ .

## References

- [1] A.A. Albert: On nonassociative division algebras. *Transactions of the American Mathematical Society* 72 (2) (1952) 296–309.
- [2] A.S. Amitsur: Differential polynomials and division algebras. *Annals of Mathematics* (1954) 245–278.
- [3] A.S. Amitsur: Non-commutative cyclic fields. *Duke Mathematical Journal* 21 (1) (1954) 87–105.
- [4] A.S. Amitsur: Generic splitting fields of central simple algebras. *Annals of Mathematics* 62 (2) (1955) 8–43.
- [5] N. Bourbaki: *Elements of mathematics*. Springer (2003).
- [6] C. Brown, S. Pumplün: How a nonassociative algebra reflects the properties of a skew polynomial. *Glasgow Mathematical Journal* 63 (1) (2021) 6–26.

- [7] C. Brown: Petit algebras and their automorphisms. PhD Thesis, University of Nottingham. Online at arXiv:1806.00822 (2018)
- [8] J. Carcanague: Quelques résultats sur les anneaux de Ore. *CR Acad. Sci. Paris Sr. AB* 269 (1969) A749–A752.
- [9] P.M. Cohn: Noncommutative unique factorization domains. *Transactions of the American Mathematical Society* 109 (2) (1963) 313–331.
- [10] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro: Computing the bound of an Ore polynomial. Applications to factorization. *Journal of Symbolic Computation* 92 (2019) 269–297.
- [11] J. Gómez-Torrecillas: Basic module theory over non-commutative rings with computational aspects of operator algebras. With an appendix by V. Levandovskyy. In: M. Barkatou, T. Cluzeau, G. Regensburger, M. Rosenkranz: *Algebraic and Algorithmic Aspects of Differential and Integral Operators. AADIOS 2012. Lecture Notes in Computer Science*. Springer (2014) 23–82.
- [12] K. R. Goodearl, J. W. Bruce, R. B. Warfield: *An introduction to noncommutative Noetherian rings*. Cambridge University Press (2004).
- [13] N. Jacobson: *Finite-dimensional division algebras over fields*. Springer (1996).
- [14] N. Jacobson: *The theory of rings*. American Mathematical Society (1943).
- [15] J.C. McConnell, C.J. Robson, L.W. Small: *Noncommutative noetherian rings*. American Mathematical Soc. (2001).
- [16] O. Ore: Theory of non-commutative polynomials. *Annals of Mathematics* (1933) 480–508.
- [17] A. Owen: On the right nucleus of Petit algebras. PhD Thesis, University of Nottingham, in preparation.
- [18] S. Pumplün: Algebras whose right nucleus is a central simple algebra. *Journal of Pure and Applied Algebra* 222 (9) (2018) 2773–2783.

Received: 4 June 2021

Accepted for publication: 15 June 2021

Communicated by: Ivan Kaygorodov