Orthogonal groups

Matevž Miščič

These notes are based on Lecture 5 of Nick Gill's course Finite Classical Groups [2], Peter Cameron's Notes on Classical Groups [1], and the monograph by Kleidman and Liebeck [3].

1 Orthogonal groups

Let Q be a non-degenerate quadratic form on a vector space V of dimension n over a finite field $\mathbf{F}_q$. We denote the associated symmetric bilinear form by β. Recall that it is defined by $\beta(u,v) = Q(u+v) - Q(u) - Q(v)$.

In the lecture about forms we have seen that V is an orthogonal direct sum of hyperbolic lines and an anisotropic subspace. The dimension of the anisotropic subspace can be either 0, 1 or 2. We thus have the following possible bases for V:

1. $B = \{v_1, w_1, \ldots, v_r, w_r\}$, where (v_i, w_i) are hyperbolic pairs.
2. $B = \{v_1, w_1, \ldots, v_r, w_r, u\}$, where (v_i, w_i) are hyperbolic pairs and u is an anisotropic vector orthogonal to all other basis vectors.
3. $B = \{v_1, w_1, \ldots, v_r, w_r, u, u'\}$, where (v_i, w_i) are hyperbolic pairs and $\langle u, u' \rangle$ is an anisotropic subspace orthogonal to $\langle v_1, w_1, \ldots, v_r, w_r \rangle$.

Moreover, in the second case we can prescribe that $Q(u) = 1$ for q even and that $Q(u) = 1$ or $Q(u) = \zeta$ for q odd, where ζ is a non-square in $\mathbf{F}_q$. In the third case we can prescribe that $Q(u) = 1$, $Q(u') = \zeta$ and $\beta(u, u') = 0$, where $x^2 + x + \zeta$ is irreducible over $\mathbf{F}_q$.

Definition 1.1. Define $\mathrm{O}(Q)$ to be the group of all isometries of Q and $\mathrm{SO}(Q)$ to be the subgroup of $\mathrm{O}(Q)$ consisting of all isometries with determinant 1.

As always, we define projective versions of these groups by factoring out their intersection with the group of scalar transformations.

Note that in the second case, the formed space (V, Q) might not be unique up to isometry, since we can have $Q(u) = 1$ or $Q(u) = \zeta$. However, both spaces have the same isometry groups. We thus also write $\mathrm{O}^+_{2r}(q)$, $\mathrm{O}_{2r+1}(q)$ and $\mathrm{O}^-_{2r+2}(q)$ for the isometry groups of the three types of formed spaces. We use analogous notation for the special and for their projective versions.

2 Reflections

All classical groups we have seen so far were generated by transvections. This is not the case for orthogonal groups in general, but they are generated by reflections.

Definition 2.1. Let $v \in V$ be non-singular. The *reflection* in v is the transformation

$$r_v \colon x \mapsto x - Q(v)^{-1}\beta(x, v)v.$$

In odd characteristic the reflection r_v maps v to $-v$ and fixes all vectors orthogonal to v, so its determinant is -1. Geometrically one can think of it as a reflection over the hyperplane $v^\perp$. In even characteristic r_v still fixes the hyperplane $v^\perp$, but vectors not perpendicular to v get translated in the direction of v, so r_v is a transvection and has determinant 1.

Proposition 2.2. *If $n \geq 5$ the group $\mathrm{O}(Q)$ is generated by reflections.*

As a consequence we see that any isometry in $\mathrm{O}(Q)$ has determinant either 1 or -1. The group $\mathrm{SO}(Q)$ has index 2 in $\mathrm{O}(Q)$ in odd characteristic and is equal to $\mathrm{O}(Q)$ in even characteristic.

3 The derived subgroup

Here we define the group $\Omega(Q)$.

Proposition 3.1. *If $n \geq 5$, then $\mathrm{SO}(Q)$ has a unique subgroup of index 2.*

Using the proposition above we can define $\Omega(Q)$ to be the unique subgroup of index 2 in $\mathrm{SO}(Q)$. In most cases $\Omega(Q)$ is the derived subgroup of $\mathrm{SO}(Q)$, for example this always holds for $n \geq 6$. However, we will need a better understanding of which elements of $\mathrm{SO}(Q)$ are in $\Omega(Q)$. We split two cases:

1. Suppose that q is even. It turns out that the subgroup of $\mathrm{SO}(Q)$ of all elements that are products of an even number of reflections is a subgroup of index 2 in $\mathrm{SO}(Q)$, so it must be equal to $\Omega(Q)$.

2. Suppose now that q is odd. Then the group $\mathbf{F}^*/(\mathbf{F}^*)^2$ has order two. We define the *spinor norm* $\theta \colon \mathrm{SO}(Q) \to \mathbf{F}^*/(\mathbf{F}^*)^2$ as follows. By Proposition 2.2, any element $g \in \mathrm{SO}(Q)$ can be written as a product of reflections $g = r_{v_1} \cdots r_{v_k}$. We then define

   $$\theta(g) = Q(v_1) \cdots Q(v_k)(\mathbf{F}^*)^2.$$

   It turns out that θ is well defined group epimorphism. The kernel of θ is thus a subgroup of index 2 in $\mathrm{SO}(Q)$, so it must be equal to $\Omega(Q)$.

4 The action on the polar space

Orthogonal groups act naturally on the set of points of the polar space associated to Q. These points are totally isotropic 1-dimensional subspaces of V.

Lemma 4.1. *The kernel of the action of $\Omega(Q)$ on the points of the polar space is the group of scalar transformations.*

Proof. Let $g \in \Omega(Q)$ be in the kernel of the action and write $V = W \oplus U$ as an orthogonal direct sum of the hyperbolic part W and the anisotropic part U. The same argument as in the case of unitary groups shows that there is a scalar λ such that $gw = \lambda w$ for all $w \in W$. It remains to show that any vector $u \in U$ also gets multiplied by λ. Since W is invariant under g and g preserves Q and β, $U = W^\perp$ is also invariant. Let $u \in U$ be non-zero. A simple calculation shows that the vector $z = v_1 - Q(u)w_1 + u$ is isotropic and thus $gz = \mu z$ for some scalar μ. We have

$$\mu v_1 - \mu Q(u) w_1 + \mu u = \mu z = gz = \lambda v_1 - \lambda Q(u) w_1 + gu.$$

Since $\mu u, gu \in U$, we have $\mu = \lambda$ and $gu = \lambda u$, and thus g is a scalar transformation. □

We now show that the action is transitive. The following remark will give us anisotropic vectors, that we will need to define reflections.

Remark 4.2. If $\dim V \geq 3$, there exists a hyperbolic pair (v, w) in V. We have $Q(v + \lambda w) = \lambda$, so $Q \colon V \to \mathbf{F}_q$ surjective.

Lemma 4.3. *Assume $n \geq 5$. Then the group $\Omega(Q)$ acts transitively on the set of points of the polar space.*

Proof. Let $\langle u \rangle$ and $\langle v \rangle$ be two points of the polar space. By Witt's lemma, there is an isometry $g \in \mathrm{O}(Q)$ such that $g(u) = v$.

Assume that the characteristic is 2. Then $\Omega(Q)$ is a subgroup of $\mathrm{O}(Q)$ of elements that are products of an even number of reflections. Take any anisotropic vector $w \in v^\perp$. Then one of $g, r_w g$ belongs to $\Omega(Q)$ and we are done.

Assume the characteristic is odd. The quadratic form Q induces a non-degenerate quadratic form on the space $v^\perp / v$ of dimension $n - 2 \geq 3$. Thus, by remark 4.2, there are anisotropic vectors $w_1, w_2 \in v^\perp$ such that $Q(w_1)$ is a square and $Q(w_2)$ is not a square. If necessary, we can compose g with r_{w_2} to make its spinor norm a square. Then we can compose it with r_{w_1} if necessary to make its determinant 1. This concludes the proof. □

Next we show primitivity. We will often need the following trick to adjust the spinor norm.

Lemma 4.4. *Let $\langle u\rangle, \langle v\rangle$ be two points, such that $\langle u, v\rangle$ is a hyperbolic line. Then there is an element $g \in \mathrm{SO}(Q)$ that fixes the points $\langle u\rangle, \langle v\rangle$ and has non-square spinor norm. Moreover, we can choose g to act trivially on $\langle u, v\rangle^{\perp}$.*

Proof. We can assume that (u, v) is a hyperbolic pair. Define $w_1 = u + v$ and $w_2 = \lambda u + v$ and let $g = r_{w_2} r_{w_1}$. Note that $Q(w_1) = 1$ and $Q(w_2) = \lambda$. Clearly $\det g = 1$ and we have

$$r_{w_1}(u) = u - w_1 = -v$$
$$r_{w_2}(v) = v - w_2 = -\lambda u$$

so g fixes both points. Its spinor norm is λ. □

Proposition 4.5. *Assume $n \geq 5$. Then the group $\Omega(Q)$ acts primitively on the set of points of the polar space.*

Proof. We begin by proving that the permutation rank is at most 3. Consider the induced action on pairs. By Lemma 4.3, the diagonal is one orbit.

We claim that all pairs of points that span a hyperbolic line are in the same orbit. Let u, v and u', v' be two hyperbolic pairs. By Witt's lemma, there is an isometry $g \in \mathrm{O}(Q)$ such that $g(u) = u'$ and $g(v) = v'$. Since $\dim(\langle u', v'\rangle^{\perp}) = n - 2 \geq 3$ and Q is non-degenerate on $\langle u', v'\rangle^{\perp}$, there is an anisotropic vector w orthogonal to both u' and v' by remark 4.2. We can assume g is a product of an even number of reflections by composing it with r_w if necessary. In even characteristic we are done. In odd characteristic we use Lemma 4.4 to adjust the spinor norm of g if necessary, and we are done.

Finally, let u, v and u', v' be two pairs with $\langle u, v\rangle$ and $\langle u', v'\rangle$ totally isotropic. By Witt's lemma, there is an isometry $g \in \mathrm{O}(Q)$ such that $g(u) = u'$ and $g(v) = v'$. As before we can assume g is a product of an even number of reflections. In even characteristic we are done. In odd characteristic we can extend u' to a hyperbolic pair (u', x) by a vector $x \in (v')^{\perp}$. Then use Lemma 4.4 on the pair u', x to adjust the spinor norm of g if necessary, and we are done.

Now the proof continues as in the case for symplectic or unitary groups. □

5 Simplicity

The proof of simplicity of $\mathrm{P}\Omega(Q)$ is more complicated than the proofs for the other classical groups. We will need to define a special type of elements, called root elements, that will play a crucial role in the proof.

Definition 5.1. A *root element* is a transformation of the form

$$R_{u,v} \colon x \mapsto x + \beta(x, v)u - \beta(x, u)v - Q(v)\beta(x, u)u,$$

where $Q(u) = \beta(u, v) = 0$.

For a fixed $u \in V$ with $Q(u) = 0$ define

$$X_u = \langle R_{u,v} \mid v \in u^\perp \rangle.$$

We will now briefly talk about the next steps in the proof of simplicity of $\Omega(Q)$.

1. An easy calculation shows that the map $\phi\colon u^\perp \to X_u$ given by $\phi(v) = R_{u,v}$ is a group epimorphism with kernel $\langle u \rangle$. It follows that $X_u \cong u^\perp / \langle u \rangle$, so it is abelian.
2. The group X_u is normal in the stabilizer of the point $\langle u \rangle$.
3. The group $\Omega(Q)$ is generated by the groups X_u for $u \in V$ with $Q(u) = 0$. It follows that the normal closure of X_u is the whole group $\Omega(Q)$.
4. Every root element is a commutator, so $\Omega(Q)$ is a perfect group.

We are now in position to apply Iwasawa's criterion to conclude that the groups $\mathrm{P}\Omega(Q)$ are simple.

Theorem 5.2. *Assume $n \geq 5$. Then the group $\mathrm{P}\Omega(Q)$ is simple.*

References

[1] Peter J. Cameron. "Notes on Classical Groups". Lecture notes, Queen Mary and Westfield College, London. 2000.

[2] Nick Gill. "Finite Classical Groups". `https://nickpgill.github.io/finite-classical-groups-2025`. Lecture notes for the London Taught Course Centre (LTCC). 2025.

[3] Peter Kleidman and Martin Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Mathematical Society Lecture Note Series 129. Cambridge University Press, 1990.