Lecture 2 - Categories & Groups

Note Title 1/21/2008

Def A (small) category is two set
- A set of objects — Obj
- A set of arrows / Morphisms — Mor

together with some extra structure:

1) To every arrow, we associate 2 objects: the source and the target
(= 2 functions $Mor \underset{t}{\overset{s}{\rightrightarrows}} Obj$)
The collection of all morphisms with source a and target b will be denoted $Hom(a,b)$
(every $f \in Mor$ is in one of these: $f \in Hom(s(f), t(f))$)

2) Morphisms "compose": if $f \in Hom(a,b)$ & $g \in Hom(b,c)$, then we have a new morphism $g \circ f \in Hom(a,c)$

3) Composition is associative ($f \circ (g \circ h) = (f \circ g) \circ h$)

4) For every object a, there is a morphism $1_a \in Hom(a,a)$ s.t. $f \circ 1_a = f$, $1_a \circ g = g$. This is the identity morphism.

Most of the objects in modern math are studied not in isolation but rather as elements in a category.

Examples: Set: $Obj = \{X \mid X \subseteq U, \text{ some huge set}\}$

$Mor = \{\text{functions from } X \to Y, \text{ some } X, Y \in Obj\}$

$\boxed{Hom(X,Y) = \{f : X \to Y\}}$ — What we normally specify.

"source" = domain

"target" = range

Most of our categories are built out of this.

k a field:

$k\text{-Mod} = Vect_k$: $Obj = \{V \mid V \text{ is a } k\text{-v.space}\}$

$Hom(V,W) = \text{linear trans } V \to W$

$\cap\!|$

$\{\text{functions from } V \to W\}$

Some new categories we will see:

Groups = Grps $\quad Obj = \{\text{groups}\}$

Rings $\quad Hom(a,b) = ?$

ComRings

If R a ring: $R\text{-Mod} \not\cong \text{Mod-}R$.

Other useful ones: Ens = all sets (not a small category)

Cat = all small categories (not small).

Loosely speaking, a universal property is one that has a nice, categorical (as opposed to object) defn.

Ex: Products Let A, B be objects. Then the product of A & B, $A \times B$ is the object w/ maps

$B \xleftarrow{\pi_B} A \times B \xrightarrow{\pi_A} A$

(the projections onto the coordinates) s.t. if $C \xrightarrow{f} A$, $C \xrightarrow{g} B$, then there is a unique map $C \xrightarrow{h} A \times B$ s.t.

$$\pi_b \circ h = g, \quad \pi_a \circ h = f.$$

In sets & V. spaces, this is the ordinary direct / cartesian product.

II. Groups

Def A **group** is a set G together with a binary operation $\cdot : G \times G \to G$ s.t.

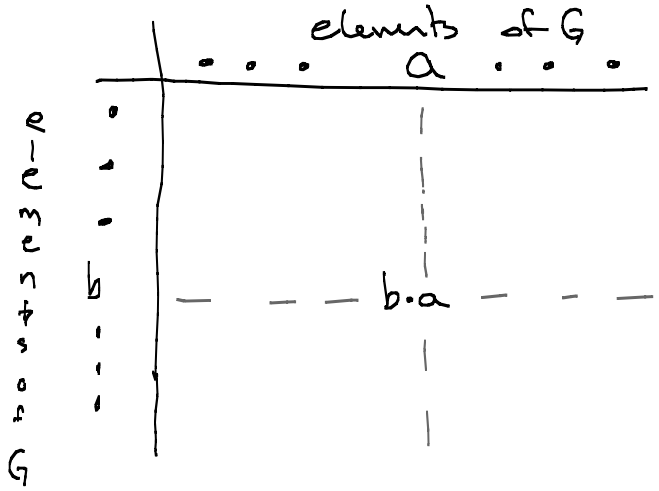
1) $\cdot$ is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$ (semigroup)
2) $\cdot$ is unital: $\exists e \in G$ s.t. $\forall g \in G$, $e \cdot g = g \cdot e = g$ (monoid)
3) Elements have inverses: $\forall g \in G$, $\exists g'$ s.t. $g \cdot g' = g' \cdot g = e$

Ex:
- $(\mathbb{Z}, +)$ is a group
- $(\mathbb{Q} - \{0\}, \cdot)$ is a group
  $(\mathbb{Q}_{>0}, \cdot)$ " " "
- If X is a set, the set of all bijections of X with itself is a group under composition
  $\Sigma_X = \{f : X \to X \mid f \text{ is } 1\text{-}1, \text{onto}\}$

Remark We could weaken axioms 2) & 3) of a group by just assuming that 2') $\exists e$ s.t. $e \cdot g = g \ \forall g$ & 3') $\forall g$, $\exists g'$ s.t. $g' \cdot g = e$.

We normally suppress the operation, talking instead about "the group G".

If G is a group, we normally specify the mult by a mult table:



Associativity is hard to see, but axioms 2 & 3 are easy to read out of the table.

Ex: $G = \{e, a, b\}$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

this is a group with 3 elements.

Thm 1 If $(G, \cdot)$ is a group then

1) The identity element is unique
2) Inverses are unique: g^{-1}
3) If g' is the inverse of g, then g is the inverse of g'
4) "Linear equations can be solved": $ax = b$ has a unique sol, as does $ya = b$.

Pf: 1) Let e, e' satisfy axiom 2). Then
$$e = e \cdot e' = e'.$$ (in fact, only used 2)).

2) Let g', h satisfy $g' \cdot g = h \cdot g = g \cdot g' = g \cdot h = e$.
then $$h = h \cdot e = h \cdot (g \cdot g') = (h \cdot g) \cdot g' = e \cdot g' = g'.$$

3) Since $g \cdot g' = g' \cdot g = e$, swapping g & g' & applying 2) gives the result.

4) $x = a^{-1}b$: $a\cdot(a^{-1}b) = (a\cdot a^{-1})\cdot b = e\cdot b = b$.

sim. $y = ba^{-1}$. ▨

Axiom 1) has a great consequence.

Thm 2 Any two ways of multiplying (in order) a sequence $x_1, \dots, x_n$ give the same result (ie we can put the parens in any way we want).

Pf By induction on n. If $n \leq 3$, it is obvious.

So pick to random products:

$$g = (x_1 \cdots x_i)(x_{i+1} \cdots x_n)$$
$$h = (x_1 \cdots x_j)(x_{j+1} \cdots x_n)$$

Since $1 \leq i, j < n$, the products in parens are independent of where we put ( ). If $i = j$, g & h are defined by the exact same product. WLOG, assume $i < j$.

So $$g = \underbrace{(x_1 \cdots x_i)}_{A} \cdot \Big(\underbrace{(x_{i+1} \cdots x_j)}_{B} \cdot \underbrace{(x_{j+1} \cdots x_n)}_{C} \Big)$$

$$h = \Big(\underbrace{(x_1 \cdots x_i)(x_{i+1} \cdots x_j)}_{A \cdot B} \Big) \cdot \underbrace{(x_{j+1} \cdots x_n)}_{C}$$

Axiom 1) $\Rightarrow$ $g = h$.

In particular, we can form powers of an element:

Def
$$g^n = \begin{cases} g \cdot g^{n-1} & n > 0 \\ e & n = 0 \\ (g^{-1})^{-n} & n < 0 \end{cases}$$

All of these are well defined operations.

Now an easy lemma about how these work together:

Lemma 3 a) $g^n \cdot g^m = g^{n+m}$

b) $(g^n)^m = g^{nm}$

In other words, exponents behave the way we expect.

Now note that for any $g \in G$,

$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ is a group under the mult from g.

Lemma 3 tells us that $(g^n)\cdot(g^m) \in \langle g \rangle$, and by def, $g^{-n}\cdot g^n = g^0 = e$, with all terms in $\langle g \rangle$.

This is the prototypical example of a subgroup:

Def A subset H of a group G is a subgroup if it is a group under the multiplication coming from G.

In particular: 1) If $h_1, h_2 \in H$, then $h_1 \cdot h_2 \in H$

2) $e \in H$

3) If $h \in H$, then $h^{-1} \in H$.

In fact, if $h \in H$, then $\langle h \rangle \subseteq H$.

Lemma 4 A subset $H \neq \emptyset$ is a subgroup iff $\forall\, g, h \in H$, $g^{-1}\cdot h \in H$.

Pf: If H is a subgroup, then "$\Rightarrow$" follows from the previous comments.

$\Leftarrow$) Let $h \in H$. Then $e = h^{-1}\cdot h \in H$ & $h^{-1} = h^{-1}\cdot e \in H$.

So if $g, h \in H$, then $g\cdot h = (g^{-1})^{-1}\cdot h \in H$ & H is a subgroup. ▨

Lemma 5 If I is a set & H_i is a family of subgroups of G indexed by $i \in I$, then $\bigcap_{i\in I} H_i$ is a subgroup of G.

Pf If $g, h \in \bigcap_{i\in I} H_i$, then $g, h \in H_i$ for all $i \in I$ $\Rightarrow$ $g^{-1}h \in H_i$ $\forall i \in I$ $\Rightarrow$ $g^{-1}h \in \bigcap_{i\in I} H_i$ $\Rightarrow$

$\bigcap_{i\in I} H_i$ is a subgroup by Lemma 4. ▨