SCP Intro to Group Theory March 11, 2024

Mathematicians: "Group theory is the study of algebraic structures known as groups"

Group Axioms

A group is a $\underbrace{\text{tuple}}_{\text{pair}}$ $(G, \cdot)$ of a set & binary operation satisfying:

1) Closure: $\forall a, b \in G,\ a \cdot b \in G$

2) Associativity: $\forall a, b, c \in G,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) Identity: $\exists!\, e \in G$ s.t. $\forall a \in G,\ a \cdot e = e \cdot a = a$

4) Inverse: $\forall a \in G,\ \exists\, b \in G$ s.t. $a \cdot b = b \cdot a = e$

Bonus: if $\forall a, b \in G,\ a \cdot b = b \cdot a$ the group is called "Abelian" else "Non-Abelian"

Ex 1. $(\mathbb{Z}, +)$ set of integers under addition $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

1) $a + b = c,\ c \in \mathbb{Z},\ \forall a, b \in \mathbb{Z}$
2) $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}$
3) $0 + a = a + 0 \quad \forall a \in \mathbb{Z}$
4) $a + (-a) = (-a) + a = 0 \quad \forall a, -a \in \mathbb{Z}$

$(\mathbb{Z}, +)$ is a group! it is also Abelian

Ex. 2 $(\mathbb{Z}, -)$ set of integers under subtraction

1) $a - b = c,\ c \in \mathbb{Z},\ \forall a, b \in \mathbb{Z}$
2) $a - (b - c) \stackrel{?}{=} (a - b) - c \quad \forall a, b, c \in \mathbb{Z}$

$3 - \underbrace{(2-1)}_{3 - 1} = 2 \qquad \underbrace{(3-2)}_{1} \underbrace{-1}_{-1} = 0$

Not a group!

Try $(\mathbb{Z}, \times)$ integers under mult.

Let's consider the permutation of three numbers.

$P(3)$: $3! \longrightarrow 6$ total permutations

$(1,2,3)$ $(1,3,2)$ $(3,2,1)$

$(2,1,3)$ $(3,1,2)$ $(2,3,1)$

Let's assign labels to these permutations:

$$e = \begin{array}{c} \begin{matrix} x & y & z \end{matrix} \\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \\ \begin{matrix} x & y & z \end{matrix} \end{array}$$

e rep. "identity" here

no change

let x, y, z be the "labels" and turn red if an element doesn't match its initial position

$$d : \begin{array}{c} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \begin{matrix} z & x & y \end{matrix} \end{array} \qquad f : \begin{array}{c} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \begin{matrix} y & z & x \end{matrix} \end{array}$$

$$a : \begin{array}{c} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\ \begin{matrix} x & z & y \end{matrix} \end{array} \qquad b = \begin{array}{c} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ \begin{matrix} z & y & x \end{matrix} \end{array} \qquad c : \begin{array}{c} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\ \begin{matrix} y & x & z \end{matrix} \end{array}$$

Now, if $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ is the "basis," how would you construct a matrix to represent each permutation?

$$e : M(e) \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \longrightarrow M(e) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

the identity rep is straightforward

$$d : M(d) \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix} \longrightarrow M(d) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$M(d) = C_3 = 120^\circ$ counterclock

$$f : M(f) \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} \longrightarrow M(f) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$M(f) = C_3^2 = C_3^{-1} = 120^\circ$ clockwise

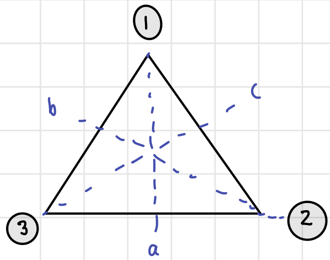
$$a : M(a) \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix} \longrightarrow M(a) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

b: $M(b)\begin{bmatrix}1\\2\\3\end{bmatrix} = \begin{bmatrix}3\\2\\1\end{bmatrix} \longrightarrow M(b) = \begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$

c: $M(c)\begin{bmatrix}1\\2\\3\end{bmatrix} = \begin{bmatrix}2\\1\\3\end{bmatrix} \longrightarrow M(c) = \begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$

How about the symmetry operations of an equilateral triangle?

Symmetry: a transformation that preserves distances and the object



6 total as well!

- E
- 2-fold rotation (mirror plane) about a, b, c
- 3-fold rotation about vertical axis out of page by $\frac{2\pi}{3}$, $\frac{4\pi}{3} = -\frac{2\pi}{3}$

E: $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \rightarrow \begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix}$ identity

D: $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \rightarrow \begin{smallmatrix} & 2 & \\ 1 & & 3\end{smallmatrix}$
$2\pi/3$ counter clock

F: $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \rightarrow \begin{smallmatrix} & 3 & \\ 2 & & 1\end{smallmatrix}$
$4\pi/3$ = counterclock or $\frac{2\pi}{3}$ clock

A: $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \rightarrow \begin{smallmatrix} & 1 & \\ 2 & & 3\end{smallmatrix}$
reflection about a

B: $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \rightarrow \begin{smallmatrix} & 3 & \\ 1 & & 2\end{smallmatrix}$
reflection about b

C: $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \rightarrow \begin{smallmatrix} & 2 & \\ 3 & & 1\end{smallmatrix}$
reflection about c

Note. A, B, C, D, E, F represent a sym op. / permutation <u>and</u> a final condition

Ex. D^2 $\begin{smallmatrix} & 1 & \\ 3 & & 2\end{smallmatrix} \xrightarrow{D} \begin{smallmatrix} & 2 & \\ 1 & & 3\end{smallmatrix} \xrightarrow{D} \begin{smallmatrix} & 3 & \\ 2 & & 1\end{smallmatrix} = F$

Mult. Table of P(3)

From "Applications of Group Theory to the Physics of Solids" by Dresselhaus why has the operations defined differently, but the relationships hold true

	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	E	D	F	B^2	C
B	B	F	E	D	C	A
C	C	D	F	E	A	B
D	D	C^1	A	B	F	E
F	F	B	C	A	E	D

→ 1 Table defined s.t. DA = C

2 Table defined s.t. AD = B

We've shown the equilateral triangle's sym. ops. and the permutation of three #'s have a one-to-one correspondence w/ each other (they are isomorphic), and both form groups

For symmetry operations of something complex like a crystal, it's tough to visualize repeated sym. ops. but let's suppose the sym. ops. are elements of a group.

If we can relate each element w/ a matrix that obeys the mult. table in the same way the elements obey it

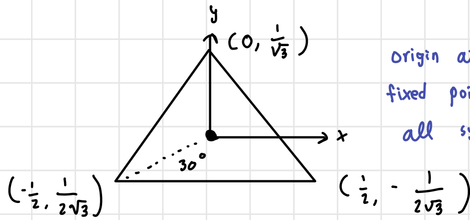
i.e. $DA = C \longrightarrow M(D)\,M(A) = M(C)$

i.e. $AD = B \longrightarrow M(A)\,M(D) = M(B)$

then we can carry out all sym. ops. arithmetically via matrix mult.

Representation: one-to-one identification of a generalized sym. op. w/ a matrix

Let the length of each side equal 1



origin at the fixed point under all sym. ops.

matrix rep: basis is $\{\vec{x}, \vec{y}\}$

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2-fold: A, B, C

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$ switch x-coords

$$B = AD = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$C = AF = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

3-fold: D F

$$D = \begin{pmatrix} -1/2 & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \qquad F = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

↺ counter-clock where $\theta = 120°$

These matrices $\{E, A, B, C, D, F\}$ constitute a matrix representation of the group that is isomorphic to P(3) and the sym. ops. of an equilateral triangle

Let's return to the 3x3 matrices we constructed to represent the permutation of three numbers, $P(3)$

$$\{M(e), M(a), M(b), M(c), M(d), M(f)\}$$

We can use similarity transformations to produce irreducible representations Γ_i which is the stepping stone we need to create a "character table"

General form of similarity transformation:

$$A' = P^{-1} A P$$

"A prime"

where A, A' are similar matrices ; P a change of basis matrix

* similar matrices represent the same linear map under (possibly) different bases *

Phrased another way, similar matrices roughly do the same thing in diff. coord. systems.

This idea is useful since we can find P^{-1}, P to block diagonalize matrices

$$A' = \begin{bmatrix} A_1 & & 0 \\ & A_2 & \\ 0 & & A_3 \end{bmatrix}$$

where there are square matrices along the diagonal and 0 everywhere else

Note. A_i obeys same mult. properties as A; same for B_i C_i D_i E_i F_i

if A' cannot be further block diagonalized, it's called an "irreducible representation"

It turns out:

$$P = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{6}} & 0 \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \qquad P^{-1} = \begin{bmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ \frac{2}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

prove to be just right for the job

$$P^{-1} M(d) P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

we recovered D from M(d)

$$P^{-1} M(f) P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

we have F!

$$P^{-1} M(a) P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$P^{-1} M(b) P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$P^{-1} M(c) P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$$P^{-1} M(e) P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Basic Definitions:

h = order

① Order of Group ≡ # of elements in G e.g. order of $P(3)$, $h = 6$

② subgroup ≡ a collection of elements in G that form a group themselves

e.g. for $P(3)$: $\{E\}$, $\{E, D, F\}$, $\{E, A\}$, $\{E, B\}$, $\{E, C\}$

③ order of an element ≡ smallest value of n in the relation $X^n = E$

e.g. $P(3)$: $\underbrace{E^1 = E}_{1}$; $\underbrace{A^2 = B^2 = C^2 = E}_{2}$; $\underbrace{D^3 = F^3 = E}_{3}$

④ Conjugation & Class

an element B conjugate A is defined by

$$B \equiv X A X^{-1} \quad \text{where } X \in G$$

can say B is the similarity transform of A by X

e.g. $P(3)$: $ABA^{-1} = A(BA) = AF = C$ $\therefore$ B conjugate to C

$A = A^{-1} = A$ reflection is its own inverse

$CBC^{-1} = C(BC) = CD = A$ $\therefore$ B conjugate to A

$C = C^{-1} = C$

$DBD^{-1} = D(BF) = DA = C$ $\therefore$ B conjugate to C

$D^{-1} = F$

$FBF^{-1} = F(BD) = FC = A$ $\therefore$ B only conj. to A, C

$\{A, B, C\}$ all conj. to each other

Class is the totality of elem. which can be obtained from a given group element by conjugation

$AFA^{-1} = A(FA) = AB = D$ $\quad$ $BFB^{-1} = B(FB) = BC = D$

$CFC^{-1} = C(FC) = CA = D$ $\quad$ $DFD^{-1} = D(FF) = DF^2 = D^2 = F$

Three obvious classes are $\{E\}$, $\underbrace{\{A, B, C\}}_{\text{2-fold sym.}}$, $\underbrace{\{D, F\}}_{\text{3-fold sym.}}$

order = 3 $\quad$ order = 2

- Properties of a conjugate:

① if A conj. w/ B:

Proof: $A = X^{-1}BX \implies XAX^{-1} = X(X^{-1}BX)X^{-1} = B$

and $B = Y^{-1}AY$ which works b/c by def, inverses are unique

② if A is conjugate w/ B & C then B & C are conj. to each other

Proof: for the reader

Characters of conjugate matrices:

Character $\equiv \chi$ $\quad$ if $A = \begin{bmatrix} a_{11} & a_{12} & \cdots \\ a_{21} & a_{22} & \\ \vdots & & \ddots \end{bmatrix}$

$$\chi(A) = \sum_j a_{jj} = Tr(A)$$

Behaviors of χ:

① if $C = AB$ & $D = BA \rightarrow \chi(C) = \chi(D)$

Proof: $\chi(C) = \sum_j c_{jj} = \sum_j \sum_k a_{jk} b_{kj}$

$\chi(D) = \sum_k d_{kk} = \sum_k \sum_j b_{kj} a_{jk} = \sum_j \sum_k a_{jk} b_{kj} = \chi(C)$

scalar so switch is ok

(2) Conjugate Matrices have identical characters

Let $C = X^{-1} A X$

$$\chi(C) = \chi\left((X^{-1}A)X\right) = \chi\left(X(X^{-1}A)\right) = \chi(A)$$

$$\underbrace{\chi(E) = 2}_{Tr(E) = 2} \qquad \underbrace{\chi(\{A, B, C\}) = 0}_{Tr(\{A,B,C\}) = 0} \qquad \underbrace{\chi(\{D, F\}) = -1}_{Tr(\{D,F\}) = -1}$$

Character Table: 2D chart of irr. reps. of each "point group" w/ their character

- describes how a basis transforms for the given sym. ops.

C_{3v}	E	$\underbrace{2C_3}_{\{D,F\}}$	$\underbrace{3\sigma_v}_{\{A,B,C\}}$
Γ_1	1	1	1
Γ_2	2	-1	0

identity rep. which doesn't change → Γ_1

2D representation since we use 2x2 mat. → Γ_2

classes equal to # irr. representations

$\chi(E) = 2$ $\quad \chi(\{A,B,C\}) = -1$ $\quad \chi(\{D,F\}) = 0$

$\# \Gamma \neq 3$

Is our table done? No.

C_{3v}	E	$2C_3$	3σ
Γ_1	1	1	1
Γ_1'	1		
Γ_2	2	-1	0

$Tr(1) = 1$

$Tr\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2$

for our group, $h = 6$; $l_i = \chi^{\Gamma_i}(E)$

$$h = \sum_i l_i^2 = \underbrace{1^2 + 2^2}_{\Gamma_1 + \Gamma_2} + 1^2 = 6$$

we know it must exist

i = all irr. reps

l_i = dimensionality of Γ_i

How can we figure out the character of Γ_1' C_3 and σ_v ?

C_3 = rot. by $\frac{2\pi}{3}$; σ_v = rot. by $\pi/2$

Use the following which can be proven from the Wonderful $\perp$ Theorem:

① $$\sum_R N_R \chi^{(\Gamma_i)}(R) = 0$$

is satisfied for all irr. reps. except the identity rep, Γ_1

Note. $\sum_R$ denotes a sum over classes (i.e. E, $C_2 = \sigma_v$, C_3)

Considering Γ_1' ; $1 \cdot (1) + 2 \cdot \underset{\chi(C_3)}{(a)} + 3 \cdot \underset{\chi(C_2)}{b} = 0$

An easy solution:

$$\left.\begin{array}{l} a = 1 \\ b = -1 \end{array}\right\} \longrightarrow \quad 1 \cdot 1 + 2 \cdot (1) + 3 \cdot (-1) = 0 \checkmark$$

C_{3v}	E	$2C_3$	3σ
Γ_1	1	1	1
Γ_1'	1	1	-1
Γ_2	2	-1	0

D_3 or C_{3v} point group:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} \frac{1}{2} & -\sqrt{3}/2 \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$$

$$C = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \qquad D = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \qquad F = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

$$\sum_R \chi^{\Gamma_i}(R)\, \chi^{\Gamma_j}(R) = h\, \delta_{ij}$$

Relation b/t reducible & irreducible rep.

$$\underbrace{\chi^{\Gamma}(R)}_{\text{character of red. rep. can be expressed as lin. combo of irr. rep.}} = \underbrace{\sum_j}_{\text{sum over ir. reps.}} a_j\, \chi^{\Gamma_j}(R)$$

Want to find a_j:

$$\sum_R \chi^{\Gamma_i}(R)\, \chi^{\Gamma}(R) = \sum_R \sum_j a_j \underbrace{\chi^{\Gamma_i}(R)\, \chi^{\Gamma_j}(R)}_{h\delta_{ij}}$$

$$= h a_i \qquad \therefore\ a_i = \frac{1}{h} \sum_R \chi^{\Gamma_i}(R)\, \chi^{\Gamma}(R)$$

D_3	E	$2C_3$	$3C_2$
Γ_1	1	1	1
Γ_1'	1	1	-1
Γ_2	2	-1	0
Γ_R	5	2	-1

Ex. find a_i → Γ_R

↑ turns out to correspond to d-orbitals

$$\Gamma_R(R) = \sum_i a_i\, \chi^{\Gamma_i}(R)$$

For Γ_1: $a_{\Gamma_1} = \underbrace{\frac{1}{6}}_{h=6} \{\overbrace{1}^{1E}(\underbrace{1}_{\Gamma_1} \cdot \underbrace{5}_{\Gamma_R}) + \overbrace{2}^{2C_3}(\underbrace{1}_{\Gamma_1} \cdot \underbrace{2}_{\Gamma_R}) + \overbrace{3}^{3C_2}(1 \cdot \underbrace{(-1)}_{}))\} = 1$

For Γ_1': $a_{\Gamma_1'} = \frac{1}{6}\{1(1\cdot 5) + 2(1\cdot 2) + 3(-1\cdot(-1))\} = 2$

For Γ_2: $a_{\Gamma_2} = \frac{1}{6}\{1(2\cdot 5) + 2(-1\cdot 2) + 3(0\cdot(-1))\} = 1$

so $\Gamma_R = \Gamma_1 + 2\Gamma_1' + \Gamma_2$

Group Theory in Cryptography

Fundamentally, cryptography is about "secret writing"
crypt graphy
where there are two steps:

send message → add "encryption" → recipient gets message → message "decrypted"

The procedures of encryption & decryption are contingent on a "key" so that the sender can alter their message in a systematic manner that the recipient can decrypt

Ex. Key is shift letters by two to the right s.t. $y \to a$, $z \to b$, $a \to c$ ...

"Hello" $\xrightarrow[\text{key}]{\text{apply}}$ "Jgnnq" You apply the key in reverse to decrypt

Of course, we've developed far more secure procedures to encrypt / decrypt, and the advent of the Advanced Encryption Standard (AES) made it convention to have keys of 128, 192, and the popular 256 bits

2^{128}, 2^{192}, 2^{256} are HUGE numbers so they're secure yet fast. Who wants to wait minutes to access a YouTube video?

It's important to note the sender key = receiver key, and keys in the past were shared via a codebook or by voice. How do we do this over the internet?

Need: A way for a server to send a private (secret) key over the public internet!

Solution: Key exchange which allows two parties to agree on a key without sending one using one-way functions one - way functions, per their name, are easy to have act in one way while being very difficult to undo

Analogy: Easy to mix paint together but hard to undo and find constituents

Diffie - Hellman Key Exchange: a common protocol used

General form is $B^x \bmod (M) = \text{scalar}$

Here, x is the exponent for an arbitrary base B, and mod (M) means take the remainder of $\frac{B^x}{M}$ as the final result

Ex. $B = 2 \quad x = 4 \quad M = 3 \xrightarrow{B^x} 2^4 = 16 \longrightarrow 16 \bmod (3) = 1$

Under this scheme, x is the private key while B and M are publicly known.

if P1: x & P2: y as their respective private keys, exchanging them looks as follows:

$$\text{agreed upon key} = (B^x \bmod (M))^y = (B^y \bmod (M))^x$$
$$= (B^{xy} \bmod (M)) = (B^{yx} \bmod (M))$$

this means let
$a = B^x \bmod (M)$
$a^y \bmod (M) = a'$
$b = B^y \bmod (M)$
$b^x \bmod (M) = b' = a'$

Ex. $B = 2$, $x = 4$, $y = 5$, $M = 3$

$$\left.\begin{aligned} B^x &= 2^4 = 16 \xrightarrow{\bmod (3)} 1 \xrightarrow{1^5} 1 \xrightarrow{\bmod (3)} 1 \\ B^y &= 2^5 = 32 \xrightarrow{\bmod (3)} 2 \xrightarrow{2^4} 16 \xrightarrow{\bmod (3)} 1 \end{aligned}\right\} \text{equal !}$$

$B^{xy} = 2^{5 \cdot 4} = 1048576 \xrightarrow{\bmod (3)} 1$

How is this related to group theory?

Let's define a cyclic group.

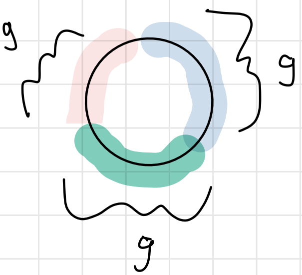
Definition. A cyclic group G is a group that can be generated by a single element $g \in G$ s.t. $\forall a \in G$, $a = g^n$ for some integer n.

Ex. Let's solely consider rotation of an equilateral triangle by 120°.

We showed that a group $\{E, D, F\}$ exists which is cyclic since each element can be "generated" from repeated mat. mult. of $M(D)$ or $M(F)$ as our binary operation. Note. there can be more than one generator in a group.

Alternatively, we could let a generator, g be $e^{\frac{2\pi i}{3}}$ and the binary operation for the group be multiplication.

$g^2 = e^{4\pi i/3}$ and $g^3 = e^{6\pi i/3} = e^{2\pi i} = \text{identity}$



We should also consider if the order matters here. Does it matter if we rotate by 120° then 240° or 240° then 120°? No!

Claim. Every cyclic group is abelian.

Proof. Let G be a cyclic group generated by $g \in G$. Suppose $x = g^m$, $y = g^n$ where $x, y \in G$, $m, n \in \mathbb{Z}$

$xy = g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$ thus $xy = yx \ \forall x, y \in G$.

All cyclic groups are therefore Abelian $\blacksquare$

As another example, the integers mod n denoted $\mathbb{Z}_n$ for $n \in \mathbb{N}$ are cyclic

Ex. $\mathbb{Z}_7$ where the generator is 1, the binary operation addition

$$1 = 1 \longrightarrow \underbrace{1+1}_{1^2} = 2 \longrightarrow \underbrace{1+1+1}_{1^3} = 3 \longrightarrow \underbrace{1+1+1+1}_{1^4} = 4 \longrightarrow \underbrace{1+1+1+1+1}_{1^5} = 5$$

1^2 in group theory notation

$$\underbrace{1+1+1+1+1+1}_{1^6} = 6 \qquad \underbrace{1+1+1+1+1+1+1}_{1^7 = e} = 0$$

Return to Diffie-Hellman:

Let g be a generator for a cyclic group G where both g and its order ($g^n = e$) are publicly known. If two want a shared key:

1) P1 selects a random integer $a \in [2, \underbrace{n-1}_{\text{n-1 to avoid e}}]$, computes g^a, then sends it to P2

2) P2 selects a random integer $b \in [2, \underbrace{n-1}_{\text{n-1 to avoid e}}]$, computes g^b, then sends it to P1

3) P1 computes $K_1 = (g^b)^a$; P2 computes $K_2 = (g^a)^b$

4) The shared key, $K_s = K_1 = K_2 \in G$

The security relies on the assumption that even if someone knew $g \in G$, and even if they saw g^a, g^b, it's computationally infeasible for someone to obtain the shared key

The above procedure is related to "the Discrete Logarithm Problem"

DLP. Let G be a cyclic group and $g \in G$ a generator. Given $h \in G$, find an integer n s.t. $g^n = h$.

if G is appropriately chosen and large enough, the DLP is considered infeasible which is why HUGE prime numbers are chosen