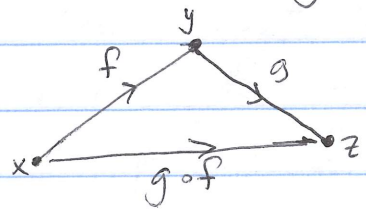
Legible, decent notes for A+

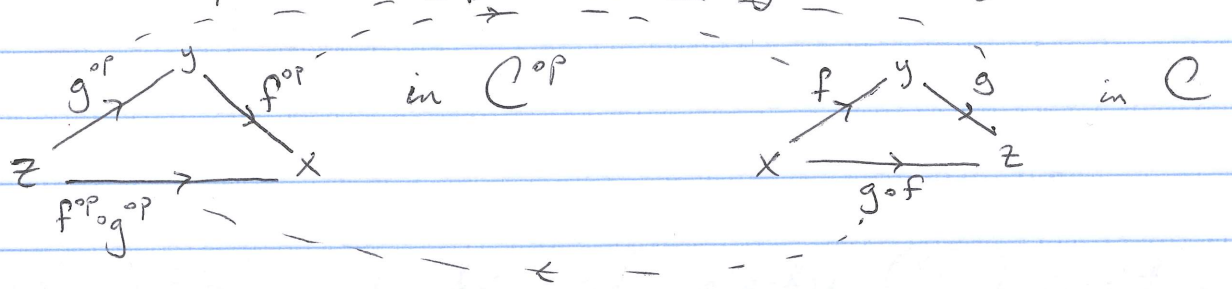
Duality

Every category C has an <u>opposite</u> C^{op}.
The objects of C and C^{op} are the same, but C^{op} "turns around" the arrows of C.
So there's a 1-1 correspondence between morphisms in C and in C^{op}, with $f: x \to y$ in C corresponding to a morphism $f^{op}: y \to x$ in C^{op}.



Composing morphisms:

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 <u>duality</u>. Should have $(C^{op})^{op} = C$. "Just like" for finite-dimensional vector spaces $(V^*)^* \cong V$

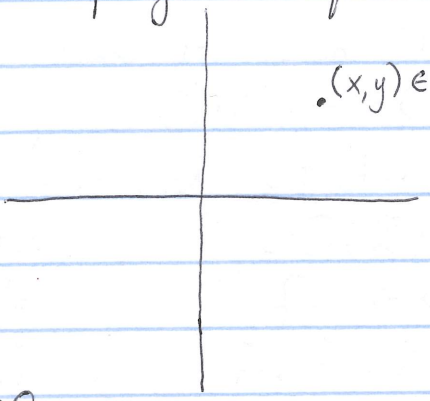
↖ natural isomorphism

It turns out that
"THE DUAL OF GEOMETRY IS ALGEBRA"

In geometry we study "points"; in algebra we study addition & multiplication (and fancier)

Greeks reasoned about algebra geometrically
Descartes realized a lot of geometry can reduce to algebra: this is called "analytic geometry".

We can associate to any finite-dimensional vector space V (over $\mathbb{R}$) a commutative ring $\mathcal{O}(V)$ consisting of all polynomial functions on V, with the usual $+$ and $\times$.



If $V = \mathbb{R}^n$, we have the algebra $\mathcal{O}(V)$ consisting of polynomials in the coordinate functions $x_1, \ldots, x_n$:

$$\mathcal{O}(V) = \underbrace{\mathbb{R}[x_1, \ldots, x_n]}_{\text{polynomials in } x_1, \ldots, x_n},$$

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:

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

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

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

(This is why people got interested in ideals)

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

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

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

Then there is an algebra $\mathcal{O}(S^1)$ of polynomial functions on the unit circle, with

$$\mathcal{O}(S^1) = \mathbb{R}[x,y]/\langle x^2+y^2-1\rangle$$

$\langle x^2+y^2-1\rangle$ ← the ideal generated by x^2+y^2-1

Thus the 1-1 map $S^1 \to \mathbb{R}^2$ 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, $f, g \in \mathcal{O}(\mathbb{R}^2)$ restrict to the same function on S^1

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

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

Algebraic geometry is the study of geometry using commutative rings.

Idea: Subspaces of V should correspond to quotient rings of $\mathcal{O}(V)$, or ideals of $\mathcal{O}(V)$.

Problems:

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

What space corresponds here? The empty set?

A "circle of radius i"? That doesn't live in $\mathbb{R}^2$.

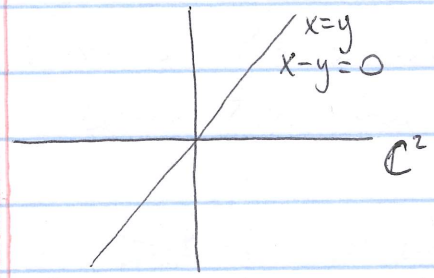
The function x^2+y^2+1 doesn't vanish on $\mathbb{R}^2$, so it seems the subspace of $\mathbb{R}^2$ corresponding to the ideal is $\emptyset$. But there is a simpler ideal that should correspond to $\emptyset$. Namely $\langle 1 \rangle$.

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

We get two different ideals corresponding to same subspace.

One way out: Use $\mathbb{C}$ instead of $\mathbb{R}$.

Problem 2) Using $\mathbb{C}$ doesn't completely fix the issue of two different ideals corresponding to the same subspace.



There's a (complex) line in $\mathbb{C}^2$ given by $x=y$, with ideal $\langle x-y \rangle$

$\langle x-y \rangle \subseteq \mathbb{C}[x,y]$

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

Algebraic geometers found a workaround, but...

Grothendieck found a better solution. He figured out what we want to do.

~~Instead~~ He cut the Gordian knot & defined a new kind of space called an affine scheme such that the correspondence between algebra & geometry is perfect.

We're going to make up a category AffSch where the objects are "affine schemes" & morphisms are maps between them, such that $\mathrm{AffSch}^{op} = \mathrm{CommRing}$

What is AffSch? Take op of both sides:

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

or $\mathrm{AffSch} = \mathrm{CommRing}^{op}$.

Example: the circle is an affine scheme; namely the commutative ring:

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

The ~~real~~ plane is another example of an affine scheme: ~~$\mathbb{R}[x,y]$~~ $\mathbb{Z}[x,y]$.

"The circle is included in the plane" means we have a homomorphism of commutative 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 a weirder notion of "space" so that $\mathrm{AffSch} = \mathrm{CommRing}^{op}$ gets generalized to something $= \mathrm{Ring}^{op}$

10/5/2015

GEOMETRY	COMMUTATIVE ALGEBRA
Algebraic geometry: $C = [\text{affine schemes}]$	Ring Theory: $C^{op} = [\text{commutative rings}]$
Topology: $C = [\text{compact Hausdorff spaces}]$	C^*-algebra Theory: $C^{op} = [\text{commutative } C^*\text{-algebras}]$
Set theory: $C = [\text{sets}]$	Logic: $C^{op} = [\text{atomic Boolean algebras}]$

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

From a compact Hausdorff space X, an algebra

$$C(X) = \{f : X \to \mathbb{C} : f \text{ is continuous}\}.$$

This is an algebra with

$$(f+g)(x) = f(x)+g(x), \quad (fg)(x) = f(x)g(x),$$
$$(cf)(x) = cf(x) \quad c \in \mathbb{C}.$$

It's a commutative algebra. Better, it's a <u>*-algebra</u> with $(f^*)(x) = \overline{f(x)}$, meaning an algebra A with $*: A \to A$ such that

$$(f+g)^* = f^* + g^*$$
$$(fg)^* = g^* f^*$$
$$(cf)^* = \bar{c} f^*$$

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 <u>C^*-algebra</u>, meaning that

$$\|fg\| \leq \|f\| \|g\|, \quad \|f^*\| = \|f\|, \text{ and}$$

"C^*-axiom": $\|f^* f\| = \|f\|^2$

$$\|f^*f\| = \sup_{x\in X} (f^*f)(x) = \sup_{x\in X} |f(x)|^2 = \left(\sup_{x\in X} |f(x)|\right)^2 = \|f\|^2.$$

So $C(X)$ is a commutative C^*-algebra. Next: morphisms.
Can we take a morphism $\phi: X \to Y$ in CHaus, i.e. a continuous map, and turn it into a (homo)morphism of commutative C^*-algebras?
A homomorphism between C^*-algebras, say $F: A \to B$, is a map such that

$F(a+b) =$
$F(ab) =$
$F(ca) =$ $\quad c \in \mathbb{C}$
$F(a^*) =$

The obvious things
$(F(a)+F(b),\ F(a)F(b),\ cF(a),\ F(a)^*)$

Assuming $\exists k>0$ such that $\|F(a)\| < k\|a\|$ $\forall a \in A$, all these imply $\|F(a)\| = \|a\|$.

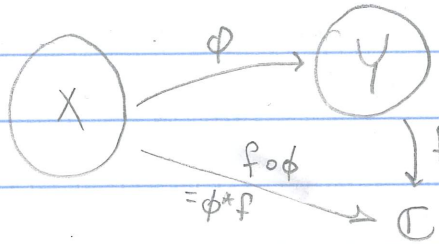
So we get a category $\mathrm{Comm}\,C^*\mathrm{Alg} = [\text{commutative } C^*\text{-algebras}, C^*\text{-algebra homomorphisms}]$

How does a continuous map $\phi: X \to Y$ between compact Hausdorff spaces give a C^*-algebra homomorphism between $C(X)$ & $C(Y)$?

We get one, $\phi^*: C(Y) \to C(X)$

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

or: $\phi^*(f) = f \circ \phi$ "ϕ pullback of f"



This is why algebra is the "dual" of geometry

This is why algebra is the "dual" of geometry – it goes backwards: $\phi: X \to Y$ gives

$$\phi^*: C(Y) \to C(X)$$

Also $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ (check this)

So we're getting a functor:

$$C: CHaus \longrightarrow Comm\,C^*Alg^{op}$$
$$X \longmapsto C(X)$$
$$\phi: X \to Y \longmapsto \phi^*: C(Y) \to C(X)$$

Gelfond–Naimark Thm: This functor is an equivalence of categories. I.e. There is a functor going back

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

such that $Spec \circ C \cong 1_{CHaus}$ (natural isomorphism)

$$C \circ Spec \cong 1_{Comm\,C^*Alg^{op}}$$

What is Spec? Given a commutative C^*-algebra A, how do we get a space $Spec(A)$?

Let's start with $A = C(X)$. Then $Spec(C(X))$ should give back X. How do we recover the points of X starting from $C(X)$? What's a point in X?

$\phi: \{*\} \to X$, where $\{*\}$ is the one-point space.

I.e. given $x \in X$ $\exists$ map

$$\phi: \{*\} \to X$$
$$* \longmapsto x$$

and conversely any map $\phi: \{x\} \to X$ determines a point in X.

Our functor $C : CHaus \to Comm\, C^*Alg$ will turn

$\phi : \{*\} \to X$ into a homomorphism

$$\phi^* : C(X) \to C(\{*\})$$
$$f \longmapsto f \circ \phi$$

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

So we get

$$\phi^* : C(X) \to C(\{*\}) \xrightarrow{\sim} \mathbb{C}$$
$$f \longmapsto f \circ \phi \longmapsto f \circ \phi(*)$$
$$\| \; f(x)$$

A point $x \in X$



gives $C(X) \to \mathbb{C}$

$f \longmapsto f(x)$ a homomorphism

Lemma - distinct points of X will give distinct homomorphisms $C(X) \to \mathbb{C}$

("There are enough continuous functions to separate points")

↳ True because of the Hausdorffness

Lemma - any C^*-algebra homomorphism $\psi : C(X) \to \mathbb{C}$ comes from a point $x \in X$ via:

$$\psi(f) = f(x) \quad \forall f \in C(X)$$

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

Given any commutative C^*-algebra A we define a set of points

$$Spec(A) = \{\psi : A \to \mathbb{C} : \psi \text{ is a } C^*\text{-algebra homomorphism}\}$$

There is a topology making $\mathrm{Spec}(A)$ into a compact Hausdorff space. In this topology

ψ_i converges to ψ iff

$\psi_i(a)$ converges to $\psi(a)$ $\forall a \in A$.

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

$\psi \in \mathrm{Spec}(B)$ $\quad \psi: B \to \mathbb{C}$ $\quad C^*$-algebra homomorphism

$$\underbrace{\underbrace{\mathrm{Spec}(F)(\psi)}_{\text{in } \mathrm{Spec}(A)}\ \underbrace{(a)}_{\in A}}_{\in \mathbb{C}} = \underbrace{\psi(\underbrace{F(a)}_{\in B})}_{\in \mathbb{C}}$$

So we get functors

$$\mathrm{CHaus} \underset{\mathrm{Spec}}{\overset{C}{\rightleftarrows}} \mathrm{Comm}\,C^*\mathrm{Alg}^{op}$$

which are inverses (up to natural isomorphism)

Note:

$$\mathrm{Spaces} \underset{\text{spectrum}}{\overset{\text{functions on the space}}{\rightleftarrows}} \text{Commutative Rings}$$

Point in a space $\rightleftarrows$ homomorphism from a commutative ring to a field

Subspace (inclusion $X \hookrightarrow Y$) monomorphism $\rightleftarrows$ Quotient ring or ideal (surjection or epimorphism $R \twoheadrightarrow$)

10/12/2015

The duality between set theory & logic

Idea:

Subset operations ($\forall x$)	Logic operations
$\cup$	$\vee$ (or)
$\cap$	$\wedge$ (and)
$\emptyset$	F (false)
X	T (true)
^{c} (complement)	$\neg$ (not)

e.g. $x \in S \cup T \iff x \in S \vee x \in T$

Last time we saw that given a compact Hausdorff space X, we get a commutative C^*-algebra

$$C(X) = \hom_{Top}(X, \mathbb{C})$$ (continuous maps from X to $\mathbb{C}$)

and, given a commutative C^*-algebra A, we get a compact Hausdorff space

$$Spec(A) = \hom_{CommC^*Alg}(A, \mathbb{C})$$ (homomorphisms of C^*-algebras)

We call $\mathbb{C}$ here a dualizing object: "the same object x in two 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...

and

$$\mathcal{D}^{op} \longrightarrow \mathcal{C}$$
$$d \longmapsto \hom_{\mathcal{D}}(d, x) \in \mathcal{C}$$

are inverse functors, so $\mathcal{C}$ & $\mathcal{D}^{op}$ are equivalent.

Let's make the mystery work again!
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:

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

Given a set X, we'll make a Boolean algebra

$$2^X = \hom_{Set}(X, 2).$$

An element here is a function $f: X \to \{0,1\}$. Any subset $S \subseteq X$ gives a characteristic function:

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

and 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 $\cup, \cap, {}^c$ on subsets of X correspond to operations $\vee, \wedge, \neg$ on functions $f: X \to \{0,1\}$

$$\chi_{S \cup T} = \chi_S \vee \chi_T \quad \text{where} \quad \chi_S \vee \chi_T = \chi_S(x) \vee \chi_T(x) \quad \text{etc.}$$

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

~~Def~~ Note: $S \subseteq T \Leftrightarrow \chi_S \leq \chi_T$

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

Note: "$\leq$" is not a separate concept:

$$\chi_S \leq \chi_T \Leftrightarrow \chi_S \wedge \chi_T = \chi_S$$
$$\Leftrightarrow \chi_S \vee \chi_T = \chi_T$$

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

Def: A distributive lattice is a lattice where $\wedge$ & $\vee$ distribute over each other.

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

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

(If a complement exists, it is unique)

Example: 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 $f(x) \leq g(x)$ $\forall x \in S$.

It thus has pointwise defined $\vee, \wedge, 0, 1, \neg$.

E.g. $(\neg f)(x) = \neg f(x)$

Not every Boolean algebra is isomorphic to one of this form! The Boolean algebras of the form 2^S are "complete atomic Boolean algebras".

Def: A complete Boolean algebra A is one where every subset $S \subseteq A$ has a least upper bound $\bigvee_{x \in S} x$ and greatest lower bound $\bigwedge_{x \in S} x$, and these distribute over each other.

Def: An <u>atom</u> in a Boolean algebra A is an element $x \in A$ such that $x \neq 0$ and if $y < x$ then $y = 0$.

Example: in 2^S the atoms correspond to the elements of S, or singletons $\{s\} \subseteq S$.

Def: A Boolean algebra is <u>atomic</u> if $\forall x \in A$, $x = \bigvee_{\lambda \in \Lambda} y_\lambda$ where $y_\lambda \in A$ are atoms.

There is a category CABA of complete atomic Boolean algebras and <u>homomorphisms</u> of complete Boolean algebras:

$\varphi : A \to B$ preserving $\vee, \wedge, 0, 1, \neg, \bigvee, \bigwedge$

enough to preserve these two

There is a category Set of sets & functions.

<u>Thm</u> Set is equivalent to $CABA^{op}$ via functors

$$\text{Set} \longrightarrow CABA^{op}$$
$$S \longmapsto 2^S = \hom_{\text{Set}}(S, 2) \quad \text{and}$$

$$CABA^{op} \longrightarrow \text{Set}$$
$$A \longmapsto \hom_{CABA}(A, 2), \quad \text{where } 2 = \{0,1\} \text{ is a CABA}$$

in the obvious way.

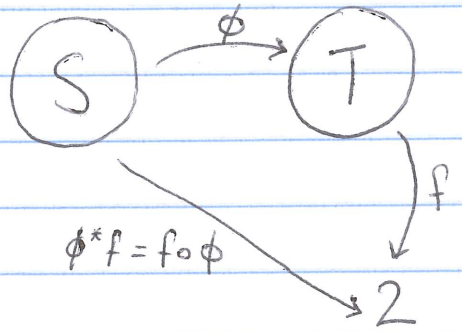
Given a function $\phi: S \to T$ we get a complete Boolean algebra homomorphism

$$\phi^*: 2^T \to 2^S \quad \text{by:}$$

$f \in 2^T$, $s \in S$

$$\underbrace{\phi^*(f)(s)}_{\in 2} = f(\phi(s))$$

This is called a pullback:



measurable subsets of $\mathbb{R}$

atomic but not complete Boolean algebra under pointwise operations

$$\{f \in L^\infty[0,1] : f(x) = 0 \text{ or } 1 \ \forall x \in X\}$$

F or T

Complete but not atomic Boolean algebra under pointwise operations.

10/19/15

GEOMETRY	ALGEBRA
Algebraic Geometry (affine schemes)	Commutative Rings
Topology (compact Hausdorff spaces)	Commutative C^*-algebras
Set Theory	Complete atomic Boolean algebras
?	Boolean algebras
?	Linear algebra (finite-dimensional vector spaces)
?	Finite abelian groups
	Propositional Logic

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 your favorite field (e.g. $\mathbb{R}$) & linear maps.
What is 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, $\text{FinVect}^{op} \cong \text{FinVect}$, with

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

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

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

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

Also, the category of [finite abelian groups, group homomorphisms] is its own "op" (but for different reasons)

In both cases you can break everything down into direct sums of building blocks

---

Change of theme

Galois Theory

Galois theory is secretly about dualities between posets.

Def: A <u>poset</u> is a partially ordered set $(S, \leq)$ where $\leq$ is reflexive, transitive & 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 two properties.

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

Given a ~~of~~ category of this sort coming from $(S, \leq)$, its opposite comes from the poset $(S, \leq^{op})$, where
$x \leq^{op} y$ ~~means~~ 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 ~~$R: D \to C$~~ $R: D \to C$ is the right adjoint of L, if there is a natural 1-1 correspondence

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

Example: Let $L: \mathrm{Set} \to \mathrm{Grp}$ (L = libre = freedom)
send any set S to the free group on S,
and $R: \mathrm{Grp} \to \mathrm{Set}$
send any group G to its underlying set.

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

What does this look like for posets?
Example: what are adjoint functors between posets $(S, \leq)$ and $(T, \leq)$?
It's a pair of order-preserving functions

$$(S, \leq) \underset{R}{\overset{L}{\rightleftarrows}} (T, \leq)$$

such that $Lx \leq y \iff x \leq Ry$.
This comes from $\hom_D(Lx, y) \cong \hom_C(x, Ry)$.

Def: A pair of adjoint functors between posets is called a Galois correspondence.

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

$$Lx \leq Lx \Rightarrow x \leq RLx$$

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 topological space – it's a closure operator on $(T, \leq)^{op}$.

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

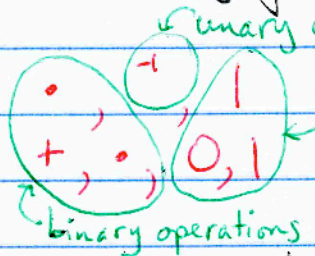
Later, we will replace T by T^{op} to make this "Finally" bit look nicer.

10/26/15

Galois Theory

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

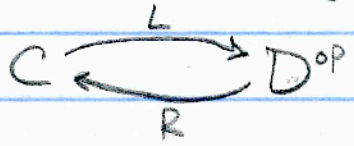
The gadgets F with $k \subseteq F \subseteq K$ form a poset with $\subseteq$ as the partial ordering. Let's call this poset D.
Galois theory uses groups to study D.
Any gadget K has a group $Aut(K)$ of "automorphisms", i.e. 1-1 & onto functions $g: K \to K$ that preserve all the operations,

e.g. (for rings)
$$g(x+y) = gx + gy$$
$$g(xy) = (gx)(gy)$$
$$g(0) = 0$$
$$g(1) = 1$$

We say an element $x \in K$ is <u>fixed</u> by $g \in Aut(K)$ if $gx = x$.
We say a subgadget $F \subseteq K$ is <u>fixed</u> by $g \in Aut(K)$ if $gx = x$ for each $x \in F$.
Notice: the subset $\{g \in Aut(K) : g \text{ fixes } F\}$ is a subgroup of $Aut(K)$.

The subgroup of $Aut(K)$ 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



i.e. order-preserving maps obeying $LG \subseteq F \Leftrightarrow G \supseteq RF$.

What's R? It maps gadgets $k \subseteq F \subseteq K$ to subgroups of $G(K|k)$. It works as follows:

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

To show $R: D^{op} \to C$ 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: it says that if g fixes F' and $F \subseteq F'$, then g fixes F.

What's L? It maps subgroups of $G(K|k)$ to gadgets $k \subseteq F \subseteq K$.
It works as follows:

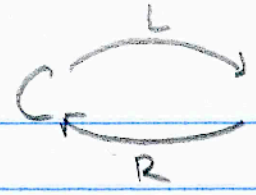
$$LG = \{x \in K : G \text{ fixes } x\} := \{x \in K : \forall g \in G,\ g \text{ fixes } x\}.$$

(Note: This is a subgadget of K!)

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

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

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

Next: Why is  a Galois correspondence?

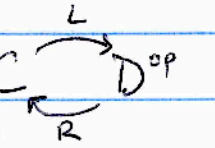
I.e., why is $LG \subseteq F \iff G \supseteq RF$

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

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

These are 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 from last time... but let's throw in an "op" this time:

Thm: Suppose  is a Galois connection.

Define $\bar{c} = RLc \quad c \in C$

$\bar{d} = LRd \quad d \in D^{(op)}$.

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

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

We say $c \in C$ is <u>closed</u> if $\bar{c} = c$, and similarly for $d \in D^{(op)}$.

L & R give a 1-1 correspondence between the closed elements of C and closed elements of D.

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

It's one with $F = LRF = L\{g \in Aut(G) : g \text{ fixes } F\}$

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

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 $G \subseteq G(K|k)$?

$$G = RLG$$
$$= R\{x \in K : x \text{ is fixed by } G\}$$
$$= \{g \in G(K|k) : g \text{ fixes } x \ \forall x \text{ fixed by } G\}$$

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 — poset of subgroups of the Galois groups.

11/2/15

Groupoids

Def: A morphism $f: x \to y$ in a category has an inverse $g: y \to x$ if $fg = 1_y$ & $gf = 1_x$. If f has an inverse, it is unique so we write it as f^{-1}.
A morphism with an inverse is called an isomorphism.
If there is an isomorphism $f: x \to y$ we say x & y are isomorphic. It is more useful to have an isomorphism than merely to know things are isomorphic.

Def: A groupoid is a category where all morphisms are isomorphisms.
E.g. 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 and $x \in C$, (notation abuse: x is an object in C) the isomorphisms $f: x \to x$ form a group under composition, called the automorphism group $\mathrm{Aut}(x)$

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

Example: Given any category C there is a groupoid, the core of C, denoted C_0, whose objects are those of C & whose morphisms are the isomorphisms of C, composed as before. Would need to check composition of isomorphisms still give isomorphisms.

Example: if $\mathrm{FinSet} = [\text{finite sets, functions}]$

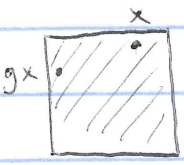
then $\mathrm{FinSet}_0 = [\text{finite sets, bijections}]$,

and if n is your favorite n-element set, $\mathrm{Aut}(n) = S_n$ the symmetric group. If you understand S_n, you understand most of what goes on in FinSet_0.

FinSet_0 "unifies" all the symmetric groups.

Example: Suppose G is a group acting on a set X:

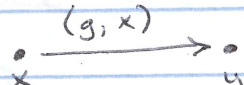
$$\alpha : G \times X \to X$$
$$(g, x) \mapsto gx$$

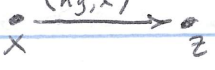


Often people form the set X/G, the quotient set where an element $[x]$ is an equivalence class of elements $x \in X$ where $x \sim y$ iff $y = gx$ $\exists g \in G$. (the orbit).

But a "better" thing to do is 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  and  is 

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

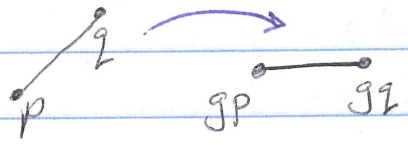
in $X//G$ we say they are isomorphic, or more precisely, we have a chosen isomorphism $(g, x) : x \to y$

To a (pretty good) 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 and morphisms have topologies.

Example: Let X be the set of line segments in the Euclidean plane.

Let G be the ~~group of~~ Euclidean group of the plane: all bijections $g: \mathbb{R}^2 \to \mathbb{R}^2$ such that $|gp - gq| = |p - q|$ (g preserves distances) i.e. g preserves distances. ← This causes angles to be preserved

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 are not counting (p,q) as the same as (q,p). We are allowing $p = q$.

X/G is the "moduli space of line segments".

$X/G \cong [0, \infty)$ length

There is a line segment (p,q) and also (q,p), but $(p,q) \sim (q,p)$ so they have the same equivalence class: they give a single point in X/G. (no negative lengths)

~~What is the automorphism~~ Consider $X//G$. Objects are line segments & morphisms are like

$$(p,q) \xrightarrow{(g;p,q)} (p',q') \quad \text{where } gp = p',\ gq = q',$$

as in the picture.

Given a groupoid $\mathcal{C}$, we can form:

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

2) for any $[x] \in \underline{\mathcal{C}}$, 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.)

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

Example: $\mathcal{C} = \mathrm{FinSet}_0$

$\underline{\mathcal{C}} \cong \mathbb{N}$ and for each $n \in \mathbb{N}$ we get a group S_n which we've seen is (isomorphic to) $\mathrm{Aut}(x)$ for any $x \in \mathrm{FinSet}_0$ with n elements.

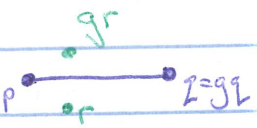
Example: $\mathcal{C} = X/\!/G$ where X is the set of line segments and G is the Euclidean group of the plane.

$\underline{\mathcal{C}} \cong [0, \infty)$

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: what's $\mathrm{Aut}((p,q))$?



$\mathrm{Aut}((p,q))$ ~~is the trivial group~~ if $p \neq q$: $\mathbb{Z}_2$.

If $p = q$: O_2 the group of all orthogonal 2×2 matrices, i.e. all rotations and reflections fixing $p \in \mathbb{R}^2$.

11/9/15

Moduli Spaces & Moduli Stacks

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

Example: 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 are pairs $x \in X$, $g \in G$, where $y = gx$.

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

Then $\underline{X/\!/G} \cong X/G$ where X/G has elements which are equivalence classes $[x]$ with $x \sim y$ when $y = gx$ for some $g \in G$.

↖ X weakly mod 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 $f: x \to x$, 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:

"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

We think of (p,q) as a line segment with a chosen first and second endpoint, which can be equal.

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

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

the space of lengths.

The moduli stack $X/\!/G$ keeps track of symmetries:

$\mathrm{Aut}[(p,q)] \cong \mathrm{Aut}((p,q))$

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

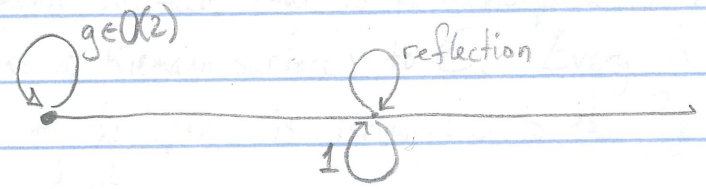
$\mathrm{Aut}((p,q)) \cong \mathbb{Z}/2$ if $p \neq q$ 

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

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

$\mathbb{Z}_2$ = $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$

So the moduli stack looks like:



Example: "The moduli stack of triangles"

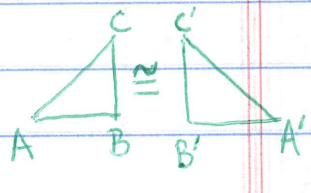
Let G be the Euclidean group as before, but now let X be the set of triangles: $X = \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2$.

These are triangles with named vertices that can be equal.

The moduli space X/G is the set of isomorphism classes of triangles. Now

$$X/G \cong [0,\infty)^3$$
$$[(p,q,r)] \longmapsto (|p-q|, |q-r|, |r-p|)$$

But does orientation matter?



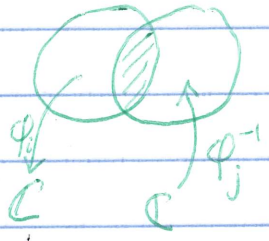
Here it seems if $p \neq q \neq r \neq p$, then (p,q,r) has as automorphisms only the identity.

If we define the triangles to be unordered triples 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.

Example: A Riemann surface is a 2-dimensional smooth manifold with charts

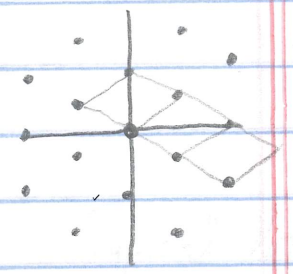
$$\varphi_i : U_i \longrightarrow \mathbb{C}$$

such that $\varphi_i \varphi_j^{-1}$ is analytic (=holomorphic)



Every Riemann surface that is 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 $\mathbb{CP}^1 \cong \mathbb{C} \cup \{\infty\}$.

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

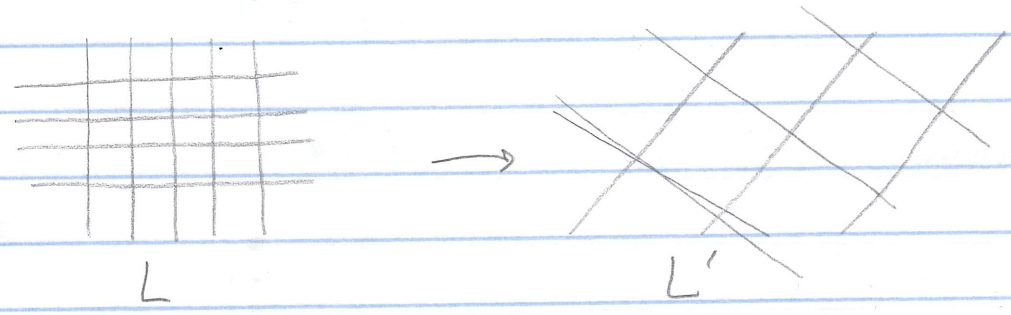


Every elliptic curve is isomorphic to one of this form: take a lattice $L \subseteq \mathbb{C}$, i.e. a subgroup of $(\mathbb{C}, +, 0)$ that's isomorphic to $\mathbb{Z}^2$, and form $\mathbb{C}/L$, getting a torus with obvious charts $\varphi_i : U_i \to \mathbb{C}$, and thus an elliptic curve.

When do two lattices L & L' give isomorphic elliptic curves: $\mathbb{C}/L \cong \mathbb{C}/L'$?

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

(the shape of the parallelograms are the same, but the size and rotation may be different.)



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

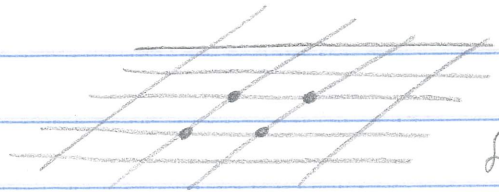
- elliptic curves as objects
- isomorphisms of Riemann surfaces as morphisms

and we're seeing $\underline{\mathcal{C}} \cong X/G$ where X is the set of lattices and $G = \mathbb{C}^*$ (nonzero complex numbers with multiplication).

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

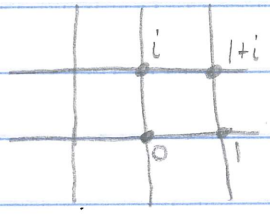
There are two elliptic curves with a bigger automorphism group:

Typical lattice/ elliptic curve



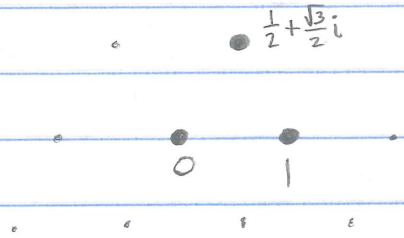
has $\mathbb{Z}/2$ as symmetries from 180° rotation $(-1)^2=1$

Gaussian elliptic curve



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

Eisenstein elliptic curve



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

11/16/15

Klein Geometry

Def: A homogeneous G-space for some group G is a G-set X, i.e. a set X with a map

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

such that $g_1(g_2 x) = (g_1 g_2)(x)$, $1x = x$

which is transitive, i.e.

$$\forall x, y \in X \quad \exists\, g \in G, \quad gx = y$$

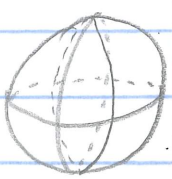
Example: In Euclidean plane geometry, $G = O(2) \ltimes \mathbb{R}^2$ is the Euclidean group and $X = \mathbb{R}^2$ is the Euclidean plane with $g = (r, t) \in O(2) \ltimes \mathbb{R}^2$ acting on $x \in \mathbb{R}^2$ by: $gx = rx + t$.

In non-Euclidean geometry, the parallel postulate fails. Here, the Euclidean group is replaced by some other 3-dimensional Lie group

Example: In spherical geometry, $G = O(3)$, i.e.

$$G = \{ g : \mathbb{R}^3 \to \mathbb{R}^3 : g \text{ is linear } \& \ gx \cdot gy = x \cdot y \text{ for all } x, y \in \mathbb{R}^3 \}$$

$$X = S^2 = \{ x \in \mathbb{R}^3 : x \cdot x = 1 \}$$



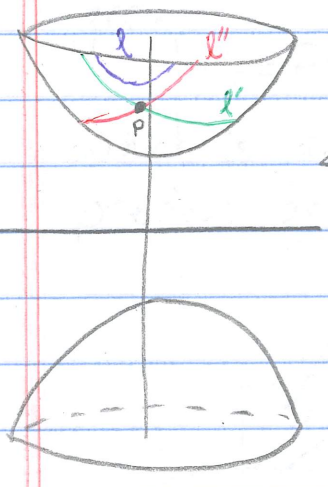
Here we can define a set of lines, namely great circles, but any two distinct lines intersect in two points, so parallel postulate fails, though other axioms of Euclid hold.

Example: In hyperbolic geometry we let $\mathbb{R}^{2,1}$ be $\mathbb{R}^3$ with the dot product $(x,y,z)\cdot(x',y',z') = xx'+yy'-zz'$ and let $G = O(2,1) = \{g: \mathbb{R}^{2,1} \to \mathbb{R}^{2,1} : g \text{ is linear } \& \; gx\cdot gy = x\cdot y \;\; \forall x,y \in \mathbb{R}^{2,1}\}$

and $X = H^2 = \{x \in \mathbb{R}^{2,1} : x\cdot x = -1\}$

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

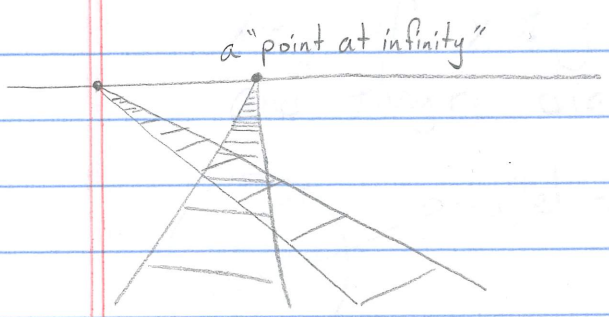
the hyperboloid.

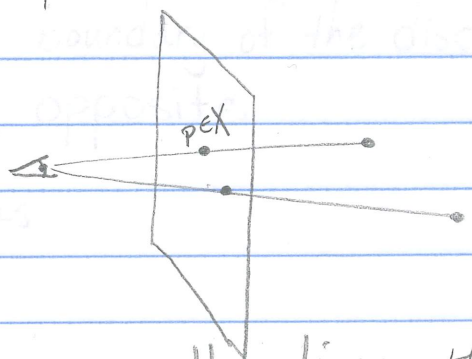


As in spherical geometry, we can define a line to be an intersection of X with some plane through the origin.

The parallel postulate fails because for any line ℓ & any point p not on that line, there are infinitely many lines (e.g. ℓ' and ℓ'') containing p but parallel to ℓ (i.e. not intersecting ℓ).

In projective (plane) geometry every pair of distinct lines intersects in exactly one point!





Points in projective geometry are really lines through the origin (your eye)

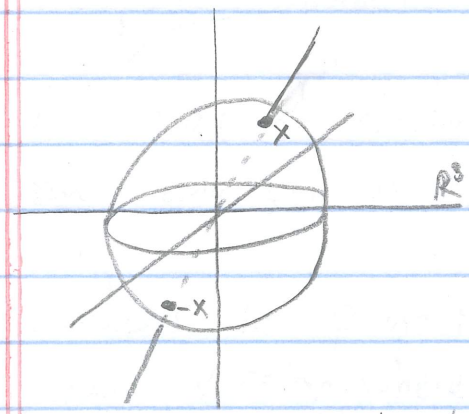
In projective geometry $X = \mathbb{R}P^2 = \{$lines through the origin in $\mathbb{R}^3\}$

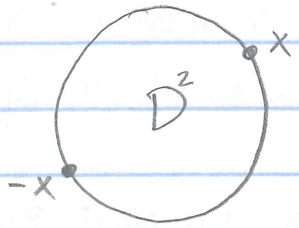
and $G = GL(3,\mathbb{R}) = \{g : \mathbb{R}^3 \to \mathbb{R}^3 : g$ linear, invertible$\}$

... or, since transformations $x \mapsto \alpha x$ $(0 \neq \alpha \in \mathbb{R})$ act trivially on X, we can use the <u>projective general linear group</u>

$$G = PGL(3,\mathbb{R}) = GL(3,\mathbb{R}) / \{\alpha I : \alpha \in \mathbb{R}\}$$

which is an 8-dimensional group, as opposed to the previous groups, which were 3-dimensional.



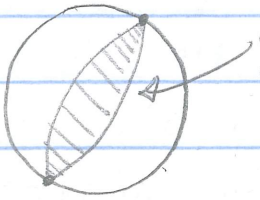


$\mathbb{R}P^2$ can be identified with $S^2/\sim$ where

$x \sim y$ iff $y = \pm x$,

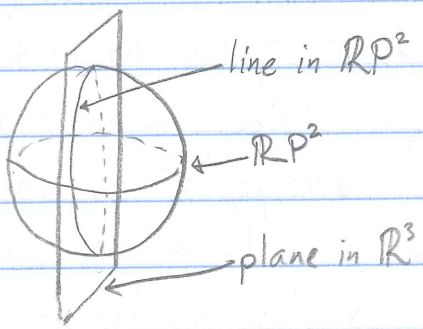
or therefore with $D^2/\sim$ where

$x \sim y$ if x & y are the boundary of the disc D^2 and they're diametrically opposite



parallel train tracks

So $\mathbb{RP}^2$ can be seen as $\mathbb{R}^2$ (homeomorphic to the interior of D^2) together with "points at infinity" coming from the boundary of the disc.
We can define a line in $\mathbb{RP}^2$ to be a plane through the origin in $\mathbb{R}^3$, which contains lots of points in $\mathbb{RP}^2$ (which were lines through the origin).



Any pair of distinct lines intersect in a unique point, and any pair of distinct points lie on a unique line.

Indeed, in projective plane geometry, any theorem has a "dual" version where the role of points and lines are switched. This is a special case of duality for posets, with $p < l$ meaning p lies on l.

Klein noticed that in all the kinds of geometry mentioned so far, we actually have two homogeneous G-space: the set of points X, but also the set of lines Y.
We also are interested in other homogeneous G-spaces, e.g. in 3d geometry we'd have a set of planes, or in 2d projective geometry we have the set of flags:

---

i.e. point-line pairs, where the point lies on the line, etc.

11/23/15

So Klein's idea was:
a <u>geometry</u> is simply a group, and a <u>type of figure</u> (point, line, flag, triangle, etc.) is a homogeneous G-space X, with an element $x \in X$ being a figure of that type.

We can keep track of (classify) all these homogeneous G-spaces by:
Thm: Suppose X is a homogeneous G-space. Pick an element $x \in X$ and let $H \subseteq G$ be the <u>stabilizer</u> of x, i.e. the subgroup
$$H = \{g \in G : gx = x\},$$
Then let G/H be the set of equivalence classes $[g]$ where $g \sim g' \iff g' = gh$. Then G/H is a homogeneous G-space with: $g[g'] = [gg']$
and as G-spaces we have
$$X \cong G/H \quad \text{via} \quad \alpha : gx \mapsto [g] \quad \forall g \in G$$
with the obvious inverse.
Here α is a <u>map of G-spaces</u>: $\alpha(gx) = g\alpha(x)$.

This allowed Klein to redefine a <u>type of figure</u> to be simply a subgroup of G, since a subgroup $H \subseteq G$ gives a transitive G-space G/H, and every transitive G-space is isomorphic to one of those.

11/23/15

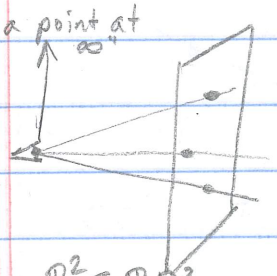
Klein Geometry

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.

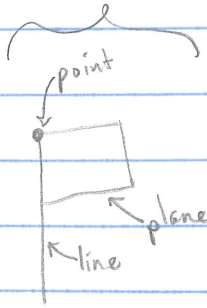
How can we do geometry this way?
We need G-invariant relations between figures.

Example: projective plane geometry: $G = PGL(3, \mathbb{R})$



$X = \{\text{lines through the origin}\}$
X is a homogeneous G-space, so
$X \cong G/H$ where $H \subseteq G$ is the stabilizer of your favorite point $p \in X$:
$H = \{h \in G : hp = p\}$

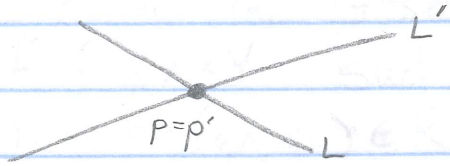
An invariant relation between points is a relation, i.e. a subset $R \subseteq X \times X$ such that
$(p,q) \in R \Rightarrow (gp, gq) \in R$ for all $p, q \in X$, $g \in G$.
But the only invariant relations in this example are $p = q$ and $p \neq q$ (because distance is not preserved by G).



More interestingly, let $Y = \{A \subseteq B : A \text{ is a 1d subspace of } \mathbb{R}^3 \text{ and } B \text{ is a 2d subspace of } \mathbb{R}^3\}$
or $Y = \{\text{flags}\}$, 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.

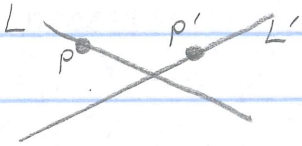
For example: (p, L) and (p', L'), where $p = p'$, $L \neq L'$



Dually, $p \neq p'$, $L = L'$:



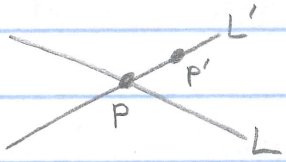
Also, $p \neq p'$, $L \neq L'$, $p \notin L'$, $p' \notin L$

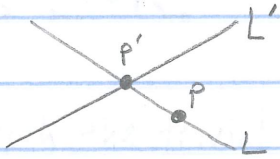


$p = p'$, $L = L'$

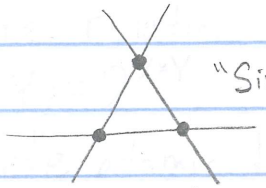


$p \neq p'$, $L \neq L'$, $p \in L'$ — dually $p \neq p'$, $L \neq L'$, $p' \in L$





All six of these relations are visible here:



Pick one flag, then pick the second flag from the six. Each choice of second flag has one of these six relations with the first flag.

For any group G, we can make up a category $GRel$ where:

- objects are G-sets
- morphisms are invariant relations,

where an <u>invariant relation</u> $R: X \nrightarrow Y$ from the G-set X 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 necessarily invariant) we can compose them to get $S \circ R: X \nrightarrow Z$:

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

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

There is a category Rel ($GRel$ with the trivial group G) where:

- objects are sets
- morphisms are relation

Here $\hom(X,Y) = 2^{X \times Y}$. Recall, for any set S, 2^S is a complete atomic boolean algebra (CABA), 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 are $R \cap S$, $R \cup S$, R^c. (Need to check more stuff...)

In fact, Rel and 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 uses sets:

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

The idea in enriched category theory is to generalize, replacing Set by some other category $\mathcal{V}$ and say
A $\mathcal{V}$-enriched category is a class of objects, and for each pair of objects x,y an object $\hom(x,y) \in \mathcal{V}$, and a composition morphism in $\mathcal{V}$:
$\circ : \hom(x,y) \otimes \hom(y,z) \to \hom(x,z)$ etc...

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

It turns out that CABAs form a monoidal category, so it makes sense to talk about a CABA-enriched category, and Rel & GRel are such.

11/30/15

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

$$\circ : \hom(x,x) \times \hom(x,x) \to \hom(x,x).$$

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 tensor product $\otimes : V \times V \to V$ obeying some rules.
Then recall a V-enriched category C has a class of objects, and for any objects $x, y \in C$, a "hom-object" $\hom(x,y) \in V$, and composition morphisms:

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

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 $m : M \otimes M \to M$ that is associative and unital.

Example: Suppose $V = \mathrm{AbGp}$ with the usual tensor product of abelian groups. Then a monoid in V is called a <u>ring</u>.
It's an abelian group M, with a multiplication:

$$m : M \otimes M \to M$$

an abelian group homomorphism, i.e. a function $m : M \times M \to M$ that's linear in each argument.

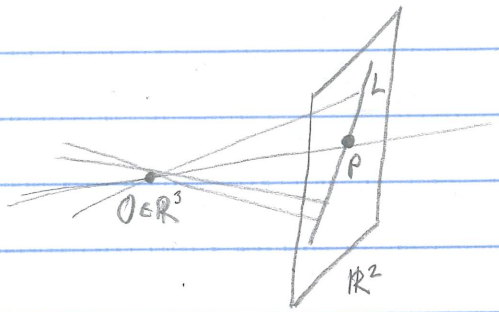
That is, $(a+b)\cdot c = a\cdot c + b\cdot c$
$a\cdot(b+c) = a\cdot b + a\cdot c$.

Example: if $V = R\text{Mod}$ for some commutative ring R, a monoid in V is called an <u>R-algebra</u>.
Example: if $V = \text{Top}$ with usual product $\times$ of topological spaces as $\otimes$, a monoid in V is called a topological monoid. (Lie groups are especially nice versions of these)

Back to our favorite example: Klein geometry.
Let G be a group, and let $GRel$ be the category with
- G-sets as objects
- G-invariant relations as morphisms.

This is 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".

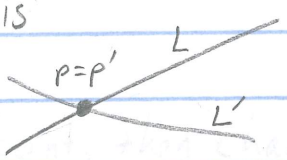
Example: Projective plane geometry.
Take $G = PGL(3,\mathbb{R})$. $Y = \{\text{flags}\} = \{(p,L) : p \subseteq \mathbb{R}^3$ is a 1d subspace, $L \subseteq \mathbb{R}^3$ is a 2d subspace, $p \subseteq L\}$



$\hom(Y,Y)$ is a monoid in CABA. What is it like? Instead of describing all the elements, let's just describe the atoms.

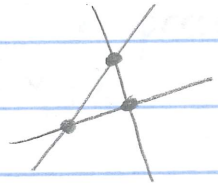
In general, given any group G and any G-sets X, Y, what are the atoms in $\hom(X,Y)$ like?
They're invariant relations $R: X \nrightarrow Y$, i.e. $R \subseteq X \times Y$ such that $(x,y) \in R \Rightarrow (gx, gy) \in R$.
But they're the smallest nonempty subsets of this form. So, any atom R must contain 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 $\hom(X,Y)$.

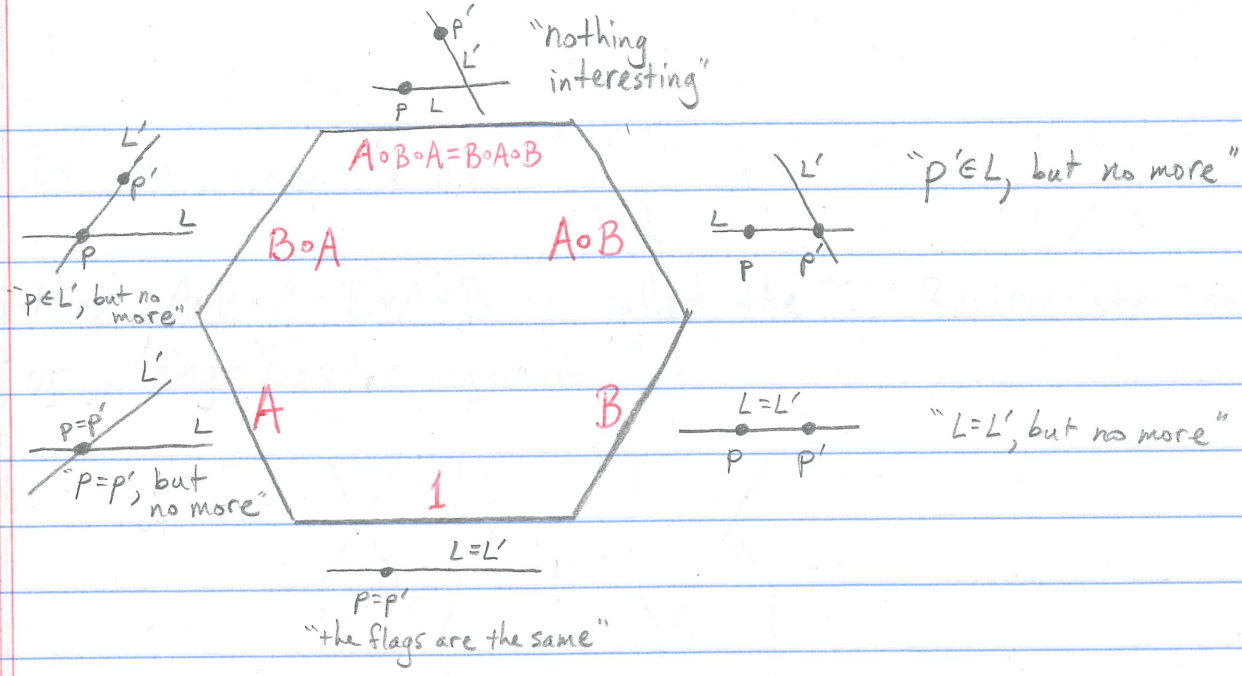
So if $G = PGL(3,\mathbb{R})$ and $Y = \{\text{flags}\}$, the atoms in $\hom(Y,Y)$ are the orbits of G acting on $Y \times Y$.
E.g. the orbit of this



$x = (p, L)$
$y = (p', L')$

is the set of all pairs of flags sharing the same point (and nothing more!)
Last time we saw all six atoms in $\hom(Y,Y)$:





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

Note: we can compose invariant relations & $1 \circ 1 = 1$

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

$$A \circ A = A \cup 1$$

If we change the line on a flag twice, the result is either changing the line or getting back to the original flag

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

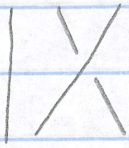
$$B \circ B = B \cup 1$$

$A \circ B$ (change the point, then change the line) is the atom, "$p' \in L$ but no more".

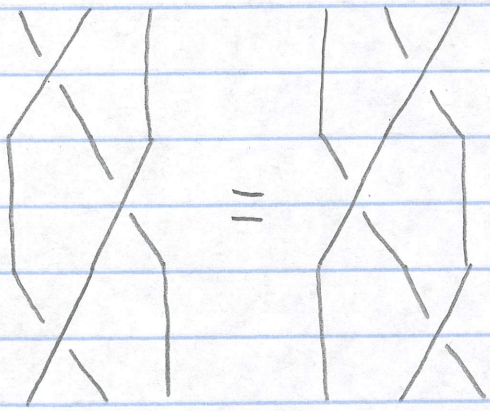
$B \circ A$ is the atom, "$p \in L'$ but no more".

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

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

If we draw A as  and B as 

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