Notes on GTM251

Yuandong Li

December 11, 2023

Contents

1 Introduction

Pace:

1. Chapter 1 (Overview)
2. §2.1-§2.4 (Group action, A_n)
3. §2.5-§2.7 (O'Nan-Scott, maximal subgroups of S_n and A_n, cover)
4. §3.1-§3.3 ($\mathrm{PSL}_n(q)$)
5. §3.4 (forms: bilinear, sesquilinear, quadratic)
6. §3.5 ($\mathrm{PSp}_{2m}(q)$)
7. §3.6 ($\mathrm{PSU}_n(q)$)
8. §3.7 ($\mathrm{P\Omega}_m(q)$, odd q)
9. §3.8 ($\mathrm{P\Omega}_{2n}(q)$, even q)
10. §3.10 (maximal subgroups of classical groups)

References:

Main: The finite simple groups - Wilson (GTM 251)

Perm.: Permutation Groups - J.D. Dixon, B. Mortimer (GTM 163)

Finite permutation groups - Wielandt

Class.: The Subgroup Structure of the Finite Classical Groups - Kleidman & Liebeck

The Maximal Subgroups of the Low-Dimensional Finite Classical Groups - J.N. Bray, et al.

[Notes] Classical Groups without Orthogonal (2021fall) - C.H. Li, P.C. Hua

More: (notes and papers to be referred)

1.1 History

Galois(1830s): A_n, $\mathrm{PSL}_2(p)$, realized the importance

Jordan-Hölder: $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$, where G_i/G_{i-1} is simple

Camille Jordan (1870): $\mathrm{PSL}_n(q)$

Sylow theorem (1872): the first tools for classifying finite simple groups

Mathieu(1860s): M_{11}, M_{12}, M_{22}, M_{23}, M_{24}

L.E. Dickson(1901): classical groups, inspired by Lie algebras

Chevalley(1955): a uniform construction of $\mathrm{PSL}_{n+1}(q)$, $\mathrm{P\Omega}_{2n+1}(q)$, $\mathrm{PSp}_{2n}(q)$, $\mathrm{P\Omega}^+_{2n}(q)$

"twisting": ${}^3D_4(q)$, ${}^2E_6(q)$

Feit-Thompson(1963): odd order is soluble, hence nonab. FSG has an involution

1960s: proof of CSFG began

1970s: 20 sporadic simple groups dicovered

1980s: CSFG was "almost" complete

3 generations of proof of CSFG:

1. 1982 Gorenstein, abandon after vol 1, too long, bugs in quasithin case
2. 1992 Lyons, Solomon, vol 1-6 done, bug fixed, vol 7? also too long
3. Aschbacher, et al., find some geometric characters to simplify the proof, fusion system?

1.2 CFSG

Every finite simple group is isomorphic to one of the followings:

i. a cyclic group C_p of prime order p;

ii. an alternating group A_n for $n \geq 5$;

iii. a classical group:

- linear: $\mathrm{PSL}_n(q)$, $n \geq 2$, except $\mathrm{PSL}_2(2)$ and $\mathrm{PSL}_2(3)$;
- unitary: $\mathrm{PSU}_n(q)$, $n \geq 3$, except $\mathrm{PSU}_3(2)$;
- symplectic: $\mathrm{PSp}_{2n}(q)$, $n \geq 2$, except $\mathrm{PSp}_4(2)$;
- orthogonal: $\mathrm{P}\Omega_{2n+1}(q)$, $n \geq 3$, q odd; $\mathrm{P}\Omega^+_{2n}(q)$, $\mathrm{P}\Omega^-_{2n}(q)$, $n \geq 4$;

where q is a power p^a of a prime p;

iv. an exceptional group of Lie type:

$$G_2(q), q \geq 3;\ F_4(q);\ E_6(q);\ {}^2E_6(q);\ {}^3D_4(q);\ E_7(q);\ E_8(q)$$

with q a prime power, or

$${}^2B_2(2^{2n+1}),\ {}^2G_2(3^{2n+1},\ {}^2F_4(2^{2n+1}),\ n \geq 1;$$

or the Tits group ${}^2F_4(2)'$;

v. one of 26 sporadic simple groups:

- the five Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24};
- the seven Leech lattice groups Co_1, Co_2, Co_3, McL, HS, Suz, J_2;
- the three Fischer groups Fi_{22} , Fi_{23}, Fi'_{24} ;
- the five Monstrous groups $\mathbb{M}$, $\mathbb{B}$, Th, HN, He;
- the six pariahs J_1, J_3, J_4, O'N, Ly, Ru.

Conversely, every group in this list is simple, and the only repetitions in this list are:

$$\begin{aligned} \mathrm{PSL}_2(4) \cong &\mathrm{PSL}_2(5) \cong A_5; \\ &\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2); \\ &\mathrm{PSL}_2(9) \cong A_6; \\ &\mathrm{PSL}_4(2) \cong A_8; \\ &\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3). \end{aligned}$$

introduction, construction, orders, simplicity, **action(reveal subgroup structure)**

1.3 After CFSG

1.3.1 Permutation group theory

Classify

- multiply-transitive groups
- 2-transitive groups
- primitive permutation groups (O'Nan-Scott Thm): reduce to AS case

1.3.2 Maximal subgroups of simple groups

A_n : O'Nan-Scott, Liebeck-Praeger-Saxl
(The symmetric difference set of AS subgroups and maximal subgroups of A_n is listed out, while listing their intersection is impossible.)

Classical: began with Aschbacher,1984, see Kleidman-Liebeck and Low-dimension.

Exceptional: Done recently by David Craven, see arXiv

Sporadic: Done. See a survey by Wilson and recent work on arXiv for the Monster.

2 The Alternating Groups

2.1 The O'Nan-Scott Theorem

2.1.1 Some Lemmas

2.1.2 The proof of the O'Nan-Scott Theorem

Last week we introduced some lemmas and proved part of the O'Nan-Scott Theorem. This week we will finish the proof of the O'Nan-Scott Theorem.

Notation: Let H be a subgroup of S_n not containing A_n, N be a minimal normal subgroup of H, and K be the stabilizer in H of a point.

H intransitive $\implies$ case (i).

H transitive imprimitive $\implies$ case (ii).

Now we assume H primitive. And hence the discussion zooms into soc(H).

$\exists N$ abelian $\implies$ case (iv)affine.

Additionally we assume $\forall N$ nonabelian.

If H has more than one minimal normal subgroups $N_1 \neq N_2$.

It can be shown that $\exists x \in S_n$ conjugates N_1 to N_2. specify x

By corollary 2.11, x also conjugates $N_2 = C_H(N_1)$ to $N_1 = C_H(N_2)$. (Why?)

Hence $H < \langle H, x \rangle$, which has a unique minimal normal subgroup $N_1 \times N_2$.

Additionally we assume H has a unique minimal normal subgroup N, which is nonabelian.

N simple $\implies C_H(N) = 1 \implies H \overset{\text{conj.}}{\curvearrowright} N$ faithfully $\implies$ case (vi)AS.

$N = T^m = T_1 \times \cdots \times T_m$ with $m > 1 \implies H \overset{\text{conj.}}{\curvearrowright} \{T_1, \cdots, T_m\}$ transitively, and K as well.

Let $K_i := p_i(K \cap N) \leq T_i$ the projection of K onto T_i. Then $K \cap N \leq K_1 \times \cdots \times K_m$.

We divide the discussion into 2 cases. Before that, we claim the following fact.

Claim: K normalizes $K_1 \times \cdots \times K_m$.

Proof. Since $K \cap N \lhd K$, $\forall k \in K$, $\forall x \in K \cap N$,

we have $x = p_1(x) \cdots p_m(x)$, and $p_1(x)^k \cdots p_m(x)^k = x^k = p_1(x^k) \cdots p_m(x^k) \in K \cap N$.

Then $p_i(x)^k = p_j(x^k)$ whenever $T_i^k = T_j$. (In direct product, equal iff. all coordinates equal.)

$\forall y \in K_1 \times \cdots \times K_m$, $\exists x_1, \cdots, x_m \in K \cap N$ s.t. $y = p_1(x_1) \cdots p_m(x_m)$.

Then $y^k = p_1(x_1)^k \cdots p_m(x_m)^k = p_1(x_{l_1}^k) \cdots p_m(x_{l_m}^k) \in K_1 \times \cdots \times K_m$, where $T_i = T_{l_i}^k$. $\square$

Case $K_i \neq T_i$ for some i:

Now $K \cap N \leq K_1 \times \cdots \times K_m < N$.

By corollary 2.15, $K_1 \times \cdots \times K_m = K \cap N$ and K permutes K_i's transitively. Let $k := |T_i : K_i|$.

Then $H = (T_1 \times \cdots \times T_m) \rtimes K \leq S_k \wr S_m \curvearrowright [T_1 : K_1] \times \cdots \times [T_m : K_m] \implies$ case (iii)PA.

Case $K_i = T_i$ for all i:

Support of $(t_1, \cdots, t_m) \in N$ is defined as $\mathrm{supp}(t) := \{i \mid t_i \neq 1\}$.

$\Omega_1 :=$ a non-empty min.(with set inclusion) supp. of an elt in $K \cap N$.

Claim: Ω_1 a block of $K, H \curvearrowright [m]$ which is induced by $K, H \curvearrowright \{T_1, \cdots, T_m\}$.

Proof. All elts in $K \cap N$ with support Ω_1 (i.e. $t_i \neq 1$ and $t_j = 1$ $\forall i \in \Omega_1, \forall j \notin \Omega_1$) together with 1 forms a normal subgroup of $K \cap N$, which maps onto a normal subgroup of hence T_i itself $\forall i \in \Omega_1$. $\forall g \in K$, if $\Omega_1 \cap \Omega_1^g \neq \emptyset, \Omega_1$, then $\exists x \in K \cap N$ s.t. $\mathrm{supp}(x) = \Omega_1$ and $\mathrm{supp}(x^g) = \Omega_1^g$. Now $[x, x^g] \neq 1$ and $\mathrm{supp}([x, x^g]) \subset \Omega_1 \cap \Omega_1^g$, contradicting to the minimality of Ω_1. $\square$

$|\Omega_1| = 1 \implies N \leq K$, a contradiction.

$|\Omega_1| = m \implies K \cap N = \{(t, \cdots, t) \mid t \in T\}$ WLOG. $N \curvearrowright [N : K \cap N] \implies$ case (v)diagonal.

$\forall i, \forall x, y \in K \cap N$, $p_i(x) = p_i(y) \implies p_i(xy^{-1}) = 1 \implies \mathrm{supp}(xy^{-1}) = \emptyset \implies xy^{-1} = 1$ i.e. $p_i|_{K \cap N}$ is injective. Since $K_i = T_i$, $p_i|_{K \cap N}$ is surjective hence bijective. Thus $K \cap N$ is now a full diagonal subgroup of N. Then the coset action $N \curvearrowright [N : K \cap N]$ is of diagonal type. Now identify each $\alpha^g \in \Omega$ with the corresponding coset $(H_\alpha \cap N)g$. The stabilizer $N_{\alpha^g} = H_{\alpha^g} \cap N = (H_\alpha \cap N)^g$ is also the stabilizer of the coset $(H_\alpha \cap N)g$.

Remark. Actually, $K \cap N$ is a full diagonal subgroup of $N \implies K \cap N = \{(t^{\varphi_1}, \cdots, t^{\varphi_m}) \mid t \in T\}$ where φ_i is an isomorphism from T to T_i. For each $\beta \in \Omega$, we have an $H_\beta \cap N$ and can determine ψ_i's basing on φ_i's, since the $H_\beta \cap N$'s are conjugate to $H_\alpha \cap N$ by the transitive group N. In detail, suppose $\alpha^g = \beta$ for some $g \in N$ and $H_\alpha \cap N = \{(t^{\varphi_1}, \cdots, t^{\varphi_m}) \mid t \in T\}$ and $H_\beta \cap N = \{(t^{\psi_1}, \cdots, t^{\psi_m}) \mid t \in T\}$ where ψ_i, φ_i are isomorphisms from T to T_i. Then $H_\alpha \cap N$ is conjugate to $H_\beta \cap N$ by g. This means we can take $(\varphi_1^{-1}\psi_1, \cdots, \varphi_m^{-1}\psi_m) = \tilde{g} \in \mathrm{Inn}(N)$ on $H_\alpha \cap N$. Thus once $(\varphi_1, \cdots, \varphi_m)$ is given, we could let $\psi : T \to H_\alpha \cap N \to H_\beta \cap N$ be $(\psi_1, \cdots, \psi_m) = (\varphi_1, \cdots, \varphi_m)\tilde{g} = (\varphi_1 \tilde{g}_1, \cdots, \varphi_m \tilde{g}_m)$.

$|\Omega_1| = k \neq 1, m$:

Suppose Ω_1 is in a block system $\{\Omega_1, \cdots, \Omega_l\}$ of K on $[m]$. Let $N_j = \bigtimes_{i \in \Omega_j} T_i$ for $j = 1, \cdots, l$. Then $N = N_1 \times \cdots \times N_l \cong T^{kl}$. For each N_j, $N_j \cap K$ is a diagonal subgroup of N_j.

$$\implies N = \left(\bigtimes_{i \in \Omega_1} T_i \right)^l \cong T^{kl}, \; N \cap K = \left(\mathrm{diag}\left(\bigtimes_{i \in \Omega_1} T_i \right) \right)^l \cong T^l.$$

The action of each $\bigtimes_{i \in \Omega_1} T_i$ is diagonal of degree $r = |T|^{k-1}$. $H \leq S_r \wr S_l \curvearrowright [r]^l \implies$ case (iii)PA.

2.2 Covering Groups

2.2.1 Schur Multiplier

A_n as quotient group of $2.A_n$.

Let $+\pi$ and $-\pi$ be the two preimages of $\pi \in A_n$ under the natural quotient map. But there is no canonical choice of which element gets which sign.

Let $+1$ be the identity in $2.A_n$. For each $\pi \in A_n$, we define $+\pi$ to be the element which multipilied together with $+1$ gives itself, and $-\pi$ for the other one.

Definition 2.1. *$\tilde{G}$ is a covering group of G if $Z(\tilde{G}) \leq \tilde{G}'$ and $\tilde{G}/Z(\tilde{G}) \cong G$.*

If $|Z(\tilde{G})| = 2, 3$, then the covering group is called double, triple cover.

Theorem 2.2 (Schur)**.** *Every finite perfect group G has a unique maximal covering group $\tilde{G}$, with the property that every other covering group is a quotient of $\tilde{G}$. We call $\tilde{G}$ the **universal covering group** of G and $Z(\tilde{G})$ the **Schur multiplier** of G, denoted as $M(G)$.*

Example 2.3 (non-perfect)**.** *$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle \alpha \rangle \times \langle \beta \rangle$ has four maximal covering groups: one Q_8 and three D_8.*

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, $Z(Q_8) = \{\pm 1\}$, $Q_8/Z(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

$D_8 = \langle a \rangle : \langle b \rangle$, $Z(D_8) = \langle a^2 \rangle$, $D_8/Z(D_8) = \langle Z(D_8)a \rangle \times \langle Z(D_8)ab \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

see my iphone

Example 2.4. *The alternating groups A_n ($n > 4$) only have double covers, except for A_6 and A_7 both with the same Schur multiplier $\mathbb{Z}_6$.*

2.2.2 Double Covers of A_n and S_n

Now we define $2.S_n$.

Firstly, let G be a set of order $2n!$, with a map φ onto S_n such that each $\pi \in S_n$ has exactly two preimages denoted as $+\pi$ and $-\pi$.

Intuitively, we should define the multiplication of G as $+\pi + \sigma = +(\pi\sigma)$ and $+\pi - \sigma = -(\pi\sigma)$.

WLOG, we denote $+(1\ 2)$ as $[1\ 2]$ and $-(1\ 2)$ as $-[1\ 2]$. Then for each transposition $\pi \in S_n$, taking $(+\pi)^{-1}$ to be a preimage of π, define the products (of 3 elements in G) $[i\ j]^{+\pi}$ and $[i\ j]^{-\pi}$ to be a same preimage of $(i^\pi\ j^\pi)$, we denote it as $-[i^\pi\ j^\pi]$. That is $[i\ j]^{\pm\pi} = -[i^\pi\ j^\pi]$.

Then define the preimage $+(a_i, a_{i+1}, \cdots, a_j)$ by

$$[a_i\ a_{i+1}\ \ \cdots\ \ a_j] = [a_i\ a_{i+1}][a_i\ a_{i+2}] \cdots [a_i\ a_j].$$

Finally by multiplying together disjoint cycles in the usual way, we obtain all elements.

The multiplication defined above is well-defined. That is, if we compute the same product in two different ways, we get the same result. A proof using construction of double cover of orthogonal group is given in Section 3.9.

Note that, by the rule $[i\ j]^{\pm\pi} = -[i^\pi\ j^\pi]$ to define $[i\ j]$'s, all the elements $\pm[i\ j]$ are conjugate. Thus they are all square to 1 or -1 simotaneously. Whatever, the elements like $\pm[1\ 2][3\ 4]$ always square to -1.

Therefore, we obtain two distinct double cover of S_n. We denote $2.S_n^+$ (actually $\mathbb{Z}_2 \times S_n$) as the one with $|[i\ j]| = 2$ (where $(i\ j)$ is identified with a coset $Z(2.S_n)a$ with a of order 2), and $2.S_n^-$ as the other one with $|[i\ j]| = 4$ ($(i\ j)$ a coset of an element of order 4). However, both of them has the same subgroup $2.A_n \cong \mathbb{Z}_2 \times A_n$ of index 2, which is the unique double cover of A_n.

Example 2.5.

- $2.S_4^+ \cong \mathbb{Z}_2 \times S_4$ *is the group of symmetries of the cube, where* S_4 *permutes the four diagonals of the cube, and* $\mathbb{Z}_2$ *permutes the two opposite vertices in a diagonal simotaneously.*
- $2.S_4^- \cong \mathrm{GL}_2(3)$ *where* S_4 *permutes the four lines through the origin in* $\mathbb{F}_3^2$*, and* $\mathbb{Z}_2$ *(i.e. scalar matrices) permutes the two points on each line simotaneously.*

  Note that $\mathrm{SL}(2,3) = 2.A_4$ *is the unique subgroup of order 24 in* $\mathrm{GL}_2(3)$*.*

2.2.3 Triple Covers of A_6 and A_7

2.3 Coxter Groups

3 The Classical Groups

3.1 Introduction

'Classical' simple groups: linear groups, unitary groups, symplectic groups, orthogonal groups.

Mainly obtained by taking $G'/Z(G')$ from suitible matrix groups G.

Definition	Simplicity	Subgroups	Automorphisms & Covering groups	Isomorphisms
$PSL_n(q)$	Iwasawa's lemma	geometry	(briefly mentioned)	projective spaces

Symplectic groups: easy to understand, orders, simplicity, subgroups, covering groups, automorphisms, generic isomorphism $\mathrm{Sp}_2(q) \cong \mathrm{SL}_2(q)$, exceptional isomorphism $\mathrm{Sp}_4(2) \cong S_6$.

Unitary groups: similar to symplectic groups.

Orthogonal groups:

- fundamental differences between the cases of $\mathrm{char}F = 2$ or odd
- subquotient is not usually simple
- to get usually simple groups, using spinor norm for odd char (see Clifford algebras and spin groups), and quasideterminant for char 2
- generic isomorphisms $\mathrm{P}\Omega_6^+(q) \cong \mathrm{PSL}_4(q)$, $\mathrm{P}\Omega_6^-(q) \cong \mathrm{PSU}_4(q)$, $\mathrm{P}\Omega_5(q) \cong \mathrm{PSp}_4(q)$ all derive from the Klein correspondence

A simple version of Aschbacher-Dynkin theorem is proved, relying heavily on representation theory.

More explicit versions for individual classes of groups see Kleidman and Liebeck's book.

Some exceptional behavior of small classical groups is related to exceptional Weyl groups.

3.2 Finite fields

Please refer to literatures about finite fields for more details.

Definition 3.1. *field* $(F, +, \cdot)$

Lemma 3.2. *All non-zero elements have the same additional order of prime p.*

Proof. $F^\times \curvearrowright F^+\backslash\{0\}$ by multiplication as group automorphism (distributive law) transitively. ☐

Definition 3.3. *The p above is the* ***characteristic*** *of F. $F_0 := \langle 1 \rangle_+$ is the* ***prime subfield*** *of F.*

Lemma 3.4. $|F| = p^d$

Proof. F is a vector space over F_0. ☐

Lemma 3.5. *$F^\times = \langle \sigma \rangle \cong \mathbb{Z}_{p^d-1}$, where σ is called a* ***Singer cycle****.*

Proof. By Vandermonde's lemma, polynomial of degree n on F has at most n solutions in F. $e := \exp(F^\times) < |F^\times| \implies x^e - 1 = 0$ has $|F^\times| > e$ solutions. $\square$

Proposition 3.6. *For any prime power $q = p^d$, $\exists_1 F$ of order q up to field isomorphism, says $\mathbb{F}_q$.*

Proof. Existance: $\mathbb{Z}/p\mathbb{Z}[x]/(f(x))$ for any irreducible polynomial $f(x)$ of degree d.

Uniqueness: If $|F| = p^d$, then $F_0 \cong \mathbb{F}_p$, F is the splitting field of $x^{p^d} - x$ over F_0, $F^\times = \langle x \rangle$. $\square$

Lemma 3.7. $\mathrm{Aut}(\mathbb{F}_q) = \langle \phi \rangle \cong \mathbb{Z}_d$*, where $\phi : x \mapsto x^p$ is called the* ***Frobenius automorphism****.*

Remark 3.8. *ϕ may not be a linear transformation on $\mathbb{F}_q^n$ since it may not preserve scalar multiplication.*

Definition 3.9. $\Gamma\mathrm{L}_n(q) := \mathrm{GL}_n(q) \rtimes \langle \phi \rangle$ *and* $\Sigma\mathrm{L}_n(q) := \mathrm{SL}_n(q) \rtimes \langle \phi \rangle$

Lemma 3.10. *$x^n = 1$ has $(n, q-1)$ solutions in $\mathbb{F}_q$.*

3.3 Linear groups

Generally speaking, the classification of a certain kind of algebraic objects goes through four steps: extracting abstract concept from various examples, accumulating natural and classical families, organizing by analysis on generic properties and finally collecting sporadic cases.

As for finite simple groups, the motivation comes from Jordan-Holder theorem, since which simple groups are deemed as elementary bricks. The families of cyclic groups and alternating groups gives the very first examples. After that, mathematicians find that there are many finite simple groups of Lie type, which stem from the study of Lie algebras. Actually, such groups forms a quite large family which turns out to be the main part of the classification and is divided into classical and exceptional parts during processing. The sporadic groups are the last part, which are found case-by-case.

In this chapter, we will introduce the family of linear groups, which is the basic case of groups of Lie type, since others can be seem as stabilizers of certain structures on vector spaces.

3.3.1 Introduction

definition, order, action, corelation

The story begins with the automorphisms of linear spaces, similar to the case of symmetric groups on sets.

Definition 3.11. *The so called* ***general linear group*** $\mathrm{GL}(n, q)$ *is the group of all invertible linear transformations over vector space $V = \mathbb{F}_q^n$, or equivalently, all invertible $n \times n$ matrices over $\mathbb{F}_q$.*

Since linear group can be defined from two ways, algebraic (A) / geometric (G), there is also two parallel ways to deal with problems of linear groups. Here we follow the geometric way.

Example 3.12. $\mathrm{GL}_2(2) \cong S_3$, $\mathrm{GL}_2(3) \cong 2.S_4$.

Remark 3.13. $\mathrm{GL}_n(q)$ *acts regularly on ordered basis of* V.
Thus $|\mathrm{GL}(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{n(n-1)/2}(q-1)\cdots(q^n-1)$.

Corollary 3.14. $\mathrm{AGL}_n(q)$ *acts 2-transitively on* $\mathbb{F}_q^n$. $\mathrm{AGL}_n(2)$ *acts 3-transitively on* $\mathbb{F}_2^n$.

Proof. Note that for any two non-zero vectors $u, v \in \mathbb{F}_2^n$, u, v are linear dependent iff. $u = v$. Thus $\mathrm{GL}_n(2)$ is 2-transitive on V. □

However, the simple groups do not come out from $\mathrm{GL}(n,q)$ directly. But we have some clues.

Proposition 3.15. *A finite non-abelian simple group is perfect and center-free.*

Generally, $\mathrm{GL}_n(q)$ is neither perfect nor center-free. Since perfection is inherited when taking quotient, we try to do two things: taking derived subgroup till perfect and then moduling center till center-free. This could lead to some simple groups.

Firstly, we need to find the derived subgroup of $\mathrm{GL}_n(q)$. Note that commutators in $\mathrm{GL}_n(q)$ are of the form $[A,B] = ABA^{-1}B^{-1}$, which has determinant 1. Hence we can restrict our scope to a subgroup.

Definition 3.16. *Consider the group homomorphism* $\det : \mathrm{GL}_n(q) \to \mathbb{F}_q^\times$, $g \mapsto \lambda_1 \cdots \lambda_n$, *its kernel is denoted as* $\mathrm{SL}_n(q)$, *named* ***special linear group***.

Remark 3.17. $|\mathrm{SL}_n(q)| = |\mathrm{GL}_n(q)|/|\mathbb{F}_q^\times| = q^{n(n-1)/2}(q^2-1)\cdots(q^n-1)$.

Similar as S_n, A_n has basic generators 2-cycles, 3-cycles resp. with the most fixed points, we look at a $\tau \in \mathrm{GL}(V)$ which fixes a hyperplane W point-wise. Suppose $V = W \oplus \langle v \rangle$. Then

Definition 3.18.

$$v^\tau = \begin{cases} \alpha v \text{ for } \alpha \in F\backslash\{0,1\}, & \tau \text{ is called a } \textbf{dilatation} \text{ or a } \textbf{homology} \text{ (in projective version)}. \\ v + w \text{ for } w \in W\backslash\{0\}, & \tau \text{ is called a } \textbf{transvection} \text{ or an } \textbf{elation} \text{ (in projective version)}. \\ \alpha v + w \text{ for } \alpha \in F\backslash\{0,1\}, w \in W, & u := v + (a-1)^{-1}w \text{ then reduce to the first case.} \end{cases}$$

A transvection is denoted by $\tau(w,\varphi)$ *where* $\varphi \in V^*\backslash\{0\}$ *with* $W = \ker\varphi$.

Lemma 3.19 (properties of transvections)**.**

1. $\tau \in \mathrm{SL}$;
2. $\tau(\alpha w, \varphi) = \tau(w, \alpha\varphi)$;
3. $\tau(w_1,\varphi)\tau(w_2,\varphi) = \tau(w_1+w_2,\varphi)$;
4. $\tau(w,\varphi_1)\tau(w,\varphi_2) = \tau(w,\varphi_1+\varphi_2)$;
5. $(\tau(w,\varphi))^g = \tau(w^g, \varphi \circ g)$, $\forall g \in \mathrm{GL}$;
6. *all transvections are conjugate in* $\mathrm{GL}_{n\geq 2}(q)$ *and* $\mathrm{SL}_{n\geq 3}(q)$ *by adjusting images in* $\ker\varphi_2\backslash\langle w_2\rangle$.

Lemma 3.20. $T_w := \{\tau(w,\varphi) \mid \varphi \in V^*, \varphi(w) = 0\}$ *is an abelian normal subgroup of* $(\mathrm{SL}_n(q))_w$.

Lemma 3.21.

i. The transvections (elations) generate SL (PSL).

ii. The transvections (elations) together with dilatations (homologies) generate GL (PGL).

Proof. Let T be the group generated by transvections. Obviously, $T \leq \mathrm{SL}$.
If $n = 1$, then $T = 1 = \mathrm{SL}_1(q)$. Suppose $n \geq 2$ and $V = W \oplus \langle v\rangle$.
Then $\forall \rho \in \mathrm{SL}_n(q)$, $\exists \tau_1 \in T$ s.t. $v^{\rho\tau_1} = v^\rho + (v - v^\rho) = v \notin W^{\rho\tau_1} \cup W$.
Then $\exists \tau_2$ s.t. $v^{\rho\tau_1\tau_2} = v$ and $W^{\rho\tau_1\tau_2} = W$. (fixing $W^{\rho\tau_1} \cap W$, $v^{\rho\tau_1}$ and taking $W^{\rho\tau_1}$ to W)
Now $(\rho\tau_1\tau_2)|_W \in \mathrm{SL}(W)$ is a product of transvections on W.
Expanding them to transvections on V we can express ρ as product of transvections. □

Lemma 3.22. $\mathrm{GL}_n(q)' = \mathrm{SL}_n(q) = \mathrm{SL}_n(q)'$ *except for* $\mathrm{SL}_2(2) \cong S_3$, $\mathrm{SL}_2(3)' \cong Q_8$.

Proof. Since $\mathrm{SL}' \leq \mathrm{GL}' \leq \mathrm{SL}$, we only need to prove $\mathrm{SL}_n(q) \leq \mathrm{SL}_n(q)'$.
It is sufficient to show that a transvection is a commutator then conjugate in $\mathrm{SL}_n(q)$.
For $n \geq 3$, $\tau(w^g - w, \varphi) = \tau(-w, f)g^{-1}\tau(w, f)g = [\tau(w,\varphi), g]$.
For $n = 2$ and $q \geq 4$, take $V = \langle u, v\rangle$, $\tau : u \mapsto u$, $v \mapsto u + v$, $g = \mathrm{diag}(a, a^{-1})$, $a \in F\backslash\{0, 1\}$.
Then $\tau((1 - a^2)u, -\varphi) = [\tau(u,\varphi), g]$.
Exceptions: $\mathrm{GL}_2(2) = \mathrm{SL}_2(2)$, $\mathrm{GL}_2(3) \cong 2.S_4 \cong Q_8 : S_3$. □

Now we consider the center. By linear algebra, $Z := Z(\mathrm{GL}(n,q))$ consists of all scalar matrices and isomorphic to $\mathbb{F}_q^\times$. And $Z(\mathrm{SL}(n,q)) \leq Z$ for the same reason.(Consider $C_{\mathrm{GL}_n(q)}(\{I + E_{ij} | i \neq j\})$.) Taking quotient we get **projective general linear groups** $\mathrm{PGL}_n(q) := \mathrm{GL}_n(q)/Z$ and **projective special linear groups** $\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/(Z \cap \mathrm{SL}_n(q))$. By definition, $\mathrm{PSL}_n(q)$ is not a subgroup but is isomorphic to a normal subgroup of $\mathrm{PGL}_n(q)$.

Remark 3.23. $|\mathrm{PGL}_n(q)| = |\mathrm{GL}_n(q)|/|\mathbb{F}_q^\times| = q^{n(n-1)/2}(q^2 - 1)\cdots(q^n - 1)$.

$|\mathrm{PSL}_n(q)| = |\mathrm{SL}_n(q)|/|Z \cap \mathrm{SL}_n(q)| = \frac{1}{(n,q-1)}q^{n(n-1)/2}(q^2 - 1)\cdots(q^n - 1)$.

Remark 3.24. *For* $(n, q) \neq (2, 2), (2, 3)$, SL *is perfect and hence a covering group of* PSL. *However, if* $q - 1 > (n, q - 1)$, *then* $Z \not\subseteq \mathrm{GL}' \leq \mathrm{SL}$ *and hence* GL *is not a covering group of* PGL.

Proposition 3.25. $\mathrm{SL} \cong \mathrm{PGL} \iff (n, q - 1) = 1$, $\mathrm{GL} = \mathrm{SL} \cong \mathrm{PGL} \cong \mathrm{PSL} \iff q = 2$.

Now we introduce some actions of linear groups.

Definition 3.26. *The **projective geometry** of $V = \mathbb{F}_q^n$ is the set of all 1-dimensional subspaces of V, denoted as* $\mathrm{PG}(n - 1, q)$.

Proposition 3.27. $\mathrm{GL}_n(q)$ *acts transitively on* $\mathrm{PG}(n-1, q)$ *with kernel* $Z(\mathrm{GL}_n(q))$. *Thus* $\mathrm{PGL}_n(q)$ *acts faithfully transitively on* $\mathrm{PG}(n - 1, q)$.

Proposition 3.28. $\mathrm{PGL}_n(q)$ *acts regularly on **frames** of* $\mathrm{PG}(n - 1, q)$, *the set of all $(n+1)$-tuples on* $\mathrm{PG}(n - 1, q)$ *with the property that no n points lie in a hyperplane.*

Corollary 3.29. $\mathrm{PGL}_2(q)$ *is sharply 3-transitive on* $\mathrm{PG}(1, q)$*, while* $\mathrm{PGL}_{n>2}(q)$ *is only 2-transitive on* $\mathrm{PG}(n-1, q)$.

Proof. Any three distinct points in $\mathrm{PG}(1, q)$ form a frame.
However, three distinct points in $\mathrm{PG}(n-1, q)$ with $n > 2$ might be collinear or not. $\square$

Remark 3.30. *Explict action of* $\mathrm{PGL}_2(q)$ *on* $\mathrm{PG}(1, q)$ *by* ***linear fractional representation****.*

Corollary 3.31. $\mathrm{PSL}_n(q)$ *acts 2-transitively on* $\mathrm{PG}(n-1, q)$ *by suitibly choosing images to adjust the determinant to be 1.*

Theorem 3.32 (Fundamental Theorem of Projective Geometry)**.** $\mathrm{Aut}(\mathrm{PG}(n-1, q)) = \mathrm{P\Gamma L}(n, q)$.

3.3.2 Simplicity of $\mathrm{PSL}_n(q)$

Lemma 3.33 (Iwasawa)**.** *If finite group G satisfies the following conditions, then G is simple.*

i. $G' = G$;

ii. *G is primitive on some set* Ω;

iii. $\exists A \trianglelefteq G_\alpha$ *where A is solvable;*

iv. $G = A^G$.

i.e. A perfect primitive group G, being the normal closure of an abelian normal subgroup A of its point stabilizer, is simple.

Proof. Suppose that $1 \neq N \trianglelefteq G$. Then, by primitivity, N is transitive on Ω and hence $G = G_\alpha N$. For any $g \in G$, $g = hn$ for some $h \in G_\alpha$ and $n \in N$.

Then $a^g = a^{hn} = a^n$, $\forall a \in A$, since $A \trianglelefteq G_\alpha$. Moreover, $a^n = a(n^{-1})^a n \in AN$ since $N \trianglelefteq G$. Thus $G = A^G = AN$.

Now, $G/N = AN/N = A/(A \cap N)$ is solvable. Meanwhile, $(G/N)' = G'N/N = GN/N = G/N$. Thus $G/N = 1$ and $G = N$, G is simple. $\square$

Theorem 3.34. $\mathrm{PSL}_n(q)$ *is a simple group except for* $\mathrm{PSL}_2(2)$ *and* $\mathrm{PSL}_2(3)$.

The proof proceeds along Iwasawa's lemma. We have check the four conditions.

i. Find a primitive action of G; 3.31

ii. Prove perfectness; 3.22

iii. Find a solvable normal subgroup A of point stabilizer; 3.20

iv. Prove $G = A^G$. 3.21

3.3.3 Generic properties

subgroups and automorphisms

Definition 3.35. *flag*

BN-pair

Proposition 3.36. *A maximal parabolic subgroup is a maximal subgroup.*

3.3.4 Sporadic behaviours

isomorphism relations, permutation representations, covering groups, conterexample given by $L_2(q)$