Category Theory Seminar

Learn the def. of
- category $\mathcal{C}$
- functor $F: \mathcal{C} \longrightarrow \mathcal{C}'$
- natural transformation
$$\begin{tikzcd} \mathcal{C} \arrow[r, bend left, "F"{name=U}] \arrow[r, bend right, "F'"'{name=D}] & \mathcal{C}' \arrow[Rightarrow, from=U, to=D, "\alpha"'] \end{tikzcd}$$

Duality

Every category $\mathcal{C}$ has an <u>opposite</u> category $\mathcal{C}^{op}$
$\mathcal{C}^{op}$ has the same objects as $\mathcal{C}$,
but the morphisms are "turned around"
So there is a 1-1 correspondence between morphisms in $\mathcal{C}$ & morphisms in $\mathcal{C}^{op}$, with $f: x \longrightarrow y$ in $\mathcal{C}$ corresponding to a morphism $f^{op}: y \longrightarrow x$ in $\mathcal{C}^{op}$.

$$\begin{tikzcd} & y \arrow[dr, "g"] & \\ x \arrow[ur, "f"] \arrow[rr, "g\circ f"'] & & z \end{tikzcd}$$

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

In $\mathcal{C}^{op}$:
$$\begin{tikzcd} & y \arrow[dr, "f^{op}"] & \\ z \arrow[ur, "g^{op}"] \arrow[rr, "f^{op}\circ g^{op} = (g\circ f)^{op}"'] & & x \end{tikzcd}$$

In $\mathcal{C}$:
$$\begin{tikzcd} & y \arrow[dr, "g"] & \\ x \arrow[ur, "f"] \arrow[rr, "g\circ f"'] & & z \end{tikzcd}$$

The study of how categories $\mathcal{C}$ relate to their partners $\mathcal{C}^{op}$ is called <u>duality</u>.

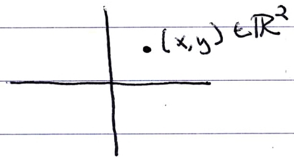
$\boxed{\text{Note}}$ $(\mathcal{C}^{op})^{op} = \mathcal{C}$
'just like' for finite-dim vector spaces $(V^*)^* \cong V$
natural isomorphism

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 & multiplication.



If $V=\mathbb{R}^n$, the algebra $\mathcal{O}(V)$ consists of polynomials in the coordinate functions $x_1,\dots,x_n$ $\quad \mathcal{O}(V) = \underbrace{\mathbb{R}[x_1,\dots,x_n]}_{\text{polynomials in } x_1,\dots,x_n}$

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:

$$X \xrightarrow[1\text{-}1]{} V$$

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

$$\mathcal{O}(V) \xrightarrow[\text{onto}]{} \mathcal{O}(X) = \mathcal{O}(V)/I \leftarrow \text{an ideal}$$

$\boxed{\text{Example}}$ 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 $\mathcal{O}(S^1) = \mathbb{R}[x,y]/\langle x^2+y^2-1\rangle \leftarrow$ the ideal generated by x^2+y^2-1

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

Problems:

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

$$\langle x^2+y^2+1\rangle = \{(x^2+y^2+1)h : h\in \mathcal{O}(\mathbb{R}^2)\}$$

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 $\emptyset$.

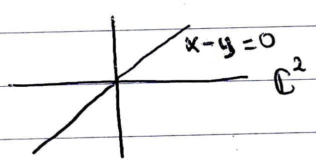
But there's another, simpler ideal that corresponds to $\emptyset \subseteq \mathbb{R}^2$. Namely $\langle 1\rangle$.

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

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



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 AffSch where objects are "affine schemes" and morphisms are maps between them, such that
$\text{AffSch}^{op} = \text{CommRing}$

What is AffSch?
Take op of both sides:
$(\text{AffSch}^{op})^{op} = \text{CommRing}^{op}$
OR $\text{AffSch} = \text{CommRing}^{op}$

$\boxed{\text{Example}}$ 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
$??? = \text{Ring}^{op}$

Geometry

Algebraic geometry:
$C = [\text{affine schemes}]$
Topology
$C = [\text{compact Hausdorff spaces}]$
Set theory
$C = [\text{sets}]$

Commutative Algebra

Ring Theory
$C^{op} = [\text{commutative rings}]$
C^*-algebra Theory
$C^{op} = [\text{commutative } C^*\text{-algebras}]$
Logic
$C^{op} = [\text{atomic Boolean algebras}]$

Look at CHaus = [compact Hausdorff space, continuous maps]
From a compact Hausdorff space X an algebra
$$C(X) = \{f : X \to \mathbb{C} : f \text{ is continuous}\}$$
This is an algebra with
$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$
$$(cf)(x) = cf(x) \qquad c \in \mathbb{C}$$
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.
$$(f+g)^* = f^* + g^*$$
$$(fg)^* = g^* f^*$$
$$(cf)^* = \bar{c} f^*$$

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:
$$\|fg\| \le \|f\|\,\|g\|$$
$$\|f^*\| = \|f\|$$
$$\|f^* f\| = \|f\|^2 \qquad \text{“}C^*\text{-axiom”}$$
$$\|f^* f\| = \sup_{x \in X} (f^* f)(x)$$
$$= \sup_{x \in X} |f(x)|^2$$
$$= \left(\sup_{x \in X} |f(x)|\right)^2$$
$$= \|f\|^2$$

So $C(X)$ is a commutative C^*-alg.

Next: can we take a morphism $\varphi : X \to Y$ in CHaus, that is a cont. map, and turn it into a (homo)morphism of comm. C^*-algebras.

A homomorphism between C^*-algs, say $F : A \to B$, is a map s.t.

$$F(a+b) = F(a) + F(b) \qquad a, b \in A$$
$$F(ab) = F(a)F(b)$$
$$F(ca) = cF(a) \qquad c \in \mathbb{C}$$
$$F(a^*) = F(a)^*$$
$$\exists\, K > 0 \text{ s.t. } \|F(a)\| < K\|a\| \quad \forall\, a \in A$$

All these imply $\|F(a)\| = \|a\|$

So we get a category
Comm C^*Alg = [comm. C^*-algebras, C^*-algebra homomorphisms]

How does a cont. map $\varphi : X \to Y$ between compact Hausdorff spaces give a C^*-alg. homo. between $C(X)$ and $C(Y)$?
We'll get one,

$$\varphi^* : C(Y) \longrightarrow C(X)$$

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

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

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[dr, bend right, "f\circ\varphi"'] & Y \arrow[d, "f"] \\ & \mathbb{C} \end{tikzcd}$$

$f \circ \varphi$
" $\varphi^* f$ "φ pullback of f"

This is why algebra is the "dual" of geometry - it goes backwards:
$\varphi : X \longrightarrow Y$ gives $\varphi^* : C(Y) \longrightarrow C(X)$
Also $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$ (check this)

So we're getting a functor:

$$\begin{aligned} C: \mathrm{CHaus} &\longrightarrow \mathrm{Comm}\ C^*\mathrm{Alg}^{op} \\ X &\longmapsto C(X) \\ \varphi: X \to Y &\longmapsto \varphi^*: C(Y) \to C(X) \end{aligned}$$

Gelfand-Naimark Thm: This functor is an equivalence of categories.

I.e. there's a functor going back:

$$\mathrm{Spec}: \mathrm{Comm}\ C^*\mathrm{Alg}^{op} \longrightarrow \mathrm{CHaus}$$

s.t. $\mathrm{Spec} \circ C \cong 1_{\mathrm{CHaus}}$ and $C \circ \mathrm{Spec} \cong 1_{\mathrm{Com}\ C^*\mathrm{Alg}}$.

natural isomorphism

What's Spec?

Given a comm. C^*-alg. A, how do we get a space $\mathrm{Spec}(A)$?

Let's do $A = C(X)$.

Then $\mathrm{Spec}(C(X))$ should give back X.

How do we recover the points of X starting from $C(X)$?

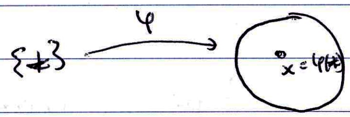
What's a point in X?

In terms of CHaus, what's a point of X?

It's a map $\varphi: \{*\} \longrightarrow X$ where $\{*\}$ is the one-point space.

i.e. given $x \in X$ there's a map

$$\begin{aligned} \varphi: \{*\} &\longrightarrow X \\ * &\longmapsto x \end{aligned}$$



& conversely any map $\varphi: \{*\} \longrightarrow X$ determines a point in X.

Our functor $C: \mathrm{CHaus} \to \mathrm{Comm}\ C^*\text{-alg}$ will turn $\varphi: \{*\} \to X$ into a homomorphism

$$\begin{aligned} \varphi^*: C(X) &\longrightarrow C(\{*\}) \\ f &\longmapsto f \circ \varphi \end{aligned}$$

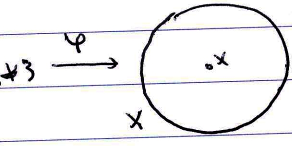
In fact $C(\{*\}) \cong \mathbb{C}$ where $g \in C(\{*\})$ gives $g(*) \in \mathbb{C}$

So we get

$$\begin{aligned} \varphi^*: C(X) &\longrightarrow C(\{*\}) \xrightarrow{\sim} \mathbb{C} \\ f &\longmapsto f \circ \varphi \longmapsto f \circ \varphi(*) \end{aligned}$$

$$f \circ \varphi(*) = f(x)$$

A point $x \in X$



gives a homorphism $C(X) \longrightarrow \mathbb{C}$
$f \longmapsto f(x)$

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

! pt $\forall$ hom.

$\boxed{\text{Lemma}}$ Distinct points of X give distinct homomorphisms $C(X) \to \mathbb{C}$.

("There are enough continuous functions to separate points" for a compact Hausdorff space)
$\to$ Stone - Weierstrass Theorem

$\exists$ pt $\forall$ hom.

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

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

So given any comm. C^*-algebra A we define a set of points
$\mathrm{Spec}(A) = \{\Psi : A \to \mathbb{C} : \Psi$ is a C^*-alg. homomorphism$\}$

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

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

$\mathrm{Spec}(F)(\Psi)(a) = \Psi(F(a))$ $\qquad$ $\Psi : B \to \mathbb{C}$ $\;$ C^*-alg homo.

$a \in A$

$F(a) \in B$

$\Psi(F(a)) \in \mathbb{C}$

So we get functors

$$\begin{tikzcd} \mathrm{CHaus} \arrow[r, bend left, "C"] & \text{Comm. } C^* \mathrm{Alg}^{op} \arrow[l, bend left, "\mathrm{Spec}"] \end{tikzcd}$$

which are inverses (up to nat. iso.)

$\boxed{\text{Note}}$

$$\begin{tikzcd} \text{Spaces} \arrow[r, bend left, "\text{functions on the space}"] & \text{Comm Rings} \arrow[l, bend left, "\text{spectrum}"] \end{tikzcd}$$

$$\begin{tikzcd} \text{Point in a space} \arrow[r, bend left] & \text{Homomorphism from a comm. ring to a field} \arrow[l, bend left] \end{tikzcd}$$

$$\begin{tikzcd} \text{Subspace} \arrow[r, bend left] & \text{Quotient ring or ideal} \arrow[l, bend left] \end{tikzcd}$$

(inclusion $X \hookrightarrow Y$) or monomorphism

(surjection or epimorphism $R \twoheadrightarrow S$)

The duality between set theory & logic.

The basic idea:

operations on subsets of X	logical operations
$\cup$	$\vee$ (or)
$\cap$	$\wedge$ (and)
$\emptyset$	$F = 0$
X	$T = 1$
complement	$\neg$ (not)

e.g. $x \in S \cup T \iff x \in S$ or $x \in T$
etc.

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.
$C(X) = \hom_{Top}(X, \mathbb{C})$ (continuous maps from X to $\mathbb{C}$)
Also, given a comm. C^*-algebra A, we get a compact Hausdorff space
$\mathrm{Spec}(A) = \hom_{Comm\, C^* Alg}(A, \mathbb{C})$ (homomorphisms of C^*-algebras)

We call $\mathbb{C}$ here a dualizing object:
"the same object x in 2 different categories $\mathcal{C}$ & $\mathcal{D}$" such that

$$\mathcal{C} \longrightarrow \mathcal{D}^{op}$$
$$c \longmapsto \hom_{\mathcal{C}}(c, x) \in \mathcal{D}$$ ← for some mysterious reason...

&

$$\mathcal{D}^{op} \longrightarrow \mathcal{C}$$
$$d \longmapsto \hom_{\mathcal{D}}(d, x) \in \mathcal{C}$$ ← for some mysterious reason...

are inverses,
so $\mathcal{C}$ & $\mathcal{D}^{op}$ 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:

Comm. C^*-algebras	Boolean algebras
$\mathbb{C}$	$2 = \{F, T\}$
$+$	$\vee$
$\cdot$	$\wedge$
0	F
1	T

So, given a set X, we'll make a Boolean algebra
$$2^X = \hom_{Set}(X, 2)$$
An element here is a fn. $f: X \longrightarrow \{0,1\}$.
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 $\cup, \cap, {}^c$ (complement) on subsets of X corr. to operations $\vee, \wedge, \neg$ on functions $f: X \longrightarrow \{0,1\}$
$$\chi_{S \cup T} = \chi_S \vee \chi_T$$
where $\chi_S \vee \chi_T(x) = \chi_S(x) \vee \chi_T(x)$
& so on.

$(2^S, \vee, \wedge, 0, 1)$ will be a Boolean algebra:

Note $S \subseteq T \iff \chi_S \leq \chi_T$
i.e. if $\chi_S(x) = 1$ then $\chi_T(x) = 1$
Note "$\leq$" is not a separate concept:
$$\chi_S \leq \chi_T \iff \chi_S \wedge \chi_T = \chi_S$$
$$\iff \chi_S \vee \chi_T = \chi_T$$

$\boxed{\text{Def}}$ A partially ordered set $(A, \leq)$ is called a lattice if every pair $a, b \in A$ has a least upper bound $a \vee b$ & greatest lower bound $a \wedge b$, and also a least element $0 = F$ and a greatest element $1 = T$.

$\boxed{\text{Def}}$ A distributive lattice is one where $\wedge$ & $\vee$ distribute over each other.

$\boxed{\text{Def}}$ A Boolean algebra is a distributive lattice A where every element $x \in A$ has a complement $\neg x$ such that

$$x \wedge \neg x = F \qquad x \vee \neg x = T$$

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

$\boxed{\text{Ex}}$ 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 $f(x) \leq g(x) \quad \forall x \in S$
It thus has pointwise defined $\vee, \wedge, 0, 1, \& \neg$,
e.g. $(\neg f)(x) = \neg f(x)$

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".

$\boxed{\text{Def}}$ 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.

$\boxed{\text{Def}}$ An atom in a Boolean algebra A is an element $x \in A$ s.t. $x \neq 0$ and if $y < x$ then $y = 0$.

$\boxed{\text{Ex}}$ In 2^S the atoms correspond to the elements of S, or singletons $\{s\} \subseteq S$.

$\boxed{\text{Def}}$ A Boolean algebra A is atomic if $\forall x \in A$, $x = \bigvee_{\lambda \in \Lambda} y_\lambda$ where $y_\lambda \in A$ are atoms.

There's a category CABA of complete atomic Boolean algebras & <u>homomorphisms</u> of complete Boolean algebras:
$\varphi : A \longrightarrow B$ preserving $\vee, \wedge, 0, 1, \neg, \bigvee, \bigwedge$

There's a category Set of sets and functions.

$\boxed{\text{Thm}}$ Set is equivalent to $CABA^{op}$ via these functors

$$\begin{aligned} \text{Set} &\longrightarrow CABA^{op} \\ S &\longmapsto 2^S = \hom_{\text{Set}}(S, 2) \end{aligned}$$

and

$$\begin{aligned} CABA^{op} &\longrightarrow \text{Set} \\ A &\longmapsto \hom_{CABA}(A, 2) \end{aligned}$$

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

Given a function $\varphi : S \longrightarrow T$ we get a complete Boolean alg. homo.

$\varphi^*(f)(s) = f(\varphi(s))$ $\quad f \in 2^T$ i.e. $f \in T \to 2$ $\quad s \in S$

This is called a pullback:

$$\begin{tikzcd} S \arrow[r, "\varphi"] \arrow[dr, bend right, "\varphi^* f = f \circ \varphi"'] & T \arrow[d, "f"] \\ & 2 \end{tikzcd}$$

$\boxed{\text{Ex}}$ $\{f \in L^\infty[0,1] : f(x) = \underset{F}{0} \text{ or } \underset{T}{1} \text{ for all } x \in X\}$

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

(There are no atoms)

10/19/15

Geometry	Algebra
Algebraic Geometry (affine schemes)	Commutative Rings
Topology (compact Hausdorff spaces)	Commutative C^*-algebras
Set Theory	Complete atomic Boolean algebras (Proposition Logic)
?	Boolean algebras
?	Linear algebra (finite-dim'l vector spaces)
?	Finite abelian groups

The opposite of the category of <u>all</u> Boolean algebras is the category of <u>Stone spaces</u>: compact Hausdorff spaces that are <u>totally disconnected</u>: 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 "$\vee$"

$A \cap B$ as "$\wedge$"

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 $T^{op} : \mathbb{R}^m \to \mathbb{R}^n$ .....

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

In fact, we have an equivalence $\text{FinVect} \xrightarrow{\sim} \text{FinVect}^{op}$, with

$T : \mathbb{R}^n \to \mathbb{R}^m \longmapsto T^t : \mathbb{R}^m \to \mathbb{R}^n$ in FinVect

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

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

$$\text{FinVect} \longrightarrow \text{FinVect}^{op}$$
$$V \longmapsto \hom(V, \mathbb{R}) = V^*$$
$$T : V \to W \longmapsto T^* : W^* \to V^* \text{ in FinVect}$$
$$(T^*)^{op} : V^* \to W^* \text{ in } \text{FinVect}^{op}$$

So, FinVect straddles the worlds of geometry & algebra, being its own opposite.

Also, the category [finite abelian groups, group homomorphisms] 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: $x \leq y$ & $y \leq x \Rightarrow x = y$.

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

$$\hom_D(Lx, y) \cong \hom_C(x, Ry) \qquad \forall x \in C, y \in D$$

$\boxed{\text{Ex}}$ Let $L: \text{Set} \to \text{Grp}$ send any set S to the free group on S and $R: \text{Grp} \to \text{Set}$ send any group G to its underlying set.

L=liberty! =freedom

Here $\hom_{\text{Grp}}(LS, G) \cong \hom_{\text{Set}}(S, RG)$

$\boxed{\text{Ex}}$ What are adjoint functors between posets $(S, \leq)$ & $(T, \leq)$?

It's a pair of order-preserving functions

$$\begin{tikzcd} (S,\leq) \arrow[r, bend left, "L"] & (T,\leq) \arrow[l, bend left, "R"] \end{tikzcd}$$

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

This comes from $\hom_D(Lx, y) \cong \hom_C(x, Ry)$

$\boxed{\text{Def}}$ A pair of adjoint functors between posets is called a <u>Galois correspondence</u>.

$\boxed{\text{Thm}}$ Suppose $(S,\leq) \underset{R}{\overset{L}{\rightleftarrows}} (T,\leq)$ is a Galois correspondence. Then we get an order-preserving map $RL: (S,\leq) \to (S,\leq)$.

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

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

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

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

Similarly write y° 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 $(T, \leq)^{op}$.

Finally, L & R give a bijection between <u>closed</u> elements of S (meaning $x \in S$ w/ $\bar{x} = x$) & <u>open</u> elements of T (meaning $y \in T$ s.t. $y^\circ = y$).

10/26/15

Galois Theory

Suppose you have any kind of algebraic gadget — a set with some operations obeying some axioms.

e.g. monoids, groups ($+, -, 0$), rings ($+, \times, 0, 1$), 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 $\subseteq$ as the partial ordering. Let's call this poset D.

Galois theory uses groups to study D.

Any gadget K has a group $\mathrm{Aut}(K)$ of "automorphisms", i.e. 1-1 & onto functions $g: K \to K$ 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 <u>fixed</u> by $g \in \mathrm{Aut}(K)$ if $gx = x$.

We say a subgadget $F \subseteq K$ is <u>fixed</u> by $g \in \mathrm{Aut}(K)$ if $gx = x$ for each $x \in F$.

$\boxed{\text{Note}}$ the subset $\{g \in \mathrm{Aut}(K) \mid g \text{ fixes } F\}$ is a subgroup of $\mathrm{Aut}(K)$.

The subgroup of $\mathrm{Aut}(K)$ fixing the subgadget $k \subseteq K$ is called the <u>Galois group</u> $G(K|k)$.

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 $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$

i.e. order-preserving maps obeying

$$LG \subseteq F \iff G \supseteq RF$$

What's R?

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

It works as follows:

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

To show $R: D^{op} \longrightarrow C$ is order preserving (i.e. a functor) we need:

$k \subseteq F \subseteq F' \subseteq K \Rightarrow R(F) \supseteq R(F')$

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

What's L?

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

It works as follows

$LG = \{x \in K : G \text{ fixes } x\}$

$= \{x \in K : \forall g \in G \;\; g \text{ fixes } x\}$ ← Note: this is a subgadget of K!

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

$G \subseteq G' \subseteq G(K|k) \Rightarrow LG \supseteq LG'$

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

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

i.e., why is $LG \subseteq F \iff G \supseteq RF$

$LG \subseteq F$ means every element of K everything fixed by G is in F

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

These are just two ways of saying the same thing.

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

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

$\boxed{\text{Thm}}$ Suppose $L: C \rightleftarrows D^{op} : R$ is a Galois connection. Define

$\bar{c} = RLc \qquad c \in C$

$\bar{d} = LRd \qquad d \in D^{op}$

These are <u>closure</u> <u>operators</u>: $c \leq \bar{c}$ & $\bar{c} = \bar{\bar{c}}$

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

We say $c \in C$ is closed if $c = \bar{c}$, and similarly for $d \in D$. L & R give a 1-1 correspondence between closed elements of C & closed elements of D.

[If we would have done C^{op} instead, we would get open operators.]

In our application, what's a "closed" subgadget $k \subseteq F \subseteq K$?

It's one with $F = LRF$

$= L\{g \in \mathrm{Aut}(G) : g \text{ fixes } F\}$

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

So a subgadget F is closed if it contains <u>all</u> $x \in K$ that are fixed by all $g \in G(K|k)$ that fix F.

What's a "closed" subgroup $G \subseteq G(K|k)$?

$G = RLG$

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

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

So: a subgroup G is closed if it's the group of all $g \in G(K|k)$ 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 $k \subseteq F \subseteq K$
2) Similarly for the closed subgroups
3) Understanding the poset C — the poset of the Galois groups.

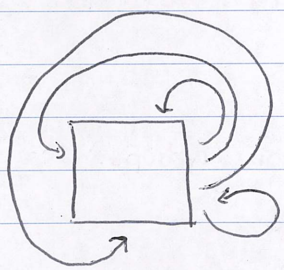
11/2/15

Groupoids

Def A morphism $f: x \to y$ in a category has an <u>inverse</u> $g: y \to x$ if $fg = 1_y$ & $gf = 1_x$.
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 <u>isomorphic</u>.

Def A <u>groupoid</u> is a category where all morphisms are isomorphisms.

Ex Any group G gives a groupoid with one object, $*$, and morphisms $g: * \to *$ corresponding to elements $g \in G$, with composition coming from multiplication in G.
Conversely any 1-object groupoid gives a group.
So "a group is a 1-object groupoid."
More generally, if C is any category & $x \in C$, the isomorphisms $f: x \to x$ form a group under composition, called the <u>automorphism group</u> $\mathrm{Aut}(x)$.



$\mathrm{Aut}(\square) \cong \mathbb{Z}_4$
(rotational symmetries)

Ex Given any category C there's a groupoid, the <u>core</u> of C, C_0, whose objects are those of C & whose morphisms are the isomorphisms of C, composed as before.

Ex If $\mathrm{FinSet} = [\text{finite sets, functions}]$
then $\mathrm{FinSet}_0 = [\text{finite sets, bijections}]$
and if n is your favorite n-element set, $\mathrm{Aut}(n) = S_n$, the symmetric group
So FinSet_0 "unifies" all the symmetric groups

$\boxed{\text{Ex}}$ Suppose G is a group acting on a set X:

$$\alpha : G \times X \longrightarrow X$$
$$(g,x) \longmapsto gx$$

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 $gx = y$.

$$x \xrightarrow{(g,x)} y$$

the composite of

$$x \xrightarrow{(g,x)} y \qquad \text{and} \qquad y \xrightarrow{(h,y)} z$$

is

$$x \xrightarrow{(hg,x)} z$$

In X/G, we say x & y are equal if $gx = y$

In $X/\!/G$, we say they are isomorphic, or more precisely, we have a chosen isomorphism $(g,x) : x \longrightarrow y$.

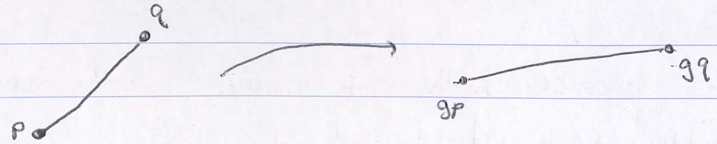
To a first approximation, a "moduli space" is a set X/G, given some obvious topology, while a "moduli stack" is a group $X/\!/G$, where the sets of objects & morphisms have topologies.

$\boxed{\text{Ex}}$ Let X be the set of line segments in the Euclidean plane. Let G be the Euclidean group of the plane:

all bijections $g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ s.t. $|gp - gq| = |p - q|$

i.e. g preserves distances

G acts on X:



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 $p = q$.

(continued)

X/G is the "moduli space of line segments"
$X/G \cong [0,\infty)$

⌜There's a line segment (p,q) and also a line segment (q,p), but $(p,q) \sim (q,p)$. So they have same equivalence class: they give a single point in X/G⌟

Next consider $X/\!/G$

Now objects are line segments & morphisms are like:

$$(p,q) \xrightarrow{(g,p,q)} (p',q')$$

where $gp = p'$ & $gq = q'$, as in the picture.

Given a groupoid C, we can form:

1) the set $\underline{C}$ of isomorphism classes of objects:
$[x]$ where $[x] = [y]$ iff $x \cong y$.
2) for any $[x] \in \underline{C}$, a group $\mathrm{Aut}(x)$, where x is any representative of $[x]$. (Note if $x \cong y$, then $\mathrm{Aut}(x) \cong \mathrm{Aut}(y)$ as groups.)

$\boxed{\text{Thm}}$ Given a groupoid C, we can recover C (up to equivalence) from $\underline{C}$ and all the groups $\mathrm{Aut}(x)$ (one for each isomorphism class in $\underline{C}$).

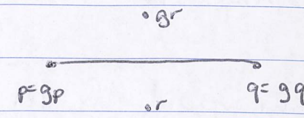
$\boxed{\text{Ex}}$ $C = \mathrm{FinSet}$
$\underline{C} \cong \mathbb{N}$
and for each $n \in \mathbb{N}$ we get a group S_n which we've seen is (iso. to) $\mathrm{Aut}(x)$ for any $x \in \mathrm{FinSet}$ with n elements.

$\boxed{\text{Ex}}$ $C = X/\!/G$ where X is the set of line segments & G is the Euclidean group of the plane.
$\underline{C} \cong [0,\infty)$

In general, $\underline{X/\!/G} = X/G$ because both are names for the set of equivalence classes $[x]$ where $x \sim y$ iff $y = gx$ $\exists\, g \in G$.
But $X/\!/G$ has more information, namely all the automorphism groups $\mathrm{Aut}(x)$, one for each equivalence class.

So in our example, what's $\mathrm{Aut}((p,q))$?

It's $\mathbb{Z}_2$ if $p \neq q$; since there is a reflection preserving (p,q)



If $p=q$ it's group $O(2)$ of all orthogonal 2×2 matrices, i.e. all rotations & reflections fixing $p \in \mathbb{R}^2$.

11/10/15

Moduli Spaces & Moduli Stacks

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

$\boxed{\text{Ex}}$ If G is a group acting on a set X, we get a groupoid $X/\!/G$, the <u>translation</u> 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 $\underline{X/\!/G} \cong X/G$ where X/G has elements $[x]$ with $x \sim y$ when $y = gx$ for some $g \in G$.

Recall

$\boxed{\text{Thm}}$ The groupoid $X/\!/G$ is equivalent to the groupoid with:

- one object $[x]$ for each $[x] \in X/G$
- one morphism $f : [x] \longrightarrow [x]$ for each morphism $f : x \longrightarrow x$ 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 <u>moduli space</u>, and $X/\!/G$ the <u>moduli stack</u>.

Last time we looked at an example:

$\boxed{\text{Ex}}$ "The moduli stack of line segments" in Euclidean geometry.

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

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.

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

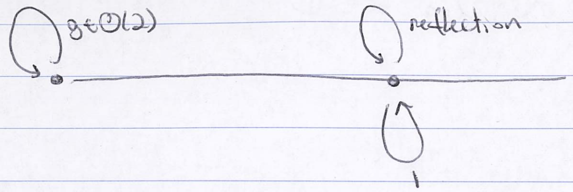
The moduli stack $X/\!/G$ keeps track of symmetries: $\text{Aut}[(p,q)] \cong \text{Aut}((p,q))$ is the subgroup of G consisting of all $g \in G$ with $(gp, gq) = (p,q)$

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

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

$\cong SO(2) \ltimes \mathbb{Z}_2$

So the moduli stack looks like



$\boxed{\text{Ex}}$ "The moduli stack of triangles"

Let G = the Euclidean group as before, but now let X 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 $\quad X/G \cong [0,\infty)^3$

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

Here it seems that if p, q, r are all distinct, (p,q,r) has as 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 isoceles would have $S_2 = \mathbb{Z}/2$.

This gives a more interesting moduli stack.

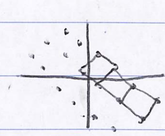
$\boxed{\text{Ex}}$ A Riemann surface is a 2-dim. smooth manifold with charts $\varphi_i : U_i \to \mathbb{C}$ s.t. $\varphi_i \varphi_j^{-1}$ is analytic (=holomorphic)

- 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 <u>Riemann sphere</u> $\mathbb{C}P^1 \cong \mathbb{C} \cup \{\infty\}$

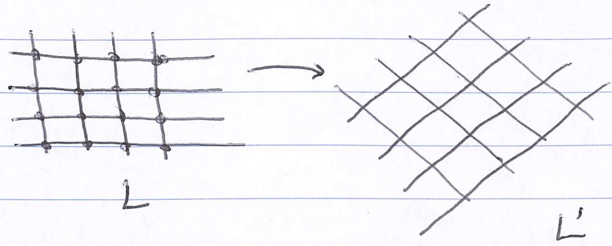
There are lots of nonisomorphic ways to make a torus into a Riemann surface — these are <u>elliptic curves</u>.

Every elliptic curve is isomorphic to one of this form:

take a <u>lattice</u> $L \subseteq \mathbb{C}$, 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 $\varphi_i : U_i \to \mathbb{C}$, and thus an elliptic curve.



When do 2 lattices L & L' give isomorphic elliptic curves: $\mathbb{C}/L \cong \mathbb{C}/L'$?
Answer: iff $L' = \alpha L$ for some nonzero $\alpha \in \mathbb{C}$



There's a groupoid $\underline{C}$ with

- elliptic curves as objects
- isomorphisms of Riemann surfaces as morphisms

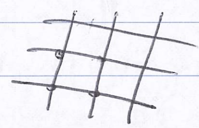
and we're seeing

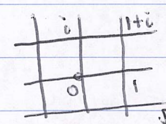
$\underline{C} \cong X/\!/G$

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

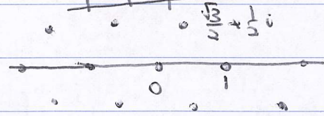
So X/G is called the <u>moduli space of elliptic curves</u>, and $X/\!/G$ is the <u>moduli stack</u> of elliptic curves.

There are 2 elliptic curves with a bigger automorphism group:

typical elliptic curve  has $\mathbb{Z}/2$ as symmetries
-180° rotation

Gaussian elliptic curve 

has $\mathbb{Z}/4$ as automorphisms
$i^4 = 1$

Eisenstein elliptic curve 

has $\mathbb{Z}/6$ as automorphisms

11/10/15

Moduli Spaces & Moduli Stacks

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

$\boxed{\text{Ex}}$ If G is a group acting on a set X, we get a groupoid $X/\!\!/G$, the <u>translation</u> 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 $\underline{X/\!\!/G} \cong X/G$ where X/G has elements $[x]$ with $x \sim y$ when $y = gx$ for some $g \in G$.

Recall

$\boxed{\text{Thm}}$ The groupoid $X/\!\!/G$ is equivalent to the groupoid with:

- one object $[x]$ for each $[x] \in X/G$
- one morphism $f: [x] \longrightarrow [x]$ for each morphism $f: x \longrightarrow x$ 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 <u>moduli space</u>, and $X/\!\!/G$ the <u>moduli stack</u>.

Last time we looked at an example:

$\boxed{\text{Ex}}$ "The moduli stack of line segments" in Euclidean geometry.

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

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

Then the moduli space is $X/G \cong [0,\infty)$ the space of lengths.

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

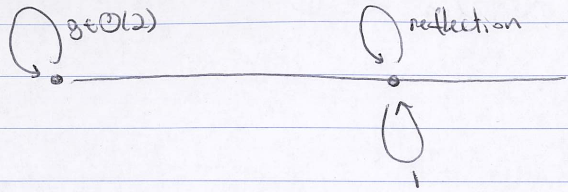
The moduli stack $X/\!\!/G$ keeps track of symmetries: $\mathrm{Aut}[(p,q)] \cong \mathrm{Aut}((p,q))$ is the subgroup of G consisting of all $g \in G$ with $(gp, gq) = (p,q)$

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

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

$\cong SO(2) \ltimes \mathbb{Z}_2$

So the moduli stack looks like



$\boxed{\text{Ex}}$ "The moduli stack of triangles"

Let G = the Euclidean group as before, but now let X 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 $\quad X/G \cong [0,\infty)^3$

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

Here it seems that if p,q,r are all distinct, (p,q,r) has as 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.

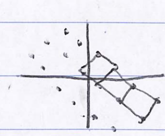
$\boxed{\text{Ex}}$ A Riemann surface is a 2-dim. smooth manifold with charts $\varphi_i : U_i \to \mathbb{C}$ s.t. $\varphi_i \varphi_j^{-1}$ is analytic (=holomorphic)

- 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 <u>Riemann sphere</u> $\mathbb{C}P^1 \cong \mathbb{C} \cup \{0\}$

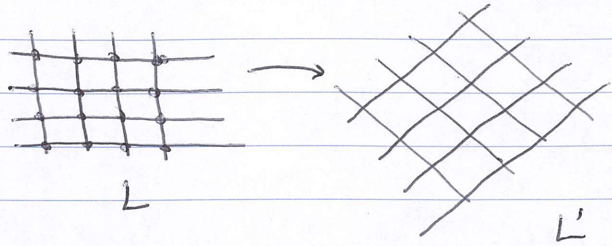
There are lots of nonisomorphic ways to make a torus into a Riemann surface — these are <u>elliptic curves</u>.

Every elliptic curve is isomorphic to one of this form:

take a <u>lattice</u> $L \subseteq \mathbb{C}$, 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 $\varphi_i : U_i \to \mathbb{C}$, and thus an elliptic curve.



When do 2 lattices L & L' give isomorphic elliptic curves: $\mathbb{C}/L \cong \mathbb{C}/L'$?
Answer: iff $L' = \alpha L$ for some nonzero $\alpha \in \mathbb{C}$



There's a groupoid $\underline{C}$ with

- elliptic curves as objects
- isomorphisms of Riemann surfaces as morphisms

and we're seeing

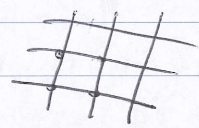
$\underline{C} \cong X/\!/G$

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

So X/G is called the <u>moduli space of elliptic curves</u>, and $X/\!/G$ is the <u>moduli stack</u> of elliptic curves.

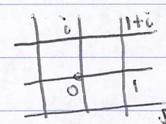
There are 2 elliptic curves with a bigger automorphism group:

typical elliptic curve



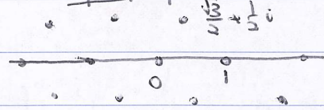
has $\mathbb{Z}/2$ as symmetries
-180° rotation

Gaussian elliptic curve



has $\mathbb{Z}/4$ as automorphisms
$i^4 = 1$

Eisenstein elliptic curve



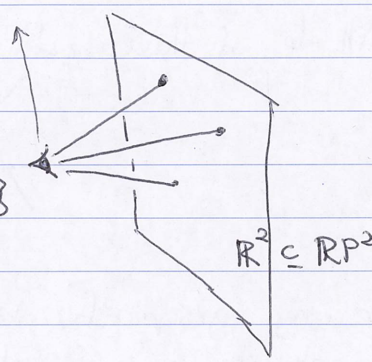
has $\mathbb{Z}/6$ as automorphisms

Klein Geometry

We've seen that:

- a <u>geometry</u> is a group G
- a <u>type of figure</u> in this geometry is a subgroup $H \subseteq G$
- 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.

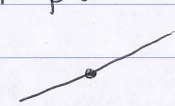


Ex projective plane geometry:
$G = PGL(3, \mathbb{R})$
$X = \{\text{lines through the origin in } \mathbb{R}^3\} = \{\text{pts in } \mathbb{RP}^2\}$
X is a homogeneous G-space, so
$X \cong G/H$ where $H \subseteq G$ is the stabilizer of your favorite point $p \in X$:
$H = \{h \in G : hp = p\}$

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 $p, q \in X$, $g \in G$

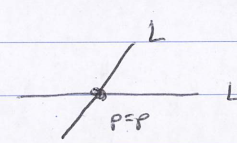
But the only invariant relations in this example are
$p = q$ and $p \neq q$
because distance is not preserved by G.

More interestingly, let $Y = \{A \subseteq B : A$ is a 1-dim. subspace of $\mathbb{R}^3$ & B is a 2-dim. subspace of $\mathbb{R}^3\}$
$= \{\text{flags}\}$
where a flag is a point $p \in \mathbb{RP}^2$ lying on a line $L \subseteq \mathbb{RP}^2$



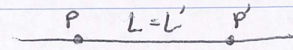
G acts transitively on Y (even the Euclidean group does), and there are various invariant relations between flags, i.e. subsets $R \subseteq Y \times Y$ invariant under G.

For example:
One invariant relation between (p, L) & (p', L') says "$p = p'$ and $L \neq L'$"

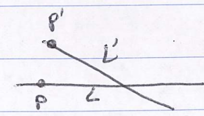


(continued)

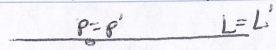
Or: "$L = L'$ and $p \neq p'$"



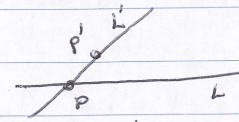
Or: "$p \neq p'$ and $L \neq L'$"



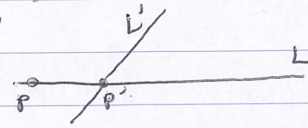
Or: "$p = p'$ and $L = L'$"



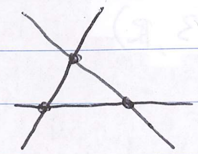
Or: "$p \in L'$ but $L \neq L'$ and $p \neq p'$"



Or: "$p' \in L$ but $L \neq L'$ and $p \neq p'$"



All 6 of these relations are visible here:



"6 flags"

For any group G, we can make up a category $G\mathrm{Rel}$ where:

- objects are G-sets
- morphisms are invariant relations

where an invariant relation $R: X \nrightarrow Y$ from the G-set to the G-set Y is a relation, i.e. a subset $R \subseteq X \times Y$ such that:

$$(x,y) \in R \Rightarrow (gx, gy) \in R \quad \forall\, x \in X,\ y \in Y,\ g \in G$$

How do we compose morphisms?

Given any relations $R: X \nrightarrow Y$ and $S: Y \nrightarrow Z$ (not nec. invariant) we can compose them to get $S \circ R: X \nrightarrow Z$:

$$S \circ R = \{(x,z) \in X \times Z : \exists\, y \in Y \text{ s.t. } (x,y) \in R \text{ and } (y,z) \in S\}$$

If R & S are invariant so is $S \circ R$.

There's a category Rel where

- objects are sets
- morphisms are relations

Here

$$\hom(X,Y) = 2^{X \times Y}$$

Recall: for any set S, 2^S is a CABA: a complete atomic boolean algebra, with

$\subseteq$ as $\leq$

$\cap$ as $\wedge$ ($=$glb)

$\cup$ as $\vee$ ($=$lub)

^{c} as $\neg$

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

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 $\hom(x,y)$, and a composition function

$\circ: \hom(x,y) \times \hom(y,z) \longrightarrow \hom(x,z)$

etc...

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

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

$\circ: \hom(x,y) \otimes \hom(y,z) \longrightarrow \hom(x,z)$

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 $\hom(x,x)$ with multiplication $\circ : \hom(x,x) \times \hom(x,x) \longrightarrow \hom(x,x)$
Conversely given a monoid M you can build a category with one object x and $\hom(x,x) = M$, with composition being multiplication in M.

More generally suppose V is a monoidal category, i.e. a category with a tensor product: $\otimes : V \times V \longrightarrow V$.
obeying some rules.

Then recall a <u>V-enriched</u> category C has a class of objects and for any objects $x,y \in C$, a "hom-object" $\hom(x,y) \in V$ & composition morphisms:
$\circ : \hom(x,y) \otimes \hom(y,z) \longrightarrow \hom(x,z)$

A 1-object V-enriched category is the same as a <u>monoid internal to V</u>, or <u>monoid in V</u>, i.e. an object $M \in V$ with a multiplication $m : M \otimes M \longrightarrow M$ that's associative and unital.

Ex Suppose $V = \mathrm{AbGp}$ 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 $m : M \otimes M \longrightarrow M$ an abelian group homomorphism, i.e. a function $m : M \times M \longrightarrow M$ 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 $V = R\mathrm{Mod}$ for some comm. ring R, a monoid in V is called an <u>R-algebra</u>.

Ex If $V = \mathrm{Top}$ with usual product $\times$ of top'l 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 $G\mathrm{Rel}$ 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".

$\boxed{\text{Ex}}$ Projective plane geometry

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

$$Y = \{\text{flags}\}$$
$$= \{(p,L) : p \subseteq \mathbb{R}^3 \text{ is a 1-dim'l subspace}, \; L \subseteq \mathbb{R}^3 \text{ is a 2-dim'l subspace}, \; p \subseteq L\}$$

$\hom(Y,Y)$ 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 $R : X \nrightarrow Y$

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

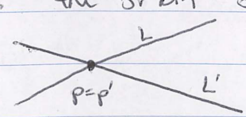
But they are the smallest nonempty subsets of this form. So, any atom R must contain a point (x,y), and thus all points of the form (gx, gy) with $g \in G$. Indeed, any orbit $\{(gx,gy) : g \in G\} \subseteq X \times Y$ is an atom in $\hom(X,Y)$.

So, if

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

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

e.g. the orbit of this

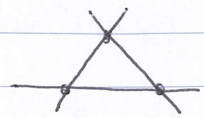


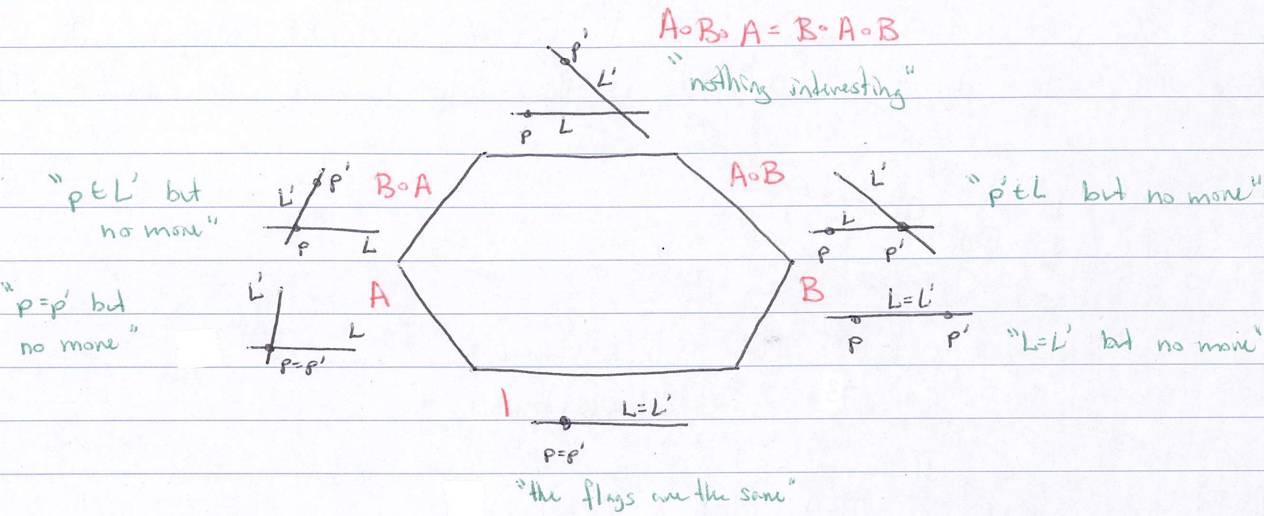
$x = (p, L)$

$y = (p', L')$

is the set of all pairs of flags sharing the point (and no more!).

Last time we saw all 6 atoms in $\hom(Y,Y)$:





The identity $1 \in \hom(Y,Y)$ is "two flags are the same"

Note we can compose invariant relation & $1 \circ 1 = 1$

Let $A \in \hom(Y,Y)$ be "having the same point but no more"

$A \circ A = A \cup 1$

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

Let $B \in \hom(Y,Y)$ be "having the same line but no more" and "changing the point"

$B \circ B = B \cup 1$

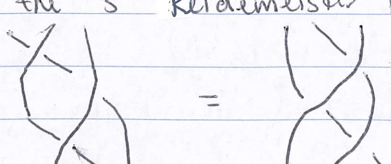
$A \circ B$ is one of our atoms, "$p' \in L$ but no more"

$B \circ A$ is another atom, "$p \in L'$ but no more"

$A \circ B \circ A = B \circ A \circ B$ is "nothing interesting"

In fact this is a presentation for our monoid in CABA, $\hom(Y,Y)$.

If we draw A as $\times|$ and B as $|\times$ then $A \circ B \circ A = B \circ A \circ B$ is called the "3rd Reidemeister move" or "Yang-Baxter equation":



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