

The background features a dense, repeating geometric pattern. It consists of interlocking shapes, primarily triangles and hexagons, outlined in red and blue. These shapes are arranged in a grid-like fashion, with small gold star-like motifs interspersed between them. The overall effect is a vibrant, intricate tessellation.

Math 3500

Algebra I: Group Theory

Book 2

Similar to HW#2: How many elements of each order does S_4 have?

1 element of order 1: $() = \text{identity}$

9 elements of order 2: $(12), (13), (14), (23), (24), (34),$ $\leftarrow \binom{4}{2} = 6$ transpositions
 $(12)(34), (13)(24), (14)(23)$ $\leftarrow \frac{1}{2!} \binom{4}{2} \binom{2}{2} = \frac{6}{2} = 3$

8 elements of order 3: $(123), (124), (132), (134), (142), (143), (234), (243)$

6 elements of order 4: $(1234), (1243), (1324), (1342), (1423), (1432)$

$24 = 4! = |S_4|$ $|S_n| = n! = 1 \times 2 \times 3 \times \dots \times n$

In S_n the number of n -cycles is $(n-1)!$

The binomial coefficient $\binom{n}{k}$ ("n choose k") is the number of ways to choose a subset of size k from a set of size n .

$\binom{n}{k} = k^{\text{th}}$ entry in n^{th} row of Pascal's Triangle

$\binom{4}{2} = \text{number of 2-subsets in } [4] = \{1,2,3,4\}$
 $= 6$

By the way, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Binomial Theorem $(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$

Pascal's Triangle

$n=0$	1							
$n=1$	1	1						
$n=2$	1	2	1					
$n=3$	1	3	3	1				
$n=4$	1	4	6	4	1			
$n=5$	1	5	10	10	5	1		
$n=6$	1	6	15	20	15	6	1	
$n=7$	1	7	21	35	35	21	7	1

A transposition is a 2-cycle $(i j) \in S_n$, $i \neq j$ in $[n] = \{1, 2, \dots, n\}$.

Products of disjoint transpositions e.g. $(1 3)(2 5)(6 8) \in S_8$
are elements of order 2.

How many elements of order 2 are there in S_7 ?

Transpositions: $(12), (13), (14), \dots, (67)$ i.e. $(i j)$ where $i \neq j$ in $[7] = \{1, 2, \dots, 7\}$

$$\binom{7}{2} = 21 \text{ transpositions}$$

Products of two disjoint transpositions e.g. $(26)(34) = (34)(26)$

$$\text{Number of these is } \frac{1}{2} \binom{7}{2} \binom{5}{2} = 105$$

Products of three disjoint transpositions e.g. $(15)(27)(36) = (15)(36)(27) = (27)(36)(15)$

$$\text{Number of these is } \frac{1}{6} \binom{7}{2} \binom{5}{2} \binom{3}{2} = \frac{21 \times 10 \times 3}{6 \cdot 2} = 105$$

Number of 3-cycles in S_7 e.g. (274) : $2 \binom{7}{3} = 2 \times 35 = 70$

Number of products of two disjoint 3-cycles: e.g. $(274)(356) = (356)(274)$

$$\frac{1}{2} \cdot 70 \cdot \binom{4}{3} \cdot 2 = 70 \cdot 4 = 280$$

Elements of order 12 in S_7 e.g. $(142)(3756)$

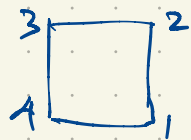
$$70 \cdot 3! = 70 \cdot 6 = 420 \text{ elements of order 12 in } S_7$$

280 + 70
= 350
elements
of order 3
in S_7

Revisiting the dihedral group of order 8 (symmetry group of a square)

$$G = \{ I, R, R^2, R^3, D, D', V, H \}$$

viewed as a group of permutations of the four vertices



$$I \mapsto ()$$

$$R \mapsto (1234)$$

$$R^2 \mapsto (13)(24)$$

$$R^3 \mapsto (1432)$$

$$H \mapsto (12)(34)$$

$$V \mapsto (14)(23)$$

$$D \mapsto (13)$$

$$D' \mapsto (24)$$

$G \cong$ subgroup of S_4 : $\{(), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}$

$$RV = (1234)(14)(23) = (24) = D' = \langle (1234), (13) \rangle$$

This is an example of a permutation group of degree 4, i.e. a subgroup of S_4 .
A permutation group of degree n is a subgroup of the symmetric group S_n .

Theorem (Cayley's Representation Theorem) Every finite group is isomorphic to a permutation group. In fact, if $|G| = n$ then G is isomorphic to a subgroup of S_n . (But we can usually do better. Eg. the dihedral group of order 8 is isomorphic to a subgroup of S_8 . But S_4 is even better.)

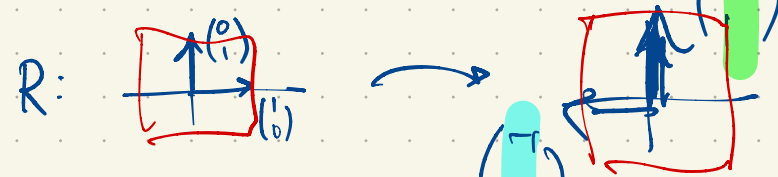
The two most important general classes of examples of groups are
(i) permutation groups (i.e. subgroups of S_n) and
(ii) linear groups (i.e. subgroups of $GL_n(F) = \{ \text{invertible } n \times n \text{ matrices over a field } F \}$). eg. $F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ (integers mod p)

The dihedral group of order 8 is also a subgroup of $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$



$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

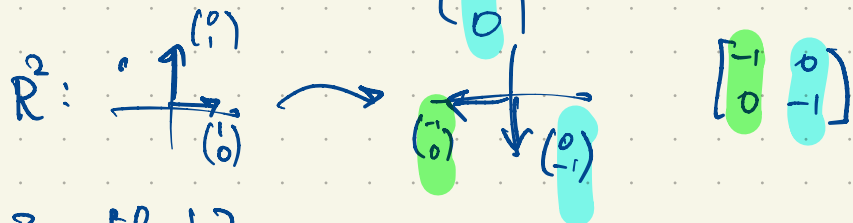
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$



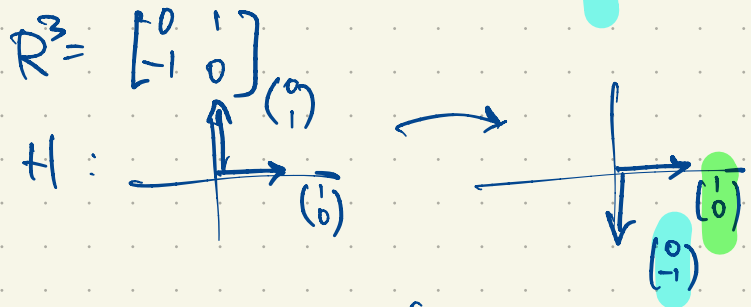
$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -y \\ x \end{bmatrix}$$

(the vector $\begin{bmatrix} x \\ y \end{bmatrix}$ rotated 90° counter-clockwise about the origin)

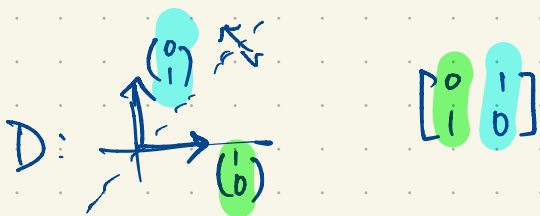


$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

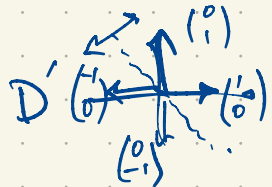


$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$G =$ symmetry group of square $\cong \left\{ \begin{matrix} I & R & R^2 & R^3 & H \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, & \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, & \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, & \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \\ & \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \end{matrix} \right\}$



$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



$$R^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

subgroup of $GL_2(\mathbb{R})$

$$\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$$

commutes with every element of G
(not so immediately obvious from the other ways of representing G).

Similar to HW2 #4, 5: $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ integers mod p .

eg. $p=3$, $F = \mathbb{F}_3 = \{0, 1, 2\}$

$$\begin{array}{r|rrr} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$$

$$\begin{array}{r|rrr} \times & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$$

$$\frac{1}{2} = 2 \quad -\frac{1}{2} = -2 = 1$$

$$F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$$

$$|F^2| = 3^2 = 9$$

2×2 matrices over F there are $3^4 = 81$ 2×2 matrices over F .

$$\begin{bmatrix} * & * \\ * & * \end{bmatrix}$$

$$GL_2(F) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in F, \underbrace{ad - bc \neq 0} \right\}$$

ie. $ad - bc = 1$ or 2 ie. $ad - bc = \pm 1$.

$$|GL_2(F)| = 8 \times 6 = 48$$

$9-1=8$ choices for first column to be nonzero
 $9-3=6$ choices for the second column to be not a scalar multiple of the first column.

eg. $g = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \in GL_2(F) \Rightarrow g^2 = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

so $|g| = 2$.

Eg. $F = \mathbb{F}_2 = \{0, 1\}$

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

ie. $\det A = 1$

Let's try $G = GL_3(F) = \{3 \times 3 \text{ matrices } A \text{ over } F \text{ such that } \det A \neq 0\}$

The total number of 3×3 matrices over F is $2^9 = 512$.

$$|G| = 7 \times 6 \times 4 = 168$$

8-1 nonzero vectors
8-2
8-4

$$\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \end{bmatrix}$$

F^3 is a 3-dimensional vector space over F

$$|F^3| = 2^3 = 8$$

eg. $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \in G$

$$A^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$$A^3 = \underbrace{\begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}}_{A^2} \underbrace{\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}}_A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$|A| = 4 = \text{the order of } A$
Note: $4 \mid 168$

$$A^4 = A^2 A^2 = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

$$F^3 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}$$

$\begin{matrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \end{matrix}$

$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ permutes the vectors as

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

ie. (4217)
= (1742)

$$= (1742)(36)$$

has order 4

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \text{ie. } (36)$$

$$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \text{ie. } (5)$$

$$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad \text{ie. } (6)$$

$B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ what is the order of $B \in GL_3(F)$, $F = \{0, 1\}$?

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$v_4 \quad v_2 \quad v_1 \quad v_6 \quad v_3 \quad v_7 \quad v_5 \quad v_4$

ie. $B = (1637542)$ has order 7.

Alternatively compute $B, B^2, B^3, B^4, B^5, B^6, B^7 = I$.

$$|S_7| = 7! = 5040$$

$\langle A, B \rangle \cong \langle (1742)(36), (1637542) \rangle$ subgroup of S_7 of order 168
 $\cong GL_3(F)$

Note: If $F = \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ (integers mod p , p prime)

and $G = GL_3(F) =$ group of invertible 3×3 matrices over F

then $|G| = (p^3 - 1)(p^3 - p)(p^3 - p^2) = p^3(p^3 - 1)(p^2 - 1)(p - 1)$

$$\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \end{bmatrix}$$

↑
nonzero vectors

↑
not scalar multiple of first col.

p^9 3×3 matrices in all;
but not all of them are invertible.

$$\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$$

multiplicative group
of order 6

$$\begin{aligned} \langle 1 \rangle &= \{1\} & \langle 6 \rangle &= \{1, 6\} \\ \langle 2 \rangle &= \{1, 2, 4\} \\ \langle 3 \rangle &= \{1, 3, 2, 6, 4, 5\} = \langle 5 \rangle \\ \langle 4 \rangle &= \{1, 4, 2\} = \langle 2 \rangle \\ \langle 5 \rangle &= \{1, 5, 4, 6, 2, 3\} \end{aligned}$$

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

=

x	1	3	2	6	4	5
1	1	3	2	6	4	5
3	3	2	6	4	5	1
2	2	6	4	5	1	3
6	6	4	5	1	3	2
4	4	5	1	3	2	6
5	5	1	3	2	6	4

$$\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\} \text{ under addition mod 6}$$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

We have an isomorphism from
 $(\mathbb{Z}/6\mathbb{Z}, +)$ to (\mathbb{F}_7^*, \cdot)

defined by $\phi: \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{F}_7^*$

$$\phi(0) = 1$$

$$\phi(1) = 3$$

$$\phi(2) = 2$$

$$\phi(3) = 6$$

$$\phi(4) = 4$$

$$\phi(5) = 5$$

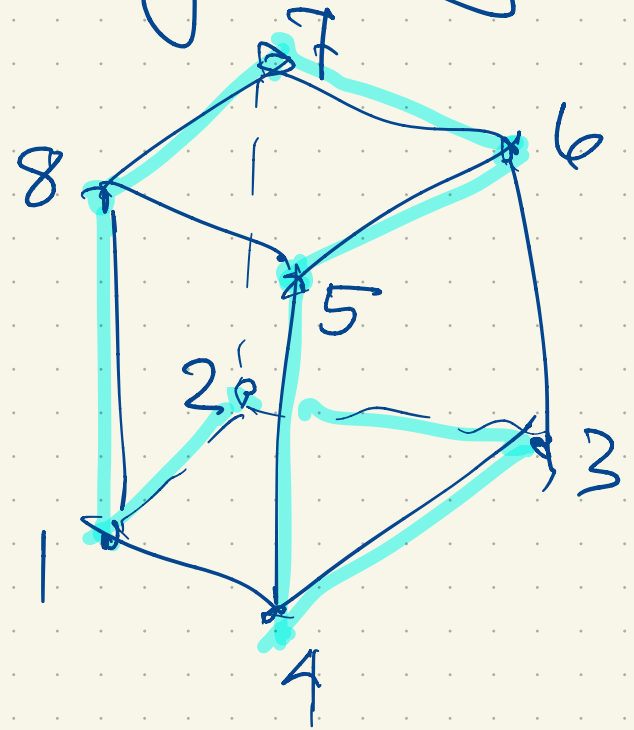
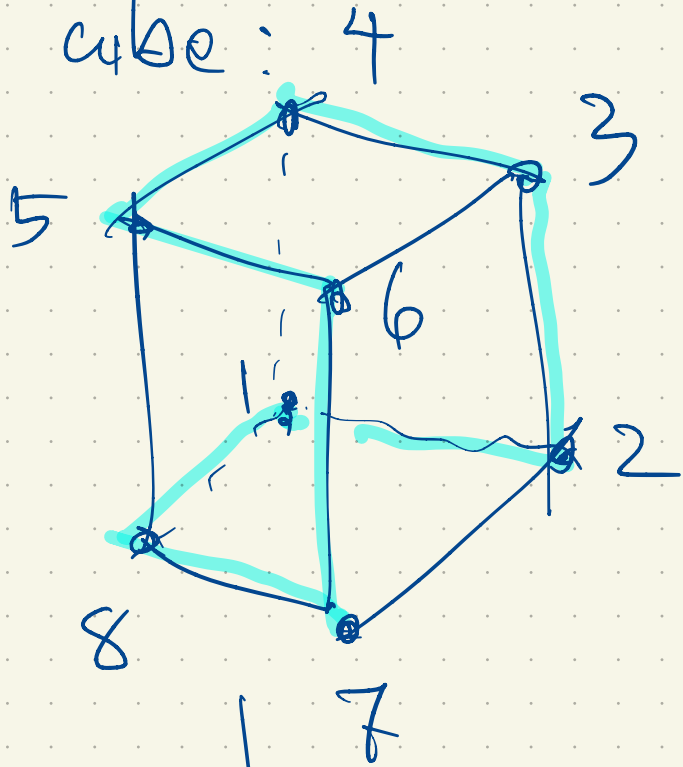
$$\phi(x+y) = \phi(x)\phi(y)$$

$$\phi(\underbrace{1+1+\dots+1}_k \text{ times}) = \underbrace{3 \cdot 3 \cdot \dots \cdot 3}_k \text{ times}$$

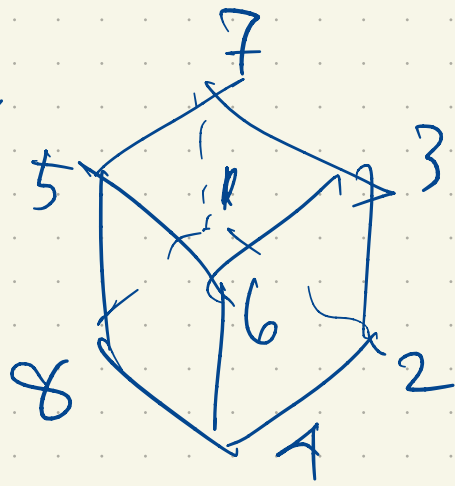
$$\phi(k) = 3^k$$

$$\phi(k+l) = 3^{k+l} = 3^k \cdot 3^l = \phi(k)\phi(l)$$

check that $(123658)(47)$ is a symmetry of
my cube:



(47) is not a symmetry



March 2026 - Apr 2026

M	W	F
9	11	13
16	18	20
23	25	27
30	1	3

Test on Mon Mar 30
covering material prior to
today

The symmetric group $S_n = \{\text{permutations of } [n]\}$
where $n = \{1, 2, \dots, n\}$ Note: there are
 n points being permuted by. $|S_n| = n! = 1 \times 2 \times \dots \times n$
permutations. THIS IS NOT THAT.

There are $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositions in S_n .

Theorem S_n is generated by its transpositions

eg. for $n=4$, $S_4 = \langle (12), (13), (14), (23), (24), (34) \rangle$.

eg. $(13)(12) = (123) = (14)(23)(12)(34)(24)(12)$

Theorem Every permutation $\sigma \in S_n$
is either even or odd, never both.
(σ is even if it's a product of an
even number of transpositions;
 σ is odd if it's a product of
an odd number of transpositions.)

\sum upper case Sigma M
 σ lower case sigma μ mu
or σ

k	$\sigma(k)$
1	2
2	3
3	1
4	4
5	5

$\sigma = (123)$

To prove the theorem, we must show is that
if $\sigma = \tau_1 \tau_2 \tau_3 \dots \tau_{2k+1}$ then $\sigma = \mu_1 \mu_2 \dots \mu_{2l}$

τ_i transpositions

μ_j transpositions

$\mu \mu$

$$() = (12)(12)$$

Proof Consider the polynomial

$$f(x_1, x_2, x_3, x_4) = (x_2 - x_1)(x_3 - x_1)(x_4 - x_1)(x_3 - x_2)(x_4 - x_2)(x_4 - x_3)$$

$$f(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_j - x_i) \quad \text{of degree } \binom{n}{2}.$$

$$\text{If } \sigma \in S_4 \text{ then } f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}) = \pm f(x_1, x_2, x_3, x_4)$$

eg. for (12) we get

$$\begin{aligned} f(x_2, x_1, x_3, x_4) &= (x_1 - x_2)(x_3 - x_2)(x_4 - x_2)(x_3 - x_1)(x_4 - x_1)(x_4 - x_3) \\ &= - f(x_1, x_2, x_3, x_4) \end{aligned}$$

for (123) we get

$$\begin{aligned} f(x_2, x_3, x_1, x_4) &= (x_3 - x_2)(x_1 - x_2)(x_4 - x_2)(x_1 - x_3)(x_4 - x_3)(x_4 - x_1) \\ &= f(x_1, x_2, x_3, x_4) \end{aligned}$$

The sign of $\sigma \in S_n$ has value $\text{sgn}(\sigma) = \pm 1$ where $f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = (\text{sgn}(\sigma)) f(x_1, x_2, \dots, x_n)$

$$\text{For } \sigma, \sigma' \in S_n, \quad \text{sgn}(\sigma\sigma') = \text{sgn}(\sigma) \text{sgn}(\sigma').$$

$\underbrace{\quad}_{\pm 1} \quad \underbrace{\quad}_{\pm 1} \quad \underbrace{\quad}_{\pm 1}$

i.e.

even	x	even	=	even
even	x	odd	=	odd
odd	x	even	=	odd
odd	x	odd	=	even

where σ is even if $\text{sgn}(\sigma) = 1$;
odd if $\text{sgn}(\sigma) = -1$.

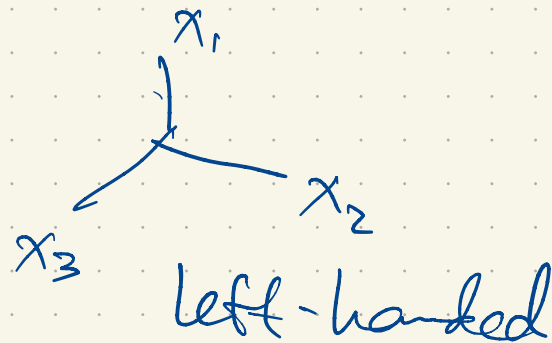
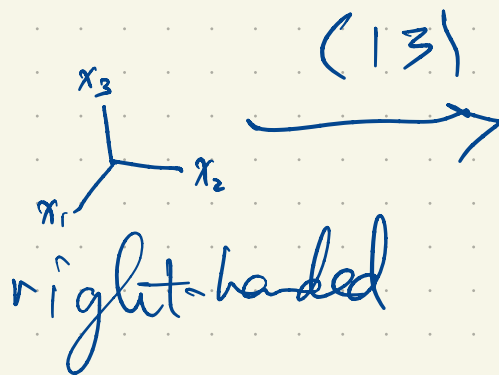
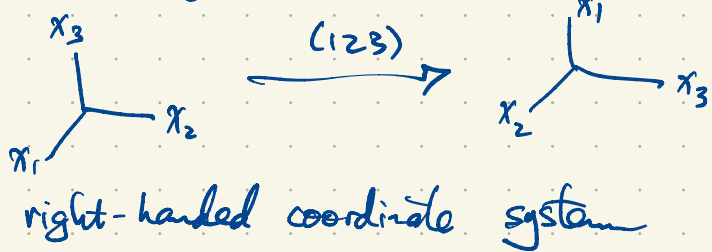
Note: Cycles of even length are odd permutations.
Cycles of odd length are even permutations.

An n -cycle (i.e. a cycle of length n) is a product of $n-1$ transpositions.

eg. (12) is an odd permutation
 $(13)(12) = (123)$ is an even permutation
 $(14)(13)(12) = (1234)$ is an odd permutation.
 $(12)(13)(14) = (1432)$

$(15764)(2389)$ is odd
 even odd

$= (14)(16)(17)(15)(29)(28)(23)$



(123) preserves orientation
 (13) reverses orientation

An $n \times n$ matrix $A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$ has determinant

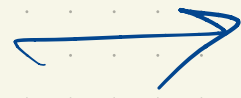
$$\det A = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1, \sigma(1)} a_{2, \sigma(2)} \dots a_{n, \sigma(n)}$$

($n!$ terms)

If $n=3$ then

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} a_{22} a_{33} + a_{12} a_{23} a_{31} + a_{13} a_{21} a_{32} - a_{13} a_{22} a_{31} - a_{12} a_{21} a_{33} - a_{11} a_{23} a_{32}$$

1	2	3	4
5	6	7	8
9	10	12	14
13	15	11	



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	



$(11, 15, 14, 12)$

$(11, 12, 14, 15)$

is an ~~even~~ ^{odd} permutation

$$|S_n| = n!$$

$A_n = \{ \text{even permutations in } S_n \} = \text{alternating group of degree } n.$

For $n \geq 2$, exactly half of the permutations in S_n are even; the others are odd.

$$|A_n| = \frac{n!}{2}$$

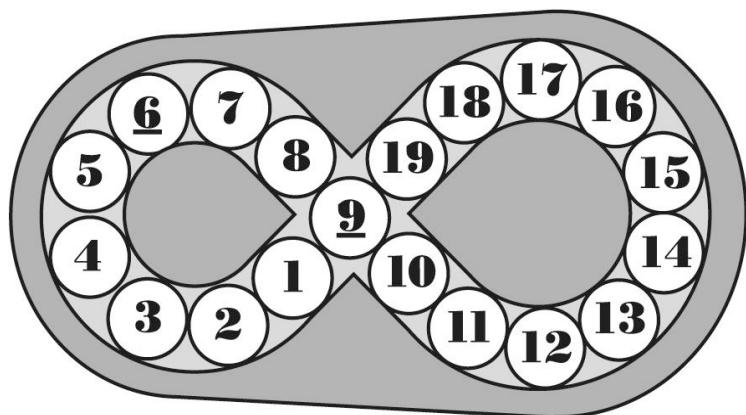
For $n=4$, $S_4 = \{ () , (12), (13), (14), (23), (24), (34), (1234), (1243), (1324), (1342), (1423), (1432), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23) \}$

$A_4 = \{ () , (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23) \}$

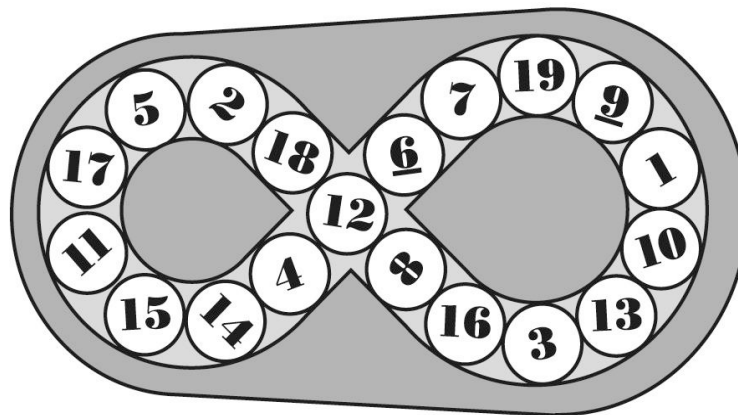
$$|S_4| = 24$$

A_4 is a subgroup of S_4 .

The odd permutations do not form a subgroup; they form a cosets.



Puzzle: Original Position



Puzzle: Altered Position

The legal moves of this puzzle form a subgroup of S_{14} :

$$\langle (1, 2, 3, 4, 5, 6, 7, 8, 9), (9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19) \rangle$$

The altered position is $(1, 4, 11, 16, 9, 12, 3, 15) \underbrace{(2, 14, 10, 8, 18, 7)}_{\text{length 6}} \underbrace{(5, 17, 19, 6)}_{\text{length 4}}$ (fixing 13)
 which is odd.
 This is not a legal move!

Warming up to Lagrange's Theorem:

Let's consider subgroups of a cyclic group $C_n = \{1, g, g^2, \dots, g^{n-1}\}$ of order n , $g^n = 1$.

$$g^i g^j = g^{i+j} \quad (\text{exponents mod } n).$$

C_n is a multiplicative group isomorphic to $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$, an additive group (integers mod n).

Special case $n=12$: $C_{12} = \{1, g, g^2, \dots, g^{11}\} = \langle g \rangle$, $g^{12} = 1$

C_{12} has 6 subgroups:

The positive integer divisors of 12 are 1, 2, 3, 4, 6, 12.

	$C_{12} = \langle g \rangle = \{1, g, g^2, \dots, g^{11}\}$	of order 12
	$\langle 1 \rangle = \{1\}$	" " 1
(trivial subgroup)	$\langle g^2 \rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$	" " 6
$\langle g^2 \rangle$	$\langle g^3 \rangle = \{1, g^3, g^6, g^9\}$	" " 4
	$\langle g^4 \rangle = \{1, g^4, g^8\}$	" " 3
	$\langle g^6 \rangle = \{1, g^6\}$	" " 2

$$\gcd(4, 6) = 2 \Rightarrow \langle g^4, g^6 \rangle = \langle g^2 \rangle$$

$$\gcd(3, 4) = 1 \Rightarrow \langle g^3, g^4 \rangle = \langle g \rangle = \langle g \rangle$$

Theorem Let n be a positive integer, and let C_n be a cyclic group of order n . Then every subgroup of C_n has order dividing n . Moreover, there is a unique subgroup of order d for every positive integer dividing n . In particular, the number of subgroups of C_n is the number of positive integer divisors of n .

$$\langle g^4, g^6 \rangle = \langle g^2 \rangle \quad \text{since } \langle g^4, g^6 \rangle \subseteq \langle g^2 \rangle \quad \text{and} \quad \langle g^2 \rangle \subseteq \langle g^4, g^6 \rangle$$

$$g^2 = (g^4)^4 (g^6)^1 \in \langle g^4, g^6 \rangle$$

$$\Rightarrow \langle g^2 \rangle \subseteq \langle g^4, g^6 \rangle$$

$$(g^5)^k = (g^7)^{(k)}$$

$$\langle g^5 \rangle = \{1, g^5, g^{10}, g^3, g^8, g, g^6, g^9, g^4, g^9, g^2, g^7\} = \langle g \rangle$$

$$= \langle g^7 \rangle = \langle g^{11} \rangle = \langle g^{-1} \rangle$$

Every element $g \in G$ generates the same cyclic subgroup as its inverse: $\langle g^{-1} \rangle = \langle g \rangle$

$$\mathbb{Z} = \{ \dots, \underbrace{-3, -2, -1}_{\text{negative integers}}, \underbrace{0}_{\text{zero}}, \underbrace{1, 2, 3}_{\text{positive integers}}, \dots \}$$

is an additive cyclic group

If $a, b, c \in \mathbb{Z}$ with $a = bc$ then

- a is a multiple of b
- b divides a
- b is a divisor of a
- $b \mid a$ ("b divides a")

(also a multiple of c)

divisibility is a relation between two integers

Note: vertical bar, not division

eg. $3 \mid 12$ (3 divides 12 since $12 = 4 \times 3$)

$$17 \mid 17$$

$$17 \mid 0 \quad \text{since } 0 = 0 \times 17$$

$$-3 \mid 12 \quad \text{since } 12 = (-4) \times (-3)$$

$$0 \mid 0 \quad \text{since } 0 = 17 \times 0$$

The divisors of 12 are $-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$. (i.e. $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$)

The positive divisors of 12 are $1, 2, 3, 4, 6, 12$.
(positive integer divisors)

The divisors of 7 are $\pm 1, \pm 7$.

$$3 \mid 12, 18 \nmid 12$$

$$18 \nmid 12, 18 \nmid 12, 12 \mid 12, 12 \nmid 13$$

$$-6 \mid -12 \quad \text{since } -12 = 2 \times (-6)$$

Let $n \in \mathbb{Z}$. Then n is even iff $2 \mid n$ iff $n \in \{ \dots, -6, -4, -2, 0, 2, 4, 6, \dots \}$

Facts about divisibility:

If $a|b$ and $b|c$, then $a|c$.

(If $c=kb$ and $b=la$ then $c=(kl)a$.)

If $a|b$ and $a|c$ then $a|(b+c)$.

If $a|c$ and $b|c$, does $a+b$ divide c ?
No.

Division with remainder:

Let $n, d \in \mathbb{Z}$ with $d > 0$.

(Note: $n \in \mathbb{Z}$ can be positive, negative or 0.)

(Division Algorithm)

Theorem There exist unique $q, r \in \mathbb{Z}$ such that $n = qd + r$, $0 \leq r < d$.

($r \in \{0, 1, 2, \dots, d-1\}$)

I'm intentionally writing q, d, r to stand for quotient, divisor, remainder.

$$21 = \underbrace{5}_{\text{quotient}} \times 4 + \underbrace{1}_{\text{remainder}}$$

$$4 \overline{) 21}$$

$$2026 = \frac{506 \times 4 + 2}{506}$$
$$\begin{array}{r} 4 \overline{) 2026} \\ \underline{20} \\ 026 \\ \underline{24} \\ 2 \end{array}$$

d divides n iff when we divide n by d , the remainder is zero.

$21 = \underline{4} \times 4 + \underline{5}$ but 4 isn't the quotient and 5 isn't the remainder since $5 \notin \{0, 1, 2, 3\}$.

$$-21 = \underline{-6} \times 4 + \underline{3}$$

$$\underline{-21 = -5 \times 4 - 1}$$

By abuse of terminology, the theorem above is named after the algorithm that computes q and r .

Let n be a positive integer and let $C_n = \{1, g, g^2, \dots, g^{n-1}\}$ be the cyclic group of order n . $g^n = 1$

The subgroups of C_n are of the form $\langle g^d \rangle$, $d|n$ ($d \geq 1$).