Finite simple groups

Maris Ozols
University of Waterloo

December 2, 2009
Introduction
Basics

Definition
A subgroup \( N \) of a group \( G \) is called normal (write \( N \trianglelefteq G \)) if \( gHg^{-1} = H \) for every \( g \in G \).
Basics

Definition
A subgroup \( N \) of a group \( G \) is called normal (write \( N \trianglelefteq G \)) if \( gHg^{-1} = H \) for every \( g \in G \).

Examples (boring)

- \( \{1_G\} \trianglelefteq G \)
- \( G \trianglelefteq G \)
Basics

Definition
A subgroup $N$ of a group $G$ is called normal (write $N \trianglelefteq G$) if $gHg^{-1} = H$ for every $g \in G$.

Examples (boring)

- $\{1_G\} \trianglelefteq G$
- $G \trianglelefteq G$

Definition
A nontrivial group $G$ is called simple if its only normal subgroups are $\{1_G\}$ and $G$ itself.
**Decomposition**

**Definition**
A normal series for a group $G$ is a sequence

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$  

Factor groups $G_{i+1}/G_i$ are called the factors of the series.
Decomposition

Definition
A normal series for a group $G$ is a sequence

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$ 

Factor groups $G_{i+1}/G_i$ are called the factors of the series.

Definition
A composition series of a group $G$ is a maximal normal series (meaning that we cannot adjoin extra terms to it).
Decomposition

Definition
A normal series for a group $G$ is a sequence

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$  

Factor groups $G_{i+1}/G_i$ are called the factors of the series.

Definition
A composition series of a group $G$ is a maximal normal series (meaning that we cannot adjoin extra terms to it).  

**Note:** All factors in a composition series are simple.
Decomposition

Definition
A normal series for a group $G$ is a sequence

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G.$$ 

Factor groups $G_{i+1}/G_i$ are called the factors of the series.

Definition
A composition series of a group $G$ is a maximal normal series (meaning that we cannot adjoin extra terms to it).

Note: All factors in a composition series are simple.

Theorem (Jordan-Hölder)
Every two composition series of a group are equivalent, i.e., have the same length and the same (unordered) family of simple factors.
The classification theorem
The classification theorem

Theorem (Classification of finite simple groups)
The following is a complete list of finite simple groups:

1. cyclic groups of prime order
2. alternating groups of degree at least 5
3. simple groups of Lie type
4. sporadic simple groups
The classification theorem

Theorem (Classification of finite simple groups)

The following is a complete list of finite simple groups:

1. cyclic groups of prime order
2. alternating groups of degree at least 5
3. simple groups of Lie type
4. sporadic simple groups

Some statistics

- Proof spreads across some 500 articles (mostly 1955–1983).
- More than 100 mathematicians among the authors.
- It is of the order of 10,000 pages long.
The classification theorem

Theorem (Classification of finite simple groups)

The following is a complete list of finite simple groups:

1. cyclic groups of prime order
2. alternating groups of degree at least 5
3. simple groups of Lie type
4. sporadic simple groups

Some statistics

- Proof spreads across some 500 articles (mostly 1955–1983).
- More than 100 mathematicians among the authors.
- It is of the order of 10,000 pages long.

The proof is being reworked and the 2nd generation proof is expected to span only a dozen of volumes.
The classification theorem

Theorem (Classification of finite simple groups)
The following is a complete list of finite simple groups:

1. cyclic groups of prime order
2. alternating groups of degree at least 5
3. simple groups of Lie type
4. sporadic simple groups

Headlines

Proof

Strategy

- Let $\mathcal{K}$ be the (conjectured) complete list of finite simple groups.
# Proof

## Strategy

- Let $\mathcal{K}$ be the (conjectured) complete list of finite simple groups.
- Proceed by induction on the order of the simple group to be classified and consider a **minimal counterexample**, i.e., let $G$ be a finite simple group of minimal order such that $G \notin \mathcal{K}$. 

---

<table>
<thead>
<tr>
<th>Introduction</th>
<th>The classification theorem</th>
<th>Finite simple groups</th>
<th>Classical groups</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Proof

Strategy

▶ Let $\mathcal{K}$ be the (conjectured) complete list of finite simple groups.
▶ Proceed by induction on the order of the simple group to be classified and consider a minimal counterexample, i.e., let $G$ be a finite simple group of minimal order such that $G \not\in \mathcal{K}$.
▶ Note that every proper subgroup $H$ of $G$ is a $\mathcal{K}$-group, i.e., has the property that $B \trianglelefteq A \trianglelefteq H \Rightarrow A/B \in \mathcal{K}$.
Proof

Strategy

- Let $\mathcal{K}$ be the (conjectured) complete list of finite simple groups.
- Proceed by induction on the order of the simple group to be classified and consider a minimal counterexample, i.e., let $G$ be a finite simple group of minimal order such that $G \notin \mathcal{K}$.
- Note that every proper subgroup $H$ of $G$ is a $\mathcal{K}$-group, i.e., has the property that $B \leq A \leq H \Rightarrow A/B \in \mathcal{K}$.

Starting point

- Odd Order Theorem (Feit-Thompson) Groups of odd order are solvable (i.e., all factors in composition series are cyclic).
Proof

Strategy

- Let $\mathcal{K}$ be the (conjectured) complete list of finite simple groups.
- Proceed by induction on the order of the simple group to be classified and consider a minimal counterexample, i.e., let $G$ be a finite simple group of minimal order such that $G \notin \mathcal{K}$.
- Note that every proper subgroup $H$ of $G$ is a $\mathcal{K}$-group, i.e., has the property that $B \trianglelefteq A \leq H \Rightarrow A/B \in \mathcal{K}$.

Starting point

- Odd Order Theorem (Feit-Thompson) Groups of odd order are solvable (i.e., all factors in composition series are cyclic).
- Equivalently, every finite non-abelian simple group is of even order.
<table>
<thead>
<tr>
<th>Introduction</th>
<th>The classification theorem</th>
<th>Finite simple groups</th>
<th>Classical groups</th>
<th>Conclusion</th>
</tr>
</thead>
</table>

Finite simple groups
Cyclic and alternating groups

Cyclic groups

\[ C_n = \mathbb{Z}/n\mathbb{Z} \quad |C_n| = n \]

\( C_p \) is simple whenever \( p \) is a prime (by Lagrange’s theorem). \( C_p \) are the only abelian finite simple groups.
Cyclic and alternating groups

Cyclic groups

\[ C_n = \mathbb{Z}/n\mathbb{Z} \quad \text{and} \quad |C_n| = n \]

\( C_p \) is simple whenever \( p \) is a prime (by Lagrange’s theorem). \( C_p \) are the only abelian finite simple groups.

Alternating groups

\[ A_n = \{ \sigma \in S_n \mid \text{sgn}(\sigma) = 1 \} \quad \text{and} \quad |A_n| = \frac{n!}{2} \]

For \( n \geq 5 \) \( A_n \) is simple (Galois, Jordan) and non-abelian.
Groups of Lie type

Chevalley and twisted Chevalley groups

There are 16 *infinite families* that can be grouped as follows:
Groups of Lie type

Chevalley and twisted Chevalley groups

There are 16 *infinite families* that can be grouped as follows:

- *classical* Lie groups (6):
Groups of Lie type

Chevalley and twisted Chevalley groups

There are 16 *infinite families* that can be grouped as follows:

- **classical** Lie groups (6):
  - linear groups (1)
  - symplectic groups (1)
  - unitary groups (1)
  - orthogonal groups (3)
Groups of Lie type

Chevalley and twisted Chevalley groups

There are 16 *infinite families* that can be grouped as follows:

- **classical Lie groups** (6):
  - **linear** groups (1)
  - **symplectic** groups (1)
  - **unitary** groups (1)
  - **orthogonal** groups (3)
- **exceptional and twisted groups of Lie type** (10)
Sporadic groups

Sporadic groups

There are 26 sporadic groups that can be grouped as follows:
Sporadic groups

There are 26 sporadic groups that can be grouped as follows:

- Mathieu groups (5)
Sporadic groups

There are 26 *sporadic groups* that can be grouped as follows:

- Mathieu groups (5)
- groups related to the Leech lattice (7)
Sporadic groups

There are 26 sporadic groups that can be grouped as follows:

- Mathieu groups (5)
- Groups related to the Leech lattice (7)
- Groups related to the Monster group (8)
Sporadic groups

There are 26 *sporadic groups* that can be grouped as follows:

- Mathieu groups (5)
- groups related to the Leech lattice (7)
- groups related to the Monster group (8)
- other groups (6)
Classical groups
## Notation

### Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>general</td>
</tr>
<tr>
<td>S</td>
<td>special</td>
</tr>
<tr>
<td>P</td>
<td>projective</td>
</tr>
<tr>
<td>Z</td>
<td>center</td>
</tr>
<tr>
<td>L</td>
<td>linear</td>
</tr>
<tr>
<td>Sp</td>
<td>symplectic</td>
</tr>
<tr>
<td>U</td>
<td>unitary</td>
</tr>
<tr>
<td>O</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>
Notation

Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>general</td>
</tr>
<tr>
<td>S</td>
<td>special</td>
</tr>
<tr>
<td>P</td>
<td>projective</td>
</tr>
<tr>
<td>Z</td>
<td>center</td>
</tr>
<tr>
<td>L</td>
<td>linear</td>
</tr>
<tr>
<td>Sp</td>
<td>symplectic</td>
</tr>
<tr>
<td>U</td>
<td>unitary</td>
</tr>
<tr>
<td>O</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>

Definitions and examples
Notation

Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>linear</td>
</tr>
<tr>
<td>S</td>
<td>symplectic</td>
</tr>
<tr>
<td>P</td>
<td>unitary</td>
</tr>
<tr>
<td>Z</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>

Definitions and examples

\[ \text{L}_n(q) := M_{n \times n}(\mathbb{F}_q) \]
Notation

Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>general</td>
</tr>
<tr>
<td>S</td>
<td>special</td>
</tr>
<tr>
<td>P</td>
<td>projective</td>
</tr>
<tr>
<td>Z</td>
<td>center</td>
</tr>
<tr>
<td>L</td>
<td>linear</td>
</tr>
<tr>
<td>Sp</td>
<td>symplectic</td>
</tr>
<tr>
<td>U</td>
<td>unitary</td>
</tr>
<tr>
<td>O</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>

Definitions and examples

\[ L_n(q) := M_{n \times n}(\mathbb{F}_q) \]

\[ \text{GL}_n(q) := \{ M \in L_n(q) \mid \det M \neq 0 \} \]
Notation

Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>linear</td>
</tr>
<tr>
<td>S</td>
<td>symplectic</td>
</tr>
<tr>
<td>P</td>
<td>unitary</td>
</tr>
<tr>
<td>Z</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>

Definitions and examples

\[
L_n(q) := M_{n \times n}(\mathbb{F}_q)
\]

\[
GL_n(q) := \{ M \in L_n(q) \mid \det M \neq 0 \}
\]

\[
SL_n(q) := \{ M \in GL_n(q) \mid \det M = 1 \}
\]
Notation

Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>general</td>
</tr>
<tr>
<td>S</td>
<td>special</td>
</tr>
<tr>
<td>P</td>
<td>projective</td>
</tr>
<tr>
<td>Z</td>
<td>center</td>
</tr>
<tr>
<td>L</td>
<td>linear</td>
</tr>
<tr>
<td>Sp</td>
<td>symplectic</td>
</tr>
<tr>
<td>U</td>
<td>unitary</td>
</tr>
<tr>
<td>O</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>

Definitions and examples

\[
L_n(q) := M_{n \times n}(\mathbb{F}_q)
\]
\[
GL_n(q) := \{ M \in L_n(q) \mid \det M \neq 0 \}
\]
\[
SL_n(q) := \{ M \in GL_n(q) \mid \det M = 1 \}
\]
\[
Z(GL_n(q)) := \{ \alpha I_n \mid \alpha \in \mathbb{F}_q^\times \} \cong \mathbb{F}_q^\times
\]
Notation

Dictionary

<table>
<thead>
<tr>
<th>Prefixes</th>
<th>Sets of matrices</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>general</td>
</tr>
<tr>
<td>S</td>
<td>special</td>
</tr>
<tr>
<td>P</td>
<td>projective</td>
</tr>
<tr>
<td>Z</td>
<td>center</td>
</tr>
<tr>
<td>L</td>
<td>linear</td>
</tr>
<tr>
<td>Sp</td>
<td>symplectic</td>
</tr>
<tr>
<td>U</td>
<td>unitary</td>
</tr>
<tr>
<td>O</td>
<td>orthogonal</td>
</tr>
</tbody>
</table>

Definitions and examples

\[
L_n(q) := M_{n \times n}(\mathbb{F}_q)
\]
\[
GL_n(q) := \{ M \in L_n(q) \mid \det M \neq 0 \}
\]
\[
SL_n(q) := \{ M \in GL_n(q) \mid \det M = 1 \}
\]
\[
Z(GL_n(q)) := \{ \alpha I_n \mid \alpha \in \mathbb{F}_q^\times \} \cong \mathbb{F}_q^\times
\]
\[
PGL_n(q) := GL_n(q)/Z(GL_n(q))
\]
Constructing simple matrix groups

“Recipe”

\[
Z(SL_n(q)) \lhd SL_n(q) \lhd GL_n(q) \subset L_n(q)
\]

\[
PSL_n(q) = SL_n(q)/Z(SL_n(q))
\]
Constructing simple matrix groups

“Recipe”

\[ Z(SL_n(q)) \triangleleft SL_n(q) \triangleleft GL_n(q) \subset L_n(q) \]
\[ PSL_n(q) = SL_n(q)/Z(SL_n(q)) \]

Description

- Take a set of matrices, e.g., \( L_n(q) \).
Constructing simple matrix groups

“Recipe”

\[ Z\left(\text{SL}_n(q)\right) \triangleleft \text{SL}_n(q) \triangleleft \text{GL}_n(q) \subset \text{L}_n(q) \]

\[ \text{PSL}_n(q) = \text{SL}_n(q)/Z\left(\text{SL}_n(q)\right) \]

Description

- Take a set of matrices, e.g., \( \text{L}_n(q) \).
- Note that \( \text{GL}_n(q) \subset \text{L}_n(q) \) is a group.
Constructing simple matrix groups

“Recipe”

\[ Z(SL_n(q)) \triangleleft SL_n(q) \triangleleft GL_n(q) \subset L_n(q) \]

\[ PSL_n(q) = SL_n(q)/Z(SL_n(q)) \]

Description

- Take a set of matrices, e.g., \( L_n(q) \).
- Note that \( GL_n(q) \subset L_n(q) \) is a group.
- \( GL_n(q) \) is not simple, since \( SL_n(q) \) is the kernel of \( \text{det} : GL_n(q) \to \mathbb{F}_q^\times \), so \( SL_n(q) \triangleleft GL_n(q) \).
Constructing simple matrix groups

“Recipe”

\[ Z(\text{SL}_n(q)) \lhd \text{SL}_n(q) \lhd \text{GL}_n(q) \subset \text{L}_n(q) \]

\[ \text{PSL}_n(q) = \text{SL}_n(q)/Z(\text{SL}_n(q)) \]

Description

- Take a set of matrices, e.g., \( \text{L}_n(q) \).
- Note that \( \text{GL}_n(q) \subset \text{L}_n(q) \) is a group.
- \( \text{GL}_n(q) \) is not simple, since \( \text{SL}_n(q) \) is the kernel of \( \det : \text{GL}_n(q) \to \mathbb{F}_q^\times \), so \( \text{SL}_n(q) \lhd \text{GL}_n(q) \).
- \( \text{SL}_n(q) \) is still not simple, since \( Z(\text{SL}_n(q)) \lhd \text{SL}_n(q) \).
Constructing simple matrix groups

“Recipe”

\[ Z(\text{SL}_n(q)) \triangleleft \text{SL}_n(q) \triangleleft \text{GL}_n(q) \subset L_n(q) \]
\[ \text{PSL}_n(q) = \text{SL}_n(q)/Z(\text{SL}_n(q)) \]

Description

- Take a set of matrices, e.g., \( L_n(q) \).
- Note that \( \text{GL}_n(q) \subset L_n(q) \) is a group.
- \( \text{GL}_n(q) \) is not simple, since \( \text{SL}_n(q) \) is the kernel of \( \det : \text{GL}_n(q) \to F_q^\times \), so \( \text{SL}_n(q) \triangleleft \text{GL}_n(q) \).
- \( \text{SL}_n(q) \) is still not simple, since \( Z(\text{SL}_n(q)) \triangleleft \text{SL}_n(q) \).
- Consider \( \text{PSL}_n(q) = \text{SL}_n(q)/Z(\text{SL}_n(q)) \).
Linear groups $\text{PSL}_n(q)$

**Definition**

The projective special linear group is

$$\text{PSL}_n(q) := \frac{\text{SL}_n(q)}{Z(\text{SL}_n(q))}$$
Linear groups $\text{PSL}_n(q)$

**Definition**

The *projective special linear group* is

$$\text{PSL}_n(q) := \frac{\text{SL}_n(q)}{\text{Z}(\text{SL}_n(q))}$$

**Theorem (Jordan–Dickson)**

$\text{PSL}_n(q)$ is simple, except for $n = 2$ and $q = 2$ or $3$. 
**Linear groups** $\text{PSL}_n(q)$

**Definition**
The projective special linear group is

$$\text{PSL}_n(q) := \text{SL}_n(q)/\text{Z}(\text{SL}_n(q))$$

**Theorem (Jordan–Dickson)**
$\text{PSL}_n(q)$ is simple, except for $n = 2$ and $q = 2$ or $3$.

**Question**
What is the order of $\text{PSL}_n(q)$?
**Order of $\text{GL}_n(q)$**

**Claim 1**

$$|\text{GL}_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2} \prod_{i=1}^{n}(q^i - 1)$$

**Proof.**

Let $v_1, \ldots, v_n \in \mathbb{F}_q^n$ be the columns of a matrix from $\text{GL}_n(q)$:
Order of $\text{GL}_n(q)$

Claim 1

$$|\text{GL}_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

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

Proof.
Let $v_1, \ldots, v_n \in \mathbb{F}_q^n$ be the columns of a matrix from $\text{GL}_n(q)$:

1. There are $q^n - 1$ non-zero vectors to choose $v_1$ from.
Order of $\text{GL}_n(q)$

Claim 1

$$|\text{GL}_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

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

Proof.

Let $v_1, \ldots, v_n \in \mathbb{F}_q^n$ be the columns of a matrix from $\text{GL}_n(q)$:

1. There are $q^n - 1$ non-zero vectors to choose $v_1$ from.
2. $|\{\alpha_1 v_1 \mid \alpha_1 \in \mathbb{F}_q\}| = q$, so there are $q^n - q$ choices for $v_2$. 
Order of $\text{GL}_n(q)$

Claim 1

$$|\text{GL}_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

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

Proof.
Let $v_1, \ldots, v_n \in \mathbb{F}_q^n$ be the columns of a matrix from $\text{GL}_n(q)$:

1. There are $q^n - 1$ non-zero vectors to choose $v_1$ from.
2. $|\{\alpha_1 v_1 \mid \alpha_1 \in \mathbb{F}_q\}| = q$, so there are $q^n - q$ choices for $v_2$.
3. $|\{\alpha_1 v_1 + \alpha_2 v_2 \mid \alpha_1, \alpha_2 \in \mathbb{F}_q\}| = q^2$, so there are $q^n - q^2$ choices for $v_2$. 
Order of $\text{GL}_n(q)$

Claim 1

$$|\text{GL}_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$$

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

Proof.

Let $v_1,\ldots,v_n \in \mathbb{F}_q^n$ be the columns of a matrix from $\text{GL}_n(q)$:

1. There are $q^n - 1$ non-zero vectors to choose $v_1$ from.
2. $|\{\alpha_1 v_1 \mid \alpha_1 \in \mathbb{F}_q\}| = q$, so there are $q^n - q$ choices for $v_2$.
3. $|\{\alpha_1 v_1 + \alpha_2 v_2 \mid \alpha_1, \alpha_2 \in \mathbb{F}_q\}| = q^2$, so there are $q^n - q^2$ choices for $v_2$.
4. etc.
Order of $\text{PSL}_n(q)$

Claim 2

$$|\text{SL}_n(q)| = |\text{GL}_n(q)| / |\mathbb{F}_q^\times| \quad \text{where} \quad |\mathbb{F}_q^\times| = q - 1$$
Order of $\text{PSL}_n(q)$

Claim 2

$$|\text{SL}_n(q)| = |\text{GL}_n(q)| / |\mathbb{F}_q^\times|$$

where $|\mathbb{F}_q^\times| = q - 1$

Claim 3

$$|\text{PSL}_n(q)| = |\text{SL}_n(q)| / d$$

where $d = \gcd(q - 1, n)$
Order of $\text{PSL}_n(q)$

Claim 2

$$|\text{SL}_n(q)| = |\text{GL}_n(q)| / |\mathbb{F}_q^\times| \quad \text{where} \quad |\mathbb{F}_q^\times| = q - 1$$

Claim 3

$$|\text{PSL}_n(q)| = |\text{SL}_n(q)| / d \quad \text{where} \quad d = \gcd(q - 1, n)$$

Conclusion

$$|\text{PSL}_n(q)| = \frac{q^{n(n-1)/2}}{\gcd(q - 1, n)} \prod_{i=2}^{n}(q^i - 1)$$
Symplectic groups $\text{PSp}_{2m}(q)$

**Definition**

Let $J := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$. The set of **symplectic matrices** is

$$\text{Sp}_{2m}(q) := \left\{ S \in \text{L}_{2m}(q) \mid SJS^T = J \right\}$$
**Symplectic groups $\text{PSp}_{2m}(q)$**

**Definition**

Let $J := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$. The set of symplectic matrices is

$$\text{Sp}_{2m}(q) := \left\{ S \in \text{L}_{2m}(q) \mid SJS^T = J \right\}$$

It turns out that $\text{Sp}_{2m}(q) \subset \text{SL}_{2m}(q)$. 


Symplectic groups $\text{PSp}_{2m}(q)$

**Definition**

Let $J := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$. The set of symplectic matrices is

$$\text{Sp}_{2m}(q) := \left\{ S \in \text{L}_{2m}(q) \mid SJS^T = J \right\}$$

It turns out that $\text{Sp}_{2m}(q) \subset \text{SL}_{2m}(q)$.

**Definition**

The **projective symplectic group** is

$$\text{PSp}_{2m}(q) := \text{Sp}_{2m}(q)/\text{Z}(\text{Sp}_{2m}(q))$$
Symplectic groups $\text{PSp}_{2m}(q)$

Definition
Let $J := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$. The set of symplectic matrices is

$$\text{Sp}_{2m}(q) := \left\{ S \in \text{L}_{2m}(q) \mid SJS^T = J \right\}$$

It turns out that $\text{Sp}_{2m}(q) \subset \text{SL}_{2m}(q)$.

Definition
The projective symplectic group is

$$\text{PSp}_{2m}(q) := \text{Sp}_{2m}(q)/\text{Z}(\text{Sp}_{2m}(q))$$

Order

$$|\text{PSp}_{2m}(q)| = \frac{q^{m^2}}{\gcd(q - 1, 2)} \prod_{i=1}^{m} (q^{2i} - 1)$$
Unitary groups $\text{PSU}_n(q^2)$

Definition

For $x \in \mathbb{F}_{q^2}$ define $\overline{x} := x^q$. Note that $\overline{\overline{x}} = x^{q^2} = x$. The set of unitary matrices is

$$U_n(q^2) := \left\{ U \in L_n(q^2) \mid U^T U = I_n \right\}$$
Unitary groups $\text{PSU}_n(q^2)$

**Definition**

For $x \in \mathbb{F}_{q^2}$ define $\bar{x} := x^q$. Note that $\bar{x} = x^{q^2} = x$. The set of unitary matrices is

$$U_n(q^2) := \left\{ U \in L_n(q^2) \mid \bar{U}^T U = I_n \right\}$$

**Definition**

The *projective special unitary group* is

$$\text{PSU}_n(q^2) := \text{SU}_n(q^2) / \text{Z}(\text{SU}_n(q^2))$$
**Unitary groups** $\text{PSU}_n(q^2)$

**Definition**
For $x \in \mathbb{F}_{q^2}$ define $\bar{x} := x^q$. Note that $\bar{x} = x^{q^2} = x$. The set of unitary matrices is

$$U_n(q^2) := \left\{ U \in L_n(q^2) \mid \bar{U}^T U = I_n \right\}$$

**Definition**
The projective special unitary group is

$$\text{PSU}_n(q^2) := SU_n(q^2)/Z(SU_n(q^2))$$

**Order**

$$|\text{PSU}_n(q^2)| = \frac{q^{n(n-1)/2}}{\gcd(q + 1, n)} \prod_{i=2}^{n} (q^i - (-1)^i)$$
Orthogonal groups

Sorry

Didn’t have time to finish this...
Conclusion
Conclusion

- Every finite group has a “unique” decomposition into finite simple groups (Jordan-Hölder Theorem).
Conclusion

- Every finite group has a “unique” decomposition into finite simple groups (Jordan-Hölder Theorem).
- The finite simple groups are (Classification Theorem):
  - cyclic groups of prime order
  - alternating groups of degree at least 5
  - simple groups of Lie type
  - sporadic simple groups
Conclusion

- Every finite group has a “unique” decomposition into finite simple groups (Jordan-Hölder Theorem).
- The finite simple groups are (Classification Theorem):
  - cyclic groups of prime order
  - alternating groups of degree at least 5
  - simple groups of Lie type
  - sporadic simple groups
- The classical groups are
  - linear groups $\text{PSL}_n(q)$
  - symplectic groups $\text{PSp}_{2m}(q)$
  - unitary groups $\text{PSU}_n(q^2)$
  - orthogonal groups
Conclusion

- Every finite group has a “unique” decomposition into **finite simple groups** (*Jordan-Hölder Theorem*).
- The finite simple groups are (**Classification Theorem**):
  - cyclic groups of prime order
  - alternating groups of degree at least 5
  - simple groups of Lie type
  - sporadic simple groups
- The classical groups are
  - linear groups $\text{PSL}_n(q)$
  - symplectic groups $\text{PSp}_{2m}(q)$
  - unitary groups $\text{PSU}_n(q^2)$
  - orthogonal groups

Thank you for your attention!