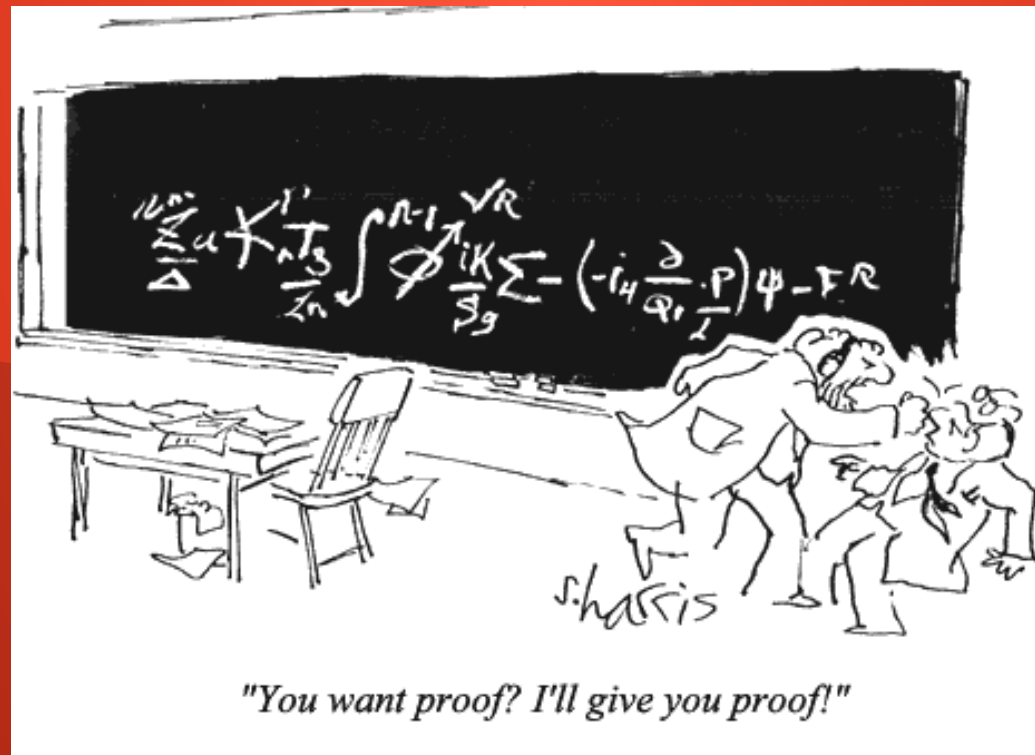


# Why We Believe Mathematical Proofs

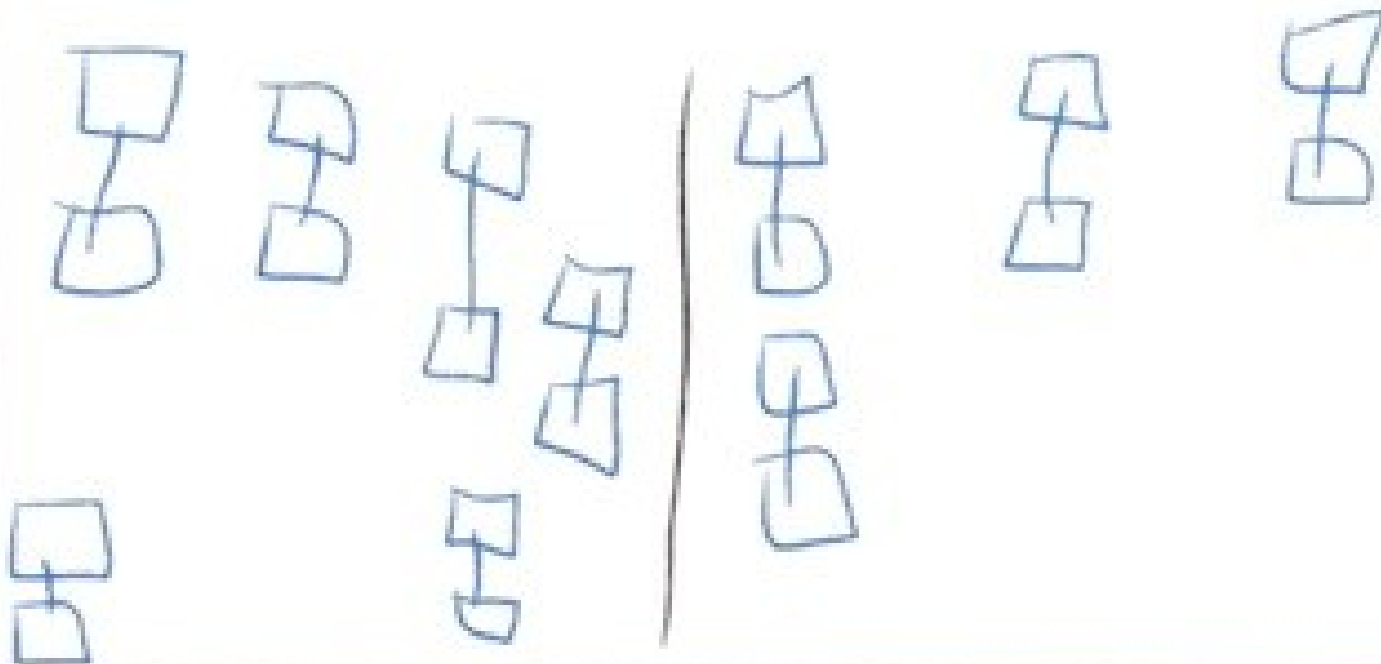
Ang Yan Sheng



Theorem: (YS Ang, 1998)  
Even + even = even.

Even + Even = Even

because they all have  
partners.



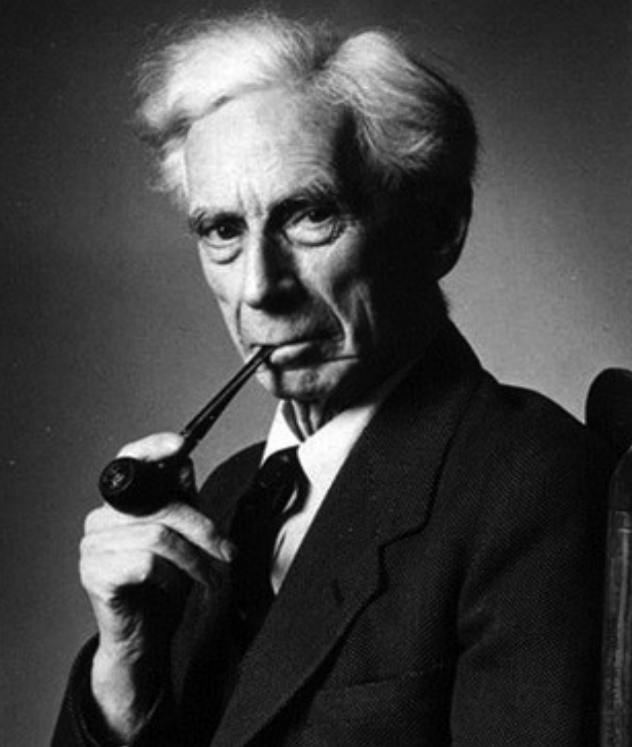
$$2a + 2b = 2(a + b)$$

Derivation (formal)

vs.

Intuition (informal)





\*54·42.  $\vdash :: \alpha \in 2 . \supset :: \beta \subset \alpha . \exists ! \beta . \beta \neq \alpha . \equiv . \beta \in t''\alpha$

*Dem.*

$\vdash . *54·4 . \supset \vdash :: \alpha = t'x \cup t'y . \supset ::$

$\beta \subset \alpha . \exists ! \beta . \equiv :: \beta = \Lambda . \vee . \beta = t'x . \vee . \beta = t'y . \vee . \beta = \alpha : \exists ! \beta :$

[\*24·53·56.\*51·161]  $\equiv :: \beta = t'x . \vee . \beta = t'y . \vee . \beta = \alpha$  (1)

$\vdash . *54·25 . \text{Transp.} *52·22 . \supset \vdash : x \neq y . \supset . t'x \cup t'y \neq t'x . t'x \cup t'y \neq t'y :$

[\*13·12]  $\supset \vdash : \alpha = t'x \cup t'y . x \neq y . \supset . \alpha \neq t'x . \alpha \neq t'y$  (2)

$\vdash . (1) . (2) . \supset \vdash :: \alpha = t'x \cup t'y . x \neq y . \supset ::$

$\beta \subset \alpha . \exists ! \beta . \beta \neq \alpha . \equiv :: \beta = t'x . \vee . \beta = t'y :$

[\*51·235]

$\equiv :: (\exists z) . z \in \alpha . \beta = t'z :$

[\*37·6]

$\equiv :: \beta \in t''\alpha$  (3)

$\vdash . (3) . *11·11·35 . *54·101 . \supset \vdash . \text{Prop}$

\*54·43.  $\vdash :: \alpha , \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

*Dem.*

$\vdash . *54·26 . \supset \vdash :: \alpha = t'x . \beta = t'y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[\*51·231]  $\equiv . t'x \cap t'y = \Lambda .$

[\*13·12]  $\equiv . \alpha \cap \beta = \Lambda$  (1)

$\vdash . (1) . *11·11·35 . \supset$

$\vdash :: (\exists x , y) . \alpha = t'x . \beta = t'y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda$  (2)

$\vdash . (2) . *11·54 . *52·1 . \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that  $1 + 1 = 2$ .

### Assertion

Ref	Expression
<b>2p2e4</b>	$\vdash (2 + 2) = 4$

### Proof of Theorem **2p2e4**

Step	Hyp	Ref	Expression
1		<a href="#">df-2</a> 8943	$\dots 3 \vdash 2 = (1 + 1)$
2	<a href="#">1</a>	<a href="#">oveq2i</a> 5389	$\dots 2 \vdash (2 + 2) = (2 + (1 + 1))$
3		<a href="#">df-4</a> 8945	$\dots 3 \vdash 4 = (3 + 1)$
4		<a href="#">df-3</a> 8944	$\dots 4 \vdash 3 = (2 + 1)$
5	<a href="#">4</a>	<a href="#">oveq1i</a> 5388	$\dots 3 \vdash (3 + 1) = ((2 + 1) + 1)$
6		<a href="#">2cn</a> 8953	$\dots 4 \vdash 2 \in \mathbb{C}$
7		<a href="#">ax-1cn</a> 8227	$\dots 4 \vdash 1 \in \mathbb{C}$
8	<a href="#">6</a> , <a href="#">7</a> , <a href="#">7</a>	<a href="#">addassi</a> 8269	$\dots 3 \vdash ((2 + 1) + 1) = (2 + (1 + 1))$
9	<a href="#">3</a> , <a href="#">5</a> , <a href="#">8</a>	<a href="#">3eqtri</a> 2106	$\dots 2 \vdash 4 = (2 + (1 + 1))$
10	<a href="#">2</a> , <a href="#">9</a>	<a href="#">eqtr4i</a> 2105	$1 \vdash (2 + 2) = 4$

Metamath  
25,933 steps

### Theorem **opreq2i** 2368

Description: Equality inference for operations.

#### Hypothesis

Ref	Expression
opreq1i.1	$\vdash A = B$

#### Assertion

Ref	Expression
<b>opreq2i</b>	$\vdash (CFA) = (CFB)$

$$A = B$$

$$2 = (1 + 1)$$

2

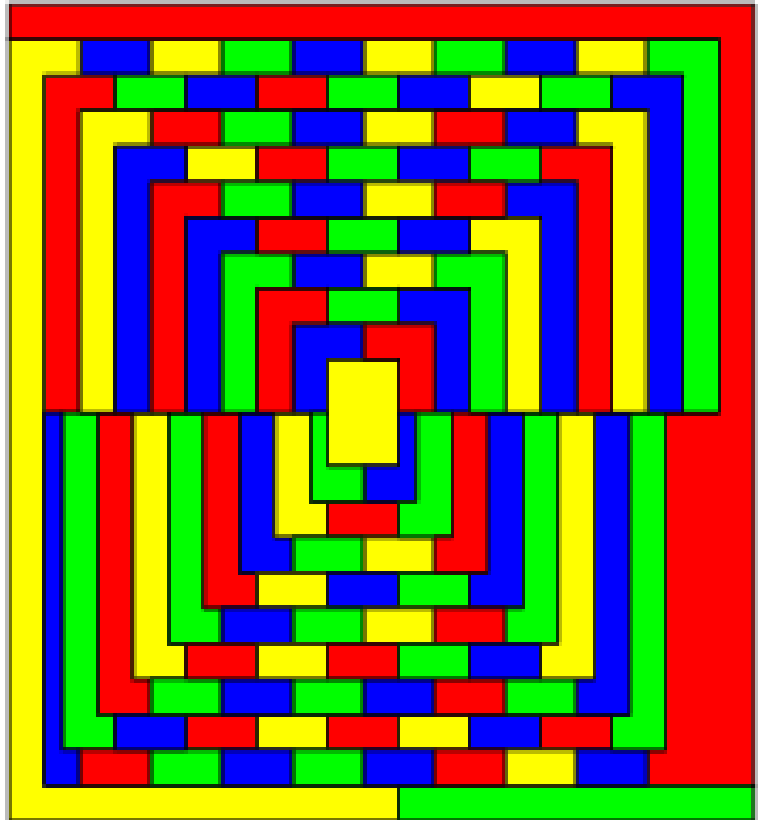
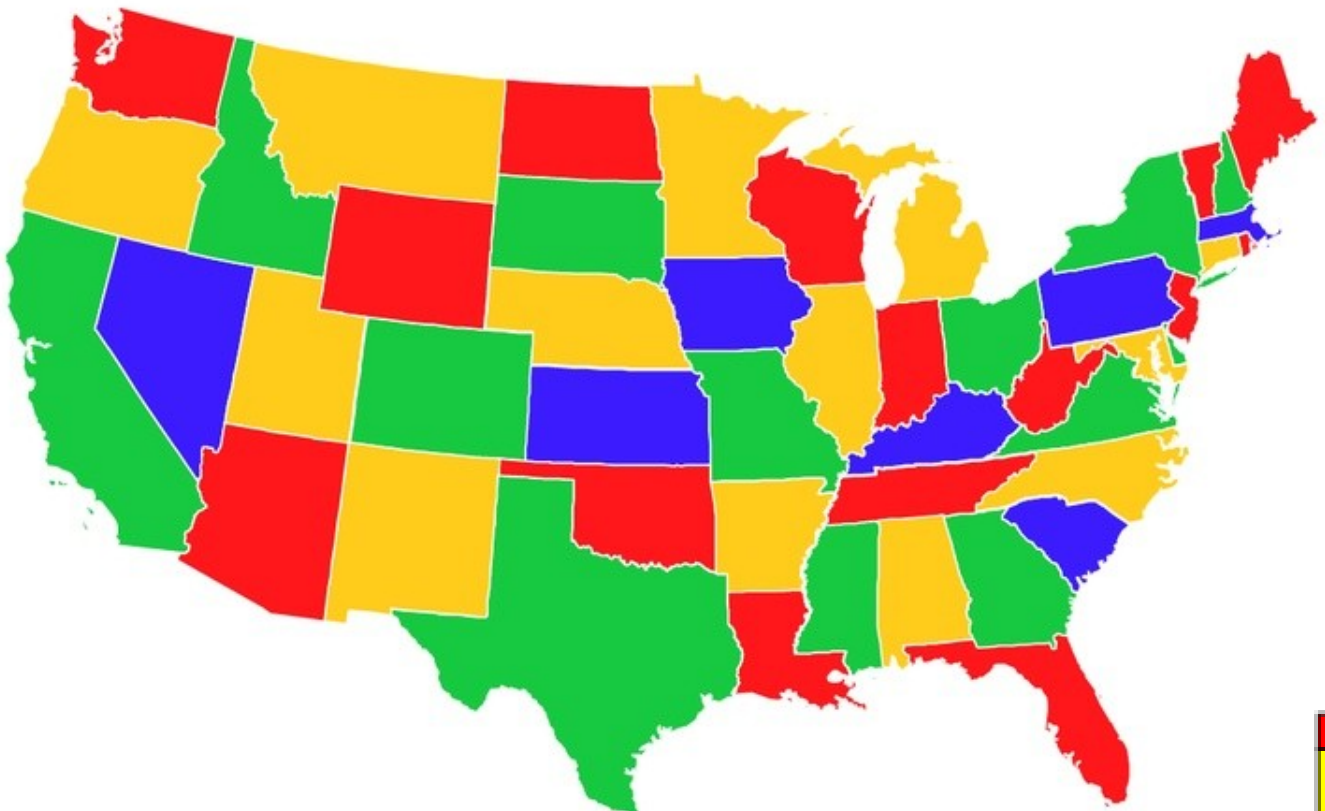
#### Proof of Theorem **2p2e4**

Step	Hyp	Ref	Expression
1		<a href="#">df-2</a> <small>3348</small>	$\vdash 2 = (1 + 1)$
2	1	<b>opreq2i</b> <small>2368</small>	$\vdash (2 + 2) = (2 + (1 + 1))$
3		<a href="#">df-4</a> <small>3350</small>	$\vdash 4 = (3 + 1)$

$$(CFA) = (CFB)$$

$$(2 + 2) = (2 + (1 + 1))$$

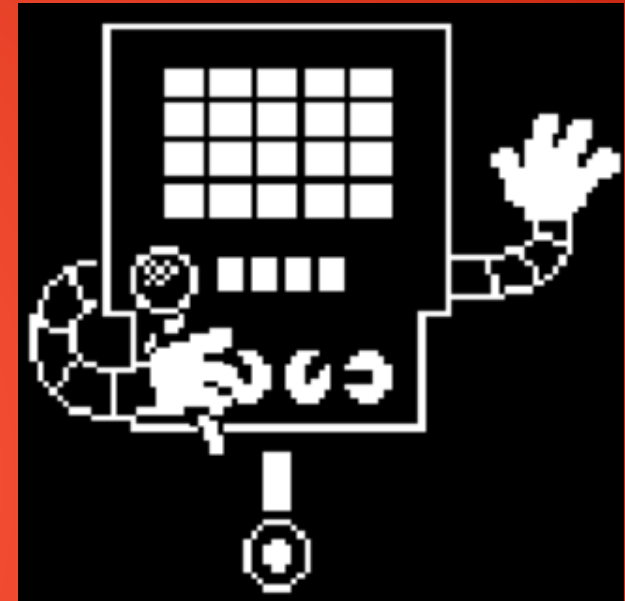
3







Appel-Haken  
(1976)



1,936 cases

1,200 hours of  
computer time



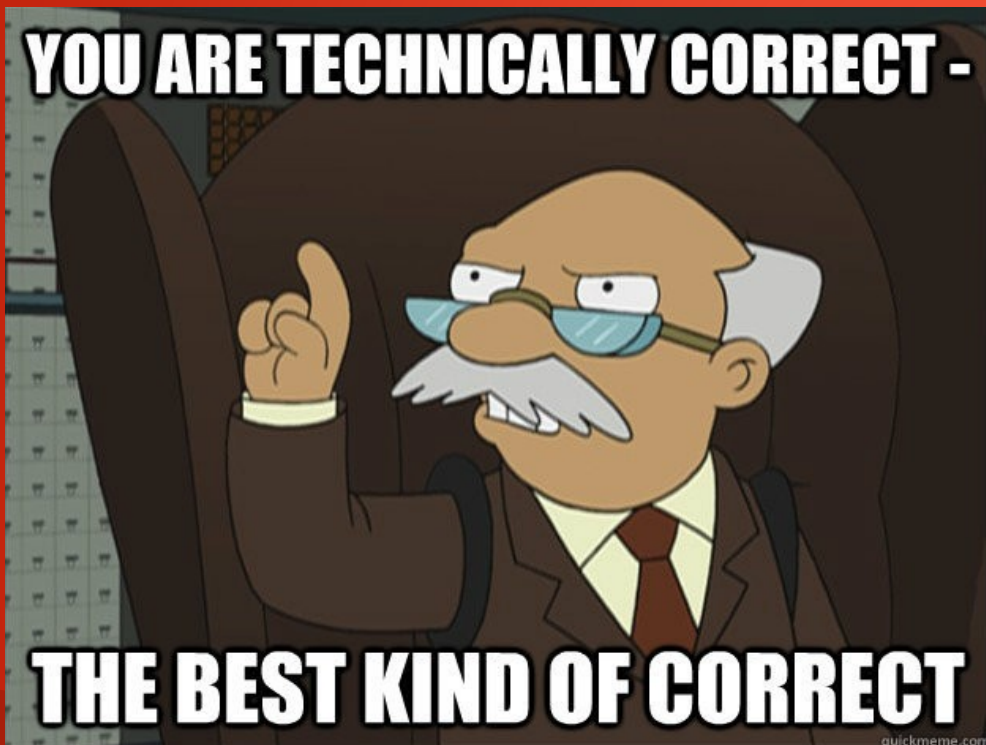
**WHAT?**



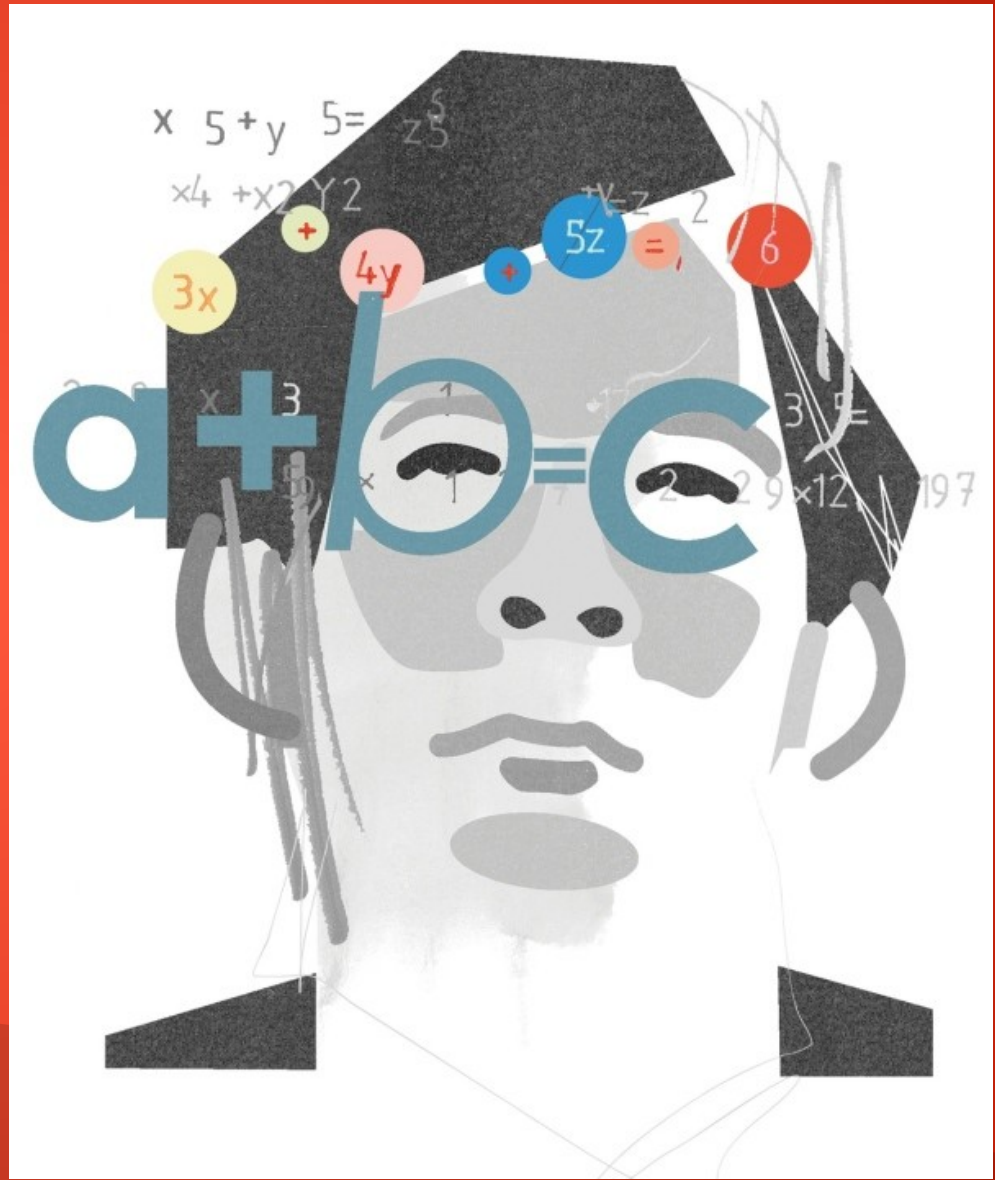
**WHY?**



**HOW?**







THE  $\mathbb{F}_l^{\times\pm}$ -SYMMETRY IS REPRESENTED IN A  $D$ - $\Theta^{\pm\text{ell}}$ -HODGE THEATER  $\dagger\mathcal{HT}^{D-\Theta^{\pm\text{ell}}}$  BY A CATEGORY EQUIVALENT TO THE GALOIS CATEGORY OF FINITE ÉTALE COVERINGS OF  $\underline{X}_K$ .

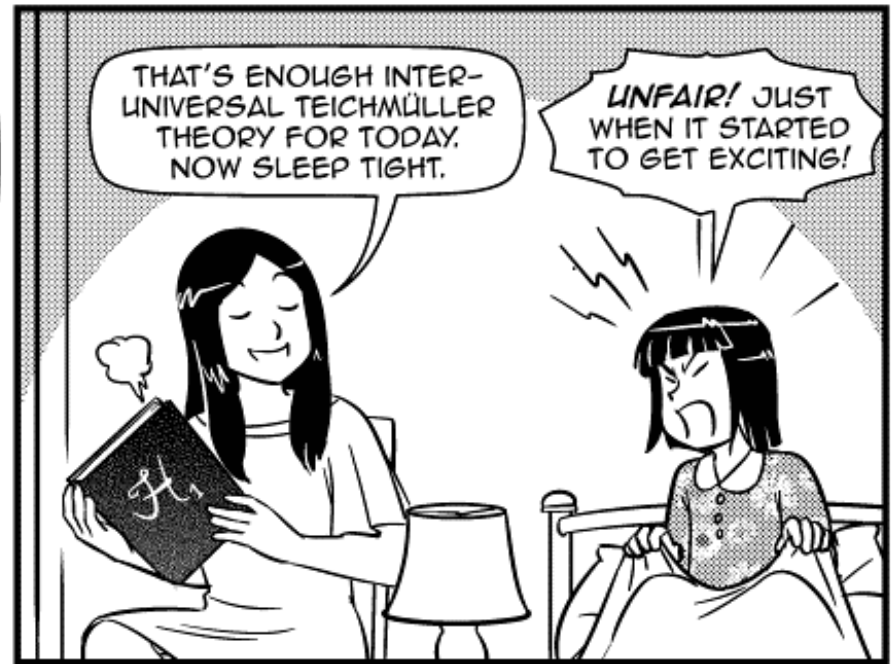


ON THE OTHER HAND, EACH OF THE LABELS REFERRED TO ABOVE IS REPRESENTED IN A  $D$ - $\Theta^{\pm\text{ell}}$ -HODGE THEATER  $\dagger\mathcal{HT}^{D-\Theta^{\pm\text{ell}}}$  BY A  $D$ -PRIME-STRIP.



THAT'S ENOUGH INTER-UNIVERSAL TEICHMÜLLER THEORY FOR TODAY. NOW SLEEP TIGHT.

UNFAIR! JUST WHEN IT STARTED TO GET EXCITING!



Étale-like

$\Theta$

Galois evaluation



### Indeterminacies

(Ind 1), (Ind 2),  
(Ind 3)

Galois evaluation

Étale-like

$\frac{t^2+1}{t^3+\dots-1}, \frac{t^7+\dots-1}{t^2+\dots+1}, \dots$

$\in F_{\text{mod}}$   
 $\in F_{\text{mod}}$

$\in F_{\text{mod}}$

$\in F_{\text{mod}}$

$q^{1^2}$   
 $q^{2^2}$

$q^{j^2}$

$q^{(l^*)^2}$



$\{\log \mathcal{O}_v^\times\}_v$

$\{\log \mathcal{O}_v^\times\}_v$

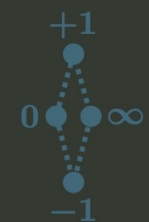
$\{\log \mathcal{O}_v^\times\}_v$

$\{\log \mathcal{O}_v^\times\}_v$

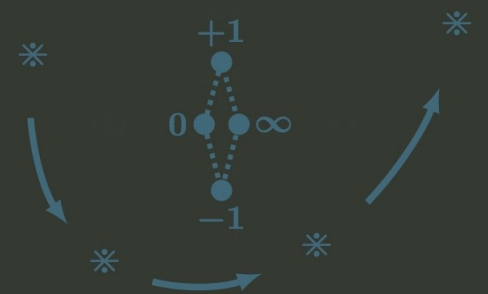
$\{\log \mathcal{O}_v^\times\}_v$

$\{\log \mathcal{O}_v^\times\}_v$

\* \*  
tripods  
( $\cong \mathbb{P}^1 \setminus \{0, 1, \infty\}$ ),  
Belyi cuspidalization



$\pm$   
 $\pm$   
theta groups,  
elliptic  
cuspidalization



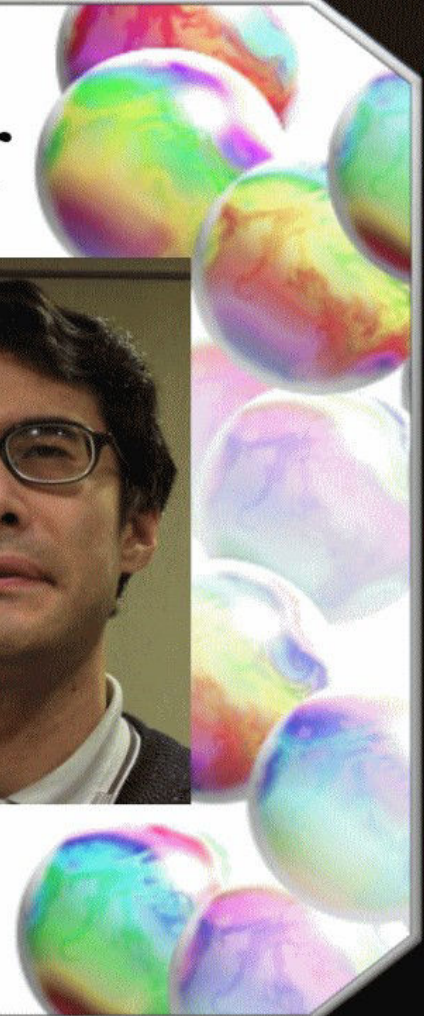
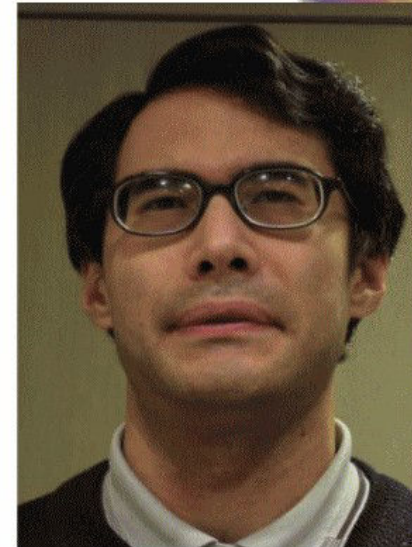


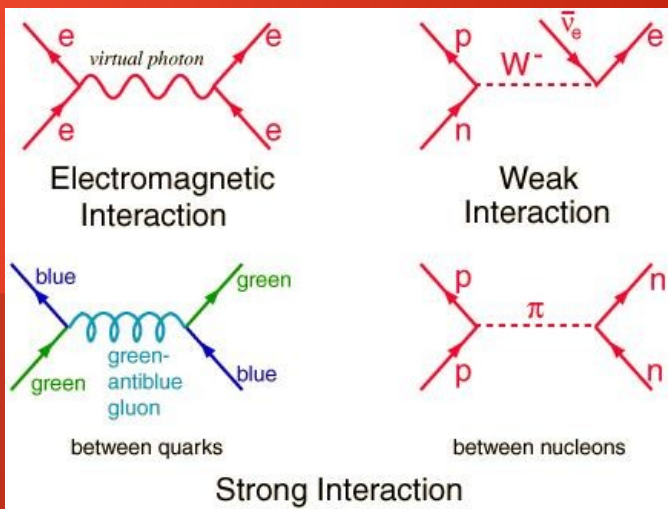
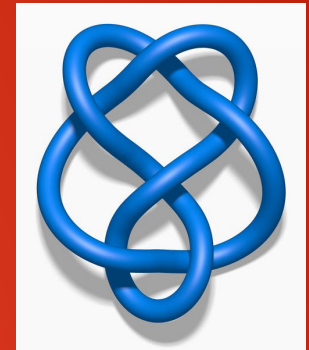
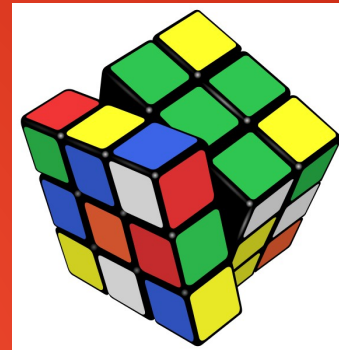
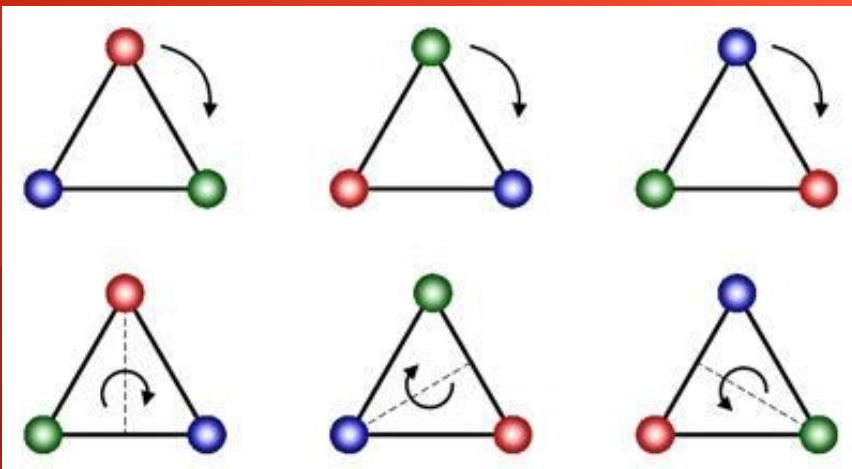
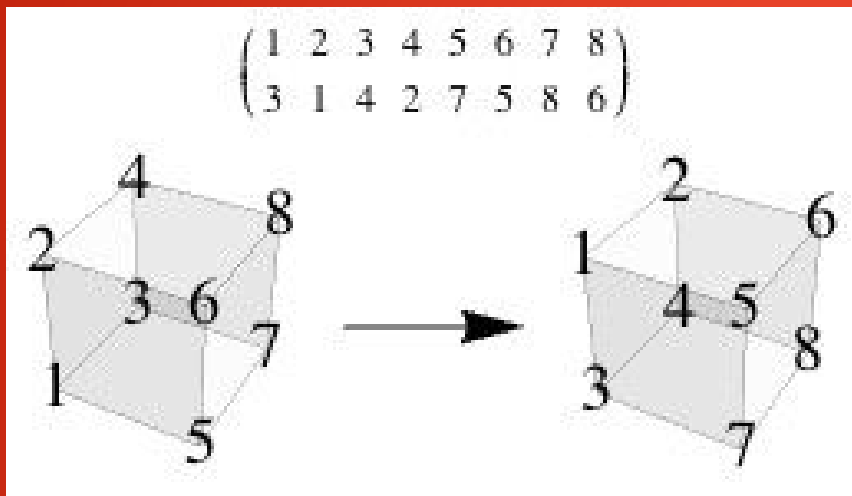
# Inter-universal Geometer

E-mail:

`motizuki@kurims.kyoto-u.ac.jp`

## Shinichi Mochizuki







# The Periodic Table Of Finite Simple Groups

$0, C_1, Z_2$
1
1

Dynkin Diagrams of Simple Lie Algebras



$A_1(4), A_1(5)$	$A_2(2)$											${}^2A_3(4)$	$C_3(3)$	$D_4(2)$	${}^2D_4(2^2)$	$G_2(2)'$	$C_2$			
$A_5$	$A_1(7)$											$B_2(3)$	$C_3(3)$	$D_4(2)$	${}^2D_4(2^2)$	${}^2A_2(9)$	$C_3$			
60	168											25920	4 585 351 680	174 182 400	197 406 720	6 048	3			
$A_1(9), B_2(2)'$	${}^2G_2(3)'$											$B_2(4)$	$C_3(5)$	$D_4(3)$	${}^2D_4(3^2)$	${}^2A_2(16)$	$C_5$			
$A_6$	$A_1(8)$											979 200	228 501 000 000 000	4 952 179 814 400	10 151 968 619 520	62 400	5			
360	504																			
$A_7$	$A_1(11)$	$E_6(2)$	$E_7(2)$	$E_8(2)$	$F_4(2)$	$G_2(3)$	${}^3D_4(2^3)$	${}^2E_6(2^2)$	${}^2B_2(2^3)$	Tits*	${}^2F_4(2)'$	${}^2G_2(3^3)$	$B_3(2)$	$C_4(3)$	$D_5(2)$	${}^2D_5(2^2)$	${}^2A_2(25)$	$C_7$		
2 520	660	214 841 575 522 005 575 270 400	7 987 879 942 675 781 700 530 467 262 480 902 918 480	27 947 816 384 336 142 280 475 751 230 454 134 376 205 778 768 254 437 992 288	3 311 126 603 366 400	4 245 696	211 341 312	76 532 479 683 774 853 939 200	29 120	17 971 200	10 073 444 472	1 451 520	$C_4(3)$	$D_5(2)$	${}^2D_5(2^2)$	${}^2A_2(25)$	126 000	7		
$A_1(2)$	$A_1(13)$	$E_6(3)$	$E_7(3)$	$E_8(3)$	$F_4(3)$	$G_2(4)$	${}^3D_4(3^3)$	${}^2E_6(3^2)$	${}^2B_2(2^5)$	${}^2F_4(2^3)$	${}^2G_2(3^5)$	$B_2(5)$	$C_3(7)$	$D_4(5)$	${}^2D_4(4^2)$	${}^2A_3(9)$	$C_{11}$			
20 160	1 092	7 207 763 587 843 803 230 628 238 393 214 840 230	1 271 379 236 938 536 142 280 475 751 230 454 134 376 205 778 768 254 437 992 288	27 947 816 384 336 142 280 475 751 230 454 134 376 205 778 768 254 437 992 288	5 734 420 792 816 671 844 761 600	251 596 800	20 560 831 566 912	14 626 935 939 569 453 963 328 688 532 377 488	32 537 600	264 905 352 699 586 176 614 400	49 825 657 439 340 552	4 680 000	$C_3(7)$	$D_4(5)$	${}^2D_4(4^2)$	${}^2A_3(9)$	67 536 471 195 648 000	3 265 920	11	
$A_9$	$A_1(17)$	$E_6(4)$	$E_7(4)$	$E_8(4)$	$F_4(4)$	$G_2(5)$	${}^3D_4(4^3)$	${}^2E_6(4^2)$	${}^2B_2(2^7)$	${}^2F_4(2^5)$	${}^2G_2(3^7)$	$B_2(7)$	$C_3(9)$	$D_5(3)$	${}^2D_4(5^2)$	${}^2A_2(64)$	$C_{13}$			
181 440	2 448	93 520 782 783 562 684 329 433 429 983 542 763 868 748 860 000	1 111 040 816 640 494 112 475 751 230 454 134 376 205 778 768 254 437 992 288	27 947 816 384 336 142 280 475 751 230 454 134 376 205 778 768 254 437 992 288	19 009 825 521 840 945 451 297 669 120 000	5 859 000 000	67 802 350 642 790 400	94 686 576 427 100 485 836 772 287 384 963 328 688 532 377 488	34 093 383 680	1 108 433 151 789 396 487 782 344 489 742 723 560 000	239 189 910 264 352 349 332 632	138 297 600	$C_3(9)$	$D_5(3)$	${}^2D_4(5^2)$	${}^2A_2(64)$	17 880 203 250 000 000 000	5 515 776	13	
$A_n$	$PSL_{n+1}(q), L_{n+1}(q)$	$E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$	${}^3D_4(q^3)$	${}^2E_6(q^2)$	${}^2B_2(2^{2n+1})$	${}^2F_4(2^{2n+1})$	${}^2G_2(3^{2n+1})$	$O_{2n+1}(q), O_{2n+1}^-(q)$	$PSp_{2n}(q)$	$C_n(q)$	$O_{2n}^+(q)$	$O_{2n}^-(q)$	$PSU_{n+1}(q)$	${}^2A_n(q^2)$	$Z_p$	
$\frac{n!}{2}$	$\frac{q^{n+1}-1}{(q-1)} \prod_{i=2}^{n+1} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$q^{2n+1}-1$	$\frac{q^{2n+1}-1}{(q-1)} \prod_{i=2}^{2n+1} (q^i-1)$	$\frac{q^{2n+1}-1}{(q-1)} \prod_{i=2}^{2n+1} (q^i-1)$	$\frac{q^{2n+1}-1}{(q-1)} \prod_{i=2}^{2n+1} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$\frac{q^{2n}-1}{(q-1)} \prod_{i=2}^{2n} (q^i-1)$	$p$

- Altering 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†

$M_{11}$	$M_{12}$	$M_{22}$	$M_{23}$	$M_{24}$	$J(1), J(11)$	$HJ$	$HJM$	$J_4$	$HS$	$McL$	$He$	$Ru$
7 920	95 040	443 520	10 200 960	244 823 040	175 560	604 800	50 232 960	86 775 571 046 077 562 880	44 352 000	898 128 000	4 030 387 200	145 926 144 000

\*For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups these are used to indicate isomorphisms. All such isomorphisms appear on the table except the family  $B_n(2^{2n}) \cong C_n(2^{2n})$ .

\*The Tits group  ${}^2F_4(2)'$  is not a group of Lie type, but is the (indefinite) commutator subgroup of  $F_4(2)$ . It is usually given honorary Lie type status.

The groups starting on the second row are the classical groups. The sporadic Suzuki group is unrelated to the families of Suzuki groups.

†Finite simple groups are determined by their order with the following exceptions:  
 $B_n(q)$  and  $C_n(q)$  for  $q$  odd,  $n > 2$ .  
 $A_n \cong A_1(2)$  and  $A_1(4)$  of order 20160.

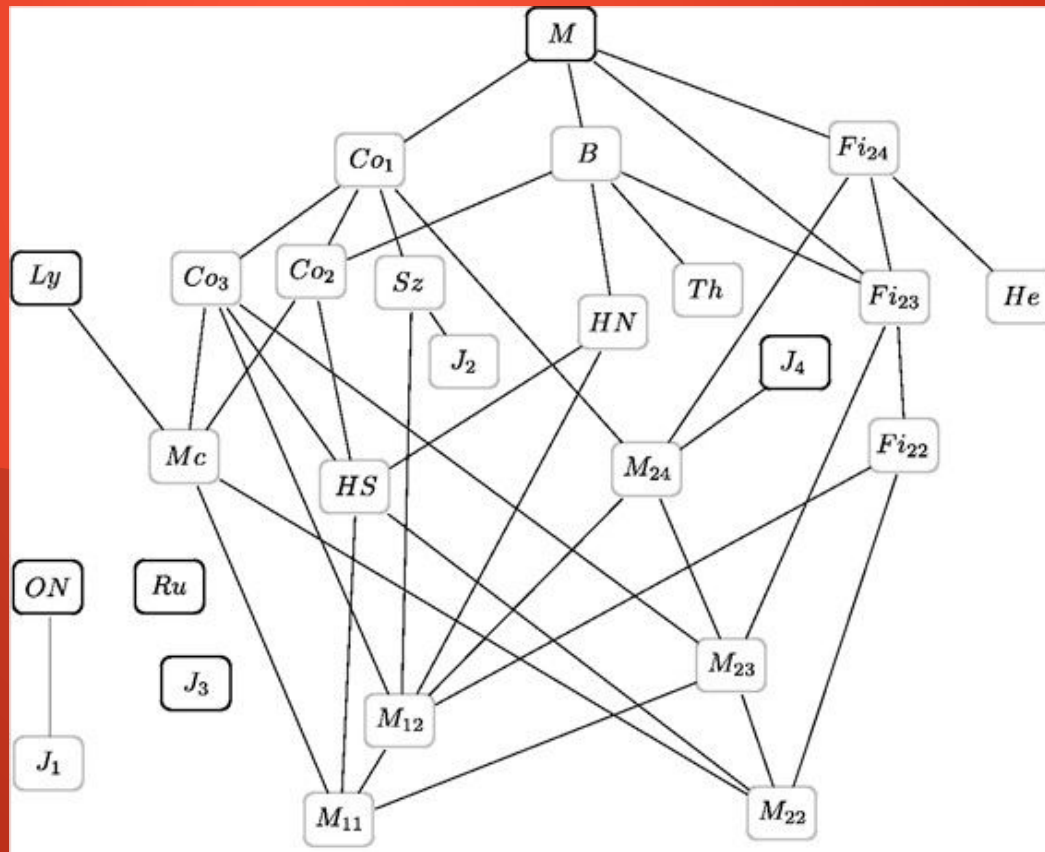
$Sz$	$O'N, O-S$	-3	-2	-1	$F_4, D$	$LyS$	$F_4, E$	$M(22)$	$M(23)$	$F_4, M(24)'$	$F_2$	$F_3, M_1$
$Suz$	$O'N$	$Co_3$	$Co_2$	$Co_1$	$HN$	$Ly$	$Th$	$Fi_{22}$	$Fi_{23}$	$Fi_{24}'$	$B$	$M$
448 345 497 600	460 815 505 920	495 766 656 000	42 305 421 312 000	4 157 776 806 543 360 000	273 030 912 000 000	51 765 179 004 000 000	90 745 943 887 872 000	64 561 751 654 400	4 089 470 473 293 004 800	1 255 205 709 190 661 721 292 800	4 157 761 481 228 426 919 177 380 344 000 000	888 639 968 962 738 737 693 754 360 000 000 000

# Enormous Theorem (1983)

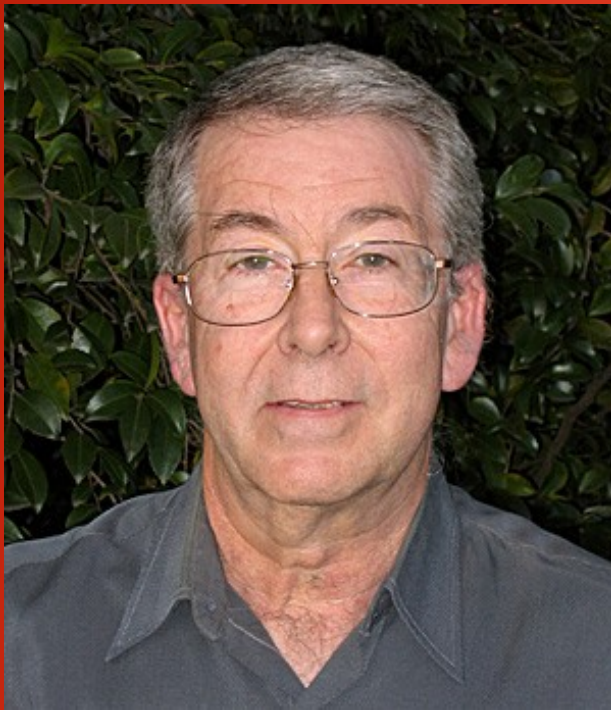
Every finite simple group belongs to either:

- one of 18 different infinite families (omitted); or
- the list of 26 exceptions.

10,000+ pages  
500+ papers  
100+ researchers



Mathieu group $M_{11}$
Mathieu group $M_{12}$
Janko group $J_1$
Mathieu group $M_{22}$
Janko group $J_2 = HJ$
Mathieu group $M_{23}$
Higman-Sims group HS
Janko group $J_3$
Mathieu group $M_{24}$
McLaughlin group McL
Held group He
Rudvalis Group Ru
Suzuki group Suz
O'Nan group O'N
Conway group $Co_3$
Conway group $Co_2$
Fischer group $Fi_{22}$
Harada-Norton group HN
Lyons Group Ly
Thompson Group Th
Fischer group $Fi_{23}$
Conway group $Co_1$
Janko group $J_4$
Fischer group $Fi'_{24}$
baby monster group $B$
monster group $M$



## Aschbacher-Smith (2004)



1,221 pages



# FIELDS ARRANGED BY PURITY

→  
MORE PURE

SOCIOLOGY IS  
JUST APPLIED  
PSYCHOLOGY

PSYCHOLOGY IS  
JUST APPLIED  
BIOLOGY.

BIOLOGY IS  
JUST APPLIED  
CHEMISTRY

WHICH IS JUST  
APPLIED PHYSICS.  
IT'S NICE TO  
BE ON TOP.

OH, HEY, I DIDN'T  
SEE YOU GUYS ALL  
THE WAY OVER THERE.



SOCIOLOGISTS

PSYCHOLOGISTS

BIOLOGISTS

CHEMISTS

PHYSICISTS

MATHEMATICIANS