



The Norm of a Skew Polynomial

S. Pumplün¹ · D. Thompson¹

Received: 24 June 2020 / Accepted: 23 March 2021 / Published online: 15 June 2021
© The Author(s) 2021

Abstract

Let D be a finite-dimensional division algebra over its center and $R = D[t; \sigma, \delta]$ a skew polynomial ring. Under certain assumptions on δ and σ , the ring of central quotients $D(t; \sigma, \delta) = \{f/g \mid f \in D[t; \sigma, \delta], g \in C(D[t; \sigma, \delta])\}$ of $D[t; \sigma, \delta]$ is a central simple algebra with reduced norm N . We calculate the norm $N(f)$ for some skew polynomials $f \in R$ and investigate when and how the reducibility of $N(f)$ reflects the reducibility of f .

Keywords Skew polynomial ring · Reducible skew polynomials · Norm

Mathematics Subject Classification (2010) Primary: 16S36

1 Introduction

Let A be a central simple algebra, $R = A[t; \sigma, \delta]$ and $A(t; \sigma, \delta) = \{f/g \mid f \in A[t; \sigma, \delta], g \in C(A[t; \sigma, \delta])\}$ the ring of central quotients of R . Under certain assumptions on δ and σ , $A(t; \sigma, \delta)$ is a central simple algebra with norm N . So far, this norm has been successfully used when investigating factorizations of polynomials $f \in \mathbb{F}_{q^n}[t; \sigma]$ (cf. [2, 3]): f is irreducible in $\mathbb{F}_{q^n}[t; \sigma]$ if and only if $N(f)$ is irreducible as a polynomial in $\mathbb{F}_q[x]$, with $x = t^n$ [2, Proposition 2.1.17].

The idea to compute the norm of a skew polynomial and use it to check if the polynomial is reducible or not can be employed for some families of skew polynomials in more general rings $R = D[t; \sigma, \delta]$ with D a division algebra of degree d : we show that if D has a subfield E of degree d and $R = D[t; \sigma]$ or $R = D[t; \delta]$ suitable, then $N(f) \in F[x]$ is a polynomial in a suitably chosen polynomial ring $F[x]$ for all $f \in R$, and f divides $N(f)$. This generalizes results by Jacobson [6, (1.6.12), Proposition 1.7.1 (i)], [6, (1.6.12), p. 31].

Presented by: Kenneth Goodearl

✉ D. Thompson
thompson.danjames@gmail.com

S. Pumplün
susanne.pumpluen@nottingham.ac.uk

¹ School of Mathematical Sciences, University of Nottingham, University Park, Nottingham NG7 2RD, UK

In particular, let K/F be a finite cyclic Galois extension of degree n with Galois group generated by σ . Then for all $f \in K[t; \sigma]$, we have $N(f) \in F[x]$ where $x = t^n$ and f divides $N(f)$. If f satisfies $(f, t)_r = 1$, and either f is not right-invariant and n is prime, or $\gcd(m, n) = 1$, then f is irreducible in $K[t; \sigma]$ if and only if $N(f)$ is irreducible as a polynomial in $F[x]$. This indeed holds more generally for all $f \in K[t; \sigma]$ such that $(f, t)_r = 1$ that are not right-invariant with bound f^* of degree mn .

We extend these results to the case that $R = D[t; \delta]$, where δ is an algebraic derivation, in particular we look at the case that $R = K[t; \delta]$, where K/F is a field extension in characteristic p of degree p^e and δ an algebraic derivation with constant field F . Any not right-invariant $f \in K[t; \delta]$ of degree m and with bound f^* of degree mn , is irreducible in $K[t; \delta]$ if and only if $N(f)$ is irreducible as a polynomial in some polynomial ring $F[x]$.

Furthermore, in some cases it is still true that a factorization of $N(f)$ in $F[x]$ provides a factorization of f .

This work is part of the second author’s PhD thesis [10].

2 Preliminaries

2.1 Skew Polynomial Rings

Let A be a unital associative ring, σ a ring endomorphism of A and $\delta : A \rightarrow A$ a left σ -derivation, i.e. an additive map such that $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in A$. The skew polynomial ring $R = A[t; \sigma, \delta]$ is the set of skew polynomials $g(t) = a_0 + a_1t + \dots + a_nt^n$ with $a_i \in A$, with term-wise addition and multiplication defined via $ta = \sigma(a)t + \delta(a)$ for all $a \in A$ [7]. Define $\text{Fix}(\sigma) = \{a \in A \mid \sigma(a) = a\}$ and $\text{Const}(\delta) = \{a \in A \mid \delta(a) = 0\}$. If $\delta = 0$, define $A[t; \sigma] = A[t; \sigma, 0]$. If $\sigma = id$, define $A[t; \delta] = A[t; id, \delta]$.

For $f(t) = a_0 + a_1t + \dots + a_nt^n \in R$ with $a_n \neq 0$, we define the degree of f as $\deg(f) = n$ and $\deg(0) = -\infty$. An element $f \in R$ is irreducible in R if it is not a unit and it has no proper factors, i.e. if there do not exist $g, h \in R$ with $1 \leq \deg(g), \deg(h) < \deg(f)$ such that $f = gh$ [6, p. 2 ff.].

Let D be a division algebra. Then a polynomial $f(t) \in D[t; \sigma, \delta]$ is bounded if there exists a nonzero polynomial $f^* \in D[t; \sigma, \delta]$ such that $D[t; \sigma, \delta]f^*$ is the largest two-sided ideal of $D[t; \sigma, \delta]$ contained in $D[t; \sigma, \delta]f$. The polynomial f^* is uniquely determined by f up to scalar multiplication by elements of D^\times . f^* is called the bound of f .

In this paper, D will always be a central simple division algebra of degree d over its center C .

2.2 The Minimal Central Left Multiple of $f \in D[t; \sigma]$

Let σ be an automorphism of D of finite order n modulo inner automorphisms, that means that $\sigma^n = i_u$ for some inner automorphism $i_u(z) = uz u^{-1}$. Then the order of $\sigma|_C$ is n . W.l.o.g., we choose $u \in \text{Fix}(\sigma)$. Let $R = D[t; \sigma]$ and define $F = C \cap \text{Fix}(\sigma)$. Then R has center

$$C(R) = F[u^{-1}t^n] = \left\{ \sum_{i=0}^k a_i(u^{-1}t^n)^i \mid a_i \in F \right\} = F[x]$$

[6, Theorem 1.1.22]. All polynomials $f \in R$ are bounded.

If the greatest common right divisor of f and t (denoted $(f, t)_r$) is one, then $f^* \in C(R)$ [3, Lemma 2.11]). From now on we assume that $(f, t)_r = 1$. For any $f \in R = D[t; \sigma]$

with a bound in $C(R)$, we can 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 $\hat{h}(x) \in F[x]$.

Lemma 1 *Let $f \in D[t; \sigma]$.*

- (i) *If $(f, t)_r = 1$, then the minimal central left multiple of f exists and is unique. It is equal to the bound of f up to a scalar multiple from D .*
- (ii) *If f is irreducible in R with minimal central left multiple $h(t) = \hat{h}(u^{-1}t^n)$, then $\hat{h}(x)$ is irreducible in $F[x]$.*
- (iii) *Let $(f, t)_r = 1$ and suppose that $\hat{h} \in F[x]$ is irreducible. Then $f = f_1 \cdots f_r$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all i, j .*

Proof (cf. [8])

- (i) Let f^* be a bound of f . Then f^* is unique up to scalar multiplication by elements in D^\times and Rf^* is the largest two-sided ideal of R contained in the left ideal Rf . In particular, this implies $f^* = gf$ for some $g \in R$. The assumption that $(f, t)_r = 1$ implies that $f^* \in C(R)$ [3, Lemma 2.11] thus f^* is the unique minimal central left multiple of f , up to some scalar.
- (ii) Since f is irreducible, obviously $(f, t)_r = 1$. Let $h(t) = \hat{h}(u^{-1}t^n)$ be the minimal central left multiple of f . Suppose \hat{h} is reducible in $F[x]$; that is, $\hat{h}(x) = \hat{h}_1(x)\hat{h}_2(x)$ for some $\hat{h}_i(x) \in F[x]$, such that $0 < \deg(\hat{h}_i) < \deg(\hat{h})$ for $i = 1, 2$. If f divides $h_1(t) = \hat{h}_1(u^{-1}t^n)$ on the right, this contradicts the minimality of h . Moreover, as f is irreducible the greatest common right divisor of f and h_1 is 1. As R is a right Euclidean domain, there exist $p, q \in R$ such that $pf + qh_1 = 1$. Multiplying everything on the right by $h_2(t) = \hat{h}_2(u^{-1}t^n)$, we obtain $pfh_2 + qh = h_2$. As f is a right divisor of h by definition, $h = rf$ for some $r \in R$. Noting that $h_2(t) \in C(R)$, this yields

$$h_2 = ph_2f + qrf = (ph_2 + qr)f.$$

Thus h_2 is a central left multiple of f of degree strictly less than h contradicting the minimality of h . Thus $\hat{h}(x)$ must be irreducible in $F[x]$.

- (iii) If $\hat{h} \in F[x]$ is irreducible then h is a two-sided maximal element in R , hence the irreducible factors h_i of any factorization $h = h_1 \cdots h_k$ of h in R are all similar. Now $h(t) = p(t)f(t)$ for some $p(t) \in R$ and so comparing the irreducible factors of f and h and employing [6, Theorem 1.2.9], we see that $f = f_1 \cdots f_r$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all i, j and $r \leq k$. □

The above results apply in particular to the special case that D is a field and $\sigma \in \text{Aut}(K)$ has order n . Then $R = K[t; \sigma]$ has center

$$C(R) = F[t^n] = \left\{ \sum_{i=0}^k a_i (t^n)^i \mid a_i \in F \right\} = F[x]$$

where $F = \text{Fix}(\sigma)$ [6, Theorem 1.1.22].

2.3 The Minimal Central Left Multiple of $f \in D[t; \delta]$

Let $R = D[t; \delta]$ where C is a field of characteristic p (we allow $D = C$). Moreover, we assume that δ is a derivation of D , such that $\delta|_C$ is algebraic with minimum polynomial

$$g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \dots + c_e t \in F[t]$$

of degree p^e , where $F = \text{Const}(\delta) \cap C$. Then $g(\delta) = id_{d_0}$ is an inner derivation of D . W.l.o.g. we choose $d_0 \in \text{Const}(\delta)$, so that $\delta(d_0) = 0$ [6, Lemma 1.5.3]. Then R has center

$$C(D[t; \delta]) = F[x] = \left\{ \sum_{i=0}^k a_i (g(t) - d_0)^i \mid a_i \in F \right\}$$

with $x = g(t) - d_0$. The two-sided $f \in D[t; \delta]$ are of the form $f(t) = uc(t)$ with $u \in D$ and $c(t) \in C(R)$ [6, Theorem 1.1.32]. All polynomials $f \in R$ are bounded.

For every $f \in R = D[t; \sigma]$ we define the *minimal central left multiple of f in R* to be the unique polynomial of minimal degree $h \in C(R) = F[x]$ such that $h = gf$ for some $g \in R$, and such that $h(t) = \hat{h}(g(t) - d_0)$ for some monic $\hat{h}(x) \in F[x]$:

Lemma 2 *Let $f \in R = D[t; \delta]$.*

- (i) *The minimal central left multiple of f exists and is unique. It is equal to f^* up to a scalar multiple in D^\times .*
- (ii) *If f is irreducible in R with minimal central left multiple $h(t) = \hat{h}(g(t) - d_0)$, then $\hat{h}(x)$ is irreducible in $F[x]$.*
- (iii) *Suppose that $\hat{h} \in F[x]$ is irreducible. Then $f = f_1 \cdots f_r$ for irreducible $f_i \in R$ such that $f_i \sim f_j$ for all i, j .*

Proof (cf. [8])

(i) Let f^* be a bound of f . Then f^* is unique up to scalar multiplication by elements in D^\times and Rf^* is the largest two-sided ideal of R contained in the left ideal Rf . Since f^* is two-sided, we know that $f^*(t) = dc(t)$ for some $c(t) \in C(R)$ and $d \in D^\times$. So assume w.l.o.g. that $f^* \in C(R)$. The rest of the proof is identical to the one of Lemma 1.

The proofs of (ii), (iii) are identical to the one of Lemma 1 (ii), (iii). □

2.4 The Algebra $(A(x), \tilde{\sigma}, ux)$

Let C/F be a finite cyclic field extension of degree n with $\text{Gal}(C/F) = \langle \sigma \rangle$. Let A be a central simple algebra of degree d with center C and suppose that σ extends to a C -algebra automorphism of A that we also will call σ . Then there exists an element $u \in A^\times$ such that $\sigma^n = i_u$ and $\sigma(u) = u$. These two relations determine u up to multiplication with elements from F^\times [9, Lemma 19.7]. Let $R = A[t; \sigma]$ and

$$A(t; \sigma) = \{f/g \mid f \in A[t; \sigma], g \in C(A[t; \sigma])\}$$

be the ring of central quotients of $A[t; \sigma]$. Then $x = u^{-1}t^n$ is a commutative indeterminate over A . The centers of $A[t; \sigma]$ and $A(t; \sigma)$ are $C(A[t; \sigma]) = F[x] = F[u^{-1}t^n]$ and

$$C(A(t; \sigma)) = \text{Quot}(C(A[t; \sigma])) = F(x),$$

where $\text{Quot}(S)$ denotes the quotient field of an integral domain S . Note that $C(A(t; \sigma))$ is a field. The ring $A(x)$ of central quotients of $A[x]$ is a subring of $A(t; \sigma)$.

$A(t; \sigma)$ is a central simple $F(x)$ -algebra, more precisely,

$$A(t; \sigma) \cong (A(x), \tilde{\sigma}, ux)$$

is a cyclic generalized crossed product [4, Theorem 2.3]. Here, $\tilde{\sigma}$ denotes the extension of σ to $A(x)$ that fixes x [4, Lemma 2.1.].

Note that when regarding $A(t; \sigma)$ as an $F(x)$ -algebra, the choice of u is lost: x depends on u , and different choices of u lead to different actions of $F(x)$ on $A(t; \sigma)$. Here and in the following we thus assume that u is fixed and $x = u^{-1}t^n$.

The algebra $A(t; \sigma)$ has center $F(x)$ and $\text{deg}A(t; \sigma) = dn$. The reduced norm N of $(A(x), \tilde{\sigma}, ux)$ is a nondegenerate form of degree dn over $F(x)$. In particular, if A is a division algebra then $A(t; \sigma)$ is a division algebra [4, Theorem 2.2.].

If A contains a strictly maximal subfield that is Galois over F with Galois group G , then $A(t; \sigma)$ is a crossed product with group G . If A is a symbol algebra over a global field F , then $A(t; \sigma)$ is a crossed product. If A is a p -algebra over a global field F , then $A(t; \sigma)$ is a cyclic crossed product [4, Corollary 2.4.].

2.5 The Algebra $(D(x), \tilde{\delta}, d_0 + x)$

Let $R = D[t; \delta]$ and

$$D(t; \delta) = \{f/g \mid f \in D[t; \sigma], g \in C(D[t; \delta])\}$$

the ring of central quotients of $D[t; \delta]$. Then the center of $D(t; \delta)$ is the field

$$C(D(t; \delta)) = \text{Quot}(C(D[t; \delta])) = F(x)$$

with $x = g(t) - d_0$. The ring of central quotients $D(x)$ of $D[x]$ is a subring of $D(t; \delta)$. Let $\tilde{\delta}$ denote the extension of δ to $D(x)$ such that $\tilde{\delta} = id_t|_{D(x)}$. Then $\tilde{\delta}|_{C(x)}$ is algebraic with minimum polynomial $g(t)$, and $D(t; \delta)$ is the central simple $F(x)$ -algebra

$$D(t; \delta) \cong (D(x), \tilde{\delta}, d_0 + x),$$

i.e. a generalized differential algebra of degree $p^e d$ [6, p. 23]. Let N be its reduced norm. Then N has degree $p^e d$. Moreover, $(D(x), \tilde{\delta}, d_0 + x)$ contains $D(x)$ as the centralizer of $C(x)$ [5, Theorem 3.1], and is free of rank p^e as a left $D(x)$ -module.

2.6 The Algebra $(K(x), \tilde{\delta}, x)$

Let K be a field of characteristic p and δ a derivation on K that is algebraic with $F = \text{Const}(\delta)$. Let $g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \dots + c_e t$ be the minimum polynomial of δ . Then K/F is a purely inseparable extension of exponent one, and $K^p \subset F$. More precisely, $K = F(u_1, \dots, u_e) = F(u_1) \otimes_F \dots \otimes_F F(u_e)$, $u_i^p = c_i \in F$, and $[K : F] = p^e$. Let $R = K[t; \delta]$ then $C(R) = F[x]$ with $x = g(t) - d_0$, $d_0 \in F$. Assume w.l.o.g. that $d_0 = 0$.

Let $\tilde{\delta}$ be the extension of δ to $K(x)$ such that $\tilde{\delta} = id_t|_{K(x)}$, then $\tilde{\delta}|_{F(x)}$ is algebraic with minimum polynomial $g(t)$. The algebra $K(t; \delta) \cong (K(x), \tilde{\delta}, x)$ is a generalized differential algebra of degree p^e over $F(x)$ [6, p. 23]. Let N be its reduced norm. N has degree p^e .

3 Using the Norm of $(K(x), \tilde{\sigma}, x)$

We start with the special case that $A = C$ in Section 2.4 (with some small changes in our notation): Let K/F be a cyclic field extension of degree n with $\text{Gal}(K/F) = \langle \sigma \rangle$,

$R = K[t; \sigma]$ and $x = t^n$. Let N be the reduced norm of the cyclic algebra $(K(x), \tilde{\sigma}, x)$ over $F(x)$ (cf. also [6, Proposition 1.4.6]). We have $\tilde{\sigma}|_K = \sigma$, and N is a nondegenerate form of degree n .

Caruso and Le Borgne [2] use $N(f)$ successfully to factorize skew polynomials $f \in \mathbb{F}_q[t, \sigma]$ over finite fields. For certain $f \in K[t, \sigma]$, the norm N of $(K(x), \tilde{\sigma}, x)$ can also be used to obtain a reducibility criterium:

For all $f \in R$, $N(f) \in F[x]$ and f divides $N(f)$ in R , more precisely, $N(f) = f(t)^\sharp f(t) = f(t)f(t)^\sharp$ and $f(t)^\sharp \in R$ [6, (1.6.12), Proposition 1.7.1 (i)]. Moreover, we have:

Theorem 3 *Let $f(t) = a_0 + a_1t + \dots + a_mt^m$ have degree m . Then*

$$N(f(t)) = N_{K/F}(a_0) + \dots + (-1)^{m(n-1)} N_{K/F}(a_m)x^m.$$

This is the generalized and corrected version of [6, Proposition 1.7.1 (ii)], which stated $(-1)^{mn} N_{K/F}(a_m)x^m$ for the leading term, and also required $m < n$. Furthermore, our proof fixes a small mistake in the proof of [2, Lemma 2.1.15].

Proof Write $f(t) = a_0 + a_1t + \dots + a_mt^m$ as

$$f(t) = P_0(x) + P_1(x)t + \dots + P_{n-1}(x)t^{n-1}$$

with $P_i(x) \in K[x]$. We can use verbatim the same proof as given in [2, Lemma 2.1.15] to obtain the matrix in $M_n(K[x])$ representing the left multiplication $\rho(f(t))$ with respect to the basis $1, t, \dots, t^{n-1}$: we have

$$\rho(f(t)) = \begin{pmatrix} P_0 & t^n \sigma(P_{n-1}) & \dots & & t^n \sigma^{n-1}(P_1) \\ P_1 & \sigma(P_0) & \dots & & \\ \vdots & & \ddots & & \vdots \\ & & & \ddots & \\ \vdots & & & & \ddots & t^n \sigma^{n-1}(P_{n-1}) \\ P_{n-1} & \dots & \dots & \dots & \sigma^{n-1}(P_0) \end{pmatrix}.$$

Thus $N(f(t))$, which is the determinant of this matrix, has as constant term the constant term of $P_0(x)\sigma(P_0(x)) \dots \sigma^{n-1}(P_0(x))$, which is $a_0(x)\sigma(a_0(x)) \dots \sigma^{n-1}(a_0(x)) = N_{K/F}(a_0)$. There are unique integers $k, r, 0 \leq r \leq n - 1$, such that we can write m as $m = kn + r$. In the sum giving the determinant of this matrix, the term of highest degree is

$$(-1)^{m(n-1)} P_i(x)\sigma(P_i(x)) \dots \sigma^{n-i-1}(P_i(x))t^n \sigma^{n-i}(P_i(x)) \dots \sigma^{n-1}(P_i(x)).$$

It has degree $m = k(n - i) + (k + 1)i = kn + i$ as polynomial in x . (The proof of [2, Lemma 2.1.15] forgot to include the factor $(-1)^{m(n-1)}$ here.) Therefore $N(f(t))$ has as highest term the highest term of this sum. The highest term is thus given by $(-1)^{m(n-1)} a_m \sigma(a_m) \dots \sigma^{n-1}(a_m) = (-1)^{m(n-1)} N_{K/F}(a_m)$. □

Let f^* be the bound of $f \in R$. Since $N(f) \in F[x]$ is a left multiple of f that lies in $C(R)$, the bound f^* of f divides $N(f)$ in R , thus $\deg(f^*) \leq \deg(N(f))$. If $(f, t)_r = 1$ then $f^* \in C(R)$, that means f^* is up to some scalar $\alpha \in K^\times$ equal to the minimal central left multiple h of f , where as before we write $h(t) = \hat{h}(t^n)$ with $\hat{h}(x) \in F[x]$.

Remark 4 In [3, Theorem 2.9, Corollary 2.12], it was proved that $\deg(f^*) \leq n \cdot \deg(f)$. We recover this result as a byproduct of the above observation that f^* divides $N(f)$ in R , knowing that $\deg(N(f)) = n \cdot \deg(f)$ in R by Theorem 3. If $\deg(f) = m$ and $\deg(f^*) = mn$ in R , it follows immediately comparing degrees that $N(f)$ is the bound of f .

Lemma 5 *Let $f \in R$. If $N(f)$ is irreducible in $F[x]$, then f is irreducible in R .*

Proof Suppose towards a contradiction that $f = gp$ for $g, p \in R$ then $N(f) = N(g)N(p)$ is reducible in $F[x]$, since both $N(g)$ and $N(p)$ lie in $F[x]$, which immediately yields the assertion. □

Theorem 6 *Let $f(t) \in R$ be a polynomial of degree m such that $(f, t)_r = 1$. Suppose that $\deg(\hat{h}) = m$ (this is always the case if, for instance, either n is prime or $\gcd(m, n) = 1$).*

- (i) *If \hat{h} is irreducible in $F[x]$ then f is irreducible in R .*
- (ii) *If f is irreducible then $N(f)$ is irreducible in $F[x]$.*

Proof Let $h \in R$ be the minimal central left multiple of f in R with $\deg(h) = nm$. We know that $N(f)$ is a two-sided multiple of f in R , therefore the bound f^* of f must divide $N(f)$ in R . Since we assume $(f, t)_r = 1$, we know that $f^* \in C(R)$ and therefore f^* equals h up to some invertible factor in F . Thus $h(t) = \hat{h}(t^n)$ must divide $N(f)$ in R . Write $N(f) = g(t)h(t)$ for some $g \in R$. By Theorem 3 we have $\deg(N(f)) = mn$ in R . Comparing degrees in R we obtain $\deg N(f) = \deg(g(t)) + mn = mn$, which implies $\deg(g) = 0$, i.e. $g(t) = a \in K^\times$. This implies that $N(f) = ah(t) = a\hat{h}(t^n)$.

- (i) If \hat{h} is irreducible in $F[x]$ then $N(f)$ is irreducible in $F[x]$ (Lemma 5), thus f is irreducible in R .
- (ii) If f is irreducible then \hat{h} is irreducible in $F[x]$ and so again $N(f)$ is irreducible in $F[x]$. □

Corollary 7 *Let $f \in R$ be a monic polynomial of degree m . Suppose that $(f, t)_r = 1$ and that $\deg(\hat{h}) = m$.*

- (i) *If $N(f(t)) = \hat{h}_1 \cdots \hat{h}_l$ such that $\hat{h}_i \in F[x]$ is irreducible, $1 \leq i \leq l$, then there exists a decomposition $f = f_1 \cdots f_l$ of f into irreducible factors, such that $N(f_i) = \hat{h}_i$ for all i , $1 \leq i \leq l$. The degree of f_i in R equals the degree of \hat{h}_i in $F[x]$ for all i .*
- (ii) *Assume that $N(f)$ is the product of l distinct irreducible factors $\hat{h}_1 \cdots \hat{h}_l$ in $F[x]$. Then f has exactly $l!$ irreducible decompositions corresponding to each possible ordering of the factors of $N(f)$.*

Proof (i) Let $N(f) = \hat{h}_1 \cdots \hat{h}_l$ with $\hat{h}_i \in F[x]$ irreducible for all i , $1 \leq i \leq l$.

Since $N(f) = af^*$ with $a \in F^\times$ because of our assumption that $\deg(\hat{h}) = m$ and knowing that $\deg(N(f)) = m$ by Theorem 3, we conclude that there is a “rough factorization” of f given by $f = g_1 \cdots g_l$ where each g_i has minimal central left multiple \hat{h}_i [3, Proposition 5.2]. Thus $N(f) = N(g_1) \cdots N(g_l) = \hat{h}_1 \cdots \hat{h}_l$ in the commutative polynomial ring $F[x]$. $F[x]$ is a unique factorization domain and the l polynomials \hat{h}_i are all irreducible in $F[x]$. Hence we can conclude that the l factors $N(g_i)$ on the left-hand side must all be irreducible as well.

Thus there is a permutation π such that $N(g_{\pi(i)}) = \hat{h}_i$ for all i . Since \hat{h}_i is the minimal central left multiple of g_i and thus divides $N(g_i)$, we can conclude that $\pi = id$.

Moreover, if $\text{deg}(g_i) = m_i$ then $\text{deg}(N(g_i)) = \text{deg}(\hat{h}_i) = m_i$ in $F[x]$, so the degrees of all the \hat{h}_i in $F[x]$ determine the degrees of the g_i . Since $(f, t)_r = 1$, also $(g_i, t)_r = 1$ for all i . By Lemma 5, we conclude that the g_i must be irreducible for all i . Denote them by f_i to conform with our previous notation.

- (ii) Assume that $N(f)$ is the product of l distinct irreducible factors. Then f is a product of l irreducible factors by (i), containing exactly one each whose reduced norm is \hat{h}_i for each irreducible \hat{h}_i in $F[x]$. Therefore f has exactly $l!$ different irreducible decompositions corresponding to each possible ordering of the distinct factors \hat{h}_i of $N(f)$. □

4 Using the Norm of the Twisted Function Field $A(t; \sigma)$

Let A be a central simple algebra of degree d with center C and $R = A[t; \sigma]$, where σ is an automorphism of A of finite order n modulo inner automorphisms, i.e. $\sigma^n = i_u$, such that $\sigma|_C \in \text{Aut}_F(C)$ has order n . Let N be the reduced norm of $(A(x), \tilde{\sigma}, ut)$.

Proposition 8 *Let $f(t) = a_0 + a_1t + \dots + a_mt^m \in C[t; \sigma] \subset R$, and suppose A has a subfield E of degree d . Then*

$$\begin{aligned} N(f(t)) &= (N_{C/F}(a_0) + \dots + (-1)^{m(n-1)}N_{C/F}(a_m)x^m)^d \\ &= N_{E/F}(a_0) + \dots + (-1)^{dm(n-1)}N_{E/F}(a_m)x^{dm}. \end{aligned}$$

Proof $\tilde{C} = (C(x)/F(x), \tilde{\sigma}|_{C(x)}, ut) = (C(x)/F(x), \tilde{\sigma}|_{C(x)}, t)$ is a subalgebra of $(A(x), \tilde{\sigma}, ut)$ of degree n over $F(x)$. Note that $\sigma|_C \in \text{Aut}_F(C)$ by our global assumption on σ at the beginning of this section. In particular, this means $\tilde{\sigma}|_{C(x)} \in \text{Aut}(C(x))$. Thus

$$N(f(t)) = (N_{\tilde{C}/F(x)}(f(t)))^d$$

for all $f(t) \in C[t; \sigma]$ by [9, Proposition. p.304]. This yields the assertions: $N_{\tilde{C}/F(x)}(f(t)) = N_{C/F}(a_0) + \dots + (-1)^{m(n-1)}N_{C/F}(a_m)x^m$ by Proposition 3 and $N_{C/F}(a_0)^d = N_{E/F}(a_0)$, $N_{C/F}(a_m)^d = N_{E/F}(a_m)$. □

Theorem 9 *Let A have a subfield E of degree d . Let $f \in A[t; \sigma]$.*

- (i) $N(f) \in F[x]$,
- (ii) f divides $N(f)$.

The proof works similarly as the one of [6, Proposition 1.7.1]:

Proof (i) We have $[C : F] = n$, $[A(x) : F(x)] = d^2n$, and $[(A(x), \tilde{\sigma}, ut) : F(x)] = d^2n^2$. The set $\{1, t, \dots, t^{n-1}\}$ generates $A[t; \sigma]$ over $A[x]$. $(A(x), \tilde{\sigma}, ut)$ is a central simple algebra of degree dn over $F(x)$ with subalgebra $A(x)$. We regard $(A(x), \tilde{\sigma}, ut)$ as a left module over its noncommutative subalgebra $A(x)$. Since $C[A[t; \sigma]] = F[x] \subset A[x]$, the set $\{1, t, \dots, t^{n-1}\}$ also generates $A(t; \sigma)$ over $A(x)$. Furthermore, we have $I_t|_{K(x)} = \sigma$, where σ denotes the extension of σ to $K(x)$ fixing x , and $A(x) \subset C_{A(t; \sigma)}(K(x))$. [4, Lemma 1.27] therefore shows that $\{1, t, \dots, t^{n-1}\}$ is free over $A(x)$, thus

$$A(t; \sigma) = \bigoplus_{i=0}^{n-1} A(x)t^i.$$

Since

$$A[t; \sigma] = \bigoplus_{i=0}^{n-1} A[x]t^i,$$

and $t^n = ux$, every $f \in R \subset (A(x), \tilde{\sigma}, ut)$ can be written as a linear combination of $1, t, \dots, t^{n-1}$ with coefficients in $A[x]$. We therefore obtain a representation ρ of $(A(x), \tilde{\sigma}, ut)$ by matrices in $M_n(A(x))$ by writing

$$t^i f(t) = \sum_{j=0}^{n-1} \rho_{ij}(f(t))t^j$$

for all $f \in R \subset (A(x), \tilde{\sigma}, ut)$ and $0 \leq i, j \leq n - 1$. Hence the matrix $\rho(f(t))$ has entries in $A[x]$ for every $f \in R$. Since A has a subfield E of degree d , we can regard A as a left module over E . Let $\{v_1, \dots, v_d\}$ be a basis for A over $E(x)$. Then $\{v_1, \dots, v_d, v_1t, \dots, v_d t, \dots, v_d t^{n-1}\}$ is a basis of $(A(x), \tilde{\sigma}, ut) = A(t; \sigma)$ as a left module over E and we now analogously obtain a representation ρ of $(A(x), \tilde{\sigma}, ut)$ by matrices in $M_{dn}(E(x))$ with respect to that basis.

For $f(t) \in R$, the matrix $\rho(f(t))$ has entries in $E[x]$, therefore it follows that

$$N(f(t)) = \det(\rho(f(t))) \in E[x] \cap F(x) = F[x].$$

(ii) Similarly as in (i), it can be shown that all the coefficients of the characteristic polynomial of $\rho(f(t))$ are contained in $F[x]$ (cf. also [9, Proposition, p. 295]) and thus $f(t)^\sharp \in R$ by [6, (1.6.12)]. Since $N(f(t)) = f(t)f(t)^\sharp = f(t)^\sharp f(t)$, it follows that $f(t)$ divides $N(f)$ in R . □

Let $f \in R = A[t; \sigma]$ have degree m and bound f^* . Observe that since $N(f) \in F[x] = C(R)$ is a left multiple of f by Lemma 9, f^* divides $N(f)$ in R , so that $\deg(f^*) \leq \deg(N(f))$, as also shown in [3, Theorem 2.9, Corollary 2.12].

The next result further generalizes [6, Proposition 1.7.1], i.e. Theorem 3.

Theorem 10 *Let $A = D$ be a division algebra which has a subfield E of degree d . Then for any $f \in D[t; \sigma]$ of degree m , $N(f)$ has degree dm .*

Proof Write $m = kn + r$ for some $0 \leq r < n$. Substituting $t^n = ux$, we obtain $f(t) = P_0(x) + P_1(x)t + \dots + P_{n-1}(x)t^{n-1} \in D[x][t; \sigma]$ where

$$P_i(x) = \begin{cases} a_i + \dots + a_{i+kn}(ux)^k & \text{for } i \leq r, \\ a_i + \dots + a_{i+(k-1)n}(ux)^{k-1} & \text{for } i > r. \end{cases}$$

Computing the left regular representation of $\rho : D[t; \sigma] \rightarrow M_n(D(x))$, we have

$$\rho(f(t)) = \begin{pmatrix} Q_{1,1}(x) & \dots & Q_{1,n}(x) \\ \vdots & & \vdots \\ Q_{n,1}(x) & \dots & Q_{n,n}(x) \end{pmatrix}$$

for some $Q_{i,j}(x) \in D[x]$ satisfying

$$t^{i-1} f = \sum_{j=1}^n Q_{ij}(x)t^{j-1}, \quad 1 \leq i \leq n,$$

[6, Proposition 1.6.9]. Moreover, it follows that

$$\deg(Q_{i,j}) = \begin{cases} \deg(P_{j-i}) & \text{for } i \leq j, \\ \deg(P_{n+j-i}) + 1 & \text{for } i > j. \end{cases}$$

Comparing the above equation with the expressions for $P_i(x)$, it follows that

$$\deg(Q_{i,j}) \leq \begin{cases} k - 1 & \text{for } i \leq j \text{ and } j - i > r, \\ k & \text{for } i \leq j \leq r + i \text{ or } j < i < n - r + j, \\ k + 1 & \text{for } i > j \text{ and } i - j \geq n - r. \end{cases}$$

with $Q_{i,j}(x) = \sigma^{i-1}(a_m)u^k x^k + \dots$ for $j - i = r$ and $Q_{i,j}(x) = \sigma^{i-1}(a_m)u^{k+1}x^{k+1} + \dots$ for $i - j = n - r$.

This means the bottom left $r \times r$ minor of $\rho(f(t))$ has elements of degree at most $k + 1$ in lower triangular entries (including the diagonal which attains this maximum degree) and the top right $n - r \times n - r$ minor of $\rho(f(t))$ has elements of degree at most $k - 1$ in the upper triangular entries (excluding the diagonal which has elements of exactly degree k). Every other element of $\rho(f(t))$ has degree at most k .

As D has a subfield of degree d , there exists a left regular representation $\omega : D \rightarrow M_d(E)$ which extends to $D[x]$ by setting $\omega(x) = xId$. The $d \times d$ block matrices representing $Q_{i,j}(x)$ are inserted for every entry $Q_{i,j}(x)$ in $\rho(f(t))$ to obtain a representation for $D[t; \sigma]$ in $M_{dn}(E[x])$.

As ω is additive and $\omega(x)$ is a diagonal matrix, $\omega(\sigma^j(g(x))) = \omega(\sigma^j(g_k)u^k)(xId)^k + \dots + \omega(\sigma^j(g_0))$ for any polynomial $g(x) = \sum_{i=0}^k g_i x^i \in D[x]$. As we are computing the determinant only to find the degree of $N(f(t))$, it is sufficient to only consider the term of highest degree in $Q_{i,j}(x)$ and ignore all terms of lower degree. We truncate $Q_{i,j}(x)$ at the highest term and apply ω to all the entries of the matrix. To determine the term of highest degree, we expand the determinant along the columns and consider only the portion of the determinant expansion which yields the maximum possible degree. As $\omega(a_m u^k) = \omega(a_m)\omega(u)^k$ is invertible, there are no zero columns in $\omega(a_m u^k)$ so it is always possible to find an expansion of the matrix yielding the highest degree. Hence the degree of $N(f(t))$ is at most $dr(k + 1) + d(n - r)k = d(kn + r) = dm$. We wish to show the coefficient of x^{dm} in $N(f(t))$ is non-zero: following a suitable expansion of $\omega \circ \rho(f(t))$ the coefficient of x^{dm} is equal to

$$\pm \det(\omega(a_m u^k)) \det(\omega(\sigma(a_m u^k))) \dots \det(\omega(\sigma^{n-r-1}(a_m u^k))) \det(\omega(\sigma^{n-r}(a_m u^{k+1}))) \dots \det(\omega(\sigma^{n-1}(a_m u^{k+1}))).$$

As σ is an automorphism, $\det(\omega(\sigma^i(a_m u^k))) \neq 0$ by our assumption on $\omega(a_m u^k)$. Thus the coefficient of x^{dm} is non-zero and $\deg(N(f(t))) = dm$. □

Example 11 We show the details of the above calculations for $d = 2, n = 3$ and $m = 7$; an actual computation of the matrix becomes difficult for any d, n, m . For $f(t) = a_0 + a_1 t + \dots + a_7 t^7 \in D[t; \sigma]$, where we assume D has a subfield E of degree d , and $t^3 = ux$, we obtain

$$\rho(f(t)) = \begin{pmatrix} a_0 + a_3 ux + a_6 u^2 x^2 & a_1 + a_4 ux + a_7 u^2 x^2 & a_2 + a_5 ux \\ \sigma(a_2 ux + a_5 u^2 x^2) & \sigma(a_0 + a_3 ux + a_6 u^2 x^2) & \sigma(a_1 + a_4 ux + a_7 u^2 x^2) \\ \sigma^2(a_1 ux + a_4 u^2 x^2 + a_7 u^3 x^3) & \sigma^2(a_2 ux + a_5 u^2 x^2) & \sigma^2(a_0 + a_3 ux + a_6 u^2 x^2) \end{pmatrix}.$$

Truncate the polynomials in the matrix at their highest terms and apply $\omega : D \rightarrow M_2(E)$ to get

$$\begin{pmatrix} \omega(a_6u^2x^2) & \omega(a_7u^2x^2) & \omega(a_5ux) \\ \omega(\sigma(a_5u^2)x^2) & \omega(\sigma(a_6u^2)x^2) & \omega(\sigma(a_7u^2)x^2) \\ \omega(\sigma^2(a_7u^3)x^3) & \omega(\sigma^2(a_5u^2)x^2) & \omega(\sigma^2(a_6u^2)x^2) \end{pmatrix} \\ = \begin{pmatrix} a_{1,1}^{(1,1)}x^2 & a_{1,1}^{(1,2)}x^2 & a_{1,1}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,1}^{(2,1)}x^2 & a_{1,1}^{(2,2)}x^2 & a_{1,1}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,1}^{(1,1)}x^2 & a_{2,1}^{(1,2)}x^2 & a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,1}^{(2,1)}x^2 & a_{2,1}^{(2,2)}x^2 & a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \\ a_{3,1}^{(1,1)}x^3 & a_{3,1}^{(1,2)}x^3 & a_{3,2}^{(1,1)}x^2 & a_{3,2}^{(1,2)}x^2 & a_{3,3}^{(1,1)}x^2 & a_{3,3}^{(1,2)}x^2 \\ a_{3,1}^{(2,1)}x^3 & a_{3,1}^{(2,2)}x^3 & a_{3,2}^{(2,1)}x^2 & a_{3,2}^{(2,2)}x^2 & a_{3,3}^{(2,1)}x^2 & a_{3,3}^{(2,2)}x^2 \end{pmatrix},$$

for some $a_{k,l}^{(i,j)} \in E$ for $i, j \in \{1, 2\}$ and $k, l \in \{1, 2, 3\}$. Then the determinant of the above matrix is equal to

$$\begin{aligned} & a_{3,1}^{(1,1)}x^3 \begin{vmatrix} a_{1,1}^{(1,2)}x^2 & a_{1,1}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,1}^{(2,2)}x^2 & a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,1}^{(1,2)}x^2 & a_{2,1}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,1}^{(2,2)}x^2 & a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \\ a_{3,1}^{(2,2)}x^3 & a_{3,2}^{(2,1)}x^2 & a_{3,2}^{(2,2)}x^2 & a_{3,3}^{(2,1)}x^2 & a_{3,3}^{(2,2)}x^2 \end{vmatrix} - a_{3,1}^{(2,1)}x^3 \begin{vmatrix} a_{1,2}^{(1,2)}x^2 & a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,2}^{(2,2)}x^2 & a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,2)}x^2 & a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,2)}x^2 & a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \\ a_{3,1}^{(1,2)}x^3 & a_{3,2}^{(1,1)}x^2 & a_{3,2}^{(1,2)}x^2 & a_{3,3}^{(1,1)}x^2 & a_{3,3}^{(1,2)}x^2 \end{vmatrix} + \dots \\ & = a_{3,1}^{(1,1)}a_{3,1}^{(2,2)}x^6 \begin{vmatrix} a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \end{vmatrix} - a_{3,1}^{(2,1)}a_{3,1}^{(1,2)}x^6 \begin{vmatrix} a_{1,1}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,1}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \end{vmatrix} + \dots \\ & = (a_{3,1}^{(1,1)}a_{3,1}^{(2,2)} - a_{3,1}^{(2,1)}a_{3,1}^{(1,2)})x^6 \begin{vmatrix} a_{1,2}^{(1,1)}x^2 & a_{1,2}^{(1,2)}x^2 & a_{1,3}^{(1,1)}x & a_{1,3}^{(1,2)}x \\ a_{1,2}^{(2,1)}x^2 & a_{1,2}^{(2,2)}x^2 & a_{1,3}^{(2,1)}x & a_{1,3}^{(2,2)}x \\ a_{2,2}^{(1,1)}x^2 & a_{2,2}^{(1,2)}x^2 & a_{2,3}^{(1,1)}x^2 & a_{2,3}^{(1,2)}x^2 \\ a_{2,2}^{(2,1)}x^2 & a_{2,2}^{(2,2)}x^2 & a_{2,3}^{(2,1)}x^2 & a_{2,3}^{(2,2)}x^2 \end{vmatrix} + \dots \end{aligned}$$

Comparing this to the matrix in terms of ω , this is equal to

$$\det(\omega(\sigma^2(a_7u^3))x^6 \begin{vmatrix} \omega(a_7u^2x^2) & \omega(a_5ux) \\ \omega(\sigma(a_6u^2)x^2) & \omega(\sigma(a_7u^2)x^2) \end{vmatrix} + \dots$$

Repeating this with the remaining block matrices, this yields

$$N(f(t)) = \det(\omega(\sigma^2(a_7u^3))\det(\omega(\sigma(a_7u^2))\det(\omega(a_7u^2))x^{14} + \text{terms of lower degree.}$$

From now on, we assume that

$$A = (E/C, \gamma, a) \text{ is a cyclic algebra over } C \text{ of degree } d,$$

$$\sigma|_E \in \text{Aut}(E) \text{ such that } \gamma \circ \sigma = \sigma \circ \gamma \text{ and } u \in E.$$

Then $\sigma|_E$ has order n . Write $m = kn + r$ for some $0 \leq r < n$.

Theorem 12 For $f(t) = a_0 + a_1t + \dots + a_mt^m \in E[t; \sigma] \subset A[t; \sigma]$, we have

$$N(f(t)) = N_{E/F}(a_0) + \dots + (-1)^{dr(n-1)} N_{E/F}(a_m) N_{E/C}(u)^r x^{dm}.$$

Proof The proof is similar to the proof of Theorem 10. Using the same notation as in that proof, the entries $Q_{i,j}(x) \in D[x]$ of $\rho(f(t))$ are determined by the relation $t^{i-1}f = \sum_{j=1}^n Q_{ij}(x)t^{j-1}$, $1 \leq i \leq n$, and

$$\rho(f(t)) = \begin{pmatrix} P_0(x) & P_1(x) & \cdots & P_{n-1}(x) \\ \sigma(P_{n-1}(x))ux & \sigma(P_0(x)) & \cdots & \sigma(P_{n-2}(x)) \\ \vdots & \ddots & & \vdots \\ \sigma^{n-m}(P_r(x))ux & & \ddots & \sigma^{n-m}(P_{r-1}(x)) \\ \vdots & & \ddots & \vdots \\ \sigma^{n-1}(P_1(x))ux & \sigma^{n-1}(P_2(x))ux & \cdots & \sigma^{n-1}(P_0(x)) \end{pmatrix},$$

where $P_i(x) \in E[x]$ for all i . Let $\{v_1, \dots, v_d\}$ be a canonical basis for A as a left E -module. Then $\{v_1, \dots, v_d, v_1t, \dots, v_dt, \dots, v_d t^{n-1}\}$ is a basis of $(A(x), \tilde{\sigma}, ut)$ as a left module over $E(x)$ and we now analogously obtain a representation ρ of $(A(x), \tilde{\sigma}, ut)$ by matrices in $M_{dn}(E(x))$ with respect to that basis. This representation is given by an $nd \times nd$ matrix obtained as follows:

Let ω be the representation of A in $M_d(E)$ which is extended to a representation of $A[x]$ in $M_d(E[x])$ by setting $\omega(x) = xI_d$. The $d \times d$ block matrices representing the entries of $\rho(f(t))$ are inserted for every entry of the previous $n \times n$ matrix (cf. for instance [9, p. 298]) with σ extended to $M_d(E)$ by acting entry-wise. For all $a \in E$, the matrix $\omega(a) \in M_d(E)$ is a $d \times d$ diagonal matrix given by

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & \gamma(a) & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \cdots & \gamma^{d-1}(a) \end{pmatrix}.$$

As a consequence, we note that $\omega(a_i x) = \omega(a_i)\omega(x) = \omega(a_i)(xI_d)$ and $\omega(a_i a_j) = \omega(a_i)\omega(a_j)$ for all $a_i, a_j \in E$. Thus we have

$$\omega \circ \rho(f(t)) = \begin{pmatrix} \omega(P_0(x)) & \omega(P_1(x)) & \cdots & \omega(P_{n-1}(x)) \\ \omega(\sigma(P_{n-1}(x))\omega(u)xId & \omega(\sigma(P_0(x))) & \cdots & \omega(P_{n-2}(x)) \\ \vdots & \ddots & & \vdots \\ \omega(\sigma^{n-m}(P_r(x))\omega(u)xId & & \ddots & \omega(\sigma^{n-m}(P_{r-1}(x))) \\ \vdots & & \ddots & \vdots \\ \omega(\sigma^{n-1}(P_1(x))\omega(u)xId & \omega(\sigma^{n-1}(P_2(x))\omega(u)xId & \cdots & \omega(\sigma^{n-1}(P_0(x))) \end{pmatrix}$$

where $\omega \circ \rho(f(t))$ is a $dn \times dn$ matrix in $M_{dn}(E[x])$.

As the $\omega(\sigma^j(P_i(x)))$ are pairwise commutative matrices, we may calculate the determinant of $\omega \circ \rho(f(t))$ by first evaluating the $n \times n$ determinant with entries in $M_d(E)$, then evaluating the resulting $d \times d$ matrix which has entries in E [1, Lemma 1, p. 546]. Thus we obtain $\det(\omega \circ \rho(f(t))) = \det(H)$, where

$$H = \omega(P_0(x))\sigma(\omega(P_0(x))) \cdots \sigma^{n-1}(\omega(P_0(x))) + \dots + (-1)^{r(n-r)}\omega(P_r(x))\sigma(\omega(P_r(x))) \cdots \sigma^n(\omega(P_r(x)))\omega(u)^r(xI_d)^r.$$

As each $\omega(P_i(x))$ is a diagonal matrix in $M_d(E)$ for all $0 \leq i \leq n - 1$, H is the diagonal matrix in $M_d(E)$ given by the entries

$$H_{ii} = \gamma^{i-1}[P_0(x)\sigma(P_0(x)) \dots \sigma^{n-1}(P_0(x)) + \dots + (-1)^{r(n-1)}P_r(x)\sigma(P_r(x)) \dots \sigma^{n-1}(P_r(x))u^r]x^r.$$

Hence

$$\det(H) = \prod_{i=1}^d \gamma^{i-1}[P_0(x)\sigma(P_0(x)) \dots \sigma^{n-1}(P_0(x)) + \dots + (-1)^{m(n-1)}P_r(x)\sigma(P_r(x)) \dots \sigma^{n-1}(P_r(x))u^r x^r].$$

We obtain the constant term of $N(f(t))$ by substituting $x = 0$. Thus the constant term equals

$$\prod_{i=1}^d \gamma^{i-1}(a_0\sigma(a_0) \dots \sigma^{n-1}(a_0)) = \prod_{i=1}^n \sigma^{i-1}(a_0\gamma(a_0) \dots \gamma^{d-1}(a_0)),$$

since γ commutes with σ . As $a_0 \in E$, this is equal to $\prod_{i=1}^n \sigma^{i-1}(N_{E/C}(a_0)) = N_{C/F}(N_{E/C}(a_0)) = N_{E/F}(a_0)$. Similarly, the leading term of $N(f(t))$ is given by the leading term of

$$\prod_{i=1}^d \gamma^{i-1}[(-1)^{r(n-1)}P_r(x)\sigma(P_r(x)) \dots \sigma^{n-1}(P_r(x))u^r x^r],$$

which is given by

$$\begin{aligned} & \prod_{i=1}^d \gamma^{i-1}[(-1)^{r(n-1)}a_m\sigma(a_m) \dots \sigma^{n-1}(a_m)u^r x^{kn} x^r] \\ &= (-1)^{dm_0(n-1)} \left[\prod_{i=1}^d \gamma^{i-1}(a_m\sigma(a_m) \dots \sigma^{n-1}(a_m)) \right] N_{E/C}(u)^{m_0} x^{d(kn+m_0)} \end{aligned}$$

since $u \in E$. As σ and γ commute and $a_m \in E$, we can express this as

$$\begin{aligned} & (-1)^{dm_0(n-1)} \left[\prod_{i=1}^n \sigma^{i-1}(a_m\gamma(a_m) \dots \gamma^{d-1}(a_m)) \right] N_{E/C}(u)^{m_0} x^{d(kn+m_0)} \\ &= (-1)^{dr(n-1)} \left[\prod_{i=1}^n \sigma^{i-1}(N_{E/C}(a_m)) \right] N_{E/C}(u)^{m_0} x^{d(kn+m_0)} \\ &= (-1)^{dm_0(n-1)} N_{C/F}(N_{E/C}(a_m)) N_{E/C}(u)^r x^{d(kn+r)}. \end{aligned}$$

As $d(kn + r) = dm$, this implies the assertion. □

If $(f, t)_r = 1$ then $f^* \in C(R)$, that means f^* is up to some scalar $\alpha \in D^\times$ equal to the minimal central left multiple h of f , where $h(t) = \hat{h}(u^{-1}t^n)$ with $\hat{h}(x) \in F[x]$. Analogously as Lemma 5 we obtain:

Lemma 13 *Let $f \in R = A[t; \sigma]$, where A has a subfield E of degree d . If $N(f)$ is irreducible in $F[x]$, then f is irreducible in R .*

Theorem 14 *Let $A = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d such that $\sigma|_E \in \text{Aut}(E)$, $u \in E$, and $\gamma \circ \sigma = \sigma \circ \gamma$. Let $f \in R$ be a polynomial such that $(f, t)_r = 1$. Suppose that $\text{deg}(\hat{h}) = dm$.*

- (i) *If \hat{h} is irreducible in $F[x]$ then f is irreducible in R .*
- (ii) *If f is irreducible then $N(f)$ is irreducible in $F[x]$.*

Proof $N(f)$ is a two-sided multiple of f in R , therefore the bound f^* of f must divide $N(f)$ in R . Since $(f, t)_r = 1$, we know that $f^* \in C(R)$ and therefore f^* equals h up to some invertible factor in F . Thus $h(t) = \hat{h}(u^{-1}t^n)$ must divide $N(f)$ in R . Write $N(f) = g(t)h(t)$ for some $g \in R$. By Theorem 12 we have $\text{deg}(N(f)) = dmn$ in R . Comparing degrees in R we obtain $\text{deg}N(f) = \text{deg}(g(t)) + dmn = dmn$, which implies $\text{deg}(g) = 0$, i.e. $g(t) = a \in A^\times$. This gives $N(f) = ah(t) = a\hat{h}(u^{-1}t^n)$.

- (i) If \hat{h} is irreducible in $F[x]$ then $N(f)$ is irreducible in $F[x]$ (Lemma 13), thus f is irreducible in R .
- (ii) If f is irreducible then \hat{h} is irreducible in $F[x]$ (Lemma 1), and so again $N(f)$ is irreducible in $F[x]$. □

We can therefore again determine the similarity classes of irreducible polynomials appearing in a factorization of certain f , and show that any order is possible for the appearance of these similarity classes:

Corollary 15 *Let $A = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d such that $\sigma|_E \in \text{Aut}(E)$, $u \in E$, and $\gamma \circ \sigma = \sigma \circ \gamma$. Let $f \in A[t; \sigma]$ be a monic polynomial, such that $(f, t)_r = 1$ and that $\text{deg}(\hat{h}) = dm$.*

- (i) *If $N(f(t)) = \hat{h}_1 \cdots \hat{h}_l$ such that $\hat{h}_i \in F[x]$ is irreducible, $1 \leq i \leq l$, then there exists a irreducible decomposition $f = f_1 \cdots f_l$ of f into irreducible factors f_i , such that $N(f_i) = \hat{h}_i$ for all i , $1 \leq i \leq l$. Moreover, $\text{deg}(f_i) = \text{deg}(N(f_i))/d$.*
- (ii) *Assume that $N(f)$ is the product of l distinct irreducible factors $\hat{h}_1 \cdots \hat{h}_l$ in $F[x]$. Then f has exactly $l!$ factorizations into irreducible factors corresponding to each possible ordering of the factors of $N(f)$.*

The proof is analogous to the one of Corollary 7.

Corollaries 7 (i) and 15 (i) generalize [2, Lemma 2.1.18] which uses a different method of proof.

Theorem 16 *Let $A = (E/C, \gamma, a)$ be a cyclic algebra over C of degree d , and $f(t) = a_0 + a_1t + \cdots + a_mt^m \in C[t; \sigma] \subset R$ be a polynomial of degree m , such that $(f, t)_r = 1$ and $\text{deg}(\hat{h}) = dm$. Then f is reducible in R and has at least d irreducible factors.*

Proof By Proposition 8,

$$N(f(t)) = (N_{C/F}(a_0) + \cdots + (-1)^{m(n-1)}N_{C/F}(a_m)x^m)^d$$

is clearly reducible in $F[x]$. Since $\text{deg}(\hat{h}) = dm$, f is reducible in R . The at least d irreducible divisors $\hat{g}_1, \dots, \hat{g}_l$ of $N(f(t))$ correspond to a decomposition $f = f_1 \cdots f_l$ of f into irreducible factors, such that $N(f_i) = \hat{g}_j$ for some suitable j , for all i , $1 \leq i \leq l$. The degree of f_i in R equals the degree of \hat{g}_j in $F[x]$ for a suitable j . □

Note that if σ is an inner automorphism (i.e. $n = 1$ and so $R = D[t]$ by a change of indeterminants), d is prime and f not right-invariant, then any f of degree m will satisfy $\deg(\hat{h}) = dm$.

More generally, we also have by [9, Proposition, p. 304]:

Proposition 17 *Let $A = (E/C, \gamma, a)$ be a cyclic algebra. Let B be a central simple algebra over $K(x)$ that is a subalgebra of $(A(x), \sigma, ut)$ and assume that $K(x)/F(x)$ is a finite field extension. Then every $f(t) \in A[t; \sigma] \cap B$ with $\deg(h) = dmn$ is reducible.*

Proof Let $K(x)/F(x)$ be a finite field extension of degree c and B be a central simple algebra over $K(x)$ of degree b . For all $f(t) \in B \cap A[t; \sigma]$ we have $N(f(t)) = N_{K(x)/F(x)}(N_{B/K(x)}(f(t)))^e$ for a suitable integer e with $d = bce$ [9, Proposition, p. 304]. Thus $N(f)$ is reducible and hence so is f , since we assumed that $\deg(h) = dmn$. □

5 The Norm Condition for Differential Polynomials in Characteristic p

5.1 The Case that $R = K[t; \delta]$

We use the notation from Section 2.6: let F be a field of characteristic p and K/F be a field extension which is purely inseparable of exponent one. Let δ be a derivation on K that is algebraic with $\text{Const}(\delta) = F$, and $g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \dots + c_e t \in F[t]$ the minimum polynomial of δ . Let $R = K[t; \delta]$ and $C(R) = F[x]$, where $x = g(t)$. Let N be the norm of $(K(x), \tilde{\delta}, x)$.

Theorem 18 (i) *For all $f \in R$ we have $N(f) \in F[x]$ and f divides $N(f)$.*

(ii) *If $f(t) = a_0 + a_1 t + \dots + a_m t^m \in R = K[t; \delta]$ has degree m , then*

$$N(f(t)) = (-1)^{m(p^e-1)} a_m^{p^e} x^m + \dots$$

Part (i) of this proof follows by an analogous argument to Theorem 9. More precisely, actually $N(f) = f(t)^\sharp f(t) = f(t)f(t)^\sharp$ and $f(t)^\sharp \in R$, cf. [6, (1.6.12) and p. 31].

Part (ii) follows similarly to Theorem 3. This generalizes and refines [6, p. 31], which states that for $f(t) = a_0 + a_1 t + \dots + a_m t^m \in R$ we have $N(f(t)) = \pm a_m^{p^e} x^m + \dots$, if $m < p^e$, where the omitted terms are of lower degree than m in x (no proof was given).

To find the constant term of $N(f)$ in Theorem 18 is difficult, let us look at one example:

Example 19 Let $p^e = 5$, $f(t) = t^4 + a$ for some $a \in K^\times$, and $g(t) = t^5 + t$. Computing $\rho(f(t))$ yields

$$\begin{pmatrix} a & 0 & 0 & 0 & 1 \\ \delta(a) + x & a - 1 & 0 & 0 & 0 \\ \delta^2(a) & 2\delta(a) + x & a - 1 & 0 & 0 \\ \delta^3(a) & 3\delta^2(a) & 3\delta(a) + x & a - 1 & 0 \\ \delta^4(a) & 4\delta^3(a) & 6\delta^2(a) & 4\delta(a) + x & a - 1 \end{pmatrix}.$$

Setting $x = 0$ and taking the determinant of $\rho(f(t))$ shows that the constant term of $N(f(t))$ is

$$\begin{aligned}
 & a^5 - 4a^4 + a^3[6 + \delta^4(a)] - a^2[4 + 3\delta^4(a) + 8\delta(a)\delta^3(a) + 6\delta^2(a)^2] \\
 & + a[1 + 3\delta^4(a) + 12\delta^2(a)^2 + 16\delta(a)\delta^3(a) + 36\delta(a)^2\delta^2(a)] \\
 & - [\delta^4(a_0) + 8\delta(a)\delta^3(a) + 6\delta^2(a)^2 + 36\delta(a)^2\delta^2(a) + 24\delta(a)^4].
 \end{aligned}$$

It is possible to compute special cases though:

Proposition 20 For $f(t) = g(t) + a$ for some $a \in K$,

$$N(f(t)) = (x + a)^{p^e}.$$

Proof Following the proof of Theorem 18, we substitute $x = g(t)$ so $f(t) = x + a \in K[x][t; \delta]$. Computing the left regular representation $\rho : K[t; \sigma] \rightarrow M_{p^e}(K[x])$, it follows that $\rho(f(t))$ is a lower triangular matrix where each diagonal entry is equal to $x + a$. As the determinant of a triangular matrix is the product of its diagonal entries, the result follows. □

Since $N(f) \in F[x] = C(R)$, f^* divides $N(f)$ in $F[x]$. Thus $\deg(f^*) \leq p^e \cdot \deg(f)$, because the degree of $N(f)$ as a polynomial in R is $m \cdot p^e$ by Theorem 18 (ii). In particular, if $\deg(f^*) = m$ in $F[x]$, comparing degrees in $F[x]$ shows that $N(f)$ is the bound of f .

The bound f^* is up to some scalar $\alpha \in K^\times$ equal to the minimal central left multiple h of f , where as before we write $h(t) = \hat{h}(g(t))$ with $\hat{h}(x) \in F[x]$ monic.

Lemma 21 Let $f \in R$. If $N(f)$ is irreducible in $F[x]$, then f is irreducible in R .

The proof is identical to the one of Lemma 13.

Theorem 22 Let $f \in R$ be a polynomial of degree m . Suppose that $\deg(\hat{h}) = m$.

- (i) If \hat{h} is irreducible in $F[x]$ then f is irreducible in R .
- (ii) If f is irreducible then $N(f)$ is irreducible in $F[x]$.

The proof is identical to the one of Theorem 14, using Theorem 18, Proposition 2 and Lemma 21.

Corollary 23 Let $f \in R$ be a monic polynomial of degree m . Suppose that $\deg(\hat{h}) = m$.

- (i) If $N(f(t)) = \hat{h}_1 \cdots \hat{h}_l$ such that $\hat{h}_i \in F[x]$ is irreducible, $1 \leq i \leq l$, then there exists a decomposition $f = f_1 \cdots f_l$ of f into irreducible factors, such that $N(f_i) = \hat{h}_i$ for all i , $1 \leq i \leq l$. The degree of f_i in R equals the degree of \hat{h}_i in $F[x]$ for all i .
- (ii) Assume that $N(f)$ is the product of l distinct irreducible factors $\hat{h}_1 \cdots \hat{h}_l$ in $F[x]$. Then f has exactly $l!$ irreducible decompositions corresponding to each possible ordering of the factors of $N(f)$.

The proof is identical to the one of Corollary 7, using Theorem 18 and Lemma 21.

5.2 The Case that $R = D[t; \delta]$

Let C be a field of characteristic p and D a central division algebra over C of degree d . Let δ be a derivation of D , such that $\delta|_C$ is algebraic with minimum polynomial $g(t) = t^{p^e} + c_1 t^{p^{e-1}} + \dots + c_e t \in F[t]$ of degree p^e , where $F = \text{Const}(\delta) \cap C$. Write $g(t) = t^{p^e} + g_0(t)$. Then $g(\delta) = id_{d_0}$ is an inner derivation of D and w.l.o.g. we choose $d_0 \in \text{Const}(\delta)$ so that $\delta(d_0) = 0$. $R = D[t; \delta]$ has center $C(R) = F[x] = F[(t^{p^e} + g_0(t) + d_0)]$.

Let N be the reduced norm of $D(t; \delta) \cong (D(x), \tilde{\delta}, d_0 + x)$ of degree $p^e d$ [6, p. 23].

Proposition 24 *Let $f(t) = a_0 + a_1 t + \dots + a_m t^m \in C[t; \delta] \subset R$, then*

$$N(f(t)) = ((-1)^{m(p^e-1)} a_m^{p^e} x^m + \dots)^d.$$

Proof $\tilde{C} = (C(x), \tilde{\delta}|_{C(x)}, d_0 + x) \cong (C(x), \tilde{\delta}, x)$ is a subalgebra of degree p^e of $(D(x), \tilde{\delta}, d_0 + x)$ over $F(x)$. Note that $\tilde{\delta}|_{C(x)} : C(x) \rightarrow C(x)$ is well-defined: since $\delta|_C$ is an algebraic derivation on C by our assumption, we can canonically extend it to get the algebraic derivation $\tilde{\delta}|_{C(x)} : C(x) \rightarrow C(x)$. Thus

$$N(f(t)) = (N_{\tilde{C}/F(x)}(f(t)))^d$$

for all $f(t) \in C[t; \sigma]$ by [9, Proposition. p. 304]. This yields the assertion. □

Theorem 25 *Let D have a subfield E of degree d .*

- (i) *For all $f \in R$ we have $N(f) \in F[x]$.*
- (ii) *f divides $N(f)$.*

Proof (i) The set $\{1, t, \dots, t^{p^e-1}\}$ generates $D[t; \delta]$ over $D[x]$. The algebra $(D(x), \tilde{\delta}, d_0 + x)$ is central simple of degree $p^e d$ over $F(x)$ with subalgebra $D(x)$. We regard $(D(x), \tilde{\delta}, d_0 + x)$ as a left module over $D(x)$. Since $C(D[t; \delta]) = F[x] \subset D[x]$, the set $\{1, t, \dots, t^{n-1}\}$ also generates $D(t; \delta)$ as a left $D(x)$ -module, and hence is a basis. Since

$$D[t; \delta] = \bigoplus_{i=0}^{p^e-1} D[x]t^i,$$

and by substituting $x = g(t) = t^{p^e} + g_0(t)$, every $f \in R \subset (D(x), \tilde{\delta}, d_0 + x)$ can be written as a polynomial $1, t, \dots, t^{p^e-1}$ with coefficients in $D[x]$. We therefore obtain a representation ρ of $(D(x), \tilde{\delta}, d_0 + x)$ by matrices in $M_{p^e}(D(x))$ by writing

$$t^i f(t) = \sum_{j=0}^{n-1} \rho_{ij}(f(t))t^j$$

for all $f \in R \subset (A(x), \tilde{\delta}, d_0 + x)$ and $0 \leq i \leq n - 1$, where $\rho_{ij}(f(t))$ is the (i, j) th entry of $\rho(f(t))$. The matrix $\rho(f(t))$ then has entries in $D[x]$ for every $f \in R$.

Let $\{v_1, \dots, v_d\}$ be a canonical basis of D as a left E -module. Then the set $\{v_1, \dots, v_d, v_1 t, \dots, v_d t, \dots, v_d t^{p^e-1}\}$ is a basis of $(D(x), \tilde{\delta}, d_0 + x)$ as a left module over $E(x)$. We can therefore analogously obtain a representation ρ of $(D(x), \tilde{\delta}, d_0 + x)$ by matrices in $M_{dp^e}(E(x))$ with respect to that basis. For $f(t) \in R$, the matrix $\rho(f(t))$

has entries in $E[x]$, therefore it follows that $N(f(t)) = \det(\rho(f(t))) \in E[x] \cap F(x) = F[x]$.

- (ii) Similarly as in (i) (and similar to [9, Proposition, p. 295]), it can be shown that all the coefficients of the characteristic polynomial of $\rho(f(t))$ are contained in $F[x]$ and thus $f(t)^\sharp \in R$ by [6, (1.6.12)]. Since $N(f(t)) = f(t)f(t)^\sharp = f(t)^\sharp f(t)$, it follows that $f(t)$ divides $N(f)$ in R . □

Theorem 26 *Let D have a subfield E of degree d and let $\omega : D \rightarrow M_d(E)$ be the left regular representation of D . Then for any $f \in R$ of degree m ,*

$$N(f) = \pm \det(\omega(a_m))^{p^e} x^{dm} + \dots$$

In particular, $N(f)$ has degree dm .

The proof follows analogously to the proof of Theorem 10.

Corollary 27 *Let $D = (E, \delta_0, a)$ be a differential algebra, $\delta|_E$ be a derivation on E , and let $f \in D[t; \delta]$ have coefficients in E and be monic. Then $N(f(t)) = \pm x^{dm} + \dots$*

Proof Through direct computations of the left regular representation of D , we see that for each $a \in E$, $\omega(a)$ is a lower triangular matrix with each entry on the lead diagonal equal to a . Hence the result follows analogously to Theorem 26. □

Since $N(f) \in F[x] = C(R)$, the bound f^* of f divides $N(f)$ in $F[x]$, so that if $\deg(f^*) = dm$ in $F[x]$, it follows again immediately that $N(f)$ is the bound of f .

Lemma 28 *Let $f \in R$. If $N(f)$ is irreducible in $F[x]$, then f is irreducible in R .*

Theorem 29 *Let $f \in R$ be a polynomial of degree m . Suppose that $\deg(\hat{h}) = dm$.*

- (i) *If \hat{h} is irreducible in $F[x]$ then f is irreducible in R .*
- (ii) *If f is irreducible then $N(f)$ is irreducible in $F[x]$.*

Corollary 30 *Let $f \in R$ be a monic polynomial of degree m . Suppose that $\deg(\hat{h}) = dm$.*

- (i) *If $N(f(t)) = \hat{h}_1 \cdots \hat{h}_l$ such that $\hat{h}_i \in F[x]$ is irreducible, $1 \leq i \leq l$, then there exists a decomposition $f = f_1 \cdots f_l$ of f into irreducible factors, such that $N(f_i) = \hat{h}_i$ for all i , $1 \leq i \leq l$. The degree of f_i in R equals the degree of \hat{h}_i in $F[x]$ for all i .*
- (ii) *Assume that $N(f)$ is the product of l distinct irreducible factors $\hat{h}_1 \cdots \hat{h}_l$ in $F[x]$. Then f has exactly $l!$ irreducible decompositions corresponding to each possible ordering of the factors of $N(f)$.*

The proofs of the above results are identical to the ones of Lemmata 13, 21, Theorem 14 and Corollary 23.

Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Bourbaki: Elements Of mathematics, Hermann (1974)
2. Caruso, X., Le Borgne, J.: A new faster algorithm for factoring skew polynomials over finite fields. *J. Symbolic Comput.* **79**(2), 411–443 (2017)
3. Gómez-Torrecillas, J., Lobillo, F.J., Navarro, G.: Computing the bound of an Ore polynomial. *App. Factor. J. Symbolic Comput.* **92**, 269–297 (2019)
4. Hanke, T.: A direct approach to noncrossed product division algebras. Dissertation, Univ. Potsdam, Naturwissenschaftliche Fakultät. Online at arXiv:1109.1580v1[math.RA] (2011)
5. Hochsmann, K.: Simple algebras and derivations. *Trans. Amer. Math. Soc.* **108**, 1–12 (1963)
6. Jacobson, N.: Finite-dimensional division algebras over fields. Springer Verlag, Berlin-Heidelberg-New York (1996)
7. Ore, O.: Theory of noncommutative polynomials. *Annals. of Math.* **34**(3), 480–508 (1933)
8. Owen, A.: On the right nucleus of Petit algebras. PhD Thesis, University of Nottingham, in preparation
9. Pierce, R.S.: Associative Algebras. Springer-Verlag, New York (1982)
10. Thompson, D., New classes of nonassociative division algebras and MRD codes. PhD Thesis, University of Nottingham, in preparation

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.