Formal proof of the Gallois correspondance in Homotopy Type Theory

Internship at LIX, École Polytechnique

September, 1st 2025

Hugo Salou

Outline

Section 1

Algebraic Topology

Paths and loops

Definition

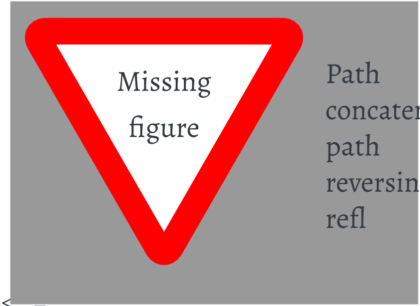
- We write $\mathbf{I}$ the ***unit interval*** $[0, 1]$.
- A ***path*** from x to y is a continuous map p from $\mathbf{I} \to X$ where $p(0) = x$ and $p(1) = y$.
- A ***loop*** at x is a path from x to x.

Operations on paths

Definition

- The ***constant loop*** at x is refl_x defined by $\mathsf{refl}_x(t) := x$.
- The ***reverse*** p^{-1} of a path p is defined by $p^{-1}(t) := p(1-t)$.
- The ***concatenation*** $p \cdot q$ of two paths p and q such that $p(1) = q(0)$ is defined by

$$(p \cdot q)(t) := \begin{cases} p(2t) & \text{if } 0 \leq t \leq \frac{1}{2} \\ q(2t-1) & \text{if } \frac{1}{2} \leq t \leq 1. \end{cases}$$



You shouldn't use *strict* equality

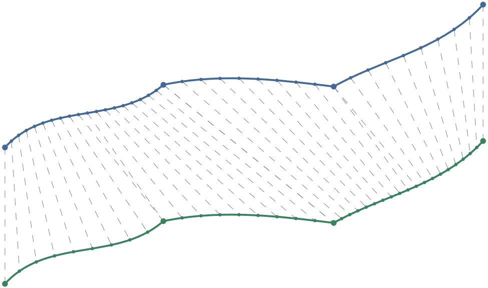


Figure 1 | *Strict equality is too restrictive*

Remark!

1. $p \cdot (q \cdot r) \not\equiv (p \cdot q) \cdot r$
2. $p \cdot \mathsf{refl}_y \not\equiv p$
3. $\mathsf{refl}_x \cdot p \not\equiv p$
4. $p \cdot p^{-1} \not\equiv \mathsf{refl}_x$
5. $p^{-1} \cdot p \not\equiv \mathsf{refl}_y$

Homotopy is the key

Definition

Given two paths p and q from x to y, a ***homotopy*** from p to q is a continuous map

$$H : \mathbf{I} \times \mathbf{I} \to X,$$

such that:

- $H(0, t) = p(t)$;
- $H(1, t) = q(t)$;
- $H(t, 0) = x$;
- $H(t, 1) = y$.

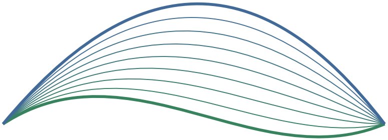


Figure 2 | *Homotopy between paths*

We write $p \sim q$ where there exists a homotopy from p to q. It's an equivalence relation!

A homotopy is a ***path between paths***:

$$\tilde{H} : \mathbf{I} \to \text{Space of paths from } x \text{ to } y$$

A homotopy is a ***path between paths***:

$$\tilde{H} : \mathbf{I} \to \text{Space of paths from } x \text{ to } y$$

... except we'd have to put a topology on the space of paths.

We fixed the "equality issues":

1. $p \cdot (q \cdot r) \sim (p \cdot q) \cdot r$
2. $p \cdot \mathsf{refl}_y \sim p$
3. $\mathsf{refl}_x \cdot p \sim p$
4. $p \cdot p^{-1} \sim \mathsf{refl}_x$
5. $p^{-1} \cdot p \sim \mathsf{refl}_y$
6. if $p \sim q$ then $p^{-1} \sim q^{-1}$
7. if $p \sim q$ and $r \sim s$ then $p \cdot r \sim q \cdot s$.

Fundamental group

Definition

The ***fundamental group*** of (X, x) is the set of homotopy classes of loops at x:

$$\pi_1(X, x) := \left. \text{Set of loops at } x \middle/ \sim \right. .$$

It's a group with path concatenation.

Some examples...

Example

The fundamental group of the sphere $\mathbb{S}^2$ is trivial.

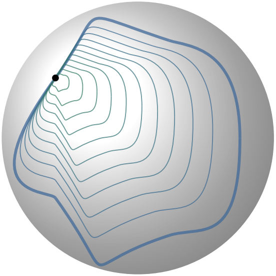


Figure 3 | *Any loop is homotopic to* refl *in* $\mathbb{S}^2$

Some examples...

Example

The fundamental group of the circle $\mathbb{S}^1$ is isomorphic to $\mathbb{Z}$.
There are some loops ℓ such that, to “transform” ℓ to refl require tearing ℓ, as there is a hole in $\mathbb{S}^1$.

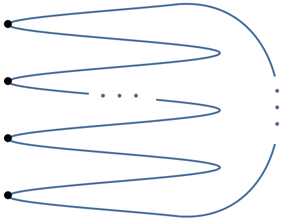


Figure 3 | *“Shape” of loops in $\mathbb{S}^1$*

It's a functor!

Remark!

A continuous pointed map $f : X \to Y$ induces a map

$$\begin{aligned} \pi_1(f) : \pi_1(X, x) &\longrightarrow \pi_1(Y, f(x)) \\ [c] &\longmapsto [f \circ c]. \end{aligned}$$

And, we have:

- $\pi_1(\mathrm{id}_X) = \mathrm{id}_{\pi_1(X)}$;
- $\pi_1(f \circ g) = \pi_1(f) \circ \pi_1(g)$.

Covering spaces

Definition

A ***covering space*** of X is:

- a space $\tilde{X}$,
- a map $p : \tilde{X} \to X$

such that, for every $x \in X$, there exists

- a neighborhood U of x,
- a discrete space D,
- and a homeomorphism $h : U \times D \to p^{-1}(U)$

such that $p(h(x', v)) = x'$.

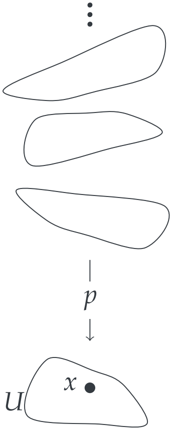


Figure 4 | *Covering space, locally*

Definition

A ***morphism of covering spaces*** is ...Continuer à papoter des revêtements et de la correspondance de Gallois

Section 2

HoTT

Types & propositions

In “regular” type theory, to ***prove*** a statement, we write it as a type and then we write a ***program*** with the corresponding type:

Curry–Howard correspondance!

We do the same thing in HoTT (except “proposition” doesn’t always mean “type” in HoTT).

Dependant types

In HoTT, some types are ***dependants***.

- ***DEPENDANT FUNCTIONS.***
  - we can have $f(x) : B(x)$ (where $x : A$), the output type can depend on the input;
  - we write $f : \prod_{x:A} B(x)$ for the type of such dependant functions;
  - it's a generalization of the $\forall$ and the $\Rightarrow$ (with the Curry–Howard correspondance).
- ***DEPENDANT PAIRS.***
  - we can have a pair (x, y) where $x : A$ and $y : B(x)$, the type of the second element can depend on the first:
  - we write $(x, y) : \sum_{x:A} B(x)$ for the type of such dependant pairs;
  - it's a generalization of the $\exists^*$ and the $\times$ (with the Curry–Howard correspondance).

Equality in HoTT

As we saw, strict equality is ***too restrictive*** for objects defined “up to continuous deformations”. We can’t interpret $x =_A y$ as “x and y are exactly equal.”

How should we interpret $x =_A y$ ***then?***

In HoTT, we interpret it as “there is a ***path*** from x to y in type A”:

$$\text{equality} \quad \rightsquigarrow \quad \text{identification/identity.}$$

Inductive principle of identity

Axiom

To prove a property $\mathcal{P}$ on identifications between x and y, it suffices to show that it holds for the constant path refl_x.

Written differently:

Axiom

Fix a point x and let $\mathcal{P}$ be a property on a point y and a path p from x to y. Then, to show that $\mathcal{P}$ holds for all pairs (y, p), it suffices to show that $\mathcal{P}(x, \mathsf{refl}_x)$ holds.

Missing figure

Inductive principle of identity

Usually we have this in head:

$$\text{if } p : x =_A y \text{ then } x \equiv y \text{ and } p \equiv \mathsf{refl}_x.$$

This is an axiom called ***Uniqueness of Identity Proofs***, ***UIP***.

In HoTT, that's not always true.

When such an implication in type A holds, we call A a ***(mere) proposition***: there is at most one proof of a proposition.

Continuity

Lemma

If $f : A \to B$ is a function then, for any $x, y : A$ there exists an operation

$$\mathsf{ap}_f : (x =_A y) \to (f(x) =_B f(y)),$$

such that $\mathsf{ap}_f(\mathsf{refl}_x) = \mathsf{refl}_{f(x)}$.

Continuity

Lemma

If $f : A \to B$ is a function then, for any $x, y : A$ there exists an operation

$$\mathsf{ap}_f : (x =_A y) \to (f(x) =_B f(y)),$$

such that $\mathsf{ap}_f(\mathsf{refl}_x) = \mathsf{refl}_{f(x)}$.

Proof

To define $\mathsf{ap}_f(p)$ for all $p : x = y$, it suffices, by induction, to assume that path p is refl_x. In this case, we define

$$\mathsf{ap}_f(p) :\equiv \mathsf{refl}_{f(x)} : f(x) =_B f(x).$$

□

Continuity

Lemma

If $f : A \to B$ *is a function then, for any* $x, y : A$ *there exists an operation*

$$\mathsf{ap}_f : (x =_A y) \to (f(x) =_B f(y)),$$

such that $\mathsf{ap}_f(\mathsf{refl}_x) = \mathsf{refl}_{f(x)}$.

Interpreting this lemma: if there is a path between x and y then there is a path between $f(x)$ and $f(y)$. ***Every function in HoTT is inherently continuous!***

Section 3

AGDA

Section 4

The Theorem

Some notations...

We write:

$$\mathrm{Covering}(A, a) := \sum_{(B,b):\mathcal{U}_\bullet} \sum_{p:(B,b)\to(A,a)} \prod_{x:A} \mathrm{isSet}(\mathrm{fib}_p(x)).$$

Section 5

The Proof

Au boulot Hugo !