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

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

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

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

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

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

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

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

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

- Cartwright, M. "**Ten Thousand Pages to Prove Simplicity**." *New Scientist* 109, 26-30, 1985.
- Cipra, B. "**Are Group Theorists Simpleminded?**" *What's Happening in the Mathematical Sciences, 1995-1996, Vol. 3*. Providence, RI: Amer. Math. Soc., pp. 82-99, 1996.

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 $G \notin \mathcal{K}$.

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 $B \trianglelefteq A \leq H \Rightarrow A/B \in \mathcal{K}$.

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).

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.

Finite simple groups

Cyclic and alternating groups

Cyclic groups

$$C_n = \mathbb{Z}/n\mathbb{Z} \qquad |C_n| = n$$

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

$$C_n = \mathbb{Z}/n\mathbb{Z} \qquad |C_n| = n$$

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

Alternating groups

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\} \qquad |A_n| = \frac{n!}{2}$$

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

Sporadic groups

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

- Mathieu groups (5)

Sporadic groups

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

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

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

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Notation

Dictionary

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Definitions and examples

Notation

Dictionary

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Definitions and examples

$$\mathrm{L}_n(q) := \mathrm{M}_{n\times n}(\mathbb{F}_q)$$

Notation

Dictionary

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Definitions and examples

$$\mathrm{L}_n(q) := \mathrm{M}_{n\times n}(\mathbb{F}_q)$$

$$\mathrm{GL}_n(q) := \{M \in \mathrm{L}_n(q) \mid \det M \neq 0\}$$

Notation

Dictionary

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Definitions and examples

$$\mathrm{L}_n(q) := \mathrm{M}_{n\times n}(\mathbb{F}_q)$$
$$\mathrm{GL}_n(q) := \{M \in \mathrm{L}_n(q) \mid \det M \neq 0\}$$
$$\mathrm{SL}_n(q) := \{M \in \mathrm{GL}_n(q) \mid \det M = 1\}$$

Notation

Dictionary

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Definitions and examples

$$\mathrm{L}_n(q) := \mathrm{M}_{n\times n}(\mathbb{F}_q)$$
$$\mathrm{GL}_n(q) := \{M \in \mathrm{L}_n(q) \mid \det M \neq 0\}$$
$$\mathrm{SL}_n(q) := \{M \in \mathrm{GL}_n(q) \mid \det M = 1\}$$
$$\mathrm{Z}\big(\mathrm{GL}_n(q)\big) := \big\{\alpha I_n \mid \alpha \in \mathbb{F}_q^\times\big\} \cong \mathbb{F}_q^\times$$

Notation

Dictionary

Prefixes	
G	general
S	special
P	projective
Z	center

Sets of matrices	
L	linear
Sp	symplectic
U	unitary
O	orthogonal

Definitions and examples

$$\begin{aligned} \mathrm{L}_n(q) &:= \mathrm{M}_{n\times n}(\mathbb{F}_q) \\ \mathrm{GL}_n(q) &:= \{M \in \mathrm{L}_n(q) \mid \det M \neq 0\} \\ \mathrm{SL}_n(q) &:= \{M \in \mathrm{GL}_n(q) \mid \det M = 1\} \\ \mathrm{Z}\big(\mathrm{GL}_n(q)\big) &:= \left\{\alpha I_n \mid \alpha \in \mathbb{F}_q^\times\right\} \cong \mathbb{F}_q^\times \\ \mathrm{PGL}_n(q) &:= \mathrm{GL}_n(q)/\mathrm{Z}\big(\mathrm{GL}_n(q)\big) \end{aligned}$$

Constructing simple matrix groups

"Recipe"

$$\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$$
$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$$

Constructing simple matrix groups

"Recipe"

$$\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$$

$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$$

Description

- Take a set of matrices, e.g., $\mathrm{L}_n(q)$.

Constructing simple matrix groups

“Recipe”

$$\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$$
$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$$

Description

- Take a set of matrices, e.g., $\mathrm{L}_n(q)$.
- Note that $\mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$ is a group.

Constructing simple matrix groups

"Recipe"

$$\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$$

$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$$

Description

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

Constructing simple matrix groups

"Recipe"

$$\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$$

$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$$

Description

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

Constructing simple matrix groups

“Recipe”

$$\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$$
$$\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$$

Description

- Take a set of matrices, e.g., $\mathrm{L}_n(q)$.
- Note that $\mathrm{GL}_n(q) \subset \mathrm{L}_n(q)$ is a group.
- $\mathrm{GL}_n(q)$ is not simple, since $\mathrm{SL}_n(q)$ is the kernel of $\det : \mathrm{GL}_n(q) \to \mathbb{F}_q^\times$, so $\mathrm{SL}_n(q) \lhd \mathrm{GL}_n(q)$.
- $\mathrm{SL}_n(q)$ is still not simple, since $\mathrm{Z}\big(\mathrm{SL}_n(q)\big) \lhd \mathrm{SL}_n(q)$.
- Consider $\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/\mathrm{Z}\big(\mathrm{SL}_n(q)\big)$.

Linear groups $\mathrm{PSL}_n(q)$

Definition

The projective special linear group is

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

Linear groups $\mathrm{PSL}_n(q)$

Definition

The projective special linear group is

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

Theorem (Jordan–Dickson)

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

Linear groups $\mathrm{PSL}_n(q)$

Definition

The projective special linear group is

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

Theorem (Jordan–Dickson)

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

Question

What is the order of $\mathrm{PSL}_n(q)$?

Order of $\mathrm{GL}_n(q)$

Claim 1

$$
\begin{aligned}
|\mathrm{GL}_n(q)| &= (q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1}) \\
&= q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-1)
\end{aligned}
$$

Proof.

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

Order of $\mathrm{GL}_n(q)$

Claim 1

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

Proof.

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

1. There are $q^n - 1$ non-zero vectors to choose v_1 from.

Order of $\mathrm{GL}_n(q)$

Claim 1

$$
\begin{aligned}
|\mathrm{GL}_n(q)| &= (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}) \\
&= q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)
\end{aligned}
$$

Proof.

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

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 $\mathrm{GL}_n(q)$

Claim 1

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

Proof.

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

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 $\mathrm{GL}_n(q)$

Claim 1

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

Proof.

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

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 $\mathrm{PSL}_n(q)$

Claim 2

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

Order of $\mathrm{PSL}_n(q)$

Claim 2

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

Claim 3

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

Order of $\mathrm{PSL}_n(q)$

Claim 2

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

Claim 3

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

Conclusion

$$|\mathrm{PSL}_n(q)| = \frac{q^{n(n-1)/2}}{\gcd(q-1,n)} \prod_{i=2}^{n} (q^i - 1)$$

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

Definition

Let $J := \left(\begin{smallmatrix} 0 & I_m \\ -I_m & 0 \end{smallmatrix}\right)$. The set of symplectic matrices is

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

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

Definition

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

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

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

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

Definition

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

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

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

Definition

The projective symplectic group is

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

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

Definition

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

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

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

Definition

The projective symplectic group is

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

Order

$$|\mathrm{PSp}_{2m}(q)| = \frac{q^{m^2}}{\gcd(q-1,2)} \prod_{i=1}^{m} (q^{2i} - 1)$$

Unitary groups $\mathrm{PSU}_n(q^2)$

Definition

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

$$\mathrm{U}_n(q^2) := \left\{ U \in \mathrm{L}_n(q^2) \mid \bar{U}^{\mathsf{T}} U = I_n \right\}$$

Unitary groups $\mathrm{PSU}_n(q^2)$

Definition

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

$$\mathrm{U}_n(q^2) := \left\{ U \in \mathrm{L}_n(q^2) \mid \bar{U}^\mathsf{T} U = I_n \right\}$$

Definition

The projective special unitary group is

$$\mathrm{PSU}_n(q^2) := \mathrm{SU}_n(q^2)/\mathrm{Z}(\mathrm{SU}_n(q^2))$$

Unitary groups $\mathrm{PSU}_n(q^2)$

Definition

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

$$\mathrm{U}_n(q^2) := \left\{ U \in \mathrm{L}_n(q^2) \mid \bar{U}^\mathsf{T} U = I_n \right\}$$

Definition

The projective special unitary group is

$$\mathrm{PSU}_n(q^2) := \mathrm{SU}_n(q^2) / \mathrm{Z}(\mathrm{SU}_n(q^2))$$

Order

$$\left|\mathrm{PSU}_n(q^2)\right| = \frac{q^{n(n-1)/2}}{\gcd(q+1, n)} \prod_{i=2}^{n} (q^i - (-1)^i)$$

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 $\mathrm{PSL}_n(q)$
  - symplectic groups $\mathrm{PSp}_{2m}(q)$
  - unitary groups $\mathrm{PSU}_n\left(q^2\right)$
  - 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 $\mathrm{PSL}_n(q)$
  - symplectic groups $\mathrm{PSp}_{2m}(q)$
  - unitary groups $\mathrm{PSU}_n\left(q^2\right)$
  - orthogonal groups

Thank you for your attention!