Category Theory Seminar

Learn the def. of

- category \( C \)
- functor \( f : C \to C' \)
- natural transformation \( \natural \)

Duality

Every category \( C \) has an opposite category \( C^{op} \)

\( C^{op} \) has the same objects as \( C \),
but the morphisms are "turned around."

So there is a 1-1 correspondence between morphisms in \( C \) &
morphisms in \( C^{op} \), with \( f : x \to y \) in \( C \) corresponding to
a morphism \( f^{op} : y \to x \) in \( C^{op} \).

\[ \begin{array}{c}
\begin{array}{c}
\text{In } C: \\
\text{In } C^{op}:
\end{array}
\end{array} \]

We compose morphisms in \( C^{op} \) by:
\( f^{op} \circ g^{op} = (g \circ f)^{op} \)

The study of how categories \( C \) relate to their partners \( C^{op} \) is
called duality.

Note \( (C^{op})^{op} = C \)

'just like' for finite-dim vector spaces \((V^*)^* \cong V\)

It turns out that the dual of geometry is algebra.

In geometry we study "points"; in algebra we study addition & multiplication.

Descartes realized we can reduce (a lot of) geometry to algebra:
this is called 'analytic geometry'.
We can associate to any finite-dimensional vector space $V$ (over the real numbers) a commutative ring $\mathcal{O}(V)$ consisting of all polynomial functions on $V$, with usual addition and multiplication.

If $V = \mathbb{R}^n$, the algebra $\mathcal{O}(V)$ consists of polynomials in the coordinate functions $x_1, \ldots, x_n$: $\mathcal{O}(V) = \mathbb{R}[x_1, \ldots, x_n]$.

So: we go from a "space" $V$ (a bunch of points) to an algebra $\mathcal{O}(V)$. Then we can describe certain subspaces of $V$:

$$X \overset{H}{\rightarrow} V$$

as quotient rings of $\mathcal{O}(V)$:

$$\mathcal{O}(V) \overset{\text{onto}}{\rightarrow} \mathcal{O}(X) = \mathcal{O}(V)/I$$

an ideal

**Example** the unit circle is a subspace of the plane:

$$S^1 \longrightarrow \mathbb{R}^2$$

where $S^1 = \{(x, y) : x^2 + y^2 - 1 = 0\}$

Then there is an algebra $\mathcal{O}(S^1)$ of polynomial functions on the unit circle, with $\mathcal{O}(S^1) = \mathbb{R}[x, y]/\langle x^2 + y^2 - 1 \rangle$ (the ideal generated by $x^2 + y^2 - 1$).

So the 1-1 map $S^1 \longrightarrow \mathbb{R}^2$ gets turned around, giving $\mathcal{O}(\mathbb{R}^2) \overset{}{\rightarrow} \mathcal{O}(S^1)$.

Which is just restriction: $f \in \mathcal{O}(\mathbb{R}^2)$ gives $f|_{S^1} \in \mathcal{O}(S^1)$.

Moreover $f, g \in \mathcal{O}(V)$ restricted to the same function on $S^1$ iff

$f - g \in \langle x^2 + y^2 - 1 \rangle$

meaning $f - g = (x^2 + y^2 - 1)h$ for some $h \in \mathcal{O}(V)$.

Algebraic geometry is the study of geometry using commutative rings.

Our idea is: subspaces of $V$ should correspond to quotient rings of $\mathcal{O}(V)$, or ideals of $\mathcal{O}(V)$.
Problems:

1) What about \( \langle x^2 + y^2 + 1 \rangle \subseteq O(\mathbb{R}^2) \)

\[ \{ h : h \in O(\mathbb{R}^2) \} \]

The function \( x^2 + y^2 + 1 \) doesn't vanish on \( \mathbb{R}^2 \), so it seems the subspace of \( \mathbb{R}^2 \) corresponding to the ideal is \( \emptyset \).

But there's another, simpler ideal that corresponds to \( \emptyset \subseteq \mathbb{R}^2 \).

Namely \( \langle 1 \rangle \).

\[ \emptyset = \{(x, y) : 1 = 0\} \]

We're getting 2 ideals corresponding to the same subspace.

One way out: use \( \mathbb{C} \) instead of \( \mathbb{R} \).

2) Alas, using \( \mathbb{C} \) doesn't completely fix the problem:

2 different ideals can correspond to the same subspace

\[ \mathbb{C}^2 \]

There is a (complex) line in \( \mathbb{C}^2 \) given by \( x = y \), with ideal \( \langle x - y \rangle \subseteq \mathbb{C}[x, y] \).

But \( (x - y)^2 \) also vanishes only on this line, so we're getting a different ideal defining the same subspace \( \langle (x - y)^2 \rangle \subseteq \mathbb{C}[x, y] \).

Algebraic geometers came up with a way around this...

But Grothendieck came along and found a better solution.

He cut the Gordian knot, and defined a new kind of space called an affine scheme such that the correspondence between algebra and geometry is perfect.
We're going to make up a category $\text{AffSch}$ whose objects are "affine schemes" and morphisms are maps between them, such that $\text{AffSch}^{op} = \text{CommRing}^{op}$.

What is $\text{AffSch}^{op}$?

Take $\text{op}$ of both sides:

$$(\text{AffSch}^{op})^{op} = \text{CommRing}^{op}$$

or $\text{AffSch} = \text{CommRing}^{op}$

**Example**

the circle is an affine scheme, namely the comm. ring:

$$\mathbb{Z}[x,y]/\langle x^2 + y^2 - 1 \rangle$$

The plane is an affine scheme, $\mathbb{Z}[x,y]$.

"The circle is included in the plane" means we have a homomorphism of comm. rings:

$$\mathbb{Z}[x,y] \longrightarrow \mathbb{Z}[x,y]/\langle x^2 + y^2 - 1 \rangle$$

namely the quotient map.

We also have: $\mathbb{R}[x,y] \longrightarrow \mathbb{R}[x,y]/\langle x^2 + y^2 - 1 \rangle$.

In "noncommutative geometry" we try to invent some new kind of "space" so that $\text{AffSch} = \text{CommRing}^{op}$ gets generalized to something like $??? = \text{Ring}^{op}$. 


Look at $\text{CHaus} = \text{[compact Hausdorff space, continuous maps]}$

From a compact Hausdorff space $X$ on algebra $C(X)$:

\[ C(X) = \{ f : X \to \mathbb{C} : f \text{ is continuous} \} \]

This is an algebra with:
\[
(f + g)(x) = f(x) + g(x) \\
(fg)(x) = f(x)g(x) \\
(cf)(x) = cf(x) \quad c \in \mathbb{C}
\]

It’s a commutative algebra.

It’s a $*$-algebra with $(f^*)(x) = \overline{f(x)}$,
meaning an algebra $A$ with $*: A \to A$ s.t.
\[
(f+g)^* = f^* + g^* \\
(fg)^* = g^* f^* \\
(cf)^* = \overline{c} f^*
\]

Also, $C(X)$ has a norm $\|f\| = \sup_{x \in X} |f(x)|$. This makes sense since $X$ is compact.

This makes $C(X)$ into a $C^*$-algebra, meaning that:
\[
\|fg\| \leq \|f\| \|g\| \\
\|f^*\| = \|f\| \\
\|f^* f\| = \|f\|^2 \\
\|f^* f\| = \sup_{x \in X} (f^* f)(x) \\
= \sup_{x \in X} |f(x)|^2 \\
= (\sup_{x \in X} |f(x)|)^2 \\
= \|f\|^2
\]

So $C(X)$ is a commutative $C^*$-alg.
A homomorphism between C*-algebras, say $F : A \to B$, is a map s.t.

- $F(a+b) = F(a) + F(b)$, $a, b \in A$
- $F(ab) = F(a)F(b)$
- $F(ca) = cF(a)$, $c \in C$
- $F(a^*) = F(a)^*$

$\exists K > 0$ s.t. $\|F(a)\| \leq K \|a\|$ all $a \in A$

All these imply $\|F(a)\| = \|a\|$. So we get a category

$$\text{Comm C*Alg} = \{\text{comm. C*-algebras, C*-algebra homomorphisms}\}$$

How does a cont. map $\Psi : X \to Y$ between compact Hausdorff spaces give a C*-alg. homo. between $C(X)$ and $C(Y)$?

We'll get one $\Psi^* : C(Y) \to C(X)$

by: $\Psi^*(f)(x) = f(\Psi(x))$, $f \in C(Y)$, $x \in X$

or: $\Psi^*(f) = f \circ \Psi$

This is why algebra is the "dual" of geometry - it goes backwards:

$\Psi : X \to Y$ gives $\Psi^* : C(Y) \to C(X)$

Also $(\Psi \circ \Psi)^* = \Psi^* \circ \Psi^*$ (check this)
So we're getting a functor:
\[ C : \text{Chaus} \rightarrow \text{Comm } C^* \text{-Alg}^{op} \]
\[ x \mapsto C(x) \]
\[ \phi : x \rightarrow y \mapsto \phi^* : C(y) \rightarrow C(x) \]

Gelfand–Naimark Thm: This functor is an equivalence of categories.
I.e. there's a functor going back:
\[ \text{Spec} : \text{Comm } C^* \text{-Alg}^{op} \rightarrow \text{Chaus} \]
\[ \text{s.t. } \text{Spec} : C \cong \text{Chaus} \text{ and } \text{Co Spec} \cong \text{Comm } C^* \text{-Alg}. \]

\[ \text{natural isomorphism} \]

What's Spec?
Given a comm. \( C^* \)-alg. \( A \), how do we get a space \( \text{Spec}(A) \)?

Let's do \( A = C(X) \).
Then \( \text{Spec}(C(X)) \) should give back \( X \).
How do we recover the points of \( X \) starting from \( C(X) \)?

What's a point in \( X \)?
In terms of \( \text{Chaus} \), what's a point of \( X \)?
It's a map \( \phi : \{ * \} \rightarrow X \) where \( \{ * \} \) is the one-point space.

\[ \phi : \{ * \} \rightarrow X \]
\[ 1 \rightarrow x \]

\[ \text{c.e. given } x \in X \text{ there's a map } \]
\[ \phi : \{ * \} \rightarrow X \]

\[ \text{conversely any map } \phi : \{ * \} \rightarrow X \]
\[ \text{determines a point in } X. \]

Our functor \( C : \text{Chaus} \rightarrow \text{Comm } C^* \text{-alg} \) will turn \( \phi : \{ * \} \rightarrow X \)
into a homomorphism
\[ \phi^* : C(X) \rightarrow C(\{ * \}) \]
\[ f \mapsto f \circ \phi \]

In fact, \( C(\{ * \}) \cong C \) where \( g \in C(\{ * \}) \) gives \( g(*) \in C \)

So we get
\[ \phi^* : C(X) \rightarrow C(\{ * \}) \rightarrow C \]
\[ f \mapsto f \circ \phi \mapsto f \circ \phi(*) \]
A point $x \in X$

$\varphi$ \rightarrow \text{Gives a homorphism } C(X) \rightarrow \mathbb{C}$

\[ f \mapsto \varphi(f(x)) \]

In short: any point $x \in X$ gives a homorphism from $C(X)$ to $\mathbb{C}$ called evaluation at $x$. 

Lemma: Distinct points of $X$ give distinct homomorphisms $C(X) \rightarrow \mathbb{C}$. 

(“There are enough continuous functions to separate points” for a compact Hausdorff space.) 

Lemma: Any $C^*$-alg. homomorphism $\Psi: C(X) \rightarrow \mathbb{C}$ comes from a point $x \in X$ via: $\Psi(f) = f(x)$ for all $f \in C(X)$.

So we get a 1-1 correspondence between points $x \in X$ and homomorphisms $\Psi: C(X) \rightarrow \mathbb{C}$.

So given any comm. $C^*$-algebra $A$ we define a set of points

$\text{Spec}(A) = \{ \Psi: A \rightarrow \mathbb{C} : \Psi \text{ is a } C^* \text{-alg. homomorphism} \}$

There's a topology making $\text{Spec}(A)$ into a compact Hausdorff space. In this topology $\Psi_e$ converges to $\Psi$ iff $\Psi_e(a) \rightarrow \Psi(a)$ for all $a \in A$.

Finally, given a $C^*$-alg. hom. $F: A \rightarrow B$, how do we get a map of spaces $\text{Spec}(F): \text{Spec}(B) \rightarrow \text{Spec}(A)$?

$\text{Spec}(F)(\Psi)(a) = \Psi(F(a))$ for all $a \in A$

$F(a) \in B$

$\Psi(F(a)) \in \mathbb{C}$
So we get functors $c$

$C$-Haus $\xrightarrow{\text{spec}}$ Comm. $C^*\text{Alg}_0$

which are inverses (up to nat. iso.)

**Note**

fractions on the space $\xrightarrow{\text{spectrum}}$ Comm Rings

Point in a space $\xrightarrow{\text{Homomorphism from a comm. ring to a field}}$

Subspace $\xrightarrow{\text{inclusion } Y \hookrightarrow X}$

$\xrightarrow{\text{quotient ring or ideal}}$ (surjection or epimorphism $R \twoheadrightarrow S$)

or monomorphism
The duality between set theory & logic:

The basic idea:

<table>
<thead>
<tr>
<th>Operations on subsets of ( X )</th>
<th>Logical operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U )</td>
<td>( \lor ) (or)</td>
</tr>
<tr>
<td>( \cap )</td>
<td>( \land ) (and)</td>
</tr>
<tr>
<td>( \emptyset )</td>
<td>( F = 0 )</td>
</tr>
<tr>
<td>( X )</td>
<td>( T = 1 )</td>
</tr>
<tr>
<td>complement</td>
<td>( \neg ) (not)</td>
</tr>
</tbody>
</table>

E.g., \( x \in S \cup T \iff x \in S \lor x \in T \)

Let's fit this into the same mold as last time.

We saw that given a compact Hausdorff space \( X \), we get a commutative \( C^* \)-alg.

\[ C(X) = \text{hom}_{\text{Top}}(X, C) \] (continuous maps from \( X \) to \( C \))

Also, given a comm. \( C^* \)-algebra \( A \), we get a compact Hausdorff space

\[ \text{Spec}(A) = \text{hom}_{\text{comm. C^*Alg}}(A, C) \] (homomorphisms of \( C^* \)-algebras)

We call \( C \) have a dualizing object:

the same object \( x \) in 2 different categories \( C \) & \( D \) such that

\[ C \rightarrow D^\text{op} \]

\[ c \rightarrow \text{hom}_{C}(c, x) \in D \]

&

\[ D^\text{op} \rightarrow C \]

\[ d \rightarrow \text{hom}_{D}(d, x) \in C \]

are inverses,

so \( C \) & \( D^\text{op} \) are equivalent.

Similarly, we'll relate sets & Boolean algebras using the dualizing object

\[ 2 = \{ 0, 1 \} \cong \{ F, T \} \]
Boolean algebras are a little bit like $C^*$-algebras, but:

<table>
<thead>
<tr>
<th>Comm. $C^*$-algebras</th>
<th>Boolean algebras</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2 = { F, T }</td>
</tr>
<tr>
<td>+</td>
<td>\lor</td>
</tr>
<tr>
<td>.</td>
<td>\land</td>
</tr>
<tr>
<td>0</td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>T</td>
</tr>
</tbody>
</table>

So, given a set $X$, we'll make a Boolean algebra

$$2^X = \text{hom}_\text{set}(X, 2)$$

An element here is a fn. $f : X \rightarrow \{ 0, 1 \}$.

Any subset $S \subseteq X$ gives such a fn:

$$\chi_S(x) = \begin{cases} 0 & x \notin S \\ 1 & x \in S \end{cases}$$

& conversely any such function gives a subset of $X$, so $2^X$ is just another way to think of the power set of $X$.

The operations $\lor, \land, \neg$ on subsets of $X$ corresponds to operations $\lor, \land, \neg$ on functions $f : X \rightarrow \{ 0, 1 \}$

$$\chi_{S \cup T} = \chi_S \lor \chi_T$$

where

$$\chi_S \lor \chi_T(x) = \chi_S(x) \lor \chi_T(x)$$

& so on.

$(2^X, \lor, \land, 0, 1)$ will be a Boolean algebra:

Note $S \subseteq T \iff \chi_S \leq \chi_T$

e.g. if $\chi_S(x) = 1$ then $\chi_T(x) = 1$

Note $\leq$ is not a separate concept:

$$\chi_S \leq \chi_T \iff \chi_S \land \chi_T = \chi_S$$

$$\iff \chi_S \lor \chi_T = \chi_T$$
A partially ordered set \((A, \leq)\) is called a lattice if every pair \(a, b \in A\) has a least upper bound \(a \lor b\) & greatest lower bound \(a \land b\), and also a least element \(0 = F\) and a greatest element \(1 = T\).

A distributive lattice is one where \(\land\) & \(\lor\) distribute over each other.

A Boolean algebra is a distributive lattice \(A\) where every element \(x \in A\) has a complement \(\neg x\), such that:

\[
x \land \neg x = F \quad x \lor \neg x = T
\]

(If a complement exists, it's unique.)

For any set \(S\), \(2^S\) is a Boolean algebra with pointwise defined \(\leq\):
given \(f, g \in 2^S\) we say \(f \leq g\) if \(f(x) \leq g(x)\) \(\forall x \in S\).

If this has pointwise defined \(\lor, \land, 0, 1, \& \neg\),

\[
e.g. \quad (\neg f)(x) = \neg f(x)
\]

Alas, not every Boolean algebra is isomorphic to one of this form!

The Boolean algebras of the form \(2^S\) are "complete atomic Boolean algebras".

A complete Boolean alg. \(A\) is one where every subset \(S \subseteq A\) has a l.u.b. \(\bigvee_{x \in S} x\) and g.l.b. \(\bigwedge_{x \in S} x\), and these distribute over each other.

An atom in a Boolean algebra \(A\) is an element \(x \in A\) s.t. \(x \neq 0\) and if \(y < x\) then \(y = 0\).

In \(2^S\) the atoms correspond to the elements of \(S\), or singletons \(\{s\} \subseteq S\).

A Boolean algebra \(A\) is atomic if \(\forall x \in A\), \(x = \bigvee\{y \in A : y \text{ are atoms}\}\).
There's a category CABA of complete atomic Boolean algebras & homomorphisms of complete Boolean algebras:
\[ Y : A \to B \text{ preserving } v, \wedge, 0, 1, \top, \bot, \land \]

There's a category Set of sets and functions.

**Thm** Set is equivalent to CABA via these functors
\[
\begin{align*}
\text{Set} & \to \text{CABA}^\text{op} \\
S & \mapsto 2^S = \text{hom}_{\text{Set}}(S, 2) \\
\text{and} \\
\text{CABA}^\text{op} & \to \text{Set} \\
A & \mapsto \text{hom}_{\text{CABA}}(A, 2)
\end{align*}
\]

where \( 2 = \{ F, T \} \) is a CABA in the obvious way.

Given a function \( Y : S \to T \) we get a complete Boolean alg. homo.
\[ Y^*(f)(s) = f(Y(s)) \quad f \in 2^T \quad \text{i.e. } f : T \to 2 \quad s \in S \]

This is called a pullback:

![Pullback diagram](image)

**Ex** \( \{ f \in L^\infty([0,1]) : f(x) = 0 \text{ or } 1 \text{ for all } x \in \mathbb{R} \} \)

This is a complete but not atomic Boolean algebra under pointwise operations.

(There are no atoms)
The opposite of the category of all Boolean algebras is the category of Stone spaces: compact Hausdorff spaces that are totally disconnected: every open set is closed (vice versa).

The Boolean algebra of a Stone space $X$ consists of its open subsets, with $A \cup B$ as "$\lor$"

$A \cap B$ as "$\land$"

$A^c$ as "$\neg$"

Let FinVect be the category of finite-dimensional vector spaces over favorite field (e.g. $\mathbb{R}$) & linear maps.

What's FinVect$^{op}$?

A typical morphism in FinVect is $T: \mathbb{R}^n \to \mathbb{R}^m$.

A morphism in FinVect$^{op}$ is thus $T^*: \mathbb{R}^m \to \mathbb{R}^n$ ....

suspiciously similar to the transpose $T^*: \mathbb{R}^m \to \mathbb{R}^n$ in FinVect.

In fact, we have an equivalence: FinVect $\rightarrow$ FinVect$^{op}$, with

$T: \mathbb{R}^n \to \mathbb{R}^m \mapsto T^*: \mathbb{R}^m \to \mathbb{R}^n$ in FinVect

in FinVect$^{op}$

c.e. $(T^*)^*: \mathbb{R}^n \to \mathbb{R}^m$ in FinVect$^{op}$

We can also get the equivalence FinVect $\cong$ FinVect$^{op}$ using $1 \in \mathbb{R}$ FinVect as our dualizing object:

$\text{FinVect} \to \text{FinVect}^{op}$

$V \mapsto \text{hom}(V, \mathbb{R}) = V^*$

$T: V \to W \mapsto T^*: W^* \to V^*$ in FinVect

$(T^*)^*: V^* \to W^*$ in FinVect$^{op}$

So, FinVect straddles the worlds of geometry & algebra, being its own opposite.
Also, the category \([\text{finite abelian group, group homomorphism}]\) is its own "op".

Galois Theory

Galois theory is secretly about dualities between posets.

**Def.** A poset is a partially ordered set \((S, \leq)\) where \(\leq\) is reflexive, transitive, and antisymmetric: \(x \leq y \land y \leq x \Rightarrow x = y\).

If \((S, \leq)\) is a poset, we get a category with elements of \(S\) as objects & there exists a unique morphism \(f: x \to y\) iff \(x \leq y\) (\(x, y \in S\)), and no morphisms \(f: x \to y\) otherwise.

In fact, the categories we get this way are precisely those with:
1) at most 1 morphism from any object \(x\) to any object \(y\)
2) if there are morphisms \(f: x \to y\) & \(g: y \to x\), then \(x = y\).

So to a category theorist, a poset is a category with these 2 properties.

Given categories of this kind, a functor is really just an order preserving map \(f: (S, \leq) \to (T, \leq)\), i.e. a function s.t. \(x \leq y\) in \(S\) \(\Rightarrow f(x) \leq f(y)\) in \(T\).

Given a category of this sort coming from the poset \((S, \leq)\), its opposite comes from the poset \((S, \leq^{op})\) where \(x \leq^{op} y\) iff \(y \leq x\).

We'll write \(x \geq y\) for \(x \leq^{op} y\).

What are adjoint functors between categories of this sort?

**Def.** Given categories \(C, D\), we say a functor \(L: C \to D\) is the left adjoint of a functor \(R: D \to C\), or \(R\) is the right adjoint of \(L\), if there is a natural 1-1 correspondence
\[
\text{hom}_D(Lx, y) \cong \text{hom}_C(x, R_y) \quad \forall x \in C, \ y \in D
\]
Let $L : \text{Set} \rightarrow \text{Grp}$ send any set $S$ to the free group on $S$ and $R : \text{Grp} \rightarrow \text{Set}$ send any group $G$ to its underlying set. Here $\text{hom}_{\text{Grp}}(LS, G) \cong \text{hom}_{\text{Set}}(S, RG)$.

What are adjoint functors between posets $(S, \leq)$ & $(T, \leq)$? It's a pair of order-preserving functions

$$L : (S, \leq) \quad \xrightarrow{\text{adjoint}} \quad (T, \leq) \quad \xleftarrow{\text{adjoint}} \quad R$$

such that: $Lx \leq y \iff x \leq Ry$

This comes from $\text{hom}_{\text{Pos}}(Lx, y) \cong \text{hom}_{\text{Pos}}(x, Ry)$.

**Def:** A pair of adjoint functors between posets is called a [Galois correspondence](#).

**Thm:** Suppose $(S, \leq) \xleftarrow{R} (T, \leq)$ is a Galois correspondence. Then we get an order-preserving map $RL : (S, \leq) \rightarrow (S, \leq)$.

Let's write $\bar{x}$ for $RLx$.

Then $x \leq \bar{x} \quad \forall x \in S$ \quad ($Lx \leq Lx \Rightarrow x \leq RLx$)

and $\bar{x} = \overline{\bar{x}} \quad \forall x \in S$.

So we say $\bar{\cdot}$ is a closure operator on the poset $(S, \leq)$.

Similarly write $y^\circ$ for $LRy$.

Then $y^\circ \leq y \quad \forall y \in T$

and $(y^\circ)^\circ = y^\circ \quad \forall y \in T$.

So $\circ$ behaves like the "interior" operation on subsets of a top. space — it's a closure operator on $(T, \leq)^\circ$.

Finally, $L & R$ give a bijection between closed elements of $S$ (meaning $x \in S$ w/ $\overline{x} = x$) & open elements of $T$ (meaning $y \in T$ s.t. $y^\circ = y$).
Suppose you have any kind of algebraic gadget - a set with some operations obeying some axioms.

E.g., monoids, groups, rings, fields.

Then we can define a "subgadget" of a gadget $k$ to be a subset $k \subseteq k$ closed under all the operations.

The gadgets $F$ with $k \subseteq F \subseteq k$ form a poset with $\leq$ as the partial ordering. Let's call this poset $D$.

Galois theory uses groups to study $D$.

Any gadget $k$ has a group $\text{Aut}(k)$ of "automorphisms", i.e., 1-1 & onto functions $g: k \rightarrow k$ that preserve all the operations.

E.g., $g(x+y) = gx + gy$
$g(xy) = (gx)(gy)$
$g(0) = 0$
$g(1) = 1$

We say an element $x \in k$ is fixed by $g \in \text{Aut}(k)$ if $gx = x$.

We say a subgadget $F \subseteq k$ is fixed by $g \in \text{Aut}(k)$ if $gx = x$ for each $x \in F$.

Note: the subset $\{g \in \text{Aut}(k) : g \text{ fixes } F \}$ is a subgroup of $\text{Aut}(k)$.

The subgroup of $\text{Aut}(k)$ fixing the subgadget $k \subseteq k$ is called the Galois group $G(K/k)$.

Let $C$ be the poset of subgroups of $G(K/k)$, where the partial ordering is $\subseteq$.
The idea is to use $C$ to study $D$.

We'll do this by constructing a Galois correspondence $C \overset{\sim}{\longrightarrow} \text{Pos } D$.

i.e., order-preserving maps obeying

$Lg \subseteq F \iff g \in RF$

What's $R$?

It maps gadgets $k \subseteq F \subseteq k$ to subgroups of the Galois group $G(K/k)$.

It works as follows:

$RF = \{g \in \text{Aut}(k) : g \text{ fixes } F\}$
To show $R: D^{op} \to C$ is order preserving (i.e. a functor) we need:

$k \leq F \leq F' \leq k \Rightarrow R(F) \leq R(F')$

This is true: if $g$ fixes $F'$ & $F \leq F'\leq$ then $g$ fixes $F$.

**What's $L$?**

It maps subgroups $h \leq G(K|L)$ to gadgets between $k$ & $k$.

It works as follows:

$Lh = \{ x \in k : h \text{ fixes } x \} = \{ x \in k : k \supset g \in G \text{ } g \text{ fixes } x \}$

Note: this is a subgadget of $k$!

To show $L: C \to D^{op}$ is order preserving we need:

$g \leq g' \leq G(K|L) \Rightarrow Lg \leq Lg'$

This is true: it says that if $x \in F$ is fixed by all $g \in G'$ then $h$ is fixed by all $g \in G$ (some $h \in h$)

**Next: why is $L: C \leftrightarrow D^{op}: R$ a Galois connection?**

i.e., why is $Lh \leq F \iff G \leq RF$

$Lh \leq F$ means everything fixed by $h$ is in $F$

$G \leq RF$ means everything fixing $F$ is in $G$.

These are just two ways of saying the same thing.

Now we can relate nice subgadgets $k \leq F \leq k$ & nice subgroups $h \leq G(K|L)$ using the theorem we saw last time...

...but now let's stick in an "op"...

**Thm** Suppose $L: C \leftrightarrow D^{op}: R$ is a Galois connection. Define

$C = RLc \quad c \in C$

$d = LRd \quad d \in D^{op}$

These are closure operators:

$c \leq \bar{c} \quad \bar{c} = \bar{c}$

$d \leq \bar{d} \quad \bar{d} = \bar{d}$ (where $\leq$ is ordering on $D$)

We say $c \in C$ is closed if $c \leq \bar{c}$, and similarly for $d \in D$. $L \& R$ give a $\Omega$ correspondence between closed elements of $C \&$ closed elements of $D$.

[If we would have done $C''$ instead, we would get open operators.]
In our application, what's a "closed" subgadget $k \leq F \leq K$?

It's one with $F = LRF$

$$= \{ g \in Aut(K) : g \text{ fixes } F \}$$

$$= \{ x \in K : x \text{ is fixed by all } g \text{ that fixes } F \}$$

So a subgadget $F$ is closed if it contains all $x \in K$ that are fixed by all $g \in \text{ Aut}(K)$ that fix $F$.

What's a "closed" subgroup $G \leq \text{ Aut}(K)$?

$G = RL G$

$$= R \{ x \in K : x \text{ is fixed by } G \}$$

$$= \{ g \in \text{ Aut}(K) : gx = x \text{ for all } x \text{ fixed by } G \}$$

So: a subgroup $G$ is closed if it's the group of all $g \in \text{ Aut}(K)$ that fix all $x$ fixed by $G$.

So: the hard part of Galois theory includes:

1) finding a more concrete characterization of the "closed" subfields $k \leq F \leq K$

2) Similarly for the closed subgroups

3) Understanding the poset $G$ - the poset of the Galois groups.
Grupoids

**Def.** A morphism $f : x \to y$ in a category has an inverse $g : y \to x$ if
\[ fg = 1_y \quad \text{and} \quad gf = 1_x \]
If $f$ has an inverse, it's unique so we write it as $f^{-1}$.

A morphism with an inverse is called an isomorphism.

If there's an isomorphism $f : x \to y$, we say $x$ & $y$ are isomorphic.

**Def.** A grupoid is a category where all morphisms are isomorphisms.

**Ex.** Any group $G$ gives a grupoid with one object, $*$, and morphisms $g : * \to *$ corresponding to elements $g \in G$, with composition coming from multiplication in $G$.

Conversely, any 1-object grupoid gives a group.
So a group is a 1-object grupoid.

More generally, if $C$ is any category & $x \in C$, the isomorphisms $f : x \to x$ form a group under composition, called the automorphism group $\text{Aut}(x)$.

\[ \text{Aut}(\square) \cong \mathbb{Z}_4 \]

(rotational symmetries)

**Ex.** Given any category $C$, there's a grupoid, the core of $C$, $C_0$, whose objects are those of $C$ & whose morphisms are the isomorphisms of $C$, composed as before.

**Ex.** If $\text{FinSet} = [\text{finite sets, functions}]$, then $\text{FinSet}_0 = [\text{finite sets, bijections}]$ and if $n$ is your favorite $n$-element set, $\text{Aut}(n) = S_n$, the symmetric group.
So $\text{FinSet}_0$ "unifies" all the symmetric groups.
Suppose \( G \) is a group acting on a set \( X \):
\[
\begin{align*}
\alpha : (g \times X) & \rightarrow X \\
(g, x) & \mapsto gx
\end{align*}
\]
Often people form the set \( X/G \), the quotient set where an element \([x]\) is an equivalence class of elements \( x \in X \) where \( x \sim y \) iff \( y = gx \) for some \( g \in G \).

But a "better" thing is to form the translation groupoid \( X//G \), where objects are elements \( x \in X \), a morphism from \( x \) to \( y \) is a pair \((g, x)\) where \( g \in G \) and \( gx = y \).

The composite of
\[
x \xrightarrow{(g, x)} y \quad \text{and} \quad y \xrightarrow{(h, y)} z
\]
is
\[
x \xrightarrow{(h, g, x)} z
\]
In \( X/G \), we say \( x \) and \( y \) are equal if \( gx = y \).
In \( X//G \), we say they are isomorphic, or more precisely, we have a chosen isomorphism \((g, x) : x \rightarrow y\).

To a first approximation, a "moduli space" is a set \( X/G \), given some obvious topology, while a "moduli stack" is a group \( X//G \), where the sets of objects & morphisms have topologies.

Let \( X \) be the set of line segments in the Euclidean plane. Let \( G \) be the Euclidean group of the plane:

- all bijections \( g : \mathbb{R}^2 \rightarrow \mathbb{R}^2 \) s.t. \( \|gp - gq\| < \|p - q\| \)
- i.e. \( g \) preserves distance

\( G \) acts on \( X \):

![Diagram of actions](image)

More precisely, \( X = \mathbb{R}^2 \times \mathbb{R}^2 \) & \( G \) acts on it via \( g(p, q) = (gp, gq) \)

We're not counting \( (p, q) \) as the same as \( (q, p) \).

We're allowing \( p = q \).
$X/G$ is the "moduli" space of line segments

$X/G \cong \mathbb{R}$

There's a line segment $(p,q)$ and also a line segment $(q,p)$, but $(p,q) \sim (q,p)$. So they have some equivalent class; they give a single point in $X/G$.

Next consider $X//G$

Now objects are line segments & morphisms are like:

$$(p,q) \sim (g \cdot p, g \cdot q)$$

where $g \cdot p = p'$ & $g \cdot q = q'$, as in the picture.

Given a groupoid $C$, we can form:

1) the set $\mathcal{C}$ of isomorphism classes of objects:
$$[x] \text{ where } [x] = [y] \text{ iff } x \sim y.$$

2) For any $[x] \in \mathcal{C}$, a group $\text{Aut}(x)$, where $x$ is any representative of $[x]$. (Note if $x \sim y$, then $\text{Aut}(x) \cong \text{Aut}(y)$ as groups.)

Then given a groupoid $C$, we can recover $C$ (up to equivalence) from $\mathcal{C}$ and all the groups $\text{Aut}(x)$ (one for each isomorphism class in $\mathcal{C}$).

**Ex:** $C = \text{Fin Set}$

$C \cong \mathbb{N}$

and for each $n \in \mathbb{N}$ we get a group $S_n$ which we've seen is (iso. to) $\text{Aut}(x)$ for any $x \in \text{Fin Set}$ with $n$ elements.

**Ex:** $C = X//G$, where $X$ is the set of line segments & $G$ is the Euclidean group of the plane.

$C \cong \mathbb{R}$

In general, $X//G = X/G$ because both are names for the set of equivalence classes $[x]$ where $x \sim y$ iff $y = gx \forall g \in G$.

But $X//G$ has more information, namely all the automorphism groups $\text{Aut}(x)$, one for each equivalence class.
So in our example, what's $\text{Aut}(G_{pq})$?

It's $\mathbb{Z}_2$ if $p \neq q$; since there is

\[ r_{pf} \quad r_{qf} \]

a reflection preserving $(p,q)$

If $p=q$, it's group $O(2)$ of all

orthogonal $2 \times 2$ matrices, i.e., all

rotations & reflections fixing $p \in \mathbb{R}^2$.  

\[ p = q \]
Moduli Spaces & Moduli Stacks

Given a groupoid $\mathcal{C}$, let $\mathcal{C}$ be the set of isomorphism classes of objects. Often $\mathcal{C}$ will have the structure of a space (e.g. a topological space, a manifold, an algebraic variety, a scheme, ...). Then $\mathcal{C}$ is called a moduli space.

**Ex.** If $G$ is a group acting on a set $X$, we get a groupoid $X//G$, the translation groupoid, where:

- objects are elements of $X$;
- morphisms $x \xrightarrow{(a,x)} y$ are pairs $x \in X, g \in G$, where $y = gx$.

Then $X//G \cong X/G$, where $X/G$ has elements $[x]$ with $x \sim y$ when $y = gx$ for some $g \in G$.

Recall

The groupoid $X//G$ is equivalent to the groupoid with:

- one object $[x]$ for each $[x] \in X/G$;
- one morphism $f : [x] \rightarrow [y]$ for each morphism $f : x \rightarrow y$ where $x$ is any chosen representative of the equivalence class $[x]$.

If $[x] \neq [y]$, there are no morphisms between them.

We often call $X//G$ a moduli space, and $X//G$ the moduli stack.

Last time we looked at an example:

**Ex.** "The moduli stack of line segments" in Euclidean geometry.

Here $X = \mathbb{R}^2 \times \mathbb{R}^2 \geq (p,q)$, $\mathcal{G} = O(2) \times \mathbb{R}^2$.

Here $G$ is the Euclidean group of the plane and we think of $(p,q)$ as a line segment with a chosen 1st & 2nd endpoint, which can be equal.

Then the moduli space is $X//G \cong [0,\infty)$, the space of lengths $[l(p,q)] \mapsto l(p,q)$.

The moduli stack $X//G$ keeps track of symmetries: $\text{Aut}([p,q]) \cong \text{Aut}((p,q))$

is the subgroup of $G$ consisting of all $g \in G$ with $(gp,qg) = (p,q)$.

$\text{Aut}((p,q)) \cong \mathbb{Z}/2$ if $p \neq q$

$\text{Aut}((p,q)) \cong O(2)$ if $p = q$.

$\cong SO(2) \otimes \mathbb{Z}_2$. 
So the moduli stack looks like

\[ \mathcal{M}_{\text{reflection}} \]

\[ \mathcal{M}_{\text{rotation}} \]

---

**Exercise**

"The moduli stack of triangles"

Let \( G = \text{the Euclidean group as before, but now let } X \text{ be the set of triangles:} \)

\[ X = \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \]

These are triangles with named vertices that can be equal.

The moduli space \( X/G \) is the set of isomorphism classes of triangles.

Now \( X/G \cong [0, \infty)^3 \)

\[ [(p, q, r)] \mapsto (|p-q|, |q-r|, |r-p|) \]

Here it seems that if \( p, q, r \) are all distinct, \((p, q, r)\) has automorphisms only the identity.

If we define a triangle to be an unordered triple of points in \( \mathbb{R}^2 \),

an equilateral triangle would have \( S_3 \) as automorphisms, and isosceles would have \( S_2 = \mathbb{Z}/2 \).

This gives a more interesting moduli stack.

---

**Exercise**

A Riemann surface is a 2-dim. smooth manifold with charts \( \varphi_i: U_i \rightarrow \mathbb{C} \)

s.t. \( \varphi_i \varphi_j^{-1} \) is analytic (=holomorphic)

- Every Riemann surface that's homeomorphic to the plane is isomorphic (as a Riemann surface) to \( \mathbb{C} \).
- Every Riemann surface homeomorphic to the sphere is isomorphic to the Riemann sphere \( \mathbb{CP}^1 \cong \mathbb{C}U\{0\} \)

There are lots of non-isomorphic ways to make a torus into a Riemann surface - these are elliptic curves.

Every elliptic curve is isomorphic to one of this form:

Take a lattice \( L \subseteq \mathbb{C} \), i.e. a subgroup of \( (\mathbb{C}, +, 0) \)

that's isomorphic to \( \mathbb{Z}^2 \), and form \( \mathbb{C}/L \), getting a torus with obvious charts \( \varphi_z: U \rightarrow \mathbb{C} \), and thus

an elliptic curve.
When do 2 lattices $L$ & $L'$ give isomorphic elliptic curves: $C/L \cong C/L'$?

**Answer:** iff $L' = \alpha L$ for some nonzero $\alpha \in \mathbb{C}$

There's a groupoid $C$ with:
- elliptic curves as objects
- isomorphisms of Riemann surfaces as morphisms

and we're seeing $C \cong X/\mathbb{Z}$

where $X$ is the set of lattices & $\mathbb{C} = \mathbb{C}^*$ (nonzero complex numbers with multiplication)

So $X/\mathbb{Z}$ is called the moduli space of elliptic curves, and $X/\mathbb{Z}$ is the moduli stack of elliptic curves.

There are 2 elliptic curves with a bigger automorphism group:

- Typical elliptic curve
  - has $\mathbb{Z}/2$ as symmetries
  - $180^\circ$ rotation

- Gaussian elliptic curve
  - has $\mathbb{Z}/4$ as automorphisms
  - $i^4 = 1$

- Eisenstein elliptic curve
  - has $\mathbb{Z}/6$ as automorphisms
Moduli Spaces & Moduli Stacks

Given a groupoid $\mathcal{C}$, let $\mathcal{C}$ be the set of isomorphism classes of objects. Often $\mathcal{C}$ will have the structure of a space (e.g. a topological space, a manifold, an algebraic variety, a scheme, ...). This $\mathcal{C}$ is called a moduli space.

**Ex.** If $G$ is a group acting on a set $X$, we get a groupoid $X//G$, the translation groupoid, where:
- objects are elements of $X$
- morphisms $x \xrightarrow{(g,x)} y$ are pairs $x \in X, g \in G$, where $y = gx$.

Then $X//G \cong X/G$ when $X/G$ has elements $[x]$ with $x \sim y$ when $y = gx$ for some $g \in G$.

Recall

**Thm.** The groupoid $X//G$ is equivalent to the groupoid with:
- one object $[X]$ for each $[x] \in X//G$
- one morphism $f: [x] \to [x]$ for each morphism $f: x \to x$ when $x$ is any chosen representative of the equivalence class $[x]$.

If $[x] \neq [y]$ there are no morphisms between them.

We often call $X//G$ a moduli space, and $X/G$ the moduli stack.

Last time we looked at an example:

**Ex.** The moduli stack of line segments in Euclidean geometry.

Here $X = \mathbb{R}^2 \times \mathbb{R}^2 \supset (p,q), \ G = O(2) \times \mathbb{R}^2$

Here $G$ is the Euclidean group of the plane and we think of $(p,q)$ as a line segment with a chosen 1st & 2nd endpoint, which can be equal.

Then the moduli space is $X//G \cong [0,\infty)$ the space of lengths $[(p,q)] \mapsto |p-q|$

The moduli stack $X//G$ keeps track of symmetries: $\text{Aut}((p,q)) \cong \text{Aut}((p,q))$

is the subgroup of $G$ consisting of all $g \in G$ with $(gp, gq) = (p,q)$

$\text{Aut}((p,q)) \cong \mathbb{Z}/2$ if $p \neq q$

$\text{Aut}((p,q)) \cong O(2)$ if $p = q$

$\cong S O(2) \times \mathbb{Z}/2$
So the moduli stack looks like

\[ \mathcal{M}_{\text{O(2)}} \to \mathcal{M}_{\text{reflection}} \]

\[ \mathcal{O} \]

Ex: "The moduli stack of triangles"

Let \( G = \text{the Euclidean group as before, but now let } X \text{ be the set of triangles:} \]

\[ X = \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \]

These are triangles with named vertices that can be equal.

The moduli space \( X/G \) is the set of isomorphism classes of triangles.

Now \( X/G \cong [0,\infty)^3 \)

\[ \left[ (p, q, r) \right] \mapsto \left[ (1-pq, 1-q^2, 1-r^2) \right] \]

Here it seems that if \( p, q, r \) are all distinct, \( (p, q, r) \) has no automorphisms only the identity.

If we define a triangle to be a unordered triple of points in \( \mathbb{R}^2 \),

an equilateral triangle would have \( S_3 \) as automorphisms, and isosceles

would have \( S_2 = \mathbb{Z}/2\mathbb{Z} \).

This gives a more interesting moduli stack.

Ex: A Riemann surface is a 2-dim. smooth manifold with charts \( Y_i: U_i \to \mathbb{C} \)

s.t. \( Y_i \circ Y_i^{-1} \) is analytic (=holomorphic)

- Every Riemann surface that's homeomorphic to the plane is isomorphic (as a

  Riemann surface) to \( \mathbb{C} \).
- Every Riemann surface homeomorphic to the sphere is isomorphic to the

  Riemann sphere \( \mathbb{CP}^1 \cong \mathbb{C}U\{0\} \).

There are lots of nonisomorphic ways to make a torus into a Riemann

surface - these are elliptic curves.

Every elliptic curve is isomorphic to one of this form:

take a lattice \( \Lambda \subset \mathbb{C} \), i.e. a subgroup of \( (\mathbb{C}, +) \)

that's isomorphic to \( \mathbb{Z}^2 \), and form \( \mathbb{C}/\Lambda \), getting a

torus with obvious charts \( Y_e: U \to \mathbb{C} \), and thus

an elliptic curve.
When do 2 lattices $L$ & $L'$ give isomorphic elliptic curves: $C/L \cong C/L'$?

Answer: iff $L' = \alpha L$ for some nonzero $\alpha \in \mathbb{C}$

There's a groupoid $C$ with:
- Elliptic curves as objects
- Isomorphisms of Riemann surfaces as morphisms

and we're seeing $C \cong X/\mathcal{G}$

where $X$ is the set of lattices & $\mathcal{G} = \mathbb{C}^*$ (nonzero complex numbers with multiplication)

So $X/\mathcal{G}$ is called the moduli space of elliptic curves, and $X/\mathcal{G}$ is the moduli stack of elliptic curves.

There are 2 elliptic curves with a bigger automorphism group:

- Typical elliptic curve has $\mathbb{Z}/2$ as symmetries:
  - $180^\circ$ rotation

- Gaussian elliptic curve has $\mathbb{Z}/4$ as automorphisms
  - $i^4 = 1$

- Eisenstein elliptic curve has $\mathbb{Z}/6$ as automorphisms
Klein Geometry

We've seen that:

• a geometry is a group \( G \)
• a type of figure in this geometry is a subgroup \( H \in G \)
• the set of figures of that type is \( G/H \) : a homogeneous \( G \)-space

How can we do geometry this way?

We need \( G \)-invariant relations between figures.

Example: projective plane geometry:

\( G = \text{PGL}(3, \mathbb{R}) \)

\( X = \{ \text{lines through the origin in } \mathbb{R}^3 \} = \{ \text{pts in } \mathbb{R}P^2 \} \)

\( X \) is a homogeneous \( G \)-space, so

\( X = G/H \) where \( H \subseteq G \) is the stabilizer of your favorite point \( p \in X \):

\( H = \{ h \in G : hp = p \} \)

An invariant relation between points is a relation, i.e., a subset \( R \subseteq X \times X \) s.t. \( (p, q) \in R \Rightarrow (gp, gq) \in R \) for all \( p, q \in X, g \in G \)

But the only invariant relation in this example are

\( p = q \) and \( p \neq q \)

because distance is not preserved by \( G \).

More interestingly, let \( Y = \{ A \subseteq B : A \text{ is a 1-dim subspace of } \mathbb{R}^3 \} \)

\( = \{ \text{flags} \} \)

where a flag is a point \( p \in \mathbb{R}P^2 \) lying on a line \( L \in \mathbb{R}P^2 \)

\( G \) acts transitively on \( Y \) (even the Euclidean group does), and there are various invariant relations between flags, i.e., subsets \( R \subseteq Y \times Y \)

invariant under \( G \).

For example:

One invariant relation between \( (p, L) \)

& \( (p', L') \) says \( p \approx p' \) and \( L \cong L' \)
Or: "\( L = L' \) and \( p \neq p' \)"

Or: "\( p \neq p' \) and \( L \neq L' \)"

Or: "\( p = p' \) and \( L = L' \)"

Or: "\( p \neq p' \) but \( L \neq L' \) and \( p \neq p' \)"

Or: "\( p \neq p' \) but \( L = L' \) and \( p \neq p' \)"

All of these relations are visible here:

"6 flags"

For any group \( G \), we can make up a category \( G\text{-Rel} \) where:
- objects are \( G \)-sets
- morphisms are invariant relations

where an invariant relation \( R: X \to Y \) from the \( G \)-set to the \( G \)-set \( Y \) is a relation, i.e. a subset \( R \subseteq X \times Y \) such that:
\[
(x,y) \in R \quad \Rightarrow \quad (g \cdot x, g \cdot y) \in R \quad \forall x \in X, y \in Y, g \in G
\]

How do we compose morphisms?

Given any relations \( R: X \to Y \) and \( S: Y \to Z \) (not necessarily invariant)
we can compose them to get \( S \circ R: X \to Z \):
\[
S \circ R = \{(x,z) \in X \times Z : \exists y \in Y \text{ s.t. } (x,y) \in R \text{ and } (y,z) \in S\}
\]

If \( R \) and \( S \) are invariant so is \( S \circ R \).

There's a category \( \text{Rel} \) where
- objects are sets
- morphisms are relations

Define
\[
\text{hom}(X,Y) = 2^{X \times Y}
\]
Recall: for any set $S$, $2^S$ is a CABA: a complete atomic boolean algebra, with

$\leq$ as $\leq$
$\cap$ as $\wedge$ ($= \text{glb}$)
$\cup$ as $\vee$ ($= \text{lub}$)
$\circ$ as $\sim$

So in Rel, $\text{hom}(X,Y)$ is not merely a set, it's a CABA. The same is true for $\text{GRel}$: e.g. if $R : X \to Y$, $S : X \to Y$ are invariant, so is $R \cap S, R \cup S, R^\circ$

In fact, Rel & GRel are "CABA-enriched categories".

What's an enriched category?

In category theory, we want to overthrow the tyranny of sets: instead of working in Set all the time, we try to prove results that hold in many categories. But the very definition of category use sets:

A category is a class of objects, and for each pair of objects $x, y$ a set $\text{hom}(x,y)$, and a composition function $\circ : \text{hom}(x,y) \times \text{hom}(y,z) \to \text{hom}(x,z)$ etc...

The idea in enriched cat. theory is to generalize, replacing Set by some other category $V$ and say:

A $V$-enriched category is a class of objects, and for each pair of objects $x, y$ an object $\text{hom}(x,y) \in V$, and a composition morphism in $V$:

$\circ : \text{hom}(x,y) \otimes \text{hom}(y,z) \to \text{hom}(x,z)$ etc...

Here we need $V$ to be a "monoidal category", i.e. a category with some sort of "tensor product" $\otimes$.

It turns out that CABA's form a monoidal category, so it makes sense to talk about a CABA-enriched category, & Rel & GRel are such.
Enriched Categories & internal monoids

A monoid is "the same" as a 1-object category: if you have a category \( C \) with one object \( x \), there's a monoid \( \text{hom}(x,x) \) with multiplication \( \circ : \text{hom}(x,x) \times \text{hom}(x,x) \rightarrow \text{hom}(x,x) \).

Conversely, given a monoid \( M \) you can build a category with one object \( x \) and \( \text{hom}(x,x) = M \), with composition being multiplication in \( M \).

More generally, suppose \( V \) is a monoidal category, i.e. a category with a tensor product: \( \otimes : V \times V \rightarrow V \).

Then recall a \( V \)-enriched category \( C \) has a class of objects and for any objects \( x,y \in C \), a "hom-object" \( \text{hom}(x,y) \in V \) & composition morphisms:

\[ \circ : \text{hom}(x,y) \otimes \text{hom}(y,z) \rightarrow \text{hom}(x,z) \]

A 1-object \( V \)-enriched category is the same as a monoid internal to \( V \), or monoid in \( V \), i.e. an object \( M \in V \) with a multiplication \( m : M \otimes M \rightarrow M \) that's associative and unital.

**Ex.** Suppose \( V = \text{AbGrp} \) with the usual tensor product of abelian groups.

Then a monoid in \( V \) is called a ring. (Ring has unit, but rng does not.)

It's an abelian group \( M \), with a multiplication \( m : M \otimes M \rightarrow M \) an abelian group homomorphism, i.e. a function \( m : M \times M \rightarrow M \) that's linear in each argument:

\[ (a+b) \cdot c = a \cdot c + b \cdot c \]
\[ a \cdot (b+c) = a \cdot b + a \cdot c \]

**Ex.** If \( V = \text{RMod} \) for some comm. ring \( R \), a monoid in \( V \) is called an \( R \)-algebra.

**Ex.** If \( V = \text{Top} \) with usual product \( \times \) of top'd spaces as \( \otimes \), a monoid in \( V \) is called a topological monoid.
Back to our favorite example: Klein geometry

Let $G$ be a group, and let $G\text{Rel}$ be the category with
$G$-sets as objects
$G$-invariant relations as morphisms.

This a CABA-enriched category. So if we take one object, i.e. one
$G$-set $X$, we can form a 1-object CABA-enriched category with
$X$ as the only object $\hom(X,X)$ is the only homset, or "hom - CABA".

**Ex1** Projective plane geometry

Take $G = \text{PGL}(3, \mathbb{R})$

$Y = \{\text{flags}\}$

$\mathcal{E}(p, L): p \in \mathbb{R}^3$ is a 1-dim subspace,
$L \subset \mathbb{R}^3$ is a 2-dim subspace,
$p \in L$

$\hom(Y,Y)$ is a monoid in CABA. What is it like?

Instead of describing all the elements, let’s just describe the atoms.

In general, given any group $G$ and any $G$-sets $X, Y$, what are the
atoms in $\hom(X,Y)$ like?

They’re invariant relations $R: X \rightarrow Y$

i.e. $R \subset X \times Y$ s.t. $(x,y) \in R \Rightarrow (gx, gy) \in R$

But they are the smallest non-empty subsets of this form. So, any
atom $R$ must contain a point $(x,y)$, and thus all points of
the form $(gx, gy)$ with $g \in G$. Indeed, any orbit
$\mathcal{E}(gx, gy): g \in G \in X \times Y$ is an atom in $\hom(X,Y)$.

So, if

$G = \text{PGL}(3, \mathbb{R})$

$Y = \{\text{flags}\}$

the atoms in $\hom(Y,Y)$ are the orbits of $G$ acting on $Y \times Y$.

e.g. the orbit of this

$\begin{array}{c}
\text{p}\text{p'}
\end{array}$

$x = (p, L)$

$y = (p', L')$

is the set of all pairs of flags sharing the point

( and no more!).
Last time we saw all 16 atoms in \( \text{hom}(4,4) \):

\[
\begin{align*}
A &\circ B, A = B \circ A \circ B \\
&\text{"nothing interesting"}
\end{align*}
\]

\[
\begin{align*}
P &\in L', \text{ but no more} \\
P' &\neq P, \text{ but no more}
\end{align*}
\]

\[
\begin{align*}
P &\neq P', \text{ but no more}
\end{align*}
\]

\[
\begin{align*}
\text{the flags are the same}
\end{align*}
\]

The relativity \( 1 \in \text{hom}(4,4) \) is "two flags are the same."

Note we can compose invariant relation \& \( |0| = 1 \)

Let \( A \in \text{hom}(4,4) \) be "having the same point but no more"

\[
A \circ A = A \cup I
\]

If you change the line on a flag twice, the result could be changing the line or getting back to the original flag.

Let \( B \in \text{hom}(4,4) \) be "having the same line but no more" and "changing the point."

\[
B \circ B = B \cup I
\]

\[
\begin{align*}
A \circ B &\text{ is one of our atoms, } "p' \in L \text{ but no more}"
\end{align*}
\]

\[
\begin{align*}
B \circ A &\text{ is another atom, } "p \in L' \text{ but no more}"
\end{align*}
\]

\[
\begin{align*}
A \circ B = B \circ A \circ B &\text{ is "nothing interesting"}
\end{align*}
\]

In fact this is a presentation for our monoid in \( \text{CABA, hom}(4,4) \).

If we draw \( A \) as \( X \) and \( B \) as \( I \) then \( A \circ B \circ A = B \circ A \circ B \) is called the "3rd Reidemeister move" or "Vonk Braid equation."

\[
\begin{align*}
= \quad =
\end{align*}
\]

This is the only relation in \( B_3 \), the 3-strand braid group.