— récap #4 —

Correspondance de Curry-Howard-Lambek.

Hugo SALOU

Le format est un peu différent cette fois, mais j'espère que ça ira. À la fin de ce document, il y a des exercices qui permettent de manipuler les (co)produits catégoriques. Au prochain « cours », on verra la suite de cette correspondance avec les *exponentielles*. Plus tard encore, on verra les *pull-backs* (*homotopiques*), qui sont des outils importants pour la preuve de la correspondance de Galois en HoTT.

N'hésitez pas à me dire si vous préférez ce format ou non.

1 Étendre Curry-Howard.

En partie #3, on a vu une correspondance entre types et propositions, et entre preuves et termes (ou expressions, ou programmes). La correspondance de Curry-Howard-Lambek est une équivalence entre :

Logique	↔	**Typage**	↔	**Catégories**
Propositions	↔	Types	↔	Objets
Preuves	↔	Termes	↔	Morphismes

La première idée est très formelle. On crée une catégorie nommée **Logique** définie par

- *objets* : propositions logiques ;
- *morphismes* : on a un morphisme de φ à ψ pour toute preuve (au sens d'arbre de preuve) de $\varphi \vdash \psi$;
- *composition* : si on a une preuve M de $\varphi \vdash \psi$ et N de $\psi \vdash \vartheta$ alors on définit leur composée par :

$$\dfrac{\dfrac{\dfrac{N}{\varphi, \psi \vdash \vartheta}}{\varphi \vdash \psi \Rightarrow \vartheta} \Rightarrow_{\mathsf{I}} \qquad \dfrac{M}{\varphi \vdash \psi}}{\varphi \vdash \vartheta} \Rightarrow_{\mathsf{E}};$$

- *identité* : on a une preuve de $\varphi \vdash \varphi$ donnée par la règle Ax.

Pour être très exact, il faudrait « simplifier » des étapes de la preuve, cela s'appelle l'*élimination des coupures* (vu en Projet Fonctionnel).

Modulo des équivalences simples, on a :

$$M : \varphi \to_{\textbf{Logique}} \psi \quad \text{ssi} \quad M \text{ preuve de } \vdash \varphi \Rightarrow \psi.$$

En général, on peut associer à une preuve de $\Gamma \vdash \varphi$ à un morphisme $(\bigwedge \Gamma) \to \varphi$ de **Logique**. Par abus de notations, je noterai $\Gamma \to \varphi$.

Dans la suite, on va montrer que notre modèle catégorique

est sympathique : on peut représenter des $\wedge$ et des $\vee$ dans cette catégorie.

2 Produit catégorique.

Dans **Set**, un produit de deux ensembles A et B est l'ensemble

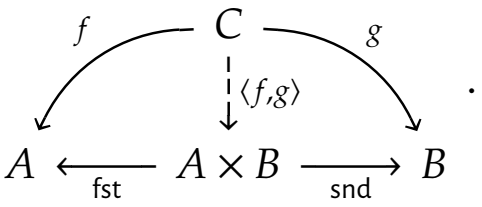
$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Cette construction a deux propriétés très importantes :

- on peut extraire a et b d'un élément de $A \times B$, c'est-à-dire, on a des fonctions

$$\mathsf{fst} : A \times B \to A \quad \text{et} \quad \mathsf{snd} : A \times B \to B \ ;$$

- la construction est « la plus simple possible », dans le sens où, si l'on a $f : C \to A$ et $g : C \to B$, alors on a une unique fonction $\langle f, g \rangle : C \to A \times B$ telle que le diagramme commute :



Question ! Pourquoi complexifier comme ça, avec des « il existe un unique [...] tel que le diagramme commute » ?

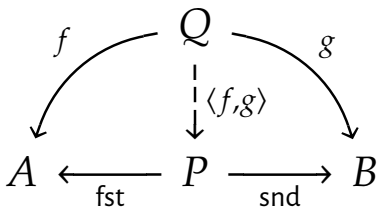
La réponse, c'est que l'on veut généraliser à d'autres caté-

gories, et que l'on ne parle pas d'*éléments* dans une catégorie mais de *morphismes*.

Définition 1. Fixons une catégorie $\mathbf{C}$, et trois objets A, B, P de la catégorie $\mathbf{C}$.

On dit que P est un *produit* (*catégorique*) de A et B si

- il existe $\mathrm{fst} : P \to A$ et $\mathrm{snd} : P \to B$ dans $\mathbf{C}$;
- pour tout objet Q de $\mathbf{C}$ muni de $f : Q \to A$ et $g : Q \to B$, il existe un unique morphisme $\langle f, g \rangle : Q \to P$ tel que



commute.

Ici, on définit le produit, non pas par ces éléments, mais par ces propriétés. Il est important de préciser que : le produit de A et B n'existe pas forcément, et s'il existe, il n'est pas nécessairement unique mais…

Exercice 1. *Le produit de A et B, s'il existe, est unique à isomorphisme près. On s'autorisera donc à écrire $A \times B$.*

Dans la catégorie **Logique**, le produit a un sens important : c'est le « ET » logique ! En effet, pour φ et ψ deux formules :

- on a une preuve de $\varphi \wedge \psi \vdash \varphi$ et de $\varphi \wedge \psi \vdash \psi$;

- c'est la « plus petite » proposition vraie ssi φ et ψ sont vraies, c'est-à-dire si $\vartheta \vdash \varphi$ et $\vartheta \vdash \psi$ alors $\vartheta \vdash \varphi \wedge \psi$ et cette preuve est unique.

Maintenant, dans une catégorie posétale $(P, \leq)$, le produit est exactement le maximum de deux éléments.

D'ailleurs, l'*unicité* du morphisme $\langle f, g \rangle$ est vraie, en considérant les deux objets comme des « boîtes noires ». En effet, dans des cas particuliers, on peut construire plusieurs morphismes.

Quelques exercices pour manipuler un peu plus les produits…

Exercice 2. *Montrer que, si le produit $A \times (B \times C)$ existe, alors $(A \times B) \times C$ aussi, et les deux sont* canoniquement *isomorphes.*

Exercice 3. *Montrer que si $A \times C$ et $B \times D$ existent, et que l'on a $f : A \to B$ et $g : C \to D$, alors il existe un unique*

$$f \times g : A \times C \to B \times D$$

tel que le diagramme suivant commute

$$\begin{array}{ccccc} A & \xleftarrow{\text{fst}} & A \times C & \xrightarrow{\text{snd}} & C \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f \times g} & & \downarrow{\scriptstyle g} \\ B & \xleftarrow[\text{fst}]{} & B \times D & \xrightarrow[\text{snd}]{} & D \end{array}.$$

Montrer que, si $\mathbf{C}$ *possède tous les produits de deux éléments, alors*

$$- \times g : \mathbf{C} \to \mathbf{C} \qquad \text{et} \qquad f \times - : \mathbf{C} \to \mathbf{C}$$

sont des foncteurs.

Ensuite, on peut s'intéresser à des exemples dans certaines catégories.

Exercice 4 (Programmes OCaml)**.** *On définit* $\mathbf{OCaml}$*, la catégorie des programmes OCaml par :*

- *objets : types OCaml* $A, B, \ldots$*;*
- *morphismes : fonctions (pures) calculables* $A \to B$*;*
- *composition : composition usuelle ;*
- *identité : fonction identité.*

Montrer que $\mathbf{OCaml}$ *possède tout produit de deux types. Refaire, dans le cas particulier de cette catégorie, une preuve de l'exercice 2.*

Exercice 5 (Monoïdes, Groupes)**.** *On considère* $\mathbf{Group}$*, la catégorie des groupes, et* $\mathbf{Monoid}$ *la catégorie des monoïdes. Montrer que le produit de deux groupes* (resp. *de deux monoïdes) existe et correspond au produit catégorique dans* $\mathbf{Group}$ (resp. $\mathbf{Monoid}$).

3 Coproduit catégorique.

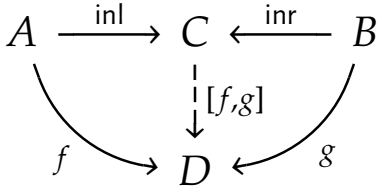
Le *coproduit* est le ***dual*** du produit, on l'obtient en inversant le sens des flèches dans la définition du produit.

Définition 2. Fixons une catégorie $\mathbf{C}$, et trois objets A, B, C

de la catégorie **C**.

On dit que C est un *coproduit* (*catégorique*) de A et B si

- il existe $\mathrm{inl} : A \to C$ et $\mathrm{inr} : B \to C$ dans **C** ;
- pour tout objet D de **C** muni de $f : A \to D$ et $g : B \to D$, il existe un unique morphisme $[f, g] : C \to D$ tel que



commute.

Dans la catégorie **OCaml**, le coproduit de deux types A et B existe toujours et est donné par le type :

$$\texttt{type}\ A + B\ \texttt{=}\ \texttt{Left of}\ A\ \texttt{|}\ \texttt{Right of}\ B,$$

avec quelques abus de notations (il s'agit du type `Either.t`). Le morphisme $[f, g]$ correspond, dans **OCaml**, à :

$$\texttt{let}\ [f, g]\ \texttt{=}\ \texttt{function Left}\ a \to f(a)\ \texttt{|}\ \texttt{Right}\ b \to g(b).$$

Parfois on l'appelle le *type somme* (et par extension la *somme catégorique*).

Sans surprise, dans le cas d'une catégorie posétale, il s'agit du minimum de deux éléments.

Exercice 6. *Montrer que dans* **Logique** *le coproduit de deux formules existe toujours et correspond à l'opération « $\vee$ ».*

Comme pour le produit, on peut montrer les résultats suivants :

- s'il existe, le coproduit est unique à isomorphisme près, on le note donc $A + B$;
- si $A + (B + C)$ existe, alors $(A + B) + C$ aussi et il sont canoniquement isomorphes ;
- si $\mathbf{C}$ possède tous les coproduits, alors $- + g$ et $f + -$ sont des foncteurs $\mathbf{C} \to \mathbf{C}$.

Un cas plus intéressant est le cas des coproduits de groupes et de monoïdes.

Exercice 7. *Pour deux groupes G et H que l'on écrit comme*

$$G = \langle g_1, \ldots, g_n, \ldots \rangle \quad \text{et} \quad H = \langle h_1, \ldots, h_n, \ldots \rangle,$$

(finis ou infinis), en supposant que $G \cap H = \emptyset$, on définit $G * H$ comme le groupe engendré

$$\langle g_1, h_1, g_2, h_2, \ldots, g_n, h_n, \ldots \rangle.$$

C'est l'ensemble des mots finis sur $G \cup H$ sans relations entre éléments de G et éléments de H. On l'appelle le ***produit libre*** *de G et H.*

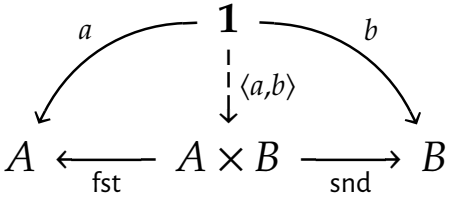
1. *Montrer que $G * H$ est le coproduit de G et H dans* **Group**.
2. *Définir, de la même manière, le coproduit dans* **Monoid**.

4 Retour sur la $\beta\eta$-conversion.

Dans cette section, on se place dans la catégorie **OCaml**.

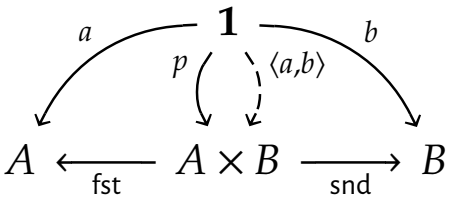
On définit $\mathbf{1}$, un type avec un unique élément noté $\langle\ \rangle$ (par exemple `unit` avec `() : unit` son unique élément). Un morphisme $\mathbf{1} \to A$ correspond à un élément du type A (en effet, on identifie $\langle\ \rangle \mapsto a$ et a).

Considérons le diagramme suivant :



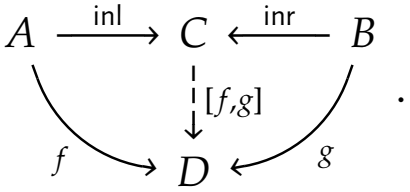
Le triangle de gauche nous dit que $\text{fst}\ \langle a, b\rangle = a$, et celui de droite que $\text{snd}\ \langle a, b\rangle = b$. Ce sont les règles de la β-réduction !

Ensuite, on peut appliquer l'unicité de $\langle a, b\rangle$:



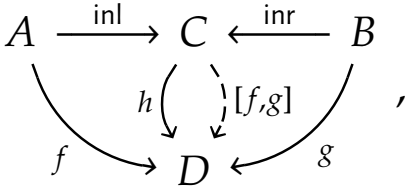
On a donc que $p = \langle a, b\rangle$ ssi $\text{fst}\ p = a$ et $\text{snd}\ p = b$. C'est la règle de l'η-conversion ! Cette règle nous permet d'identifier $\langle \text{fst}\ p, \text{snd}\ p\rangle$ avec p.

Pour le coproduit, on considère le diagramme



On a que $[f, g](\mathsf{inl}\ a) = f(a)$ et $[f, g](\mathsf{inr}\ b) = g(b)$, qui sont exactement les règles de la β-réduction (il faut imaginer la construction $[-, -']$ comme une version très simple du `match`, on a donc comment évaluer ce `match`).

En considérant le diagramme



on a que $h = [f, g]$ ssi $h(\mathsf{inl}\ a) = f(a)$ et $h(\mathsf{inr}\ b) = g(b)$, en appliquant l'unicité de $[f, g]$. C'est l'η-conversion ! On peut donc identifier [inl, inr] avec l'identité.

5 Récap' de Curry-Howard-Lambek.

Au prochain « cours », on verra les éléments de la table ci-après dont je n'ai pas encore parlé.

LOGIQUE	**TYPAGE**	**CATÉGORIES**
M preuve de $\Gamma \vdash A$	M terme tel que $\Gamma \vdash M : A$	M morphisme $M : \Gamma \to A$
$A \wedge B$	$A * B$	$A \times B$
$A \vee B$	$A + B$	$A + B$
$A \Rightarrow B$	$A \to B$	B^A
$\top$	$\mathbf{1}$	1
$\bot$	$\mathbf{0}$	0

Table 1 | *Correspondance de Curry-Howard-Lambek*