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

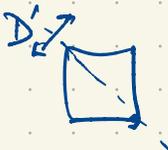R^3 = $270°$ counterclockwise rotation = $90°$ clockwise rotation

$R^4 = I$

D = reflection

$D' =$

$H =$

$V =$

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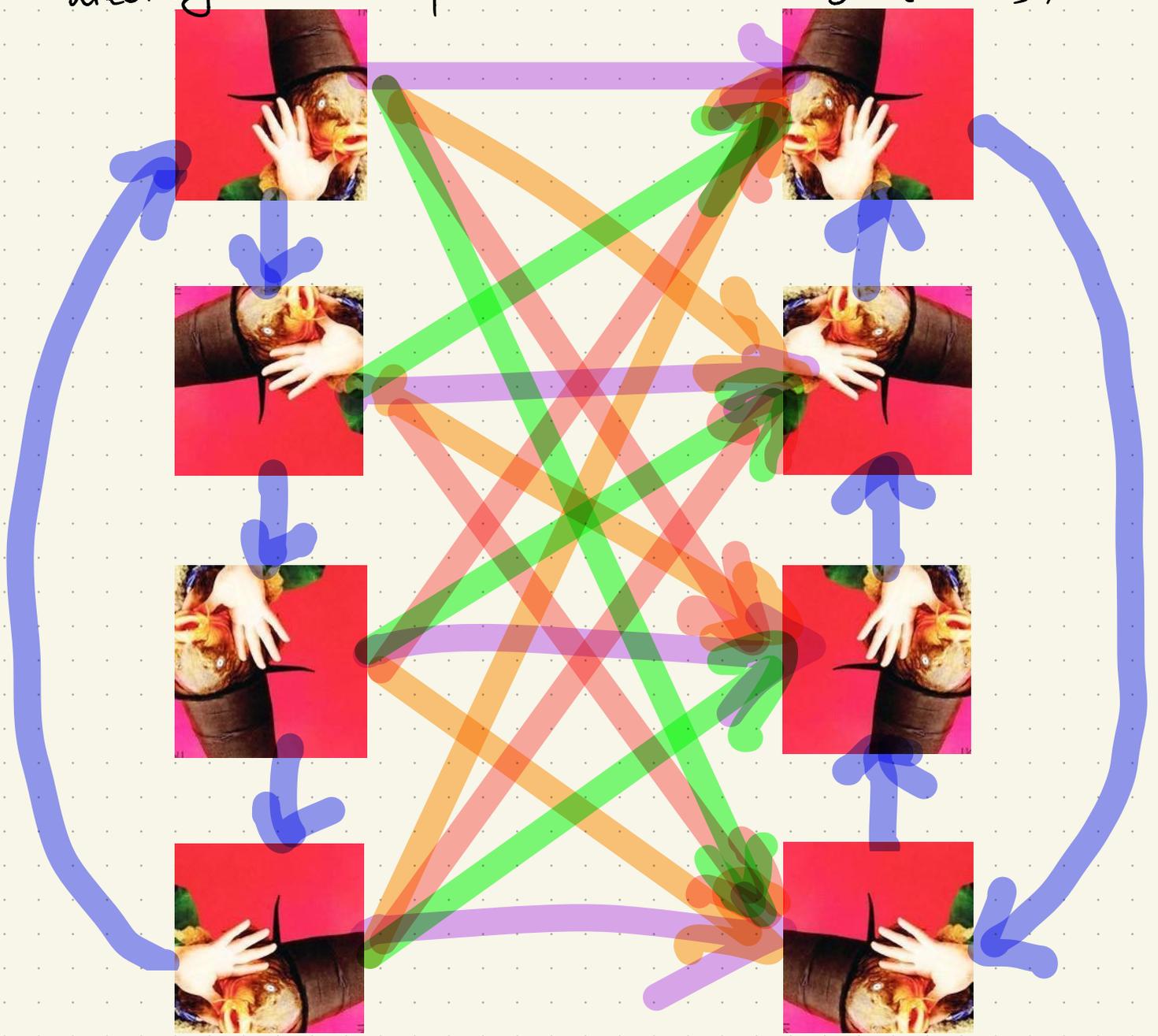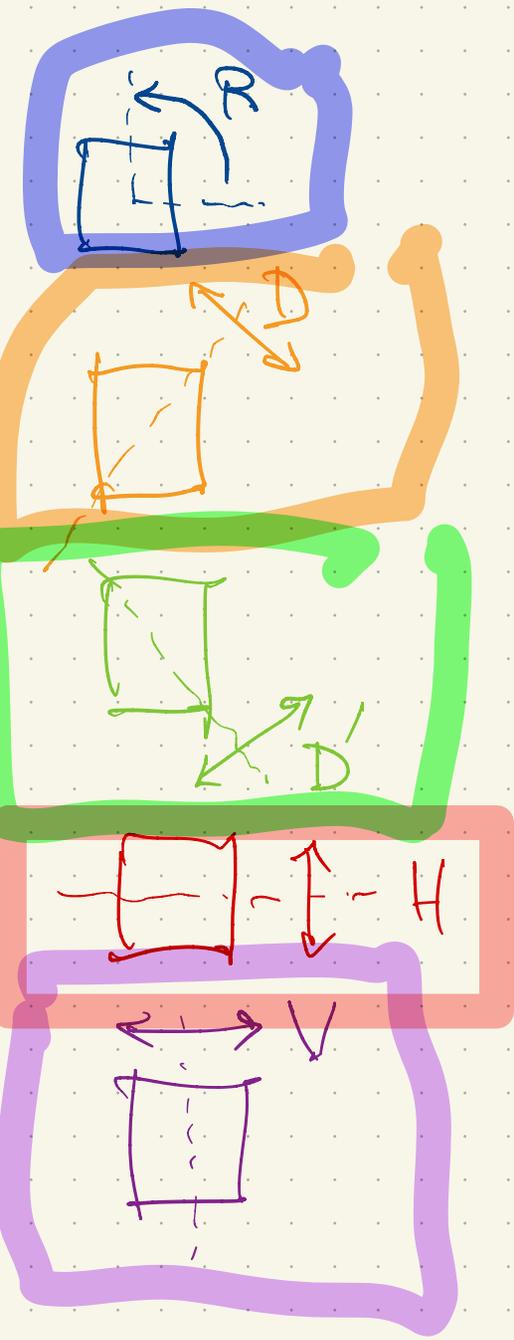
Symmetry group
of square $G = \{I, R, R^2, R^3, D, D', H, V\}$

Composition: $RD = V$ $HV = R^2$ Note: H and V commute (ie. HV = VH)
(right-to-left) $DR = H$ $VH = R^2$ but R and D do not commute (RD ≠ 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.)
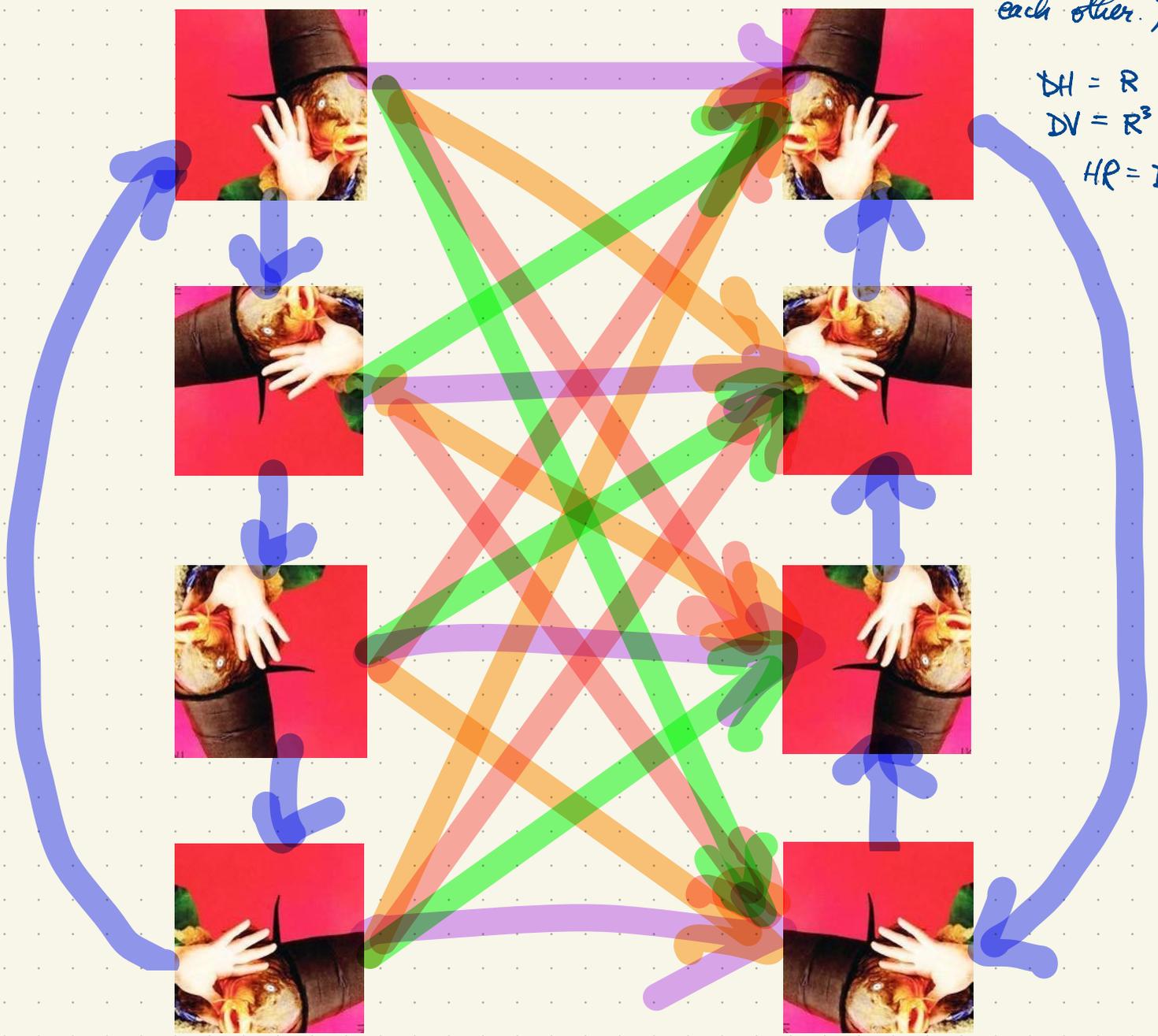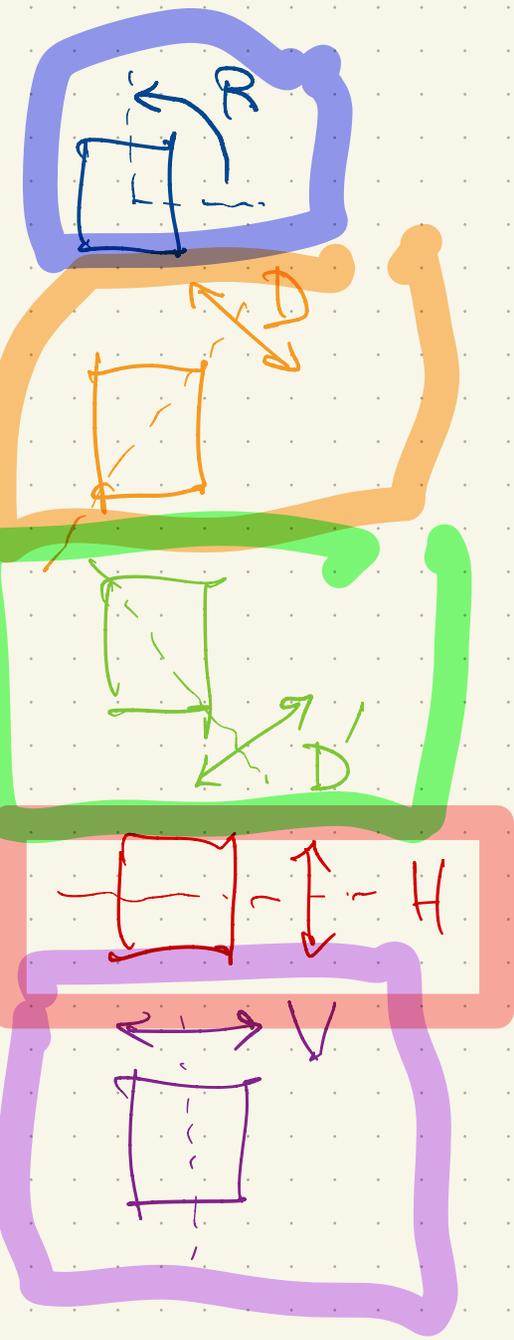
$DH = R$
$DV = R^3$
$HR = D'$

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

The order of a group G is $|G|$ = number of elements in G.
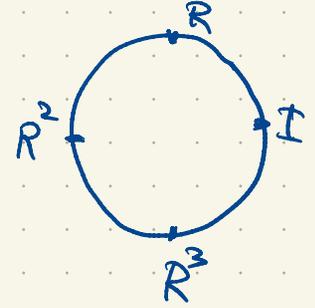
G has five elements of order 2: D, D', H, V, R^2; two elements of order 4: R, R^3; one element of order 1: I.

	I	R	R²	R³	D	D'	H	V
I	I	R	R²	R³	D	D'	H	V
R	R	R²	R³	I	V	H	D	D'
R²	R²	R³	I	R	D'	D	V	H
R³	R³	I	R	R²	H	V	D'	D
D	D	H	D'	V	I	R²	R	R³
D'	D'	V	D	H	R²	I	R³	R
H	H	D'	V	D	R³	R	I	R²
V	V	D	H	D'	R	R³	R²	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 ith element "times" the jth element.

In the multiplication table, each group element appears exactly once in each row and column.
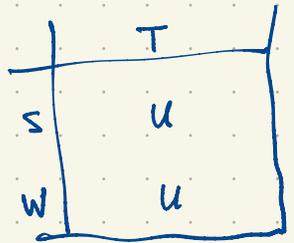
$\Rightarrow$ $ST = U = WT \Rightarrow$ $ST \cdot T^{-1} = WT \cdot T^{-1} \Rightarrow S = W$

Associativity holds!

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

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

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

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

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

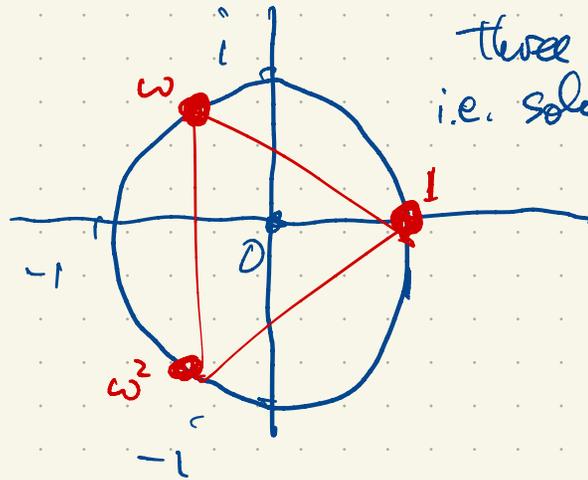| x	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

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

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

$\{1, \omega, \omega^2\}$ 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 <u>cyclic group</u> is a group
generated by one element i.e.

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

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

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

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

$\qquad g^0 = 1$

If $G = \{1, g, h\}$ is a group
then $g^2 = h$ so $G = \{1, g, g^2\}$.
(the <u>cyclic group</u> 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. $\mathbb{Z}/3\mathbb{Z}$ = { integers mod 3 } = {0, 1, 2}   2+2=1 in this group with identity element 0.

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

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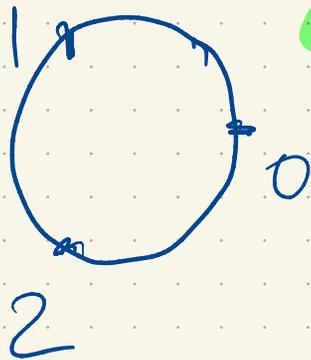
+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	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 $\phi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \langle \omega \rangle$ 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 $\langle \omega \rangle$.

+	j
i	i+j

$\longrightarrow$

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

==Some infinite groups:==

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

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 $\frac{1}{a} \cdot a = 1 =$ 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   Multiplication in $\mathbb{R}$

$\mathbb{R}^{\times} = \{a \in \mathbb{R} : a \neq 0\} = \{\text{all nonzero real numbers}\} = \underbrace{(-\infty, 0)}_{\substack{\text{negative} \\ \text{reals}}} \cup \underbrace{(0, \infty)}_{\substack{\text{positive} \\ \text{reals}}}$ is often written using '$\times$' or '$\cdot$' or e.g.

"times" symbol

$2 \times 3 = 6$

$2 \cdot 3 = 6$

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

identity : 1

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

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

associativity : $(ab)c = a(bc)$ for all $a,b,c \in \mathbb{R}^{\times}$.   juxtaposition   times symbol   dot

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

1 has order 1 (as in any group).

-1 has order 2

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

==$((0,\infty), \times)$ is a group==

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

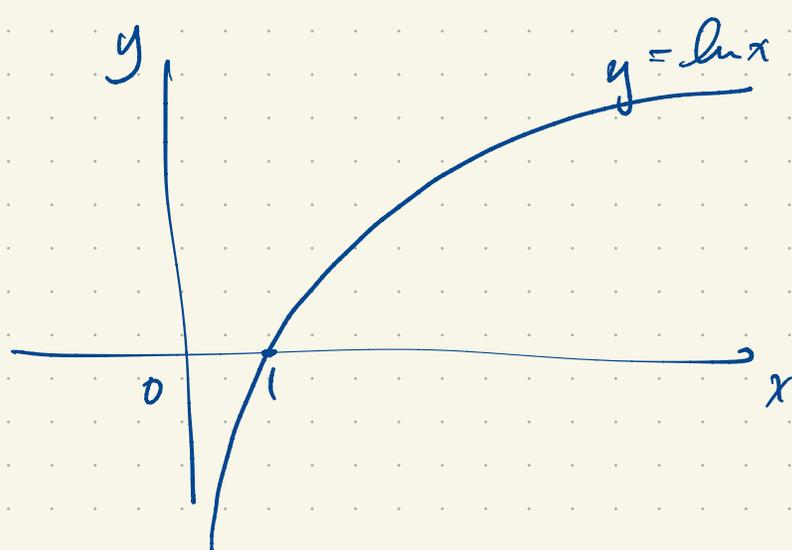$(\mathbb{R}, +)$ and $((0,\infty), \times)$ are isomorphic groups.

$\ln$

$\exp$

$ab = ?$

$\ln a \longleftarrow a$

$\ln b \longleftarrow b$

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

$y = \ln x$

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

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

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 $G \times G \longrightarrow G$, $(x, y) \longmapsto *(x, y)$ written as $x * y$

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

$(a,b) \longmapsto a^b$.

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 $1^a = a$, ie. $1^2 = 2$. 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.

$$\underset{\text{"}\wedge\text{"}}{\uparrow} \quad a^\wedge b = a^b$$

Moreover, exponentiation is not associative. Check: does

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

eg. $(3^\wedge 3)^\wedge 2 \overset{?}{=} 3^\wedge(3^\wedge 2)$

$$\underbrace{\qquad}_{27^2 = 729} \qquad \underbrace{\qquad}_{3^9 = 19683}$$

$$(2^\wedge 2)^\wedge 2 \overset{?}{=} 2^\wedge(2^\wedge 2)$$
$$4^2 = 16 \qquad 2^4 = 16$$

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

$(-1)^{1/2} = ?$ i? $-i$?

$0^{-1} = ?$ undefined !

Subtraction is a binary operation on $\mathbb{R}$: $(a,b) \longmapsto a-b$.
If $e \in \mathbb{R}$ is a binary operation for subtraction then $a-e = a = e-a$ for all $a \in \mathbb{R}$.

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

Is subtraction associative? Does $(x-y)-z = x-(y-z)$ for all $x,y,z \in \mathbb{R}$?
Try $(3-4)-7 = -1-7 = -8$ $\Big\}$ Not equal.   Subtraction is nonassociative.
     $3-(4-7) = 3-(-3) = 6$

Eg. let $n \geq 1$ (a positive integer) and let $G = \{n \times n$ invertible $n \times n$ 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 $\det A \neq 0$. $GL_1(\mathbb{R}) = \mathbb{R}^\times$

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

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

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

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

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

$A^5 = A^3 A^2 = -A^2 = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$

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

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

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

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ 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 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = I$.

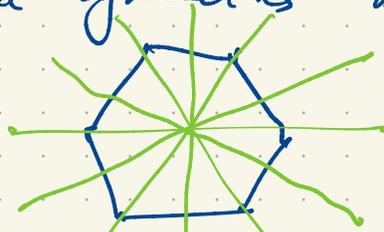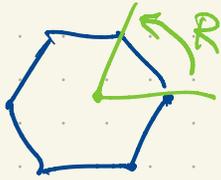**Most** elements in G have infinite order.

Most elements in G do not commute.

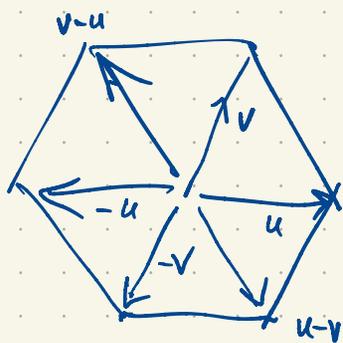For every positive integer n, there exist element(s) in G of order n. How do we construct them?

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)

$$Ru = v$$
$$Rv = -u+v = v-u$$
$$R(au+bv) = aRu + bRv = av + b(v-u)$$
$$= -bu + (a+b)v$$

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

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

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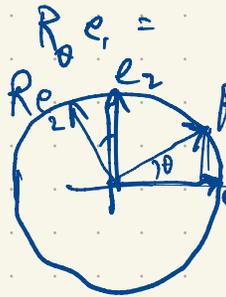
$R_\theta e_1 = $
$R_\theta e_1 = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$, $R_\theta e_2 = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$

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

For $\theta = 60° = \frac{\pi}{3}$, $\cos\frac{\pi}{3} = \frac{1}{2}$, $\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$

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

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 $(0,\infty) \leq \mathbb{R}^\times = (-\infty, 0) \cup (0,\infty)$. $SL_2(\mathbb{R}) \leq GL_2(\mathbb{R})$.

$$
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & c & 1 & b \\
b & b & 1 & c & a \\
c & c & b & a & 1 \\
\end{array}
\quad \text{or} \quad
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & 1 & c & b \\
b & b & c & 1 & a \\
c & c & b & a & 1 \\
\end{array}
\quad \text{or} \quad
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & b & c & 1 \\
b & b & c & 1 & a \\
c & c & 1 & a & b \\
\end{array}
\quad \text{or} \quad
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & 1 & c & b \\
b & b & c & a & 1 \\
c & c & b & 1 & a \\
\end{array}
$$

cyclic group of order 4   cyclic group of order 4

Groups of order 4:

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

this group has 1 element of order 1; 3 elements $\cdots$ 2. (the Klein four-group.)

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

$\langle b \rangle = \{1, b, b^2, b^3\}$
$\phantom{\langle b \rangle = \{1,} a c$

Rewrite
$1 \longrightarrow 1$
$a \longrightarrow b$
$b \longrightarrow a$
$c \longrightarrow c$

$(ab)c = cc = 1$
$a(bc) = aa = 1$
$(ab)b = cb = a$
$a(bb) = a1 = a$

$$
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & b & c & 1 \\
b & b & c & 1 & a \\
c & c & 1 & a & b \\
\end{array}
\;\cong\;
\begin{array}{c|cccc}
 & 1 & b & a & c \\
\hline
1 & 1 & b & a & c \\
b & b & a & c & 1 \\
a & a & c & 1 & b \\
c & c & 1 & b & a \\
\end{array}
\;=\;
\begin{array}{c|cccc}
 & 1 & a & b & c \\
\hline
1 & 1 & a & b & c \\
a & a & 1 & c & b \\
b & b & c & a & 1 \\
c & c & b & 1 & a \\
\end{array}
$$

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 $\cdots$ '' 4.

Suppose G is a multiplicative group.

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

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 $g, g^2, \ldots, g^{n-1}$ are non-identity elements in G whereas $g^n = 1$.

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

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

$\qquad\qquad\qquad\qquad\qquad\qquad g$

$g^{-2} g^5 =$

Why don't we write $\frac{1}{A}$ for $A \in GL_n(\mathbb{R})$?   We do write $\frac{1}{5}$ for $5 \in \mathbb{R}^\times$.
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? $(gh)^{-1}(gh) = 1$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (h^{-1} g^{-1})(gh) = h^{-1}(g^{-1} g)h = h^{-1} 1 h = h^{-1} h = 1.$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (gh)(h^{-1} g^{-1}) = 1.$

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

$$e * x = x * e = x$$
$$e' * x = x * e' = x \qquad \text{for all } x \in G.$$

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

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

$$\begin{cases} x * y = y * x = e \\ x * z = z * x = e \end{cases} \qquad \text{so } y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$

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

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