10. Unitary groups

Throughout this section β is a non-degenerate σ-sesquilinear form on a n-dimensional vector space V over a finite field $k = \mathbb{F}_{q^2}$; write k_0 for the unique subfield $\mathbb{F}_q$.

We assume that $\sigma^2 = 1 \neq \sigma$ and observe that k_0 is the fixed field of σ and recall the *trace* and *norm* functions:

$$\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q,\ x \mapsto x + x^\sigma;$$
$$\mathrm{N} : \mathbb{F}_{q^2} \to \mathbb{F}_q,\ x \mapsto x \cdot x^\sigma.$$

By (E81) these functions are surjective.

Recall that we have a *unitary basis*, as follows. Note that, for $i = 1, \dots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs.

($\mathbf{U_{2r}}$) with basis $\{v_1, w_1, \dots, v_r, w_r\}$.
($\mathbf{u_{2r+1}}$) with basis $\{v_1, w_1, \dots, v_r, w_r, u\}$ where $\langle u \rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \dots, v_r, w_r \rangle$.

In fact it will be easier to work with an orthonormal basis:

Lemma 55. *There is a basis $\{v_1, \dots, v_n\}$ of V such that $\beta(v_i, v_j) = \delta_{ij}$.*

Proof. let v_1 be a non-isotropic vector. Since N is surjective we can normalize so that $\beta(v_1, v_1) = 1$. Now we contine in $\langle v_1 \rangle^\perp$, which is a $n-1$-dimensional vector space on which β is non-degenerate. □

Note that, writing vectors with respect to an orthonormal basis, β has the form

herm (16) $$\beta((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{i=1}^{n} x_i y_i^\sigma.$$

The presence of a unitary basis (or, indeed, of an orthonormal basis) implies the following facts, which we leave as an exercise.

> **(E98)** *Let β_1 and β_2 be non-degenerate σ-Hermitian forms defined on a n-dimensional vector space V over the field $k = \mathbb{F}_{q^2}$. Then* $\mathrm{Isom}(\beta_1)$ *and* $\mathrm{Isom}(\beta_2)$ *(resp.* $\mathrm{Sim}(\beta_1)$ *and* $\mathrm{Sim}(\beta_2)$*) are conjugate subgroups of* $\mathrm{GL}_n(k)$*. Furthermore* $\mathrm{SemiSim}(\beta_1)$ *and* $\mathrm{SemiSim}(\beta_2)$ *are conjugate subgroups of* $\Gamma\mathrm{L}_n(k)$*.*

These facts allow us to make the following definitions. We write K for the set of invertible scalar matrices over k.

- $\mathrm{GU}_n(k)$ is the isometry group of β;
- $\mathrm{SU}_n(k)$ is the special isometry group of β, i.e. it equals $\mathrm{GU}_n(k) \cap \mathrm{SL}_n(k)$.
- $\Gamma\mathrm{U}_n(k)$ is the semi-similarity group of β;
- $\mathrm{PSU}_n(k) = \mathrm{SU}_n(k)/(K \cap \mathrm{SU}_n(k))$;
- $\mathrm{PGU}_n(k) = \mathrm{GU}_n(k)/(K \cap \mathrm{GU}_n(k))$;
- $\mathrm{P}\Gamma\mathrm{U}_n(k) = \Gamma\mathrm{U}_n(k)/K$

If $k = \mathbb{F}_q$ we may write $\mathrm{Sp}_{2r}(q)$ for $\mathrm{Sp}_{2r}(k)$ and likewise for the other groups.

Warning:

- Recall that $\mathrm{GSp}_{2r}(k)$ was the set of similarities of an alternating form, whereas here $\mathrm{GU}_n(k)$ is the set of isometries of a Hermitian form. Also, in the symplectic situation we didn't need to distinguish between the special isometry group and the full isometry group, since all isometries were special. That is not the case here.
- For all classical groups over the finite field $k = \mathbb{F}_q$, **apart from the unitary ones**, any name $\mathrm{X}_n(k)$ has a synonym given by $\mathrm{X}_n(q)$. In the unitary case, though, the group can

only be defined over a field of square order; thus if $\mathrm{X}_n(k)$ is one of the listed unitary groups defined over the field $k = \mathbb{F}_{q^2}$, then we use the synonym $\mathrm{X}_n(q)$.
- While we're mentioning synonyms, note that the notation $\mathrm{U}_n(q)$ is used in various places, but its meaning varies. Sometimes it is a synonym for $\mathrm{GU}_n(k)$, at other times it means $\mathrm{PSU}_n(k)$.

Our next lemma throws up another significant difference to the symplectic case - there all vectors are isotropic, while in the unitary case that is far from true.

ry count **Lemma 56.** *The number of non-zero isotropic vectors in V is*

$$x_n := (q^n - (-1)^n)(q^{n-1} - (-1)^{n-1}).$$

The number of hyperbolic pairs is $x_n \cdot q^{2n-3}$.

Proof. We use an orthonormal basis, and then counting isotropic vectors is equivalent to counting solutions of $\sum_{i=1}^n \alpha_i \alpha_i^\sigma = 0$.
- If $\alpha_1 = 0$, then we obtain x_{n-1} such solutions;
- If $\alpha_1 \neq 0$, then $\alpha_1^{q+1} = -\sum_{i=2}^n \alpha_i^{q+1}$. If we fix the left hand side, there are $q+1$ choices for α_1 (since k^* is cyclic of order q^2-1). On the other hand there are $((q^2)^{n-1} - 1) - x_{n-1}$ choices for the right hand side, and we obtain $(q+1)(q^{2n-2} - 1 - x_{n-1})$ solutions of this kind.

We conclude that $x_n = x_{n-1} + (q+1)(q^{2n-2} - 1 - x_{n-1})$ and, since $x_1 = 0$, the result follows.

Now consider hyperbolic pairs. Given v_1 we need to show that we can choose w_1 in q^{2n-3} ways. Observe that $v_1^\perp / \langle v_1 \rangle$ is a non-degenerate $(n-2)$-dimensional unitary space, so has x_{n-2} non-zero isotropic vectors. Thus there are $q^2 x_{n-2}$ isotropic vectors $\alpha v_1 + x$ in $v_1^\perp$ with $x \neq 0$, and therefore $q^2 x_{n-2} + q^2 - 1$ non-zero isotropic vectors in $v_1^\perp$ in total.

Our choice for w_1 must be a non-zero isotropic vector that is not in $v_1^\perp$ - there are, therefore $x_n - (q^2 x_{n-2} + q^2 - 1)$ of these. We must normalize to ensure that $\beta(v_1, w_1) = 0$ and we conclude that there are $\frac{1}{q^2-1}(q^2 x_{n-2} + q^2 - 1)$ possibilities for w_1. The result follows. □

Corollary 57.
- $|\mathrm{GU}_n(q)| = q^{\frac{1}{2}n(n-1)} \prod_{i=1}^n (q^i - (-1)^i)$.
- $|\mathrm{PGU}_n(q)| = |\mathrm{SU}_n(q)| = \frac{|\mathrm{GU}_n(q)|}{q+1}$.
- $\mathrm{PSU}_n(q)| = \frac{|\mathrm{SU}_n(q)|}{(n,q+1)}$.

Proof. The first identity follows immediately from the previous lemma, using the fact that $|\mathrm{GU}_1(q)| = q+1$.

For the second refer to (16) and note that the matrix λI lies in $\mathrm{GU}_n(q)$ if and only if $\lambda^{q+1} = 1$. This gives the identity for PGU. For SU observe that if $g \in \mathrm{GU}_n(q)$, then $\mathrm{N}(\det(g)) = 1$ and, since N is onto $\mathbb{F}_q^*$, the result follows.

For the third observe that $\lambda I \in \mathrm{SU}_n(q)$ if and only if $\lambda^{q+1} = \lambda^n = 1$. The result follows. □

10.1. **Unitary transvections.** Recall that a transvection is a linear map of the form

$$T_{f,a} : V \to V,\ v \mapsto v + (vf)a$$

where $f \in V^*$ and $a \in \ker(f)$. As in the symplectic case we would like to know which transvections lie in $\mathrm{GU}_n(k)$ - we call these *unitary transvections*. (Recall that transvections, by definition, have determinant 1, thus all unitary transvections lie in $\mathrm{SU}_n(k)$.)

ry trans **Lemma 58.** *The unitary transvections are*

$$T_{f,a} : v \mapsto v + \lambda \beta(v, a) a$$

where a is isotropic and $\mathrm{Tr}(\lambda) = 0$.

Proof. For $T_{f,a}$ to lie in $\mathrm{GU}_n(q)$ we require that

$$\beta(v+(vf)a, w+(wf)a) = \beta(v,w),\ \forall v,w\in V$$
$$\iff (wf)^\sigma\beta(v,a)+(vf)\beta(a,w)+(vf)(wf)^\sigma\beta(a,a)=0,\ \forall v,w\in V.$$

Taking $w=a$ we observe that then $(vf)\beta(a,a)=0$ for all v and so $\beta(a,a)=0$ and a is isotropic.

Now choose w so that $\beta(a,w)=-1$, and observe that then $vf=(wf)^\sigma\beta(v,a)$. But, letting $w=v$ such that $\beta(a,w)\in\mathbb{F}_q^*$ we see that

$$(wf)^\sigma\beta(w,a)=wf\beta(a,w)$$

and so $\mathrm{Tr}(wf)=\overline{(wf)}+wf=0$.

Thus all unitary transvections have the given form. It is easy to check that, conversely, all linear maps of the given form are indeed unitary transvections. □

e: su2

(E99*) *$\mathrm{SU}_2(q)\cong\mathrm{SL}_2(q)$ and, moreover, the action of $\mathrm{SU}_2(q)$ on the set of points of the associated polar space is isomorphic to the action of $\mathrm{SL}_2(q)$ on the set of points of $\mathrm{PG}_1(q)$.*

Lemma 59. *The action of $\mathrm{PSU}_n(q)$ on the points of the associated polar space is faithful, of permutation rank ≤ 3 and primitive.*

Proof. We make use of the existence of a unitary basis. Suppose $g\in\mathrm{SU}_n(q)$ fixes every point of the associated polar space. Let $(v_1,w_1),\dots,(v_r,w_r)$ be r mutually orthogonal hyperbolic pairs. Since v_i+v_j is isotropic, we conclude that g scales all vectors v_i by the same scalar, and similarly for all vectors w_i. In addition w_i-v_i is isotropic and we conclude that g scales v_i and w_i by the same scalar. This yields faithfulness when n is even. When n is odd, we observe that if u is orthogonal to $\langle v_i,w_i\rangle$ such that $\beta(u,u)=-2$, then $u+v_1+w_1$ is isotropic and so u is scaled by the same scalar as v_1 and w_1. We conclude that the action is faithful in this case also.

(E 99) implies that the action is primitive of rank 2 when $n=2$, thus we assume that $n\geq 3$. Witt's lemma implies that the action of $\mathrm{GU}_n(q)$ on the points of the associated polar space is transitive. To see that, given two points $\langle v\rangle$ and $\langle w\rangle$, there exists $g\in\mathrm{PSU}_n(q)$ such that $\langle v\rangle^g=\langle w\rangle$, one simply adjusts the determinant of a corresponding element in $\mathrm{GU}_n(q)$.

Suppose that, for $i=1,2$, $(\langle v_i\rangle,\langle w_i\rangle)$ are pairs of points such that $\beta(v_i,w_i)\neq 0$. We may assume, in fact, that $\beta(v_i,w_i)=1$ and so, by Witt's lemma, there exists an element of $\mathrm{GU}_n(q)$ that maps $\langle v_1,w_1\rangle$ to $\langle v_2,w_2\rangle$; indeed, since $\mathrm{SU}_2(q)\cong\mathrm{SL}_2(q)$, there exists an element of $\mathrm{GU}_n(q)$ that maps (v_1,w_1) to (v_2,w_2). As in the previous paragraph one can adjust the determinant so that the element lies in $\mathrm{SU}_n(q)$ and we conclude that all pairs $(\langle v_i\rangle,\langle w_i\rangle)$ which are not orthogonal lie in a single orbit of $\mathrm{PSU}_n(q)$.

Note that when $n=3$, all pairs $(\langle v_i\rangle,\langle w_i\rangle)$ are not orthogonal, and we conclude immediately that the permutation rank is equal to 2 (and hence the action is primitive). Assume from here on that $n>3$.

Suppose next that, for $i=1,2$, $(\langle v_i\rangle,\langle w_i\rangle)$ are pairs of points such that $\beta(v_i,w_i)=0$. Since $\mathrm{PSU}_n(q)$ is transitive on points, we can assume that $v_1=v_2$, and we simply write v for this element. There are two cases:

- Suppose that $W:=\langle v,w_1,w_2\rangle$ is totally isotropic. Then there exists $g\in\mathrm{SL}(W)<\mathrm{SU}_n(q)$ such that $\langle v\rangle^g=\langle v\rangle$ and $\langle w_1\rangle^g=\langle w_2\rangle$.
- Suppose that $W=\langle v,w_1,w_2\rangle$ is not totally isotropic, i.e. $\beta(w_1,w_2)\neq 0$ and $L:=\langle w_1,\rangle w_2$ is a hyperbolic plane. Then, by Witt's Lemma, there exists $g\in\mathrm{SU}_n(q)$ fixing L set-wise, and $L^\perp$ point-wise, taking $\langle w_1\rangle$ to $\langle w_2\rangle$.

We conclude, in every case that the set of pairs $(\langle v_i\rangle,\langle w_i\rangle)$ which are orthogonal lie in a single orbit of $\mathrm{PSU}_n(q)$, and hence the action is of permutation rank 3. Now the proof is concluded as

in the symplectic case: a congruence must be a union of the diagonal and one of the other two orbits on Ω^2. We must prove that neither of these two possibilities yields an equivalence relation.

(E100*) *Prove that if $\beta(x,y)=0$, then there exists z with $\beta(x,z),\beta(y,z)\neq 0$.*

(E101*) *Prove that if $\beta(x,y)\neq 0$, then there exists z with $\beta(x,z)=\beta(y,z)=0$.*

□

To apply Iwasawa's Criterion we will need to know the structure of the centralizer in the action just studied.

abilizer **Lemma 60.** *Let $G=\mathrm{SU}_n(q)$ and let Ω be the points of the associated polar space. Let $\omega\in\Omega$. Then*

$$G_\omega \cong Q \rtimes (\mathrm{SU}_{n-2}(q)\times \mathrm{GL}_1(q^2))$$

where Q is an elementary abelian group of order q^{2n-3}.

Proof. Since $\mathrm{SU}_n(q)$ acts transitively on the set of points of its polar space, we can take ω to be any point of the polar space. Choose a unitary basis for V ordered as follows:

$$\{v_1,\dots,v_r,w_r,\dots,w_1\},\text{ if } n \text{ is even},$$
$$\{v_1,\dots,v_r,x,w_r,\dots,w_1\},\text{ if } n \text{ is odd},$$

where x is an anisotropic vector in V. We set $\omega=\langle w_1\rangle$. Now it is easy to see that

$$G_{\langle w_1\rangle} = \left\{ g := \left(\begin{array}{c|ccc|c} a & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \hline 0 & & & & b_{n-2} \\ \vdots & & A & & \vdots \\ 0 & & & & b_1 \\ \hline 0 & 0 & \cdots & 0 & a^{-1} \end{array}\right) \;\middle|\; \begin{array}{l} a_1,\dots,a_{n-1}\in\mathbb{F}_{q^2}, \\ b_i=-a_i^\sigma, \\ a_{n-1}+a_{n-1}^\sigma = -\sum_{i=1}^{\lfloor \frac{n}{2}\rfloor} a_i a_{n-1-i}^\sigma, \\ a\in\mathbb{F}_{q^2}^*, A\in\mathrm{SU}_{n-2}(k) \end{array} \right\}. \tag{17}$$

Now there is a natural epimomorphism

$$G_{\langle w_1\rangle}\to \mathrm{SU}_{n-2}(q)\times\mathrm{GL}_1(q^2), g\mapsto (A,a)$$

and the kernel of this map is the group

$$Q := \left\{ g := \left(\begin{array}{c|ccc|c} 1 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \hline 0 & & & & b_{n-2} \\ \vdots & & I & & \vdots \\ 0 & & & & b_1 \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array}\right) \;\middle|\; \begin{array}{l} a_1,\dots,a_{n-1}\in\mathbb{F}_{q^2}, \\ b_i=-a_i^\sigma, \\ a_{n-1}+a_{n-1}^\sigma = -\sum_{i=1}^{\lfloor \frac{n}{2}\rfloor} a_i a_{n-1-i}^\sigma \end{array} \right\} \tag{18}$$

and one can check that Q is indeed elementary abelian of order q^{2n-3}.

(E102) *Prove that this extension is split.*

□

As with the symplectic group we need to know that the normal closure of Q contains the group generated by transvections in $\mathrm{SU}_n(q)$. The next exercise implies this, and can be proved similarly to Lemma 48.

(E103) *Every unitary transvection is contained in a conjugate of the group Q defined in Lemma 60.*

For the next couple of results we define

$$D := \langle t \in \mathrm{SU}_n(q) \mid t \text{ is a transvection} \rangle;$$
$$\Gamma := \{v \in V \mid \beta(v,v) = 1\}.$$

Lemma 61. *D is transitive on Γ except when $(n,q) = (3,2)$.*

Proof. Let $x, y \in \Gamma$. We must show that there exists $d \in D$ such that $xd = y$.

Suppose that $\beta(x,y) = 0$**.** Then $\{x,y\}$ is an orthonormal basis for a unitary hyperbolic plane and $\mathrm{SU}_2(q)$ acts on $\langle x,y\rangle$ naturally; indeed $\mathrm{SU}_2(q)$ acts on $\Gamma \cap \langle x,y\rangle$.

Let us calculate $|\Gamma \cap \langle x,y\rangle|$: By Lemma 56 there are $(q^2-1)(q+1)$ non-zero isotropic vectors in V, thus the number of non-isotropic vectors in V is

$$q^4 - (q^2-1)(q+1) - 1 = (q^2-q)(q^2-1).$$

Now, since $\beta(v,v)$ takes any value in $\mathbb{F}_q = \mathrm{Fix}(\sigma)$, we conclude that $|\Gamma \cap \langle x,y\rangle| = (q^2-q)(q+1)$. Since the stabilizer in $\mathrm{SU}_2(q)$ of any element of $\Gamma \cap \langle x,y\rangle$ is trivial, and since

$$|\mathrm{SU}_2(q)| = (q^2-q)(q+1),$$

we conclude that $\mathrm{SU}_2(q)$ acts transitively on $\Gamma \cap \langle x,y\rangle$. Since, by (E99), $\mathrm{SU}_2(q) \leq D$ we are done.

Suppose that $\beta(x,y) \neq 0$**.** If $n > 3$, then $\dim(x^\perp \cap y^\perp) = n-2 \geq 1$ and so there exists $z \in x^\perp \cap y^\perp$. Now we can apply the previous case to the pairs (x,z) and (z,y) to yield an element mapping x to y. This yields the result for $n > 3$.

We are left with the case $\beta(x,y) \neq 0$ and $n = 3$ when, by assumption, $q > 2$.

(E104*) *Complete this proof.*

□

ans unit **Lemma 62.** *$\mathrm{SU}_n(q)$ is generated by transvections except when $(n,q) = (3,2)$.*

Proof. The result is true for $n = 2$, so we assume that $n > 2$ and $q > 2$ if $n = 3$. We will proceed by induction, hence we will need the following result to complete the base case.

(E105*) *Prove that $\mathrm{SU}_4(2)$ is generated by transvections.*

Write $G := \mathrm{SU}_n(q)$ and let $v \in \Gamma$. The previous lemma implies that $G = G_v D$. Note, moreover, that $G_V = \mathrm{SU}_{n-1}(q)$ (this is clear by considering the action on the non-degenerate space $\langle v\rangle^\perp$). Induction implies that $\mathrm{SU}_{n-1}(q)$ is generated by transvections, thus G is generated by transvections. □

Corollary 63. *Let Q be the subgroup defined in Lemma 60. Then*

$$\langle Q^g \mid g \in G\rangle = \mathrm{SU}_n(q).$$

We are ready to prove our main theorem.

y simple **Theorem 64.** *$\mathrm{PSU}_n(q)$ is simple unless*

$$(n,q) \in \{(2,2), (2,3), (3,2)\}.$$

Proof. (E99) implies the result when $n = 2$. Thus assume that $n > 3$ and observe that, in light of the results so far, Iwasawa's criterion implies that it is sufficient to prove that $\mathrm{PSU}_n(q)$ is perfect except when $(n,q) = (3,2)$. Lemma 62 implies that it is sufficient to prove that all transvections can be written as commutators.

Assume that $q \geq 3$. Observe that, $\mathrm{SU}_3(q)$, defined with respect to a basis $\{v_1, x, w_1\}$, contains the element

$$(b,a) := \begin{pmatrix} 1 & 0 & 0 \\ -a^\sigma & 1 & 0 \\ b & a & 1 \end{pmatrix}$$

provided $aa^\sigma + b + b^\sigma = 0$. The element (b, a) is a transvection if and only if $a = 0$, and every transvection in $\mathrm{SU}_n(q)$ lies inside a subgroup $\mathrm{SU}_3(q)$ preserving a non-degenerate 3-dimensional subspace.

Now observe that

$$[(b_1, 1), (b_2, a_2)] = (a_2^\sigma - a_2, 0).$$

We claim that we can write any $(c, 0)$ in this way, provided $c + c^\sigma = 0$. This follows, because $c \in \ker(1 + \sigma)$ implies that $c \in \mathrm{Im}(1 - \sigma)$ and so $c = d - d^\sigma$ for some d. Now take $a_2 = d^\sigma$ and the result follows.

(E106) *Prove the result for $q = 2$ and $n \geq 4$.*

□

Exercise (E99) implies that we have already met two of the exceptional groups from Theorem 64, namely $\mathrm{PSU}_2(2)$ and $\mathrm{PSU}_2(3)$. The final group is dealt with in the following exercise.

(E107*) *Prove that $\mathrm{PSU}_3(2) \cong E \rtimes Q$ where E is an elementary abelian group of order 9 and Q is a quaternion group of order 8.*

We conclude with a result concerning isomorphisms between unitary groups and other simple groups. In light of (E99) we restrict to the case $n \geq 3$; see [Tay92] for a proof.

Proposition 65. *Let $G = \mathrm{PSU}_n(q)$ with $n \geq 3$. Let H be a simple alternating, linear or symplectic group. Then $G \cong H$ if and only if $G = \mathrm{PSU}_4(2)$ and $H = \mathrm{PSp}_4(3)$.*

11. Orthogonal groups

We will not give a full treatment of the orthogonal groups, as we do not have time, but we'll try and give a broad overview. Throughout this section V is an n-dimensional vector space over the field $k = \mathbb{F}_q$ and $Q : V \to \mathbb{F}_q$ is a non-degenerate quadratic form.

Recall first that we have the following possibilities for (V, Q). (Note that, in all cases, for $i = 1, \ldots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs, with $Q(v_i) = Q(w_i) = 0$.)

- $(\mathbf{O^+_{2r}})$ with basis $\{v_1, w_1, \ldots, v_r, w_r\}$.
- $(\mathbf{O_{2r+1}})$ with basis $\{v_1, w_1, \ldots, v_r, w_r, u\}$ where $u \in \langle v_1, w_2, \ldots, v_r, w_r\rangle^\perp$ is anisotropic. We can prescribe, moreover, that $Q(u) = 1$ or, if q is odd, $Q(u)$ is 1 or a non-square.
- $(\mathbf{O^-_{2r+2}})$ with basis $\{v_1, w_1, \ldots, v_r, w_r, u, u'\}$ where $\langle u, u'\rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \ldots, v_r, w_r\rangle$. We can prescribe, moreover, that $Q(u) = 1$, $Q(u') = a$ and $x^2 + x + a$ is irreducible in $\mathbb{F}_q[x]$.

Note that, although there are two non-isomorphic spaces O_{2r+1}, the corresponding polar spaces, and hence the corresponding isometry (resp. similarity/ semisimilarity) groups are all isomorphic.

This remark allows us to make the following definitions. Note that, throughout,

$$\varepsilon \text{ is } \begin{cases} +\text{ or } -, & \text{if } n \text{ is even;} \\ \text{blank}, & \text{if } n \text{ is odd.} \end{cases}$$

- $\Gamma\mathrm{O}^\varepsilon_n(q)$ is the semisimilarity group of Q;
- $\mathrm{GO}^\varepsilon_n(q)$ is the similarity group of Q;
- $\mathrm{O}^\varepsilon_n(q)$ is the isometry group of Q;
- $\mathrm{SO}^\varepsilon_n(q)$ is the special isometry group of Q, i.e. it equals $\mathrm{O}^\varepsilon_n(q) \cap \mathrm{SL}_n(q)$.
- $\Omega^\varepsilon_n(q)$ is a subgroup of $\mathrm{SO}^\varepsilon_n(q)$ of index 1 or 2. We give a definition at the end of this section.[10]

[10] In most cases $\Omega^\varepsilon_n(q) = (\mathrm{O}_n(\varepsilon(q))'$, the derived subgroup of $\mathrm{O}_n(\varepsilon(q))$. This is true, for instance, provided $n \geq 6$.

For all of the listed groups X, there is a projective version $\mathrm{P}X = X/(X \cap K)$ where K is the set of scalar matrices.[11]

The groups we're primarily interested in are $\mathrm{P}\Omega_n^\varepsilon(q)$ as these are simple unless n and q are in a certain small range. Our treatment begins similarly to the other classical groups:

al count

Lemma 66.

(1) *Let x_n^ε be the number of non-trivial singular vectors. Then*
- $x_{2m}^\varepsilon = (q^m - \varepsilon 1)(q^{m-1} + \varepsilon 1)$;
- $x_{2m+1} = q^{2m} - 1$.

(2) *The number of hyperbolic pairs is $x_n^\varepsilon \cdot q^{n-2}$.*

Proof. Clearly $x_1 = x_2^- = 0$. On the other hand, a space of type O_2^+ is a hyperbolic line, thus if (v, w) is a hyperbolic pair, then $Q(av + bw) = ab$ and so the singular vectors lie in $\langle v\rangle \cup \langle w\rangle$ and $x_2^+ = 2(q-1)$.

Now for any $n \geq 3$, an orthogonal space admits a basis which is an orthogonal direct sum of a set of mutually orthgonal hyperbolic lines with one of the spaces already covered. Consider the different cases in turn.

($\mathbf{O_{2r}^+}$) with $Q(\sum a_i v_i + \sum b_i w_i) = \sum a_i b_i$. Then $Q(v) = 0$ iff either
- $a_1 = 0$, b_1 is anything and the 'tail' of the vector in O_{2r-2}^+ is singular. This gives $q(x_{2r-2}^+ + 1) - 1$ possibilities. (The '+1' and the '−1' are there to account for zero vectors.)
- $a_1 \neq 0$ and $b_1 = a_1^{-1} \sum_{i=2}^r b_i w_i$. This gives $(q-1)q^{2r-2}$ possibilities.

We conclude that $x_{2r}^+ = (q-1)q^{2r-2} + q(x_{2r-2}^+ + 1) - 1$ and the result follows by induction.

($\mathbf{O_{2m}^-}$) Exactly the same reasoning as before implies that

$$x_{2m}^- = (q-1)q^{2m-2} + q(x_{2m-2}^- + 1) - 1$$

and the result follows by induction.

($\mathbf{O_{2r+1}}$) This time we obtain that

$$x_{2r+1} = (q-1)q^{2r-2} + q(x_{2r-1} + 1) - 1$$

and the result follows.

To calculate the number of hyperbolic pairs (v, w), simply observe that the number of choices for the first entry v is x_n. To find w we choose any vector in the complement of $\ker(\beta_v)$ where $\beta_v : V \to k, w \mapsto \beta(v, w)$. Since β_v is a non-zero linear functional, its kernel has dimension $n-1$ and the number of vectors in the complement of the kernel is, therefore, $q^n - q^{n-1}$. Now we must restrict to those elements for which $\beta(v, w) = 1$ and we obtain $\frac{1}{q-1}(q^n - q^{n-1})$ as required. □

We will use Lemma 66 to calculate the size of $O_n^\varepsilon(q)$ using induction on n. The base cases are treated in the following exercise.

all orth

(E108) *$O_1(q) = \{\pm I\}$ and $O_2^\varepsilon(q) \cong D_{2(q-\varepsilon 1)}$.*

Lemma 67.
- $|O_{2m}^\varepsilon(q)| = 2q^{m(m-1)}(q^m - \varepsilon 1) \prod_{i=1}^{m-1}(q^{2i} - 1)$.
- $|O_{2m+1}(q)| = (2, q-1)q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1)$.

[11] Some authors label orthogonal groups slightly differently. I've chosen terminology that is consistent with [KL90] but, for instance, some people write $\mathrm{GO}_n^\varepsilon(q)$ for the isometry group of Q, rather than the similarity group.

Proof. As in previous sections we use the fact that $\mathrm{Isom}(Q)$ acts regularly on the set of orthogonal bases. To count orthogonal bases we choose (x, y) to be a hyperbolic pair and invoke Lemma 66, before using induction to count the number of orthogonal bases in $\langle x, y\rangle^\perp$. The result follows, using (E108) for the base case. □

e: ccc

(E109*) *Prove that*

$$|\mathrm{SO}^\varepsilon_n(q)| = |\mathrm{PO}^\varepsilon_n(q)| = \frac{1}{(2, q-1)}|\mathrm{O}^\varepsilon_n(q)|.$$

A full definition of the subgroup $\Omega^\varepsilon_n(q)$ will be given at the end of this section, however we pre-empt that a little by treating the case when n is odd:

- If q is even, define $\Omega_{2m+1}(q) = \mathrm{SO}_{2m+1}(q)$;
- If q is odd and $m \geq 1$, define $\Omega_{2m+1}(q)$ to be the unique index 2 subgroup of $\mathrm{SO}_{2m+1}(q)$. With this definition $\mathrm{P}\Omega^\varepsilon_n(q)$ is the unique index 2 subgroup of $\mathrm{PSO}_{2m+1}(q)$.

The existence of this 'unique index 2 subgroup' is not at all obvious, and we defer further discussion for now. However we have enough information to present the next important result.

a q even

Lemma 68.

(1) *If q is even, then $\Omega_{2m+1}(q) = \mathrm{SO}_{2m+1}(q) \cong \mathrm{Sp}_{2m}(q)$.*
(2) *If q is odd, then $\mathrm{P}\Omega_{2m+1}(q)$ and $\mathrm{PSp}_{2m}(q)$ have the same order. If, in addition $m > 2$, then $\mathrm{P}\Omega_{2m+1}(q) \ncong \mathrm{PSp}_{2m+1}(q)$.*

Proof. Let Q be a non-degenerate quadratic form of type O_{2m+1} and assume that q is even. The polarization of Q, β_Q is alternating and, since the dimension is odd, it must be degenerate. However (E73) implies that $\mathrm{Rad}(\beta_Q)$ has dimension 1. Let $\mathrm{Rad}(\beta_Q) = \langle z\rangle$ and choose z so that $Q(z) = 1$. Now the space $V/\langle z\rangle$ is non-degenerate and symplectic of order $2m$.

The action of $\mathrm{SO}_{2m+1}(q)$ on V induces an action by isometry on $V/\langle z\rangle$ and we obtain a homomorphism $\mathrm{SO}_{2m+1}(q) \to \mathrm{Sp}_{2m}(q)$. One can check that the kernel of this homomorphism is trivial, hence we obtain an embedding. However checking orders we see that the two groups have the same cardinality and so $\mathrm{SO}_{2m+1}(q) \cong \mathrm{Sp}_{2m}(q)$. Now, since $\Omega_{2m+1}(q)$ is the derived subgroup of $\mathrm{O}_{2m+1}(q)$, and since $\mathrm{Sp}_{2m}(q)$ is perfect (since $(m, q) \notin \{(1, 2), (2, 2)\}$), we conclude that $\Omega_{2m+1}(q) = \mathrm{SO}_{2m+1}(q)$.

Result (2) follows from the following exercise.

(E110) *Let q be odd. Show that $\mathrm{PSp}_{2m}(q)$ has $\lfloor \frac{m}{2} \rfloor + 1$ conjugacy classes of involutions, while $\mathrm{P}\Omega_{2m+1}(q)$ has m conjugacy classes of involutions.*

□

The proof of Lemma 68 implies that $\Omega_{2m+1}(q) = \mathrm{SO}_{2m+1}(q)$ when q is even, and that this group is simple, except when $(m, q) = (1, 2)$ or $(2, 2)$.

In light of Lemma 68 most authors tend not to study $\Omega_{2m+1}(q)$ when q is even, opting instead to study the isomorphic group $\mathrm{Sp}_{2m}(q)$ (see, for instance, [KL90]). The following couple of results show in addition that, when $n \leq 6$, $\mathrm{P}\Omega^\varepsilon_n(q)$ does not yield a new simple group. Indeed (E108) implies that already for $n \leq 2$.

Lemma 69. $\mathrm{P}\Omega_3(q) \cong \mathrm{PSL}_2(q)$.

Proof. Lemma 68 implies the result when q is even. Suppose that q is odd. Let Ω be the set of homogeneous polynomials over $\mathbb{F}_q$ in variables x and y of degree 2, i.e.

$$\Omega := \{rx^2 + sxy + ty^2 \mid r, s, t \in Fq\}.^{12}$$

[12] An equivalent formulation is to take Ω to be equal to $\mathrm{Sym}^2(V)$, the symmetric square of $V = \mathbb{F}_q^2$. Clearly $\mathrm{GL}_2(q)$ acts on V naturally via the homomorphism ρ defined below.

Then $G = \mathrm{GL}_2(q)$ acts on Ω by substitution, i.e. given

$$g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

we define

$$x^g = ax + by \text{ and } y^g = cx + dy$$

and observe that we have a well-defined action. Indeed, identifying $f = rx^2 + sxy + ty^2$ with $\begin{pmatrix} r & s & t \end{pmatrix}$, we have $f^g = \begin{pmatrix} r & s & t \end{pmatrix} \rho(g)$ where

$$\rho : \mathrm{GL}_2(q) \to \mathrm{GL}_3(q), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

Observe that $\ker(\rho) = \{\pm I\}$ and define a quadratic form on $V = (\mathbb{F}_q)^3$ via

$$Q\begin{pmatrix} r & s & t \end{pmatrix} = 4rt - s^2.$$

One can check that Q is non-degenerate and that, for $g \in G$,

$$Q(f^{\rho(g)}) = \rho(f)(\det(g))^2.$$

This implies that $\mathrm{SL}_2(q).2/\langle -I \rangle \leq O_3(q)$ (in fact it is an index 2 subgroup), and so $\mathrm{SL}_2(q)/\langle -I \rangle$ is an index 2 subgroup of $SO_3(q)$. If $q > 3$, then $\mathrm{SL}_2(q)/\langle -I \rangle$ must be the derived subgroup of $O_3(q)$ (since it is perfect and of index 4), and the result follows. For $q \in \{2, 3\}$ we omit the proof. □

The proof of the following lemma is omitted. It is proved in a similar fashion to the last lemma.

Lemma 70.

(1) $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q)$.
(2) $\mathrm{P}\Omega_4^-(q) \cong \mathrm{PSL}_2(q^2)$.
(3) $\mathrm{P}\Omega_5(q) \cong \mathrm{PSp}_4(q)$.
(4) $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$.
(5) $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$.

11.1. **Simplicity.** We conclude with a statement concerning the simplicity of $\mathrm{P}\Omega_n^\varepsilon(q)$. The last two lemmas imply the result for $n = 5$ and 6. Indeed they also imply that $\mathrm{P}\Omega_3(q)$ and $\mathrm{P}\Omega_4^-(q)$ are simple, but we do not include this in the statement.

n simple

Theorem 71. *If $n \geq 5$, then $\mathrm{P}\Omega_n^\varepsilon(q)$ is simple.*

The proof of this theorem is a little different to the previous cases we have studied, and we will not write it down. The following exercise highlights one major difference.

(E111*) *$SO_n^\varepsilon(q)$ contains a transvection if and only if q is even.*

The second major hurdle is, of course, that we have yet to give a proper definition of the group $\Omega_n^\varepsilon(q)$. Most of the time one can take it to equal the derived subgroup of $O_n^\varepsilon(q)$, but even if one ignores the caveat 'most of the time', this definition is still unwieldy in practice. We will finish by sketching a more explicit definition of $\Omega_n^\varepsilon(q)$.

Let $v \in V$ be a non-singular vector and define the *reflection in v* as the map

$$r_v : V \to V, x \mapsto x - \frac{\beta_Q(v, x)}{Q(v)} v.$$

(Observe that r_v satisfies the first condition for a map to be a transvection, since $r_v - I$ has rank 1, but it does not satisfy the second, since $(r_v - I)^2 \neq 0$.) One can check that $r_v \in \mathrm{Isom}(Q)$, that $r_v^2 = 1$, and that

$$\det(r_v) = \begin{cases} -1, & \text{if } q \text{ is odd;} \\ 1, & \text{if } q \text{ is even.} \end{cases}$$

Now the following result is [KL90, Prop 2.5.6].

spinor

Lemma 72. $\mathrm{Isom}(Q) = \langle r_v \mid Q(v) \neq 0 \rangle$, *provided* $\mathrm{Isom}(Q) \neq \mathrm{O}_4^+(2)$.

Now our definition is as follows:

- Suppose that q is even and that $\mathrm{Isom}(Q) \neq \mathrm{O}_4^+(2)$. We can assume that n is even by Lemma 68 and thus, by (E109), $\mathrm{O}_n^\varepsilon(q) = \mathrm{SO}_n^\varepsilon(q)$ and by Lemma 72, every element of $\mathrm{SO}_n^\varepsilon(q)$ can be written as a product of reflections. Now the subgroup of S consisting of products of an even number of reflections has index 2 in $\mathrm{SO}_n^\varepsilon(q)$ and this is the group $\Omega_n^\varepsilon(q)$. It is not a priori clear that this action yields an index 2 subgroup - the next exercise shows that it is true when $\varepsilon = +$.

  (E112*) *Prove that this definition yields an index 2 subgroup when $\varepsilon = +$, by showing that in the natural action of G on $\mathcal{U}_r$, the set of maximal totally singular subspaces, any reflection acts as an odd permutation on $\mathcal{U}_r$.*

- Suppose that q is odd and that $n \geq 2$. Consider the group $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ which has order 2.[13] Lemma 72 implies that every element of $\mathrm{SO}_n^\varepsilon(q)$ can be written as an even number of reflections $g = r_{v_1} \cdots r_{v_k}$, for some non-singular vectors v_i. Define the *spinor norm*,

$$\theta : \mathrm{SO}_n^\varepsilon(q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^2, \quad g \mapsto \prod_{i=1}^{k} \beta_Q(v_i, v_i) \pmod{(\mathbb{F}_q^*)^2}.$$

  It turns out that θ is a well-defined homomorphism, and that it is surjective. In particular $\ker(\theta)$ is an index 2 subgroup of $\mathrm{SO}_n^\varepsilon(q)$, and this is the subgroup $\Omega_n^\varepsilon(q)$.

  (E113) *Calculate the order of $|\Omega_n^\varepsilon(q)|$ when $(n, q, \varepsilon) \neq (4, 2, +)$.*

We do not give a definition of $\Omega_4^+(2)$. Those interested should consult [KL90, p. 30]. We finish with a result which we do not prove, but which guarantees that our work on the orthogonal groups has yielded some genuinely new simple groups:

Theorem 73. *If $n \geq 7$, then $\mathrm{P}\Omega_n^\varepsilon(q)$ is not isomorphic to any other classical or alternating group, unless n is odd and q is even.*

References

[Cam] P. Cameron, *Projective and polar spaces*, Lecture notes available at `http://www.maths.qmul.ac.uk/ pjc/pps/`.

[KL90] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.

[Ros94] John S. Rose, *A course on group theory*, Dover Publications Inc. New York, 1994, Reprint of the 1978 original [Dover, New York].

[Tay92] Donald E. Taylor, *The geometry of the classical groups*, Sigma Series in Pure Mathematics, vol. 9, Heldermann Verlag, Berlin, 1992.

[Tit74] Jacques Tits, *Buildings of spherical type and finite BN-pairs*, Lecture Notes in Mathematics, Vol. 386, Springer-Verlag, Berlin, 1974.

[13] We write $(\mathbb{F}_q^*)^2$ for the set of non-zero squares in $\mathbb{F}_q^*$. It is an index 2 subgroup of $\mathbb{F}_q^*$.