BULLETIN OF THE
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Volume 16, Number 2, June 1988

ORTHOGONAL GROUP ACTIONS ON RATIONAL FUNCTION FIELDS

BY

HUAH CHU (朱樺)

Abstract. Let F_q be the finite field, Q be a nondegenerate quadratic form on $(F_q)^n$, $O(n, Q)$ the orthogonal group defined by Q. Let $O(n, Q)$ act on the rational function field $K(x_1, \cdots, x_n)$ linearly. We give the generators of the invariant subfields $F_q(x_1, \cdots, x_n)^{O(n,Q)}$, $n = 2, 3$, and show that they are purely transcendental over F_q.

Let K be any field, $K(x_1, \cdots, x_n)$ be the rational function field of n variables, G a finite group of K-automorphisms on $K(x_1, \cdots, x_n)$. A generalized version of Noether's problem asks for which group G and which field K the invariant subfield $K(x_1, \cdots, x_n)^G$ would be purely transcendental over K. Swan [5] gave a counterexample which is the cyclic action on $Q(x_1, \cdots, x_{47})$.

If G acts linearly on $K(x_1, \cdots, x_n)$, that is $G \leq \mathrm{GL}_n(K)$. There are many reasults about the invariants in the case of the field with characteristic 0 (See, e.g. [4]). But the entire theory of invariants of finite groups becomes much more complicated and much less understood in characteristic p.

When $G = \mathrm{GL}_n(F_q)$, Dickson ([2], [6]) first show that $F_q(x_1, \cdots, x_n)^G = F_q(U_{n,0}, U_{n,1}, \cdots, U_{n,n-1})$. The "Dickson invariants" $U_{n,i}$ is defined by

$$\prod_{a_1, \cdots, a_n \in F_q} \{T - (a_1 x_1 + \cdots + a_n x_n)\} = T^{q^n} - U_{n,n-1} T^{q^{n-1}} + \cdots + (-1)^n U_{n,0} T.$$

When $G = \mathrm{PGL}_n(F_q)$, M. Kang, E. T. Tan and the author [1] use "Dickson invariants" to construct $F_q(x_1, \cdots, x_{n-1})^G$ and show that it is also purely transcendental over F_q.

Received by the editors October 5, 1987 and in revised form January 4, 1988.

In this note, we consider the invariants of the orthogonal group actions. Let Q be a nondegenerate quadratic form on $(F_q)^n$, $O(n, Q)$ be the orthogonal group defined by Q. Let $O(n, Q)$ act on $F_q(x_1, \cdots, x_n)$ linearly. We settle the cases of $n=2$ and $n=3$ by showing that $F_q(x, y)^{O(2,Q)}$ and $F_q(x, y, z)^{O(3,Q)}$ are purely transcendental over F_q. We also give the generators for these fields explicitly.

1. **Preliminary.** Let F_q be the finite field with q elements, $R = F_q[x_1, \cdots, x_n]$ be the polynomial ring over F_q and $K = F_q(x_1, \cdots, x_n)$ the rational function field of n variables. Let G be a subgroup of $\mathrm{GL}_n(F_q)$. G acts on R linearly. Namely, for $\sigma = (a_{ij}) \in G$, define

$$\sigma x_i = a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n.$$

This action also induces an action of G on K. Let $R^G := \{f \in R \mid \sigma(f) = f$ for all $\sigma \in G\}$ and $K^G := \{f/g \in K \mid \sigma(f/g) = f/g$ for all $\sigma \in G\}$ be the invariant subring and invariant subfield, respectively. Note that K^G is the quotient field of R^G.

Let $\mathrm{char}\, F_q \neq 2$, $Q(x_1, \cdots, x_n)$ be a nondegenerate quadratic form on $V := (F_q)^n$. A quadratic form of a given rank is determined by its discriminant. Since a quadratic form is diagonalizable, there are the following four types of quadratic forms:

$$\begin{aligned}
&\text{For even } n, \ (\alpha) \quad x_1^2 - x_2^2 + \cdots + x_{n-1}^2 - x_n^2, \\
&\qquad\qquad (\beta) \quad x_1^2 - x_2^2 + \cdots + x_{n-1}^2 - \delta x_n^2; \\
&\text{For odd } n, \ (\gamma) \quad x_1^2 - x_2^2 + \cdots + x_{n-2}^2 - x_{n-1}^2 - x_n^2, \\
&\qquad\qquad (\delta) \quad x_1^2 - x_2^2 + \cdots + x_{n-2}^2 - x_{n-1}^2 - \delta x_n^2,
\end{aligned}$$

where δ is a nonsquare in F_q. The orthogonal group $O(n, Q)$ is defined as $\{\sigma \in \mathrm{GL}_n(F_q) \mid Q(\sigma v) = Q(v)$ for all $v \in V\}$. For $\sigma = (a_{ij}) \in \mathrm{GL}_n(F_q)$, $Q = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \cdots + \alpha_n x_n^2$, $\sigma \in O(n, Q)$ if and only if

$$(a_{ij})^t \begin{bmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{bmatrix} (a_{ij}) = \begin{bmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{bmatrix},$$

that is,

$$(1)\qquad \begin{cases} \sum_{1\le i\le n} \alpha_i a_{ik}^2 = \alpha_k & k = 1, \cdots, n, \\ \sum_{1\le i\le n} \alpha_i a_{il} a_{ik} = 0 & l \neq k. \end{cases}$$

Because $O(V, \delta Q) = O(V, Q)$, the quadratic forms (γ) and (δ) have the same orthogonal group.

In the case of $n = 2$, we take $Q_1 = x^2 - y^2$, $Q_2 = x^2 - \delta y^2$, then $|O(2, Q_1)| = 2(q-1)$, $|O(2, Q_2)| = 2(q+1)$. In the case of $n = 3$, we take $Q = x^2 - y^2 - z^2$, then $|O(3, Q)| = 2q(q^2-1)$. For the detail of this preliminary, we refer to [3, §6.3 and 6.10].

2. We first give the invariants of $O(2, Q)$ action on $F_q(x, y)$.

THEOREM 1. *Let $R = F_q[x, y]$ be the polynomial ring over the finite field F_q, q odd, $K = F_q(x, y)$ the rational function field of two variables. Let $Q_1 = x^2 - y^2$, $Q_2 = x^2 - \delta y^2$, $\delta \notin F_q^2$, be two nondegenerate quadratic forms and $G_i = O(2, Q_i)$ be the orthogonal group determined by Q_i, $i = 1, 2$. Then*

(a) $R^{G_1} = F_q[x^2 - y^2,\ x^{q-1} + x^{q-3}y^2 + \cdots + x^2 y^{q-3} + y^{q-1}]$,
$K^{G_1} = F_q(x^2 - y^2,\ x^{q+1} - y^{q+1})$;

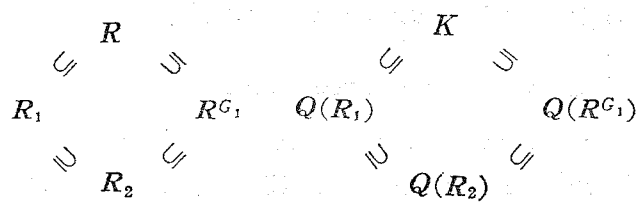
(b) $R^{G_2} = F_q[x^2 - \delta y^2,\ x^{q+1} - \delta y^{q+1}]$,
$K^{G_2} = F_q(x^2 - \delta y^2,\ x^{q+1} - \delta y^{q+1})$.

Moreover, R^{G_1} and R^{G_2} are polynomial rings over F_q, K^{G_1} and K^{G_2} are purely transcendental over F_q.

Proof. (a) Using the identities (1), it is easy to check that $x^2 - y^2$ and $x^{q+1} - y^{q+1}$ are invariants. Since

$$x^{q-1} + x^{q-3}y^2 + \cdots + x^2 y^{q-3} + y^{q-1} = x^{q+1} - y^{q+1}/x^2 - y^2,$$

so $R_2 := F_q[x^2 - y^2,\ x^{q-1} + x^{q-3}y^2 + \cdots + y^{q-1}] \subset R^{G_1}$. Set $u := x^2 - y^2$, $R_1 := F_q[x^2, y^2] = F_q[x^2 - y^2, y^2]$ and let $Q(R_i)$ be the quotient field of R_i. Consider the following sequence of subrings:



Since

$$x^{q-1} + x^{q-3}y^2 + \cdots + y^{q-1} = \frac{(u + y^2)^{(q+1)/2} - y^{q+1}}{u}$$
$$= \left(\frac{q-1}{2}\right) y^{q-1} + (\text{lower terms}),$$

R_1 is integral over R_2 and $[Q(R_1) : Q(R_2)] = (q-1)/2$. Moreover, $[K : Q(R_1)] = 4$. Thus R is integral over R_2 and $[K : Q(R_2)] = 2(q-1)$. From the Galois theory, $[K : Q(R^{G_1})] = |G| = 2(q-1)$, so $K^G = Q(R^{G_1}) = Q(R_2) = F_q(x^2 - y^2, x^{q+1} - y^{q+1})$.

Since the transcendence degree of R_2 over F_q is two and R_2 is generated by two elements, R_2 is a polynomial ring. On the other hand, R^{G_1} is integral ever R_2 and R_2 is integrally closed. Thus $R^{G_1} = R_2$.

The proof of (b) is similar to that of (a). If we set $u' := x^2 - \delta y^2$, then

$$x^{q+1} - \delta y^{q+1} = (u' + \delta y^2)^{(q+1)/2} - \delta y^{q+1}$$
$$= (\delta^{(q+1)/2} - \delta)\, y^{q+1} + (\text{lower terms}).$$

Since δ is a nonsquare, $\delta^{(q+1)/2} \neq \delta$. Thus $F_q[x^2, y^2]$ is integral over $F_q[x^2 - \delta y^2, x^{q+1} - \delta y^{q+1}]$, $[F_q(x^2, y^2) : F_q(x^2 - \delta y^2, x^{q+1} - \delta y^{q+1})] = (q+1)/2$. Note that $|G_2| = 2(q+1)$. All other arguments are the same as (a).

3. Next we find the invariants of $O(3, Q)$ action on $F_q(x, y, z)$.

THEOREM 2. *Let $K = F_q(x, y, z)$ be the rational function field over F_q, q an odd prime power. Let $Q = x^2 - y^2 - z^2$ be a nondegenerate quadratic form and $G = O(3, Q)$ be the orthogonal group determined by Q. Then*

$$K^G = F_q(x^2 - y^2 - z^2,\ x^{q+1} - y^{q+1} - z^{q+1},\ x^{q^2+1} - y^{q^2+1} - z^{q^2+1})$$

and which is purely transcendental over F_q.

Proof. We prove it by three steps.

First step: It is easy to check that $x^2 - y^2 - z^2$, $x^{q+1} - y^{q+1} - z^{q+1}$, $x^{q^2+1} - y^{q^2+1} - z^{q^2+1}$ are invariants. Since $[K : K^G] = |G| = 2q(q^2-1)$,

hence it is enough to prove that

$$[K : F_q(x^2 - y^2 - z^2,\ x^{q+1} - y^{q+1} - z^{q+1},\ x^{q^2+1} - y^{q^2+1} - z^{q^2+1})] = 2q(q^2 - 1).$$

Set

$$K_1 := F_q(x^2 - y^2 - z^2,\ x^{q+1} - y^{q+1} - z^{q+1},\ z) = F_q(x^2 - y^2,\ x^{q+1} - y^{q+1},\ z),$$

$$K_2 := F_q(x^2 - y^2 - z^2,\ x^{q+1} - y^{q+1} - z^{q+1},\ x^{q^2+1} - y^{q^2+1} - z^{q^2+1}).$$

Then $K \supset K_1 \supset K_2$. From the result of Theorem 1(a), $[K : K_1] = 2(q-1)$. It remains to show that $[K_1 : K_2] = q(q+1)$.

Second step: Since $x^{q^2+1} - y^{q^2+1} \in F_q[x, y]^{G_1}$ where $G_1 = O(2, Q_1)$ is defined as in Theorem 1, so there are uniquely determined γ, α_i and $\beta_j \in F_q$ such that

$$\begin{aligned} x^{q^2+1} - y^{q^2+1} = {} & \gamma\left(\frac{x^{q+1} - y^{q+1}}{x^2 - y^2}\right)^{q+1}(x^2 - y^2) \\ & + \sum_{1 \le i \le (q+1)/2} \alpha_i \left(\frac{x^{q+1} - y^{q+1}}{x^2 - y^2}\right)^{q+1-2i} \\ & \quad \cdot (x^2 - y^2)^{i(q-1)+1} \\ & + \sum_{1 \le j \le (q+1)/2} \beta_j \left(\frac{x^{q+1} - y^{q+1}}{x^2 - y^2}\right)^{q+2-2j} \\ & \quad \cdot (x^2 - y^2)^{j(q-1)-(q-3)/2}. \end{aligned} \tag{2}$$

Divide (2) by $x^2 - y^2$ and set $x = y$. Then

$$\frac{q^2+1}{2} = \gamma\left(\frac{q+1}{2}\right)^{q+1} = \gamma\left(\frac{q+1}{2}\right)^2.$$

It follows that $\gamma = 2$. Multiplying (2) by $(x^2 - y^2)^q$, we get

$$\begin{aligned} & - x^{(q+1)^2} + 2x^{q^2+q}y^{q+1} - x^{q^2+1}y^{2q} - y^{2q}x^{q^2+1} \\ & \qquad + 2x^{q+1}y^{q^2+q} - y^{(q+1)^2} \\ & = \sum_{1 \le i \le (q+1)/2} \alpha_i (x^{q+1} - y^{q+1})^{q+1-2i}(x^2 - y^2)^{i(q+1)} \\ & \qquad + \sum_{1 \le j \le (q+1)/2} \beta_j (x^{q+1} - y^{q+1})^{q+2-2j} \\ & \qquad\quad \cdot (x^2 - y^2)^{j(q+1)-(q+1)/2}. \end{aligned}$$

Comparing the coefficients of $x^{(q+1)^2}$, we have

$$-1 = \sum_{1\le i\le (q+1)/2} \alpha_i + \sum_{1\le j\le (q+1)/2} \beta_j. \tag{3}$$

Comparing the coefficients of $x^{(q+1)^2-2k}y^{2k}$, $1 \le k \le (q-1)/2$, we have

$$0 = \sum_{1\le i\le (q+1)/2} (-1)^k \binom{i(q+1)}{k} \alpha_i + \sum_{1\le j\le (q+1)/2} (-1)^k \binom{j(q+1) - (q+1)/2}{k} \beta_j . \tag{4}$$

Using the mod p combinatorial identities

$$\binom{aq+b}{c} \equiv \binom{b}{c} \pmod{p} \tag{5}$$

for $q = p^\alpha$ and $0 \le b,\ c < q$, (4) becomes

$$0 = \sum_{1\le i\le (q+1)/2} \binom{i}{k} \alpha_i + \sum_{1\le j\le (q+1)/2} \binom{(q-1)/2 + j}{k} \beta_j . \tag{6}$$

The system of equations (3), (6) has a unique solution by (2). If we set $\beta_1 = \cdots = \beta_{(q+1)/2} = 0$ in (3), (6), we get

$$\begin{cases} \displaystyle\sum_{1\le i\le (q+1)/2} \alpha_i = -1 \\ \displaystyle\sum_{1\le i\le (q+1)/2} \binom{i}{k} \alpha_i = 0, \qquad 1 \le k \le (q-1)/2 . \end{cases} \tag{7}$$

It is not difficult to check that the matrix

$$\begin{pmatrix} \binom{1}{0} & \binom{2}{0} & \cdots & \binom{(q+1)/2}{0} \\ \binom{1}{1} & \binom{2}{1} & \cdots & \binom{(q+1)/2}{1} \\ \vdots & \vdots & & \vdots \\ \binom{1}{(q-1)/2} & \binom{2}{(q-1)/2} & \cdots & \binom{(q+1)/2}{(q-1)/2} \end{pmatrix}$$

has determinant $\not\equiv 0 \pmod{p}$. Here we adopt the conventions $\binom{a}{b} = 0$ if $a < b$ and $\binom{a}{0} = 1$. Hence the solution of (3), (6) is $(\alpha_1, \cdots, \alpha_{(q+1)/2}, 0, \cdots, 0)$ where $\{\alpha_i\}$ satisfy (7).

Third step: Let $u := x^2 - y^2$, $v := x^{q+1} - y^{q+1}$. Using (2) and the fact that $\beta_i = 0$, we have

$$x^{q^2+1} - y^{q^2+1} - z^{q^2+1}$$
$$= 2\left(\frac{v}{u}\right)^{q+1} u + \sum_{1\le i\le (q+1)/2} \alpha_i \left(\frac{v}{u}\right)^{q+1-2i} u^{i(q-1)+1} - z^{q^2+1},$$

where $\{\alpha_i\}$ satisfy (7). Set $\bar{u} := u - z^2$, $\bar{v} := v - z^{q+1}$. Then

$$x^{q^2+1} - y^{q^2+1} - z^{q^2+1}$$
$$= 2\frac{(\bar{v} + z^{q+1})^{q+1}}{(\bar{u} + z^2)^q}$$
$$+ \sum_{1\le i\le (q+1)/2} \alpha_i (\bar{v} + z^{q+1})^{q+1-2i} (\bar{u} + z^2)^{i(q+1)-q} - z^{q^2+1}$$
$$= \frac{1}{(z^2 + \bar{u})^q} \Big\{ 2(z^{q+1} + \bar{v})^{q+1}$$
$$+ \sum_{1\le i\le (q+1)/2} \alpha_i (z^{q+1} + \bar{v})^{q+1-2i} (z^2 + \bar{u})^{i(q+1)}$$
$$- z^{q^2+1}(z^2 + \bar{u})^q \Big\}.$$

The coefficient of $z^{(q+1)^2}$ in the numerator is

$$2 + \alpha_1 + \cdots + \alpha_{(q+1)/2} - 1. \tag{8}$$

The coefficients of $z^{(q+1)^2-2k}$, $1 \le k \le (q-1)/2$, are

$$\left[\binom{q+1}{k}\alpha_1 + \binom{2(q+1)}{k}\alpha_2 + \cdots + \binom{((q+1)/2)(q+1)}{k}\alpha_{(q+1)/2}\right]\bar{u}^k$$
$$= \left[\sum_{1\le i\le (q+1)/2} \binom{i}{k}\alpha_i\right]\bar{u}^k. \tag{9}$$

Here we use the identities (5). The coefficient of z^{q^2+q} is

$$2(q+1)\bar{v} + \sum_{1\le i\le (q+1)/2} \alpha_i \binom{i(q+1)}{(q+1)/2} \bar{u}^{(q+1)/2} + \sum \alpha_i (q + 1 - 2i)\bar{v}$$
$$= \left[2 + \sum_{1\le i\le (q+1)/2} (1-2i)\alpha_i\right]\bar{v} + \alpha_{(q+1)/2}\,\bar{u}^{(q+1)/2}$$
$$= \bar{v} + \alpha_{(q+1)/2}\,\bar{u}^{(q+1)/2} \neq 0,$$

since $2 + \sum \alpha_i = 1$ and $\sum i\alpha_i = 0$. From the identities (7), the coefficients in (8) and (9) are all zero. Therefore

$$x^{q^2+1} - y^{q^2+1} - z^{q^2+1}$$
$$= \frac{1}{(z^2 + \bar{u})^q} \{(\bar{v} + \alpha_{(q+1)/2}\,\bar{u}^{(q+1)/2})\, z^{q^2+q} + \cdots\}.$$

Since $K_1 = F_q(\bar{u}, \bar{v}, z)$, $K_2 = F_q(\bar{u}, \bar{v}, x^{q^2+1} - y^{q^2+1} - z^{q^2+1})$, it follows that $[K_1 : K_2] = q(q+1)$. The theorem is proved.

REMARKS. (1) The invariants of $O(3, Q)$ action of $F_q[x, y, z]$ are not so easy to determine. For example, if $q = 3$ the invariant subring is $F_3[x^2 - y^2 - z^2,\ x^4 - y^4 - z^4,\ x^2(y^2 - z^2)^2]$

(2) Let $Q(x_1, \cdots, x_n)$ be a nondegenerate quadratic form. Define the polynomials

$$P_i(x_1, \cdots, x_n) = Q(x_1^{(q^i+1)/2}, \cdots, x_n^{(q^i+1)/2}), \quad \text{for } i = 0, 1, 2, \cdots$$

Note that $P_0 = Q$. It is not difficult to check that P_i are invariant under the $O(n, Q)$ action. We conjecture that: the invariant subfield of $O(n, Q)$ action on $F_q(x_1, \cdots, x_n)$ is $F_q(P_0, P_1, \cdots, P_{n-1})$. But we can't prove it for the cases of $n > 3$.

REFERENCES

1. H. Chu, M. Kang and E. T. Tan, *The invariants of the projective linear group actions*, Preprint.

2. L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc., 12 (1911), 75-98.

3. N. Jacobson, *Basic Algebra* I, the first edition, W. H. Freeman and Comp, 1974, San Francisco.

4. R. P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer, Math. Soc., 1 (1979), 475-511.

5. R. G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math., 7 (1969), 148-158.

6. C. Wilkson, *A primer on the Dickson invariants*, in "Proc. of the Northwestern Homotopy Theory Conference", Contemporary Math., 19 (1983), 421-434.

Department of Mathematics
National Taiwan University
Taipei, Taiwan, R. O. C.