Czechoslovak Mathematical Journal, 67 (142) (2017), 655–698

INVARIANTS OF FINITE GROUPS GENERATED BY GENERALIZED TRANSVECTIONS IN THE MODULAR CASE

Xiang Han, Jizhu Nan, Dalian, † Chander K. Gupta, Winnipeg

Received February 2, 2016. First published July 12, 2017.

Abstract. We investigate the invariant rings of two classes of finite groups $G \leqslant \mathrm{GL}(n, F_q)$ which are generated by a number of generalized transvections with an invariant subspace H over a finite field F_q in the modular case. We name these groups generalized transvection groups. One class is concerned with a given invariant subspace which involves roots of unity. Constructing quotient groups and tensors, we deduce the invariant rings and study their Cohen-Macaulay and Gorenstein properties. The other is concerned with different invariant subspaces which have the same dimension. We provide a explicit classification of these groups and calculate their invariant rings.

Keywords: invariant ring; transvection; generalized transvection group

MSC 2010: 13A50, 20F55, 20F99

1. Introduction

Let F_q be a finite field, where $q = p^\nu$, $\nu \in Z^+$. Suppose that $x_1, \ldots, x_n \in V = F_q^n$ form a basis and $z_1, \ldots, z_n \in V^*$ form the dual basis to $\{x_1, \ldots, x_n\}$. We denote by $F_q[V]$ the graded algebra of polynomial functions on V, which is defined to be the symmetric algebra on V^*. Hence $F_q[V] = F_q[z_1, \ldots, z_n]$. If G is a finite group, and $\varrho\colon\ G \hookrightarrow \mathrm{GL}(n, F_q)$ is a representation of G over F_q, then, via ϱ, G acts on the left of the vector space $V = F_q^n$. A central theme in invariant theory is the study of the induced action on the algebra of polynomial functions $F_q[V]$ on V. This action arises from the left action of G on V^* defined by $(g \cdot z)(v) = z(\varrho(g)^{-1} \cdot v)$ for $g \in G,\ z \in V^*$, and $v \in V$, and its extensions to $S^m(V^*)$, the mth symmetric power of V^*, which fit together to give a left G-action on $F_q[V]$ by algebra automorphisms. By definition,

Project supported by the National Natural Science Foundation of China (Grant No. 11371343).

DOI: 10.21136/CMJ.2017.0044-16

the *ring of invariants* [17], denoted by $F_q[V]^G$, is

$$F_q[V]^G = \{f \in F_q[V] \colon\ g \cdot f = f,\ \forall\, g \in G\}.$$

This is a graded subalgebra of $F_q[V]$.

In this paper, we are mainly concerned with the invariant rings of two classes of groups $G \leqslant \mathrm{GL}(n, F_q)$ generated by generalized transvections and some related properties over a finite field F_q. In this case, the order of group G is divisible by the characteristic of the field F_q. Here are the two classes of groups $G \leqslant \mathrm{GL}(n, F_q)$:

$$\begin{cases} (1)\ G \text{ with a given invariant subspace and several roots of unity} \\ \quad \text{(Section 2 and 3)}, \\ (2)\ G \text{ with different invariant subspaces which have the same dimension} \\ \quad \text{(Section 4)}. \end{cases}$$

The definitions of the two classes of groups will be introduced in the sequel.

Nakajima in [13] introduces pseudo-reflections and transvections. In addition, he studies finite groups $G \subseteq \mathrm{GL}(V)$ whose rings of invariants are polynomial in the modular case when $n = 2$ (see [13]) and when G are p-groups over a prime field $F = F_p$ (see [15]). Kemple, Malle in [11] determine finite irreducible subgroups G of $\mathrm{GL}(V)$ such that $F[V]^G$ are polynomial rings in the modular case. Neusel, Smith in [16] also study transvections. They adopt a method associated with configurations of hyperplanes and calculate several invariant rings of groups which are polynomial and an invariant ring of a group which is Cohen-Macaulay.

If an invariant ring fails to be polynomial, people usually study its Cohen-Macaulay and Gorenstein properties. Hochster, Eagon in [9] show that in the non-modular case if a finite group G acts on a Cohen-Macaulay ring R then R^G is Cohen-Macaulay. In the modular case, although an invariant ring R^G in three or fewer variables is Cohen-Macaulay (see [18]), it may fail to be Cohen-Macaulay in more variables even if R is Cohen-Macaulay. Bertin in [2] gives such a counter-example with lowest possible dimension, the regular representation of the group $Z/4$ over a field of characteristic 2. In fact, Campbell at al. in [5] prove that a class of vector invariant rings $F[\bigoplus_m V]^P$ is not Cohen-Macaulay if $m \geqslant 3$ for any finite p-groups P in the modular case. For the sake of Gorenstein property, Bass in [1] studies and concludes several results. In the non-modular case, Stanley in [20] and Bruns and Herzog in [4] prove that every subgroup of the special linear group $\mathrm{SL}(n, F)$ is Gorenstein. In the modular case, Braun in [3] proves that if a group G contains no pseudo-reflection, then $F_q[V]^G$ is Gorenstein. And we in [8] indicate that an invariant ring $F_q[V]^G$ is Gorenstein when the definition of the group G involves a root of unity.

A plan of this paper follows. In the remainder of this section, we list the main results in this paper and illustrate terminology used in the sequel. In the second section, we study properties of i-transvections and determine the invariant rings of groups generated by i-transvections with a given invariant subspace. Constructing quotient groups and tensors is the key ingredient in the approach applied in this section. In the third section, we investigate the invariant rings of groups generated by (ω, i)-transvections with two roots of unity and their Cohen-Macaulay and Gorenstein properties. Then we extend these results to a generalization in which the groups are generated by (ω, i)-transvections with several roots of unity. In the fourth section, we consider the groups with different invariant subspaces which have the same dimension. Before computing invariant rings, we need to figure out the structures of these groups. Hence we provide a classification of them.

Below is a list of our main results in this paper.

(1) In Theorem 3.2, we determine the invariant ring $F_q[V]^{G(\omega_1,\omega_2)}$ of the group $G(\omega_1, \omega_2)$ where ω_1 and ω_2 are two roots of unity.

(2) In Proposition 3.8 and Proposition 3.11, we prove that the invariant ring $F_q[V]^{G(\omega_1,\omega_2)}$ is Cohen-Macaulay, and indicate the conditions for it to be Gorenstein.

(3) In Theorem 3.14, we extend the result in Theorem 3.2 to a generalization which involves several roots of unity.

(4) In Theorem 4.5, we consider the groups G with different invariant subspaces which have the same dimension. We determine the structures of these groups. There are totally four kinds of such groups up to isomorphism.

(5) In Proposition 4.9, Proposition 4.11, Proposition 4.12 and Proposition 4.15, we calculate the invariant rings of these four kinds of groups, respectively.

(6) In Proposition 4.14, we discuss a property of the Dickson polynomials $d_{n,0}, \ldots, d_{n,n-1}$: $\sqrt[q-1]{d_{n,0}} = d_{n,0}^{1/(q-1)} \in F_q[V]$ but other $d_{n,r}^{1/(q-1)} \notin F_q[V]$ for $r = 1, \ldots, n-1$.

Next, we begin with a short review of some basic definitions concerning invariant and pseudo-reflection as a preliminary to introducing i-transvections and i-reflections which will be needed in this paper. We adopt the definitions from [22] and [13].

Definition 1.1 ([22]). Given an element $T \in \mathrm{GL}(n, F_q)$, we denote the dimension of the subspace $\mathrm{Im}(I-T) \subset V$ by $\mathrm{Res}(T)$. Hence the dimension of the subspace $\mathrm{Ker}(I-T)$ is equal to $(n - \mathrm{Res}(T))$.

In a finite group $G \subseteq \mathrm{GL}(V)$, a pseudo-reflection $T \in G$ satisfies equality $\dim(\mathrm{Im}(I-T)) = 1$ (see [13]), i.e., $\mathrm{Res}(T) = 1$. A pseudo-reflection $T \neq I$ is called a *transvection* (see [13]) if $T|_{(I-T)V} = I$, and a *reflection* (see [13]) if $T|_{(I-T)V} = -I$. Similarly, we define i-transvection and i-reflection.

Definition 1.2. Denote the floor of a number a by $[a]$. Let $T \in \mathrm{GL}(n, F_q)$ satisfy $\mathrm{Res}(T) = i$ where $1 \leqslant i \leqslant [n/2]$. Then T is called an *i-transvection* if $T|_{(I-T)V} = I$, and an *i-reflection* if $T|_{(I-T)V} = -I$. A subspace $H \subset V = F_q^n$ is called the *invariant subspace* of T if $H = \mathrm{Ker}(I - T)$, and the subspace $L = \mathrm{Im}(I - T) \subset V$ is called the *line subspace* of T.

Remark. (1) Given an i-transvection T with the invariant subspace H and the line subspace L, since $T|_{(I-T)V} = I$ and $(I - T)V = \mathrm{Im}(I - T)$, it yields that $\mathrm{Im}(I - T) \subseteq \mathrm{Ker}(I - T)$, i.e., $L \subseteq H$.

(2) In Lemma 2.8, after obtaining the matrix form of i-transvection, we find that the definition of i-transvection is invalid for $[n/2] < i \leqslant n - 1$. Hence we will extend it to $[n/2] < i \leqslant n - 1$ in Definition 2.9.

Definition 1.3. We denote the group generated by all i-transvections with the same invariant subspace H by $G_{i,H}^+$. The space H is called the *invariant subspace* of the group $G_{i,H}^+$.

Note. For convenience, $G_{i,H}^+$ is briefly denoted by G_i^+ in the sequel.

At the end of this section, we introduce several important invariants and propositions which will be frequently used in this paper. First, we introduce the Dickson algebra.

Definition 1.4 ([17], Lemma 6.1.1)**.** Let F_q be the Galois field with q elements and $V = F_q^n$ the n-dimensional vector space over F_q. Set $\Phi_n(X) = \prod_{z \in V^*} (X + z) \in F_q[V][X]$. Then $\Phi_n(X)$ is q-polynomial, in the sense that $\Phi_n(X) = \sum_{i=0}^{n} (d_{n,i} X^{q^i})$. $d_{n,0}, \ldots, d_{n,n}$ are called the *Dickson polynomials* with degrees $\deg(d_{n,i}) = (q^n - q^i)$ for $i = 0, \ldots, n$. $L = d_{n,0}^{1/(q-1)}$ is called the *Euler class*. The ring $F_q[d_{n,0}, \ldots, d_{n,n-1}]$ is called the *Dickson algebra*. Notice that $d_{n,n} = 1$.

The formulas of the Dickson polynomials are provided in [17], Theorem 6.1.7. And we shall make use of them in Section 4.

Next, we list the definition of the top Chern class.

Definition 1.5 ([17], page 79)**.** Let V be a finite dimensional representation of a finite group G and $B \subset V$ an orbit. Set $C_{\mathrm{top}}(B) = \prod_{v \in B} (v)$, which is called the *top Chern class* of B.

In this paper we concentrate on a special case which has a close relation with the Dickson polynomials. Let $\{z_1, \ldots, z_n\}$ be a basis for V^* and G a finite group. If the orbit of z_j is $\{z_j + \lambda_1 z_{t_1} + \ldots + \lambda_i z_{t_i} \colon \lambda_1, \ldots, \lambda_i \in F_q\}$ where $j, t_1, \ldots, t_i \in \{1, \ldots, n\}$

are distinct, then its cardinality is equal to q^i. Referring to [17], Theorem 6.1.7, its top Chern class is

$$C_{\text{top}}(z_j) = z_j^{q^i} + \sum_{r=0}^{i-1}(d_{i,r} \cdot z_j^{q^r}),$$

where $d_{i,r}$ is the Dickson polynomial in $z_{t_1}, \ldots, z_{t_i}$ with degree $q^i - q^r$ for $r = 0, \ldots, i-1$. Since $C_{\text{top}}(z_j)$ is q-polynomial, we substitute $C_{q^i}(z_j)$ for $C_{\text{top}}(z_j)$ in this case.

A system of parameters (see [17]) for an algebra A over the field F is a finite set of algebraically independent elements $h_1, \ldots, h_n$ in A such that the ring extension $F[h_1, \ldots, h_n] \subseteq A$ is finite. The following proposition states a method to determine the polynomial rings of invariants.

Proposition 1.6 ([17], Proposition 4.5.5)**.** *Let $G \hookrightarrow \mathrm{GL}(n, F)$ be a representation of a finite group G over the field F. Suppose $F[V]^G$ contains a system of parameters $f_1, \ldots, f_n$ such that $\deg(f_1) \ldots \deg(f_n) = |G|$. Then $F[V]^G \cong F[f_1, \ldots, f_n]$.*

2. The properties of i-transvections and invariants of the group G_i^+

The properties of 1-transvections, i.e., transvections, are studied in [17]. In this section, we extend the results to i-transvections for $i = 1, \ldots, n-1$. Then we compute the invariant ring $F_q[V]^{G_i^+}$ of the group G_i^+ and introduce a related group $G_i(\omega)$ where ω is a root of unity.

Let $T \in \mathrm{GL}(n, F_q)$ be an i-transvection and $x_1, \ldots, x_i \in \mathrm{Im}(I - T)$ linearly independent vectors. So $x_1, \ldots, x_i$ form a basis of $\mathrm{Im}(I - T)$. Then

$$T\colon V \to V$$
$$v \to v + \varphi_1(v) \cdot x_1 + \ldots + \varphi_i(v) \cdot x_i,$$

where

$$\varphi\colon V \to F_q^i$$
$$v \to (\varphi_1(v), \ldots, \varphi_i(v)).$$

The linearity of T entails the linearity of φ. Notice that $\mathrm{Ker}(\varphi) = \mathrm{Ker}(I - T)$.

The following lemma is simple but important.

Lemma 2.1. *Let T be an i-transvection, $\{x_1, \ldots, x_i\}$ a basis of the subspace $\mathrm{Im}(I-T) \subset V$, and $\varphi = (\varphi_1, \ldots, \varphi_i)\colon V \to F_q^i$ a nonzero linear map associated with T as defined above. If $v = \sum_{j=1}^{i}(k_j x_j) \in \mathrm{Im}(I-T)$, where $k_1, \ldots, k_i \in F_q$, then $\varphi_1(v) = \ldots = \varphi_i(v) = 0$.*

P r o o f. Since T is an i-transvection, $T|_{(I-T)V} = I$. Since $v = \sum_{j=1}^{i}(k_j x_j) \in \mathrm{Im}(I-T) = (I-T)V$, it follows that

$$\sum_{j=1}^{i}(k_j x_j) = v = T(v) = v + \sum_{l=1}^{i}(\varphi_l(v) \cdot x_l),$$

i.e.,

$$\sum_{l=1}^{i}(\varphi_l(v) \cdot x_l) = 0.$$

Since $x_1, \ldots, x_i$ are linearly independent, the result follows. □

Definition 2.2. Let $x_1, \ldots, x_i$ be vectors (not required to be linearly independent), and $\varphi = (\varphi_1, \ldots, \varphi_i)$ a nonzero linear map from V to F_q^i with $\varphi_l(x_j) = 0$ for all $1 \leqslant l, j \leqslant i$. Define a linear transformation

$$t(\varphi, x_1, \ldots, x_i)\colon V \to V$$
$$v \to v + \varphi_1(v) \cdot x_1 + \ldots + \varphi_i(v) \cdot x_i.$$

Notice $t(\varphi, 0, \ldots, 0) = I$.

Lemma 2.3. *Let $\varphi = (\varphi_1, \ldots, \varphi_i)\colon V \to F_q^i$ be a nonzero linear map with $\mathrm{Ker}(\varphi) = H$.*

(1) If T is an i-transvection with the invariant subspace $H = \mathrm{Ker}(I-T)$ and the line subspace $L = \mathrm{Im}(I-T) \subseteq H$, then there exists a unique basis $\{x_1, \ldots, x_i\}$ of L such that $T = t(\varphi, x_1, \ldots, x_i)$ with $\varphi_l(x_j) = 0$ for all $1 \leqslant l, j \leqslant i$.

(2) If $\{x_1, \ldots, x_i\}$ is a basis of some i-dimensional subspace $L \subseteq H$, then there exist a unique i-transvection T with the invariant subspace $H = \mathrm{Ker}(I-T)$ and the line subspace $L = \mathrm{Im}(I-T)$ such that $T = t(\varphi, x_1, \ldots, x_i)$ with $\varphi_l(x_j) = 0$ for all $1 \leqslant l, j \leqslant i$.

P r o o f. (1) Since $\varphi = (\varphi_1, \ldots, \varphi_i)\colon V \to F_q^i$ is a linear map with $\mathrm{Ker}(\varphi) = H = \mathrm{Ker}(I-T)$, there exists a basis $\{x_1, \ldots, x_i\}$ of $L = \mathrm{Im}(I-T)$ such that

$$T(v) = v + \sum_{l=1}^{i}(\varphi_l(v) \cdot x_l) = t(\varphi, x_1, \ldots, x_i)(v),$$

where $\varphi_l(x_j) = 0$ for all $1 \leqslant l,\ j \leqslant i$ by the definition of T, Lemma 2.1 and Definition 2.2. Suppose that $x_1, \ldots, x_{n-i}$ span H and $x_1, \ldots, x_n$ span V. Then

$$T(x_j) = \begin{cases} x_j & \text{if } j \leqslant n-i, \\ x_j + \sum\limits_{1 \leqslant l \leqslant i} (c_{jl} x_l) & \text{if } j > n-i. \end{cases}$$

The matrix $C = (c_{jl})_{i \times i}$ is invertible since $H = \mathrm{Ker}(I - T)$. Similarly, the restriction of φ to the span of $x_{n-i+1}, \ldots, x_n$ gives another invertible matrix $B = (\varphi(x_{n-i+1}), \ldots, \varphi(x_n))^t$. This implies a unique basis $B^{-1}C(x_1, \ldots, x_i)^t$ satisfying the result.

(2) It is straightforward to check that $T = t(\varphi, x_1, \ldots, x_i)$ is the unique i-transvection with the invariant subspace $H = \mathrm{Ker}(I - T)$ and the line subspace $L = \mathrm{Im}(I - T)$. □

Recall that $L = \mathrm{Im}(I - T) \subseteq H = \mathrm{Ker}(I - T)$ for an i-transvection T. According to Lemma 2.3, we can see that if a nonzero linear map $\varphi = (\varphi_1, \ldots, \varphi_i)$ is given with $\mathrm{Ker}(\varphi) = H$, then an i-transvection T with this invariant subspace H is in one-to-one correspondence to a basis $\{x_1, \ldots, x_i\}$ of a subspace of H. Since the group G_i^+ is generated by all i-transvections with the same invariant subspace H, it is sufficient to study bases of subspaces of H instead of i-transvections when we study the generators of G_i^+. Before the study of generators, we collect some elementary properties of i-transvections and the construction of $t(\varphi, x_1, \ldots, x_i)$.

Lemma 2.4. *Let $\varphi\colon V \to F_q^i$ be a nonzero linear map, $T_1 = t(\varphi, x_1, \ldots, x_i)$ and $T_2 = t(\varphi, y_1, \ldots, y_i)$ two i-transvections with the same invariant subspace $H = \mathrm{Ker}(\varphi)$. Suppose that $\{x_1, \ldots, x_i\}$ is a basis of the line subspace of T_1 and $\{y_1, \ldots, y_i\}$ is a basis of the line subspace of T_2 with $\varphi_l(x_j) = \varphi_l(y_j) = 0$ for all $1 \leqslant l,\ j \leqslant i$. Then*

$$\begin{aligned} t(\varphi, x_1, \ldots, x_i) \cdot t(\varphi, y_1, \ldots, y_i) &= t(\varphi, x_1 + y_1, \ldots, x_i + y_i) \\ &= t(\varphi, y_1, \ldots, y_i) \cdot t(\varphi, x_1, \ldots, x_i), \end{aligned}$$

i.e., $T_1 T_2(v) = T_2 T_1(v)$ for all $v \in V$.

P r o o f. According to Definition 2.2, we derive

$$\begin{aligned} &t(\varphi, x_1, \ldots, x_i)(t(\varphi, y_1, \ldots, y_i)(v)) \\ &\qquad = t(\varphi, x_1, \ldots, x_i)\Big(v + \sum_{l=1}^{i} (\varphi_l(v) \cdot y_l)\Big) \\ &\qquad = \Big(v + \sum_{j=1}^{i} (\varphi_j(v) \cdot x_j)\Big) + \sum_{l=1}^{i} \Big(\varphi_l(v) \cdot \Big(y_l + \sum_{j=1}^{i} (\varphi_j(y_l) \cdot x_j)\Big)\Big) \end{aligned}$$

$$= \left(v + \sum_{j=1}^{i}(\varphi_j(v)\cdot x_j)\right) + \sum_{l=1}^{i}(\varphi_l(v)\cdot y_l)$$
$$= v + \sum_{j=1}^{i}(\varphi_j(v)\cdot(x_j+y_j)) = t(\varphi, x_1+y_1,\dots,x_i+y_i)(v).$$

□

Lemma 2.5. *Let $\varphi = (\varphi_1,\dots,\varphi_i)\colon V \to F_q^i$ be a nonzero linear map, $T = t(\varphi, x_1,\dots,x_i)$ an i-transvection with the invariant subspace $H = \mathrm{Ker}(\varphi)$ and $\varphi_l(x_j) = 0$ for all $1 \leqslant l, j \leqslant i$. Denote by $F_q^* = F_q \setminus \{0\}$ the multiplication group of the field F_q. Then*

$$t(a\varphi, x_1,\dots,x_i) = t(\varphi, ax_1,\dots,ax_i), \quad a \in F_q^*.$$

P r o o f. According to Definition 2.2, the formula follows from the following computation:

$$t(a\varphi, x_1,\dots,x_i)(v) = v + \sum_{l=1}^{i}(a\varphi_l(v)\cdot x_l)$$
$$= v + \sum_{l=1}^{i}(\varphi_l(v)\cdot ax_l) = t(\varphi, ax_1,\dots,ax_i)(v).$$

□

We emphasize that two i-transvections with the same invariant subspace H may generate a k-transvection for some $k < i$. For example, let $\varphi = (\varphi_1,\varphi_2)\colon V \to F_q^2$ be a nonzero linear map, $T_1 = t(\varphi, x, y_1)$ and $T_2 = t(\varphi, -x, y_2)$ two 2-transvections where $y_1 + y_2 \neq 0$. Notice that they have the same invariant subspace $H = \mathrm{Ker}(\varphi)$. However, $T_1T_2 = t(\varphi, 0, y_1+y_2)$, which is a 1-transvection. Besides, the invariant subspace H' of $T_1T_2 = t(\varphi, 0, y_1+y_2)$ contains the common invariant subspace H of T_1 and T_2. In fact, $t(\varphi, 0, y_1+y_2) = t(\varphi', y_1+y_2)$ where $\varphi' = \varphi_2\colon V \to F_q$ is a nonzero linear map. Hence $\mathrm{Ker}(\varphi) \subset \mathrm{Ker}(\varphi')$, i.e., $H \subseteq H'$.

Recall that the group G_i^+ with an invariant subspace H are generated by all i-transvections with the same invariant subspace H in Definition 1.3. The preceding discussion can be generalized in the following lemma.

Lemma 2.6. *Let $\varphi = (\varphi_1,\dots,\varphi_i)\colon V \to F_q^i$ be a nonzero linear map, and $H = \mathrm{Ker}(\varphi)$ a subspace of V. If a k-transvection $T' = t(\varphi, x_1',\dots,x_i')$ with an invariant subspace H' is an element in the group G_i^+ with the invariant subspace H for some $0 \leqslant k \leqslant i$, then*

(1) $H \subseteq H'$;
(2) *the vectors* $x'_1, \ldots, x'_i \in H$;
(3) *and* $T'^{-1} = t(\varphi, -x'_1, \ldots, -x'_i)$.

P r o o f. Suppose that $T' = T_1 \ldots T_l \in G_i^+$, where $T_j = t(\varphi, x_1^j, \ldots, x_i^j) \in G_i^+$, is an i-transvection with the invariant subspace H for $j = 1, \ldots, l$. It follows that $x_1^j, \ldots, x_i^j \in H$ for all $j = 1, \ldots, l$. According to Lemma 2.4, $T' = t(\varphi, x'_1, \ldots, x'_i) = t\Big(\varphi, \sum\limits_{j=1}^{l} x_1^j, \ldots, \sum\limits_{j=1}^{l} x_i^j\Big)$, i.e., $x'_1 = \sum\limits_{j=1}^{l} x_1^j, \ldots, x'_i = \sum\limits_{j=1}^{l} x_i^j$. Hence $x'_1, \ldots, x'_i \in H$. Since $x'_1, \ldots, x'_i$ span a k-dimensional subspace for some $0 \leqslant k \leqslant i$, it follows that $H \subseteq H'$. If $T_1 T_2 = t(\varphi, 0, \ldots, 0) = I$, then $T_1^{-1} = T_2 = t(\varphi, -x'_1, \ldots, -x'_i)$ according to Definition 2.2. □

Remark. (1) It is easily seen that Lemma 2.4 and Lemma 2.5 both hold for all elements in the group G_i^+.

(2) A basis $\{x_1, \ldots, x_i\}$ of the line subspace L is ordered, i.e., the bases $\{x_1, \ldots, x_i\}$ and $\{x_{\sigma(1)}, \ldots, x_{\sigma(i)}\}$ are not the same if $1 \neq \sigma \in S_i$ where S_i is the symmetric group on i letters, since

$$\begin{aligned} t(\varphi, x_1, \ldots, x_i)(v) &= v + \sum_{l=1}^{i} (\varphi_l(v) \cdot x_l)) \\ &\neq v + \sum_{l=1}^{i} (\varphi_l(v) \cdot x_{\sigma(l)})) = t(\varphi, x_{\sigma(1)}, \ldots, x_{\sigma(i)})(v). \end{aligned}$$

A basis $\{x_1, \ldots, x_i\}$ of a subspace of H is in a one-to-one correspondence to an i-transvection T with the invariant subspace H if $\varphi = (\varphi_1, \ldots, \varphi_i)$ is given with $\mathrm{Ker}(\varphi) = H$ by Lemma 2.3. Therefore we can derive the following conclusion.

Proposition 2.7. *Let* F_q *be a finite field,* $q = p^\nu$, $\nu \in Z^+$, $V = F_q^n$ *a linear space,* $H \subset V$ *a subspace with* $\dim H = (n - i)$, *and* $\varphi = (\varphi_1, \ldots, \varphi_i)\colon V \to F_q^i$ *a given nonzero linear map with* $\mathrm{Ker}(\varphi) = H$. *If the group* G_i^+ *is generated by all* i*-transvections with the invariant subspace* H, *then the map*

$$\begin{gathered} \tau\colon \underbrace{H \times \ldots \times H}_{i \text{ copies}} \to G_i^+ \\ (x_1, \ldots, x_i) \mapsto t(\varphi, x_1, \ldots, x_i) \end{gathered}$$

is an isomorphism of groups. Therefore, G_i^+ *is an elementary abelian* p*-subgroup of the special linear group* $\mathrm{SL}(n, F_q)$ *and the order* $|G_i^+| = (q^{n-i})^i = q^{in-i^2}$.

P r o o f. The map τ is bijective by Lemma 2.3 and Lemma 2.6, and a homomorphism of groups by Lemma 2.4. Since F_q is a finite additive group with order $q = p^\nu$, $H \subset V = F_q^n$ is an elementary abelian p-group, so is G_i^+.

Since $\dim H = (n-i)$, we have $|H| = q^{n-i}$ and $|G_i^+| = (q^{n-i})^i = q^{in-i^2}$.

Let $\mathrm{Det}\colon G_i^+ \to F_q^*$ be the determinant homomorphism of groups. We denote by $|\mathrm{Det}(G_i^+)|$ the order of $\mathrm{Det}(G_i^+)$, then $|\mathrm{Det}(G_i^+)|$ divides $|G_i^+| = q^{in-i^2}$.

If $q = p = 2$, it follows that $\mathrm{Det}(G_i^+) = \{1\}$, so G_i^+ is a subgroup of $\mathrm{SL}(n, F_q)$.

In the other cases, we suppose that $G_i^+ \nsubseteq \mathrm{SL}(n, F_q)$, so $|\mathrm{Det}(G_i^+)| > 1$. Since $|\mathrm{Det}(G_i^+)|$ divides $|F_q^*| = q - 1$, it means that $|\mathrm{Det}(G_i^+)|$ is a nontrivial factor of $(q-1)$, which is a contradiction to that $|\mathrm{Det}(G_i^+)|$ divides $|G_i^+| = q^{in-i^2}$. Hence $G_i^+ \subset \mathrm{SL}(n, F_q)$. □

Given an element $z \in V^*$, we denote a subspace $W = \{v \in V\colon z \cdot v = 0\} \subset V$ by $\mathrm{Ker}\langle z\rangle$. In this section, we fix $H = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle$. Before turning to the invariant ring $F_q[V]^{G_i^+}$ of the group G_i^+, we must emphasize that $F_q[V]^{G_i^+}$ is relevant to the invariant subspace H. In fact, it depends only on H according to Definition 2.9 and Proposition 2.10. We will introduce the groups in Section 4 when H is unfixed.

In order to determine the structure of the invariant ring $F_q[V]^{G_i^+}$, let us consider the matrix forms of elements in the group G_i^+.

Lemma 2.8. *Let $H = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle$ be the invariant subspace of the group G_i^+. Suppose that $1 \leqslant i \leqslant [n/2]$. We denote by $\mathrm{Mat}_{n-i,i}(F_q)$ the vector space of $(n-i) \times i$ matrices over F_q. Then the matrices of elements in the group G_i^+ are of the form*

$$\begin{pmatrix} I_{n-i} & * \\ 0 & I_i \end{pmatrix}$$

where $* \in \mathrm{Mat}_{n-i,i}(F_q)$. Besides, all such matrices of elements are included in the group G_i^+.

P r o o f. Since $H = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle$, it is straightforward by Definition 1.2 and Proposition 2.7. □

Remark. The definition of the group G_i^+ is invalid for $[n/2] < i \leqslant n-1$ by Lemma 2.8 since the definition of $\mathrm{Res}(T) = i$ is invalid for $[n/2] < i \leqslant n-1$. Nevertheless, we find that if $H = \mathrm{Ker}\langle z_{t_1}, \ldots, z_{t_l}\rangle$ is the invariant subspace of an i-transvection T, then $i = l$ by Proposition 2.7. Hence we can extend the definitions of $\mathrm{Res}(T)$ and i-transvection as follows.

Definition 2.9. Let an element $T \in \mathrm{GL}(n, F_q)$ be isomorphic to the matrix form

$$\begin{pmatrix} I_{n-i} & A \\ 0 & I_i \end{pmatrix}$$

where $A \in \mathrm{Mat}_{n-i,i}(F_q)$ is of full column rank. Then $\mathrm{Ker}(I-T) = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle$. We denote the number i by $\mathrm{Res}(T)$. T is called an *i-transvection* and the subspace $H = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle$ is called the *invariant subspace* of T.

One can easily check that $\mathrm{Res}(T)$ is the same as in Definition 1.1 for $1 \leqslant i \leqslant [n/2]$ and it is valid for $[n/2] < i \leqslant n-1$.

According to Definition 2.9, we conclude that the elements in the group G_i^+ are all of the forms in Lemma 2.8 for all $1 \leqslant i \leqslant n-1$. Furthermore, the invariant ring is well defined for all $1 \leqslant i \leqslant n-1$ since it only depends on the matrix forms in the group G_i^+.

Now we are in a position to compute the invariant ring $F_q[V]^{G_i^+}$.

Proposition 2.10. *Let $C_{q^i}(z_j)$ be the top Chern class of z_j for $j = 1, \ldots, n-i$, which is defined in Definition* 1.5. *Then*

$$F_q[V]^{G_i^+} = F_q[C_{q^i}(z_1), \ldots, C_{q^i}(z_{n-i}), z_{n-i+1}, \ldots, z_n].$$

It is a polynomial algebra.

P r o o f. Referring to the matrix in Lemma 2.8, the top Chern class of z_j, $1 \leqslant j \leqslant n-i$, is

$$\begin{aligned} C_{q^i}(z_j) &= \prod_{\lambda_1,\ldots,\lambda_i \in F_q} (z_j + \lambda_1 z_{n-i+1} + \ldots + \lambda_i z_n) \\ &= z_j^{q^i} + \sum_{r=0}^{i-1} (d_{i,r} \cdot z_j^{q^r}), \end{aligned}$$

where $d_{i,r}$ is the Dickson polynomial in $z_{n-i+1}, \ldots, z_n$ with degree $q^i - q^r$ for $r = 0, \ldots, i-1$. Since $C_{q^i}(z_1), \ldots, C_{q^i}(z_{n-i}), z_{n-i+1}, \ldots, z_n$ form a system of parameters of $F_q[V]^{G_i^+}$, and $\deg(C_{q^i}(z_j)) = q^i$ for all $1 \leqslant j \leqslant n-i$, we have

$$|G_i^+| = q^{i(n-i)} = \prod_{j=1}^{n-i} \deg(C_{q^i}(z_j)) \cdot \prod_{t=n-i+1}^{n} \deg(z_t).$$

The result follows from Proposition 1.6. □

Remark. The invariant ring $F_q[V]^{G_i^+}$ is also given by Neusel, Smith in [16] and Nakajima in [13]. Neusel, Smith take an arrangement of hyperplanes, see [16], i.e., a set of hyperplanes $\{H_1, \ldots, H_l\}$, and consider the invariants of the stabilizer

and hyperplanewise stabilizer subgroup which is an isomorphic to the group G_i^+. Nakajima directly considers a group, see [13],

$$A(m,n:q)=\left\{\begin{pmatrix} I_m & M \\ 0 & I_n \end{pmatrix} :\ M\in \mathrm{Mat}_{n,m}(F_q)\right\},$$

which is an isomorphic to the group G_i^+. The work we present here is to show the properties of i-transvection.

Next, we consider a generalization of the results of Neusel, Smith and Nakajima.

Definition 2.11. Let $T\in \mathrm{GL}(n,F_q)$ satisfy $\mathrm{Res}(T)=i$ where $1\leqslant i\leqslant n-1$. Then T is called an (ω,i)-*transvection* if $T|_{(I-T)V}=\omega I$, where $\omega\in F_q$ is a kth root of unity. A subspace $H\subset V$ is called the *invariant subspace* of T if $H=\mathrm{Ker}(I-T)$ and the subspace $L=\mathrm{Im}(I-T)\subset V$ is called the *line subspace* of T.

Notice that an (ω,i)-transvection is an i-transvection if $\omega=1$, and an i-reflection if $\omega=-1$ according to Definition 1.2. Since $T|_{(I-T)V}=\omega I$, certainly the line subspace $L=\mathrm{Im}(I-T)$ is expanded ω-fold by T. We now indicate the matrix form of T.

Proposition 2.12. *Let $T\in \mathrm{GL}(n,F_q)$ be an (ω,i)-transvection with the invariant subspace $\mathrm{Ker}(I-T)=H=\mathrm{Ker}\langle z_{n-i+1},\dots,z_n\rangle\subset V$. Then the matrix form of T is*

$$\begin{pmatrix} I_{n-i} & A \\ 0 & \omega I_i \end{pmatrix}$$

where $A\in \mathrm{Mat}_{n-i,i}(F_q)$. Besides, if $\omega=1$, then A is of full column rank.

P r o o f. Since $\mathrm{Res}(T)=i$ and $H=\mathrm{Ker}\langle z_{n-i+1},\dots,z_n\rangle$, the matrix form of T is

$$\begin{pmatrix} I_{n-i} & A \\ 0 & B \end{pmatrix}$$

where $A\in \mathrm{Mat}_{n-i,i}(F_q)$ and $B\in \mathrm{GL}(i,F_q)$.

In addition, since $T|_{(I-T)V}=\omega I$, it is easy enough to figure out that $B=\omega I_i$.

If $\omega=1$, the result follows from Definition 2.9. □

Remark. If $\omega\neq 1$, then T is indeed an (ω,i)-transvection for any $A\in \mathrm{Mat}_{n-i,i}(F_q)$.

In [8], we calculate the invariant ring of a group generated by all these elements provided in Proposition 2.12. Here is the result.

Proposition 2.13 ([8], Theorem 3.2)**.** *Let $\omega \in F_q$ be a kth root of unity. We define a group*

$$G_i(\omega) = \left\langle \begin{pmatrix} I_{n-i} & * \\ & \omega I_i \end{pmatrix} : * \in \mathrm{Mat}_{n-i,i}(F_q) \right\rangle.$$

Then

$$F_q[V]^{G_i(\omega)} = \bigoplus_{\substack{m=0 \\ k|m}}^{i(k-1)} \left(\bigoplus_{\substack{l_1+\ldots+l_i=m \\ 0\leqslant l_1,\ldots,l_i\leqslant k-1}} (z_{n-i+1}^{l_1} \ldots z_n^{l_i}) \cdot M \right),$$

where $M = F_q[C_{q^i}(z_1), \ldots, C_{q^i}(z_{n-i}), z_{n-i+1}^k, \ldots, z_n^k]$.

We also present some properties of this invariant ring $F_q[V]^{G_i(\omega)}$ in the same article.

Proposition 2.14 ([8], Section 3)**.** *The invariant ring $F_q[V]^{G_i(\omega)}$ satisfies the following conditions.*

(1) *It is Cohen-Macaulay.*
(2) *It is Gorenstein if and only if $i = 1$ or $k \mid i$.*
(3) *It is a complete intersection if and only if* (i) *$i = 1$ or* (ii) *$i = 2$ and $k = 1, 2$.*

3. Groups generated by (ω, i)-transvections with two roots of unity

In this section, we shall calculate the invariant rings of groups generated by (ω, i)-transvections with two roots of unity. After that, we extend the result to a generalization.

Definition 3.1. Let ω_1, $\omega_2 \in F_q$ be two roots of unity with orders k_1 and k_2, respectively. Let

$$\Delta_{1,n_1}(\omega_1) = \left\{ \begin{pmatrix} \omega_1 I_{n_1} & * \\ 0 & I_{n_2} \end{pmatrix} : * \in \mathrm{Mat}_{n_1,n_2}(F_q) \right\}$$

and

$$\Delta_{2,n_2}(\omega_2) = \left\{ \begin{pmatrix} I_{n_1} & * \\ 0 & \omega_2 I_{n_2} \end{pmatrix} : * \in \mathrm{Mat}_{n_1,n_2}(F_q) \right\}$$

be two sets. Define a group $G_{n_1,n_2}(\omega_1, \omega_2) = \langle T : T \in \Delta_{1,n_1}(\omega_1) \cup \Delta_{2,n_2}(\omega_2) \rangle \subseteq \mathrm{GL}(n, F_q)$. One can easily check that its order is $|G_{n_1,n_2}(\omega_1, \omega_2)| = k_1 \cdot k_2 \cdot q^{n_1 n_2}$.

Note. For convenience, $G_{n_1,n_2}(\omega_1, \omega_2)$ is briefly denoted by $G(\omega_1, \omega_2)$.

Referring to the matrices in the generating set $\Delta_{1,n_1}(\omega_1) \cup \Delta_{2,n_2}(\omega_2)$ of the group $G(\omega_1, \omega_2)$, we can observe that the element $T \in G(\omega_1, \omega_2)$ is of the form

$$\begin{pmatrix} \omega_1^{j_1(T)} I_{n_1} & * \\ 0 & \omega_2^{j_2(T)} I_{n_2} \end{pmatrix},$$

where $j_1(T), j_2(T) \in Z$ are irrelevant to each other and $* \in \mathrm{Mat}_{n_1,n_2}(F_q)$.

Before computing the invariants, we introduce a notation for convenience. Let $X_1, \ldots, X_t$ be finite sets. Define a new set

$$X_1 \times \ldots \times X_t = \left\{ \prod_{i=1}^{t} x_i \colon\ x_i \in X_i \right\}.$$

Hence the cardinality of this set is equal to $\prod_{i=1}^{t} \mathrm{Card}(X_i)$ where $\mathrm{Card}(X_i)$ denotes the cardinality of the set X_i for $i = 1, \ldots, t$.

Now we calculate the invariant ring of the group $G(\omega_1, \omega_2)$.

Theorem 3.2. *The invariant ring of the group $G(\omega_1, \omega_2)$ is*

$$F_q[V]^{G(\omega_1,\omega_2)} = \bigoplus_{b \in K} b \cdot M,$$

where

$$M = F_q[C_{q^{n_2}}(z_1)^{k_1}, \ldots, C_{q^{n_2}}(z_{n_1})^{k_1}, z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2}],$$

and

$$K = \left\{ \bigcup_{\substack{m_1=0 \\ k_1 \mid m_1}}^{n_1(k_1-1)} \left\{ \bigcup_{\substack{l_1+\ldots+l_{n_1}=m_1 \\ 0 \leqslant l_1,\ldots,l_{n_1} \leqslant k_1-1}} \{C_{q^{n_2}}(z_1)^{l_1} \ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}\} \right\} \right\}$$
$$\times \left\{ \bigcup_{\substack{m_2=0 \\ k_2 \mid m_2}}^{n_2(k_2-1)} \left\{ \bigcup_{\substack{j_1+\ldots+j_{n_2}=m_2 \\ 0 \leqslant j_1,\ldots,j_{n_2} \leqslant k_2-1}} \{z_{n_1+1}^{j_1} \ldots z_{n_1+n_2}^{j_{n_2}}\} \right\} \right\}.$$

In the formulas, $C_{q^{n_2}}(z_j) = z_j^{q^{n_2}} + \sum_{r=0}^{n_2-1} (d_{n_2,r} \cdot z_j^{q^r})$ for $j = 1, \ldots, n_1$, and $d_{n_2,r}$ is the Dickson polynomial in $z_{n_1+1}, \ldots, z_{n_1+n_2}$ with degree $q^{n_2} - q^r$ for $r = 0, \ldots, n_2 - 1$.

Before embarking upon the proof of this theorem, we require a preliminary result.

Lemma 3.3. *Let J be a group generated by*

$$\begin{pmatrix} \omega_1 I_{n_1} & 0 \\ 0 & I_{n_2} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} I_{n_1} & 0 \\ 0 & \omega_2 I_{n_2} \end{pmatrix},$$

where ω_1, $\omega_2 \in F_q$ are two roots of unity with orders k_1 and k_2, respectively. Then

$$F_q[V]^J = \bigoplus_{b \in L} b \cdot N,$$

where

$$N = F_q[z_1^{k_1}, \ldots, z_{n_1}^{k_1}, z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2}],$$

and

$$L = \left\{ \bigcup_{\substack{m_1=0 \\ k_1 | m_1}}^{n_1(k_1-1)} \left\{ \bigcup_{\substack{l_1+\ldots+l_{n_1}=m_1 \\ 0 \leqslant l_1,\ldots,l_{n_1} \leqslant k_1-1}} \{ z_1^{l_1} \ldots z_{n_1}^{l_{n_1}} \} \right\} \right\}$$
$$\times \left\{ \bigcup_{\substack{m_2=0 \\ k_2 | m_2}}^{n_2(k_2-1)} \left\{ \bigcup_{\substack{j_1+\ldots+j_{n_2}=m_2 \\ 0 \leqslant j_1,\ldots,j_{n_2} \leqslant k_2-1}} \{ z_{n_1+1}^{j_1} \ldots z_{n_1+n_2}^{j_{n_2}} \} \right\} \right\}.$$

P r o o f. Every element $T \in J$ is of the form

$$\begin{pmatrix} \omega_1^{h_1(T)} I_{n_1} & 0 \\ 0 & \omega_2^{h_2(T)} I_{n_2} \end{pmatrix},$$

where $h_1(T), h_2(T) \in Z$ are irrelevant to each other.

It is easy enough to check that $z_1^{k_1}, \ldots, z_{n_1}^{k_1}$, $z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2}$ are all invariants and form a system of parameters of $F_q[V]^J$. We now computer other invariants.

Since every element $T \in J$ is a diagonal matrix, the action of T on $F_q[V]$ sends monomials to monomials. Suppose that $f = z_1^{l_1} \ldots z_{n_1}^{l_{n_1}} z_{n_1+1}^{j_1} \ldots z_{n_1+n_2}^{j_{n_2}}$ is an invariant but does not belong to $F_q[z_1^{k_1}, \ldots, z_{n_1}^{k_1}, z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2}]$. This yields that

$$f = T \cdot f = \omega_1^{(l_1+\ldots+l_{n_1})h_1(T)} \omega_2^{(j_1+\ldots+j_{n_2})h_2(T)} z_1^{l_1} \ldots z_{n_1}^{l_{n_1}} z_{n_1+1}^{j_1} \ldots z_{n_1+n_2}^{j_{n_2}}.$$

Hence

$$\omega_1^{(l_1+\ldots+l_{n_1})h_1(T)} \omega_2^{(j_1+\ldots+j_{n_2})h_2(T)} = 1 \in F_q,$$

where $0 \leqslant h_1(T) \leqslant k_1 - 1$ and $0 \leqslant h_2(T) \leqslant k_2 - 1$. Since this equation holds for every $T \in J$, on the one hand, setting $h_1(T) = 0$ and $h_2(T) = 1$, we deduce that $k_2 \mid j_1 + \ldots + j_{n_2}$; on the other hand, setting $h_1(T) = 1$ and $h_2(T) = 0$, we have that $k_1 \mid l_1 + \ldots + l_{n_1}$. Therefore, if f is an invariant and $f \notin F_q[z_1^{k_1}, \ldots, z_{n_1}^{k_1}, z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2}]$, then $k_1 \mid l_1 + \ldots + l_{n_1}$ and $k_2 \mid j_1 + \ldots + j_{n_2}$. The result follows. □

Reasoning as above, we now come to the proof of Theorem 3.2.

P r o o f of Theorem 3.2. Referring to Definition 1.3 and Lemma 2.8, the group

$$G_{n_2}^{+} = \left\langle \begin{pmatrix} I_{n_1} & * \\ & I_{n_2} \end{pmatrix} : * \in \mathrm{Mat}_{n_1,n_2}(F_q) \right\rangle$$

is generated by all n_2-transvections with the same invariant subspace $H = \mathrm{Ker}\langle z_{n_1+1}, \ldots, z_{n_1+n_2}\rangle$. In addition, it is a normal subgroup of the group $G(\omega_1, \omega_2)$ and $G(\omega_1, \omega_2)/G_{n_2}^{+} = J$, where the quotient group J is defined in Lemma 3.3. Consequently,

$$\begin{aligned} F_q[V]^{G(\omega_1,\omega_2)} &= (F_q[V]^{G_{n_2}^{+}})^{G(\omega_1,\omega_2)/G_{n_2}^{+}} \\ &= F_q[C_{q^{n_2}}(z_1), \ldots, C_{q^{n_2}}(z_{n_1}), z_{n_1+1}, \ldots, z_{n_1+n_2}]^J \\ &= \bigoplus_{b\in K} b \cdot M, \end{aligned}$$

where M and K are defined in Theorem 3.2. The second equation holds by Proposition 2.10 and the last equation holds by Lemma 3.3. □

Remark. If G is an abelian group which is generated by pseudo-reflections and $\mathrm{Syl}_p(G)$ is its p-Sylow subgroup, Nakajima in [14] proves that $F_p[V]^G$ is polynomial if and only if $F_p[V]^{\mathrm{Syl}_p(G)}$ is polynomial. This is no longer the case when G is non-abelian. For example, $G_{n_2}^{+}$ is the p-Sylow subgroup of the group $G(\omega_1, \omega_2)$, and $F_q[V]^{G_{n_2}^{+}}$ is polynomial by Proposition 2.10 but $F_q[V]^{G(\omega_1,\omega_2)}$ is not polynomial by Theorem 3.2.

Here we give an example to show what we have done.

Example 3.4. Let $p = 5$ and $q = p^2 = 25$. Suppose that $\{x_1, \ldots, x_5\}$ is a basis for $V = F_{25}^5$ and $\{z_1, \ldots, z_5\}$ is a dual basis for V^* to $\{x_1, \ldots, x_5\}$. Let ω_1, ω_2, $\omega_3 \in F_{25}$ be three roots of unity with order 2, 3 and 4, respectively. We construct two groups as follows:

$$\begin{aligned} G(\omega_1, \omega_2) &= \left\langle \begin{pmatrix} \omega_1 I_2 & * \\ 0 & I_3 \end{pmatrix}, \begin{pmatrix} I_2 & * \\ 0 & \omega_2 I_3 \end{pmatrix} : * \in \mathrm{Mat}_{2,3}(F_{25}) \right\rangle, \\ G(\omega_3, \omega_2) &= \left\langle \begin{pmatrix} \omega_3 I_2 & * \\ 0 & I_3 \end{pmatrix}, \begin{pmatrix} I_2 & * \\ 0 & \omega_2 I_3 \end{pmatrix} : * \in \mathrm{Mat}_{2,3}(F_{25}) \right\rangle. \end{aligned}$$

Notice that $n_1 = 2$ and $n_2 = 3$. Then referring to Theorem 3.2, we conclude that

$$F_{25}[V]^{G(\omega_1,\omega_2)} = \bigoplus_{b\in K} b \cdot M,$$

where

$$M = F_{25}[C_{25^3}(z_1)^2, C_{25^3}(z_2)^2, z_3^3, z_4^3, z_5^3],$$

$$K = \{1, C_{25^3}(z_1)C_{25^3}(z_2)\} \times \{1, z_3^2z_4, z_3^2z_5, z_3z_4^2, z_3z_4z_5, z_3z_5^2, z_4^2z_5, z_4z_5^2, z_3^2z_4^2z_5^2\}$$

and

$$F_{25}[V]^{G(\omega_3,\omega_2)} = \bigoplus_{b' \in K'} b' \cdot M',$$

where

$$\begin{aligned} M' &= F_{25}[C_{25^3}(z_1)^4, C_{25^3}(z_2)^4, z_3^3, z_4^3, z_5^3], \\ K' &= \{1, C_{25^3}(z_1)^3C_{25^3}(z_2), C_{25^3}(z_1)^2C_{25^3}(z_2)^2, C_{25^3}(z_1)C_{25^3}(z_2)^3\} \\ &\quad \times \{1, z_3^2z_4, z_3^2z_5, z_3z_4^2, z_3z_4z_5, z_3z_5^2, z_4^2z_5, z_4z_5^2, z_3^2z_4^2z_5^2\}. \end{aligned}$$

Since we have already got the invariant ring $F_q[V]^{G(\omega_1,\omega_2)}$, what increases the interest in, and the importance of our results, is the Cohen-Macaulay and Gorenstein properties. Next, we discuss these properties.

First of all, we prove that $F_q[V]^{G(\omega_1,\omega_2)}$ is Cohen-Macaulay. We need some preliminaries before stating a lemma used in the proof of Cohen-Macaulay property.

Definition 3.5 ([6], Definition 2.4.6)**.** Let F be a field and G a finite group. If $f_1, \ldots, f_r \in F[V]^G$ is a homogeneous system of parameters, then f_i is called *primary invariant*. Therefore the invariant ring $F[V]^G$ is a finite $F[f_1, \ldots, f_r]$-module, say

$$F[V]^G = Mg_1 + Mg_2 + \ldots + Mg_s,$$

where $M = F[f_1, \ldots, f_r]$ and $g_1, \ldots, g_s \in F[V]^G$ are homogeneous. The invariants $g_1, \ldots, g_s$ are called *secondary invariants*.

According to Definition 3.5, all primary invariants form a system of parameters for $F_q[V]^G$.

The next lemma allows us to determine whether an invariant ring is Cohen-Macaulay if we have known the primary and secondary invariants, even in the modular case.

Lemma 3.6 ([6], Theorem 3.7.1)**.** *Let F be a field and G a finite group. Assume that the action of G on V is faithful. Let $f_1, \ldots, f_n \in F[V]^G$ be primary invariants of degrees $d_1, \ldots, d_n$, and let $g_1, \ldots, g_m$ be a minimal system of secondary invariants. Then*

$$m \geqslant \frac{d_1 \ldots d_n}{|G|}$$

with equality if and only if $F[V]^G$ is Cohen-Macaulay.

Lemma 3.6 reduces the problem of proving Cohen-Macaulay properties to that of computing the degrees of primary invariants and counting the cardinality of a minimal system of secondary invariants.

Lemma 3.7. *In the invariant ring* $F_q[V]^{G(\omega_1,\omega_2)}$,

$$C_{q^{n_2}}(z_1)^{k_1},\dots,C_{q^{n_2}}(z_{n_1})^{k_1},z_{n_1+1}^{k_2},\dots,z_{n_1+n_2}^{k_2}\in M$$

are primary invariants and

$$K=\left\{\bigcup_{\substack{m_1=0\\ k_1|m_1}}^{n_1(k_1-1)}\left\{\bigcup_{\substack{l_1+\dots+l_{n_1}=m_1\\ 0\leqslant l_1,\dots,l_{n_1}\leqslant k_1-1}}\{C_{q^{n_2}}(z_1)^{l_1}\dots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}\}\right\}\right\}$$
$$\times\left\{\bigcup_{\substack{m_2=0\\ k_2|m_2}}^{n_2(k_2-1)}\left\{\bigcup_{\substack{j_1+\dots+j_{n_2}=m_2\\ 0\leqslant j_1,\dots,j_{n_2}\leqslant k_2-1}}\{z_{n_1+1}^{j_1}\dots z_{n_1+n_2}^{j_{n_2}}\}\right\}\right\}$$

is a minimal system of secondary invariants where M *and* K *are defined in Theorem* 3.2.

P r o o f. It is a direct conclusion by Theorem 3.2 and Definition 3.5. □

Now we come to the Cohen-Macaulay property.

Proposition 3.8. *With the preceding hypotheses and notation,* $F_q[V]^{G(\omega_1,\omega_2)}$ *is Cohen-Macaulay.*

P r o o f. $C_{q^{n_2}}(z_1)^{k_1},\dots,C_{q^{n_2}}(z_{n_1})^{k_1},z_{n_1+1}^{k_2},\dots,z_{n_1+n_2}^{k_2}$ are all primary invariants by Lemma 3.7. Moreover, $\deg(C_{q^{n_2}}(z_j)^{k_1})=k_1q^{n_2}$ for all $1\leqslant j\leqslant n_1$, and $\deg(z_i^{k_2})=k_2$ for all $n_1+1\leqslant i\leqslant n_1+n_2$. To complete the proof, it is sufficient to count the cardinality of the minimal system of secondary invariants K. For convenience, we introduce sets

$$A=\left\{\bigcup_{\substack{m_1=0\\ k_1|m_1}}^{n_1(k_1-1)}\left\{\bigcup_{\substack{l_1+\dots+l_{n_1}=m_1\\ 0\leqslant l_1,\dots,l_{n_1}\leqslant k_1-1}}\{C_{q^{n_2}}(z_1)^{l_1}\dots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}\}\right\}\right\},$$
$$B=\left\{\bigcup_{\substack{m_2=0\\ k_2|m_2}}^{n_2(k_2-1)}\left\{\bigcup_{\substack{j_1+\dots+j_{n_2}=m_2\\ 0\leqslant j_1,\dots,j_{n_2}\leqslant k_2-1}}\{z_{n_1+1}^{j_1}\dots z_{n_1+n_2}^{j_{n_2}}\}\right\}\right\}.$$

So $K = A \times B$ for short. We first count the cardinality of the set A. There exist $k_1^{n_1}$ elements $C_{q^{n_2}}(z_1)^{l_1} \ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}$ where $0 \leqslant l_1, \ldots, l_{n_1} \leqslant k_1 - 1$. In addition, it requires that

$$l_1 + \ldots + l_{n_1} = m_1 \equiv 0 \pmod{k_1},$$

hence $\mathrm{Card}(A) = k_1^{n_1 - 1}$ according to number theory. A similar argument applies to the set B for counting the cardinality, so $\mathrm{Card}(B) = k_2^{n_2 - 1}$. Therefore

$$\mathrm{Card}(K) = \mathrm{Card}(A) \cdot \mathrm{Card}(B) = k_1^{n_1 - 1} \cdot k_2^{n_2 - 1}.$$

With the preceding argument, this induces

$$\begin{aligned} \mathrm{Card}(K) = k_1^{n_1 - 1} \cdot k_2^{n_2 - 1} &= \frac{(k_1 \cdot q^{n_2})^{n_1} \cdot k_2^{n_2}}{k_1 \cdot k_2 \cdot q^{n_1 n_2}} \\ &= \frac{\Big(\prod_{j=1}^{n_1} \deg(C_{q^{n_2}}(z_j)^{k_1})\Big) \cdot \Big(\prod_{i=n_1+1}^{n_1+n_2} \deg(z_i^{k_2})\Big)}{|G(\omega_1, \omega_2)|}. \end{aligned}$$

The result follows from Lemma 3.6. □

Remark. Hochster and Eagon in [9] show that in the non-modular case if a finite group G acts on a Cohen-Macaulay ring R then R^G is Cohen-Macaulay. In this paper, Proposition 3.8 proves that in the modular case, the invariant ring $F_q[V]^{G(\omega_1, \omega_2)}$ is also Cohen-Macaulay.

Next, we discuss the Gorenstein property of $F_q[V]^{G(\omega_1, \omega_2)}$. If A is a Noetherian ring, a *parameter ideal*, see [17], for A is an ideal generated by a system of parameters for A. A commutative graded connected Noetherian algebra over a field is called *Gorenstein*, see [17], if it is Cohen-Macaulay and every parameter ideal is irreducible. We prove that it only depends on the numbers k_1, k_2, n_1 and n_2. To begin we need the following characterization of Gorenstein algebra.

Definition 3.9 ([17], page 124)**.** A commutative graded connected algebra A over a field F is called a *Poincaré duality algebra* of dimension d if

(i) $A_i = 0$ for $i > d$,

(ii) $\dim_F(A_d) = 1$,

(iii) the pairing $A_i \otimes_F A_{d-i} \to A_d$ given by multiplication is nonsingular. A nonzero element $[A]$ of A_d is referred to as a *fundamental class* for A.

Lemma 3.10 ([17], Corollary 5.7.4)**.** *Let A be a Noetherian commutative graded connected Cohen-Macaulay algebra of Krull dimension d and let $I \subset A$ be a parameter ideal. Then the following conditions are equivalent.*

(i) *A is Gorenstein.*

(ii) *A/I is a Poincaré duality algebra.*

Remark. If $R = F[x_1, \ldots, x_n]$ is a polynomial ring, then it is Gorenstein since taking $I = \langle x_1, \ldots, x_n \rangle$ as a parameter ideal we deduce that R/I is a field, so a Poincaré duality algebra.

Proposition 3.11. *For the invariant ring $F_q[V]^{G(\omega_1,\omega_2)}$, suppose ω_1, $\omega_2 \in F_q$ are two roots of unity with orders k_1 and k_2, respectively, and n $(= n_1 + n_2)$ is the size of matrix which is defined in Definition* 3.1*. Then the invariant ring $F_q[V]^{G(\omega_1,\omega_2)}$ is Gorenstein if and only if $n_j = 1$ or $k_j | n_j$ for $j = 1, 2$.*

P r o o f. (1) Suppose $n_1 = n_2 = 1$. Then

$$F_q[V]^{G(\omega_1,\omega_2)} = F_q[C_q(z_1)^{k_1}, z_2^{k_2}]$$

is a polynomial ring by Theorem 3.2. Hence $F_q[V]^{G(\omega_1,\omega_2)}$ is certainly Gorenstein.

(2) Suppose $n_1 \neq 1 = n_2$. To work with the Gorenstein property of $F_q[V]^{G(\omega_1,\omega_2)}$, it will suffice to obtain the information about the Poincaré duality algebra. So we take

$$I = \langle C_q(z_1)^{k_1}, \ldots, C_q(z_{n_1})^{k_1}, z_{n_1+1}^{k_2} \rangle$$

as a parameter ideal. We may therefore compute the fundamental class $[A]$ of $A = F_q[V]^{G(\omega_1,\omega_2)}/I$.

Let $F_q[V]^{G(\omega_1,\omega_2)}$ be Gorenstein. According to Definition 3.9, $[A]$ is a highest graded element in the Poincaré duality algebra A. And there exists no monomial $f \in A$ such that f and $[A]$ have the same grade and are F_q-linearly independent.

Notice that $[A]$ is of the form $C_q(z_1)^{l_1} \ldots C_q(z_{n_1})^{l_{n_1}}$. If $l_1, \ldots, l_{n_1}$ are not all equal, without loss of generality, let $l_1 > l_2$. Then $(C_q(z_1)^{l_1})(C_q(z_2)^{l_2})(C_q(z_3)^{l_3}) \ldots (C_q(z_{n_1})^{l_{n_1}})$ and $(C_q(z_1)^{l_2})(C_q(z_2)^{l_1})(C_q(z_3)^{l_3}) \ldots (C_q(z_{n_1})^{l_{n_1}})$ are F_q-linearly independent with the same grade. So there exist two different fundamental classes, which is a contradiction. Hence $l_1 = \ldots = l_{n_1}$.

Furthermore, since $[A]$ is the highest graded secondary invariant and $0 \leqslant l_1, \ldots, l_{n_1} \leqslant k_1 - 1$, we conclude that $l_1 = \ldots = l_{n_1} = k_1 - 1$ and that $\deg([A]) = \sum_{i=1}^{n_1} (l_i \cdot q) = n_1 \cdot (k_1 - 1) \cdot q$. Since $[A] \in A$, it follows that $k_1 | \deg([A])$, i.e., $k_1 | (n_1 \cdot (k_1 - 1) \cdot q)$. Notice that $\omega_1 \in F_q$ is a k_1th root of unity and $k_1 | (q - 1)$, hence we obtain $k_1 | n_1$. And the conclusion follows.

(3) Suppose $n_1 = 1 \neq n_2$. Then we take

$$I = \langle C_{q^{n_2}}(z_1)^{k_1}, z_2^{k_2}, \ldots, z_{1+n_2}^{k_2} \rangle$$

as a parameter ideal, it yields that $k_2 | n_2$ by an argument similar to Case (2).

(4) Finally, suppose $n_1 \neq 1 \neq n_2$. We take

$$I = \langle C_{q^{n_2}}(z_1)^{k_1}, \ldots, C_{q^{n_2}}(z_{n_1})^{k_1}, z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2} \rangle$$

as a parameter ideal, it yields that $k_1 | n_1$ and $k_2 | n_2$ by an argument similar to Case (2). Notice that the polynomial $C_{q^{n_2}}(z_1)^{k_1-1} \ldots C_{q^{n_2}}(z_{n_1})^{k_1-1} z_{n_1+1}^{k_2-1} \ldots z_{n_1+n_2}^{k_2-1}$ is the fundamental class of the Poincaré duality algebra $A = F_q[V]^{G(\omega_1,\omega_2)}/I$.

Conversely, suppose $n_1 \neq 1 \neq n_2$. We take

$$I = \langle C_{q^{n_2}}(z_1)^{k_1}, \ldots, C_{q^{n_2}}(z_{n_1})^{k_1}, z_{n_1+1}^{k_2}, \ldots, z_{n_1+n_2}^{k_2} \rangle$$

as a parameter ideal. It is easy enough to verify that $A = F_q[V]^{G(\omega_1,\omega_2)}/I$ is a Poincaré duality algebra according to Definition 3.9. Hence $F_q[V]^{G(\omega_1,\omega_2)}$ is Gorenstein.

The other cases are similar and thus omitted. □

Remark. In the non-modular case, Stanley in [20] and Bruns and Herzog in [4] prove that if $G \subset \mathrm{SL}(n, F_q)$, then $F[V]^G$ is Gorenstein. In Proposition 3.11, if $k_1 | n_1$ and $k_2 | n_2$, then $G \subset \mathrm{SL}(n, F_q)$. Hence we have proved a special case of their result in the modular case.

In view of the preceding discussion, we present an example with these properties.

Example 3.12. We continue to discuss Example 3.4.

(1) According to Proposition 3.8, the invariant rings $F_{25}[V]^{G(\omega_1,\omega_2)}$ and $F_{25}[V]^{G(\omega_3,\omega_2)}$ are both Cohen-Macaulay.

(2) Since $k_1 = n_1 = 2$ and $k_2 = n_2 = 3$, it follows that $k_1 | n_1$ and $k_2 | n_2$. Hence the invariant ring $F_q[V]^{G(\omega_1,\omega_2)}$ is Gorenstein by Proposition 3.11. However, the invariant ring $F_q[V]^{G(\omega_3,\omega_2)}$ is not Gorenstein since $k_3 = 4$ does not divide $n_1 = 2$.

In the remainder of this section, we consider the invariant ring of a group generated by (ω, i)-transvections with several roots of unity. The result is a straightforward extension of our previous result to the invariant ring of $G(\omega_1, \omega_2)$ and thus presented without proof.

Definition 3.13. Let $\omega_1, \ldots, \omega_l, \varrho_1, \ldots, \varrho_k \in F_q$ be $l+k$ roots of unity with orders $a_1, \ldots, a_l$, $b_1, \ldots, b_k$, respectively. Define sets of matrices

$$\Delta_{t,i_t}(\omega_t) = \left\{ \left(\begin{array}{ccc|ccc} I_{i_1} & & 0 & & & \\ & \ddots & & & & \\ \vdots & & \vdots & & * & \\ & \omega_t I_{i_t} & & & & \\ & & \ddots & & & \\ 0 & & I_{i_l} & & & \\ \hline & & & I_{j_1} & \ldots & 0 \\ & 0 & & \vdots & \ddots & \vdots \\ & & & 0 & \ldots & I_{j_k} \end{array} \right) : * \in \mathrm{Mat}_{\imath,\jmath}(F_q) \right\}$$

for $t = 1, \ldots, l$, and

$$\Delta_{l+s,j_s}(\varrho_s) = \left\{ \left(\begin{array}{ccc|ccc} I_{i_1} & \ldots & 0 & & & \\ \vdots & \ddots & \vdots & & * & \\ 0 & \ldots & I_{i_l} & & & \\ \hline & & & I_{j_1} & \ldots & 0 \\ & & & & \ddots & \\ & 0 & & \vdots & \varrho_s I_{j_s} & \vdots \\ & & & & & \ddots \\ & & & 0 & \ldots & I_{j_k} \end{array} \right) : * \in \mathrm{Mat}_{\imath,\jmath}(F_q) \right\}$$

for $s = 1, \ldots, k$, where $\imath = i_1 + \ldots + i_l$ and $\jmath = j_1 + \ldots + j_k$. Let the group $G_{\imath,\jmath}(\omega_1, \ldots, \omega_l, \varrho_1, \ldots, \varrho_k)$ be generated by the matrices in the union of sets

$$\Delta_{1,i_1}(\omega_1) \cup \ldots \cup \Delta_{l,i_l}(\omega_l) \cup \Delta_{l+1,j_1}(\varrho_1) \cup \ldots \cup \Delta_{l+k,j_k}(\varrho_k).$$

Then the order of the group $G_{\imath,\jmath}(\omega_1, \ldots, \omega_l, \varrho_1, \ldots, \varrho_k)$ is equal to $q^{\imath\jmath} \cdot \Big(\prod_{t=1}^{l} a_t\Big) \cdot \Big(\prod_{s=1}^{k} b_s\Big)$.

Note. For convenience, $G_{\imath,\jmath}(\omega_1, \ldots, \omega_l, \varrho_1, \ldots, \varrho_k)$ is briefly denoted by $G(\underline{\omega}, \underline{\varrho})$.

Next, we determine the invariant ring of the group $G(\underline{\omega}, \underline{\varrho})$. Let

$$C_{q^\jmath}(z_t) = z_t^{q^\jmath} + \sum_{r=0}^{\jmath-1} (d_{\jmath,r} \cdot z_t^{q^r})$$

for $t = 1, \ldots, \imath$, where $d_{\jmath,r}$ is the Dickson polynomial in $z_{\imath+1}, \ldots, z_{\imath+\jmath}$ with degree $q^\jmath - q^r$ for $r = 0, \ldots, \jmath - 1$. Since the invariant ring $F_q[V]^{G(\underline{\omega},\underline{\varrho})}$ has a tremendously long formula, we prefer to list the primary invariants and a minimal system of secondary invariants.

Theorem 3.14. *Let $\omega_1, \ldots, \omega_l, \varrho_1, \ldots, \varrho_k \in F_q$ be $l+k$ roots of unity with orders $a_1, \ldots, a_l, b_1, \ldots, b_k$, respectively. The group $G(\underline{\omega}, \underline{\varrho})$ is defined in Definition* 3.13. *Denote $\imath = i_1 + \ldots + i_l$ and $\jmath = j_1 + \ldots + j_k$. Then in the invariant ring $F_q[V]^{G(\underline{\omega},\underline{\varrho})}$,*

$$M = \{C_{q^\jmath}(z_1)^{a_1}, \ldots, C_{q^\jmath}(z_{i_1})^{a_1}, C_{q^\jmath}(z_{i_1+1})^{a_2}, \ldots, C_{q^\jmath}(z_\imath)^{a_l}, z_{\imath+1}^{b_1}, \ldots, z_{\imath+j_1}^{b_1}, z_{\imath+j_1+1}^{b_2}, \ldots, z_{\imath+\jmath}^{b_k}\}$$

is a set of primary invariants and

$$K = \prod_{t=0}^{l-1}\left\{\bigcup_{\substack{m_t=0\\ a_{t+1}|m_t}}^{i_{t+1}(a_{t+1}-1)}\left\{\bigcup_{\substack{c_1+\ldots+c_{i_{t+1}}=m_t\\ 0\leqslant c_1,\ldots,c_{i_{t+1}}\leqslant a_{t+1}-1}}\{C_{q^\jmath}(z_{i_0+\ldots+i_t+1})^{c_1}\ldots C_{q^\jmath}(z_{i_0+\ldots+i_{t+1}})^{c_{i_{t+1}}}\}\right\}\right\}$$
$$\times \prod_{s=0}^{k-1}\left\{\bigcup_{\substack{m_s=0\\ b_{s+1}|m_s}}^{j_{s+1}(b_{s+1}-1)}\left\{\bigcup_{\substack{d_1+\ldots+d_{j_{s+1}}=m_s\\ 0\leqslant d_1,\ldots,d_{j_{s+1}}\leqslant b_{s+1}-1}}\{(z_{\imath+j_0+\ldots+j_s+1})^{d_1}\ldots(z_{\imath+j_0+\ldots+j_{s+1}})^{d_{j_{s+1}}}\}\right\}\right\}$$

is a minimal system of secondary invariants where $i_0 = j_0 = 0$. The primary and secondary invariants yield a direct sum decomposition of the invariant ring $F_q[V]^{G(\underline{\omega},\underline{\varrho})}$.

Applying a method similar to Proposition 3.8, we can deduce the following result.

Proposition 3.15. *The invariant ring $F_q[V]^{G(\underline{\omega},\underline{\varrho})}$ is Cohen-Macaulay.*

Finally, we come to the Gorenstein property.

Proposition 3.16. *The invariant ring $F_q[V]^{G(\underline{\omega},\underline{\varrho})}$ is Gorenstein if and only if the following two conditions both hold:* (i) *$i_t = 1$ or $a_t | i_t$ for all $t = 1, \ldots, l$; and* (ii) *$j_s = 1$ or $b_s | j_s$ for all $s = 1, \ldots, k$.*

4. Groups with invariant subspaces which have the same dimension

In Section 2, we have discussed the groups generated by i-transvections with a given invariant subspace H. For instance, the group G_i^+ with $H = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle$ is studied in Proposition 2.10. In this section, we focus on the groups generated by i-transvections with several invariant subspaces which have the same dimension. Before computing the invariant rings, we need to determine the structures of these groups. By calculating the fixed vectors in the vector spaces V and V^* under the action of a group G, we prove that there are totally four kinds of groups. After that, we calculate the invariant rings of each kind of groups separately.

We denote a subspace $W = \{k\cdot x \in V\colon\ k \in F_q\} \subseteq V$ by $\mathrm{Span}_{F_q}\langle x\rangle$ and a subspace $W' = \{k\cdot z \in V^*\colon\ k \in F_q\} \subseteq V^*$ by $\mathrm{Span}_{F_q}\langle z\rangle$. Let A be a set, $B \subset A$ a subset. We define the set $A \setminus B = \{x\colon\ x \in A, x \notin B\}$. A linear transform $T \in \mathrm{GL}(n, F_q)$ is said to *fix a space* W, if $Tv = v$ for all $v \in W$.

Lemma 2.8 tells us the matrix form of an element in the group generated by all i-transvections with the invariant subspace $H = \mathrm{Ker}\langle z_{n-i+1}, \ldots, z_n\rangle = \mathrm{Span}_{F_q}\langle x_1, \ldots, x_{n-i}\rangle$. Similarly, we can obtain the matrix form with other invariant subspaces. Lemmas 4.1–4.3 follow directly from Lemma 2.8 by permuting the basis $\{x_1, \ldots, x_n\}$ of F_q and thus they are presented without proof.

Lemma 4.1. *If a subspace $H = \mathrm{Ker}\langle z_{l_1}, \ldots, z_{l_i}\rangle = \mathrm{Span}_{F_q}\langle x_{h_1}, \ldots, x_{h_{n-i}}\rangle$, where the set $\{h_1, \ldots, h_{n-i}\} = \{1, \ldots, n\} \setminus \{l_1, \ldots, l_i\}$, then the matrix form $(a_{\alpha\beta})_{n\times n}$ of an element T in the group generated by all i-transvections with this invariant subspace H satisfies:*

(1) *the main diagonal entry is $a_{\alpha\alpha} = 1$ for all $\alpha \in \{1, \ldots, n\}$;*
(2) *$a_{\alpha\beta} \in F_q$ is arbitrary for all $\alpha \in \{h_1, \ldots, h_{n-i}\}$ for all $\beta \in \{l_1, \ldots, l_i\}$;*
(3) *and other entries are all zero.*

Conversely, if a matrix satisfies (1)–(3), then it is an element in the group generated by all i-transvections with the invariant subspace $H = \mathrm{Ker}\langle z_{l_1}, \ldots, z_{l_i}\rangle = \mathrm{Span}_{F_q}\langle x_{h_1}, \ldots, x_{h_{n-i}}\rangle$, where $\{h_1, \ldots, h_{n-i}\} = \{1, \ldots, n\} \setminus \{l_1, \ldots, l_i\}$.

Lemma 4.2. *Let $x_1, \ldots, x_n \in V = F_q^n$ form a basis and $z_1, \ldots, z_n \in V^*$ a dual basis to $\{x_1, \ldots, x_n\}$. Suppose that $T = (a_{\alpha\beta})_{n\times n}$ is an element in the group generated by all i-transvections with the invariant subspace H.*

(1) *If T fixes a subspace $\mathrm{Span}_{F_q}\langle x_r\rangle \subset V$ for some $r \in \{1, \ldots, n\}$, then $a_{rr} = 1$ and $a_{\alpha r} = 0$ in the matrix form of T for all $\alpha \in \{1, \ldots, n\} \setminus \{r\}$.*
(2) *If T fixes a subspace $\mathrm{Span}_{F_q}\langle z_r\rangle \subset V^*$ for some $r \in \{1, \ldots, n\}$, then $a_{rr} = 1$ and $a_{r\beta} = 0$ in the matrix form of T for all $\beta \in \{1, \ldots, n\} \setminus \{r\}$.*

Lemma 4.3. *If a subspace* $H = \mathrm{Ker}\langle z_{l_1}, \ldots, z_{l_i}\rangle = \mathrm{Span}_{F_q}\langle x_{h_1}, \ldots, x_{h_{n-i}}\rangle$ *is the invariant subspace of an* i*-transvection* T*, where the set* $\{h_1, \ldots, h_{n-i}\} = \{1, \ldots, n\} \setminus \{l_1, \ldots, l_i\}$*, then* T *fixes the subspaces* $\mathrm{Span}_{F_q}\langle x_{h_1}, \ldots, x_{h_{n-i}}\rangle \subset V$ *and* $\mathrm{Span}_{F_q}\langle z_{l_1}, \ldots, z_{l_i}\rangle \subset V^*$.

Conversely, if a linear transform $T = (a_{\alpha\beta})_{n\times n}$ fixes the above two subspaces, then it is an i-transvection with the invariant subspace $H = \mathrm{Ker}\langle z_{l_1}, \ldots, z_{l_i}\rangle = \mathrm{Span}_{F_q}\langle x_{h_1}, \ldots, x_{h_{n-i}}\rangle$, where the set $\{h_1, \ldots, h_{n-i}\} = \{1, \ldots, n\} \setminus \{l_1, \ldots, l_i\}$.

We next establish an example to show what we have done.

Example 4.4. Let F_q be a finite field where $q = p^\nu$, $\nu \in Z^*$. We set $n = 4$. Then $x_1, \ldots, x_4 \in V = F_q^4$ form a basis and $z_1, \ldots, z_4 \in V^*$ form a dual basis to $\{x_1, \ldots, x_4\}$.

Here we offer several sets of 1-transvections, 2-transvections and 3-transvections. In each of the following matrices, every empty entry is zero which is omitted, and the symbols $* \in F_q$.

1-transvections: let $H_1 = \mathrm{Ker}\langle z_3\rangle = \mathrm{Span}_{F_q}\langle x_1, x_2, x_4\rangle$ and $H_2 = \mathrm{Ker}\langle z_4\rangle = \mathrm{Span}_{F_q}\langle x_1, x_2, x_3\rangle$, then

$$\Delta_1 = \left\{ \begin{pmatrix} 1 & & * & \\ & 1 & * & \\ & & 1 & \\ & & * & 1 \end{pmatrix} \right\} \quad \text{and} \quad \Delta_2 = \left\{ \begin{pmatrix} 1 & & & * \\ & 1 & & * \\ & & 1 & * \\ & & & 1 \end{pmatrix} \right\}$$

are sets of 1-transvections with the same invariant subspaces H_1 and H_2, respectively. It is clear that every element in the set Δ_1 fixes $\mathrm{Span}_{F_q}\langle x_1, x_2, x_4\rangle$ and $\mathrm{Span}_{F_q}\langle z_3\rangle$.

2-transvections: let $H_3 = \mathrm{Ker}\langle z_2, z_3\rangle = \mathrm{Span}_{F_q}\langle x_1, x_4\rangle$, $H_4 = \mathrm{Ker}\langle z_1, z_4\rangle = \mathrm{Span}_{F_q}\langle x_2, x_3\rangle$ and $H_5 = \mathrm{Ker}\langle z_2, z_4\rangle = \mathrm{Span}_{F_q}\langle x_1, x_3\rangle$, then

$$\Delta_3 = \left\{ \begin{pmatrix} 1 & * & * & \\ & 1 & & \\ & & 1 & \\ & * & * & 1 \end{pmatrix} \right\}, \ \Delta_4 = \left\{ \begin{pmatrix} 1 & & & \\ * & 1 & & * \\ * & & 1 & * \\ & & & 1 \end{pmatrix} \right\}, \ \Delta_5 = \left\{ \begin{pmatrix} 1 & * & & * \\ & 1 & & \\ & * & 1 & * \\ & & & 1 \end{pmatrix} \right\}$$

are sets of 2-transvections with the same invariant subspaces H_3, H_4 and H_5, respectively.

3-transvections: let $H_6 = \mathrm{Ker}\langle z_1, z_2, z_4\rangle = \mathrm{Span}_{F_q}\langle x_3\rangle$ and $H_7 = \mathrm{Ker}\langle z_1, z_3, z_4\rangle = \mathrm{Span}_{F_q}\langle x_2\rangle$, then

$$\Delta_6 = \left\{ \begin{pmatrix} 1 & & & \\ & 1 & & \\ * & * & 1 & * \\ & & & 1 \end{pmatrix} \right\} \quad \text{and} \quad \Delta_7 = \left\{ \begin{pmatrix} 1 & & & \\ * & 1 & * & * \\ & & 1 & \\ & & & 1 \end{pmatrix} \right\}$$

are sets of 3-transvections with the same invariant subspaces H_6 and H_7, respectively.

We will structure several groups generated by these sets of i-transvections and compute their invariant rings in the sequel.

Next, we concentrate on the groups generated by i-transvections with several arbitrary invariant subspaces which have the same dimension.

Theorem 4.5. *Let $k \geqslant 2$ and $1 \leqslant i \leqslant n-1$ be two given integers. Let*

$$\begin{aligned} H_1 &= \mathrm{Ker}\langle z_{h_1^1}, \ldots, z_{h_i^1}\rangle = \mathrm{Span}_{F_q}\langle \{x_1, \ldots, x_n\} \setminus \{x_{h_1^1}, \ldots, x_{h_i^1}\}\rangle, \\ &\vdots \\ H_k &= \mathrm{Ker}\langle z_{h_1^k}, \ldots, z_{h_i^k}\rangle = \mathrm{Span}_{F_q}\langle \{x_1, \ldots, x_n\} \setminus \{x_{h_1^k}, \ldots, x_{h_i^k}\}\rangle \end{aligned}$$

be different $(n-i)$-dimensional subspaces where $z_{h_\beta^\alpha} \in \{z_1, \ldots, z_n\}$ for all $1 \leqslant \alpha \leqslant k$ and $1 \leqslant \beta \leqslant i$. Suppose that Δ_m is the set of all i-transvections with the same invariant subspace H_m for $m = 1, \ldots, k$. Define a group $G_{i,k} = \langle T\colon\ T \in \Delta_1 \cup \ldots \cup \Delta_k\rangle$. Then

$$G_{i,k} \cong \left\{ \left(\begin{array}{c|cc} I_{n-t} & *_1 & \\ \hline 0 & I_{t-l} & 0 \\ 0 & *_2 & \mathrm{SL}(l, F_q) \end{array} \right) : \begin{array}{l} *_1 \in \mathrm{Mat}_{n-t,t}(F_q), \\ *_2 \in \mathrm{Mat}_{l,t-l}(F_q) \end{array} \right\}.$$

The integers t and l, which are irrelevant to each other, satisfy $2 \leqslant l \leqslant t \leqslant n$.

There is some preparatory work to be done before proving this theorem.

Definition 4.6. Denote by $E(ij)$ the matrix $(a_{\alpha\beta})_{n\times n}$ whose
(1) main diagonal entry is $a_{\alpha\alpha} = 1$ for all $\alpha \in \{1, \ldots, n\}$,
(2) $a_{ij} = 1$,
(3) and the other entries are all zero.

Denote by $E(-ij)$ the matrix $(a_{\alpha\beta})_{n\times n}$ whose
(1) main diagonal entry is $a_{\alpha\alpha} = 1$ for all $\alpha \in \{1, \ldots, n\}$,
(2) $a_{ij} = -1$,
(3) and the other entries are all zero.

Denote by $E(\pm ij)$ the two matrices $E(ij)$ and $E(-ij)$.

Based on this notation, we derive a special case of Whitehead formula as follows.

Lemma 4.7 ([12])**.**

$$E(-ij)\times E(-kl)\times E(ij)\times E(kl)=\begin{cases}E(il) & \text{if } j=k,\ i\neq l,\\ E(-kj) & \text{if } j\neq k,\ i=l.\end{cases}$$

It is well known that $\{E(\pm ij)\colon 1\leqslant i\neq j\leqslant n\}$ *is the set of generators of the special linear group* $\mathrm{SL}(n,F_q)$*. Lemma* 4.7 *indicates several relations between these generators in preparation for getting a simple set of generators. Now, we come to the proof of Theorem* 4.5.

P r o o f of Theorem 4.5. Denote the subgroup $S_j=\langle T\colon T\in\Delta_j\rangle\subset G_{i,k}$ for $j=1,\ldots,k$. The union of sets $\Delta_1\cup\ldots\cup\Delta_k$ is a generating set of the group $G_{i,k}$, so is the union of subgroups $S_1\cup\ldots\cup S_k$.

We consider the following three statements for these k different invariant subspaces $H_1,\ldots,H_k$:

▷ *Statement* (a): $\exists\ r_1\in\{1,\ldots,n\}$, such that $x_{r_1}\in\bigcap\limits_{m=1}^{k}H_m$;

▷ *Statement* (b): $\exists\ r_2\in\{1,\ldots,n\}$, such that $x_{r_2}\notin\bigcup\limits_{m=1}^{k}H_m$;

▷ *Statement* (c): $\exists\ r_3\in\{1,\ldots,n\}$, such that $x_{r_3}\in H_{m_1}$ but $x_{r_3}\notin H_{m_2}$ for some $m_1,m_2\in\{1,\ldots,k\}$.

Next, let us explicitly exploit the influence of Statements (a), (b) and (c) on the matrix forms of elements in the group $G_{i,k}$ separately. Let $T=(a_{\alpha\beta})_{n\times n}\in G_{i,k}$ be an element.

Influence of Statement (a). First, we discuss the influence on the columns of matrix forms. According to Statement (a), $\mathrm{Span}_{F_q}\langle x_{r_1}\rangle\subseteq H_m$ for all $m\in\{1,\ldots,k\}$, hence every i-transvection in the generating set $\Delta_1\cup\ldots\cup\Delta_k$ fixes $\mathrm{Span}_{F_q}\langle x_{r_1}\rangle$ according to Lemma 4.3, so does $T=(a_{\alpha\beta})_{n\times n}\in G_{i,k}$. Therefore $a_{r_1r_1}=1$ and $a_{\alpha r_1}=0$ for all $\alpha\in\{1,\ldots,n\}\setminus\{r_1\}$, in the matrix form of $T=(a_{\alpha\beta})_{n\times n}$ according to Lemma 4.2.

Next, we study the influence on the rows of matrix forms. Without loss of generality, we suppose that $x_1,\ldots,x_{n-t}\in\bigcap\limits_{m=1}^{k}H_m$, but $x_{n-t+1},\ldots,x_n\notin\bigcap\limits_{m=1}^{k}H_m$ for some integer $2\leqslant t\leqslant n$. Notice $2\leqslant k$, so $2\leqslant t$. If $t=n$, then $\bigcap\limits_{m=1}^{k}H_m=\emptyset$. Referring to the previous discussion, we indicate that the first $(n-t)$ columns of the matrix form of T agree with the first $(n-t)$ columns of the identity matrix $I\in\mathrm{GL}(n,F_q)$.

Now, we come to the first $n-t$ rows of the matrix form of T. Since for all $\beta\in\{n-t+1,\ldots,n\}$, $x_\beta\notin\bigcap\limits_{m=1}^{k}H_m$, there exists an integer $c\in\{1,\ldots,k\}$ such that $x_\beta\notin H_c=\mathrm{Ker}\langle z_{h_1^c},\ldots,z_{h_i^c}\rangle$, so $\beta\in\{h_1^c,\ldots,h_i^c\}$. Let $T_c=(b_{\alpha\beta})_{n\times n}\in S_c=\langle T\colon T\in\Delta_c\rangle$ be an element with the invariant subspace H_c, then T_c fixes $\mathrm{Span}_{F_q}\langle z_\beta\rangle$

according to Lemma 4.3, i.e., $\mathrm{Ker}\langle z_\beta\rangle \supset H_c$. It yields that $b_{\alpha\beta} \in F_q$ can be an arbitrary number for all $\alpha \in \{1,\ldots,n-t\}$, in the matrix form of $T_c = (b_{\alpha\beta})_{n\times n}$ according to Lemma 4.1. For every $\beta \in \{n-t+1,\ldots,n\}$, there exists such an i-transvection T_c. Notice that T_c is one generator of the group $G_{i,k}$, hence the matrix form of the element $T \in G_{i,k}$ is

$$\begin{pmatrix} I_{n-t} & * \\ 0 & B \end{pmatrix}, \tag{1}$$

where $* \in \mathrm{Mat}_{n-t,t}(F_q)$ and $B \in \mathrm{GL}(t, F_q)$.

Influence of Statement (b). For all $m \in \{1,\ldots,k\}$, since $x_{r_2} \notin H_m$, $T_m \in \Delta_m$ cannot fix $\mathrm{Span}_{F_q}\langle x_{r_2}\rangle$. According to Lemma 4.3, T_m fixes $\mathrm{Span}_{F_q}\langle z_{r_2}\rangle$, so does $T = (a_{\alpha\beta})_{n\times n} \in G_{i,k}$. Therefore $a_{r_2r_2} = 1$ and $a_{r_2\beta} = 0$ for all $\beta \in \{1,\ldots,n\}\setminus\{r_2\}$, in the matrix form of $T = (a_{\alpha\beta})_{n\times n}$ according to Lemma 4.2.

Next, we study the influence on the columns of matrix forms. Without loss of generality, suppose that $\mathrm{Span}_{F_q}\langle z_{n-t+1},\ldots,z_{n-l}\rangle \subset V^*$ is the maximum subspace fixed by every i-transvection in the generating set $\Delta_1\cup\ldots\cup\Delta_k$ where t is the integer presented in the influence of Statement (a) and $1 \leqslant l \leqslant t$ for some integer l. By an argument similar to that in the influence of Statement (a) on the rows of the matrix form of $T = (a_{\alpha\beta})_{n\times n}$, we can deduce that $a_{\alpha\beta} \in F_q$ can be an arbitrary number for all $\alpha \in \{1,\ldots,n-t\}\cup\{n-l+1,\ldots,n\}$ for all $\beta \in \{n-t+1,\ldots,n-l\}$, according to Lemma 4.1. Therefore, the matrix form of the element $T \in G_{i,k}$ is

$$\begin{pmatrix} C_1 & *_1 & C_2 \\ 0 & I_{t-l} & 0 \\ C_3 & *_2 & C_4 \end{pmatrix}, \tag{2}$$

where $*_1 \in \mathrm{Mat}_{n-t,t-l}(F_q)$, $*_2 \in \mathrm{Mat}_{l,t-l}(F_q)$ and $\begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix} \in \mathrm{GL}(n-t+l, F_q)$.

Influence of Statement (c). We still adopt the previous notation, i.e., $x_1,\ldots,x_{n-t} \in \bigcap_{m=1}^{k} H_m$, $x_{n-t+1},\ldots,x_n \notin \bigcap_{m=1}^{k} H_m$, and $\mathrm{Span}_{F_q}\langle z_{n-t+1},\ldots,z_{n-l}\rangle \subset V^*$ is the maximum subspace fixed by every i-transvection in the generating set $\Delta_1\cup\ldots\cup\Delta_k$. Based on matrices (1) and (2) we conclude that the matrix form of T is

$$\begin{pmatrix} I_{n-t} & *_1 & *_2 \\ 0 & I_{t-l} & 0 \\ 0 & *_3 & A \end{pmatrix}, \tag{3}$$

where $*_1 \in \mathrm{Mat}_{n-t,t-l}(F_q)$, $*_2 \in \mathrm{Mat}_{n-t,l}(F_q)$, $*_3 \in \mathrm{Mat}_{l,t-l}(F_q)$ and $A \in \mathrm{GL}(l, F_q)$ according to the influence of Statements (a) and (b).

Next, we will prove that the bottom right block A in matrix (3) is exactly the special linear group $\mathrm{SL}(l, F_q)$ according to the influence of Statement (c). Since $\{E(\pm\alpha\beta)\colon\ n-l+1 \leqslant \alpha \neq \beta \leqslant n\}$ is a set of generators of the special linear group $\mathrm{SL}(l, F_q)$, it will suffice to prove that every $E(\alpha\beta)$ and $E(-\alpha\beta)$ for all $\alpha \neq \beta \in \{n-l+1, \ldots, n\}$, can be equal to a product of several i-transvections in the union of sets $\Delta_1 \cup \ldots \cup \Delta_k$.

Before solving this problem, we emphasize that if $T = (a_{\alpha\beta})_{n\times n} \in S_m$ is an element with the invariant subspace $H_m = \mathrm{Ker}\langle z_{h_1^m}, \ldots, z_{h_i^m}\rangle$ for any $1 \leqslant m \leqslant k$, then there are totally i entries in the row α and totally $(n-i)$ entries in the column β which can be arbitrary numbers in the matrix form of T according to Lemma 4.1, for all $\alpha \in \{1, \ldots, n\} \setminus \{h_1^m, \ldots, h_i^m\}$ and for all $\beta \in \{h_1^m, \ldots, h_i^m\}$.

Now, we return to discuss the influence of Statement (c). Statement (c) is: for all $r_3 \in \{n-l+1, \ldots, n\}$, there exist two integers $m_1, m_2 \in \{1, \ldots, k\}$ such that $x_{r_3} \in H_{m_1}$ but $x_{r_3} \notin H_{m_2}$. Since $k \geqslant 2$, Statement (c) is always true. Hence $n-l+1 < n$, i.e., $2 \leqslant l$. Referring to Statement (c), for every $\beta' \in \{n-l+1, \ldots, n\}$ there exists an integer $m \in \{1, \ldots, k\}$ such that $x_{\beta'} \notin H_m$, so $H_m \subset \mathrm{Ker}\langle z_{\beta'}\rangle$ according to Lemma 4.1. Let us fix β' and m. Suppose that $T_m = (a_{\alpha\beta})_{n\times n} \in S_m = \langle T\colon\ T \in \Delta_m\rangle$ is an element with the invariant subspace H_m, so there are totally $(n-i)$ entries in the column β' which can be arbitrary numbers in the matrix form of T_m. Specially,

$$T_m \begin{cases} \text{(i) can become } \mathrm{E}(\pm\alpha_1\beta'), \ldots, \mathrm{E}(\pm\alpha_{n-i}\beta') \\ \qquad \text{for some subset } \{\alpha_1, \ldots, \alpha_{n-i}\} \subset \{1, \ldots, \beta'-1, \beta'+1, \ldots, n\}; \\ \text{(ii) cannot become } \mathrm{E}(\pm\alpha_{n-i+1}\beta'), \ldots, \mathrm{E}(\pm\alpha_{n-1}\beta') \\ \qquad \text{for the subset } \{\alpha_{n-i+1}, \ldots, \alpha_{n-1}\} \\ \qquad\qquad = \{1, \ldots, \beta'-1, \beta'+1, \ldots, n\} \setminus \{\alpha_1, \ldots, \alpha_{n-i}\}. \end{cases}$$

Without loss of generality, suppose that $\{\alpha_{n-i+1}, \ldots, \alpha_d\} \subset \{n-l+1, \ldots, n\}$. Notice that $E(\pm\alpha_{n-i+1}\beta'), \ldots, E(\pm\alpha_d\beta') \in \{E(\pm\alpha\beta)\colon\ n-l+1 \leqslant \alpha \neq \beta \leqslant n\}$, but T_m can become none of them. Hence we need to prove that each of them can be generated by T_m and another element $T_{m'} \in S_{m'} = \langle T\colon\ T \in \Delta_{m'}\rangle$ with another invariant subspace $H_{m'}$.

We first consider $E(\pm\alpha_{n-i+1}\beta')$.

Since $\alpha_{n-i+1} \in \{n-l+1, \ldots, n\}$, there exists an integer $m' \in \{1, \ldots, k\}$ such that $x_{\alpha_{n-i+1}} \in H_{m'}$ according to Statement (c). Let $T_{m'} = (b_{\alpha\beta})_{n\times n} \in S_{m'} = \langle T\colon\ T \in \Delta_{m'}\rangle$ be an element with the invariant subspace $H_{m'}$, so there are totally i entries in the row α_{n-i+1} which can be arbitrary numbers in the matrix form of $T_{m'}$ by Lemma 4.1. Hence $T_{m'}$ can become $E(\pm\alpha_{n-i+1}\gamma_1), \ldots, E(\pm\alpha_{n-i+1}\gamma_i)$ for some

subset $\{\gamma_1, \ldots, \gamma_i\} \subset \{1, \ldots, n\} \setminus \{\alpha_{n-i+1}\}$. Since

$$\begin{aligned}\mathrm{Card}(\{\alpha_1, \ldots, \alpha_{n-i}\}) + \mathrm{Card}(\{\gamma_1, \ldots, \gamma_i\}) &= n - i + i = n > n - 1 \\ &= \mathrm{Card}(\{1, \ldots, n\} \setminus \{\alpha_{n-i+1}\}),\end{aligned}$$

it follows that

$$\{\alpha_1, \ldots, \alpha_{n-i}\} \cap \{\gamma_1, \ldots, \gamma_i\} \neq \emptyset.$$

We suppose that $\eta \in \{\alpha_1, \ldots, \alpha_{n-i}\} \cap \{\gamma_1, \ldots, \gamma_i\}$. Referring to Lemma 4.7, it yields that

$$\begin{aligned}E(\alpha_{n-i+1}\beta') &= E(-\alpha_{n-i+1}\eta) \cdot E(-\eta\beta') \cdot E(\alpha_{n-i+1}\eta) \cdot E(\eta\beta'), \\ E(-\alpha_{n-i+1}\beta') &= E(-\eta\beta') \cdot E(-\alpha_{n-i+1}\eta) \cdot E(\eta\beta') \cdot E(\alpha_{n-i+1}\eta).\end{aligned}$$

Since T_m can become $E(\pm\eta\beta')$ and $T_{m'}$ can become $E(\pm\alpha_{n-i+1}\eta)$, $E(\pm\alpha_{n-i+1}\beta')$ can be generated by T_m and $T_{m'}$.

Similarly, we can prove that $E(\pm\alpha_{n-i+2}\beta'), \ldots, E(\pm\alpha_d\beta')$ can be generated by i-transvections T_m and $T_{m'} \in \Delta_{m'}$ for some $m' \in \{1, \ldots, k\}$. Since $\beta' \in \{n - l + 1, \ldots, n\}$ is arbitrary, every element in the set of generators $\{E(\pm\alpha\beta) \colon n-l+1 \leqslant \alpha \neq \beta \leqslant n\}$ of the special linear group $\mathrm{SL}(l, F_q)$ can be generated by several elements in the union of subgroups $S_1 \cup \ldots \cup S_k$, i.e., in the generating set $\Delta_1 \cup \ldots \cup \Delta_k$. Hence the bottom right block A in matrix (3) is precisely equal to the special linear group $\mathrm{SL}(l, F_q)$. Therefore we conclude that the matrix form of T is

$$\begin{pmatrix} I_{n-t} & *_1 & *_2 \\ 0 & I_{t-l} & 0 \\ 0 & *_3 & \mathrm{SL}(l, F_q) \end{pmatrix},$$

where $*_1 \in \mathrm{Mat}_{n-t,t-l}(F_q)$, $*_2 \in \mathrm{Mat}_{n-t,l}(F_q)$ and $*_3 \in \mathrm{Mat}_{l,t-l}(F_q)$.

Reasoning as above, we have completed the proof. □

In order to show the connection with and difference from the existing results, we divide the groups $G_{i,k}$ into four kinds. Notice that Statement (c) is always true since $k \geqslant 2$.

(1) If only Statement (c) is true, then $2 \leqslant l = t = n$, so the group $G_{i,k}$ is the special linear group $\mathrm{SL}(n, F_q)$ with order $1/(q-1) \cdot \prod_{j=0}^{n-1} (q^n - q^j)$ and we denote it by G_1.

(2) If Statements (a) and (c) are true, then $2 \leqslant l = t < n$, so the group is

$$G_{i,k} \cong \left\{ \begin{pmatrix} I_{n-t} & * \\ 0 & \mathrm{SL}(t, F_q) \end{pmatrix} \colon * \in \mathrm{Mat}_{n-t,t}(F_q) \right\}$$

with order $q^{(n-t)t}/(q-1)\cdot\prod_{j=0}^{t-1}\left(q^t-q^j\right)$ and we denote it by G_2.

(3) If Statements (b) and (c) are true, then $2\leqslant l<t=n$, so the group is

$$G_{i,k}\cong\left\{\begin{pmatrix} I_{n-l} & 0\\ * & \mathrm{SL}(l,F_q)\end{pmatrix}:\ *\in\mathrm{Mat}_{l,n-l}(F_q)\right\}$$

with order $q^{l(n-l)}/(q-1)\cdot\prod_{j=0}^{l-1}(q^l-q^j)$ and we denote it by G_3.

(4) If Statements (a), (b) and (c) are all true, then $2\leqslant l<t\leqslant n-1$, so the group is

$$G_{i,k}\cong\left\{\left(\begin{array}{c|cc} I_{n-t} & *_1 & \\ \hline 0 & I_{t-l} & 0\\ 0 & *_2 & \mathrm{SL}(l,F_q)\end{array}\right):\ \begin{array}{l}*_1\in\mathrm{Mat}_{n-t,t}(F_q),\\ *_2\in\mathrm{Mat}_{l,t-l}(F_q)\end{array}\right\}$$

with order $q^{(n-t)t+l(t-l)}/(q-1)\cdot\prod_{j=0}^{l-1}(q^l-q^j)$ and we denote it by G_4.

We prepare for a description of Theorem 4.5 with an example. We continue to discuss Example 4.4.

Example 4.8. As mentioned in Example 4.4, let $n=4$, and let Δ_j be a set of i-transvections with the same invariant subspace H_j for $j=1,\ldots,7$.

First, we set a group $J_1=\langle T:\ T\in\Delta_3\cup\Delta_4\cup\Delta_5\rangle$. Only Statement (c) is true for the invariant subspaces H_3,H_4 and H_5, so J_1 is the special linear group $\mathrm{SL}(4,F_q)$ according to Theorem 4.5. In fact, one can check that $\langle T:\ T\in\Delta_3\cup\Delta_4\cup\Delta_5\rangle=\langle T:\ T\in\Delta_3\cup\Delta_4\rangle$.

Then we set a group $J_2=\langle T:\ T\in\Delta_1\cup\Delta_2\rangle$. Since Statements (a) and (c) are true for the invariant subspaces H_1 and H_2, it follows that

$$J_2=\left\{\begin{pmatrix} I_2 & *\\ 0 & \mathrm{SL}(2,F_q)\end{pmatrix}:\ *\in\mathrm{Mat}_{2,2}(F_q)\right\}.$$

Next, we set a group $J_3=\langle T:\ T\in\Delta_6\cup\Delta_7\rangle$. Since Statements (b) and (c) are true for the invariant subspaces H_6 and H_7, it follows that

$$J_3=\left\{\left(\begin{array}{c|cc|c} 1 & 0 & 0 & 0\\ \hline * & & & *\\ & \mathrm{SL}(2,F_q) & & \\ * & & & *\\ \hline 0 & 0 & 0 & 1\end{array}\right):\ *\in F_q\right\}\cong\left\{\begin{pmatrix} I_2 & 0\\ * & \mathrm{SL}(2,F_q)\end{pmatrix}:\ *\in\mathrm{Mat}_{2,2}(F_q)\right\}.$$

Finally, we set a group $J_4 = \langle T\colon\ T \in \Delta_3 \cup \Delta_5\rangle$. Since Statements (a), (b) and (c) are all true for the invariant subspaces H_3 and H_5, it follows that

$$J_4 = \left\{ \left(\begin{array}{cc|cc} 1 & * & * & * \\ 0 & 1 & 0 & 0 \\ \hline 0 & * & & \\ & & \mathrm{SL}(2, F_q) & \\ 0 & * & & \end{array} \right) \colon\ * \in F_q \right\}.$$

We next take up the investigation of the invariant rings of every kind of groups separately.

The group G_1 is the special linear group $\mathrm{SL}(n, F_q)$ whose invariant ring is calculated by Dickson in [7]. And we list the result as follows.

Proposition 4.9 ([7]). *The invariant ring of the group $G_1 = \mathrm{SL}(n, F_q)$ is*

$$F_q[V]^{G_1} = F_q[d_{n,1}, \ldots, d_{n,n-1}, L_n],$$

where $d_{n,r}$ is the Dickson polynomial in $z_1, \ldots, z_n$ with degree $q^n - q^r$ for $r = 0, \ldots, n-1$, and $L_n = d_{n,0}^{1/(q-1)}$ is the Euler class.

Before computing the invariant ring of the group G_2, we prove a very useful lemma.

Lemma 4.10. *Let $\omega \in F_q$ be a kth root of unity and $n = n_1 + n_2$. Suppose that $G \subseteq \mathrm{GL}(n, F_q)$ is a group with a set of generators*

$$\left\{ T_i = \begin{pmatrix} \omega I_{n_1} & * \\ 0 & A_i \end{pmatrix} \colon\ * \in \mathrm{Mat}_{n_1,n_2}(F_q),\ A_i \in \mathrm{GL}(n_2, F_q),\ i \in I \right\}.$$

Then (1) *the invariants of the group $G(A) = \langle A_i\colon\ i \in I\rangle$ are also the ones of the group G;*

(2) *the polynomials $C_{q^{n_2}}(z_1)^k, \ldots, C_{q^{n_2}}(z_{n_1})^k$ and $C_{q^{n_2}}(z_1)^{l_1} \ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}$, where $k | l_1 + \ldots + l_{n_1}$, are all invariants of the group G where $C_{q^{n_2}}(z_j)$ is provided in Definition* 1.5 *for $j = 1, \ldots, n_1$.*

P r o o f. (1) According to the matrix form of generator T_i for all $i \in I$, it is easy to observe that the action of T_i on $\mathrm{Span}_{F_q}\langle z_{n_1+1}, \ldots, z_{n_1+n_2}\rangle$ is equivalent to the action of A_i on the same subspace. Therefore, if $f \in F_q[z_{n_1+1}, \ldots, z_{n_1+n_2}]^{G(A)}$, then $T_i \cdot f = A_i \cdot f = f$, i.e., $f \in F_q[z_1, \ldots, z_{n_1+n_2}]^G$.

(2) All orbits of z_1 are of the form

$$\{\omega^j z_1 + \lambda_1 z_{n_1+1} + \ldots + \lambda_{n_2} z_{n_1+n_2}\colon\ 0 \leqslant j \leqslant k-1,\ \lambda_1, \ldots, \lambda_{n_2} \in F_q\}.$$

Since $\omega^q = \omega \in F_q$, it follows that

$$\begin{aligned} C_{\mathrm{top}}(z_1) &= \prod_{j=0}^{k-1}\Big(\prod_{\lambda_1,\ldots,\lambda_{n_2}\in F_q}(\omega^j z_1 + \lambda_1 z_{n_1+1} + \ldots + \lambda_{n_2} z_{n_1+n_2})\Big) \\ &= \prod_{j=0}^{k-1}\Big(\sum_{r=0}^{n_2} d_{n_2,r}\cdot(\omega^j z_1)^{q^r}\Big) = \Big(\prod_{j=0}^{k-1}\omega^j\Big)\cdot\Big(\sum_{r=0}^{n_2} d_{n_2,r}\cdot z_1^{q^r}\Big)^k. \end{aligned}$$

If k is odd, then

$$C_{\mathrm{top}}(z_1) = 1\cdot\Big(\sum_{r=0}^{n_2} d_{n_2,r}\cdot z_1^{q^r}\Big)^k = C_{q^{n_2}}(z_1)^k,$$

which belongs to $F_q[V]^G$. If k is even, then

$$C_{\mathrm{top}}(z_1) = -1\cdot\Big(\sum_{r=0}^{n_2} d_{n_2,r}\cdot z_1^{q^r}\Big)^k = -C_{q^{n_2}}(z_1)^k,$$

which belongs to $F_q[V]^G$. Since $F_q[V]^G$ is an additive group, $C_{q^{n_2}}(z_1)^k \in F_q[V]^G$.

Similarly, $C_{q^{n_2}}(z_2)^k, \ldots, C_{q^{n_2}}(z_{n_1})^k \in F_q[V]^G$.

We next prove that $C_{q^{n_2}}(z_1)^{l_1}\ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}} \in F_q[V]^G$, where $k \mid l_1 + \ldots + l_{n_1}$. To investigate this problem, we suppose that T_i is a generator of the group G for all $i \in I$. By a simple computation,

$$\begin{aligned} T_i(C_{q^{n_2}}(z_1)^{l_1}\ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}) &= (\omega^{l_1}\cdot C_{q^{n_2}}(z_1)^{l_1})\ldots(\omega^{l_{n_1}}\cdot C_{q^{n_2}}(z_{n_1})^{l_{n_1}}) \\ &= \omega^{(l_1+\ldots+l_{n_1})}\cdot(C_{q^{n_2}}(z_1)^{l_1}\ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}) \end{aligned}$$

due to the matrix form of T_i. Since $k \mid l_1 + \ldots + l_{n_1}$, it yields that $C_{q^{n_2}}(z_1)^{l_1}\ldots C_{q^{n_2}}(z_{n_1})^{l_{n_1}}$ is an invariant of the group G.

Reasoning as above, we deduce the results. □

Remark. By the same method, we can extend this lemma to a generalization which involves several roots of unity.

Referring to Lemma 4.10, we can easily determine the invariant ring of the group G_2.

Proposition 4.11. *The invariant ring of the group G_2 is*

$$F_q[V]^{G_2} = F_q[C_{q^t}(z_1), \ldots, C_{q^t}(z_{n-t}), d_{t,1}, \ldots, d_{t,t-1}, L_t],$$

where $C_{q^t}(z_j) = z_j^{q^t} + \sum_{r=0}^{t-1} (d_{t,r} \cdot z_j^{q^r})$ *for* $j = 1, \ldots, n-t$, $d_{t,r}$ *is the Dickson polynomial in* $z_{n-t+1}, \ldots, z_n$ *with degree* $q^t - q^r$ *for* $r = 0, \ldots, t-1$, *and* $L_t = d_{t,0}^{1/(q-1)}$ *is the Euler class.*

P r o o f. Since $d_{t,1}, \ldots, d_{t,t-1}, L_t \in F_q[z_{n-t+1}, \ldots, z_n]^{\mathrm{SL}(t,F_q)}$, they all are invariants of $F_q[V]^{G_2}$ according to Lemma 4.10. And by the same lemma, $C_{q^t}(z_1), \ldots, C_{q^t}(z_{n-t}) \in F_q[V]^{G_2}$. In addition, $C_{q^t}(z_1), \ldots, C_{q^t}(z_{n-t}), d_{t,1}, \ldots, d_{t,t-1}, L_t$ form a system of parameters of $F_q[V]^{G_2}$.

Based on Definition 1.4, $\deg(d_{t,r}) = q^t - q^r$ for $r = 0, \ldots, t-1$. And based on Definition 1.5, $\deg(C_{q^t}(z_j)) = q^t$ for all $j = 1, \ldots, n-t$. Since the order of the group G_2 is $q^{(n-t)t} \cdot 1/(q-1) \cdot \prod_{j=0}^{t-1} (q^t - q^j)$ and $\deg(L_t) = (q^t - q^0)/(q-1)$, we have

$$|G_2| = \deg(L_t) \cdot \prod_{r=1}^{t-1} \deg(d_{t,r}) \cdot \prod_{j=1}^{n-t} \deg(C_{q^t}(z_j)).$$

And the result follows from Proposition 1.6. □

Next, we are going to study the invariant ring of the group G_3. In [21], Steinberg considers a subgroup $G(n-l) \subseteq \mathrm{GL}(n, F_q)$ defined by the requirement that $g \in G(n-l)$ if and only if the first $n-l$ rows of the matrix of g agree with the first $n-l$ rows of the identity matrix $I \in \mathrm{GL}(n, F_q)$. He computes the invariant ring $F_q[V]^{G(n-l)} = F_q[z_1, \ldots, z_{n-l}, d_{n,n-l}, \ldots, d_{n,n-1}]$. The group G_3 here is a subgroup of $G(n-l)$, and the order is $|G_3| = 1/(q-1)|G(n-l)|$, so $F_q[V]^{G_3} \supset F_q[V]^{G(n-l)}$. We describe $F_q[V]^{G_3}$ in the following proposition.

Proposition 4.12. *The invariant ring of the group G_3 is*

$$F_q[V]^{G_3} = F_q[z_1, \ldots, z_{n-l}, h_{n,n-l}, d_{n,n-l+1}, \ldots, d_{n,n-1}],$$

where $d_{n,r}$ is the Dickson polynomial in $z_1, \ldots, z_n$ with degree $q^n - q^r$ for $r = n-l+1, \ldots, n-1$, and

$$h_{n,n-l} = \left\{ \prod_{\substack{\mu_1,\ldots,\mu_l \in F_q \text{ not all zeros,} \\ \lambda_1,\ldots,\lambda_{n-l} \in F_q}} (\lambda_1 z_1 + \ldots + \lambda_{n-l} z_{n-l} + \mu_1 z_{n-l+1} + \ldots + \mu_l z_n) \right\}^{1/(q-1)}.$$

Before we prove this proposition, let us first make an explanation. The relationship between the group $G(n-l)$ and its subgroup G_3 is similar to the one between the group $\mathrm{GL}(n,F_q)$ and its subgroup $\mathrm{SL}(n,F_q)$. It is well known that

$$F_q[V]^{\mathrm{GL}(n,F_q)} = F_q[d_{n,0}, d_{n,1}, \ldots, d_{n,n-1}],$$
$$F_q[V]^{\mathrm{SL}(n,F_q)} = F_q[L_n, d_{n,1}, \ldots, d_{n,n-1}],$$

where $L_n = d_{n,0}^{1/(q-1)}$. Similarly, we wish to find a polynomial f in the set of generators $S = \{z_1, \ldots, z_{n-l}, d_{n,n-l}, \ldots, d_{n,n-1}\}$ of $F_q[V]^{G(n-l)}$. Then we take $f^{1/(q-1)}$ instead of f in the set S to form a set of generators of $F_q[V]^{G_3}$. Unfortunately, it turns out that this is misleading. We shall prove that only $d_{n,0}^{1/(q-1)} = L_n \in F_q[V]$ but the other $d_{n,r}^{1/(q-1)} \notin F_q[V]$ for $r = 1, \ldots, n-1$ in Proposition 4.14. So the previous method used in $F_q[V]^{\mathrm{SL}(n,F_q)}$ cannot work. This fact forces us to seek a new invariant for $F_q[V]^{G_3}$ and it is $h_{n,n-l}$. In fact, $h_{n,n-l}$ is a $(q-1)$-root of the product of orbits of z_{n-l+1} under the action of the group G_3. We first prove that $h_{n,n-l} \in F_q[V]^{G_3}$.

Lemma 4.13. *Define*

$$h_{n,n-l} = \left(\prod_{\substack{\mu_1,\ldots,\mu_l \in F_q \text{ not all zeros},\\ \lambda_1,\ldots,\lambda_{n-l} \in F_q}} (\lambda_1 z_1 + \ldots + \lambda_{n-l} z_{n-l} + \mu_1 z_{n-l+1} + \ldots + \mu_l z_n) \right)^{1/(q-1)},$$

then $h_{n,n-l} \in F_q[V]^{G_3}$.

P r o o f. We apply induction on $(n-l)$ to prove that $h_{n,n-l} \in F_q[V]$.

First, let $n-l=1$. Since $\lambda_1^{q^i-1} = 1 \in F_q$ for all $i = 0, \ldots, n-1$, and the Euler class is $d_{n-1,0}^{1/(q-1)} = L_{n-1} \in F_q[V]$, we obtain

$$\begin{aligned}
h_{n,1} &= \left(\prod_{\substack{\mu_1,\ldots,\mu_{n-1} \in F_q \text{ not all zeros},\\ \lambda_1 \in F_q}} (\lambda_1 z_1 + \mu_1 z_2 + \ldots + \mu_{n-1} z_n) \right)^{1/(q-1)} \\
&= \left(\prod_{\substack{\mu_1,\ldots,\mu_{n-1} \in F_q \text{ not all zeros},\\ 0 \neq \lambda_1 \in F_q}} (\lambda_1 z_1 + \mu_1 z_2 + \ldots + \mu_{n-1} z_n) \right)^{1/(q-1)} \times d_{n-1,0}^{1/(q-1)} \\
&= \left(\prod_{0 \neq \lambda_1 \in F_q} \left(\sum_{r=0}^{n-1} (d_{n-1,r} \cdot \lambda_1^{q^r-1} \cdot z_1^{q^r-1}) \right) \right)^{1/(q-1)} \times L_{n-1} \\
&= \left(\sum_{r=0}^{n-1} (d_{n-1,r} \cdot z_1^{q^r-1}) \right) \times L_{n-1},
\end{aligned}$$

which belongs to $F_q[V]$.

Suppose that the result is true on $n-l<k$. We now come to $n-l=k$. According to the Euler class $L_{n-k}=d_{n-k,0}^{1/(q-1)}\in F_q[V]$, we have

$$\begin{aligned}
h_{n,k} &= \Bigg(\prod_{\substack{\lambda_1,\ldots,\lambda_k\in F_q\\ \text{not all zeros}}}\Bigg(\prod_{\substack{\mu_1,\ldots,\mu_{n-k}\in F_q\\ \text{not all zeros}}}(\lambda_1 z_1+\ldots+\lambda_k z_k \\
&\qquad +\mu_1 z_{k+1}+\ldots+\mu_{n-k}z_n)\Bigg)\Bigg)^{1/(q-1)}\times d_{n-k,0}^{1/(q-1)} \\
&= \Bigg(\prod_{\substack{\lambda_2,\ldots,\lambda_k\in F_q\\ \text{not all zeros},\\ \lambda_1=0}}\Bigg(\prod_{\substack{\mu_1,\ldots,\mu_{n-k}\in F_q\\ \text{not all zeros}}}((\lambda_2 z_2+\ldots+\lambda_k z_k) \\
&\qquad +\mu_1 z_{k+1}+\ldots+\mu_{n-k}z_n)\Bigg)\Bigg)^{1/(q-1)}\times L_{n-k} \\
&\quad\times\Bigg(\prod_{\substack{\lambda_1\neq 0,\\ \lambda_2,\ldots,\lambda_k\in F_q}}\Bigg(\prod_{\substack{\mu_1,\ldots,\mu_{n-k}\in F_q\\ \text{not all zeros}}}\lambda_1\Big(\Big(z_1+\frac{\lambda_2}{\lambda_1}z_2+\ldots+\frac{\lambda_k}{\lambda_1}z_k\Big) \\
&\qquad +\frac{\mu_1}{\lambda_1}z_{k+1}+\ldots+\frac{\mu_{n-k}}{\lambda_1}z_n\Big)\Bigg)\Bigg)^{1/(q-1)} \\
&= \Bigg(\prod_{\substack{\lambda_2,\ldots,\lambda_k\in F_q\\ \text{not all zeros},\\ \lambda_1=0}}\Bigg(\prod_{\substack{\mu_1,\ldots,\mu_{n-k}\in F_q\\ \text{not all zeros}}}((\lambda_2 z_2+\ldots+\lambda_k z_k) \\
&\qquad +\mu_1 z_{k+1}+\ldots+\mu_{n-k}z_n)\Bigg)\Bigg)^{1/(q-1)}\times L_{n-k} \\
&\quad\times\Bigg(\prod_{\substack{\lambda_1\neq 0,\\ \lambda'_2,\ldots,\lambda'_k\in F_q}}\lambda_1^{q^{n-k}-1}\Bigg(\sum_{r=0}^{n-k}(d_{n-k,r}\cdot(z_1+\lambda'_2z_2+\ldots+\lambda'_kz_k)^{q^r-1})\Bigg)\Bigg)^{1/(q-1)},
\end{aligned}$$

where $d_{n-k,r}$ is the Dickson polynomial in $z_{k+1},\ldots,z_n$ with degree $q^{n-k}-q^r$ for $r=0,\ldots,n-k$, and $\lambda'_j=\lambda_j/\lambda_1$ for $j=2,\ldots,k$.

Denote

$$\begin{aligned}
A &= \Bigg(\prod_{\substack{\lambda_2,\ldots,\lambda_k\in F_q\\ \text{not all zeros},\\ \lambda_1=0}}\Bigg(\prod_{\substack{\mu_1,\ldots,\mu_{n-k}\in F_q\\ \text{not all zeros}}}((\lambda_2 z_2+\ldots+\lambda_k z_k) \\
&\qquad +\mu_1 z_{k+1}+\ldots+\mu_{n-k}z_n)\Bigg)\Bigg)^{1/(q-1)}\times L_{n-k}, \\
B &= \Bigg(\prod_{\substack{\lambda_1\neq 0,\\ \lambda'_2,\ldots,\lambda'_k\in F_q}}\lambda_1^{q^{n-k}-1}\Bigg(\sum_{r=0}^{n-k}(d_{n-k,r}\cdot(z_1+\lambda'_2z_2+\ldots+\lambda'_kz_k)^{q^r-1})\Bigg)\Bigg)^{1/(q-1)}.
\end{aligned}$$

Since

$$A = \left(\prod_{\substack{\mu_1,\ldots,\mu_{n-k}\in F_q \text{ not all zeros},\\ \lambda_2,\ldots,\lambda_k\in F_q}} (\lambda_2 z_2 + \ldots + \lambda_k z_k + \mu_1 z_{k+1} + \ldots + \mu_{n-k} z_n) \right)^{1/(q-1)},$$

we conclude $A \in F_q[V]$ by induction.

In addition, since $\lambda_1^{q^{n-k}-1} = 1 \in F_q$, it follows that

$$B = \left(\left(\prod_{\lambda_2',\ldots,\lambda_k'\in F_q} \left(\sum_{r=0}^{n-k} (d_{n-k,r} \cdot (z_1 + \lambda_2' z_2 + \ldots + \lambda_k' z_k)^{q^r-1}) \right) \right)^{q-1} \right)^{1/(q-1)}$$
$$= \prod_{\lambda_2',\ldots,\lambda_k'\in F_q} \left(\sum_{r=0}^{n-k} (d_{n-k,r} \cdot (z_1 + \lambda_2' z_2 + \ldots + \lambda_k' z_k)^{q^r-1}) \right).$$

Hence $B \in F_q[V]$.

Therefore $h_{n,k} = A \times B \in F_q[V]$.

Since $h_{n,n-l}$ is a $(q-1)$-root of the product of orbits of z_{n-l+1} under the action of the group G_3, we deduce that $h_{n,n-l} \in F_q[V]^{G_3}$. □

Now, we come to the proof of Proposition 4.12.

P r o o f of Proposition 4.12. Referring to Lemma 4.13, it follows that $h_{n,n-l} \in F_q[V]^{G_3}$ and $\deg(h_{n,n-l}) = q^{(n-l)}(q^l - 1)/(q-1)$.

To finish this proof, it will suffice to indicate that $z_1, \ldots, z_{n-l}$, $h_{n,n-l}$, $d_{n,n-l+1}, \ldots, d_{n,n-1}$ form a system of parameters for $F_q[V]^{G_3}$.

For every field extension $\overline{F_q} \supset F_q$, we consider the linear space $\overline{V} = \overline{F_q}^n$. Since $z_1, \ldots, z_{n-l}$ are algebraically independent, it follows that

$$\bigcap_{j=1}^{n-l} \mathrm{Ker}\langle z_j \rangle = \{(0, \ldots, 0, x_{n-l+1}, \ldots, x_n) \colon\ x_{n-l+1}, \ldots, x_n \in \overline{F_q}\}.$$

Next, we consider $\bigcap_{j=n-l+1}^{n-1} \mathrm{Ker}\langle d_{n,j} \rangle \cap \mathrm{Ker}\langle h_{n,n-l} \rangle$. Taking $z_1 = \ldots = z_{n-l} = 0$, we obtain

$$h_{n,n-l} = \left(\left(\prod_{\mu_1,\ldots,\mu_l\in f_q \text{ not all zeros}} (\mu_1 z_{n-l+1} + \ldots + \mu_l z_n) \right)^{q^{n-l}} \right)^{1/(q-1)}$$
$$= (d_{l,0})^{(q^{n-l})/(q-1)} = (L_l)^{q^{n-l}}.$$

In addition, we denote by $d_{n,r}|_{z_1=\ldots=z_{n-l}=0}$ the formula of the Dickson algebra $d_{n,r}$ in which $z_1 = \ldots = z_{n-l} = 0$. Referring to Definition 1.4, we conclude that

$$d_{n,r}|_{z_1=\ldots=z_{n-l}=0} = d_{l,r-n+l} \quad \text{for } r = n-l+1, \ldots, n-1.$$

Since $(L_l)^{q^{n-l}}, d_{l,1}, \ldots, d_{l,l-1}$ with respect to $z_{n-l+1}, \ldots, z_n$ are algebraically independent, it follows that

$$\bigcap_{j=1}^{l-1} \operatorname{Ker}\langle d_{l,j}\rangle \cap \operatorname{Ker}\langle (L_l)^{q^{n-l}}\rangle = \{(x_1, \ldots, x_{n-l}, 0, \ldots, 0) \colon\ x_1, \ldots, x_{n-l} \in \overline{F_q}\}.$$

Moreover,

$$\bigcap_{j=n-l+1}^{n-1} \operatorname{Ker}\langle d_{n,j}\rangle \cap \operatorname{Ker}\langle h_{n,n-l}\rangle \subseteq \bigcap_{j=1}^{l-1} \operatorname{Ker}\langle d_{l,j}\rangle \cap \operatorname{Ker}\langle (L_l)^{q^{n-l}}\rangle.$$

Hence

$$\left(\bigcap_{j=1}^{n-l} \operatorname{Ker}\langle z_j\rangle\right) \cap \left(\bigcap_{j=n-l+1}^{n-1} \operatorname{Ker}\langle d_{n,j}\rangle\right) \cap \operatorname{Ker}\langle h_{n,n-l}\rangle = \{(0, \ldots, 0)\}.$$

Therefore $z_1, \ldots, z_{n-l}, h_{n,n-l}, d_{n,n-l+1}, \ldots, d_{n,n-1}$ form a system of parameters for $F_q[V]^{G_3}$ according to [17], Proposition A.3.6.

In addition, since $\deg(d_{n,r}) = q^n - q^r$ for $r = n-l+1, \ldots, n-1$, this yields that

$$\left(\prod_{j=1}^{n-l} \deg(z_j)\right) \cdot \left(\prod_{r=n-l+1}^{n-1} \deg(d_{n,r})\right) \cdot \deg(h_{n,n-l})$$
$$= (q^n - q^{n-l+1}) \cdot \ldots \cdot (q^n - q^{n-1}) \cdot \frac{q^{n-l} \cdot (q^l - 1)}{q-1} = |G_3|.$$

And the result follows from Proposition 1.6. □

Remark. Since the invariant ring $F_q[V]^{G_3}$ is polynomial, we can also compute $F_q[V]^{G_3}$ by the gluing method in [10]. The result is presented here without computation and proof. Let $d_{l,k}$ be the Dickson polynomial in $z_{n-l+1}, \ldots, z_n$ with degree $q^l - q^k$ for $k = 0, \ldots, l-1$ and $C_{q^{n-l}}(z_t) = \prod_{\mu_1, \ldots, \mu_{n-l} \in F_q} (z_t + \mu_1 z_1 + \ldots + \mu_{n-l} z_{n-l})$ for $t = n-l+1, \ldots, n$. We denote by $d_{l,k}|_{(z_t \mapsto C_{q^{n-l}}(z_t),\ n-l+1 \leqslant t \leqslant n)}$ the formula of the Dickson polynomial $d_{l,k}$ in which $C_{q^{n-l}}(z_t)$ replaces z_t for all $n-l+1 \leqslant t \leqslant n$. According to the gluing method, we calculate

$$F_q[V]^{G_3} = F_q[z_1, \ldots, z_{n-l}, (d_{l,0}|_{(z_t \mapsto C_{q^{n-l}}(z_t),\ n-l+1 \leqslant t \leqslant n)})^{1/(q-1)},$$
$$d_{l,1}|_{(z_t \mapsto C_{q^{n-l}}(z_t),\ n-l+1 \leqslant t \leqslant n)}, \ldots, d_{l,l-1}|_{(z_t \mapsto C_{q^{n-l}}(z_t),\ n-l+1 \leqslant t \leqslant n)}].$$

We can prove that

$$h_{n,n-l} = (d_{l,0}|_{(z_t \mapsto C_{q^{n-l}}(z_t),\ n-l+1 \leqslant t \leqslant n)})^{1/(q-1)},$$
$$d_{n,n-l+r} \neq d_{l,r}|_{(z_t \mapsto C_{q^{n-l}}(z_t),\ n-l+1 \leqslant t \leqslant n)}, \quad r = 1, \ldots, l-1.$$

Hence we have obtained two different systems of parameters for the invariant ring $F_q[V]^{G_3}$.

There are two reasons for preferring the method applied in the proof of Proposition 4.12 to the gluing method. First, the formulas of invariants in Proposition 4.12 are more explicit than the ones obtained by the gluing method. Second, Proposition 4.12 leads to an interesting property of the Dickson polynomials which we do not find in other papers.

We now digress temporarily from studying the invariant ring, in order to deal with the property of the Dickson polynomials.

Proposition 4.14. *Let $d_{n,r}$ denote the Dickson polynomial in $z_1, \ldots, z_n$ with degree $q^n - q^r$ for $r = 0, \ldots, n-1$, then the Euler class $d_{n,0}^{1/(q-1)} = L_n \in F_q[V]$ but other $d_{n,r}^{1/(q-1)} \notin F_q[V]$ for all $r = 1, \ldots, n-1$.*

P r o o f. Denote $F_q = \{0, a_1, a_2 \ldots, a_{q-1}\}$ where $a_1 = 1$. Since $V^* \cong F_q^n$, we consider every element in the dual space V^* as a linear form. So there are totally $(q^n - 1)$ linear forms except 0 and they divide into totally $(q^n - 1)/(q-1)$ linear independent classes. Denote by $\{l_1, \ldots, l_{(q^n-1)/(q-1)}\}$ a complete set of representatives of these $(q^n - 1)/(q-1)$ linear independent classes.

Referring to [17], Proposition 6.1.7, the Dickson polynomial

$$d_{n,r} = (-1)^{n-r}\left(\sum_{\substack{W^* \subseteq V^* \\ \dim(W^*)=r}} \left(\prod_{\substack{z \notin W^* \\ z \in V^*}} z\right)\right)$$

for $r = 0, \ldots, n-1$, where $z \in V^*$ is a linear form.

Given a linear form l_1, there are totally $(q-2)$ nonzero linear dependent forms $a_2 l_1, \ldots, a_{q-1} l_1$ in the dual space V^*. And their product including $l_1 = a_1 l_1$ is

$$\prod_{i=1}^{q-1} (a_i l_1) = l_1^{q-1} \cdot \prod_{i=1}^{q-1} a_i = -l_1^{q-1}$$

according to the field theory. Notice that if $p = 2$, then $-1 = 1$.

We now prove this proposition.

Referring to [19], it follows that the Euler class $d_{n,0}^{1/(q-1)} = L_n \in F_q[V]$. In fact,

$$d_{n,0}^{1/(q-1)} = \left((-1)^n \sum_{\substack{W^* \subseteq V^* \\ \dim(W^*)=0}} \left(\prod_{\substack{z \notin W^* \\ z \in V^*}} z\right)\right)^{1/(q-1)}$$
$$= \left((-1)^n \prod_{j=1}^{(q^n-1)/(q-1)} \left(\prod_{i=1}^{q-1} a_i l_j\right)\right)^{1/(q-1)} = \pm \prod_{j=1}^{(q^n-1)/(q-1)} l_j \in F_q[V].$$

Next, we prove that $d_{n,r}^{1/(q-1)} \notin F_q[V]$ for all $r = 1, \ldots, n-1$.

Since the degree of $d_{n,r}$ is $q^n - q^r$, this yields that $d_{n,r}$ is a sum of products of any $(q^n - q^r)/(q-1)$ linear independent classes, i.e.,

$$d_{n,r} = (-1)^{n-r}\left(\sum_{\dim(W^*)=r} \left(\prod_{\substack{j \in \{1,\ldots,(q^n-1)/(q-1)\} \\ l_j \notin W^*}} \left(\prod_{i=1}^{q-1} a_i l_j\right)\right)\right)$$
$$= (-1)^{n-r}\left(\sum_{\{t_1,\ldots,t_I\} \subseteq \{1,\ldots,(q^n-1)/(q-1)\}} (-1)^I (l_{t_1} \cdot \ldots \cdot l_{t_I})^{q-1}\right)$$

where $I = (q^n - q^r)/(q-1)$. In this formula, $\{t_1, \ldots, t_I\}$ runs over all subsets of $\{1, \ldots, (q^n-1)/(q-1)\}$. Hence the coefficient of the Dickson polynomial $d_{n,r}$ is always ± 1 for $r = 1, \ldots, n-1$. If we have proved $|d_{n,r}|^{1/(q-1)} \notin F_q[V]$, then $d_{n,r}^{1/(q-1)} \notin F_q[V]$. Therefore we omit the coefficient ± 1 for convenience.

We introduce the lexicographical order on $\{l_1, \ldots, l_{(q^n-1)/(q-1)}\}$ with $l_1 > l_2 > \ldots > l_{(q^n-1)/(q-1)}$, and denote

$$S_I = \left(\sum_{\{t_1,\ldots,t_I\} \subseteq \{1,\ldots,(q^n-1)/(q-1)\}} (l_{t_1} \ldots l_{t_I})^{q-1}\right).$$

Notice that the leading term of S_I is $(l_1 \ldots l_I)^{q-1}$.

Our goal is to prove $S_I^{1/(q-1)} \notin F_q[V]$. Suppose that $S_I^{1/(q-1)} = H \in F_q[V]$. Without loss of generality, let

$$H = \sum_j l_1^{a_{j,1}} \ldots l_{(q^n-1)/(q-1)}^{a_{j,(q^n-1)/(q-1)}},$$

where $0 \leqslant a_{j,l} \leqslant (q^n-1)/(q-1)$ for $l = 1, \ldots, (q^n-1)/(q-1)$.

Since S_I is symmetric and homogeneous, so is H, hence $a_{j,1} + \ldots + a_{j,(q^n-1)/(q-1)} = I = (q^n - q^r)/(q-1)$ for every j. Notice that $r \geqslant 1$, so $I = (q^n - q^r)/(q-1) < (q^n-1)/(q-1)$, which forces that there are several zeros among $a_{j,1}, \ldots,$

$a_{j,(q^n-1)/(q-1)}$. We consider the leading term of H, i.e., $j = 1$. According to the lexicographical order, the leading term of H^{q-1} is $\binom{q-1}{0}(l_1^{a_{1,1}} \dots l_{(q^n-1)/(q-1)}^{a_{1,(q^n-1)/(q-1)}})^{q-1}$ and the leading term of S_I is $(l_1 \dots l_I)^{q-1}$. Since $H^{q-1} = S_I$, it follows that

$$\binom{q-1}{0}(l_1^{a_{1,1}} \dots l_{(q^n-1)/(q-1)}^{a_{1,(q^n-1)/(q-1)}})^{q-1} = (l_1 \dots l_I)^{q-1}.$$

Hence $a_{1,1} = \dots = a_{1,I} = 1$ and $a_{1,I+1} = \dots = a_{1,(q^n-1)/(q-1)} = 0$. Since H is symmetric and homogeneous, it follows that

$$H = \sum_{\{t_1,\dots,t_I\} \subseteq \{1,\dots,(q^n-1)/(q-1)\}} (l_{t_1} \dots l_{t_I}),$$

where $\{t_1, \dots, t_I\}$ runs over all subsets of $\{1, \dots, (q^n-1)/(q-1)\}$. Then the leading term of H is $l_1 \dots l_I$ and the second term is $l_1 \dots l_{I-1} l_{I+1}$. Since p does not divide $\binom{q-1}{1} = q-1$, there is a term

$$0 \neq \binom{q-1}{1} \cdot (l_1 \dots l_I)^{q-2} \cdot (l_1 \dots l_{I-1} l_{I+1}) = \ -l_1^{q-1} \dots l_{I-1}^{q-1} l_I^{q-2} l_{I+1}$$

in H^{q-1}, which cannot be a term of S_I since it is not homogeneous. Therefore $H^{q-1} \neq S_I$.

Reasoning as above, we cannot find a polynomial $H \in F_q[V]$ such that $H^{q-1} = S_I$, therefore $d_{n,r}^{1/(q-1)} \notin F_q[V]$ for all $r = 1, \dots, n-1$. □

Finally, we consider the group G_4. Referring to Theorem 4.5, we observe that the matrix forms of elements in the group G_4 are combined with the ones in the group G_2 and the ones in the group G_3 in such a way that the invariant ring $F_q[V]^{G_4}$ can be obtained by combining the invariant rings $F_q[V]^{G_2}$ and $F_q[V]^{G_3}$.

Proposition 4.15. *The invariant ring of the group G_4 is*

$$F_q[V]^{G_4} = F_q[C_{q^t}(z_1), \dots, C_{q^t}(z_{n-t}), z_{n-t+1}, \dots, z_{n-l}, h_{t,t-l}, d_{t,t-l+1}, \dots, d_{t,t-1}],$$

where $C_{q^t}(z_j) = z_j^{q^t} + \sum_{r=0}^{t-1}(d_{t,r} \cdot z_j^{q^r})$ is the top Chern class for $j = 1, \dots, n-t$, $d_{t,r}$ is the Dickson polynomial in $z_{n-t+1}, \dots, z_n$ with degree $q^t - q^r$ for $r = 0, \dots, t-1$, and

$$h_{t,t-l} = \left(\prod_{\substack{\mu_1,\dots,\mu_l \in F_q \text{ not all zeros,} \\ \lambda_1,\dots,\lambda_{t-l} \in F_q}} (\lambda_1 z_{n-t+1} + \dots + \lambda_{t-l} z_{n-l} + \mu_1 z_{n-l+1} + \dots + \mu_l z_n) \right)^{1/(q-1)}.$$

P r o o f. According to Lemma 4.10, it we have that $C_{q^t}(z_1), \ldots, C_{q^t}(z_{n-t})$, $z_{n-t+1}, \ldots, z_{n-l}, h_{t,t-l}, d_{t,t-l+1}, \ldots, d_{t,t-1} \in F_q[V]^{G_4}$. With an argument similar to that shown in the proof of Proposition 4.12, we conclude that they form a system of parameters for the invariant ring $F_q[V]^{G_4}$. In addition, since the product of their degrees is

$$q^{t(n-t)} \cdot \frac{q^{t-l}(q^l-1)}{q-1} \cdot \prod_{j=t-l+1}^{t-1} (q^t - q^j),$$

which is equal to the order of the group G_4, the result follows from Proposition 1.6. □

Remark. Similarly to Proposition 4.12, we can also calculate another system of parameters for the invariant ring $F_q[V]^{G_4}$ by the gluing method [10]. We omit the process here.

Up to now, our calculation of all invariant rings of these four kinds of groups is complete and we utilize our results in the following example.

Example 4.16. We continue the same example discussed in Example 4.4 and Example 4.8. Below is the list of the invariant rings of these groups.

(1) The group $J_1 = \langle T\colon\ T \in \Delta_3 \cup \Delta_4 \cup \Delta_5 \rangle$; then

$$F_q[V]^{J_1} = F_q[L_4, d_{4,1}, d_{4,2}, d_{4,3}],$$

where $d_{4,r}$ is the Dickson polynomial in $z_1, \ldots, z_4$ with degree $q^4 - q^r$ for $r = 0, \ldots, 3$, and $L_4 = d_{4,0}^{1/(q-1)}$ is the Euler class.

(2) The group $J_2 = \langle T\colon\ T \in \Delta_1 \cup \Delta_2 \rangle$; then

$$F_q[V]^{J_2} = F_q[C_{q^2}(z_1), C_{q^2}(z_2), L_2, d_{2,1}],$$

where $C_{q^2}(z_j) = z_j^{q^2} + \sum_{r=0}^{1} (d_{2,r} \cdot z_j^{q^r})$ is the top Chern class for $j = 1, 2$, $d_{2,r}$ is the Dickson polynomial in z_3 and z_4 with degree $q^2 - q^r$ for $r = 0, 1$, and $L_2 = d_{2,0}^{1/(q-1)}$ is the Euler class.

(3) The group $J_3 = \langle T\colon\ T \in \Delta_6 \cup \Delta_7 \rangle$; then

$$F_q[V]^{J_3} = F_q[z_1, h_{4,2}, d_{4,3}, z_4],$$

where $d_{4,3}$ is the Dickson polynomial in $z_1, \ldots, z_4$ with degree $q^4 - q^3$ and

$$h_{4,2} = \left(\prod_{\substack{\mu_1, \mu_2 \in F_q \text{ not all zeros,} \\ \lambda_1, \lambda_2 \in F_q}} (\lambda_1 z_1 + \mu_1 z_2 + \mu_2 z_3 + \lambda_2 z_4) \right)^{1/(q-1)}.$$

(4) The group $J_4 = \langle T\colon\ T \in \Delta_3 \cup \Delta_5 \rangle$; then

$$F_q[V]^{J_4} = F_q[C_{q^3}(z_1), z_2, h_{3,1}, d_{3,2}],$$

where $C_{q^3}(z_1) = z_1^{q^3} + \sum_{r=0}^{2} (d_{3,r} \cdot z_1^{q^r})$ is the top Chern class, $d_{3,r}$ is the Dickson polynomial in $z_2,\ z_3$ and z_4 with degree $q^3 - q^r$ for $r = 0, 1, 2$, and

$$h_{3,1} = \left(\prod_{\substack{\mu_1,\mu_2 \in F_q \text{ not all zeros,} \\ \lambda_1 \in F_q}} (\lambda_1 z_2 + \mu_1 z_3 + \mu_2 z_4) \right)^{1/(q-1)}.$$

Acknowledgment. We were deeply saddened under the shadow of a great loss in the passing of our beloved friend, Chander K. Gupta. We are grateful for her hospitality and assistance during the visit to University of Manitoba in 2015. She will be remembered forever.

We would also like to thank the referee of the paper for helpful comments.

References

[1] *H. Bass*: On the ubiquity of Gorenstein rings. Math. Z. *82* (1963), 8–28. zbl MR doi
[2] *M.-J. Bertin*: Anneaux d'invariants d'anneaux de polynômes, en caractéristique p. C. R. Acad. Sci., Paris, Sér. A *264* (1967), 653–656. (In French.) zbl MR
[3] *A. Braun*: On the Gorenstein property for modular invariants. J. Algebra *345* (2011), 81–99. zbl MR doi
[4] *W. Bruns, J. Herzog*: Cohen-Macaulay Rings. Cambridge Studies in Advanced Mathematics 39, Cambridge University Press, Cambridge, 1998. zbl doi
[5] *H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank, D. L. Wehlau*: Non-Cohen-Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants. Can. Math. Bull. *42* (1999), 155–161. zbl MR doi
[6] *H. Derksen, G. Kemper*: Computational Invariant Theory. Encyclopaedia of Mathematical Sciences 130, Invariant Theory and Algebraic Transformation Groups 1, Springer, Berlin, 2002. zbl MR doi
[7] *L. E. Dickson*: Invariants of binary forms under modular transformations. Amer. M. S. Trans. *8* (1907), 205–232. zbl MR doi
[8] *X. Han, J. Nan, K. Nam*: The invariants of generalized transvection groups in the modular case. Commun. Math. Res. *33* (2017), 160–176.
[9] *M. Hochster, J. A. Eagon*: Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. Am. J. Math. *93* (1971), 1020–1058. zbl MR doi
[10] *J. Huang*: A gluing construction for polynomial invariants. J. Algebra *328* (2011), 432–442. zbl MR doi
[11] *G. Kemper, G. Malle*: The finite irreducible linear groups with polynomial ring of invariants. Transform. Groups *2* (1997), 57–89. zbl MR doi
[12] *J. W. Milnor*: Introduction to Algebraic K-Theory. Annals of Mathematics Studies 72, Princeton University Press and University of Tokyo Press, Princeton, 1971. zbl MR doi

[13] *H. Nakajima*: Invariants of finite groups generated by pseudo-reflections in positive characteristic. Tsukuba J. Math. *3* (1979), 109–122. zbl MR
[14] *H. Nakajima*: Modular representations of abelian groups with regular rings of invariants. Nagoya Math. J. *86* (1982), 229–248. zbl MR doi
[15] *H. Nakajima*: Regular rings of invariants of unipotent groups. J. Algebra *85* (1983), 253–286. zbl MR doi
[16] *M. D. Neusel, L. Smith*: Polynomial invariants of groups associated to configurations of hyperplanes over finite fields. J. Pure Appl. Algebra *122* (1997), 87–105. zbl MR doi
[17] *M. D. Neusel, L. Smith*: Invariant Theory of Finite Groups. Mathematical Surveys and Monographs 94, American Mathematical Society, Providence, 2002. zbl MR doi
[18] *L. Smith*: Some rings of invariants that are Cohen-Macaulay. Can. Math. Bull. *39* (1996), 238–240. zbl MR doi
[19] *L. Smith, R. E. Stong*: On the invariant theory of finite groups: Orbit polynomials and splitting principles. J. Algebra *110* (1987), 134–157. zbl MR doi
[20] *R. P. Stanley*: Invariants of finite groups and their applications to combinatorics. Bull. Am. Math. Soc., New Ser. *1* (1979), 475–511. zbl MR doi
[21] *R. Steinberg*: On Dickson's theorem on invariants. J. Fac. Sci., Univ. Tokyo, Sect. I A *34* (1987), 699–707. zbl MR
[22] *H. You, J. Lan*: Decomposition of matrices into 2-involutions. Linear Algebra Appl. *186* (1993), 235–253. zbl MR doi

Authors' addresses: Xiang Han, Jizhu Nan, School of Mathematical Sciences, Dalian University of Technology, No. 2 Linggong Road, Dalian, 116024, Ganjingzi, Liaoning, P. R. China, e-mail: xianghan328@yahoo.com, jznan@163.com; Chander K. Gupta, Department of Mathematics, University of Manitoba, Machray Hall 420, 186 Dysart Rd, Winnipeg, MB R3T 2M8, Canada.