UDC 512.5

Jizhu Nan, Yufang Qin (Dalian Univ. Technology, China)

ON INVARIANTS OF ROOT SUBGROUPS OF FINITE CLASSICAL GROUPS *

ПРО ІНВАРІАНТИ КОРЕНЕВИХ ПІДГРУП СКІНЧЕННИХ КЛАСИЧНИХ ГРУП

We show that invariant fields $F_q(X_1,\ldots,X_n)^G$ are purely transcendental over F_q if G are root subgroups of finite classical groups. The key step is to find good similar groups of our groups. Moreover, the invariant rings of the root subgroups of special linear groups are shown to be polynomial rings, and their corresponding Poincaré series are presented.

Показано, що інваріантні поля $F_q(X_1,\ldots,X_n)^G$ є чисто трансцендентними над F_q, якщо G — кореневі підгрупи скінченних класичних груп. Ключовим місцем доведення є знаходження гарних подібних груп для наших груп. Крім того, показано, що інваріантні кільця кореневих підгруп спеціальних лінійних груп є поліноміальними кільцями. Також наведено відповідні ряди Пуанкаре.

1. Introduction. Let F_q be a finite field with char$F_q = p$, and $GL(n,F_q)$ be the general linear group. For any $T=(t_{ij})\in GL(n,F_q)$, it induces an F_q-linear action σ_T on the rational function field $F_q(X_1,\ldots,X_n)$ defined by

$$\sigma_T(f(X_1,\ldots,X_n)) = f(\sigma_T(X_1),\ldots,\sigma_T(X_n))$$

for all $f(X_1,\ldots,X_n)\in F_q(X_1,\ldots,X_n)$, where

$$\sigma_T(X_i) = t_{i1}X_1 + t_{i2}X_2 + \ldots + t_{in}X_n, \quad i=1,2,\ldots,n.$$

For a group $G\le GL(n,F_q)$, Noether's problem asks whether the rational invariant field

$$F_q(X_1,\ldots,X_n)^G = \big\{f\in F_q(X_1,\ldots,X_n)\colon \sigma_T(f)=f \ \text{ for all } \ T\in G\big\}$$

is purely transcendental over F_q.

When $G=GL(n,F_q)$, Dickson [1] gave an affirmative answer by giving the explicit transcendental bases. Chu [6] considered the invariant fields of finite orthogonal groups and obtained similar results for $n=2,3$. Cohen [7] showed the result is true when $n=4$, and finally the general case was settled by Carlisle and Kropholler [8]. But they all assumed that the characteristic of F_q is odd. The case of characteristic two was settled by Rajaei [12] using quadratic form language and by Tang and Wan [14] using matrix methods. Relatively recently, Chu [10] gave a unified treat on finding the transcendental bases of the invariant fields of some finite classical groups of the form

$$G_{A_\rho} = \big\{Q\in GL(n,F_q)\colon Q'AQ^\rho = A\big\},$$

where $A\in GL(n,F_q)$ and ρ is an automorphism of F_q.

In the paper, we consider the root subgroups of finite classical groups by giving explicit transcendental bases. The key of our method is to find good similar groups of root subgroups and consequently obtain the explicit transcendental bases through studying the similar groups.

* Supported by the National Natural Science Foundation of China.

Based on our results on the invariant fields of root subgroups of the special linear groups, we show that the invariant rings of root subgroups of the special linear groups are polynomial rings and consequently derive the Poincaré series of these invariant rings. In the modular case, examples of groups whose invariant rings are polynomial rings are, to name a few, the general and special linear groups $GL(n, F_q)$ and $SL(n, F_q)$ [1], the group of unipotent upper triangular matrices $G \leq$ $\leq GL(n, F_q)$ [5], the orthogonal and unitary groups $O(n, K, S)$ and $U(n, K, H)$ for $n \leq 3$ and $n \leq 2$, respectively [4], and the complex reflection groups G_{29} and G_{31} of Shephard and Todd [2]. Also, the root subgroup of the special linear group is such an example.

Let us recall the definitions of the root subgroups of classical groups [11]. In these definitions, denote by K an arbitrary field.

The *root subgroup* of the special linear group $SL(n, K)$ is the subgroup $\widetilde{X}_{ij} = \{T_{ij}(c)\colon c \in K\}$ $(i \neq j)$ or its conjugate subgroup in $GL(n, K)$, where $T_{ij}(c) = I + cE_{ij}$ and E_{ij} is the $(n \times n)$-matrix with the (i, j)-entry 1 and other entries 0. We denote the root subgroup $P^{-1}\widetilde{X}_{ij}P$ of $SL(n, K)$ by $X_{ij,P}$ with $P \in GL(n, K)$.

Assume that K has an involutive automorphism $\phi\colon a \mapsto \bar{a}$. The unitary group $U(n, K, H)$ is defined to be the group $\{A \in GL(n, K)\colon AH\bar{A}' = H\}$, where

$$H = \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ -I^{(\nu)} & 0 & 0 \\ 0 & 0 & H_0 \end{pmatrix}$$

is the congruence normal form of the nonsingular Hermitian matrix and $H_0 \in GL(n - 2\nu, K)$ is a definite diagonal matrix.

The *long root subgroup* of $U(n, K, H)$ is the subgroup

$$T_u = \{I + H\bar{u}'su\colon s \in \mathrm{Tr}K\},$$

where u is a fixed n-dimensional row vector satisfying $uH\bar{u}' = H$ and $\mathrm{Tr}K = \{a + \bar{a}\colon a \in K\}$. And the *short root subgroup* of $U(n, K, H)$ is

$$T_{u,w} = \big\{I + H\bar{w}'au + H(\overline{au})'w\colon a \in K\},$$

where u, w are noncollinear n-dimensional row vectors satisfying $uH\bar{u}' = wH\bar{w}' = uH\bar{w}' = 0$.

Let $\mathrm{char}K \neq 2$. The orthogonal group $O(n, K, S)$ is defined to be the group $\{A \in GL(n, K)\colon$ $ASA' = S\}$, where

$$S = \begin{pmatrix} 0 & I^{(\nu)} & 0 \\ I^{(\nu)} & 0 & 0 \\ 0 & 0 & \Delta \end{pmatrix}$$

is the congruence normal form of the nonsingular symmetric matrix and $\Delta \in GL(n - 2\nu, K)$ is a definite symmetric matrix. The *long root subgroup* of $O(n, K, S)$ is

$$Y_{u,w} = \{I + Sw'au - Sau'w\colon a \in K\},$$

where u, w are noncollinear n-dimensional row vectors satisfying $uSu' = wSw' = uSw' = 0$. The element of $Y_{u,w}$ is also called an orthogonal 2-transvection. The *short root subgroup* of $O(n, K, S)$ is

$$\widehat{Y}_{u,w} = \{I + Sw'au - Sau'(w + Q(w)au) \colon a \in K\},$$

where u, w are noncollinear n-dimensional row vectors satisfying $uSu' = uSw' = 0$ and $wSw' = 2Q(w) \neq 0$, Q is a quadratic form on the n-dimensional vector space over K. For the definitions of the long root subgroups and short root subgroups of symplectic groups the reader is referred to [11].

2. Invariant fields of root subgroups of the special linear groups over finite fields. In this section, we give the explicit transcendental bases of invariant fields of root subgroups of the special linear groups over finite fields. First of all, we prove a lemma which is very useful in the paper.

Lemma 2.1. *Let $K[X_1, \ldots, X_n]$ be the polynomial ring over an arbitrary field K. Assume that $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$ are algebraically independent over K, then for any $P = (p_{ij}) \in GL(n, K)$, $\sigma_P(f_1), \ldots, \sigma_P(f_n) \in K[X_1, \ldots, X_n]$ are algebraically independent over K.*

Proof. Since for any $P \in GL(n, K)$,

$$\det\begin{pmatrix} \dfrac{\partial\sigma_P(f_1(X_1,\ldots,X_n))}{\partial X_1} & \ldots & \dfrac{\partial\sigma_P(f_1(X_1,\ldots,X_n))}{\partial X_n} \\ \vdots & & \vdots \\ \dfrac{\partial\sigma_P(f_n(X_1,\ldots,X_n))}{\partial X_1} & \ldots & \dfrac{\partial\sigma_P(f_n(X_1,\ldots,X_n))}{\partial X_n} \end{pmatrix} =$$

$$= \det\begin{pmatrix} \dfrac{\partial f_1\left(\sum_{i=1}^n p_{1i}X_i, \ldots, \sum_{i=1}^n p_{ni}X_i\right)}{\partial X_1} & \ldots & \dfrac{\partial f_1\left(\sum_{i=1}^n p_{1i}X_i, \ldots, \sum_{i=1}^n p_{ni}X_i\right)}{\partial X_n} \\ \vdots & & \vdots \\ \dfrac{\partial f_n\left(\sum_{i=1}^n p_{1i}X_i, \ldots, \sum_{i=1}^n p_{ni}X_i\right)}{\partial X_1} & \ldots & \dfrac{\partial f_n\left(\sum_{i=1}^n p_{1i}X_i, \ldots, \sum_{i=1}^n p_{ni}X_i\right)}{\partial X_n} \end{pmatrix} =$$

$$= \det\begin{pmatrix} \sum_{i=1}^n p_{i1}f_{1i} & \ldots & \sum_{i=1}^n p_{in}f_{1i} \\ \vdots & & \vdots \\ \sum_{i=1}^n p_{i1}f_{ni} & \ldots & \sum_{i=1}^n p_{in}f_{ni} \end{pmatrix} = \det\begin{pmatrix} f_{11} & \ldots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \ldots & f_{nn} \end{pmatrix} \det(P) =$$

$$= \det\begin{pmatrix} \dfrac{\partial f_1(X_1,\ldots,X_n)}{\partial X_1} & \ldots & \dfrac{\partial f_1(X_1,\ldots,X_n)}{\partial X_n} \\ \vdots & & \vdots \\ \dfrac{\partial f_n(X_1,\ldots,X_n)}{\partial X_1} & \ldots & \dfrac{\partial f_n(X_1,\ldots,X_n)}{\partial X_n} \end{pmatrix} \det(P) \neq 0,$$

where $f_{ij} = \dfrac{\partial f_i(Y_1,\ldots,Y_n)}{\partial Y_j}$ if we let $Y_i = \sum_{l=1}^n p_{il}X_l$. It follows that $\sigma_P(f_1), \ldots, \sigma_P(f_n) \in K[X_1, \ldots, X_n]$ are algebraically independent over K.

Lemma 2.1 is proved.

Now we pay attention to discussing the root subgroup $X_{i_0j_0,P}$ of the special linear group. For convenience, we set $i_0 > j_0$.

Theorem 2.1. *Let $f_i = X_i$ for $1 \le i \le n$, $i \ne i_0$, $f_{i_0} = X_{i_0}X_{j_0}^{q-1} - X_{i_0}^q$ and $g_i = \sigma_{P^{-1}}(f_i)$ for $1 \le i \le n$. Then we have $F_q(X_1,\ldots,X_n)^{X_{i_0j_0,P}} = F_q(g_1,g_2,\ldots,g_n)$.*

Proof. It is clear that

$$\det\left(\frac{\partial f_i}{\partial X_j}\right)_{1\le i,j\le n} \ne 0,$$

whence $g_1,g_2,\ldots,g_n$ are algebraically independent over F_q by Lemma 2.1.

Suppose that $F_q(X_1,\ldots,X_n)$ is Galois over $F_q(f_1,\ldots,f_n)$ with Galois group G_1. We claim that $G_1 = \widetilde{X}_{i_0j_0}$. The inclusion $\widetilde{X}_{i_0j_0} \subset G_1$ is trivial. Conversely, for any $Q = (q_{ij}) \in G_1$, the assumption σ_Q leaves f_1 invariant implies that $q_{11} = 1$ and $q_{12} = \ldots = q_{1n} = 0$. Similarly, we know that $q_{ii} = 1$ and $q_{ij} = 0$, for $1 \le i \ne j \le n$ and $i \ne i_0$. Furthermore, σ_Q leaves f_{i_0} invariant, i.e., $\left(\sum_{k=1}^n q_{i_0k}X_k\right)\left(\sum_{k=1}^n q_{j_0k}X_k\right)^{q-1} - \sum_{k=1}^n q_{i_0k}X_k^q = X_{i_0}X_{j_0}^{q-1} - X_{i_0}^q$, which shows that $q_{i_0i_0} = 1$, $q_{i_0j_0}$ is arbitrary and $q_{i_0j} = 0$ for $j \ne i_0, j_0$. Hence $G_1 \subset \widetilde{X}_{i_0j_0}$, and this proves the claim.

Let $F_q(X_1,\ldots,X_n)$ be Galois over $F_q(g_1,\ldots,g_n)$ with Galois group G_2. To prove the theorem, it suffices to prove that $X_{i_0j_0,P} = G_2$. For any $Q = P^{-1}TP \in X_{i_0j_0,P}$ with $T \in \widetilde{X}_{i_0j_0}$, the fact σ_T leaves $f_1,\ldots,f_n$ invariant implies that σ_Q leaves $g_1,\ldots,g_n$ invariant. Consequently, $X_{i_0j_0,P} \subset G_2$. For the inverse inclusion, since for every $Q \in G_2$, σ_Q leaves $g_1,\ldots,g_n$ invariant, i.e., $\sigma_Q(g_i) = g_i$ and $\sigma_{PQP^{-1}}(f_i) = f_i (1 \le i \le n)$, we conclude that $PQP^{-1} \in \widetilde{X}_{i_0j_0}$ by the previous claim. Hence, $Q \in X_{i_0j_0,P}$ and $X_{i_0j_0,P} \subset G_2$, as required.

Theorem 2.1 is proved.

***Remark* 2.1.** (1) Let us present two examples to understand Theorem 2.1. When $P = I$, $X_{i_0j_0,I} = \widetilde{X}_{i_0j_0}$. Then $F_q(X_1,\ldots,X_n)^{X_{i_0j_0,I}} = F_q(X_1,\ldots,X_{i_0}X_{j_0}^{q-1} - X_{i_0}^q,\ldots,X_n)$; Assume that $P = (p_{ij}) \in GL(3,F_q)$ and $P^{-1} = (r_{ij})$. By Theorem 2.1, we know that $F_q(X_1,X_2,X_3)^{X_{21,P}} =$ $= F_q(r_{11}X_1 + r_{12}X_2 + r_{13}X_3, (r_{21}X_1 + r_{22}X_2 + r_{23}X_3)(r_{11}X_1 + r_{12}X_2 + r_{13}X_3)^{q-1} - (r_{21}X_1 +$ $+ r_{22}X_2 + r_{23}X_3)^q, r_{31}X_1 + r_{32}X_2 + r_{33}X_3)$.

(2) For any two root subgroups $X_{i_0j_0,P_1}$ and $X_{i_0j_0,P_2}$ with $1 \le i_0 \ne j_0 \le n$, if $F_q(X_1,\ldots,X_n)^{X_{i_0j_0,P_1}} = F_q(h_1,h_2,\ldots,h_n)$, then $F_q(X_1,\ldots,X_n)^{X_{i_0j_0,P_2}} = F_q(\sigma_{T^{-1}}(h_1),\ldots$ $\ldots,\sigma_{T^{-1}}(h_n))$ with $P_2 = P_1T$.

(3) More generally, if a group $G \le GL(n,K)$ satisfies $G = Q\widetilde{G}Q^{-1}$ with Q a fixed inverse $(n\times n)$-matrix, then the transcendental basis of the invariant field of $\widetilde{G}$ reduces a transcendental basis of the invariant field of our group G.

(4) If we let $\tilde{f}_i = X_i$ for $1 \le i \le n$, $i \ne i_0$, $\tilde{f}_{i_0} = \prod_{c\in F_q}(cX_{j_0} + X_{i_0})$ and $\tilde{g}_i = \sigma_{P^{-1}}\tilde{f}_i$ for $1 \le i \le n$, then following arguments similar to Theorem 2.1 we can prove that $\tilde{g}_1,\ldots,\tilde{g}_n$ form a second transcendental basis of $F_q(X_1,\ldots,X_n)^{X_{i_0j_0,P}}$ over F_q.

3. Invariant fields of root subgroups of finite unitary, orthogonal and symplectic groups. In this section, we begin with discussing the long root subgroups of finite unitary groups. Let us define polynomials

$$P_{nk} = \big(X_1, \ldots, X_n\big) H \begin{pmatrix} X_1^{q^{2k+1}} \\ \vdots \\ X_n^{q^{2k+1}} \end{pmatrix} = \sum_{1 \le i,j \le n} h_{ij} X_i X_j^{q^{2k+1}}, \quad k = 0, 1, \ldots .$$

Before we prove the main result on the long root subgroup of $U(n, K, H)$, we need the following lemmas.

Lemma 3.1 [10]. *For $Q \in GL(n, F_q)$, the following statements are equivalent*:

(1) $Q \in U(n, F_q, H)$;

(2) σ_Q *fixes* P_{nk} *for all* k;

(3) σ_Q *fixes* P_{nk} *for some* $k \ge 1$.

Lemma 3.2 [3]. *If X and Y are $(m \times n)$-matrices with rank m, then there exists a unitary matrix $U \in U(n, K, H)$ such that $X = UY$ if and only if $XH\bar{X}' = YH\bar{Y}'$.*

Remark **3.1.** The analogues of Lemmas 3.1, 3.2 for orthogonal and symplectic groups are also true (see [3, 10]).

Lemma 3.3 [3]. *Any unitary transvection in $U(n, K, H)$ can be represented as $I + H\bar{u}'su$, where $uH\bar{u}' = 0$ and $\bar{s} = s$. And any unitary transvection is unitary similar to the normal form*

$$\begin{pmatrix} I^{(\nu)} & & \\ K & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix}, \tag{3.1}$$

where

$$K = \begin{pmatrix} s & \\ & 0^{(\nu-1)} \end{pmatrix}.$$

By Lemma 3.3, there exists a unitary matrix R such that

$$R^{-1}(I + H\bar{u}'su)R = \begin{pmatrix} I^{(\nu)} & & \\ K & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix}, \tag{3.2}$$

where

$$K = \begin{pmatrix} s & \\ & 0^{(\nu-1)} \end{pmatrix}$$

and the matrix R is independent on s. Let $\widetilde{T_u}$ be the group consisting of all the matrices of the form (3.2). Then we have that $T_u = R\widetilde{T_u}R^{-1}$ and $\widetilde{T_u}$ is the similar group of T_u for which we are searching.

Lemma 3.4. *Let $f_2 = \sum_{1 \le i,j \le n} h_{ij} X_i X_j^{q^3}$, $f_{\nu+1} = X_{\nu+1} X_1^{q-1} - X_{\nu+1}^q$ and $f_i = X_i$ for all $1 \le i \le n$, $i \ne 2, \nu+1$. Then we have $F_q(X_1, \ldots, X_n)^{\widetilde{T_u}} = F_q(f_1, f_2, \ldots, f_n)$.*

Proof. It is trivial that $f_1, f_2, \ldots, f_n$ are algebraically independent over F_q by the fact

$$\det\left(\frac{\partial f_i}{\partial X_j}\right)_{1 \le i,j \le n} \ne 0.$$

Suppose that $F_q(X_1, \ldots, X_n)$ is Galois over $F_q(f_1, \ldots, f_n)$ with Galois group G. We only need to prove that $G = \widetilde{T}_u$. The inclusion $\widetilde{T}_u \subset G$ is obvious. Conversely, for any $Q \in G$, one can easily conclude that $p_{ii} = 1$ and $p_{ij} = 0$ $(1 \le i, j \le n, i \ne 2, \nu+1, i \ne j)$ from the fact that σ_Q leaves f_i $(1 \le i \le n,\ i \ne 2, \nu+1)$.

Moreover, σ_Q leaves $f_{\nu+1}$ invariant, i.e., $(p_{\nu+1,1}X_1 + \ldots + p_{\nu+1,n}X_n)X_1^{q-1} - (p_{\nu+1,1}X_1 + \ldots \ldots + p_{\nu+1,n}X_n)^q = X_{\nu+1}X_1^{q-1} - X_{\nu+1}^q$, then we know that $p_{\nu+1,j} = 0$ for $2 \le j \le n, j \ne \nu+1$ and $p_{\nu+1,\nu+1} = 1$. According to Lemma 3.1, the fact σ_Q leaves f_2 invariant shows that $Q \in U(n, F_q, H)$, which implies that $p_{22} = 1$, $p_{2j} = 0$ $(j \ne 2)$ and $p_{\nu+1,1} = \bar{p}_{\nu+1,1}$. Therefore, we have that $Q \in \widetilde{T}_u$ and $G = \widetilde{T}_u$.

Lemma 3.4 is proved.

From Lemmas 3.1, 3.3 and 3.4, we deduce the following theorem.

Theorem 3.1. *Let f_i, $1 \le i \le n$, be as in Lemma* 3.4 *and $g_i = Rf_i$ for $1 \le i \le n$. Then we have $F_q(X_1, \ldots, X_n)^{T_u} = F_q(g_1, g_2, \ldots, g_n)$.*

Proof. By Lemmas 2.1 and 3.4, we know that $g_1, \ldots, g_n$ are algebraically independent over F_q.

Suppose that $F_q(X_1, \ldots, X_n)$ is Galois over $F_q(g_1, \ldots, g_n)$ with Galois group G. According to Lemmas 3.3 and 3.4, we have that $G = T_u$ by using the same arguments as in Theorem 2.1, and the proof of this theorem is complete.

Now we come to the short root subgroup $T_{u,w}$ of $U(n, K, H)$. By the normal form of $T_{u,w}$, we obtain the similar group of $T_{u,w}$.

Lemma 3.5. *The element $I + H\bar{w}'au + H(\overline{au})'w$ of the short root subgroup $T_{u,w}$ is unitary similar to the normal form*

$$\begin{pmatrix} I^{(\nu)} & & \\ K & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix}, \tag{3.3}$$

where

$$K = \begin{pmatrix} 0 & a & \\ \bar{a} & 0 & \\ & & 0^{(\nu-2)} \end{pmatrix}.$$

Proof. We represent the matrix $I + H\bar{w}'au + H(\overline{au})'w$ as the following form:

$$I + H\big((\overline{au})', \bar{w}'\big)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} au \\ w \end{pmatrix}. \tag{3.4}$$

Observe that

$$\begin{pmatrix} au \\ w \end{pmatrix} H\big((\overline{au})', \bar{w}'\big) = 0$$

from the conditon that $uH\bar{u}' = wH\bar{w}' = uH\bar{w}' = 0$. Clearly,

$$\begin{pmatrix} a & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \end{pmatrix} H \begin{pmatrix} a & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \end{pmatrix}' = 0.$$

So by Lemma 3.2, there exists a unitary matrix R_0 such that

$$\begin{pmatrix} au \\ w \end{pmatrix} = \begin{pmatrix} a & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \end{pmatrix} R_0. \tag{3.5}$$

Substituting (3.5) into (3.4), we get

$$R_0(I + H\bar{w}'au + H(\overline{au})'w)R_0^{-1} = \begin{pmatrix} I^{(\nu)} & & \\ K & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix},$$

where

$$K = \begin{pmatrix} 0 & a & \\ \bar{a} & 0 & \\ & & 0^{(\nu-2)} \end{pmatrix}.$$

Lemma 3.5 is proved.

***Remark* 3.2.** In Lemma 3.5, it is proved that there exists a unitary matrix R_0 such that $R_0(I + H\bar{w}'au + H(\overline{au})'w)R_0^{-1}$ has the form (3.3). We remark that the matrix R_0 here is independent on the choice of a.

Theorem 3.2. *Let* $f_{\nu+1} = X_{\nu+1}X_2^{q-1} - X_{\nu+1}^q$, $f_{\nu+2} = \sum h_{ij}X_iX_j^{q^3}$ *and* $f_i = X_i$ *for all* $1 \leq i \leq n, i \neq \nu{+}1, \nu{+}2$. *Let* $g_i = R_0^{-1}f_i$ *with* $1 \leq i \leq n$. *Then we have that* $F_q(X_1, \ldots, X_n)^{T_{u,w}} = F_q(g_1, g_2, \ldots, g_n)$.

Proof. Similar to the proof of Theorem 3.1.

In the following, let us pay attention to the discussion of the long root subgroups and the short root subgroups of the finite orthogonal groups.

Lemma 3.6 [3]. *Any orthogonal* 2*-transvection is orthogonal similar to the following normal form*:

$$\begin{pmatrix} I^{(\nu)} & & \\ K & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix}, \tag{3.6}$$

where

$$K = \begin{pmatrix} 0 & 1 & \\ -1 & 0 & \\ & & 0^{(\nu-2)} \end{pmatrix}.$$

Lemma 3.7. *The element $I + Sw'au - Sau'(w + Q(w)au)$ of the short root subgroup $\widehat{Y}_{u,w}$ is orthogonal similar to the normal form*

$$\begin{pmatrix} K_2 & & & \\ & I^{(\nu-2)} & & \\ K_1 & & K_3 & \\ & & & I^{(n-\nu-2)} \end{pmatrix}, \tag{3.7}$$

where

$$K_1 = \begin{pmatrix} 0 & -aQ(w) \\ -aQ(w) & -a^2Q(w) \end{pmatrix}, \qquad K_2 = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \qquad \text{and} \qquad K_3 = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}.$$

Proof. We prove the normal form of $I + Sw'au - Sau'(w + Q(w)au)$ through considering the normal form of its transpose matrix. Note that $I + au'wS - (aw' + a^2Q(w)u')uS$ can be written as

$$I + \left(w', u'\right) \begin{pmatrix} 0 & -a \\ a & -a^2Q(w) \end{pmatrix} \begin{pmatrix} w \\ u \end{pmatrix} S.$$

Let

$$T = \begin{pmatrix} Q(w) & 0 & 0^{(1,\nu-2)} & 1 & 0^{(1,\nu-1)} & 0^{(n-2\nu)} \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then we have

$$TST' = \begin{pmatrix} 2Q(w) & 0 \\ 0 & 0 \end{pmatrix}.$$

Moreover,

$$\begin{pmatrix} w \\ u \end{pmatrix} S \begin{pmatrix} w \\ u \end{pmatrix}' = \begin{pmatrix} 2Q(w) & 0 \\ 0 & 0 \end{pmatrix}$$

from the assumption that $uSu' = uSw' = 0$ and $wSw' = 2Q(w)$. So by Remark 3.1 there exists an orthogonal matrix R_2 such that

$$\begin{pmatrix} w \\ u \end{pmatrix} = TR_2.$$

Consequently, we know that

$$R_2^{\prime -1} \left[I + \left(w', u'\right) \begin{pmatrix} 0 & -a \\ a & -a^2Q(w) \end{pmatrix} \begin{pmatrix} w \\ u \end{pmatrix} S \right] R_2' = \begin{pmatrix} K_2' & & K_1' & \\ & I^{(\nu-2)} & & \\ & & K_3' & \\ & & & I^{(n-\nu-2)} \end{pmatrix}, \tag{3.8}$$

where

$$K_1' = \begin{pmatrix} 0 & -aQ(w) \\ -aQ(w) & -a^2Q(w) \end{pmatrix}, \qquad K_2' = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \qquad \text{and} \qquad K_3' = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}.$$

Taking the transpose of both sides of equality (3.8), then we have that $I+Sw'au-Sau'(w+Q(w)au)$ is orthogonal similar to

$$\begin{pmatrix} K_2 & & & \\ & I^{(\nu-2)} & & \\ K_1 & & K_3 & \\ & & & I^{(n-\nu-2)} \end{pmatrix},$$

as desired.

Lemma 3.7 is proved.

By Lemma 3.6, there exists an orthogonal matrix R_1 such that

$$R_1^{-1}(I + Sw'au - Sau'w)R_1 = \begin{pmatrix} I^{(\nu)} & & \\ K & I^{(\nu)} & \\ & & I^{(n-2\nu)} \end{pmatrix},$$

where

$$K = \begin{pmatrix} 0 & a & \\ -a & 0 & \\ & & 0^{(\nu-2)} \end{pmatrix}.$$

Using similar arguments as in the proof of Theorem 3.1, we get the following theorem. The details are omitted.

Theorem 3.3. (1) *Let* $f_{\nu+1} = X_{\nu+1}X_2^{q-1} - X_{\nu+1}^q$, $f_{\nu+2} = \sum s_{ij}X_iX_j^q$ *and* $f_i = X_i$ *for all* $1 \leq i \leq n, i \neq \nu+1, \nu+2$. *Assume that* $g_i = R_1 f_i$ *with* $1 \leq i \leq n$. *Then we have* $F_q(X_1, \ldots, X_n)^{Y_{u,w}} = F_q(g_1, g_2, \ldots, g_n)$.

(2) *Let* $f_1 = X_1X_2^{q-1} - X_1^q$, $f_{\nu+1} = X_{\nu+1}X_2^{q-1} - X_{\nu+1}^q$, $f_{\nu+2} = \sum s_{ij}X_iX_j^q$ *and* $f_i = X_i$ *for all* $1 \leq i \leq n-1$, $i \neq 1, \nu+1, \nu+2$. *Assume that* $g_i = R_2^{-1} f_i$ *with* $1 \leq i \leq n$. *Then we have* $F_q(X_1, \ldots, X_n)^{\widehat{Y}_{u,w}} = F_q(g_1, g_2, \ldots, g_n)$.

Remark **3.3.** Note that the techniques we use can be applied to the case of the root subgroups of finite sympletic groups.

4. Invariant rings of root subgroups of the special linear groups over finite fields and Poincaré series. In the section, we show that the invariant rings of the root subgroups $X_{i_0j_0,P}$ of the special linear groups over finite fields are polynomial rings, and we give the Poincaré series of the invariant rings $F_q[X_1, \ldots, X_n]^{X_{i_0j_0,P}}$.

Here is an algorithm to check if the invariant ring is a polynomial ring.

Lemma 4.1 [9]. *Let* I *be the invariant ring of a finite group* $G \leq GL(n, K)$ *over an arbitrary field* K *and* $f_1, \ldots, f_n \in I$ *be homogeneous invariants of degrees* $d_1, \ldots, d_n$. *Then the following statements are equivalent*:

(1) $I = K[f_1, \ldots, f_n]$;

(2) $f_1, f_2, \ldots, f_n$ *are algebraically independent over* K *and* $\prod_{i=1}^{n} d_i = |G|$.

Theorem 4.1. *Let* $g_1, \ldots, g_n$ *and* $\tilde{g}_1, \ldots, \tilde{g}_n$ *be as in Theorem* 2.1 *and in Remark* 2.1. *Then* $F_q[X_1, \ldots, X_n]^{X_{i_0 j_0, P}} = F_q[g_1, g_2, \ldots, g_n] = F_q[\tilde{g}_1, \tilde{g}_2, \ldots, \tilde{g}_n]$.

Proof. This assertion follows form Lemma 4.1 and the fact

$$|X_{i_0 j_0, P}| = \prod_{i=1}^{n} \deg(g_i) = \prod_{i=1}^{n} \deg(\tilde{g}_i) = q.$$

Theorem 4.1 is proved.

Let $M = K[x_1, \ldots, x_n]$ be a polynomial ring over an arbitrary field with $\deg(x_i) = k_i$. Then the Poincaré series of M is equal to $\prod_{i=1}^{n} \dfrac{1}{1 - t^{k_i}}$ (see [13], Ch. 16.1, Ch. 7.1). From this assertion and Theorem 4.1, we have the following theorem.

Theorem 4.2. *The Poincaré series of the invariant ring* $F_q[X_1, \ldots, X_n]^{X_{i_0 j_0, P}}$ *of the root subgroup* $X_{i_0 j_0, P}$ *is equal to*

$$\frac{1}{(1-t)^{n-1}(1-t^q)}.$$

1. *Dickson L. E.* A fundamental system of invariants of the general modular linear group with a solution of the form problem // Trans. Amer. Math. Soc. – 1911. – **12**. – P. 75 – 98.
2. *Shephard G. C., Todd J. A.* Finite unitary reflection groups // Can. J. Math. – 1954. – **6**. – P. 274 – 304.
3. *Hua L. G., Wan Z. X.* Classical groups (in Chinese). – Shanghai: Shanghai Sci. and Technology Press, 1963.
4. *Nakajima H.* Invariants of finite groups generated by pseudo-reflections in positive characteristic // Tsukuba J. Math. – 1979. – **3**. – P. 109 – 122.
5. *Wilkerson C.* A primer on the Dickson invariants // Amer. Math. Soc. Contemp. Math. – 1983. – **19**. – P. 421 – 434.
6. *Chu H.* Orthogonal group actions on rational function fields // Bull. Inst. Math. Acad. Sinica. – 1988. – **16**. – P. 115 – 122.
7. *Cohen S. D.* Rational function invariant under an orthogonal group // Bull. London Math. Soc. – 1990. – **22**. – P. 217 – 221.
8. *Carlisle D., Kropholler P. H.* Rational invariants of certain orthogonal and unitary groups // Bull. London Math. Soc. – 1992. – **24**. – P. 57 – 60.
9. *Kemper G.* Calculating invariant rings of finite groups over arbitrary fields // J. Symb. Comput. – 1996. – **21**. – P. 351 – 366.
10. *Chu H.* Suplementary note on ‘rational invariants of certain orthogonal and unitary groups’ // Bull. London Math. Soc. – 1997. – **29**. – P. 37 – 42.
11. *Li S. Z.* Subgroup structure of classical groups (in Chinese). – Shanghai: Shanghai Sci. and Technical Publ., 1998.
12. *Rajaei S. M.* Rational invariants of certain orthogonal groups over finite fields of characteristic two // Communs Algebra. – 2000. – **28**. – P. 2367 – 2393.
13. *Kane R.* Reflection groups and invariant theory // CMS Books in Math. – New York: Springer-Verlag, 2001.
14. *Tang Z. M., Wan Z. X.* A matrix approach to the rational invariants of certain classical groups over finite fields of characteristic two // Finite Fields and their Appl. – 2006. – **12**. – P. 186 – 210.
15. *Nan J. Z., Chen Y.* Rational invariants of certain classical similitude groups over finite fields // Indiana Univ. Math. J. – 2008. – **4**. – P. 1947 – 1958.

Received 08.03.12