Nobusawa, N.
Osaka J. Math.
17 (1980), 407-410

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 $a, b, \cdots, c$ is denoted by $\langle a, b, \cdots, c\rangle$. Especially $\langle a\rangle$ is denoted by $\bar{a}$. Let $A=\{\bar{a}\,|\,(a, a)=1\}$. 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 papeıs. 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 $(c, c)=(a, a)$. Thıs is possible since $\langle a, b\rangle^{\perp}$ is universal, *i.e.*, $k=\{(u, u)\,|\,u\in\langle a, b\rangle^{\perp}\}$. 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.

Lemma 2. *In Lemma* 1, τ_1 *and* τ_2 *can be taken in* Ω, *if* $\langle a, x\rangle$ *is non-singular.*

Proof. Any isometry on $\langle a, x\rangle^{\perp}$ is extended to an isometry on V by letting it operate trivially on $\langle a, x\rangle$. So, by multiplying τ_i by an isometry on $\langle a, x\rangle^{\perp}$ if necessary, we may assume that τ_i is contained in $O^+(V)$, the group of rotations. Next we recall that $O^+(V)/\Omega \cong k^*/k^{*2}$, where the isomorphism is induced by the spinorial norm θ. (See [1].) So, if necessary, choose ρ_i suitably on $\langle a, x\rangle^{\perp}$ such that $\theta(\rho_i\tau_i)=1$, which implies that $\rho_i\tau_i\in\Omega$. Take $\rho_i\tau_i$ for τ_i, and the proof is completed.

Lemma 3. *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 non-singular of dim* 2. *If* τ *is an element in* $G(V)$ *such that dim* $\langle a, a^{\tau}\rangle=2.$, *then there exist* τ_1 *and* τ_2 *in* $G(V)$ *such that*

$$a^{\tau_1^{-1}\tau\tau_1\tau_2^{-1}\tau^{-1}\tau_2} = b\,.$$

Proof. Let $x=a^{\tau}$ in Lemma 1. The above identity follows easily.

Lemma 4. *Suppose that either dim* $V>4$ *or dim* $V=4$ *and* $k\neq F_3$. *Let* a *and* b *be elements in* V *such that* $(a, a)=(b, b)\neq 0$ *and that* $\langle a, b\rangle$ *is singular of dim* 2. *Then there exists* c *such that* $(c, c)=(a, a)$ *and that* $\langle a, c\rangle$ *and* $\langle b, c\rangle$ *are both non-singular.*

Proof. Since $\langle a, b\rangle$ is singular, $b=\pm a+t$ with $(a, t)=0$ and $(t, t)=0$ as noted in the proof of Lemma 1. Without losing generality, we may assume that $b=a+t$. Then there exists t' in $\langle a\rangle^{\perp}$ such that $(t', t')=0$ and $(t, t')=\frac{1}{2}(a, a)$. (See [1], p. 119.) When dim $V>4$, we have dim $\langle a, t, t'\rangle^{\perp}\geq 2$ and hence there exists c in $\langle a, t, t'\rangle^{\perp}$ such that $(c, c)=(a, a)$. c satisfies the conditions in Lemma 4. Suppose that dim $V=4$ and that $k\neq F_3$. Put $c=\alpha a+\beta t+\gamma t'$. Then, $(c, c)=(a, a)$ if and only if $\alpha^2(a, a)+2\beta\gamma(t, t')=(a, a)$, i.e., $\alpha^2+\beta\gamma=1$. Suppose that this is satisfied. Then, $(a, a)=(c, c)=(b, b)$, and so, $\langle a, c\rangle$ is non-singular if and only if $\alpha\neq\pm 1$ as we noted before. Also, $\langle b, c\rangle$ is non-singular if and only if $\alpha+\frac{1}{2}\gamma\neq\pm 1$. For, $\langle b, c\rangle$ is non-singular if and only if $(b, c)\neq\pm(c, c)$ which implies $(\alpha+\frac{1}{2}\gamma)\,(a, a)\neq\pm(a, a)$. If the characteristic of $k\neq 3$, let $\alpha=\frac{1}{2}$, $\beta=\frac{1}{4}$ and $\gamma=3$. If the characteristic$=3$ and $k\neq F_3$, let ε be an element in k such that $\varepsilon^2=-1$, and let $\alpha=1+\varepsilon$, $\beta=-2-\varepsilon$ and $\gamma=\varepsilon$. Then $\alpha^2+\beta\gamma=1$, $\alpha\neq\pm 1$ and $\alpha+\frac{1}{2}\gamma\neq\pm 1$, the proof being completed.

Theorem 1. *Suppose that either dim* $V>4$ *or dim* $V=4$ *and* $k\neq F_3$. *Let* a *and* b *be elements in* V *such that* $(a, a)=(b, b)\neq 0$ *and that dim* $\langle a, b\rangle=2$. *Let* δ *be any non-zero element in* k. *Then there exist* $a_i (i=1,\cdots,4)$ *such that* $(a_i, a_i)=\delta$ *and that* $a^{\sigma_{a_1}\sigma_{a_2}\sigma_{a_3}\sigma_{a_4}}=b$. *Especially,* A *is transitive symmetric set.*

Proof. First suppose that $\langle a, b\rangle$ is non-singular. Let $d=a+u$, where $u\neq 0$ is chosen in $\langle a\rangle^{\perp}$ so that $(d, d)=\delta$. Clearly dim $\langle a, a^{\sigma_d}\rangle=2$, and hence by Lemma 3 there exist τ_1 and τ_2 in $G(V)$ such that $a^{\tau_1^{-1}\sigma_d\tau_1\tau_2^{-1}\sigma_d\tau_2}=b$, *i.e.*, $a^{\sigma_{a_1}\sigma_{a_2}}=b$, where $a_1=d^{\tau_1}$ and $a_2=d^{\tau_2}$. Let $a_3=a_4=a_1$, and Theorem 1 holds in this case. If $\langle a, b\rangle$ is singular, we use Lemma 4. Let c be an element given in Lemma 4. Apply the above argument on $\langle a, c\rangle$ and $\langle c, b\rangle$. We can find a_i $(i=1, \cdots, 4)$ such that $a^{\sigma_{a_1}\sigma_{a_2}}=c$ and $c^{\sigma_{a_3}\sigma_{a_4}}=b$. The proof is completed.

Lemma 5. *Suppose that dim* $V\geq 3$. *Let* B *be a block in* A, *i.e., a set of imprimitivity with respect to* $\langle\sigma_a \mid \bar{a}\in A\rangle$. *Suppose that* B *contains more than one element. Then* B *contains* $\bar{a}_1$ *and* $\bar{a}_2$ *such that* $(a_1, a_1)=(a_2, a_2)=1$ *and that* $\langle a_1, a_2\rangle$ *is non-singular of dim* 2.

Proof. Let $\bar{a}$ and $\bar{b}$ two different elements in B with $(a, a)=(b, b)=1$. If $\langle a, b\rangle$ is non-singular, we have nothing to prove. So, assume that $\langle a, b\rangle$ is singular. We may assume that $b=a+t$ with $(a, t)=0$ and $(t, t)=0$ as before. Let t' be an element in $\langle a\rangle^{\perp}$ such that $(t', t')=0$ and $(t, t')=\frac{1}{2}$. Let $c=t+t'$. Then $(c, c)=1$, $a^{\sigma_c}=a$ and $b^{\sigma_c}=b-2(b, c)c=a-t'$. Therefore by the definition of a block, $\overline{a-t'}\in B$. Let $a_1=b$ and $a_2=a-t'$. $\bar{a}_1$ and $\bar{a}_2\in B$, and $\langle a_1, a_2\rangle$ is non-singular since $(a_1, a_2)=1-\frac{1}{2}\neq\pm 1$.

Corollary. *Suppose that either dim* $V>4$ *or dim* $V=4$ *and* $k\neq F_3$. *Then* $\Omega\subseteq H(A)$.

Proof. We must show $\sigma_x\sigma_y\sigma_x\sigma_y\in H(A)$, where $\sigma_x\neq\sigma_y$. By Theorem 1, there exists an element τ in $H(A)$ such that $y^{\sigma_x}=y^{\tau}$. Let $\rho=\tau\sigma_x^{-1}$. Since $y^{\rho}=y$, we have $\rho^{-1}\sigma_y\rho=\sigma_y$, or $\sigma_y\rho=\rho\sigma_y$. Then $\sigma_x\sigma_y\sigma_x\sigma_y=(\rho^{-1}\tau)\sigma_y(\rho^{-1}\tau)^{-1}\sigma_y=\rho^{-1}(\tau\sigma_y\tau^{-1}\sigma_y)\rho$. Since $H(A)$ is normal in $G(V)$, we have $\Omega\subseteq H(A)$.

Theorem 2. *Suppose that either dim* $V>4$ *or dim* $V=4$ *and* $k\neq F_3$. *Then* A *is a primitive symmetric set.*

Proof. Let B be a block containing more than one element. By Lemma 5, we may assume that B contains $\bar{a}$ and $\bar{b}$ such that $(a, a)=(b, b)=1$ and that $\langle a, b\rangle$ is non-singular of dim 2. Let c be any element such that $(c, c)=1$ and that $\langle a, c\rangle$ is non-singular of dim 2. By Lemma 2 and Corollary, there exist τ_1 and τ_2 in $H(A)$ and an element d in V such that $a^{\tau_1}=a$, $b^{\tau_1}=d$, $a^{\tau_2}=c$ and $b^{\tau_2}=d$. From the first two, we conclude that $\bar{d}\in B$, and from the last two, $\bar{c}\in B$. Next, let e by any element such that $(e, e)=1$ and that $\langle a, e\rangle$ is singular. By Lemma 4, there exists an element f such that $(f, f)=1$ and that $\langle a, f\rangle$ and $\langle f, e\rangle$ are both non-singular. Then applying the previous discussion, we have $\bar{f}\in B$ and then $\bar{e}\in B$. Thus $A=B$, and A is primitive.

EXAMPLE 1. Let dim $V=4$ and $k=F_5$. Let $(x, x)=x_1^2+x_2^2+x_3^2+x_4^2$.

Then A consists of 60 elements. We can show that A is isomorphic with the alternating group A_5 considered as a symmetric set. In fact, A has generators: $\bar{a}_1$, $\bar{a}_1$, $\bar{a}_3$ and $\bar{a}_4$, where $a_1=(1, 0, 0, 0)$, $a_2=(1, 2, 1, 0)$, $a_3=(0, 1, 0, 0)$ and $a_4=(0, 2, 1, 1)$. If we denote $\sigma_i=\sigma_{a_i}$, then $(\sigma_1\sigma_2)^5=(\sigma_2\sigma_3)^3=(\sigma_3\sigma_4)^3=id$, and otherwise $(\sigma_i\sigma_j)^2=id$. We illustrate these in a diagram:

$$\bar{a}_1 \overset{5}{\text{———}} \bar{a}_2 \overset{3}{\text{———}} \bar{a}_3 \overset{3}{\text{———}} \bar{a}_4 .$$

We have an isomorphism φ of A onto A_5 given by $\varphi(\bar{a}_1)=id$, $\varphi(\bar{a}_2)=(12345)$, $\varphi(\bar{a}_3)=(12)(34)$ and $\varphi(\bar{a}_4)=(12)(35)$. The group $\bar{H}(A_5)$ is isomorphic with $A_5\times A_5$. (See [5].) Thus $\bar{H}(A)\cong A_5\times A_5$. This result is also given from Theorem 5.22 of [1], p. 203.

EXAMPLE 2. Let dim $V=4$ and $k=F_5$. Let $(x, x)=2x_1^2+x_2^2+x_3^2+x_4^2$. In this case, A consists of 65 elements. A has generators: $\bar{b}_1$, $\bar{b}_2$, $\bar{b}_3$ and $\bar{b}_4$, where $b_1=(0, 1, 0, 0)$, $b_2=(0, 2, 1, 1)$, $b_3=(0, 0, 1, 0)$ and $b_4=(2, 0, 2, 3)$. The diagram is

$$\bar{b}_1 \overset{3}{\text{———}} \bar{b}_2 \overset{5}{\text{———}} \bar{b}_3 \overset{3}{\text{———}} \bar{b}_4 .$$

This primitive set of order 65 is not found in [2], [4]. Note that in [2], [4], a primitive set is called simple. For this A, $\bar{H}(A)$ is isomorphic with $PSL_2(F_{25})$ from Theorem 5.21 of [1], p. 202.

EXAMPLE 3. Let dim $V=4$ and $k=F_3$. Let $(x, x)=x_1^2+x_2^2+x_3^2+x_4^2$. A consists of 12 elements and is isomorphic with A_4. It is not primitive.

EXAMPLE 4. Let dim $V=3$ and $k=F_5$. Let $(x, x)=x_1^2+x_2^2+x_3^2$. A consists of 15 elements. We can show that A is isomorphic with the symmetric subset of A_5 consisting of $(i\, j)\ (k\ l)$, where i, j, k and l are all distict. A is not primitive. $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ is a non-trivial block.

References

[1] E. Artin: Geometric algebra, Interscience, New York, 1957.

[2] Y. Ikeda and N. Nobussawa: *On symmetric sets of unimodular symmetric matrices,* Osaka J. Math **14** (1977), 471–480.

[3] H. Nagao: *A remark on simple symmetric sets,* Osaka J. Math. **16** (1979), 349–352.

[4] N. Nobusawa: *Simple symmetric sets and simple groups,* Osaka J. Math. **14** (1977), 411–415.

[5] N. Umaya: *On symmetric structure of a group,* Proc. Japan Acad. **52** (1976), 174–176.

Department of Mathematics
University of Hawaii
Honolulu, Hawaii 96822
U.S.A.