compare with your study of axioms for a vector space

Two motivating examples of groups

Integers modulo n

The relation of congruence modulo n on $\mathbb{Z}$ (for a fixed integer $n > 0$).

$\mathbb{Z}$ is partioned into n congruence classes / equivalence classes. mod n

$$[0], [1], [2], \ldots, [n-1]$$

$$[x] = \{ y : x \simeq y \pmod n \}$$

These can be added and multiplied

Use $\mathbb{Z}_n = \{ [0], [1], \ldots, [n-1] \}$

Eg 3.2

$\mathbb{Z}_8$ under multiplication.

a nice closed system algebraic.

– but not a group. 6 has no multipliative inverse.

But 5 does, so do 1, 3, 7, all self inverses, i.e. $5^{-1} = 5$ etc

Prop 3.4

part (6).

For mult. mod n. a^{-1} exists iff $\gcd(a,n) = 1$

i.e. a, n are coprime

Proof

$\exists\ b \in \mathbb{Z}_n \quad ab \equiv 1 \mod n$

$\iff$ " $\quad n \mid (ab - 1)$

$\iff$ " $\exists q \in \mathbb{Z}\ ab - 1 = qn$

$\iff \exists b \in \mathbb{Z}_n, \exists q \in \mathbb{Z} \quad 1 = ab - qn.$

i.e. 1 is a lin. comb. of a, n

$\iff \gcd(a,n) = 1$, from numb. theory last week.

So we see in $\mathbb{Z}_8$.

$\gcd(1,8) = \gcd(3,8) = \gcd(5,8) = \gcd(7,8) = 1$

But 2, 4, 6, 0 are <u>not</u> coprime to 8.

From this example

$(\mathbb{Z}_8, +)$ will be a group

$(\mathbb{Z}_8, \times)$ will not be, because it lacks inverses for some of its elements.

But this can be fixed.

Second example not numerical.

Symmetries of objects in $\mathbb{R}^2$.

the transformations of $\mathbb{R}^2$ (distance preserving = isometry) that leave the shape unchanged.

Eg Symmetries of a regular triangle. 

ρ "rho"

identity = id.

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

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

"mu"

reflection in axis through $A = \mu_1$

" " " " $B = \mu_2$

" " " " $C = \mu_3$

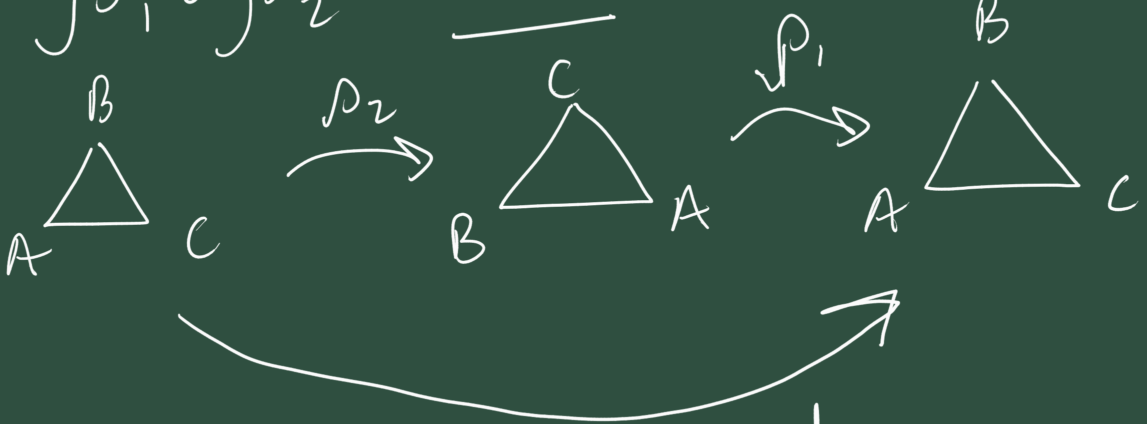
These are all the symmetries of $\triangle$

Lets call this $D_3 = \{ id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3 \}$

The natural operation we can apply to the elements of D_3 is composition. Applying transformations in sequence.

e.g. $\rho_1 \circ \rho_2$ means ρ_1 after ρ_2

$$\rho_1 \circ \rho_2 = \underline{\quad id \quad}$$



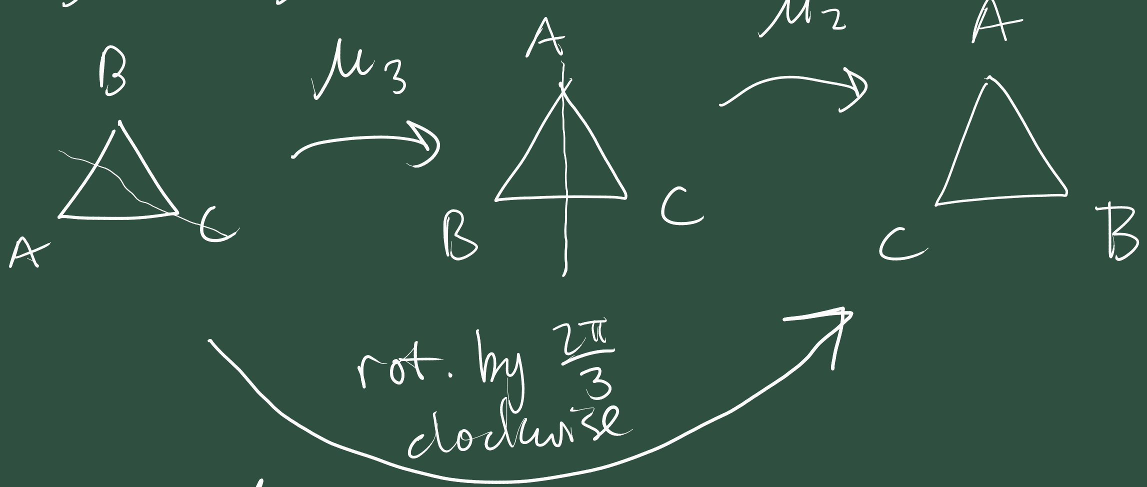
$$\rho_1 \circ \rho_2 = id.$$

composing any two symmetries will produce another one of the six symmetries
So we get a closed algebraic system

$(D_3, \circ)$. It has an operation table (Cayley tables)

$\circ$	y
x	$x \circ y$

$$\mu_2 \circ \mu_3 = \rho_1$$



$$\mu_2 \circ \mu_3 = \rho_1$$

$\circ$	rot	refle
rot	rot	refle
refle	reflec	rot.

all elements have inverses. $\rightarrow x \circ x^{-1} = id$

$id^{-1} = id$

$\rho_1^{-1} = \rho_2$, $\rho_2^{-1} = \rho_1$ $\qquad$ $rot^{-1} = rot$ (potentially different)

$\mu_1^{-1} = \mu_1^{-1}$, $\mu_2^{-1} = \mu_2$, $\mu_3^{-1} = \mu_3$

a reflection is always self-inverse.

$(D_3, \circ)$ we will call a group

<u>Warning</u> Be aware of ordering when composing.

$$x \circ y = x \text{ \underline{after} } y.$$

<u>Group definition</u> (non-empty)

A group is a non-empty set G together with a binary operation on G

$$\circ : G \times G \longrightarrow G.$$

i.e for $a, b \in G$, $a \circ b \in G$. (closure)

Satisfying

- $\circ$ is associative.
  $\forall\, a, b, c \in G$ $\quad a \circ (b \circ c) = (a \circ b) \circ c$
- $\exists$ an identity element $e \in G$ for $\circ$ on G

i.e. $\forall\, a \in G \quad e \circ a = a \circ e = a$

- G contains inverses for <u>all</u> its elements.

i.e. $\forall\, a \in G \ \exists\, a^{-1} \in G$ s.t.

$$a \circ a^{-1} = a^{-1} \circ a = e$$

This is a group $(G, \circ)$

<u>Abelian</u> groups are those where operation is commutative.

$$\forall\, a, b \in G \quad a \circ b = b \circ a.$$

<u>Non-abelian</u> groups are the others.

$(D_3, \circ)$ is non-abelian

e.g. $\mu_1 \circ \mu_2 = \rho_1$
$\qquad\qquad\qquad\ \ \#$
$\quad\ \ \mu_2 \circ \mu_1 = \rho_2$

<u>Examples</u> $(\mathbb{Z}, +)$ $\quad e = 0$ (infinite)

associativity ✓, closed ✓, inverses given $a \in \mathbb{Z}$ its inverse $-a$

(when using $+$ for operation, always use

$-a$ for a inverse)

$(\mathbb{Z}_n, +)$ a finite group

given $a \in \mathbb{Z}_n$ $\quad -a \in [n-a]$

$0 \leq a \leq n-1$

$(\mathbb{Z}_8, \times)$ is <u>not</u> a group.

closed ✓ associative ✓ identity $e=1$ ✓

inverses ✗ eg. 2 has no inverse

neither does 0, 4, 6.

But 1, 3, 5, 7 do have inverses.

$$U(n) = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$$

"units modulo n" $\quad (U(n), \times)$ will be a group

$$\boxed{\begin{gathered}\gcd(a,n) = \gcd(b,n) = 1 \\ \implies \gcd(ab,n) = 1\end{gathered}}$$

$\implies$ closure

assoc ✓ $\quad e=1$ ✓ $\quad$ inverses exist thanks to prop 3.4 (6).

$U(8) = \{1, 3, 5, 7\}$

(in my number theory notes I use $\mathbb{Z}_n^\times$ for $U(n)$).

$(D_3, \circ)$ is a group

closed ✓ associative?

Well for function composition, it's always associative.

$$\underbrace{(f \circ (g \circ h))}(x) = f((g \circ h)(x))$$
$$= f(g(h(x)))$$
$$= (f \circ g)(h(x))$$
$$= \underbrace{((f \circ g) \circ h)}(x)$$

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

id = id. ✓, Inverses exist.

Actually there is a <u>infinite</u>

family of such groups

$(D_n, \circ)$ = symmetry of the regular n-sided polygon

Dihedral groups

For every vector space you've looked at $(V, F, +, \cdot)$ the pair $(V,+)$

scalars

is an Abelian group.

Matrix groups

infinite

$M_n(\mathbb{R})$ = set of all square $n \times n$ matrices.

$(M_n(\mathbb{R}), +)$ is an Abelian group

closed ✓ assoc. ✓ identity $= \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \\ 0 & \cdots & 0 \end{pmatrix}$ zero matrix.

inverses for $A \in M_n(\mathbb{R})$ its inverse is $-A$

But $(M_n(\mathbb{R}), \times)$ is <u>not</u> a group

$id = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ multiplicative inverse matrices don't always exist

$\begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$ has no inverse as its determinant is 0.

<u>Fix</u>

$$GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) : \det(A) \neq 0 \}$$

"General Linear Group"

<u>is</u> a group

$$\det(AB) = \underline{\det(A)} \cdot \underline{\det(B)}$$

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

Exercises Testing the definition

$\boxed{Q7}$ $S = \mathbb{R} \setminus \{-1\}$.

define a new operation $*$ on S by the rule
$$a * b = a + b + ab$$

Prove $(S, *)$ is an abelian group.

Is $*$ closed on S? ie.

given $a, b \in S \overset{?}{\Longrightarrow} a * b \in S$

for sure $a + b + ab \in \mathbb{R}$ since $a, b \in \mathbb{R}$

But could $\boxed{a + b + ab = -1 \quad ?}$

$$\iff a + b(1+a) = -1$$

$$\iff b(1+a) = -1 - a$$

$$\iff b = \frac{-1-a}{1+a} = \frac{-(1+a)}{(1+a)} = -1$$

$(1 + a \neq 0$ since $a \in S)$ a contradiction.

So therefore $a, b \in S \Longrightarrow a * b \in S$

Closure ✓

Associativity.

Consider $a, b, c \in S$

$$a * (b*c) = a + (b*c) + a(b*c)$$
$$= a + b + c + bc + a(b + c + bc)$$
$$= a + b + c + \underline{bc} + \underline{ab} + \underline{ac} + \underline{abc}$$
$$= (a+b+ab) + c + (a+b+ab)c$$
$$= (a+b+ab) * c, \text{ def of } *$$
$$= (a*b) * c, \text{ def of } *$$

Therefore $*$ is associative on S. ✓

identity. $a*b = a + b + ab$

so $e = 0$ ✓

inverses given $a \in S$, is $a^{-1} \in S$?

So this is the question, does there exist an $a^{-1} \in S$ such that

$$a * a^{-1} = 0$$

$$\Longleftrightarrow \quad a + a^{-1} + aa^{-1} = 0$$

$\Leftrightarrow \quad a + a^{-1}(1+a) = 0$

$\Leftrightarrow \quad a^{-1} = \dfrac{-a}{1+a}$, $1+a \neq 0$, $a \in S$

maybe a slight worry.

could $\dfrac{-a}{1+a} = -1$?

$\Rightarrow -a = -1 - a$

$\Rightarrow 0 = -1$, Nonsense.

So yes S has inverses for all its elements.

So $(S, *)$ is a group.

Abelian

$a * b = a + b + ab$

$= b + a + ba$, using known commutativity of + and .

$= b * a$