Journal of Algebra 398 (2014) 55–62

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Near-vector spaces determined by finite fields

K.-T. Howell [a], J.H. Meyer [b,*]

[a] Department of Mathematical Sciences, Stellenbosch University, Stellenbosch 7600, South Africa
[b] Department of Mathematics and Applied Mathematics, University of the Free State, PO Box 339, Bloemfontein 9300, South Africa

ARTICLE INFO

Article history:
Received 17 January 2012
Available online 15 October 2013
Communicated by Michel Van den Bergh

Keywords:
Finite fields
Near-vector spaces

ABSTRACT

We derive conditions on the integers q and r necessary and sufficient for the identity $(a^q + b^q)^r = (a^r + b^r)^q$ to hold over a finite field. As an application, we use the result to characterize all finite-dimensional near-vector spaces determined by an arbitrary finite field.

1. Introduction

In [2], the concept of a vector space, i.e., linear space, is generalized by André to a structure comprising a bit more non-linearity, the so-called near-vector space. In [7] van der Walt showed how to construct an arbitrary finite-dimensional near-vector space, using a finite number of near-fields, all having isomorphic multiplicative semigroups. In [5] this construction is used to characterize all finite-dimensional near-vector spaces in case all near-fields are equal to $\mathbb{Z}_p$, p a prime. Our aim in this paper is to extend these results to the case where all the near-fields are equal to an arbitrary finite field, using properties of the equation $(a^q + b^q)^r = (a^r + b^r)^q$, where $a, b \in GF(p^n)$, the finite field with p^n elements.

The following section collects a series of results (some of which are well known) regarding finite fields. These will be needed in the final section.

2. Results related to $GF(p^n)$

Throughout this paper we fix a prime p, a positive integer n, and let $F = GF(p^n)$, the field with p^n elements. Also, ϕ will denote Euler's totient function.

* Corresponding author.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2013.09.019

Lemma 2.1. *Let $(1+b)^k = 1+b^k$ for all $b \in F$, where $0 < k < p^n - 1$. Then $k \in \{1, p, p^2, \ldots, p^{n-1}\}$.*

Proof. For $k > 1$, consider the polynomial $f(x) = (1+x)^k - x^k - 1 \in F[x]$ of degree less than or equal to $k-1$. If $f(x) \neq 0$, then it has at most $k-1$ zeros in F. But it is given that $f(b) = 0$ for all $b \in F$, so that f has to be the zero polynomial. As $f(x) = \sum_{i=1}^{k-1} \binom{k}{i} x^i = 0$, we have that $p \mid \binom{k}{i}$ for all $1 \leqslant i \leqslant k-1$, since $\operatorname{char}(F) = p$. We note that $p \mid \binom{k}{1}$ implies that $p \mid k$. Now assume that $k = p^t m$, where $t \geqslant 1$, and $p \nmid m$, $m > 1$. Then we have a contradiction between $p \mid \binom{p^t m}{p^t}$ and $\binom{p^t m}{p^t} \equiv m \pmod{p}$ [3, Theorem 13.8]. Consequently, $k \in \{1, p, p^2, \ldots, p^{n-1}\}$. $\square$

Theorem 2.2. *Let $q_1, q_2 \in \{1, 2, \ldots, p^n - 1\}$ with $\gcd(q_i, p^n - 1) = 1$ $(i = 1, 2)$ and $q_1 < q_2$. Then $(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1}$ for all $a, b \in F$ if and only if $q_1 \equiv q_2 p^l \pmod{p^n - 1}$ for some $l \in \{0, 1, \ldots, n-1\}$.*

Proof. If $q_1 \equiv q_2 p^l \pmod{p^n - 1}$ for some $0 \leqslant l \leqslant n-1$, then $x^{q_1} = x^{q_2 p^l}$ for all $x \in F$. So,

$$\left(a^{q_2} + b^{q_2}\right)^{q_1} = \left(a^{q_2} + b^{q_2}\right)^{q_2 p^l} = \left(a^{q_2 p^l} + b^{q_2 p^l}\right)^{q_2} = \left(a^{q_1} + b^{q_1}\right)^{q_2},$$

for all $a, b \in F$. Conversely, suppose that $(a^{q_1} + b^{q_1})^{q_2} = (a^{q_2} + b^{q_2})^{q_1}$ for all $a, b \in F$. Let $s \in \mathbb{Z}$ $(1 \leqslant s \leqslant p^n - 2)$ such that $q_2 s \equiv 1 \pmod{p^n - 1}$. Let $a = 1$, $b = y^s$. Then $(1 + y^{q_1 s})^{q_2} = (1+y)^{q_1}$ for all $y \in F$. This implies that $1 + y^{q_1 s} = (1+y)^{q_1 s}$ for all $y \in F$. Let $k \in \mathbb{Z}$ $(1 \leqslant k \leqslant p^n - 2)$ with $k \equiv q_1 s \pmod{p^n - 1}$. Then $1 + y^k = (1+y)^k$ for all $y \in F$. By Lemma 2.1, $k = p^l$ where $l \in \{0, 1, \ldots, n-1\}$. So $p^l \equiv q_1 s \pmod{p^n - 1}$ implying that $p^l q_2 \equiv q_1 \pmod{p^n - 1}$. $\square$

Definition 2.3. A finite sequence of m integers $q_1, q_2, \ldots, q_m$ is called *suitable with respect to $F = GF(p^n)$* if

(a) $1 \leqslant q_i \leqslant p^n - 1$ and $\gcd(q_i, p^n - 1) = 1$ for all $i = 1, \ldots, m$;
(b) no q_i can be replaced by a smaller q_i' that also satisfies (a) and such that $q_i \equiv q_i' p^l \pmod{p^n - 1}$ for some $l \in \{0, 1, \ldots, n-1\}$.

Suitable sequences are always written in non-decreasing order: $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_m$.

Hence, to obtain a suitable sequence with respect to $GF(p^n)$, simply make a list of the smallest members of all the cosets determined by the subgroup $\langle p \rangle$ of the multiplicative group $U(p^n - 1) = \{k \in \mathbb{Z}\colon\ 1 \leqslant k \leqslant p^n - 1$ and $\gcd(k, p^n - 1) = 1\}$. Then select (possibly with repetition) any m members from this list, and write them down in non-decreasing order. Note that there will be $\phi(p^n - 1)/n$ elements in the list to choose from.

The next result can be found in most text books that contain a section on finite fields, such as [1].

Lemma 2.4. *Each element of F has a q-th root in F if and only if $\gcd(q, p^n - 1) = 1$.*

This lemma can be used to prove:

Proposition 2.5. *Let ψ be an automorphism of the group $(F^*, \cdot)$. Then there exists $q \in \mathbb{Z}$, with $1 \leqslant q \leqslant p^n - 1$ and $\gcd(q, p^n - 1) = 1$, such that $\psi(x) = x^q$ for all $x \in F^*$.*

Example 2.6. (See [4, pp. 67–68].) Consider $F = GF(3^2)$. The q's with $1 \leqslant q \leqslant 3^2 - 1$ and $\gcd(q, 3^2 - 1) = 1$, are $q = 1, 3, 5, 7$. So $\psi(x) = x^q$ for each of these q's are exactly the automorphisms of the group $(F^*, \cdot)$. Take $q = 5$, for example: