Math 3500

Algebra I: Group Theory

Book 1

Symmetry group of a square  :

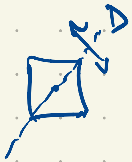
$G = \{I, R, R^2, R^3, H, V, D, D'\}$

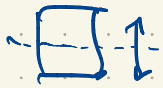
R = counter-clockwise rotation about center by 90°

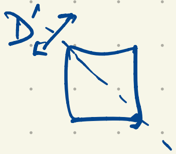
R^2 = 180° rotation about center

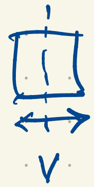
R^3 = 270° counterclockwise rotation = 90° clockwise rotation

$R^4 = I$

D = reflection 

H =  H

D' = 

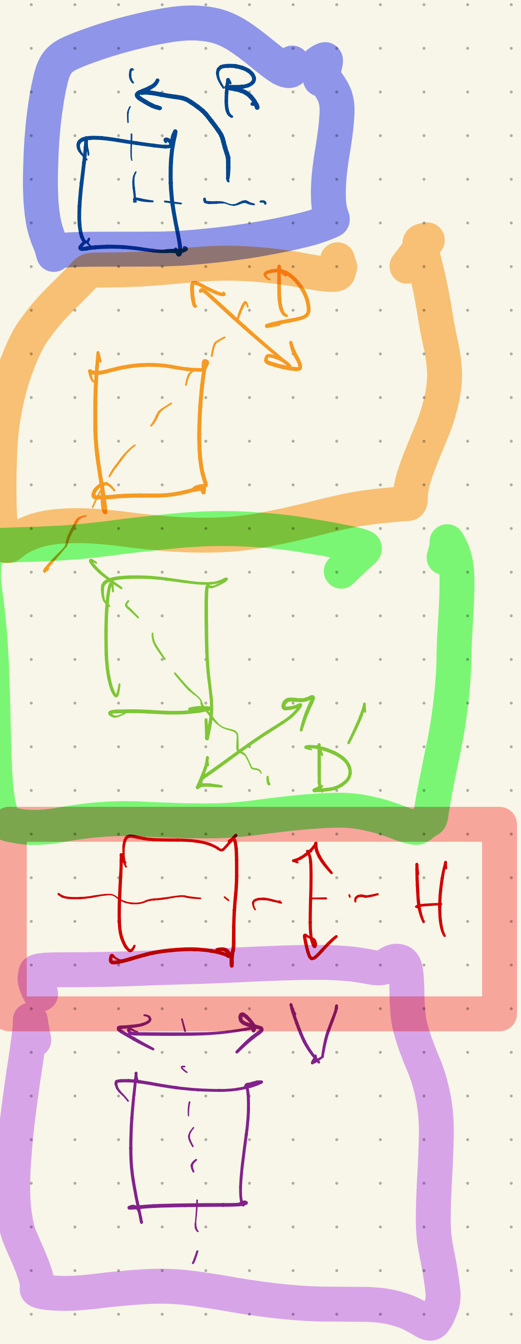
V = 

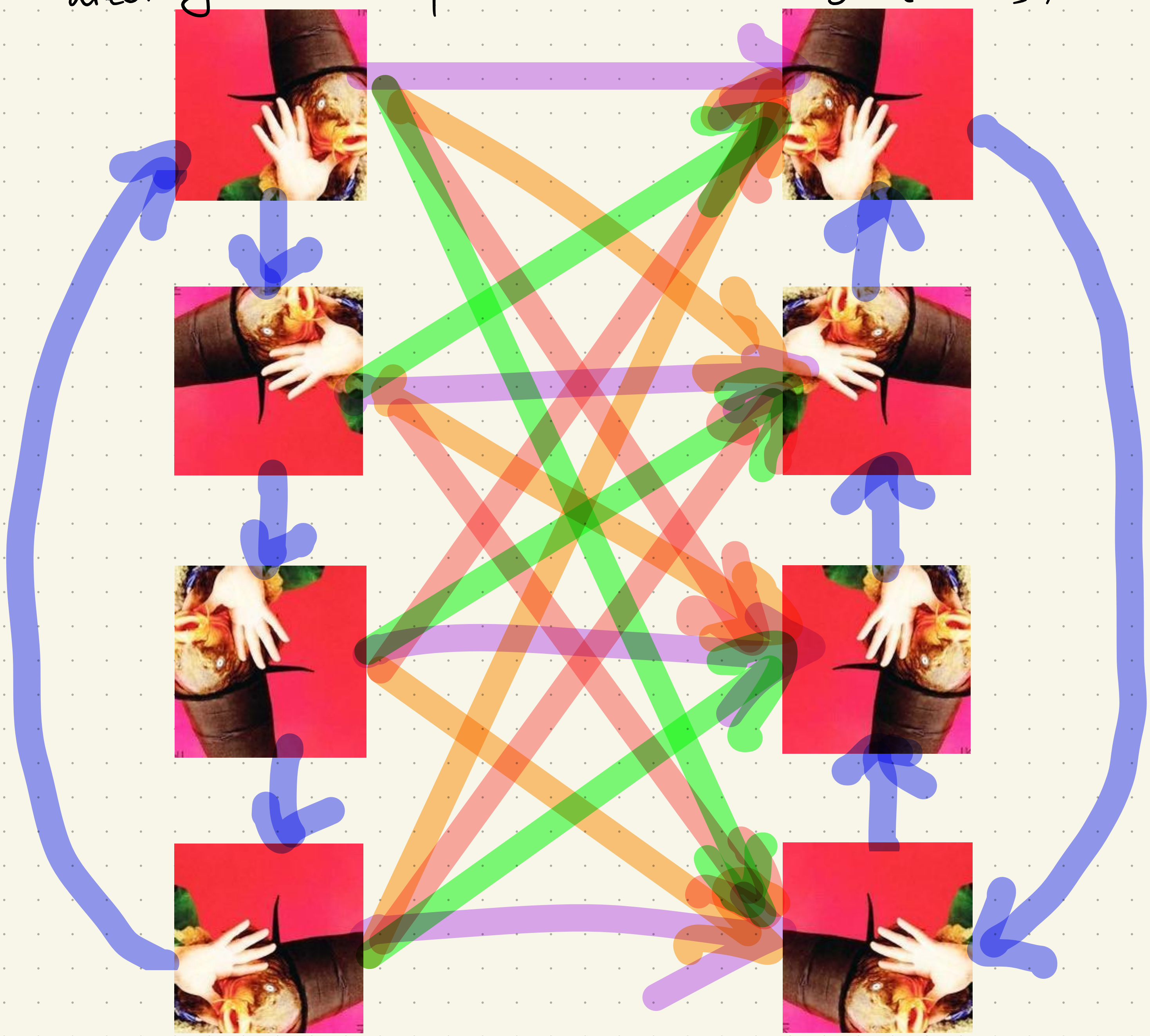
Symmetry group of square $G = \{I, R, R^2, R^3, D, D', H, V\}$

Group elements are transformations/functions/maps/mappings/arrows (not the images/squares on which the group elements act).

Virtual symmetries reverse orientation; (eg. reflections)

direct symmetries preserve orientation. (eg. rotations)





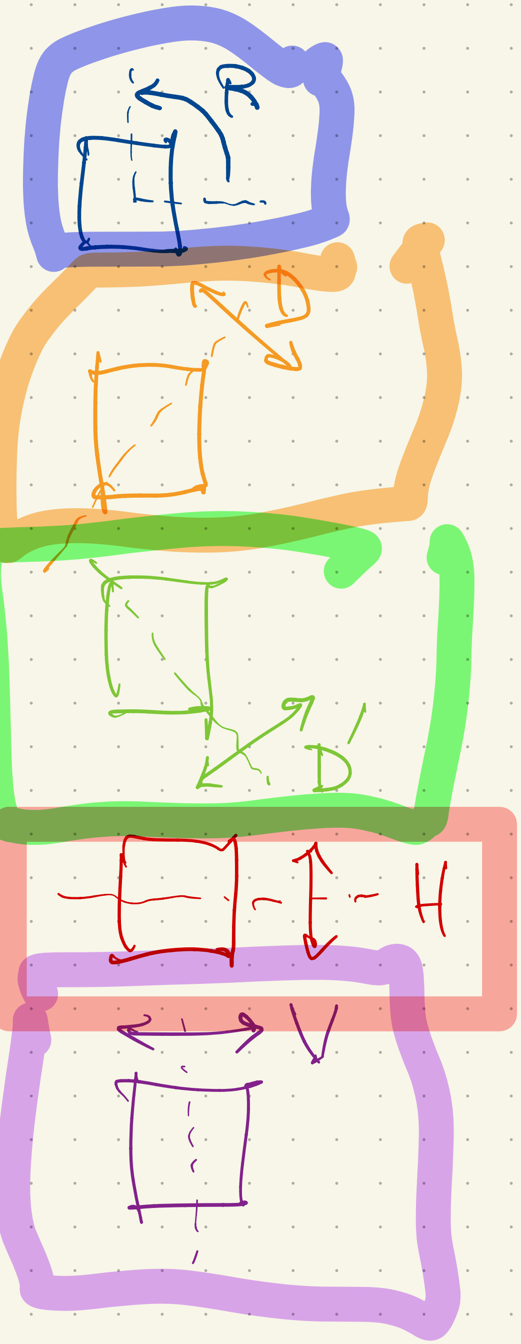
Symmetry group of square $G = \{I, R, R^2, R^3, D, D', H, V\}$

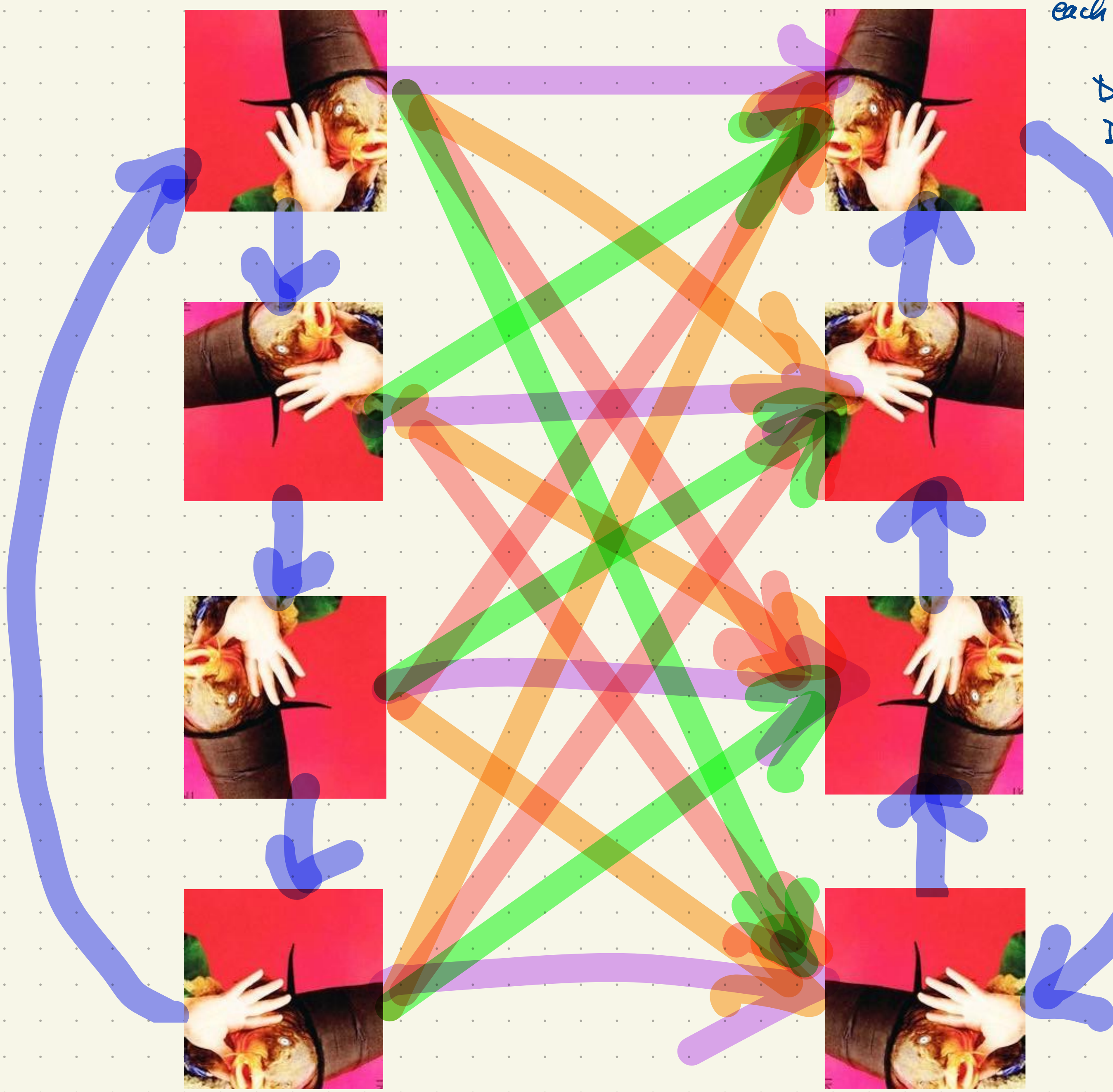
Composition (right-to-left): $RD = V$ $\quad HV = R^2$

$DR = H$ $\quad VH = R^2$

Note: H and V commute (ie. $HV = VH$) but R and D do not commute ($RD \neq DR$)

We say that G is nonabelian because its elements do not all commute with each other. (A group is abelian iff all its elements commute with each other.)





$DH = R$

$DV = R^3$

$HR = D'$

The multiplication table of G: $G = \{I, R, R^2, R^3, D, D', H, V\}$ is the dihedral group of order 8.

The order of a group G is $|G|$ = number of elements in G.

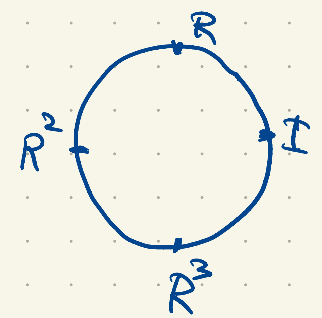
	I	R	R^2	R^3	D	D'	H	V
I	I	R	R^2	R^3	D	D'	H	V
R	R	R^2	R^3	I	V	H	D	D'
R^2	R^2	R^3	I	R	D'	D	V	H
R^3	R^3	I	R	R^2	H	V	D'	D
D	D	H	D'	V	I	R^2	R	R^3
D'	D'	V	D	H	R^2	I	R^3	R
H	H	D'	V	D	R^3	R	I	R^2
V	V	D	H	D'	R	R^3	R^2	I

G has five elements of order 2: D, D', H, V, R^2; two elements of order 4: R, R^3; one element of order 1: I.

$DR^2 = DR\cdot R = HR = D'$

$D'R^2 = D'R\cdot R = VR = D$

$\langle R\rangle = \{I, R, R^2, R^3\}$



The (i,j) entry (i.e. row i, column j) indicates the i^{th} element "times" the j^{th} element.

In the multiplication table, each group element appears exactly once in each row and column.

	T
S	U
W	U

$\Rightarrow ST = U = WT \Rightarrow ST\cdot T^{-1} = WT\cdot T^{-1} \Rightarrow S = W$

Associativity holds!

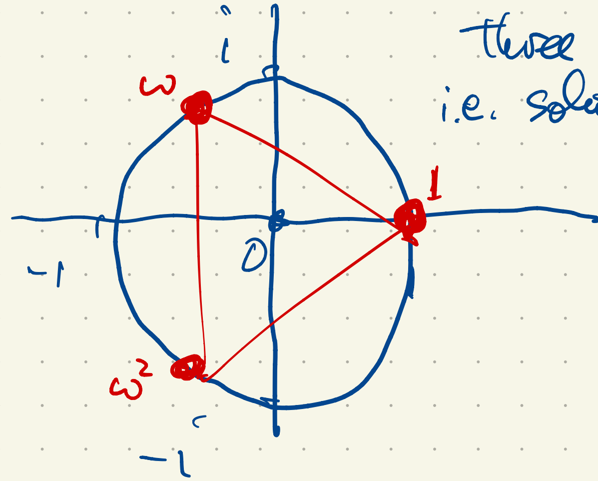
$f\circ(g\circ h) = (f\circ g)\circ h$

$f(g(h(x)))$

Eg. $\{1, \omega, \omega^2\}$, $\omega = \frac{-1+i\sqrt{3}}{2} = e^{i2\pi/3}$

omega $\neq$ w

x	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω



three cube roots of unity in $\mathbb{C}$: i.e. solutions of $x^3 = 1$, $x \in \mathbb{C}$.

$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$

$\mathbb{Q} = \{\text{rational numbers}\} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$

$\mathbb{Z} = \{\ldots -3, -2, -1, 0, 1, 2 \ldots\}$

$\{1, \omega, \omega^2\}$ is a group of order 3 having two elements of order 3: ω, ω^2 and one element of order 1: 1.

Any group of order 3 is cyclic: it must have the ~~form~~ $\{1, g, g^2\}$, $g^3 = 1$.

	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

A cyclic group is a group generated by one element i.e.

$G = \{\ldots g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\}$
$= \{g^k : k \in \mathbb{Z}\}$

i.e. consists of all powers of $g \in G$.

$\langle g \rangle$ = group generated by g
$= \{g^k : k \in \mathbb{Z}\}$

$g^k g^l = g^{k+l}$ for all $k, l \in \mathbb{Z}$

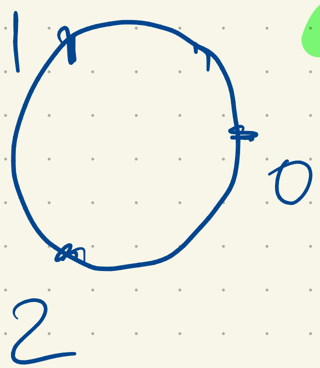
$g^0 = 1$

If $G = \{1, g, h\}$ is a group then $g^2 = h$ so $G = \{1, g, g^2\}$.
(the cyclic group of order 3).

	1	g	g^2
1	1	g	g^2
g	g	g^2	1
g^2	g^2	1	g

Note: The order of any group element $g \in G$ is $|\langle g \rangle| = |g|$

Eg. $\mathbb{Z}/3\mathbb{Z} = \{\text{integers mod } 3\} = \{0,1,2\}$ $\quad 2+2=1$ in this group with identity element 0.



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

$-1=2$
$-2=1$
$-0=0$

$1-2=2$

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

These two groups of order 3 are essentially the same as seen by their Cayley table (addition table and multiplication table respectively). More precisely, the groups $(\mathbb{Z}/3\mathbb{Z}, +)$ is isomorphic to $(\langle\omega\rangle, \times)$ i.e. $(\mathbb{Z}/3\mathbb{Z}, +) \cong (\langle\omega\rangle, *)$.

This means there is a bijection $\phi : \mathbb{Z}/3\mathbb{Z} \to \langle\omega\rangle$ satisfying $\phi(\underset{\text{addition in } \mathbb{Z}/3\mathbb{Z}}{i+j}) = \underset{\text{multiplication in } \mathbb{C} \text{ or in } \langle\omega\rangle}{\phi(i)\phi(j)}$ for all $i,j \in \mathbb{Z}/3\mathbb{Z}$.

+	j
i	$i+j$

$\longrightarrow$

×	$\phi(j)$
$\phi(i)$	$\phi(i)\phi(j)$