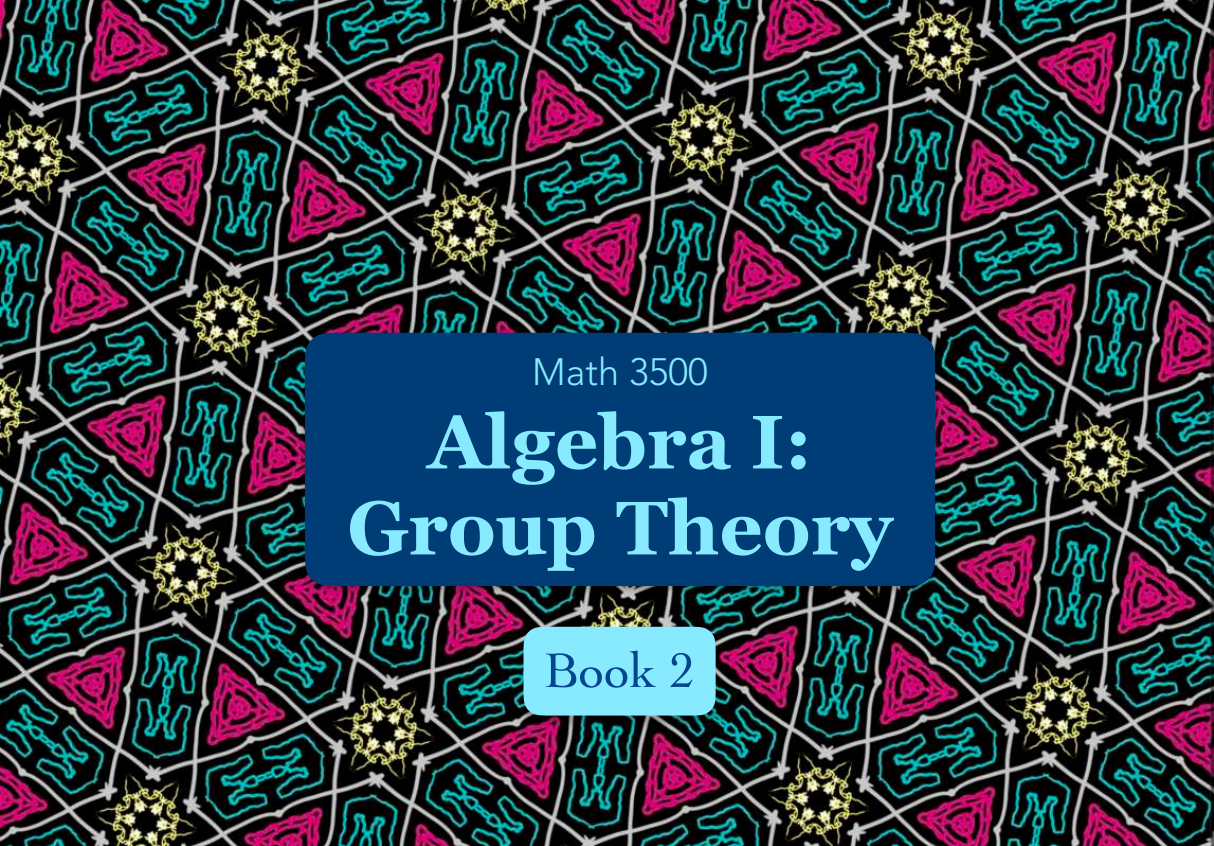

Math 3500
Algebra I:
Group Theory
Book 2

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 $(n-1)!$

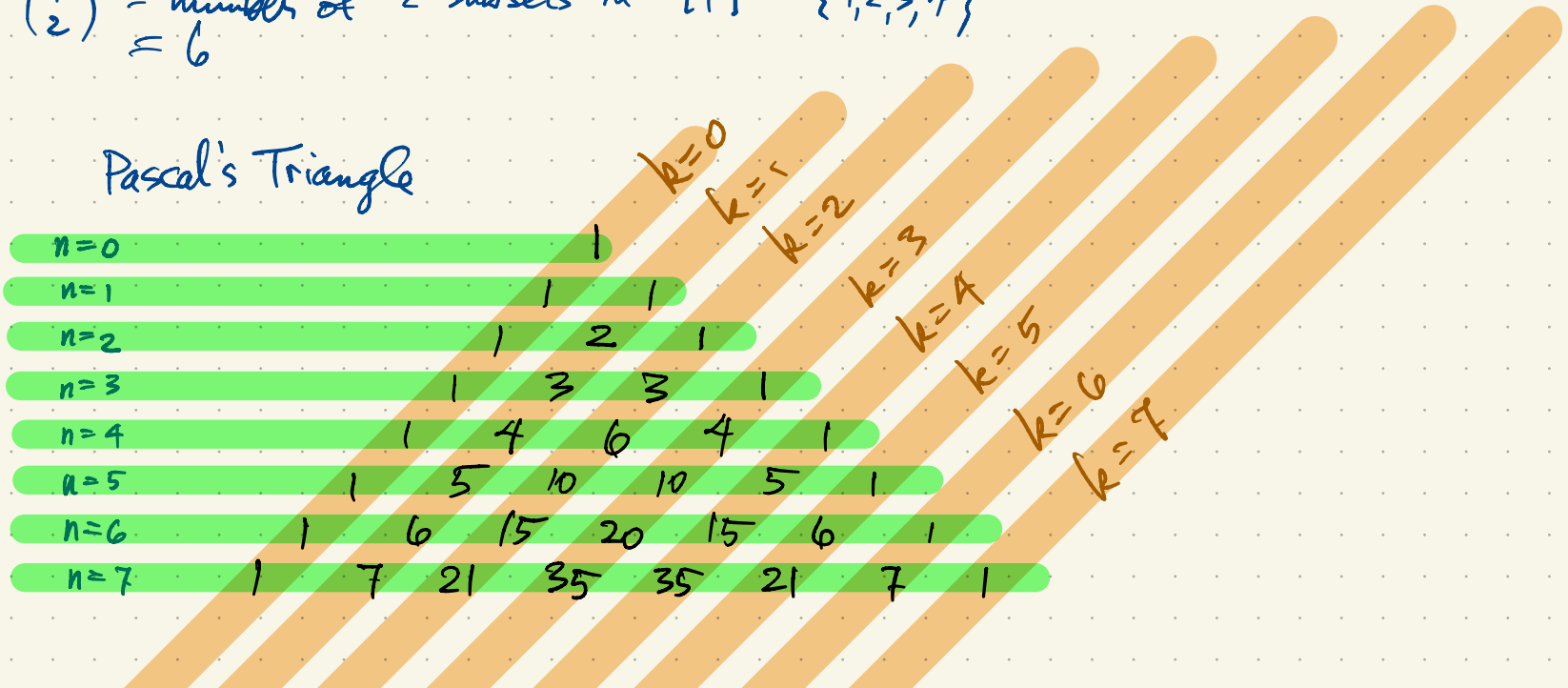
The binomial coefficient $\binom{n}{k}$ ("n choose k") is the number of ways to choose a subset of size k from a set of size n.

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

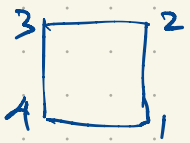
Elements of order 12 in S_7 eg. $(142)(3756)$

$70 \cdot 3! = 70 \cdot 6 = 420$ 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 $GL_2(\mathbb{R}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc \neq 0\}$.

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 $\cong \{\underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{I}, \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_{R}, \underbrace{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}_{R^2}, \underbrace{\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}}_{R^3}, \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}_{H}, \underbrace{\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}}_{V}, \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}_{D}, \underbrace{\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}}_{D'}\}$ 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. $(4217) = (1742)$

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

$\| \quad GL_3(F)$

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

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

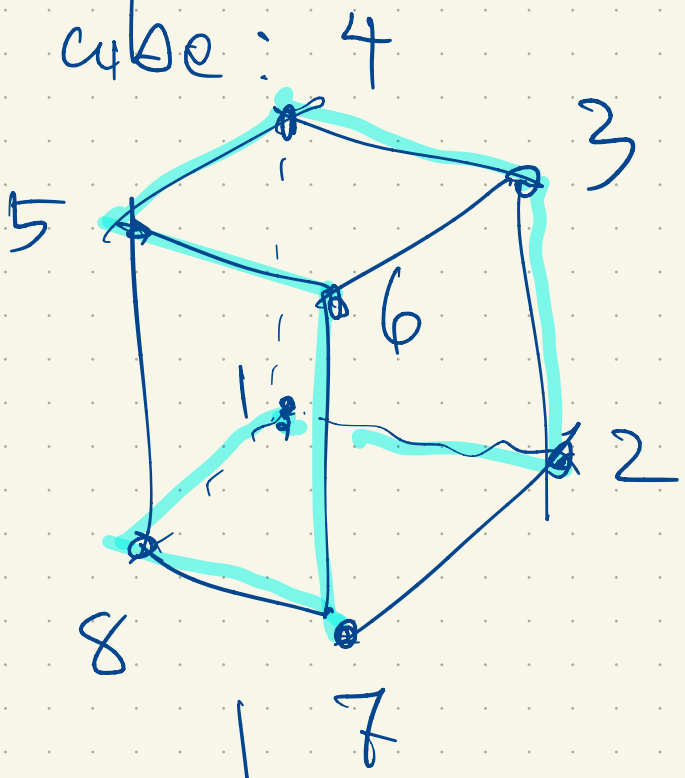
$\phi(x+y) = \phi(x)\phi(y)$

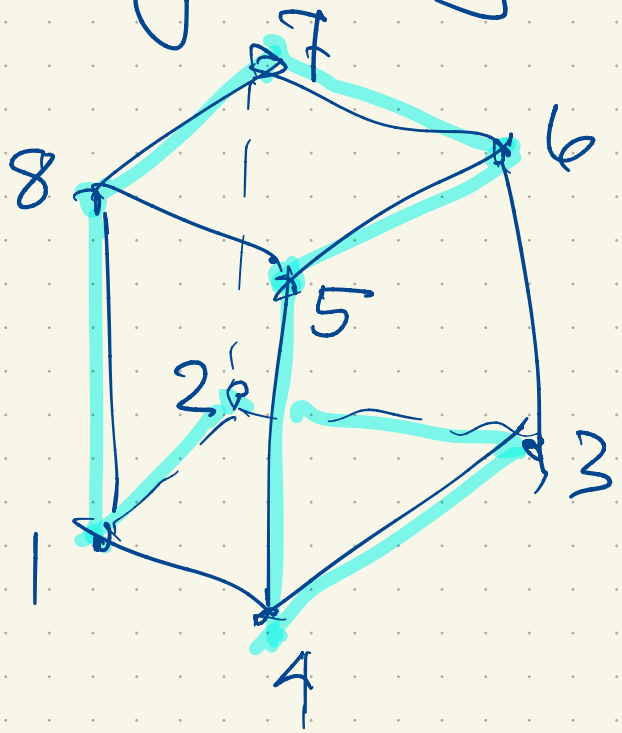
$\phi(\underbrace{1+1+\cdots+1}_{k \text{ times}}) = \underbrace{3\cdot 3\cdot\cdots\cdot 3}_{k \text{ times}}$

$\phi(k) = 3^k$

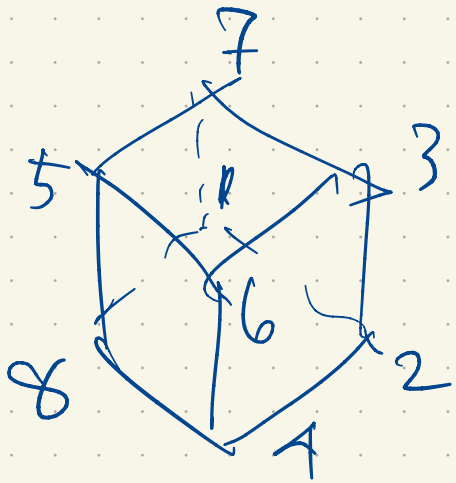
$\phi(k+l) = 3^{k+l} = 3^k \cdot 3^l = \phi(k)\phi(l)$

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 $\sigma \neq \underbrace{\mu_1 \mu_2 \cdots \mu_{2l}}_{\mu_j \text{ transpositions}}$

μm

$() = (12)(12)$

Proof Consider the polynomial

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

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

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 (12) we get

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

For (123) we get

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

$- \cdot - = +$

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

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

± 1 $\quad \pm 1 \quad \pm 1$

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

i.e. even × even = even
even × odd = odd
odd × even = odd
odd × odd = even

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

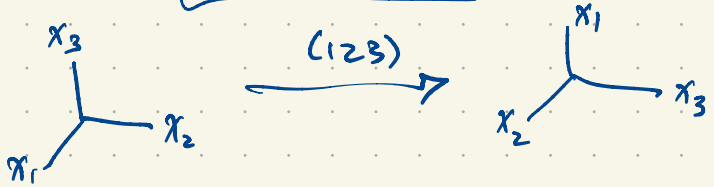
$(14)(13)(12) = (1234)$ is an odd permutation.

$(2)(13)(14) = (1432)$

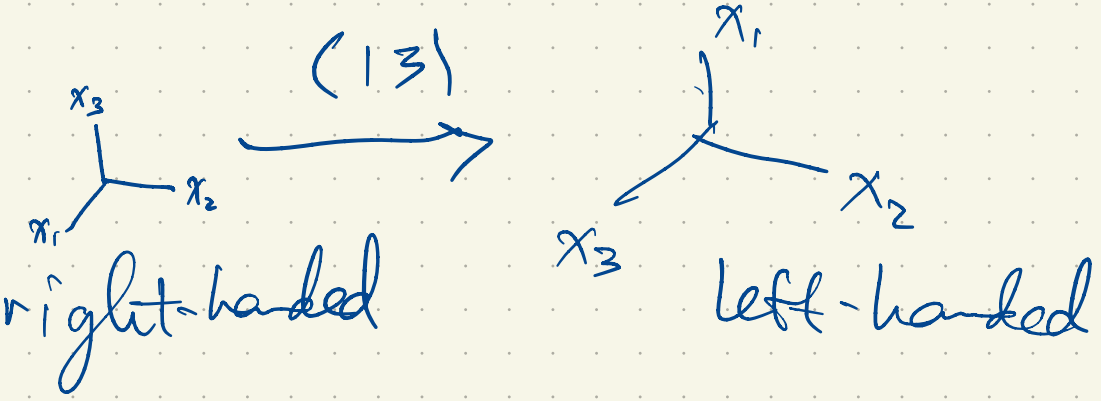
$(15764)(2389)$ is odd

(even) (odd)

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



right-handed coordinate system



right-handed left-handed

(123) preserves orientation

(13) reverses orientation

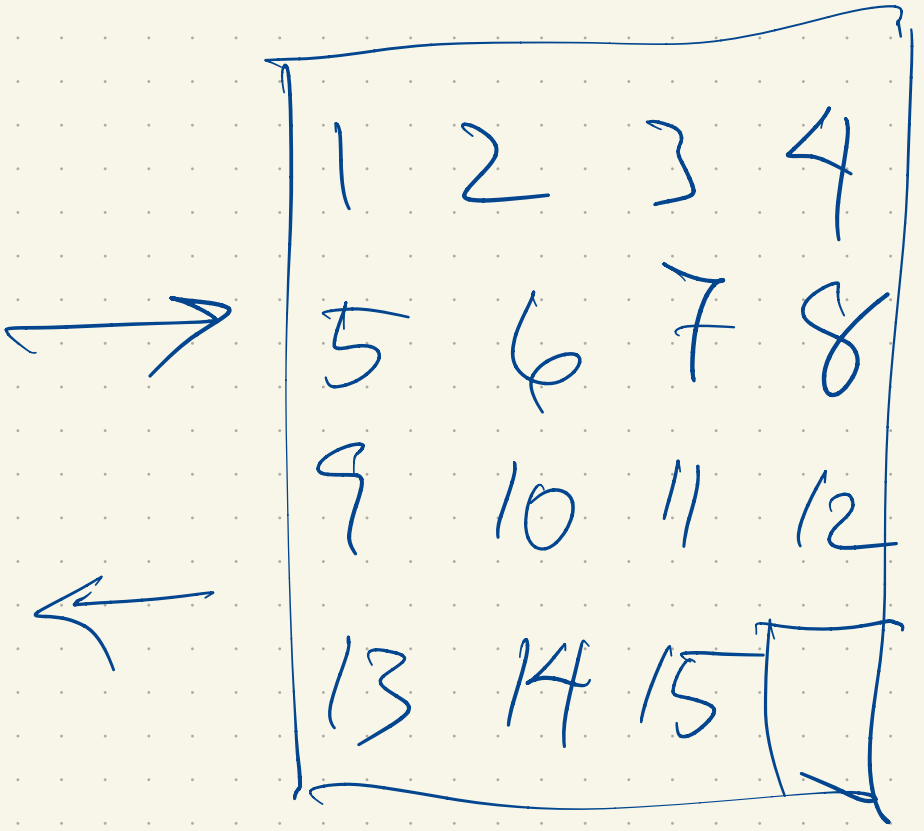
An $n \times n$ matrix $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ has determinant

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

($n!$ terms)

If $n = 3$ then

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



(11, 15, 14, 12)

(11, 12, 14, 15)

is an ~~even~~ odd permutation

$|S_n| = n!$

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

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

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

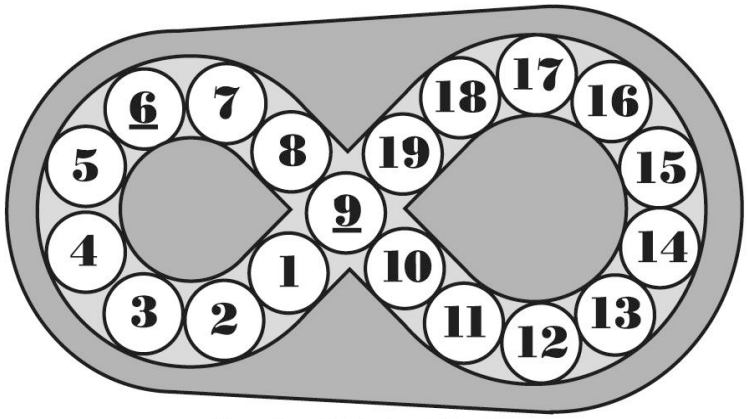
For $n=4$, $S_4 = \{(), (12), (13), (14), (23), (24), (34), (1234), (1243), (1324), (1342), (1423), (1432),$
$(123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$

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

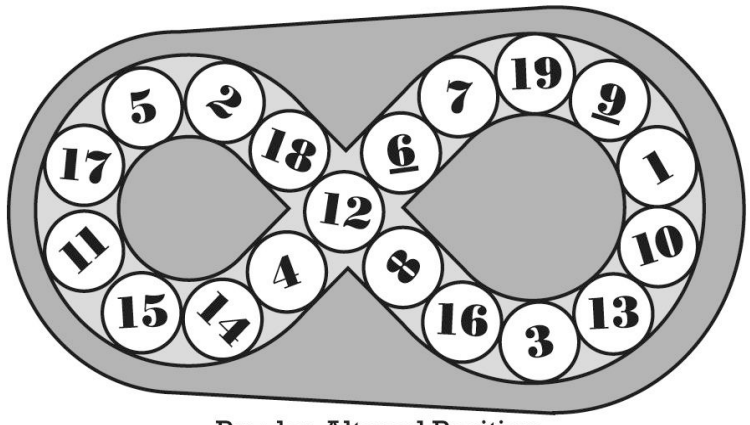
$|S_4| = 24$

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_{19}:

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

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

Warming up to Lagrange's Theorem:

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

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

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

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

C_{12} has 6 subgroups:

$C_{12} = \langle g \rangle = \{1, g, g^2, \cdots, g^{11}\}$ of order 12

(trivial subgroup) $\langle 1 \rangle = \{1\}$ 1

$\langle g^{12} \rangle$

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

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

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

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

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.

$\langle g^4, g^6 \rangle = \langle g^2 \rangle$ since $\langle g^4, g^6 \rangle \subseteq \langle g^2 \rangle$ and $\langle g^2 \rangle \subseteq \langle g^4, g^6 \rangle$

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

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

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

$\langle g^5 \rangle = \{1, g^5, g^{10}, g^3, g^8, g, g^6, g^{11}, g^4, g^9, g^2, g^7\} = \langle g \rangle$

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

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

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is an additive cyclic group

negative integers | zero | positive integers

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

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

divisibility is a relation between two integers

Note: vertical bar, not division

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

$17 \mid 17$

$17 \mid 0$ since $0 = 0 \times 17$

$-3 \mid 12$ since $12 = (-4) \times (-3)$

$0 \mid 0$ 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 $\pm 1, \pm 7$.

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

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

$-6 \mid -12$ since $-12 = 2 \times (-6)$

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

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 $a|(b\pm c)$.

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.)

Theorem (Division Algorithm) there exist unique $q, r \in \mathbb{Z}$ such that $n = qd + r$, $0 \le r < d$.

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

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

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

quotient, remainder

$4 \nmid 21$

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

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

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 $5 \notin \{0, 1, 2, 3\}$.

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

$-21 = -5 \times 4 - 1$

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

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 $d \mid n$. 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

$$h = g^k = g^{qd+r} = g^{qd} g^r = (g^d)^q g^r \Rightarrow g^r \in H$$

($h \in H$; $g^d \in H$)

$$g^r = (g^{qd})^{-1} h \in H$$

($g^{qd} \in H$, $h \in H$)

$r \in \{0, 1, 2, \dots, d-1\}$ 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. $d \mid k$, $k = qd$, $h = g^k = (g^d)^q \in \langle g^d \rangle$. Thus $H \subseteq \langle g^d \rangle$ and $H = \langle g^d \rangle$.

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

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

□