BULL. AUSTRAL. MATH. SOC. 12F20, 20G40
VOL. 48 (1993) [313–319]

THE INVARIANTS OF ORTHOGONAL GROUP ACTIONS

LI CHIANG AND YU-CHING HUNG

Let F_q be the finite field of order q, an odd number, Q a non-degenerate quadratic form on F_q^n, $O(n, Q)$ the orthogonal group defined by Q. Regard $O(n, Q)$ as a linear group of F_q-automorphisms acting linearly on the rational function field $F_q(x_1, \ldots, x_n)$. We shall prove that the invariant subfield $F_q(x_1, \ldots, x_n)^{O(n,Q)}$ is a purely transcendental extension over F_q for $n = 5$ by giving a set of generators for it.

1. INTRODUCTION

Let F_q be the finite field of odd prime power order q, $Q(x_1, \ldots, x_n)$ a nondegenerate quadratic form on $V := F_q^n$. The orthogonal group $O(n, Q)$ determined by $Q(x_1, \ldots, x_n)$ is defined as $\{\sigma \in GL(n, F_q) : Q(\sigma \mathbf{v}) = Q(\mathbf{v}) \text{ for all } \mathbf{v} \in F_q^n\}$. Because a quadratic form is diagonalisable, $Q(x_1, \ldots, x_n)$ can be represented in one of the following forms:

$$Q(x_1, \ldots, x_n) = x_1^2 - x_2^2 + x_3^2 - \ldots - x_{n-1}^2 - \varepsilon x_n^2 \quad \text{for odd } n,$$

or

$$Q(x_1, \ldots, x_n) = x_1^2 - x_2^2 + x_3^2 - \ldots + x_{n-1}^2 - \varepsilon x_n^2 \quad \text{for even } n,$$

where $\varepsilon = 1$ or $\varepsilon = \delta$, a nonsquare in F_q. Since $O(n, \delta Q) = O(n, Q)$, $Q(x_1, \ldots, x_n)$ can be specified uniquely when n is odd [4, Section 6.3, 6.10]. The orthogonal group $O(n, Q)$, a subgroup of $GL(n, F_q)$, acts as a linear group of F_q-automorphisms on the polynomial ring $F_q[x_1, \ldots, x_n]$ and on the rational function field $F_q(x_1, \ldots, x_n)$ in a natural way.

For convenience, we introduce some notations defined as in [3, p.217, 218]: $R_n := F_q[x_1, \ldots, x_n]$, $K_n := F_q(x_1, \ldots, x_n)$, $K_n^+ := K_n^{O(n,Q)}$, $R_n^+ := R_n^{O(n,Q)}$, $Q_n(i) := Q\left(x_1^{(q^i+1)/2}, \ldots, x_n^{(q^i+1)/2}\right)$ and $K_n^* := F_q(Q_n(0), \ldots, Q_n(n-1))$. It is noted in [2] that $Q_n(i)$ is invariant under $O(n, Q)$ for each $i \geqslant 0$. Thus, the invariant subfield K_n^+ contains K_n^*.

Received 28 October 1992
Partially supported by the National Science Council of the Republic of China under grant NSC 81-0208-M-003-04.

In 1988, Chu [2] conjectured that K_n^+ is exactly K_n^* for all n, and that K_n^+ is purely transcendental over F_q. Chu [2] has proved his conjecture for $n = 2, 3$. In 1989, Cohen [3] proved the case $n = 4$. They also obtained the invariant subring R_n^+ for $n = 2, 3$. But they could not prove the conjecture for higher values of n. A full solution of this problem has been given in [1] by Carlisle and Kropholler, making use of Dickson's invariant theorem. In this note, we provide a proof for $n = 5$ (Section 3) without using Dickson's invariant theorem. We also give a set of generators of the invariant subring R_4^+ (Section 2, Theorem 3). Our main theorem is following:

THEOREM 1. *For $n \leqslant 5$, $K_n^+ = K_n^*$, which is purely transcendental over F_q.*

2. THE INVARIANT SUBRING OF $O(4, Q)$ ACTING ON $F_q[x, y, z, t]$

Through this section, δ denotes a fixed nonsquare in F_q. We let

$$Q_4(x, y, z, t) = x^2 + y^2 - \delta z^2 - t^2 \quad \text{(a form in four variables).} \tag{1}$$

For $Q_2(x, y) = x^2 - \delta y^2$, $Q_2(2)$ and $Q_2(3)$ are in $R_2^+ = F_q[Q_2(0), Q_2(1)]$ [2, Theorem 1]. Thus there exist two 2-variable polynomials $f(u, v)$ and $g(u, v)$ such that

$$Q_2(2) = f(Q_2(0), Q_2(1)) \quad \text{and} \quad Q_2(3) = g(Q_2(0), Q_2(1)). \tag{2}$$

For $Q_3(x, y, z) = x^2 + y^2 - \delta z^2$ or $Q_3(x, y, z) = -x^2 + y^2 + \delta z^2$ we have the following theorem. The proof is similar to that of [3, Theorem 1.2].

THEOREM 2. *Let $Q_3(x, y, z) = x^2 + y^2 - \delta z^2$ or $Q_3(x, y, z) = -x^2 + y^2 + \delta z^2$. Then*

$$R_3^+ = F_q[Q_3(0), Q_3(1), Q_3^*],$$

where

$$Q_3^* = \frac{Q_3(2) - Q_3(0)^{(q^2+1)/2}}{Q_3(1) + Q_3(0)^{(q+1)/2}}. \tag{3}$$

In fact, by [4, Section 6.3], the invariant ring R_3^+ is the same as that in [3, Theorem 1.2].

Our main theorem in this section is following:

THEOREM 3. *Let Q_4 be defined by (1). Then $R_4^+ = F_q[Q_4(0), Q_4(1), Q_4(2), Q_4^*]$ with*

$$Q_4^* = \frac{Q_4(3) - g(Q_4(0), Q_4(1))}{Q_4(2) - f(Q_4(0), Q_4(1))}$$

where f and g are as in (2).

The following lemma is an important key to the proof of Theorem 3.

https://doi.org/10.1017/S0004972700015720 Published online by Cambridge University Press

LEMMA 4. *Let $a(u, v, w, s)$ be a polynomial in the polynomial ring $F_q[u, v, w, s]$. If $a(Q_2(0), Q_2(1), Q_2(2), Q_2(3)) = 0$, then $a(u, v, w, s)$ is in the ideal generated by $A(u, v, w)$ and $B(u, v, s)$, where $A(u, v, w) = w - f(u, v) \in F_q[u, v, w, s]$, $B(u, v, s) = s - g(u, v) \in F_q[u, v, w, s]$ and f, g are as in (2).*

PROOF: $A(u, v, w)$ and $B(u, v, s)$ are monic polynomials with respect to w and s. Applying the division algorithm, we get

$$a(u, v, w, s) = B(u, v, s)p(u, v, w, s) + A(u, v, w)q(u, v, w) + r(u, v)$$

where $p(u, v, w, s)$, $q(u, v, w)$ and $r(u, v)$ are in $F_q[u, v, w, s]$. Because $a(Q_2(0), Q_2(1), Q_2(2), Q_2(3)) = 0$, $B(Q_2(0), Q_2(1), Q_2(3)) = 0$ and $A(Q_2(0), Q_2(1), Q_2(2)) = 0$, we have $r(Q_2(0), Q_2(1)) = 0$. But $Q_2(0)$ and $Q_2(1)$ are algebraically independent over F_q, whence $r(u, v) = 0$. □

We now prove Theorem 3. Let $Q_3(x, y, z) = x^2 + y^2 - \delta z^2 \in F_q[x, y, z]$. Because $Q_3(3) \in R_3^+$, by Theorem 2, there exists a three-variable polynomial h_1 such that $Q_3(3) = h_1(Q_3(0), Q_3(3), Q_3^*)$, where Q_3^* is defined by (3), and the degree in the third variable of h_1 does not exceed $q + 1$ [3, (4.5)]. Therefore, there are another three-variable polynomial h and some positive integer $d \leqslant q + 1$ such that

$$Q_4(3)[Q_3(1) + Q_3(0)^{(q+1)/2}]^d + h(Q_3(0), Q_3(1), Q_3(2)) = 0. \tag{4}$$

By [1] we can deduce that d can be taken to be q, but we shall prove this ourselves. Substituting $Q_3(i) = x^2 + y^2 - \delta z^2 = Q_4(i) + t^2$ into (3), we have

$$\begin{aligned}\left(Q_4(3) + t^{q^3+1}\right)[(Q_4(1) + t^{q+1}) + (Q_4(0) + t^2)^{(q+1)/2}]^d \\ + h\left(Q_4(0) + t^2, Q_4(1) + t^{q+1}, Q_4(2) + t^{q^3+1}\right) = 0.\end{aligned}$$

Hence there is a polynomial

$$\begin{aligned}G(u, v, w, s, t) = \left(s + t^{q^3+1}\right)[(v + t^{q+1}) + (u + t^2)^{(q+1)/2}]^d \\ + h\left(u + t^2, v + t^{q+1}, w + t^{q^3+1}\right)\end{aligned} \tag{5}$$

such that

$$G(Q_4(0), Q_4(1), Q_4(2), Q_4(3), t) = 0. \tag{6}$$

We write G as

$$G(u, v, w, s, t) = \sum_{k=0}^{M} a_k(u, v, w, s)t^k, \quad a_M(u, v, w, s) \neq 0. \tag{7}$$

https://doi.org/10.1017/S0004972700015720 Published online by Cambridge University Press

Let $Q_2 = y^2 - \delta z^2$. There is no difference between $Q_2 + t^2 = y^2 - \delta z^2 + t^2$ and $Q_4 + t^2 = x^2 + y^2 - \delta z^2$ other than interchanging t and x, thus

$$G(Q_2(0), Q_2(1), Q_2(2), Q_2(3), t) = \sum_{k=0}^{M} a_k(Q_2(0), Q_2(1), Q_2(2), Q_2(3))t^k = 0.$$

Because $Q_2 = y^2 - \delta z^2$ is independent of t, then $a_k(Q_2(0), Q_2(1), Q_2(2), Q_2(3)) = 0$ for all $k = 0, 1, \ldots, M$. By Lemma 4, all $a_k(u, v, w, s)$ must be in the ideal generated by $A(u, v, w)$ and $B(u, v, s)$. If the coefficient a_k contains no s, then $A(u, v, w)$ is a factor of $a_k(u, v, w)$. Combining this with (5), we have

$$\begin{aligned} G(u, v, w, s, t) = [s - g(u, v)]\left[\left(v + t^{q+1}\right) + \left(u + t^2\right)^{(q+1)/2}\right]^d \\ + [w - f(u, v)]h_2(u, v, w, t) \end{aligned}$$

for some polynomial $h_2(u, v, w, t) \in F_q[u, v, w, t]$. Now by (6),

$$\begin{aligned} &[Q_4(3) - g(Q_4(0), Q_4(1))]\left[\left(Q_4(1) + t^{q+1}\right) + \left(Q_4(0) + t^2\right)^{(q+1)/2}\right]^d \\ &\quad = -[Q_4(2) - f(Q_4(0), Q_4(1))]h_2(Q_4(0), Q_4(1), Q_4(2), t). \end{aligned}$$

Then

$$\begin{aligned} Q_4(2) - f(Q_4(0), Q_4(1)) \mid [Q_4(3) - g(Q_4(0), Q_4(1))]\left[\left(Q_4(1) + t^{q+1}\right)\right. \\ \left. + \left(Q_4(0) + t^2\right)^{(q+1)/2}\right]^d. \end{aligned}$$

(Notation: $a \mid b$ means a is a factor of b.) Applying the same method and replacing $Q = x^2 + y^2 - \delta z^2$ with $Q = -x^2 + t^2 + \delta z^2$, we get that

$$\begin{aligned} Q_4(2) - f(Q_4(0), Q_4(1)) \mid [Q_4(3) - g(Q_4(0), Q_4(1))]\left[\left(-Q_4(1) + y^{q+1}\right)\right. \\ \left. + \left(-Q_4(0) + y^2\right)^{(q+1)/2}\right]^d. \end{aligned}$$

By symmetry, we also get

$$\begin{aligned} Q_4(2) - f(Q_4(0), Q_4(1)) \mid [Q_4(3) - g(Q_4(0), Q_4(1))]\left[\left(-Q_4(1) + x^{q+1}\right)\right. \\ \left. + \left(-Q_4(0) + x^2\right)^{(q+1)/2}\right]^d. \end{aligned}$$

Since there is no common non-unit factor of $\left[\left(-Q_4(1) + y^{q+1}\right) + \left(-Q_4(0) + y^2\right)^{(q+1)/2}\right]^d$, $\left[\left(-Q_4(1) + x^{q+1}\right) + \left(-Q_4(0) + x^2\right)^{(q+1)/2}\right]^d$ and $\left[\left(Q_4(1) + t^{q+1}\right) + \left(Q_4(0) + t^2\right)^{(q+1)/2}\right]^d$, we have

$$Q_4(2) - f(Q_4(0), Q_4(1)) \mid [Q_4(3) - g(Q_4(0), Q_4(1))]. \tag{8}$$

Hence, we conclude that

$$Q_4^* = \frac{Q_4(3) - g(Q_4(0), Q_4(1))}{Q_4(2) - f(Q_4(0), Q_4(1))} \in F_q[x, y, z, t].$$

and also that

$$Q_4(2) - f(Q_4(0), Q_4(1)) \mid a_k(Q_4(0), Q_4(1), Q_4(2), Q_4(3))$$

for all $k = 0, \ldots, M$. Moreover, if we set $t = 0$ or $y = 0$ in (8) we get

$$Q_3(2) - f(Q_3(0), Q_3(1)) \mid Q_3(3) - g(Q_3(0), Q_3(1))$$

for the quadratic form $Q_3 = x^2 + y^2 - \delta z^2$ or $Q_3 = -x^2 + t^2 + \delta z^2$. By [3, Lemma 2.4], we have

$$w - f(u, v) \equiv \left(w - u^{(q^2+1)/2}\right) \quad \left(\text{mod } v + u^{(q+1)/2}\right).$$

But, by Theorem 2, we have

$$Q_3(1) + Q_3(0)^{(q+1)/2} \mid Q_3(2) - Q_3(0)^{(q^2+1)/2}.$$

Then

$$Q_3(1) + Q_3(0)^{(q+1)/2} \mid Q_3(2) - f(Q_3(0), Q_3(1))$$

and therefore $Q_3(1) + Q_3(0)^{(q+1)/2}$ is a factor of $Q_3(3) - g(Q_3(0), Q_3(1))$. So,

$$\frac{Q_3(3) - g(Q_3(0), Q_3(1))}{Q_3(1) + Q_3(0)^{(q+1)/2}} \in R_3^+ = F_q[Q_3(0), Q_3(1), Q_3^*].$$

Then

$$(9) \qquad Q_3(3) - g(Q_3(0), Q_3(1)) = \left(Q_3(1) + Q_3(0)^{(q+1)/2}\right) h_3(Q_3(0), Q_3(1), Q_3^*)$$

where the polynomial h_3 is in $F_q[Q_3(0), Q_3(1), Q_3^*]$ and the degree in Q_3^* of h_3 does not exceed $q+1$. This can be proved by counting the homogeneous degrees. Comparing (4) and (9), we conclude that $d \leqslant q$ if we minimise d. By [3, Theorem 1.1] and [4, Theorem 6.17], t has $[K_3^+(t) : K_4^+] = [K_4 : K_4^+]/[K_4 : K_3^+(t)] = |O(4, Q_4)| / |O(3, Q_3)| = q^3 + q$ conjugates in K_4 over K_4^+. Thus the highest power of t in the polynomial $G(u, v, w, s, t)$ is not less than $q^3 + q$.

Now if we take $d = q$, the leading coefficient a_M of t in (7) is a homogeneous polynomial for variables x, y, z, t with degree not greater than $q^3 + 1 + q(q+1) - (q^3 + q) = q^2 + 1$.

On the other hand, all coefficients a_k in (7) are divisible by $Q_4(2) - f(Q_4(0), Q_4(1))$, a homogeneous polynomial with degree $q^2 + 1$, and hence $a_M(u, v, w, s) =$

https://doi.org/10.1017/S0004972700015720 Published online by Cambridge University Press

$\gamma(w - f(u, v))$ for some unit $\gamma \in F_q$. Dividing $G(u, v, w, s, t)$ by $\gamma(w - f(u, v))$, we get a monic polynomial of t in $F_q[u, v, w, (s - g(u, v))/(w - f(u, v)), t]$. This implies that t is integral over

$$R := F_q[Q_4(0), Q_4(1), Q_4(2), \frac{Q_4(3) - g(Q_4(0), Q_4(1))}{Q_4(2) - f(Q_4(0), Q_4(1))}].$$

By the same process x and y are integral over R and, hence, so is z.

Now $R_4 = F_q[x, y, z, t]$ is integral over R and $R \subset R_4^+ \subset R_4$, so R_4^+ is also integral over R. Since R, a unique factorisation domain, is integrally closed in its field of quotients $Q(R) = K_4^* = K_4^+$ and $R \subset R_4^+ \subset Q(R)$, R is also integrally closed in R_4^+. Thus $R_4^+ = R$. This completes the proof of Theorem 3. □

3. The proof of Theorem 1

We now prove Theorem 1. Consider $Q_4(4) \in R_4^+$, where $Q_4(x, y, z, t)$ is defined by (1). By Theorem 3 we have a four-variable polynomial h_4 such that

$$Q_4(4) - h_4(Q_4(0), Q_4(1), Q_4(2), Q_4^*) = 0. \tag{10}$$

Q_4^* is a homogeneous polynomial in $F_q[x, y, z, t]$ of degree $q^3 + 1 - (q^2 + 1) = q^3 - q^2$ and $Q_4(4)$ has degree $q^4 + 1$. Thus, the degree in Q_4^* does not exceed

$$\frac{q^4 + 1}{q^3 - q^2} < q + 2$$

for $q \geqslant 3$. Hence, multiplying (10) by $[Q_4(2) - f(Q_4(0), Q_4(1))]^{q+1}$, we get

$$Q_4(4)[Q_4(2) - f(Q_4(0), Q_4(1))]^{q+1} - h_5(Q_4(0), Q_4(1), Q_4(2), Q_4(3)) = 0. \tag{11}$$

By [**3**, Section 6.3], we may assume that our five-variable quadratic form is

$$Q_5 = x^2 + y^2 - \delta z^2 - t^2 - \theta^2,$$

where δ is a non-square in F_q. Substituting $Q_4(i) = Q_5(i) + \theta^{q^i+1}$, $i = 0, 1, 2, 3, 4$ into (11), we obtain

$$\begin{aligned}\left(Q_5(4) + \theta^{q^4+1}\right)[\left(Q_5(2) + \theta^{q^2+1}\right) - f(Q_5(0) + \theta^2, Q_5(1) + \theta^{q+1})]^{q+1} \\ - h_5\left(Q_5(0) + \theta^2, Q_5(1) + \theta^{q+1}, Q_5(2) + \theta^{q^2+1}, Q_5(3) + \theta^{q^3+1}\right) = 0.\end{aligned} \tag{12}$$

Let $L := F_q(Q_4(0), Q_4(1), Q_4(2), Q_4(3), \theta) = K_5^*(\theta)$. Then it is clear that

$$F_q(x, y, z, t, \theta) = K_5 \supset L = K_4^+(\theta) \supset K_5^* = F_q(Q_5(0), Q_5(1), Q_5(2), Q_5(3), Q_5(4)).$$

https://doi.org/10.1017/S0004972700015720 Published online by Cambridge University Press

Let $m := [L : K_5^*]$. Then, by (12), $m \leqslant q^4 + 1 + (q+1)(q^2+1) < 2q^2(q^2-1)$ for $q \geqslant 3$.

Because the Galois group of K_5 over L is isomorphic to $O(4, Q_4)$ and the Galois group of K_5 over K_5^+ is isomorphic to $O(5, Q_5)$, we have $[K_5 : L] = |O(4, Q_4)|$ and $[K_5 : K_5^+] = |O(5, Q_5)|$. Hence

$$[K_5 : K_5^*] = m\,|O(4, Q_4)| < 2q^2(q^2-1)\,|O(4, Q_4)| = 4q^4(q^2-1)^2(q^2+1).$$

Since $K_5 \supset K_5^+ \supset K_5^*$, $[K_5 : K_5^+] = |O(5, Q_5)| = 2q^4(q^2-1)^2(q^2+1)$ is a divisor of $[K_5 : K_5^*]$. Thus $[K_5 : K_5^+] = 2q^4(q^2-1)^2(q^2+1) = [K_5 : K_5^*]$. So we get $K_5^+ = K_5^*$. This completes the proof of Theorem 1. □

References

[1] D. Carlisle and P.H. Kropholler, 'Rational invariants of certain orthogonal and unitary groups', (preprint).

[2] H. Chu, 'Orthogonal group action on rational functions fields', *Bull. Inst. Math. Acad. Sinica* **16** (1988), 115–122.

[3] S.D. Cohen, 'Rational function invariant under an orthogonal group', *Bull. London Math. Soc.* **22** (1990), 217–221.

[4] N. Jacobson, *Basic algebra I*, 1st ed. (Freeman and Company, New York, San Francisco, 1974).

Department of Mathematics
National Taiwan Normal University
Taipei
Taiwan
Republic of China