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

A R T I C L E   I N F O

Article history:
Received 16 March 2015
Received in revised form 18 August 2015
Accepted 20 August 2015
Available online 14 September 2015
Communicated by Dieter Jungnickel

MSC:
16S36
11T55
12Y05
11T71

Keywords:
Skew polynomial rings
Finite fields
Period of polynomials

A B S T R A C T

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) ⇔ (ii) and (iii) ⇒ (iv) ⇔ (v);
b) if $|R/Rg| < \infty$ and f is not a zero divisor and is such that $fR = Rf$ we also have (ii) ⇒ (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.