Jan28

Wednesday, January 27, 2021 8:59 PM

Fundamental Definition

A set G with a binary operation

$$*: G \times G \longrightarrow G$$

is called a group if:

→ (Associativity) 1) $(a * b) * c = a * (b * c) \quad \forall a, b, c$

→ (Identity) 2) $\exists\, e \in G$ s.t. $a * e = e * a = a \quad \forall a$

→ (Inverse) 3) $\forall\, a \in G \;\exists\, a^{-1} \in G$ s.t. $a * \underline{a^{-1}} = e = \underline{a^{-1}} * a$

First Properties of Groups

Last time G a group

a) • The identity is unique.

b) • For each $a \in G$, a^{-1} is unique.

→ c) • If $a * b = e$, $a^{-1} = b$ & $b^{-1} = a$

↑ Exercise.

This time

Propn G a group.

(i) $(a^{-1})^{-1} = a$ any $a \in G$

(ii) $(a*b)^{-1} = \underline{(b^{-1})*(a^{-1})}$ any $a, b \in G$.

Proof

i) Want inverse of a^{-1}

Find some b s.t. $a^{-1} * b = e$ (by (c) above)

But $(a^{-1}) * a = e$ already

So $(a^{-1})^{-1} = a$ we win!

ii) Exercise. (similar).

In algebra we like to solve equations.

$ax = b$ solve for x. ←

We also like to cancel stuff.

$\cancel{a}c = \cancel{a}d$

Propn (Cancellation)

G a group. $a, b, c, d \in G$.

i) $ac = ad \Longrightarrow c = d$

ii) $cb = db \Longrightarrow c = d$

Pf/

$$ac = ad$$

$a^{-1}(ac) = a^{-1}(ad)$ (mult on left by a^{-1})

$(a^{-1}a)c = (a^{-1}a)d$ (assoc)

$ec = ed$ (inverse)

$c = d$ (identity) ∎

ii) identical

Notational Remark

Usually we will drop the * from our notation, write the binary operation in G multiplicatively.

$$a * b \leftrightsquigarrow ab$$

Furthermore

$n \geq 1 \quad a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n\text{-times}}$

$$a^{-n} = \overbrace{(a^{-1})(a^{-1}) \cdots (a^{-1})}$$

Corollary G a group

① • $ax = b$ has a unique solution

$x = a^{-1}b$

② • $xa = b$ has unique soln

$x = ba^{-1}$

Pf/ Uniqueness of pt 1

$u \in G$ any solution

$$au = b = (a \cdot a^{-1})b = a \cdot (a^{-1}b)$$

cancel the a's.

Examples

① $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$

assoc ✓

identity $e = 0$

Inverse $\underline{(a^{-1}) = -a}$

⚠ $\text{"}a^n\text{"} = \underline{n\cdot a}$

↑

do operation n-times

② $(\mathbb{Q}\setminus\{0\},\times)$, $(\mathbb{R}\setminus\{0\},\times)$

$(\mathbb{Q}_{>0},\times)$, $(\mathbb{R}_{>0},\times)$

↑ positive

assoc ✓

identity $= 1$

Inverse $= a^{-1} = \frac{1}{a}$

Exercise

why don't we include 0?

⚠ $(\mathbb{Z}\setminus\{0\},\times)$ not a group because 2 has no inverse.

③ Linear algebra

V a vector space.

$v_1 + v_2$ vector addition.

$\Longrightarrow$ V into a group.

In particular $(\mathbb{R}^n, +)$ is a group.

Rmk

A vector space is a group w/ more structure... $\mathbb{R}$-action.

④ $\times$ = cross product

$$\mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$$

Not associative.

Example 3 motivates...

Defⁿ $(A, *)$, $(B, \bullet)$ be 2 groups. The direct product of A & B is

$$A \times B = \{(a,b) \mid a \in A, \ b \in B\}$$

s.t. $(a_1, b_1) \cdot (a_2, b_2)$

$$= (a_1 * a_2, \ b_1 \bullet b_2)$$

Exercise This is a group.

⑤ $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

with $+$ is a group.

$\bar{a} + \bar{b} = \overline{a+b}$

$e = \bar{0} = \bar{n}$

$$\bar{a}^{-1} = \overline{-a} = \overline{n-a} \qquad (\bar{a} + \overline{n-a} = \bar{n} = \bar{0})$$

Check assoc

$$\begin{aligned}(\bar{a}+\bar{b})+\bar{c} &= \overline{a+b} + \bar{c}\\ &= \overline{(a+b)+c}\\ &= \overline{a+(b+c)} \quad \text{(assoc of ints)}\\ &= \bar{a} + (\overline{b+c})\\ &= \bar{a} + (\bar{b}+\bar{c})\end{aligned}$$

Exercise $(\mathbb{Z}/n\mathbb{Z}, \times)$ not a group.

⑥ $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a,m)=1\}$

This is a group under $\times$.

Exercise
- $e = \bar{1}$
- Inverse extended euclidean alg.
- $\bar{a}, \bar{b} \in (\mathbb{Z}/m\mathbb{Z})^\times$
  $\Longrightarrow \overline{ab}$ is too.

Remark

In each of the groups we've seen so far, we have

$$ab = ba \qquad \forall\ a, b \in G.$$

Def^n If G is a group & $ab = ba$ for all $a, b \in G$ then we call G an abelian group.

⑦ $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \det \neq 0 \right\}$

under matrix mult.

assoc ✓ (Linear algebra).

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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\det} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Check All this makes $GL_2(\mathbb{R})$ into a group.

Observe

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in GL_2(\mathbb{R})$$

$a \neq b$

$a, b \neq 0$

Compute

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}a&0\\0&b\end{pmatrix} \quad \& \quad \begin{pmatrix}a&0\\0&b\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

$\|$

$\begin{pmatrix}a&b\\0&b\end{pmatrix}$ not equal $\begin{pmatrix}a&a\\0&b\end{pmatrix}$

Nonabelian group.

Observations

→ In $\mathbb{Z}/8\mathbb{Z}$, $\bar{2}+\bar{2}+\bar{2}+\bar{2} = \bar{0}$ $|\bar{2}|=4$

In $\mathbb{Z}$ nothing like this ever happens

$|1|=\infty$

→ In $(\mathbb{Z}/7\mathbb{Z})^\times$

$$\bar{2}^1 = \bar{2}$$
$$\bar{2}^2 = \bar{4}$$
$$\bar{2}^3 = \bar{8} = \bar{1}$$

$|\bar{2}| = 3$

Def^n

Let G be a group, $x \in G$.

The order of x is the minimal positive n s.t. $x^n = e = 1$

We call this $|x|$.

If no such n exists we say $|x| = \infty$.

Notation rmk

G a gp, write 1 or 1_G for e.

Def^n

If G is a group & a finite set we call G a finite group

The order of G is $|G| = \#G$

Exercise

$x \in G$ & G is finite then $|x| \leq |G|$.

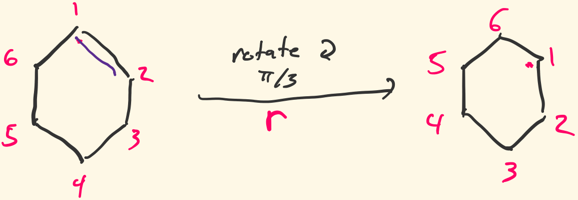
Notation

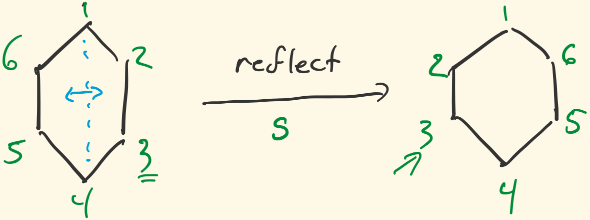
$G = \{g_1, g_2, \cdots g_n\}$ a finite group. Then we can write it's multiplication table:

	g_1	g_2	$\cdots$	g_n
g_1	$g_1 \cdot g_1$	$g_1 \cdot g_2$		$g_1 \cdot g_n$
g_2	$g_2 \cdot g_1$	$g_2 \cdot g_2$	$\cdots$	$g_2 \cdot g_n$
$\vdots$			$\vdots$	
g_n				

Important Example: Dihedral groups.

Symmetries of hexagon





Observe A symmetry of hex gives a function

$$\{1,2,\dots,6\} \longrightarrow \{1,2,3,\dots,6\}$$

$$r(1)=2$$

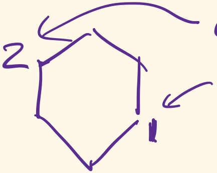
$$s(3)=5$$

* This function completely determines the symmetry.

* Not true Every such function

gives you a symmetry.

eg/



can't do this w/out breaking the hex.

$\sigma(1)=3$ & $\sigma(2)=6$ not a function corresponding to a symmetry.

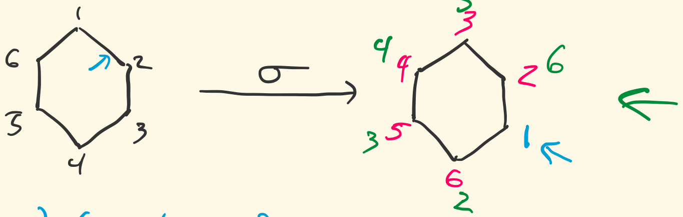
Prop

Let D_{12} be the set of symmetries of a hexagon.
Then D_{12} is a group.

pf/
- * identity is do nothing.
- * Inverse is undo symmetry.
- * Associativity follows bc composition of functions is associative.

Next Step: Compute $|D_{\underline{\underline{12}}}| = \underline{\underline{12}}$

$\sigma \in D_{12}$



1) 6 options for $\sigma(1)$

2) 2 options remaining for $\sigma(2)$

3) once I know where 1 & 2 go I'm done.

4) All distinct.

$$\Rightarrow |D_{12}| = 6 \cdot 2 = 12$$

Exercise (Algebraic Structure of D_{12})

i) $1, r, r^2, r^3, r^4, r^5$ are all distinct.

do nothing

$r \cdot r$ = rotate by $2\pi/3$

& $r^6 = 1$

so $|r| = 6$.

ii) $|s| = 2$

→ iii) $s \neq r^i$ for any i.

Hint: consider orientations.

iv) $sr^i \neq sr^j$

$0 \le i, j < 6$

$i \neq j$

v) $r^i \neq sr^j$

any i, j

use algebra. "Cancellation" reduce to (i) & (iii)

Consequence of (i) – (v)

$$\{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\} = D_{12}$$

all distinct

But there are 12 of them!!

$$D_{12} = \{s^i r^j \mid i = 0, 1, \quad j = 0, 1 \dots 5\}.$$

Geometric Consequence:

Any symmetry of the hexagon is a combo of rotations by $\pi/3$ & reflexions about vertical axis.

Exercise

i) $\underline{rs = sr^{-1}}$

Hint
Recall that a symmetry is determined by what it does to 1 & 2.

$$r \cdot s = r \circ s$$

$rs(1) = r(s(1))$

ii) Inductively

$$\underline{r^i \cdot s = s \cdot r^{-i}}$$

$$\begin{aligned} r^2 s &= (r\cdot r)\cdot s \\ &= r\cdot (rs) \\ &= r\cdot (s r^{-1}) \\ &= (rs)\cdot r^{-1} \\ &= (sr^{-1})(r^{-1}) = sr^{-2} \end{aligned}$$

Now we have a purely algebraic characterization of D_{12}.

Know all elts

Know how to multiply algebraically.

$$\begin{array}{c|ccccccc} & 1 & r & r^2 & \cdots & sr^3 & sr^4 & sr^5 \\ \hline 1 & & & & & & & \\ r & & & & & & & \\ r^2 & & & & & & & \\ \vdots & & & & & & & \\ r^5 & & & & & \boxed{sr^4} & & \\ s & & & & & & & \\ sr & & & & & & & \\ \vdots & & & & & & & \\ sr^5 & & & & & & & \end{array}$$

$$\begin{aligned} r^5 \cdot sr^3 &= sr^{-5}\cdot r^3 \\ &= sr^{-2} \\ &= sr^4 \end{aligned}$$

$r^{-2} = r^4$

$r^{-2} = r^6 \cdot r^{-2}$

Algebraic Characterization of D_{12}

Generators: r, s ← All of D_{12} comes from multiplying together these elements.

Relations:

$r^6 = 1$

$s^2 = 1$

} order of symbols

$rs = sr^{-1}$ ← how the symbols play.

We write

$$D_{12} = \langle r, s \mid r^6 = s^2 = 1 \quad rs = sr^{-1} \rangle$$

↑ This is called a Presentation of D_{12}.