

PRIMITIVE SYMMETRIC SETS IN FINITE ORTHOGONAL GEOMETRY

NOBUO NOBUSAWA

(Received January 22, 1979)

Let V be a vector space over a finite field k of characteristic $\neq 2$, and (x, y) a non-degenerate symmetric bilinear form on V . For an element a in V with $(a, a) \neq 0$, we denote by σ_a the reflection in the hyperplane orthogonal to a . A subspace generated by a, b, \dots, c is denoted by $\langle a, b, \dots, c \rangle$. Especially $\langle a \rangle$ is denoted by \bar{a} . Let $A = \{a \mid (a, a) = 1\}$. We can define a symmetric structure on A by $\bar{a} \circ \bar{b} = \bar{c}$, where $c = a^{\sigma_b}$. The main object of this note is to show that if $\dim V > 4$ or if $\dim V = 4$ and $k \neq F_3$ (the field of three elements), then A is a primitive symmetric set. For the primitive symmetric set, see [3]. Group-theoretically this implies that the centralizer of the involution σ_a in the orthogonal group is a maximal subgroup.

Let $G(V)$ be the orthogonal group, and Ω its commutator subgroup. Let $H(A)$ be the group generated by $\sigma_a \sigma_b$ where $(a, a) = (b, b) = 1$. Note that the restriction of $H(A)$ onto A is called the group of displacements and is denoted by $H(A)$ in the previous papers. We denote the latter by $\bar{H}(A)$.

Lemma 1. *Suppose that $\dim V \geq 4$. Let a and b be elements in V such that $(a, a) = (b, b) \neq 0$ and that $\langle a, b \rangle$ is a non-singular subspace of $\dim 2$. If x is an element in V such that $(x, x) = (a, a)$ and $\dim \langle a, x \rangle = 2$, then there exist τ_1 and τ_2 in $G(V)$ and c in V such that $a^{\tau_1} = a$, $x^{\tau_1} = c$, $a^{\tau_2} = b$ and $x^{\tau_2} = c$.*

Proof. First, we note that if y and z are elements in V such that $(y, y) = (z, z) \neq 0$ and that $\dim \langle y, z \rangle = 2$, then $\langle y, z \rangle$ is non-singular if and only if $(y, z) \neq \pm(y, y)$. For, let $z = \alpha y + t$ with α in k and t in V such that $(y, t) = 0$ and $t \neq 0$. Then $\langle y, z \rangle$ is singular if and only if $(t, t) = 0$, if and only if $\alpha = \pm 1$, if and only if $(y, z) = \pm(y, y)$. Now, put $c = \beta(a+b) + u$ with β in k and u in V such that $u \in \langle a, b \rangle^\perp$. We let $\beta = (a, x) ((a, a) + (a, b))^{-1}$. This is possible since $(a, a) \neq -(a, b)$ as noted first. Then $(a, c) = (b, c) = (a, x)$. Next, select u suitably in $\langle a, b \rangle^\perp$ so that $(c, c) = (a, a)$. This is possible since $\langle a, b \rangle^\perp$ is universal, i.e., $k = \{(u, u) \mid u \in \langle a, b \rangle^\perp\}$. Note $\dim V \geq 4$ and hence $\dim \langle a, b \rangle^\perp \geq 2$. Thus, we have $\langle a, x \rangle \cong \langle a, c \rangle \cong \langle b, c \rangle$, the first elements corresponding to the first, and the second to the second by the isomorphisms. Then by Witt's theorem, we have the consequence stated in Lemma 1.