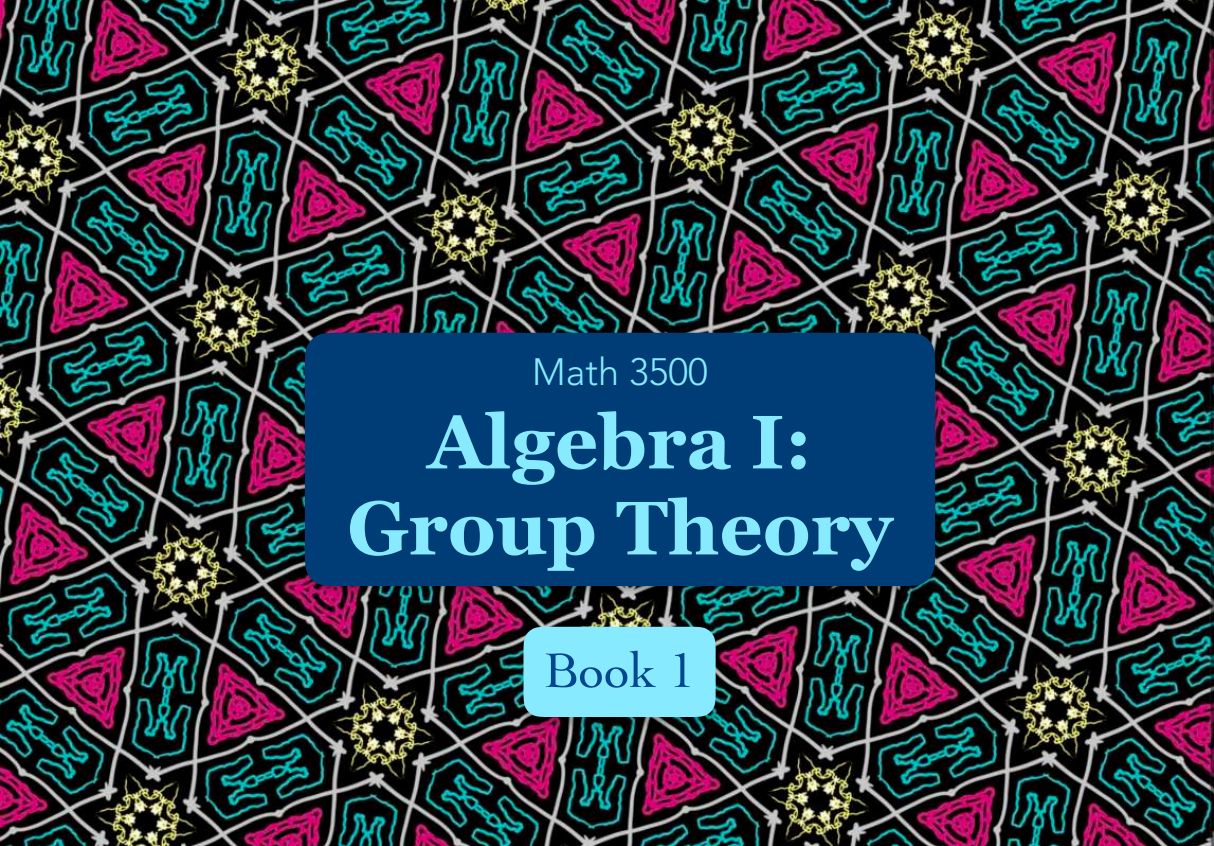




Math 3500

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°

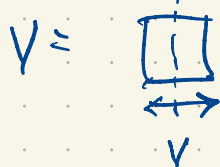
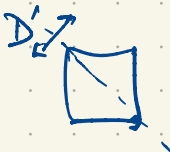
R^2 = 180° rotation about center

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

$$R^4 = I$$

D = reflection

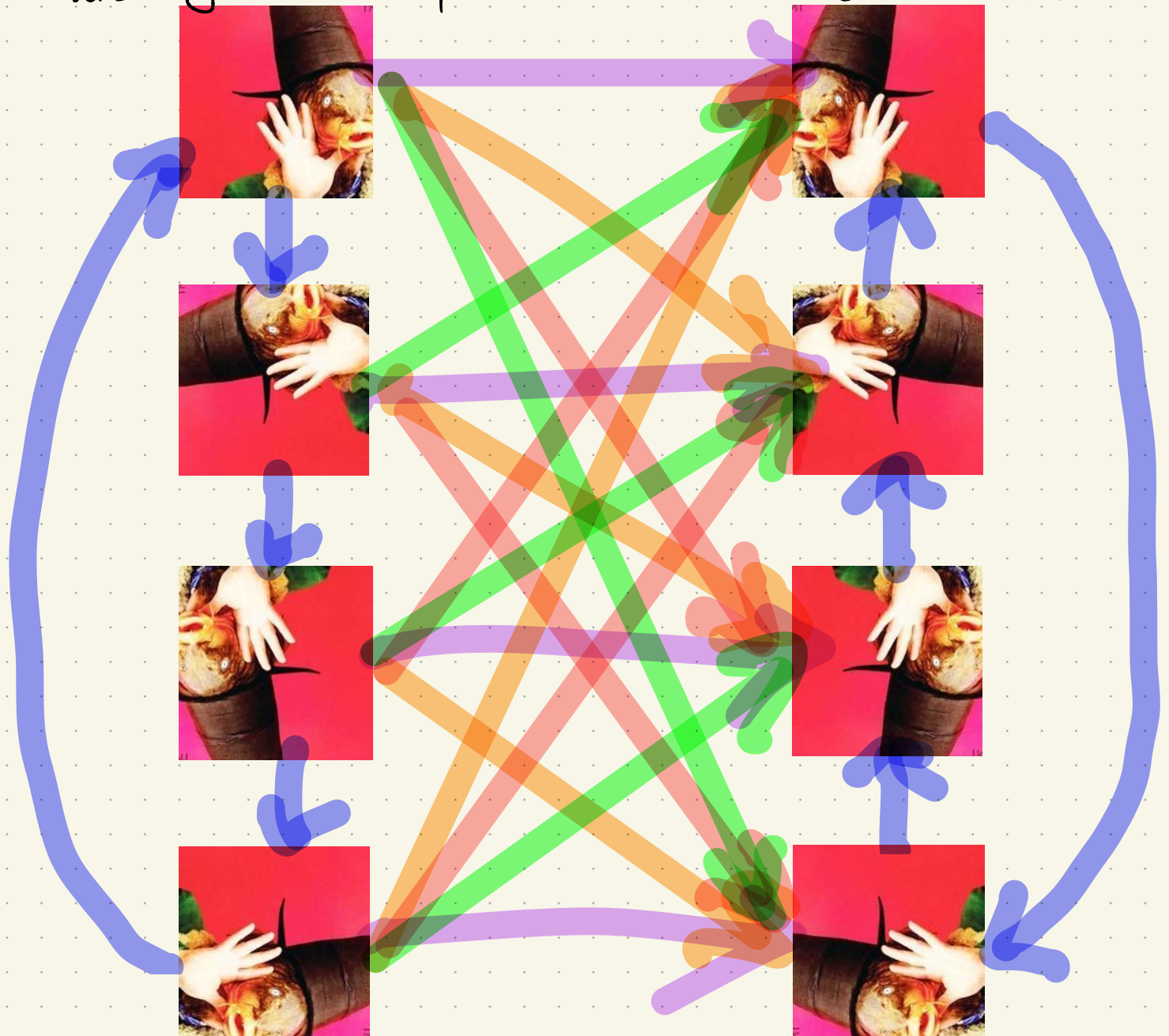
D' =



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)

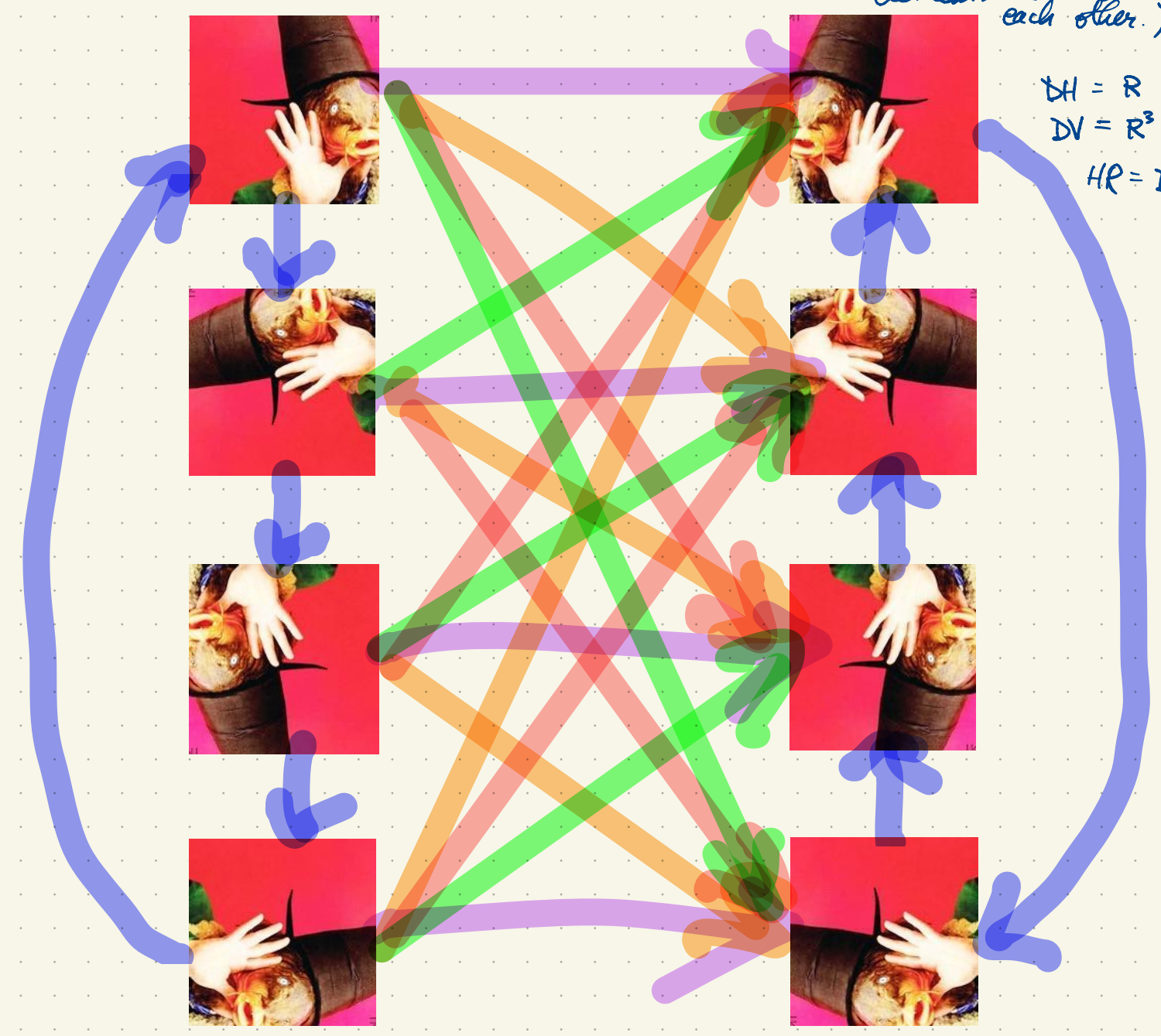


Symmetry group of square $G = \{I, R, R^2, R^3, D, D', H, V\}$

Composition (right-to-left)
 $RD = V$
 $DR = H$

$HV = R^2$
 $VH = R^2$

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 $|G| = \text{number of elements in } G$.

G has five elements of order 2:

D, D', H, V, R^2

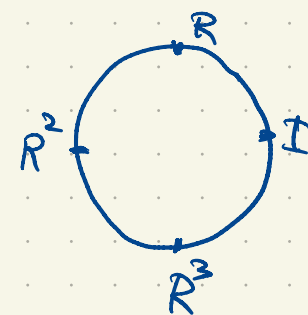
two elements of order 4: R, R^3

one element of order 1: I .

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

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

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



	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

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

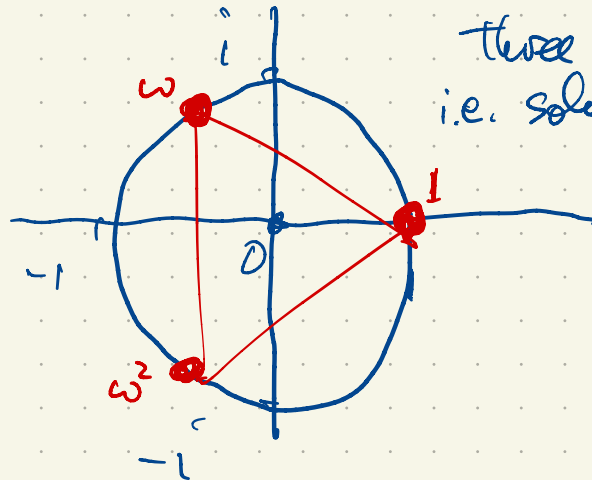
$$\Rightarrow ST = U = WT \Rightarrow \cancel{ST} \cdot \cancel{T} = \cancel{WT} \cdot \cancel{T} \Rightarrow S = W$$

Associativity holds!
 $f \circ (g \circ h) = (f \circ g) \circ h$
 $f(g(h(x)))$

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

$\omega \neq \omega^2$

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 $x^3 = 1$, $x \in \mathbb{C}$.

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

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

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

$\{1, \omega, \omega^2\}$ 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.

$$G = \{g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots\}$$

$$= \{g^k : k \in \mathbb{Z}\}$$

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

$$\langle g \rangle = \text{group generated by } g$$

$$= \{g^k : k \in \mathbb{Z}\}$$

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

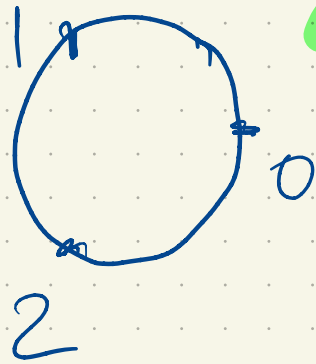
$$g^0 = 1$$

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 $|\langle g \rangle| = |g|$

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



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

$$\begin{aligned} -1 &= 2 \\ -2 &= 1 \\ -0 &= 0 \end{aligned}$$

$$1-2=2$$

$\times$	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. $(\mathbb{Z}/3\mathbb{Z}, +) \cong (\langle \omega \rangle, \times)$.

this means there is a bijection $\phi: \mathbb{Z}/3\mathbb{Z} \rightarrow \langle \omega \rangle$ satisfying $\phi(i+j) = \phi(i)\phi(j)$ for all $i, j \in \mathbb{Z}/3\mathbb{Z}$.

addition
in $\mathbb{Z}/3\mathbb{Z}$

multiplication in $\mathbb{C}$
or in $\langle \omega \rangle$.

$$\begin{array}{c|c} + & j \\ \hline i & i+j \end{array} \longrightarrow \begin{array}{c|c} \times & \phi(j) \\ \hline \phi(i) & \phi(i)\phi(j) \end{array}$$

Some infinite groups:

$(\mathbb{R}, +)$ is a group. Identity element 0. $0 + a = a$

Inverses: inverse of $a \in \mathbb{R}$ is $-a$ since $a + (-a) = 0$

Associativity: $(a+b)+c = a+(b+c)$

(By the way, in this group, the identity 0 has order 1; every nonidentity element has infinite order. This group is abelian since $a+b = b+a$ for all $a, b \in \mathbb{R}$.)

$(\mathbb{R}, \times)$ is not a group. Here the identity element is $1 \in \mathbb{R}$ since $1a = a$.

In general $a \in \mathbb{R}$ does not have an inverse.

If $a \neq 0$ then $a^{-1} = \frac{1}{a}$ is the inverse of a since $\frac{1}{a} \cdot a = 1 = \text{identity}$.

But $0 \in \mathbb{R}$ has no multiplicative inverse: $\square \cdot 0 = 1$ has no solution in $\mathbb{R}$.

The associative law holds for multiplication in $\mathbb{R}$: $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{R}$

Fixing the previous example: one idea

$$\mathbb{R}^* = \{a \in \mathbb{R} : a \neq 0\} = \{\text{all nonzero real numbers}\} = \underbrace{(-\infty, 0)}_{\text{negative reals}} \cup \underbrace{(0, \infty)}_{\text{positive reals}}$$

Multiplication in $\mathbb{R}$ is often written using 'x' or '.' or juxtaposition e.g.

"times" symbol.

$(\mathbb{R}^*, \times)$ is a multiplicative group

identity: 1

inverses: $a^{-1} = \frac{1}{a}$ is the inverse of $a \in \mathbb{R}^*$

associativity: $(ab)c = a(bc)$ for all $a, b, c \in \mathbb{R}^*$

(By the way, this group is abelian and infinite.)

1 has order 1 (as in any group).

-1 has order 2

Any $a \in \mathbb{R}^*$ other than ± 1 has infinite order.

$$2 \times 3 = 6$$

$$2.3 = 6$$

$$ab = a \times b = a \cdot b$$

juxtaposition times symbol dot

$(\{0, \infty\}, \times)$ is a group

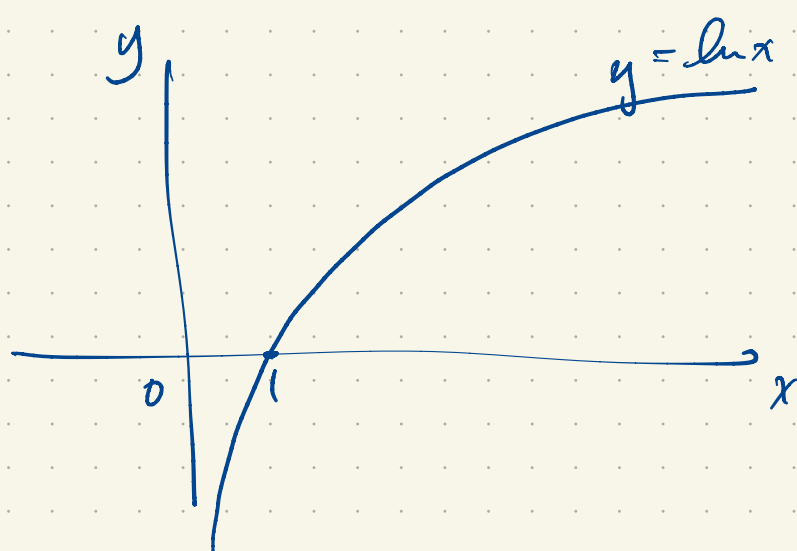
1 is the identity (order 1). All other elements have infinite order.

$(\mathbb{R}, +)$ and $(0, \infty), \times)$ are isomorphic groups.



$\exp$

$$ab = ?$$



$$\ln a \leftarrow a$$

$$\ln b \leftarrow b$$

$$\ln a + \ln b \rightarrow e^{\ln a + \ln b} = e^{\ln a} \cdot e^{\ln b} = ab$$

$\ln$ is a group isomorphism from $(0, \infty), \times)$ to $(\mathbb{R}, +)$.

The inverse function, $\exp(a) = e^a$, is a group isomorphism from $(\mathbb{R}, +)$ to $(0, \infty), \times)$.

A group is a set G together with a binary operation $*$ on G such that

(i) there is an element $e \in G$ such that $e * x = x * e = x$ for every $x \in G$;

(i.e. e is an identity element for $*$);

(ii) for every $x \in G$ there is an element $y \in G$ such that $x * y = e = y * x$

(i.e. y is an inverse element for x);

(iii) for all $x, y, z \in G$, $(x * y) * z = x * (y * z)$ (i.e. $*$ is associative).

Note: a binary operation $*$ on G is a function $G \times G \rightarrow G$, $(x, y) \mapsto \underbrace{* (x, y)}_{\text{written as } x * y}$

Eg. exponentiation is a binary operation on $(0, \infty) = \{\text{positive real numbers}\}$.

$$(a, b) \mapsto a^b$$

Is this a group operation?

If $e \in (0, \infty)$ is an identity element for this operation then $e^a = a$ and $a^e = a$ for all $a \in (0, \infty)$. Then $2^e = 2$ so $e = 1$. But then $1^a = a$, i.e. $1^2 = 2$. This does not hold. So exponentiation is a binary operation on $(0, \infty)$ which has no identity element.

So $((0, \infty), \text{exponentiation})$ is not a group.

$$\begin{array}{c} \uparrow \\ \text{"1"} \end{array} \quad a^1 = a^e$$

Moreover, exponentiation is not associative. Check: does

$$(x^y)^z = x^{(y^z)}? \quad \text{No!}$$

$$\text{eg. } \underbrace{(3^3)^2}_{27^2 = 729} \stackrel{?}{=} \underbrace{3^{(3^2)}}_{3^9 = 19683}$$

$$\underbrace{(2^2)^2}_{4^2 = 16} \stackrel{?}{=} \underbrace{2^{(2^2)}}_{2^4 = 16}$$

Exponentiation is not a binary operation on $\mathbb{R}$.

$$(-1)^{\frac{1}{2}} = ? \quad i? \quad -i?$$

$$0^{-1} = ? \quad \text{undefined!}$$

Subtraction is a binary operation on $\mathbb{R}$: $(a, b) \mapsto a - b$.

If $e \in \mathbb{R}$ is a binary operation for subtraction then $a - e = a = e - a$ for all $a \in \mathbb{R}$.

$$2 - e = 2, \quad e - 2 = 2 \quad \text{No value } e \in \mathbb{R} \text{ satisfies both of these conditions.}$$

Is subtraction associative? Does $(x - y) - z = x - (y - z)$ for all $x, y, z \in \mathbb{R}$?

$$\text{Try } \left. \begin{array}{l} (3 - 4) - 7 = -1 - 7 = -8 \\ 3 - (4 - 7) = 3 - (-3) = 6 \end{array} \right\} \text{Not equal.} \quad \text{Subtraction is nonassociative.}$$

Ex. let $n \geq 1$ (a positive integer) and let $G = \{n \times n \text{ invertible } n \times n \text{ matrices with real entries}\} = GL_n(\mathbb{R})$ (general linear group of $n \times n$ real matrices).

Note: an $n \times n$ matrix A is in G iff $\det A \neq 0$.

$$GL_1(\mathbb{R}) = \mathbb{R}^*$$

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element.

eg. $n=2$: the group $G = GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad-bc \neq 0 \right\}$. Identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

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

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

$$A^3 = AA^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} = -I$$

$$A^4 = A^3A = -A = \begin{bmatrix} 0 & -1 \\ -1 & -1 \end{bmatrix}$$

$$A^5 = A^3A^2 = -A^2 = \begin{bmatrix} -1 & -1 \\ -1 & -2 \end{bmatrix}$$

$$A^6 = A^3A^3 = (-I)(-I) = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{so } A \text{ has order 6.}$$

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

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

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \quad \text{shear}$$

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



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

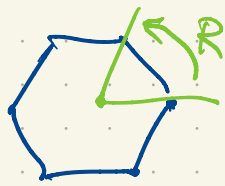
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order: there is no positive integer n for which $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = I$.

Most elements in G have infinite order.

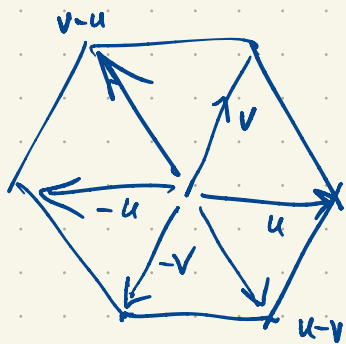
Most elements in G do not commute

For every positive integer n , there exist element(s) in G of order n . How do we construct them?

A regular hexagon has twelve symmetries forming a dihedral group of order 12.
Six of these are rotational symmetries and six reflective symmetries



R (a 60° rotation about the centre with an (x,y) coordinate system also centered at this point) gives an element of $G = GL_2(\mathbb{R})$ of order 6.
I'll choose a basis $\{u, v\}$ for $\mathbb{R}^2$ as shown:



(this is not the standard basis)

$$Ru = v$$

$$Rv = -u + v = v - u$$

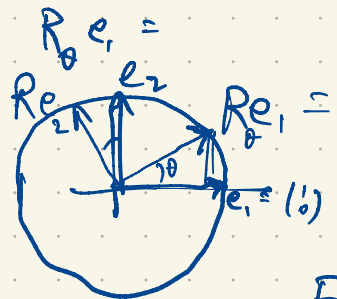
$$R(qu + bv) = qRu + bRv = qv + b(v - u) = -bu + (a+b)v$$

Writing vectors in $\mathbb{R}^2$ as column vectors of coefficients with respect to our basis.

$$R: \begin{bmatrix} a \\ b \end{bmatrix} \mapsto \begin{bmatrix} -b \\ a+b \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

So this matrix represents R and it has order 6.

What if we choose the standard basis $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$?
Now let R_θ be the counter-clockwise rotation about the origin by angle θ .



$$R_\theta e_1 = \begin{bmatrix} \cos \theta \\ \sin \theta \end{bmatrix}, \quad R_\theta e_2 = \begin{bmatrix} -\sin \theta \\ \cos \theta \end{bmatrix}$$

$$R_\theta \text{ is represented by } \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix}$$

$$\text{For } \theta = 60^\circ = \frac{\pi}{3}, \quad \cos \frac{\pi}{3} = \frac{1}{2}, \quad \sin \frac{\pi}{3} = \frac{\sqrt{3}}{2}$$

$$R_{\frac{\pi}{3}} = \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix}$$

is an element of $GL_2(\mathbb{R})$ of order 6.

In fact $R_\theta \in SL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$. This is a **subgroup** of $GL_2(\mathbb{R})$:
Just like $(0, \infty) \leq \mathbb{R}^+ = (-\infty, 0) \cup (0, \infty)$. $SL_2(\mathbb{R}) \leq GL_2(\mathbb{R})$.

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

or

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

or

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

or

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

Groups of order 4:

Let G be a multiplicative group of order 4 with elements $1, a, b, c$ where 1 is the identity.

cyclic group of order 4

$$G = \langle a \rangle = \{1, a, a^2, a^3\}$$

Cyclic group of order 4
 $\langle b \rangle = \{1, b, b^2, b^3\}$
 $\begin{matrix} b^2 & c \\ a^3 & c \end{matrix}$

This group has 1 element of order 1;
 (the Klein four-group) 3 elements of order 2.

Rewrite

1	→	1
a	→	b
b	→	a
c	→	c

$$\left. \begin{aligned} (ab)c &= cc = 1 \\ a(bc) &= aa = 1 \end{aligned} \right\}$$

$$\left. \begin{aligned} (ab)b &= cb = a \\ a(bb) &= a1 = a \end{aligned} \right\}$$

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

$\cong$

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

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

There are essentially two groups of order 4:
 a cyclic group of order 4
 and the Klein four-group.

The cyclic group of order 4 has 1 element of order 1;
 1 " " 2;
 2 elements of order 4.

Suppose G is a multiplicative group.

Every element $g \in G$ generates a cyclic subgroup $\langle g \rangle = \{\text{all powers of } g\}$
 $= \{g^k : k \in \mathbb{Z}\} = \{\dots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \dots\}$.

If $\langle g \rangle = G$ then G is cyclic.

If g has finite order n then $|g| = |\langle g \rangle| = n$. This requires some thought to fully understand. If $|g| = n$ then $g, g^2, \dots, g^{n-1}$ are non-identity elements in G whereas $g^n = 1$.

$$g^k g^l = g^{k+l}, \quad (g^k)^l = g^{kl} \quad \text{for all } k, l \in \mathbb{Z}.$$

$$g^2 g^3 = (gg)(ggg) = g^5$$

g

$$g^2 g^5 =$$

Why don't we write $\frac{1}{A}$ for $A \in GL_n(\mathbb{R})$? We do write $\frac{1}{s}$ for $s \in \mathbb{R}^\times$.

$$\text{In } \mathbb{R}^\times, \frac{1}{ab} = \frac{1}{a} \cdot \frac{1}{b}$$

Does $(AB)^{-1} = A^{-1}B^{-1}$? No; $(AB)^{-1} = B^{-1}A^{-1}$

In any multiplicative group, $(gh)^{-1} = h^{-1}g^{-1}$. Why? $(gh)^{-1}(gh) = 1$

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}1h = h^{-1}h = 1.$$

$$(g^{-1})^n = (g^n)^{-1} = g^{-n}$$

$$(gh)(h^{-1}g^{-1}) = 1.$$

If G is any group with operation $*$ and identity e , then G has a unique identity e . why? If $e' \in G$ is also an identity then

$$e * x = x * e = x$$

$$e' * x = x * e' = x$$

for all $x \in G$.

Then $e = e * e' = e'$.

ASIDE

Russell's Paradox

Let S be the set of all sets A such that $A \notin A$.

The set of all ideas is not an element of S .

The set of all birds is an element of S .

Is $S \in S$? If $S \in S$ then $S \notin S$.

If $S \notin S$ then $S \in S$.

If G is a group with identity e , then every element $x \in G$ has a unique inverse. why? If $y, z \in G$ are inverses for x then

$$\begin{cases} x * y = y * x = e \\ x * z = z * x = e \end{cases}$$

$$\text{so } y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$

Now since inverses are unique, we are justified in writing x^{-1} as the inverse for x .

$$\frac{a}{b} = b^{-1}a \text{ or } ab^{-1} ?$$

The Shoe-Sock Theorem: $(ab)^{-1} = b^{-1}a^{-1}$

Symmetric groups S_n = symmetric group of degree n
 = set of all permutations of $\{1, 2, \dots, n\}$

A bijection $f: A \rightarrow B$ is a function that is one-to-one and onto.

A permutation of A is a bijection $f: A \rightarrow A$.

If $|A| = n$ then there are $n! = 1 \times 2 \times 3 \times \dots \times n$ permutations of A .

Eg. $n=5$. $S_5 = \{\text{all permutations of } [5]\}$, $[5] = \{1, 2, 3, 4, 5\}$

$$|S_5| = 5! = 1 \times 2 \times 3 \times 4 \times 5 = 120$$

eg $f, g \in S_5$ defined by

x	$f(x)$	$g(x)$	$f \circ g(x)$	$g \circ f(x)$
1	2	2	1	5
2	1	5	3	2
3	4	3	4	4
4	5	4	5	1
5	3	1	2	3

$$|f| = 6$$

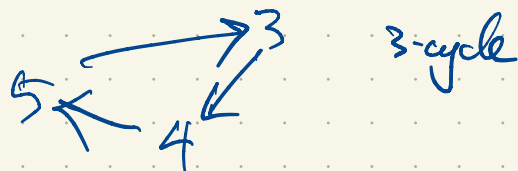
$$(1) = (1)(2)(3)(4)(5) = \text{identity}$$

Cycle notation for permutations:

$$f = (1\ 2)(3\ 4\ 5)$$

$$g = (1\ 2\ 5)(3)(4) = (1\ 2\ 5)$$

$$\begin{aligned} fg &= (1\ 2)(3\ 4\ 5)(1\ 2\ 5) \\ &= (1)(2\ 3\ 4\ 5) \\ &= (2\ 3\ 4\ 5) \end{aligned}$$



$$\begin{aligned} gf &= (1\ 2\ 5)(1\ 2)(3\ 4\ 5) \\ &= (1\ 5\ 3\ 4)(2) \\ &= (1\ 5\ 3\ 4) \end{aligned}$$