Czechoslovak Mathematical Journal

Hiroyuki Ishibashi

Minimal set of generators of symplectic groups over finite fields

Czechoslovak Mathematical Journal, Vol. 30 (1980), No. 4, 629–632

Persistent URL: `http://dml.cz/dmlcz/101710`

Czechoslovak Mathematical Journal, 30 (105) 1980, Praha

MINIMAL SET OF GENERATORS OF SYMPLECTIC GROUPS OVER FINITE FIELDS

Hiroyuki Ishibashi, Sakado

(Received January 3, 1979)

1. INTRODUCTION

Let E be a finite field with the prime field F. $E - \{0\}$ is the multiplicative cyclic group generated by an element α. We suppose $[E : F] > 1$, in particular, the number of E, $|E| > 3$. V denotes n-dimensional vector space over E with a non-singular alternating form. We have a canonical base $\{x_i, y_i \mid 1 \leqq i \leqq m,\ n = 2m\}$ for V, i.e., $x_i x_j = y_i y_j = 0$ for all i, j, and $x_i y_j = 0$ or 1 according to $i \neq j$ or $i = j$(resp.). $\mathrm{Sp}_n(E)$ or $\mathrm{Sp}(E)$ is the symplectic group on V. An element σ in $\mathrm{Sp}(V)$ is called an *isometry on* V. If σ fixes a hyperplane of V, then σ is called a *transvection on* V. The set of all transvections is denoted by T. We know T generates $\mathrm{Sp}(E)$. However it does not need the whole T to generate $\mathrm{Sp}(E)$.

In the present paper we shall give a minimal set of generators of $\mathrm{Sp}(E)$ which consists of n elements of T and an element Δ of $\mathrm{Sp}(E)$.

$\mathrm{Sp}(F)$ is the symplectic subgroup of $\mathrm{Sp}(E)$ defined on $V_1 = \bigoplus_{i=1}^{m} (Fx_i \oplus Fy_i)$.

Let Δ be an isometry of $\mathrm{Sp}(E)$ defined by $\Delta x_i = \alpha^{-1} x_i$ and $\Delta y_i = \alpha y_i$ for each i in $\{1, 2, \ldots, m\}$.

The our goal is the following:

Theorem. $\mathrm{Sp}_n(E)$ *is generated by* Δ *and* n *transvections in* $\mathrm{Sp}_n(F)$. *This system of generators is minimal.*

For subsets U and W of V, the set theoretic difference is denoted by $U - W$. $M \oplus N$ denotes a direct sum of subspaces.

2. TRANSVECTIONS

For a subset U of V, we define $U^* = \{x \in V \mid xU = 0\}$.

Let x, y be vectors in V with $xy \neq 0$, and a be an element of E. Then $V = Ex \oplus y^*$. Hence a linear map τ defined by $\tau x = x + ay$ and $\tau = 1$ on y^* is a transvection if

$a \neq 0$ and is identity map if $a = 0$. τ is denoted by $\tau_{x,ay}$ and y^* or $(Ey)^*$ is called the *axis of* τ.

Conversely, any transvection τ can be expressed as above for some $x, y \in V$ and $a \in E$.

We note x is not unique, more precisely, for any z with $zy \neq 0$, there exists b in E with $\tau_{x,ay} = \tau_{z,by}$.

3. PROOF OF THE THEOREM

We have $E = F(\alpha)$ and the canonical base $\{x_i, y_i \mid 1 \leqq i \leqq m\}$ for V.

Notations.

$z = x_1 + x_2 + \ldots + x_i$, $1 \leqq i \leqq m$.

$S = \{\tau_{z_i, y_i}, \tau_{y_i, z_i} \mid 1 \leqq i \leqq m\}$, (hence $|S| = n$ and $S \subset \mathrm{Sp}(F)$).

$\Delta \in \mathrm{Sp}(E)$ with $\Delta x_i = \alpha^{-1} x_i$ and $\Delta y_i = \alpha y_i$ for $i = 1, 2, \ldots, m$.

$T =$ the set of transvections in $\mathrm{Sp}(E)$.

$T_{y_i} =$ the set of transvections in $\mathrm{Sp}(E)$ with axis y_i^*.

$T_{z_i} =$ the set of transvections in $\mathrm{Sp}(E)$ with axis z_i^*.

Let $G = [S, \Delta]$, i.e., the subgroup generated by S and Δ in $\mathrm{Sp}_n(E)$. Then our purpose is to show $G = \mathrm{Sp}_n(E)$. Since $\mathrm{Sp}_n(E) = [T]$, it suffices to show $T \subset G$.

Lemma 3.1. *For some even numbers* r *and* s, *it holds* $\alpha^r + \alpha^s = \alpha$ *or* $\alpha^r - \alpha^s = \alpha$.

Proof. Since $\alpha \neq 1$, we have $\alpha - 1 \neq 0$. Write $\alpha - 1 = \alpha^s$. If s is even, then the lemma is clear (let $r = 0$). If s is odd, then $\alpha^2 - \alpha = \alpha^{s+1}$ gives the lemma. Q.E.D.

Lemma 3.2. $T_{y_i} \subset G$ *and* $T_{z_i} \subset G$ *for any* i *in* $\{1, \ldots, m\}$.

Proof. Since $\Delta \tau_{z_i, y_i} \Delta^{-1} = \tau_{\Delta z_i, \Delta y_i} = \tau_{\alpha^{-1} z_i, \alpha y_i} = \tau_{z_i, \alpha^2 y_i}$, it is obvious that for any even r, $\tau_{z_i, \alpha^r y_i}$ is contained in G. Next, by Lemma 3.1, taking some even r and s, we have $\tau_{z_i, \alpha y_i}$ in G, because $(\tau_{z_i, \alpha^r y_i})(\tau_{z_i, \alpha^s y_i})^{\pm 1} = \tau_{z_i, (\alpha^r \pm \alpha^s) y_i}$. Since $\Delta \tau_{z_i, \alpha y_i} \Delta^{-1} = \tau_{z_i, \alpha^3 y_i}$, by the same way as above, we see G contains $\tau_{z_i, \alpha^r y_i}$ for all odd r, whence for any integer r.

Take any τ in T_{y_i}. Since $z_i y_i \neq 0$, τ is written as $\tau = \tau_{z_i, a y_i}$ for some a in E. Since $E - \{0\}$ is a cyclic group generated by α, we have $T_{y_i} \subset G$.

By the same way we have $T_{z_i} \subset G$. Q.E.D.

Definition. Let $v \in V$ and write $v = \sum_{i=1}^{m} (a_i x_i + b_i y_i)$, $a_i, b \in E$. Then $\{h_i, k_i\}$ are projections defined by $h_i(v) = a_i$ and $k_i(v) = b_i$, for $1 \leqq i \leqq m$.

Definition. For $j = 1, \dots, m$ we define $G_j = [\tau_{y_i,z_i}, \tau_{z_i,y_i} \mid 1 \leqq i \leqq j]$.

Lemma 3.3. *Let $0 \neq v \in V$ and $1 < j$ be the largest number with $h_j(v) \neq 0$ or $k_j(v) \neq 0$, then there exists ϱ in G_j such that $h_{j-1}(\varrho v) \neq 0$, $h_j(\varrho v) \neq 0$ and $k_j(\varrho v) \neq 0$.*

Proof. i) Case of $h_j(v) \neq 0$.

By $h_j(v) \neq 0$, we have $vy_j \neq 0$. Hence for any a in E we can define $\theta_1 = \tau_{v,ay_j}$ and have $\theta_1 v = v + ay_j$. Since $|E| > 2$, there exists a in E with $k_j(\theta_1 v) = k_j(v) + a \neq 0$ and $(\theta_1 v) z_j = vz_j - a \neq 0$. We take such a. Then we can define $\theta_2 = \tau_{\theta_1 v, bz_j}$ for any b in E. Therefore, $\theta_2\theta_1 v = v + ay_j + bz_j$ and $k_j(\theta_2\theta_1 v) = k_j(\theta_1 v) \neq 0$. Again by $|E| > 2$, we can choose b with $h_j(\theta_2\theta_1 v) = h_j(v) + b \neq 0$ and $h_{j-1}(\theta_2\theta_1 v) = h_{j-1}(v) + b \neq 0$.

Thus $\varrho = \theta_2\theta_1$ is the desired one.

ii) Case of $h_j(v) = 0$.

We shall show that for some θ in G_j we have $h_j(\theta v) \neq 0$, i.e., reduce the case to the first.

First we show there exists θ_1 in G_j with $h_i(\theta_1 v) \neq 0$ for some i in $\{1, \dots, j\}$. So we assume $h_i(v) = 0$ for all $i = 1, \dots, j$. This implies, for some i in $\{1, \dots, j\}$, we have $vz_i \neq 0$, since V is non-singular. Put $\theta_1 = \tau_{v,z_i}$ for such i. Then we have $h_i(\theta_1 v) = h_i(v + z_i) = 1 \neq 0$.

Next, since $h_i(\theta_1 v) \neq 0$, we have $(\theta_1 v) y_i \neq 0$. Hence $\theta_2 = \tau_{\theta_1 v, ay_i}$ is well-defined for all a in E. Since $|E| > 1$, we have $(\theta_2\theta_1 v) z_j = (\theta_1 v + ay_i) z_j = (\theta_1 v) z_j - a \neq 0$ for some a. Take such a. Then $\theta_3 = \tau_{\theta_2\theta_1 v, bz_j}$ is defined for any b in E and we have $\theta_3\theta_2\theta_1 v = \theta_2\theta_1 v + bz_j$. Therefore, for a suitable choice of b we have $h_j(\theta_3\theta_2\theta_1 v) \neq 0$, i.e., $\theta = \theta_3\theta_2\theta_1$ is the desired one. Q.E.D.

Lemma 3.4. *Let $v \in V$, and $h_{j-1}(v) \neq 0$, $h_j(v) \neq 0$ and $k_j(v) \neq 0$. Then there exists θ in G_j with $h_j(\theta v) = k_j(\theta v) = 0$.*

Proof. To simplify the notations we write $a = h_{j-1}(v)$, $b = h_j(v)$ and $c = k_j(v)$. Then, since $b \neq 0$, we can define $\theta_1 = \tau_{v,-cy_j}$. Since $a \neq 0$, we can also define $\theta_2 = \tau_{\theta_1 v, dy_{j-1}}$ for any $d \in E$. Take d with $(\theta_1 v + dy_{j-1}) z_j \neq 0$. Then $\theta_3 = \tau_{\theta_2\theta_1 v, -bz_j}$ is well-defined and $\theta = \theta_3\theta_2\theta_1$ is the desired one. Q.E.D.

Lemma 3.5. *Let $0 \neq v \in V$. Then, there exists σ in G such that $\sigma v \in Ex_1$ or Ey_1.*

Proof. Let j be the largest number with $h_j(v) \neq 0$ or $k_j(v) \neq 0$. We shall prove the lemma by the induction on j.

Let $j = 1$. Then we may write $v = ax_1 + by_1$, $a, b \in E$. If $a = 0$ then let $\sigma = 1$. If $a \neq 0$, then for $\sigma = \tau_{v,-by_1}$ we have σv in Ex_1.

Next, let $j > 1$. Then by Lemma 3.3 there exists ϱ in G_j with $h_{j-1}(\varrho v) \neq 0$, $h_j(\varrho v) \neq 0$ and $k_j(\varrho v) \neq 0$. Hence, by Lemma 3.4 we have θ in G_j with $h_j(\theta\varrho v) = k_j(\theta\varrho v) = 0$. Thus, by the induction on j we complete the proof. Q.E.D.

Take any $\tau \neq 1$ in T and write $\tau = \tau_{u,v}$. Let σ be an isometry as in the lemma. Then $\sigma\tau_{u,v}\sigma^{-1}$ is contained in T_{z_1} or T_{y_1} (note $z_1 = x_1$). Since $T_{z_1}, T_{y_1} \subset G$, we have $T \subset G$. Thus, we have proved that $\mathrm{Sp}_n(V)$ is generated by S and Δ. It is clear that $\{S, \Delta\}$ is minimal.

References

[1] *J. Dieudonné:* "La Geometrie des Groupes Classiques", Springer-Verlag Berlin—Heidelberg—New York (1971).

[2] *H. Ishibashi:* Generators of an Orthogonal Group over a Finite Field, Czechoslovak Math. J. *28* (1978) 419—433.

[3] *H. Ishibashi:* Generators of a Symplectic Group over a Local Valuation Domain, J. Algebra *53* (1978) 125—128.

[4] *O. T. O'Meara:* "Symplectic Groups" A.M.S. Math. Surveys *16* (1978).

Authors adaress: Department of Mathematics, Josai University, Sakado, Saitama, Japan.