ABSTRACT

Let Q be a nondegenerate quadratic form over the finite field $\mathbb{F}_q$ of odd prime power order q with char$\mathbb{F}_q \neq 2$ and Let $O_n(\mathbb{F}_q)$ be the associated orthogonal group. Let $O_n(\mathbb{F}_q)$ act linearly on the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$. In this thesis we find the invariant subring $\mathbb{F}_q[x_1, x_2, x_3, x_4, x_5]^{O_5(\mathbb{F}_q)}$ with explicit generators. We also prove that this subring is a UFD.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field of odd prime power order q, $R = \mathbb{F}_q[x_1, \ldots, x_n]$ the polynomial ring over $\mathbb{F}_q$ and $K = \mathbb{F}_q(x_1, \ldots, x_n)$ the rational field of n variables. If G is a subgroup of $GL_n(\mathbb{F}_q)$, then G induces an action on R and K. In other words, if we fix a basis of $\mathbb{F}_q^n$, then every $\sigma \in GL_n(\mathbb{F}_q)$ can be represented as $(a_{ij}) \in GL_n(\mathbb{F}_q)$, and the induced action is

$$\begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \end{pmatrix} = (a_{ij}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Let $R^G := \{f \in R | \sigma(f) = f \text{ for all } \sigma \in G\}$ and $K^G := \{f/g \in K | \sigma(f/g) = f/g \text{ for all } \sigma \in G\}$ be the invariant subring and the invariant subfield, respectively. It is obvious that K^G is the quotient field of R^G and $R^G = R \cap K^G$.

Given a nondegenerate quadratic form $Q(x_1, \ldots, x_n)$ on $V = \mathbb{F}_q^n$, the orthogonal group $O_n(\mathbb{F}_q)$ is the set of all linear transformations σ on V such that $Q(\sigma v) = Q(v)$ for all v in V. There are two equivalence classes of nondegenerate quadratic forms and they are distinguished by their discriminants. A quadratic form Q can be taken to be a diagonal form and indeed can be specified as follows:

$$\begin{array}{rll} \text{For even } n, & (\alpha) & Q^+ = x_1^2 - x_2^2 + \cdots + x_{n-1}^2 - x_n^2, \\ & (\beta) & Q^- = x_1^2 - x_2^2 + \cdots + x_{n-1}^2 - dx_n^2; \\ \text{For odd } n, & (\gamma) & Q^+ = x_1^2 - x_2^2 + \cdots + x_{n-2}^2 - x_{n-1}^2 + x_n^2, \end{array}$$

where d is a nonsquare in $\mathbb{F}_q$(see[7], Section 6.3, 6.10).

Let $Q = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$ be a nondegenerate form. Define $Q_{nk} = \lambda_1 x_1^{q^k+1} + \cdots + \lambda_n x_n^{q^k+1}$. Now we are going to summarize some results about the invariant subring and invariant subfield of the orthogonal group.

Theorem 1.1. [2]

$$\mathbb{F}_q(x_1, \cdots, x_n)^{O_n(\mathbb{F}_q)} = \mathbb{F}_q(Q_{n0}, \cdots, Q_{n,n-1}).$$

Theorem 1.2. [5]

$$\begin{aligned} \mathbb{F}_q[x_1, x_2]^{O_2(\mathbb{F}_q, Q_2^+)} &= \mathbb{F}_q[Q_{20}, \frac{Q_{21}}{Q_{20}}]; \\ \mathbb{F}_q[x_1, x_2]^{O_2(\mathbb{F}_q, Q_2^-)} &= \mathbb{F}_q[Q_{20}, Q_{21}]. \end{aligned}$$

Theorem 1.3. [6]

$$\mathbb{F}_q[x_1, x_2, x_3]^{O_3(\mathbb{F}_q)} = \mathbb{F}_q[Q_{30}, Q_{31}, \frac{Q_{32} - Q_{30}^{\frac{q^2+1}{2}}}{Q_{31} - Q_{30}^{\frac{q+1}{2}}}].$$

Theorem 1.4. [4]

$$\mathbb{F}_q[x_1, x_2, x_3, x_4]^{O_4(\mathbb{F}_q, Q_4^+)} = \mathbb{F}_q[Q_{40}, Q_{41}, Q_{42}, \frac{G_1(Q_{40}, Q_{41}, Q_{42}, Q_{43})}{F(Q_{40}, Q_{41}, Q_{42})}, \frac{G_2(Q_{40}, Q_{41}, Q_{42}, Q_{43})}{F(Q_{40}, Q_{41}, Q_{42})}],$$

where

$$\begin{aligned} F(Y_0, Y_1, Y_2) &= (Y_2 Y_0^q - Y_1^{q+1}) - (Y_1^2 - Y_0^{q+1})^{\frac{q+1}{2}}, \\ G_1(Y_0, Y_1, Y_2, Y_3) &= Y_3 Y_0^q - Y_1 Y_2^q - (Y_1^2 - Y_0^{q^2+1})^{\frac{q-1}{2}}(Y_1 Y_2 - Y_0 Y_1^q), \text{ and} \\ G_2(Y_0, Y_1, Y_2, Y_3) &= Y_3 Y_1^q - Y_1^{q^2+1} - (Y_2^2 - Y_0^{q^2+1})^{\frac{q+1}{2}}. \end{aligned}$$

Remark 1.1. *Let*

$$R_4^* := \mathbb{F}_q[Q_{40}, Q_{41}, Q_{42}, \frac{G_1(Q_{40}, Q_{41}, Q_{42}, Q_{43})}{F(Q_{40}, Q_{41}, Q_{42})}, \frac{G_2(Q_{40}, Q_{41}, Q_{42}, Q_{43})}{F(Q_{40}, Q_{41}, Q_{42})}].$$

In the process of the proof of Theorem1.4, the author has shown R_4 is integral over R_4^*. We need this to prove our main theorem.

Theorem 1.5. [3]

$$\mathbb{F}_q[x_1, x_2, x_3, x_4]^{O_4(\mathbb{F}_q, Q_4^-)} = \mathbb{F}_q[Q_{40}, Q_{41}, Q_{42}, \frac{f(Q_{40}, Q_{41}, Q_{42}, Q_{43})}{g(Q_{40}, Q_{41}, Q_{42})}],$$

for some polynomials f and g.

We also describe the Nagata's lemma here which we need later.

Theorem 1.6. *(Nagata) If x is a prime element of an integral domain R, and if a prime Q not containing x is principal in $R[x^{-1}]$, then Q is principal. In particular, if $R[x^{-1}]$ is factorial, then R is factorial.*