Bull. Aust. Math. Soc. **85** (2012), 19–25
doi:10.1017/S000497271100253X

THE INVARIANTS FIELD OF SOME FINITE PROJECTIVE LINEAR GROUP ACTIONS

YIN CHEN

(Received 11 April 2011)

Abstract

Let F_q be a finite field with q elements, V an n-dimensional vector space over F_q and $\mathcal{V}$ the projective space associated to V. Let $\mathrm{G} \le \mathrm{GL}_n(F_q)$ be a classical group and PG be the corresponding projective group. In this note we prove that if $F_q(V)^{\mathrm{G}}$ is purely transcendental over F_q with homogeneous polynomial generators, then $F_q(\mathcal{V})^{\mathrm{PG}}$ is also purely transcendental over F_q. We compute explicitly the generators of $F_q(\mathcal{V})^{\mathrm{PG}}$ when G is the symplectic, unitary or orthogonal group.

2010 *Mathematics subject classification*: primary 12F20; secondary 20G40.
Keywords and phrases: invariants field, finite field, projective actions.

1. Introduction

Let F_q be a finite field with q elements, V an n-dimensional vector space over F_q and $\mathcal{V}$ the projective space associated to V. Let G be a classical group contained in the general linear group $\mathrm{GL}_n(F_q)$. It is well known that the center $\mathcal{Z}$ of $\mathrm{GL}_n(F_q)$ consists of the matrices $tI_n (t \in F_q \backslash \{0\})$. The quotient group $\mathrm{G}/(\mathrm{G} \cap \mathcal{Z})$ is said to be the *projective group* associated to G and is denoted by PG. Let $F_q(\mathcal{V}) = F_q(x_1, x_2, \ldots, x_{n-1})$ denote the rational function field over F_q. For each $\sigma \in \mathrm{PG}$, we can choose a preimage $T_\sigma = (t_{ij})$ in G such that σ acts on $F_q(\mathcal{V})$ by the rule

$$\sigma \cdot x_i = \frac{t_{in} + \sum_{j=1}^{n-1} t_{ij} x_j}{t_{nn} + \sum_{j=1}^{n-1} t_{nj} x_j}, \quad 1 \le i \le n-1.$$

The subfield $F_q(\mathcal{V})^{\mathrm{PG}} = \{f \in F_q(\mathcal{V}) : \sigma \cdot f = f \text{ for all } \sigma \in \mathrm{PG}\}$ is called the *invariants field* of PG on $F_q(\mathcal{V})$. One may ask whether $F_q(\mathcal{V})^{\mathrm{PG}}$ is purely transcendental over F_q for a classical group G.

For $\mathrm{G} = \mathrm{GL}_n(F_q)$, Chu *et al.* [3] gave an affirmative answer:

$$F_q(\mathcal{V})^{\mathrm{PGL}_n(F_q)} = F_q(u_1, u_2, \ldots, u_{n-1}),$$

This work was supported by the Fundamental Research Funds for the Central Universities (No. 111494216) and National Natural Science Foundation of China (No. 11026136).

where $u_1 = \tilde{Q}_{n,1}^{(q^n-1)/(q-1)}\tilde{L}_n^{-q^n+q}$ and $u_i = \tilde{Q}_{n,i}\tilde{Q}_{n,1}^{(q^n-q^i)/(q-1)}\tilde{L}_n^{-q^n+q^i}$ for $2 \le i \le n-1$, with

$$\tilde{L}_n = \det\begin{bmatrix} x_1 & x_2 & \cdots & x_{n-1} & 1 \\ x_1^q & x_2^q & \cdots & x_{n-1}^q & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{q^{n-1}} & x_2^{q^{n-1}} & \cdots & x_{n-1}^{q^{n-1}} & 1 \end{bmatrix}$$

and

$$\tilde{Q}_{n,i} = \det\begin{bmatrix} x_1 & x_2 & \cdots & x_{n-1} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{q^{i-1}} & x_2^{q^{i-1}} & \cdots & x_{n-1}^{q^{i-1}} & 1 \\ x_1^{q^{i+1}} & x_2^{q^{i+1}} & \cdots & x_{n-1}^{q^{i+1}} & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{q^n} & x_2^{q^n} & \cdots & x_{n-1}^{q^n} & 1 \end{bmatrix} \cdot \tilde{L}_n^{-1}.$$

The most crucial step in the proof of this result is to reduce the computation of $F_q(\mathcal{V})^{\mathrm{PGL}_n(F_q)}$ to a problem of finding a basis of a free abelian group of rank $n-1$. Using the same strategy, the invariants subfield $F_q(\mathcal{V})^{\mathrm{PSL}_n(F_q)}$ for the special linear group $\mathrm{SL}_n(F_q)$ was also computed in [3].

On the other hand, it is well known that G acts naturally on the rational function field $F_q(V)$ and the invariants field $F_q(V)^{\mathrm{G}}$ is purely transcendental for many classical groups G, such as the symplectic group $\mathrm{Sp}_{2n}(F_q)$, unitary group $\mathrm{U}_n(F_{q^2})$ and orthogonal group $\mathrm{O}_n(F_q)$ (see [1, 2, 4, 5]).

In this note we shall prove a more general result by extending the method in [3] to the classical group G for which $F_q(V)^{\mathrm{G}}$ is purely transcendental with homogeneous polynomial generators. The following Theorem 2.2 is our main result. Applying this theorem, we shall compute explicitly the generators of $F_q(\mathcal{V})^{\mathrm{PSp}_{2n}(F_q)}$ (Corollary 3.2), $F_{q^2}(\mathcal{V})^{\mathrm{PU}_n(F_{q^2})}$ (Corollary 3.3) and $F_q(\mathcal{V})^{\mathrm{PO}_n(F_q)}$(Corollary 3.4).

2. A general result

We first note that the field $F_q(\mathcal{V})$ can be embedded in a field $F_q(y_1, \ldots, y_n)$ in n variables over F_q by defining $x_i = y_1/y_n$ for $i = 1, \ldots, n-1$. Specifically, if g, h are homogeneous polynomials in the polynomial ring $F_q[y_1, \ldots, y_n]$ and we define the degree of g/h by $\deg g/h = \deg g - \deg h$, then $F_q(\mathcal{V})$ is just the set of degree-zero elements in $F_q(y_1, \ldots, y_n)$. Moreover, for each $\sigma \in \mathrm{PG}$, it is easy to see that the action of σ on $F_q(\mathcal{V})$ is the induced action of its preimage T_σ in G on $F_q(y_1, \ldots, y_n)$. Thus $F_q(\mathcal{V})^{\mathrm{PG}}$ is just the set of degree-zero elements in $F_q(y_1, \ldots, y_n)^{\mathrm{G}}$; the latter is well known for many classical groups (see [1, 2, 4, 5]).

https://doi.org/10.1017/S000497271100253X Published online by Cambridge University Press

LEMMA 2.1. *If $F_q(y_1, \dots, y_n)^{\mathrm{G}} = F_q(g_1, \dots, g_n)$ is purely transcendental over F_q, where $g_1, \dots, g_n$ are homogeneous polynomials with degrees $d_1 \le \cdots \le d_n$ respectively, then $F_q(\mathcal{V})^{\mathrm{PG}}$ is generated over F_q by monomials of the form*

$$g_1^{\beta_1} g_2^{\beta_2} \cdots g_n^{\beta_n}, \quad \beta_i \in \mathbb{Z} \text{ and } \sum_{i=1}^{n} \beta_i d_i = 0. \tag{2.1}$$

PROOF. Since each element in $F_q(\mathcal{V})^{\mathrm{PG}}$ is of the form gh^{-1}, where both g and h are F_q-linear combinations of monomials

$$g_1^{\gamma_1} g_2^{\gamma_2} \cdots g_n^{\gamma_n}, \quad \gamma_i \in \mathbb{N} \cup \{0\} \text{ and } \sum_{i=1}^{n} \gamma_i d_i = m,$$

we can choose a fixed n-tuple $(\alpha_1, \dots, \alpha_n)$ such that $\alpha_i \ge 0$ and $\sum_{i=1}^{n} \alpha_i d_i = m$. Let $\beta_i = \gamma_i - \alpha_i$. Then any monomial which may appear in g or h is of the form

$$g_1^{\alpha_1+\beta_1} g_2^{\alpha_2+\beta_2} \cdots g_n^{\alpha_n+\beta_n}, \quad \sum_{i=1}^{n} \beta_i d_i = 0.$$

Dividing both the denominator and numerator in gh^{-1} by $g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_n^{\alpha_n}$ completes the proof. □

Let $\mathcal{N}$ be the free abelian group (written additively) of rank n with free basis $g_1, g_2, \dots, g_n$. We define $\phi : \mathcal{N} \to \mathbb{Z}$ by $g_i \mapsto d_i$, then ϕ is a group homomorphism and so the kernel is

$$\mathrm{Ker}(\phi) = \Big\{ \sum_{i=1}^{n} \beta_i g_i : \sum_{i=1}^{n} \beta_i d_i = 0 \Big\}.$$

Let d be the great common divisor of $d_1, \dots, d_n$. Then the image of ϕ is just $d\mathbb{Z}$. There exist integers $\beta_{01}, \dots, \beta_{0n}$ such that $\sum_{i=1}^{n} \beta_{0i} d_i = d$, thus

$$\phi\Big(\sum_{i=1}^{n} \beta_{0i} g_i \Big) = d$$

and we have

$$\mathcal{N} = \mathrm{Ker}(\phi) \oplus \mathbb{Z}\Big(\sum_{i=1}^{n} \beta_{0i} g_i \Big).$$

Hence $\mathrm{Ker}(\phi)$ is a free abelian group of rank $n-1$. Choose

$$e_1 = \sum_{i=1}^{n} \beta_{1i} g_i, \quad \dots, \quad e_{n-1} = \sum_{i=1}^{n} \beta_{(n-1)i} g_i$$

as a basis of $\mathrm{Ker}(\phi)$. We are now ready to prove the following theorem.

THEOREM 2.2. *If $F_q(y_1, \dots, y_n)^{\mathrm{G}} = F_q(g_1, \dots, g_n)$ is purely transcendental over F_q, where $g_1, \dots, g_n$ are homogeneous polynomials with degrees $d_1 \le \cdots \le d_n$ respectively, then $F_q(\mathcal{V})^{\mathrm{PG}} = F_q(u_1, u_2, \dots, u_{n-1})$, where for $j = 1, \dots, n-1$,*

$$u_j = \prod_{i=1}^{n} g_i(x_1, \dots, x_{n-1}, 1)^{\beta_{ji}}.$$

https://doi.org/10.1017/S000497271100253X Published online by Cambridge University Press

PROOF. Note that the transcendental degree of $F_q(\mathcal{V})^{\mathrm{G}}$ over F_q is equal to $n-1$. By Lemma 2.1 it suffices to show that each monomial f in (2.1) can be generated by $u_1, u_2, \ldots, u_{n-1}$.

Let $f = g_1^{\beta_1} g_2^{\beta_2} \cdots g_n^{\beta_n}$ with $\sum_{i=1}^n \beta_i d_i = 0$. Then the element $\beta_1 g_1 + \cdots + \beta_n g_n$ in $\mathcal{N}$ can be expressed as $k_1 e_1 + \cdots + k_{n-1} e_{n-1}$ for some integers k_i. That is, $f = e_1^{k_1} \cdots e_{n-1}^{k_{n-1}}$. Since each g_i is homogeneous, then

$$\begin{aligned} g_i(y_1, \ldots, y_{n-1}, y_n) &= g_i(x_1 y_n, \ldots, x_{n-1} y_n, y_n) \\ &= y_n^{d_i} g_i(x_1, \ldots, x_{n-1}, 1). \end{aligned}$$

Since $\sum_{i=1}^n \beta_{ji} d_i = 0$ for each $j = 1, \ldots, n-1$, we have

$$\begin{aligned} e_j &= \prod_{i=1}^n \Big(y_n^{\sum_{i=1}^n \beta_{ji} d_i} g_i(x_1, \ldots, x_{n-1}, 1)^{\beta_{ji}} \Big) \\ &= \prod_{i=1}^n g_i(x_1, \ldots, x_{n-1}, 1)^{\beta_{ji}} \\ &= u_j. \end{aligned}$$

This completes the proof. □

3. Some classical groups

In this section, we first compute $F_q(\mathcal{V})^{\mathrm{PSp}_{2n}(F_q)}$ explicitly for the projective symplectic group $\mathrm{PSp}_{2n}(F_q)$. The generators of $F_{q^2}(\mathcal{V})^{\mathrm{PU}_n(F_{q^2})}$ and $F_q(\mathcal{V})^{\mathrm{PO}_n(F_q)}$ can be computed using the same techniques, so the details are omitted.

Let $\mathcal{B}(x, y)$ be the alternating bilinear form on the $2n$-dimensional vector space F_q^{2n} and $B = (b_{ij})$ be the associated matrix of $\mathcal{B}$. Then B is skew-symmetric and the associated symplectic group, $\mathrm{Sp}_{2n}(F_q, \mathcal{B})$ can be written as

$$\mathrm{Sp}_{2n}(F_q, \mathcal{B}) = \{T \in \mathrm{GL}_{2n}(F_q) : T^t B T = B\}.$$

Naturally, the group $\mathrm{Sp}_{2n}(F_q, \mathcal{B})$ can act on $F_q(y_1, y_2, \ldots, y_{2n})$ and we know that the field of invariants $F_q(y_1, y_2, \ldots, y_{2n})^{\mathrm{Sp}_{2n}(F_q, \mathcal{B})} = F_q(S_{2n,1}, S_{2n,2}, \ldots, S_{2n,2n})$, where

$$\begin{aligned} S_{2n,k} &= (y_1, \ldots, y_{2n}) B \begin{pmatrix} y_1^{q^k} \\ \vdots \\ y_{2n}^{q^k} \end{pmatrix} \\ &= \sum_{1 \le i < j \le 2n} b_{ij} (y_i y_j^{q^k} - y_i^{q^k} y_j), \quad k = 1, 2, 3, \ldots. \end{aligned}$$

Note that the degree of $S_{2n,k}$ equals $q^k + 1$. Let

$$d = \gcd\{q + 1, q^2 + 1, \ldots, q^{2n} + 1\}.$$

https://doi.org/10.1017/S000497271100253X Published online by Cambridge University Press

Then $d = \gcd\{q+1, q^2+1, q^4+1, \dots, q^{2^s}+1; 2^{s-1} \le n\}$ since $q+1$ divides q^r+1 for odd positive integers r. Actually, we have the following result.

LEMMA 3.1. *We have $d = 2$ if q is odd, and $d = 1$ if q is even.*

PROOF. We note that $q^2+1 = (q+1)(q-1)+2$. Thus 2 divides $d = \gcd\{q+1, q^2+1\} = \gcd\{q-1, 2\}$. It is clear that $d = 2$ if q is odd, and $d = 1$ if q is even. □

Choose α, β such that $\alpha(q+1) + \beta(q^2+1) = d$. In this case, $(\mathcal{N}, +)$ is the free abelian group of rank $2n$ with free basis $S_{2n,1}, S_{2n,2}, \dots, S_{2n,2n}$. It is easy to see that $S_{2n,k} - ((q^k+1)/d)(\alpha S_{2n,1} + \beta S_{2n,2})$ $(k = 1, 2, \dots, 2n)$ generates $\operatorname{Ker}\phi$. On the other hand, we note that $\operatorname{Ker}\phi$ is a free abelian group of rank $2n-1$ and

$$S_{2n,1} - \frac{q+1}{d}(\alpha S_{2n,1} + \beta S_{2n,2}) = \beta\Big(\frac{q^2+1}{d}S_{2n,1} - \frac{q+1}{d}S_{2n,2}\Big),$$
$$S_{2n,2} - \frac{q^2+1}{d}(\alpha S_{2n,1} + \beta S_{2n,2}) = -\alpha\Big(\frac{q^2+1}{d}S_{2n,1} - \frac{q+1}{d}S_{2n,2}\Big).$$

Thus

$$\Big\{\frac{q^2+1}{d}S_{2n,1} - \frac{q+1}{d}S_{2n,2}\Big\} \cup \Big\{S_{2n,k} - \frac{q^k+1}{d}(\alpha S_{2n,1} + \beta S_{2n,2}), 3 \le k \le 2n\Big\}$$

is just a basis of $\operatorname{Ker}\phi$.

For $k = 1, 2, 3, \dots,$ we define

$$\tilde{S}_{2n,k} = (x_1, \dots, x_{2n-1}, 1)B\begin{pmatrix} x_1^{q^k} \\ \vdots \\ x_{2n-1}^{q^k} \\ 1 \end{pmatrix}.$$

Then by Theorem 2.2 we have the following corollary.

COROLLARY 3.2. (1) *If* char F_q *is not 2, then* $F_q(\mathcal{V})^{\mathrm{PSp}_{2n}(F_q,\mathcal{B})} = F_q(s_1, s_2, \dots, s_{2n-1})$, *where*

$$s_1 = \tilde{S}_{2n,1}^{(q^2+1)/2}\tilde{S}_{2n,2}^{-(q+1)/2},$$
$$s_i = \tilde{S}_{2n,i+1}\tilde{S}_{2n,1}^{((q-1)(q^{i+1}+1))/2}\tilde{S}_{2n,2}^{-(q^{i+1}+1)/2}, \quad 2 \le i \le 2n-1.$$

(2) *If* char F_q *is 2 then $q = 2^s$ for some positive integer s. Note that*

$$(2^{2s-1} - 2^s + 1)(q+1) - 2^{s-1}(q^2+1) = 1.$$

Letting $\alpha = 2^{2s-1} - 2^s + 1$ and $\beta = -2^{s-1}$, then in this case $F_q(\mathcal{V})^{\mathrm{PSp}_{2n}(F_q,\mathcal{B})} = F_q(s_1, s_2, \dots, s_{2n-1})$, where

$$s_1 = \tilde{S}_{2n,1}^{q^2+1}\tilde{S}_{2n,2}^{-(q+1)},$$
$$s_i = \tilde{S}_{2n,i+1}\tilde{S}_{2n,1}^{-\alpha(q^{i+1}+1)}\tilde{S}_{2n,2}^{-\beta(q^{i+1}+1)}, \quad 2 \le i \le 2n-1.$$

https://doi.org/10.1017/S000497271100253X Published online by Cambridge University Press

We conclude this note by giving the explicit generators of invariants fields of projective unitary group and projective orthogonal group.

Let $\rho : a \mapsto a^q$ be the unique involution of F_{q^2}, $\mathcal{H}(x, y)$ be the Hermitian form on the n-dimensional vector space $F_{q^2}^n$ and $H = (h_{ij})$ be the associated matrix of $\mathcal{H}$. Then H is Hermitian and the associated unitary group, $U_n(F_{q^2}, \mathcal{H})$, can be written as $U_n(F_{q^2}, \mathcal{H}) = \{T \in \mathrm{GL}_n(F_{q^2}) : T^t H T^\rho = H\}$. We define

$$\tilde{H}_{n,k} = (x_1, \ldots, x_{n-1}, 1) H \begin{pmatrix} x_1^{q^{2k+1}} \\ \vdots \\ x_{n-1}^{q^{2k+1}} \\ 1 \end{pmatrix}, \quad k = 0, 1, 2, \ldots.$$

Then we have the following corollary.

Corollary 3.3. *We have* $F_{q^2}(\mathcal{V})^{\mathrm{PU}_n(F_{q^2},\mathcal{H})} = F_{q^2}(h_1, h_2, \ldots, h_{n-1})$, *where*

$$h_i = \tilde{H}_{n,i} \tilde{H}_{n,0}^{-(q^{2i+1}+1)/(q+1)}, \quad 1 \le i \le n-1.$$

Assume that char F_q is not 2. Let $\mathcal{O}(x, y)$ be the symmetric bilinear form on the n-dimensional vector space F_q^n and $A = (a_{ij})$ be the associated matrix of $\mathcal{O}$. Then A is symmetric and the associated orthogonal group, $\mathrm{O}_n(F_q, \mathcal{O})$, can be written as $\mathrm{O}_n(F_q, \mathcal{O}) = \{T \in \mathrm{GL}_n(F_q) : T^t A T = A\}$. Define

$$\tilde{A}_{n,k} = (x_1, \ldots, x_{n-1}, 1) A \begin{pmatrix} x_1^{q^k} \\ \vdots \\ x_{n-1}^{q^k} \\ 1 \end{pmatrix}, \quad k = 0, 1, 2, \ldots.$$

We have the following corollary.

Corollary 3.4. *If* char $F_q \neq 2$ *then* $F_q(\mathcal{V})^{\mathrm{PO}_n(F_q,\mathcal{O})} = F_q(w_1, w_2, \ldots, w_{n-1})$, *where*

$$w_i = \tilde{A}_{n,i} \tilde{A}_{n,0}^{-(q^i+1)/2}, \quad 1 \le i \le n-1.$$

Remark 3.5. If char F_q is 2, then up to isomorphisms, the orthogonal groups over F_q are of just three types. We will obtain similar conclusions by applying the same techniques and the result of Tang and Wan [5].

Acknowledgements

This paper was completed during the author's visit to CIM at Nankai University in 2011 under the Scheme of Visiting Scholars. He would like to thank Professor Chengming Bai for his invitation and hospitality. The author is grateful to an anonymous referee for valuable comments and suggestions.

References

[1] D. Carlisle and P. Kropholler, 'Rational invariants of certain orthogonal and unitary groups', *Bull. Lond. Math. Soc.* **24**(1) (1992), 57–60.

[2] H. Chu, 'Supplementary note on "rational invariants of certain orthogonal and unitary groups"', *Bull. Lond. Math. Soc.* **29**(1) (1997), 37–42.

[3] H. Chu, M. C. Kang and E. J. Tan, 'The invariants of projective linear group actions', *Bull. Aust. Math. Soc.* **39**(1) (1989), 107–117.

[4] J. Nan and Y. Chen, 'Rational invariants of certain classical similitude groups over finite fields', *Indiana Univ. Math. J.* **57**(4) (2008), 1947–1957.

[5] Z. Tang and Z. Wan, 'A matrix approach to the rational invariants of certain classical groups over finite fields of characteristic two', *Finite Fields Appl.* **12**(2) (2006), 186–210.

YIN CHEN, School of Mathematics and Statistics, Northeast Normal University, Changchun 130024, PR China
e-mail: ychen@nenu.edu.cn