

The background features a repeating geometric pattern. It consists of a grid of white lines forming a lattice of triangles and hexagons. Within these shapes, there are intricate, stylized designs in red and blue. Interspersed throughout the pattern are small, golden, star-like or floral motifs. The overall effect is a rich, textured, and mathematically inspired aesthetic.

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  $n^{\text{th}}$  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.  $(142)(3756)$

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

$$280 + 70$$

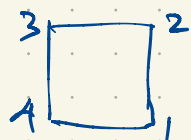
$$= 350$$

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.)

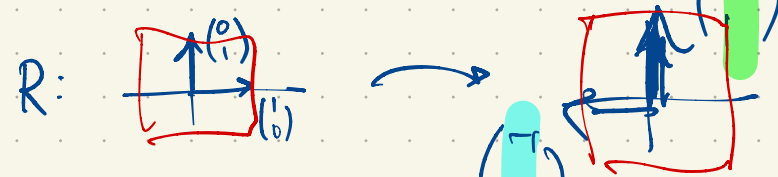
The two most important general classes of examples of groups are  
(i) permutation groups (i.e. subgroups of  $S_n$ ) and  
(ii) linear groups (i.e. subgroups of  $GL_n(F) = \{ \text{invertible } n \times n \text{ matrices over a field } F \}$ ). eg.  $F = \mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p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

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



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

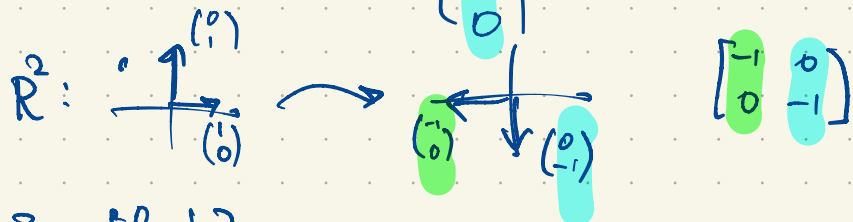
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix}$$



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

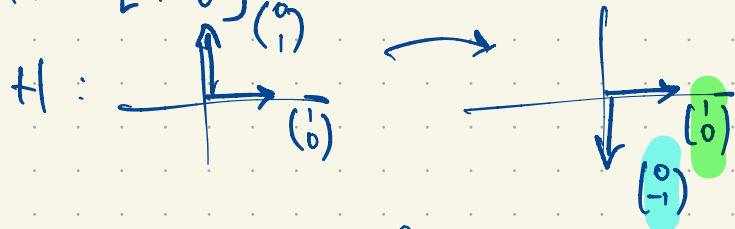
$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -y \\ x \end{bmatrix}$$

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



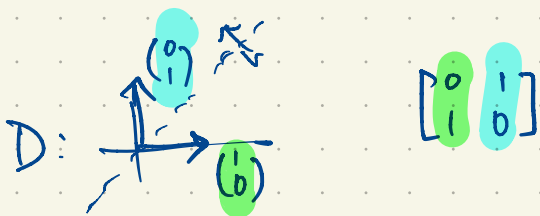
$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$R^3 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

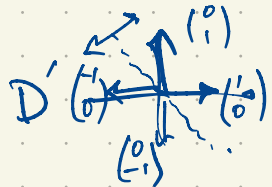


$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

$G =$  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.  $p=3$ ,  $F = \mathbb{F}_3 = \{0, 1, 2\}$   $F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$

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

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

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

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

$2 \times 2$  matrices over  $F$  there are  $3^4 = 81$   $2 \times 2$  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  $3 \times 3$  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

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

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  $3 \times 3$  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.

$p^9$   $3 \times 3$  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  $\phi: \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{F}_7^*$

$$\phi(0) = 1$$

$$\phi(1) = 3$$

$$\phi(2) = 2$$

$$\phi(3) = 6$$

$$\phi(4) = 4$$

$$\phi(5) = 5$$

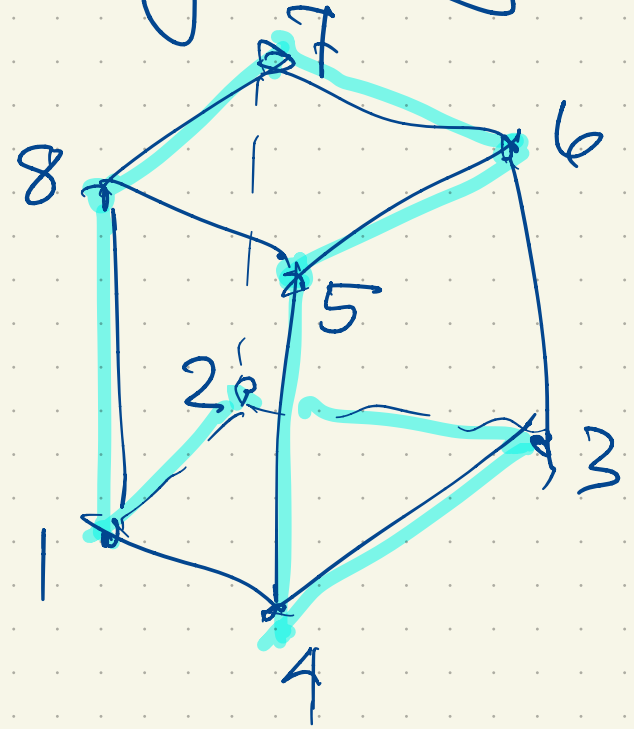
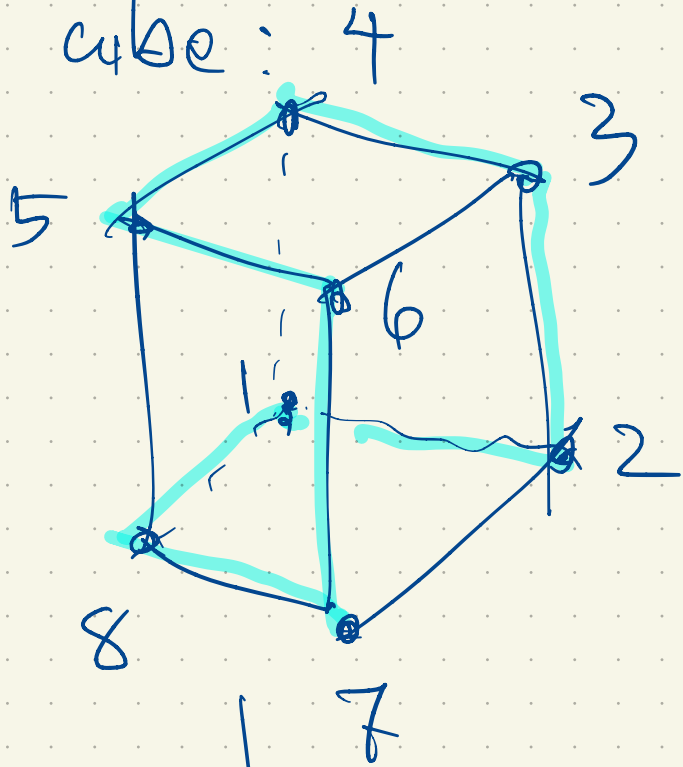
$$\phi(x+y) = \phi(x)\phi(y)$$

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

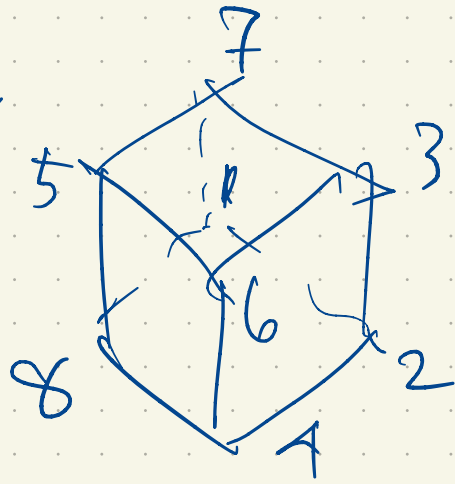
$$\phi(k) = 3^k$$

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

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.  
( $\sigma$  is even if it's a product of an  
even number of transpositions;  
 $\sigma$  is odd if it's a product of  
an odd number of transpositions.)

$\sum$  upper case Sigma M  
 $\sigma$  lower case sigma  $\mu$  mu  
or  $\sigma$

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  $\sigma = \mu_1 \mu_2 \dots \mu_{2l}$

$\tau_i$  transpositions

$\mu_j$  transpositions

$\mu \mu$

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

Proof Consider the polynomial

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

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

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

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

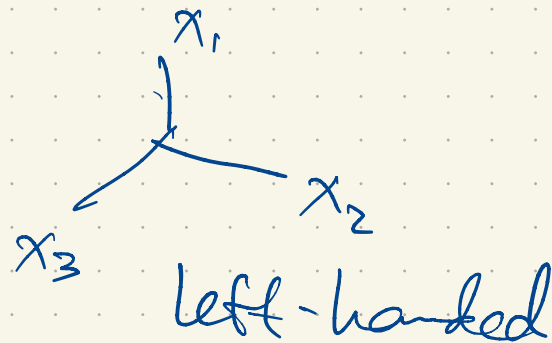
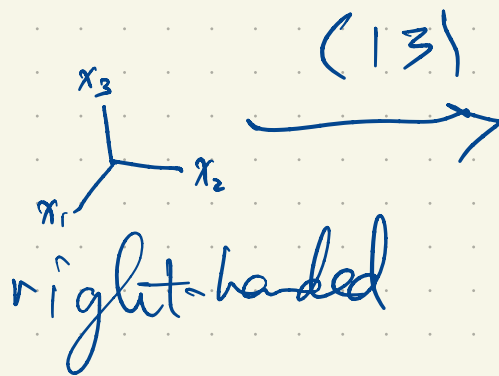
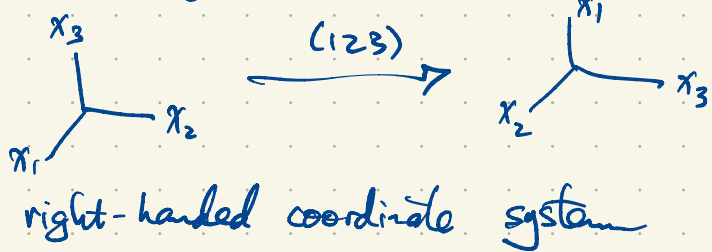
Note: Cycles of even length are odd permutations.  
Cycles of odd length are even permutations.

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

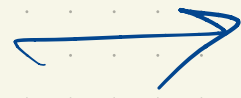
$$\det A = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1, \sigma(1)} a_{2, \sigma(2)} \dots a_{n, \sigma(n)}$$

( $n!$  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~~ <sup>odd</sup> 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.

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

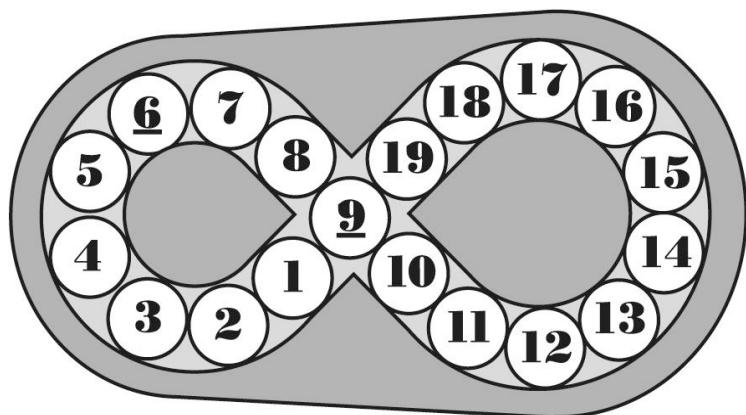
For  $n=4$ ,  $S_4 = \{ () , (12), (13), (14), (23), (24), (34), (1234), (1243), (1324), (1342), (1423), (1432), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23) \}$

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

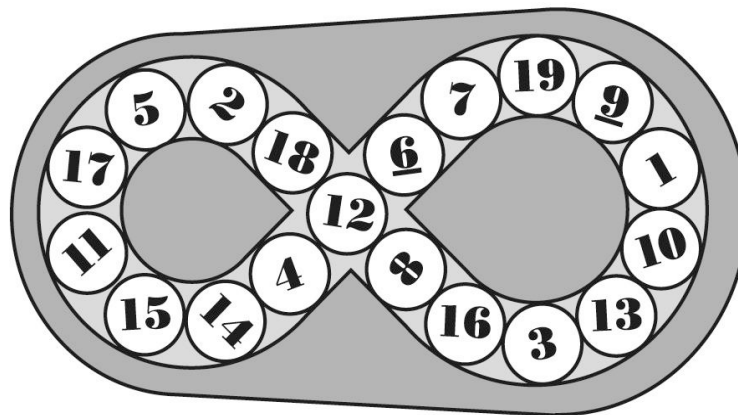
$$|S_4| = 24$$

$A_4$  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
- $\langle g^2 \rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$  " " 6
- $\langle g^3 \rangle = \{1, g^3, g^6, g^9\}$  " " 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  $n$ .

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

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

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

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

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

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

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

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

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.

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

$$4 \overline{) 21}$$

$$2026 = \frac{506 \times 4 + 2}{506}$$

$$\begin{array}{r} 4 \overline{) 2026} \\ \underline{20} \phantom{00} \\ 026 \phantom{00} \\ \underline{24} \phantom{00} \\ 2 \phantom{00} \end{array}$$

$d$  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  $r$ .

Theorem

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  $\langle g^d \rangle$ ,  $d|n$  ( $d \geq 1$ ).

Proof Let  $H \leq C_n$  (i.e.  $H$  is a subgroup of  $C_n$ ).  
 Certainly  $1 \in H$ . If  $H = \{1\}$  (the trivial subgroup). This is the special case in which  $d=n$ , and there is nothing more to say in this case.

Henceforth  $|H| \geq 2$  and  $H$  contains at least one of  $g, g^2, g^3, \dots, g^{n-1}$ .  
 Let  $d \in \{1, 2, \dots, n-1\}$  be minimal such that  $g^d \in H$ . We will show that  $\langle g^d \rangle = H$ , and that  $d|n$ . Clearly  $\langle g^d \rangle \subseteq H$  since  $H$  is a subgroup. Next we must show that  $H \subseteq \langle g^d \rangle$ . Consider any  $h \in H$ ; we must show that  $h \in \langle g^d \rangle$ . Note that  $h = g^k$  for some  $k \in \{0, 1, 2, \dots, n-1\}$ . By the Division Algorithm,  $k = qd + r$  for some  $q, r \in \mathbb{Z}$  with  $0 \leq r < d$ . So  $h = g^k = g^{qd+r} = g^{qd} g^r = \underbrace{(g^d)^q}_{\in H} g^r \Rightarrow g^r \in H$   
 $g^r = (g^{qd})^{-1} h \in H$

$r \in \{0, 1, 2, \dots, d-1\}$  but  $r \notin \{1, 2, \dots, d-1\}$  since  $g^d$  is the smallest (nontrivial) power of  $g$  in  $H$ .

So  $r=0$ , i.e.  $d|k$ ,  $k=qd$ ,  $h = g^k = (g^d)^q \in \langle g^d \rangle$ . Thus  $H \subseteq \langle g^d \rangle$  and  $H = \langle g^d \rangle$ .

To prove  $d|n$ , we have  $n = q'd + r'$  for some  $q', r' \in \mathbb{Z}$  with  $0 \leq r' < d$ , so

$$1 = g^n = g^{q'd+r'} = (g^d)^{q'} g^{r'} \Rightarrow g^{r'} = (g^d)^{-q'} \in \langle g^d \rangle = H \Rightarrow r' = 0 \Rightarrow n = q'd \Rightarrow d|n.$$

□

Let  $G, H$  be groups. A function  $f: G \rightarrow H$  is a homomorphism if  
 $f(ab) = f(a)f(b)$  for all  $a, b \in G$ . ( $G$  is the domain of  $f$ ;  $H$  is the range of  $f$ )

(For now, assume  $G, H$  are multiplicative)

Eg. if  $f$  is a bijjective homomorphism, then  $f$  is an isomorphism.  
 (1:1 and onto)

If  $f$  is onto ( $f$  is a surjective homomorphism) then  $f$  is an epimorphism.

If  $f$  is one-to-one ( $f$  is an injective homomorphism) then  $f$  is a monomorphism.

If  $f: G \rightarrow G$  is an isomorphism,  $f$  is an automorphism of  $G$ .

If  $f: G \rightarrow G$  is any homomorphism,  $f$  is an endomorphism of  $G$ .

Eg. Every isomorphism is a homomorphism.

The trivial homomorphism  $G \rightarrow H$  is the function  $g \mapsto 1_H$  for every  $g \in G$ .  
 i.e.  $g \mapsto 1_H$

$1_H$  = identity element of  $H$ .

$1_G$  = identity element of  $G$ .

$1$  = identity in either case (if no confusion arises)

The trivial homomorphism  $g \mapsto 1_H$  is  $\begin{cases} \text{one-to-one} & \text{iff } G = \{1_G\}; \\ \text{onto} & \text{iff } H = \{1_H\}; \\ \text{bijective} & \text{iff } G = \{1_G\} \text{ and } H = \{1_H\}. \end{cases}$

Mathematicians often abuse notation by writing  $G=1$  to mean  $G = \{1_G\}$  (a trivial group i.e. a group of order 1).

A more interesting homomorphism? (something "in between" trivial and bijective.)

For  $n \geq 2$ ,  $\text{sgn}: S_n \rightarrow \{\pm 1\} \leftarrow C_2$  (cyclic group of order 2)

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even;} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$$

$\text{sgn}$  is not one-to-one or onto unless  $n=2$ .

(if  $n=2$  then  $\text{sgn}() = +1$   
 $\text{sgn}(12) = -1$  is bijective)

eg. Let  $G = GL_n(\mathbb{R}) = \{n \times n \text{ matrices } A \text{ with real entries}\}$   
invertible

$$H = \mathbb{R}^* = \{\text{all nonzero real numbers}\} \cong GL_1(\mathbb{R})$$

↑  
Identifying  $[e]$  with  $a$   
gives equality (by abuse  
of notation)

There is a well-known homomorphism  
 $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$

$$\text{i.e. } \det(AB) = (\det A)(\det B).$$

This homomorphism from  $GL_n(\mathbb{R})$  onto  $\mathbb{R}^*$ .

It's not one-to-one unless  $n=1$ , in which case it is an isomorphism  $GL_1(\mathbb{R}) \xrightarrow{\cong} \mathbb{R}^*$ .

Why is  $\det: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$  onto?

Given  $a \in \mathbb{R}^*$ ,  $\det \begin{bmatrix} a & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = a$ .

If  $n \geq 2$  then  $\det \begin{bmatrix} a & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = a = \det \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & a \end{bmatrix}$  so  $\det$  is not one-to-one.

Vector spaces: linear transformations :: Groups: homomorphisms

Every vector space can be viewed as an additive group (ignore scalar multiplication).

Linear transformations are homomorphisms.

$\mathbb{Z}^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in \mathbb{Z}\}$  is an additive group (abelian) with usual componentwise addition

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

$$(0, \dots, 0) = \text{identity}$$

Inverse of  $(a_1, \dots, a_n)$  is  $(-a_1, \dots, -a_n)$

Every nonidentity element of  $\mathbb{Z}^n$  has infinite order.

Any  $m \times n$  matrix with integer entries, say  $A$ , defines a homomorphism  $\mathbb{Z}^n \rightarrow \mathbb{Z}^m$ ,

$$v \mapsto Av$$

$$A(v+w) = Av + Aw$$

column vector  
 $v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$

$$f(v+w) = f(v) + f(w)$$

$\mathbb{Z}^n$  is not a vector space.

$\mathbb{R}^n$  is a vector space.

A linear transformation  $T: \mathbb{R}^n \rightarrow \mathbb{R}^m$  is defined by an  $m \times n$  matrix i.e.

$$T(v) = Av \quad \text{where } A \text{ is an } m \times n \text{ matrix with real entries.}$$

We can forget about the scalar multiplication to get examples of additive (abelian) groups.

So every linear transformation  $T: V \rightarrow W$  gives us more examples of homomorphisms of additive groups.

If  $n$  is a positive integer and  $A$  is a square  $n \times n$  matrix with integer entries then  $T: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ ,  $v \mapsto Av$  is a homomorphism.

If  $\det A = 0$  then  $A$  is not onto, not one-to-one.

If  $\det A = 2$  then  $A$  is one-to-one, but not onto.

Try  $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ ,  $\det A = 2$ ,  $A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2x \\ y \end{bmatrix}$ . We have a homomorphism  $\mathbb{Z}^2 \rightarrow \mathbb{Z}^2$

which is one-to-one but not onto.

If  $A \begin{bmatrix} x \\ y \end{bmatrix} = A \begin{bmatrix} x' \\ y' \end{bmatrix}$  then  $\begin{bmatrix} 2x \\ y \end{bmatrix} = \begin{bmatrix} 2x' \\ y' \end{bmatrix}$  so  $x = x'$ ,  $y = y'$ .

But there is no  $\begin{bmatrix} x \\ y \end{bmatrix}$  such that  $A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \end{bmatrix}$  since  $2x = 3$ ,  $y = 5$  has no solution in  $\mathbb{Z}^2$ .

Eg.  $F = \mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$  where  $p$  is a prime  
(finite field of order  $p$ ).

Take  $n=2$  and consider the vector space  $V = F^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in F \right\}$ ,  
an additive abelian group of order  $p^2$ .

Every homomorphism  $V \rightarrow V$  is a linear transformation over the field  $F$ .

If  $T: V \rightarrow V$  is a homomorphism then  $T(v+w) = T(v) + T(w)$ .

$$T(2v) = T(v+v) = T(v) + T(v) = 2T(v)$$

$$T(3v) = T(2v+v) = T(2v) + T(v) = 2T(v) + T(v) = 3T(v)$$

In fact  $T(kv) = kT(v)$  for all  $k \in \mathbb{F}_p$ .

So  $Tv = Av$  for some  $2 \times 2$  matrix  $A$  over  $F$ .

There are exactly  $p^4$  homomorphisms  $V \rightarrow V$ .

How many of these  $p^4$  homomorphisms are automorphisms of  $V$ ?

$$(p^2-1)(p^2-p) = |GL_2(F)|$$

The Klein four-group (any group of order 4 which is not cyclic)

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

eg.  $G \cong \{1, 3, 5, 7\}$  under multiplication mod 8

or  $\langle (12)(34), (13)(24) \rangle < S_4$

$$= \{(), (12)(34), (13)(24), (14)(23)\}$$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1