Books:
Alperin and Bell (Springer), John S. Rose (Dover), M. Suzuki
This course will follow book of Wilson’s, which is relatively harder to read.

1 Introduction

$G$ is a group, finite; $|G|$ its order.

**Theorem 1.1 (Lagrange)**

$G$ finite, $H \leq G \implies |H||G|

**Sketch proof**

Distinct right cosets $Hg = \{hg| h \in H\}$ cover $G$ and all have size $|H|

$(G : H)$ the set of all right cosets of $H$ in $G$. Then $|G| = |H| \cdot |G : H|$

The map $\theta : G \to H$ is a homomorphism if $(g_1 \cdot g_2)\theta = g_1\theta \cdot g_2\theta$

It is an isomorphism of groups if also bijective

$\ker(\theta) = \{g \in G| g\theta = e_H\}$

$\theta$ is injective $\iff \ker \theta = \{e_G\}$

$\ker \theta \trianglelefteq G$

$K \leq G$ is a normal subgroup of $G$, write $K \trianglelefteq G$, if $Kg = gK \forall g \in G$

$G$ is simple if there are no normal subgroups other than $\{1\}$ and $G$, equivalently, $G$ simple $\iff$ any non-trivial homom from $G$ is injective

$K \trianglelefteq G$, can form $G/K$, a quotient group (or factor group) on the set $(G : K)$, by $Kg_1Kg_2 = Kg_1g_2$

$|G/K| = |G|/|K|$

**Theorem 1.2 (Isomorphism Theorem)**

If $\theta : G \to H$ homomorphism, then $\ker \theta \trianglelefteq G$, $\text{Im} \theta = \{g\theta| g \in G\} \leq H$, and there is an isomorphism $G/\ker \theta \cong \text{Im} \theta$

**Sketch proof**

Writing $K = \ker \theta$, check $K \trianglelefteq G$, $\text{Im} \theta \leq H$ and

$\overline{\theta} : G/K \to \text{Im} \theta$

$Kg \mapsto g\theta$

is a well-defined isomorphism
So, homomorphic images of $G$ are just quotients of $G$

**Note:** If $K \lhd G$, then

\[
\pi : G \rightarrow \overline{G} := G/K \\
g \mapsto \overline{g} := Kg
\]

i.e. quotients of $G$ are homomorphic images of $G$

\[
\theta : G \xrightarrow{\pi} \text{Im } \theta \xrightarrow{\theta} G/K
\]

**Theorem 1.3 (Second Isomorphism Theorem - Correspondence Theorem)**

Let $K \lhd G$. Then every subgroup $\overline{H}$ of $G/K$ is of the form $H/K$ for some unique $H$ with $K \leq H \leq G$. We get a lattice isomorphism between \{all subgroups of $G/K$\} and \{all subgroups of $G$ containing $K$\}

\[
\begin{array}{ccc}
G/K & \dashv & G \\
H/K \Rightarrow \overline{H} & \dashv & H \\
\{1_{G/K}\} & \dashv & K
\end{array}
\]

Moreover, $H/K \not\lhd G/K \iff H \not\lhd G$ and if so $\frac{G/K}{H/K} \cong G/H$

**Proof**

If $H \lhd G$, define a homomorphism

\[
G/K \rightarrow G/H \\
Kg \rightarrow Hg
\]

This is a homomorphism surjective onto $G/H$, kernel $H/K$ \hfill $\square$

**Theorem 1.4 (Third Isomorphism Theorem)**

Let $K \lhd G$, $H \leq G$. Then $HK \leq G$ ($HK := \{hk | h \in H, k \in K\}$) $H \cap K \lhd H$ and $H/H \cap K \cong HK/K$

**Proof**

The homomorphism

\[
\pi|_H : H \rightarrow G/K \\
h \mapsto Kh
\]

has image $HK/K$, kernel $H \cap K$ \hfill $\square$

The group of automorphisms is

\[
\text{Aut}(G) = \{ \theta : G \rightarrow G \text{ isomorphisms} \}
\]

with group operation being composition, we write $g^x$ for the image of $g \in G$ under $x \in \text{Aut}(G)$

Inner automorphisms (conjugation autos) are, for $g \in G$, $\theta_g : x \mapsto g^{-1}xg$ for $x \in G$

Then $\theta_g$ is an auto of $G$ and the map $\theta : G \rightarrow \text{Aut}(G)$ $g \mapsto \theta_g$ is a homomorphism.
Define the followings:

| Inner automorphisms | $\text{Inn}(G) := \text{Im} \theta \subseteq \text{Aut}(G)$ |
| Outer automorphism group | $\text{Out}(G) := \text{Aut}(G)/\text{Inn}(G)$ |
| Centre of $G$ | $Z(G) = \ker \theta = \{z \in G | zx = xz \, \forall x \in G\}$ |

(Note that for $G$ abelian, $Z(G) = G$, $\text{Inn}(G) = \{e\}$, $\text{Aut}(G) = \text{Out}(G)$)

**Exercise:** $\text{Aut}(D_8) \cong D_8$, $\text{Aut}(Q_8) \cong S_4$, $\text{Aut}(A_5) \cong S_5$

**Exercise:** $G = p^d$-elementary abelian of order $p^d$ (i.e. an abelian group of order $p^d$ with $x^p = 1 \, \forall x \in G$), then $\text{Aut}(G) = \text{GL}_d(p)$

If $G$ is finite.
If $Z(G) = \{1\}$, then $G \cong \text{Inn}(G) \subseteq \text{Aut}(G)$

If $G$ is simple, we have Schreier “conjecture”

$\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$ is “small” and solvable

This is a theorem now, as a consequence of the classification of finite simple groups.
E.g. $\text{Aut}(A_n) = S_n$ for $n = 5$ or $n > 6$

$\text{Aut}(A_6) = \Sigma_6$, group of order $2 \cdot 6!$

Important definition: $G^*$ is almost simple if there is a simple group $G$ with $G \cong \text{Inn}(G) \trianglelefteq G^* \leq \text{Aut}(G)$
(G is the unique minimal normal subgroup of $G^*$, and $G^*/\text{Out}(G)$)

Example: $H \trianglelefteq K \trianglelefteq G \Rightarrow H \trianglelefteq G$ (Exercise: give an example)

**Definition**

$K\,\text{char}\,G$ ($K$ is characteristic subgroup of $G$) if $K^\alpha := \alpha(K) = K \, \forall \alpha \in \text{Aut}(G)$
i.e. $K$ is $\alpha$-invariant $\forall \alpha \in \text{Aut}(G)$

$G$ is characteristically simple group if it has no proper non-trivial characteristic subgroup

$K\,\text{char}\,G \Rightarrow K \trianglelefteq G$, since $\text{Inn}(G) \leq \text{Aut}(G)$

**Exercise:**

(1) $H\,\text{char}\,K \trianglelefteq G \Rightarrow H \trianglelefteq G$

(2) $H\,\text{char}\,K\,\text{char}\,G \Rightarrow \text{H}\,\text{char}\,G$

Example: $Z(G)\,\text{char}\,G$, $G'\,\text{char}\,G$

$G' = \langle [x,y] | x,y \in G \rangle$ - commutator subgroup

**Exercise:** $K \trianglelefteq G$, $G/K$ abelian $\Leftrightarrow G' \leq K$

$G$ is perfect if $G = G'$
2 Series, Jordan-Hölder Theorem

$G$ is finite (or, if infinite, need some DCC)

**Definition**
A series is a chain of subgroups $G_i$:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$$

A series is **normal** if also $G_i \trianglelefteq G \forall i$

A proper series for $G$ has all quotients $G_i/G_{i-1}$ nontrivial.

A proper series is a composition series if all quotients $G_i/G_{i-1}$ are simple (so, a composition series is one that cannot be properly refined)

**Theorem 2.1**
Any finite group has a composition series

**Proof**
If $G$ simple, stop.
Otherwise, let $K$ be a maximal normal subgroup of $G$; then $G/K$ simple and $|K| < |G|$ so contained in $K$

*Remark.* This is constructive; in fact $1 \trianglelefteq H \trianglelefteq G$ is a series for any $H \trianglelefteq G$

E.g.: $\mathbb{Z}$ has no (finite) composition series

**Theorem 2.2 (Jordan-Hölder)**
Let $G$ be finite. Then any two composition series have the same quotients, counted with multiplicity

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_a = G$$

and $$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_b = G$$

two composition series, then $a = b$ and the collectors $\{G_i/G_{i-1}\}$ and $\{H_i/H_{i-1}\}$ are the same up to isomorphism

**Example:**

```
\begin{array}{c}
S_4 \\
A_4 \\
V_4 \\
\{1\}
\end{array}
```

```
\begin{array}{c}
C_6 \\
C_3 \\
\{1\}
\end{array}
```

**Proof**
Put $H = H_{b-1}$, $K = G_{a-1}$

*Case:* $H = K$

Since $|H| < |G|$, induction applies:

We have two composition series of $H$, so they are "isomorphic"

*Case:* $H \neq K
Note that \( HK \trianglelefteq G \implies G = HK \) by maximality

\[
\begin{array}{c}
H \\
\hline
H \cap K \\
\hline
K
\end{array}
\]

\[
\begin{array}{c}
H_b = 2 \\
\hline
L_c = 2
\end{array}
\]

\[
\begin{array}{c}
\{1\}
\end{array}
\]

Find a composition series for \( H \cap K \)

Then we have four composition series for \( G \). They are isomorphic series “naturally defined”

Firstly, by induction, the two composition series for \( H \) are isomorphic (induction hypothesis), and so are those for \( K \)

Hence, the two left series for \( G \) are isomorphic, and so are the two on the right.

But also the two in the middle are isomorphic:

This is because, \( G/H = HK/H \cong K/H \cap K \), and \( G/K \cong H/H \cap K \)

Remark. All finite groups can be “broken up” into simples, i.e. have series with all quotients simple.

On the other hand, building all finite groups out of simple groups is complicated.

E.g. There are, up to isomorphism, 26 different groups of order \( 2^6 \), all have six composition factor \( C_2 \)

E.g. Composition factors \( C_2, A_5: C_2 \times A_5, \quad S_5 = \text{Aut}(A_5), \quad SL_2(5) \)

\[(Z(SL_2(5)) = \{\pm I\}, SL_2(5)/\{\pm I\} \cong A_5)\]

A chief series is a proper normal series which cannot be properly refined to a proper normal series.

i.e. \( \forall i \exists A \trianglelefteq G \) s.t. \( G_i \trianglelefteq A \trianglelefteq G_{i+1} \). The chief factors are characteristically simple

E.g. \( S_4 = A_4 = V_4 = 1 \)

Any finite group has a chief series.

Any normal series can be refined to a chief series.

Any two chief series are “isomorphic”

**Theorem 2.3**

Let \( N \) be minimal normal subgroup of \( G \). Then \( N \) is direct product of isomorphic simple groups, all conjugate in \( G \)

**Proof**

Let \( K \) be a minimal normal subgroup of \( N \).

If \( K = N \), stop

If \( K \trianglelefteq N \), then \( K \not\trianglelefteq G \)

\[\Rightarrow \exists g_1 \in G \text{ with } K^{g_1} \neq K \Rightarrow K \cap K^{g_1} = \{1\}\]

Let \( K_2 := K K^{g_1} \) (which is \( \trianglelefteq N \))

Since \( K \cap K^{g_1} \trianglelefteq N \Rightarrow K_2 \cong K \times K^{g_1} \)

If \( K_2 = N \), stop

Otherwise, \( K_2 \trianglelefteq N \Rightarrow K_2 \not\trianglelefteq G \Rightarrow \exists h \in G \text{ with } K_2^h \neq K_2 \)

i.e. \( \exists k \in K \text{ s.t. } (kk^{g_1})^h \notin K_2 \)

Notice \( (kk^{g_1})^h = k^h \cdot k^{g_1}^h \) (Aim: \( \exists g_2 \in G \text{ s.t. } K_2 \cap K^{g_2} = \{1\} \))

\[\Rightarrow \begin{cases} \text{ either } k^h \notin KK_1 \Rightarrow K^h \not\trianglelefteq K_2 \quad g_2 := h \\ \text{ or } k^{g_1} \notin KK_1 \Rightarrow K^{g_1} \not\trianglelefteq K_2 \quad g_2 := g_1 h \end{cases}\]
\[ K_3 := K_2 K^{g_2} \trianglelefteq N, \text{ and } K_2 \cap K^{g_2} = 1, \text{ so } K_3 \cong K \times K_2. \]

Continue this and we get \( N \cong K \times K^{g_1} \times K^{g_2} \times \cdots \times K^{g_k}. \)

Finally, \( K \) is simple, since, if \( X \trianglelefteq K \), then \( X \trianglelefteq N \) (as \( N \cong K \times K^{g_2} \times \cdots \times K^{g_k} \)), so \( X = K \) by minimality of \( K \) as normal in \( N \)

\[ \square \]

**Remark.**

1. The proof applies to characteristically simple groups \( N \) i.e. Characteristically simple group \( N \) are direct products of isomorphic simple groups.

In particular, all chief factors of a finite group are also direct products of isomorphic simple groups.

2. If \( N \) is characteristically simple group, then \( N = T_1 \times \cdots \times T_k \), with each \( T_i \cong T \) some simple group.

Exercise:

1. If \( T = C_p \) then \( N = V_k(p) \), a vector space over \( \mathbb{F}_p \) of dimension \( k \). There are \[ p^{k-1} + \frac{p^k - 1}{p - 1} = \cdots \]

normal subgroup

2. If \( T \) is non-abelian simple, there are precisely \( 2^k \) normal subgroup. Namely, \( T_{i_1} \times T_{i_2} \times \cdots \times T_{i_l} \)

### 2.1 Groups with operators, \( X \)-groups

(see J.S. Rose book for more details)

**Definition**

\( X \) group, \( G \) is an \( X \)-group if \( \phi : X \to \text{Aut}(G) \) a homomorphism

Define operation of \( X \) on \( G \) by \( g^x := g^{(x^\phi)} \)

\[ H \leq G \] is an \( X \)-subgroup of \( G \), write \( H \leq_X G \), if \( H \) is \( X \)-invariant (Note: \( H \leq_X G \Rightarrow H \) is an \( X \)-group)

If \( H \trianglelefteq G, H \leq_X G \Rightarrow G/H \) is an \( X \)-group via \( (Hg)^x := Hg^x \)

If \( G_1, G_2 \) are \( X \)-groups (\( X \) fixed) a homomorphism \( \alpha : G_1 \to G_2 \) is an \( X \)-homomorphism if \( (g^x)^\alpha = (g^\alpha)^x \) for \( x \in X, g \in G_1 \)

An \( X \)-group is \( X \)-simple if it has no non-trivial normal \( X \)-invariant subgroups

If \( G \) is an \( X \)-group, an \( X \)-composition series is a series

\[ 1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_a = G \]

with each \( G_i \leq_X G_{i+1}, G_i \trianglelefteq G_{i+1} \), which cannot be properly refined.

E.g.

<table>
<thead>
<tr>
<th>( G )</th>
<th>( X )</th>
<th>( X )-subgroup</th>
<th>( X )-series</th>
<th>( X )-comp. series</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G )</td>
<td>( 1 )</td>
<td>subgroup</td>
<td>series</td>
<td>comp. series</td>
</tr>
<tr>
<td>( G )</td>
<td>( \text{Inn}(G) )</td>
<td>normal subgroup</td>
<td>normal series</td>
<td>chief series</td>
</tr>
<tr>
<td>( G )</td>
<td>( \text{Aut}(G) )</td>
<td>normal subgroup</td>
<td>normal series</td>
<td>chief series</td>
</tr>
</tbody>
</table>

Another example: \( G \)-modules

\( G \) any group, \( \rho : G \to GL(V) \) a finite dimensional representation over some field. Set \( X = \text{Im} \rho \), then \( V \) is an \( X \)-group

In this setup, one proves existence of \( X \)-composition series, \( X \)-isomorphism theorems and \( X \)-Jordan-Hölder theorem
3 (Finite) Nilpotent Groups

**Definition**
The normal series $1 = G_0 \unlhd G_1 \unlhd \ldots \unlhd G_n = G$ is a central series if $G_i/G_{i-1} \leq Z(G/G_{i-1}) \forall i$

$G$ is nilpotent (of class $a$) if it has a central series (the shortest such of length $a$)

Upper central series is the series of groups $Z_i(G)$ s.t. $Z_0(G) = 1, Z_1(G) = Z(G), Z_{i+1}(G) \unlhd G$ with $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$

so, $G$ nilpotent (of class $a$) $\iff G/Z(G)$ nilpotent of class $a - 1$

$G$ nilpotent of class 1 $\iff G$ abelian

**Theorem 3.1**
Finite $p$-groups are nilpotent. If $|G| = p^e$, then class of $G < e$

**Proof**
$|G| = p^e$. If $e = 2$ then $G$ is abelian, so class 1.
Now $Z(G) \neq 1$
$\Rightarrow |G/Z(G)| < p^e \Rightarrow$ nilpotent of class $< e - 1$
$\Rightarrow G$ nilpotent of class $< e$

\[
\begin{array}{ccccccc}
1 & Z(G) & Z_2(G) & Z_3(G) & \cdots & G \\
| & | & | & | & | & |
1 & Z(G/Z(G)) & \cdots & \cdots & G/Z(G)
\end{array}
\]

E.g. $G = D_{2^e}$ is nilpotent of class $e - 1$, $(e \geq 2)$
If $e = 2$, $D_{2^e} = \langle \alpha, \beta | \alpha^2 = 1, \beta \alpha \beta = \alpha \rangle = V_4$, so clear
If $e > 2$, $Z(D_{2^e}) = 2$ and $D_{2^e}/Z(D_{2^e}) \cong D_{2^{e-1}}$

**Theorem 3.2**
For finite groups, TFAE:

1. $G$ is nilpotent
2. $H \not\subset G \Rightarrow H \not\subset N_G(H)$
3. Each Sylow subgroup of $G$ is normal in $G$
4. $G$ is a direct product of its Sylow subgroups, one for each prime dividing $|G|$

**Exercise:**
- $G$ nilpotent, $H < G \Rightarrow H$ nilpotent
- Any homomorphic image of $G$ is nilpotent
- Direct product of nilpotent groups is nilpotent group

**Proof**
(1) $\Rightarrow$ (2) Let $H \not\subset G$. Take $i$ maximal s.t. $Z_i(G) \leq H$
May assume $i = 0$ (factor out $Z_i(G)$)
$\Rightarrow Z(G) \not\subset H$. But $Z(G) \leq N_G(H) \Rightarrow H \not\subset N_G(H)$

(2) $\Rightarrow$ (3) Let $P$ be a Sylow $p$-subgroup of $G$

**Claim:** For any $G$, $N_G(N_G(P)) = N_G(P)$ for $P$ Sylow in $G$
Proof of Claim:
$P \in \text{Syl}_p(N_G(P))$ and $P \trianglelefteq N_G(P)$ \implies $P \text{ char } N_G(P)$
This is because $P$ is the only subgroup of $N_G(P)$ with order $|P|$, this implies all automorphism of $N_G(P)$ sends $P$ to itself

Also, since $N_G(P) \trianglelefteq N_G(N_G(P))$
\implies $P \trianglelefteq N_G(N_G(P))$
\implies $N_G(N_G(P)) = N_G(P)$ \hfill \blacksquare

By hypothesis of (2), have $N_G(P) = G$

(3) \implies (4) Let $P_1, \ldots, P_k$ be the Sylow $p$-subgroups of $G$, one for each prime $p | |G|$. Each $P_i \trianglelefteq G$
by hypothesis of (3),
\implies $P_1 P_2 \cdots P_k \trianglelefteq G$ s.t. $|P_1 P_2 \cdots P_k| = |G|
\implies G = P_1 P_2 \cdots P_k$, and $P_1 \cap \prod_{j \neq i} P_j = \{1\}$ by considering their orders
\implies $G \cong P_1 \times P_2 \times \cdots \times P_k$

(4) \implies (1) Follows from Exercise above and Theorem 3.1

Corollary 3.3
$G$ nilpotent, $H < G$ maximal \implies $H \trianglelefteq G$ index $p$, some prime $p$

Proof
$N_G(H) \unlhd H$ \implies $H \trianglelefteq G$
$G/H$ has no proper subgroups \implies cyclic of prime order for some prime $p$ \hfill \blacksquare

Note
If $K \trianglelefteq G$ and $K \leq H \leq G$, then $H/K \trianglelefteq Z(G/K) \iff ([h, g] | h \in H, g \in G) = [H, G] \leq K$

Definition
Lower central series for $G$ nilpotent is the chain $\Gamma_i(G)$ s.t. $\Gamma_1(G) = G, \Gamma_{i+1}(G) = [\Gamma_i(G), G]$
If $1 = G_0 \trianglelefteq \cdots \trianglelefteq G_a = G$ is a central series, then $\Gamma_{a+i+1}(G) \leq G_i \leq Z_i(G)$
In particular, $\forall c, \Gamma_{c+1}(G) = 1 \iff Z_c(G) = G$

3.1 Two nilpotent characteristic subgroups of a finite group $G$

$G$ any finite groups

Definition
The Fitting subgroup (nilpotent radical of $G$), $F(G)$, is the maximal subgroup amongst all normal nilpotent subgroups of $G$

Proposition 3.4
In a finite group, there is a unique maximal normal nilpotent subgroup:
If $H, K$ are nilpotent normal subgroups of $G$, so is $HK$
(i.e. $F(G)$ well-defined)

Proof
The last claim is clear if $H, K$ are both $p$-groups
\implies $O_p(G)$, the unique maximal normal $p$-subgroup of $G$ exist

Claim: $F(G) = O_{p_1}(G) \times \cdots \times O_{p_k}(G)$, where the $p_i$ are the prime divisors of $|G|$
Proof of Claim:  
RHS is nilpotent and normal  
If $K \trianglelefteq G$, nilpotent, and $P$ is a Sylow $p$-subgroup of $K$, then $P \text{ char } K \trianglelefteq G \Rightarrow P \trianglelefteq G \Rightarrow P \leq O_p(G) \Rightarrow K \leq \text{RHS}$

Definition  
$G$ any finite group, the Frattini subgroup of $G$, $\Phi(G)$, is the intersection of all maximal subgroups of $G$.

Note: $\Phi \text{ char } G$

Definition  
$g \in G$ is a non-generator of $G$ if whenever $G = \langle X, g \rangle$ we have $G = \langle X \rangle$.

Lemma 3.5  
$\Phi(G) = \{ g \in G | g \text{ non-generator } \}$

Proof  
If $g \notin \Phi$, then $\exists M < G$ maximal with $g \notin M$  
$\Rightarrow G = \langle M, g \rangle$, but $\langle M \rangle = M < G$  
$\Rightarrow g$ is not a non-generator

Conversely, assume $\exists X < G$ with $G = \langle X, g \rangle$ but $G > \langle X \rangle$  
Let $M < G$ maximal with $\langle X \rangle \leq M$  
Then $g \notin M \Rightarrow g \notin \Phi(G)$

Denote $\text{Syl}_p(G)$ as the set of Sylow $p$-subgroup of $G$.

Proposition 3.6  
For any $G$ finite, $\Phi(G)$ is nilpotent ($\Rightarrow \Phi(G) \leq F(G)$)

Proof  
Uses an important general lemma (Lemma 3.7) known as Frattini argument

Lemma 3.7 (Frattini argument)  
$G$ finite group, $K \trianglelefteq G$, $P \in \text{Syl}_p(K)$  
Then $G = N_G(P)\Phi(G)$ so by Lemma 3.5, $G = N_G(P)$, so $P \trianglelefteq \Phi(G)$. Thus $\Phi(G)$ nilpotent.

Lemma 3.8  
If $G$ is a $p$-group, then $G/\Phi(G)$ is an elementary abelian group, and hence a vector space over $\mathbb{F}_p$. In fact, $\Phi(G) = G'/G^p$

Proof  
If $M$ is maximal subgroup of $G$, then $M \trianglelefteq G$ of index $p$ so $G' \leq \Phi(G)$ (as $G/M$ abelian), and $G^p = \langle g^p | g \in G \rangle \leq \Phi(G)$ so $G'/G^p \leq \Phi(G)$
Equality: If \( g \in G \setminus G'G^p \), consider its image in \( \overline{G} = G/G'G^p \). Then \( \overline{g} \neq \overline{0} \), a non-zero vector, so let \( \overline{g}, \overline{g_2}, \ldots, \overline{g_k} \) be a basis.
Then \( g \) is not a non-generator (\( G = \langle g, g_2, \ldots, g_k, \Phi \rangle \)).

**Definition**
Minimal generating set for \( G \): no element of the set can be deleted and still generate \( G \).

**Theorem 3.9 (Burnside’s Basis Theorem)**
If \( G \) is a finite \( p \)-group, any two minimal generating sets for \( G \) have the same size, \( \dim_{\mathbb{F}_p} G/\Phi(G) \).

**Proof**
exercise: if \( g_1, \ldots, g_k \) is a minimal generating set for \( G \), then \( \overline{g_1}, \ldots, \overline{g_k} \) is a basis for \( G/\Phi(G) \).

**Remark.** \( S_5 = \langle (12), (12345) \rangle = \langle (12), (23), (34), (45) \rangle \)
both are minimal generating set, with different size.

**Question** What is the maximal size of a minimal generating set? What do minimal generating sets of maximal size look like?
4 Soluble (Solvable) groups

**Definition**
A derived series for \( G \) is a series \( G^{(i)} \) s.t. \( G^{(0)} = G \), \( G^{(i+1)} = [G^{(i)}, G^{(i)}] \) (so \( G' = G^{(1)} = \Gamma_2(G) \))

A group is soluble if \( G^{(v)} = 1 \) for some \( v \)

**Remark.**
- Nilpotent \( \Rightarrow \) soluble
- \( S_3 \) is soluble but not nilpotent
- simple soluble \( \Rightarrow C_p \) for some prime \( p \)

**Lemma 4.1**
TFAE:

1. \( G \) is soluble
2. The chief factors are elementary abelian
3. The composition factors are cyclic of prime order

**Proof**

\((1) \Rightarrow (2) \Rightarrow (3)\) is clear

\((3) \Rightarrow (1):\)

If \( 1 \leq \cdots \leq H_1 \trianglelefteq H_0 = G \) with abelian factors, then \( G^{(i)} \leq H_i \), by indicator:

\[ G^{(0)} = H^{(0)} \quad \text{and} \quad G^{(i+1)} = (G^{(i)})' \leq H_i' \leq H_{i+1} \]

**Exercise:** Subgroups, quotients, direct products of soluble groups are soluble

**Exercise:** \( H, K \trianglelefteq G \), both \( H, K \) soluble \( \Rightarrow HK \) is a soluble normal subgroup of \( G \). Hence, using the fact that if \( N, G/N \) soluble then \( G \) soluble, we can define the soluble radical of \( G \), i.e. the maximal normal soluble subgroup of \( G \)

**Theorem 4.2 (Galois)**

\( G \) finite soluble group, \( M < G \) maximal subgroup of \( G \)

\[ |G : M| = p^a \] for some prime power \( p^a \)

**Proof**

Let \( K \trianglelefteq G \) minimal normal. Then \( K \) is elementary abelian \( p \)-group, for some prime \( p \). (The proof here is much easier than before: \( K \) is soluble, and \( K' \) char \( K \) so \( K' = 1 \), so \( K \) is abelian. \( O_p(K) \) char \( K \) and \( K^p \) char \( K \), so \( K \) elementary abelian \( p \)-group for some \( p \))

If \( K \leq M \), induction applies to \( M/K < G/K \), so assume not. Then \( G = KM \) (since \( M \not\trianglelefteq KM \leq G \))

And \( K \cap M = 1 \): \( K \cap M \trianglelefteq M \), \( K \cap M \trianglelefteq K \) (as \( K \) is abelian) so \( K \cap M \not\trianglelefteq G \), so \( K \cap M = 1 \) by minimality of \( K \not\trianglelefteq G \)

So \( |G : M| = |K| = p^a \), for some \( a \)

**Remark.** Here \( K \) is a regular normal subgroup of \( G \) on \( (G : M) \) (regular = transitive and only identity fixes all point)
4.1 Hall’s Theorem on Finite Soluble Groups

\[ \pi = \text{Set of primes} \]
\[ n \in \mathbb{N}, \text{write } n = n_\pi n_{\pi'} \text{ where} \]
\[ (p_1^{l_1} \cdots p_k^{l_k})_{\pi} = \prod_{p_i \in \pi} p_i^{l_i} \quad (\pi\text{-part}) \]
\[ (p_1^{l_1} \cdots p_k^{l_k})_{\pi'} \notin \pi \quad (\pi'\text{-part}) \]

A \( \pi\)-group \( H \) is a finite group with \( |H| = |H|_\pi \)
A subgroup \( H \) of \( G \) is a Hall \( \pi\)-subgroup of \( G \) if \( |H| = |G|_\pi \), so subgroup of \( G \) of maximal possible \( \pi\)-order

**Remark.** \( \pi = \{p\} \)
Hall \( \pi\)-subgroup = Sylow \( p\)-subgroup
Hall \( \pi'\) subgroup = Hall \( p\)-complement subgroup

**Theorem 4.3**
If \( G \) is a finite soluble group, \( \pi \) is a set of primes

1. \( G \) has a Hall \( \pi\)-subgroup
2. Any two are conjugate in \( G \)
3. Any \( \pi\)-subgroup of \( G \) is in some Hall \( \pi\)-subgroup

**Example:** \( GL_3(2) \) has no Hall 3-complement, and has two non-conjugate Hall 7-complement

\[
\begin{pmatrix}
1 & * & * \\
0 & * & * \\
0 & * & *
\end{pmatrix}
\]
\[
\begin{pmatrix}
1 & 0 & 0 \\
* & * & *
\end{pmatrix}
\]

**Proof**
Let \( |G| = mn \), with \( m = |G|_\pi \), \( n = |G|_{\pi'} \)
Induction on \( n \). If \( n = 1 \), then trivial. So assume \( n > 1 \)

**Case 1:**
Assume \( \exists 1 \neq K \trianglelefteq G \) with \( |K| = m_1n_1 \) with \( n_1 < n \)

1. Now \( |G/K| = \frac{m}{m_1} \frac{n}{n_1} \), so by induction, \( G/K \) has a subgroup \( S/K \) of order \( \frac{m}{m_1} \) with \( K \leq S < G \)
   Then \( |S| = mn_1 < |G| \). By induction, \( S \) (and hence \( G \)) has a subgroup of order \( m \)

2. If \( H_1, H_2 \) are subgroups of \( G \), order \( m \), then in \( G \), \( H_1, H_2 \) are Hall \( \pi\)-subgroups. By induction, \( \exists x = Kx \in G \) with \( x^{-1}H_2x = H_1 \).
   \( \Rightarrow \) \( x^{-1}H_2Kx = H_1K \) \( \Rightarrow \) \( x^{-1}H_2, H_1 \) are Hall \( \pi\)-subgroup in \( H_1K \), so conjugate. Apply induction.

3. Let \( P \) be any \( \pi\)-subgroup of \( G \). Then \( \overline{P} = PK/K \) is a \( \pi\)-subgroup in \( \overline{G} \) \( \Rightarrow \) \( \overline{P} \subseteq \text{some Hall \( \pi\)-subgroup} \)
   \( S = S/K \) of \( G/K \) \( (K \leq S < G) \)
   \( S \) order \( mn_1 \). By induction in \( S \), we see that \( P \subseteq \text{some Hall \( \pi\)-subgroup in} \ G \)

**Case 2:**
Any non-identity normal subgroup of \( G \) has order divisible by \( n \) (\( \forall 1 \neq N \trianglelefteq G, n|N| \))
Let \( K \) be maximal normal in \( G \). Then \( |K| = p^a \) for some prime power \( p^a \), \( K \) elementary abelian.
Then \( n|p^a \), whence \( n = p^a \) as \( p^a|nm \) and \( (n, m) = 1 \)

Let \( L \trianglelefteq G \) containing \( K \) s.t. \( \overline{L} = L/K \) minimal normal in \( G/K \). Then \( |L| = q^b \) for some prime power \( q^b \) with \( p \neq q \)
Let $Q$ be a Sylow $p$-subgroup of $L$. $|L| = p^aq^b$, $L = KQ$ (by Frattini argument)

\[ G \xrightarrow{N_G(Q)} L = KQ \xrightarrow{Q} K \xrightarrow{1} 1 \]

1. **Claim:** $N_G(Q)$ is a Hall $\pi$-subgroup

**Proof of Claim:**
Firstly, Frattini argument: $G = LN_G(Q) = KQN_G(Q) = KN_G(Q)$

$\Rightarrow m|N_G(Q)$

$K \cap N_G(Q) = 1$, as

- $K \cap N_G(Q) \leq K$ (since $K$ abelian)
- $K \cap N_G(Q) \leq N_G(Q)$ (since $K \leq G$)

$\Rightarrow K \cap N_G(Q) \leq G$, but $K$ minimal normal, and $K \nleq N_G(Q)$ as $Q \nleq G$

$\Rightarrow |N_G(Q)| = m \Rightarrow H = N_G(Q)$ is a Hall subgroup

2. Let $H_2$ be any other Hall $\pi$-subgroup of $G$

Since $LH_2 \leq G$, with $|G| = |LH_2|$

$\Rightarrow G = LH_2$

Now $|L \cap H_2| = q^b$ (as $LH_2/L \cong H_2/L \cap H_2$)

$\Rightarrow L \cap H_2$ is a Sylow $q$-subgroup of $L$

$\Rightarrow Q^x = L \cap H_2$ for some $x \in L$

$H_2 \leq N_G(L \cap H_2) = N_G(Q)^x = N_G(Q^x) = H^x \Rightarrow H_2 = H^x$ (since they are of same order)

3. Let $P$ be a $\pi$-subgroup of $G$, with $|P| = m' < m$

Now $|G : H| = n$ which is $\pi'$-number

$|G : PK| = m/m'$ which is $\pi$-number

$\Rightarrow P, H \cap PK$ have the same order: $|G : H \cap PK| = |G : H||G : PK|$ (by Lemma 4.4, to be shown) $= \frac{nm}{m'}$

So $P, H \cap PK$ are both Hall $\pi$-subgroups in $PK$

$\Rightarrow$ conjugate there by (2)

$\Rightarrow P$ is conjugate to a subgroup of $H$

\[ \square \]

**Lemma 4.4**

$G$ any finite group let $A_1, A_2$ be subgroups of coprime indices $n_1, n_2$.

Then $G = A_1A_2$ (a factorization of $G$) and $|G : A_1 \cap A_2| = n_1n_2$
Theorem 4.5 (Theorem of Ore)

If $G$ is finite soluble, $A_1, A_2$ maximal subgroup of $G$, not conjugate then $G = A_1 A_2$

Proof as Exercise (hard)

Factorisation in almost simple groups are interesting, important and rare. See later.

Definition

If $|G| = p_1^{e_1} \cdots p_k^{e_k}$ with the $p_i$ distinct primes, a Sylow basis of $G$ is $\{P_1, \ldots, P_k\}$ with $|P_i| = p_i^{e_i}$ s.t. $P_i P_j = P_j P_i \forall i, j$ (so that $P_i P_j \leq G \forall i, j$)

Note: $P_i P_j = P_j P_i \Rightarrow P_i P_j \leq G \forall i, j$ and in fact $P_i, P_j, \ldots P_k \leq G \forall \{i_1, \ldots, i_t\} \subseteq \{1, \ldots, k\}$ — we get Hall subgroups this way

Theorem 4.6

If $G$ is a finite soluble group, $G$ has Sylow basis, and any two are conjugate

Proof

Let $|G| = p_1^{e_1} \cdots p_k^{e_k}$, with the $p_i$ distinct primes.

Let $H_i$ be a (Hall) $p_i$-complement. (i.e. has order $|G|/p_i^{e_i}$)

Put $P_i = \bigcap_{i \neq j} H_i$ 

$\Rightarrow |P_i| = p_i^{e_i}$, using Lemma 4.4

And $P_i P_j = \bigcap_{i \neq j} H_i$ 

Conjugacy: Let $\{P_1, \ldots, P_k\}$ and $\{P_1^*, \ldots, P_k^*\}$ be Sylow bases with $|P_i| = |P_i^*|$, so $P_i, P_i^* \in Syl_{p_i}(G)$

Put $H_i = P_1 \cdots P_{i-1} P_{i+1} \cdots P_k$

and $H_i^* = P_1^* \cdots P_{i-1}^* P_{i+1}^* \cdots P_k^*$

Claim: $\exists g \in G$ with $H_i^g = H_i^* \forall i$

Proof of Claim:

First, $3g_1$ with $H_i^{g_1} = H_i^*$ (Hall)

Now assume we found $g_{i-1}$ with $H_j^{g_{i-1}} = H_j^* \forall j \leq i - 1$

Change notation if necessary so that $H_j = H_i^* \forall \leq i - 1$

Now $G = H_i P_i$, and let $x \in G$ with $H_i^x = H_i^*$ (Hall)

$\Rightarrow x = hz$ with $h \in H_i$, $z \in P_i$

$\Rightarrow H_i^z = H_i^*$ and $z \in P_i \leq H_i \forall j < i$

$\Rightarrow H_i^j = H_i^*$ for $j \leq i$

After $k$ steps, finished.

Given claim, we have $P_i^g = P_i^* \forall i$
**Theorem 4.7 (Wielandt)**

$G$ finite, $H_1, H_2, H_3$ soluble subgroups of $G$ with $|G : H_i| = n_i$ pairwise coprime. Then $G$ soluble

**Proof**

Looking for $N \leq G$ soluble with $G/N$ soluble by induction (then $G$ soluble)

Note that $G = H_1H_2 = H_1H_3 = H_2H_3$, by Lemma 4.4 May assume $H_i \neq 1 \forall i$. Let $K$ minimal normal in $H_1$

$\Rightarrow K$ elementary abelian $p$-group.

WLOG, $p \nmid n_2$

**Claim:** This implies $K \leq H_2$

**Proof of Claim:** By Lemma 4.4

$$|K(H_1 \cap H_2) : H_1 \cap H_2| = |K : K \cap H_1 \cap H_2|$$

so $K \leq H_1 \cap H_2$

Now let $N = \langle K^g | g \in G \rangle$ - the $G$ normal closure of $K$

$\Rightarrow N = \langle K^{h_1h_2} | h_i \in H_i \rangle$ = $\langle K^{h_2} | h_2 \in H_2 \rangle \leq H_2$

$\Rightarrow N \leq G, N \leq H_2$

It follows that $N$ is soluble (as $H_2$ is), and $G/N$ is soluble by induction hypothesis.

**Theorem 4.8 (P.Hall)**

If the finite group $G$ has a Hall $p$-complement for each prime $p | |G|$, then $G$ is soluble

**Proof**

$|G| = p_1^{e_1} \cdots p_k^{e_k}$

If $k = 1$, $G$ is nilpotent. Done

If $k = 2$, this is Burnside’s $p^aq^b$ Theorem, this uses representation theory

Assume $k \geq 3$, let $H_i$ be a Hall $p_i$-complement.

By induction, $H_i$ is soluble $\forall i$ (Lemma 4.4)

Now use Theorem 4.7

**Lemma 4.9**

$G$ finite soluble group $\Rightarrow C_G(F(G)) \leq F(G)$

(So $G/Z(F(G)) \leq \text{Aut}(F(G))$)

**Proof**

Put $F = F(G), Z = Z(F(G)), C = C_G(F(G))$. So $Z = C \cap F$

Assume $C \nsubseteq F$. Let $H \leq G$ with $Z < H$

$\mathcal{H}$ minimal normal in $\overline{C} = C/Z$: Since $\mathcal{H}$ is elementar yabelian, have $\mathcal{H}' \leq Z$

Then $H$ is nilpotent (so $H \leq F$ - not so): minimal normal in $H$,

$\Gamma_3(H) = [H', H] \leq [Z, C] = 1$

\[15\]
5 Interlude

In finite simple groups here been classified:

- $C_p$, $p$ prime
- $A_n$, $n \geq 5$
- $L_d(q)$, $d \geq 2$, if $d = 2$ then $q \geq 4$
- $U_d(q)$, $d \geq 3$, if $d = 3$ then $q \geq 3$
- $Sp_{2m}(q)$, $m \geq 2$, if $m = 2$ then $q \geq 3$
- $PSL_d^\epsilon(q)$, $d \geq 7$
  - if $d$ even then $G$ doubly infinite families, denoted by $\epsilon = \pm$
  - if $d$ odd then $\epsilon$ is empty

10 families, exceptional groups of Lie type ($q$ denote prime power):

- $G_2(q)$, $F_4(q)$, $E_6^+(q)$, $E_6^-(q)$, $E_7(q)$, $E_8(q)$
- $^3D_4(q)$
- $^2B_2(q)$ with $q = 2^{2a+1}$
- $^2G_2(q)$ with $q = 3^{2a+1}$
- $^2F_4(q)$ with $q = 2^{2a+1}$

26 sporadic simple groups

$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, \ldots, M$

In applications, have usually a finite groups acting in some way, e.g as a group of permutations, or a group of matrices (in this case, this is representation theory, mainly used to study the first 5 families mentioned)

We will be consider the first case mainly (i.e. acting as groups of permutations)
e.g.1: as a group of automorphisms of a graph, e.g. Peterson graph e.g.2: as a group acting on roots of polynomial

Recall about permutation actions:

- $G$ finite group, $\Omega$ a finite set. $G$ acts on $\Omega$ if there is a map $\Omega \times G \to \Omega$ 
  s.t. $\omega 1 = \omega$, $\omega gh = (\omega g)h \ \forall \omega \in \Omega, g, h \in G$
  - If so, for $g \in G$, the map $\phi_g : \Omega \to \Omega$ 
    $\omega \mapsto \omega g$ 
  - and the map $\phi : G \to \text{Sym}(\Omega)$ is a homomorphism, called a permutation representation of $G$

The kernel of the action, $G_{(\Omega)} := \ker \phi$. Then $G\phi = G^{\Omega} := G/G_{(\Omega)} \leq \text{Sym}(\Omega)$

The action is faithful if $G_{(\Omega)} = 1$

If $G$ acts on $\Omega$, the orbit of $G$ containing $\alpha$ is $\alpha G = \{\alpha g | g \in G\}$

$G$ is transitive on $\Omega$ if $\alpha G = \Omega \ \forall \alpha \in \Omega$

Problems about actions are usually easily reduced to problems about transitive actions (consider the actions on orbits). So the assumption of $G$ transitive is common.

If $G$ acts on $\Omega_1, \Omega_2$, then $\theta : \Omega_1 \to \Omega_2$ is a $G$-homomorphism if $(\alpha g)\theta = (\alpha \theta)g \ \forall \alpha \in \Omega_1, g \in G$

$\theta$ is a $G$-isomorphism if it is also bijective.

Also note that $(G : G_\alpha)$ is the $G$-space of all right cosets of $G_\alpha = \{g \in G | \alpha g = \alpha\}$, with action obtained by $(G_\alpha x)g = G_\alpha(xg)$
Lemma 5.1
If $G$ is transitive on $\Omega$, and $\alpha \in \Omega$, then actions of $G$ on $\Omega$ and on $(G:G_{\alpha})$ are $G$-isomorphic

Proof

$\theta : \Omega \to (G:G_{\alpha})$

$\alpha x \mapsto G_{\alpha}x$

is bijective, commutes with the actions of $G$

Example:

$(G:H),(G:K)$ are $G$-isomorphic iff $H,K$ are $G$-conjugate

Definition

A equivalence relation $\rho$ is a $G$-congruence on $\Omega$ if $\alpha \rho \beta \Rightarrow \alpha g \rho \beta g \forall g \in G$

Trivial means either equality or universal.

If $G$ is transitive on $\Omega$, then $G$ is primitive if \[\] non-trivial $G$-congruence on $\Omega$

Remark. Kernels of $G$-homomorphism are “blocks” of $G$-congruences

Lemma 5.2

$G$ transitive on $\Omega$, $\rho$ a non-trivial $G$-congruence on $\Omega$, $\alpha \in \Omega$, $\rho(\alpha)$ the (equiv.) class of $\alpha$: $\rho(\alpha) := \{\beta \in \Omega | \alpha \rho \beta\}$

(1) The (setwise) stabilizer of $\rho(\alpha)$ in $G$ acts transitively on $\rho(\alpha)$

(2) $\rho(\alpha)$ is the union of some $G_{\alpha}$-orbits, including $\{\alpha\}$

(3) $G$ is transitive on the set $\Omega/\rho$ of $\rho$-classes (blocks), so all the $\rho$-classes have the same size

(4) $G_{\alpha} \trianglelefteq G_{\rho(\alpha)} \trianglelefteq G$

Conversely, if $G_{\alpha} \trianglelefteq H \trianglelefteq G$, can define a non-trivial $G$-congruence on $\Omega$ by:

(a) $\gamma \rho \beta \Leftrightarrow \beta = \gamma h$, some $h \in H$

(b) $\gamma \rho \beta \Rightarrow \gamma g \rho \beta g \forall g$

Proof

(1) Let $\beta \in \rho(\alpha)$, $G$ transitive on $\Omega$

$\Rightarrow \exists g \in G$ with $\beta = \alpha \Rightarrow \rho(\alpha)$ must be kept invariant by $g \Rightarrow g \in G_{\rho(\alpha)}$

(2) $G_{\alpha}$ keeps $\rho(\alpha)$ invariant

(3) $\alpha \in \rho(\alpha)$ and if $\rho(\beta)$ another block, $\exists g \in G$ s.t. $\alpha g = \beta \Rightarrow \rho(\alpha)g = \rho(\beta)$

(4) First claim is clear. Proof of converse:

If $G_{\alpha} \trianglelefteq H \trianglelefteq G$, the $\rho$ defined is clearly non-trivial $G$-congruence.

$\Rightarrow \Omega/\rho = \{\Gamma g | g \in G\}$ where $\Gamma = \alpha H$

Claim: The blocks form a partition of $\Omega$

Proof of Claim:

They cover $\Omega$. So we want: $(\Gamma \cap \Gamma g \neq \emptyset \Rightarrow \Gamma = \Gamma g)$

$\beta \in \Gamma \cap \Gamma g \Rightarrow \beta = \alpha h_1 = \alpha h_2 g$ some $h_1, h_2 \in H$

$\Rightarrow h_2 h_1^{-1} \in G_{\alpha} \trianglelefteq H \Rightarrow g \in H \Rightarrow \Gamma g = \Gamma$

□
Corollary 5.3
Set up as Lemma 5.2, by (4), \( G \) primitive on \( \Omega \) \( \iff \) \( G \) maximal subgroup of \( G \)

Corollary 5.4
Set up as Lemma 5.2, by (3), all blocks have the same size, dividing \( |\Omega| \).
If \( G \) transitive of prime degree (degree means size of \( \Omega \)) \( \Rightarrow \) \( G \) primitive

Lemma 5.5
\( G \) primitive on \( \Omega \), \( \alpha \neq \beta \) \( \Rightarrow \) \( G = \langle G_\alpha, G_\beta \rangle \), unless \( G \) is \( C_p \) of degree \( p \)
In fact, if \( G \) transitive, \( \alpha \in \Omega \), then \( \text{fix}(G_\alpha) = \{ \beta | \beta h = \beta \ ∀ h \in G_\alpha \} \) is a block of a congruence.

Proof
Let \( G \) be transitive. Define \( \alpha \rho \beta \) if \( G_\alpha = G_\beta \) (note: \( \beta \in \text{fix}(G_\alpha) \Rightarrow G_\alpha = G_\beta \))
Claim: This is a \( G \)-congruence
Proof of Claim:
\( g \in G \). \( \alpha \rho \beta \Rightarrow G_\alpha = G_\beta \Rightarrow G_{\alpha g} = G_{\beta g} \Rightarrow \alpha g \rho \beta g \)
\( \text{fix}(G_\alpha) = \rho(\alpha) \). So, if \( G \) is primitive on \( \Omega \), the congruence above is trivial (equality or universal).
If equality, then \( G_\alpha \neq G_\beta \), both maximal \( \Rightarrow G = \langle G_\alpha, G_\beta \rangle \)
If universal, then \( G_\alpha \) fixes \( \Omega \) pointwise \( \Rightarrow G_\alpha = 1 \)
and as \( G_\alpha \) maximal, then \( G \) is \( C_p \) for some prime \( p \)

Lemma 5.6
Let \( G \) transitive on \( \Omega \), let \( 1 \neq N \trianglelefteq G \). The \( N \)-orbits form a \( G \)-invariant partition of \( \Omega \)

Proof
Exercise

Corollary 5.7
If \( G \) is primitive, \( 1 \neq N \trianglelefteq G \) \( \Rightarrow \) \( N \) transitive on \( \Omega \)

Exercise: Let \( G \) be transitive of degree prime \( p \), (i.e. \( |\Omega| = p \) and hence \( G \leq S_p \))
Let \( N \) be minimal normal subgroup of \( G \). Then \( N \) is simple (possibly \( C_p \)), and \( G/N \) is abelian of order dividing \( p-1 \) (use Frattini argument and \( G \leq S_p \). Note if \( P \) is order \( p \), \( N_{S_p}(P) \) has order \( p(p-1) \), so \( G' = N \) is simple)

Dichotomy for primitive groups: 2-transitive groups, simply-primitive groups

2-transitive groups

Definition
\( G \) on \( \Omega \) is 2-transitive on \( \Omega \) if \( G \) is transitive on ordered pairs of distinct points of \( \Omega \), i.e. if \( \alpha_1 \neq \alpha_2, \beta_1 \neq \beta_2 \), then \( \exists g \in G \) with \( \alpha_1 g = \beta_1 \)
\( k \)-transitive is defined similarly on \( k \)-tuples
Remark. \( G \) is \( k \)-transitive on \( \Omega \) of degree \( n \), then \( n(n-1)(n-k+1) \mid |G| \)

Example:
\( S_n \) on \([1, n]\) is \( n \)-transitive
\( A_n \) is \((n - 2)\)-transitive but not \((n - 1)\)-transitive

Example:
\( G = PGL_d(q) \) - projective general linear group = \( GL_d(q) / \{ \text{scalars} \} \) acts on \( \Omega = \{ \text{1-dim. subspaces of} \)
\[V_\alpha(q) = \mathbb{P}_{d-1}(q)\]
\[|\Omega| = \frac{q^d - 1}{q - 1}\]

G is 2-transitive on \(\Omega\)

G is 3-transitive \iff \(d = 2\)

G is 4-transitive \iff \(d = 2, q = 3, G = PGL_2(3) \cong S_4\)

**Example:** \(G = AGL_d(p), (d \geq 1)\) the group of “symmetries” of \(\Omega = V_d(p)\)

i.e. \(\langle\text{translations, linear transformations}\rangle \subseteq \text{Sym}(V)\)

\(K = \{t_v|v \in V\}\) where \(t_v : x \mapsto x + v\), subgroup of translation

\(G_0 = GL_d(p)\) is acting on \(\Omega\) as linear transformation

\(\Rightarrow\) transitive on \(\Omega \setminus \{0\}\)

\(\Rightarrow\) 2-transitive on \(\Omega\)

(Exercise) \(G\) is 3-transitive \iff \(d = 2, \) or \(d = 1, p = 3\) (i.e. \(G \cong S_3\))

(Exercise) \(G\) is 4-transitive \iff \(d = 2 = p, AGL_2(2) \cong S_4\)

In fact:

(1) \(K \trianglelefteq AGL\), since \(\forall h \in G_0, h^{-1}t_v h = t_{vh} \forall x \in V\)

(2) \(K\) is a regular normal elementary abelian subgroup

(3) \(K \cap G_0 = 1, AGL = G_0 K\)

Any \(g \in G\) is \(g = hk\) for some unique \(h \in H, k \in K\)

\((h_1k_1)(h_2k_2) = (h_1h_2)(k_1^{h_2}k_2)\)

**Definition**

Semidirect product \(H \ltimes K:\)

\(H, K\) groups, \(\theta : H \rightarrow \text{Aut}(K)\)

Elements of \(H \otimes K\) are of form \((h, k)\) s.t.

\[(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1^{h_2}\theta_k) \quad \forall h_i \in H, k_i \in K\]

This is a group, with normal subgroup \(\cong K\) and a subgroup \(\cong H\), s.t. \(H \cap K = 1, G = HK\)

(Direct product is a special case)

**Lemma 5.8**

Let \(G\) be primitive on \(\Omega\), let \(K \trianglelefteq G\) a regular normal subgroup (so \(K\) is transitive with \(K_\alpha = 1 \forall \alpha\))

(1) \(K\) is minimal normal in \(G\) (so it is a direct product of isomorphic simple groups, possibly \(C_p\))

(2) Let \(\alpha \in \Omega\), we can identify \(\Omega\) and \(K\) in such a way that the actions of \(G_\alpha\) on \(\Omega\) and on \(K\) is isomorphic

(3) If \(G\) is 2-transitive, then \(K\) is elementary abelian

(4) If \(K\) is elementary abelian, then \(K\) is in fact a vector space \(V_d(p)\) over \(\mathbb{F}_p\) and action of \(G\) on \(\Omega\) is isomorphic to a subgroup of \(AGL_d(p)\) acting as above

In fact, \(G_\alpha (\leftrightarrow G_0, \text{stabiliser of vector } 0)\) is an irreducible subgroup of \(GL_d(p)\)

(This is because if some proper subspace \(L\) of \(K\) is \(G_\alpha\)-invariant, then \(G_\alpha \not\leq LG_\alpha \not\leq G\))

**Proof**

(1) If \(1 \neq L \trianglelefteq G \Rightarrow L\) is transitive \Rightarrow \(|K| = |\Omega||L|

\Rightarrow\) if \(L \leq K\), then \(L = K\)
(2) \( \alpha \in \Omega \), any \( \beta \) is \( \alpha k \) for unique \( k \)
\( \Omega \leftrightarrow K \)
If \( g \in G_\alpha \), \( \alpha kg = \alpha g^{-1}k g = \alpha k^g \leftrightarrow k^g \)

(3) Let \( G \) be 2-transitive. By (2), \( G_\alpha \) is transitive on \( \Omega \setminus \{\alpha\} \)
\( \Rightarrow \ G_\alpha \) transitive on \( K \setminus \{1\} \) by conjugations
\( \Rightarrow \ \forall k \in K \setminus \{1\} \), they have the same order \( p \), some prime \( p \)
\( \Rightarrow \ K \) is a \( p \)-group \( \Rightarrow \) elementary abelian

(4) Notation: \( K \) is a vector space written multiplicatively.
\( G = G_\alpha K \).
Action of \( K \):
Take \( k' \in K \), we have the correspondence
\[ (k)k' \leftrightarrow (\alpha k)k' = \alpha (kk') \leftrightarrow kk' \]
\( \Rightarrow \) action by \( k' \) is just by translation
Action of \( G_\alpha \):
Take \( h \in G_\alpha \), \( h \) acts on \( K \) by \( k \mapsto h^{-1}kh \)
This is a linear transformation: \( h^{-1}(k_1k_2)h = h^{-1}k_1h \cdot h^{-1}k_2h \) (and scalar multiple)

\[ \square \]

**Theorem 5.9 (Burnside)**
Let \( G \) be a 2-transitive primitive group on \( \Omega \), \( |\Omega| = n \). Let \( N \) be minimal normal subgroup of \( G \). Then

either (a) \( N \) elementary abelian \( p \)-group (some \( p \)), \( G \leq AGL_d(p) \) \((p^d - 1)|G_0|\)

or (b) \( N \) is non-abelian simple

**Proof**
If \( N \) is regular, then get (a) by Lemma 5.8. So we assume \( N \) is not regular (and aim to get (b))

Claim: \( N \) is primitive on \( \Omega \)

**Proof of Claim:**
Assume not. Let \( \Gamma \) be a minimal non-trivial block of \( N \) on \( \Omega \)
\( \Rightarrow \ |\Gamma \cap \Gamma g| \leq 1, g \in G \), unless \( \Gamma = \Gamma g \)
\( \Gamma g \) is another \( N \)-block (possibly in a different system of imprimitivity)
\( \Rightarrow \ \Gamma \cap \Gamma g \) is also an \( N \)-block, so either \( \Gamma = \Gamma g \) or \( |\Gamma \cap \Gamma g| \leq 1 \)

Write \( B = \{\Gamma g | g \in G\} \) - “lines”. Any 2 points in \( \Omega \) are on a unique line
\( \Rightarrow \) all pairs of points are (by \( G \) 2-transitivity)

Let \( \alpha \in \Omega \). Now \( N_\alpha \) fixes setwise each line on \( \alpha \)

Claim: \( N_{\alpha \beta} = 1 \) for \( \alpha \neq \beta \)

**Proof of Claim:**
\( N_{\alpha \beta} \) fixes all points not on line(\( \alpha, \beta \))
Repeat with \( \alpha, \gamma \) and get \( N_{\alpha \beta} = 1 \)

Hence \( N \) is a Frobenius groups (i.e. transitive, \( N_\alpha \neq 1 \forall \alpha \), and \( N_{\alpha \beta} = 1 \forall \alpha, \beta \))

\( \Rightarrow \ \exists \) characteristic regular subgroup \( K \leq N \) \((5.1)\)

(see Remark for proof of this in our case)
\( \Rightarrow \ K \leq G \Rightarrow N = K \Rightarrow N \) is regular \#
Recall Theorem 2.3: \( N \) minimal normal \( \Rightarrow N = T_1 \times \cdots \times T_k \) with \( T_i \cong T \) for all \( i \) and \( T \) simple.

Also, by Corollary 5.7, each \( T_i \) is transitive on \( \Omega \)

**Claim:** \( k = 1, N \) is simple, non-abelian

**Proof of Claim:**
If \( k > 1 \), then \( T_i \) is regular.

\( \Rightarrow |N| = |T|^{|k|}, n = |T| \) (note \( n \) is size of \( \Omega \)), by Lemma 5.10

this orbits of \( N_\alpha \) on \( \Omega \setminus \{\alpha\} \) have all the same size dividing \( n - 1 \) (by Corollary 5.4)

\( N_\alpha \trianglelefteq G_\alpha, G_\alpha \) transitive on \( \Omega \setminus \{\alpha\} \)

\( |N_\alpha| = |T|^{k-1} \)

On the other hand, \( (n - 1, |N_\alpha|) = 1 \)

\( \Rightarrow N_\alpha = 1 \)

\( \Rightarrow k = 1 \)

\( \Rightarrow N \) simple, non-abelian (if abelian, then regular by the next Lemma 5.10)

We have now completed the proof.

**Remark.** We give a proof of the statement (5.1) under the set up of the lemma

**Claim:** \( G \) is 2-transitive, \( N \trianglelefteq G \) and \( N \) Frobenius \( \Rightarrow \exists K \leq N \) characteristic regular subgroup of \( N \)

**Proof**
Let \( K = \{1\} \cup \{x \in N | x \text{ have no fixed points on } \Omega\} \)

Let \( n = |\Omega| \)

\( |K| = n, |N| = nc \) where \( c = |N_\alpha| \)

\( N = K \cup \left( \bigcup_{\alpha \in \Omega} N_\alpha \setminus \{1\} \right) \)

\( K \) is a transitive set:
If \( k \in K \setminus \{1\} \) takes \( \alpha \) to \( \beta \), let \( g \in G_\alpha \) take \( \beta \) to \( \gamma \)
then \( k^g \in K \setminus \{1\} \) with \( k^g : \alpha \mapsto \gamma \)

\( K \leq N \)

If not, let \( k_1, k_2 \in K \text{ with } k_1k_2^{-1} \notin K \Rightarrow k_1 \neq k_2 \) and \( k_1k_2^{-1} \) fixes some \( \alpha \) - then \( \alpha k_1 = \alpha k_2 \)

\( \Rightarrow K \) cannot be transitive

\( \Rightarrow K \trianglelefteq G \) (as \( k^g \in K \forall k \in K, g \in G \))

**Definition**
Action of \( G \) on \( \Omega \) is **semi-regular** if \( g \in G \) fixes any point of \( \Omega \) \( \Rightarrow g = 1 \)

**Lemma 5.10**
If \( M \) transitive subgroup of \( \text{Sym}(\Omega) \), then \( C_{\text{Sym}(\Omega)}(M) \) is a semi-regular

**Proof**
Exercise

**Simply Primitive Groups**

**Definition**
\( G \) is simply primitive on \( \Omega \) if it is primitive but not 2-transitive

Orbits of \( G_\alpha \): \( \Gamma_0(\alpha) = \{\alpha\}, \Gamma_1(\alpha), \ldots, \Gamma_{r-1}(\alpha) \)

where \( r \) is the number of these for \( G_\alpha \), called the **rank** of \( G \) on \( \Omega \)

Note \( r = 2 \iff G \) is 2-transitive
For $r > 2$
the subdegree $n_i = |\Gamma_i(\alpha)|$
\[1 = n_0 \leq n_1 \leq \cdots \leq n_{r-1}\]
\[\sum_0^r n_i = n\]

We can consider the induced action of $G$ on $\Omega \times \Omega$:
\[(\alpha, \beta)g = (\alpha g, \beta g) \quad g \in G; \alpha, \beta \in \Omega\]

Get orbits $\Gamma_0, \Gamma_1, \ldots, \Gamma_{r-1}$, these are called orbitals of $G$
\[\Rightarrow \Gamma_i(\alpha) = \{\beta \in \Omega | (\alpha, \beta) \in \Gamma\}\]
\[|\Gamma_i| = n \cdot n_i\]

The orbitals give orbital graphs on $\Omega$ (a directed graph):
If $\Gamma$ is an orbital, then $\Gamma^* = \{(\beta, \alpha) | (\alpha, \beta) \in \Gamma\}$ is also an orbital
$\Gamma$ and $\Gamma^*$ are paired
We get complete $G$-invariant $r$-colouring of the complete graph on the vertices in $\Omega$
$G_1 = $ Peterson graph
$|\Omega| = \binom{5}{2} = 10 \quad G = Aut(Peterson) = S_5$
(Automorphism group of graph $G$, $Aut(G)$, acts on the set of vertices preserves edge)

Rank=3: $n_0 = 1, \Gamma_0(\{1, 2\})$ (trivial edges from $\{i, j\}$ to $\{i, j\}$)
$n_1 = 3, \Gamma_1(12)$ (edges of a Petersen graph, i.e. edges with vertex $\{i, j\}$ and $\{k, l\}$ with $\{i, j\} \cap \{k, l\} = \emptyset$)
$n_2 = 6, \Gamma_2(12)$ (all other edges of $K_{10}$, i.e. edges with vertex $\{i, j\}$ and $\{i, k\}, j \neq k$)

Exercise: $S_n$ acts on $\binom{n}{2}$ (stabilizer $S_{n-1} \times S_2$) as a primitive rank 3 group, subdegrees 1 ($\leftrightarrow 12$),
$2n - 2, \binom{n-2}{2}$
$S_n$ acts on $\binom{n}{k}, \frac{n}{2} > l \leq 1$, rank is $l + 1$

Remark. If $G$ is an undirected graph, we have the notion of distance
$G \leq Aut(G)$, $G$ preserves distance
Say $G$ is distance transitive on $G$ if given $\alpha_1, \alpha_2$ has distance $d$ and $\beta_1, \beta_2$ has distance $d$, then $\exists g \in G$
s.t. $\alpha_1 g = \beta_1$
What are these on regular symmetric graphs?

Exercise: $S_n$ is distance transitive on the graph $\Omega = \binom{n}{l}$ $l$-subsets of $[1, n]$, edges $A - B$ if $|A \cap B| = l - 1$
If $G$ is primitive, $n_1 = 1 \Rightarrow n_i = 1 \forall i \Rightarrow G$ regular (see 5.4 or 5 or 6)
Exercise: $n_1 = 2 \Rightarrow n_i = 2 \forall i \Rightarrow G = D_{2p}$ on $p$ points
Sim’s Conjecture: $n_1$ fixed $\Rightarrow |G_\alpha|$ bounded

**Proposition 5.11 (D.G. Higman)**
Let $G$ be transitive on $\Omega$. Then $G$ is primitive $\Leftrightarrow$ all the non-diagonal orbital graphs are connected

**Proof**
Exercise (very very hard)
Permutation Character

$G$ acts on $\Omega$, a permutation group, $\pi(g) = |\text{fix}_\Omega(g)|$ is a character of $G$ of the permutation representation.

**Lemma 5.12**

If $G \leq \text{Sym}(\Omega)$, permutation character $\pi$

Then $\langle \pi, 1 \rangle_G = \frac{1}{|G|} \sum_g \pi(g) = \#(\text{orb}(G, \Omega))$

So $G$ is transitive $\Omega \iff \langle \pi, 1 \rangle_G = 1$

**Proof**

$$\#(\text{orb}(G, \Omega)) = \sum_{\alpha \in \Omega} |G_\alpha| = \# \{(\alpha, g) \in G \times \Omega | \alpha g = \alpha\} = \sum_{g \in G} \pi(g)$$

\[\square\]

**Lemma 5.13**

$G$ acts on $\Omega_1, \Omega_2$, with characters $\pi_1, \pi_2$

Then $\langle \pi_1, \pi_2 \rangle_G = \# \text{ orbits of } G \text{ on } \Omega_1 \times \Omega_2$

In particular, if $G$ acts transitively on $\Omega$, with character $\pi$, then $\langle \pi, \pi \rangle = \text{rank}_\Omega(G)$

**Proof**

First part:

$$\langle \pi_1, \pi_2 \rangle_G = \langle \pi_1 \pi_2, 1 \rangle_G$$

Note $\pi_1 \pi_2$ is the permutation character of $G$ on $\Omega_1 \times \Omega_2$

$G$ is 2-transitive on $\Omega$: $\pi = 1 + \chi$, $\chi$ irreducible

$G$ is rank 3: $\pi = 1 + \chi_1 + \chi_2$, $\chi_i$ distinct irreducible

\[\square\]

**Definition**

$G$ acts on $\Omega$ is **multiplicity-free** if its permutation character is $\pi = 1 + \chi_1 + \cdots + \chi_v$ with the $\chi_i$ distinct

**Question:** Classify such permutation groups

**Remark.** If $G$ is distance-transitive on an undirected graph than its permutation character is multiplicity-free

**Exercise:** Show that if $G$ has permutation rank $\leq 5$ then $G$ is multiplicity-free

**Exercise:** If $G$ is transitive on $\Omega$, $\exists g \in G$ with $\pi(g) = 0$
### 6 Alternating Groups

\[ |S_n| = n! \quad , \quad |A_n| = n!/2, \quad A_n \text{ consist of all the even permutations.} \]

\[ S_n, A_n \text{ acts naturally on } \Omega = [1, n] \]

\[ A_n \text{ is } (n-2)\text{-transitive on } [1, n], \quad S_n \text{ is } n\text{-transitive} \]

Also recall: \( A_n \) is generated by the 3-cycles \((ijk)\) on \([1, n]\) (e.g., \((12)(34) = (124)(134), \quad (12)(13) = (123)\), also note multiplication is defined such that left one acts first)

**Theorem 6.1**

\( A_n \) is (non-abelian) simple for \( n \geq 5 \) (Note for \( n = 3, \quad A_3 \) is abelian simple)

**Proof I**

Induction on \( n \):

- \( A_5 \) is simple (prove this). Let \( n > 5 \), assume true for \( n - 1 \)

Let \( G = A_n \), let \( 1 \neq K \not| G \Rightarrow K_\alpha \not| G_\alpha (\equiv A_{n-1}) \) for \( \alpha \in [1, n] \)

Now \( G_\alpha \) is simple by induction hypothesis \( \Rightarrow K_\alpha = 1 \) or \( K_\alpha = G_\alpha \)

Case \( K_\alpha = 1 \): Impossible. Because \( K \) is transitive regular, so by Lemma 5.8 and the statement above it about \( AGL \) being at most 3-transitive (except if \( n = 4 \)) gives a contradiction

Case \( K_\alpha = G_\alpha \): This implies that \( K = G \) (as \( K \) would contains a 3-cycles, and hence all 3-cycles, on \([1, n]\), as these conjugate in \( A_n \))

**Proof II**

Start as before, get \( K \) regular on \([1, n]\) \( \Rightarrow |K| = n \)

\( \Rightarrow K \) contains a whole \( A_n \)-ccls of elements.

But, in fact, the \( A_n \)-ccls are larger than \( n - 1 \) (see later)

**Proof III**

(This proof is elementary) Suppose \( 1 \neq K \not| G \)

**Claim:** \( K \) contains a 3-cycle

**Proof of Claim:**

Let \( 1 \neq g \in K \), fixing as many points of \([1, n]\) as possible.

We claim \( g \) is a 3-cycle, suppose this is not true, there are 2 possibilities:

1. All cycles of \( g \) have size 2: \( g = (12)(34) \cdots , \) let \( x = (345) \) Then \( [g, x] \neq 1 \), but fixes \( \{1, 2\} \cup \text{fix}(g) \setminus \{5\} \neq 2 \)

2. \( g = (123 \ldots 45 \ldots) \Rightarrow [g, x] \neq 1 \)

But \( \text{fix}([g, x]) = \text{fix}(g) \cup \{2\} \) (check)

Claim \( \Rightarrow K \) contains all 3-cycles (all conjugate) \( \Rightarrow K = A_n \)

**Theorem 6.2**

Let \( G \leq A_n \), \( G \) primitive, \( G \) containing a 3-cycle. Then \( G = A_n \)

**Proof**

Define \( G \)-congruence \( \rho \) on \([1, n]\):

\[ \alpha \rho \beta \text{ if } \alpha = \beta \text{ on 3-cycle } (\alpha \beta \gamma) \in G \text{ for some } \gamma \]

Then \( \rho \) is reflexive, symmetric, \( G \)-invariant

And, \( \rho \) is transitive: since \( \alpha \rho \beta \rho \gamma \Rightarrow \exists (\alpha \beta \delta) \in G \) if \( \delta = \gamma \)

If \( \delta \neq \gamma \exists (\beta \gamma e) \) so \( (\alpha \beta \delta), (\beta \gamma e) \leq G \text{ is } A_4 \text{ or } A_5 \Rightarrow (by \alpha \rho \beta) (\alpha \beta \gamma) \in G \)
⇒ \( \alpha, \beta \) lie in a 3-cycle in \( G \) for any \( \alpha, \beta \) (as \( \rho \) universal)
⇒ Let \( \alpha, \beta, \gamma \in [1, n] \) distinct, let \((\alpha\beta\gamma), (\beta\gamma\epsilon)\) be suitable 3-cycles (using \( \alpha \rho \beta, \beta \rho \gamma \)) ⇒ \((\alpha\beta\gamma) \in G\) by above
⇒ have all 3-cycles of \( A_n \) in \( G \) ⇒ \( G = A_n \)

\( G \) primitive on \( \Omega \), say \( \Gamma \) is Jordan set if the pointwise stabiliser in \( G \) of \( \overline{\Gamma} = \Omega \setminus \Gamma \) is transitive on \( \Gamma \)
\( \Gamma \) is a primitive Jordan set if \( G \) is primitive on \( \Gamma \)
Note: If \( k \)-transitive on \( \Omega \), then any subset of size \( n - k + 1 \) is a Jordan set

Exercise: If \( G \) is a primitive group with primitive Jordan set (size \( m \)), then show that \( G \) is \((n - m + 1)\)-transitive
(Hint: Consider \( \Gamma, \Gamma g, \Gamma \setminus (\Gamma g \cap \Gamma) \) is a block of non-primitive of \( G \) \( \Gamma \) on \( \Gamma \), so just a singleton)

**Corollary 6.3**
\( G \) primitive on \( \Gamma \), \(|\Omega| = n \), if \( \frac{n}{2} < p < n - 2 \), if \( p | |G| \) ⇒ \( G \geq A_n \) (such prime exists for \( n \geq 8 \))

**Proof**
Exercise

Exercise*: If \( G \) is primitive on \( S_n \), and \( p \) is a prime with \( \frac{n}{2} < p < n - 2 \). If \( G \) contains a \( p \)-cycle then \( G \geq A_n \)
Hence: if \( \frac{n}{2} < p < n - 2 \) a prime, then \( p \mid |G| \)

Recall, conjugacy classes of elements of \( S_n \) corresponds to partitions of \( n \):
Two elements of \( S_n \) are conjugate in \( S_n \) ⇔ they have same cycle-type (in disjoint cycle notation)
**Notation:** \( n_1^{a_1}n_2^{a_2} \cdots n_k^{a_k} \) means \( a_i \) of \( n_i \)-cycles, \( n_1 > n_2 > \cdots > n_k \geq 1 \), \( n = \sum a_i n_i \)

**Lemma 6.4**
The size of \( S_n \)-conjugacy class of elements of type \( n_1^{a_1} \cdots n_k^{a_k} \) is

\[
\frac{n!}{a_1!(n_1)^{a_1} \cdots a_k!(n_k)^{a_k}}
\]

Centralizer of one such element is a direct product of \( k \) wreath products:

\[
(C_{n_1}^{a_1} \times S_{a_1}) \times (C_{n_2}^{a_2} \times S_{a_2}) \times \cdots \times (C_{n_k}^{a_k} \times S_{a_k})
\]

**Proof**
n! permutation of \( n \) numbers, hence explain the numerator.
We need to quotient out those which determine the same cycle:
There are \( n_i \) ways to write the same \( n_i \)-cycle, and we have \( a_i \) of those, so have \( n_i^{a_i} \) in the denominator
Also there are \( a_i! \) ways to permute these \( a_i \) lot of \( n_i \)-cycle.

**Lemma 6.5**
Conjugacy classes of elements in \( A_n \): elements in \( A_n \) have type \( n_1^{a_1} \cdots n_k^{a_k} \) with \( \sum n_i a_i \) even
For such elements, the conjugacy classes under \( A_n \) is the whole of its \( S_n \)-ccl, unless all the \( n_i \) are odd, all the \( a_i = 1 \); this is the only case where \( C_{S_n}(x) = C_{A_n}(x) \) so then the \( S_n \)-ccl splits into two \( A_n \)-ccls of equal length

**Proof**
Exercise

25
6.1 Structure of Aut($A_n$)

Note, $A_m \rightarrow A_k \Rightarrow k \geq m$

$m \geq 5 \Rightarrow$ any action of $A_m$ is on $\geq m$ points

**Lemma 6.6**
If $n > 6$, then $\forall H \leq A_n$ s.t. $H \cong A_{n-1} \Rightarrow H = (A_n)_\alpha$ of some $\alpha \in [1,n]$ 

**Proof**
$n = 4, 5$ Use Sylow. So assume $n > 6$ now.
Now $A_{n-1}$ is simple, so $H$ has no permutation of degree $k$ with $1 < k < n - 1$
Assume $H$ is not a stabilizer of some point.
$\Rightarrow H$ is transitive on $[1,n]$ an in fact primitive there.

Now $n > 7$ (as $7 \not| A_6$). Let $x \in H$ which goes to 3-cycles in $A_{n-1}$ under our isomorphism $\phi : H \rightarrow A_{n-1}$
Now $C_{A_{n-1}}(x\phi) = (x\phi) \times A_{(n-1)-3}$
$\Rightarrow C_H(x) > A_{n-4}$
$\Rightarrow C_A(x) \geq C_H(x) > A_{n-4}$
$\Rightarrow x$ is a 3-cycle on $[1,n]$ (other elements of order 3 have smaller centralizer)
$\Rightarrow H = A_n$ by Corollary 6.3

**Remark.** This fails for $n = 6$ because
(1) $A_5$ acts on transitively on the set of size 6 of its Sylow 5-subgroups
(2) $C_{A_6}(1^{31}) = C_{A_b}(3^2)$
$\mid ccl_{A_b}(123)\mid = \mid ccl_{A_b}(123)(456)\mid$
$\mid ccl_{S_6}(123)(45)\mid = \mid ccl_{S_6}(123456)\mid$
$\mid ccl_{S_6}(12)\mid = \mid ccl_{S_6}(12)(34)(56)\mid$

**Theorem 6.7**
$Aut(A_n) = S_n$, for $n > 3$, unless $n = 6$

**Proof**
Assume $n \geq 4, n \neq 6$. Any automorphism permutes the subgroups of $A_n$ isomorphic to $A_{n-1}$. There are precisely $n$ of these, one corresponding to each point of $[1,n]$, so any automorphism induces a permutation of $[1,n]$.
$\Rightarrow$ have the injection $Aut(A_n) \hookrightarrow S_n$
This is obviously surjective because conjugation by element of $S_n$ is an automorphism. $\Rightarrow$ $Aut(A_6) \cong S_6$

**Theorem 6.8**
$Aut(A_6) = \Sigma_6$, a group of order 1440, containing $S_6$ as a subgroup of index 2.

**Proof**
Existence:
Let $G$ e a simple group of order 60 (e.g. $A_5$)
$\Rightarrow G$ has 6 Sylow 5-subgroup, on which it acts.
$\Rightarrow \exists$ faithful permutation representation $\phi : G \rightarrow A_6$

$G\phi \leq A_6$ of index 6, this gives a permutation representation $A_6 \rightarrow A_6$ which must be an isomorphism.
This automorphism takes $G\phi$ (now a transitive subgroup of $A_6$) to the stabiliser of a point of $A_6$.
Now the elements of order 3 on the left are type $3^2$ (as $3 \not| \frac{60}{6}$), but those on the right are of the type $1^{63}$
$\Rightarrow$ this automorphism is not induced by conjugations
$\Rightarrow$ $Aut(A_6) > S_6$

Index 2:
Any automorphism fixing the ccl of 3-cycles is induced by conjugation from $S_6$
There are only two ccls of elements order 3
If \( \theta_1, \theta_2 \) are two automorphism swapping these two classes (i.e. \( \theta_1, \theta_2 \in \Sigma_6 \setminus S_6 \)), then \( \theta_1^{-1} \theta_2 \) fixes each of these ccls, so is in \( S_6 \)
\[ |\Sigma_6 : S_6| = 2 \]

**Corollary 6.9**

\( G \) simple order 60 \( \Rightarrow G \cong A_5 \cong PSL_2(5) \cong PSL_2(4) \)

**Proof**
The proof of Theorem 6.8 uses an arbitrary simple group of order 60.

Example: (Bochart)

\( H \) a primitive subgroup of \( S_n \), not containing \( A_n \)
Then \( |H| \leq n!/\lfloor \frac{n+1}{2} \rfloor! \) (e.g. \( n = 6, S_5 \) on Syl_3)
Let \( k \) be maximal s.t. \( H \cap S_k = 1 \); \( |H| = |HS_n/2| \leq n! \) and \( |\Gamma| = k \). Take \( \Gamma \) s.t. \( |\Gamma| = k \) and \( H \cap \text{Sym}(\Gamma) = 1 \)

**Claim:** \( k \geq \frac{n}{2} \)

**Proof of Claim:**
\[ \exists g(\neq 1) \in H \cap \text{Sym}(\Gamma), \alpha g \neq \alpha, \alpha \in \Gamma \]
\[ [g, h] \text{ is 3-cycle (check)} \]
\[ \exists h(\neq 1) \in H \cap \text{Sym}(\Gamma \cup \{\alpha}\}) \]
\[ \Rightarrow H \geq A_n \]

Sylow \( p \)-subgroups of \( S_n \):
\[ n = n_1 p^{e_1} + n_2 p^{e_2} + \cdots + n_e p + n_{e+1} \quad 0 \leq n_i < p \]

Concentrating on the case \( p^{e_1}, e_1 = 1 : \)
\[ p_2, e_1 = 2: \quad (C_p)^p \times C_p \]
\[ \vdots \]
\[ p_n \]
\[ p_{n+1} \]
\[ (P_n)^p \times C_p \]

Any Sylow \( p \)-subgroup is
\[ \prod_{1 \leq i \leq e_1} \frac{P_{e_i} \times \cdots \times P_{e_j}}{n_i \text{ times}} \]

Thus has the right order

How about maximal subgroups \( H \) of \( A_n, S_n \) (and other subgroups \( G \) with \( A_6 < G \leq \Sigma_6 \))?

What if \( H \) is intransitive on \([1, n]\)? Then \( H \) has an orbit of size \( 1 \leq k \leq \frac{n}{2} \) and \( H \leq S_k \times S_{n-k} \)
So the maximal subgroups intransitive on \([1, n]\) are precisely \( S_k \times S_{n-k} \) for \( 1 \leq k \leq \frac{n}{2} \)

**Lemma 6.10**
The maximal intransitive subgroups of \( S_n \) are \( S_k \times S_{n-k} \) for \( 1 \leq k \leq \frac{n}{2} \)
These are maximal in \( S_n \) unless \( k = \frac{n}{2} \) (\( n = 2k, S_k \times S_k < (S_k \times S_k) \times S_2 < S_{2k} \))

**Proof**
Let \( S_k \times S_{n-k} < X \leq S_n \)
Then \( X \) on \([1, n]\) is transitive, in fact primitive, (unless \( n = 2k \)), since \( X \) is then 2-transitive. If not, take \( \alpha \) from \( k, X_\alpha \) has suborbits of size \( 1, k-1, n-k \). Take \( \beta \) from \( n-k, X_\beta \) has suborbits size \( 1, k, n-k-1 \) Impossible unless \( n = 2k \)
But \( X \) contains a transposition and 3-cycle.
\[ \Rightarrow X \geq A_n \]
Addition to previous lectures: 
\[ A_n \trianglelefteq S_n \leq \text{Aut}(A_n) \]
\[ \theta : \text{Aut}(A_n) \to S_n \]
\[ K = \ker \theta, \ K \cap A_n = \{1\} \Rightarrow [K, A_n] = 1 \Rightarrow K = 1 \text{ so } \theta \text{ injective} \]

Exercise: Sylvester’s construction of an outer automorphism of $S_6$ (Wilson Ex 2.19)

### 6.2 Wreath Products

Let $C$ be a group, let $D$ be a permutation group on $\Delta$

The wreath product $C \wr \Delta D$ is the semidirect product of the base group $C^\Delta$ (the direct product of $|\Delta|$ copies of $C$) by $D$, with $D$ acting by permuting the components:

\[ (c_{\delta_1}, c_{\delta_2}, \ldots, c_{\delta_l})d = (c_{\delta_1d^{-1}}, c_{\delta_2d^{-1}}, \ldots, c_{\delta_l^{-1}}) \]

i.e. $C \wr D = C^\Delta \ltimes D$

Suppose now $C$ acts on $\Gamma$ as a permutation group. The imprimitive action of $C \wr D$ on $\Gamma \times \Delta$:

Action of base group: \( (\mu, \delta)(c_{\delta_1}, \ldots, c_{\delta_l}) = (\gamma c_{\delta}, \delta) \)

Action of $D$: \( (\mu, \delta)d = (\mu, \delta d) \)

For $\delta \in \Gamma$, let $\Gamma_\delta = \{ (\mu, \delta) | \mu \in \Gamma \}$ (block of imprimitivity), then $B = \{ \Gamma_\delta | \delta \in \Delta \}$ is the set of blocks

\[ \Rightarrow C \wr D \text{ is imprimitive on } \Gamma \times \Delta \]

In particular, have $S_k \wr S_l$ imprimitive on $\Gamma \times \Delta$, with $|\Gamma| = k, |\Delta| = l$

**Lemma 6.11**

Let $G$ be (transitive but) imprimitive on $\Gamma$, $|\Gamma| = n$ so $G \leq S_n$, with $l$ blocks of size $k$. Then $G \leq S_k \wr S_l$ (the full stabilizer of this partition of $\Gamma$ into blocks). Moreover, these groups $S_k \wr S_l$ are maximal in $S_n$ ($n = kl$)

**Proof**

(Proof of moreover part): $S_k \wr S_l < H \leq S_n$. Then $H$ on $[1, n]$ is transitive, in fact primitive.

$H_\alpha$ contains $S_{k-1} \times S_k \wr S_{l-1}$

But $H$ contains transpositions $\Rightarrow H = S_n$ (c.f. Theorem 6.2) \qed

**Remark.** If we are in $A_n$ rather than $S_n$, use the 3-cycles in $H$, unless $k = 2$. The case $k = 2$ is harder

and have to use elements of type $2^2$, in fact it is false if $n = 8$: $S_2 \wr S_4 \leq AGL(3, 2)$ \( \text{index } 7 \)

How about $G$ primitive on $[1, n]$?

Let $N_1, N_2$ be minimal normal in $G$ and $N_1 \neq N_2$

Then $[N_1, N_2] = 1$, and the $N_1, N_2$ are both transitive on $[1, n]$, so regular on $[1, n]$ and $C_G(N_1) = N_2, C_G(N_2) = N_1$ (c.f. Lemma 5.10)

Also, the $N_i$ are non-abelian.

It follows that $G$ has at most two minimal normal subgroups.

If two, these are non-abelian, isomorphic to each other:

Put $N = N_1 \times N_2$ (the socle of $G$)

Put $H = N_{\theta} \Rightarrow N = HN_1 = HN_2$ and $H \cap N_i = 1$

$\Rightarrow H \cong H/H \cap N_i \cong HN_1/N_1 = N_1N_2/N_1 \cong N_2$ and by symmetry $H \cong N_1$

In fact, by Lemma 5.8, can identify $\Omega$ and $N_2$ so that $N_2$ acts by right regular action: $n * L n_2 = n n_2$

for $n \in \Omega, n_2 \in N_2$

$\Rightarrow$ Nacts by left regular action on $\Omega$ as above since $N_1 = C_{S_n}(N_2)$: $n * L n_1 = n_1^{-1} n$ for $n \in \Omega, n_1 \in N_1$

These actions commutes: $n * L n_1 * n_2 = n_1^{-1} n n_2 = n * R n_2 * L n_1$

So $N$ acts on $\Omega$ by $n * (n_1, n_2) = n_1^{-1} n n_2$

This is so-called diagonal action, due to Burnside
E.g. \( A_5 \times A_5 \) acting on \( A_5 \): \( x(g,h) = g^{-1}hx \), \( G_1 = \{(g,g) \mid g \in A_5 \} \)
The \( G_1 \) orbits are ccls in \( A_5 \)

Now \( G \leq N_{S_n}(N) \), but also \( \exists g \in N_{S_n}(N) \setminus G \): 
g acts as \( n \mapsto n^{-1} \) 
\( \Rightarrow \) \( G \) is never maximal in \( S_n \) (or \( A_n \))
\( \Rightarrow \) \( N = T^{2k} \) where \( T \) is non-abelian simple and \( n = |T|^k \)

Summarizing:

**Lemma 6.12**
If \( G \) is primitive subgroup of \( S_n \), then \( G \) has at most two minimal normal subgroup.
If have two, they have to be regular, non-abelian, isomorphic to (each other) \( T^k \) with \( T \) non-abelian simple, \( k \geq 1 \), with \( n = |T|^k \)
And \( G \) is not maximal in \( S_n \) (or \( A_n \))

**Exercise:** \( G \times G \) on \( G \) by \( g \ast (g_1,g_2) = g_1^{-1}gg_2 \) is transitive; it is primitive \( \iff \) \( G \) simple

**Lemma 6.13**
(c.f. Lemma 5.8) If \( G \) has a regular elementary abelian normal subgroup, then \( G \leq AGL_d(p) \leq S_n \), 
\( n = p^d \)
In addition, if \( G \) transitive, \( G \) is primitive \( \iff \) \( G_0 \) is an irreducible linear group on \( V_d(p) \)

Let \( G \) primitive with a unique minimal normal subgroup \( N \)
If that is abelian, then \( |N| = p^d \) and have \( G_0 \) being an irreducible linear group on \( V_d(p) \)

### 6.3 The primitive (product) action of wreath products

\( C \) acts on \( \Gamma \), \( D \) acts on \( \Delta \) \( |\Gamma| = k \), \( |\Delta| = l \)
\( C \wr D \) acts on \( \Gamma^\Delta \), degree \( k^l \) (not \( \Gamma \times \Delta \) as \( C \wr D = C^\Delta \ltimes D \))

Action by base group \( C^\Delta \):
\[
(\gamma_\delta_1, \ldots, \gamma_\delta_l)(c_\delta_1, \ldots) = (\gamma_\delta_1c_\delta_1, \ldots, \gamma_\delta_lc_\delta_l) \quad \text{(coordinate-wise)}
\]
\[
(\gamma_\delta_1, \ldots, \gamma_\delta_l)d = (\gamma_\delta_1d^{-1}, \ldots, \gamma_\delta_l)d^{-1})
\]

**Lemma 6.14**
If \( D \) transitive on \( \Delta \), \( C \) primitive on \( \Gamma \) but not regular \( C_p \), then \( C \wr D \) is primitive on \( \Gamma^\Delta \), degree \( k^l \)

**Proof**
Let \( \gamma \in \Gamma \). The stabilizer of the constant point \( (\gamma, \gamma, \ldots, \gamma) \) is \( H = C_{\gamma} \wr D \)

**Claim:** \( H \) is maximal in \( C \wr D \)

**Proof of Claim:**
Exercise

Example:
\( W(k,l) = S_k \wr S_l \), degree \( n = k^l \), with \( k \geq 3 \) is primitive
If \( k = 3 \) or \( 5 \), we have an elementary abelian regular normal subgroup
\( \Rightarrow \) previous case \( \Rightarrow \) assume \( k \geq 5 \)
This is usually maximal in \( S_k \), \( n = k^l \)
Exercise:
\[ W(k, l) \text{ with } k \geq 2 \text{ has rank } l + 1, \text{ subdegrees are } 1, l(k - 1), \binom{l}{2}(k - 1)^2, \ldots, \binom{l}{l}(k - 1)^l. \]

### 6.4 Diagonal Actions

\[ N = T^m, T \text{ non-abelian simple, } n = |T|^{m-1}, m \geq 2 \]

\[ D := \{(t, \ldots, t) \in T^m | t \in T\} \subset N \]

diagonal subgroup of \( N \), \( \Omega = (N : D) \)

\[ D(T, m) := N_{S_m}(T^m) \]. In fact, \( D(T, m)/T^m \cong \text{Out}(T) \times S_m \) (Note that \( \text{Out}(T) = \text{Aut}(T)/T \) here)

Action of \( N \): \( D(x_1, \ldots, x_m)(t_1, \ldots, t_m) = D(x_1t_1, \ldots, x_mt_m) \)

Action of \( \text{Aut}(T) \): \( D(x_1, \ldots, x_m)\alpha = D(x_1^\alpha, \ldots, x_m^\alpha) \)

Action of \( S_m \): \( D(x_1, \ldots, x_m)\pi = D(x_1\pi^{-1}, \ldots, x_m\pi^{-1}) \)

Example:
\( m = 2, D(T, 2) = (T \times T) \cdot (\text{Aut}(T) \times C_2) \)

may identify \( \Omega \) with \( T \):

\[
\begin{align*}
(t_1, t_2) : & \quad t \mapsto t_1^{-1}t_2 \\
\alpha : & \quad t \mapsto t^\alpha \\
\pi(\in S_2) : & \quad t \mapsto t^{-1}
\end{align*}
\]

\( G < S_n, n = |T|^{m-1} \) is of diagonal type if \( T^m \leq G \leq D(T, m) \). Such \( G \) is primitive \( \iff \) the action of the subgroup of \( S_m \) on coordinates is primitive.

The groups \( D(T, m) \) is usually maximal in \( S_n \) or \( A_n \)

**Theorem 6.15 (O’Nan Scott)**

If \( G < S_n \) primitive, then \( G \) is either almost simple or \( G \) is a subgroup of one of:

1. \( S_k \times S_{n-k} \)
2. \( S_k \text{ wr } S_{n/k} \)
3. \( AGL_d(p) \) (affine action), \( n = p^d \), a prime power
4. \( W(k, l) \) (product action), \( n = k^l, k \geq 5 \)
5. \( D(T, m) \) (diagonal action), \( n = |T|^{m-1}, m \geq 2, T \) non-abelian simple

(Proof omitted, see Wilson’s book, also, a more precise revision for primitive permutation groups giving a structure)

**Corollary 6.16**

Maximal subgroups of \( S_n \) (or \( A_n \)):

1. \( S_k \times S_{n-k}, k < \frac{n}{2}, \) intransitive
2. \( S_k \text{ wr } S_l, n = k \times l, \) imprimitive
3. \( AGL_d(p), n = p^d \)
4. \( D(T, m), n = |T|^{m-1} \)
5. \( G \) primitive almost simple
Proof
May appear later (or not)
In fact, with a stronger version for $G$ primitive subgroups of $S_n$:
$G$ is almost simple except in cases we have seen (plus one other)

But which are maximal in $S_n$ (or $A_n$)?
Example:
$S_5 < S_{10}$ on $\binom{5}{2}$, $(S_5 : S_3 \times S_2)$, maximal? Do not know
$S_6 < S_{10}$ on $3|3$ (partition into three 3s), $(S_6 : S_3 \wr S_2)$
$S_5 < S_6 < S_{10}$
Let $G = S_6$, $H = S_5$, have a factorisation of $S_6$:

$$G = S_6$$
$$G_\alpha = S_3 \wr S_2$$
$$S_5 = H$$

$H$ is transitive, on $S_6$: $S_3 \wr S_2$
So need to know factorisation

$$G = AB$$
$$A \wr S_2$$
$$B$$

these are now known for $G$ almost simple. The question is answered

Upshot: $G$ almost simple and primitive of degree $n$ $\Rightarrow$ $G$ maximal in $A_n$ or $S_n$ unless in a list

Example:
$G = S_m$ $|A||B|$ large
Let $\frac{m}{2} < p < m - 2$, a prime (exists for $m \geq 8$, by Chebychev)
$\Rightarrow p|m! \Rightarrow p||A| \text{ or } p||B|$
$m! = |AB| = \frac{|A||B|}{|A \cap B|}$

By remarks earlier, if $A$ is primitive on $[1, m]$ then $A \geq A_m$ #
$\Rightarrow A$ is intransitive on $[1, m]$ (cannot be transitive but imprimitive as $p||A|)$
$\Rightarrow A = S_k \times S_{m-k}$ for some $k$ with $1 \leq k < \frac{m}{2}$

Case $k = 1$ is not very interesting.
Assume $k > 1$. Then $B$ is transitive on $\binom{m}{k}$ ($k$-subsets of $[1, m]$). We say $B$ is $k$-homogeneous on $[1, m]$

$k = 2 : B$ is 2-transitive on $|B|$ odd (in fact, it is solvable)
$k > 2 : G$ is $k$-homogeneous $\Rightarrow G$ is $(k - 1)$-homogeneous

Exercise: If $\pi_k$ is the permutation character of $S_m$ on $\binom{m}{k}$, then $\pi_k = \pi_{k-1} + \chi_k$ where $\chi_k$ is irreducible (use $\langle \pi_k, \pi_l \rangle = 1 + \min(l, k)$)
$\Rightarrow B$ a is known group
So, to find maximal subgroup of $S_m$ (or $A_m$), it is necessary and sufficient to find the maximal subgroup of all smaller almost simple groups.

### 6.5 Doubly transitive representations of $S_m$ or $A_m$

**Theorem 6.17 (Maillet)**
If $S_m$ (or $A_m$) is 2-transitive degree $n$, then $n = m$, or one of the below ($m \leq 8$)

1. $m = 5; n = 6$
2. $m = 6; n = 6$ or $10$
3. $m = 7, 8; n = 15$ and this only happens in $A_m$

**Lemma 6.18**
If $G$ is a transitive permutation group on $\Omega$, and $G$ has a ccl $C \neq \{1\}$, then $G$ has a non-trivial subdegree at most $|C|$

**Proof**
Fix $c \in C$. Let $\alpha \in \Omega$ with $\beta = \alpha c \neq \alpha$. Consider $\beta G_\alpha$:

If $\omega \in \beta G_\alpha$, have $\omega = \beta h$ some $h \in G_\alpha$

$\Rightarrow \omega = \alpha h^{-1} c h$ with $h^{-1} ch \in C$

**Sketch Proof of Theorem 6.17**
In $S_m$, take $C = \{\text{transposition}\}$
In $A_m$, take $C = \{3\text{-cycles}\}$

$\Rightarrow n - 1 \leq \frac{1}{2} m(m - 1)$

Let $H$ be the stabiliser of a point in $[1, n]$

$\Rightarrow |S_m : H| = m$ and $H$ maximal on $S_m$

If $H$ is primitive on $[1, m]$, then “small” by Bochert (see Example after Corollary 6.9):

$\frac{m+1}{2}! \leq 1 + \frac{1}{2} m(m - 1) \Rightarrow m \leq 6$

(If in $A_m$, get $m \leq 8$)

If $H$ is transitive but not primitive on $[1, m]$, then $H = S_k wr S_{m/k}$, the action is on $k|k|\cdots|k$, not 2-transitive on $m > 6$

If $H$ is intransitive on $[1, m]$, the action of $S_m$ is on $\binom{n}{k}$, not 2-transitive unless $k = 1$

### 7 Linear Groups

Let $F$ be a field, here usually finite $F = \mathbb{F}_q$, $q = p^l$

$GL_d(F)$, group of invertible linear transformation on $V = V_d(F)$

For $F = \mathbb{F}_q$, write $GL_d(q)$, group of all non-singular $d \times d$-matrices over $F$

$|GL_d(q)| = (q^d - 1)(q^d - q)\cdots(q^d - q^{d-1})$

$SL_d(q) \leq GL_d(q)$ matrices of determinant 1

$|SL_d(q)| = |GL_d(q)|/(q - 1)$

$PGL_d(q) := GL_d(q)/Z$, where $Z = \{\text{scalar matrices in GL}\}$

$L_d(q) = PSL_d(q) := SL_d(q)/Z \cap SL_d(q)$, has order $|SL_d(q)|/e$, where $e = (d, q - 1)$

$PGL_d(q)$ acts naturally on the set of 1-subspaces of $V_d(q)$ (i.e. the projective space of dimension $d - 1$, $\mathbb{F}_{d-1}(q)$, of size $\frac{q^d - 1}{q - 1}$)

Recall: $PGL_d(q)$ is 2-transitive, and is 3-transitive $\iff d = 2$

$PSL_2(q)$ is 2-transitive, and is 3-transitive $\iff q = 2^l$
More on $d = 2$: “Möbius action” of $PGL_2(q)$ of degree $q + 1$, $\mathbb{F}_q \cup \{\infty\}$

**Lemma 7.1**
$$\langle (x, y) \rangle \leftrightarrow \begin{cases} \frac{x}{y} & y \neq 0 \\ \infty & y = 0 \end{cases}$$
$$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az + b}{cz + d} \quad ????

$PSL_2(q) = \{z \mapsto \frac{az + b}{cz + d} | ad - bc \text{ is a non-zero square}\}$

$AGL_1(q) = \{z \mapsto az + b | a \neq 0\}$

$G_{\alpha \beta \gamma} = 1$, any $\alpha, \beta, \gamma$ distinct

$G_{0 \infty} = \{z \mapsto \alpha z | a \neq 0\}$

$G$ is 3-transitive, with $G_{\alpha \beta \gamma} = 1 \forall \alpha \beta \gamma$

Generators of $PGL_2(q)$:
- $z \mapsto z + 1$
- $z \mapsto \lambda z$ \quad ($\langle \lambda \rangle = \mathbb{F}_q^\times$)
- $z \mapsto -1/z$

**Lemma 7.2**

<table>
<thead>
<tr>
<th>$q$</th>
<th>Group</th>
<th>order</th>
<th>degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$L_2(2) \cong S_3$</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>$L_2(3) \cong A_4$</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>$L_2(4) \cong A_5$</td>
<td>60</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>$L_2(5) \cong A_5$</td>
<td>60</td>
<td>6</td>
</tr>
</tbody>
</table>

Also: $L_2(9) \cong A_6 \cong \Omega_4^+ (3)$, $L_2(7) \cong L_3(2)$, $L_4(2) \cong A_8 \cong \Omega_6^+ (2)$, $L_4(2) \not\cong L_3(4)$

**Proof**

Exercise

**Theorem 7.3**

$L_d(q)$ is simple for $d \geq 2$, unless $d = 2, q \leq 3$

To prove this, we need Iwasawa’s Lemma:

**Lemma 7.4 (Iwasawa’s Lemma)**

Let $G$ be a perfect group (i.e. $G' = G$) acting primitively on a set $\Omega$, let $\alpha \in \Omega$, and assume $G_{\alpha}$ has a normal subgroup $K$ which is abelian (or just solvable) with $G = \langle K^g | g \in G \rangle$

If $N \unlhd G$, then $N \leq G_{(\Omega)}$, the kernel of $G$ on $\Omega$, or $N = G$

So $G/G_{(\Omega)}$ is simple

**Example:**

$A_n$ is simple: Consider $G = A_n$ acting on $\binom{n}{3}$, the 3-subsets, (for $n = 6, 3|3$)

$G_{\alpha} = (S_{n-3} \times S_3) \cap A_n, K = \langle (123) \rangle$

**Proof**

Assume $N \not\leq G_{(\Omega)}$, so $N$ transitive on $\Omega$

$\Rightarrow G = NG_{\alpha}$. Hence $NK \not\unlhd NG_{\alpha} = G$

Now, $\langle K^g | g \in G \rangle = G$

$\Rightarrow NK = G$

$\Rightarrow G/N \cong NK/N \cong K/K \cap N$ is abelian

$\Rightarrow G' \leq N$, but $G = G'$

$\Rightarrow N = G$

□
Definition

$t \in SL_d(q)$ is a transvection if $t - 1$ has rank 1 and $(t - 1)^2 = 0$
(JNF has 1 block size 2, all other size 1) 

Note: If $t$ is a transvection on $V$, then wrt some basis $B$ of $V$, $t$ has matrix of form

\[
\begin{pmatrix}
1 & 0 \\
0 & \ddots \\
0 & 1 & 1
\end{pmatrix}
\]

This is because, let $W = \ker(t - 1)$, let $v_d \in V \setminus W$, let $v_1 = v_d(t - 1)$
extend the basis $v_1, \ldots, v_d - 1$ of $W$, get $B = \{v_1, \ldots, v_{d-1}, v_d\}$
Also, the elementary matrices $E^{(s)}$ are transvections $X_{ij}(\lambda), X_{ij}(\lambda)^{-1} = X_{ij}(-\lambda)$

Transvection subgroup: $X_{ij} = \{X_{ij}(\lambda) | \lambda \in F_q\}$

Exercise: All transvections are conjugate in $SL_d(q)$ if $l = 2$. If $d = 2, q$ odd then two ccls

Proposition 7.5

$SL_d(q)$ is generated by the transvections

Proof

Linear algebra: any matrix of det 1 can be reduced to $I_A$ by applying elementary row operations

$v_i := v_i + \lambda v_j, i \neq j$

Each of these operations is just multiplication on the left by a matrix $E^{(s)}$

$E^{(n)} \cdots E^{(1)} A = I \Rightarrow A = (E^{(1)})^{-1} \cdots (E^{(n)})^{-1}$

Proof of Theorem 7.3

Let $G = SL_d(q)$. Then $G$ is 2-transitive, hence primitive, on $\Omega = \{1$-subspaces of $V_d(q)\}$

Kernel $G(\Omega) = \{\text{scalar matrices}\}$

Let $\alpha = \langle(1, 0 \cdots 0)\rangle$

\[
\Rightarrow \quad G_{\alpha} = \left\{ \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ \lambda_2 & \ddots & \ddots \\ \vdots & \ddots & H_{d-1} \\ \lambda_d \\ \end{pmatrix} : \lambda_i \in F_q \right\}, \quad K = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ \lambda_2 & \ddots & \ddots \\ \vdots & \ddots & I_{n-1} \\ \lambda_d \\ \end{pmatrix} : \lambda_i \in F_q \right\}
\]

elementary abelian order $q^{d-1}$ normal in $G_{\alpha}$

The elements of $K \setminus \{1\}$ are transvections.

We shall check they generate $G$, and each is a commutator in $G$ (shown in next proposition)

Proposition 7.6

$(d > 1)$ All transvections are commutators, except when $d = 2, q \leq 3$

Proof

If $d \geq 3$

\[
\begin{pmatrix} 1 & 1 \\ \alpha & 1 \\ \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \beta & 1 \\ \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -\alpha & 1 \\ \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -\beta & 1 \\ \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -(\alpha \beta) & 1 \\ \end{pmatrix}
\]

so if $\alpha \neq 0$, take $\beta = \alpha^{-1} \gamma$

$d = 2$:

\[
\begin{pmatrix} \alpha^{-1} & 1 \\ \alpha & 1 \\ \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \beta & 1 \\ \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \alpha^{-1} & 1 \\ \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \alpha^2 \beta & 1 \\ \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \beta (\alpha^2 - 1) & 1 \\ \end{pmatrix}
\]

So given $\gamma$, take $\alpha \neq 0$ with $\alpha^2 \neq 1$ ($q > 3$)

and $\beta = \gamma (\alpha^2 - 1)^{-1}$, to get $\begin{pmatrix} 1 \\ \gamma \\ \end{pmatrix}$ as a commutator
7.1 Some subgroup of $GL_d(q)$ or $SL_d(q)$

Parabolic:

(1) $B = \left\{ \begin{pmatrix} * & \cdots & 0 \\ \# & \cdots & * \end{pmatrix} \mid * \in F^*, \# \in F \right\}$ - Borel subgroup

(2) lower triangular

(3) $U = \left\{ \begin{pmatrix} 1 & \cdots & 0 \\ \# & \cdots & 1 \end{pmatrix} \mid \# \in F \right\}$ - lower unitriangular matrix $|U| = q^{\frac{1}{2}d(d-1)}$ a Sylow $p$-subgroup

$B = U \rtimes T$, with $T = \left\{ \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \# & \cdots & \lambda_d \end{pmatrix} \mid \lambda_i \in F^\times \right\}$ diagonal matrices or split torus

$V = V_d(q)$ $B$ is the stabilizer of a complete flag: $0 = V_0 < V_1 < V_2 \cdots < V = V_d$

Other flags: $0 < V_i < V_j < \cdots < V = V_d$

Stabilisers of flags are parabolic subgroups

maximal parabolic is just a stabilizer of a subspace of $W$ of $V$

$P_k$ is the stabilizer of a $k$-subgroup $W$ of $V$:

$P_k = \left\{ \begin{pmatrix} A_k & 0 \\ C & B_{d-k} \end{pmatrix} \mid (A, B) \in GL_k \times GL_{d-k}, C \text{ any of } k \times k \text{ matrix} \right\}$

(choose basis $e_1, \ldots, e_k$ of $W$ extend to a basis $e_1, \ldots, e_k, \ldots, e_h$ for $V$)

The subgroup $U_k = \left\{ \begin{pmatrix} I_k & 0 \\ * & I_{d-k} \end{pmatrix} \right\}$ is a normal subgroup of $P_k$;

$L_k = \begin{pmatrix} A_k & 0 \\ 0 & B_{d-k} \end{pmatrix}$ - complement to $U_k$ in $P_k$, the Levi subgroup of linear group of $P_k$

Then $P_k = U_k \rtimes L_k$

By the way, $N = \text{all monomial matrices}$, then $N = N_G(T)$

$T = B \cap N$, $W = N/T$ - Weyl group

Example: $GL_d(q)$, $W = \text{Sym}_d$

Remark. The subgroups of $GL_d(q)$ containing $B$ are precisely the parabolics obtained by stabilizing the flags obtained by deleting some members of the complete flag for $B$

Exercise:

$G = GL_d(q)$ has permutation rank $k + 1$ for $(G : P_k)$ ($P_k$ stabiliser of $W$, dim $k$), $1 \leq k \leq \frac{d}{2}$

And, $P_k$ is a maximal subgroup of $GL_d(q)$

Some other subgroups:

some families of geometric subgroup

Then theorem of Aschbache tells you that any subgroup $H$ of $SL$ lies in one of these or $H/Z(H)$ is almost simple, irreducible, etc....

(1) $P_k$ - the stabilizer of a $k$-subspace $W$ of $V$

(2) $V = V_1 \oplus \cdots \oplus V_k$, $d = ka$, dim $V_i = a$

$GL_a(F) \wr \text{Sym}_k$
(3) \[ V = V_1 \otimes V_2, \dim V_i = d_i, \quad d = d_1d_2, d_1 \neq d_2 \]
\[ GL_{d_1}(F) \otimes GL_{d_2}(F) \]

(4) \[ V = V_1 \otimes \cdots \otimes V_k, \quad \dim V_i = a, \quad d = a^k \]
\[ GL_a(F) \text{ wr Sym}_k \]

(5) Subfield subgroup \( \mathbb{F}_{q'} < \mathbb{F}_q \)
\[ V = W \otimes \mathbb{F}_{q'}, \quad \dim_{\mathbb{F}_{q'}} W = d \]
\[ GL_d(q') < GL_d(q) \]

(6) Extension field subgroups \( GL_{d/e}(q^e) < GL_d(q) \)

(7) "Extraspecial"

(8) Classical

Upslot: Questions about maximal subgroups of linear groups can be reduced to question about modular representation theory of quasi-almost simple groups

7.2 Automorphism group of \( PSL_d(q) \)

\[ PSL_d(q), \quad q = p^f, \quad \text{Outer automorphisms come in different flavours:} \]

\[ \begin{array}{cccc}
L_d(q) & \cong & PGL_d(q) & \cong & P\Gamma L_d(q) & \cong & \text{Aut} \\
\text{(index)} & \cong & \text{(d,q-1) ln diag} & \cong & f & \text{field auto} & \cong & 2 \text{ if } d > 2 \text{ graph auto} \\
\end{array} \]

\[ \Gamma L_d(q): \text{ semilinear transformation of } V = V_d(q) \]
\[ (r + w)\theta = r\theta + w\theta \]
\[ \exists \sigma \in \Gamma = \text{Gal}(\mathbb{F}_q / \mathbb{F}_p)(\lambda v)\theta = \lambda^\sigma v\theta \quad (\sigma \text{ depends on } \theta) \]

Fix a basis,
\[ \begin{pmatrix}
    a_{11} & \cdots & a_{1d} \\
    \vdots & \ddots & \vdots \\
    a_{d1} & \cdots & a_{dd} \\
\end{pmatrix}^\sigma =
\begin{pmatrix}
    a_{11}^\sigma & \cdots & a_{1d}^\sigma \\
    \vdots & \ddots & \vdots \\
    a_{d1}^\sigma & \cdots & a_{dd}^\sigma \\
\end{pmatrix} \]

\[ \Gamma L_d(q) = GL_d(q) \rtimes \Gamma \]

finally, a graph auto: \( A \mapsto A^{-t} \) (inverse transpose of \( A \)) an auto of \( GL \)

Exercise: Graph auto is inner if \( d = 2 \), outer otherwise
\[ \text{Aut} := P\Gamma L \rtimes \langle \tau \rangle \]

Theorem 7.7 (Steinberg, for groups of Lie type)
The Aut. group of \( L_2(q) \) is \( P\Gamma L_2(q) \)
The Aut. group of \( L_d(q) \) with \( d > 2 \) in \( P\Gamma L_d(q) : C_2 \) (semicolon denotes semidirect product)

Sketch
Need to show no more automorphisms. Let \( G = PSL_d(q) \), \( V = V_d(q) \), \( \phi \in \text{Aut}(L_d(q)) \), \( q = p^f \)

Any \( p \)-local subgroup (i.e. normaliser of a \( p \)-subgroup) stabilise (set-wise) a subspace \( \Rightarrow \) in \( P_k \) for some \( k \):
\[ H = N_G(Q), \quad Q \text{ a } p \text{-subgroup, let} \]
\[ W := \text{fix}_V(Q) \]

is a subspace kept invariant by \( N_G(Q) \). Note that if the ccls of stabilisers of hyperplanes is not \( \phi \)-invariant, adjust \( \phi \) by a graph automorphism. (note that it would have been swapped with the ccls of stabilisers of 1-spaces, as the only possibility by structure of \( P_k \)).

So assume \( \phi \) keeps the set of hyperplanes invariant, and then it follows that it keeps the set of \( k \)-spaces invariant for all \( k \). In particular, \( \phi \) acts on the set of 1-spaces.
\( G = SL_d(q) \) is transitive on the set of complete flags, so may assume that \( \phi \) stabilises a complete flags, and in fact, may assume that \( \phi \) stabilises \( \langle v_1 \rangle, \langle v_2 \rangle, \ldots, \langle v_d \rangle \), with \( \{v_1, \ldots, v_d\} \) a basis. Moreover, using a diagonal automorphism, if necessary, to adjust \( \phi \), we may assume \( \phi \) fixes \( v_1, \ldots, v_d \).

We now claim that such \( \phi \) is induced by a Galois automorphism of \( \mathbb{F}_q / \mathbb{F}_p \), i.e. \( \phi \) is semilinear on
\[
\begin{pmatrix}
1 \\
\lambda \\
\ddots \\
1
\end{pmatrix}
\begin{pmatrix}
1 \\
\mu \\
\ddots \\
1
\end{pmatrix}
= \begin{pmatrix}
1 \\
\lambda + \mu \\
\ddots \\
1
\end{pmatrix}
\]
\( \phi : \)
\[
\begin{pmatrix}
1 \\
\lambda \\
\ddots \\
1
\end{pmatrix}
\begin{pmatrix}
1 \\
\mu \\
\ddots \\
1
\end{pmatrix}
= \begin{pmatrix}
1 \\
\lambda^\sigma + \mu^\sigma \\
\ddots \\
1
\end{pmatrix}
\]
\( \lambda^\sigma \in \mathbb{F}_q, (\lambda + \mu)^\sigma = \lambda^\sigma + \mu^\sigma \)
\[
\begin{pmatrix}
\lambda \\
\lambda^{-1} \\
\ddots \\
I
\end{pmatrix}
\begin{pmatrix}
\mu \\
\mu^{-1} \\
\ddots \\
I
\end{pmatrix}
\to (\lambda \mu)^\sigma = \lambda^\sigma \mu^\sigma
\]
\[\Rightarrow \sigma \in \text{Gal}(\mathbb{F}_q) \]
A general proof: In Carter’s book, Groups of Lie type

\[\square\]

### 7.3 Some isomorphisms and interesting actions

**Exercise:** Any simple group of order 168 is isom. to \( L_2(7) \)

**Lemma 7.8**

\( L_2(2) \cong L_3(7) \)

**Proof**

\( L_3(2) \) acts on \( \mathbb{F}_2(2) \): \( V = V_3(2) \)

- points: 1-subspace of \( V \)
- lines: 2-subspace of \( V \)
- incidence: subspace of \( V \)

Fano plane (any 2 points on a unique line (of size 3)) (see picture)

In fact, can ??? mod 7 points so that 013, 124, 235, ... are lines

\( \mathbb{F}_7 \)

\( g : u \mapsto u + 1 \) on \( \mathbb{F}_7 \) (points to points, lines to lines), \( g = (0123456) \)

\( h : u \mapsto 2u \) in \( N(\langle g \rangle) \), \( h = (124)(365) \)

\( t = (12)(36) \in N_G(\langle h \rangle) \)

These generate \( L_3(2) \)

Let \( G = L_3(2) \) (or any simple group of order 168)

\( n_p(G) = 8, |N_G(P)| = 21 \)

Let \( P \in Syl_7(G) \), say \( P = \langle g \rangle \)

Number the Sylow 7-subgroups as \( P = \infty, 0, 1, \ldots, 6 \)

Choose one of the Sylow 7-subgroup as 0 and \( g : z \mapsto z + 1 \), then all the numbering are determined
Let \( h \in N_G(P) \), order 3, \( h: z \mapsto 2z \) \( (N_G(P) = N_{A_7}(P)) \)
\( \exists t \in N_G(h) \), order 2, inverting \( h \) (know this is subgroup \( L_2(2) \))
Now the stabiliser of any point in \( Syl_7(G) \) has odd order, so \( t \) is fixed-point-free in this action of degree 8:
\[
(0\infty)(1x)(2y)(4z)
\]
(\( x, y, z \in \{3, 5, 6\} \) but not known which yet)
Conjugating \( t \) by \( h \) or \( h^{-1} \), we may assume \( t: 1 \leftrightarrow 6 \)
Then \( 2t = 3 \), since \( 2t = 1ht = 1th^{-1} = 6h^{-1} = 3 \), so we get
\[
(0\infty)(16)(23)(45)
\]
Thus, \( t: z \mapsto -1/z^{-1} \)
\( \Rightarrow \) \( L_3(2) \leq L_2(7) \), so \( \cong \) by order \( \blacksquare \)

**Lemma 7.9**
\( A_6 \cong L_2(9) \), \( S_6 \cong P\Sigma L_2(9) \) (\( \Sigma \) field autos), \( \Sigma_6 \cong P\Gamma L_2(9) \)

**Proof**
Produce an action of \( A_6 \) degree 10 (3|3 - stab. is \( (S_3 \text{ wr } S_2) \cap A_6 \))
Put \( F_q = \{0, \pm 1, \pm i, \pm (1 \pm i)\} \)
Let \( g_1: z \mapsto z + 1 \), \( g_2: z \mapsto z + i \)
Now \( h \) also fixes partition 156|234
Rest of notation is now fixed, \( t: z \mapsto -1/z^{-1} \)
\( \Rightarrow \) \( A_6 \leq L_2(9) \)
The above part demonstrates actions of \( A_6 \) on \( F_q \cup \{\infty\} = F_1(9) \)
It yields \( A_6 \) can be “embedded” into \( L_2(9) \)
Now (56) acts as \( z \mapsto z^l \) a field automorphism
\( \Rightarrow \) \( S_6 \cong P\Sigma L_2(9) \) \( \blacksquare \)

Note: \( \text{Gal}(F_{p^l} / F) \) is generated by \( z \mapsto z^p \) and is cyclic of order \( l \)

Some 2-transitive actions of \( L_d(q) \):
\( L_d(q) \) is 2-transitive on \( \frac{q^d - 1}{q - 1} \) (2 actions for \( d > 2 \), 1 action for \( d = 2 \))
plus: \( L_2(7) \), deg 7 (2 action)
\( L_2(9) \), deg 6
\( L_2(11) \), deg 11
\( P\Sigma L_2(8) \cong 2G_2(3) \), deg 28
\( L_4(2) \cong A_8 \), deg 8

8 **symplectic Groups** \( Sp_d(q) \leq GL_d(q) \)

**Definition**
If \( f \) a bilinear alternating non-singular form on \( V = V_d(q) \), \( f \) is called symplectic form (We are taking definition \( f(v, v) = 0 \) for alternating because \( f(v, w) = -f(w, v) \) is weaker when \( \text{char} = 2 \))
Non-degenerate (non-singular): \( \forall v \neq 0, \exists w \text{ s.t. } f(v, w) \neq 0 \)
\( \Rightarrow \) \( V^\perp := \{w|f(v, w) = 0\} \neq V \) \( \forall v \neq 0 \)

38
Lemma 8.1
If $f$ is a symplectic form on $V$, there exists basis $e_1, f_1, e_2, f_2, \ldots e_m, f_n$ with $f(e_i, e_j) = 0 = f(f_i, f_j)$ and $f(e_i, f_j) = \delta_{ij}$

Proof
Construct:
Let $e_1 \neq 0$. Take $f_1 \in V \setminus e_1^\perp$ (non-empty) with (after scaling) $f(e_1, f_1) = 1$. Continue this process in $\langle e_1, f_1 \rangle^\perp$

Definition
Such $e_i, f_i$ is a hyperbolic pair
Then the matrix of $f$ under this basis is
\[
\begin{pmatrix}
-1 & 1 \\
-1 & 1 \\
\vdots & \ddots \\
-1 & \cdots \\
1 & \cdots \\
\vdots & \ddots \\
1 & \cdots \\
\end{pmatrix}
\]
or taking $e_1, e_2, \ldots, f_1, f_2, \ldots$

Let $G = Sp_{2m}(q)$ preserves this form, i.e. $G = \{g \in GL_{2m}(q), f(vg, wg) = f(v, w) \ \forall v, w \in V\}$
In terms of matrices $\{A \in GL_{2m}(q)|A^tJA = J\}$

$Sp_{2m}(q)$ is regular in its action on the symplectic bases. (transitive with trivial stabiliser)

Lemma 8.2
$|Sp_{2m}(q)| = (q^{2m} - 1)(q^{2m-1})|Sp_{2m-2}(q)| = \cdots = q^{m^2} \prod_{i=1}^{m} q^{2i} - 1$

Lemma 8.3
$Sp_2(q) \cong SL_2(q)$.

Proof
$A^t \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} A = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix}$ for $ad - bc = 1$

$Z(Sp_{2m}(q)) = \{\pm I\}, PS_{2m}(q) \cong Sp_{2m}(q)/\{\pm I\}$

Definition
symplectic transvections are those transvections in $Sp$
\[
t_{v, \lambda} : x \mapsto x - \lambda f(x, v)v
\]
E.g. $v = e_1$:
$f(x, e_1) = 0$ for other basis
\[ f(x, f_1) = 1, \text{ so under basis } e_1, e_2, \ldots, e_m, f_m, \ldots, f_1: \]
\[
\begin{pmatrix}
1 & \cdots & 1 \\
\vdots & \ddots & \vdots \\
\lambda & \cdots & 1
\end{pmatrix}
\]

**Proposition 8.4**

\( \text{Sp}_{2n}(q) \) is generated by these transvections

**Proof**

\( G = \{ \text{these transvections} \} \), will show \( G \) is transitive on the set of symplectic basis

1. \( G \) is transitive on the set of all vectors:
   
   To go from \( v \) to \( w \). If \( v \perp w \), then \( \forall t_{v-w, \lambda} = v + \lambda f(v, w)(v-w) \)

   Take \( \lambda = -f(v, w)^{-1} \) we get \( \forall t_{v-w, \lambda} = w \)

   If \( v \perp w \), choose \( x \in V \setminus (v^\perp \cup w^\perp) \)

   and go \( v \mapsto x \mapsto w \) by the above method

2. \( G \) is transitive on the set of hyperbolic pairs:
   
   \( (v, w_1) \) and \( (v, w_2) \) are hyperbolic pair

   If \( w_1 \not\perp w_2 \), take \( t_{w_1-w_2, \lambda} \) as in is to send \( w_1 \mapsto w_2 \)

   If \( w_1 \perp w_2 \), go \( w_1 \mapsto w_1 + v \mapsto w_2 \) which fixing \( v \)

3. \( G \) transitive on the set of symplectic basis by induction

   If \( B' = \{ e'_1, f'_1, \ldots \} \) may assume \( e'_1 = e_1, f'_1 = f_1 \) by (2)

   Then work in \( \langle e_1, f_1 \rangle = V_{2m-2}(q) \) with symplectic form obtained by restriction. Induction do the rest

**Corollary 8.5**

\( \text{Sp}_{2m}(q) \subseteq \text{SL}_{2m}(q) \)

**Proposition 8.6**

Transvections in \( \text{Sp}_{2m}(q) \) are commutators, unless \((2m, q)\) is one of \((2, 2), (2, 3)(4, 2)\)

**Proof**

This is true as \( \text{Sp}_{2}(q) = \text{SL}_{2}(q) \) for \( q \geq 3 \)

So only have to check cases \( \text{Sp}_{4}(3) \) and \( \text{Sp}_{6}(2) \) (exercise)

\( \langle \text{Sp}_{2m}(q), \text{SL}_{2m}(q) \rangle \)

**Theorem 8.7**

\( \text{PSp}_{2m}(q) \) is simple, except for \( \text{PSp}_{2}(2) \cong S_3, \text{PSp}_{2}(3) \cong A_4, \text{PSp}_{4}(2) \cong S_6 \)

**Proof**

Use Iwasawa’s Lemma 8.8

**Lemma 8.8 (Iwasawa)**

The action of \( \text{Sp}_{2m}(q) \) on the \( \frac{q^{2m-1}}{q-1} \) points of \( \mathbb{F}_{2m-1}(q) \) is rank 3, with subdegrees \( 1, q(q^{2m-2}-1)/(q-1), q^{2m-1} \)

This stabilizer of \( \langle v \rangle \) is \( P_1 = \left\{ \begin{pmatrix}
\lambda & 0 & 0 \\
* & A & 0 \\
* & * & \lambda^{-1}
\end{pmatrix} \mid \lambda \in \mathbb{F}_q^*, A \in \text{Sp}_{2m-2}(q) \right\} \) with normal subgroup \( \left\{ \begin{pmatrix}
1 & 0 & 0 \\
0 & I & 0 \\
0 & 0 & 1
\end{pmatrix} \right\} = \{ t_{v, \lambda} \mid \lambda \in \mathbb{F}_q \} \)
The action is primitive, kernel is \( \{ \pm I \} \)

**Proof**

\( v \in V \), suborbits \( \{ \langle v \rangle \} \) (size 1), \( \{ \langle w \rangle | w \in v^\perp - \langle v \rangle \} \), \( \{ \langle w \rangle | w \in V \setminus v^\perp \} \) (size \( q^{2m-1} \))

The action is primitive since any non-trivial block would consist of \( \{ \langle v \rangle \} \) together with one of the \( G_{\langle v \rangle} \)-orbits, but the size does not divide \( q^m-1 \).

Finally, \( G_{\langle v \rangle} = P_1 \) - see below about \( P_k \)

\[ \Box \]

**Proposition 8.9**

\( Sp_4(2) \cong S_6 \), so not perfect

**Proof**

\( S_6 \) on \( U = V_6(2) \) natural action as permutations of coordinates.

\( W = \{(x_1, \ldots, x_6) | \sum x_i \equiv 0 \mod 2 \} \)

\( f(x,y) = \sum x_iy_i \), bilinear form on \( U \)

\( W^\perp = \{(1,1,\ldots,1)\} \)

\( W \supseteq W^\perp \) a 4-dimensional space over \( \mathbb{F}_2 \) with a symplectic form preserved by \( S_6 \)

\( \Rightarrow \) \( S_6 \leq Sp_4(2) \) on \( V \)

\( \Rightarrow \) \( S_6 \cong Sp_4(2) \) by order.

\[ \Box \]

**Exercise:** \( S_{2m+2} \leq Sp_{2m}(2) \)

### 8.1 Parabolic subgroups in \( Sp_{2m}(q) \)

\( V = V_{2m}(\mathbb{F}_q) \)

A complete symplectic flag: 0 < \( W_1 = \langle e_1 \rangle < W_2 = \langle e_1, e_2 \rangle < \cdots < W_m = \langle e_1, \ldots, e_m \rangle < W_{m+1} = \langle e_1, \ldots, e_m, f_m \rangle \) \( W_i \) isotropic, so \( f|_{W_i} \) is 0, for each \( 1 \leq i \leq m \)

\( B \) Borel stabilises such a complete flag

The parabola are stabilisers of some flags

Maximal parabolic subgroup \( P_k := \) Stabilisers of \( W_k \) with \( W_k \subseteq W_{m+k}^\perp \)

\( P_k \) stabilise \( W = \langle e_1, \ldots, e_k \rangle \) and \( W^\perp = \langle e_1, \ldots, e_m, f_{k+1}, \ldots, f_m \rangle \) (dim \( 2m-k \))

\( W^\perp/W = \langle \overline{e}_{k+1}, \ldots, \overline{e}_m, \overline{f}_{k+1}, \ldots, \overline{f}_m \rangle \) - Symplectic space dim \( 2(m-k) \)

\( P_k \) contains a Levi subgroup \( GL_k \times Sp_{2(m-k)} : \begin{pmatrix} A & B \\ \overline{A}^t & \overline{B} \end{pmatrix} \) (on \( W, W^\perp/W, V/W^\perp \))

Kernel of the homomorphism \( P_k \rightarrow L_k \) is \( Q_k = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} \)

\( Q_k \) is the unipotent radical of \( P_k \), order \( q^{k(k+1)/2}q^{2(m-k)} \), often a “special” \( p \)-group:

\( Q' = Z(Q) = \Phi(Q) \), order \( q^{k(k-1)/2} \)

Example

\( 2m = 4, k = 1 \)

\( Q_1 = \left\{ \begin{pmatrix} 1 & \alpha \\ \beta & 1 \end{pmatrix} \right\} \), e.g. \( q = 3 \), can get \( \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \) as a product of commutator

\( k = 2, Q_2 = \left\{ \begin{pmatrix} I & 0 \\ C & I \end{pmatrix} | C = C^t \right\} \)
Exercise: \( P_1, P_m \) in general?

Remark. \( Sp_{2m}(q) \) is \( C_m(q) \) as group of Lie type

The other interesting stabilisers of subspace \( W \) have \( W \cap W^\perp = 0 \)

\[
V = W \oplus W^\perp \quad (\dim W = 2k, \dim W^\perp = 2(m - k))
\]

\[
N_k = S_{P2k}(q) \times S_{P2(m-k)}(q) < S_{P2m}(q)
\]

\( (Sp(2) \cong S_6 \text{ deg } 6,10) \)
2-transitive actions of \( Sp_{2m}(q) \): \( 2m = 2, \deg q + 1 \) and \( \deg q \) if \( q \in \{5,7,11\} \)
and \( Sp_{2m}(2) \) \( \deg 2^{m-1}(2^m \pm 1) \) on the two classes of orthogonal forms.

Automorphism groups: \( PSp_{2m}(q) \cong PGSp_{2m}(q) \) (diagonal \((2, q-1))\), \( g : f(vg, wg) = \lambda_g f(v, w) \in \mathbb{F}_q \)
\( PSp_{2m}(q) \cong PGSp_{2m}(q) \cong PG2m(q) \cong Aut \) (this last \( \cong \) has index 1 except for \( Sp(2f) \) then index 2)

9 Unitary Groups

\( F = \mathbb{F}_q^2 > \mathbb{F}_q \) a quadratic extension, \( V = V_d(q^2)\)

\[
\sigma : \alpha \mapsto \alpha^q \quad (\sigma) = \text{Gal}(\mathbb{F}_q^2 / \mathbb{F}_q)
\]

\[
\alpha \mapsto \overline{\alpha} \quad N(\alpha) = \alpha^{q+1}, N : \mathbb{F}_q^2 \rightarrow \mathbb{F}_q \quad \text{onto}
\]

Let \( f \) be a \( \sigma \)-Hermitian, left linear, non-singular form

\[
GU_d(q) = \{ g \in GL_d(q^2) \mid f(vg, wg) = f(v, w) \}
\]

If \( \dim V \geq 2 \Rightarrow \exists \) isotropic vectors:

Since, let \( v \in V \) with \( f(v, v) \neq 0 \)

Let \( u \in v^\perp \)

If \( u \) not isotropic, consider \( f(u + \lambda v, u + \lambda v) = f(u, u) + \lambda \overline{\lambda} f(v, v) \) - can make it zero by choice of \( \lambda \)

Unitary bases:

(1) \( d = 2m \quad e_1, f_1, \ldots, e_m, f_m \) as usual: \( f(e_i, f_j) = \delta_{ij}, \text{etc.} \)

\( d = 2m + 1 \quad e_1, f_1, \ldots, e_m, v \quad v \perp e_i, f_j, f(v, v) = 1 \)

\( \Rightarrow \) all forms are equivalent, for each dimension

(2) Also, have an orthonormal bases

Lemma 9.1

\[
|GU_d(q)| = q^{\frac{1}{2}(d(d-1))} (q^d - (-1)^d)(q^{d-1} - (-1)^{d-1}) \cdots (q^2 - 1)(q + 1)
\]

Proof

Write

\[
z_d = \# \text{ isotropic vectors in dimension } d
\]

\[
y_d = \# \text{ vectors norm 1} \quad \Rightarrow \quad q^{2d} = 1 + z_d + (q - 1)y_d
\]

Also, \( z_{d+1} = z_d + (q^2 - 1)y_d = -qz_d + (q^{2d} - 1)(q + 1) \)

Since \( z_0 = 0 = z_1 \), can solve recurrence: \( z_d = (q^d - (-1)^d)(q^{d-1} - (-1)^{d-1}) \)

\( \Rightarrow \quad y_d = q^{d-1}(q^d - (-1)^d) \)

The order of \( GU \) follows, by induction along an orthonormal basis
\[ |SU| = |GU|/(q+1) \quad , \quad |PSU| = |GU|/(q+1) \gcd(d,q+1) \]

In particular, \( PSL_2(q) \cong PSU_2(q) \)

**Lemma 9.2**

\( PSU_3(q) \) acts 2-transitively on the isotropic points of \( \mathbb{P}_2(q^2) \). There are \( q^3 + 1 \) of these; for larger \( d \), this leads to a primitive rank 3 action.

**Proof**

\( e \) is isotropic. Let \( f_1, f_2 \) isotropic in \( V \setminus \langle e^\perp \rangle \) (Note: no isotropic vectors in \( e^\perp \) as \( d = 3 \))

Can swap \( e, f_1, f_2 \), using an element in \( GU_3(q) \)

\[ \Rightarrow (GU_3)_e \] transitive of degree \( q^3 \), and \( SU_3 \) has index \( q + 1 \) in \( GU_3 \)

\[ \Rightarrow \] still transitive

For \( d \geq 3 \), \( PSU_d(q) \) is simple except for \( PSU_3(2) \) (order 72, 2-transitive on 9), c.f. Iwasawa Lemma

Maximal parabolic subgroups: \( P_k = \) stabiliser of a totally isotropic \( k \)-vector space = \( GL_k(q^2) \times GU_{d-2k}(q) \)

10 Orthogonal Groups

Quadratic form \( Q : V \rightarrow F = \mathbb{F}_q \)

s.t. \( Q(\lambda v) = \lambda^2 Q(v) \)

\[ Q(u + v) = Q(u) + Q(v) + f(u,v) \]

with \( f \) bilinear symmetric form

\[ \Rightarrow 2Q(v) = f(v,v) \]

In char \( F \neq 2 \), have \( Q \leftrightarrow f \) symmetric

If char \( F = 2 \), \( f \) does not determine \( Q \), and \( f \) is alternating

10.1 Case: Odd characteristic

work with \( f \) symmetric, bilinear, non-degenerate

**Lemma 10.1**

Two equivalence classes of such form:

Either \( \exists \) orthonormal basis for \( V \)

Or \( \exists \) orthonormal basis with \( f(v_i,v_i) = 1 \forall i < d \)

\[ f(v_d,v_d) = \alpha \] some non-square \( \alpha \)

**Proof**

Find \( v_1 \) s.t. \( f(v_1,v_1) \neq 0 \). “Normalize” to either 1 or \( \alpha \) (\( \alpha \) fixed non-square). Now continue in \( v_1^\perp \)

If \( f(v_1,v_1) = f(v_2,v_2) = \alpha \), can replace inside \( \langle v_1,v_2 \rangle \)

Choose \( \lambda^2 + \mu^2 \) s.t. \( \not{\text{not}} \) a square in \( F \); normalize to \( \alpha^{-1} \)

\[ \Rightarrow \lambda v_1 + \mu v_2, \mu v_1 - \lambda v_2 \] are orthonormal

\[ d = 2m + 1 \] odd: Get the same group both forms \( GO_{2m+1}(q) \)

\[ d = 2m \] even: The groups different.

More useful distinction:

(1) maximal totally isotropic space has dimension (called **Witt index**) \( m \), \( Q_{2m}^+ \)

(2) Witt index \( m - 1 \), \( Q_{2m}^- \)
Write

\[ GO_{2m}^\epsilon (q) = \{ g \in GL_{2m}(q) | Q_{2m}^\epsilon (vg) = Q(v) \ \forall v \} \quad (\epsilon = \pm) \]

**Lemma 10.2**

If \( d = 2 \), there may or may not exists isotropic vectors: according to type of \( Q \) and \( q \equiv \pm 1 \) mod 4

**Proof**

\( q \equiv 1 \) mod 4: If \( f(u, u) = 1 = f(v, v) \) an \( u \perp v \), let \( i = \sqrt{-1} \in F \)

\[ f(u + iv, u + iv) = 0 \implies u + iv \text{ isotropic} \]

If \( f(u, v) = 1, f(v, v) = \alpha \), with \( u \perp v \)

\[ f(u + \lambda v) = 1 + \lambda^2 \alpha \]

\[ f(u + \lambda v) \neq 0 \text{ with } \lambda \in F \]

\( q \equiv 3 \) mod 4: Other way round \( \square \)

If \( d > 2 \), isotropic vector exist, so the forms are:

1. \( Q_{2m}^+ \leftrightarrow f^+ : e_1, f_1, \ldots, e_m, f_m \)

2. \( Q_{2m}^- \leftrightarrow f^- : e_1, f_2, \ldots, e_{m-1}, f_{m-1}, d, d' \) with \( \langle d, d' \rangle = O_2^-, d, d' \perp e_i, f_j \ \forall i, j \), \( f(d, d) = 1 \) (in fact have \( f(d, d') = 1 \), see later)

Related groups:

\[ GO_2^+ (q) = D_{2(q-1)} \quad GO_2^- (q) = D_{2(q+1)} \]

\( d = 2 \):

\[ GO_2^+ (q) = D_{2(q-1)}: \]

\( e_1, f_1 \), cyclic group order \( q - 1 \): \( e_1 \mapsto \lambda e_1, f_1 \mapsto \lambda^{-1} f_1 \)

\( t \) inverting: \( e_1 \leftrightarrow f_1 \)

No more elements: \( \langle e_1 \rangle, \langle f_1 \rangle \) are the only isotropic points

\[ GO_2^- (q) = D_{2(q+1)}: \]

Let \( V = \mathbb{F}_q^2 - \dim 2 \) over \( \mathbb{F}_q \)

\( Q(v) = N(v) = v^{q+1} \) This is a quadratic form, no isotropic vectors

Cyclic group order \( q + 1 \): \( N(\lambda) = 1 \implies v \mapsto \lambda v \) is an isometry

inverted by \( t : v \leftrightarrow v^q \)

No others- e.g. the stabiliser of 1 consits of \( i \) and \( v \leftrightarrow v^q \) (check)

**Lemma 10.3**

\[ |GO_{2m-1}(q)| = 2q^{m^2} (q^{2m} - 1)(q^{2m-2} - 1) \cdots (q^2 - 1) \]

\[ |GO_{2m}^\epsilon (q)| = 2q^{m(m-1)}(q^2 - 1)(q^4 - 1) \cdots (q^{2m-2} - 1)(q^m - \epsilon 1) \]

**Proof**

By induction, going up in steps of 2.

Let \( z_m = \#(\text{non-zero}) \text{ isotropic vectors in dimension } 2m + 1 \text{ or } 2m \)

**Claim:** \( z_m = q^{2m} - 1 \) for \( Q_{2m+1} \) and \( z_m = (q^m - \epsilon)(q^{m-1} + \epsilon) \) for \( Q_{2m}^\epsilon \)

**Proof of Claim:**

Correct for dimension 1, 2 (both \( \epsilon \))

Let \( \dim V = n + 2, V = U \oplus W \) (i.e. \( U \perp W \)) with \( U \) dimension 2 with some type, \( W \) dimension \( n \) of same type.
Isotropic \( v \in V \) is \( u + w \) - both norm 0 but not both zero vector, OR, norms are \( \lambda(\neq 0), -\lambda \) 
\[ z_{m+1} = (2q - 1)(1 + z_m) + (q - 1)(q^n - 1 - z_m) - 1 = qz_m + (q - 1)(q^n + 1) \] - now obtained formula in each case  

Having chosen \( e_1 \), need \( f_1 \) with \( e_1, f_1 \) hyperbolic:

**Claim:** This can be done in \( q^{n-1} \) ways (hence formulae follow)

**Proof of Claim:**
Number of isotropic vectors in \( e_1^\perp \):
\[ e_1^\perp /\langle e_1 \rangle \] is a space of same type - so \( z_{m-1} \) isotropic vectors \( \langle e_1 \rangle + v \) 
\[ qz_m - (q - 1) \] isotropic vectors in \( e_1^\perp \)
\[ \frac{1}{q-1}(z_m - qz_{m-1} - q + 1) \] choices of \( f_1 \)

\[ \square \]

### 10.2 Even characteristic

Work with quadratic form \( Q \) over \( F = \mathbb{F}_q \), char 2
Let \( f \) be the associated bilinear alternating form - \( f(v, v) = 0 \)
\[ \text{rad } f = \{ w | f(v, w) = 0 \quad \forall v \} \]
\[ \text{rad } Q = \{ w \in \text{rad}(f)|Q(w) = 0 \} \]
\[ \text{rad } Q \leq \text{rad } f \leq V \] (subspaces), codimension of \( \text{rad } f \) over \( \text{rad } Q \) is 0 or 1:
\[ Q_{\text{rad } f} : \text{rad } f \rightarrow F \] semilinear \( Q(v + w) = Q(v) + Q(w), Q(\lambda v) = \lambda^2 Q(v) \)
Norm of \( v = Q(v) \), \( v \) is isotropic if \( Q(v) = 0 \)
\( Q \) non-singular: \( \text{rad } Q = 0 \)
\( Q \) non-degenerate: \( \text{rad } f = 0 \)

Let \( Q \) non-singular \( \Rightarrow \) \( \text{rad } f \) has dimension \( \leq 1 \)
Look at \( \dim V = 2m + 1 \) odd \( \Rightarrow \) \( \text{rad } f \dim 1 \) because \( V/\text{rad}(V) \) has dimension \( 2m \) even, with a non-singular alternating form
\[ GO_{2m+1}(q) \leq SP_{2m}(q) \]
**Note:** in fact, \( |PO_{2m+1}(q)| = |PSp_{2m}(q)| \) for \( q \) odd, NOT isomorphic if \( 2m > 4 \)

Now look at \( \dim V = 2m \) even
Now handle things as before, choose a symplectic type basis as much as poss with \( Q(v) = 0 \)
**Note:** \( Q(e) = 0, f(e, f) = 1 \) \( \Rightarrow \) can adjust \( f \) to have \( Q(f) = 0 \) (is \( Q(f + \lambda e) = Q(f) + \lambda \), so replace \( f \) by \( f + Q(f)e \))

If \( \dim V > 2, 3 \) isotropic vectors: there are vectors \( u \perp v \)
if \( Q(v) \neq 0 \), then \( Q(v + \lambda u) = Q(v) + \lambda^2 Q(u) \)
\[ \Rightarrow \] Take \( \lambda^2 = Q(v)/Q(u) \), then \( v + \lambda u \) isotropic

So consider \( \dim V = 2: v, w \) basis
Let \( Q(v) = 1 = f(v, w), Q(w + \lambda v) = Q(w) + \lambda^2 + \lambda \)
\[ \Rightarrow \] at most 2 forms, and in fact, exactly two:
\( Q_2^+: e_1, f_1 \) hyperbolic pair (isotropic vectors exists)
\( Q_2^- : v, w \) s.t. \( Q(v) = 1, f(v, w) = 1, Q(w) = \mu \in F \) s.t. \( X^2 + X + \mu \) irreducible (no isotropic vectors)

Now get:
\( Q_{2m}^- : e_1, f_1, \ldots, e_m, f_m \) -isotropic, etc.
\( Q_{2m}^- : e_1, f_1, \ldots, e_{m-1}, f_{m-1}, v, w \) where \( v, w \) are as in \( Q_2^- \)
$GO_{2m}(q)$

$|SO_{2m}| = \frac{1}{2}|GO_{2m}|$ for $q$ odd

$SO = GO$ for $q$ even

$PSO^\times_{2m}$ NOT simple, has a subgroup index $P\Omega^\times_{2m}(q)$ which is simple if $\dim > 4$ (hard to prove the existence of this, see Wilson)

Some isomorphisms:

1. $P\Omega_5(q) \cong L_2(q)$, $q$ odd, $W = V_2, V = S^2W$ (see Wilson page 96, and example sheet)
2. $P\Omega_4(q) \cong L_2(q) \times L_2(q)$
3. $P\Omega^-_1(q) \cong L_2(q^2)$
4. $L_4(q) \cong P\Omega^+_6(q)$ on $\wedge^2 V_4$

$GO^\times_{2m} \leq Sp_{2m}(q)$

$q = 2 \implies$ two 2-transitive actions
Index

acting, 16
almost simple group, 3
Automorphism group, $\text{Aut}(G)$, 2
blocks, 17
Borel subgroup, 35
Burnside’s $p^aq^b$ Theorem, 15
Burnside’s Basis Theorem, 10
Burnside’s Theorem, 20
characteristic subgroup, 3
characteristically simple group, 3
commutator subgroup, 3
Correspondence Theorem, 2
degree, 18
subdegree, 22
diagonal action, 28
diagonal subgroup, 30
diagonal type, 30
distance, 22
distance transitive, 22

elementary abelian $p$-group, 3
factor group, 1
factorisable, 14
factorization of group, 13
faithful action, 16
Fano plane, 37
Fitting subgroup, $F(G)$, 8
fix($G_\alpha$), 18
Frattini argument, 9
Frattini subgroup, $\Phi(G)$, 9
Frobenius groups, 20
$G$-congruence
trivial, 17
$G$-congruence, 17
$G$-homomorphism, 16
$G$-isomorphism, 16
$G^p$, 9
$G^{q^2}$, 16

Hall $\pi$-subgroup, 12
Hall $p$-complement subgroup, 12
homomorphism
of groups, 1
hyperbolic pair, 39

Inner automorphism, $\text{Inn}(G)$, 2
Isomorphism Theorem, 1
isotropic, 45

Jordan set, 25
primitive, 25
Jordan-Hölder Theorem, 4

$k$-homogeneous, 31
$k$-transitive, 18
kernel of action $G_{(\Omega)}$, 16
Levi subgroup, 35
of $Sp_{2m}(q)$, 41
line, 20
minimal generating set, 10
multiplicity-free, 23

nilpotent group, 7
nilpotent radical of $G$, $F(G)$, 8
non-generator, 9
normal closure, 15
normal subgroup, 1
$O_p(G)$, 8
orbit $\alpha G$, 16
orbital, 22
diagonal, 22
paired $\Gamma^*$, 22
Orthogonal group $GO_d(q)^e$, 44
Outer automorphism group, $Out(G)$, 3

$p$-local subgroup, 36
P.Hall Theorem, 15
parabolic, 35
perfect, 3
permutation actions, 16
permutation representation, 16
$\pi'$-part of $n$, 12
$\pi$-group, 12
$\pi$-part of $n$, 12
primitive, 17
projective general linear group $PGL_d(q)$, 18
$PSU_d(q)$, 43

quotient group, 1

rank
of groups, 21
regular group, 11
$\rho(\alpha)$, 17

Second Isomorphism Theorem, 2
semi-regular, 21
semidirect product, 19
series, 4
central, 7
chief, 5
composition, 4
derived, 11
lower central, 8
normal, 4
proper, 4
upper central, 7
simple group, 1
simply primitive, 21
socle, 28
soluble group, 11
soluble radical, 11
split torus, 35
$SU_d(q)$, 43
Syl$_p(G)$, 9
Sylow basis, 14

Third Isomorphism Theorem, 2
transitive on $\Omega$, 16
transvection, 34
symplectic, 39

unipotent radical, 41
Unitary group $GU_d(q)$, 42
unitriangular matrix, 35

$W(k,l) = S_k \wr S_l$, 29
Witt index, 43
wreath product, 25
wreath product $C \wr_\Delta D$, 28