SOME SUBGROUPS OF $SL_n(\mathbf{F}_2)$

BY

JACK MCLAUGHLIN[1]

1. Introduction

In this paper we determine those irreducible subgroups of $SL_n(\mathbf{F}_2)$ which are generated by transvections.

THEOREM. *Let V be a vector space of dimension $n \geqq 2$ over $\mathbf{F}_2$ and let G be an irreducible subgroup of $SL(V)$ which is generated by transvections. If $G \neq SL(V)$ then $n \geqq 4$ and G is one of the following subgroups of $Sp(V)$: $Sp(V)$, $O_{-1}(V)$, $O_1(V)$ (except at $n = 4$), the symmetric group of degree $n + 2$, or the symmetric group of degree $n + 1$.*

This result has some relevance to the question left open in [3].

Some of the notation and terminology of [3] will be used and we review it briefly there. (Since we work over a finite prime field our assumption that G is generated by transvections is equivalent to the assumption that G is generated by subgroups of root type.) If G contains the transvection τ with $P = \operatorname{Im}(\tau - 1)$ and $H = \operatorname{Ker}(\tau - 1)$ we say P is a *center* (for G), H is an *axis* (for G). Also we say P is a center for H and H is an axis for P. The set of centers for G is C and the set of axes for G is A. For $P \in C$, $a(P)$ is the intersection of the axes of P and for $H \in A$, $c(H)$ is the sum of the centers for H.

2. Preliminary lemmas

Our determination will be made by induction on n; in this section we collect some information needed for the induction. G is a group satisfying the hypotheses of the theorem.

LEMMA 2.1. *G is transitive on C and A.*

Proof. Choose P such that $\dim a(P)$ is maximal. Then Lemma 2 of [3] tells us that G has an orbit of centers containing P and all centers off $a(P)$. Since G is irreducible there cannot be a second orbit. Likewise for A.

LEMMA 2.2. *If $P \in C$ and $a(P)$ is not a hyperplane then $G = SL(V)$.*

Proof. Choose $P \in C$ and suppose S is another center on $a(P)$. By Lemma 4 of [3] we have a center Q off $a(P)$ and $a(S)$. Let K be a hyperplane over $Q + a(P)$. Since $K \supseteq a(P)$, K is an axis for P. Then using Lemma 2 of [3] we see K is an axis for Q and then K is an axis for S. Thus all points on $P + S$ are centers. Since G is irreducible, C spans V and consequently every

Received May 24, 1967.

[1] Research supported in part by a grant from the National Science Foundation.

point of V is in C. Now let H be an axis for P. If $Q \subseteq H$ and $Q \nsubseteq a(P)$ then Q is a center for H (again Lemma 2 of [3]). Hence $c(H) = H$. Now dualize the remarks at the beginning of the proof and see that every hyperplane is an axis. Lemma 3 of [3] completes the proof.

These two lemmas are valid for arbitrary irreducible groups generated by subgroups of root type.

From now on we suppose $G \neq SL(V)$. Then for $P \in C$, $a(P)$ is a hyperplane, $P^\perp$, and for $H \in A$, $c(H)$ is a point, $H^\perp$. We also are assuming that the ground field is $\mathbf{F}_2$ and consequently for each $P \in C$ there is a unique transvection τ_P with center P, axis $P^\perp$. These involutions form a single conjugate class—which generates G. If P and Q are two centers then $\tau_P \tau_Q$ has order 1, 2, or 3 according as $P = Q$, $P \neq Q \subseteq P^\perp$, $Q \nsubseteq P^\perp$. For $P \in C$, $\Delta(P)$ will be the centers $\neq P$ lying on $P^\perp$ and $\Gamma(P)$ will be the centers off $P^\perp$.

LEMMA 2.3. $P + \sum \Delta(P) = P^\perp$.

Proof. Choose $Q \in \Gamma(P)$; it will suffice to show that all centers are on $P + Q + \sum \Delta(P)$. Suppose $R \in \Gamma(P) \cap \Gamma(Q)$. Then $(R + Q) \cap P^\perp = S$ is a center and

$$R \subseteq Q + S \subseteq Q + P + \sum \Delta(P).$$

If $R \in \Gamma(P) \cap \Delta(Q)$ let T be the third point on $P + R$. Then

$$T \in \Gamma(P) \cap \Gamma(Q) \quad \text{so} \quad R \subseteq P + T \subseteq Q + P + \sum \Delta(P).$$

The same sort of argument yields:

LEMMA 2.4. *If $P \in C$ and $Q \in \Gamma(P)$ then G is generated by τ_Q, τ_P, and those τ_S with $S \in \Delta(P)$.*

COROLLARY. *G is primitive on C.*

For if $P \in C$ and $G_P \subset M \subseteq G$, then we have $\eta(P) \neq P$. Then $\eta(P^\perp) \neq P^\perp$ and by Lemma 2.3. there will be a center $S \subseteq P^\perp$ with $Q = \eta(S) \nsubseteq P^\perp$. But $\tau_Q = \eta \tau_S \eta^{-1} \in M$ so $M = G$.

LEMMA 2.5. *G_P is transitive on $\Gamma(P)$.*

Proof. If $R, Q \in \Gamma(P)$ and $R \in \Gamma(Q)$ then $P^\perp \cap (Q + R) = S$ is a center, $\tau_S \in G_P$ and $\tau_S(Q) = R$. If $R \in \Delta(Q)$ let T be the third point on $P + R$; then T and R are in the same G_p-orbit—as are T and Q.

LEMMA 2.6. *Let $G_P^* = \langle \tau_S \mid S \in \Delta(P) \rangle$; then G_P^* is transitive on $\Delta(P)$.*

Proof. Suppose R, $S \in \Delta(P)$ are in different G_P-orbits. Then $T \in \Delta(R)$ or $T \in \Delta(S)$ for otherwise $\langle \tau_R, \tau_T, \tau_S \rangle$ moves R to S (via T). In particular $R \in \Delta(S)$ so we can choose $Q \in \Gamma(R) \cap \Gamma(S)$. If $P \subseteq R + S$ then $P = Q^\perp \cap (R + S)$ and $Q \in \Delta(P)$—against the above remark. Hence $P + R + S$ has dimension 3 and

$$Q \in \Gamma(P) \cap \Gamma(R) \cap \Gamma(S).$$

Let $X = (P + S) \cap Q^\perp$, $Y = (P + R) \cap Q^\perp$, Z be the third point on $X + Y$, and U be the third point on $P + Z$. Now $\langle \tau_P, \tau_Q, \tau_R, \tau_S\rangle$ fixes X and moves P to R. Hence G moves S to U and $U \in C$. The dual of Lemma 2.3 tells us that for some $T \in \Delta(P)$, $X \nsubseteq T^\perp$. Then $S \nsubseteq T^\perp$ so $R \subseteq T^\perp$. But now $U \nsubseteq T^\perp$ so S and U are in the same G_P^*-orbit. Symmetry will finish the argument.

Corollary. *If $P \in C$ and for some $S \in \Delta(P)$ the third point on $P + S$ is in C then $G = Sp(V)$.*

For this will then be true for each S in $\Delta(P)$ and consequently the third point on the line joining any two centers is a center. $V = \sum C$ so all points of V are centers. Then all hyperplanes are axes and the corollary follows from Lemma 3 of [3].

Lemma 2.7. *The dimension of V is at least 4.*

Proof. Recall that we are now supposing $G \neq SL(V)$ so certainly $n > 2$. If $\geqq 3$ then $\Delta(P)$ is not empty by Lemma 2.3. If $n = 3$ and $S \in \Delta(P)$ then $P^\perp = S + P = S^\perp$ against our hypothesis that each axis has a unique center.

If $P \in C$ and $S \in \Delta(P)$ then τ_S induces a transvection on $P^\perp/P$ with center $P + S/P$ and axis $P^\perp \cap S^\perp/P$. Let $G(P)$ be the subgroup of $SL(P^\perp/P)$ generated by all such transvections.

Lemma 2.8. *$G(P)$ is an irreducible group.*

Proof. Suppose X/P is stable for $G(P)$. Then for $S \in \Delta(P)$, τ_S fixes X so either $S \subseteq X$ or $S^\perp \supseteq X$. Using Lemmas 2.6 and 2.3 we have $S \subseteq X$ implies $X = P^\perp$ and $S^\perp \supseteq X$ implies $X = P$.

Corollary. *The centers for $G(P)$ are precisely the $S + P/P$ with $S \in \Delta(P)$, and the dual statement for axes.*

For $G(P)$ is transitive on this set of centers and being an irreducible group it is transitive on its full set of centers.

Lemma 2.9. *If $n > 4$ then $G(P) \neq SL(P^\perp/P)$.*

Proof. If $G = Sp(V)$ this is certainly so. Otherwise by the corollary to Lemma 2.6 we know that for $S \in \Delta(P)$, the third point on $P + S$ is not a center. If $G(P) = SL(P^\perp/P)$ then G_P^* is doubly transitive on $\Delta(P)$, so for $S \in \Delta(P)$ $G_{P,S}$ is transitive on $\Delta(P) - \{S\}$. Then if $\Delta(P) \cap \Delta(S)$ is not empty $\Delta(P) - \{S\} \subseteq \Delta(S)$ and we find $P^\perp \subseteq S^\perp$—a contradiction. If $n > 4$ so $\dim P^\perp > 3$ then we can choose R, S, T in $\Delta(P)$ so $P \nsubseteq R + S + T$ and $\dim (R + S + T) = 3$. The preceding remarks tell us that distinct centers on $R + S + T$ are not perpendicular and consequently all points on $R + S + T$ are centers. On the other hand $S^\perp \cap (R + S + T)$ is a line thru S in $S^\perp$ and so contain at most two centers. This contradiction finishes the proof.

3. Construction of the polarity

V continues to be a vector space of dimension $n \geqq 2$ over $\mathbf{F}_2$ and G is an irreducible subgroup of $SL(V)$ which is generated by transvections. We suppose each member of C has a unique axis and each member of A has a unique center. We refer to this correspondence between C and A as the *partial polarity* determined by G.

LEMMA 3.1. *The partial polarity determined by G extends uniquely to a null polarity on the subspaces of V.*

Proof. We go by induction on n. For $n = 2$ there is nothing to do; take $n > 2$. By Lemma 2.7 we know $n \geqq 4$ and Lemmas 2.8 and 2.9 tell us that the group $G(P)$ satisfies the hypotheses of the lemma. Hence the partial polarity determined by $G(P)$ extends uniquely to a null polarity on the subspaces of $P^\perp/P$. We proceed to assemble some facts which will allow us to build the desired polarity.

(1) If $P \in C$ and $X = \bigcap\{Q^\perp \mid Q \in \Gamma(P)\}$ then $X = 0$.

X is stable for G_P so $S \in \Delta(P)$ implies $S \subseteq X$ or $S^\perp \supseteq X$. By Lemma 4 of [3], $S \nsubseteq X$ so $S^\perp \supseteq X$. Thus X is on all axes and $X = 0$.

(2) If X is a point then $X \subseteq P^\perp$ for some $P \in C$.

Suppose false, choose $P \in C$ and let Y be the third point on $P + X$. If $Q \in \Gamma(P)$ then $Y = Q^\perp \cap (P + X)$ against (1).

(3) If X is a point and $Y = \bigcap\{H \in A \mid H \supseteq X\}$ then $Y = X$.

Choose $P \in C$ so $X \subseteq P^\perp$; an induction hypothesis tells us that

$$P + X = \bigcap\{H \in A \mid H \supseteq P + X\}.$$

It suffices then to produce $Q \in \Gamma(P)$ with $Q^\perp \supseteq X$. If such does not exist we arrive at a contradiction as in the proof of (2).

(4) If $P, S_1, \cdots S_m \in C$ and $P \subseteq \sum S_i$ then $P^\perp \supseteq \bigcap S_i^\perp$.

Suppose false for some minimal m. If all $S_i \subseteq S_1^\perp$ we may suppose, by induction, that $P^\perp \cap S_1^\perp/S_1 \supseteq \bigcap(S_1^\perp \cap S_i^\perp)/S_1$. Then

$$P^\perp \supseteq \bigcap(S_1^\perp \cap S_i^\perp) = \bigcap S_i^\perp.$$

So we suppose $S_1 \nsubseteq S_2^\perp$. Then all three points on $S_1 + S_2$ are centers and

$$P \subseteq T + S_3 + \cdots + S_m$$

where T is one of the points on $S_1 + S_2$. By the minimality of m,

$$P^\perp \supseteq T^\perp \cap S_3^\perp \cap \cdots \cap S_m^\perp .$$

Since $\tau_T \in \langle \tau_{S_1}, \tau_{S_2} \rangle$, τ_T fixes $S_1^\perp \cap S_2^\perp$ and $T^\perp \supseteq S_1^\perp \cap S_2^\perp$. Thus we have a contradiction and the statement is true for all m.

(5) If X is a point then $H = \sum \{P \in C \mid P^{\perp} \supseteq X\}$ is a hyperplane containing X.

We first note that if $Q \in C$ and $Q^{\perp} \not\supseteq X$ then by (4), $Q \not\subseteq H$. Thus $H \neq V$. Now choose $P \in C$ with $P \neq X$ and $X \subseteq P^{\perp}$. By induction we have

$$P + \sum \{S \in \Delta(P) \mid S^{\perp} \supseteq X\}$$

is a hyperplane of $P^{\perp}$ which contains $P + X$. Thus it suffices to find $Q \in \Gamma(P)$ with $Q^{\perp} \supseteq X$ and (3) tells us such Q exist.

If $X \in C$ then the hyperplane determined in (5) is just $X^{\perp}$; if X is any point we now write $X^{\perp}$ for the hyperplane determined in (5). We can then improve (4).

(6) If X is a point, $S_i \in C$ and $X \subseteq \sum S_i$ then $X^{\perp} \supseteq \bigcap S_i^{\perp}$.

The argument is, as in (4), by induction.

(7) If X and Y are points with $X \subseteq Y^{\perp}$ then $Y \subseteq X^{\perp}$.

Since $Y^{\perp} = \sum \{S \in C \mid S^{\perp} \supseteq Y\}$, (6) says

$$X^{\perp} \supseteq \bigcap\{H \in A \mid H \supseteq Y\} = Y$$

by (3).

With (7) we've finished the proof of the lemma—we have a one-one map from the points of V onto the hyperplanes of V which behaves properly with respect to incidence. Such a map extends uniquely to a polarity. We have $X \subseteq X^{\perp}$ for all points X so we have a null polarity

4. $G(P)$ is the symplectic group

We keep the assumptions of § 3. Then $G \subseteq Sp(V)$.

LEMMA 4.1. *If $G \subset Sp(V)$ and $G(P) = Sp(P^{\perp}/P)$ then G is one of the orthogonal groups.*

Proof. We have $n \geqq 4$ and for $P \in C$, each line through P on $P^{\perp}$ contains exactly one other center. Define Q on V by $Q(0) = 0$ and for $x \neq 0$, $Q(x) = 1$ or 0 according as $\langle x \rangle$ is a center or not. Then $Q(\sigma x) = Q(x)$ for all $\sigma \in G$ and all $x \in V$. Choose x, y distinct in V and different from 0. We want to show

$$Q(x) + Q(y) + Q(x + y) = 0 \quad \text{or} \quad 1$$

according as $\langle x \rangle \subseteq \langle y \rangle^{\perp}$ or not. If $\langle x \rangle \in C$ then our relation comes directly from the definition of Q. We suppose then that x and y are not centers. If $\langle x \rangle \subseteq \langle y \rangle^{\perp}$ then x, y and $x + y$ are mutually perpendicular so $x + y$ is not a center and our relation holds. Now suppose $\langle x \rangle \not\subseteq \langle y \rangle^{\perp}$ and choose a center $\langle z \rangle \subseteq \langle y \rangle^{\perp}$. Let f be an alternate form on V which yields our polarity. Then $f(y + z, x + z) = 1 + f(z, x)$ and we see $\langle x + z \rangle \subseteq \langle y + z \rangle^{\perp}$ if and only if $\langle x + y \rangle$ is not a center. Hence in either case $\langle x + y \rangle$ is a center and we have the desired relation. Thus Q is a quadratic function belonging to f and

$G \subseteq O(Q)$. Since G contains all the orthogonal transvections $G = O(Q)$. (We cannot be in the situation $n = 4$, Q of maximal index, because there the subgroup of $O(Q)$ generated by transvections is not irreducible).

5. $G(P)$ is a symmetric group

The irreducible symplectic representation of degree $2k$ over $\mathbf{F}_2$ of the symmetric groups of degree $2k + 1$ and $2k + 2$ is described in [1].

LEMMA 5.1. *If $n \geqq 6$ and $G(P)$ is the symmetric group of degree n or $n - 1$ then G is the symmetric group of degree $n + 2$ or $n + 1$.*

Proof. For this and the remaining lemma we will need some of the numerical relations on the parameters of a primitive group of rank 3. These are developed in [2] and we use the notation of that paper. We use m for either n or $n - 1$. Our assumptions tell us some of the parameters immediately. Thus

$$k = |\Delta(P)| = \binom{m}{2} \quad \text{and} \quad \lambda = |\Delta(P) \cap \Delta(S)| = \binom{m-2}{2}$$

(here $S \in \Delta(P)$). We want to determine

$$l = |\Gamma(P)| \quad \text{and} \quad \mu = |\Delta(P) \cap \Delta(Q)|$$

for $Q \in \Gamma(P)$. In $\Gamma(P)$ we have Q, the $k - \mu$ elements in $\Delta(Q) - (\Delta(Q) \cap \Delta(P))$ and the $1 + k - \mu$ elements consisting of the third point on $Q + S$ as S runs over the centers on $P^\perp$ and off $P^\perp \cap Q^\perp$. So $l = 2(1 + k - \mu)$. From [2] we have the relation $\mu l = k(k - \lambda - 1)$ so

$$\mu^2 - (k + 1)\mu + \tfrac{1}{2}k(k - \lambda - 1) = 0.$$

From the known values of k and λ we obtain $\mu = m$ or $\binom{m-1}{2}$.

From [2] we know that $d = (\lambda - \mu)^2 + 4(k - \mu)$ is a square. If $\mu = m$,

$$d = d(m) = \tfrac{1}{4}(m - 1)^2(m - 6)^2 + 2m(m - 3).$$

We see $d(5) = 24$, $d(6) = 36$, and $d(7) = 65$. The parameters coming from $m = 6$, $\mu = 6$ are those of $U_4(2)$ on the cosets of $Sp_4(2)$, however we can ignore $m = 6$ here since $S_6 = Sp_4(2)$—a case disposed of in the previous section. Thus we may assume that if $\mu = m$ then $m > 7$.

We now count the lines full of centers on $P^\perp$—call such lines h-lines. If $S \in \Delta(P)$, there are $2(m - 2)$ members of $\Delta(P)$ which are not on $S^\perp$. Hence there are $m - 2$ h-lines through S on $P^\perp$. So if h is the number of h-lines on $P^\perp$ we have $3h = \binom{m}{2}(m - 2)$.

Choose $Q \in \Gamma(P)$ and let E_i be the orbits of $G_{P,Q}$ on $\Delta(P) \cap \Delta(Q)$. Set $\mu_i = |E_i|$ and $s_i = |$ h-lines on $P^\perp \cap Q^\perp$ passing through an S in $E_i|$. Since each h-line on $P^\perp$ is either on $P^\perp \cap Q^\perp$ or meets $P^\perp \cap Q^\perp$ in a point we have

$$\tfrac{1}{3}\binom{m}{2}(m - 2) = \sum \tfrac{1}{3}\mu_i s_i + \sum \mu_i(m - 2 - s_i)$$

$$= \mu(m - 2) - \tfrac{2}{3}\sum \mu_i s_i .$$

Hence

$$3\mu = \binom{m}{2} + (2/(m - 2)) \sum \mu_i s_i .$$

In particular, $3\mu \geqq \binom{m}{2}$ so if $\mu = m$ then $m \leqq 7$. Hence we may suppose that $\mu = \binom{m-1}{2}$ and then $l = 2m$. Thus each center is on exactly m h-lines. If we choose $S \in \Delta(P)$, there will be just 2 h-lines through S and off $P^\perp$. Take T in $\Delta(P) \cap \Delta(S)$ and R in $\Delta(P)$ off $S^\perp$ and $T^\perp$. If X is the third center on $S + R$ then $T + R$ and $T + X$ are the 2 h-lines through T and off $S^\perp$—each lies in $P^\perp$. Now keep $S \in \Delta(P)$ and choose $Q \in \Gamma(P) \cap \Gamma(S)$. The above remark shows that $T \in \Delta(P) \cap \Delta(S)$ implies that $T \in \Delta(P) \cap \Delta(Q)$.

We have $S_i \in \Delta(P)$, $i = 1, 2, \cdots, m - 1$ such that if $\tau_i = \tau_{S_i}$ then $\tau_i \tau_{i+1}$ has order 3 and all other pairs commute. Choose $Q \in \Gamma(P) \cap \Gamma(S_1)$ and put $\sigma = \tau_P$, $\tau = \tau_Q$. If τ and τ_2 do not commute replace τ_2 by $\tau_1 \tau_2 \tau_1$. One way or the other we see that G is generated by the involutions $\sigma, \tau, \tau_1, \cdots, \tau_{m-1}$ where the product of adjacent members in this list has order 3 and all others commute. Thus $G = S_{m+2}$—that is $G = S_{n+1}$ or S_{n+2}.

6. $G(P)$ is an orthogonal group

We will have a proof of the theorem if we prove

LEMMA 6.1. *$G(P)$ is an orthogonal group only when it is a symmetric group.*

Proof. We suppose $n = 2m \geqq 6$ and that $G(P)$ is one of the orthogonal groups of degree $2(m - 1)$. Then we know

$$k = 2^{m-2}(2^{m-1} - \varepsilon) \quad \text{and} \quad \lambda = 2^{2(m-2)} - 1.$$

(Here $\varepsilon = \pm 1$ according as the form for $G(P)$ has maximal index or not.) As in §5 we have

$$\mu^2 - (k + 1)\mu + \tfrac{1}{2}k(k - \lambda - 1) = 0.$$

Hence $(k + 1)^2 - 2k(k - \lambda - 1)$ is a square—say y^2. Then

$$\begin{aligned} y^2 - 1 &= k(2\lambda + 4 - k) \\ &= 2^{m-2}(2^{m-1} - \varepsilon)(2 + \varepsilon 2^{m-2}) \\ &= 2^{m-1}(2^{m-1} - \varepsilon)(1 + \varepsilon 2^{m-3}). \end{aligned}$$

If $\varepsilon = -1$ then $m = 3$ and $G(P)$ is the symmetric group of degree 5. We suppose $\varepsilon = 1$, set $x = m - 1$ and then

$$y^2 - 1 = 2^x(2^x - 1)(2^{x-2} + 1).$$

Since the orthogonal group of maximal index in dimension 4 is not generated by transvections we have $x \geqq 3$. If $y \equiv 1\ (4)$ then $y = \alpha \cdot 2^{x-1} + 1$ for some α and we have

$$\alpha(\alpha \cdot 2^{x-2} + 1) = (2^x - 1)(2^{x-2} + 1) \quad \text{and} \quad \alpha \equiv -1(2^{x-2}).$$

Write $\alpha = \beta 2^{x-2} - 1$. Then $\alpha > 1$ so $\beta = 1, 2$, or 3. We can rewrite our condition as

$$\alpha(\alpha - 1)2^{x-2} = (2^{x-2} + 1)(2^x - (\alpha + 1))$$
$$= (2^{x-2} + 1)2^{x-2}(4 - \beta).$$

Hence $\alpha(\alpha - 1)/2 = (2^{x-2} + 1)(2 - \beta/2)$ and $\beta = 2$. This determines $x = 3$ and $G(P)$ is the symmetric group of degree 8. Finally suppose $y \equiv -1$ (4)—say $y + 1 = \alpha 2^{x-1}$. Then $\alpha(\alpha 2^{x-2} - 1) = (2^x - 1)(2^{x-2} + 1)$ and $\alpha = \beta \cdot 2^{x-2} + 1$. Then $\alpha > 1$ and consequently $\alpha \leqq 4$. This forces $x = 3$ which this time is a contradiction.

7. Concluding remarks

The well-known identifications of the Weyl groups of type E can be read from our list. Let V be a vector space of dimension n over $\mathbf{F}_2$ and let (A_{ij}) be the Cartan matrix for E_n. Choose a base $\{x_i\}$ for V and let G be the subgroup of $SL(V)$ generated by the mappings τ_i given by $\tau_i x_j = x_j + A_{ij} x_i$. The τ_i are transvections with center $\langle x_i \rangle$. If f is the alternate bilinear on V whose matrix with respect to the given base is (A_{ij}) then G is in the group of f. For $n = 6$ and 8, f is non-singular and for $n = 7$, f has a radical, $\langle x \rangle$, of dimension 1. Thus if W is the Weyl group of E_n we have a homomorphism from W into $Sp(V)$ in the first two cases and into $Sp(V/\langle x \rangle)$ in the latter case. For $n = 7$ and 8, $-1 \in W$ so -1 is in the kernel of our homomorphism in these two cases. Since W is transitive on the roots, the image of our homomorphism will be an irreducible group (generated by transvections). Since W is finite the kernel of our homomorphism is a 2-group. Knowing the order of W and scanning our list for the possible images of W we see $W \cong O_6(-1, \mathbf{F}_2)$ at $n = 6$, $W/\langle -1 \rangle \cong Sp_6(\mathbf{F}_2)$ at $n = 7$, and $W/\langle -1 \rangle \cong O_8(1, \mathbf{F}_2)$ at $n = 8$.

Bibliography

1. L. E. Dickson, *Representation of the general symmetric group as linear groups in finite and infinite fields*, Trans. Amer. Math. Soc, vol. 9 (1908) pp. 121–148.
2. D. G. Higman, *Finite permutation groups of rank* 3, Math. Zeitschrift, vol. 86 (1964), pp. 145–156.
3. Jack McLaughlin, *Some groups generated by transvections*, Arch. Math., to appear.

The University of Michigan
Ann Arbor, Michigan