Duality

Every category C has an opposite C^{op}. C^{op} has the same objects as C, but the morphisms are "turned around". So there's a 1-1 correspondence between morphisms in C & morphisms in C^{op}, with $f: x \to y$ in C corresponding to a morphism $f^{op}: y \to x$ in C^{op}. We compose morphisms in C^{op} by: $f^{op} \circ g^{op} = (g \circ f)^{op}$.

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

Note: $(C^{op})^{op} = C$. Just like for finite-dimensional vector spaces, $(V^*)^* \cong V$ via a 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 through "analytic geometry".

We can associate to any finite dimensional vector space over $\mathbb{R}$ a commutative ring $\mathcal{O}(V)$ consisting of all polynomial functions on V. If $V = \mathbb{R}^n$, the algebra $\mathcal{O}(V)$ consists of polynomials in the coordinate functions $x_1, \dots, x_n$: $\mathcal{O}(V) = \mathbb{R}[x_1, \dots, x_n]$.

So we go from a "space" V (a bunch of points) to an algebra $\mathcal{O}(V)$.

Then we can describe certain subspaces X of V: $X \xrightarrow{1\text{-}1} V$ as quotient algebras $\mathcal{O}(V)$: $\mathcal{O}(V) \xrightarrow{\text{onto}} \mathcal{O}(X) = \mathcal{O}(V)/I$ for an ideal I.

Example: the unit circle is a subspace of the plane: $S^1 \hookrightarrow \mathbb{R}^2$, where $S^1 = \{(x,y) : x^2 + y^2 - 1 = 0\}$. Then there's an algebra $\mathcal{O}(S^1)$ of polynomials on S^1 with $\mathcal{O}(S^1) = \mathbb{R}[x,y]/\langle x^2+y^2-1 \rangle$. So the 1-1 map $S^1 \to \mathbb{R}^2$ gets turned around, giving $\mathcal{O}(\mathbb{R}^2) \to \mathcal{O}(S^1)$ which is just restriction $f \mapsto f|_{S^1}$. Moreover $f, g \in \mathcal{O}(\mathbb{R}^2)$ restrict to the same function on S^1 iff $f - g \in \langle x^2+y^2-1 \rangle$.

Algebraic geometry is the study of geometry using commutative rings.

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

Problems:

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

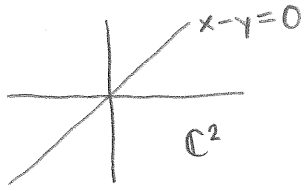
The function x^2+y^2+1 doesn't vanish on $\mathbb{R}^2$, so it seems the corresponding subspace of $\mathbb{R}^2$ is $\emptyset$.

But there's another, simpler ideal corresponding to $\emptyset \subset \mathbb{R}^2$, namely $\langle 1\rangle$.

So $\emptyset = \{(x,y) : 1 = 0\}$, but we're getting 2 ideals corresponding to the same subspace. One way out is to use $\mathbb{C}$ instead of $\mathbb{R}$.

2) Alas, using $\mathbb{C}$ doesn't completely fix the problem of 2 different ideals corresponding to the same subspace.

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



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 & found a better solution.

He 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 whose objects are "affine schemes" & morphisms are maps between them, in such a way that $\text{AffSch}^{op} = \text{CommRing}$. Just take $\text{AffSch} = \text{CommRing}^{op}$.

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 the affine scheme $\mathbb{Z}[x,y]$.

"The circle is included in the plane" means we have a homomorphism of commutative rings $\mathbb{Z}[x,y] \to \mathbb{Z}[x,y]/\langle x^2+y^2-1\rangle$.

In "noncommutative geometry", we come up with a new kind of space so that $? = \text{Ring}^{op}$.

GEOMETRY	ALGEBRA (COMMUTATIVE)
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, we get a commutative algebra $C(X) = \{f: X \to \mathbb{C} : f \text{ is continuous}\}$. 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 $\|f\| = \sup_{x \in X} |f(x)|$, which makes sense by compactness. This makes $C(X)$ into a C^*-algebra, meaning: $\|fg\| \leq \|f\|\|g\|$, $\|f^*\| = \|f\|$, & $\|f^* f\| = \|f\|^2$. So $C(X)$ is a commutative C^*-algebra.

Next, can we turn a morphism $\phi: X \to Y$ in $CHaus$ into a morphism of comm. C^*-algs? A homomorphism $F: A \to B$ between C^*-algs. is a map s.t. $F(a+b) = F(a) + F(b)$, $F(ab) = F(a)F(b)$, $F(ca) = cF(a)$, $F(a^*) = F(a)^*$, $\|F(a)\| \leq K\|a\|$ for some $K > 0$. All these imply $\|F(a)\| = \|a\|$.

So we get a category $CommC^*Alg = [\text{comm. } C^*\text{-algs., } C^*\text{-alg. homomorphisms}]$.

How does a continuous map $\phi: X \to Y$ b/w compact Hausdorff spaces give a C^*-alg. homomorphism $C(X)$ & $C(Y)$? We'll get one, $\phi^*: C(Y) \to C(X)$ defined by $\phi^*(f) = f \circ \phi$, the "pull back" of f along ϕ. Note $(\phi \circ \psi)^* = \psi^* \circ \phi^*$. So we're getting a functor

$$\begin{aligned} CHaus &\xrightarrow{C} CommC^*Alg^{op} \\ X &\longmapsto C(X) \\ \phi: X \to Y &\longmapsto \phi^*: C(Y) \to C(X) \end{aligned}$$

Gelfand-Naimark Thm: This functor is an equivalence of categories, i.e. there's a functor $\mathrm{Spec}: \mathrm{Comm}C^*\mathrm{Alg}^{op} \to \mathrm{CHaus}$ such that $\mathrm{Spec} \circ C \simeq 1_{\mathrm{CHaus}}$ & $C \circ \mathrm{Spec} \simeq 1_{\mathrm{Comm}C^*\mathrm{Alg}^{op}}$ are natural isomorphisms.

What is Spec? Given a comm. C^*-alg. A, how do we get $\mathrm{Spec}(A)$? Let's do $A = C(X)$. Then $\mathrm{Spec}(C(X))$ should be X. How do we recover the points of X starting from $C(X)$? But what's a point in X in terms of CHaus? It's a map $\phi: \{*\} \to X$ where $\{*\}$ is the one-point space, which is an object in CHaus. So given $x \in X$, $\phi(*) = x$, & conversely any map $\phi: \{*\} \to X$ determines a point in X. Our functor $C: \mathrm{CHaus} \to \mathrm{Comm.}\, C^*\mathrm{Alg}^{op}$ will turn $\phi: \{*\} \to X$ into a homomorphism $\phi^*: C(X) \to C(\{*\})$. In fact, $C(\{*\}) \cong \mathbb{C}$ where $g \in C(\{*\})$ gives $g(*) \in \mathbb{C}$. So $\phi^*: C(X) \to \mathbb{C}$ is $\phi^*(f) = f \circ \phi(*) = f(x)$. Thus a point $x \in X$ gives a homomorphism $C(X) \to \mathbb{C}$, $f \mapsto f(x)$, which is just "evaluation at x".

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).

Lemma: Any C^*-alg. homomorphism $C(X) \xrightarrow{\psi} \mathbb{C}$ comes from some $x \in X$ via $\psi(f) = f(x)$.

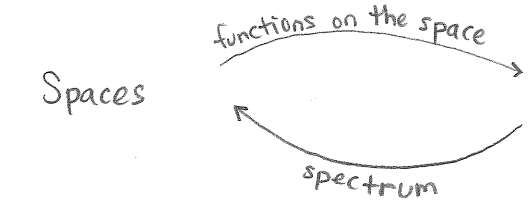
Together these lemmas yield a 1-1 correspondence between points $x \in X$ & homos. $\psi: C(X) \to \mathbb{C}$. So given any comm. C^*-alg. A, define $\mathrm{Spec}(A) = \{\psi: A \to \mathbb{C} \mid \psi \text{ is a } \mathbb{C}^*\text{-alg. hom.}\}$.

There's a topology making $\mathrm{Spec}(A)$ into a compact Hausdorff space. In this topology, ψ_i converges to ψ iff $\psi_i(a)$ converges to $\psi(a)$ for all $a \in A$.

Finally, given a C^*-alg. hom. $F: A \to B$., we define a map of spaces $\mathrm{Spec}(F): \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ by $\mathrm{Spec}(F)(\psi) = \psi \circ F$.

So we get functors $CHaus \underset{Spec}{\overset{C}{\rightleftarrows}} Comm\,C^*Alg^{op}$ which are inverses up to natural isomorphism.

Note:



points in a space $\rightleftarrows$ homomorphisms from a comm. ring to a field

subspace $\rightleftarrows$ quotient ring or ideal

$\chi_S(x) = \begin{cases} 0 & \text{if } x \notin S \\ 1 & \text{if } x \in S \end{cases}$ & 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 $\cup, \cap, ^c$ on subsets of X correspond to operations $\vee, \wedge, \neg$ on functions $f: X \to \{0,1\}$. We have:

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

Also: $S \subseteq T \Leftrightarrow \chi_S \leq \chi_T$ (i.e. $\chi_S(x) = 1 \Rightarrow \chi_T(x) = 1$). Note "$\leq$" is not a separate concept, so actually we can say

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

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

Defn A distributive lattice is one where $\wedge$ & $\vee$ distribute over each other.

Defn A Boolean algebra is a distributive lattice A where every $x \in A$ has a complement $\neg x$ such that $x \wedge \neg x = F$ & $x \vee \neg x = T$. (If a complement exists, it's unique).

Ex For any set S, 2^S is a Boolean algebra with pointwise defined $\leq$, meaning that given $f, g \in 2^S$, we say $f \leq g$ whenever $f(x) \leq g(x)$ $\forall x \in S$. It thus has pointwise defined $\wedge, \vee, 0, 1$, & $\neg$, 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".

Defn A complete Boolean algebra A is one where every subset $S \subseteq A$ has a l.u.b. $\bigvee_{x \in S} x$ & a g.l.b. $\bigwedge_{x \in S} x$ such that they distribute over each other.

Defn An atom in a Boolean algebra A is an element $x \in A$ such that $x \neq 0$ & if $y < x$ then $y = 0$.

Ex In 2^S, the atoms are the elements of S, or singletons $\{s\} \in S$.

Defn A Boolean algebra 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 whose morphisms $\phi: A \to B$ preserve $\vee, \wedge, 0, 1, \neg, \bigvee, \bigwedge$.

There's of course a category Set of sets & functions.

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

$$\begin{array}{ccc} \text{Set} \longrightarrow \text{CABA}^{op} & \& & \text{CABA}^{op} \longrightarrow \text{Set} \\ S \longmapsto 2^S = \text{Hom}_{\text{Set}}(S, 2) & & A \longmapsto \text{Hom}_{\text{CABA}}(A, 2) \end{array}$$

where morphisms are given via pullback in the obvious way.

Ex $\{f \in L^\infty[0,1] : f(x) = 0 \text{ or } 1 \ \forall x \in [0,1]\}$ is a complete but not atomic Boolean algebra under pointwise operations.

The opposite of the category of all Boolean algebras is the category of Stone spaces: compact Hausdorff spaces that are totally disconnected, in which 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 & linear maps. What's FinVect^{op}? A typical morphism in FinVect is $T: \mathbb{R}^n \to \mathbb{R}^m$, so a morphism in FinVect^{op} is $T^{op}: \mathbb{R}^m \to \mathbb{R}^n$. This is suspiciously similar to the transpose $T^t: \mathbb{R}^m \to \mathbb{R}^n$ in FinVect. In fact, $\text{FinVect} \xrightarrow{\sim} \text{FinVect}^{op}$, with:

$$\underset{\text{in FinVect}}{T: \mathbb{R}^n \to \mathbb{R}^m} \quad \mapsto \quad \underset{\text{in FinVect}^{op}}{(T^t)^{op}: \mathbb{R}^n \to \mathbb{R}^m} \quad \text{or} \quad \underset{\text{in FinVect}}{T^t: \mathbb{R}^m \to \mathbb{R}^n}$$

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

$$\begin{aligned} \text{FinVect} &\longrightarrow \text{FinVect}^{op} \\ V &\mapsto \text{Hom}(V, \mathbb{R}) = V^* \\ T: V \to W &\mapsto \underset{\text{in FinVect}}{T^*: W^* \to V^*} \quad \text{or} \quad \underset{\text{in FinVect}^{op}}{(T^*)^{op}: V^* \to W^*} \end{aligned}$$

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

Also, the category of finite abelian groups & group homomorphisms is its own opposite.

Galois Theory

Galois Theory is secretly about dualities between posets (partially ordered sets).

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

The categories that we get in this way are precisely those with:

1) at most one 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 $f: (S, \leq) \to (T, \leq)$.

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 $x \geq y$.

What are adjoint functors between categories of this sort?

Defn: Given categories C, D, we say a functor $L: C \to D$ is <u>left adjoint</u> of a functor $R: D \to C$, or R is <u>right adjoint</u> of L, if there's a natural 1-1 correspondence $\mathrm{Hom}_D(Lx, y) \cong \mathrm{Hom}_C(x, Ry)$ $\forall$ $x \in C, y \in D$.

Example: Let L: Set $\to$ Grp send any set S to the free group on S, & R: Grp $\to$ Set send any group G to its underlying set.
[L = liberty! = freedom]
Here, $\mathrm{Hom}_{Grp}(LS, G) \cong \mathrm{Hom}_{Set}(S, RG)$.

Example: What are adjoint functors between posets $(S, \leq)$ & $(T, \leq)$?
It's a pair of order-preserving functions $(S, \leq) \underset{R}{\overset{L}{\rightleftarrows}} (T, \leq)$ such that $Lx \leq y$ iff $x \leq Ry$, which comes from $\mathrm{Hom}_T(Lx, y) \cong \mathrm{Hom}_S(x, Ry)$.

Defn: A pair of adjoint functors between posets is called a <u>Galois correspondence</u>.

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 $x \leq \bar{x}$ $\forall$ $x \in S$ (because $Lx \leq Lx \Rightarrow x \leq RLx$) & $\bar{\bar{x}} = \bar{x}$ $\forall$ $x \in S$. So we say $\bar{\cdot}$ is a <u>closure operator</u> on the poset $(S, \leq)$. Similarly, write y° for LRy. Then $y^\circ \leq y$ $\forall$ $y \in T$ & $(y^\circ)^\circ = y^\circ$ $\forall$ $y \in T$. 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/ $x = \bar{x}$) & <u>open</u> elements of T (meaning $y \in T$ w/ $y^\circ = y$).

Galois Theory

Suppose you have any kind of algebraic gadget - a set with some operations obeying some axioms. For example: monoids, groups, rings, fields. Then we can define a "subgadget" of a gadget K to be a subset $k \subseteq K$ which is closed under all the operations.

The gadgets F such that $k \subseteq F \subseteq K$ 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 $g: K \to K$ which preserve all the operations. For example, $g(x+y) = g(x) + g(y)$, $g(xy) = g(x)g(y)$, $g(0) = 0$, $g(1) = 1$ when K is a ring. We say an element $x \in K$ is <u>fixed</u> by $g \in \mathrm{Aut}(K)$ if $g(x) = x$. We say a subgadget $F \subseteq K$ is <u>fixed</u> by $g \in \mathrm{Aut}(K)$ if $g(x) = x$ for each $x \in F$. Notice the subset $\{g \in \mathrm{Aut}(K) : g \text{ fixes } F\}$ 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 $G(K|k)$ with the partial order $\subseteq$. 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 $R: D^{op} \to C$ is order-preserving (i.e. a functor), we need: $k \subseteq F \subseteq F' \subseteq K \Rightarrow RF \supseteq RF'$. This is true: it says 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: $LG = \{x \in K : G \text{ fixes } x\} := \{x \in K : \forall\, g \in G,\ g \text{ fixes } x\}$. 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: it says that if $x \in F$ is fixed by all $g \in G'$, then it's fixed by all $g \in G$.

Next, why is $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$ a Galois connection? That is, why is $LG \subseteq F \Leftrightarrow G \supseteq RF$? $LG \subseteq F$ means every element of K fixed by G is in F. $G \supseteq RF$ means every element of $Aut(K)$ 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".

Thm. – Suppose $C \underset{R}{\overset{L}{\rightleftarrows}} D^{op}$ is a Galois connection. Define $\bar{c} = RLc$ $\forall\, c \in C$ & $\bar{d} = LRd$ $\forall\, d \in D$. These are <u>closure operators</u>: $c \leq \bar{c}$ & $\bar{c} = \bar{\bar{c}}$ and $d \leq \bar{d}$ & $\bar{d} = \bar{\bar{d}}$. We say $c \in C$ is <u>closed</u> if $c = \bar{c}$ & similarly for $d \in D$. L & R give a 1-1 correspondence between closed elements of C & closed elements of D.

In our application, what's a "closed" subgadget $k \subseteq F \subseteq K$? It's one with $F = LRF = L\{g \in Aut(G) : g \text{ fixes } F\} = \{x \in K : x \text{ is fixed by all } g \text{ that fix } F\}$. So, a subgadget F is closed if it contains all $x \in K$ that are fixed by all $g \in G(K|k)$ that fix F.

What's a "closed" subgroup $G \subseteq G(K|k)$? It's one with $G = RLG = R\{x \in K : G \text{ fixes } x\} = \{g \in Aut(K) : g \text{ fixes all } x \in K \text{ fixed by } G\}$. So, a subgroup G is closed if it's the group of all $g \in Aut(K)$ that fix all $x \in K$ fixed by G.

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 of subgroups of the Galois group

* Pf of Thm – We know: $c \leq c' \Rightarrow Lc \geq Lc'$; $d \geq d' \Rightarrow Rd \leq Rd'$; & $Lc \geq d \Leftrightarrow c \leq Rd$.
(1) $Lc \geq Lc \Rightarrow c \leq RLc = \bar{c}$; (2) $Rd \leq Rd \Rightarrow \bar{d} = LRd \geq d$; (3) $\bar{c} \leq \bar{\bar{c}}$ by (1) & $RLc \geq RLc \Rightarrow LRLc \geq Lc \Rightarrow RLRLc \leq RLc \Rightarrow \bar{\bar{c}} \geq \bar{c} \Rightarrow \bar{c} = \bar{\bar{c}}$; (4) note $L\bar{c} = \overline{Lc}$ & so $c = \bar{c} \Rightarrow Lc = L\bar{c} = \overline{Lc}$. (Apply similar arguments to d.)
(5) $RL\bar{c} = \bar{c}$ & $LR\bar{d} = \bar{d}$ because $\bar{\bar{c}} = \bar{c}$ & $\bar{\bar{d}} = \bar{d}$, so L & R are inverses on closed elements.

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's unique, so we write it as f^{-1}. A morphism with an inverse is called an isomorphism. If there's an isomorphism $f: x \to y$, we say x & y are isomorphic.

Def. – A groupoid is a category where all morphisms are isomorphisms.

Example – Any group G gives a groupoid with one object, $*$, & 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 automorphism group $\mathrm{Aut}(X)$.

Example – Given any category C, there's a groupoid, the core C_0 of C, whose objects are those of C & whose morphisms are the isomorphisms of C, composed as before.

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, then $\mathrm{Aut}(n) = S_n$, the symmetric group. So 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 elt. $[x]$ is an equivalence class of elts $x \in X$ 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 $g \in G$ & $gx = y$; $x \xrightarrow{(g,x)} y$. The composite of $x \xrightarrow{(g,x)} y$ & $y \xrightarrow{(h,z)} z$ 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 $(g,x): x \to y$.

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

Example - Let X be the set of line segments in the Euclidean plane. Let G be the Euclidean group of the plane: all bijections $g: \mathbb{R}^2 \to \mathbb{R}^2$ that preserve 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) the same as (q,p). We're allowing $p = q$.

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

Given a line segment (p,q), there's a line segment (q,p), but $(p,q) \sim (q,p)$, so they have the same equivalence class & hence give the same element of 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.

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

Example - $C = \mathrm{FinSet}_0$. $\underline{C} \cong \mathbb{N}$. & 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 - $C = X//G$ 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 $y = gx$ for some $g \in G$.

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

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

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. topological space, manifold, algebraic variety, scheme, etc.) Then $\underline{C}$ 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

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

are pairs (g,x) with $g \in G$, $x \in X$, & $y = gx$.

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

Recall:

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

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

Note: if $[x] \neq [y]$, there are no morphisms between them.

We often call X/G a moduli space, & $X/\!/G$ the moduli stack.

Last time we looked at an example:

Example: "The moduli stack of line segments" in Euclidean geometry. Here,

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

$G = O(2) \ltimes \mathbb{R}^2$ is the Euclidean group of the plane

Here 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:

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

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 $p \neq q$ 

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

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

So the moduli stack looks like: 

Example: "The moduli space 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 $X/G \cong [0,\infty)^3$

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

Here it seems that if p,q,r are all distinct, then (p,q,r) has as automorphisms only the identity. If we define a triangle to be an unordered triple of points in $\mathbb{R}^2$, then an equilateral triangle would have S_3 as automorphisms, & isosceles would have $S_2 \cong \mathbb{Z}/2$. This gives a more interesting moduli stack.

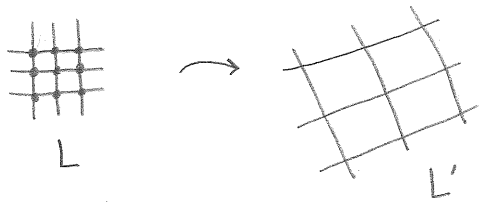
Example: A Riemann surface is a 2-dim. smooth manifold with charts $\phi_i : U_i \to \mathbb{C}$ such that $\phi_i \circ \phi_j^{-1}$ is analytic (=holomorphic). Every Riemann surface that's homeomorphic to the plane is isomorphic (as a Riemann surface) to $\mathbb{C}$. Every Riemann surface homeomorphic to the sphere is isomorphic to the Riemann sphere $\mathbb{CP}^1 \cong \mathbb{C} \cup \{\infty\}$.

There are lots of nonisomorphic ways to make a torus into a Riemann surface – these are elliptic curves. Every elliptic curve is isomorphic to one of this form:

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

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

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



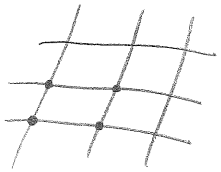
There's a groupoid $\mathcal{C}$ with:

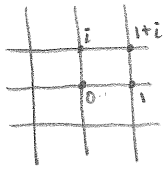
- elliptic curves as objects
- isomorphisms of Riemann surfaces as morphisms

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

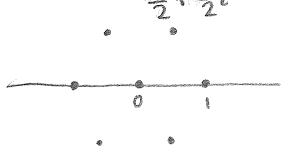
So X/G is called the moduli space of elliptic curves, & $X/\!/G$ is the moduli stack of elliptic curves.

There are two elliptic curves with a bigger automorphism group:

typical elliptic curve  has $\mathbb{Z}/2$ as automorphisms ($180°$ 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

Klein Geometry

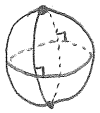
Def. - A homogeneous G-space for some group G is a set X on which G acts transitively, i.e. there's a map $G \times X \to X$ such that $(g, x) \mapsto gx$

$g_1(g_2x) = (g_1g_2)x$, $1x = x$, & $\forall\, x, y \in X \;\exists\; g \in G$ w/ $gx = y$.

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

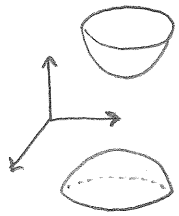
In non-Euclidean geometry, the parallel postulate fails. Here the Euclidean group is replaced by some other 3-dimensional Lie group.

Ex. - In spherical geometry, $G = O(3) = \{g : \mathbb{R}^3 \to \mathbb{R}^3 \mid g \text{ is linear \& } gx \cdot gy = x \cdot y \;\forall\, x, y \in \mathbb{R}^3\}$, & $X = S^2 = \{x \in \mathbb{R}^3 \mid x \cdot x = 1\}$. Here we can define a set of lines, namely great circles:



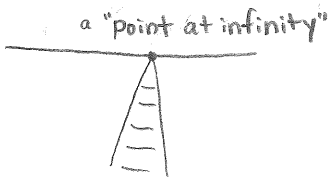
But any 2 distinct lines intersect at 2 points, so the parallel postulate fails, yet other axioms of Euclidean geometry hold.

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

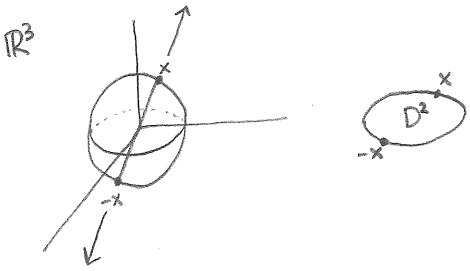


As in spherical geometry, we can define a line to be an intersection of X with some plane through the origin. The parallel postulate fails because for any line ℓ & any point P not on ℓ, there are infinitely many lines ℓ' containing P yet not intersecting ℓ.

In projective (plane) geometry, every pair of distinct lines intersect in exactly 1 point!

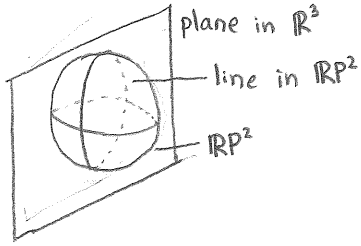


In projective geometry, $X = \mathbb{R}P^2 = \{\text{lines through the origin in } \mathbb{R}^3\}$, & $G = GL(3,\mathbb{R}) = \{g : \mathbb{R}^3 \to \mathbb{R}^3 \mid g \text{ linear \& invertible}\}$ or, since transformations $x \mapsto \lambda x$ for some $0 \neq \lambda \in \mathbb{R}$ act trivially on X, we can use the projective general linear group $G = PGL(3,\mathbb{R}) = GL(3,\mathbb{R})/\{\lambda I : \lambda \in \mathbb{R}\}$, 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 $x \sim y$ iff x & y are on the boundary of the disc D^2 & diametrically opposite. So $\mathbb{R}P^2$ 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 $\mathbb{R}P^2$ to be a plane through the origin in $\mathbb{R}^3$, which contains lots of points in $\mathbb{R}P^2$ (which were lines through the origin).



Any pair of distinct lines intersect in a unique point, & 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 & lines are switched.

This is a special case of duality for posets, with $p < \ell$ meaning p lies on ℓ.

Klein noticed that in all the kinds of geometry mentioned so far, we have two homogeneous G-spaces: the set X of points but also the set Y of lines. We also are interested in other homogeneous G-spaces, e.g. in 3d geometry we'd have a set of planes, or in 2d Euclidean geometry we have the set of flags, i.e. point-line pairs where the point lies on the line, etc.

So Klein's idea was: a <u>geometry</u> is simply a group, & a <u>type of figure</u> (point, line, flag, triangle, etc.) is a homogeneous G-space X, whose elements $x \in X$ are figures of that type.

We can classify all these homogeneous G-spaces by:

Thm.- Suppose X is a homogeneous G-space. Pick an element $x \in X$. Let $H \subseteq G$ be the stabilizer 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 $g[g'] = [gg']$ & $X \cong G/H$ as G-spaces via $gx \overset{\alpha}{\mapsto} [g]$ $\forall$ $g \in G$. (Here α is a map of G-spaces, meaning $\alpha(gx) = g\alpha(x)$ $\forall$ $g \in G$.

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, & every transitive G-space is isomorphic to one of those.

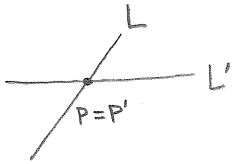
Klein Geometry

We've seen that:

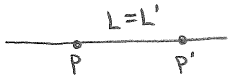
- a geometry is a group G
- a type of figure in this geometry is a subgroup $H \subseteq G$
- the set of figures of that type is G/H : a homogeneous G-space

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

Example: projective plane geometry
$G = PGL(3,\mathbb{R})$, $X = \{\text{lines through the origin in } \mathbb{R}^3\} = \{\text{points in } \mathbb{RP}^2\}$
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 $R \subseteq X \times X$ such that $(p,q) \in R \Rightarrow (gp, gq) \in R \quad \forall\ p,q \in X$ & $g \in G$.
But the only invariant relations in this example are $p = q$ & $p \neq q$ because distance is not preserved by G.
More interestingly, let $Y = \{A \subseteq B : A \text{ is 1-dim. subspace of } B \text{ is 2-dim. subspace of } \mathbb{R}^3\} = \{\text{flags}\}$, 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), & there are various invariant relations between flags, i.e. subsets $R \subseteq Y \times Y$ invariant under G.
For example:

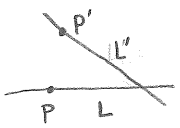


One invariant relation between (p,L) & (p',L') says "$p = p'$ & $L \neq L'$".
Or:



"$L = L'$ & $p \neq p'$"

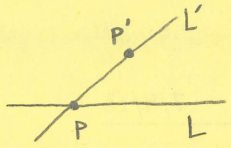
Or:



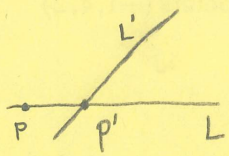
"$p \neq p'$ & $L = L'$ & $p \notin L'$ & $p' \notin L$"

Or:

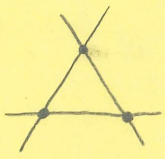
"$p = p'$ & $L = L'$"

Or: 

"$p \in L'$ but $L \neq L'$ & $p \neq p'$"

Finally: 

"$p' \in L$ but $L \neq L'$ & $p \neq p'$"

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 X to the G-set Y is a relation, i.e. a subset $R \subseteq X \times Y$ such that $(x,y) \in R \Rightarrow (gx, gy) \in R$ $\forall\ x \in X,\ y \in Y,\ g \in G$.

How do we compose morphisms?

Given any relations $R: X \nrightarrow Y$ & $S: Y \nrightarrow Z$ (not necessarily invariant), we can compose them to get $S \circ R: X \nrightarrow Z$:

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

If R & S are invariant then 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 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 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 uses sets. The idea in enriched category theory is to generalize, replacing Set by some other category V & say:

A V-enriched category is a class of objects, & for each pair of objects x, y an object $\hom(x,y) \in V$, & a composition morphism $\circ : \hom(x,y) \otimes \hom(y,z) \longrightarrow \hom(x,z)$ in V, 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 $\circ : \hom(x,x) \times \hom(x,x) \to \hom(x,x)$. Conversely, given a monoid M you can build a category with one object x & $\hom(x,x) = M$, with composition being multiplication in M.

More generally suppose V is a monoidal category with tensor product $\otimes$. Then recall a V-enriched category C has a class of objects & for any objects $x, y \in C$, a "hom-object" $\hom(x,y) \in V$ & composition of morphisms $\circ : \hom(x,y) \otimes \hom(y,z) \to \hom(x,z)$.

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

Examples:

1. Suppose $V = \mathrm{AbGp}$ with $\otimes = \otimes_{\mathbb{Z}}$. Then a monoid in V is called a ring.
2. If $V = R\mathrm{Mod}$ with $\otimes = \otimes_R$, then a monoid in V is called an R-algebra.
3. If $V = \mathrm{Top}$ with $\otimes = \times$, then a monoid in V is a topological monoid.

Back to our favorite example: Klein geometry. Let G be a group, & let $G\mathrm{Rel}$ be the category with:

- G-sets as objects
- G-invariant relations as morphisms

This is a CABA-enriched category. So, if we take 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 "hom-CABA"

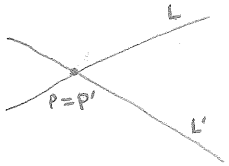
Example: Projective plane geometry.

Take $G = PGL(3,\mathbb{R})$ & $Y = \{(p, L) : p \subseteq \mathbb{R}^3$ is a 1-dim. subspace, $L \subseteq \mathbb{R}^3$ is a 2-dim. subspace, $p \subseteq L\}$, the set of flags.

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

In general, given any group G & 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) & thus all points of the form (gx,gy) for $g \in G$. Indeed, any orbit $\{(gx,gy) : g \in G\} \subseteq X \times Y$ is an atom in $\hom(X,Y)$.

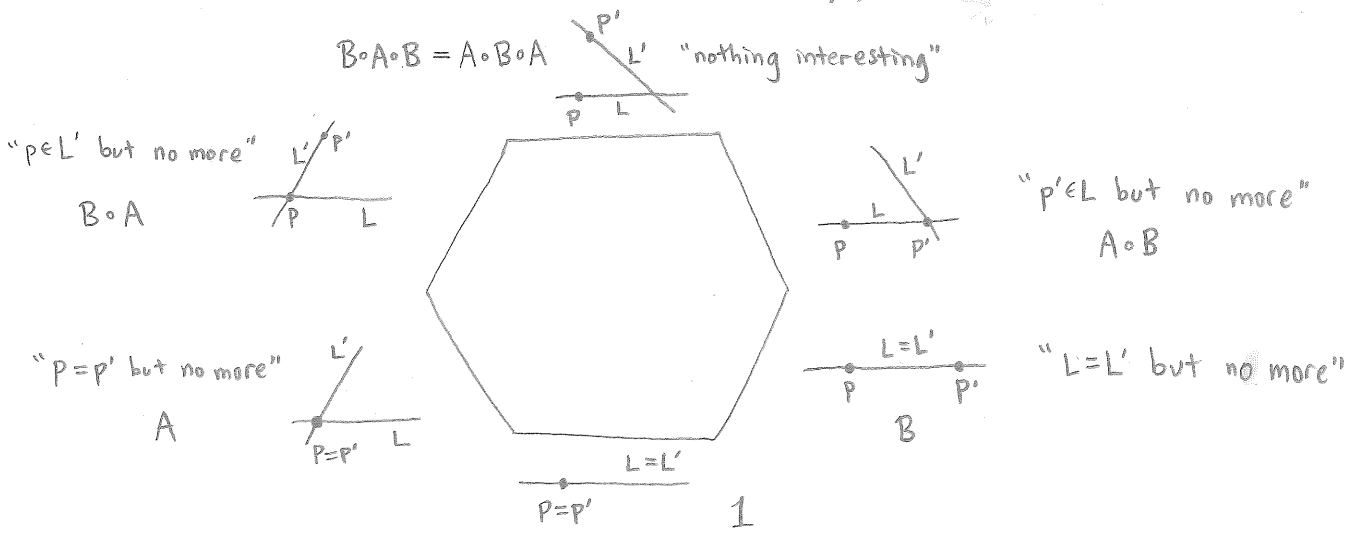
So, if $G = PGL(3,\mathbb{R})$ & $Y = \{\text{flags}\}$, then the atoms in $\hom(X,Y)$ are the orbits of G acting on $Y \times Y$. E.g. the orbit of this pair of flags



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

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

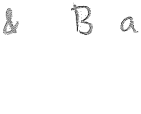
Last time we saw all 6 atoms in $\hom(Y,Y)$:

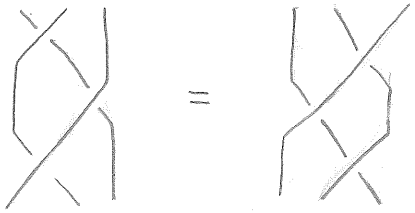


The identity $1 \in \hom(Y,Y)$ is "two flags are the same". Note we can compose invariant relations & $1 \circ 1 = 1$.

Let $A \in \hom(Y,Y)$ be "having the same point but no more". Then $A \circ A = A \cup 1$, because 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" & "changing the point". Then $B \circ B = B \cup 1$. Now $A \circ B$ is one of our atoms, "$p' \in L$ but no more", while $B \circ A$ is another atom, "$p \in L'$ but no more". Finally, $A \circ B \circ A = B \circ A \circ B$ is "nothing interesting". In fact this is a presentation for our monoid in CABA, $\hom(Y,Y)$.

If we draw A as  & 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.