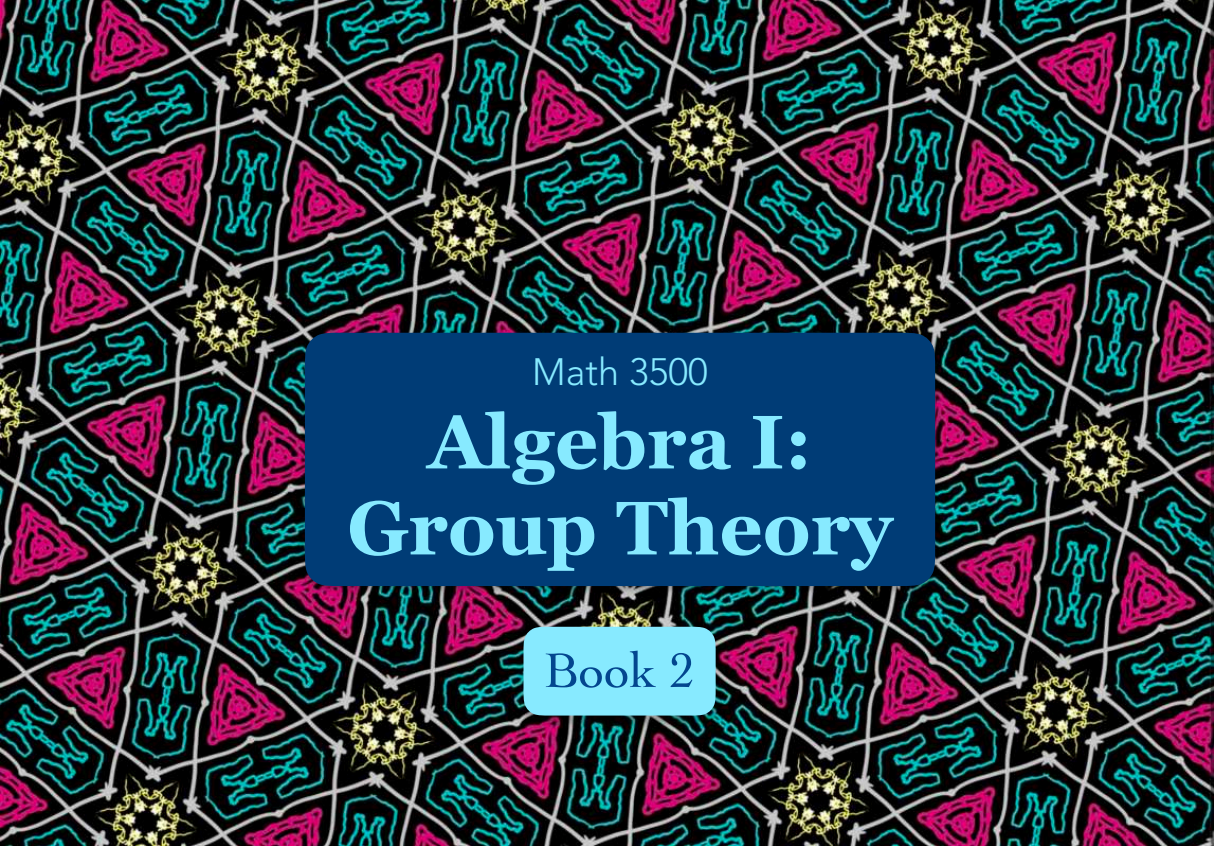

Math 3500
Algebra I:
Group Theory
Book 2

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

1 element of order 1: $()$ = identity

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

$(12)(34), (13)(24), (14)(23)$ ← $\frac{1}{2!}\binom{4}{2}\binom{2}{2} = \frac{6}{2} = 3$

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

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

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

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

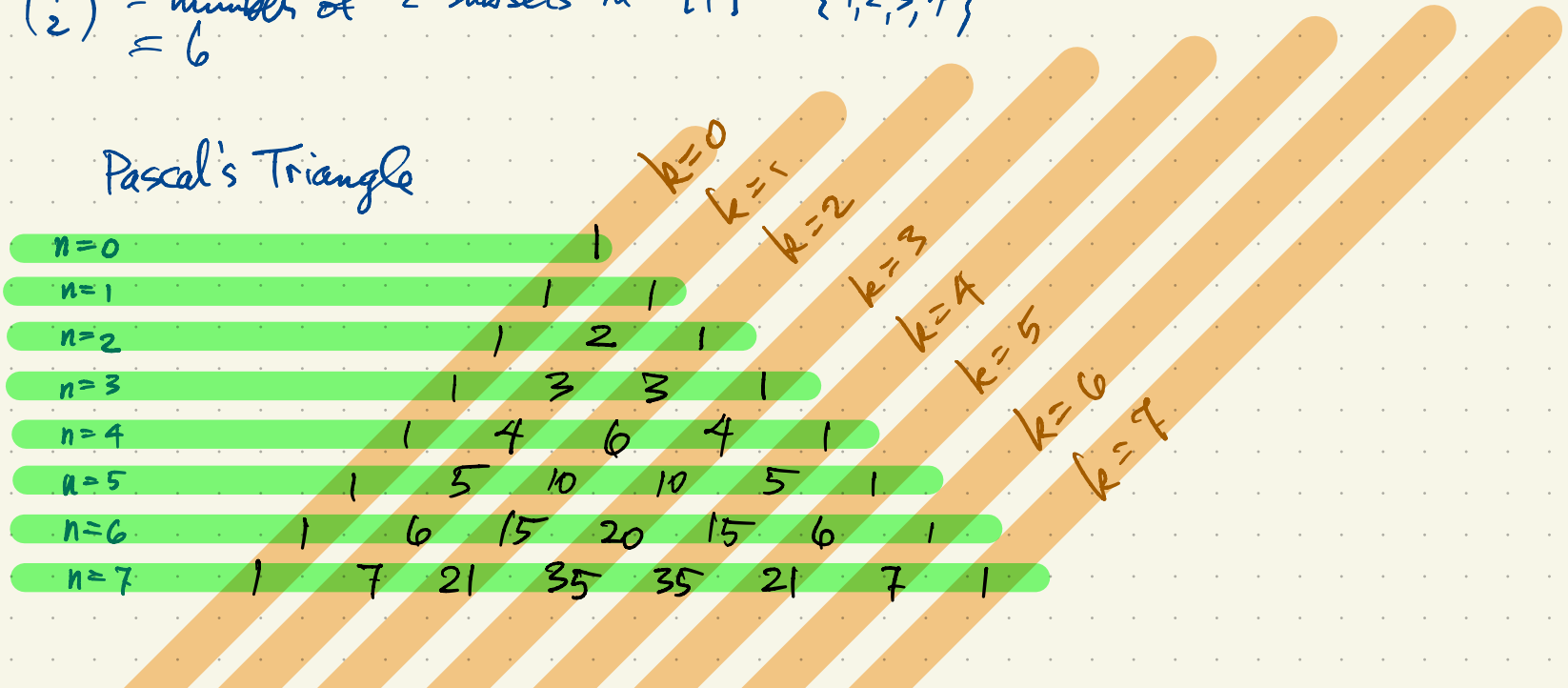
The binomial coefficient $\binom{n}{k}$ ("n choose k") is the number of ways to choose a subset of size k from a set of size n.

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

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

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

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



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

Products of disjoint transpositions eg. $(1\ 3)(2\ 5)(6\ 8) \in S_8$ 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 $[7] = \{1, 2, \dots, 7\}$

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

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

Number of these is $\frac{1}{2}\underbrace{\binom{7}{2}}_{21}\underbrace{\binom{5}{2}}_{10} = 105$.

Products of three disjoint transpositions eg. $(15)(27)(36) = (15)(36)(27) = (27)(15)(36) = \dots$

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

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

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

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

$280 + 70 = 350$ elements of order 3 in S_7

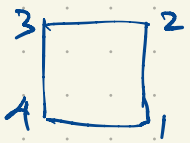
Elements of order 12 in S_7 eg. $(142)(3756)$

$70 \cdot 3! = 70 \cdot 6 = 420$ elements of order 12 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



$I \longmapsto ()$

$R \longmapsto (1234)$

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

$R^3 \longmapsto (1432)$

$H \longmapsto (12)(34)$

$V \longmapsto (14)(23)$

$D \longmapsto (13)$

$D' \longmapsto (24)$

$G \cong$ 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 $GL_n(F) = \{$ invertible $n \times n$ 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 $GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}$.

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

R: $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ $\quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -y \\ x \end{bmatrix}$ (the vector $\begin{bmatrix} x \\ y \end{bmatrix}$ rotated 90° counter-clockwise about the origin)

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

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

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

G = symmetry group of square $\cong \left\{ \underset{I}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \underset{R}{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}, \underset{R^2}{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}, \underset{R^3}{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}}, \underset{H}{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \underset{V}{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \underset{D}{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \underset{D'}{\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}} \right\}$ subgroup of $GL_2(\mathbb{R})$

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

D': $\left\langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle$

$R^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ commutes with every element of G (not so immediately obvious from the other ways of representing G).

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

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

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

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

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

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

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

2×2 matrices over F there are $3^4 = 81$ 2×2 matrices over F. $\begin{bmatrix} * & * \\ * & * \end{bmatrix}$

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

i.e. $ad - bc = 1$ or 2 i.e. $ad - bc = \pm 1$.

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

$q-1 = 8$ choices for first column to be nonzero

$q-3 = 6$ 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. $F = \mathbb{F}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Let's try $G = GL_3(F) = \{3\times 3$ matrices A over F such that $\det A \neq 0\}$ i.e. $\det A = 1$

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

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

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

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

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

- 7: $8-1$ nonzero vectors
- 6: $8-2$
- 4: $8-4$

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

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

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

$|A| = 4 =$ the order of A

Note: $4 \mid 168$

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

$$F^3 = \{\underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}}_{v_0}, \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}}_{v_1}, \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{v_2}, \underbrace{\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}}_{v_3}, \underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}}_{v_4}, \underbrace{\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}}_{v_5}, \underbrace{\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}}_{v_6}, \underbrace{\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}}_{v_7}\}$$

$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ permutes the vectors as $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ i.e. $(4217) = (1742)$

$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ i.e. (36)

$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ i.e. (5)

$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ i.e. (0)

$= (1742)(36)$

has order 4.

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

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

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

i.e. $B = (1\,6\,3\,7\,5\,4\,2)$ 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

$\| $

$GL_3(F)$

Note: If $F = \mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ (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.

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

$\mathbb{F}_7^\times = \{1,2,3,4,5,6\}$ multiplicative group of order 6

$\langle 1\rangle = \{1\}$
$\langle 2\rangle = \{1,2,4\}$
$\langle 3\rangle = \{1,3,2,6,4,5\} = \langle 5\rangle$
$\langle 4\rangle = \{1,4,2\} = \langle 2\rangle$
$\langle 5\rangle = \{1,5,4,6,2,3\}$
$\langle 6\rangle = \{1,6\}$

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

$\mathbb{Z}/6\mathbb{Z} = \{0,1,2,3,4,5\}$ 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 $(\mathbb{F}_7^\times, \times)$

defined by $\phi: \mathbb{Z}/6\mathbb{Z} \to \mathbb{F}_7^\times$

$\phi(0) = 1$
$\phi(1) = 3$
$\phi(2) = 2$
$\phi(3) = 6$
$\phi(4) = 4$
$\phi(5) = 5$

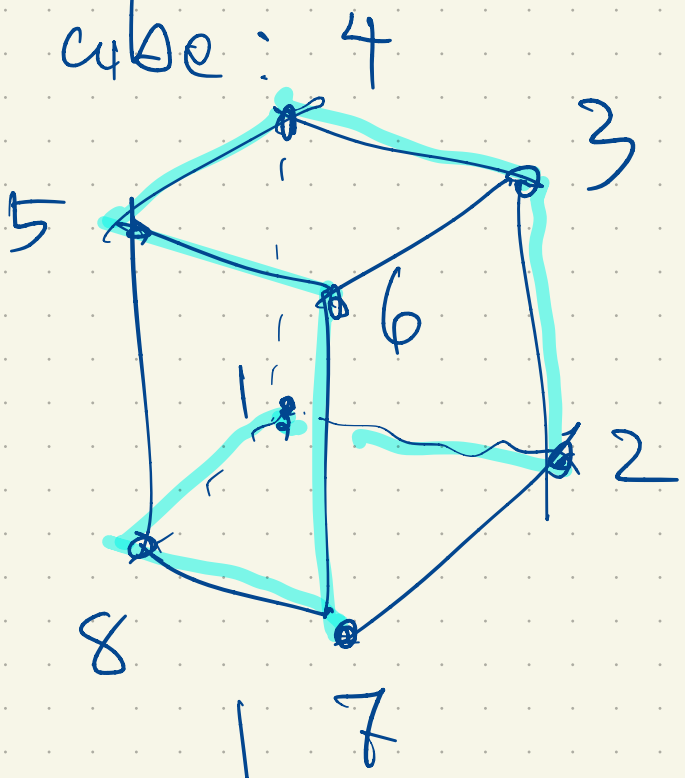
$\phi(x+y) = \phi(x)\phi(y)$

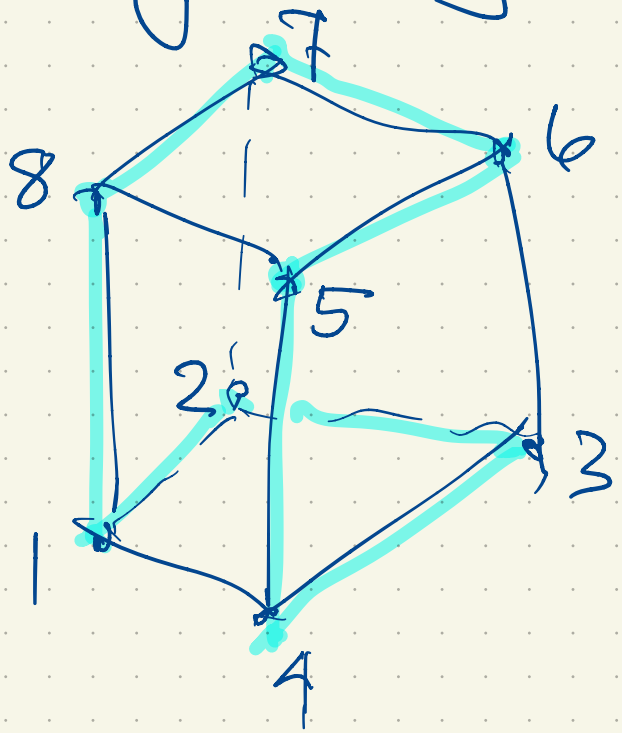
$\phi(\underbrace{1+1+\cdots+1}_{k \text{ times}}) = \underbrace{3\cdot 3\cdot\cdots\cdot 3}_{k \text{ times}}$

$\phi(k) = 3^k$

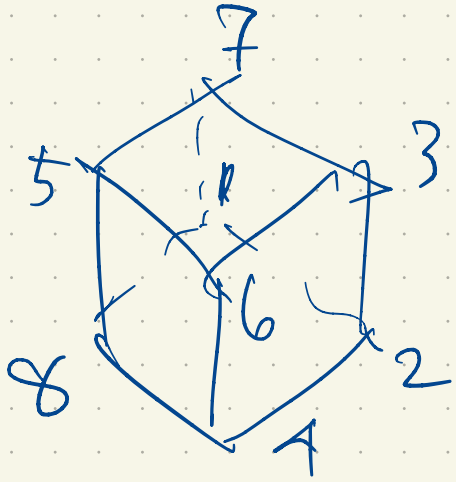
$\phi(k+l) = 3^{k+l} = 3^k \cdot 3^l = \phi(k)\phi(l)$

check that $(12365\,8)(47)$ 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 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. $(13)(12) = (123) = (14)(23)(12)(34)(24)(12)$

Σ upper case Sigma M mu

σ or s lower case sigma μ

k	σ(k)
1	2
2	3
3	1
4	4
5	5

$\sigma = (123)$

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.)

To prove the theorem, we must show is that if $\sigma = \underbrace{\tau_1 \tau_2 \tau_3 \cdots \tau_{2k+1}}_{\tau_i \text{ transpositions}}$ then $\sigma \neq \underbrace{\mu_1 \mu_2 \cdots \mu_{2l}}_{\mu_j \text{ transpositions}}$ μ_m

$() = (12)(12)$

Proof Consider the polynomial

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

$$= \prod_{1 \le i < j \le n} (x_j - x_i) \quad \text{of degree } \binom{n}{2}.$$

If $\sigma \in S_4$ 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 $(1\,2)$ we get

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

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