Lecture 2: Linear groups

Robert A. Wilson

Queen Mary, University of London

LTCC, 13th October 2008

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
  - $P\Omega_{2n+1}(q)$;
  - $P\Omega_{2n}^{+}(q)$;
  - $P\Omega_{2n}^{-}(q)$.

Finite fields

A field is a set F with all the usual arithmetical operations and rules.

- $\{F, +, -, 0\}$ is an abelian group;
- $\{F^*, ., /, 1\}$ is an abelian group, where $F^* = F \setminus \{0\}$;
- $x(y+z) = xy + xz$

Example: the integers modulo p, where p is a prime.

More finite fields

- In any finite field F, the subfield F_0 generated by 1 has prime order, p.
- F is a vector space, of dimension d, over F_0, so has p^d elements.
- In fact, there is exactly one field of each such order p^d.
- To make such a field, pick an irreducible polynomial f of degree d, and construct the quotient $F_0[x]/(f)$ of the polynomial ring.
- Example: $p = 2$, $f(x) = x^2 + x + 1$, gives a field of order 4 as $F_4 = \{0, 1, \omega, \overline{\omega}\}$ with $\omega^2 = \overline{\omega}$ and $\omega + \overline{\omega} = 1$.

LINEAR GROUPS

The general linear group

- $GL_n(q)$ is the group of all invertible $n \times n$ matrices with entries in the field $F = \mathbb{F}_q$ of order q.
- The scalar matrices form a normal subgroup Z of order $q - 1$.
- the projective general linear group $PGL_n(q) = GL_n(q)/Z$.
- The determinant map $\det : GL_n(q) \to F^*$ is a group homomorphism.
- Its kernel is the special linear group $SL_n(q)$.
- The projective special linear group $PSL_n(q) = SL_n(q)/(Z \cap SL_n(q))$.

The orders of the linear groups

- How many invertible matrices are there?
- Choose each row to be linearly independent of the previous rows.
- The first i rows span an i-dimensional space, which has q^i vectors.
- Therefore there are $q^n - q^i$ choices for the $(i + 1)$th row.
- Hence $|GL_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$.
- $|SL_n(q)| = |PGL_n(q)| = |GL_n(q)|/(q - 1)$.
- $|PSL_n(q)| = |SL_n(q)|/\mathrm{gcd}(n, q - 1)$.

An example: $GL_2(2)$

- $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$ with $1+1=0$.
- The 2-dimensional vector space F^2 has four vectors, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$.
- The first row can be any of the 3 non-zero vectors.
- The second row can be any of the remaining 2 non-zero vectors.
- Hence $|GL_2(2)| = 6$.
- $GL_2(2)$ acts on the vector space by permuting the three non-zero vectors in all possible ways.
- Hence $GL_2(2) \cong S_3$.

More examples

- $PGL_2(3) \cong S_4$, permuting the four 1-dimensional subspaces;
- $PSL_2(3) \cong A_4$;
- $PSL_2(4) \cong A_5$, permuting the five 1-dimensional subspaces;
- $PSL_2(5) \cong A_5$, and $PGL_2(5) \cong S_5$.
- In fact, $PSL_n(q)$ is a simple group except for the cases $PSL_2(2) \cong S_3$ and $PSL_2(3) \cong A_4$.

Iwasawa's Lemma

The easiest way to prove simplicity of $PSL_n(q)$ is to use:

Theorem (Iwasawa's lemma)

If G is a finite perfect group acting faithfully and primitively on a set Ω, and the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.

Proof of Iwasawa's Lemma

- Otherwise, choose a normal subgroup K with $1 < K < G$.
- Choose a point stabilizer H with $K \not\leq H$.
- Hence $G = HK$ since H is maximal.
- Any $g \in G$ can be written $g = hk$.
- Any conjugate of A is $g^{-1}Ag = k^{-1}h^{-1}Ahk = k^{-1}Ak \leq AK$.
- Therefore $G = AK$.
- Now $G/K = AK/K \cong A/(A \cap K)$ is abelian.
- But G is perfect, so has no nontrivial abelian quotients.
- Contradiction.

Simplicity of $PSL_n(q)$

- Let $PSL_n(q)$ act on the 1-dimensional subspaces of F^n.
- This action is 2-transitive, so primitive.
- The stabilizer of the point $\langle(1,0,0,\ldots,0)\rangle$ consists (modulo scalars) of matrices $\begin{pmatrix}\lambda & 0\\ v & M\end{pmatrix}$.
- It has a normal abelian subgroup consisting of matrices $\begin{pmatrix}1 & 0\\ v & I_{n-1}\end{pmatrix}$.
- These matrices encode elementary row operations, and you learnt in linear algebra that every matrix of determinant 1 is a product of such matrices.

Simplicity of $PSL_n(q)$, cont.

- To prove that $PSL_n(q)$ is perfect it suffices to prove that these matrices (transvections) are commutators.
- If $n \geq 3$ observe that

$$\left[\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&0&0\\0&1&0\\0&x&1\end{pmatrix}\right]=\begin{pmatrix}1&0&0\\0&1&0\\-x&0&1\end{pmatrix}$$

- If $q \geq 4$ then $\mathbb{F}_q$ has an element x with $x^3 \neq x$, so

$$\left[\begin{pmatrix}1&0\\y&1\end{pmatrix},\begin{pmatrix}x&0\\0&x^{-1}\end{pmatrix}\right]=\begin{pmatrix}1&0\\y(x^2-1)&1\end{pmatrix}$$

- Hence by Iwasawa's Lemma, $PSL_n(q)$ is simple whenever $n \geq 3$ or $q \geq 4$.

COFFEE BREAK

SUBGROUPS OF GENERAL LINEAR GROUPS

Subspace stabilizers

- The stabilizer of a subspace of dimension k looks like this:

$$\begin{matrix} k \rightarrow \\ n-k \rightarrow \end{matrix} \begin{pmatrix} GL_k(q) & 0 \\ q^{k(n-k)} & GL_{n-k}(q) \end{pmatrix}$$

- The subgroup of matrices of shape $\begin{pmatrix} I_k & 0 \\ A & I_{n-k} \end{pmatrix}$ is a normal abelian subgroup.
- The quotient by this subgroup is isomorphic to $GL_k(q) \times GL_{n-k}(q)$.

Imprimitive subgroups

Suppose $V = V_1 \oplus \cdots \oplus V_k$ is a direct sum of k subspaces each of dimension m.

- The stabilizer of this decomposition of the vector space has a normal subgroup $GL_m(q) \times \cdots \times GL_m(q)$ acting on $V_1, \ldots, V_k$ separately.
- There is also a subgroup S_k permuting these k subspaces.
- Together these generate a wreath product $GL_m(q) \wr S_k$.

Tensor products

If $A = (a_{ij}) \in GL_k(q)$ and $B = (b_{ij}) \in GL_m(q)$ then the following matrix is in $GL_{km}(q)$:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1k}B \\ a_{21}B & a_{22}B & \cdots & a_{2k}B \\ \vdots & & & \\ a_{k1}B & a_{k2}B & \cdots & a_{kk}B \end{pmatrix}$$

If we multiply A by a scalar λ, and B by the inverse λ^{-1}, then this matrix does not change.
Factoring out by the scalars we have

$$PGL_k(q) \times PGL_m(q) < PGL_{km}(q)$$

Wreathed tensor products

Repeating this construction with m copies of $GL_k(q)$ we get

$$PGL_k(q) \times \cdots \times PGL_k(q) < PGL_{k^m}(q)$$

We can also permute the m copies of $PGL_k(q)$ with a copy of S_m.
Together these give a wreath product

$$PGL_k(q) \wr S_m < PGL_{k^m}(q)$$

Extraspecial groups

Suppose r is an odd prime, and α is an element of order r in the field F (so r is a divisor of $|F|-1$).

- Let R be the group generated by the $r \times r$ matrices

$$\begin{pmatrix} \alpha & 0 & 0 & \cdots & 0 \\ 0 & \alpha^2 & 0 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & & \cdots & 0 \\ 0 & 0 & & \cdots & \alpha^{r-1} \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

- Then R is non-abelian of order r^3
- Taking the tensor product of k copies of R gives an extraspecial group of order r^{1+2k} acting on a space of dimension r^k.

Extraspecial groups, cont.

A slightly different construction is required for the prime 2

- Both D_8 and Q_8 have 2-dimensional representations
- Tensoring them together gives extraspecial groups of order 2^{1+2k}, with representations of degree 2^k
- In fact $D_8 \otimes D_8 = Q_8 \otimes Q_8$, so there are just two extraspecial groups of each order.
- If the field contains elements of order 4, you can adjoin these scalars to make a bigger group which contains both extraspecial groups.

Almost quasi-simple groups

- A group G is quasi-simple if $G = G'$ and $G/Z(G)$ is simple
- Example: $SL_n(q)$ is quasi-simple except for $SL_2(2)$ and $SL_2(3)$
- A group G is almost quasi-simple (for us - this is not entirely standard terminology) if G/Z is almost simple, where Z is a suitable group of scalar matrices.

The Aschbacher–Dynkin theorem

Every subgroup of $GL_n(q)$ which does not contain $SL_n(q)$ is contained in the stabilizer of one of the following

- a subspace of dimension k
- a direct sum of k subspaces of dimension m, where $n = km$
- a tensor product $F^k \otimes F^m$, where $n = km$
- a tensor product of m copies of F^k, where $n = k^m$
- an extraspecial group r^{1+2k}, where $n = r^k$
- an almost quasi-simple subgroup

THE END