The subgroup Ω for orthogonal groups

In the case of the linear group, it is shown in the text that $PSL(n, F)$ (that is, the group $SL(n)$ of determinant one matrices, divided by its center) is usually a simple group. In the case of symplectic group, $PSp(2n, F)$ (the group of symplectic matrices divided by its center) is usually a simple group. In the case of the orthogonal group (as Yelena will explain on March 28), what turns out to be simple is *not* $PSO(V)$ (the orthogonal group of V divided by its center). Instead there is a mysterious subgroup $\Omega(V)$ of $SO(V)$, and what is usually simple is $P\Omega(V)$. The purpose of these notes is first to explain why this complication arises, and then to give the general definition of $\Omega(V)$ (along with some of its basic properties).

So why should the complication arise? There are some hints of it already in the case of the linear group. We made a lot of use of $GL(n, F)$, the group of all invertible $n \times n$ matrices with entries in F. The most obvious normal subgroup of $GL(n, F)$ is its center, the group $F^\times$ of (non-zero) scalar matrices. Dividing by the center gives

$$PGL(n, F) = GL(n, F)/F^\times, \tag{1}$$

the projective general linear group. We saw that this group acts faithfully on the projective space $\mathbb{P}^{n-1}(F)$, and generally it's a great group to work with. Most of the steps in Iwasawa's theorem (for proving a group is simple) apply to $PGL(n, F)$. The only part that doesn't work is that $PGL(n, F)$ need not be its own derived group.

In some sense the reason for this failure is that $GL(n, F)$ has another "obvious" normal subgroup: the group $SL(n, F)$ of determinant one matrices. Once you remember this group, it becomes obvious that any commutator in $GL(n, F)$ must belong to $SL(n, F)$. In fact it turns out that $SL(n, F)$ is (usually) the derived group of $GL(n, F)$ (see page 9 of the text). At any rate, we get a normal subgroup $PSL(n, F)$ of $PGL(n, F)$. A little more precisely,

$$\begin{aligned} PSL(n, F) &= SL(n, F)/(\text{scalar matrices in } SL(n, F)) \\ &= SL(n, F)/(n\text{th roots of 1 in } F^\times). \end{aligned} \tag{2}$$

What's going on is that the scalar matrices of determinant one are precisely the nth roots of 1 in the field F (see page 6 of the text). We're going to see that the relationship between $SO(V)$ and its normal subgroup $\Omega(V)$ is similar to the relationship between $PGL(n, F)$ and its normal subgroup $PSL(n, F)$. So we begin by recalling a little bit about that relationship.

The determinant map is a well-defined surjective group homomorphism from $GL(n, F)$ to $F^\times$ with kernel $SL(n, F)$:

$$\det\colon GL(n, F) \to F^\times, \qquad \ker(\det) = SL(n, F). \tag{3}$$

The determinant of a scalar matrix is equal to the nth power of the scalar. Writing $(F^\times)^n$ for the group of all nth powers in F, we can deduce easily that there is a well-defined surjective group homomorphism "projective determinant,"

$$P\det\colon PGL(n, F) \to F^\times/(F^\times)^n, \qquad \ker(P\det) = PSL(n, F). \tag{4(a)}$$

(This terminology is not standard or common.) It follows that $PGL(n,F)$ is different from $PSL(n,F)$ if and only if $F^\times$ is different from $(F^\times)^n$. In particular,

$$PGL(n,F) = PSL(n,F) \quad \text{if } F \text{ is algebraically closed.} \tag{4)(b}$$

For the real numbers, every number is an nth power if and only if n is odd; so $PGL(n,\mathbb{R})$ is the same as $PSL(n,\mathbb{R})$ if and only if n is odd. For the finite field $\mathbb{F}_q$, every element is an nth power if and only if n and $q-1$ are relatively prime; so $PGL(n,\mathbb{F}_q)$ is the same as $PSL(n,\mathbb{F}_q)$ if and only if n and $q-1$ are relatively prime.

In order to understand $\Omega(V)$ for the orthogonal groups, you might think of $SO(V)$ as being something like $PGL(n,F)$, and its subgroup $\Omega(V)$ as being like $PSL(n,F)$. The text eventually explains a way to make this analogy complete, by defining something called the "spin group" $Spin(V)$ (analogous to $SL(n,F)$), and a group homomorphism from $Spin(V)$ to $SO(V)$ whose image is exactly $\Omega(V)$. I'm not going to do that in general, although I'll do some special cases by hand. Here is the first one.

We are going to make a relationship between $PGL(2,F)$ and the orthogonal group of a certain three-dimensional vector space. For this example, assume that the characteristic of F is not 2. Define

$$V = \{2\times 2 \text{ matrices with entries in } F\}. \tag{5)(a}$$

We define a symmetric bilinear form on V by

$$B(X,Y) = \mathrm{tr}(XY). \tag{5)(b}$$

(Recall that the trace of a square matrix is the sum of the diagonal entries. The form is symmetric because the trace of XY is equal to the trace of YX.) We choose as a basis of V the four matrices

$$\begin{aligned} e_{12} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, & e_{21} &= \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \\ e_{11} - e_{22} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & e_{11} + e_{22} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned} \tag{5)(c}$$

It's a simple matter to compute the matrix of the form B in this basis. For example, $e_{12}e_{21} = e_{11}$, which has trace equal to 1, so $B(e_{12},e_{21}) = 1$. Continuing in this way, we find that the matrix of B in this basis is

$$\widehat{B} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}. \tag{5)(d}$$

The determinant of $\widehat{B}$ is -4, so (since the characteristic of F is not 2) B is nondegenerate.

Consider now the one-dimensional subspace $\langle e_{11}+e_{22}\rangle$ spanned by the identity matrix. Since the form takes the value 2 on the identity matrix, the subspace is non-degenerate. Define

$$W = \langle e_{11}+e_{22}\rangle^\perp = \{X \in V \mid \mathrm{tr}(X) = 0\}. \tag{5)(e}$$

By Proposition 2.9 of the text, we have an orthogonal direct sum decomposition

$$V = W \oplus \langle e_{11} + e_{22} \rangle, \tag{5)(f}$$

The restriction B_W of B to W has matrix

$$\widehat{B_W} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}. \tag{5)(g}$$

This matrix has determinant -2, so B_W is non-degenerate.

Proposition 6. *Suppose F is a field of characteristic not equal to 2. Define a four-dimensional orthogonal space V (the 2×2 matrices) and three-dimensional subspace W (matrices of trace zero) as in (5) above.*

(1) *There is a group homomorphism*

$$\pi_V \colon GL(2, F) \to O(V), \qquad \pi_V(g)X = gXg^{-1} \qquad (X \in V).$$

(2) *Every linear transformation $\pi_V(g)$ fixes the identity matrix $e_{11} + e_{22}$, and therefore preserves its orthogonal complement W. Write*

$$\pi_W \colon GL(2, F) \to O(W)$$

for the restriction of π_V to W.

(3) *We have*

$$\ker \pi_V = \ker \pi_W = F^\times,$$

the scalar matrices in $GL(2, F)$. The homomorphism π_W therefore defines an injective homomorphism

$$\overline{\pi_W} \colon PGL(2, F) \hookrightarrow O(W).$$

(4) *In the basis $\{e_{12}, e_{21}, e_{11} - e_{22}\}$ for W, the homomorphism π_W is*

$$\pi_W \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad - bc} \begin{pmatrix} a^2 & -b^2 & -2ab \\ -c^2 & d^2 & 2dc \\ -ac & bd & ad + bc \end{pmatrix}.$$

The matrix on the right has determinant equal to 1, so we actually have

$$\overline{\pi_W} \colon PGL(2, F) \hookrightarrow SO(W).$$

(5) *The image of $\overline{\pi_W}$ is equal to $SO(W)$.*

Most of this proposition can be generalized from 2×2 matrices to $n \times n$ matrices without difficulty: we get a natural quadratic form on the $n^2 - 1$-dimensional vector space W_n of matrices of trace zero, and an injective group homomorphism

$$\overline{\pi_W} \colon PGL(n, F) \hookrightarrow SO(W_n). \tag{7}$$

What fails is only the very last step: this homomorphism is not surjective if $n \geq 3$.

Proof. That π_V is a homomorphism to linear transformations on the space of matrices is very easy; the main point is to check that it respects the bilinear form B. If X and Y are 2×2 matrices, then

$$\begin{aligned} B(\pi_V(g)X, \pi_V(g)Y) &= B(gXg^{-1}, gYg^{-1}) \\ &= \operatorname{tr} gXg^{-1}gYg^{-1} \\ &= \operatorname{tr} g(XY)g^{-1}. \end{aligned}$$

Now use the fact that $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, applied to the matrices $A = gXY$ and $B = g^{-1}$. We get

$$= \operatorname{tr} g^{-1}gXY = \operatorname{tr}(XY) = B(X, Y).$$

This shows that $\pi_V(g)$ belongs to $O(V)$, proving (1). Part (2) is very easy.

For part (3), the kernel of π_V consists of all invertible matrices that commute with all matrices. These are precisely the invertible scalar matrices. Since everything commutes with the identity matrix, commuting with all matrices is exactly the same as commuting with all trace zero matrices (cf. (5)(f)); so $\ker \pi_V = \ker \pi_W$. This is (3).

Part (4) explicitly computes the map $X \to gXg^{-1}$. The first step is the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

To compute the first column on the right in (4), we have to perform the multiplication

$$\frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

and then express the result as a linear combination of e_{12}, e_{21}, and $e_{11} - e_{22}$. I will leave the verifications to you.

The determinant of the 3×3 matrix in (4) is clearly a polynomial of degree 6 in a, b, c, and d, divided by $(ad - bc)^3$ (coming from the scalar factor in front). You can compute this quotient and find that it's identically 1; but here is a non-computational argument that it had to come out that way. We have a rational function of a, b, c, and d. The rational function has integer coefficients in the numerator and denominator, and doesn't depend on the field F. Because an orthogonal matrix must have determinant ± 1, this rational function can take only the values $+1$ and -1. In case F is infinite, this forces the rational function to be equal to $+1$ or to -1. When $g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ the right side is clearly the identity matrix, so the constant has to be $+1$. This proves (4).

Part (5) is the hard part. The idea is to reduce to studying the stabilizer of a special line in W, and there to write everything explicitly. Here's the reduction step.

Lemma 8. *In the setting of Proposition 6, suppose that $X \in W$ is a non-zero matrix such that $B(X, X) = 0$. Then there is a matrix $g \in SL(2, F)$ and a non-zero scalar a such that*

$$\pi_W(g)e_{12} = a^{-1}X.$$

I'll give the proof in a moment. Now we need to study the line $[e_{12}]$ in the projective space of W.

Lemma 9. *In the setting of Proposition 6, consider the subgroup*

$$P = \{T \in O(W) \mid T[e_{12}] = [e_{12}]\},$$

the stabilizer in $O(W)$ of the line through e_{12}.

(1) *In the basis $\{e_{12}, e_{21}, e_{11} - e_{22}\}$ for W, the group P is*

$$P = \left\{ \begin{pmatrix} k & -ky^2 & -2\epsilon ky \\ 0 & k^{-1} & 0 \\ 0 & y & \epsilon \end{pmatrix} \mid k \in F^\times, y \in F, \epsilon = \pm 1 \right\}.$$

Here ϵ is equal to the determinant of the matrix; so the matrix belongs to $SO(W)$ if and only if $\epsilon = 1$.

(2) *In the setting of Proposition 6(4), the matrix $\pi_W \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belongs to P if and only if $c = 0$. For such matrices, we have*

$$\pi_W \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a/d & -b^2/ad & -2b/d \\ 0 & d/a & 0 \\ 0 & b/a & 1 \end{pmatrix}.$$

(3) *We have*

$$\pi_W(GL(2, F)) \cap P = SO(W) \cap P.$$

For this result also I postpone the proof for a moment.

We now return to the proof of Proposition 6(5). So suppose $T \in SO(W)$. The vector $e_{12} \in W$ is non-zero, but $B(e_{12}, e_{12}) = 0$. It follows that $X = TW$ is a non-zero vector such that $B(X, X) = 0$. By Lemma 8, there is a $g \in SL(2, F)$ so that

$$[\pi_W(g)e_{12}] = [Te_{12}].$$

(The notation means equality of the lines through $\pi_W(g)e_{12}$ and Te_{12}.) Therefore $\pi_W(g^{-1})T \in P \cap SO(W)$. By Lemma 9, there is an $h \in GL(2, F)$ so that

$$\pi_W(g^{-1})T = \pi_W(h).$$

Therefore $T = \pi_W(gh)$, as we wished to show. $\square$

Proof of Lemma 8. By hypothesis

$$X = \begin{pmatrix} a & b \\ c & -a \end{pmatrix},$$

with a, b, and c not all zero. We calculate

$$X^2 = \begin{pmatrix} a^2 + bc & 0 \\ 0 & a^2 + bc \end{pmatrix}$$

$$0 = B(X, X) = \operatorname{tr} X^2 = 2(a^2 + bc).$$

Since the characteristic of F is not 2, this means that $a^2 + bc = 0$, and therefore (by the first calculation) that $X^2 = 0$. Since X is not zero, there is some vector v so that $Xv \neq 0$. Furthermore $X(Xv) = X^2 v = 0$, so Xv cannot be a multiple of v; so for any $a \in F^\times$, the pair $\{Xv, av\}$ is a basis of F^2. In this basis, the matrix of X is $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = ae_{12}$. Let g_a be the change of basis matrix relating the standard basis of F^2 to $\{Xv, av\}$: that is, the matrix whose columns are Xv and av. Then

$$g_a^{-1} X g_a = ae_{12};$$

equivalently, $\pi_W(g_a)e_{12} = a^{-1}X$. Changing the constant a scales the second column of g_a, and so scales $\det(g_a)$; so for an appropriate choice of a, we have $g_a \in SL(2, F)$, as we wished to show. $\square$

Proof of Lemma 9. Part (1) is analogous to Proposition 12 of the notes on the symplectic group; I will prove something more general for orthogonal groups in Proposition xx below. For part (2), the first assertion is clear from comparing Proposition 6(4) to the formula in part (1). The formula for $\pi_W \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is just a specialization of Proposition 6(4). Part (3) is now clear. $\square$

Corollary 10. *Suppose that W_0 is a three-dimensional vector space over a field F of characteristic not 2. Suppose B_0 is a symmetric non-degenerate bilinear form on W_0, and suppose that W_0 contains at least one non-zero vector u with $B_0(u, u) = 0$.*

(1) *The special orthogonal group $SO(W_0)$ is naturally isomorphic to $PGL(2, F)$.*
(2) *The image of $PSL(2, F)$ under this isomorphism is a normal subgroup that we will call $\Omega(W_0)$ of $SO(W_0)$, equal to the commutator subgroup of $SO(W_0)$.*
(3) *There is a natural isomorphism*

$$SO(W_0)/\Omega(W_0) \to F^\times/(F^\times)^2.$$

(4) *The group $\Omega(W_0)$ is simple as long as $F \neq \mathbb{F}_3$.*

Proof. From the existence of a vector of length 0, one can get in W_0 a hyperbolic plane H_0 in W_0, and then an orthogonal decomposition $W_0 = H_0 \oplus H_0^\perp$. Because W_0 is three-dimensional, $H_0^\perp = \langle w_0 \rangle$ is a line. Because B_0 is assumed non-degenerate, the vector w_0 must have non-zero length: $B_0(w_0, w_0) = a \neq 0$. Now let $B_0' = (2/a) \cdot B_0$. This is another symmetric bilinear form on W_0, defining exactly the same orthogonal group. We have $B_0'(w, w) = 2$, so with respect to B_0', W_0 is the orthogonal direct sum of a hyperbolic plane and the span of a vector of length 2. By (5)(g), (W_0, B_0') is equivalent to the pair (W, B_W) of (5). Therefore $O(W) \simeq O(W_0)$. In Proposition 6 we proved that $SO(W)$ is isomorphic to $PGL(2, F)$, so this result is inherited by the isomorphic group $SO(W_0)$. This proves (1). Part (2) is a consequence of the fact that $SL(2, F)$ is the commutator subgroup of $GL(2, F)$. Part (3) follows from equation (4)(a) above. The simplicity of $\Omega(W)$ is just the simplicity of $PSL(2, F)$. $\square$

That's a pretty complete account of Ω in the case of three-dimensional orthogonal spaces. In order to get going in higher dimensions, we need a little machinery.

For the balance of this paper, we fix an n-dimensional vector space V over a field F, and a non-degenerate symmetric bilinear form B on B. We will assume that

$$\text{(11)(a)} \qquad \dim V \geq 3, \qquad \operatorname{char} F \neq 2.$$

In addition, we will assume that

$$\text{(11)(b)} \qquad V \text{ contains a non-zero vector } u \text{ such that } B(u,u) = 0.$$

In this setting (which generalizes that of Corollary 10), we are going to construct a normal subgroup $\Omega(V)$ of the orthogonal group $O(V)$. In the text starting on page 53, the group that I've written N_u below is called K_u. The letter N seems to me to fit much better with standard terminology.

Proposition 12. *In the setting of (11), suppose that $y \in \langle u \rangle^\perp$ is a vector orthogonal to the isotropic vector u. Define a linear transformation $\rho_{u,y}$ on V by*

$$\rho_{u,y}(x) = x - B(x,u)y + B(x,y)u - \frac{1}{2}B(y,y)B(x,u)u.$$

(1) *The linear transformation $\rho_{u,y}$ belongs to $SO(V)$. If $a \in F$ is a non-zero scalar, then $\rho_{au,y} = \rho_{u,ay}$.*
(2) *We have $\rho_{u,y}\rho_{u,z} = \rho_{u,y+z}$.*
(3) *We have $\rho_{u,y} = I$ (the identity map on V) if and only if $y \in \langle u \rangle$.*
(4) *The collection of linear transformations*

$$N_u = \{\rho_{u,y} \mid y \in \langle u \rangle^\perp\}$$

is an abelian group, isomorphic to the additive group of the quotient vector space

$$W = \langle u \rangle^\perp / \langle u \rangle$$

(which has dimension $n-2$ over F).
(5) *The vector space W carries a natural nondegenerate symmetric bilinear form B_W: if y and z in $\langle u \rangle^\perp$ are representatives for $\overline{y}$ and $\overline{z}$ in W, then*

$$B_W(\overline{y}, \overline{z}) = B(y,z).$$

(6) *Write P_u for the stabilizer in $O(V)$ of the line $[u]$. Each element $p \in P_u$ acts naturally on the vector space W, and we get in this way a surjective group homomorphism*

$$m \colon P_u \to O(W).$$

Similarly, p sends u to a multiple of itself, defining a surjective group homomorphism

$$a \colon P_u \to F^\times, \qquad p \cdot u = a(p)u.$$

(7) *If $y \in \langle u \rangle^\perp$ and $p \in P_u$, then*

$$p\rho_{u,y}p^{-1} = \rho_{a(p)u, m(p)y} = \rho_{u, a(p)m(p)y}.$$

In particular, N_u is a normal subgroup of P_u.
(8) *The quotient group P_u/N_u is isomorphic (by the homomorphism $a \times m$) to the product $F^\times \times O(W)$. Intersecting with the special orthogonal group gives*

$$(SO(V) \cap P_u)/N_u \simeq F^\times \times SO(W).$$

(9) *The group N_u is contained in the commutator subgroup of $SO(V) \cap P_u$.*

The most obvious question raised by Proposition 12 is this: where did the elements $\rho_{u,y}$ come from? Perhaps the simplest answer to this question may be found in the reformulation at equation (18)(d) below. There I have chosen a second vector v making a hyperbolic pair with u. The idea is to invent an orthogonal transformation ρ that fixes u. It must therefore carry v to some other vector whose pairing with u is equal to 1. This other vector must be v, plus some multiple of u, plus something orthogonal to u and v. So pick first the something orthogonal to u and v, and call it $-y$. So far we're forced to write

$$\rho(u) = u, \qquad \rho(v) = v - y - au.$$

The requirement that $\rho(v)$ have length 0 forces $a = -B(y,y)/2$. This shows that the middle formula in (18)(d) is forced on us by the requirement that ρ be orthogonal. The last formula is just the simplest possible extension of ρ to all of V.

Before embarking on the proof of this proposition, let us see how it leads to the group $\Omega(V)$.

Definition 13. In the setting of (11) and Proposition 12, we define

$$\Omega(V) = \text{group generated by all } N_u,\ u \text{ isotropic in } V.$$

By Proposition 12(1), $\Omega(V)$ is a subgroup of $SO(V)$.

The definition of N_u makes it almost obvious that for any $\tau \in O(V)$, we have

$$\tau N_u \tau^{-1} = N_{\tau u}. \tag{14)(a}$$

From this it follows at once that

(14)(b) $\qquad \Omega(V)$ is a normal subgroup of $O(V)$ and of $SO(V)$.

As a consequence of Proposition 12(9), we have

(14)(b) $\qquad \Omega(V)$ is contained in the commutator subgroup of $SO(V)$.

Proof of Proposition 12. The ideas is to imitate the proof of Proposition 12 in the notes on the symplectic group: to construct lots of elements of P_u by hand, and see how to compose them. We can start without doing any work. For (1), we have to show that if x_1 and x_2 are in V, then

$$B(\rho_{u,y}(x_1), \rho_{u,y}(x_2)) = B(x_1, x_2). \tag{15}$$

According to the definition,

$$\rho_{u,y}(x_i) = x_i - B(x_i,u)y + [B(x_i,y) - \frac{1}{2}B(y,y)B(x_i,u)]u,$$

a sum of three vectors. So the left side of (15) expands (using bilinearity) as a sum of nine terms. One is equal to the right side, and four are zero because

$B(u,u) = B(u,y) = 0$. So we need to show that the sum of the remaining four terms is equal to zero. This is

$$\begin{aligned}
&- B(x_2,u)B(x_1,y) + [B(x_2,y) - \frac{1}{2}B(y,y)B(x_2,u)]B(x_1,u) \\
&- B(x_1,u)B(x_2,y) + [B(x_1,y) - \frac{1}{2}B(y,y)B(x_1,u)]B(x_2,u) \\
&+ B(x_1,u)B(x_2,u)B(y,y).
\end{aligned}$$

This sum is indeed equal to zero, proving that $\rho_{u,y} \in O(V)$.

Next we will show that $\rho_{u,y}$ has determinant equal to 1. In fact we will prove more. A linear transformation T on a finite-dimensional vector space V is called *unipotent* if $(T-I)^m = 0$ for some positive integer m. It is a nice exercise in linear algebra to prove that any unipotent linear transformation must have determinant one. (A cheap way to prove this involves noticing that all the eigenvalues of T must be equal to 1; but you can probably think of something nicer.) So it is enough to prove that

$$(\rho_{u,y} - I)^3 = 0. \tag{16)(a}$$

To prove this, notice first that

$$(\rho_{u,y} - I)(x) = -B(x,u)y + [B(x,y) - \frac{1}{2}B(y,y)B(x,u)]u, \tag{16)(b}$$

a linear combination of u and y. So it is enough to prove that

$$(\rho_{u,y} - I)(y) \in \langle u \rangle, (\rho_{u,y} - I)(u) = 0. \tag{16)(c}$$

(For then applying $(\rho_{u,y} - I)$ once puts us in the span of u and y; applying it a second time puts us in the span of u; and applying it a third time gives zero.) The first assertion of (16)(c) is clear from (16)(a), since $B(y,u) = 0$. The second is also clear from (16)(a), since $B(u,u) = B(u,y) = 0$. This proves that $\rho_{u,y}$ is unipotent, and therefore of determinant 1. The last formula in (1) is an immediate consequence of the definition.

The identity in (2) follows by a straightforward calculation from the definition, which I will omit.

For (3), suppose first that $y = au$. According to (16)(b),

$$(\rho_{u,au} - I)(x) = -B(x,u)(au) + [B(x,au) - \frac{1}{2}B(au,au)B(x,u)]u.$$

Since $B(u,u) = 0$, this simplifies to

$$(\rho_{u,au} - I)(x) = -B(x,u)(au) + B(x,au)u,$$

which is zero by since B is bilinear. Next, suppose that y is not a multiple of u. Since B is non-degenerate, we can find $x \in V$ with $B(x,u) \neq 0$. Formula (16)(b) therefore says

$$(\rho_{u,au} - I)(x) = \text{non-zero multiple of } y \text{ plus multiple of } u,$$

which cannot be zero since y is not a multiple of u.

Part (4) is an abstract restatement of (3). Parts (5)–(7) are formal and easy, except for the surjectivity of the homomorphisms a and m. To prove that, and to prepare for the proof of (8), we will use a little more structure. We have essentially already said that the nondegeneracy of B allows us to choose a vector v' so that $B(u, v') = 1$. If we define

$$v = v' - \frac{1}{2}B(v', v')u,$$

then we get

(17)(a) $$B(v, v) = B(u, u) = 0, \qquad B(u, v) = 1;$$

that is, u and v are a standard basis of a hyperbolic plane $H \subset V$. The vector v is *not* uniquely determined by u. It's an entertaining exercise to prove that the collection of all possible choices of v is equal to

$$\{\rho_{u,y}(v) \mid y \in \langle u\rangle^\perp\}.$$

Write

(17)(b) $$W_0 = H^\perp = \{w \in V \mid B(w, u) = B(w, v) = 0.$$

According to Proposition 2.9 in the text,

(17)(c) $$V = H \oplus W_0,$$

an orthogonal direct sum decomposition. The form B_{W_0} (the restriction of B to W_0 is non-degenerate. It's very easy to see that

$$\langle u\rangle^\perp = W_0 \oplus \langle u\rangle,$$

so the quotient vector space

(17)(d) $$W = \langle u\rangle^\perp / \langle u\rangle \simeq W_0.$$

This isomorphism respects the bilinear forms, so $O(W_0) \simeq O(W)$.

Using the structure in (17) just as we did in the symplectic group notes, we can now define some elements of the stabilizer P_u in $O(V)$ of the line $[u]$. Just as in that case, we can define these elements by saying what they do to u, what they do to v, and what they do to elements $w \in W_0$.

For any $k \in F^\times$, define

(18)(a) $$a_k(u) = ku, \qquad a_k(v) = k^{-1}v, \qquad a_k(w) = w \quad (w \in W_0).$$

It's easy to check that a_k belongs to P_u. For any $\tau \in O(W_0)$, define

(18)(b) $$m_\tau(u) = u, \qquad m_\tau(v) = v, \qquad m_tau(w) = \tau(w) \quad (w \in W_0).$$

Finally, define

(18)(c) $$A = \{a_k \mid k \in F^\times\}, \qquad M = \{m_\tau \mid \tau \in O(W_0)\}$$

These are commuting subgroups of P_u, isomorphic to $F^\times$ and $SO(W_0)$ respectively.

The remaining elements we need from P_u are the elements $\rho_{u,y}$ of Proposition 12. In that setting we had $y \in \langle u\rangle^\perp$, and y was determined only up to a multiple of u. Now its convenient to regard y as a uniquely determined element of W_0. In this case we have

(18)(d) $$\rho_{u,y}(u) = u, \quad \rho_{u,y}(v) = v - y - \frac{1}{2}B(y, y)u, \quad \rho_{u,y}(w) = w - B(w, y)u$$

for any $w \in W_0$.

Lemma 19. *In the notation of (18), every element $p \in P_u$ has a unique representation as a product*

$$p = m_\tau a_k \rho_{u,y} \qquad (k \in F^\times, \tau \in O(W_0), y \in W_0.$$

In terms of the homomorphisms defined in Proposition 12(6), and the identification $O(W) \simeq O(W_0)$, we have

$$a(p) = k, \qquad m(p) = \tau.$$

In particular, the homomorphism

$$a \times m \colon P_u \to F^\times \times SO(W)$$

is surjective, with kernel equal to N_u.

The proof is exactly parallel to that of Proposition 12 in the symplectic group notes, so I'll omit it. Parts (6) and (8) of Proposition 12 follow.

For part (9), we compute using (7) for $p \in P_u$

$$\rho_{u,y} p \rho_{u,y}^{-1} p^{-1} = \rho_{u,y} \rho_{u,a(p)m(p)y}^{-1} = \rho_{u,y-a(p)m(p)y}$$

Choose p so that $a(p) \neq 1$ and $m(p) = 1$, as is possible by (8). In this case $p \in SO(V)$, so we see that $\rho_{u,(1-a(p))y}$ is a commutator in $SO(V) \cap P_u$. Since $a(p) \neq 1$, this includes all of N_u. $\square$