Abstract

In this thesis, we obtain a sufficient condition for the existence of a primitive normal pair $(\alpha, f(\alpha))$ over $\mathbb{F}_{q^n}$, where $f(x)$ is a non-exceptional rational function over $\mathbb{F}_{q^n}$ of degree sum m. Additionally, for rational functions of degree sum 4, we prove that there are only 37 and 16 exceptional values of (q, n) for $q = 2^k$ and $q = 3^k$ respectively.

Next, we provide a sufficient condition for the existence of primitive normal pair $(\alpha, f(\alpha))$ over $\mathbb{F}_{q^n}$ with norm and trace of α to be prescribed in $\mathbb{F}_q$, where $f(x) \in \mathbb{F}_{q^n}(x)$ is a rational function of degree sum m. Particularly, we investigate the rational functions of degree sum 4 over $\mathbb{F}_{q^n}$, where $q = 11^k$ and demonstrate that there are only 3 exceptional pairs $(q, n), n \geq 7$ for which such kind of primitive normal pair may not exist. In general, we showed that such elements always exist except for finitely many choices of (q, n).

Further, we extend our work to the existence of primitive normal triple $(\alpha, \beta, f(\alpha, \beta))$ over $\mathbb{F}_{q^n}$, where $f(x, y) = ax^2 + bxy + cy^2 \in \mathbb{F}_{q^n}[x], b^2 \neq 4ac$. Next, we generalize this result for the existence of r-primitive k-normal triple over $\mathbb{F}_{q^n}$ and discuss the existence of 2-primitive 1-normal element α and 2-primitive element β in $\mathbb{F}_{q^n}$ such that $f(\alpha, \beta)$ is also 2-primitive for $q = 3^t$, where t is a positive integer.

Next, we generalize our work on the existence of primitive triples by defining primarily exceptional rational functions in n indeterminates. We discussed the existence of triples $(\alpha, \beta, f(\alpha, \beta))$ over $\mathbb{F}_q$, where α, β are primitive and $f(\alpha, \beta)$ is an r-primitive element of $\mathbb{F}_q$. In particular, this implies the existence of $\mathbb{F}_q$-primitive points on the surfaces of the form $z^r = f(x, y)$, where $r|q-1$. As an example, we applied our results to the unit sphere over $\mathbb{F}_q$.

Next work in the thesis deals with primitive polynomials. Primitive polynomials have their applications in stream cipher cryptosystems. These cryptosystems use linear feedback shift registers (LFSRs) to generate their secret keys. There are different kinds of key-stream generators like filter generators, combination generators, clock-controlled generators, etc. For a combination generator, the connection polynomial is the product of connection polynomials of constituent LFSRs. The cryptographic systems using LFSRs as their components are vulnerable to correlation attacks. The attack heavily depends on the t-nomial multiples of the connection polynomial for small values of t. In this thesis, we obtain the exact number of 4-nomial and 5-nomial

multiples of the product of primitive polynomials. This helps us to choose a more suitable connection polynomial to resist the correlation attacks. Next, we disprove a conjecture by Maitra, Gupta, and Venkateswarlu.