17. 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 write $\overline{\alpha} = \alpha^{\sigma}$ for $\alpha \in k$. Note that k_0 is the fixed field of σ and recall the *trace* and *norm* functions:

Tr :
$$\mathbb{F}_{q^2} \to \mathbb{F}_q$$
, $x \mapsto x + x^{\sigma}$;
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, ..., r, (v_i, w_i) are mutually orthogonal hyperbolic pairs.

 $(\mathbf{U}_{2\mathbf{r}})$ with basis $\{v_1, w_1, \dots, v_r, w_r\}$.

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

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

Lemma 17.1. There is a basis $\{v_1, \ldots, v_n\}$ 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

(26)
$$\beta((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sum_{i=1}^n x_i y_i^{\sigma}.$$

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

(E17.1) 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 $\operatorname{Isom}(\beta_1)$ and $\operatorname{Isom}(\beta_2)$ (resp. $\operatorname{Sim}(\beta_1)$ and $\operatorname{Sim}(\beta_2)$) are conjugate subgroups of $\operatorname{GL}_n(k)$. Furthermore $\operatorname{SemiSim}(\beta_1)$ and $\operatorname{SemiSim}(\beta_2)$ are conjugate subgroups of $\Gamma \operatorname{L}_n(k)$.

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

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

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

- Warning:
 - Recall that $\operatorname{GSp}_{2r}(k)$ was the set of similarities of an alternating form, whereas here $\operatorname{GU}_n(k)$ 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 $X_n(k)$ has a synonym given by $X_n(q)$. In the unitary case, though, the group can only be defined over a field of square order; thus if $X_n(k)$ is one of the listed unitary groups defined over the field $k = \mathbb{F}_{q^2}$, then we use the synonym $X_n(q)$.
 - While we're mentioning synonyms, note that the notation $U_n(q)$ is used in various places, but its meaning varies. Sometimes it is a synonym for $GU_n(k)$, at other times it means $PSU_n(k)$.

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.

Lemma 17.2. 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 $\sum_{i=0}^{n} \alpha_i \alpha_i^{\sigma} = 0.$

- If α₁ = 0, then we obtain x_{n-1} such solutions;
 If α₁ ≠ 0, then α₁^{q+1} = Σ_{i=2}ⁿ α_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. Thus

$$x_n = x_{n-1} + (q+1)(q^{2n-2} - 1 - x_{n-1}).$$

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} 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 $q^2 x_{n-2} + q^2 - 1$ isotropic vectors in v_1^{\perp} in total.

Our choice for w_1 must be an 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 $\frac{1}{q^2-1}(q^2x_{n-2}+q^2-1)$ possibilities for w_1 . The result follows.

Corollary 17.3. • $|\operatorname{GU}_n(q)| = q^{\frac{1}{2}n(n-1)} \prod_{i=1}^n (q^i - (-1)^i).$ • $|\operatorname{PGU}_n(q)| = |\operatorname{SU}_n(q)| = \frac{|\operatorname{GU}_n(q)|}{q+1}.$

•
$$\operatorname{PSU}_n(q) = \frac{|\operatorname{SU}_n(q)|}{(n,q+1)}$$
.

Proof. We prove the first identity similarly to how one proves the order of $GL_n(q)$. Suppose that we have fixed a unitary basis $\{v_1, w_1, v_2, w_2, \dots$ Let $g \in \mathrm{GU}_n(q)$ and consider the possible entries in the first two columns of g. These are the image of v_1 and w_1 respectively, and so these two images must, together, form a hyperbolic pair. Then Lemma 17.2 implies that the number of possibilities for the first two columns is

$$(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})q^{2n-3}$$

Writing L for the hyperbolic line spanned by the first two columns of g, it is clear that the remaining columns lie in L^{\perp} , a unitary space of dimension n-2. Now the result follows by induction.

For the second identity refer to (26) 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 $\lambda I \in SU_n(q)$ if and only if $\lambda^{q+1} = \lambda^n = 1$. The result follows.

17.1. 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 $SU_n(k)$.)

Lemma 17.4. The unitary transvections are

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

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

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

$$\beta(v + (vf)a, w + (wf)a) = \beta(v, w), \forall v, w \in V$$
$$\iff \overline{(wf)}\beta(v, a) + (vf)\beta(a, w) + (vf)\overline{(wf)}\beta(a, a) = 0, \forall v, w \in V$$

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 $vf = \overline{(wf)}\beta(v, a)$. But, letting w = v such that $\beta(a, w) \in \mathbb{F}_a^*$ we see that

$$(wf)\beta(w,a) + wf\beta(a,w)$$

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

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. \Box

(E17.2*) $SU_2(q) \cong SL_2(q)$ and, moreover, the action of $SU_2(q)$ on the set of points of the associated polar space is isomorphic to the action of $SL_2(q)$ on the set of points of $PG_1(q)$.

Lemma 17.5. The action of $PSU_n(q)$ on the points of the associated polar space is faithful, of permutation $rank \leq 3$ and primitive.

Proof. We make use of the existence of a unitary basis. Suppose $g \in SU_n(q)$ fixes every point of the associated polar space. Let $(v_1, w_1), \ldots, (v_r, w_r)$ 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 . Let $\alpha \in \mathbb{F}_{q^2}$ such that $\alpha^q = -1$. Then $\alpha v_i + w_i$ 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 mutually orthogonal to w_i 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.

(E17.2) implies that the action is primitive of rank 2 when n = 2, thus we assume that $n \ge 3$. Witt's lemma implies that the action of $\operatorname{GU}_n(q)$ 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 $g \in \operatorname{PSU}_n(q)$ such that $\langle v \rangle^g = \langle w \rangle$, one simply adjusts the determinant of a corresponding element in $\operatorname{GU}_n(q)$.

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 $\text{PSU}_n(q)$ is transitive on points, we can assume that $v_1 = v_2$, and we simply write v for this element. Assume, first, that $n \ge 6$. There are two cases:

- Suppose that $W := \langle v, w_1, w_2 \rangle$ is totally isotropic. Then there exists $g \in SL(W)$ such that $\langle v \rangle^g = \langle v \rangle$ and $\langle w_1 \rangle^g = \langle w_2 \rangle$. Now we use Witt's lemma (and an adjustment of determinant) to extend to $SU_n(q)$.
- Suppose that $W = \langle v, w_1, w_2 \rangle$ is not totally isotropic, i.e. $\beta(w_1, w_2) \neq 0$ and $L := \langle w_1, w_2 \rangle$ is a hyperbolic plane. By Witt's Lemma, there exists $g \in \operatorname{GU}_n(q)$ such that $\langle v \rangle^g = v_1, \langle w_i \rangle^g = \langle w_i \rangle$ and $\{v_1, v_2, w_1, cw_2, x_1, x_2\}$ is a unitary basis for a non-degenerate 6-dimensional subspace of V (here c is some scalar). It is clear that, by adjusting the determinant, we may assume that $g \in \operatorname{SU}_n(q)$. Now observe that $\langle v_1, w_1, x_1 \rangle$ and $\langle v_2, w_2, x_1 \rangle$ are totally isotropic, and by the previous bullet point, we are done.

If, on the other hand, n > 6, then V contains no 3-dimensional totally isotropic subspaces and we conclude that W is not totally isotropic. But in this case there exists $g \in SU_n(q)$ 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 $PSU_n(q)$, 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.

(E17.3*) Prove that if $\beta(x, y) = 0$, then there exists z with $\beta(x, z), \beta(y, z) \neq 0$. (E17.4*) 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 stabilizer in the action just studied. **Lemma 17.6.** Let $G = SU_n(q)$ 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 $SU_n(q)$ 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:

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

where x is an anisotropic vector in V. We set $\omega = \langle w_1 \rangle$. Now it is easy to see that $G_{\langle w_1 \rangle}$ contains the following two subgroups:

$$(27) H := \left\{ g := \begin{pmatrix} a \mid 0 & \cdots & 0 \mid & 0 \\ 0 \mid & & & 0 \\ \vdots \mid & A \mid & \vdots \\ 0 \mid & & & 0 \\ \hline 0 \mid 0 & \cdots & 0 \mid (a^{-1})^{\sigma} \end{pmatrix} \middle| a \in \mathbb{F}_{q^2}^*, A \in \mathrm{SU}_{n-2}(k) \right\}; \\ (27) Q := \left\{ g := \begin{pmatrix} 1 \mid a_1 & \cdots & a_{n-2} \mid a_{n-1} \\ 0 \mid & & & b_{n-2} \\ \vdots \mid & I \mid & & b_{n-2} \\ \vdots \mid & I \mid & & \vdots \\ 0 \mid & & & & b_{n-2} \\ \vdots \mid & I \mid & & \vdots \\ 0 \mid & & & & b_{1} \\ \hline 0 \mid & & & & 0 \\ \hline 0 \mid 0 & \cdots & 0 \mid & & 1 \end{pmatrix} \middle| \begin{array}{c} a_1, \dots, a_{n-1} \in \mathbb{F}_{q^2}, \\ a_{n-1} + a_{n-1}^{\sigma} = -\sum_{i=1}^{\lceil \frac{n}{2} \rceil} a_i a_{n-i}^{\sigma}, \\ b_i = -a_i^{\sigma}, \\ \end{vmatrix} \right\}.$$

The following facts are easy to check:

- (1) $Q \cap H = \{1\};$
- (2) $|G_{\langle w_1 \rangle}| = |Q| \cdot |H|;$
- (3) Q is isomorphic to the additive group $(\mathbb{F}_q^{2n-3}, +);$
- (4) $H \cong SU_{n-2}(q) \times \operatorname{GL}_1(q^2).$

The first two items imply that $G_{\langle w_1 \rangle} = Q \cdot H$. One can easily check that H normalizes Q, and thus Q is normal in $G_{\langle w_1 \rangle}$ and we conclude that $G_{\langle w_1 \rangle} = Q \rtimes H$. Now the last two items complete the proof.

As with the symplectic group we need to know that the normal closure of Q contains the group generated by transvections in $SU_n(q)$. The next exercise implies this, and can be proved similarly to Lemma 16.7.

(E17.5) Every unitary transvection is contained in a conjugate of the group Q defined in Lemma 17.6.

For the next couple of results we define

$$D := \langle t \in SU_n(q) \mid t \text{ is a transvection} \rangle;$$

$$\Gamma := \{ v \in V \mid \beta(v, v) = 1 \}.$$

Lemma 17.7. D is transitive on Γ except when (n,q) = (3,2).

Proof. Let $x, y \in D$. 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 $SU_2(q)$ acts on $\langle x, y \rangle$ naturally; indeed $SU_2(q)$ acts on $\Gamma \cap \langle x, y \rangle$.

Let us calculate $|\Gamma \cap \langle x, y \rangle|$: By Lemma 17.2 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 $\mathbb{F}_q = \operatorname{Fix}(\sigma)$, we conclude that $|\Gamma \cap \langle x, y \rangle| = (q^2 - q)(q + 1)$. Since the stabilizer in $\operatorname{SU}_2(q)$ of any element of $\Gamma \cap \langle x, y \rangle$ is trivial (because the stabilizer of v also stabilizes v^{\perp}), and since

$$|SU_2(q)| = (q^2 - q)(q + 1),$$

we conclude that $SU_2(q)$ acts transitively on $\Gamma \cap \langle x, y \rangle$. Since, by (E17.2), $SU_2(q) \leq D$ 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.

(E17.6*) Complete this proof.

Lemma 17.8. $SU_n(q)$ 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.

 $(E17.7^*)$ Prove that $SU_4(2)$ 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. \Box

Corollary 17.9. Let Q be the subgroup defined in Lemma 17.6. Then

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

We are ready to prove our main theorem.

Theorem 17.10. $PSU_n(q)$ is simple unless

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

Proof. (E17.2) 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 $PSU_n(q)$ is perfect except when (n, q) = (3, 2). Lemma 17.8 implies that it is sufficient to prove that all transvections can be written as commutators.

Assume that $q \ge 3$. Observe that $SU_3(q)$, 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 $SU_n(q)$ lies inside a subgroup $SU_3(q)$ preserving a non-degenerate 3-dimensional subspace.

Now observe that

$$[(b_1, a_1), (b_2, a_2)] = (a_1 a_2^{\sigma} - a_1^{\sigma} a_2, 0).$$

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 $c \in \operatorname{Im}(1 - \sigma)$ and so $c = d - d^{\sigma}$ for some d. Now take $a_1 \neq 0$ and $a_2 = (a_1^{-1}d)^{\sigma}$ and the result follows.

(E17.8) Prove the result for q = 2 and $n \ge 4$.

Exercise (E17.2) implies that we have already met two of the exceptional groups from Theorem 17.10, namely $PSU_2(2)$ and $PSU_2(3)$. The final group is dealt with in the following exercise.

(E17.9*) Prove that $PSU_3(2) \cong E \rtimes Q$ 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 (E17.2) we restrict to the case $n \ge 3$; see [Tay92] for a proof.

Proposition 17.11. Let $G = PSU_n(q)$ with $n \ge 3$. Let H be a simple alternating, linear or symplectic group. Then $G \cong H$ if and only if $G = PSU_4(2)$ and $H = PSp_4(3)$.