NZMRI Summer School
The classical groups

Colva Roney-Dougal
colva.roney-dougal@st-andrews.ac.uk

School of Mathematics and Statistics, University of St Andrews

Nelson, 10 January 2018

University of St Andrews

Automorphisms of quasisimple groups

G is quasisimple if $G = [G, G]$ and $G/Z(G)$ is nonabelian simple.

Lemma 43

Let $G = Z{\cdot}S$ be quasisimple, with Z central and S nonabelian simple. Then $\mathrm{Aut}(G)$ embeds in $\mathrm{Aut}(S)$.

Proof.

Let $\alpha \in \mathrm{Aut}(G)$.
If α induces 1 on $S = G/Z$, then $\forall g \in G$, $\exists\ z_g \in Z$ s.t. $g^\alpha = gz_g$.
Hence $\forall g, h \in G$, $[g, h]^\alpha = [g, h]$, and α is trivial on $G = [G, G]$.
Thus $\mathrm{Aut}(G)$ acts faithfully on $G/Z = S$. □

$\mathrm{SL}_d(q)$ is (generally) quasisimple: $\mathrm{Aut}(\mathrm{SL}_d(q))$ embeds in $\mathrm{Aut}(\mathrm{PSL}_d(q))$.

A crash course on finite fields

Theorem 44 (Fundamental Theorem of Finite Fields)

For each prime p and each $e \geq 1$ there is exactly one field of order $q = p^e$, up to isomorphism, and these are the only finite fields.

The multiplicative gp $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic of order $q - 1$. A generator λ of $\mathbb{F}_q^*$ is a primitive element of $\mathbb{F}_q$.

$\mathrm{Aut}(\mathbb{F}_q) \cong C_e$, with generator the Frobenius automorphism $\phi : x \mapsto x^p$.

Diagonal automorphisms of $\mathrm{PSL}_d(q)$

Defn: $g \in \mathrm{GL}_d(q)$. c_g induces a diagonal outer aut of $(P)\mathrm{SL}_d(q)$.

$\mathrm{PGL}_d(q) = \mathrm{GL}_d(q)/(\mathbb{F}_q^* I_d)$.

Lemma 45

Let $\delta = \mathrm{diag}(\lambda, 1, \ldots, 1) \in \mathrm{GL}_d(q)$. Then $\langle \mathrm{SL}_d(q), \delta \rangle = \mathrm{GL}_d(q)$ and $|c_\delta| = (q-1, d) = |\mathrm{PGL}_d(q) : \mathrm{PSL}_d(q)|$.

Proof.

$\det(\delta) = \lambda$ and $\mathrm{GL}_d(q)/\mathrm{SL}_d(q) \cong \langle \lambda \rangle$, so $\langle \mathrm{SL}_d(q), \delta \rangle = \mathrm{GL}_d(q)$.

$|\det(\mathbb{F}_q^* I_d)| = |(\mathbb{F}_q^*)^d| = (q-1)/(q-1, d)$.

$\mathrm{PSL}_d(q) = \mathrm{SL}_d(q)/(\mathbb{F}_q^* I_d \cap \mathrm{SL}_d(q)) \cong (\mathrm{SL}_d(q)\mathbb{F}_q^*)/\mathbb{F}_q^*$.

Hence $|c_\delta| = |\mathrm{GL}_d(q) : \mathrm{SL}_d(q)\mathbb{F}_q^*| = \frac{q-1}{\det \mathbb{F}_q^*} = (q-1, d)$. $\square$

Semilinear maps

Defn: V, W - vec spaces over $\mathbb{F}_q$. $\theta \in \mathrm{Aut}(\mathbb{F}_q)$.
A θ-semilinear map is $f : V \to W$ s.t. $\forall\ v, w \in V$, $\lambda \in \mathbb{F}_q$
$(v + w)f = vf + wf$ and $(\lambda v)f = \lambda^\theta(vf)$.
f is non-singular if $vf = 0 \Rightarrow v = 0$.
f is semilinear if is θ-semilinear for some θ.

Lemma 46

The set of all non-singular semilinear maps $f : V \to V$ forms a gp, denoted $\Gamma\mathrm{L}(V)$ or $\Gamma\mathrm{L}_d(q)$.

Defn: $\mathrm{P}\Gamma\mathrm{L}_d(q) := \Gamma\mathrm{L}_d(q)/\mathbb{F}_q^*$.

Lemma 47

The map $\Gamma\mathrm{L}_d(q) \to \mathrm{Aut}(\mathbb{F}_q)$, sending each θ-semilinear map to θ, is a homomorphism with kernel $\mathrm{GL}_d(q)$. Hence $\Gamma\mathrm{L}_d(q) \cong \mathrm{GL}_d(q) : \langle\phi\rangle$, and $\phi : (g_{ij}) \mapsto (g_{ij}^\phi)$.

Sketch proof Homom claims: exercise.
$(a_1, \ldots, a_d)\phi = (a_1^\phi, \ldots, a_d^\phi)$.
Can check: $(a_1, \ldots, a_d)\phi^{-1}g\phi = (a_1, \ldots, a_d)(g_{ij}^\phi)$. □

$\mathrm{Aut}(\mathrm{PSL}_d(q))$.

The inverse-transpose map $\iota : x \mapsto x^{-\mathrm{T}} \in \mathrm{Aut}(\mathrm{GL}_d(q))$. Defining $(g\theta)^\iota = g^\iota\theta$ extends ι to $\mathrm{Aut}(\Gamma\mathrm{L}_d(q))$.

Lemma 48

ι is an automorphism of $\mathrm{SL}_d(q)$ of order two, and is induced by an element of $\Gamma\mathrm{L}_d(q)$ iff $d = 2$.

Proof.

If $g \in \mathrm{SL}_d(q)$ then $\det(g^{-1}) = \det(g^{\mathrm{T}}) = 1$, and $g^{\iota^2} = g$.
"If" claim of the second sentence:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

□

Theorem 49

If $d \geq 3$ then $\mathrm{Aut}(\mathrm{PSL}_d(q)) = \mathrm{P\Gamma L}_d(q) : \langle\iota\rangle = \mathrm{PSL}_d(q).\langle\delta, \phi, \iota\rangle$.
$\mathrm{Aut}(\mathrm{PSL}_2(q)) = \mathrm{P\Gamma L}_2(q)$.

Hence $\mathrm{Aut}(\mathrm{A}_6) \cong \mathrm{Aut}(\mathrm{PSL}_2(9)) \cong \mathrm{PSL}_2(9).\langle\delta, \phi\rangle \cong \mathrm{PSL}_2(9).2^2$.

Reducible and imprimitive subgroups of $\mathrm{GL}_d(q)$

$v_1, \ldots, v_d$ – standard basis for $\mathbb{F}_q^d$.

Theorem 50

$G \leq \mathrm{GL}_d(q)$ reducible, stabilising $W \leq V$, dimension k. Then up $\mathrm{GL}_d(q)$-conjugacy, $W = \langle v_1, \ldots, v_k \rangle$ and $G \leq P_k =$

$$\left\{ \begin{pmatrix} A & 0 \\ X & B \end{pmatrix} \ : \ A \in \mathrm{GL}_k(q), B \in \mathrm{GL}_{d-k}(q), X \textit{ arbitrary} \right\}.$$

Up to conjugacy in $\Gamma\mathrm{L}_d(q) : \langle \iota \rangle$, $k \leq d/2$.

Theorem 51

$G \leq \mathrm{GL}_d(q)$, irreducible. If $V = V_1 \oplus \cdots \oplus V_k$, and G permutes the V_i then up to $\mathrm{GL}_d(q)$-conjugacy $G \leq \mathrm{GL}(\langle v_1, \ldots, v_{d/k} \rangle) \wr \mathrm{S}_k$. Say G is imprimitive.

Example 52

$\mathrm{GL}_1(q) \wr \mathrm{S}_d$ is all matrices with one non-zero entry in each row and column. Preserves $\langle v_1 \rangle \oplus \cdots \oplus \langle v_d \rangle$.

Subfield and semilinear subgroups of $\mathrm{GL}_d(q)$

Let q_0 properly divide q. Then there is a natural embedding $\mathrm{GL}_d(q_0) \to \mathrm{GL}_d(q)$.

Defn: $G \leq \mathrm{GL}_d(q)$ is a subfield group if $\exists g \in \mathrm{GL}_d(q)$ s.t. $G^g \leq \langle \mathrm{GL}_d(q_0), \mathbb{F}_q^* \rangle$ for some q_0.

If $|\mathbb{F}_q : \mathbb{F}_{q_0}|$ not prime, then $\exists$ q_1 s.t. $\mathrm{GL}_d(q_0) < \mathrm{GL}_d(q_1) < \mathrm{GL}_d(q)$, so G not maximal. Otherwise, $\langle \mathrm{GL}_d(q_0), \mathbb{F}_q^* \rangle$ is generally maximal.

$\mathbb{F}_{q^s}$ is a vector space over $\mathbb{F}_q$. Hence $V_s := \mathbb{F}_{q^s}^{d/s} \cong \mathbb{F}_q^d$. This induces embeddings $\mathbb{F}_{q^s}^* \to \mathrm{GL}_d(q)$, and $\Gamma\mathrm{L}_{d/s}(q^s) \to N_{\mathrm{GL}_d(q)}(\mathbb{F}_{q^s}^*) \leq \mathrm{GL}_d(q)$.

Abuse of notation! Here $\Gamma\mathrm{L}_{d/s}(q^s)$ is semilinear maps f on $\mathbb{F}_{q^s}^{d/s}$ s.t. $(\lambda v)f = \lambda(vf)$ $\forall \lambda \in \mathbb{F}_q$.
For example, $\Gamma\mathrm{L}_{6/3}(4^3) \not\cong \Gamma\mathrm{L}_{4/2}(8^2)$.

Defn: $H \leq \mathrm{GL}_d(q)$ is semilinear if $\exists$ divisor s of d, and an $\mathbb{F}_q$-vec space isom $V_s \to V$, s.t. all elements of H act semilinearly on V_s.
s prime $\Rightarrow \Gamma\mathrm{L}_{d/s}(q^s)$ is generally maximal.

Aschbacher's Theorem for $\mathrm{GL}_d(q)$

Let $G \leq \mathrm{GL}_d(q)$. Then G is in one of the following classes:

- $\mathcal{C}_1$ Reducible groups.
- $\mathcal{C}_2$ Imprimitive groups.
- $\mathcal{C}_3$ Semilinear groups.
- $\mathcal{C}_4$ Tensor product groups.
- $\mathcal{C}_5$ Subfield groups.
- $\mathcal{C}_6$ Normalisers of extraspecial r-groups.
- $\mathcal{C}_7$ Tensor-induced groups
- $\mathcal{C}_8$ Classical groups.
- $\mathcal{S}$ $G/Z(G)$ almost simple; $G \notin \mathcal{C}_1 \cup \mathcal{C}_3 \cup \mathcal{C}_5 \cup \mathcal{C}_8$.

Aschbacher's Thm $B\Delta$: H – intersection of a maximal subgp of $\mathrm{GL}_d(q)$ with $\mathrm{SL}_d(q)$, $H \in \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_8$. Then all $\Gamma\mathrm{L}_d(q) : \langle \iota \rangle$-conjugates of H are conjugate in $\mathrm{GL}_d(q)$; except P_k and P_{d-k}.

Intro to classical groups: forms

$V = \mathbb{F}_q^d$, $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$.

Defn: A σ-sesquilinear form is a map $\beta : V \times V \to \mathbb{F}_q$ s.t. $\forall u, v, w \in V$, $\lambda, \mu \in \mathbb{F}_q$:

- $\beta(u + v, w) = \beta(u, w) + \beta(v, w)$.
- $\beta(u, v + w) = \beta(u, v) + \beta(u, w)$.
- $\beta(\lambda u, \mu v) = \lambda \mu^\sigma \beta(u, v)$.

β is bilinear if $\sigma = 1$, and symmetric if $\beta(u, v) = \beta(v, u)$.

Example 53

$u \cdot v = \sum_{i=1}^d u_i v_i$ is a symmetric bilinear form.

Defn: A quadratic form is a map $Q : V \to \mathbb{F}_q$ s.t. $\forall u, v \in V$, $\lambda \in \mathbb{F}_q$:

- $Q(\lambda v) = \lambda^2 Q(v)$.
- $\beta(u, v) := Q(u + v) - Q(u) - Q(v)$ is a symmetric bilinear form, the polar form of Q.

Classifying forms

Defn: A σ-sesquilinear form β is quasi-symmetric if $\exists\ \lambda \in \mathbb{F}_q^*$ and $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ s.t. $\forall u, v \in V$, $\beta(v, u) = \lambda\beta(u, v)^\theta$.

Theorem 54 (Birkhoff-von Neumann)

β – non-zero quasi-symmetric σ-sesquilinear form. Then $\sigma = \theta$, and up to similarity, one of the following holds:

1. $\sigma = 1$, $\lambda = -1$ *and* $\beta(v, v) = 0$. *Symplectic.* $\beta(u, v) = -\beta(v, u)$.
2. $|\sigma| = 2$ *and* $\lambda = 1$. *Unitary.* $\beta(u, v) = \beta(v, u)^\sigma$
3. $\sigma = 1$ *and* $\lambda = 1$. *Orthogonal.* $\beta(u, v) = \beta(v, u)$.

Defn: β is non-degenerate if $\beta(u, v) = 0\ \forall\ u \in V \Rightarrow v = 0$. Q is non-degenerate if polar form is non-degenerate.

Defn: A classical form is a non-degenerate unitary, symplectic or quadratic form, or the zero form.

Unitary forms require $\mathbb{F} = \mathbb{F}_{q^2}$. Set $u = 2$ if form is unitary, $u = 1$ o/wise.

Subspaces of classical geometries (V, κ)

Defn: Let $f = \beta$ or f be the polar form of Q. $W \leq (V, \kappa)$ is

- non-degenerate if $f\,|_W$ is non-degenerate.
- totally isotropic if $f\,|_W$ is identically zero.
- totally singular (t.s.) if $\kappa\,|_W$ is identically zero.

Defn: Invertible linear map $g : (V, \beta_V) \to (W, \beta_W)$ is an isometry if $\forall u, v \in V$, $\beta_V(u, v) = \beta_W(ug, vg)$.
$\mathrm{Isom}(\kappa) := \{$all isometries $V \to V\}$.

Theorem 55 (Witt's Theorem)

*$(V_1, \kappa_1), (V_2, \kappa_2)$ – isometric classical geometries, with $W_i \leq V_i$.
Let $g : (W_1, \kappa_1) \to (W_2, \kappa_2)$ be an isometry.
Then g extends to an isometry from V_1 to V_2.*

Corollary 56

All maxl t.s. subspaces of (V, κ) have the same dim.

This dim is the Witt index of κ. Two possibilities if $\kappa = Q$ and d even; one o/wise.

Classical groups: definitions and simplicity

Theorem 57

κ_1, κ_2 – classical forms of same type, with same Witt index, and not quadratic in odd dim. Then $\exists\ g \in \mathrm{GL}_d(q^u)$ s.t. $\mathrm{Isom}(\kappa_1)^g = \mathrm{Isom}(\kappa_2)$.

Defn: κ – classical form on $\mathbb{F}_{q^u}^d$, $G = \mathrm{Isom}(\kappa)$ is:
κ unitary: $\mathrm{GU}_d(q)$. κ symplectic: $\mathrm{Sp}_d(q)$.
κ quadratic: $\mathrm{GO}_d^{\varepsilon}(q)$. d odd $\Rightarrow \varepsilon = \circ$ and q odd;
d even: Witt index $d/2 \Rightarrow \varepsilon = +$, Witt index $d/2 - 1 \Rightarrow \varepsilon = -$.

Theorem 58

If $g \in \mathrm{Sp}_d(q)$ then $\det(g) = 1$ and d is even.

$G \cap \mathrm{SL}_d(q^u)$ is the special isometry group: $\mathrm{SU}_d(q)$, $\mathrm{SO}_d^{\varepsilon}(q)$.
for $d \geq 7$: $\Omega_d^{\varepsilon}(q) := \mathrm{SO}_d^{\varepsilon}(q)'$.
Make projective version of each group by factoring by scalars.

Theorem 59

The groups $\mathrm{PSU}_d(q)$ ($d \geq 3$), $\mathrm{PSp}_d(q)$ ($d \geq 4$ even), $\mathrm{P}\Omega_d^{\varepsilon}(q)$ ($d \geq 7$) are simple except $\mathrm{PSU}_3(2)$, $\mathrm{PSp}_4(2)$.

Subgroups of the other classical groups

Aschbacher's theorem describes all subgroups of $\mathrm{GL}_d(q)$.

So describes all subgroups of each classical group.

With a non-zero form, we can refine the statement.

Some classes may not exist for some types of classical form.

Some classes may split into more than one type.

To properly describe the maximal subgroups of the classical groups we need to understand these possibilities.

We'll look at some examples in the symplectic group.

Fix a standard symplectic form by fixing a basis of $V = \mathbb{F}_q^{2m} = \mathbb{F}_q^d$: $e_1, \ldots, e_m, f_m, \ldots, f_1$ s.t. $\beta(e_i, e_j) = 0 = \beta(f_i, f_j)$. $\beta(e_i, f_j) = \delta_{ij}$.

Reducible subgroups of symplectic groups

Lemma 60

$G \leq \mathrm{Sp}_d(q)$ – reducible, stabilising $0 < W < V$. If $G|_W$ is irreducible then W is totally isotropic or non-degenerate.

Proof.

Suppose not. Let $U := \{u \in W : \ \beta(w,u) = 0 \ \forall w \in W\}$.
$0 < U < W$. $\forall\ u \in U$, $w \in W$, $g \in G$, $\beta(ug, wg) = \beta(u, v) = 0$.
Hence $Ug = U$, and $G|_W$ is reducible. □

Theorem 61

$G \leq \mathrm{Sp}_d(q)$ – reducible, stabilising t.i. W, dim k. Up to Sp-conjugacy $G \leq$

$$\left\{ \begin{pmatrix} A & 0 & 0 \\ * & B & 0 \\ * & * & J^{-1}A^{-\mathrm{T}}J \end{pmatrix} \ : \ A \in \mathrm{GL}_k(q), B \in \mathrm{Sp}_{d-2k}(q) \right\}.$$

Theorem 62

$G \leq \mathrm{Sp}_d(q)$ – reducible, stabilising non-degenerate W, dim k. Up to Sp-conjugacy, $G \leq \mathrm{Sp}_k(q) \times \mathrm{Sp}_{d-k}(q)$.

Imprimitive subgroups of symplectic groups

An imprimitive group stabilises a decomposition $V = V_1 \oplus \cdots \oplus V_k$, and (in general) acts transitively on it.
Can show only two possibilities:

- Each V_i is totally singular.
- Each V_i is nondegenerate.

Theorem 63
$G \leq \mathrm{Sp}_d(q)$ imprimitive, with V_i totally singular. Then $k = 2$ and $G \leq \mathrm{GL}_{d/2}(q).2$.

Theorem 64
$G \leq \mathrm{Sp}_d(q)$ imprimitive. Then d/k even, and $G \leq \mathrm{Sp}_{d/k}(q) \wr \mathrm{S}_k$.

Exercises on Lecture 3

1. Show that $\Gamma\mathrm{L}(V)$ is a group and that the map $\Gamma\mathrm{L}_d(q) \to \mathsf{Aut}(\mathbb{F}_q)$ is a homomorphism.
2. Show that if $p \neq 2$ and $q = p^e$ then a quadratic form on $\mathbb{F}_q^d$ is completely determined by its polar form.
3. Prove that $\mathrm{PSL}_d(q)$ is simple if $(d, q) \neq (2, 2), (2, 3)$. You will need: Iwasawa's Lemma G – finite perfect, acting faithfully and primitively on Ω, s.t. G_α has a normal abelian subgroup A s.t. $\langle g^{-1}Ag : g \in G\rangle = G$. Then G is simple. $\square$

   3.1 Let $\Omega = \{$1-dim subspaces of $\mathbb{F}_q^d\}$. Show that $\mathsf{SL}_d(q)$ acts on Ω, and that $\mathrm{PSL}_d(q)$ acts faithfully and primitively on Ω.

   3.2 Show that $(\mathsf{SL}_d(q))_{\langle v_1\rangle}$ has a normal abelian subgroup A.

   3.3 Show that every element of A is a transvection: a matrix m s.t. $m - I_d$ has rank 1, and $(m - I_d)^2 = 0$.

   3.4 Show that every transvection is contained in a conjugate of A, and that $\mathsf{SL}_d(q)$ is generated by transvections.

   3.5 Show that if $(d, q) \neq (2, 3)$ then $\mathsf{SL}_d(q)$ is perfect. [Hint: show every transvection is a commutator].