Group defn

$(G, \circ)$ A pair of a non-empty set G with a closed bin. op. $\circ : G \times G \longrightarrow G$

$$(a, b) \longmapsto a \circ b$$

satisfying

- associative. $\forall\, a, b, c \in G$ $\quad (a \circ b) \circ c = a \circ (b \circ c)$
- identity $\exists\, e \in G\ \forall a \in G\ \ a \circ e = e \circ a = a$
- inverses. $\forall\, a \in G\ \ \exists\, a^{-1} \in G\ \ a \circ a^{-1} = a^{-1} \circ a = e.$

Some basic properties flow from this definition

Prop 3.17 The identity in G is unique.

Proof Suppose that $e, e' \in G$ are both identities.

Consider $e \circ e'$

$$\boxed{e'} = \underbrace{e \circ e'}_{\in G} = \boxed{e}$$

because e is an identity

because e' is an identity.

So $e' = e$. Therefore the identity

is unique.

Prop 3.18 Inverses are unique.

Proof Let $g \in G$. Suppose $g', g'' \in G$ are both inverses for g.

Consider $g' g g''$

since g'' an inverse for g

$$e g'' = (g' g) g'' \underset{\text{by associativity}}{=} g'(g g'') = g' e = g'$$

$$\parallel$$
$$g''$$

So $g'' = g'$

So inverses are unique.

Prop. 3.19 L.A. $(AB)^{-1} = B^{-1} A^{-1}$

True in all groups.

$\forall\, a, b \in G.\quad (ab)^{-1} = b^{-1} a^{-1}$

Prop 3.20 $\forall\, a \in G \quad (a^{-1})^{-1} = a$

Prop 3.21 Simple equations like $ax = b$? Solve for x.

or $xa = b$ } given $a, b \in G$

can be solved with unique solutions.

eg. $ax = b$

$(a^{-1}a)x = a^{-1}b$

$\Rightarrow x = \underline{\underline{a^{-1}b}} \in G$

$xa = b$

$\Rightarrow x = ba^{-1} \in G$

<u>Prop 3.22</u> Cancellation laws

$ba = ca \Rightarrow b = c$

also $ab = ac \Rightarrow b = c$.

Q? $ab = ca$ "conjugate of c by a"

$\Rightarrow b = a^{-1}ca$

or $\Rightarrow c = aba^{-1}$

L.A. $P^{-1}AP$

Exponential notation can be used in groups and follows the expected laws.

i.e. If $g \in G$, $(G, \circ)$ is a group and $n \in \mathbb{Z}$, $n > 0$

$$g^n := \underbrace{g \circ g \circ g \circ \cdots \circ g}_{n \text{ copies of } g}$$

$$g^{-n} := \underbrace{g^{-1} \circ g^{-1} \circ \cdots \circ g^{-1}}_{n \text{ copies of } g^{-1}}$$

$$g^0 := e$$

<u>Theorem 3.23</u> Expected rules for exponents.

<u>But</u> when using additive notation for a group $(G, +)$ then rather than powers we speak of multiples.

$$ng := \underbrace{g + g + \cdots + g}_{n \text{ copies of } g}$$

Consider

$$(gh)^n = ghgh \cdots gh$$

provided g, h <u>commute</u>

$$g^n h^n$$

$$= g \cdots g \, h \cdots h$$

$$m(g+h) = g+h+g+h+\cdots$$
$$\cdots+g+h$$
$$= mg+mh$$

Remember The convention in group theory is that $+$ notation is only used for Abelian gps.

What about g^m? for a group element g and positive integer m?

What does ng mean? Well just write it as g^n

Subgroups.

(compare this with your previous study of vector spaces and their subspaces)

A subgroup H of an existing group G is a subset of G (ie $H \subseteq G$) which forms a group using the same operation of G.

For any group G there are always two subgroups we can immediately point to.

Trivial subgroup $H = \{e\} \subset G$.

and the whole group G itself.

$$G \subseteq G.$$

The ~~real~~ subgroups of G we'll really be interested in are its proper non-trivial subgroups

$H \neq G$ $\qquad\qquad$ $H \neq \{e\}$

Eg 3.24

$$\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}$$

$$G = (\mathbb{R}^*, \times)$$

Consider $\mathbb{Q}^* = \{q \in \mathbb{Q} : q \neq 0\} \subset \mathbb{R}^*$

$\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$.

$\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}^*$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}^*$$

$1 \in \mathbb{Q}^*$, multiplication is associative

$\mathbb{Q}^*$ contain inverses for all its elements.

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \in \mathbb{Q}^*$$

so $\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$.

Ex. 3.25 $\quad H = \{1, -1, i, -i\} < \mathbb{C}^*$

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

So H is a closed system

$(-i)^2 = i^2 = -1$

<u>Ex 3.26</u> Recall $GL_n(\mathbb{R})$

"general linear group" of all invertible $n \times n$ matrices.

it has a subgroup

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$$

special linear group.

if $\det(A) = 1$

$$\det(A^{-1}) = \frac{1}{\det(A)} = 1$$

Prop 3.30 allows us to check whether a given subset H is a subgroup of G.

Prop 3.31 is a compressed form of 3.30.

H is a subgroup of G iff.

1. $H \neq \phi$
2. $\forall\, h_1, h_2 \in H \quad h_1 h_2^{-1} \in H$

Q35| Consider $G = D_3$ = symmetry group of $\triangle$.

Identify all its subgroups.

$$D_3 = \{ id, \underbrace{\rho_1, \rho_2}, \underbrace{\mu_1, \mu_2, \mu_3} \}$$

rotations. reflections

$\rho_1 =$ rot. by $\frac{2\pi}{3}$ radians clockwise

$\rho_2 =$ " " $\frac{4\pi}{3}$

" "

Let's hear the subgroups

$\{id\}$, D_3,

Consider $H = \{id, \rho_1, \rho_2\}$

$\rho_1 \circ \rho_2 = id \in H$
$= \rho_2 \circ \rho_1$

$\rho_1^2 = \rho_1 \circ \rho_1 = \rho_2 \in H$

$\rho_2^2 = \rho_2 \circ \rho_2 = \rho_1 \in H.$

$\rho_1^{-1} = \rho_2$, $\rho_2^{-1} = \rho_1$, $id^{-1} = id$

So by prop 3.30 H is a subgroup of the rotational group.

For instance $K = \{id, \rho_1\}$ fails to be a subgroup since. $\rho_1^{-1} \notin K$.

What about.

$L = \{id, \mu_1, \mu_2, \mu_3\}$

But $\mu_1 \circ \mu_2 = \rho_1 \notin L$ so L is not a subgroup

What about $P = \{id, \mu_1, \mu_3\}$?

No, because $\mu_1 \circ \mu_3 = \rho_2 \notin P$

What $Q = \{id, \mu_1\}$?

Prop 3.30 1, 2, 3 ✓ So Q is a subgroup.

$R = \{id, \mu_2\}$
$S = \{id, \mu_3\}$ also subgroups

Any more? D_3 has $\underline{\quad 2^6 \quad}$ subsets.

But id must be present, so really only 2^5 subsets $2^5 = 32$

Got six subgroups

Certainly any $\{id, \mu_i, \mu_j\}$

$i \neq j$ will fail since $\mu_i \circ \mu_j = \rho_1$ or ρ_2

what about

$\{id, \mu_i, \mu_j, \rho_k\}$

but notice $\mu_i \circ \mu_j = \rho_k$

but $\mu_j \circ \mu_i = \rho_l \neq \rho_k$

so closure will again fail.

with a little more checking

$\Longrightarrow D_3$ has six subgroups.