Lecture 3: Classical groups

Robert A. Wilson

Queen Mary, University of London

LTCC, 19th October 2009

INTRODUCTION

Classical groups

The six families of classical finite simple groups are all essentially matrix groups over finite fields:

- the projective special linear groups $PSL_n(q)$;
- the projective special unitary group $PSU_n(q)$;
- the projective symplectic groups $PSp_{2n}(q)$;
- three families of orthogonal groups
  - $P\Omega_{2n+1}(q)$;
  - $P\Omega_{2n}^{+}(q)$;
  - $P\Omega_{2n}^{-}(q)$.

Bilinear forms

A bilinear form on a vector space V is a map $B : V \times V \to F$ satisfying

$$\begin{aligned} B(\lambda u + v, w) &= \lambda B(u, w) + B(v, w), \\ B(u, \lambda v + w) &= \lambda B(u, v) + B(u, w) \end{aligned}$$

It is

- symmetric if $B(u, v) = B(v, u)$
- skew-symmetric if $B(u, v) = -B(v, u)$
- alternating if $B(v, v) = 0$.

An alternating bilinear form is always skew-symmetric, but the converse is true if and only if the characteristic is not 2. Why?

Quadratic forms

A quadratic form is a map $Q : V \to F$ satisfying

$$Q(\lambda u + v) = \lambda^2 Q(u) + \lambda B(u, v) + Q(v)$$

where B is the associated bilinear form.
The quadratic form can be recovered from the bilinear form as $Q(v) = \frac{1}{2}B(v, v)$ if and only if the characteristic is not 2.
In characteristic 2, the associated bilinear form is alternating, since

$$0 = Q(v + v) = 2Q(v) + B(v, v) = B(v, v).$$

Conjugate-symmetric sesquilinear forms

Let F be the field of order q^2, and let $\bar{}$ denote the field automorphism $x \mapsto x^q$.
$B : V \times V \to F$ is conjugate-symmetric sesquilinear if

- $B(\lambda u + v, w) = \lambda B(u, w) + B(v, w)$, and
- $B(w, v) = \overline{B(v, w)}$.
- Consequently $B(u, \lambda v + w) = \overline{\lambda} B(u, v) + B(u, w)$.

Properties of forms

- perpendicular vectors: $u \perp v$ means $B(u, v) = 0$.
- $S^\perp = \{v \in V \mid x \perp v \text{ for all } x \in S\}$.
- v is isotropic if $B(v, v) = 0$ (or $Q(v) = 0$).
- The radical $\mathrm{rad}(B)$ of B is $V^\perp$.
- B is non-singular if $\mathrm{rad}(B) = 0$, and singular otherwise.
- Similarly the radical of Q is the subspace of isotropic vectors in the radical of the associated B.
- A subspace is non-singular if the form restricted to the subspace is non-singular.
- A subspace is totally isotropic if the form restricted to the subspace is identically zero.

Isometries and similarities

An isometry of B is a linear map $\phi : V \to V$ which preserves the form, $B(u^\phi, v^\phi) = B(u, v)$.
Similarly, an isometry of Q is a map ϕ which satisfies $Q(v^\phi) = Q(v)$.
A similarity allows changes of scale: that is

$$B(u^\phi, v^\phi) = \lambda_\phi B(u, v)$$

or

$$Q(v^\phi) = \lambda_\phi Q(v).$$

Classification of alternating bilinear forms

If we can find vectors u, v such that $B(u, v) = \lambda \neq 0$, then take our first two basis vectors to be u and $\lambda^{-1}v$, so that the form has matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Now restrict to $\{u, v\}^{\perp}$ and continue.
When there are no such vectors left, the form is identically zero.
Notice that the rank of B is always even.
Up to change of basis, there is a unique non-singular form.

Classification of sesquilinear forms

If there is a vector v with $B(v, v) = \lambda \neq 0$, then $\lambda = \overline{\lambda}$ which implies that there exists $\mu \in F$ with $\mu\overline{\mu} = \mu^{q+1} = \lambda$.
Therefore $v' = \mu^{-1}v$ satisfies $B(v', v') = 1$.
Now restrict to $v^{\perp}$ and continue.
If there is no such v, then we can easily show that the form is identically zero.
Again, there is a unique non-singular form, up to change of basis.

Classification of symmetric bilinear forms

We can diagonalise the form as in the unitary case, but adjusting the scalars requires more care.
Odd characteristic only
If $B(v, v) = \lambda$ is a square, $\lambda = \mu^2$, then we can replace v by $v' = \mu^{-1}v$ and get $B(v', v') = 1$.
But if $B(v, v)$ is not a square, the best we can do is adjust it to be equal to our favourite non-square α, say.
Now we can replace two copies of α by two copies of 1, by picking λ and μ such that $\lambda^2 + \mu^2 = \alpha^{-1}$, and changing basis via $x' = \lambda x + \mu y$ and $y' = \mu x - \lambda y$.
In this case there are exactly two non-singular forms, up to change of basis.

Classification of quadratic forms

This is only necessary in characteristic 2.
Again we find that there are exactly two non-singular forms, up to change of basis.
The first one has matrix equal to the identity matrix, and is called of plus type.
The second one has a 2×2 block $\begin{pmatrix} 1 & 1 \\ 0 & \mu \end{pmatrix}$ where $x^2 + x + \mu$ is irreducible over F_q, and is called of minus type.

Witt's Lemma

If (V, B) and (W, C) are isometric spaces, with B and C non-singular, and either

- alternating bilinear, or
- conjugate-symmetric sesquilinear, or
- symmetric bilinear in odd characteristic

then any isometry between a subspace X of V and a subspace Y of W extends to an isometry of V with W.

COFFEE BREAK

DEFINITIONS OF THE CLASSICAL GROUPS

Symplectic groups

The symplectic group $Sp_{2n}(q)$ is the isometry group of a non-singular alternating bilinear form on $V = {F_q}^{2n}$.
To calculate its order, count the number of ways of choosing a standard basis.
Pick the first vector in $q^{2n} - 1$ ways.
Of the $q^{2n} - q$ vectors which are linearly independent of the first, $q^{2n-1} - q$ are orthogonal to it, and q^{2n-1} have each non-zero inner product. So there are q^{2n-1} choices for the second vector.
By induction on n, the order of $Sp_{2n}(q)$ is

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

Structure of symplectic groups

- The only scalars in $Sp_{2n}(q)$ are ± 1. Why?
- Every element in $Sp_{2n}(q)$ has determinant 1. (This is unfortunately not obvious.)
- $Sp_2(q) \cong SL_2(q)$, by direct calculation: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ preserves the standard symplectic form if and only if $B((a,b),(c,d)) = 1$, that is $ad - bc = 1$.
- $Sp_4(2) \cong S_6$.
- All other projective symplectic groups are simple. (Proof using transvections and Iwasawa's Lemma as for $PSL_n(q)$.)

Unitary groups

The (general) unitary group $(G)U_n(q)$ is the isometry group of a non-singular conjugate-symmetric sesquilinear form on V of dimension n over F_{q^2}.
It is not quite so easy to calculate the order this time.
Induction on n gives the number of vectors of norm 1 as

$$q^{n-1}(q^n - (-1)^n).$$

Then another induction on n gives the order of the group as

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

Structure of unitary groups

- $M \in U_n(q)$ iff $M\overline{M}^T = I_n$
- In particular, if $\det(M) = \lambda$ then $\lambda\overline{\lambda} = 1$, and there are $q+1$ possibilities for λ.
- the special unitary group $SU_n(q)$ is the subgroup of matrices of determinant 1, and is a normal subgroup of index $q+1$.
- The scalars in $GU_n(q)$ are those satisfying $\lambda.\overline{\lambda} = 1$, so form a normal subgroup of order $q+1$.
- The scalars in $SU_n(q)$ form a group of order $(n, q+1)$.

Structure of unitary groups, II

- $PSU_2(q) \cong PSL_2(q)$
- $PSU_3(2)$ has order $72 = 2^3.3^2$ so is not simple (e.g. by Burnside's p^aq^b-theorem)
- $PSU_3(2) \cong 3^2{:}Q_8$ and $PGU_3(2) \cong 3^2{:}SL_2(3)$
- All other $PSU_n(q)$ are simple.

Orthogonal groups, odd characteristic

- The orthogonal groups are the isometry groups of non-singular symmetric bilinear forms.
- Since there are two types of forms, there are two types of groups.
- But in odd dimensions, the two types of forms are scalar multiples of each other, so the two groups are the same.
- In even dimensions, $2n$ say, the form has plus type if there is a totally isotropic subspace of dimension n.
- This is not the same as having an orthonormal basis.
- The other forms have minus type, and their maximal totally isotropic subspaces have dimension $n-1$.

Structure of orthogonal groups, odd characteristic

- Any element of any orthogonal group has determinant ± 1. Why?
- The subgroup of index 2 consisting of matrices of determinant 1 is the special orthogonal group.
- The subgroup of scalars has order 2.
- The resulting projective special orthogonal group is NOT simple in general.
- There is (usually) a further subgroup of index 2, which is not so easy to describe.

The spinor norm

- (With some exceptions?) orthogonal groups are generated by reflections:

$$r_v : x \mapsto x - 2\frac{B(x,v)}{B(v,v)}v.$$

- The reflections have determinant -1, so the special orthogonal group is generated by even products of reflections.
- The reflections are of two types: the reflecting vector either has norm a square in F, or a non-square.
- The subgroup of even products which contain an even number of each type has index 2 (this is NOT obvious!), and is called $\Omega_n(q)$.
- The projective version $P\Omega_n(q)$ is simple, provided $n \geq 5$.

Orthogonal groups, characteristic 2

- These are defined as the isometry groups of non-degenerate quadratic forms. This means that the associated bilinear form is non-singular, so the dimension is even.
- The determinant is always 1.
- The only scalar in the orthogonal group is 1.
- Spinor norms have no meaning.
- But still the orthogonal groups are not simple.

The quasideterminant

- If $Q(v) = 1$, the orthogonal transvection in v is the map
$$t_v : x \mapsto x + B(x, v)v.$$
- In fact, the orthogonal group is generated by these.
- There is a subgroup of index 2 consisting of the even products of orthogonal transvections. (This is NOT obvious.)
- This subgroup is simple provided $n \geq 6$.

THE END

Small-dimensional orthogonal groups

What about dimensions up to 4?

- In dimension 2, orthogonal groups are dihedral
- $PSO_3(q) \cong PGL_2(q)$
- $PSO_4^+(q) \cong (PSL_2(q) \times PSL_2(q)).2$
- $PSO_4^-(q) \cong PSL_2(q^2).2$
- Indeed, we can go further: $PSO_5(q) \cong PSp_4(q).2$, an extension by an automorphism which multiplies the form by a non-square.
- $PSO_6^+(q) \cong PSL_4(q).2$, an extension by the 'duality' automorphism $M \mapsto (M^T)^{-1}$
- $PSO_6^-(q) \cong PSU_4(q).2$, an extension by the field automorphism $x \mapsto x^q$ (applied to each matrix entry, in the case of the standard unitary form).