TECHNISCHE HOGESCHOOL EINDHOVEN
Afdeling Algemene Wetenschappen
Onderafdeling der Wiskunde

CLASSICAL GROUPS

by

Prof. Dr. D.G. Higman

With an appendix by D.E. Taylor

August 1978

August 1978

Technological University Eindhoven
Netherlands

Department of Mathematics

Classical Groups

by

D.G. Higman

With an appendix by D.E. Taylor

T.H.-Report 78-WSK-04

Inhoudsbeschrijving

CLASSICAL GROUPS

D.G. Higman

August 1978

JdG, 29 Juli 2005

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE

TECHNOLOGICAL UNIVERSITY EINDHOVEN
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS

Classical Groups

by

D.G. Higman

with an appendix

by

D.E. Taylor

T.H.-Report 78-WSK-04

August 1978

Preface

These are notes taken by W. Haemers and H. Wilbrink of an introductory course on classical groups (over commutative fields) given in the spring semester 1978 at the Department of Mathematics of the Technological University Eindhoven.
The main goal was the determination of the normal structure (assuming positive index in the unitary and orthogonal cases) by the method introduced by Iwasawa for the linear case and applied by Tamagawa to orthogonal groups.
Because of time considerations orthogonal groups over fields of characteristic 2 were omitted.
Some discussion of the sporadic isomorphisms is included.
An appendix by D.E. Taylor contains a uniform treatment of generic isomorphisms and a construction of the Suzuki groups.

D.G. Higman

1. Group actions and Iwasawa's lemma

Let G be a group with identity 1, say. An action of G on a set $X \neq \emptyset$ is a map: $G \times X \to X$, $(g,x) \mapsto gx$, such that

1) $(gh)x = g(hx)$

2) $1x = x$

$(g,h \in G,\ x \in X)$.

One can easily verify that an action of G on X is equivalent to a homomorphism: $G \to \Sigma_X$, where Σ_X denotes the symmetric group on X. The kernel of an action is the kernel of the corresponding homomorphism. An action is faithful if the kernel is trivial (= {1}). If the action is faithful then G is isomorphic to a subgroup of Σ_X, i.e. a permutation group. If the action has kernel K then G induces a faithful action of G/K on X.

A G-set (G-space) is a set $X \neq \emptyset$ with a given action of G on X. Two G-sets X and Y are isomorphic iff there is a bijection $\varphi: X \to Y$ such that $\varphi(gx) = g\varphi(x)$ $(g \in G,\ x \in X)$. Two actions of G are equivalent if the corresponding G-spaces are isomorphic.

A subset $Y \subseteq X$ is stable or a G-subspace (if $Y \neq \emptyset$) if $gy \in Y$ for all $y \in Y$, $g \in G$. If $Y \subseteq X$ is stable and $Y \neq \emptyset$ then G acts on Y.

Example. $\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$, the upper half plane of $\mathbb{C}$.
$SL_2(\mathbb{R})$ is the group of all matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a,b,c,d \in \mathbb{R}$ and $ad - bc = 1$. Let this group act on $\tilde{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ in the following way; if $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R})$ and $z \in \tilde{\mathbb{C}}$ then $gz := \frac{az + b}{cz + d}$. It follows easily that $\operatorname{Im}(gz) = \operatorname{Im}(z)/|cz + d|^2$ which implies that $\mathbb{H}$ is stable under $SL_2(\mathbb{R})$. The kernel of this action is $\{\pm I\}$, so $PSL_2(\mathbb{R}) := SL_2(\mathbb{R})/\{\pm I\}$ acts faithfully on $\tilde{\mathbb{C}}$. $SL_2(\mathbb{Z})$ is the subgroup of $SL_2(\mathbb{R})$ with coefficients in $\mathbb{Z}$. $G := SL_2(\mathbb{Z})/\{\pm I\}$ is the modular group. One can identify $SL_2(\mathbb{R})$ with $SL(\mathbb{R}^2)$, the group of all linear transformations of $\mathbb{R}^2$ with determinant 1. $SL(\mathbb{R}^2)$ acts on the points of the projective line based on $\mathbb{R}^2$, i.e. the 1 - dim subspaces of $\mathbb{R}^2$.

Let X be a G-space, $x,y \in X$. Define

$$x \sim y :\Leftrightarrow (gx = y \text{ for some } g \in G) .$$

Then ~ is an equivalence relation; the equivalence classes are the orbits. The action is transitive if there is only 1 orbit (= X). Each orbit is stable and transitive, each G-space is uniquely partitioned into a disjoint union of transitive G-spaces. Let X be a G-space, $H \subseteq G$, $Y \subseteq X$, then $HY := \{hy \mid h \in H,\ y \in Y\}$, $hY := \{h\}Y$ etc. The orbit containing $x \in X$ is Gx. If $H \leq G$ then $G/H := \{gH \mid g \in G\}$

is a transitive G-space according to $(g,hH) \mapsto (gh)H$, the natural action. Its kernel is the core of H in G, i.e. the join of all normal subgroups of G contained in H. A G-space is homogeneous if it is isomorphic with one of the form G/H for some $H \le G$.

Let X be a G-space, $x \in X$, $Y \subseteq X$, $Y \neq \emptyset$.

$G_x := \{g \in G \mid gx = x\}$ is the stabilizer of x in G,

$G_Y := N_G(Y) := \{g \in G \mid gY = Y\}$ is the (set-wise) stabilizer or normalizer of Y,

$G_{[Y]} := C_G(Y) := \{g \in G \mid gy = g, \forall y \in Y\} = \bigcap_{y \in Y} G_y$ is the pointwise stabilizer or centralizer of Y .

For $H \subseteq G$, $g \in G$, ${}^gH := gHg^{-1}$ is a conjugate of H in G.

The following properties are obvious:

1.1. a) G_x, G_Y, $G_{[Y]}$ are subgroups of G.

b) $G_x = G_{\{x\}} = G_{[\{x\}]}$ $(x \in X)$.

c) $G_{[X]}$ is the kernel of the action of G on X.

d) G_Y acts on Y with kernel $G_{[Y]}$. The corresponding permutation group will be denoted by G^Y so we have an exact sequence

$$1 \to G_{[Y]} \to G_Y \to G^Y \to 1$$

with G^Y a permutation group on Y, $G^Y \simeq G_Y/G_{[Y]}$.

In particular we have an exact sequence

$$1 \to G_{[X]} \to G \to G^X \to 1 \quad \text{with } G^X \le \Sigma_X$$

(An exact sequence is a sequence of homomorphisms $\ldots \to G \xrightarrow{\varphi} H \xrightarrow{\psi} K \to \ldots$ such that image of φ = kernel of ψ.

For example $1 \to G_{[Y]} \to G_Y$ means that the homomorphism $G_{[Y]} \to G_Y$ is injective etc.)

e) ${}^g(G_x) = G_{gx}$, ${}^g(G_Y) = G_{gY}$, ${}^g(G_{[Y]}) = G_{[gY]}$.

1.2. Let X be a G-space, $x \in X$ then $Gx \simeq G/G_x$ as G-spaces.

Proof. Take the map $gx \to gG_x$ for the isomorphism. □

As a corollary we have

1.3. Every transitive G-space is homogeneous.

1.4. If $H,K \leq G$ then G/H and G/K are isomorphic G-spaces iff H and K are conjugate.
Proof. If $H = {}^{g_1}K$ let the isomorphism φ be defined by

$$\varphi(gH) := gg_1K, \quad g \in G .$$

Conversely if φ is an isomorphism and $\varphi(H) = g_1K$ it follows that $H = {}^{g_1}K$. □

Assume G tra X (i.e. G acts transitively on X). An (imprimitive) block is a subset B of X, such that $gB \cap B \neq \emptyset$ implies $gB = B$ for all $g \in G$. The blocks $\emptyset$, $\{x\}$, X are trivial blocks. The action is imprimitive if there exists a non-trivial block, primitive otherwise. If $B \neq \emptyset$ is a block, then $\{gB \mid g \in G\}$ is a partition of X into blocks and G acts transitively on this set of blocks according to $(g,hB) \mapsto ghB$.

1.5. Suppose G tra X and let $x \in X$. The map $B \mapsto G_B$ is an isomorphism of the lattice of blocks containing x onto the lattice of subgroups of G containing G_x (the inverse map is $H \mapsto H_x$ for all $G_x \leq H \leq G$).

As a corollary to 1.5 we have

1.6. G pri X (i.e. G acts primitively on X) iff G_x is a maximal subgroup for some (hence for all) $x \in X$.

1.7. If G pri X and $N \trianglelefteq G$ then $N \leq G_{[X]}$ or N tra X.
Proof. Take $x \in X$ and suppose $N \nleq G_{[X]}$ then $N \nleq G_x$ (since $N \leq G_x$ implies $N = {}^gN \leq {}^gG_x = G_{gx}$ for all $g \in G$). Hence, by 1.6, $G = NG_x$. If $g \in G$ then $g = nh$ for some $n \in N$, $h \in G_x$ so $gx = nhx = nx$. □

Let X be a set and $k \in \mathbb{N}$, $k \geq 1$. We denote by X^k the k-fold Cartesian product of X with itself, $[{X \atop k}]$ the set of all $(x_1,\dots,x_k) \in X^k$ with $x_i \neq x_j$ $(1 \leq i < j \leq k)$, $\binom{X}{k}$ the set of all k-subsets of X.
An action of G on X induces actions on X^k, $[{X \atop k}]$ and $\binom{X}{k}$.

Remark. Take $(x_1,\dots,x_k) \in [{X \atop k}]$. The set $\{(y_1,\dots,y_k) \mid \{y_1,\dots,y_k\} = \{x_1,\dots,x_k\}\} \subset [{X \atop k}]$ is an imprimitive block for Σ_X. The action on this set of blocks is equivalent to the action on $\binom{X}{k}$.

Let X be a G-space and $k \in \mathbb{N}$, $k \geq 1$. The action is <u>regular</u> if G tra X and $G_x^X = 1$, for all $x \in X$ (note that if G is faithful and regular on X, then for any $x \in X$ the map $g \mapsto gx$ is a bijection of G onto X). The action is <u>k-fold transitive</u> or <u>k-transitive</u> (notation: G k-tra X) if G tra $[{X \atop k}]$. The action is <u>sharply k-(fold) transitive</u> if G acts regularly on $[{X \atop k}]$. The action is <u>k-homogeneous</u> if G tra $({X \atop k})$. In particular G 1-tra X means G tra X. Clearly G k-tra X implies G $(k-1)$-tra X.

1.8. G 2-tra X implies G pri X.
<u>Proof</u>. Let B be a block, $|B| \geq 2$. Take $x,y \in B$, $x \neq y$ and let $z \in X \backslash \{x\}$. There exists a $g \in G$ such that $gx = x$ and $gy = z$. From $x = gx \in B \cap gB$ it follows that $B = gB$ and so $z = gy \in gB = B$ i.e. $B = X$. □

Let G be a group. The <u>derived</u> or <u>commutator subgroup</u> G' of G is the intersection of all $N \trianglelefteq G$ such that G/N is Abelian. It follows that

$$G' = \langle [g,h] := ghg^{-1}h^{-1} \mid g,h \in G \rangle ,$$

the group generated by the commutators of G. Of course G/G' is Abelian, and G is Abelian iff $G' = 1$. We say that G is <u>simple</u> if the only normal subgroups of G are 1 and G itself.

1.9. (Iwasawa's lemma). Let G pri X, $x \in X$. Assume there exists $A(x) \trianglelefteq G_x$, such that A(x) is Abelian and $G = \langle {}^gA(x) \mid g \in G \rangle$. Then

a) $N \trianglelefteq G$ implies $N \leq G_{[X]}$ or $N \geq G'$.
b) If $G = G'$ then $G/G_{[X]}$ is simple.

<u>Proof</u>.
a) If $N \nleq G_{[X]}$ then $N \nleq G_x$ so $G = NG_x$. We claim: $G = NA(x)$. Indeed, let $g \in G$, since $g = nh$ for some $n \in N$, $h \in G_x$ we have ${}^gA(x) = {}^{nh}A(x) = {}^nA(x) \leq NA(x)$ and so $G = \langle {}^gA(x) \mid g \in G \rangle \leq NA(x) \leq G$ i.e. $NA(x) = G$. Now $G/N = NA(x)/N \simeq A(x)/N \cap A(x)$, which is Abelian, so $N \geq G'$.
b) Suppose $\bar{N} \trianglelefteq G/G_{[X]}$ then $\bar{N} = N/G_{[X]}$ with $G_{[X]} \leq N \trianglelefteq G$. If $\bar{N} \neq 1$ then $N \neq G_{[X]}$ hence by a) $N \geq G'$. From $G = G'$ it now follows that $N = G$, i.e. $\bar{N} = G/G_{[X]}$. □

2. The general linear group

Let V be a vectorspace over a field $\mathbb{F}$, dim V = n, $2 \le n < \infty$. GL(V) := the group of all non-singular linear transformations of V. This section is devoted to finding the normal subgroups of GL(V).

Let $v_1, \dots, v_n$ be a basis of V, $T \in GL(V)$, $T(v_i) = \sum_{j=1}^{n} a_{ji} v_j$, with $a_{ij} \in \mathbb{F}$. The map $T \mapsto A = (a_{ij})$ is an isomorphism of GL(V) onto $GL(n,\mathbb{F}) := GL_n(\mathbb{F}) :=$ the general linear group (of degree n over $\mathbb{F}$) := the group of all non-singular $n \times n$-matrices. Let $\mathbb{F}^*$ be the multiplicative group of the non-zero elements of $\mathbb{F}$. The determinant map det: $GL(V) \to \mathbb{F}^*$ is a group homomorphism and is onto. The kernel of det is $SL(V) = \{T \in GL(V) \mid \det T = 1\}$ so we have an exact sequence

$$1 \to SL(V) \to GL(V) \xrightarrow{\det} \mathbb{F}^* \to 1$$

and $GL(V)/SL(V) \simeq \mathbb{F}^*$ is Abelian (hence $SL(V) \ge GL(V)'$). $SL(V) \simeq SL(n,\mathbb{F}) := SL_n(\mathbb{F})$ = the special linear group (of degree n over $\mathbb{F}$) := the group of all $n \times n$-matrices with coefficients in $\mathbb{F}$ and determinant 1. GL(V) acts faithfully on $V^{\#} := V \setminus \{0\}$, $GL(V) \le \Sigma_{V^{\#}}$

2.1. GL(V) acts faithfully and regularly on the set of all ordered bases of V. Thus there is a 1-1 correspondence between GL(V) and the set of ordered bases of V. If $|\mathbb{F}| = q < \infty$ then $|GL(V)| = \#$ ordered bases of $V = (q^n - 1)(q^n - q)(q^n - q^2)\dots$ $\dots(q^n - q^{n-1})$, so

$$|GL(V)| = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1), \quad |SL(V)| = \frac{|GL(V)|}{|\mathbb{F}^*|} = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1) .$$

2.2. If $x \in V^{\#}$ then $\{ax \mid a \in \mathbb{F}^*\}$ is an imprimitive block. The corresponding action of GL(V) on blocks is equivalent to the action of GL(V) on the points of the projective space based on V i.e. on the 1-dimensional subspaces of V. Note that if $|\mathbb{F}| = 2$, then the action of GL(V) on $V^{\#}$ is equivalent to the action on the points of the projective space.

The projective space PV based on V is the lattice of subspaces of V. If V has dimension n then PV has dimension $n - 1$. The subspaces of V are the linear varieties or flats of PV. The codimension of a k-flat ($k + 1$ dimensional subspace of V) := codimension of the corresponding subspace ($= n - k - 1$). Dictionary:

PV	V
point	1-dim subspace
line	2-dim subspace
plane	3-dim subspace
k-dim lin variety } k-flat	(k + 1)-dim subspace
hyperplane	hyperplane (through 0)

A line of PV contains $|\mathbb{F}| + 1$ points. GL(V) acts on the k-flats of PV for all k. Look at the action on the points (0-flats) of PV. We have an exact sequence

$$1 \to Z(V) \to GL(V) \to PGL(V) \to 1 ,$$

where Z(V) is the kernel of this action, and $PGL(V) := GL(V)^{\text{points}} \simeq GL(V)/Z(V)$. PGL(V) is the <u>projective general linear group</u> (<u>of degree</u> n <u>over</u> $\mathbb{F}$).

2.3. $Z(V)$ = all nonzero scalar transformations $\{aI \mid a \in \mathbb{F}^*\}$.

<u>Proof</u>. Clearly $\{aI \mid a \in \mathbb{F}^*\} \leq Z(V)$. Suppose $v_1,\ldots,v_n$ is a basis of V. Let T be an element of Z(V). Then $T(v_i) = a_i v_i$ for some $a_i \in \mathbb{F}^*$, and $T(v_1 + \ldots + v_n) = a(v_1 + \ldots + v_n)$ for some $a \in \mathbb{F}$. Hence $a = a_1 = a_2 = \ldots = a_n$ and $T = aI$. □

$$PGL(V) \simeq PGL(n,\mathbb{F}) := GL(n,\mathbb{F})/\{aI \mid a \in \mathbb{F}^*\}.$$

2.4. If $|\mathbb{F}| = q$ then

$$|PGL(V)| = \frac{|GL(V)|}{|Z(V)|} = \frac{|GL(V)|}{(q-1)} = |SL(V)| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1) .$$

2.5. $Z(V)$ = center of $GL(V)$ = centralizer of $SL(V)$ in $GL(V)$. (If G is a group, $H \leq G$ then $C_G(H) := \{g \in G \mid gh = hg, \forall h \in H\}$ is the <u>centralizer</u> of H in G; $C_G(G)$ is the <u>center</u> of G.)

<u>Proof</u>. Clearly $Z(V) \leq C_{GL(V)}(GL(V)) \leq C_{GL(V)}(SL(V))$. Suppose $A \in GL(n,F)$ centralizes $SL(n,F)$ then $A(I + E_{ij}) = (I + E_{ij})A$ for all $i \neq j$. (E_{ij} is the matrix with a 1 in the (i,j)-position and 0's elsewhere.) Hence $AE_{ij} = E_{ij}A$ for all $i \neq j$ and so $A = aI$, $a \in \mathbb{F}$. □

SL(V) acts on the points of PV. We have an exact sequence

$$1 \to Z_0(V) \to SL(V) \to PSL(V) \to 1$$

where $Z_0(V)$ is the kernel of the action. $PSL(V) = SL(V)^{\text{points}} \simeq SL(V)/Z_0(V)$ and $PSL(V) \leq PGL(V) \leq \Sigma_{\text{pts}}$.

2.6. $Z_0(V) = Z(V) \cap SL(V) =$ center of $SL(V) = \{aI \mid a \in \mathbb{F}^*,\ a^n = 1\} \simeq$ the group of the n-th roots of unity in $\mathbb{F}$. Define $Z(n,\mathbb{F}) := \{aI \mid a \in \mathbb{F}^*\}$ = the group of all non-singular $n \times n$ scalar matrices, $Z_0(n,\mathbb{F}) := Z(n,\mathbb{F}) \cap SL(n,\mathbb{F})$ then

$$PSL(V) \simeq PSL(n,\mathbb{F}) := SL(n,\mathbb{F})/Z_0(n,\mathbb{F}) \ .$$

$PSL(n,\mathbb{F})$ is the <u>projective special linear group of degree n over</u> $\mathbb{F}$.

2.7. If $|\mathbb{F}| = q$ then $|PSL(V)| = \frac{1}{d}|SL(V)| = \frac{1}{d} q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1)$ where $d = (n, q-1)$.

With $(\mathbb{F}^*)^n := \{a^n \mid a \in \mathbb{F}^*\}$ we have the following commutative diagram in which the rows and columns are all exact. (Notice that $Z(V) \simeq \mathbb{F}^*$.)

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \to & (F^*)^n & \to & \mathbb{F}^* & \to & \mathbb{F}^*/(\mathbb{F}^*)^n & \to & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \to & Z(V) & \to & GL(V) & \to & PGL(V) & \to & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
1 & \to & Z_0(V) & \to & SL(V) & \to & PSL(V) & \to & 1 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

If $|\mathbb{F}| = q < \infty$ we sometimes write $GL(n,q)$ instead of $GL(n,\mathbb{F})$ etc. We have seen:

$$|GL(n,q)| = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1)$$

$$|SL(n,q)| = |PGL(n,q)| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1)$$

$$|PSL(n,q)| = \frac{1}{d} q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1),\ d = (n, q-1) \ .$$

<u>Remark</u>. Notice the order coincidence $|SL(n,q)| = |PGL(n,q)|$. In general (i.e. iff $d = (n,q-1) \neq 1$) $PGL(n,q) \not\simeq SL(n,q)$ since the center of $PGL(n,q)$ is 1.

An <u>n-simplex</u> in PV is a set of $n+1$ points no n of which are in a hyperplane. For any n-simplex $\{P_1,\dots,P_{n+1}\}$ we can choose a basis $v_1,\dots,v_n$ of V such that $P_i = \langle v_i \rangle$, $1 \le i \le n$, and $P_{n+1} = \langle \sum_{i=1}^{n} v_i \rangle$. This implies that $GL(V)$ acts regularly on the set of ordered simplices.
The following properties are easy to verify:

2.8. GL(V) 2-tra pts of PV.

If $n \geq 3$ then GL(V) and SL(V) not 3-tra on pts of PV (there are collinear and non-collinear triples of pts).

If $n = 2$ then GL(V) sharply 3-tra pts (in this case we usually view PV as the set $\mathbb{F} \cup \{\infty\}$ in such a way that the point $\langle (x_1,x_2) \rangle$ corresponds to $x_1/x_2 \in \mathbb{F}$ if $x_2 \neq 0$ and $\langle (1,0) \rangle \leftrightarrow \infty$. Thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(V)$ induces the Möbius transformation $(x \mapsto \frac{ax+b}{cx+d}) \in PGL(V)$. Notice that $(x \mapsto \frac{ax+b}{cx+d}) \in PSL(V)$ iff $ad - bc = \square$ (= a square in $\mathbb{F}$)).

If q is even then $PSL(2,q) = PGL(2,q)$ acts sharply 3-tra on pts.

If q is odd then $|PSL(2,q)| = \frac{1}{2}|PGL(2,q)|$ and PSL(2,q) is not 3-tra on pts.

If $q \equiv -1$ (4) then PSL(2,q) is 3-homogeneous. (Let x_1,x_2,x_3 be three distinct pts of $\mathbb{F} \cup \{\infty\}$. Define $g_1,g_2 \in PGL(2,q)$ by

$$g_1(x) = \frac{x_2 - x_3}{x_2 - x_1} \cdot \frac{x - x_1}{x - x_3}, \quad g_2(x) = \frac{x_3 - x_2}{x_3 - x_1} \cdot \frac{x - x_1}{x - x_2}$$

then $g_1(\{x_1,x_2,x_3\}) = g_2(\{x_1,x_2,x_3\}) = \{0,1,\infty\}$. Since $-1 \neq \square$ either $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = \square$ or $-1(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = \square$ i.e. either g_1 or g_2 is in PSL(2,q).).

SL(V) acts 2-tra on the pts of PV.

<u>The normal structure of GL(V)</u>

Let V^* denote the space of all linear functionals of V. Let $c \in V$, $\varphi \in V^*$ and define the map $\tau = \tau_{\varphi,c}: V \to V$ by $x \mapsto x + \varphi(x)c$. Clearly τ is a linear transformation of V, and $\tau_{0,c} = 1$.

2.9. If $\varphi(c) = -1$ then the kernel of $\tau = \langle c \rangle$.

2.10. If $\varphi(c) \neq -1$ then the kernel of $\tau = \{0\}$ hence $\tau \in GL(V)$.

<u>Proof</u>. Take $x \in \ker \tau$, then $x = -\varphi(x)c$ hence $x \in \langle c \rangle$; kernel of $\tau \neq \{0\} \Leftrightarrow \ker \tau = \langle c \rangle \Leftrightarrow c = -\varphi(c)c \Leftrightarrow \varphi(c) = -1$.

The linear transformation τ is called a <u>transvection</u> if $\varphi(c) = 0$. If $\varphi \neq 0$ then the kernel of φ is a hyperplane. This hyperplane contains c iff $\tau_{\varphi,c}$ is a transvection. A transvection $\tau_{\varphi,c}$ has matrix

$$\begin{pmatrix} 1 & & \varphi(v_n) \\ & \ddots & \\ & & 1 \end{pmatrix}$$

if we choose a basis $v_1,\dots,v_n$ of V such that $v_1,\dots,v_{n-1} \in \ker\varphi$ and $v_1 = c$. The determinant of a transvection equals 1, hence SL(V) contains all transvections. On the other hand all matrices

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \ddots & & & & \\ * & * & \cdots & * & 1 & * \cdots & * \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & & & * & & \\ & \ddots & & * & & \\ & & \ddots & \vdots & & \\ & & & * & & \\ & & & 1 & & \\ & & & * & \ddots & \\ & & & \vdots & & \\ & & & * & & 1 \end{pmatrix}$$

representent transvections.
In particular $I + aE_{ij}$, $a \in \mathbb{F}^*$, $i \neq j$, represent transvections. If $\varphi(c) \notin \{0,-1\}$ $\tau_{\varphi,c}$ is called a <u>dilatation</u>. If $v_1,\dots,v_n$ is a basis of V such that, $v_i \in \ker\varphi$ $(1 \le i \le n-1)$ and $v_n = c$ then the matrix of the dilatation $\tau_{\varphi,c}$ is

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & 1+\varphi(c) \end{pmatrix}.$$

On the other hand any matrix

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & * & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

with $* \neq 0,1$ represents a dilatation. The determinant of τ equals $1+\varphi(c) \notin \{0,1\}$ so $\tau \in GL(V)\backslash SL(V)$. The following properties are **easily** verified.

2.11. a) $\tau = \tau_{\varphi,c}$ fixes every vector in the kernel of φ.
b) $\tau = \tau_{\varphi,c}$ fixes every subspace containing c.

2.12. a) $\tau_{\varphi,ac} = \tau_{a\varphi,c}$ $(a \in \mathbb{F}^*)$.
b) If $\varphi_1(c) = 0$ then $\tau_{\varphi_1,c}\tau_{\varphi_2,c} = \tau_{\varphi_1+\varphi_2,c}$.
c) For any $T \in GL(V)$: ${}^{T}(\tau_{\varphi,c}) = \tau_{\varphi T^{-1},Tc}$.

Let H be a hyperplane of PV, let P be a point in H. Define the set of transvections $X_{H,P} := \{\tau_{\varphi,c} \mid \varphi(H) = 0,\ \langle c\rangle = P\}$.

2.13. $X_{H,P} \leq SL(V)_{H,P}$ and $X_{H,P} \trianglelefteq GL(V)_{H,P}$ for ${}^T(X_{H,P}) = X_{T(H),T(P)}$ for all $T \in GL(V)$.

2.14. $X_{H,P} \simeq (\mathbb{F},+)$ by result 2.12.

2.15. Let L be a line such that $L \cap H = P$ then $X_{H,P}$ acts faithfully and regularly on the points of $L\backslash\{P\}$.

Proof. Suppose P, Q and R are distinct points of L, $P = \langle p\rangle$, $Q = \langle q\rangle$, $R = \langle ap + q\rangle$. Choose $\varphi \in V^*$ such that $H = \ker \varphi$ and $\varphi(q) = a$ then $\tau_{\varphi,p} \in X_{H,P}$ and $\tau_{\varphi,p}(q) = q + \varphi(q)p = q + ap \therefore \tau_{\varphi,p}(Q) = R$. If $\tau \in X_{H,P}$ fixes any point not on H then $\tau = 1$. Suppose τ fixes $Q \not\leq H$, $Q = \langle q\rangle$, $\tau(q) = aq$ for some $a \in \mathbb{F}^*$ then $\tau(q) = aq = q + \varphi(q)p$ i.e. $\varphi(q) = 0$ hence $\varphi = 0$ and so $\tau = 1$. □

Let P be a point. Define $X_P := \{\tau_{\varphi,c} \mid \varphi \in V^*, \varphi(c) = 0, P = \langle c\rangle\}$.

2.16. $X_P \leq SL(V)_P$, $X_P \trianglelefteq GL(V)_P$ since ${}^T(X_P) = X_{T(P)}$ for all $T \in GL(V)$.

2.17. $X_P = \bigcup_{\substack{H \\ P\leq H}} X_{P,H}$, a partition (i.e. $X_{P,H_1} \cap X_{P,H_2} = 1$, $H_1 \neq H_2$).

2.18. X_P acts regularly on the points different from P of any line L through P.

Proof. Let H be a hyperplane such that $H \cap L = P$, then $X_{H,P}$ tra $L\backslash\{P\}$, and $X_{H,P} \leq X_P$, hence X_P tra $L\backslash\{P\}$. Suppose $\tau \in X_P$ fixes $Q \subseteq L$, $Q \neq P$. From 2.17 we see that $\tau \in X_{H,P}$ for some hyperplane H containing P. If $L \subseteq H$ then τ acts trivially on H and so τ acts trivially on L. If $L \subseteq H$ then $\tau = 1$ by 2.15. □

2.19. Let $c \in V$, $P = \langle c\rangle$. Define the homomorphism $\Phi\colon V^* \to \mathbb{F}$ by $\Phi(\varphi) = \varphi(c)$, then $X_P \simeq$ kernel Φ.

Proof. The isomorphism is given by $\tau_{\varphi,c} \mapsto \varphi$. □

2.20. GL(V) is generated by the transformations $\tau_{\varphi,c}$, $\varphi \in V^*$, $c \in V\backslash\{0\}$. SL(V) is generated by the transvections $\tau_{\varphi,c}$ $\varphi \in V^*$, $c \in V\backslash\{0\}$, $\varphi(c) = 0$.

Proof. Any $A \in GL(n,\mathbb{F})$ can be reduced to the form $\begin{pmatrix} I & 0 \\ 0 & * \end{pmatrix}$ (where $* = 1$ iff $A \in SL(n,\mathbb{F})$), by elementary row operations of the form: add a multiple of one row to a different row. Each such operation can be obtained by multiplication with a matrix of the form $I + aE_{ij}$, $i \neq j$. □

2.21. As a corollary we have $SL(V) = \langle {}^T X_P \mid T \in SL(V)\rangle$, indeed ${}^T X_P = X_{T(P)}$, and SL(V) is transitive on the points.

We have the following structure

$$\begin{array}{rl} GL(V) & \\ & \} \simeq \mathbb{F}^*, \text{ Abelian} \\ SL(V) & \\ & \} \; PSL(V) \\ Z(V) \cap SL(V) = Z_0(V) & \\ & \} \text{ central} \\ 1 & \end{array}$$

We shall obtain the simplicity of PSL(V) from Iwasawa's lemma applied to the action of SL(V) on the points. We have $SL(V) = \langle {}^T X_P \mid T \in SL(V) \rangle$ with $X_P \trianglelefteq SL(V)_P$ and (from 2.19) X_P is Abelian. So we still have to show:

1) SL(V) is primitive on the points, and

2) $SL(V) = SL(V)'$.

2.22. SL(V) acts 2-transitively on the points.

Proof. We show that $SL(V)_P$ is transitive on the points different from P. Take distinct points P, Q and R. Suppose P, Q and R are on one line L. Take a hyperplane H such that $H \cap L = P$, then $X_{H,P}$ takes Q to R, and $X_{H,P} \leq SL(V)_P$. Suppose P, Q and R are not collinear. Let L be the line through Q and R. Take a point $S \subseteq L$, $S \neq Q,R$ and a hyperplane H containing P such that $H \cap L = S$, then $X_{H,S}$ fixes P and moves Q to R. □

2.23. In case $n \geq 3$ then $SL(V) = SL(V)'$.

Proof. $[I + aE_{ij}, I + bE_{jk}] = I + abE_{ik}$ for all $a,b \in \mathbb{F}^*$, i,j and k distinct (note that $E_{ij}E_{k\ell} = 0$, and $E_{ij}E_{jk} = E_{ik}$ for all distinct i,j,k and ℓ. In particular $(I + aE_{ij})^{-1} = I - aE_{ij}$ for all $i \neq j$). With respect to a suitable basis, every transvection can be written as $I + abE_{ij}$. □

2.24. If $n = 2$ and $|\mathbb{F}| \geq 4$ then $SL(V) = SL(V)'$.

Proof. Let $\tau = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ be a transvection. Take $a \in \mathbb{F}^*$ such that $a^2 \neq 1$. Put $b = \frac{c}{a^2 - 1}$ then $\tau = [\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}]$. □

2.25. If $(n,\mathbb{F}) \neq (2,GF(2)), (2,GF(3))$ then $PSL(n,\mathbb{F})$ is simple.

Proof. Apply Iwasawa's lemma. □

2.26. If $(n,\mathbb{F}) \neq (2,GF(2)), (2,GF(3))$ and $N \leq GL(V)$ then $N \trianglelefteq GL(V)$ iff $N \leq Z(V)$ or $N \geq GL(V)' = SL(V)$.

Proof.

a) $GL(V)' = SL(V)$. Indeed $GL(V)/SL(V) \simeq \mathbb{F}^*$ is Abelian, hence $GL(V)' \leq SL(V) = SL(V)' \leq GL(V)'$.

b) If $N \leq Z(V)$ then obviously $N \trianglelefteq GL(V)$. If $N \geq GL(V)'$ then $N/GL(V)' \trianglelefteq GL(V)/GL(V)'$, which is Abelian, so $N \trianglelefteq GL(V)$.

c) Let $N \trianglelefteq GL(V)$, $N \not\leq Z(V)$. Define $\bar{N} := NZ(V)/Z(V) \leq PGL(V)$. Suppose $N \cap SL(V) \leq Z_0(V)$ then $\bar{N} \cap PSL(V) = 1$ and so $\bar{N}$ and $PSL(V)$ commute elementwise. Moreover $\bar{N}$ is transitive on points. Fix a point P, take $G \in PSL(V)_P$, $\bar{n} \in \bar{N}$ then $G\bar{n}(p) = \bar{n}G(p) = \bar{n}(p)$, so $PSL(V)_P$ acts trivially on the points, a contradiction. Hence $N \cap SL(V) \not\leq Z_0(V)$ and so $N \geq SL(V)$ by the first part of Iwasawa's lemma. □

Order coincidences and sporadic isomorphisms involving PSL(n,q) and A_m

1) $PSL(2,2) \simeq \Sigma_3$	order: 6
2) $PSL(2,3) \simeq A_4$	12
3) $PSL(2,4) \simeq PSL(2,5) \simeq A_5$	60
4) $PSL(2,7) \simeq PSL(3,2)$	168
5) $PSL(2,9) \simeq A_6$	360
6) $PSL(3,4) \not\simeq PSL(4,2) \simeq A_8$	20160

Result 1, 2 and $PSL(2,4) \simeq A_5$ are straightforward. Using Sylow's theorem one can prove that there is only one simple group of order 60 and 168 (cf. [7], p. 183-185), this proves 3) and 4). It is easy to prove that the centers of the sylow-2 subgroups of PSL(3,4) and PSL(4,2) have order 4 and 2 resp., this proves the first part of 6). For the details, and for result 5 we refer to [5] or [7]. We will now sketch a proof of $PSL(4,2) \simeq A_8$ due to A. Wagner (on collineation groups of Projective Spaces I, MATH. Z. 76, 411-426 (1961)): the projective plane of order 2 (**Fano plane**) can be represented by the array

$$\begin{matrix} 1&2&3&4&5&6&7 \\ 2&3&4&5&6&7&1 \\ 4&5&6&7&1&2&3 \end{matrix} .$$

Let A_7 act on this array to produce $\frac{|A_7|}{|PSL(3,2)|} = 15$ different projective planes of order 2. Define a new incidence structure $\mathcal{P}$, whose "points" are the 15 planes, and whose "lines" are the 35 triples out of {1,...,7}. A "line" is incident with a "point" if the corresponding triple represents a line of the corresponding Fano plane. By verification it follows that $\mathcal{P}$ is a projective space, hence $\mathcal{P} = PG(3,2)$, whose automorphism group is PSL(4,2). Thus we have $A_7 \leq PSL(4,2)$ with index 8, hence $PSL(4,2) \leq \Sigma_8$, so $PSL(4,2) \simeq A_8$. Alternative proofs of all sporadic isomorphisms involving alternating and classical groups will be given at a later date.

We remark on some natural questions arising from our geometrical discussion of GL(V). (Details can be found in [1], [3] and [6].) We assume $n \geq 3$. For the case $n = 2$ we refer to [3].
A collineation of PV is a permutation of the points which induces a permutation of the lines. The group of all collineations of PV is denoted by Coll PV. Of course $PSL(V) \leq PGL(V) \leq \text{Coll } PV$.

Questions
1) What is the analytic description of Coll PV?
2) What is the synthetic description of PGL(V) and PSL(V)?

About 1). Let $\tau \in \text{Aut}\,\mathbb{F}$. A τ-semilinear transformation of V is a map $T: V \to V$ such that $T(x+y) = T(x) + T(y)$, $T(ax) = \tau(a)T(x)$ for all $x,y \in V$, $a \in \mathbb{F}^*$.
If S σ-semilinear and T τ-semilinear then $ST(ax) = S(\tau(a)T(x)) = \sigma\tau(a)ST(x)$, hence ST is $\sigma\tau$-semilinear.
We define $\Gamma L(V)$:= the group of all non-singular semilinear transformations of V. $\Gamma L(V)$ acts on the points; Z(V) is the kernel. We have:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & & \uparrow & & & & \\ & & & & \text{Aut}\,\mathbb{F} & & & & \\ & & & & \uparrow & & & & \\ 1 & \to & Z(V) & \to & \Gamma L(V) & \to & P\Gamma L(V) & \to & 1 \quad \text{(exact)} \\ & & & & \uparrow & & & & \\ & & & & GL(V) & & & & \\ & & & & \uparrow & & & & \\ & & & & 1 & & & & \end{array}$$

1) $P\Gamma L(V) = \text{Coll } PV$.

About 2). A collineation σ of PV is central if σ fixes all points of some hyperplane H and all lines through some point P. If $\sigma \neq 1$ then H and P are uniquely determined and P together with the points of H is the complete set of fixed points of σ. H is called the axis and P the center. A central collineation is called an elation in case $P \subseteq H$. A projectivity is the product of central collineations, a perspectivity is the product of elations.

2) A central collineation is induced by exactly one linear transformation of the form $\tau_{\varphi,c}$.
3) PGL(V) is the group of all projectivities. PSL(V) is the group of all perspectivities.

3. Pairings and bilinear forms

a) Dual spaces

Let $\mathbb{F}$ be a field and let V and W be vector spaces over $\mathbb{F}$. Define $\mathrm{Hom}(V,W) := \mathrm{Hom}_{\mathbb{F}}(V,W) :=$ the vector space of all linear transformations from V to W (addition and scalar multiplication defined pointwise). Suppose the dimensions of V and W are finite, let $v_1,\dots,v_m$ and $w_1,\dots,w_n$ be bases for V and W respectively. Then $T_{ij}(v_k) = \delta_{kj}w_i$ defines $T_{ij} \in \mathrm{Hom}(V,W)$ and $\{T_{ij} \mid 1 \le i \le n, 1 \le j \le m\}$ is a basis of Hom(V,W). So the dimension of Hom(V,W) equals mn. In case $W = \mathbb{F}$ we write $V^* := \mathrm{Hom}(V,\mathbb{F})$ and V^* is called the dual space of V. If $v_1,\dots,v_m$ is a basis of V then the dual basis $v_1^*,\dots,v_m^*$ of V^* is defined by $v_i^*(v_j) := \delta_{ij}$ $(i,j = 1,\dots,m)$. The map $v_i \mapsto v_i^*$ determines an isomorphism of V with V^*. If the dimension is infinite then V and V^* are not isomorphic. There is a natural isomorphism σ of V onto a subspace of V^{**}, namely

$$\sigma(x)\{f\} := f(x), \quad x \in V,\ f \in V^* .$$

If the dimension of V is finite then $\sigma\colon V \xrightarrow{\sim} V^{**}$ (i.e. σ is an isomorphism of V and V^{**}).

b) Pairings

Let V and W be finite dimensional vectorspaces over the field $\mathbb{F}$. Bil(V,W) denotes the space of all bilinear maps $f\colon V \times W \to \mathbb{F}$ (Example: $W = V^*$; $(x,\varphi) \mapsto \varphi(x)$).

Let $v_1,\dots,v_m$ and $w_1,\dots,w_n$ be bases of V and W resp., let $f \in \mathrm{Bil}(V,W)$ and A the $m \times n$ matrix $(f(v_i,w_j))$. The map $f \mapsto A$ is an isomorphism of Bil(V,W) and $\mathbb{F}_{m\times n}$. Define new bases for V and W by $v_i' := \sum_{j=1}^m p_{ij}v_j$ and $w_i' := \sum_{j=1}^n q_{ij}w_j$. Put $P = (p_{ij})$, $Q = (q_{ij})$ then $(f(v_i',w_j')) = PAQ^t$. We speak of $f \in \mathrm{Bil}(V,W)$ as a pairing of V and W. Fix a pairing $f \in \mathrm{Bil}(V,W)$. We define

$$L_f := \{x \in V \mid f(x,y) = 0,\ \forall y \in W\}$$

and

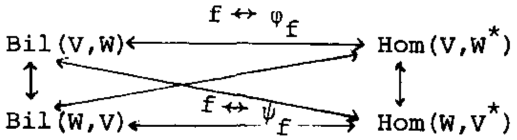
$$R_f := \{y \in W \mid f(x,y) = 0,\ \forall x \in V\},$$

the left and right kernel of f.

We now have the linear maps

$$\left.\begin{array}{l}\varphi_f\colon V \to W^*,\ \varphi_f(x)(y) := f(x,y)\\ \psi_f\colon W \to V^*,\ \psi_f(y)(x) := f(x,y)\end{array}\right\} \quad x \in V,\ y \in W .$$

Note that the kernel of $\varphi_f = L_f$ and the kernel of $\psi_f = R_f$. We have the following commutative diagram of isomorphisms:



Again fix $f \in \mathrm{Bil}(V,W)$. Let $H \le V$, $K \le W$ and define

$$H^\perp := \{y \in W \mid f(x,y) = 0,\ \forall x \in H\}$$

and

$$^\perp K := \{x \in V \mid f(x,y) = 0,\ \forall y \in K\}\ .$$

3.1. $H^\perp \le W$; $H_1 \le H_2$ implies $H_1^\perp \ge H_2^\perp$, $\forall H, H_1, H_2 \le V$.
$^\perp K \le V$; $K_1 \le K_2$ implies $^\perp K_1 \ge {}^\perp K_2$, $\forall K, K_1, K_2 \le W$.
$V^\perp = R_f$, $^\perp W = L_f$.
$^\perp(H^\perp) \ge H$, $\forall H \le V$; $(^\perp K)^\perp \ge K$, $\forall K \le W$.

3.2. If $H \le V$ then there is a linear injection $W/H^\perp \to H^*$, so codim $H^\perp \le \dim H$.
Proof. The map $f_1 : H \times W/H^\perp \to \mathbb{F}$, $(x, H^\perp + y) \mapsto f(x,y)$ is a well defined pairing of H and $W/H^\perp$. Suppose $H^\perp + y \in R_{f_1}$ then $f(x,y) = 0$ for all $x \in H$. Hence $y \in H^\perp$ so $H^\perp + y = H^\perp \equiv 0$ in $W/H^\perp$. This implies $R_{f_1} = 0$ hence $\psi_{f_1} : W/H^\perp \to H^*$ is injective. □

3.3. If $L_f = 0$ and $K \le W$, then we have an injection $^\perp K \to (W/K)^*$ so $\dim {}^\perp K \le$ codim K.
Proof. The map $f_2 : {}^\perp K \times W/K \to \mathbb{F}$, $(x, K+y) \mapsto f(x,y)$ is a well defined pairing. Suppose $x \in L_{f_2}$ then $f(x,y) = 0$ for all $y \in W$. Hence $x \in L_f$ so $x = 0$. This implies $L_{f_2} = 0$, hence $\varphi_{f_2} : K \to (W/K)^*$ is injective. □

3.4. If $L_f = 0$ and $H \le V$ then codim $H^\perp = \dim H$ and $^\perp(H^\perp) = H$.
Proof. $\dim {}^\perp(H^\perp) \overset{(3.3)}{\le}$ codim $H^\perp \overset{(3.2)}{\le} \dim H \overset{(3.1)}{\le} \dim {}^\perp(H^\perp)$. Hence codim $H^\perp = \dim H = \dim {}^\perp(H^\perp)$. □

3.5. If $L_f = 0$ then codim $R_f = \dim V$.
Proof. $R_f = V^\perp$, so take $H = V$ in 3.4. □

3.6. codim L_f = codim R_f.
Proof. The map $f_0 : V/L_f \times W$, $(L_f + x, y) \mapsto f(x,y)$ is a well defined pairing. $L_{f_0} = 0$ and $R_{f_0} = R_f$, hence $\dim V/L_f$ = codim R_f by 3.5. □

Call f nondegenerate if $L_f = R_f = 0$ (this is equivalent to $\dim V = \dim W$ and $\det A \ne 0$ for any matrix A of f).

3.7. If f is a nondegenerate pairing of V and W, then

i) dim V = dim W.

ii) $\varphi_f: V \tilde{\to} W^*$ and $\psi_f: W \tilde{\to} V^*$.

iii) dim H = codim $H^\perp$, for all $H \le V$.
dim K = codim ${}^\perp K$, for all $K \le W$.

iv) ${}^\perp(H^\perp) = H$, for all $H \le V$.
$({}^\perp K)^\perp = K$, for all $K \le W$.

v) $H \mapsto H^\perp$ is a 1-1 inclusion reversing map from the subspaces of V to the subspaces of W. The inverse is $K \mapsto {}^\perp K$.

Example. The pairing of V and V^* defined by $(x,\lambda) \mapsto \lambda(x)$ is nondegenerate; $\varphi: V \to V^{**}$ is σ (the natural isomorphism); $\psi: V^* \to V^*$ is the identity.

c) Bilinear forms

Let V denote a finite dimensional vectorspace over the field $\mathbb{F}$. Let f be a bilinear form on V (i.e. a pairing of V with V). Let $v_1,\dots,v_n$ and $v'_1,\dots,v'_n$ be two bases of V such that $v'_i = \sum_{i=1}^n p_{ij}v_j$, $i = 1,\dots,n$. Put $P = (p_{ij})$, $A = (f(v_i,v_j))$ then $(f(v'_i,v'_j)) = PAP^t$. Det A, determined up to a nonzero square in $\mathbb{F}$, is called the discriminant of f.

3.8. The following are equivalent:
f is nondegenerate;
$L_f = 0$;
$R_f = 0$;
$\varphi_f: V \tilde{\to} V^*$;
$\psi_f: V \tilde{\to} V^*$;
The discriminant of $f \neq 0$.

3.9. If f is a nondegenerate bilinear form on V and $H \le V$, then dim H = codim $H^\perp$ = codim ${}^\perp H$, ${}^\perp(H^\perp) = ({}^\perp H)^\perp = H$ and the map $H \mapsto H^\perp$ is an inclusion reversing permutation of the subspaces of V with inverse $H \mapsto {}^\perp H$ (in projective terminology: the map $H \mapsto H^\perp$ is a correlation of PV $(n \ge 3)$).

Example. $V = \mathbb{R}^n$, $f(x,y) = xy^t = \sum_{i=1}^n x_i y_i$, $f(x,y) = 0$ iff $f(y,x) = 0$ iff x and y are orthogonal. Take $H \le \mathbb{R}^n$ then $H^\perp = {}^\perp H$ is the orthogonal complement of H. $\dim H + \dim H^\perp = n$, $H \cap H^\perp = 0$, $\mathbb{R}^n = H \oplus H^\perp$.

In general we say x is orthogonal to y, notation $x \perp y$, iff $f(x,y) = 0$. It can happen that $x \perp y$ whilst $y \not\perp x$. We call f reflexive if $f(x,y) = 0$ iff $f(y,x) = 0$ for all $x,y \in V$ (so $\perp$ is a symmetric relation). If f is reflexive then ${}^{\perp}H = H^{\perp}$ for all $H \leq V$. It is possible that $H^{\perp} \cap H \neq 0$ therefore we prefer to call $H^{\perp}$ the perp(endicular) of H (rather than the orthogonal complement).

If a nondegenerate bilinear form f on V is reflexive, then the correlation $H \mapsto H^{\perp}$, $H \leq V$ has period two, i.e. $H^{\perp\perp} = H$. A correlation of period two is a polarity.

Let $f \in \mathrm{Bil}(V,V)$ then

i) f is symmetric if $f(x,y) = f(y,x)$ for all $x,y \in V$.
ii) f is skew-symmetric if $f(x,y) = -f(y,x)$ for all $x,y \in V$.
iii) f is alternate (symplectic) if $f(x,x) = 0$ for all $x \in V$.

3.10. If f is alternate then f is skew-symmetric.
Proof. $0 = f(x+y,x+y) = f(x,y) + f(y,x)$, for all $x,y \in V$. □

3.11. If char. $\mathbb{F} = 2$: f is symmetric iff f is skew-symmetric.

3.12. If char. $\mathbb{F} \neq 2$: f is alternate iff f is skew-symmetric.
Proof. "⇐": $f(x,x) = -f(x,x)$, hence $2f(x,x) = 0$, thus $f(x,x) = 0$. □

3.13. $f \in \mathrm{Bil}(V,V)$ is reflexive iff f is symmetric or alternate.
Proof. "⇐": It is clear that symmetric and alternate forms are reflexive.
"⇒": Assume f is reflexive. Then for all $a,b,c \in V$:

$$f(a,f(a,c)b - f(a,b)c) = f(a,c)f(a,b) - f(a,b)f(a,c) = 0,$$

hence $f(f(a,c)b - f(a,b)c,a) = 0$, i.e.

$$(*) \qquad f(a,c)f(b,a) - f(a,b)f(c,a) = 0, \qquad \text{for all } a,b,c \in V .$$

Take $a = c$ in (*): $f(a,a)(f(b,a) - f(a,b)) = 0$. Thus

$$(**) \qquad f(b,a) \neq f(a,b) \text{ implies } f(a,a) = f(b,b) = 0, \qquad \text{for all } a,b \in V .$$

Assume f is not symmetric, i.e. $f(a,b) \neq f(b,a)$ for some $a,b \in V$. Then $f(a,a) = f(b,b) = 0$. We wish to prove that $f(c,c) = 0$, for all $c \in V$. Assume $f(c,c) \neq 0$ for some $c \in V$. From (**) it follows $f(a,c) = f(c,a)$ and $f(b,c) = f(c,b)$. Then by (*) $f(a,c)(f(b,a) - f(a,b)) = 0$, hence $f(a,c) = 0 = f(c,a)$ and similarly $f(b,c) = 0 = f(c,b)$. Now we have

$$f(a+c,b) = f(a,b) + f(c,b) = f(a,b)$$

$$f(b,a+c) = f(b,a) + f(b,c) = f(b,a) \ .$$

By $f(a,b) \neq f(b,a)$ and (**) we have $f(a+c,a+c) = 0$, but $f(a+c,a+c) =$ $= f(a,a) + f(a,c) + f(c,a) + f(c,c) = f(c,c) = 0$ # . ||

d) Quadratic forms

A quadratic form is a map $Q: V \to \mathbb{F}$, such that

i) $Q(ax) = a^2 Q(x)$, for all $a \in \mathbb{F}$, $x \in V$.

ii) $f(x,y) := Q(x+y) - Q(x) - Q(y)$, $x,y \in V$ defines a bilinear form f on V.

3.14. f is symmetric.

3.15. $f(x,x) = 2Q(x)$ for all $x \in V$.

3.16. If char $\mathbb{F} \neq 2$: $Q(x) = \frac{1}{2}f(x,x)$, Q is uniquely determined by f. Moreover if f is any symmetric bilinear form on V then $Q(x) = \frac{1}{2}f(x,x)$ is a quadratic form having f as its associated bilinear form.

3.17. If char $\mathbb{F} = 2$: $f(x,x) = 0$ for all $x \in V$, i.e. f is alternate.

e) Reflexive bilinear form spaces

A pair (V,f), with V a finite dimensional vectorspace over the field $\mathbb{F}$, and f a reflexive bilinear form on V is called a reflexive bilinear form space. We say that (V,f) is symplectic if f is alternate, orthogonal if f is symmetric and char $\mathbb{F} \neq 2$. We assume char $\mathbb{F} \neq 2$ if f is symmetric: symmetric non-alternate bilinear forms in case char $\mathbb{F} = 2$ are explicitly excluded.
An isometry of (V,f) into (V',f') is an injective linear map $T: V \to V'$ such that $f'(T(x),T(y)) = f(x,y)$, for all $x,y \in V$. The radical of (V,f) is rad $(V,f) := V^{\perp}$; (V,f) is nondegenerate if rad$(V,f) = 0$, i.e. if f is nondegenerate. We take the following point of view: f is fixed; speak of the space V, meaning the reflexive bilinear form space (V,f) and say that V is symplectic, alternate, nondegenerate etc. according as (V,f) has the corresponding property.

3.18. If $U \leq V$ then $(U, f \mid U \times U)$ is a reflexive bilinear form space of the same type as V, and rad $U = U \cap U^{\perp}$.

If $V = V_1 \oplus \ldots \oplus V_r$ and the V_i are pairwise orthogonal then V is the <u>orthogonal direct sum</u> of $V_1, \ldots, V_r$ and we write $V = V_1 \perp \ldots \perp V_r$.
Given reflexive bilinear form spaces (V_i, f_i), $i = 1, \ldots, r$ we can define a bilinear form f on the direct sum $V = V_1 \oplus \ldots \oplus V_r$ by $f(x,y) = \sum_{i=1}^{r} f_i(x_i, y_i)$, $x = x_1 + \ldots + x_r$, $y = y_1 + \ldots + y_r$, $x_i, y_i \in V_i$, which is reflexive if the (V_i, f_i) are all of the same type. Identifying V_i with a subspace of V as usual we have $V = V_1 \perp \ldots \perp V_r$.

3.19. Suppose $V = V_1 + \ldots + V_r$ with V_i orthogonal to V_j for all $i \neq j$.

i) rad V = rad $V_1 + \ldots +$ rad V_r.

ii) If V_i is nondegenerate for $i = 1, \ldots, r$ then V is nondegenerate and $V = V_1 \perp \ldots \perp V_r$.

3.20. a) The map $V/\text{rad } V \times V/\text{rad } V \to \mathbb{F}$ defined by $(\text{rad } V + x, \text{rad } V + y) \mapsto f(x,y)$ is a well defined nondegenerate bilinear form on V/rad V.

b) If $V = \text{rad } V \oplus U$ then U is nondegenerate and $V = \text{rad } V \perp U$ and the natural isomorphism $U \to V/\text{rad } V$, $u \mapsto \text{rad } V + u$ is an isometry.

3.21. Suppose $V = V_1 \perp \ldots \perp V_r$, $U = U_1 \perp \ldots \perp U_r$, U and V spaces over the same field $\mathbb{F}$. Let $S_i: V_i \to U_i$ be an isometry $1 \le i \le r$. We can define an isometry $S: V \to U$ by $S(x) = S_1(x_1) + \ldots + S_r(x_r)$ for $x = x_1 + \ldots + x_r \in V$, $x_i \in V_i$. S is called the <u>orthogonal direct sum</u> of the S_i and we write $S = S_1 \perp \ldots \perp S_r$.

3.22. If $V = V_1 \perp \ldots \perp V_r$ and S_i is an isometry of $V_i \to V_i$, $1 \le i \le r$ then $S = S_1 \perp \ldots \perp S_r$ is an isometry of V onto V and $\det S = \det S_1 \ldots \det S_r$. If $T = T_1 \perp \ldots \perp T_r$, where T_i is an isometry of $V_i \to V_i$ then $ST = S_1T_1 \perp \ldots \perp S_rT_r$.

3.23. If V is nondegenerate and $U \le V$ then

a) $U^{\perp\perp} = U$ and $\dim U + \dim U^{\perp} = \dim V$.

b) rad U = rad $U^{\perp} = U \cap U^{\perp}$.

c) U is nondegenerate iff $U^{\perp}$ is nondegenerate.

d) U is nondegenerate iff $V = U \perp U^{\perp}$.

3.24. If $V = U \perp W$ with U,W nondegenerate then $W = U^{\perp}$.

(Note that we did not use **char $\mathbb{F} \neq 2$ so far).**
$x \in V$ is <u>isotropic</u> if $(x,x) = 0$ (notation: $(x,y) := f(x,y)$). $U \le V$ is <u>isotropic</u> if $U = 0$ or if there exists a nonzero vector $x \in U$ which is isotropic.

$U \leq V$ is totally isotropic if $(x,y) = 0$ for all $x,y \in U$, i.e. if rad $U = U$.

Note: A point P (of PV), i.e. a 1-dim subspace of V, is isotropic iff it is degenerate iff P is spanned by an isotropic vector.

3.25. If V is orthogonal and every vector of V is isotropic then V is totally isotropic.

Proof. f is symmetric. Every vector of V is isotropic means f is alternate, hence skew-symmetric. Therefore $f = 0$ (char $\mathbb{F} \neq 2$!). □

Let P be a point. P is isotropic iff $P \subseteq P^{\perp}$ ($P^{\perp}$ is the polar hyperplane of P). V is symplectic iff every point is isotropic. A line (2-dim subspace) is hyperbolic if it is nondegenerate and isotropic.

3.26. a) The hyperbolic lines are those of the form $P + Q$, where P and Q are nonorthogonal isotropic points.

b) The totally isotropic lines are those of the form $P + Q$, where P and Q are orthogonal isotropic points.

Proof.

a) Suppose L is hyperbolic, then there exists an isotropic point $P = \langle p \rangle \subseteq L$. Let $R = \langle r \rangle$ be a second point on L. $R \perp P$ would imply $P \subseteq \text{rad } L = 0$ so $R \not\perp P$ i.e. $(p,r) \neq 0$. If V is symplectic we have nothing to prove. Assume V is orthogonal. Let $q := ap + r$, $a \in \mathbb{F}$, then $(q,q) = 2a(p,r) + (r,r)$ so take $a = -\frac{(r,r)}{2(p,r)}$ then $(q,q) = 0$ and $Q := \langle q \rangle$ is isotropic and $L = P + Q$. If $L = P + Q$ with P and Q isotropic $(p,q) = a \neq 0$ then L has discriminant $\det\begin{bmatrix} 0 & a \\ \pm a & 0 \end{bmatrix} = \pm a^2 \neq 0$, so L is hyperbolic.

b) Trivial. □

An ordered pair P,Q of points is hyperbolic if P and Q are isotropic and not orthogonal. An ordered pair of vectors u,v is hyperbolic if $(u,u) = (v,v) = 0$ and $(u,v) = 1$. A line is hyperbolic if it passes through a hyperbolic pair of points, i.e. iff it is spanned by a hyperbolic pair of vectors.

Structure of reflexive bilinear form spaces

3.27. Let V be a symplectic space. Then

a) V is an orthogonal direct sum

$$V = P_1 \perp \ldots \perp P_s \perp L_1 \perp \ldots \perp L_r$$

where $P_1, \ldots, P_s$ are isotropic points and $L_1, \ldots, L_r$ are hyperbolic lines.

b) If V is decomposed as in a) then

$$\text{rad } V = P_1 \perp \ldots \perp P_s .$$

Proof.

a) Call a subspace $U \leq V$ indecomposable if it is not an orthogonal direct sum of proper subspaces. Certainly V is an orthogonal direct sum of indecomposable subspaces. By 3.20 b) rad U = U or rad U = 0 i.e. U is totally isotropic or nondegenerate. If U is totally isotropic then U is a point. If U is nondegenerate then $\dim U \geq 2$. Let P be a point of U then there exists a point $Q \subseteq U$ with $Q \not\perp P$. Now $L := P + Q$ is a hyperbolic line, L is nondegenerate, so $U = L \perp (L^\perp \cap U)$ i.e. $U = L$. This proves a).

b) According to 3.19

$$\text{rad } V = \text{rad } P_1 \perp \ldots \perp \text{rad } L_r = P_1 \perp \ldots \perp P_s . \qquad \square$$

The codimension of rad V (= 2r) is the rank of V.

3.28. Two symplectic spaces over $\mathbb{F}$ are isometric iff they have the same dimension and rank. A nondegenerate symplectic space V has even dimension.

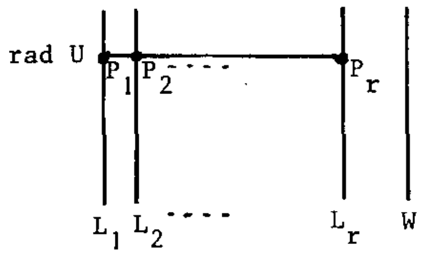
3.29. An orthogonal space is an orthogonal direct sum

$$V = P_1 \perp \ldots \perp P_s \perp Q_1 \perp \ldots \perp Q_r$$

with P_i isotropic $1 \leq i \leq s$, Q_i not isotropic $1 \leq i \leq r$.

Proof. We only need to determine the indecomposable subspaces. If U is totally isotropic then U is a point. If U is nondegenerate then there exists a nonisotropic point P in U bij 3.25. So $U = P \perp (P^\perp \cap U)$ hence U is a point. $\square$

3.30. Let V be a nondegenerate space, $U \leq V$. Choose a complement W for rad U, $U = \text{rad } U \perp W$ and a basis $u_1, \ldots, u_r$ of rad U. Put $P_i := \langle u_i \rangle$, $1 \leq i \leq r$. Then



1) there exists pairwise orthogonal hyperbolic lines $L_1, \ldots, L_r$ all orthogonal to W such that $P_i \subseteq L_i$, $1 \leq i \leq r$. Thus $\bar{U} = L_1 \perp L_2 \perp \ldots \perp L_r \perp W$ is a nondegenerate subspace containing U.

2) If $\sigma: U \to V'$ is an isometry of U onto some nondegenerate space V' then σ can be extended to an isometry $\bar{\sigma}: \bar{U} \to V'$.

Proof.

1) We use induction on r. There is nothing to prove if $r = 0$ $(U = \bar{U})$. Assume $r > 0$ and put $U_0 = \langle u_1,\dots,u_{r-1}\rangle \perp W$, so $\mathrm{rad}\ U_0 = \langle u_1,\dots,u_{r-1}\rangle = \mathrm{rad}\ U_0^{\perp}$. Since $P_r \not\subseteq U_0$ we have $U_0^{\perp} \subsetneq P_r^{\perp}$ so there exists a point $X \subseteq U_0^{\perp}$ with $X \not\perp P_r$. Now $L_r := P_r + X$ is a hyperbolic line and $L_r \subseteq U_0^{\perp}$. Since $L_r^{\perp}$ is nondegenerate we may apply the induction hypothesis to $U_0 = \mathrm{rad}\ U_0 \perp W \subseteq L_r^{\perp}$ to get pairwise orthogonal lines $L_1,\dots,L_{r-1}$ all orthogonal to W such that $P_i \subseteq L_i$ $1 \le i \le r-1$. This completes the induction.

2) Let $L_1,\dots,L_r$ be the hyperbolic lines constructed in 1). Then $L_i = \langle u_i, v_i\rangle$, u_i, v_i a hyperbolic pair, $1 \le i \le r$. Let $U' := \sigma(U)$, $u_i' := \sigma(u_i)$, $1 \le i \le r$, then $u_1',\dots,u_r'$ is a basis of rad U', $U' = \mathrm{rad}\ U' \perp W'$ with $W' := \sigma(W)$. Put $\bar{U}' = L_1' \perp\dots\perp L_r' \perp W'$ where $L_i' = \langle u_i', v_i'\rangle$, u_i', v_i' a hyperbolic pair, applying 1) to U'. Then $\bar{\sigma}(u_i) = u_i'$, $\bar{\sigma}(v_i) = v_i'$, $1 \le i \le r$, $\bar{\sigma}/W = \sigma/W$ is an isometry extending σ. □

3.31. If V is a nondegenerate symmetric space and x and y are nonisotropic vectors such that $(x,x) = (y,y)$ then there exists an isometry τ of V such that $\tau(x) = y$.

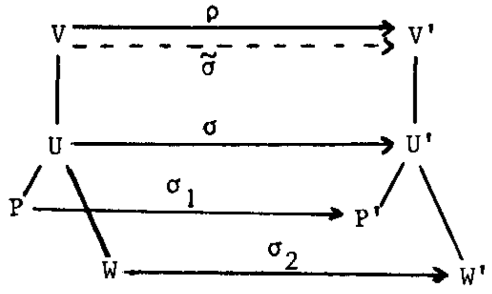
Proof. Since V is symmetric we have $x+y \perp x-y$. Since not both $(x+y,x+y) = 2((x,x) + (x,y))$ and $(x-y,x-y) = 2((x,x) - (x,y))$ can be 0 one of $x+y$ and $x-y$ is nonisotropic. Let $z = x + \varepsilon y$ with $\varepsilon = \pm 1$ such that z is nonisotropic. Then $V = \langle z\rangle \perp H$, $H = \langle z\rangle^{\perp}$ and $x - \varepsilon y \in H$. Let $\mu = \tau_{\varphi,z}$, $H = \ker \varphi$, $\varphi(z) = -2$. Then $\mu = 1_H \perp -1_{\langle z\rangle}$ so μ is an isometry, and $\mu(z) = \mu(x + \varepsilon y) = -x - \varepsilon y$, $\mu(x - \varepsilon y) = x - \varepsilon y$ hence $\mu(x) = -\varepsilon y$. So if $\varepsilon = -1$ we can take $\tau = \mu$, if $\varepsilon = +1$ we can take $\tau = -1_V \mu$. □

3.32. (Witt's theorem). Let V and V' be nondegenerate spaces and let $\rho: V \to V'$ be an isometry of V onto V' and $\sigma: U \to V'$ an isometry of a subspace U of V into V', then σ can be extended to an isometry $\tilde{\sigma}: V \to V'$.

Proof. By 3.30 we may assume that U is nondegenerate.

Case V is symplectic: $V = U \perp U^{\perp}$, $V' = U' \perp (U')^{\perp}$ where $U' := \sigma(U)$. $U^{\perp}$ and $(U')^{\perp}$ are nondegenerate symplectic spaces of the same dimension. Hence by 3.28 there exists an isometry τ of $U^{\perp}$ onto $(U')^{\perp}$. Then $\tilde{\sigma} := \sigma \perp \tau$ is an isometry of V extending σ.

Case V is orthogonal: Induction on dim U. If dim U = 1 an obvious application of 3.31. Assume dim U > 1, then $U = P \perp W$, $W = P^{\perp} \cap U$, P nonisotropic point. Let $U' := \sigma(U)$, $P' := \sigma(P)$, $W' := \sigma(W)$, $\sigma_1 := \sigma|P$, $\sigma_2 := \sigma|W$.



By induction we have an extension $\tilde{\sigma}_1: V \to V'$ of σ_1 and $\tilde{\sigma}_1(P) = P'$ so $\tilde{\sigma}_1(P^\perp) = (P')^\perp$. As $P^\perp$ is nondegenerate and $W \subseteq P^\perp$ we may apply induction hypothesis to $W \subseteq P^\perp$, $\sigma_2: W \to (P')^\perp$ to get an isometry $\tilde{\sigma}_2: P^\perp \to (P')^\perp$ extending σ_2. Now $V = P \perp P^\perp$ and $\tilde{\sigma} := \sigma_1 \perp \tilde{\sigma}_2$ is an isometry of V onto V' extending σ. □

Let V be nondegenerate. We may define: <u>index</u> V := max dim of a totally isotropic subspace of V. By 3.23 a) it follows that index $V \leq \frac{1}{2}$ dim V, with equality if V is symplectic because of 3.27.

3.33. All maximal totally isotropic subspaces of V have the same dimension, so index V = the dimension of any such subspace.
<u>Proof</u>. Apply Witt's theorem. □

3.34. Let V be a nondegenerate space of index r. Then

1) $V = H_{2r} \perp W$, where H_{2r} is an orthogonal direct sum of r hyperbolic lines and W is nonisotropic.
2) The geometry of W is independent of the choice of H_{2r}.

<u>Proof</u>.

1) Let U be a totally isotropic subspace of dim r. By 3.30 there exists $H_{2r} \supseteq U$. An H_{2s} has a totally isotropic subspace of dim s, so 2r is the max dimension of such a subspace. Moreover, $V = H_{2r} \perp W$, $W := H_{2r}^\perp$ and if $0 \neq x \in W$ is isotropic then $\langle H_{2r}, x\rangle$ contains a totally isotropic subspace of dim r + 1 $\#$.
2) Follows from Witt's theorem: If H'_{2r} is a second such sum of hyperbolic lines, then certainly there is an isometry σ of H_{2r} onto H'_{2r}. The σ extends to an isometry $\tilde{\sigma}$ of V and $\tilde{\sigma}(H_{2r}^\perp) = (H'_{2r})^\perp$. □

4. The symplectic group

Let (V,f) be a nondegenerate reflexive bilinear form space. The group of all isometries of (V,f) is denoted by $Sp(V)$ if (V,f) is symplectic and by $O(V,f)$ if (V,f) is orthogonal. $Sp(V)$ is called the symplectic group, $O(V,f)$ the orthogonal group. Let $v_1,\dots,v_n$ be a basis of V, and let $E = (f(v_i,v_j))$ be the corresponding matrix of f. Let $T \in GL(V)$ and $A \in GL(n,\mathbb{F})$ the matrix of T with respect to this basis. Then T is an isometry iff $AEA^t = E$.
We define $Sp(n,\mathbb{F}) := \{A \in GL(n,\mathbb{F}) \mid AEA^t = E\}$ if (V,f) is of symplectic type, $O(n,\mathbb{F},f) := \{A \in GL(n,\mathbb{F}) \mid AEA^t = E\}$ if (V,f) is of orthogonal type. Clearly $Sp(V) \simeq Sp(n,\mathbb{F})$ and $O(V,f) \simeq O(n,\mathbb{F},f)$.

4.1. Isometries of (V,f) have determinant ± 1.

Assume (V,f) is symplectic

By 3.27 V has even dimension $n = 2r$ and a symplectic basis $u_1,u_{-1},u_2,u_{-2},\dots$ $\dots,u_r,u_{-r}$, such that $(u_1,u_{-1}) = \dots = (u_r,u_{-r}) = 1$, $(u_i,u_j) = 0$ if $i + j \neq 0$.

4.2. $Sp(V)$ acts faithfully and regularly on the ordered symplectic bases.

Assume $\mathbb{F} = \mathbb{F}_q$, We can determine $|Sp(V)|$ by counting the ordered symplectic bases. Define $L := \langle u_1,u_{-1}\rangle$, then L is an hyperbolic line and $L^\perp = \langle u_2,u_{-2},\dots,u_r,u_{-r}\rangle$ is a nondegenerate symplectic space of dimension $2(r-1)$. Let $\varphi(r)$ denote the number of ordered symplectic bases, then $\varphi(r) = (\#$ hyperbolic pairs of vectors$)\cdot\varphi(r-1)$. Suppose u,v is a hyperbolic pair of vectors, then u,w is a hyperbolic pair iff $(u,v-w) = 0$, i.e. iff $v-w \in \langle u\rangle^\perp$. Hence the number of hyperbolic pairs equals $(q^{2r}-1)q^{2r-1}$, so $\varphi(r) = (q^{2r}-1)q^{2r-1} \cdot \varphi(r-1)$, and with $\varphi(1) = (q^2-1)q$ we find $\varphi(r) = q^{r^2}\prod_{i=1}^{r}(q^{2i}-1)$.

4.3. $|Sp(n,GF(q))| = q^{(\frac{n}{2})^2}\cdot\prod_{i=1}^{n/2}(q^{2i}-1)$.

If $n = 2$ then $|Sp(2,GF(q))| = q(q^2-1) = |SL(2,GF(q))|$. In fact:

4.4. $Sp(2,\mathbb{F}) \simeq SL(2,\mathbb{F})$ for any field $\mathbb{F}$.
Proof. Choose a hyperbolic pair of vectors as a basis of V. Then $E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and for any matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have $AEA^t = \begin{pmatrix} 0 & ad-bc \\ bc-ad & 0 \end{pmatrix} = E$ iff $ad-bc = 1$ i.e. iff $A \in SL(2,\mathbb{F})$. □

We consider the action of Sp(V) on the points of PV. We have an exact sequence

$$1 \to Zp(V) \to Sp(V) \to PSp(V) \to 1 \ ,$$

where $PSp(V) := Sp(V)^{\text{points}}$, $Zp(V)$ = kernel of this action = $Z(V) \cap Sp(V)$. A scalar transformation λI is in Sp(V) iff $\lambda I\ E\ \lambda I = E$, i.e. iff $\lambda = \pm 1$. Hence $Zp(V) = \{\pm 1\}$. If $\mathbb{F} = GF(q)$ then

$$|PSp(n,GF(q))| = \frac{1}{d}|Sp(n,GF(q))| = \frac{1}{d}\, q^{(\frac{n}{2})^2} \prod_{i=1}^{n/2} (q^{2i}-1)\ ,\ d = (2,q-1).$$

We know already that isometries have determinant +1 or -1. We shall show that symplectic isometries have determinant +1. First of all we determine the transformations $\tau_{\varphi,p}$ which are in Sp(V). Assume $\varphi \neq 0$, so $\tau := \tau_{\varphi,p} \neq 1$ and let $H := \ker \varphi$, $P := \langle p\rangle$ then

$\tau(Q) = Q$, for all $Q \subseteq H$, hence

$\tau(Q^{\perp}) = Q^{\perp}$, for all $Q \subseteq H$, hence

$P \subseteq Q^{\perp}$, for all $Q \subseteq H$, $Q \neq H^{\perp}$, hence

$Q \subseteq P^{\perp}$, for all $Q \subseteq H$, $Q \neq H^{\perp}$, hence

$H \backslash H^{\perp} \subseteq P^{\perp}$ so $H = P^{\perp}$.

This shows that $\tau \in X_{P,P^{\perp}}$. Conversely if $P = \langle p\rangle$ is any point and $1 \neq \tau \in X_{P,P^{\perp}}$ then $\tau(x) = x + a(p,x)p$ for some $a \in \mathbb{F}^*$, and τ is an isometry for $(\tau(x),\tau(y)) = (x,y) + a(p,x)(p,y) + a(x,p)(p,y) + a^2(p,x)(p,y)(p,p) = (x,y)$.

4.5. $X_{P,P^{\perp}} \leq Sp(V)$ for all points P.

If $T \in Sp(V)$ then $T(P^{\perp}) = T(P)^{\perp}$ so ${}^{T}(X_{P,P^{\perp}}) = X_{T(P),T(P)^{\perp}}$.

4.6. $X_{P,P^{\perp}} \trianglelefteq Sp(V)_{P,P^{\perp}} = Sp(V)_P = Sp(V)_{P^{\perp}}$.

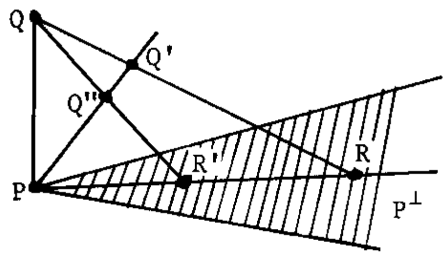
The elements of $X_{P,P^{\perp}}$ are called <u>symplectic transvections</u>. We know $X_{P,P^{\perp}} \simeq (\mathbb{F},+)$ is Abelian.

4.7. Sp(V) is generated by the symplectic transvections so $Sp(V) = \langle {}^{T}(X_{P,P^{\perp}}) \mid T \in Sp(V)\rangle$ since Sp(V) is transitive on the points of PV.

<u>Proof</u>. Let G(V) be the subgroup of Sp(V) generated by symplectic transvections. We show that G(V) is transitive on the ordered symplectic bases.

1) $G(V)$ is transitive on the vectors $\neq 0$. Let $u,v \in V\setminus\{0\}$.
<u>Case $u \not\perp v$</u>: $P := \langle u + v\rangle$ is a point on $L = \langle u,v\rangle$ and $P^{\perp} \cap L = P$. We know that $X_{P,P^{\perp}}$ moves u to v.
<u>Case $u \perp v$</u>: There exists a vector w such that $w \not\perp u$ and $w \not\perp v$, because $\langle u\rangle^{\perp} \cup \langle v\rangle^{\perp} \neq V$. Move u to w and w to v.

2) $G(V)$ is transitive on the hyperbolic pairs of vectors. Let $u,v;\ u'v'$ be hyperbolic pairs of vectors. By 1) we may assume $u = u'$. We must show the existance of $T \in G(V)$ such that $T(u) = u$, $T(v) = v'$. Let $P := \langle u\rangle$, $Q := \langle v\rangle$, $Q' := \langle v'\rangle$.
<u>Case P,Q,Q' collinear</u>: $L := P + Q + Q'$ is a line. Then $P^{\perp} \cap L = P$ and $X_{P,P^{\perp}}$ moves v to v' and fixes u.
<u>Case P,Q,Q' not collinear</u>: Let $R := (Q + Q') \cap P^{\perp}$. Suppose $Q \not\subseteq R^{\perp}$ then $X_{R,R^{\perp}}$ moves v to v' and fixes u. If $Q \subseteq R^{\perp}$ we take a point Q'' on $P + Q'$, $Q'' \neq P,Q'$. Let $R' := (Q + Q'') \cap P^{\perp}$. From $Q \subseteq R^{\perp}$ it follows that $R \subseteq Q^{\perp}$. Then $(P + R) \cap Q^{\perp} = R$ as $P \not\subseteq Q^{\perp}$. Hence $R' \not\subseteq Q^{\perp}$ as $R' \subseteq P + R$, $R' \neq R$. Thus $X_{R',(R')^{\perp}}$ moves Q to Q'' and Q'' can be moved to Q'.



3) $G(V)$ is transitive on ordered symplectic bases. Let $u_1,u_{-1},\dots,u_r,u_{-r}$ and $v_1,v_{-1},\dots,v_r,v_{-r}$ be two symplectic bases. We can assume $u_1 = v_1$, $u_{-1} = v_{-1}$ by 2). Then, if $L = \langle u_1,u_{-1}\rangle$, $L^{\perp} = \langle u_2,u_{-2},\dots,u_r,u_{-r}\rangle = \langle v_2,v_{-2},\dots,v_r,v_{-r}\rangle$. By induction there exists a $\sigma \in G(L^{\perp})$ such that $\sigma(u_i) = v_i$, $i = \pm 2,\dots,\pm r$. Put $T = 1_L \perp \sigma$ then T maps the one basis to the other. Clearly $T \in G(V)$ for if λ is a symplectic transvection of $L^{\perp}$ then $1_L \perp \lambda$ is a symplectic transvection of V. □

4.8. $T \in Sp(V)$ implies $\det T = 1$.

4.9. Center of $Sp(V) = \{\pm 1\}$.
<u>Proof</u>. Let T be in the center of $Sp(V)$ then ${}^{T}(X_{P,P^{\perp}}) = X_{P,P^{\perp}}$ for all points P. Therefore $T(P) = P$ for all P, i.e. $T \in Zp(V) = \{\pm 1\}$. □

4.10. $Sp(V)$
$\{\pm 1\}$ = center $Sp(V)$ } $PSp(V)$, simple?
1

In order to prove simplicity of PSp(V) we want to apply Iwasawa's lemma to the action of Sp(V) on the points of PV. So we still have to prove

a) Sp(V) acts primitively on the points.

b) Sp(V) is perfect.

Because $Sp(2,\mathbb{F}) \simeq SL(2,\mathbb{F})$ there will be exceptions to b) and we can restrict our investigations to $n \geq 4$. Now $n = 4$, $|\mathbb{F}| = 2$ is the first case and $|Sp(4,2)| = 2^4(2^2-1)(2^4-1) = 6! = |\Sigma_6|$. In fact

4.11. $Sp(4,2) \simeq PSp(4,2) \simeq \Sigma_6$ so PSp(4,2) is not simple.

This is an immediate corollary of:

4.12. $\Sigma_{2n+2} \leq Sp(2n,2)$.

Proof. Let X be a set of $2n+2$ points. The partitions of X into two subsets with an even number of points form a vectorspace of dimension 2n over GF(2) if we define addition by

$$\{A,X\backslash A\} + \{B,X\backslash B\} := \{A \dotplus B,\ X\backslash(A \dotplus B)\},\ A,B \subseteq X,\ |A| = |B| \equiv 0(2).$$

($A \dotplus B$ = symmetric difference of A and B = $(A \cup B)\backslash(A \cap B)$).

We can define a nondegenerate symplectic form on this vectorspace by

$$(\{A,X\backslash A\}, \{B,X\backslash B\}) := |A \cap B| \bmod 2,\ A,B \subseteq X,\ |A| = |B| \equiv 0(2).$$

It is clear that Σ_{2n+2} leaves this form invariant, hence $\Sigma_{2n+2} \leq Sp(2n,2)$. □

There is also a nice proof of 4.11 using the isomorphism $PSL(4,2) \simeq A_8$. Construct a polarity of PG(3,2) using A_6. A_6 commutes with this polarity ∴ $A_6 \leq PSp(4,2)$ so $\Sigma_6 \simeq PSp(4,2)$.

Let X denote the set of points of PV, $1 = 1_X$ the diagonal subset of X^2.

$$\alpha_1 := \{(P,Q) \notin 1 \mid P \perp Q\},\ \alpha_2 := \{(P,Q) \mid P \not\perp Q\}.$$

Clearly $X^2 = 1 \cup \alpha_1 \cup \alpha_2$ moreover by 4.2 we have

4.13. 1, α_1 and α_2 are the orbits for the componentwise action of Sp(V) on X^2 i.e. $X^2/Sp(V) = \{1,\alpha_1,\alpha_2\}$.

Note. 4.13 means that Sp(V) has rank 3 in its action on X i.e. PSp(V) is a rank 3 permutation group on X (if G tra X than G is said to be of rank r if G has r orbits on X^2).

Let $P \in X$, define for $i \in \{1,2\}$ $P\alpha_i := \{Q \mid (P,Q) \in \alpha_i\}$ so $P\alpha_i$ is the set of vertices in the graph (X,α_i) adjacent to P.

4.14. P, $P\alpha_1$ and $P\alpha_2$ are orbits for $Sp(V)_P$ acting on X i.e. $X/Sp(V)_P = \{\{P\},P\alpha_1,P\alpha_2\}$.

Note. (X,α_1), (X,α_2) is a pair of complementary strongly regular graphs or equivalently $(X,\{1,\alpha_1,\alpha_2\})$ is an association scheme with 2 treatments.

4.15. $Sp(V)$ pri X.

Proof. Let B be an imprimitive block, $|B| > 1$. We have to prove that $B = X$. Let $P \in B$, if $B \cap P\alpha_i \neq \emptyset$ then $P\alpha_i \subseteq B$. Moreover $Q\alpha_i \subseteq B$ for every $Q \in B$ since $Sp(V)_B$ tra B.

Case $B \cap P\alpha_1 \neq \emptyset$: Let R be any point not in $\{P\} \cup P\alpha_1 = P^{\perp}$, take $Q \in (R+P)^{\perp}$ then $R \in Q\alpha_1$ and $Q \in P\alpha_1 \subseteq B$, hence $R \in Q\alpha_1 \subseteq B$ i.e. $B = X$.

Case $B \cap P\alpha_2 \neq \emptyset$: Let R be any point not in $\{P\} \cup P\alpha_2$. Take $Q \in X\backslash(P^{\perp} \cup R^{\perp})$ then $Q \in P\alpha_2$ and $R \in Q\alpha_2 \subseteq B$, $\therefore$ $B = X$. □

Note. The essential thing in the above proof is that (X,α_1) and (X,α_2) are shown to be connected. The general statement is: Suppose G tra X then G pri X iff all graphs (X,α) are connected, $\alpha \in X^2/G$, $\alpha \neq 1$.

4.16. $Sp(n,\mathbb{F})$, $n = 2r$ is perfect unless $(n,|\mathbb{F}|) = (2,2)$, $(2,3)$, $(4,2)$.

Proof. Suppose $Sp(n,\mathbb{F})$ is perfect for some $n \geq 2$ and let $\tau \in X_{P,P^{\perp}}$ be a symplectic transvection in $Sp(n+2,\mathbb{F})$. Let L be a hyperbolic line such that $P \subseteq L^{\perp}$ then $V = L \perp L^{\perp}$ and $\tau = 1_L \perp \sigma$ where $\sigma = \tau \mid L^{\perp}$ is a symplectic transvection in $Sp(L^{\perp})$. Then σ is a product of commutators in $Sp(L^{\perp})$. If $\lambda,\mu \in Sp(L^{\perp})$ then $1_L \perp (\lambda,\mu) = (1_L \perp \lambda, 1_L \perp \mu)$, hence τ is a product of commutators in $Sp(n+2,\mathbb{F})$ $\therefore$ $Sp(n+2,\mathbb{F})$ is perfect. So

(*) If $SP(n,\mathbb{F})$ is perfect so is $Sp(m,\mathbb{F})$ for all $m \geq n$.

By 4.4 and 2.24 we have:

(**) If $|\mathbb{F}| > 3$ then $Sp(n,\mathbb{F})$ is perfect for all $n \geq 2$.

It remains to show that $Sp(4,3)$ and $Sp(6,2)$ are perfect. In each case it suffices to show the existence of a single transvections $\neq 1$ in the commutator subgroup (if $1 \neq \tau \in Sp(V)'$ is a symplectic transvection then $\tau \in X_{P,P^{\perp}}$ for some P. Since $X_{P,P^{\perp}} \simeq (\mathbb{F},+)$ has order 2 or 3, τ generates $X_{P,P^{\perp}}$ so $X_{P,P^{\perp}} \leq Sp(V)'$. Therefore $X_{T(P),T(P)'} = {}^{T}X_{P,P^{\perp}} \leq {}^{T}(Sp(V)') = Sp(V)'$ for all $T \in Sp(V)$). For this use the following. Let $u_1,u_{-1},u_2,u_{-2},\dots,u_r,u_{-r}$ be a symplectic basis of V. Rearrange: $u_1,\dots,u_r,u_{-1},\dots,u_{-r}$ then the matrix of our form looks like

$$E = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix}$$

Let $M := \langle u_1,\dots,u_r\rangle$, $N := \langle u_{-1},\dots,u_{-r}\rangle$.

1) If $T \in SL(V)$, $T(M) = M$ and $T(N) = N$, then T has matrix $\begin{bmatrix} A & 0 \\ 0 & C\end{bmatrix}$ and we see that $T \in Sp(V)$ iff $AC^t = I$. Hence the matrices $\begin{bmatrix} A & 0 \\ 0 & A^{-t}\end{bmatrix}$, $A \in GL(r,\mathbb{F})$ represent precisely those elements of Sp(V) which fix M and N.

2) If $S \in SL(V)$ and $S|M = 1_M$ then S has matrix $\begin{bmatrix} I & B \\ 0 & C\end{bmatrix}$ and $S \in Sp(V)$ iff $B = B^t$ and $C = I$. Hence the matrices $\begin{bmatrix} I & B \\ 0 & I\end{bmatrix}$ with $B = B^t \in \mathbb{F}_{r\times r}$ represent precisely the elements of Sp(V) fixing every vector of M.

If $T = \begin{bmatrix} A & 0 \\ 0 & A^{-t}\end{bmatrix}$, $S = \begin{bmatrix} I & B \\ 0 & I\end{bmatrix}$, $A \in GL(r,\mathbb{F})$, $B = B^t \in \mathbb{F}_{r\times r}$, then

$$(T,S) = \begin{bmatrix} A & 0 \\ 0 & A^{-t}\end{bmatrix}\begin{bmatrix} I & B \\ 0 & I\end{bmatrix}\begin{bmatrix} A^{-1} & 0 \\ 0 & A^{t}\end{bmatrix}\begin{bmatrix} I & -B \\ 0 & I\end{bmatrix} = \begin{bmatrix} I & ABA^t - B \\ 0 & I\end{bmatrix}.$$

To complete the proof of 4.16 we make suitable choices for A and B such that (T,S) represents a transvection. If $n = 4$, $\mathbb{F} = GF(3)$ take $A = \begin{bmatrix} 1 & 1 \\ 1 & 0\end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ -1 & 0\end{bmatrix}$ then $ABA^t - B = \begin{bmatrix} 1 & 0 \\ 0 & 0\end{bmatrix}$. If $n = 6$, $\mathbb{F} = GF(2)$, take

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0\end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1\end{bmatrix} \text{ then } ABA^t - B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0\end{bmatrix}. \quad \square$$

4.17. $PSp(n,\mathbb{F})$ is simple provided that $(n,|\mathbb{F}|) \neq (2,2), (2,3), (4,2)$.

Proof. Apply Iwasawa's lemma. □

Remark. Suppose V is a nondegenerate symplectic space of dim $n = 2r \geq 4$, X := points of PV, $\mathcal{L}$ = the totally isotropic lines. Then

1) 2 points lie on at most one line of $\mathcal{L}$.
2) Given a line $L \in \mathcal{L}$ and a point P not on L either
   a) exactly one point of L is joined by a line to P or
   b) every point of L is joined by a line to P.
   (Indeed, if $P \subseteq L^\perp$ then every point of L is collinear with P, if $P \nsubseteq L^\perp$ then $P^\perp \cap L = Q$ and Q is the unique point of L which is collinear with P).
3) Every line of $\mathcal{L}$ has at least 3 points and dually through every point pass at least 3 lines.

A system of points and lines satisfying 1), 2) and 3) is called a polar space. The polar spaces (with a mild finiteness condition) have been classified in the Buekenhout-Shult theorem. If b) does not occur the polar space is called a generalized quadrangle. This happens for example with $(X,\mathcal{L})$ when $n=4$ because then $L = L^{\perp}$.

5. The unitary group

Let $\mathbb{F}$ be a field, σ an automorphism of $\mathbb{F}$. We often write $\sigma(a) = \bar{a}$, $a \in \mathbb{F}$. Let V be a vectorspace over $\mathbb{F}$. A map $f: V \times V \to \mathbb{F}$ is σ-sesquilinear if $f(ax,y) = \bar{a}f(x,y)$, $f(x,ay) = af(x,y)$, $f(x+y,z) = f(x,z) + f(y,z)$, $f(x,y+z) = f(x,y) + f(x,z)$, for all $a \in \mathbb{F}$, $x,y,z \in V$.
We can define a new vectorspace structure on $(V,+)$ as follows: $a.x := \sigma^{-1}(a)x$, $a \in \mathbb{F}$, $x \in V$. We write ${}^{\sigma}V$ to denote $(V,+)$ with this new vectorspace structure. The σ-sesquilinear forms on V are precisely the pairings of ${}^{\sigma}V$ with V. In this way the theory of pairings can be applied to sesquilinear forms.
Let $H \leq V$ (notice that H is also a subspace of ${}^{\sigma}V$) then

$$H^{\perp} := \{x \in V \mid (H,x) = 0\};\ {}^{\perp}H := \{x \in V \mid (x,H) = 0\} .$$

The σ-sesquilinear form f is nondegenerate if ${}^{\perp}V = 0$ (or $V^{\perp} = 0$), which is equivalent to $\mathrm{Det}(f(x_i,x_j)) \neq 0$, where $x_1,\ldots,x_n$ is a basis of V.

5.1. If the σ-sesquilinear form f is nondegenerate then $H \mapsto H^{\perp}$ is an inclusion reversing permutation of the subspaces of V with inverse $H \mapsto {}^{\perp}H$ and $\dim H^{\perp} = \operatorname{codim} H$. Thus f induces a correlation of PV. (Every correlation is induced in this way provided $\dim V \geq 3$).

We state some facts about fields:

Let σ be an automorphism of the field $\mathbb{F}$, $\sigma^2 = 1$, $\sigma \neq 1$ and $\mathbb{F}_0$ the fixed field of σ, i.e. $\mathbb{F}_0 = \{a \in \mathbb{F} \mid \bar{a} = a\}$. Then $\mathbb{F}:\mathbb{F}_0 = 2$ and $\langle\sigma\rangle$ is the Galois group of $\mathbb{F}/\mathbb{F}_0$ (i.e. $\langle\sigma\rangle$ contains all the automorphisms of $\mathbb{F}$ that leave $\mathbb{F}_0$ fixed).
We define the maps:
trace: $\mathbb{F} \to \mathbb{F}_0$, $a \mapsto \bar{a} + a$, and norm: $\mathbb{F}^* \to \mathbb{F}_0^*$, $a \mapsto \bar{a}a$. We have

i) $\bar{a} + a = 0$ iff $a = c - \bar{c}$ for some $c \in \mathbb{F}$.

ii) $\bar{a}a = 1$ iff $a = \bar{d}/d$ for some $d \in \mathbb{F}$.

Indeed, take u such that $u + \bar{u} \neq 0$ and put $c = (u+\bar{u})^{-1}a\bar{u}$ in case i), and take u such that $a\bar{u} + u \neq 0$ and put $d = \bar{a}u + \bar{u}$ in case ii). From i) and ii) it follows that trace and norm are surjective if $|\mathbb{F}| < \infty$. A σ-sesquilinear form f on V is

reflexive if $f(x,y) = 0$ implies $f(y,x) = 0$, for all $x,y \in V$.
σ-hermitian if $\sigma^2 = 1$, $\sigma \neq 1$ and $f(x,y) = \overline{f(y,x)}$, for all $x,y \in V$.
σ-skew hermitian if $\sigma^2 = 1$, $\sigma \neq 1$ and $f(x,y) = -\overline{f(y,x)}$, for all $x,y \in V$.
Hermitian and skew hermitian forms are reflexive. If f is reflexive we define $\operatorname{rad} f := V^{\perp}$ $(= {}^{\perp}V)$. The form f is nondegenerate iff $\operatorname{rad} f = 0$. The nondegenerate reflexive σ-sesquilinear forms induce polarities of PV.

5.2. Let f be a nondegenerate reflexive σ-sesquilinear form on V and assume $\dim V \geq 2$. Then either

a) $\sigma = 1$ and f is symmetric or alternate, or
b) $\sigma^2 = 1$, $\sigma \neq 1$ and af is σ-hermitian for some $a \in \mathbb{F}^*$.

Proof. $\varphi_x\colon y \mapsto \sigma^{-1}f(y,x)$ is a linear functional for each $x \in V$, $\psi_x\colon y \mapsto f(x,y)$ is a linear functional for each $x \in V$. Clearly $\varphi_x(y) = 0$ iff $\psi_x(y) = 0$. This implies that for each $x \in V$ there exists $\lambda_x \in \mathbb{F}$ such that $\sigma^{-1}f(y,x) = \lambda_x f(x,y)$ for all $y \in V$. So $\sigma^{-1}f(z,x+y) = \lambda_{x+y}f(x+y,z) = \lambda_x f(x,z) + \lambda_y f(y,z)$,

$\therefore f(\lambda_{x+y}(x+y) - \lambda_x x - \lambda_y y, z) = 0$ for all $z \in V$.
$\therefore \lambda_{x+y}(x+y) - \lambda_x x - \lambda_y y = 0$.

If x and y are independent we have $\lambda_{x+y} = \lambda_x = \lambda_y$. If x and y are dependent, take z independent of x and y (we took $\dim V \geq 2$) then $\lambda_x = \lambda_z = \lambda_y$. This shows that λ_x does not depend on x. Write $\lambda = \lambda_x$. We have

$$\exists_{\lambda\in\mathbb{F}} \forall_{x,y\in V} [f(x,y) = \lambda\sigma^{-1}f(y,x)] .$$

$$f(x,y) = \lambda\sigma^{-1}(\lambda\sigma^{-1}f(x,y)) = \lambda\sigma^{-2}f(x,y)\sigma^{-1}(\lambda) .$$

Take $f(x,y) = 1$. Then $\lambda\sigma^{-1}(\lambda) = 1$, hence $f(x,y) = \lambda\sigma^{-2}f(x,y)\lambda^{-1}$, so $\sigma^{-2} = 1$ and we have

a) if $\sigma = 1$ then $\lambda^2 = 1$, $\lambda = \pm 1$,
b) if $\sigma \neq 1$ then $f(x,y) = \lambda\overline{f(y,x)}$. Take u such that $\bar{u}/u = \lambda$, then $uf(x,y) = \overline{uf(y,x)}$. □

Suppose f is hermitian, $a \in \mathbb{F}^*$ then

i) $a = \bar{a}$, i.e. $a \in \mathbb{F}_0$, implies af is hermitian,
ii) $a = -\bar{a}$, i.e. a is skew, implies af is skew hermitian.

Certainly skew elements exist, so w.l.o.g. we may assume that f is either hermitian or skew hermitian. A unitary space (V,f) consists of a vectorspace V together with a hermitian or skew hermitian σ-sesquilinear form for V. As before we define isotropic, totally isotropic, nonisotropic, isometry etc.; rad(V,f) = rad f = rad V. The unitary group U(V,f) = U(V) = U(f) := the group of all isometries of (V,f); $U^+(V,f)$ (= SU(V,f)) = the determinant 1 subgroup of U(V,f).

Let (V,f) be a nondegenerate unitary space, assume f is skew hermitian. A line L in V is hyperbolic if it is nondegenerate and isotropic. Let P = <p> be an isotropic point of L and R = <r> be any other point of L. We want an isotropic point $Q \neq P$ on L. For $Q = \langle ap + r\rangle$ we have $(ap + r,\ ap + r) = \bar{a}(p,r) + a(r,p) + (r,r)$. Now $(r,r) = -\overline{(r,r)}$ so $(r,r) = c - \bar{c}$ for some $c \in \mathbb{F}$. Put $(p,r) = b$ ($b \neq 0$ since otherwise $P \subseteq$ rad L) then $(ap + r,\ ap + r) = \bar{a}b - a\bar{b} + c - \bar{c} = \bar{a}b + c - \overline{(\bar{a}b + c)} = 0$ if we let $a = -\bar{c}/\bar{b}$.

An ordered pair p,q of vectors is <u>hyperbolic</u> if p and q are isotropic and $(p,q) = 1$. An ordered pair P,Q of points is hyperbolic if P and Q are isotropic and $P \not\perp Q$.

5.3. For a line L the following are equivalent

a) L is hyperbolic.

b) $L = \langle p,q\rangle$, where p,q is a hyperbolic pair of vectors.

c) $L = P + Q$, where P,Q is a hyperbolic pair of points.

Let $P + Q$, $P = \langle p\rangle$, $Q = \langle q\rangle$, be a hyperbolic line, p and q a hyperbolic pair of vectors then $p + aq$, $a \in \mathbb{F}$ is isotropic iff $a = \bar{a}$, i.e. $a \in \mathbb{F}_0$. The isotropic points $\neq Q$ are in a 1-1 correspondence with the field elements of $\mathbb{F}_0$, e.g. if $|\mathbb{F}_0| = q$ then $|\mathbb{F}| = q^2$ and $q+1$ of the q^2+1 points on a hyperbolic line are isotropic. Put $L_0 = \langle p,q\rangle_{\mathbb{F}_0} = \mathbb{F}_0 p \oplus \mathbb{F}_0 q$ then $f \mid L_0 \times L_0$ is a nondegenerate alternate form on L_0, i.e. L_0 is a symplectic hyperbolic line, the points of L_0 are precisely the isotropic points of L. The matrix of $f \mid L \times L$ is $J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $A \in SL(2,\mathbb{F})$ represents an element of $U^+(L)$ iff $AJ\bar{A}^t = J$ iff $A \in SL(2,\mathbb{F}_0)$: If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $ad - bc = 1$ then $AJ\bar{A}^t = J$ iff $a\bar{b} = b\bar{a}$, $c\bar{d} = d\bar{c}$, $a\bar{d} - b\bar{c} = 1$, i.e. iff $a = \bar{a}$, $b = \bar{b}$, $c = \bar{c}$, $d = \bar{d}$.

5.4. If L is a hyperbolic line then $U^+(L) \approx SL(2,\mathbb{F}_0)$ $(\approx Sp(2,\mathbb{F}_0))$.

Let V be a unitary space.

5.5. An indecomposable subspace $\neq 0$ is a point.

<u>Proof</u>. Let H be an indecomposable subspace of $V \neq 0$.

1) If H is degenerate then H is an isotropic point.

2) If H is nondegenerate then H contains a nonisotropic point. Indeed, suppose P is an isotropic point of H. Since $P \not\subseteq$ rad H there exists a point $Q \subseteq H$, $Q \not\perp P$. The line $L = P + Q$ is nondegenerate. Thus L is a hyperbolic line. Hence L contains a nonisotropic point. If R is a nonisotropic point of H then $H = R \perp (R^\perp \cap H)$ ∴ $H = R$. □

5.6. A unitary space V is an orthogonal direct sum of points, $V = P_1 \perp \ldots \perp P_s \perp Q_1 \perp \ldots \perp Q_t$, with $P_1,\ldots,P_s$ isotropic, $Q_1,\ldots,Q_t$ nonisotropic. If V is so decomposed then rad $V = P_1 \perp \ldots \perp P_s$.

5.7. If $\mathbb{F}$ is finite and dim $V \geq 2$ then V is isotropic.

Proof. It suffices to prove that an orthogonal direct sum $L = P \perp Q$ of non-isotropic points P and Q is isotropic. We may assume that f is hermitian. Let $P = \langle p\rangle$, $Q = \langle q\rangle$, $a := (p,p)$ then $a = \bar{a}$ so $a \in \mathbb{F}_0$. The norm is onto, so for suitable $\alpha \in \mathbb{F}$: $(\alpha p, \alpha p) = \bar{\alpha}\alpha a = 1$, i.e. we may assume $(p,p) = (q,q) = 1$. Then $(p + cq, p + cq) = 1 + \bar{c}c$ and we may take $c \in \mathbb{F}$ such that $\bar{c}c = -1$. □

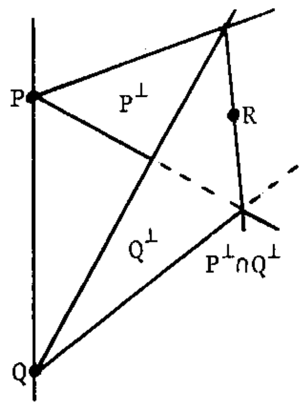
5.8. If $|\mathbb{F}| < \infty$ and V nondegenerate of dim n, then

$$V = \begin{cases} L_1 \perp \ldots \perp L_s & \text{if } n = 2s \\ L_1 \perp \ldots \perp L_s \perp P & \text{if } n = 2s + 1 \end{cases}$$

where the L_i's are hyperbolic lines and P is a nonisotropic point.

5.9. If $|\mathbb{F}| = q^2 < \infty$ and V nondegenerate of dim n then $\varphi(n) = \#$ of isotropic (non-zero) vectors $= (q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})$ and $\#$ of hyperbolic pairs of vectors $= q^{2n-3}\varphi(n)$.

Proof. Let P and Q be isotropic points such that $P + Q$ is non-degenerate. $\#$ isotropic points $= \varphi(n)/(q^2 - 1) = \#$ isotropic points on $P^\perp$ + $\#$ isotropic points off $P^\perp$. $P^\perp \cap Q^\perp = (P+Q)^\perp$ is nondegenerate. Each of the $\varphi(n-2)/(q^2-1)$ isotropic points R on $P^\perp \cap Q^\perp$ yields a totally isotropic line $P + R$. Hence, $\#$ isotropic points on $P^\perp = \frac{\varphi(n-2)}{q^2-1} q^2 + 1$.



Each of the $q^{2(n-1)}$ points S off $P^\perp$ yields a hyperbolic line $P + S$ containing q isotropic points. Hence, $\#$ isotropic points off $P^\perp = q.q^{2(n-1)}/q^2 = q^{2n-3}$. We get:
$\varphi(n) = q^2\varphi(n-2) + q^{2n-1} + q^{2n-3} + q^2 - 1$, $\varphi(0) = \varphi(1) = 0$.
This proves the required identities. □

Note that $\varphi(2)/(q^2-1) = q + 1$, $\varphi(3)/(q^2-1) = q^3 + 1$.

5.10. $|U(n,q)| = q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - (-1)^i)$.

Proof. Count the number of unitary bases using 5.9 and $|U(1,q)| = q + 1$ $|U(2,q)| = q(q^2-1)(q+1)$. □

The determinant map is a map from $U(V)$ onto $U_1 := \{\lambda \in \mathbb{F} \mid \lambda\bar{\lambda} = 1\}$. We have the exact sequence

$$1 \to U^+(V) \to U(V) \to U_1 \to 1 .$$

The isometries in $U^+(V)$, i.e. with det = 1, are called rotations.

If $|\mathbb{F}| = q^2 < \infty$ then $|U_1| = q + 1$, so $|U^+(V)| = \frac{1}{q+1} U(V)$,

$$|U^+(V)| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - (-1)^i) .$$

Look at the action of U(V) on the points of PV. We have the exact sequences

$$1 \to Z(V) \cap U(V) \to U(V) \to PU(V) \to 1 ,$$

$$1 \to Z(V) \cap U^+(V) \to U^+(V) \to PU^+(V) \to 1 ,$$

where $PU(V) = U(V)^{pts}$, $PU^+(V) = U^+(V)^{pts}$, $Z(V) \cap U(V) = \{\lambda I \mid \lambda\bar{\lambda} = 1\}$ and $Z(V) \cap U^+(V) = \{\lambda I \mid \lambda\bar{\lambda} = 1, \lambda^n = 1\}$. We have $|Z(V) \cap U(V)| = q + 1$, $|Z(V) \cap U^+(V)| = (n,q+1)$, hence

5.11. $|PU(n,q)| = q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - (-1)^i)$ $(= |U^+(n,q)|)$.

$|PU^+(n,q)| = d^{-1} q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - (-1)^i)$, $d = (n,q+1)$.

5.12. Result 3.30 holds with the same proof.

5.13. Witt's theorem (result 3.32) still holds but requires a different proof. We shall give a proof at the end of this chapter.

As a consequence we have

5.14. $U^+(V)$ is transitive on vectors of a given length $\neq 0$.

Suppose V is nondegenerate. The <u>index</u> ν of V is the maximal dimension of a totally isotropic subspace of V. So $\nu \geq 1$ iff V is isotropic. Witt's theorem implies that any two maximal isotropic subspaces have the same dimension, so ν is the dimension of any maximal totally isotropic subspace.

<u>Unitary transvections</u>

Let V be a nondegenerate unitary space. Assume f is skew-hermitian. Which transformations of the form $\tau_{\varphi,p}: x \mapsto x + \varphi(x)p$ are in U(V)? Suppose $\tau = \tau_{\varphi,p} \in U(V)$ then for all $x,y \in V$:

$$(x,y) = (\tau(x),\tau(y)) = (x + \varphi(x)p, y + \varphi(y)p) =$$

$$= (x,y) + \varphi(y)(x,p) + \overline{\varphi(x)}(p,y) + \overline{\varphi(x)}\varphi(y)(p,p) .$$

Hence,

(*) $\varphi(y)(x,p) + \overline{\varphi(x)}(p,y) + \overline{\varphi(x)}\varphi(y)(p,p) = 0,\ \forall x,y \in V$.

Put $H := \ker\varphi$ and fix $y \in V\backslash H$. By (*) $\varphi(y)(x,p) = 0$ for all $x \in H$. So, $(x,p) = 0$ for all $x \in H$. Therefore $H = P^{\perp}$, $P = \langle p\rangle$, and $\varphi(x) = a(p,x)$ for some $a \in \mathbb{F}$. Substitution of this result in (*) yields:

$$a(p,y)(x,p) + \bar{a}\overline{(p,x)}(p,y) + a\bar{a}\overline{(p,x)}(p,y)(p,p) = 0,\ \forall x,y \in V .$$

Take $x,y \in V\backslash H$ and divide by $(p,y)(p,x)$ to obtain $a - \bar{a} - a\bar{a}(p,p) = 0$. This condition is necessary and sufficient for $\tau_{\varphi,p}$ to be in $U(V)$. Clearly such a transformation is a transvection if and only if $(p,p) = 0$. □

The transvections of the form $\tau(x) = x + a(p,x)p$, $(p,p) = 0$, $a \in \mathbb{F}_0$ are the <u>unitary transvections</u>. Clearly all unitary transvections are in $U^+(V)$.
Let $P = \langle p\rangle$ be an isotropic point, $Y_p := \{\tau \mid \tau(x) = x + a(p,x)p,\ a \in \mathbb{F}_0\}$ is an Abelian group $\simeq (\mathbb{F}_0,+)$: Suppose L is a hyperbolic line through P, if L_0 is the subline of isotropic points on L then $Y_P|L = X_{PP^{\perp}}(L_0) \simeq (\mathbb{F}_0,+)$. Also $Y_P \trianglelefteq U^+(V)_P$.
Define, $T(V)$:= the subgroup of $U^+(V)$ generated by the unitary transvections. We want $U^+(V) = T(V)$. To examine this define $\sigma \in U^+(V)$ to be a <u>hyperbolic rotation</u> if there exists a hyperbolic line L such that σ fixes every vector of $L^{\perp}$, $\sigma = 1_{L^{\perp}} \perp \tau$, $\tau \in U^+(L) \simeq SL(2,L_0)$.

5.15. (Dieudonné). If $\mathbb{F}_0 \neq GF(2)$, $\nu \geq 1$, $n \geq 2$, then $U^+(V)$ is generated by the hyperbolic rotations.
<u>Proof</u>. Induction on n. For n = 2, O.K. Let $u \in U^+(V)$, x a nonisotropic vector such that $\langle x\rangle^{\perp}$ is isotropic. We shall show that there exist a product of hyperbolic rotations v such that $vu(x) = x$. Then the result follows by induction applied to $vu \mid \langle x\rangle^{\perp}$.
If $u(x) = x$ there is nothing to prove, so assume $u(x) \neq x$. We reduce to the case in which $u(x) - x$ is nonisotropic. Suppose $u(x) - x \neq 0$ is isotropic, put $(u(x),x) = \alpha$ then $0 = (u(x) - x, u(x) - x) = (u(x),u(x)) - (u(x),x) - {}$ $+ (x,u(x)) + (x,x) = 2(x,x) - \bar{\alpha} - \alpha$ (f is hermitian).

(*) $2(x,x) = \alpha + \bar{\alpha}$.

<u>Assume $\alpha \neq 0$</u>. If $\lambda \in U_1$ (i.e. $\lambda\bar{\lambda} = 1$) then

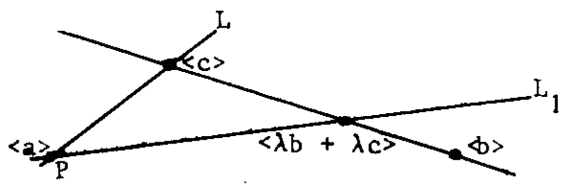
$$(u(x) - \lambda x, u(x) - \lambda x) = 2(x,x) - \lambda\bar{\alpha} - \bar{\lambda}\alpha = \bar{\alpha} + \alpha - \lambda\bar{\alpha} - \bar{\lambda}\alpha .$$

If $u(x) - \lambda x$ isotropic for all $\lambda \in U_1$ then $\bar{\alpha} + \alpha - \lambda\bar{\alpha} - \bar{\lambda}\alpha = 0$, $\forall\lambda \in U_1$. Hence $(\bar{\alpha} + \alpha)\lambda - \lambda^2\bar{\alpha} - \alpha = 0$, $\forall\lambda \in U_1$, a contradiction since $|U_1| \geq 3$.

So $u(x) - \lambda x$ is nonisotropic for some $\lambda \in U_1$.
Since $(\lambda x, \lambda x) = (x,x) = (u(x),u(x))$ it follows from 5.14 that there exists $\sigma \in U^+(V)$ s.t $\sigma(\lambda x) = u(x)$. Now $\sigma(\lambda x) - \lambda x = u(x) - \lambda x$ is nonisotropic, so (assuming the result for $u(x) - x$ nonisotropic) there exist a product of hyperbolic rotations v_1 s.t. $v_1\sigma(\lambda x) = \lambda x$, i.e. $v_1u(x) = \lambda x$. Similarly there exists $\tau \in U^+(V)$ s.t. $\tau(x) = \lambda x$. Also $\tau(x) - x = \lambda x - x = (\lambda - 1)x$ is nonisotropic for $\lambda \neq 1$. Hence there exists a product of hyperbolic rotations w such that $w\tau(x) = x$, i.e. $w(\lambda x) = x$. Therefore, with $v := wv_1$, a product of hyperbolic rotations, we have,

$$vu(x) = wv_1u(x) = w(\lambda x) = x .$$

Assume $\alpha = 0$. Now $2(x,x) = 0$ by $(*)$ so char $\mathbb{F} = 2$. There exist $\lambda,\mu \in \mathbb{F}^*$ such that $\lambda\bar{\lambda} + \mu\bar{\mu} = 1$ (since $\mathbb{F}_0 \neq GF(2)$ we can take $\sigma \in \mathbb{F}^*$ s.t $\sigma + \bar{\sigma} = 0$ and $\sigma + 1 \neq 0$. Put $\lambda = \frac{\sigma}{1+\sigma}$, $\mu = \frac{1}{1+\sigma}$). Put $y = \lambda x + \mu u(x)$ then $(y,y) = (x,x) = (u(x),u(x))$ and $(y,x) \neq 0$, $(y,u(x)) \neq 0$. Applying the case $\alpha \neq 0$ twice yields: $\exists v,w$ products of hyperbolic rotations such that $v(u(x)) = y$ and $w(y) = x$. Hence $wv(u(x)) = w(y) = x$.
We are reduced to the case in which $u(x) - x$ is nonisotropic.
Assume $u(x) - x$ is nonisotropic. Put $P = \langle u(x) - x\rangle$ and let L be a hyperbolic line through P. We have $V = L \perp L^\perp$, $x = y + z$, $u(x) = y' + z'$ with $y,y' \in L$ and $z,z' \in L^\perp$. Since $z - z' = x - u(x) + y' - y \in L^\perp \cap L = 0$ it follows that $z = z'$. Therefore $(x,x) = (u(x),u(x))$ implies $(y,y) = (y',y')$.
If y is nonisotropic then there exists $\sigma \in U^+(L)$ such that $\sigma(y') = y$. Put $v = \sigma \perp 1_{L^\perp}$ then v is a hyperbolic rotation and $vu(x) = v(y' + z') = v(y') + z' = y + z = x$. We are done in this case. Assume therefore that y is isotropic.
The proof consists in showing that we may choose a new hyperbolic line L_1 through P such that the projection y_1 of x on L_1 is nonisotropic.
We have $V = P \perp P^\perp$, $x = a + b$, $a \in P$, $b \in P^\perp$. Put $c = y - a \in L$.



1) $a \neq 0$ so $P = \langle a\rangle$. For suppose $a = 0$ then $x \in P^\perp$, so $0 = (x,u(x) - x) = (x,u(x)) - (x,x) = (x,u(x)) - (u(x),u(x)) = (x - u(x),u(x))$. Hence $(u(x) - x,u(x) - x) = 0$, which is a contradiction.
2) $(a,b) = (a,c) = 0$ (hence $\langle a\rangle \neq \langle c\rangle$). Clearly $a \in P$, $b \in P^\perp$ implies $(a,b) = 0$. From $P \subseteq L$ it follows $z \in L^\perp \subseteq P^\perp$, so $(a,x) = (a,y) + (a,z) = (a,y)$. Also $(a,x) = (a,a) + (a,b) = (a,a)$. Thus $(a,y-a) = 0$.

3) $(b,c) = (c,c) = -(a,a) \in \mathbb{F}_0^*$.
Since $y = a + c \in L$, and $a \in P \subseteq L$ it follows that $c \in L$. From $x = a + b = y + z =$ $= a + c + z$ we see that $b = c + z$. Hence $(b,c) = (c,c) + (z,c) = (c,c)$. Also $(c,c) = (y-a, y-a) = -(y,a) - (a,y) + (a,a) = -(a,a)$.

It will suffice to show that there exist λ and μ such that $L_1 = \langle a, \lambda b + \mu c\rangle$ is a hyperbolic line and the projection y_1 of x on L_1 is nonisotropic. Put $(b,b) = \alpha \in \mathbb{F}_0$, and $-(a,a) = \beta \in \mathbb{F}_0^*$ then

$$(a + \lambda b + \mu c,\ a + \lambda b + \mu c) = -\beta + \lambda\bar{\lambda}\alpha + (\bar{\lambda}\mu + \bar{\mu}\lambda)\beta + \mu\bar{\mu}\beta \ ,$$

so $a + \lambda b + \mu c$ is isotropic if and only if

$$(*) \qquad \lambda\bar{\lambda}\alpha + (\bar{\lambda}\mu + \bar{\mu}\lambda)\beta + \mu\bar{\mu}\beta = \beta \ .$$

Since $(a, a + \lambda b + \mu c) = (a,a) = -\beta \neq 0$ it follows that L_1 is a hyperbolic line. Write $x = y_1 + (x - y_1)$ with $y_1 \in L_1$ and $x - y_1 \in L^{\perp}$, so $(x - y_1, y_1) = 0$. We show that λ and μ exist such that $(*)$ holds and such that $(x - d, d) \neq 0$ for every isotropic point $\langle d\rangle$ on L_1. This guarantees that y_1 is nonisotropic. Assume $(*)$ holds, i.e. $a + \lambda b + \mu c$ is isotropic, then $d = a + \rho(\lambda b + \mu c)$ is isotropic iff $\rho\bar{\rho} = 1$. Now $(x - d, d) = (x,d) = (a + b,\ a + \rho(\lambda b + \mu c)) =$ $= -\beta + \rho(\lambda a + \mu\beta)$, so $(x - d, d) = 0$ implies $\beta = \rho(\lambda\alpha + \mu\beta)$ hence $\bar{\rho}(\bar{\lambda}\alpha + \bar{\mu}\beta) = \beta$, $\beta^2 = (\lambda\alpha + \mu\beta)(\bar{\lambda}\alpha + \bar{\mu}\beta)$ and so, using $(*)$, we obtain $(1 - \bar{\mu}\mu)(\alpha - \beta) = 0$. Suppose $\alpha = \beta$, i.e. $(b,b) = -(a,a)$, then $(x,x) = (a + b, a + b) = 0$, which is a contradiction. Therefore, if there exists an isotropic point $\langle d\rangle$ on L_1 such that $(x - d, d) = 0$ then $\mu\bar{\mu} = 1$.
We are now reduced to showing that there exist $\lambda, \mu \in \mathbb{F}$ satisfying $(*)$ and such that $\mu\bar{\mu} \neq 1$.
We show: There exist $\lambda, \mu \in \mathbb{F}$ satisfying $(*)$ and $\mu\bar{\mu} \neq 1$, $\lambda \neq 0$, $\lambda + \mu \neq 0$.
If we put $\gamma := (\beta - \alpha)/\beta$ and use the transformation

$$\xi = \frac{\lambda + \mu}{\mu} \ , \ \eta = \frac{1}{\lambda}$$

we see that this is equivalent to:
There exist $\xi, \eta \in \mathbb{F}$ such that $\xi\bar{\xi} - \eta\bar{\eta} = \gamma$, $\xi + \bar{\xi} \neq 1 + \gamma$, $\xi \neq 0$, $\eta \neq 0$. Since the trace: $\mathbb{F} \to \mathbb{F}_0$ is onto and $\mathbb{F}_0 \neq GF(2)$ there exists $\xi_1 \in \mathbb{F}$, $\xi_1 \neq 0, \gamma$ such that $\xi_1 + \bar{\xi}_1 = 1 + \gamma$. Put $\eta := \xi_1 - \gamma$ then $\eta \neq 0$ and $\xi_1\bar{\xi}_1 - \eta\bar{\eta} = \gamma$.
There exists $\xi \in \mathbb{F}^*$ such that $\xi\bar{\xi} = \xi_1\bar{\xi}_1$ but $\xi_1 + \bar{\xi}_1 \neq \xi + \bar{\xi}$. Hence $\xi\bar{\xi} - \eta\bar{\eta} =$ $= \xi_1\bar{\xi}_1 - \eta\bar{\eta} = \gamma$, $\xi + \bar{\xi} \neq \xi_1 + \bar{\xi}_1 = 1 + \gamma$, $\xi \neq 0$, $\eta \neq 0$. □

5.16. If $|\mathbb{F}_0| \neq 2$, $\nu \geq 1$, $n \geq 2$ then $U^+(V) = T(V)$.
Proof. Because $SL(2,\mathbb{F}_0)$ is generated by transvections it follows from 5.4 that $T(V)$ contains all hyperbolic rotations. Hence $T(V) = U^+(V)$ by 5.15. □

5.17. If $\nu \geq 1$, $n \geq 2$ then $T(V) = U^+(V)$ unless $\mathbb{F}_0 = GF(2)$ and $n = 3$.

In order to prove 5.17 we take, until further notice, $\mathbb{F}_0 = GF(2)$, $\mathbb{F} = \mathbb{F}(\theta)$, $\theta^2 + \theta + 1 = 0$. Let L be a hyperbolic line with points $\langle p\rangle$, $\langle q\rangle$, $\langle p+q\rangle$, $\langle p+\theta q\rangle$, $\langle p+\theta^2 q\rangle$ such that $(p,p) = (q,q) = (p+q,\, p+q) = 0$, $(p,q) = (q,p) = 1$, $(p+\theta q,\, p+\theta^2 q) = 0$.

5.18. a) $T(L)$ is 2-transitive on the 3 isotropic points of L ($T(L) = U^+(L) = SL(2,\mathbb{F}_0)$).

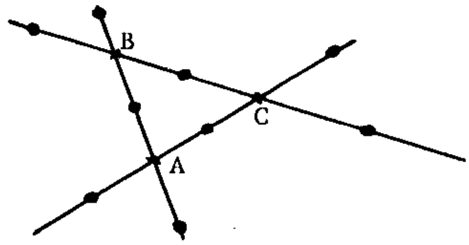
b) $T(L)$ is transitive on the 6 nonisotropic vectors of L.

Proof.

a) We know this already.

b) $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ \theta\end{pmatrix} = \begin{pmatrix}\theta\\ 1\end{pmatrix}$, $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\ \theta\end{pmatrix} = \begin{pmatrix}\theta^2\\ \theta\end{pmatrix}$, $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1\\ \theta\end{pmatrix} = \begin{pmatrix}1\\ \theta^2\end{pmatrix}$. □

Consider the case $n = 3$. The 12 nonisotropic points fall into 4 sets, each consisting of 3 pairwise orthogonal points A,B,C (given any nonisotropic point A, $A^\perp$ is a hyperbolic line containing two nonisotropic points $\neq A$ $B = \langle p+\theta q\rangle$ and $C = \langle p+\theta^2 q\rangle$ such that $B \perp C$).



Claim. These 4 sets are the orbits for $T(V)$ acting on the nonisotropic points.

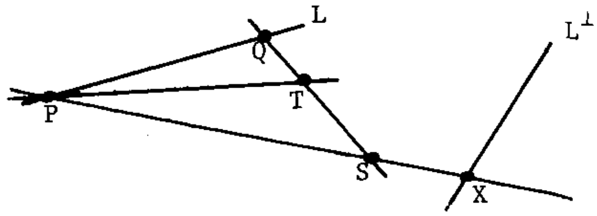
Proof. It suffices to show that every unitary transvection maps A to A,B or C. This is clear, for the 9 isotropic points of PV are the 9 isotropic points of $A+B$, $A+C$ and $B+C$. □

Now by 5.18 b) $T(V)$ is transitive on the 9 vectors representing the points of each triangle A,B,C. If v is a nonisotropic vector then $T(V)_v = T(V)_{\langle v\rangle^\perp}$ has order 6 ($\langle v\rangle^\perp$ is a hyperbolic line $T(V)_{\langle v\rangle^\perp} \simeq T(\langle v\rangle^\perp) \simeq SL(2,2)$). Hence $|T(V)| = 9.6 = 3^3.2$, but $|U^+(V)| = 2^3.3^3$ and therefore

5.19. If $n = 3$ then $U^+(V) : T(V) = 4$.

5.20. If $n = 4$, P an isotropic point then $T(V)_P$ is transitive on the hyperbolic lines through P.

Proof. There are 16 hyperbolic lines through P. Let L be one of these, and Q an isotropic point on L, $Q \neq P$. Furthermore we let X be an isotropic point



on the hyperbolic line $L^{\perp}$. Clearly $P + X$ is a totally isotropic line. Take a point $S \subseteq P + X$, $S \neq P,X$ then $S \not\leq Q$, so $Q + S$ is a hyperbolic line and the set of isotropic points on $Q + S$ is $\{Q,S,T\}$, say. Now Y_S fixes P and moves Q to T. Thus $T(V)_P$ moves L to $P + T$. We get 9 distinct images for L on taking the 3 possible choices for X and the 3 corresponding choices for S. Thus each orbit for $T(V)_P$ acting on the 16 hyperbolic lines through P contains at least 9 lines. Hence $T(V)_P$ is transitive on the hyperbolic lines through P. □

5.21. If $n = 4$ then $T(V)$ is transitive on the hyperbolic lines.

Proof. Let L be a hyperbolic line and P an isotropic point on L. Let M be another hyperbolic line. If $M \nsubseteq P^{\perp}$ then there exists a point $Q \subseteq M$, Q isotropic and $Q \nsubseteq P^{\perp}$, so $P + Q$ is a hyperbolic line. By 5.20, $T(V)$ moves L to $P + Q$ and $P + Q$ to M. If $M \subseteq P^{\perp}$ let R be any isotropic point on M. Suppose every hyperbolic line through Q is on $P^{\perp}$, then $V = Q^{\perp} \cup P^{\perp}$, which is not possible. Hence there exists a hyperbolic line N through Q, $N \nsubseteq P^{\perp}$. Now we can move L to N and N to M. □

5.22. If $n = 4$ then $T(V)$ is transitive on the nonisotropic vectors and the nonisotropic points.

Proof. Apply 5.18 b) and 5.21. □

5.23. If $n = 4$ then $T(V) = U^{+}(V)$.

Proof. $|U^{+}(V)| = 2^{6}.3^{4}.5$. Write $V = L \perp L^{\perp}$ with L a hyperbolic line. Then $T(V)_L \gtrsim T(L) \times T(L^{\perp})$ and so, by 5.18 a), 36 divides $|T(V)_L|$. Since $T(V):T(V)_L = \#$ hyperbolic lines $= \frac{45.16}{3} = 15.16$ we get $36.15.16 = 2^{6}.3^{3}.5$ divides $|T(V)|$. Now write $V = \langle v\rangle \perp \langle v\rangle^{\perp}$, v a nonisotropic vector. Clearly $T(V)_v \gtrsim T(\langle v\rangle^{\perp})$ and $|T(\langle v\rangle^{\perp})| = \frac{|U^{+}(\langle v\rangle^{\perp})|}{4} = 2.3^{3}$ by 5.19. Also, by 5.22, $T(V):T(V)_v = \#$ nonisotropic vectors $= 120 = 3.40$. Hence 3^{4} divides $|T(V)|$, and so $T(V) = U^{+}(V)$. □

5.24. If $n \geq 4$ then $T(V) = U^{+}(V)$.

Proof. Induction on n, $n = 4$ is O.K. by 5.23. Assume $n > 4$. Let x be a nonisotropic vector then $T(V)_x \gtrsim T(\langle x\rangle^{\perp}) \simeq U^{+}(\langle x\rangle^{\perp})$, (by induction hypothesis) hence $|U^{+}(n-1,2)|$ divides $|T(V)_x|$.

Define $\sigma(n)$ to be the number of nonisotropic vectors, $\sigma(n) = (2^{2n} - 1) - + (2^{n} - (-1)^{n}).(2^{n-1} - (-1)^{n-1}) = (2^{n} - (-1)^{n})2^{n-1}$. Since $T(V)$ is tra on the nonisotropic vectors, $\sigma(n).|U^{+}(n-1,2)|$ divides $|T(V)|$. Now

$$\sigma(n).|U^{+}(n-1,2)| = 2^{n-1}(2^{n} - (-1)^{n}).2^{\binom{n-1}{2}}\prod_{i=2}^{n-1}(2^{i} - (-1)^{i}) = 2^{\binom{n}{2}}\prod_{i=2}^{n}(2^{i} - (-1)^{i}) =$$

$= |U^+(V)|$.

Hence, $U^+(V) = T(V)$. □

We return to a general field $\mathbb{F}$.

We leave as an exercise the proof of

5.25. If $\nu = 1$ then $U^+(V)$ is 2-tra on the isotropic points. If $\nu \geq 2$ then $U^+(V)$ has rank 3 and is pri on the isotropic points.
In any case, if $\nu \geq 1$ then $U^+(V)$ is primitive on the isotropic points.

5.26. If $\nu \geq 1$ then $U^+(V)$ is perfect unless $(n, |\mathbb{F}_0|) = (2,2)$, $(2,3)$ or $(3,2)$.

Proof.

a) Case $|\mathbb{F}_0| > 3$. Let L be a hyperbolic line. We know $U^+(L) \simeq SL(L_0)$ is perfect, so $U^+(V)'$ contains all hyperbolic rotations. Hence $U^+(V)' = U^+(V)$.

b) Case $|\mathbb{F}_0| = 3$, $n \geq 3$. It suffices to prove the result for $n = 3$. Take a basis such that the matrix of our form, $E = \begin{pmatrix} 0 & 1 & \\ -1 & 0 & \\ & & \gamma \end{pmatrix}$, γ skew. Then

$S = \begin{pmatrix} a & & \\ & (\bar{a})^{-1} & \\ & & \bar{a}(a^{-1}) \end{pmatrix} \in U^+(V)$, $T = \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix} \in U^+(V)$, and $(S,T) =$

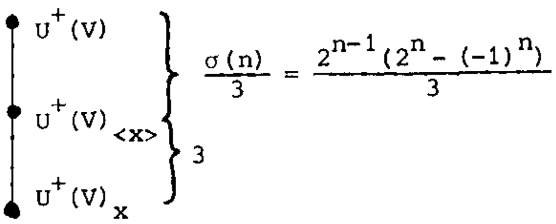
$= \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix} \in U^+(V)'$ if we take $a\bar{a} = -1$.

c) Case $|\mathbb{F}_0| = 2$, $n \geq 4$. It suffices to prove the result for $n = 4$. Take $\mathbb{F} = \mathbb{F}_0(\theta)$ where $\theta^2 + \theta + 1 = 0$. The same construction applies as in the symplectic case: The form has matrix $E = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ and $S = \begin{pmatrix} I & B \\ 0 & I \end{pmatrix} \in U^+(V)$ if B is 2×2 matrix, $B = B^* := (\bar{B})^t$, $T = \begin{pmatrix} A & 0 \\ 0 & (A^*)^{-1} \end{pmatrix} \in U^+(V)$ if $A \in GL(2,4)$. Now $(S,T) := \begin{pmatrix} I & ABA^*-B \\ 0 & I \end{pmatrix}$ represents a transvection if we take $A = \begin{pmatrix} 1 & \theta \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ because $ABA^* - B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. □

5.27. If $\nu \geq 1$ then $PU^+(V)$ is simple unless $(n, |\mathbb{F}_0|) = (2,2)$, $(2,3)$ or $(3,2)$.

Proof. Apply Iwasawa's lemma. □

If $n \geq 4$, $|\mathbb{F}_0| = 2$ then $U^+(V)$ has rank 3 on the nonisotropic points. We have for a nonisotropic point $\langle x \rangle$:



The orbits for $U^{+}(V)_{<x>}$ on the nonisotropic points are $\{<x>\}$, the nonisotropic points $P \perp <x>$ of length $k = \sigma(n-1)/3$, and the nonisotropic points $P \not\perp <x>$ of length $\ell = \frac{\sigma(n)}{3} - \frac{\sigma(n-1)}{3} - 1$. If P,Q are nonisotropic points, $P \perp Q$ then $\lambda = \#$ nonisotropic points $R \perp P, Q = \frac{\sigma(n-2)}{3}$.
If $n = 4$ we get a (strongly regularly) rank 3-graph on 40 vertices with $k = 12$, $\lambda = 2$. There are precisely two rank 3-graphs with these parameters, both having PSp(4,3) as an automorphism group. Hence

5.28. $U^{+}(4,2) = PU^{+}(4,2) \approx PSp(4,3)$.

We also have

5.29. $Sp(2n,q) \leq U^{+}(2n,q)$.

We conclude this section with another proof of Witt's theorem. Suppose that V is a vector space of dimension n with a symplectic, orthogonal or unitary geometry defined by a reflexive sesquilinear form f. In the case of an orthogonal geometry on V we suppose that $f(x,y) = Q(x+y) - Q(x) - Q(y)$ where Q is a quadratic form. In all cases we assume that f is nondegenerate.

5.30. Suppose that L is a nondegenerate two-dimensional subspace of V which contains an isotropic vector $u \neq 0$. Then $L = <u,v>$ where v is an isotropic vector such that $f(u,v) = 1$. If the geometry is orthogonal and $Q(u) = 0$, then v may be chosen so that $Q(v) = 0$.
Proof. We have $L = <u,w>$ for some w such that $\alpha = f(u,w) \neq 0$. For a symplectic geometry take $v = \alpha^{-1}w$. For an orthogonal geometry take $v = -Q(w)\alpha^{-2}u + \alpha^{-1}w$. For a unitary geometry we may suppose f is skew-hermitian, then if $\beta = f(w,w)$ we have $\beta + \bar{\beta} = 0$. Choose λ such that $\beta = \lambda - \bar{\lambda}$ and set $v = -\lambda\alpha^{-2}u + \alpha^{-1}w$. □

5.31. If $V = U \oplus W$ and $\sigma: U \to V$, $\tau: W \to V$ are isometries such that $\text{im}\,\sigma \cap \text{im}\,\tau = 0$ and $f(\sigma(u),\tau(w)) = f(u,w)$ for all $u \in U$, $w \in W$, then the map $\sigma \oplus \tau: V \to V: u + w \mapsto \sigma(u) + \tau(w)$ is also an isometry.
Proof. For an orthogonal geometry and $u \in U$, $w \in W$ we have $Q(\sigma(u) + \tau(w)) = Q(\sigma(u)) + Q(\tau(w)) + f(\sigma(u),\tau(w)) = Q(u) + Q(w) + f(u,w) = Q(u + w)$. A similar calculation establishes the lemma for the other types of geometry. □

5.32. (Witt's theorem). Let U be a subspace of V and suppose that $\sigma: U \to V$ is an isometry. Then σ has an extension to an isometry $\bar{\sigma}: V \to V$.

Proof. Let H be a hyperplane of U and let τ be the restriction of σ to H. By induction on dim U, τ has an extension $\bar{\tau}: V \to V$. We may suppose that $\bar{\tau}$ does not extend σ and replacing σ by $\bar{\tau}^{-1}\sigma$ we may suppose that σ is the identity on H; hence $P = \text{im}(\sigma - 1)$ has dimension 1. For $u,v \in U$ we have $f(\sigma(u),\sigma(v) - v) = f(u - \sigma(u),v)$ so that $H \subseteq P^{\perp}$ and $U \subseteq P^{\perp}$ if and only if $\sigma(U) \subseteq P^{\perp}$.
If $U \not\subseteq P^{\perp}$, then $U \cap P^{\perp} = \sigma(U) \cap P^{\perp} = H$. Let W be a complement to H in $P^{\perp}$. Then $V = W \oplus U$ and for $w \in W$, $u \in U$ we have $f(w,\sigma(u)) = f(w,u)$, hence by 5.31 $\bar{\sigma} = 1_W \oplus \sigma$ is an isometry.
Thus we may suppose that $U \subseteq P^{\perp}$ and $\sigma(U) \subseteq P^{\perp}$; hence $P \subseteq P^{\perp}$. If $U \neq \sigma(U)$, $u \in U - H$ and $v \in \sigma(U) - H$, then $Q = \langle u + v\rangle$ is a common complement to U and $\sigma(U)$ in $U + \sigma(U)$. Let W be a complement to $U + \sigma(U)$ in $P^{\perp}$ and set $S = W + Q$. Then $P^{\perp} = S \oplus U = S \oplus \sigma(U)$ and by 5.31, $1_S \oplus \sigma$ is an isometry of $P^{\perp}$. If $U = \sigma(U)$, let S be any complement to U in $P^{\perp}$, then again $1_S \oplus \sigma$ is an isometry of $P^{\perp}$. In both cases the extension of σ to $P^{\perp}$ has been constructed so that it acts as the identity on a hyperplane of $P^{\perp}$. Thus we may suppose that $U = P^{\perp} = \sigma(U)$.
Suppose that $P = \langle u\rangle$. If $u = \sigma(v) - v$ and if the geometry is orthogonal, then

$$Q(u) = Q(\sigma(v)) + Q(v) - f(\sigma(v),v) = 2Q(v) - f(v,v) = 0 .$$

Apply 5.30 to a two-dimensional subspace $L \not\subseteq U$ such that $P \subseteq L$. Then $L = \langle u,w\rangle$ where $f(u,w) = 1$ and w is isotropic (and $Q(w) = 0$ if the geometry is orthogonal). Consider the linear functional $V \to F$ which takes w to 0 and $v \in U$ to $f(\sigma^{-1}(v),w)$. Since f is nondegenerate there is a vector w' such that $f(\sigma^{-1}(v),w) = f(v,w')$ for all $v \in U$. Apply 5.30 to $\langle\sigma(u),w'\rangle$, noting that $w' \notin U$, to obtain an isotropic vector $\tau(w)$ (with $Q(\tau(w)) = 0$ if necessary) such that $f(\sigma(w),\tau(w)) = 1$, and $\langle\tau(w),u\rangle = \langle w',u\rangle$. Then $f(\sigma(v),\tau(w)) = f(\sigma(v),w') = f(v,w)$ so by 5.31, $\sigma \oplus \tau$ is an isometry of V which extends σ.
This completes the proof. □

6. Orthogonal groups, char $\mathbb{F} \neq 2$

Let V be a nondegenerate orthogonal space, char $\mathbb{F} \neq 2$. $Q(x) = \frac{1}{2}f(x,x)$ is a quadratic form on V, $f(x,y) = Q(x+y) - Q(x) - Q(y)$. Say Q is universal if $Q(x)$ takes all values in $\mathbb{F}$.

6.1. If f is nondegenerate and either

a) $\nu \geq 1$, or

b) $\mathbb{F}$ is finite and dim $V \geq 2$, then Q is universal.

Proof.

a) Let x be an isotropic vector $\neq 0$ in V. Then there exists a vector y such that $f(x,y) = 1$. For all $b \in \mathbb{F}$ we have

$$Q(bx + y) = b + Q(y) \ .$$

b) We may assume dim V = 2 and V has no isotropic vectors $\neq 0$. With respect to an orthogonal basis u,v of V, Q has the form

$$Q(xu + yv) = ax^2 + by^2 \ .$$

Thus we must show: If $a,b \in \mathbb{F}$ are such that $ab \neq 0$ and $ax^2 + by^2 \neq 0$, for all $x,y \in \mathbb{F}$ with $(x,y) \neq (0,0)$ then $ax^2 + by^2 = c$ is solvable for all $c \in \mathbb{F}$. We may assume that $a = 1$. Since $x^2 + by^2 \neq 0$, $\forall (x,y) \neq (0,0)$, $-b$ is not a square, and $\mathbb{F}^*(\sqrt{-b}) \to \mathbb{F}^*$, $x + \sqrt{-b}\, y \mapsto x^2 + by^2$ is the norm map, which we know is onto. □

$O(V,f) = O(v) = O(Q)$ denotes the group of isometries of V and is called the orthogonal group.

As char $\mathbb{F} \neq 2$, $O(V) = \{T \in GL(V) \mid Q(T(x)) = Q(x),\ \forall x \in V\}$. If E is the matrix of the form and A the matrix of a linear transformation T, then

$$T \in O(V) \Leftrightarrow AEA^t = E \ .$$

In particular elements of $O(V)$ have det $= \pm 1$. Thus we have the homomorphism det: $O(V) \to \{\pm 1\}$ with kernel $O^+(V) := \{T \in O(V) \mid \det T = 1\}$.

We shall see that $O(V) \neq O^+(V)$, hence $O(V) : O^+(V) = 2$ and the sequence

$$1 \to O^+(V) \to O(V) \xrightarrow{\det} \{\pm 1\} \to 1$$

is exact.

The elements of $O^+(V)$ are called rotations, $O^+(V)$ is called the rotation group. Clearly $O(V) \cap Z(V) = \{\pm 1\}$ and n is odd implies $-1 \in O^+(V)$, n is even implies $-1 \notin O^+(V)$. By looking at the actions on the points of PV we obtain exact sequences

$$1 \to \{\pm 1\} \to O(V) \to PO(V) \to 1 ,$$

$$1 \to \{\pm 1\} \to O^+(V) \to PO^+(V) \to 1, \text{ if } n \text{ is even} .$$

If n is odd then $O^+(V) \approx PO^+(V)$.

We want to find out which transformations $x \to x + \varphi(x)p$ are in $O(V)$. Let $\tau(x) = x + \varphi(x)p$, $P = \langle p\rangle$, $\varphi \neq 0$, $H = \ker \varphi$, $\varphi(p) \neq -1$. Then $\tau \in O(V)$ iff

$$\varphi(y)(x,p) + \varphi(x)(p,y) + \varphi(x)\varphi(y)(p,p) = 0 .$$

Assume $\tau \in O(V)$. If $(p,p) = 0$ then by taking $x = y$ we get $2\varphi(x)(x,p) = 0$ for all $x \in V$, $V = H \cup P^{\perp}$ which is impossible. So $(p,p) \neq 0$.

If $\varphi(p) = 0$ take $x = p$ then $\varphi(y)(p,p) = 0$ for all $y \in V$ so $V = H$ ⨳. So $\varphi(p) \neq 0$.

Assume $x \in H$, $\varphi(x) = 0$. Then $\varphi(y)(x,p) = 0$ for all $y \in V$, hence $(x,p) = 0$. Therefore $H = P^{\perp}$ and $\tau(x) = x + a(x,p)p$ for some $a \in \mathbb{F}$. By substitution we get

$$a(x,p)^2 + a(x,p)^2 + a^2(x,p)^2(p,p) = 0, \quad \text{for all } x \in V .$$

Hence $a = -2/(p,p)$ and $\tau(x) = x - \frac{2(x,p)}{(p,p)} p$. Such a transformation is called a <u>symmetry</u>. Note that a symmetry only depends on $P = \langle p\rangle$; we write $\tau = \tau_p = \tau_P$. The determinant of a symmetry equals -1 so $O(V) \neq O^+(V)$, hence $O(V) : O^+(V) = 2$. If $n = 2$, $\nu \geq 1$ (ν = the index) then $O^+(V) \approx \mathbb{F}^*$, $O(V) \simeq \mathbb{F}^*.\mathbb{Z}_2$.

<u>The theorem of Cartan-Dieudonné</u>

It is easy to prove that

6.2. $O(V)$ is generated by symmetries.

<u>Proof</u>. Take $S \in O(V)$, x a nonisotropic vector. Then $(x,x) = (S(x),S(x)) \neq 0$ so there exists a symmetry τ_w such that for $S' := \tau_w S$, $S'(x) = \pm x$ (as in the proof of 3.31). Then S' stabilizes the nondegenerate space $\langle x\rangle^{\perp}$ of dimension $n-1$. By induction on the dimension, $S'|\langle x\rangle^{\perp}$ is a product of symmetries of $\langle x\rangle^{\perp}$. But a symmetry of $\langle x\rangle^{\perp}$ is the restriction to $\langle x\rangle$ of a symmetry of V, so $S'|\langle x\rangle^{\perp} = \tau_{a_1}\cdots\tau_{a_m}|\langle x\rangle^{\perp}$, $a_1,\dots,a_m \in \langle x\rangle^{\perp}$. Then $S'' = S'\tau_{a_m}\cdots\tau_{a_1}$ is the identity on $\langle x\rangle^{\perp}$ and $S''(x) = S'(x) = \pm x$. If $S''(x) = x$ then $S'' = 1$ and if $S''(x) = -x$ then $S'' = \tau_x$. In either case S', and hence S, is a product of symmetries. □

6.3. $n \geq 3 \Rightarrow O(V)' = O^+(V)'$.

Proof.

a) $O(V)'$ is generated by the commutators $[\tau_a,\tau_b] = (\tau_a\tau_b)^2$. Namely, H := the subgroup generated by all $(\tau_a\tau_b)^2$, is a normal subgroup of $O(V)$ and $O(V)/H$ is generated by the cosets $H\tau_a$ and so is commutative. Hence $H \geq O(V)'$ so $H = O(V)'$.

b) Every $[\tau_a,\tau_b]$ is a product of commutators of rotations.
n odd. Now $-1 \in O(V) - O^+(V)$ so $-\tau_a \in O^+(V)$. Since $[\tau_a,\tau_b] = [-\tau_a,-\tau_b]$ we are done.
n even. So $n \geq 4$. Let $U = \langle a,b \rangle$. If $U^\perp$ is totally isotropic then $U^\perp \leq U^{\perp\perp} = U$. But $\dim U^\perp = n - \dim U \geq n-2 \geq 2$ and hence $U = U^\perp$. This is a contradiction since U contains nonisotropic vectors. Thus there exists a nonisotropic vector $w \in U^\perp$. Then τ_w commutes with τ_a and τ_b so $[\tau_a,\tau_b] = [\tau_a\tau_w,\tau_b\tau_w]$ a commutator of two rotations.

By a) and b) $O(V)' \leq O^+(V)'$ so $O(V)' = O^+(V)'$. □

An important improvement of 6.2 is

6.4. (Cartan-Dieudonné). If $\dim V = n$, then any orthogonal transformation $\eta \in O(V)$ is a product of at most n symmetries.

Proof. (Artin).

1) Suppose there is a nonisotropic vector u fixed by η. Then η fixes $\langle u \rangle^\perp$ and by induction on n, $\eta|\langle u \rangle^\perp$ is a product of $\leq n-1$ symmetries and therefore so is η.

2) Suppose there is a nonisotropic vector u such that $w := u - \eta u$ is nonisotropic. Then we have a symmetry τ_w such that $\eta' = \tau_w\eta$ fixes u. Hence η' is a product of $\leq n-1$ symmetries, so $\eta = \tau_w\eta'$ is a product of $\leq n$ symmetries.

3) Suppose $\dim V = 2$. If there are no isotropic vectors $\neq 0$, we are done by 1) and 2). Hence we may assume V is a hyperbolic line, $V = \langle u,v \rangle$, u,v a hyperbolic pair. There are two cases η: $u \mapsto au$, $v \mapsto a^{-1}v$ and η: $u \mapsto av$, $v \mapsto a^{-1}u$, $(a \in \mathbb{F})$. In the first case we may assume $a \neq 1$. Since $w = u+v$ and $w - \eta w = (1-a)u + (1-a^{-1})v$ are nonisotropic we are done by 2). In the second case $w = u + av$ is a nonisotropic vector fixed by η, so we are done by 1).

4) By 1), 2) and 3) we are reduced to the case in which $\dim V \geq 3$, the subspace V_1 of fixed vectors of η is totally isotropic and $u - \eta u$ is isotropic for nonisotropic vector u. We want to prove that $(1-\eta)V$ is totally isotropic. It suffices to show that every vector in $(1-\eta)V$ is isotropic.

Suppose w is a nonzero isotropic vector. Since dim V > 3 there exists a nonisotropic vector u orthogonal to w. Then $w \pm u$ are nonisotropic vectors orthogonal to w. We therefore have that $u - \eta u$, $w + u - \eta(w+u)$, $w - u - \eta(w-u)$ are isotropic. It follows that $w - \eta w$ is isotropic and hence that $(1-\eta)V$ is totally isotropic.

Now $V_1 \subseteq V_1^{\perp} \subseteq (1-\eta)V$ and $(1-\eta)V \subseteq ((1-\eta)V)^{\perp} \subseteq V_1$ so $V_1 = V_1^{\perp} = (1-\eta)V$.
Since $n = \dim V = \dim V_1 + \dim V_1^{\perp}$, n is even. And for $x \in V$, $(1-\eta)^2 x = 0$, i.e. $(1-\eta)^2 = 0$. It follows that η is a rotation.
Thus if τ_w is any symmetry, $\eta' = \tau_w \eta$ is improper and must be a product of $k \leq n$ symmetries with k odd.
Hence $k \leq n-1$, so $\eta = \tau_w \eta'$ is a product of $k+1 \leq n$ symmetries. □

Dieudonné's theorem 5.15 for the unitary group requires the existence of nonzero isotropic vectors. The fact that this condition is not inherited by nondegenerate subspaces (of dim ≥ 2) if the field $\mathbb{F}$ is infinite stands in the way of giving a proof of Dieudonné's theorem analogous to Artins proof of the Cartan-Dieudonné theorem. Such a proof can be given for the case of finite $\mathbb{F}$.

6.5. Every rotation has a nonzero fixed vector if n is odd and every improper rotation (i.e. element of $O(V) - O^+(V)$) has a nonzero fixed vector if n is even.

Proof.

a) The intersection of k hyperplanes has dimension $\geq n-k$.

b) For $S \in O(V)$ have $S = \tau_{a_1} \cdots \tau_{a_k}$ with $k \leq n$. Each τ_{a_i} has a hyperplane of fixed vectors so S has a subspace of fixed vectors of dimension $\geq n-k$.
$S \in O^+(V) \Leftrightarrow k$ even $\Rightarrow k < n$ if n odd.
$S \in O(V) - O^+(V) \Leftrightarrow k$ odd $\Rightarrow k < n$ if n even. □

Siegel transformations

Assume $n \geq 3$, $\nu \geq 1$.
Let x be a an isotropic vector, $P = \langle x \rangle$, $u \in P^{\perp}$. Define $\rho_{x,u}: P^{\perp} \to P^{\perp}$ by

$$\rho_{x,u}(z) = z + (z,u)x, \quad z \in P^{\perp} .$$

Then $\rho_{x,u}$ is an isometry of $P^{\perp}$.
Hence, by Witt's theorem, there exists an extension of $\rho_{x,u}$ to an isometry of V. We give a direct proof of the existence of this extension and at the same time prove uniqueness which is important later on. Fix a hyperbolic line L through P, let $Q = \langle y \rangle$ be an isotropic point on L, $(x,y) = 1$.
Now $V = L \perp L^{\perp} = P^{\perp} \oplus Q$, $P^{\perp} = P + L^{\perp}$. Write $u = cx + u'$ with $u' \in L^{\perp}$ then $\rho_{x,u}(z) = \rho_{x,u'}(z)$ because $(z,u) = (z,u')$ for all $z \in P^{\perp}$. So w.l.o.g. we may assume $u \in L^{\perp}$. Extend $\rho_{x,u}$ to a linear transformation of V by

$$\rho_{x,u}(y) = ax + by + v, \quad v \in L^{\perp} .$$

Now $\rho_{x,u} \in O^+(V)$ iff $Q(\rho_{x,u}(y)) = 0$ and $(\rho_{x,u}(y),\rho_{x,u}(z)) = (y,z)$ for all $z \in P^\perp$. This is equivalent to: $Q(\rho_{x,u}(y)) = 0$, $(\rho_{x,u}(y),\rho_{x,u}(x)) = 1$ and $(\rho_{x,u}(y),\rho_{x,u}(z)) = (y,z) = 0$ for all $z \in L^\perp$.
So $\rho_{x,u} \in O^+(V)$ iff $2ab + (v,v) = 0$, $b = 1$ and $(v,z) + b(z,u) = 0$ for all $z \in L^\perp$, i.e. iff $a = -\frac{1}{2}(v,v)$, $b = 1$, $u = -v$.
The unique extension of $\rho_{x,u}$ to an isometry of V is given by

$$\rho_{x,u}(z) = z + (z,u)x, \quad z \in P^\perp \text{ and}$$

$$\rho_{x,u}(y) = -\frac{(u,u)}{2}x + y - u, \quad u \in L^\perp.$$

These transformations are called the <u>Siegel transformations</u>, $\Omega = \Omega(V)$ denotes the subgroup of $O(V)$ generated by the Siegel transformations.
Let X := the set of all isotropic points of PV. For $P \in X$ define $H_P := \langle \rho_{x,u} \mid P = \langle x\rangle,\ u \in P^\perp\rangle$. For $z \in P^\perp$ and $T \in O(V)$,

$$\rho_{ax,u}(z) = z + (z,u)ax = z + (z,au)x = \rho_{x,au}(z),$$

$$\rho_{x,u_1}\rho_{x,u_2}(z) = \rho_{x,u_1}(z+(z,u_2)x) = z+(z,u_1)x+(z,u_2)x = \rho_{x,u_1+u_2}(z),$$

and

$$T\rho_{x,u}T^{-1}(z) = T(T^{-1}(z) + (T^{-1}z,u)x) = z + (z,Tu)T(x) = \rho_{T(x),T(u)}(z).$$

Because of the uniqueness of the extensions it follows that

$$\rho_{ax,u} = \rho_{x,au},\ \rho_{x,u_1}\rho_{x,u_2} = \rho_{x,u_1+u_2} \text{ and}$$

$$T\rho_{x,u}T^{-1} = \rho_{T(x),T(u)}, \quad T \in O(V).$$

From these equations and the fact that Ω is transitive on X (see 6.12) we have:

6.6. H_P is a normal abelian subgroup of Ω_P.

6.7. ${}^TH_P = H_{T(P)}$, for all $T \in O(V)$.

6.8. $\Omega = \langle {}^TH_P \mid T \in \Omega\rangle$.

Our main goal is to show that $\Omega = O(V)'$ and to apply Iwasawa's lemma to the action of Ω on the isotropic points to show that $\Omega/\Omega \cap \{\pm 1\}$ is a simple group. There are exceptions to both statements.

We assume $n \geq 3$, $\nu \geq 1$.
The set of isotropic points X is stable under the action of O(V) on the points. Moreover, if $\eta \in O(V)$ fixes every isotropic point, then η fixes every hyperbolic line pointwise, so η fixes every point. That is, the kernel of the action of O(V) on X is $\{\pm 1\}$ and PO(V) acts faithfully on X. In particular, therefore, we have a faithful action of $P\Omega \simeq \Omega/\Omega \cap \{\pm 1\}$ on X.
Concerning the action of Ω on X, the essential fact for our purposes is

6.9. $(\nu,n) \neq (2,4) \Rightarrow \Omega$ pri X.

This is a consequence of 6.14 below.
Let $\alpha := \{(P,Q) \in X^2 \mid P \perp Q,\ P \neq Q\}$.
$\beta := \{(P,Q) \in X^2 \mid P \not\perp Q\}$.

6.10. 1) $\nu = 1 \Rightarrow \alpha = 0$.
2) $\nu \geq 2$, $n \geq 5 \Rightarrow (X,\alpha)$ connected, diameter 2.
Proof.
1) definition.
2) $P,Q \in X$, $P \not\perp Q$. There exists a totally isotropic line L through P. Then $L \subseteq P^\perp$, $P^\perp \cap Q^\perp = (P+Q)^\perp \subseteq P^\perp$. Since $\dim L = 2$, $\dim(P^\perp \cap Q^\perp) = n-2$, $\dim P^\perp = n-1$, L and $(P^\perp \cap Q^\perp)$ intersect in an isotropic point R. ||

6.11. (X,β) connected, diameter 2.
Proof. Let $P = \langle x\rangle$, $Q = \langle y\rangle \in X$, $P \perp Q$.
There exists $\langle u\rangle \notin P^\perp \cup Q^\perp$. Can assume $(x,u) = (y,u) = 1$. Replace u by $z = u - ax$ to get $Q(z) = 0$.
Then $R = \langle z\rangle \notin P^\perp \cup Q^\perp$, $R \in X$. □

6.12. Ω tra X, $\beta \in X^2/\Omega$.
Proof.
i) First show H_P tra P_β for $P \in X$ (where $P_\beta := \{Q \in X \mid (P,Q) \in \beta\}$).
Let $P = \langle x\rangle$ and take $Q = \langle y\rangle$ and $R = \langle z\rangle$ in P_β. Assume as we may that $(x,y) = (x,z) = 1$. Have $V = P + Q + U$, $U = (P+Q)^\perp = \langle x,y\rangle^\perp$ so $z = ax + by + u$, $u \in U$. We see that $b = 1$, $a = -Q(u)$, so $z = y - Q(u)x + u$.
Hence $\rho_{x,-u}(y) = z$ as required.
ii) Next prove Ω tra X. Take $P = \langle x\rangle$, $Q = \langle y\rangle \in X$. Claim: there exists a $R \in X$, $R \not\perp P$, and $R \not\perp Q$. If $P \perp Q$ have this by (the proof of) 6.11. Assume $P \not\perp Q$. Then $L = P + Q$ is a hyperbolic line. Can assume $(x,y) = 1$. Let u be a non-

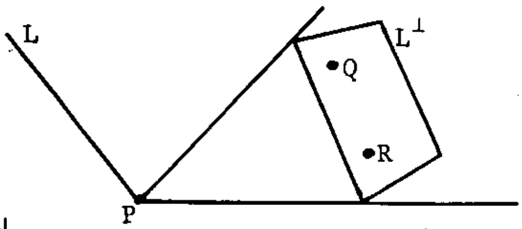
isotropic vector of $L^\perp$ and let $z = x - Q(u)y + u$. Then $Q(z) = 0$, $(z,x) = -Q(u) \neq 0$ and $(z,y) = 1$. Take $R = \langle z\rangle$. Now Ω_R moves P to Q by i).

iii) $\beta \in X^2/\Omega$ by i) and ii). ||

6.13. $\nu \geq 2,\ n \geq 5 \Rightarrow \alpha \in X^2/\Omega$.

Proof. Take $Q,R \in P\alpha \subseteq P^\perp - \{P\}$.

i) Assume $Q \not\perp R$. Then $Q + R \subseteq P^\perp$ so there exists a hyperbolic line L through P such that $Q,R \subseteq L^\perp$.
Then $\Omega(L^\perp)$ moves Q to R by 6.12. But $\Omega(L^\perp)$ is naturally in $\Omega(V)_P$. Hence $\Omega(V)_P$ moves Q to R.



ii) Assume $Q \perp R$. There exists $S \in P^\perp$ such that $S \not\perp Q$ and $S \not\perp R$: there exists $\langle u\rangle \subseteq P^\perp$ such that $\langle u\rangle \nsubseteq Q^\perp \cup R^\perp$, so $(u,x) = 0$ and can assume $(u,y) = (u,z) = 1$ (where $P = \langle x\rangle$, $Q = \langle y\rangle$ and $R = \langle z\rangle$).
Replace u by $s = u - ay$ to get $Q(s) = 0$. Take $S = \langle s\rangle$. Then Ω_P moves Q to S and S to R. □

By 6.10, 6.11, 6.12 and 6.13 we have

6.14. $\nu = 1 \Rightarrow \Omega$ 2-tra X.
$\nu \geq 2,\ n \geq 5 \Rightarrow \Omega$ pri rank 3 X.

Now we turn to the problems of identifying Ω as the commutator subgroup of $O(V)$ and proving that Ω is perfect.

6.15. $\Omega \geq O(V)'$.

Proof.

i) L hyperbolic line, u nonisotropic vector. There is $\rho \in \Omega$ such that $\rho(u) \in L$. Namely there is $u_1 \in L$ such that $Q(u_1) = Q(u)$ and then there exists $\eta \in O(V)$ such that $\eta(u_1) = u$. By 6.12, Ω is tra on the set of hyperbolic lines so there is $\rho \in \Omega$ such that $\rho\eta(L) = L$. Then $\rho(u) \in L$. Thus if τ_u is a symmetry, there is $\rho \in \Omega$ such that $\rho\tau_u\rho^{-1} = \tau_{u'}$, $u' \in L$.

ii) $O_L := \langle\tau_u \mid u \in L\rangle$.
$O(L)$ acts trivially on $L^\perp$. $\eta \mapsto \eta|L$ is an isomorphism of O_L onto $O(L)$. Define $O_L^+ :=$ the subgroup of O_L generated by products of pairs of symmetries with $u \in L$.

$O^+_L \cong O^+(L)$ abelian as L is hyperbolic line. If $\zeta \in O^+(V)$ then $\zeta = \tau_{u_1}\cdots\tau_{u_{2k}}$, u_i nonisotropic. By i) there is $\rho_i \in \Omega$ such that $u_i' = \rho u_i \in L$. Then $\zeta = \rho_1^{-1}\tau_{u_1'}\rho_1\cdots\rho_{2k}^{-1}\tau_{u_{2k}'}\rho_{2k} = \rho\tau_{u_1'}\cdots\tau_{u_{2k}'}$, $\rho \in \Omega$ as $\Omega \trianglelefteq O(V)$.

Hence $O^+(V) \leq \Omega O^+_L$. We know that $\Omega \leq O^+(V)$, hence $O^+(V) = \Omega O^+_L$.

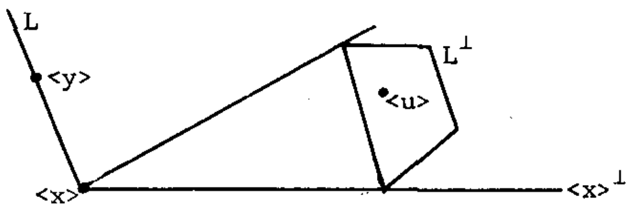
$\therefore O^+(V)/\Omega \simeq O^+_L/O^+_L \cap \Omega$ abelian.

$\therefore \Omega \geq O^+(V)'$.

$\therefore \Omega \geq O(V)'$ by 6.3. □

6.16. $\nu \geq 1$, $n \geq 3$, $(n,|\mathbb{F}|) \neq (3,3)$, $(\nu,n,|\mathbb{F}|) \neq (2,4,3)$ implies $\Omega = O(V)' = \Omega'$.

Proof. By 6.15 it suffices to prove that $\Omega = \Omega'$. Show $\rho_{x,u} \in \Omega'$ for all isotropic x and all $u \in \langle x\rangle^\perp$. Let $L = \langle x,y\rangle$ be a hyperbolic line through $\langle x\rangle$. We may assume that $u \in L^\perp$. Let O_L be as above, $O_L \simeq O(L)$.



For $a \in \mathbb{F}^*$ there exists $\eta_a \in O_L$ such that $\eta_a x = ax$, $\eta_a y = a^{-1}y$. Moreover, there exists $\tau \in O_L$ such that $\tau x = y$, $\tau y = x$. If $|\mathbb{F}| \geq 4$ we may take $a \in \mathbb{F}^*$ with $a^2 \neq 1$. Then for $\alpha = \eta_a^2$, $\beta = \rho_{x,(a^2-1)^{-1}u}$, $\alpha\beta\alpha^{-1}\beta^{-1} = \rho_{x,u}$.

Hence $\rho_{x,u} \in \Omega'$ since $\alpha \in \Omega$ (if a group G is generated by involutions then $g^2 \in G'$ for all $g \in G$, so $\alpha = \eta_a^2 \in O(V)' \leq \Omega$).

Assume $\mathbb{F} = GF(3)$, $n \geq 4$ and $\nu = 1$ if $n = 4$.

It suffices to assume that u is nonisotropic.

Claim: there exists a nonisotropic vector $v \in L^\perp \cap \langle u\rangle^\perp$ such that $Q(u) = Q(v)$.

Case i). $n = 4$, $\nu = 1$.

$L^\perp$ is 2-dimensional and has no isotropic vector $\neq 0$. $L^\perp = \langle u,v\rangle$, $(u,v) = 0$ and $Q(u) = Q(v)$ as $Q(u) = -Q(v)$ implies that $L^\perp$ is hyperbolic.

Case ii). $n \geq 5$.

$L^\perp \cap \langle u\rangle^\perp$ is a nondegenerate subspace of dim ≥ 2, so Q restricted to $L^\perp \cap \langle u\rangle^\perp$ is universal.

$\therefore Q(v) = Q(u)$ for some $v \in \langle u\rangle^\perp \cap L^\perp$.

This proves the claim.

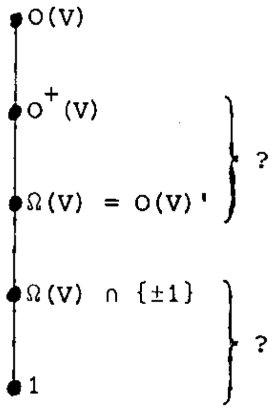
Now there exists $\tau \in O(V)$ such that $\tau(x) = x$, $\tau(u) = -v$, $\tau(v) = u$. So $\tau^2(x) = x$, $\tau^2(u) = -u$ and $\tau^2\rho_{x,u}\tau^{-2}\rho_{x,u} = \rho_{x,u}$.

$\therefore \rho_{x,u} \in \Omega'$. □

Now a direct application of Iwasawa's lemma gives

6.17. $\nu \geq 1$, $n \geq 3$, $(\nu,n) \neq (2,4)$, $(n,\mathbb{F}) \neq (3,GF(3))$ implies $\Omega/\Omega \cap \{\pm 1\}$ is simple.

In addition to the question of what is going on in the exceptional cases of 6.17 we are left with certain obvious questions about the structure of $O(V)$



Before going into these questions we take a look at orthogonal geometries over finite fields (char $\neq 2$).

<u>Orthogonal groups over finite fields (char $\neq 2$)</u>

We take $\mathbb{F} = GF(q)$, q odd. Then $\mathbb{F}^* = (\mathbb{F}^*)^2 \cup (\mathbb{F}^*)^2 g$, where g is a fixed nonsquare. Let V be a nondegenerate orthogonal space of dimension n over $\mathbb{F}$.

<u>Case $n = 1$</u>: $V = \langle x \rangle$, x nonisotropic, either $(x,x) = 1$ or $(x,x) = g$.

<u>Case $n = 2$</u>: $V = \langle x,y \rangle$, V is hyperbolic iff V is isotropic, i.e. iff $\nu = 1$; in this case we put $\varepsilon := +1$. V has no isotropic points iff $\nu = 0$; in this case we put $\varepsilon := -1$. A hyperbolic line has exactly 2 isotropic points. Indeed, if $(x,x) = (y,y) = 0$, $(x,y) = 1$ then $(ax + by, ax + by) = 2ab = 0$ iff $a = 0$ or $b = 0$. So the number of nonisotropic points equals $q - \varepsilon$ in both cases. Hence,

$\#$ nonisotropic vectors $= (q-\varepsilon)(q-1)$,

$\#$ isotropic nonzero vectors $= q^2 - 1 - (q-\varepsilon)(q-1) = (q-1)(\varepsilon+1) = q + \varepsilon q - 1 - \varepsilon$.

The symmetries in $O(V)$ are in 1-1 correspondence with the nonisotropic points. The symmetries constitute a coset of $O^+(V)$ in $O(V)$ different from $O^+(V)$. Therefore $|O^+(V)| = q - \varepsilon$.

We may assume that there exists an $x \in V$ such that $(x,x) = 1$. Then $V = \langle x \rangle \perp \langle x \rangle^{\perp}$, $V = \langle x,y \rangle$, $y \in \langle x \rangle^{\perp}$. We may take y such that $(y,y) = -1$ or $-g$. Now $(ax + by, ax + by) = a^2 - b^2$ or $a^2 - gb^2$, so V is hyperbolic if $(y,y) = -1$, nonisotropic if $(y,y) = -g$. The matrices of the forms are $\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & \\ & -g \end{pmatrix}$ respectively; the quadratic forms are $x^2 - y^2$ if $\varepsilon = +1$ and $x^2 - gy^2$ if $\varepsilon = -1$.

Case $n \geq 3$: If $n = 3$ (i.e. if $n \geq 3$) then V contains an isotropic nonzero vector. Indeed, take $x \in V$ such that $(x,x) = 1$, there exists a $y \in \langle x\rangle^{\perp}$, such that $(y,y) = -1$ by 6.1. Now $x + y$ is isotropic.
By 3.34 we have $V = H_{2r} \perp W$, where H_{2r} is an orthogonal direct sum of r hyperbolic lines, and W is a nondegenerate space of index 0. We have the following possibilities for W:
W is a nondegenerate point, $W = \langle x\rangle$, $(x,x) = 1$ or $(x,x) = g$.
W is a nonisotropic line $W = \langle x,y\rangle$, $(x,x) = 1$, $(x,y) = 0$, $(y,y) = -g$.
$W = 0$.
Thus there are four types of geometries:

$$n \text{ odd} \begin{cases} \text{I} & V = L_1 \perp \ldots \perp L_{\frac{1}{2}(n-1)} \perp \langle x\rangle,\ \langle x,x\rangle = 1 \\ \text{II} & V = L_1 \perp \ldots \perp L_{\frac{1}{2}(n-1)} \perp \langle x\rangle,\ \langle x,x\rangle = g \end{cases}$$

$$n \text{ even} \begin{cases} \text{III} & V = L_1 \perp \ldots \perp L_{\frac{1}{2}n-1} \perp W,\ W \text{ a nonisotropic line},\ \nu = \frac{n-2}{2} \\ \text{IV} & V = L_1 \perp \ldots \perp L_{\frac{1}{2}n},\ \nu = \frac{n}{2}. \end{cases}$$

There is no essential difference between I and II, that is, they have the same group of isometries. For type III we define $\varepsilon := -1$, for type IV we put $\varepsilon := +1$.

Assume $n \geq 3$. Let V be a nondegenerate orthogonal space of dimension n. Let $\varphi(n)$ denote the number of isotropic nonzero vectors.
Let P be an isotropic point, L a hyperbolic line through P, then $L^{\perp}$ is a nondegenerate space of dimension $n-2$.

$$\#\ \text{isotropic points} = \frac{\varphi(n)}{q-1} = 1 + \frac{\varphi(n-2)}{q-1}q + q^{n-2}$$

$$\therefore\ \varphi(n) = q\varphi(n-2) + q^{n-2}(q-1) + q - 1 =$$

$$= q\varphi(n-2) + q^{n-1} - q^{n-2} + q - 1.$$

$$\therefore\ \varphi(n) - q^{n-1} + 1 = q(\varphi(n-2) - q^{n-3} + 1)$$

$$\therefore\ q^{-n/2}(\varphi(n) - q^{n-1} + 1) = q^{-(n-2)/2}(\varphi(n-2) - q^{n-3} + 1).$$

Hence $q^{-n/2}(\varphi(n) - q^{n-1} + 1) =: c$ only depends on the parity of n.

$$\therefore\ \varphi(n) = cq^{n/2} + q^{n-1} - 1.$$

Types I and II: $\varphi(1) = 0$ implies $c = 0$, so $\varphi(n) = q^{n-1} - 1$.
Types III and IV: $\varphi(2) = q + \varepsilon q - 1 - \varepsilon$ implies $c = \varepsilon - \frac{\varepsilon}{q}$, so

$$\varphi(n) = q^{n/2}(\varepsilon - \frac{\varepsilon}{q}) + q^{n-1} - 1 = (q^{n/2} - \varepsilon)(q^{n/2-1} + \varepsilon).$$

Every hyperbolic line contains exactly 2 isotropic points. Hence, $\lambda(n)$, the number of hyperbolic pairs of vectors, equals $q^{n-2}\varphi(n)$. Put $\Phi(n) = |O^+(V)|$ and let $L = \langle x,y \rangle$ be a hyperbolic line, x,y a hyperbolic pair of vectors. Since $O^+(V)$ is transitive on the hyperbolic pairs of vectors, $\Phi(n) = \lambda(n)|O^+(V)_{x,y}|$. Since $O^+(V)_{x,y}$ fixes every vector on L, $O^+(V)_{x,y} \simeq O^+(L^\perp)$. Hence $|O^+(V)| = \lambda(n)|O^+(L^\perp)|$, so $\Phi(n) = \lambda(n)\Phi(n-2)$.

Case n odd: $\Phi(1) = 1$, $\Phi(n) = \lambda(n)\lambda(n-2)\ldots\lambda(3) = q^{(n-2)+(n-4)+\ldots}(q^{n-1}-1)$ $(q^{n-3}-3)\ldots(q^2-1)$

$$\Phi(n) = q^{\frac{(n-1)^2}{4}} \prod_{i=1}^{\frac{n-1}{2}} (q^{2i}-1) .$$

Case n even: $O(V) = O^+(V) + (O(V) - O^+(V))$, so for $n = 2$, $\Phi(2) = |O^+(V)| = |O(V) - O^+(V)| = \#\,\text{symmetries} = \#$ nonisotropic points $= q - \varepsilon$.

$$\begin{aligned}\Phi(n) &= \lambda(n)\lambda(n-2)\ldots\lambda(4)(q-\varepsilon)\\ &= q^{(n-2)+(n-4)+\ldots+2} \prod_{i=2}^{\frac{n}{2}} (q^i-\varepsilon)(q^{i-1}+\varepsilon)(q-\varepsilon)\\ &= q^{\frac{n(n-2)}{4}} q^{\frac{n}{2}}-\varepsilon \prod_{i=1}^{\frac{n-2}{2}} (q^{2i}-1)\end{aligned}$$

$$|O^+(V)| = \begin{cases} q^{\frac{(n-1)^2}{4}} \prod_{i=1}^{\frac{n-1}{2}} (q^{2i}-1) & \text{if n is odd}\\ q^{\frac{n(n-2)}{4}} (q^{\frac{n}{2}}-\varepsilon) \prod_{i=1}^{\frac{n-2}{2}} (q^{2i}-1) & \text{if n is even .}\end{cases}$$

The spinorial norm

Let V be a nondegenerate orthogonal space char $\neq 2$. For $\sigma \in O(V)$, $\sigma = \tau_{a_1}\ldots\tau_{a_k}$ define $\theta(\sigma) := (a_1,a_1)(a_2,a_2)\ldots(a_k,a_k)\mathbb{F}^{*2} \in \mathbb{F}^*/\mathbb{F}^{*2}$.

6.18. $\theta(\sigma)$ is independent of the representation of σ as a product of symmetries (proof later).

It is immediate that $\theta\colon O(V) \to \mathbb{F}^*/\mathbb{F}^{*2}$ is a homomorphism of groups.

Definition. $\Omega(V) := O(V)'$.

For $n \geq 3$, $\nu \geq 1$ this is consistent with our previous definition (except for $(n,|\mathbb{F}|) = (3,3)$, $(\nu,n,|\mathbb{F}|) = (2,4,3)$). As im θ is Abelian, $\Omega(V) \leq \ker\theta$. Call $\theta\colon O^+(V) \to \mathbb{F}^*/\mathbb{F}^{*2}$ the spinorial norm and $O'(V) := \ker\theta|O^+(V)$ the spinorial kernel. We have $\Omega(V) \leq O'(V)$. The ideal situation is: $\Omega(V) = O'(V)$ and $1 \to \Omega(V) \to O^+(V) \overset{\theta}{\to} \mathbb{F}^*/\mathbb{F}^{*2} \to 1$ is exact.

6.19. $\sigma = \tau_a\tau_b \in O'(V)$ implies $\sigma \in \Omega(V)$.

Proof. $\theta(\sigma) = (a,a)(b,b)\mathbb{F}^{*2} = 1$ so $(a,a)(b,b) = \alpha^2$, $\alpha \in \mathbb{F}^*$. Let $b_1 := \frac{(a,a)}{\alpha} b$ then $\tau_{b_1} = \tau_b$ and $(b_1,b_1) = (a,a)$ so, by Witt's theorem, there exists a $\lambda \in O(V)$ such that $\lambda(a) = b_1$. Then $\lambda\tau_a\lambda^{-1} = \tau_{b_1}$. Let $f : O(V) \to O(V)/\Omega(V)$ be the natural map then $f(\sigma) = f(\tau_a\tau_b) = f(\tau_a\tau_{b_1}) =$
$= f(\tau_a\lambda\tau_a\lambda^{-1}) = 1$, so $\sigma \in \Omega(V)$. □

6.20. If $n = 2$ or 3 then $O'(V) = \Omega(V)$.

Proof. Cartan-Dieudonné.

6.21. If $\nu \geq 1$ then $O'(V) = \Omega(V)$.

Proof. Let $L = \langle x,y\rangle$ be a hyperbolic line, x,y a hyperbolic pair of vectors.

(1) $O'(L) = \Omega(L)$ by 6.20.

(2) If $a \in V$ then there exists a $b \in L$ such that $(a,a) = (b,b)$
$((\alpha x + \beta y, \alpha x + \beta y) = 2\alpha\beta)$.
Let $\sigma = \tau_{a_1} \ldots \tau_{a_k} \in O'(V)$. Choose $b_1,\ldots,b_k \in L$ such that $(a_i,a_i) = (b_i,b_i)$, $i = 1,\ldots,k$. Put $\sigma_1 = \tau_{b_1} \ldots \tau_{b_k}$ then $\theta(\sigma) = \theta(\sigma_1) = 1$. Let $f : O(V) \to O(V)/\Omega(V)$ be the natural map then $f(\sigma) = f(\sigma_1)$ (there is a $\lambda_i \in O(V)$ such that $\lambda_i(a_i) = b_i$, etc.). Each τ_{b_i} fixes every vector in $L^\perp$ so $\sigma_1 = \sigma_2 \perp 1_{L^\perp}$ and by 6.19, $\sigma_2 \in \Omega(L)$ since $\theta(\sigma_2) = \theta(\sigma_1) = 1$. Therefore $\sigma_1 \in \Omega(V)$ so $f(\sigma) = f(\sigma_1) = 1$, $\therefore \sigma \in \Omega(V)$. □

6.22. If $\nu \geq 1$ then $1 \to \Omega(V) \to O^+(V) \overset{\theta}{\to} \mathbb{F}^*/\mathbb{F}^{*2} \to 1$ is exact.

Proof. Since $\nu \geq 1$, $(\ ,\ )$ takes all values in $\mathbb{F}^*$. □

6.23. $-1 \in O'(V)$ iff n is even and the discriminant is a square.

Proof. If n is odd then $-1 \notin O^+(V)$ so $-1 \notin O'(V)$. Suppose n is even. Let $a_1,a_2,\ldots,a_n$ be an orthogonal basis of V. Then $-1 = \tau_{a_1}\tau_{a_2},\ldots,\tau_{a_n}$ so $\theta(-1) = \text{discr } V$. □

Let $\mathbb{F} = GF(q)$, q odd. Now $\mathbb{F}^* : \mathbb{F}^{*2} = 2$ so $O^+(V) : \Omega(V) = 2$ (the case $n = 2$, $\nu = 0$ is included), $\therefore |\Omega(V)| = \frac{1}{2}|O^+(V)|$. $|P\Omega(V)| = \frac{1}{2}|O^+(V)|$ if $-1 \notin \Omega(V)$, $|P\Omega(V)| = \frac{1}{4}|O^+(V)|$ if $-1 \in \Omega(V)$.
By 6.23, $-1 \in \Omega(V)$ iff n even and discr $V \in \mathbb{F}^{*2}$. If n is even, discr $V = (-1)^{n/2}$ or $(-1)^{n/2}g$, g a nonsquare according as $\varepsilon = 1$ or $\varepsilon = -1$. Hence discr V is a square iff $4 | q^{n/2} - \varepsilon$

$$|P\Omega(V)| = \begin{cases} \frac{1}{2} q^{\frac{1}{4}(n-1)^2} \prod_{i=1}^{\frac{n-1}{2}} (q^{2i} - 1) & \text{if } n \text{ odd}. \\ \\ \frac{1}{d} q^{\frac{1}{4}n(n-2)} (q^{\frac{n}{2}} - \varepsilon) \prod_{i=1}^{\frac{n-2}{2}} (q^{2i} - 1), \quad d = (4, q^{\frac{n}{2}} - \varepsilon) & \text{if } n \text{ even}. \end{cases}$$

Clifford Algebra

Let V be an orthogonal space, char $\neq 2$. We want to construct an algebra generated by V such that $xy + yx = 2(x,y)$. $T(V)$ denotes the tensor algebra on V, $\mathcal{A}$ denotes the 2-sided ideal in $T(V)$ generated by the elements $x \otimes y + y \otimes x - 2(x,y)$, $x,y \in V$. $C(V) := T(V)/\mathcal{A}$ is the Clifford Algebra and we have a linear map $V \to C(V)$, defined by $x \mapsto \mathcal{A} + x$. Let $a_1, a_2, \ldots, a_n$ be an orthogonal basis of V. Put $e_i := \mathcal{A} + a_i$ and for all $H \subseteq \{1,2,\ldots,n\}$ put $e_H := e_{i_1} e_{i_2} \ldots e_{i_p}$, where $\{i_1, i_2, \ldots, i_p\} = H$, $i_1 < i_2 < \ldots < i_p$, $e_\emptyset := 1$. Then $\{e_H | H \subseteq \{1,2,\ldots,n\}$ is a basis for $C(V)$ so $\dim C(V) = 2^n$.
$e_A e_B = \gamma_{A,B}\, e_{A \dotplus B}$, $\gamma_{A,B} = (-1)^{\rho(A,B)} \prod_{i \in A \cap B} (a_i, a_i)$ with $\rho(A,B) = \#$ of inversions in the sequence obtained by juxtaposing A and B. Identify V with its image in $C(V)$ (so a_i is identified with e_i).
Evidently V generates $C(V)$.
For $x,y \in V$ $xy + yx = 2(x,y)$, $xy = -yx$ if $x \perp y$, $x^2 = (x,x)$.
$C^+(V) := \Sigma \mathbb{F} e_H$ with $|H| \equiv 0 \pmod 2$
$C^-(V) := \Sigma \mathbb{F} e_H$ with $|H| \equiv 1 \pmod 2$
$C(V) = C^+(V) \oplus C^-(V)$, $\dim C^+(V) = \dim C^-(V) = 2^{n-1}$ and $+.+ \subseteq +$, $+.- \subseteq -$ etc.
$C^+(V)$ is a subalgebra of $C(V)$.
We have an anti-automorphism γ of $T(V)$ such that $\gamma : x_1 \otimes \ldots \otimes x_p \mapsto x_p \otimes \ldots \otimes x_1$ and $\gamma(\mathcal{A}) \leq \mathcal{A}$. Hence γ induces an anti-automorphism J of $C(V)$ such that $J : x_1 \ldots x_p \mapsto x_p \ldots x_1$, $x_i \in V$. J stabilizes $C^+(V)$ and $C^-(V)$. Define $N(\alpha) = \alpha\alpha^J$ for $\alpha \in C(V)$.

Example. V nondegenerate, $n = 3$, a_1, a_2, a_3 an orthogonal basis of V.
$C^+(V)$ is generated by 1, $i_1 = a_2a_3$, $i_2 = a_3a_1$, $i_3 = a_1a_2$.

$$i_1i_2 = -i_2i_1 = -(a_3,a_3)i_3 \ , \quad i_1^2 = -(a_2,a_2)(a_3,a_3) \ ,$$
$$i_2i_3 = -i_3i_2 = -(a_1,a_1)i_1 \ , \quad i_2^2 = -(a_1,a_1)(a_3,a_3) \ ,$$
$$i_3i_1 = -i_1i_3 = -(a_2,a_2)i_2 \ , \quad i_3^2 = -(a_1,a_1)(a_2,a_2) \ .$$

$C^+(V)$ is a generalized quaternion algebra.

$N(x_0 + x_1i_1 + x_2i_2 + x_3i_3) =$
$= (x_0 + x_1i_1 + x_2i_2 + x_3i_3)(x_0 - x_1i_1 - x_2i_2 - x_3i_3) =$
$= x_0^2 + (a_2,a_2)(a_3,a_3)x_1^2 + (a_1,a_1)(a_3,a_3)x_2^2 + (a_1,a_1)(a_2,a_2)x_3^2$.

Suppose $\nu \geq 1$, x,y a hyperbolic pair of vectors, $a_1 = x + \frac{1}{2}y$, $a_2 = x - \frac{1}{2}y$, a_3 a nonisotropic vector $\perp a_1,a_2$. Then $(a_1,a_1) = (a_2,a_2) = 1$, $(a_3,a_3) = a \in \mathbb{F}^*$. We have in this case a faithful representation of $C^+(V)$ in $\mathbb{F}_2$, the algebra of the 2×2 matrices over $\mathbb{F}$.

$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i_1 \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$, $i_2 \mapsto \begin{pmatrix} 0 & a \\ -1 & 0 \end{pmatrix}$, $i_3 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. These matrices span $\mathbb{F}_2$ so $C^+(V) \simeq \mathbb{F}_2$. The group of units of $C^+(V)$ is $GL(2,\mathbb{F})$.

For $S \subseteq \{1,\dots,n\}$ we have $e_S^2 = (-1)^* \prod_{i \in S} (a_i,a_i)$. Hence e_S is a unit and e_S^{-1} is a scalar multiple of e_S. If $S,T \subseteq \{1,\dots,n\}$ then $e_Se_T = (-1)^{|S||T|-|S\cap T|}e_Te_S$ so $e_Te_Se_T^{-1} = (-1)^{|S||T|-|S\cap T|}e_S$.
Define $C_0(V)$:= centralizer of $C^+(V)$, $C_0(V)$ is spanned by the $e_S \in C_0(V)$.
Let $S \subseteq \{1,2,\dots,n\}$ then $e_S \in C_0(V)$ iff $e_Te_Se_T^{-1} = e_S$ for all $T \subseteq \{1,\dots,n\}$, $|T| \equiv 0 \pmod 2$, i.e. iff $|S||T| - |S \cap T| \equiv 0 \pmod 2$ for all T, $|T| \equiv 0 \pmod 2$. Hence, $S = \emptyset$ or $S = \Omega$, $C_0(V) = \mathbb{F} \oplus \mathbb{F}e_\Omega$.
The center of $C^+(V)$ is $\mathbb{F}$ if n is odd, $C_0(V)$ if n is even. The center of $C(V) \subseteq$ center of $C^+(V)$, and $e_\Omega \in$ center of $C(V)$ iff $e_ie_\Omega e_i^{-1} = e_\Omega$ for all i, i.e. iff $|\Omega| - |\Omega \cap \{i\}| \equiv 0 \pmod 2$, i.e. iff $n - 1 \equiv 0 \pmod 2$.
Therefore, center of $C(V) = \mathbb{F}$ if n even, center of $C(V) = C_0(V)$ if n odd.
Centralizer of $C(V)$ in $C^+(V)$ = center of $C(V) \cap C^+(V) = \mathbb{F}$.
We say that $\alpha,\beta \in C(V)$ anticommute if $\alpha\beta = -\beta\alpha$. We determine the elements which anticommute with all elements of V. $e_ie_Se_i^{-1} = e_S$, for all i $\Leftrightarrow$ $|S| - |S \cap \{i\}| \equiv 1 \pmod 2$, for all i $\Leftrightarrow S = \Omega$, $n \equiv 0 \pmod 2$. If n is odd no element anticommutes with all elements of V, if n is even $\mathbb{F}e_\Omega$ anticommutes with all elements of V.

Define $R(V) :=$ all units $\alpha \in C(V)$ such that $\alpha^{-1}x\alpha \in V$, for all $x \in V$, and $R_0(V) :=$ all products of nonisotropic vectors (regular elements). Then $R_0(V) \leq R(V)$ (Suppose a is a nonisotropic vector then $a^{-1} = \frac{a}{(a,a)}$ and $ax = 2(a,x) - xa$ for all $x \in V$, hence $axa^{-1} = \frac{2(a,x)}{(a,a)} a - x = -\tau_a(x))$. For each $\alpha \in R(V)$ we define $S_\alpha : V \to V$, $x \mapsto \alpha x \alpha^{-1}$. Since $xy + yx = 2(x,y)$ for all $x,y \in V$ it follows that $2(x,y) = S_\alpha(xy+yx) = S_\alpha(x)S_\alpha(y) + S_\alpha(y)S_\alpha(x) = 2(S_\alpha(x), S_\alpha(y))$ for all $x,y \in V$, so $S_\alpha \in O(V)$. If a is a nonisotropic vector, $S_a = -\tau_a$.

We have an exact sequence

$$1 \to \begin{Bmatrix} \mathbb{F}^* & (n \text{ even}) \\ C_0^*(V) & (n \text{ odd}) \end{Bmatrix} \to R(V) \overset{S}{\to} O(V)$$

where $C_0^*(V)$ is the group of units of $C_0(V)$ and $S : R(V) \to O(V)$, $\alpha \mapsto S_\alpha$. Let $D(V) := R(V) \cap C^+(V)$ then we have an exact sequence

$$1 \to \mathbb{F}^* \to D(V) \overset{S}{\to} O^+(V) \to 1$$

in all cases.

Proof. Let $\sigma \in O(V)$, $\sigma = \tau_{a_1}\tau_{a_2} \cdots \tau_{a_k}$. Put $\alpha = a_1 \ldots a_k \in R_0(V)$ then $S_\alpha = (-1)^k\sigma$. Note that $S(D(V)) \supseteq O^+(V)$.

Case n even: Now im $S = O(V)$ for -1 is a rotation, so, if σ is improper, S_α is improper.

We have an exact sequence

$$1 \to \mathbb{F}^* \to R(V) \overset{S}{\to} O(V) \to 1 .$$

Claim $R(V) = R_0(V)$: Take $\beta \in R(V)$, let $\sigma = S_\beta$, then $\sigma = S_\alpha$ for some $\alpha \in R_0(V)$. Therefore $\beta \in \mathbb{F}^*\alpha$ so $\beta \in R_0(V)$. Hence, $D(V) =$ all products of an even number of nonisotropic vectors, $S(D(V)) = O^+(V)$ so

$$1 \to \mathbb{F}^* \to D(V) \overset{S}{\to} O^+(V) \to 1$$

is exact.

Case n odd: Now im $S = O^+(V)$. Suppose im $S = O(V)$ then $-1 = S_\alpha$ for some $\alpha \in R(V)$, i.e. $S_\alpha(x) = -x$, $\forall_{x \in V}$. Hence $\alpha x \alpha^{-1} = -x$, for all $x \in V$, which is impossible if n odd. We have

$$1 \to C_0^*(V) \to R(V) \overset{S}{\to} O^+(V) \to 1 \text{ , exact}$$

$$1 \to \mathbb{F}^* \to D(V) \overset{S}{\to} O^+(V) \to 1 \quad \text{, exact.}$$

The same argument as before gives:

D(V) = all products of an even number of nonisotropic vectors. □

Let $\alpha \in D(V)$, $\alpha = a_1 \dots a_k$ then $N(\alpha) = \alpha\alpha^J = a_1 \dots a_k a_k \dots a_1 = (a_1,a_1)\dots(a_k,a_k)$ so $\theta(S_\alpha) = N(\alpha)\mathbb{F}^{*2}$. Put $D_2(V) = \{\alpha \in D(V) \mid N(\alpha) \in \mathbb{F}^{*2}\}$ then,

$$1 \to \mathbb{F}^* \to D_2(V) \overset{S}{\to} O'(V) \to 1$$

is exact. Put $D_0(V) = \{\alpha \in D(V) \mid N(\alpha) = 1\}$ then,

$$1 \to \{\pm 1\} \to D_0(V) \overset{S}{\to} O'(V) \to 1$$

is exact.

Applications.

6.24. Spinorial norm. $\theta : O(V) \to \mathbb{F}^*/\mathbb{F}^{*2}$ is well-defined.

Proof. If $\tau_{a_1} \dots \tau_{a_k} = 1$ then $(a_1,a_1)\dots(a_k,a_k) \in \mathbb{F}^{*2}$ for k even, so $\alpha = a_1 \dots a_k \in D(V)$, $N(\alpha) = (a_1,a_1)\dots(a_k,a_k)$. Since $1 = \tau_{a_1}\dots\tau_{a_k} = S_\alpha$, $\alpha \in \ker S = \mathbb{F}^*$ so $N(\alpha) = \alpha^2$. □

6.25. Generic isomorphisms

n=3. We determine the fixed elements of J : $e_S = e_S^J = (-1)^{\binom{|S|}{2}} e_S$ iff $\binom{|S|}{2}$ even, i.e. iff $|S| = 0$ or 1.

Fixed elements of J: $\mathbb{F} \oplus V$

Fixed elements of J in $C^+(V)$: $\mathbb{F}$

Fixed elements of J in $C^-(V)$: V.

Claim. $D(V)$ = all units in $C^+(V)$. Namely if α is a unit in $C^+(V)$, then $N(\alpha)^J = (\alpha\alpha^J)^J = \alpha\alpha^J = N(\alpha)$ so $N(\alpha) \in \mathbb{F}^*$ and $\alpha^{-1} = \frac{1}{N(\alpha)}\alpha^J$. Hence

$\alpha x\alpha^{-1} = \frac{1}{N(\alpha)} \alpha x\alpha^J$ is fixed by J and in $C^-(V)$ for every $x \in V$, so $\alpha x\alpha^{-1} \in V$ for all $x \in V$. Therefore $\alpha \in D(V)$. □

Take $\nu = 1$: $C^+(V) \simeq \mathbb{F}_2$, $D(V) \simeq GL(2,\mathbb{F})$ so $O^+(V) \simeq PGL(2,\mathbb{F})$. For $\alpha \in C^+(V)$, $N(\alpha)$ is the determinant of the corresponding element in $\mathbb{F}_2$ so $D_0(V) \simeq SL(2,\mathbb{F})$ and $\Omega(V) = O'(V) \simeq PSL(2,\mathbb{F})$.

<u>n=4.</u> $C_0(V) = \mathbb{F} \oplus \mathbb{F} e_\Omega$, discr $V = G$, $e_\Omega^2 = G$.

case $\nu = 1$: (this corresponds to $\nu \geq 0$, G not a square) $P\Omega(V) = PSL(2,\mathbb{F}(\sqrt{G}))$; if $\mathbb{F} = GF(q)$ then $P\Omega(4,q,\varepsilon = -1) \simeq PSL(2,q^2)$.

case $\nu = 2$: $P\Omega(V) \simeq PSL(2,\mathbb{F}) \times PSL(2,\mathbb{F})$; if $\mathbb{F} = GF(q)$ then $P\Omega(4,q,\varepsilon = 1) \simeq PSL(2,q) \times PSL(2,q)$.

For details of the case n = 4 see [1] or [6].

References

1. E. Artin, Geometric Algebra. Interscience, New York and London (1957).

2. E. Artin, The orders of the classical simple groups. Comm. Pure Appl. Math. 8 (1955), 455-472.

3. R. Baer, Linear algebra and projective geometry. Academic Press, New York (1952).

4. C. Chevally, The algebraic theory of spinors. Columbia University Press, New York (1954).

5. J. Dieudonné, Sur les groupes classiques. Hermann, Paris (1958).

6. J. Dieudonné, La geometrie des groupes classiques, Springer, Berlin-Göttingen-Heidelberg (1955).

7. B. Huppert, Endliche Gruppen, Springer-Verlag, Berlin-Heidelberg-New York (1967).

8. N. Jacobson, Basic algebra I. W.H. Freeman and Company, San Francisco (1974).

Appendix

The geometry of the Klein quadric

In this appendix we assume familiarity with the elementary theory of the exterior algebra of a vector space and with the theory of reflexive bilinear forms. Our central theme is the relationship between the geometry of a four dimensional space and the geometry of its exterior square. From this we obtain certain isomorphisms between classical groups and ultimately a detailed description of the Suzuki groups.

1. Grassman's relations

Let V be a vector space of dimension n over a field F, let $\Lambda_p V$ denote the p-th exterior power of V and let $\Lambda^p V$ denote the p-th exterior power of the dual space V^* of V. There is a pairing between $\Lambda_p V$ and $\Lambda^p V$ which allows us to regard $\Lambda^p V$ as the dual space of $\Lambda_p V$. For $v_1,\dots,v_p \in V$ and $\varphi_1,\dots,\varphi_p \in V^*$ the pairing between $v_1 \wedge \dots \wedge v_p$ and $\varphi_1 \wedge \dots \wedge \varphi_p$ is given by

$$\text{(1.1)} \qquad \langle v_1 \wedge \dots \wedge v_p \,,\; \varphi_1 \wedge \dots \wedge \varphi_p \rangle = \det(\varphi_i(v_j)) \,.$$

More generally, there is a bilinear mapping $\llcorner : \Lambda_p V \times \Lambda^q V \to \Lambda_{p-q} V$ called the <u>interior product</u> which reduces to the above pairing when $p = q$. For $\xi \in \Lambda_p V$ and $\alpha \in \Lambda^q V$, $\xi \llcorner \alpha$ is defined by

$$\text{(1.2)} \qquad \langle \xi \llcorner \alpha, \beta \rangle = \langle \xi, \alpha \wedge \beta \rangle \qquad \underline{\text{for all}} \;\; \beta \in \Lambda^{p-q} V \,.$$

Let $e_1,\dots,e_n$ be a basis for V and let $\omega_1,\dots,\omega_n$ be the corresponding dual basis for V^*. If P is a subset of $\{1,\dots,n\}$ we shall suppose that the elements $i_1,\dots,i_p$ of P are ordered so that $i_1 < i_1 < \dots < i_p$, then define $e_P = e_{i_1} \wedge \dots \wedge e_{i_p}$ and $\omega_P = \omega_{i_1} \wedge \dots \wedge \omega_{i_p}$. The elements e_P with $|P| = p$ form a basis for $\Lambda_p V$. In terms of these basis elements the interior product becomes

$$\text{(1.3)} \qquad e_P \llcorner \omega_Q = \begin{cases} 0 & Q \not\subseteq P \\ \varepsilon_{P,Q}\, e_{P-Q} & Q \subseteq P \end{cases}$$

where $\varepsilon_{P,Q}$ is the sign of the permutation which takes P in its natural order to (Q,P - Q) with Q and P - Q in natural order. From (1.3) we deduce that if W is a subspace of V and $\xi \in \Lambda_p W$, then $\xi \llcorner \alpha \in \Lambda_{p-q} W$ for any $\alpha \in \Lambda^q V$.

An element of $\Lambda_p V$ is said to be <u>decomposable</u> if it can be written in the form $v_1 \wedge \dots \wedge v_p$ for some $v_1,\dots,v_p \in V$. The vectors $v_1,\dots,v_p$ are linearly dependent if and only if $v_1 \wedge \dots \wedge v_p = 0$. If $v_1,\dots,v_p$ and $w_1,\dots,w_p$ are two sets of linearly independent vectors, then the subspaces $\langle v_1,\dots,v_p\rangle$ and $\langle w_1,\dots,w_p\rangle$ coincide if and only if $v_1 \wedge \dots \wedge v_p = a\, w_1 \wedge \dots \wedge w_p$ for some non-zero element $a \in F$. A convenient characterization of the decomposable elements is given by <u>Grassman's relations</u>:

(1.4) $\xi \in \Lambda_p V$ <u>is decomposable if and only if</u>

$\xi \wedge (\xi \llcorner \varphi) = 0$ <u>for all</u> $\varphi \in \Lambda^{p-1} V$.

<u>Proof</u>. Suppose that $\xi = v_1 \wedge \dots \wedge v_p$ and $\varphi \in \Lambda^{p-1} V$.
From the comment following (1.3) we have $\xi \llcorner \varphi \in \langle v_1,\dots,v_p\rangle$ and therefore $\xi \wedge (\xi \llcorner \varphi) = 0$.
Conversely, suppose that $\xi \in \Lambda_p V$ and $\xi \wedge (\xi \llcorner \varphi) = 0$ for all $\varphi \in \Lambda^{p-1} V$. Let W be the subspace of V consisting of the vectors v such that $\xi \wedge v = 0$. Let $e_1,\dots,e_k$ be a basis for W and extend this to a basis $e_1,\dots,e_n$ for V. We can write $\xi = \Sigma \xi_P e_P$, where $\xi_P \in F$ and the summation is over the p-element subsets of $\{1,\dots,n\}$. Since $\xi \wedge e_i = 0$ for $1 \le i \le k$ it follows that $\xi = e_1 \wedge \dots \wedge e_k \wedge \xi'$ for some $\xi' \in \Lambda_{p-k} V$. But now (1.3) implies $p = k$, hence $\xi' \in F$ and ξ is decomposable. □

(1.5) <u>If</u> $\xi \in \Lambda_p V$, $\eta \in \Lambda_q V$ <u>and</u> $\omega \in V^*$, <u>then</u>

$$(\xi \wedge \eta) \llcorner \omega = (\xi \llcorner \omega) \wedge \eta + (-1)^p \xi \wedge (\eta \llcorner \omega) .$$

<u>Proof</u>. This is a consequence of (1.3) and the fact that the formula is bilinear in ξ and η. □

To conclude this section we describe the relationship between linear transformations of V and the interior product. A linear transformation T of V induces a linear transformation $\Lambda_p T$ of $\Lambda_p V$ such that $(\Lambda_p T)(v_1 \wedge \ldots \wedge v_p) = Tv_1 \wedge \ldots \wedge Tv_p$. In turn $\Lambda_p T$ induces a linear transformation $\Lambda^p T$ of $\Lambda^p V$ such that $<\xi, (\Lambda^p T)\alpha> = <(\Lambda_p T)\xi, \alpha>$ for all $\xi \in \Lambda_p V$ and $\alpha \in \Lambda^p V$. An easy calculation now shows that

(1.6) $$(\Lambda_{p-q} T)(\xi \llcorner (\Lambda^q T)\alpha) = ((\Lambda_p T)\xi) \llcorner \alpha$$

<u>for all</u> $\xi \in \Lambda_p V$ <u>and</u> $\alpha \in \Lambda^q V$.

2. <u>The Klein quadric</u>

We shall continue to use the notation introduced in the previous section and now we make the assumption that the dimension of V is four. In this case we shall show that Grassman's relations for elements of $\Lambda_2 V$ reduce to a single quadratic equation. First suppose that $\xi = \sum_{i<j} p_{ij} e_i \wedge e_j$ and set $\tilde{e} = e_1 \wedge e_2 \wedge e_3 \wedge e_4$. Then

(2.1) $$\xi \wedge \xi = 2Q(\xi)\tilde{e}, \quad \text{where}$$

(2.2) $$Q(\xi) = p_{12}p_{34} - p_{13}p_{24} + p_{14}p_{23} .$$

The function $Q : \Lambda_2 V \to F$ is a non-degenerate quadratic form on $\Lambda_2 V$ of index 3. Its polar form is $f(\xi,\eta) = Q(\xi + \eta) - Q(\xi) - Q(\eta)$ and we have

(2.3) (i) $\xi \wedge \eta = f(\xi,\eta)\tilde{e}$ <u>for all</u> $\xi, \eta \in \Lambda_2 V$.

(ii) $\xi \wedge (\xi \llcorner \varphi) = Q(\xi)\tilde{e} \llcorner \varphi$ <u>for all</u> $\xi \in \Lambda_2 V$, $\varphi \in V^*$.

<u>Proof</u>. From the definitions of $Q(\xi)$ and $f(\xi,\eta)$ we have $2\xi \wedge \eta = 2f(\xi,\eta)\tilde{e}$ and from (1.5) we have $(\xi \wedge \xi) \llcorner \varphi = 2\xi \wedge (\xi \llcorner \varphi)$ so that (i) and (ii) hold for all fields of characteristic zero and hence for all fields without restriction. □

(2.4) $\xi \in \Lambda_2 V$ is decomposable if and only if $Q(\xi) = 0$.

Proof. This is an immediate consequence of (1.4) and (2.3)(ii). □

The set of points of the projective space $P(\Lambda_2 V)$ which are isotropic with respect to Q is known as the Klein quadric. In section 1 we saw that the decomposable elements of $\Lambda_p V$ represent the subspaces of V of dimension p. In particular, the points of the Klein quadric are in one to one correspondence with the lines of PV; the line $L = \langle u,v \rangle$ corresponds to the isotropic point $[L] = \langle u \wedge v \rangle$.
If X is a set of points of $P(\Lambda_2 V)$, let $X^{\perp}$ denote the points orthogonal to every point of X with respect to f. From (2.3)(i) we deduce

(2.5) If L and M are lines of PV, then L and M have non-empty intersection if and only if $[L] \in [M]^{\perp}$. □

For each point P of PV let [P] denote the set of points of $P(\Lambda_2 V)$ which correspond to the lines through P. By (2.5) we see that [P] is a maximal totally isotropic subspace of $P(\Lambda_2 V)$; that is, a plane contained in the Klein quadric. Similarly, if H is a plane of PV, then the set [H] of the points of $P(\Lambda_2 V)$ which correspond to the lines of H is also a totally isotropic plane of $P(\Lambda_2 V)$. A totally isotropic line of $P(\Lambda_2 V)$ is spanned by an orthogonal pair of isotropic points and by (2.5) these points correspond to a pair of intersecting lines of PV. Thus a totally isotropic line of $P(\Lambda_2 V)$ corresponds to a pair (P,H), where P is a point of PV and H is a plane through P; the points of the totally isotropic line correspond to the lines of H which contain P. From this we deduce

(2.6)(i) There are just two types of maximal isotropic subspaces of $P(\Lambda_2 V)$, namely those of the type [P], where P is a point and those of the type [H], where H is a plane.

(ii) Each totally isotropic line of $P(\Lambda_2 V)$ is contained in exactly one totally isotropic plane of each type.

(iii) Distinct totally isotropic planes of $P(\Lambda_2 V)$ are of the same type if and only if their intersection is a point. □

An interpretation of the non-isotropic points of $P(\Lambda_2 V)$ will be given in section 3.

If T is a linear transformation of V, then $(\Lambda_4 T)\tilde{e} = (\det T)\tilde{e}$ and so from (1.6) and (2.3)(ii) we have

2.7) $\qquad Q((\Lambda_2 T)\xi) = (\det T)Q(\xi)$ <u>for all</u> $\xi \in \Lambda_2 V$.

Furthermore, if σ is an automorphism of F and $\xi = \sum_{i<j} p_{ij} e_i \wedge e_j$ we define $\sigma(\xi) = \sum_{i<j} \sigma(p_{ij}) e_i \wedge e_j$. Then $Q(\sigma(\xi)) = \sigma(Q(\xi))$ and it follows that every semilinear transformation of V induces a semilinear transformation of $\Lambda_2 V$ which preserves the zeros of Q.
Thus we have a homomorphism from the group $\Gamma L(V)$ of invertible semilinear transformations of V to the group $\Gamma O_+(\Lambda_2 V)$ of invertible semilinear transformations of $\Lambda_2 V$ which preserve the zeros of Q; the kernel is easily seen to be $\{\pm I\}$. Let $P\Gamma L(V)$ and $P\Gamma O_+(\Lambda_2 V)$ denote the groups induced by $\Gamma L(V)$ and $\Gamma O_+(\Lambda_2 V)$ on the projective spaces PV and $P(\Lambda_2 V)$. By the Fundamental Theorem of Projective Geometry $P\Gamma L(V)$ is the group of all collineations of PV. The homomorphism from $\Gamma L(V)$ to $\Gamma O_+(\Lambda_2 V)$ induces an embedding of $P\Gamma L(V)$ in $P\Gamma O_+(\Lambda_2 V)$. The elements of $P\Gamma O_+(\Lambda_2 V)$ which do not come from collineations of PV correspond to correlations of PV and the rest of this section will be devoted to describing this correspondence.

A correlation of PV is induced by a semilinear isomorphism $\beta : V \to V^*$ or equivalently, a sesquilinear form $b(x,y) = \beta(x)y$. If σ is the field automorphism associated with β, the <u>transpose</u> of β is defined to be the isomorphism $\beta^t : V \to V^*$ which takes y to $\sigma^{-1}b(-,y)$. Let β^* denote the inverse of β^t. If $W \subseteq V$, the annihilator of W is $W^0 = \{\varphi \in V^* \mid \varphi(w) = 0$ for all $w \in W\}$, similarly the annihilator of $X \subseteq V^*$ is $X^0 = \{v \in V \mid \chi(v) = 0$ for all $\chi \in X\}$. Recall that when W is a subspace $W^{00} = W$ and $U \subseteq W$ implies $W^0 \subseteq U^0$.

(2.5) $\qquad$ <u>If</u> W <u>is a subspace of</u> V, <u>then</u> $\beta(W)^0 = \beta^*(W^0)$.

Proof. $v \in \beta^*(W^0)$ iff $\beta^t(v) \in W^0$ iff $b(w,v) = 0$ for all $w \in W$ iff $\beta(w) \in \langle v\rangle^0$ for all $w \in W$ iff $v \in \beta(W)^0$. □

The correlation induced by β is the permutation of the subspaces of V which takes W to $\beta(W)^0$. From β we obtain an isomorphism $\Lambda_2 V \to \Lambda^2 V$ which sends $u \wedge v$ to $\beta u \wedge \beta v$ and which we again denote by β. There is also an isomorphism $\Lambda^2 V \to \Lambda_2 V$ which sends φ to $\tilde{e} \llcorner \varphi$ and its inverse sends $\xi \in \Lambda_2 V$ to the linear functional $f(\xi,-)$ because from (1.3) and the definition of f we have

$$\text{(2.9)} \qquad \tilde{e} \llcorner f(\xi,-) = \xi \qquad \text{for all } \xi \in \Lambda_2 V .$$

Thus the mapping $\tilde{\beta} : \Lambda_2 V \to \Lambda_2 V$ defined by $\tilde{\beta}\xi = \tilde{e} \llcorner \beta\xi$ is a semilinear transformation of $\Lambda_2 V$ and we have

$$\text{(2.10)} \qquad Q(\tilde{\beta}\xi) = \langle \tilde{e}, \beta\tilde{e}\rangle \sigma(Q(\xi)) .$$

Proof. Since $\xi \to f(\xi,-)$ is the inverse of $\varphi \to \tilde{e} \llcorner \varphi$ we have $2Q(\tilde{\beta}\xi) = f(\tilde{e} \llcorner \beta\xi, \tilde{e} \llcorner \beta\xi)$ $= \langle \tilde{e} \llcorner \beta\xi, \beta\xi\rangle = \langle e, \beta\xi \wedge \beta\xi\rangle = 2\sigma Q(\xi)\langle \tilde{e}, \beta\tilde{e}\rangle$. Thus (2.10) holds for all fields of characteristic zero and hence it holds generally. □

The number $\langle \tilde{e}, \beta\tilde{e}\rangle$ is the <u>discriminant</u> of β; from (1.1) it is equal to $\det(b(e_i, e_j))$.

(2.11) <u>If</u> X <u>is a point</u>, <u>line or plane of</u> PV, <u>then</u> $\tilde{\beta}[X] = [\beta(X)^0]$

Proof. For $0 \neq \alpha \wedge \beta \in \Lambda^2 V$ it follows from (1.3) that $\tilde{e} \llcorner (\alpha \wedge \beta)$ represents the annihilator of $\langle \alpha, \beta\rangle$. Hence if L is a line, $\beta[L] = [\beta(L)^0]$. The corresponding result for points and planes follows from this. □

Let $P\Gamma L^*(V)$ denote the group of all collineations and correlations of V. The main result of this section is

$$\text{(2.12)} \qquad P\Gamma L^*(V) \simeq P\Gamma O_+(\Lambda_2 V) .$$

Proof. We have already seen that every element of $P\Gamma L^*(V)$ induces an element of $P\Gamma O_+(\Lambda_2 V)$. The converse is an immediate consequence of (2.6). □

For use in later sections we describe the group $P\Gamma L^*(V)$ in greater detail. For $T \in \Gamma L(V)$, let T^* be the semilinear transformation of V^* defined by $T^*\varphi = \tau\varphi T^{-1}$, where τ is the field automorphism associated with T. If we identify a subspace of V with its annihilator in V^*, then T and T^* induce the same collineation of PV. Similarly, if $\beta : V \to V^*$ represents a correlation, then by (2.8) β^* also represents this correlation. Now let T' be the transformation of $V \oplus V^*$ which takes (u,φ) to $(Tu, T^*\varphi)$ and let β' be the transformation which takes (u,φ) to $(\beta^*\varphi, \beta u)$. Let $\Gamma L^*(V)$ be the set of all these T' and β'.

(2.13) $\Gamma L^*(V)$ is a group.

Proof. To show that $\Gamma L^*(V)$ is closed under multiplication we must show that $(\beta T)^* = \beta^* T^*$, $(T^*\beta) = T\beta^*$, $(\beta_1^*\beta_2)^* = \beta_1\beta_2^*$ and $(ST)^* = S^*T^*$. These relations follow easily from the definitions of T^* and β^*. □

If $Z(V) = \{(\lambda I)' \mid \lambda \in F\}$, then $P\Gamma L^*(V) \cong \Gamma L^*(V)/Z(V)$. As a corollary to (2.13) we have

(2.14) If $T \in \Gamma L(V)$ and β represents a correlation then $\beta^{-1}T^*\beta$ corresponds to the conjugate of T' by β'. □

Let GL(V) be the subgroup of $\Gamma L(V)$ consisting of the linear transformations, let SL(V) be those of determinant 1 and let PGL(V) and PSL(V) be the corresponding groups induced on PV. Similarly, let $O_+(\Lambda_2 V)$ be the group of linear transformations T of $\Lambda_2 V$ such that $Q(T\xi) = Q(\xi)$ for all $\xi \in \Lambda_2 V$, let $\Omega_+(\Lambda_2 V)$ be the derived group of $O_+(\Lambda_2 V)$ and let $PO_+(\Lambda_2 V)$ and $P\Omega_+(\Lambda_2 V)$ be the corresponding projective groups. (The + indicates that the quadratic form has maimum index). From (2.12) we have

(2.15) $PSL(V) \simeq P\Omega_+(\Lambda_2 V)$.

When F is the finite field GF(q) the groups are usually written PSL(4,q) and $P\Omega_+(6,q)$ so that (2.15) becomes

(2.16) $PSL(4,q) \simeq P\Omega_+(6,Q)$.

The group SL(V) is generated by transvections; that is, transformations $x \to x + \varphi(x)y$, where $\varphi \in V^*$ and $\varphi(y) = 0$. Given such a transvection τ we choose the basis of V so that $y = e_1$ and $\varphi = \omega_4$. Let $\xi = - e_1 \wedge e_2$, $\eta = e_3 \wedge e_4$ and $\mu = e_1 \wedge e_3$. Then for $\rho = \Lambda_2\tau$ we have

(2.17) $$\rho(\eta) = \eta - \mu$$

$$\rho(\theta) = \theta + f(\theta,\mu)\xi \qquad \text{for } \theta \in \langle\xi\rangle^{\perp}$$

Thus ρ is a Siegel transformation of Λ_2V. The homomorphism from $\Gamma L(V)$ to $\Gamma O_+(\Lambda_2V)$ takes SL(V) to $\Omega_+(\Lambda_2V) \simeq SL(V)/\{\pm I\}$, hence $\Omega_+(\Lambda_2V)$ is generated by the Siegel transformations (2.17).

Finally, we remark that the results of this section do not depend on the choice of basis for V since changing the basis merely changes Q, f and $\tilde{\beta}$ by scalar factors. This justifies the calculations leading to (2.17). However, the presence of these scalar factors means that the isomorphism (2.12) does not lift to an isomorphism between $\Gamma L^*(V)$ and $\Gamma O_+(\Lambda_2V)$.

3. Null polarities

Suppose that b is a non-degenerate alternating form on V and choose the basis so that e_1, e_2 and e_4, e_3 are mutually orthogonal hyperbolic pairs. Let $\beta : V \to V^*$ be the isomorphism induced by b, that is $\beta(u)v = b(u,v)$, and let $\tilde{\beta}$ be the corresponding linear transformation of Λ_2V as defined in section 2. In this case the correlation induced on PV is said to be a null polarity. An easy calculation using the definition of $\tilde{\beta}$ shows that it leaves $e_1 \wedge e_3$, $e_2 \wedge e_4$, $e_1 \wedge e_4$ and $e_2 \wedge e_3$ fixed and interchanges $e_1 \wedge e_2$ with $e_3 \wedge e_4$. Therefore, if we set $\theta = e_1 \wedge e_2 - e_3 \wedge e_4$, then

(3.1) $$\tilde{\beta}(\xi) = \xi + f(\xi,\theta)\theta \qquad \underline{\text{for all}}\ \xi \in \Lambda_2V .$$

and $\tilde{\beta}$ is the symmetry which leaves the hyperplane $W = \langle\theta\rangle^{\perp}$ fixed pointwise.

It follows from (2.11) that a line L of PV is totally isotropic if and only if [L] is a fixed point of $\tilde{\beta}$. Hence

(3.2) <u>The totally isotropic lines of</u> PV <u>are in one-to-one correspondence with the isotropic points of</u> PW.

If P is a point of PV, then $[P] \cap W$ is the (totally isotropic) line of $P(\Lambda_2 V)$ corresponding to the set of totally isotropic lines of PV through P. By (2.6)(ii) $[P^\perp]$ is uniquely determined as the totally isotropic plane $\neq [P]$ of $P(\Lambda_2 V)$ which contains $[P] \cap W$. In particular, the configuration of points and totally isotropic lines of PV is dual to the configuration of points and totally isotropic lines of PW. These configurations are known as <u>generalized quadrangles</u> since for each line L and point P not on L there is a unique point on L which is joined by a line to P (namely $L \cap P^\perp$).
If $\langle\xi\rangle$ is a non-isotropic point of $P(\Lambda_2 V)$, then any hyperbolic line through $\langle\xi\rangle$ meets the Klein quadric in exactly two points. Thus ξ can be written in the form $e_1 \wedge e_2 - e_3 \wedge e_4$ for some basis e_1, e_2, e_3, e_4 of V. Since there is a unique alternating form on V for which e_1, e_2 and e_4, e_3 are orthogonal hyperbolic pairs, it follows that there is a bijection between the null polarities of PV and the non-isotropic points of $P(\Lambda_2 V)$.

Now suppose that T is a semilinear transformation of V and let σ be the associated field automorphism. The group $\Gamma Sp(V)$ is defined to be the set of all those semilinear transformations for which there is a scalar λ such that $b(Tu,Tv) = \lambda\sigma b(u,v)$ for all $u,v \in V$. Those linear transformations of $\Gamma Sp(V)$ for which $\lambda = 1$ form the <u>symplectic group</u> Sp(V). As usual let $P\Gamma Sp(V)$ and PSp(v) denote the corresponding projective groups.
Let $\Gamma O(W)$ denote the group of semilinear transformations of W which preserve the zeros of Q, let $O(W) = \Gamma O(W) \cap O_+(\Lambda_2 V)$ and let $\Omega(W)$ be the derived group of O(W). Since $\tilde{\beta}$ is the only element of $O_+(\Lambda_2 V)$ which leaves W fixed pointwise it follows that $\langle\tilde{\beta}\rangle \times O(W)$ is the subgroup of $O_+(\Lambda_2 V)$ which leaves W fixed. Finally, let $P\Gamma O(W)$, PO(W) and $P\Omega(W)$ denote the

corresponding projective groups.

(3.2) $P\Gamma Sp(V) \simeq P\Gamma O(W)$.

Proof. If $T \in \Gamma Sp(V)$, then T permutes the totally isotropic lines of PV among themselves and hence $\Lambda_2 T$ fixes W, i.e. $\Lambda_2 T \in \Gamma O(W)$. Conversely, it follows from (2.12) that each element of $P\Gamma O(W)$ arises from a collineation or correlation of PV but by multiplying by the correlation β if necessary we may suppose it arises from a collineation and hence from a semilinear transformation T such that $\Lambda_2 T$ fixes W. If $T^* = \sigma\Lambda^1 T^{-1}$, where σ is the field automorphism associated with T, then $T^*\beta$ and βT induce the same correlation of PV, hence they are equal up to a scalar factor and therefore $T \in \Gamma Sp(V)$. It follows from (2.12) that $P\Gamma Sp(V) \simeq P\Gamma O(W)$. □

(3.3) $Sp(V)/\{\pm I\} \simeq \Omega(W)$.

Proof. We know that $Sp(V)/\{\pm I\}$ is isomorphic to a normal subgroup of $O(W)$ with abelian factor group and since $Sp(V)' = Sp(V)$, the result follows from the definition of $\Omega(W)$. □

Note that $T \in SL(V)$ belongs to $Sp(V)$ iff $T^*\beta = \beta T$ iff $\Lambda_2 T$ commutes with $\tilde{\beta}$. Hence $\Omega(W)$ is the centralizer of $\tilde{\beta}$ in $\Omega_+(\Lambda_2 V)$.

For the case of the finite field GF(q) the groups PSp(V) and $P\Omega(W)$ are written PSp(4,q) and $P\Omega(5,q)$ respectively so that from (3.3) we have

(3.4) $PSp(4,q) \simeq P\Omega(5,q)$.

Since Sp(V) is generated by transvections it follows from the remarks at the end of section 2 that $\Omega(W)$ is generated by the corresponding Siegel transformations.

4. Unitary polarities of index 2

Throughout this section b will denote a non-degenerate skew symmetric hermition form of index 2 which is semilinear in the first variable and $\beta : V \to V^*$ will denote the semilinear isomorphism such that $\beta(u)v = b(u,v)$. The correlation induced on PV is called a unitary polarity. (In the case of a finite field this is the only type of unitary polarity possible.) Let $x \to \bar{x}$ be the associated field automorphism and let F_0 be its fixed field. Then $F = F_0[\theta]$ and θ satisfies the quadratic equation $\theta^2 - a\theta + b = 0$, where $a = \theta + \bar{\theta}$ and $b = \theta\bar{\theta}$ belong to F_0.
Choose the basis of V so that e_1, e_2 and e_4, e_3 are mutually orthogonal hyperbolic pairs. Just as in section 3 $\tilde{\beta}$ fixes $e_1 \wedge e_3$, $e_2 \wedge e_4$, $e_1 \wedge e_4$ and $e_2 \wedge e_3$ and interchanges $e_1 \wedge e_2$, with $e_3 \wedge e_4$. However in this case $\tilde{\beta}$ is a semilinear transformation and its set of fixed points is the F_0-space W_0 with basis $\xi_1 = e_1 \wedge e_2 + e_3 \wedge e_4$, $\xi_2 = -\theta e_1 \wedge e_2 - \bar{\theta} e_3 \wedge e_4$, $\xi_3 = e_1 \wedge e_3$, $\xi_4 = e_2 \wedge e_4$, $\xi_5 = e_1 \wedge e_4$ and $\xi_6 = e_2 \wedge e_3$. The value of the quadratic form on

$$\xi = \sum_{i=1}^{6} x_i \xi_i \in W_0$$

is

$$(4.1) \qquad Q(\xi) = x_1^2 - ax_1x_2 + bx_2^2 - x_3x_4 + x_5x_6 .$$

Thus the restriction of Q to W_0 is a non-degenerate quadratic form of index 2.

(4.2) If $\tilde{\beta}$ fixes the point $\langle\xi\rangle$ of $P(\Lambda_2 V)$, then $\tilde{\beta}$ fixes a non-zero vector $x\xi$ for some $x \in F$.

Proof. Suppose that $\tilde{\beta}\xi = y\xi$ and set $x = 1 + y$, then $\tilde{\beta}$ fixes $x\xi$. If $y = -1$, choose x so that $x + \bar{x} = 0$ but $x \neq 0$. □

From (2.11) a line L of PV is totally isotropic if and only if [L] is fixed by $\tilde{\beta}$ hence by (4.2) the totally isotropic lines of PV are in one-to-one correspondence with the isotropic points of PW_0. Let $[L]_0$ denote the point of PW_0 representing the totally isotropic line L.

The points $[L]_0$ and $[M]_0$ of PW_0 are orthogonal if and only if L and M have a point in common. Hence the totally isotropic points of PV are in one-to-one correspondence with the totally isotropic lines of PW_0. As in section 3 the configuration of totally isotropic points and lines of PV is dual so the configuration of totally isotropic points and lines of PW_0, and again these configurations are generalized quadrangles.

The notation for groups associated with b and the restriction of Q to W_0 follows the pattern established in the previous sections. Thus $\Gamma U(V)$ denotes the group of semilinear transformations T with associated field automorphism σ such that for some λ, $b(Tu,Tv) = \lambda\sigma b(Tu,Tv)$ for all $u,v \in V$. The subgroup of transformations for which $\sigma = 1$ and $\lambda = 1$ is $U(V)$ and the subgroup of $U(V)$ of transformations of determinant 1 is $U^+(V)$. The corresponding projective groups are $P\Gamma U(V)$, $PU(V)$ and $PU^+(V)$ respectively. Similarly the groups $\Gamma O_-(W_0)$, $O_-(W_0)$ and $\Omega_-(W_0)$ are defined in the same way as $\Gamma O_+(\Lambda_2 V)$, $O_+(\Lambda_2 V)$ and $\Omega_+(\Lambda_2 V)$ and the $-$ indicates that the form has index 2. The corresponding projective groups are $P\Gamma O_-(W_0)$, $PO_-(W_0)$ and $P\Omega_-(W_0)$ respectively.

(4.3) $\quad P\Gamma U(V) \simeq P\Gamma O_-(W_0)$.

Proof. As in the proof of (3.2) $T \in \Gamma U(V)$ permutes the totally isotropic lines of V among themselves and hence $\Lambda_2 T$ fixes W_0. To see that the restriction of the isomorphism (2.12) takes $P\Gamma U(V)$ onto $P\Gamma O_-(W_0)$ we apply the argument used in (3.2). □

(4.4) $\quad U^+(V)/\{\pm I\} \simeq \Omega_-(W_0)$.

Proof. The proof of (3.3) goes over without change. □

When $F = GF(q^2)$, we have $F_0 = GF(q)$ and the groups $PU^+(V)$ and $P\Omega_-(W_0)$ are written $PU^+(4,q)$ and $P\Omega_-(6,q)$ respectively. From (4.4) we have

(4.5) $\quad PU^+(4,q) \simeq P\Omega_-(6,q)$.

Since $U^+(V)$ is generated by transvections it follows that $\Omega_-(W_0)$ is generated by Siegel transformations.

We have already observed that the non-isotropic points of $P(\Lambda_2 V)$ correspond to the null polarities of PV and since W_0 is the set of fixed elements of $\tilde{\beta}$ we can now see that the non-isotropic points of PW_0 correspond to the null polarities of PV which commute with the unitary polarity β.

5. Line stabilizers

Instead of using the methods of sections 3 and 4 to investigate orthogonal polarities of V we prefer to obtain the three and four dimensional orthogonal groups as line stabilizers in the five and six dimensional orthogonal groups. This approach avoids having to treat fields of even characteristic separately.

Suppose that L is a hyperbolic line of $P(\Lambda_2 V)$ and let $\langle\xi\rangle$ and $\langle\eta\rangle$ be the isotropic points on L.
Choose the basis of V so that $\xi = e_1 \wedge e_2$ and $\eta = e_3 \wedge e_4$. Let $M = \langle e_1, e_2\rangle$ and $N = \langle e_3, e_4\rangle$. The subgroup of PGL(V) which fixes both M and N is PGL(M) × PGL(N). The image of this group in $P\Gamma O_+(\Lambda_2 V)$ fixes L (pointwise) and therefore acts on $U = L^\perp$. We observed in section 3 that the null polarity $\tilde{\beta}$ described there fixes U pointwise and interchanges ξ with η. It follows that β commutes with PGL(M) × PGL(N). However, if ν is a polarity for which M and N are totally isotropic lines, then $\tilde{\nu}$ fixes $\langle\xi\rangle$ and $\langle\eta\rangle$ and acts on U.
Suppose that T is a linear transformation which acts on M and fixes N pointwise; i.e. T represents an element of PGL(M). Then from 2.14 the conjugate of T by ν is $\nu^{-1}T^*\nu$. If $x \in M$, then $\nu x \in M^0$ hence $T^*\nu x = \nu x$ and therefore $\nu^{-1}T^*\nu$ fixes M pointwise. This means that conjugation by ν interchanges PGL(M) with PGL(N).
The restriction of Q to U is a quadratic form of index 2; let $P\Gamma O_+(U)$ denote the corresponding orthogonal group. An element of $P\Gamma O_+(U)$ can be

regarded as an element of $P\Gamma O_+(\Lambda_2 V)$ which fixes L pointwise. It follows from the discussion above and the isomorphism (2.12) that

(5.1) $(PGL(M) \times PGL(N))Aut(F)\langle\nu\rangle \simeq P\Gamma O_+(U)$.

For $F = GF(q)$, we have

(5.2) $(PGL(2,q) \times PGL(2,q))Aut(GF(q))\langle\nu\rangle \simeq P\Gamma O_+(4,q)$.

As usual, let $\Omega_+(U)$ denote the derived group of the subgroup $O_+(V)$ of $O_+(\Lambda_2 V)$ which acts on U and fixes L pointwise. From the isomorphism $SL(V)/\{\pm I\} \simeq \Omega_+(\Lambda_2 V)$ of section 2 we see that $\Omega_+(U)$ is the central product $(SL(M) \times SL(N))/\{\pm I\}$. Hence for $F = GF(q)$ we have

(5.3) $(SL(2,q) \times SL(2,q))/\{\pm I\} \simeq \Omega_+(4,q)$

and therefore

(5.4) $PSL(2,q) \times PSL(2,q) \simeq P\Omega_+(4,q)$

Next let us consider a line stabilizer in the group $P\Gamma O(W)$ studied in section 3. This time it is convenient to take $L = \langle\xi,\eta\rangle$, where $\xi = e_1 \wedge e_3$ and $\eta = e_2 \wedge e_4$. Then $M = \langle e_1,e_3\rangle$ and $N = \langle e_2,e_4\rangle$ are totally isotropic with respect to the null polarity β studied in section 3. Let $U_1 = L^\perp \cap W$. The subgroup of $P\Gamma O(W)$ which fixes L pointwise is the orthogonal group $P\Gamma O(U_1)$ and the subgroup of $P\Gamma Sp(V)$ to which it corresponds via the isomorphism (3.2) is the centralizer of β in $(PGL(M) \times PGL(N))Aut(F)$.

(5.5) $P\Gamma L(M) \simeq P\Gamma O(U_1)$.

Proof. The centralizer of β in $PGL(M) \times PGL(N)$ consists of the elements $(T,\beta^{-1}T^*\beta)$, where $T \in PGL(M)$ and it is therefore isomorphic to $PGL(M)$. □

When $F = GF(q)$ we have

(5.6) $P\Gamma L(2,q) \simeq P\Gamma O(3,q)$.

Similarly,

(5.7) $PSL(2,q) \simeq P\Omega(3,q)$.

Finally, we consider a line stabilizer in the group $P\Gamma U(W_0)$ of section 4. Now β denotes the unitary polarity of that section and L,M and N retain the same meaning as above. Let $U_0 = L^{\perp} \cap W_0$ and let $P\Gamma O_-(U_0)$ be the corresponding orthogonal group; note that the restriction of Q to U_0 is a quadratic form of index 1. In this case the proof of (5.5) yields

(5.8) $\quad P\Gamma L(M) \simeq P\Gamma O_-(U_0)$.

When $F = GF(q^2)$ we have

(5.9) $\quad P\Gamma L(2,q^2) \simeq P\Gamma O_-(4,q)$.

Similarly,

(5.10) $\quad PSL(2,q^2) \simeq P\Omega_-(4.q)$.

6. Odd dimensional orthogonal groups over $GF(2^a)$

For this section only let W be a vector space of dimension 2n + 1 over $GF(2^a)$ and let $Q : W \to GF(2^a)$ be a quadratic form with polar form $f(x,y) = Q(x + y) - Q(x) - Q(y)$. We shall suppose that Q is non-degenerate; that is, Q does not vanish on the non-zero vectors of the radical of W with respect to f. This assumption forces rad W to have dimension 1 and we may write $W = \text{rad } W \perp V'$, where $\text{rad } W = \langle e_0 \rangle$ and $Q(e_0) = 1$. Let O(W) be the group of linear transformations T of W such that $Q(Tw) = Q(w)$ for all $w \in W$. Then for $T \in O(W)$ and $w \in W$ we may write $Tw = T_0w + T_1w$, where $T_0w \in \text{rad } W$ and $T_1w \in V'$. In particular, $Te_0 = e_0$ and for $v_1v' \in V'$ we have $f(T_1v,T_1v') = f(v,v')$ and therefore T_1 belongs to the group Sp(V') of linear transformations of V' which preserve the alternating form f. Conversely, if $T_1 \in Sp(V')$ and $v \in V'$, let $\lambda(v)$ be the (unique) element of $GF(2^a)$ such that $\lambda(v)^2 = Q(v) + Q(T,v)$. Define $T : W \to W$ by $Te_0 = e_0$ and $Tv = T_1v + \lambda(v)e_0$, for $v \in V$. Then $T \in O(W)$. This proves

(6.1) $O(W) \simeq Sp(V')$,

or in another notation

(6.2) $O(2n+1,2^a) \simeq Sp(2n,2^a)$.

Note that the projection from W onto V' induces a bijection between the zeros of Q and the elements of V'.

7. The twisted polarity

Now consider a vector space V of dimension 4 over $GF(2^a)$ with a non-degenerate alternating form b as in section 3. The considerations of section 6 apply to the subspace W of $\Lambda_2 V$ with basis $e_1 \wedge e_2 + e_3 \wedge e_4$, $e_1 \wedge e_3$, $e_2 \wedge e_4$, $e_1 \wedge e_4$ and $e_2 \wedge e_3$. We have rad W = $\langle e_1 \wedge e_2 + e_3 \wedge e_4 \rangle$ and we may suppose that $V' = \langle e_1 \wedge e_3, e_2 \wedge e_4, e_1 \wedge e_4, e_2 \wedge e_3 \rangle$. Let $\pi : W \to V$ be the linear transformation defined by $\pi(\text{rad } W) = 0$. $\pi(e_1 \wedge e_3) = e_1$, $\pi(e_2 \wedge e_4) = e_2$, $\pi(e_1 \wedge e_4) = e_3$ and $\pi(e_2 \wedge e_3) = e_4$. Then π induces an isometry between V' and V.

If $L = \langle u,v \rangle$ is a totally isotropic line of PV, then $\langle u \wedge v \rangle$ is an isotropic point of W and $\delta(L) = \langle \pi(u \wedge v) \rangle$ is a point of PV. The results of the previous sections show that δ is a bijection between the totally isotropic lines and the points of PV. If P is a point of PV, then the line $[P] \cap W$ projects to a totally isotropic line $\delta(P)$ of PV and if P is on L, then $\delta(L)$ is on $\delta(P)$. (Notice that $[P] \cap W$ and $[P^\perp] \cap W$ coincide so that in W we have lost the distinction between points and planes of PV.)

If $T \in Sp(V)$, then $\Lambda_2 T \in O(W)$ and by (6.1) $\Lambda_2 T$ corresponds to an element $T_1 \in Sp(V)$. If $\bar{T}$ and $\bar{T}_1$ denote the images of T and T_1 in PSp(V), then by construction $\bar{T}_1 = \delta \bar{T} \delta^{-1}$. Hence δ induces an outer automorphism of PSp(V).

Let $u = \sum_{i=1}^{4} x_i e_i$, $v = \sum_{i=1}^{4} y_i e_i$ and $w = \sum_{i=1}^{4} z_i e_i$ and suppose that $b(u,v) = b(u,w) = 0$. We set $\xi = u \wedge v$, $\eta = u \wedge w$, $v' = \pi(\xi)$ and $w' = \pi(\eta)$. A straightforward calculation shows that $\delta(\langle u \rangle) = \langle v',w' \rangle$ and

$$(7.1) \qquad v' \wedge w' =$$

$$b(v,w)[(x_1x_2 + x_3x_4)(e_1 \wedge e_2 + e_3 \wedge e_4) + x_1^2e_1 \wedge e_3 +$$

$$+ x_2^2e_2 \wedge e_4 + x_3^2e_1 \wedge e_4 + x_4^2e_2 \wedge e_3] .$$

Let τ be the automorphism of $GF(2^a)$ such that $\tau(x) = x^2$ for all $x \in GF(2^a)$, then from (7.1) and the definition of δ we have

(7.2) $\qquad \delta^2(P) = \tau(P)$ <u>for all points</u> P.

If a is odd, then $GF(2^a)$ has an automorphism σ such that $\sigma^2 = \tau$. In this case we set $\rho(P) = \sigma^{-1}\delta(P)$ and $\rho(L) = \sigma^{-1}\delta(L)$, for each point P and line L of PV. Then $\rho^2 = 1$ and P_1 is on $\rho(P_2)$ if and only if P_2 is on $\rho(P_1)$. We call ρ the <u>twisted polarity</u> of PV.

The <u>Suzuki group</u> $Sz(2^a)$ is defined to be the centralizer of ρ in $PSp(4,2^a)$.

8. <u>The Suzuki groups</u>

We continue the investigations of section 7 under the assumption that V has dimension 4 over GF(q), where $q = 2^a$ and a is odd. And we shall now write field automorphisms as exponents. Let $O = \{P \in PV | P \in \rho(P)\}$, then $\langle u \rangle \in O$ if and only if $u^\sigma \wedge v' \wedge w' = 0$ and by (7.1) this is the case if and only if

$$(8.1) \qquad x_1^\sigma x_2^2 + x_3^2x_2^\sigma + x_1x_2x_4^\sigma + x_3x_4^{1+\sigma} = 0$$

$$x_1^\sigma x_4^2 + x_1^2x_2^\sigma + x_1x_2x_3^\sigma + x_3^{1+\sigma}x_4 = 0$$

$$x_3^{2+\sigma} + x_1^2x_4^\sigma + x_1^{1+\sigma}x_2 + x_1^\sigma x_3x_4 = 0$$

$$x_1x_2^{1+\sigma} + x_2^\sigma x_3x_4 + x_2^2x_3^\sigma + x_4^{2+\sigma} = 0$$

The plane $<e_2>^\perp$ has equation $x_1 = 0$ so from (8.1) we see that $<e_2>^\perp \cap O = <e_2>$. Let ∞ denote the point $<e_2>$ and let A be the affine space obtained from PV by deleting $\infty^\perp$. As affine coordinates we take $x = x_3/x_1$, $y = x_4/x_1$ and $z = x_2/x_1$. Then (8.1) is equivalent to the single condition

(8.2) $$y^\sigma + z + x^{2+\sigma} + xy = 0 \ .$$

It follows from (8.2) that $|O| = 1 + q^2$.

In order to describe the group Sz(q) we shall represent the elements of PSp(4,q) by matrices with respect to the basis e_1, e_3, e_4, e_2. It is a straightforward calculation to check that the following matrices induce collineations which belong to PSp(4,q).

(8.3) $$\tau(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & a^\sigma & 1 & 0 \\ ab+a^{2+\sigma}+b^\sigma & b+a^{1+\sigma} & a & 1 \end{pmatrix}$$

(8.4) $$\eta(k) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & k & 0 & 0 \\ 0 & 0 & k^{1+\sigma} & 0 \\ 0 & 0 & 0 & k^{2+\sigma} \end{pmatrix}$$

These collineations fix ∞ and commute with ρ and we have

(8.5) $$\tau(a,b)\tau(c,d) = \tau(a + c, b + d + a^\sigma c)$$

(8.6) $$\eta(k)\tau(a,b)\eta(k)^{-1} = \tau(ka, k^{1+\sigma}b) \ .$$

Thus the group $T = \{\tau(a,b) \mid a,b \in GF(q)\}$ has order q^2 and is normalized by the group $E = \{\eta(k) \mid k \in GF(q)^\times\}$ of order $q - 1$. The group T acts regularly on the points of O in A since $\tau(a,b)$ takes the point with coordinates $(0,0,0)^t$ to the point with coordinates $(a,b,ab + a^{2+\sigma} + b^\sigma)^t$.

The matrix

(8.7) $$w = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

induces a collineation which commutes with ρ and interchanges ∞ and $(0,0,0)^t$. Hence $Sz(q)$ acts doubly transitively on O.

Let φ be an element of $Sz(q)$ which fixes $\langle e_1 \rangle$ and $\langle e_2 \rangle$. Then φ can be represented by a matrix

(8.8) $$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ 0 & 0 & 0 & e \end{pmatrix}$$

The image of $(0,y,y^\sigma)^t \in O$ under φ is $(by,\ dy,\ ey^\sigma)^t$ and since φ preserves O, (8.2) implies

(8.9) $$bdy^2 + b^{2+\sigma}y^{2+\sigma} + (d^\sigma + e)y^\sigma = 0 \qquad \text{for all } y \in GF(q) .$$

In order to exploit this equation we use the theorem of Artin that distinct endomorphisms of a field are linearly independent.

<u>Proof</u>. If $\chi_1,\dots,\chi_k$ are endomorphisms of F and $a_1\chi_1 + \dots + a_i\chi_i = 0$ with $a_i \neq 0$ and i as small as possible, then for any x we have $a_1\chi_1(x)\chi_1 + \dots + a_i\chi_i(x)\chi_i = 0$, hence $(a_1\chi_i(x) - a_1\chi_1(x))\chi_1 + \dots + (a_{i-1}\chi_i(x) - a_{i-1}\chi_{i-1}(x))\chi_{i-1} = 0$, a contradiction.

If $q \neq 2$, the endomorphisms $y \to y^2$, $y \to y^{2+\sigma}$ and $y \to y^\sigma$ are distinct, hence $b = 0$ and $e = d^\sigma$. Now consider the image of $(x,0,x^{2+\sigma}) \in O$ under φ to obtain

(8.10) $$c^\sigma x^\sigma + (d^\sigma + a^{2+\sigma})x^{2+\sigma} + acx^2 = 0 .$$

It follows that $c = 0$ and $d^\sigma = a^{2+\sigma}$, hence $\varphi = \eta(a)$.

If $q = 2$ it is not difficult to see that the subgroup of $PSp(4,2)$ which preserves O is the symmetric group S_5 but from (7.1) the subgroup which commutes with ρ has order 20. In all cases we see that $Sz(q)_\infty = T.H$ and hence

$$(8.11) \qquad |Sz(q)| = (q^2 + 1)q^2(q - 1)$$

Since the subgroup T is clearly in the derived group of $Sz(q)$, $q \neq 2$, and since $Sz(q)$ is generated by the conjugates of T it follows from Iwasawa's lemma that $Sz(q)$ is simple when $q \neq 2$. Notice that the order of $Sz(q)$ is never divisible by 3. It is a deep theorem of Thompson that these are the only finite simple groups with this property.

If $P \in O$, then $P^\perp \cap O = P$, since this is true for $P = \infty$ and $Sz(q)$ acts transitively on O. The lines of A which pass through ∞ are the intersections of planes $x = a$ and $y = b$, hence they meet O in just one point of A. A plane of A which contains ∞ has an equation $ax + by = c$ so from (8.2) each plane through ∞ (other than $\infty^\perp$) meets O in $q + 1$ points. Thus every plane which contains at least 2 points of O meets O in $q + 1$ points. Call these sets of $q + 1$ points the blocks of O. Since any 3 points of O lie in a unique plane we have a 3-$(q^2 + 1, q + 1, 1)$ design on O. It follows that there are $q(q^2 + 1)$ planes which meet O in $q + 1$ points and these together with the $q^2 + 1$ tangent planes constitute all the planes of the space. If $P,Q \in O$ and $\rho(P),\rho(Q)$ belong to a common plane H, then $H^\perp = \rho(P) \cap \rho(Q)$ and $P + Q = \rho(H^\perp)$ is totally isotropic, whence $Q \in P^\perp$, a contradiction. Thus if $\varphi \in Sz(q)$ fixes a plane through $\rho(P)$, then $\varphi(P) = P$ and therefore the stabilizer of such a plane has order $q(q - 1)$. It follows that $Sz(q)$ is transitive on the blocks of the 3-$(q^2 + 1, q + 1, 1)$ design.

9. <u>The isomorphisms</u> $A_8 \cong GL(4,2)$ <u>and</u> $\Sigma_6 \cong Sp(4,2)$

Let X be a set of $2m + 2$ elements and let U be the set of partitions (X_1,X_2) of X such that $|X_1|$ and $|X_2|$ are even. We make U into a vector space of

dimension 2m over GF(2) by defining the sum of (X_1,X_2) and (X_1',X_2') to be the partition $(X_1 \# X_1', X_2 \# X_2')$, where $\#$ denotes symmetric difference.
If $x = (X_1,X_2)$ is a partition we set $Q(x) = \frac{1}{2}|X_1|$ (mod 2), then Q is a non-degenerate quadratic form on U and Q is preserved by the symmetric group of X. In particular, if m = 3, then the index of Q is 3 and we have $\Sigma_8 \subseteq O_+(6,2)$. By a result of section 2, $O_+(6,2)$ is isomorphic to GL(4,2) extended by a correlation. Since $|\Sigma_8| = 2|GL(4,2)|$, we have $\Sigma_8 \simeq O_+(6,2)$ and $A_8 \simeq GL(4,2)$.
A transposition in Σ_8 acts as the identity on a subspace of dimension 5 in U, hence it corresponds to a symplectic polarity of GL(4,2). It follows that $\Sigma_6 \simeq Sp(4,2)$. The twisted polarity of section 7 induces an outer automorphism of Σ_6.

References

J. Tits, Les Groupes simples de Suzuki et Ree, Séminaire Bourbaki 1960/61, no 210.

J. Tits, Ovoïdes et groupes de Suzuki, Arch. Mat. 13 (1962) 187-198 et 17 (1966) 136-153.

H. Luneburg, Die Suzukigruppen und ihre Geometrien, Springer Verlag, Berlin, Heidelberg, New York (1965).

Group orders

Group	Order	
A_m	$\frac{1}{2}m!$	
$PSL(n,q)$	$\frac{1}{d} q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - 1)$	$n \geq 2$, $d = (n,q-1)$
$PU^+(n,q)$	$\frac{1}{d} q^{\binom{n}{2}} \prod_{i=2}^{n} (q^i - (-1)^i)$	$n \geq 2$, $d = (n,q+1)$
$PSp(2n,q)$	$\frac{1}{d} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$	$n \geq 1$, $d = (2,q-1)$
$P\Omega(2n+1,q)$	$\frac{1}{d} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$	$n \geq 1$, $d = (2,q-1)$
$P\Omega_{\varepsilon}(2n,q)$	$\frac{1}{d} q^{n(n-1)} (q^n - \varepsilon) \prod_{i=1}^{n-1} (q^{2i} - 1)$	$n \geq 1$, $d = (4,q^n - \varepsilon)$
$Sz(q)$	$(q^2 + 1)q^2(q - 1)$	

Isomorphisms

1) $PSL(2,q) \simeq PU^+(2,q) \simeq PSp(2,q) \simeq P\Omega(3,q) \simeq \begin{cases} \Sigma_3 & \text{if } q = 2 \\ A_4 & \text{if } q = 3 \end{cases}$,

2) $P\Omega(5,q) \simeq PSp(4,q)$,

3) $P\Omega_+(4,q) \simeq PSL(2,q) \times PSL(2,q)$,

4) $P\Omega_-(4,q) \simeq PSL(2,q^2)$,

5) $P\Omega_+(6,q) \simeq PSL(4,q)$,

6) $P\Omega_-(6,q) \simeq PU^+(4,q)$,

7) $P\Omega(2n + 1, 2^a) \simeq PSp(2n,2^a)$,

8) $PSL(2,3) \simeq A_4$;	order 12 ,
9) $PSL(2,4) \simeq PSL(2,5) \simeq A_5$;	order 60 ,
10) $PSL(2,7) \simeq PSL(3,2)$;	order 168 ,
11) $PSL(2,9) \simeq A_6$;	order 360 ,
12) $PSL(4,2) \simeq A_8$;	order 20160 ,
13) $PU^+(4,2) \simeq PSp(4,3)$;	order 25920 ,

Order coincidences

14) $|PSL(3,4)| = |PSL(4,2)| = |A_8| = 20160$,

$PSL(3,4) \not\simeq PSL(4,2) \simeq A_8$.

15) If q is odd, $2n \geq 6$ then,

$|PSp(2n,q)| = |P\Omega(2n + 1,q)|$ but $PSp(2n,q) \not\simeq P\Omega(2n + 1,q)$.

All groups 1) ... 6) are simple with the following exceptions:

a) $PSL(2,2) \simeq PU^+(2,2) \simeq PSp(2,2) \simeq P\Omega(3,2) \simeq \Sigma_3$.

b) $PSL(2,3) \simeq PU^+(2,3) \simeq PSp(2,3) \simeq P\Omega(3,3) \simeq A_4$.

c) $PU^+(3,2)$ of order $72 = 2^3.3^2$, solvable.

d) $PSp(4,2) \simeq \Sigma_6 \simeq P\Omega(5,2)$ of order 720.

e) $P\Omega_+(4,q)$.