Math 122

Professor: Hiro Lee Tanaka

Logistics, et cetera.

What'll you learn in this class?

Groups + Rings

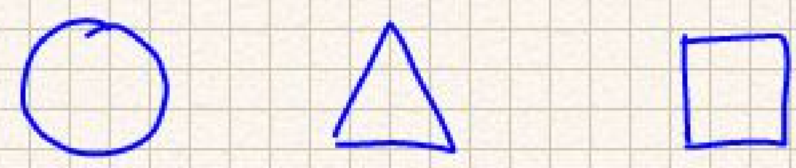
(Name for) concept	Whole #'s	Derivatives	Groups	Rings
This concept expresses ... ? (math is a language for conveying ideas; so what idea do these words embody?)	Counting, Quantity	Rate of change, Linearization	Symmetries	Functions on Spaces eg in Linear Algebra, planes are certain sets closed under scaling + adding. NOT how Greeks would express them!
Some mathematical consequences			"Algebraization" of geometry (Descartes → Present Day) "Geometrization" of algebra	
Some Applications (outside of pure math)			Noether's Thm (Physics) RSA algorithm (Cryptography) Logic circuits as "cosheaves" Homology / shape of data sets etc etc	

Most of this class focuses on groups.

(Rings are covered more next semester.)

Let's begin!

Fix some object X.



shapes

V vector space

What do we mean by a symmetry of X?

We usually have some structure of X in mind (shape, distance, linearity, etc)

A symmetry of X should be a map

$$\phi : X \longrightarrow X$$

which

(a) preserves the structure, and

$\text{dist}(x,y) = \text{dist}(\phi(x), \phi(y))$

$\phi(x+y) = \phi(x) + \phi(y)$

(b) can be undone.

Let's take a stab at expressing this (at first glance arbitrary) heuristic:

Let $G = \{\phi\}$ be the set of symmetries of X.

(1) If ϕ_1, ϕ_2 preserve structure, so should $\phi_2 \circ \phi_1$ and $\phi_1 \circ \phi_2$.

$\Longrightarrow$ Can compose elements of G.

$\Longrightarrow$ $G \times G \xrightarrow{m} G$, associative.

(2) "Doing nothing" should be a symmetry of X.

$\Longrightarrow$ $id_X \in G$. $id_X \circ \phi = \phi \circ id_X = \phi$.

(3) Since every ϕ can be undone, we should have $\phi^{-1} \in G$ so

$\phi \circ \phi^{-1} = id_X$,

$\phi^{-1} \circ \phi = id_X$.

Now we define this
without any reference to X.

<u>Defn</u> A <u>group</u> is a pair
$$(G, m)$$
where G is a set, and
m is a map
$$\begin{aligned} G \times G &\longrightarrow G \\ (g_1, g_2) &\longmapsto m(g_1, g_2) \\ &\qquad =: g_1 g_2 =: g_1 \cdot g_2 \end{aligned}$$
such that

(1) m is associative. i.e.,
$$m(m(g_1, g_2), g_3) = m(g_1, m(g_2, g_3))$$
i.e.,
$$(g_1 g_2) g_3 = g_1 (g_2 g_3) \quad \text{or} \quad (g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$$

(2) $\exists$ an element $1_G \in G$ s.t.
$$m(1_G, g) = g = m(g, 1_G).$$
i.e.,
$$1_G g = g = g 1_G \quad \text{or} \quad 1_G \cdot g = g = g \cdot 1_G$$

(3) $\forall g \in G$, $\exists$ element $h \in G$ s.t.
$$m(g, h) = 1_G = m(h, g).$$
i.e., $gh = 1_G = hg$. or $g \cdot h = 1_G = h \cdot g$.

We often write $g^{-1} := h$, "the inverse of g."

Ex Let

$$G = \{\cdots, -1, 0, 1, \cdots\}$$

be the set of integers.

Define

$$G \times G \xrightarrow{m} G$$

by

$$m(g,h) = g+h. \qquad \text{(ie, addition)}$$

Ex

$$m(-2,3) = 1.$$

Then

(1) m is associative, since

$$(g+h)+k = g+(h+k)$$

(2) $0 = 1_G$ is the identity,

since

$$m(0,g) = 0+g = g.$$

$$m(g,0) = g+0 = g.$$

(3) Every element has an inverse:

$$m(g,-g) = g+(-g) = 0.$$

Ex Fix $n \geq 1$. Then

$$G = GL_n(\mathbb{R}) = \{n \times n \text{ real matrices st } \det \neq 0\}$$

is a group, where

$$m: G \times G \longrightarrow G$$

is given by multiplication of matrices.

This shows $gh \neq hg$ in general!

(1) since matrix mult. is assoc.

(2) since the identity matrix does the job.

(3) $\det(g) \neq 0 \Rightarrow g$ invertible.

Exer Let $G = \mathbb{Z}$
$= \{\ldots, -1, 0, 1, \ldots\}$

and let
$$m: G \times G \longrightarrow G$$
$$(a,b) \longmapsto a \times b$$

ex $(2,3) \longmapsto 6$

Show (G, m) is NOT a group.

The above exercise shows it's important to know m. Regardless, we will often abbreviate, and say things like

"Let G be a group"

omitting mention of m.

Exer Let $g, h, k \in G$.

Show
$$gh = gk \Rightarrow h = k.$$

Likewise, show
$$hg = kg \Rightarrow h = k.$$

Cancellation law.

Exer

Let $G = \mathbb{R} - \{0\}$
(the set of real numbers w/ 0 removed).

Let
$$m: G \times G \longrightarrow G$$
$$(a,b) \longmapsto a \times b.$$

Show (G, m) is a group. We denote it $\mathbb{R}^\times$ from now on.

Maps of groups

Whenever you define an idea, it's good to know what kinds of functions are friends w/ that idea.

Ex

Sets S, T ⟷ any function $f: S \to T$

Spaces X, Y ⟷ continuous functions $f: X \to Y$

Smooth curves + surfaces X, Y ⟷ differentiable functions $f: X \to Y$

Groups G, H ⟷ group homomorphisms $\phi: G \to H$

Defn Let G, H be groups. A group homomorphism from G to H is a fxn

$$\phi: G \longrightarrow H$$

such that

$$\phi(g_1)\phi(g_2) = \phi(g_1 g_2)$$

multiplication in H multiplication in G.

Exer Fix $n \geq 0$.

Show

$$\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$$
$$A \longmapsto \det(A)$$

is a group homomorphism.

Exer Show

$$\exp : \mathbb{Z} \longrightarrow \mathbb{R}^\times$$
$$a \longmapsto e^a$$

is a group homomorphism.