Finite Simple Groups

Caitlin Ho Calum Lehrach Simon Beyzerov Taya Yakovenko

Worcester Polytechnic Institute

Table of Contents

Definition

A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G and is denoted $H \triangleleft G$.

Definition

A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G and is denoted $H \lhd G$.

Definition

A group is simple if its only normal subgroups are the trivial subgroup and the group itself.

Recall these theorems taken from Gallian [1]:

Theorem (Sylow's Third Theorem)

Let p be a prime and let G be a group of order $p^k m$, where p does not divide m. Then the number n of Sylow p-subgroups of G is equal to $1 \mod p$ and divides m.

Corollary

A Sylow p-subgroup is normal in G if and only if it is the unique Sylow p-subgroup, or equivalently, $n_p = 1$.

Theorem (Sylow Test for Nonsimplicity)

Let n be a positive integer that is not prime, and let p be a prime divisor of n. If 1 is the only divisor of n that is equal to $1 \mod p$, then there does not exist a simple group of order n.

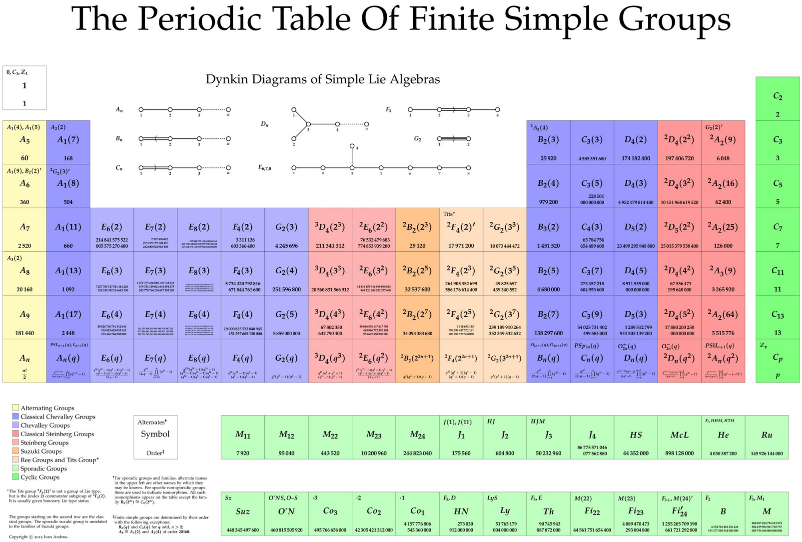
Examples

There are no simple groups of order 351.
Since $|G| = 351 = 3^3 \cdot 13$, Sylow's Third Theorem tells us that n_{13} divides $3^3 = 27$ so $n_{13} \in \{1, 3, 9, 27\}$. Additionally, we have that $n_{13} \equiv 1 \mod 13$. Thus the only possibilities are $n_{13} = 1$ or 27. A Sylow 13-subgroup P has order 13 and a Sylow 3-subgroup Q has order $3^3 = 27$. Thus $P \cap Q = \{e\}$. Suppose $n_{13} = 27$. Every Sylow 13-subgroup contains 12 nonidentity elements, so G must contain $27 \cdot 12 = 324$ elements of order 13. This leaves $351 - 324 = 27$ elements in G with order not 13. Thus, G contains only one Sylow 3-subgroup, so G cannot be simple.

Theorem (Classification of Finite Simple Groups)

Every finite simple group is (isomorphic to) one of the following:

1. Cyclic group $\mathbb{Z}_p$ of prime order p
2. Alternating group A_n for $n \geq 5$
3. One of the 16 infinite families of groups of Lie Type
4. One of the 26 sporadic groups



The Periodic Table Of Finite Simple Groups
Dynkin Diagrams of Simple Lie Algebras
0, C1, Z1 1 1
A5 60
A1(7) 168
A6 360
A1(8) 504
A7 2 520
A1(11) 660
E6(2)
E7(2)
E8(2)
F4(2) 3 311 126 603 366 400
G2(3) 4 245 696
3D4(2^3) 211 341 312
2E6(2^2) 76 532 479 683 774 853 939 200
2B2(2^3) 29 120
Tits* 2F4(2)' 17 971 200
2G2(3^3) 10 073 444 472
B3(2) 1 451 520
C4(3) 65 784 756 654 489 600
D5(2) 23 499 295 948 800
2D5(2^2) 25 015 379 558 400
2A2(25) 126 000
A8 20 160
A1(13) 1 092
E6(3)
E7(3)
E8(3)
F4(3) 5 734 420 792 816 671 844 761 600
G2(4) 251 596 800
3D4(3^3) 20 560 831 566 912
2E6(3^2)
2B2(2^5) 32 537 600
2F4(2^3) 264 905 352 699 586 176 614 400
2G2(3^5) 49 825 657 439 340 552
B2(5) 4 680 000
C3(7) 273 457 218 604 953 600
D4(5) 8 911 539 000 000 000 000
2D4(4^2) 67 536 471 195 648 000
2A3(9) 3 265 920
A9 181 440
A1(17) 2 448
E6(4)
E7(4)
E8(4)
F4(4) 19 009 825 523 840 945 451 297 669 120 000
G2(5) 5 859 000 000
3D4(4^3) 67 802 350 642 790 400
2E6(4^2)
2B2(2^7) 34 093 383 680
2F4(2^5)
2G2(3^7) 239 189 910 264 352 349 332 632
B2(7) 138 297 600
C3(9) 54 025 731 402 499 584 000
D5(3) 1 289 512 799 941 305 139 200
2D4(5^2) 17 880 203 250 000 000 000
2A2(64) 5 515 776
An n!/2
An(q)
E6(q)
E7(q)
E8(q)
F4(q)
G2(q)
3D4(q^3)
2E6(q^2)
2B2(2^{2n+1})
2F4(2^{2n+1})
2G2(3^{2n+1})
Bn(q)
Cn(q)
Dn(q)
2Dn(q^2)
2An(q^2)
2A3(4) B2(3) 25 920
C3(3) 4 585 351 680
D4(2) 174 182 400
2D4(2^2) 197 406 720
G2(2)' 2A2(9) 6 048
B2(4) 979 200
C3(5) 228 501 000 000 000
D4(3) 4 952 179 814 400
2D4(3^2) 10 151 968 619 520
2A2(16) 62 400
C2 2
C3 3
C5 5
C7 7
C11 11
C13 13
Zp Cp p
Alternating Groups
Classical Chevalley Groups
Chevalley Groups
Classical Steinberg Groups
Steinberg Groups
Suzuki Groups
Ree Groups and Tits Group*
Sporadic Groups
Cyclic Groups
Alternates† Symbol Order‡
M11 7 920
M12 95 040
M22 443 520
M23 10 200 960
M24 244 823 040
J1 175 560
J2 604 800
J3 50 232 960
J4 86 775 571 046 077 562 880
HS 44 352 000
McL 898 128 000
He 4 030 387 200
Ru 145 926 144 000
Suz 448 345 497 600
O'N 460 815 505 920
Co3 495 766 656 000
Co2 42 305 421 312 000
Co1 4 157 776 806 543 360 000
HN 273 030 912 000 000
Ly 51 765 179 004 000 000
Th 90 745 943 887 872 000
Fi22 64 561 751 654 400
Fi23 4 089 470 473 293 004 800
Fi'24 1 255 205 709 190 661 721 292 800
B
M
Copyright © 2012 Ivan Andrus.

Cyclic groups of prime order

Examples

Consider the cyclic group $G = (\mathbb{Z}_3, +)$: If H is a subgroup of G, then its order must divide $|G| = 3$. Since $p = 3$ is prime, its only divisors are 1 and 3, so either $H = G$ or H is the trivial (identity) group.

Theorem

Every abelian simple group is (isomorphic to) $\mathbb{Z}_p$.

Alternating groups

Theorem

Any An, where $n \neq 4$, is a finite simple group.

Prove that A4 is not Simple

Proof.

We consider the subgroup $H = [1, (12)(34), (13)(24), (14)(23)]$ in A4. We can verify that this is a normal subgroup by knowing that conjugation $(gHg^{-1} = H)$ does not alter cycle structure. Outside of the identity element, all of the elements are products of two disjoint transpositions and therefore must equal another product of two disjoint transpositions. Therefore H is normal and A4 cannot be simple.

We can see H is normal by observing that it is isomorphic to the Klein 4-Group, $\mathbb{Z}_2 \times \mathbb{Z}_2$ □

Proving An is simple for $n \geq 5$

- Determine that for $n \geq 5$, all elements of An are products of 3-cycles.
- All 3-cycles in An are conjugate, and therefore are normal.
- For any An, this 3-cycle is the only nontrivial normal subgroup. Thus, An is equal to the 3-cycle. An must then be a finite simple group.

Proving simplicity for $n = 1, 2, 3$ is trivial.

Example

Consider the Alternating group A6

- We set H to be the set of conjugacy classes, $H = [(1), (123), (123)(456), (12)(34), (12345), (23456), (1234)(56)]$
- (123) is the only 3-cycle element that is invariant under conjugation.
- The only normal subgroups of A6 are (1) and elements in the form (123), so A6 is a simple finite group.

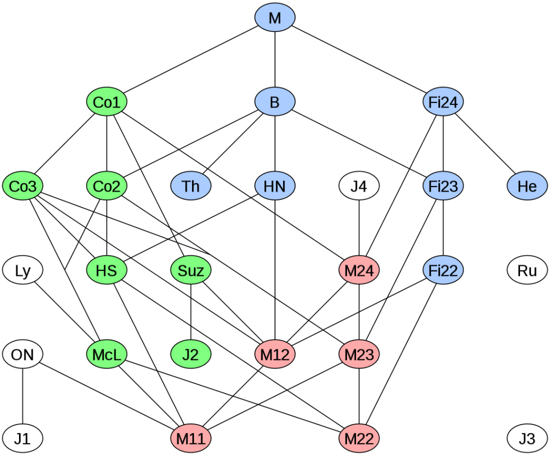
Sporadic groups

- The sporadic groups are the 26 finite simple groups that do not fit into any of the four infinite families of finite simple groups (i.e., the cyclic groups of prime order, alternating groups of degree at least five, Lie-type Chevalley groups, and Lie-type groups)
- The smallest sporadic group is the Mathieu group $M_1 1$, which has order 7920, and the largest is the monster group, which has order 808017424794512875886459904961710757005754368000000000.

Sporadic groups

Mathieu group M_{11}	7920	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
Mathieu group M_{12}	95040	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
Janko group J_1	175560	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
Mathieu group M_{22}	443520	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
Janko group $J_2 = HJ$	604800	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
Mathieu group M_{23}	10200960	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
Higman-Sims group HS	44352000	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
Janko group J_3	50232960	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
Mathieu group M_{24}	244823040	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
McLaughlin group McL	898128000	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Held group He	4030387200	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Rudvalis Group Ru	145926144000	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
Suzuki group Suz	448345497600	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
O'Nan group O'N	460815505920	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
Conway group Co_3	495766656000	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Conway group Co_2	42305421312000	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fischer group Fi_{22}	64561751654400	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
Harada-Norton group HN	273030912000000	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Lyons Group Ly	51765179004000000	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
Thompson Group Th	90745943887872000	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
Fischer group Fi_{23}	4089470473293004800	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Conway group Co_1	4157776806543360000	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Janko group J_4	86775571046077562880	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Fischer group Fi'_{24}	1255205709190661721292800	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
baby monster group B	4154781481226426191177580544000000	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
monster group M	808017424794512875886459904961710757005754368000000000	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Sporadic groups



The Monster group

- 20 out of the 26 sporadic groups can be "grouped" together into a Happy Family with the other 6 known as Pariahs based on the monster group.
- The monster group is the largest (around $10^5 4$) and describes symmetries of a 196883 dimension object
- It takes around 4GB of memory to express only one element of the Monster Group; some groups that have many more elements have much less computationally demanding elements

The Monstrous Moonshine Conjecture

- 1970s John McKay - series expansion of modular forms and elliptic functions
- 1992 Richard Borcherds - defined a connection between monster and string theory

Split in group-theoretic research in late 19th century prompted by Sophus Lie's discovery of Lie groups:

- "Discrete" groups/symmetries
- "Continuous" groups/symmetries (Lie group)

Sophus Lie

Split in group-theoretic research in late 19th century prompted by Sophus Lie's discovery of Lie groups:

- "Discrete" groups/symmetries
- "Continuous" groups/symmetries (Lie group)

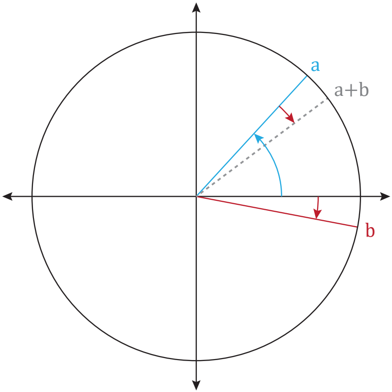
Sophus Lie

Definition

A Lie group is a group that is also a finite dimensional smooth manifold, in which the group operations of multiplication and inversion are smooth maps.

Examples

Additive group of rotations of the unit circle $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$.



Simple Lie groups

- Classified by Killing in 1890 [2]
- 4 classical Lie groups, 5 exceptional Lie groups
  - Classical: A_n, B_n, C_n, D_n
  - Exceptional: G_2, F_4, E_6, E_7, E_8

Simple Lie groups

- Classified by Killing in 1890 [2]
- 4 classical Lie groups, 5 exceptional Lie groups
  - Classical: A_n, B_n, C_n, D_n
  - Exceptional: G_2, F_4, E_6, E_7, E_8

Examples

B_n describes the odd special orthogonal group $SO(n)$, the group of $n \times n$ (for odd n) rotation matrices with determinant 1 (e.g., $SO(3)$ is the 3D rotation group).

Lie groups are typically defined over continuous fields like $\mathbb{R}$ or $\mathbb{C}$.

Can we use continuous groups to get more finite simple groups?
From simple Lie groups $\rightarrow$ finite simple groups?

Lie groups are typically defined over continuous fields like $\mathbb{R}$ or $\mathbb{C}$.

Can we use continuous groups to get more finite simple groups?
From simple Lie groups $\rightarrow$ finite simple groups?

In 1955, Chevalley's seminal work...

- showed a connection between the two group types

Claude Chevalley

Lie groups are typically defined over continuous fields like $\mathbb{R}$ or $\mathbb{C}$.

Can we use continuous groups to get more finite simple groups?
From simple Lie groups $\rightarrow$ finite simple groups?

In 1955, Chevalley's seminal work...

- showed a connection between the two group types
- discovered finite analogues of simple Lie groups
  - finite simple group of Lie type
  - defined over finite fields $\mathbb{F}$

Claude Chevalley

Definition

A field $\mathbb{F}$ is a set defined under two operators $+$ and $\cdot$ that satisfies:

- Closure under addition and multiplication
- Associativity of addition and multiplication
- Commutativity of addition and multiplication
- Additive and multiplicative identity
- Additive and multiplicative inverses (*subtraction* and *division* exist)
- Distributivity of multiplication over addition $(a \cdot (b + c) = (a \cdot b) + (a \cdot c))$

Definition

A finite field is a field of finite order (e.g., $\mathbb{Z}_p$ is a finite field).

Classifications of finite simple groups of Lie type

Generalizing Chevalley's techniques, group-theorists discovered new finite simple groups. The full classification of finite simple groups of Lie type soon followed:

1. Adjoint Chevalley groups
2. Twisted adjoint Chevalley groups
   - Steinberg groups (1959)
   - Suzuki-Ree groups (1960-61)
3. Tits group

Lie groups of Lie type

Adjoint Chevalley groups

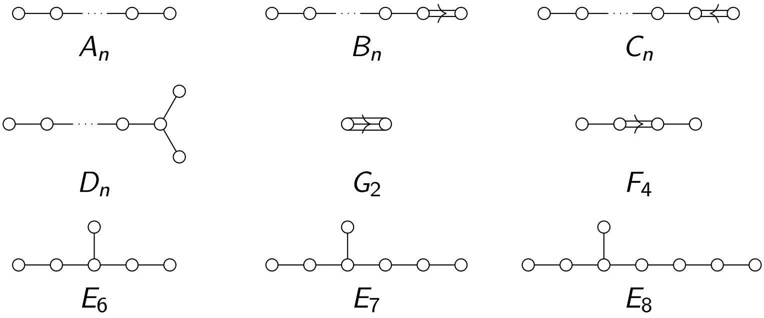
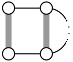


Table: Dynkin diagrams of finite simple groups of Lie type (adjoint Chevalley)

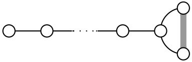
Lie groups of Lie type

Twisted adjoint Chevalley groups

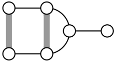
Steinberg



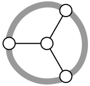
^2A_n



^2D_n



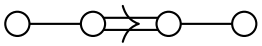
$^2E_6$



$^4D_4$

Suzuki-Ree

$^2B_2$



$^2F_4$

$^2G_2$

Tits

$^2F(2)'$

Table: Dynkin diagrams of twisted adjoint Chevalley groups

Bibliography

[1] Joseph A. Gallian. “Finite Simple Groups”. In: *Contemporary Abstract Algebra*. CRC, Taylor &; Francis Group, 2021, pp. 459–479.

[2] Wilhelm Killing. “Die Zusammensetzung der stetigen endlichen Transformationsgruppen”. In: *Mathematische Annalen* 36.2 (June 1890), pp. 161–189. DOI: 10.1007/bf01207837. URL: https://doi.org/10.1007/bf01207837.