Finite Fields and Their Applications 37 (2016) 1–13

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Exponents of skew polynomials

Ahmed Cherchem [a], André Leroy [b,*]

[a] USTHB, Faculté de Mathématiques, BP 32 El Alia, Bab Ezzouar, Algiers, Algeria
[b] Université d'Artois, Faculté Jean Perrin, Rue Jean Souvraz 62 307, Lens, France

ARTICLE INFO

Article history:
Received 16 March 2015
Received in revised form 18 August 2015
Accepted 20 August 2015
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
16S36
11T55
12Y05
11T71

Keywords:
Skew polynomial rings
Finite fields
Period of polynomials

ABSTRACT

We introduce the notion of a relative exponent for two elements in a finite ring and apply this to define and study the exponent of a polynomial in an Ore extension of the form $\mathbb{F}_q[t;\theta]$. This generalizes the classical notion of exponent (a.k.a. order or period) of a polynomial with coefficients in a finite field. The classical connections between the exponent of a polynomial, the order of its roots and of its companion matrix are obtained via the study of a notion of skew order of an element in a finite group.

1. Introduction

Let $f(x) \in \mathbb{F}_q[x]$ such that $f(0) \neq 0$. It is well known (cf. p. 75 [7]) that there exists a positive integer $e = e(f)$ such that $f(x)$ divides $x^e - 1$. The least such e is the exponent of $f(x)$ (a.k.a. order or period of $f(x)$). This definition is very important for the study of polynomials over finite fields and in coding theory. We will generalize it to a

* Corresponding author.
E-mail addresses: ahmedcherchem@gmail.com (A. Cherchem), andre.leroy@univ-artois.fr (A. Leroy).

http://dx.doi.org/10.1016/j.ffa.2015.08.004
1071-5797/

setting that will encapsulate the case of polynomials in general Ore extensions over finite rings. Applications in (non-necessarily commutative) coding theory will be developed in a future paper. In the case of automorphism type Ore extensions the situation is somewhat similar to what it is in the classical case. We make use of the fact that in the polynomial ring $R = A[t;\sigma]$, where σ is an automorphism of the ring A, the polynomial t is invariant i.e., $Rt = tR$. In a general Ore extension $A[t;\sigma,\delta]$ the polynomial t is no longer invariant but since A is finite, there will often exist an invariant polynomial that can play its role. This leads us to define and study, in Section 2, the relative exponent of two elements of a ring in a quite general setting. Section 3 is essentially devoted to the study of exponents of polynomials in $\mathbb{F}_q[t;\theta]$. This ring has been shown to be useful in different contexts and in particular in coding theory (see [1–3,8]).

2. Relative exponents in general finite rings

Lemma 2.1. *Let R be a ring with 1 and $f, g \in R$ be such that $fg \in Rf$. Let $r_g : R/Rf \to R/Rf$ the right multiplication by g. Consider the following statements:*

(i) the map r_g is one-to-one;
(ii) for any $h \in R$, if $hg \in Rf$ then $h \in Rf$;
(iii) there exists a positive integer e such that $f^e - 1 \in Rg$;
(iv) the map r_g is onto;
(v) $Rg + Rf = R$.

Then:

a) we always have (i)$\Leftrightarrow$(ii) and (iii)$\Rightarrow$(iv)$\Leftrightarrow$(v);
b) if $|R/Rg| < \infty$ and f is not a zero divisor and is such that $fR = Rf$ we also have (ii)$\Rightarrow$(iii);
c) if conditions b) are satisfied and moreover $|R/Rf| < \infty$, then the statements (i) to (v) are equivalent.

Proof. a) and c) are left to the reader. We prove only part b). Since $|R/Rg| < \infty$, the cosets $f^i + Rg$, for $i \geq 1$, cannot be all distinct, then there exist integers $0 < l < s$ such that $f^l(1 - f^{s-l}) \in Rg$ and hence there exists $h \in R$ such that $f^l(1 - f^{s-l}) = hg \in Rf$. Statement (ii) and the fact that $Rf = fR$ ensure that there exist $q_1, q_1' \in R$ such that $h = q_1 f = f q_1'$. Since f is not a zero divisor we have $f^{l-1}(1-f^{s-l}) = q_1' g \in Rf$. Repeating this argument leads to the existence of $q_2', q_3', \ldots, q_l' \in R$ such that $f^{l-i}(1 - f^{s-l}) = q_i' g$, for $2 \leq i \leq l$. In particular, we have $1 - f^{s-l} = q_l' g \in Rg$. □

The above Lemma 2.1 leads to the definition (a) hereafter. In the second definition we briefly recall the notion of an Ore extension.

Definitions 2.1.

(a) For $f, g \in R$ the right exponent of g relative to f is the smallest strictly positive integer $e = e_r(g, f)$, when it exists, such that $f^e - 1 \in Rg$ i.e., g is a right divisor of $f^e - 1$. Similarly we can define the notion of left exponent of g relative to f.
(b) Let A be a ring, $\sigma \in Aut(A)$ and $\delta \in End(R, +)$ be a σ-derivation of A. The skew polynomial ring (a.k.a. Ore extension) $R = A[t; \sigma, \delta]$ consists of polynomials written as $\sum a_i t^i \in R$ and equipped with the usual addition while the multiplication is based on the following "rule of commutation": $ta = \sigma(a)t + \delta(a)$. We will mainly be concerned with the case when A is a finite ring and $\delta = 0$.
(c) If $\mathbb{F}_q$ is a finite field with $q = p^l$ for some prime p and positive integer l, we denote by θ the Frobenius map defined by $\theta(a) = a^p$ for all $a \in \mathbb{F}_q$. The ring $\mathbb{F}_q[t; \theta]$ will be referred to as an Ore–Frobenius ring.

Examples 2.1. Let $q = p^n$, p a prime.

1) Let $R = \mathbb{F}_q[x]$, $f(x) = x$, $g(x) \in R$ such that $g(0) \neq 0$ (so that condition (i) of the lemma is satisfied). Then $e_r(g, x)$ always exists and is the classical exponent of g (cf. p. 75 [7]).
2) Let $R = \mathbb{F}_q[t; \theta]$, where θ is the Frobenius automorphism, $f(t) = t$ and $g(t) \in R$ with nonzero constant term. Then $e_r(g, f = t)$ is the exponent that will be studied in Section 3. There, we present the ring $\mathbb{F}_q[t; \theta]$ and concrete ways of computing this exponent.
3) More generally than the previous example, we can consider a finite ring A, an automorphism $\sigma \in Aut(A)$ and $f(t) = t \in R = A[t; \sigma]$. If $g(t) \in R$ is such that its constant term is invertible then $Rg + Rt = R$ and all the conditions of the lemma will be satisfied. This example will be useful in the next section while considering the embedding of the Frobenius–Ore extension in a ring of the form $M_n(\mathbb{F}_q)[t; \theta]$.
4) Let $A = \mathbb{F}_q[x]/(x^p)$, $R = A[t; \frac{d}{dx}]$, $f = t^p$, $g = g(t)$, monic, with $Rg + Rt^p = R$. Since for $a \in A$ and $m \in \mathbb{N}$ we have $t^m a = \sum_{i=0}^{m} \binom{m}{i} a^{(i)} t^{m-i}$, where $a^{(i)}$ is the ith derivative, then $t^p a = at^p$, so $Rf = fR$ and the above Lemma 2.1 implies that $e_r(g, f)$ exists.
5) Consider an invertible matrix $A \in M_n(\mathbb{F}_q)$. If $g(x) = x - A \in M_n(\mathbb{F}_q)[x]$ and $f(x) = x$, then we easily check that the exponent of $g(x)$ relative to x coincides with the order of A in $GL_n(\mathbb{F}_q)$.

Let us give some basic properties of the relative exponent.

Lemma 2.2. *Suppose that f, g, h are elements in a ring R such that $e_r(g, f)$ and $e_r(h, f)$ exist. Then:*

a) g is a right factor of $f^l - 1$ if and only if $e_r(g, f)$ divides l;

b) if g is a right factor of h then $e_r(g,f)$ divides $e_r(h,f)$;
c) if $Rg \cap Rh = Rm$ then $e_r(m,f)$ exists and $e_r(m,f)$ is the least common multiple of $e_r(g,f)$ and $e_r(h,f)$.

Proof. a) Put $e := e_r(g,f)$ and suppose there exists $h \in R$ such that $hg = f^l - 1$. Let $q, r \in \mathbb{N}$ be such that $l = qe + r$ with $0 \leq r < e$. This gives $hg = f^l - 1 = f^{qe+r} - 1 = f^r(f^{qe} - 1) + f^r - 1$. Since $f^e - 1 \in Rg$, we also have $f^{qe} - 1 \in Rg$ and hence $f^r - 1 \in Rg$. This contradicts the definition of $e_r(g,f)$ unless $r = 0$ and e divides l, as required. Conversely, suppose that $eq = l$. We then have $f^l - 1 = (f^q)^e - 1 = (1 + f^e + \cdots + f^{e(q-1)})(f^e - 1) \in Rg$.

b) Put $e' := e_r(h,f)$. Since g is a right factor of h and h is a right factor of $f^{e'} - 1$, then g is a right factor of $f^{e'} - 1$ and hence e divides e'.

c) For simplicity let us write $e(g), e(h), e(m)$ instead of $e_r(g,f), e_r(h,f), e_r(m,f)$. Let us also put e for the least common multiple of $e(g)$ and $e(h)$. Since g and h divide m on the right, we get that $e(g)$ and $e(h)$ both divide $e(m)$ and hence also e divides $e(m)$. On the other hand, g right divides $f^{e(g)} - 1$ and hence also $f^e - 1$. Similarly h right divides $f^e - 1$. Since $Rg \cap Rh = Rm$, we get that m right divides $f^e - 1$. □

We will see in Section 3 that in the case of $\mathbb{F}_q[t;\theta]$ the left and right exponents of a polynomial relative to t exist and are the same.

The study of exponents of polynomials in a skew polynomial ring $A[t;\sigma]$ is related to a notion of order of an element in a group with an automorphism. We introduce this definition and study some of its elementary properties.

Definitions 2.2. Let G be a group and $\sigma \in Aut(G)$.

1) Let $g \in G$ and $n \in \mathbb{N}$. We define the nth norm of g, denoted $N_n(g)$ by $N_0(g) = 1$ and, for $n \geq 1$,

$$N_n(g) = \sigma^{n-1}(g)\sigma^{n-2}(g)\cdots\sigma(g)g.$$

2) An element $g \in G$ is of finite σ-order if there exists a nonzero $l \in \mathbb{N}$ such that $N_l(g) = 1$. In this case $ord_\sigma(g)$ is the smallest l such that $N_l(g) = 1$.
3) For two elements $x, g \in G$ we define $x \underset{\sigma}{\circ} g := \sigma(x)gx^{-1}$. We say that two elements $g, h \in G$ are σ-conjugate if there exists an element $x \in G$ such that $h = \sigma(x)gx^{-1}$.

We can also define the σ-order of an element using the "increasing power of σ" i.e., ${}^{\sigma}N_n(g) := g\sigma(g)\cdots\sigma^{n-1}(g)$. We will not use this second definition except while considering the left evaluation of skew polynomial ring (cf. Remark 3.1(b)). Notice also that for any group G and $\sigma \in Aut(G)$, the σ-conjugacy is an equivalence relation on G.

We give, in the following easy proposition, some relations between the above definitions.

Proposition 2.1. *Let G be a finite group and $\sigma \in Aut(G)$. Then*

a) for $l, s \in \mathbb{N}$, $N_{l+s}(g) = \sigma^l(N_s(g))N_l(g) = \sigma^s(N_l(g))N_s(g)$;
b) for $l, q \in \mathbb{N}$, we have $N_{lq}(g) = \sigma^{l(q-1)}(N_l(g))\sigma^{l(q-2)}(N_l(g)) \cdots \sigma^l(N_l(g))N_l(g)$;
c) any $g \in G$ is of finite σ-order;
d) $N_r(g) = 1$ if and only if $ord_\sigma(g)$ divides r;
e) if $\tau \in Aut(G)$ is such that $\sigma\tau = \tau\sigma$, then $ord_\sigma(g) = ord_\sigma(\tau(g))$;
f) for any $s \in \mathbb{N}$, $N_s(\sigma(g)hg^{-1}) = \sigma^s(g)N_s(h)g^{-1}$. With our notations this means $N_s(g \underset{\sigma}{\circ} h) = g \underset{\sigma^s}{\circ} N_s(h)$;
g) if $\sigma^l = \mathrm{id}$, then
i) $\sigma(N_l(g)) = gN_l(g)g^{-1}$;
ii) $ord_\sigma(g) | l \cdot ord(N_l(g))$.

Proof. a) By definition we have: $N_{l+s}(g) = \sigma^{l+s-1}(g) \cdots \sigma(g)g = \sigma^l\left(\sigma^{s-1}(g) \cdots \sigma(g)g\right) \times \sigma^{l-1}(g) \cdots \sigma(g)g = \sigma^l(N_s(g))N_l(g)$. The second equality is shown similarly.

b) This follows easily from the statement a) above.

c) Since the group G is finite, for any $g \in G$, there must exist $l, s \in \mathbb{N}$ with $s \neq 0$, such that $N_{l+s}(g) = N_l(g)$. The statement a) above then implies that $N_s(g) = 1$. This yields the result.

d) Let us put $l := ord_\sigma(g)$. By definition we must have $N_l(g) = 1$ and $l \leq r$. Let us write $r = lq + s$ where $s < l$. We have $1 = N_r(g) = N_{lq+s}(g) = \sigma^s(N_{lq}(g))N_s(g)$. The point b) above then implies that $1 = N_s(g)$. Since $s < l$ this shows that $s = 0$, as desired.

e) and f) These are left to the reader.

g) i) We compute: $\sigma(N_l(g)) = \sigma^l(g)\sigma^{l-1}(g) \cdots \sigma(g) = gN_l(g)g^{-1}$.

ii) Since $\sigma^l = \mathrm{id}$, statement b) above shows that $N_{ls}(g) = N_l(g)^s$. If s is the order of $N_l(g)$ in G, we get $N_{ls}(g) = N_l(g)^s = 1$. Part d) above then implies that $ord_\sigma(g)$ divides $ls = l \cdot ord(N_l(g))$. □

In the case of a finite cyclic group, the last point of the previous lemma is more precise.

Corollary 2.1. *Let $G = \langle g \rangle$ be a finite cyclic group and let l be the order of an automorphism $\sigma \in Aut(G)$. Then we have $ord_\sigma(g) = l \cdot ord(N_l(g))$.*

Proof. We already know that $ord_\sigma(g)$ divides $l \cdot ord(N_l(g))$. Let $p, n \in \mathbb{N}$ be such that $\sigma(g) = g^p$ and $n := |G| = ord(g)$. Since $\sigma^l = \mathrm{id}$, we have that $g^{p^l} = \sigma^l(g) = g$ and hence $g^{p^l-1} = 1$. Since $n = ord(g)$, we conclude that n divides $p^l - 1$. We write $ord_\sigma(g) = il + r$ for $i \in \mathbb{N}$ and $0 \leq r < l$ and, using the above lemma, we have $1 = N_{il+r}(g) = N_l(g)^i N_r(g) = g^{i[l]+[r]}$, where $[l] = \dfrac{p^l - 1}{p - 1}$ and $[r] = \dfrac{p^r - 1}{p - 1}$. This implies that n divides $i[l]+[r]$. Hence there exists $m \in \mathbb{N}$ such that $n(p-1)m = i(p^l-1)+(p^r-1)$. The fact that n divides $p^l - 1$ implies that n also divides $p^r - 1$. This shows that, for any $x \in G$, $\sigma^r(x) = x^{p^r} = x$. Since $0 \leq r < l$ and l is the order of σ, we must have $r = 0$ and

$1 = g^{i[l]} = N_l(g)^i$. This yields that $ord(N_l(g))$ divides i and hence $l \cdot ord(N_l(g))$ divides $li = ord_\sigma(g)$, as desired. □

Example 2.1. Recall that for $q = p^n$, where p is a prime number and n is a positive integer, the multiplicative group of nonzero elements $\mathbb{F}_q^*$ is cyclic. Moreover the classical norm $N_n(x) = \theta^{n-1}(x) \cdots \theta(x)x$, where θ is the Frobenius automorphism, is an onto map with values in $\mathbb{F}_p^*$. The above corollary then shows that if x is a generator of $\mathbb{F}_q^*$, $ord_\theta(x) = n.ord(N_n(x))$.

3. Exponents in $\mathbb{F}_q[t;\theta]$

Let us recall some facts about the noncommutative ring $\mathbb{F}_q[t;\theta]$, where $q = p^l$ for some prime p and $l \in \mathbb{N}$ and θ is the Frobenius automorphism of $\mathbb{F}_q$: $\theta(a) = a^p$. The elements of $\mathbb{F}_q[t;\theta]$ are polynomials $\sum_{i=0}^n a_i t^i, a_i \in \mathbb{F}_q$. They are added as ordinary polynomials and the multiplication is based on the commutation law:

$$ta = \theta(a)\, t = a^p t, \text{ for } a \in \mathbb{F}_q.$$

This ring is called an Ore–Frobenius extension and its elements are skew polynomials. It is a left and right Euclidean domain. In particular, for $f(t) \in \mathbb{F}_q[t;\theta]$ and $a \in \mathbb{F}_q$, there exist a unique polynomial $q(t) \in \mathbb{F}_q[t;\theta]$ and a unique $r \in \mathbb{F}_q$ such that $f(t) = q(t)(t-a)+r$. Now, we define $f(a)$, the (right) evaluation of f at a, by $f(a) := r$, and hence if $f(t) = \sum_{i=0}^n c_i t^i$, we have

$$f(a) = c_0 + \sum_{i=1}^{n} c_i \theta^{i-1}(a) \cdots \theta(a)\, a = \sum_{i=0}^{n} c_i N_i(a) = \sum_{i=0}^{n} c_i a^{[i]},$$

where $[i] := p^{i-1} + p^{i-2} + \cdots + p + 1 = \dfrac{p^i - 1}{p-1}$.

Definition 3.1. Let $\mathbb{F}_q$ be a finite field and θ be the Frobenius automorphism of $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[t;\theta]$ be a nonzero polynomial. If $f(0) \neq 0$, the right exponent of f is defined by $e_r(f) := e_r(f,t)$. If $f(0) = 0$, we write $f(t) = t^m g(t)$, where $m \in \mathbb{N}$ and $g \in \mathbb{F}_q[t;\theta]$ with $g(0) \neq 0$ are uniquely determined, then $e_r(f) := e_r(g,t)$. We define the left exponent similarly.

Remarks 3.1.

(a) Let us remark that if $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ and $f(t) \in R := \mathbb{F}_q[t;\theta] \subseteq R' := \mathbb{F}_{q'}(t;\theta]$ then we may compute $e_{r,R}(f)$, the right exponent of $f(t)$ considered as an element of R and $e_{r,R'}(f)$ the right exponent of f considered as an element of R'. In fact, these two numbers coincide. To show this, first notice that $e_{r,R'}(f) \leq e_{r,R}(f)$. On the other hand, it is easy to prove, by induction on $\deg(h)$, that if $f \in R$ and $h \in R'$ are

such that $hf \in R$ then h is actually an element of R. Applying this to our situation we conclude that if $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ and $f(t) \in \mathbb{F}_q[t;\theta] \subseteq \mathbb{F}_{q'}[t;\theta]$, $h(t) \in \mathbb{F}_{q'}[t;\theta]$ are such that $h(t)f(t) = t^s - 1$, where $s = e_{r,R'}(f) \in \mathbb{N}$, then, in fact, $h(t) \in \mathbb{F}_q[t;\theta]$. This shows that $e_{r,R}(f) \leq s$ and we obtain that $e_{r,R}(f) = e_{r,R'}(f)$. We conclude that the definition of $e_r(f)$ is independent of the finite field where f is supposed to have its coefficients.

(b) Let us mention that the left evaluation of a polynomial $f(t) = \sum_{i=0}^{n} a_i t^i \in \mathbb{F}_q[t,\theta]$ at $c \in \mathbb{F}_q$ is easily seen to be given by

$$\sum_{i=0}^{n} c\theta^{-1}(c)\theta^{-2}(c)\cdots\theta^{-(i-1)}(c)\theta^{-i}(a_i).$$

In particular, for $e \in \mathbb{N}$, $t - c$ left divides $t^e - 1$ if and only if

$$c\theta^{-1}(c)\theta^{-2}(c)\cdots\theta^{-(e-1)} = 1.$$

This will be used at the end of the proof of Theorem 3.1.

Example 3.1. Let $\mathbb{F}_4 = \{0, 1, a, a^2 = a + 1\}$ be the field of 4 elements and θ be the Frobenius automorphism defined by $\theta(a) = a^2$. Consider the polynomial $f(t) = t - a \in \mathbb{F}_4[t;\theta]$. In the classical case, when $f \in \mathbb{F}_4[t]$, the exponent is 3. However, when $f \in \mathbb{F}_4[t;\theta]$, we have $(t - a^2)(t - a) = t^2 - ta - a^2t + a^3 = t^2 - (\theta(a) + a^2)t + 1 = t^2 - 1$. Thus we conclude that $e_r(f) = 2$.

We will need to work with the ring $M_n(\mathbb{F}_q)$ of matrices over $\mathbb{F}_q = \mathbb{F}_{p^l}$. For $C = (c_{ij})_{1\leq i,j\leq n} \in M_n(\mathbb{F}_q)$ a matrix with entries in $\mathbb{F}_q$, we set $\theta(C) = (\theta(c_{ij}))_{1\leq i,j\leq n}$. We collect some easy facts about the skew polynomial ring $M_n(\mathbb{F}_q)[t;\theta]$ in the following lemma. Notice that the statement 4. in this lemma allows us to speak about the exponent of a polynomial in $M_n(\mathbb{F}_q)[t;\theta]$.

Lemma 3.1. *With the above notations the following holds:*

1. *The map θ defined on $M_n(\mathbb{F}_q)$ is a ring automorphism of order l (where $q = p^l$).*
2. *We have a ring isomorphism $M_n(\mathbb{F}_q)[t;\theta] \cong M_n(\mathbb{F}_q[t;\theta])$.*
3. *For $A \in M_n(\mathbb{F}_q)$ and $f(t) = \sum_{i=0}^{n} a_i t^i \in M_n(\mathbb{F}_q)[t;\theta]$, we have that $f(A) = \sum_{i=0}^{n} a_i A^{[i]} = 0$ if and only if $t - A$ right divides $f(t)$ in $M_n(\mathbb{F}_q)[t;\theta]$.*
4. *If $f(t) \in M_n(\mathbb{F}_q)[t;\theta]$ is such that its independent term is invertible then $e_r(f(t), t)$ exists. In other words there exists $e := e_r(f(t), t)$ which is minimal such that $f(t)$ right divides $t^e - 1$ in $M_n(\mathbb{F}_q)[t;\theta]$.*

For the convenience of the reader we briefly recall some results on semi-linear transformations (they are special cases of the Pseudo-linear transformations, cf [4,5] and

[6] for more information) that will be used in the proof of the following theorem. Let $\theta \in Aut(A)$ be an automorphism of the ring A. For C a $d \times d$ matrix in $M_d(A)$, we define $T_C : A^d \longrightarrow A^d$ by $T_C(\underline{v}) = \theta(\underline{v})C$, where $\underline{v}$ stands for a row vector. We easily see that, for $e \in \mathbb{N}$, $T_C^e(\underline{v}) = \theta^e(\underline{v})N_e(C)$. An obvious consequence of Theorem 1.10 in [6] gives a characterization as to when a polynomial $f(t) \in R = A[t;\theta]$ is such that $f \in Rg$. If $g(t) \in A[t;\theta]$ is a monic polynomial of degree d we let $T_g = T_{C_g}$ stand for the semi-linear map defined on A^d by the companion matrix C_g associated to g. We then have that $f(t) \in Rg$ if and only if $f(T_g)(1,0,\ldots,0) = (0,\ldots,0) \in A^d$.

Theorem 3.1. *Let* $g(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in \mathbb{F}_q[t;\theta]$ *with* $a_0 \neq 0$ *and*

$$C_g = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix} \in GL_n(\mathbb{F}_q)$$

the companion matrix of g. *Then*

1. $e_r(t - C_g) = ord_\theta(C_g)$.
2. $e_r(g) = ord_\theta(C_g)$.
3. *The left and right exponent of the polynomial* g *are equal.*

Proof.

1. Let us put $e := e_r(t - C_g)$ and $l := ord_\theta(C_g)$. We then have $t - C_g$ right divides $t^e - 1$ and hence $N_e(C_g) = \mathrm{id}$, which means that $l = ord_\theta(C_g)$ divides e. On the other hand, if $N_l(C_g) = \mathrm{id}$ we get that $(t^l - 1)(C_g) = 0$ and so $t - C_g$ right divides $t^l - 1$ in $M_n(\mathbb{F}_q)[t;\theta]$. This yields that e divides l, as desired.
2. Put $m := ord_\theta(C_g)$ and remark that, thanks to the part 1. of the theorem, there exists a polynomial $q(t) = (q_{ij}(t)) \in M_n(\mathbb{F}_q)[t;\theta] = M_n(\mathbb{F}_q[t;\theta])$ such that $q(t)(t - C_g) = t^m - 1$. Equating the first row entries on both side we get
   - $q_{11}(t)t + q_{1n}(t)a_0 = t^m - 1$ for the (11) entry,
   - $-q_{1i}(t)t + q_{1,i+1}(t)t + q_{1,n}(t)a_i = 0$ for the entries $(1,i)$ and $2 \leq i \leq n-2$,
   - $-q_{1,n-1}(t) + q_{1,n}(t)(t + a_{n-1}) = 0$ for the $(1,n)$ entry.

   Going backwards we then get successively $q_{1,n-1}(t) = q_{1,n}(t)(t + a_{n-1})$ and replacing $q_{1,n-1}(t)$ in the previous equation leads to $q_{1,n-2}(t) = q_{1,n}(t)(t^2 + a_{n-1}t + a_{n-2})$. More generally for $1 \leq i \leq n-1$ we obtain

$$q_{1,n-i}(t) = q_{1,n}(t)(t^i + a_{n-1}t^{i-1} + \cdots + a_{n-i}) \quad \text{for } 1 \leq i \leq n-1.$$

   In particular, $q_{1,1}(t) = q_{1,n}(t)(t^{n-1} + \cdots + a_2t + a_1)$. Replacing this value in the first equation $q_{11}(t)t + q_{1n}(t)a_0 = t^m - 1$ above we get $q_{1,n}g(t) = t^m - 1$. This shows that

$e_r(g(t))$ divides m. For the converse suppose that $e = e_r(g(t))$ and let $q(t)g(t) = t^e - 1 \in R := \mathbb{F}_q[t;\theta] \subset M_n(\mathbb{F}_q)[t;\theta]$. Put $d := \deg g(t)$. We have $t^e - 1 \in Rg$ and hence by Theorem 1.10 in [6] (see also the comments before this theorem) we get that $(T_g^e - 1)(I, 0, \ldots, 0) = (0, 0, \ldots, 0) \in M_d(\mathbb{F}_q)^d$, where the entries of the vectors are square matrices of size $d = \deg(g)$. This leads to $\theta^e(I, 0, \ldots, 0)N_e(C_g) = (I, 0, \ldots, 0)$ and hence $N_e(C_g) = I$. So that $ord_\theta(C_g)$ divides e. This yields the desired result.

3. We must show that, for $e = e_r(g)$, the polynomial $g(t)$ divides $t^e - 1$ on the right and on the left. Now $e_r(g) = ord_\theta(C_g)$. Working in $\mathbb{M}_d(\mathbb{F}_q)[t;\theta]$ with $d = \deg g(t)$, we have $ord_\theta(C_g) = e_r(t - C_g)$. In $\mathbb{M}_d(\mathbb{F}_q)[t;\theta]$, $t - C_g$ is a right factor of $t^e - 1$ if and only if

$$\theta^{e-1}(C_g) \cdots \theta(C_g) C_g = 1.$$

Applying θ^{1-e}, to this equality, we get

$$C_g \theta^{-1}(C_g) \cdots \theta^{1-e}(C_g) = 1.$$

This means that $t - C_g$ is a left factor of $t^e - 1$ (cf. Remark 3.1(b)). Hence $e_r(t - C_g) = e_\ell(t - C_g)$. □

The equality of the right and left exponent of a polynomial of an Ore–Frobenius extension has the following interesting consequence.

Corollary 3.1. *For any polynomial $g(t) \in \mathbb{F}_q[t;\theta]$ with nonzero constant term, and for any $l \in \mathbb{N}$, $g(t)$ is a right factor of $t^l - 1$ if and only if it is a left factor of $t^l - 1$.*

Proof. Suppose that $g = g(t)$ right divides $t^l - 1$, this implies that $e = e_r(g) = e_l(g)$ divides l, say $l = eq$, for some $q \in \mathbb{N}$. Since g also left divides $t^e - 1$ and $t^l - 1 = (t^e - 1)((t^e)^{q-1} + \cdots + t^e + t + 1)$ we conclude that g left divides $t^l - 1$. The converse implication is obtained in the same way. □

In the sequel, we shall write $e(f)$ for the exponent of $f \in \mathbb{F}_q[t;\theta]$.

Example 3.2. Consider the polynomial $g(t) = t^3 + at + 1 \in \mathbb{F}_4[t;\theta]$. The companion matrix of g is

$$C_g = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a & 0 \end{pmatrix},$$

then

$$N_2(C_g) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a^2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & a & 0 \\ 0 & 1 & a^2 \end{pmatrix}.$$

Since the order of $N_2(C_g)$ in $GL_3(\mathbb{F}_4)$ is 4, then, by Proposition 2.1, we have $ord_\theta(C_g)$ divides $2ord(N_2(C_g)) = 8$, and $N_8(C_g) = N_2(C_g)^4 = \mathrm{id}$, hence $e(g) = 8$. One can verify that

$$\left(t^5 + a^2t^3 + t^2 + at + 1\right)\left(t^3 + at + 1\right) = t^8 + 1.$$

Note that the classical exponent of g is 21.

Example 3.3. Let $\mathbb{F}_8 = \left\{0, 1, a, a^2, \ldots, a^6; a^3 = a + 1\right\}$ and $\theta(a) = a^2$. Consider the polynomial $g(t) = t^2 + at + 1 \in \mathbb{F}_8[t;\theta]$. The companion matrix of g is

$$C_g = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix},$$

then, by computing $N_i(C_g)$ for $i = 1, 2, \ldots$, we obtain $e(g) = 9$. In this case, the classical exponent is also equal to 9. However, in $\mathbb{F}_8[t;\theta]$ we have the factorization

$$\left(t^7 + a^2t^6 + at^5 + a^3t^4 + a^6t^3 + at^2 + at + 1\right)\left(t^2 + at + 1\right) = t^9 + 1,$$

while in $\mathbb{F}_8[t]$ the factorization is

$$\left(t^7 + at^6 + a^6t^5 + a^3t^4 + a^3t^3 + a^6t^2 + at + 1\right)\left(t^2 + at + 1\right) = t^9 + 1.$$

In the sequel, we denote by $\overline{\mathbb{F}_q}$ the algebraic closure of $\mathbb{F}_q$. We need a small lemma which is the analogue of a very well-known fact in the commutative setting.

Lemma 3.2. *Let $g(t) \in \mathbb{F}_q[t;\theta]$ be a monic irreducible polynomial and $\alpha \in \overline{\mathbb{F}_q}$ such that $g(\alpha) = 0$ (i.e., $t - \alpha$ right divides $g(t)$ in $\overline{\mathbb{F}_q}[t;\theta]$). Then for any $h(t) \in \mathbb{F}_q[t;\theta]$ such that $h(\alpha) = 0$, $g(t)$ right divides $h(t)$ in $\mathbb{F}_q[t;\theta]$.*

Proof. Let p be the characteristic of the finite field $\mathbb{F}_q$ and write $q = p^n$, for some $n \in \mathbb{N}$. Let us first notice that Theorem 2.5 1) in [6] implies that there exists $\alpha \in \overline{\mathbb{F}_q}$ such that $g(\alpha) = 0$. We let q' be such that $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ and $\alpha \in \mathbb{F}_{q'}$. If we denote by l the dimension of the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$, we have $q' = q^l = p^{nl}$. Let us then observe that we can extend θ to an automorphism of $\mathbb{F}_{q'}[t;\theta]$ by defining $\theta(t) = t$. The polynomials fixed by θ^n are exactly the elements of $\mathbb{F}_q[t;\theta]$, and one can easily check that $g(\theta^{in}(\alpha)) = 0$ for $i = 0, \ldots, l-1$. This implies that the least left common multiple $m(t)$ of the set $\{t - \theta^{in}(\alpha) \mid 0 \leq i \leq l-1\}$ right divides $g(t)$ in $\mathbb{F}_{q'}[t;\theta]$. Since $m(t)$ is fixed under the action of θ^n, we get that $m(t) \in \mathbb{F}_q[t;\theta]$. The fact that $g(t)$ is irreducible then implies that $m(t) = g(t)$.

Now, if $h(t) \in \mathbb{F}_q[t;\theta]$ is such that $h(\alpha) = 0$ we get that, for all $0 \leq i \leq l-1$, $h(\theta^{ni}(\alpha)) = 0$ and hence $m(t) = g(t)$ right divides $h(t)$ in $\mathbb{F}_q[t;\theta]$, as desired. □

In the next proposition we will use the following convenient notations : for $g_1, \ldots, g_s \in R = \mathbb{F}_q[t;\theta]$ we denote by $[g_1, \ldots, g_s]_\ell$ the least left common multiple of $g_1, \ldots, g_s$. Similar notations are used for the least common multiple of integers.

Proposition 3.1. *Let $q = p^l$ and let $g, g_1, \ldots, g_s$ be monic polynomials in $\mathbb{F}_q[t;\theta]$ with nonzero constant terms. Then:*

(a) the polynomial g is a right (resp., left) factor of $t^c - 1$, where c is a positive integer, if and only if $e(g)$ divides c;
(b) if g is a right (resp., left) factor of h, then $e(g)$ divides $e(h)$;
(c) with the notations introduced before the statement of the proposition we have $e([g_1, \ldots, g_s]_\ell) = lcm(e(g_1), \ldots, e(g_s))$;
(d) for $\alpha \in \mathbb{F}_q^*, e(t-\alpha) = ord_\theta(\alpha)$;
(e) if α is a primitive element of $\mathbb{F}_q = \mathbb{F}_{p^l}$, then $e(t-\alpha) = l(p-1)$;
(f) if $\alpha \in \overline{\mathbb{F}_q}$ is such that $t - \alpha$ is a right (resp., left) factor of $g(t)$ in $\overline{\mathbb{F}_q}[t;\theta]$ and $g(t)$ is irreducible in $\mathbb{F}_q[t;\theta]$, then $e(g) = ord_\theta(\alpha)$;
(g) the map θ can be extended to $\mathbb{F}_q[t;\theta]$ via $\theta(t) = t$. We then have
1) $e(g(t)) = e(\theta(g(t)))$, for $g(t) \in \mathbb{F}_q[t;\theta]$,
2) If $h(t) = [g(t), \theta(g(t)), \ldots, \theta^{l-1}(g(t))]_\ell$, then $e(h(t)) = e(g(t))$ and $\theta(h(t)) = h(t)$ (equivalently $th(t) = h(t)t$).

Proof. (a) and (b) follow easily from our earlier results.

(c) This result is true for general relative exponents, as might be checked using Lemma 2.2(c). We give another self-contained proof. We denote by g the least left common multiple of $g_1, \ldots, g_s$ i.e., $g := [g_1, \ldots, g_s]_\ell$, $e := [e_1, \ldots, e_s]$ where, for $1 \leq i \leq s$, $e_i := e(g_i)$. Since for $1 \leq i \leq s$, g_i right divides g, we have that e_i divides $e(g)$ and hence e divides $e(g)$. On the other hand, for $1 \leq i \leq s$, g_i divides on the right $t^{e_i} - 1$ and hence also $t^e - 1$. This leads to the fact that g divides on the right $t^e - 1$ and so $e(g)$ divides e. This yields the proof.

(d) This comes directly from Theorem 3.1 by considering $g(t) = t - \alpha$.

(e) Suppose that $\alpha \in \mathbb{F}_q$ is of order $q-1 = p^l - 1$ and put $e := e(t-\alpha)$. The definition of $[l(p-1)]$ gives

$$[n(p-1)] = \frac{p^{l(p-1)} - 1}{p-1} = \frac{(p^l - 1)(p^{l(p-2)} + \cdots + p^l + 1)}{p-1}.$$

Since for $i \in \mathbb{N}$, $p^i \equiv 1 \mod (p-1)$, we conclude that $p-1$ divides $p^{l(p-2)} + \cdots + p^l + 1$, and hence $p^l - 1$ divides $[l(p-1)]$. This leads to $N_{l(p-1)}(\alpha) = \alpha^{[l(p-1)]} = 1$, so e divides $l(p-1)$ and there exists an integer s such that

$$es = l(p-1). \tag{1}$$

On the other hand, $N_e(\alpha) = \alpha^{[e]} = 1$, then $p^l - 1$ divides $[e]$, hence $p-1$ divides $[e] = p^{e-1} + \cdots + p + 1$. Using again the fact that, for $i \in \mathbb{N}$, we have $p^i \equiv 1 \mod (p-1)$, then $[e] \equiv e \equiv 0 \mod (p-1)$, and there exists an integer k such that

$$e = k(p-1). \tag{2}$$

We then obtain

$$l = ks. \tag{3}$$

Now, $e = e(t-\alpha) = ord_\theta(\alpha)$ gives that $1 = N_e(\alpha) = \alpha^{[e]}$ and $p^l - 1$ divides $[e]$. Let thus $a \in \mathbb{N}$ be such that $[e] = a(p^l - 1)$. Write $e = lb + r$, with $0 \leq r < l$. We then have

$$[e] = \frac{\left(p^{lb} - 1\right) p^r + p^r - 1}{p-1} = \frac{\left(p^l - 1\right)\left(p^{l(b-1)} + \cdots + p^l + 1\right)p^r + p^r - 1}{p-1},$$

so $p^l - 1$ divides $[e]$ which divides

$$(p-1)[e] = \left(p^l - 1\right)\left(p^{l(b-1)} + \cdots + p^l + 1\right)p^r + p^r - 1,$$

which implies that $r = 0$, hence

$$e = lb, \tag{4}$$

and $(p-1)[e] = (p-1)a\left(p^l - 1\right) = \left(p^l - 1\right)\left(p^{l(b-1)} + \cdots + p^l + 1\right)$, then $(p-1)a = p^{l(b-1)} + \cdots + p^l + 1$ and this implies that $b \equiv 0 \mod (p-1)$, so there exists an integer c such that

$$b = c(p-1). \tag{5}$$

Finally, using successively (2), (4) and (3), we obtain

$$e = k(p-1) = lb = ksb = ksc(p-1),$$

this yields $s = c = 1$, then $l = k$, and $e = l(p-1)$, as desired.

(f) Put $l := ord_\theta(\alpha)$. Statements a) and d) above show that $l = e(t-\alpha)$ divides $e(g)$. On the other hand, we also have $N_l(\alpha) = 1$ and hence $(t^l - 1)(\alpha) = 0$ and Lemma 3.2 shows that $g(t)$ divides $t^l - 1$. Statement a) above implies that $e_r(g)$ divides l. This yields the proof.

(g) 1) is due to the fact that polynomials of the form $t^r - 1$, $r \in \mathbb{N}$, are invariant under the extension of θ.

2) is now an obvious consequence of (c) above. □

Let us end this paper with the following proposition which gives more information on the exponent of a power g^b.

Proposition 3.2. *Let $g(t) \in \mathbb{F}_q[t;\theta]$ with nonzero constant term and let $e = e_r(g)$ be its exponent. Suppose that $t^e - 1 = hg = gh$, which is the case when the order of θ divides e. Let b be a positive integer, and s be the least integer such that $p^s \geqslant b$. Then $e\left(g^b\right) = ep^u$, where $0 \leq u \leq s$.*

Proof. Put $c := e\left(g^b\right)$. Since g right divides g^b, Proposition 3.1 shows that $e = e_r(g)$ divides c. Moreover, since $g(t)$ right divides $t^e - 1$ and $gh = hg = t^e - 1$ then $g^b(t)$ right divides $(t^e-1)^b$, so $g^b(t)$ right divides $(t^e-1)^{p^s} = t^{ep^s} - 1$. Hence Proposition 3.1 implies that c divides ep^s. Since c is a multiple of e, this gives $c = e\left(g^b\right) = ep^u$, where $0 \leq u \leq s$. □

4. Conclusion

We have defined the notion of relative exponent of two elements in a ring, paying particular attention to the case of a finite ring. This has then been applied to the case of skew polynomials over finite rings. The case of polynomials of a Frobenius–Ore extension $\mathbb{F}_q[t;\theta]$ has been specifically targeted in order to extend classical theorems related to the exponent (a.k.a. period) of a polynomial over a finite field.

Acknowledgment

We would like to thank the referees for their careful readings and comments. Part of this work was done during the first author's visit to the Université d'Artois. He would like to thank the members of this institution for their welcome.

References

[1] D. Boucher, F. Ulmer, Coding with skew polynomial rings, J. Symb. Comput. 44 (2009) 1644–1656.
[2] D. Boucher, F. Ulmer, Linear codes using skew polynomials with automorphisms and derivations, Des. Codes Cryptogr. 70 (2014) 405–431.
[3] A. Boulagouaz, A. Leroy, (σ,δ)-codes, Adv. Math. Commun. (2013) 463–474.
[4] N. Jacobson, Pseudo-linear transformations, Ann. Math. 38 (1937) 484–507.
[5] A. Leroy, Pseudo-linear transformations and evaluation in Ore extensions, Bull. Belg. Math. Soc. Simon Stevin 2 (3) (1995) 321–347.
[6] A. Leroy, Noncommutative polynomial maps, J. Algebra Appl. 11 (04) (August 2012).
[7] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, 1994.
[8] S. Lopez-Permouth, Y. Szabo, Convolutional codes with additional algebraic structure, J. Pure Appl. Algebra 217 (5) (2013).