Abstract

For q, a prime power, $\mathbb{F}_q$ denotes the field of order q. Then, the group $\mathbb{F}_q^\times := \mathbb{F}_q \backslash \{0\}$ of units of $\mathbb{F}_q$ is cyclic and a generator of this group is referred to as a primitive element of the field. In fact, $\mathbb{F}_q$ has exactly $\varphi(q-1)$ primitive elements, φ being Euler's totient function. Let r be a divisor of $(q-1)$. An r-primitive element in $\mathbb{F}_q$ is an element of $\mathbb{F}_q^\times$ of order $(q-1)/r$. Evidently, if α is a primitive element, then for every divisor r of $(q-1)$, α^r is an r-primitive element so that primitive elements are 1-primitive elements. An element α belonging to the degree n extension $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is referred to as normal over $\mathbb{F}_q$ if $B_\alpha = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ spans $\mathbb{F}_{q^n}$ as an $\mathbb{F}_q$-vector space. It is necessary and sufficient for $\alpha \in \mathbb{F}_{q^n}$ to be normal over $\mathbb{F}_q$ that the polynomials $g_\alpha(x) = \alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-1}} x + \alpha^{q^{n-1}}$ and $x^n - 1$ are relatively prime over $\mathbb{F}_{q^n}$. Using this equivalence, the notion of k-normal elements was introduced by Huczynska et. al. in 2003; an element $\alpha \in \mathbb{F}_{q^n}$ is k-normal over $\mathbb{F}_q$ if the gcd of the polynomials $g_\alpha(x)$ and $x^n - 1$ in $\mathbb{F}_{q^n}[x]$ has degree k. Equivalently, an element α belonging to $\mathbb{F}_{q^n}$ is k-normal over $\mathbb{F}_q$ if and only if the span of $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ over $\mathbb{F}_q$ is $(n-k)$-dimensional. Observe that 0-normal elements are normal elements. In the recent time, quite a few people worked on elements that are k-normal or r-primitive or both. It is worth mentioning that, primitive elements have wide applications in coding theory and cryptography. If r is small, an r-primitive element may be used as a replacement of a primitive element in many applications. If for a rational function $f(x)$, both α and $f(\alpha)$ are primitive elements in $\mathbb{F}_q$, the pair $(\alpha, f(\alpha))$, is referred to as a primitive pair; in the past, people studied the existence of such pairs.

In this thesis, we deal with the question of the existence of primitive pair; in fact, we improve the known bounds for even or odd rational functions for $q \equiv 3 \pmod 4$. Further, for $r_1, r_2 > 0$ both dividing $(q^n - 1)$, $k_1, k_2 \geqslant 0$ such that there are polynomials dividing $(x^n - 1)$ with degrees k_1 and k_2, $a, b \in \mathbb{F}_q$ with $a \neq 0$, we study for a rational function $f(x) \in \mathbb{F}_{q^n}(x)$ the existence of an element in $\mathbb{F}_{q^n}$ which is both k_1-normal and r_1-primitive with its norm equal to a and its trace equal to b such that its image under f is both k_2-normal and r_2-primitive in $\mathbb{F}_{q^n}$. We obtain an implicit condition on q and n for the existence of such a pair. We discuss a few numerical examples. Moreover, if we impose an additional condition on k_1, k_2, namely, $n \geqslant 2(k_1 + k_2) + 5$, then for every n such that $x^n - 1$ has divisors of degree k_1 and k_2 and for all but finitely many prime powers q such that $r_1, r_2 \mid q^n - 1$, there exists $\alpha \in \mathbb{F}_{q^n}$ with the desired property. Also, in this thesis, we deal with the existence of r-primitive elements in arithmetic progression by using a new formulation of the characteristic function for r-primitive elements belonging to $\mathbb{F}_q$. In fact, we find a condition on q for the existence of $\alpha \in \mathbb{F}_q^\times$ for a given $n \geqslant 2$ and $\beta \in \mathbb{F}_q^\times$ such that each of $\alpha, \alpha + \beta, \alpha + 2\beta, \ldots, \alpha + (n-1)\beta \in \mathbb{F}_q^\times$ is r-primitive in $\mathbb{F}_q^\times$. Furthermore, as a consequence, the number of arithmetic progressions in $\mathbb{F}_q$ consisting of r-primitive elements of length n, is asymptotic to $\frac{q}{(q-1)^n}\varphi(\frac{q-1}{r})^n$. Besides, using a traditional method, we improved the existence criterion for such arithmetic progressions in $\mathbb{F}_q$ when $q \equiv 3 \pmod 4$.