Journée Mathématiques et Informatique
Mercredi 28 Février 1990
Université de Picardie
Vol.1, 1990, pp.9-21.

ESQUISSES, STRUCTURES ET ALGORITHMES

René GUITART (U. Paris VII)

BUT

Le but premier de cette conférence est de montrer explicitement le fait suivant :
Il existe un point de vue - à savoir le point de vue des *esquisses* - depuis lequel la définition des structures mathématiques classiques (comme les structures d'anneau, de corps) et la définition des algorithmes (comme la fonction factorielle) sont des procédures identiques.

Deuxièmement, on évoquera l'un des intérêts de ce point de vue des esquisses qui est que de nombreux problèmes mathématiques relatifs aux structures ou aux algorithmes sont susceptibles de se mettre sous la forme d'un *problème de prolongement initial le long d'un morphisme d'esquisse*, et par suite sous la forme d'un *problème de construction d'un modèle initial d'une esquisse.*
Cette possibilité ouvre une voie d'étude de l'impossibilité ou de l'ambiguïté des réponses possibles aux problèmes mal déterminés, en permettant d'associer à chaque problème un espace topologique à homotopie près représentant son indétermination, et ensuite des invariants algébriques mesurant cette indétermination.

CATEGORIES ET FONCTEURS

La théorie des catégories a été initiée par S. Eilenberg et S. Mac Lane (voir [0]), pour donner un statut mathématique à la notion jusqu'alors vague de naturalité.

Une *catégorie* **C** est la donnée de :

- un ensemble $\mathbf{C}_0$ dont les éléments A,B,..., sont appelés les objets de **C**,
- un ensemble $\mathbf{C}_1$ dont les éléments f,g,..., sont appelés les morphismes de **C**,
- deux applications $d_0, d_1 : \mathbf{C}_1 \longrightarrow \mathbf{C}_0$ et une application $i : \mathbf{C}_0 \longrightarrow \mathbf{C}_1$, (pour $f \in \mathbf{C}_1$, $d_0(f)$, notée $d_0 f$, est appelée "source de f", $d_1(f)$, notée $d_1 f$, est appelée "but de f", et, pour $C \in \mathbf{C}_0$, i(C), notée i_C, est appelée "identité sur C"), telles que

$$d_0 \circ i = d_1 \circ i = Id_{\mathbf{C}_0}$$

On convient de représenter l'information " $f \in \mathbf{C}_1$, $d_0 f = A, d_1 f = B$ " par :

$$f : A \longrightarrow B.$$

- Une application $k : \mathbf{C}_2 \longrightarrow \mathbf{C}_1$, avec

$$\mathbf{C}_2 = \left\{ (g,f) \in \mathbf{C}_1 \times \mathbf{C}_1 \ ; \ d_0 g = d_1 f \right\}$$

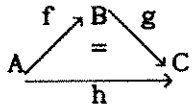
(pour $(g,f) \in \mathbf{C}_2$, k((g,f)) est notée g.f et appelée composé de f suivi de g)

avec les conditions :

- pour tout $f \in C_1$, $f : A \longrightarrow B$, on a : $f.i_A = f = i_B.f$,
- pour tout $(g,f) \in C_2$ on a $d_0(g.f) = d_0 f$ et $d_1(g.f) = d_1 g$,
- pout tout (h,g,f) tels que $(h,g) \in C_2$ et $(g,f) \in C_2$, on a

$$(h.g).f = h.(g.f)$$

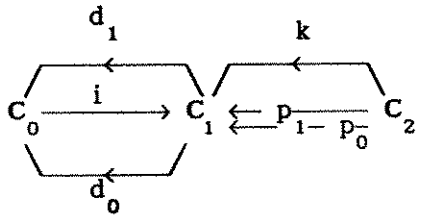
On convient de représenter l'information "h=g.f" par :



On définit les deux applications de projection p_1, $p_0 : C_2 \longrightarrow C_1$ par

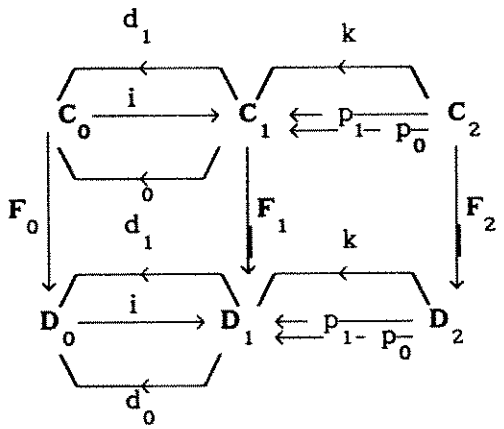
$$p_1((g,f)) = f, \text{ et } p_0((g,f)) = g$$

et alors on peut figurer ensembles les ingrédients définissant **C** ainsi :



Si C et D sont deux catégories, on désigne abusivement par i, d_0, d_1, k (ou "."), p_0,p_1, les opérations identité, source, but, composition et projections dans **C** ou bien les mêmes opérations dans **D**, et un *foncteur* **F** de **C** vers **D** est la donnée notée $F : C \longrightarrow D$, pour chaque objet C de **C** d'un objet F_0A de **D**, et pour chaque morphisme $f : C \longrightarrow C'$ d'un morphisme $F_1 f : FC \longrightarrow FC'$, et ceci de façon que $F_1 i_C = i_{F_0 C'}$ pour tout $C \in C_0$, et de façon que $F_1(g.f) = (F_1 g).(F_1 f)$, pour tout $(g,f) \in C_2$. On pose alors $F_2((g,f)) = (F_1 g, F_1 f)$, pour tout $(g,f) \in C_2$.

Ainsi, la donnée d'un foncteur $F : C \longrightarrow D$ équivaut à la donnée de trois applications $F_i : C_i \longrightarrow D_i$, i=0,1,2, telles que dans le diagramme d'applications suivant on ait les équations indiquées :



$$i \circ F_0 = F_1 \circ i$$
$$F_0 \circ d_0 = d_0 \circ F_1$$
$$F_0 \circ d_1 = d_1 \circ F_1$$
$$F_1 \circ p_0 = p_0 \circ F_2$$
$$F_1 \circ p_1 = p_1 \circ F_2$$
$$F_1 \circ k = k \circ F_2$$

Si dans la définition de catégorie on remplace les conditions que $\mathbf{C}_0$ et $\mathbf{C}_1$ soient des ensembles par la demande que ce soient des classes, on dit alors que **C** est une *grosse catégorie*, et, pour insister, lorsque $\mathbf{C}_0$ et $\mathbf{C}_1$ sont des ensembles on dira que **C** est une *petite catégorie*.

Soit $\mathcal{U}$ un univers, i.e. un modèle de la théorie des ensembles Z.F. On obtient une grosse catégorie notée **Ens** en prenant pour objets les ensembles éléments de $\mathcal{U}$, en prenant pour morphismes de E vers F les applications de E vers F, et en prenant pour composé $g.f = g \circ f$, la fonction composée de f suivie de g, ceci pour $f : E \longrightarrow F$ et $g : F \longrightarrow G$.
On obtient la grosse catégorie **Top** en prenant pour objets les espaces topologiques dont l'ensemble sous-jacent est élément de $\mathcal{U}$, et pour morphismes entre ces espaces les applications continues, la composition étant la composition des applications sous-jacentes.
On obtient la grosse catégorie **Gr** en prenant pour objets les groupes dont l'ensemble sous-jacent est élément de $\mathcal{U}$, et pour morphismes entre ces groupes les homomorphismes de groupes, la composition étant la composition des applications sous-jacentes.
On obtient la grosse catégorie **Cat** en prenant pour objets les petites catégories, pour morphismes de **C** vers **D** les foncteurs de **C** vers **D**, la composition étant définie par $(G.F)_i = G_i \circ F_i$, pour i=0,1,2.

$(1,\Pi,\Sigma)$-ESQUISSE

Une *esquisse* est un graphe multiplicatif (ou système générateur par composition d'une catégorie) où sont marqués des cônes projectifs et des cônes inductifs. La théorie des esquisses a été initiée par A. et C. Ehresmann (voir [1] à [4]), et a donné lieu à de nombreuses applications en géométrie différentielle, en algèbre, en théorie des modèles. Je voudrais, ici, seulement inviter à l'étude des esquisses, qui constituent non seulement un langage naturel, mais aussi une méthode efficace. Aussi, je ne définirai pas en toute généralité les graphes multiplicatifs, les cônes projectifs et les cônes inductifs, les limites projectives et les limites inductives, parce que pour un premier contact avec ce domaine cela serait trop lourd et technique, et masquerait les idées de base qui sont très simples.
Je n'utiliserai donc explicitement qu'un cas particulier de la notion d'esquisse, que j'appellerai les $(1,\Pi,\Sigma)$-esquisses, dont l'usage ne nécessitera que la connaissance des limites projectives particulières que sont les objets finaux et les produits finis et des limites inductives particulières que sont les sommes finies.

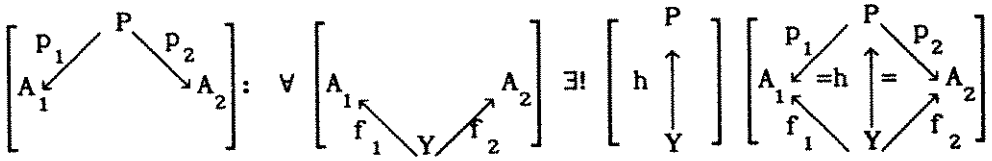
Objet Final 1

On appelle *objet final* 1 dans une catégorie **A**, un objet **1** de **A** tel que pour tout objet X de **A** il existe un unique morphisme $t : X \longrightarrow 1$. Par exemple si **A** est la catégorie **Ens** dont les objets sont les ensembles et dont les morphismes sont les applications, $1 = \{\emptyset\}$ est final.

Produit $P=\Pi(A_1,A_2)=A_1 \times A_2$

Soit A_1 et A_2 deux objets d'une catégorie **A**. On dit que (P, p_1, p_2) est un *produit* de A_1 et A_2 dans **A** si et seulement si P est un objet de **A**, p_1 et p_2

sont des morphismes de **A**, $p_1 : P \longrightarrow A_1$, $p_2 : P \longrightarrow A_2$, tels que pour chaque objet Y de **A**, chaque morphisme $f_1 : Y \longrightarrow A_1$ de **A** et chaque morphisme $f_2 : Y \longrightarrow A_2$ de **A**, il existe un et un seul morphisme $h : Y \longrightarrow P$ tel que $p_1.h=f_1$ & $p_2.h=f_2$.



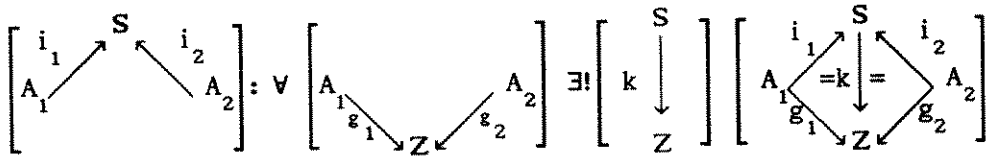
Si P existe il est unique à isomorphisme près, et noté $P=\Pi(A_1,A_2)=A_1 \times A_2$.
Et h est noté (f_1,f_2).
Par exemple, si **A** est la catégorie **Ens**, si A_1 et A_2 sont deux ensembles, un produit s'obtient en prenant :

$$P = \left\{(a_1,a_2) \ ; \ a_1 \in A_1, \ a_2 \in A_2\right\}, \ p_1(a_1,a_2)=a_1, \ p_2(a_1,a_2)=a_2$$

Dans ce cas, h est déterminée par $h(y)=(f_1(y),f_2(y))$.

Somme $S=\Sigma(A_1,A_2)=A_1+A_2$

Soit A_1 et A_2 deux objets d'une catégorie **A**. On dit que (S, i_1, i_2) est une *somme* de A_1 et A_2 dans **A** si et seulement si S est un objet de **A**, i_1 et i_2 sont des morphismes de **A**, $i_1 : A_1 \longrightarrow S$, $i_2 : A_2 \longrightarrow S$, tels que pour chaque objet Z de **A**, chaque morphisme $g_1 : A_1 \longrightarrow Z$ de **A**, et chaque morphisme $g_2 : A_2 \longrightarrow Z$ de **A**, il existe un et un seul morphisme $k : S \longrightarrow Z$ tel que $k.i_1=g_1$ & $k.i_2=g_2$.



Si S existe il est unique à isomorphisme près et noté $S=\Sigma(A_1,A_2)=A_1+A_2$.
Et k est noté $\begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$.
Par exemple, si **A** est la catégorie **Ens**, si A_1 et A_2 sont deux ensembles, une somme s'obtient en prenant :

$$S = \left\{(a,\imath) \ ; \ \imath=1,2, \ a \in A_\imath\right\}, \ i_1(a_1)=(a_1,1), \ i_2(a_2)=(a_2,2)$$

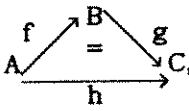
Dans ce cas, k est déterminée par $k(a_1,1)=g_1(a_1)$ & $k(a_2,2)=g_2(a_2)$.

$(1,\Pi,\Sigma)$_esquisse

Une $(1,\Pi,\Sigma)$-*esquisse* consiste en :
- un ensemble d' objets : A, B, C,...

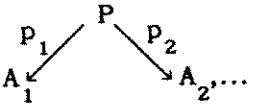
- un ensemble de flèches entre ces objets : $A \xrightarrow{f} B$, $B \xrightarrow{g} C$, $A \xrightarrow{h} C$, ...

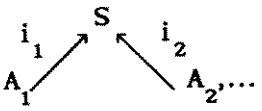
- pour certains objets A, une flèche Id_A, candidate à être l'identité sur A.

- des équations entre ces flèches : 

[pour g.f=h],...

- un candidat à être un objet terminal : 1

- des candidats à être des produits : 

- des candidats à être des sommes : 

Si σ et τ sont deux $(1,\Pi,\Sigma)$-esquisses, un *morphisme de σ vers τ* est la donnée notée $\phi : \sigma \longrightarrow \tau$, pour chaque objet A de σ, d'un objet ϕA de τ, et, pour chaque flèche f de σ, d'une flèche ϕf de τ, et ceci de façon que :

- si $A \xrightarrow{f} B$, alors $\phi A \xrightarrow{\phi f} \phi B$
- si $f = Id_A$, alors $\phi f = Id_{\phi A}$
- si g.f=h, alors $\phi f.\phi g = \phi h$
- si 1 est candidat à être terminal dans σ, alors $\phi 1$ est candidat à être terminal dans τ
- si (P, p_1, p_2) est un candidat à être un produit dans σ, alors $(\phi P, \phi p_1, \phi p_2)$ est un candidat à être un produit dans τ
- si (S, i_1, i_2) est un candidat à être une somme dans σ, alors $(\phi S, \phi i_1, \phi i_2)$ est un candidat à être une somme dans τ

Si σ est une $(1,\Pi,\Sigma)$-esquisse, un *modèle de σ* est un morphisme de σ vers **Ens** considérée comme l'esquisse dont les objets sont les ensembles, dont les flèches sont les applications entre ensembles, où Id_E est définie pour tout ensemble E comme l'application identique de E sur soi-même, où g.f=h si et seulement si le composé $g \circ f$ des deux applications g et f est égal à l'application h, où les candidats à être des objets terminaux, des produits et des sommes, sont précisément les objets terminaux, les produits et les sommes dans la catégorie **Ens**. Un modèle M de σ est noté $M : \sigma \longrightarrow$ **Ens**.
Bien entendu si **Ens** désigne la catégorie de toutes les applications entre les ensembles éléments d'un modèle de ZF, **Ens** ne constitue pas véritablement ainsi une $(1,\Pi,\Sigma)$-esquisse, puisque les objets (et les flèches) de **Ens** ne constituent pas un ensemble mais une classe stricte. On dira que **Ens** est une "grosse" $(1,\Pi,\Sigma)$-esquisse. Mais comme dans la définition des morphismes de $(1,\Pi,\Sigma)$-esquisses la condition que les objets et les flèches constituent des ensembles n'intervient pas, notre définition de modèle de σ est correcte.

Catégorie des modèles d'une $(1,\Pi,\Sigma)$-esquisse σ

Soit σ une $(1,\Pi,\Sigma)$-esquisse. On désigne par **Mod(σ)** la catégorie des modèles de σ, dont les objets sont, donc, les modèles M de σ, $M : \sigma \longrightarrow$ **Ens**, et où un morphisme m de $M : \sigma \longrightarrow$ **Ens** vers $M' : \sigma \longrightarrow$ **Ens** est la donnée, pour chaque

objet A de σ d'une application m_A : MA$\longrightarrow$M'A, et ceci de façon que, pour toute flèche f : A$\longrightarrow$B de σ on ait $(M'f)\circ m_A=m_B\circ(Mf)$. Et la composition dans **Mod**(σ) est définie par $(m'.m)_A=m'_A\circ m_A$. On écrit alors m : M$\longrightarrow$M'.

Si ϕ : $\sigma\longrightarrow\tau$ est un morphisme de $(1,\Pi,\Sigma)$-esquisses, alors on détermine un foncteur ou morphisme de catégorie **Mod**(ϕ) : **Mod**(τ)$\longrightarrow$**Mod**(σ) en associant à chaque modèle M de τ le modèle **Mod**(ϕ)(M) de σ défini par

Mod(ϕ)(M)(A)=M(ϕ(A)) et **Mod**(ϕ)(M)(f)=M(ϕ(f)),

et en associant à chaque morphisme m : M$\longrightarrow$M' le morphisme **Mod**(ϕ)(m) : **Mod**(ϕ)(M)$\longrightarrow$**Mod**(ϕ)(M') déterminé par $\mathbf{Mod}(\phi)(m)_A=m_{\phi(A)}$.

On abrègera **Mod**(ϕ)(M) par M.ϕ, et **Mod**(ϕ)(m) par m.ϕ.

Si **C** est une catégorie et si σ est une $(1,\Pi,\Sigma)$-esquisse telle que **C**$\cong$**Mod**(σ), alors on dit que **C** *est esquissée par* σ. Alors σ joue le rôle d'une syntaxe pour **C**, et **C** le rôle d'une sémantique pour σ. Un premier jeu basique en théorie des esquisses sera celui des traductions *syntaxe*$\longrightarrow$*sémantique* et *sémantique*$\longrightarrow$*syntaxe*. Ainsi dans certains cas la "forme" de l'esquisse σ permet d'obtenir des propriétés de **C**. Par exemple si σ ne comporte pas de candidats à être des sommes, alors **C** possède toutes les petites limites inductives et projectives (en particulier **C** possède un élément final, des produits et des sommes de toute paire d'objets).

$(1,\Pi,\Sigma)$-ESQUISSE DE LA STRUCTURE "CORPS"

Un corps est un ensemble K où sont donnés deux éléments notés 0 et 1, deux opérations binaires notées + et $\times$, une opération unaire partielle notée $()^{-1}$, le tout satisfaisant à des axiomes, dont les deux suivants :

* Associativité de l'addition

$$\forall x,y,z\ [x+(y+z)=(x+y)+z]$$

** Inversibilité des éléments non-nuls

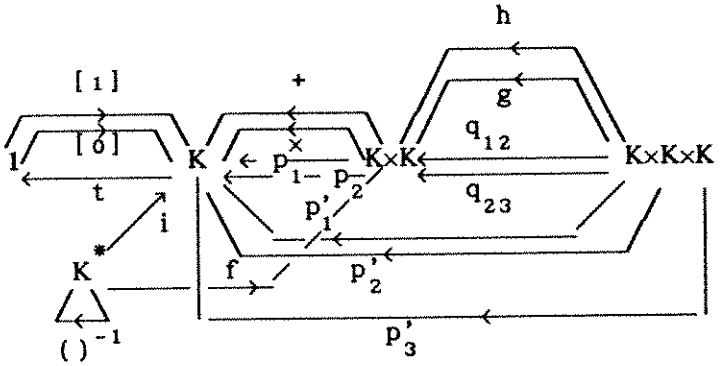
$$\forall x\ [(x=0)\vee((x)^{-1}\text{ est défini }\wedge\ x\times(x)^{-1}=1)]$$

Nous pouvons exprimer ces axiomes, et tous les axiomes de corps, par la donnée d'une $(1,\Pi,\Sigma)$-esquisse κ, de sorte que la catégorie des corps soit isomorphe à **Mod**(κ).

Voici donc comment construire κ de sorte que la donnée d'un corps soit la donnée d'un modèle de κ.

Pour commencer, κ comportera :

- 5 objets, notés 1, K, K^*, K$\times$K, K$\times$K$\times$K,
- des flèches [0], [1], +, $\times$, $()^{-1}$, t, i, p_1, p_2, p'_1, p'_2, p'_3, q_{12}, q_{23}, f, g, et h, disposées entre les objets comme sur le dessin ci-après,



- les équations suivantes :

$$* \begin{cases} p_1 \cdot q_{12} = p'_1,\ p_2 \cdot q_{12} = p'_2\ ;\ p_1 \cdot q_{23} = p'_2,\ p_2 \cdot q_{23} = p'_3 \\ p_1 \cdot g = +\cdot q_{12},\ p_2 \cdot g = p'_3\ ;\ p_1 \cdot h = p'_1,\ p_2 \cdot h = +\cdot q_{23} \\ +\cdot g = +\cdot h \end{cases}$$

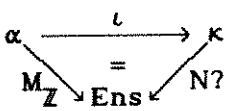
$$** \begin{cases} p_1 \cdot f = i,\ p_2 \cdot f = i \cdot ()^{-1} \\ x \cdot f = [1] \cdot t \cdot i \end{cases}$$

- la donnée de 1 comme candidat à être objet terminal,
- la donnée de $(K\times K,\ p_1,\ p_2)$ et la donnée de $(K\times K\times K,\ p'_1,\ p'_2,\ p'_3)$ comme candidats à être des produits,
- la donnée de (K, [0], i) comme candidat à être une somme.

A ce point, nous avons sous les yeux une $(1,\Pi,\Sigma)$-esquisse κ^- dont un modèle est exactement la donnée d'un ensemble K, de deux éléments 0 et 1 dans cet ensemble, de deux opérations binaires + et × et d'une opération partielle $()^{-1}$, le tout satisfaisant aux axiomes * et **.
La $(1,\Pi,\Sigma)$-esquisse de corps κ s'obtient en continuant cette construction, en ajoutant à κ^- les autres axiomes de corps, qui eux aussi, comme * et **, s'expriment par des équations.

Si dans la $(1,\Pi,\Sigma)$-esquisse de corps κ on supprime la spécification de $(K^*,[0],i)$ comme candidat à être une somme, et la donnée de $()^{-1}$ et des flèches qui en dérivent, comme, par exemple f, et la donnée des équations où ces flèches interviennent, ce qui nous reste est la $(1, \Pi, \Sigma)$-esquisse d'anneau α, et l'inclusion ι : $\alpha \longrightarrow \kappa$ est un morphisme de $(1, \Pi, \Sigma)$-esquisses, et **Mod**(ι) est l'inclusion de la catégorie des corps dans la catégorie des anneaux.

Alors, étant donné un anneau, par exemple l'anneau $\mathbb{Z}$, sous la forme d'un modèle $M_{\mathbb{Z}}$ de α, $M_{\mathbb{Z}}$: $\alpha \longrightarrow$ **Ens**, la question *"$\mathbb{Z}$ est-il un corps ?"* est évidemment équivalente à la question *"existe-t-il un modèle* N *de* κ *tel que* $N.\iota = M_{\mathbb{Z}}$ *?*, question que nous écrirons, avec $M_{\mathbb{Z}}(K)=\mathbb{Z}$,



$(1,\Pi,\Sigma)$-ESQUISSE DE L'ALGORITHME "FACTORIELLE"

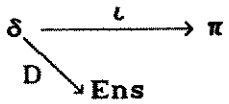
La fonction "factorielle" est définie par récurrence par

$$\begin{cases} fac(0)=1 \\ fac(n)=n\times fac(n-1),\ \text{si } n>0 \end{cases}$$

soit, en COMMON LISP, par le programme :

```
(DEFUN FAC(N)
        (COND ((ZEROP N) 1)
              (T (* N (FAC (- N 1))))))
```

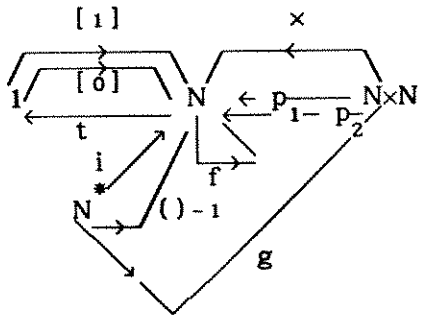
Nous allons voir que cela peut s'exprimer par une donnée de la forme



où ι est un morphisme entre deux $(1,\Pi,\Sigma)$-esquisses δ et π, où D est un modèle de δ.

Soit π la $(1,\Pi,\Sigma)$-esquisse comportant

- 4 objets **1**, N, N^*, N×N,
- des flèches [0], [1], ×, ()-1, t, i, p_1, p_2, f et g, disposées entre les objets comme sur le dessin ci-après,



- les équations suivantes :

$$\begin{cases} f.[0]=[1] \\ f.i=\times.g \\ p_1.g=i\ ,\ p_2.g=\ f.()\text{-}1 \end{cases}$$

- la donnée de 1 comme candidat à être terminal,
- la donnée de $(N\times N,\ p_1,\ p_2)$ comme candidat à être un produit,
- la donné de (N, [0], i) comme candidat à être une somme.

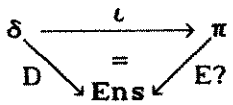
Soit δ la sous-$(1,\Pi,\Sigma)$-esquisse de π obtenue en supprimant dans π les flèches f et g et les équations où ces flèches figurent, soit $\iota : \delta \longrightarrow \pi$ l'inclusion de δ dans π, et soit $D : \delta \longrightarrow$ **Ens** le modèle de δ défini par :
D(N) = $\mathbb{N}$ (ensemble des entiers naturels),

$D(\mathbb{N}^*) = \mathbb{N}^*$ (ensemble des entiers naturels non nuls),

$D(i)$ = l'inclusion canonique de $\mathbb{N}^*$ dans $\mathbb{N}$,
$D(\times) = \times : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}$ la multiplication des entiers naturels,

$D((\,)_{-1}) = (\,)_{-1} : \mathbb{N}^* \longrightarrow \mathbb{N}$, la fonction qui retire 1 à un entier non nul,
le reste de la définition de D étant forcé par l'exigence que D soit un modèle de δ.

On considère alors le problème

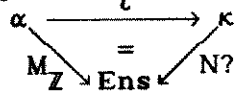


Ce problème admet une unique solution E, donnée par:

$E(f) = fac$, c'est-à-dire $E(f)(n) = fac(n) = n!$, et $E(g)(n) = (n, (n-1)!)$.

On peut donc considérer que, étant donnée une description (par δ et D) des fonctions disponibles sur un ordinateur déterminé, la donnée de π et de l'inclusion ι de δ dans π est un programme, un algorithme, pour calculer la fonction factorielle.

On remarque maintenant que le problème "$\mathbb{Z}$ *est-il un corps ?*", soit



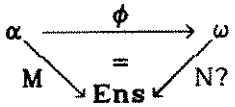
est aussi le problème de déterminer une fonction, à savoir la fonction $(\,)^{-1}:\mathbb{Z}^* \longrightarrow \mathbb{Z}^*$, comme $(\,)^{-1} = N((\,)^{-1})$. La donnée de κ et de l'inclusion ι de α dans κ est un programme, un algorithme, pour calculer la fonction $(\,)^{-1}$.

PROBLEMES DE PROLONGEMENTS ET DE MODELES INITIAUX

Considérons les trois problèmes suivants

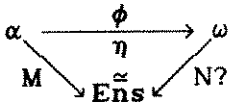
problème 1 :

Etant données α et ω deux $(1,\Pi,\Sigma)$-esquisses, $\phi : \alpha \longrightarrow \omega$ un morphisme de $(1,\Pi,\Sigma)$-esquisses, et $M : \alpha \longrightarrow$ **Ens** un modèle de α, construire un modèle N de ω, $N : \omega \longrightarrow$ **Ens**, tel que $N.\phi = M$:



problème 2 :

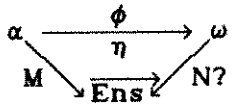
Etant données α et ω deux $(1,\Pi,\Sigma)$-esquisses, $\phi : \alpha \longrightarrow \omega$ un morphisme de $(1,\Pi,\Sigma)$-esquisses, et $M : \alpha \longrightarrow$ **Ens** un modèle de α, construire un modèle N de ω, $N : \omega \longrightarrow$ **Ens**, et un isomorphisme $\eta : M \longrightarrow N.\phi$:



problème 3 :

Etant données α et ω deux $(1,\Pi,\Sigma)$-esquisses, $\phi : \alpha \longrightarrow \omega$ un morphisme de

$(1,\Pi,\Sigma)$-esquisses, et $M : \alpha \longrightarrow \mathbf{Ens}$ un modèle de α, construire un modèle N de ω, $N : \omega \longrightarrow \mathbf{Ens}$, et un morphisme $\eta : M \longrightarrow N.\phi$:



Un problème du type *1* peut avoir une unique solution (exemple de factorielle ci-dessus), pas de solution (exemple ci-dessus du problème de savoir si $\mathbb{Z}$ est un corps), ou bien plusieurs solutions (par exemple si α est vide, les solutions N sont les modèles de ω). Le *problème 3* a plus de solutions que le *problème 2* qui a plus de solutions que le *problème 1.*
La possibilité de plusieurs solutions a priori à ces problèmes suggère de rechercher les solutions "économiques" c'est-à-dire avec le moins de générateurs possibles et pas de relations non-nécessaires. Précisément on considère les problèmes suivants :

problème 1-i :

Construire une solution N_0 du *problème 1* qui de plus soit *initiale*, c'est-à-dire telle que pour toute autre solution N du *problème 1* il existe un unique morphisme $m : N_0 \longrightarrow N$ tel que $m.\phi=Id_M$.

problème 2-i :

Construire une solution (N_0,η_0) du *problème 2* qui soit *initiale*, c'est-à-dire telle que pour toute autre solution (N,η) du *problème 2* il existe un unique morphisme $m : N_0 \longrightarrow N$ tel que $(m.\phi)\eta_0=\eta$.

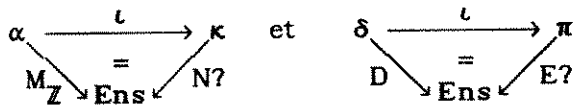
problème 3-i :

Construire une solution (N_0,η_0) du *problème 3* qui soit *initiale*, c'est-à-dire telle que pour toute autre solution (N,η) du *problème 3* il existe un unique morphisme $m : N_0 \longrightarrow N$ tel que $(m.\phi)\eta_0=\eta$.

Si l'un de ces problèmes admet une solution elle est unique à isomorphisme près.

Ces *problèmes 1,2,3,1-i,2-i,3-i* sont appelés des *problèmes de prolongement.*

Plus haut nous avons envisagé les questions *"$\mathbb{Z}$ est-il un corps?"* et *"quelle est la valeur de* factorielle?" comme exprimables sous les formes



Hors, dans ces deux cas, les *problèmes 1* et *2* sont équivalents. Par exemple si (F,η) est une solution du *problème 2* pour (D,ι), la fonction factorielle s'obtient comme $\eta_N^{-1}.F(f).\eta_N$. Et, comme, vue la nature de ι, ces *problèmes 1* et *2* ont au plus une solution, ils sont équivalents aux *problèmes 1-i* et *2-i.*

Bien entendu dans la situation générale, pour un (M,ϕ) quelconque, la situation n'est pas ainsi. Le *problème 1* peut très bien avoir plusieurs

solutions et le *problème 1-i* correspondant avoir zéro solution. En particulier si α est vide le *problème 1-i* est le problème de trouver un modèle initial de ω, ce qui admet une solution si ω ne comporte pas de spécifications de candidats à être des sommes, et qui sinon n'admet pas en général de solution (par exemple si $\omega = \kappa$, la $(1,\Pi,\Sigma)$-esquisse de corps).

Si l'on considère une donnée du type $(\mathbf{M},\phi)$ comme la <u>syntaxe</u> d'un problème sur une structure ou d'un problème de calcul d'un algorithme, cela doit aller de pair avec la fixation d'une <u>sémantique</u>, soit ici le choix d'un problème de prolongement tel que la résolution de ce problème de prolongement pour $(\mathbf{M},\phi)$ coïncide avec la résolution du problème sur la structure ou du calcul de l'algorithme envisagé pour débuter.

Etant donné le *problème 3* et le *problème 3-i* correspondant, il existe une $(1,\Pi,\Sigma)$-esquisse λ telle que le *problème 3* soit équivalent à la recherche d'un modèle de λ, et que le *problème 3-i* soit équivalent à la recherche d'un modèle initial de λ. Cette λ s'obtient en ajoutant à ω un candidat 1 à être objet terminal, en ajoutant, pour chaque objet A de α et chaque élément $a\in\mathbf{M}A$ une flèche noté $a_\in : 1\longrightarrow\phi A$, en ajoutant, pour chaque morphisme $f:A\longrightarrow A'$ les équations $f.a_\in=\mathbf{M}(f)(a)_\in$.

Etant donné le *problème 2* et le *problème 2-i* correspondant, il existe une esquisse μ telle que le *problème 2* soit équivalent à la recherche d'un modèle de μ, et que le *problème 2-i* soit équivalent à la recherche d'un modèle initial de μ. Cette μ s'obtient en ajoutant à λ, pour chaque objet A de α, $(\phi A,\ (a_\in)_{a\in\mathbf{M}A})$ comme candidat à être une somme. Comme $\mathbf{M}A$ n'est pas nécessairement fini, cette esquisse n'est plus une $(1,\Pi,\Sigma)$-esquisse exactement, puisque comportant des spécifications de candidats à être des sommes infinies, mais ce que nous pourrions appeler une $(1,\Pi,\Sigma_\infty)$-esquisse.

Les questions *"$\mathbb{Z}$ est-il un corps?"* et *"quelle est la valeur de* factorielle?" qui nous intéressent, sont donc ainsi transposables en des questions du type

"construire un modèle initial d'une esquisse μ".

Beaucoup de problèmes mathématiques se ramènent à un problème de ce type, du moins si l'on admet des esquisses générales, où sont spécifiables des candidats à être des limites projectives et inductives quelconques.

LES CORPS LIBREMENT ENGENDRES PAR $\mathbb{Z}$

Considérons le problème *"construire un modèle initial de l'esquisse μ"*, et notons-le $\mathrm{cmi}(\mu)$.
La solution peut bien sûr ne pas exister, mais il existe *une* méthode pour tenter de la construire formellement comme "algèbre de termes généralisée", méthode qui dans sa mise en oeuvre même révèle, s'il y a lieu, l'impossibilité d'aboutir. Je vais préciser maintenant ce point, sur l'exemple du problème *"construire un corps initial"*.
Considérons d'abord le problème de construire le groupe G librement engendré par un alphabet X. Ce problème est du type $\mathrm{cmi}(\mu)$ pour une esquisse μ convenable. On construit la solution comme "algèbre de termes" i.e. comme quotient par les axiomes de groupe des termes ou concaténations d'éléments de X et d'opérations de la théorie des groupes, à savoir des expressions du genre $(x\times((y\times z)\times(x\times z)))$,etc. Dans ce cas précis, vu que l'on quotientera par l'associativité, on peut substituer à ces expressions des "mots" comme xyzxz,etc.

En fait, lorsqu'il s'agit d'une esquisse μ quelconque, cette construction des termes est systématisée, nécessite éventuellement une récurrence transfinie qui se stoppe effectivement, mais surtout, lorsque μ ne décrit pas une structure algébrique, nécessite l'introduction de choix arbitraires, qui s'il sont inévitables, vont faire échouer la construction de l'unique modèle initial.
Regardons cette question de choix arbitraire à l'oeuvre dans le problème de la construction d'un corps librement engendré par $\mathbb{Z}$, c'est-à-dire d'un corps initial, soit le problème cmi(κ).

On commence avec $\mathbb{Z}$. On CHOISIT une fonction $c : \mathbb{Z}^* \longrightarrow \{0,1\}$ quelconque.

Alors on peut construire formellement un anneau commutatif unitaire $\mathbb{Z}_c$ et $u_c : \mathbb{Z} \longrightarrow \mathbb{Z}_c$ avec :

- $\forall n \in \mathbb{Z}$ $c(n)=0 \longrightarrow u_c(n)=0$
- $\forall n \in \mathbb{Z}$ $c(n)=1 \longrightarrow u_c(n)$ est inversible
- u_c est un homomorphisme unitaire d'anneau, et $\{u_c(n) ; n \in \mathbb{Z}\}$ engendre $\mathbb{Z}_c$.

Cas I . Si pour tout $n \neq 0$ on a $c(n)=1$, alors $\mathbb{Z}_c=0$

Cas II. S'il existe $n \neq 0$ et $k \neq 0$ avec $c(n)=0$ et $c(kn)=1$, alors $\mathbb{Z}_c=1$ (le "corps" où $0=1$).

Cas III. Si on n'est ni dans le cas I ni dans le cas II, soit $n_0=\inf\{n>0 ; c(n)=0\}$. Alors si $n>n_0$, $n=kn_0+r$, $r<n_0$, et $c(n)=0$ si et seulement si n_0 divise n. Si $m<n_0$, il existe un $m' \in \mathbb{Z}_c$ tel que $mm'=1$, et donc si m' n'est pas formel, $mm'=1$ modulo n_0, soit $mm'+kn_0=1$, et donc (Bézout) m et n_0 sont premiers. Si c'est le cas pour tout $m<n_0$, alors n_0 est premier, et $\mathbb{Z}_c=\mathbb{Z}/n_0\mathbb{Z}$, avec n_0 premier.
En fait si n_0 n'est pas premier, l'un des m' est formel, car de $n_0=mp$ on tire que $mp=0$ dans $\mathbb{Z}_c$, et alors $m'm=1$ donne $m'mp=p=0$, donc $\mathbb{Z}_c=1$.

Ici la construction s'achève en une étape, sans avoir à faire de récurrence. Mais la construction ne peut s'effectuer que par une levée d'arbitraire, un choix d'une fonction c qui fonctionne ainsi : si on veut librement transformer $\mathbb{Z}$ en un corps, il faut que dans ce corps tout élément n de $\mathbb{Z}$ devienne 0 ou inversible ; mais rien dans $\mathbb{Z}$ ou dans la théorie des corps ne permet de décider a priori si n "doit" devenir 0 ou bien si n "doit" devenir inversible ; la fonction c prend la décision. Et c'est le caractère inévitable d'un tel choix arbitraire qui fait qu'il n'existe pas de corps initial, mais plusieurs "candidats malheureux" ($\mathbb{Q}$, 1, les $\mathbb{Z}/p\mathbb{Z}$) dépendant de différentes fonctions c.
Maintenant, a posteriori, on peut constater que ce qui distingue les uns des autres nos candidats c'est leur *caractéristique*. Autrement dit, il sont chacun solution d'un problème précisé : "construire un corps de caractéristique p donnée librement engendré par $\mathbb{Z}$".
On peut considérer que l'impossibilité de résoudre cmi(κ) est décrite par l'ensemble des choix c nécessaires pour poursuivre la construction des termes, en première approximation. Mais en fait des choix différents peuvent donner le même "candidat malheureux", et représenter donc la même alternative, si bien que ce qui représente réellement l'impossibilité de

résoudre cmi(κ) c'est l'ensemble des caractéristiques possibles pour un corps, soit $\{0\}\cup\{p\in\mathbb{N}\ ;\ p \text{ premier}\}\cup\{\infty\}$ =: CAR. Ce CAR est donc la géométrie intrinsèque de l'indétermination du problème cmi(κ).

RESOLUTION DE P(X)=0

Soit $P\in\mathbb{Q}[X]$. Résoudre formellement P c'est construire formellement (soit par adjonctions formelles successives de symboles) un corps K extension de $\mathbb{Q}$ tel que dans K le polynôme P soit complètement décomposé.
Considérons le problème de *"construire une résolution initiale de* P". Cela constitue un problème du type cmi(ρ_P) pour une esquisse ρ_P convenable.

Ce problème n'admet pas de solution, parce que, comme le dit Galois, il comporte une *ambiguïté*, décrite par le groupe de Galois de P, Galois(P).

INDETERMINATION

Les problèmes *"construire un corps initial"* et *"construire une résolution initiale de* P" n'ont pas de solution. On peut considérer que ces problèmes sont ainsi posés par ignorance, sont des énoncés provisoires mal déterminés, jusqu'à ce que, en tentant de les résoudre on découvre l'importance de la notion de caractéristique pour un corps et l'importance du groupe de Galois pour une équation polynomiale, soit l'importance de l'ensemble CAR et du groupe Galois(P) pour les problèmes cmi(κ) et cmi(ρ_P).

Si un algorithme est donné, comme nous l'avons montré sur l'exemple de l'algorithme de la fonction factorielle, sous la forme d'un *problème 2-i*, on ne sait pas a priori si cet algorithme détermine bien au moins une fonction et une fonction unique. Comme cet algorithme équivaut à un problème cmi(μ), nous somme confronté au problème suivant :

Etant donné une esquisse μ, *décrire l'indétermination du problème* cmi(μ)

(Nous envisageons ici ce problème pour une esquisse quelconque, et pas seulement pour une (1,Π,Σ)-esquisse, cela étant indispensable pour obtenir des applications intéressantes, comme par exemple le cas $\mu = \rho_P$).

Il est effectivement possible (voir [7]) d'associer à μ un *type d'homotopie* gμ représentant l'indétermination de cmi(μ). En particulier on aura gκ = CAR, et $\pi_1 g\rho_P$ = Galois(P). La construction générale de gμ consiste à utiliser le théorème A de Quillen et le théorème du diagramme localement libre de Guitart-Lair (voir [5] et [6]) pour montrer qu'il existe dans la classe /N**Mod**(μ)/ (réalisation géométrique du nerf de la catégorie des modèles de μ) un ensemble gμ tel que l'inclusion de gμ dans /N**Mod**(μ)/ soit une équivalence d'homotopie.

L'existence de gμ est un garde-fou, une garantie générale que la recherche d'invariants algébriques mesurant l'indétermination d'un problème cmi(μ) n'est pas démesurée, puisque de tels invariants se définissent alors par exemples comme $\pi_1 g\mu$, $H^n(g\mu,\mathbb{R})$, $H_n(g\mu,\mathbb{Z})$,etc. Mais c'est ensuite une autre histoire que de calculer explicitement, algébriquement, ces groupes à partir de la donnée μ, voir à partir de l'algorithme auquel est associée μ.

REFERENCES

[0] S. Eilenberg and S. Mac Lane, *General Theory of Natural Equivalences*, Trans. A.M.S. 58 (1945), 231-294.

[1] C. Ehresmann, *Introduction to the theory of structured categories*, Department of math., University of Kansas, Technical Report 10, 1966, 95 pages.

[2] C. Ehresmann, *Sur les structures algébriques*, C.R.A.S. Paris, t.264, p.840-843, 17 mai 1967.

[3] C. Ehresmann, *Esquisses et types des structures algébriques*, Bul. Inst. Pol. Din Iasi, serie noua, t.XIV (XVIII), fasc.1-2. 1968, pp.1-14.

[4] A. and C. Ehresmann, *Categories of sketched structures*, Cahiers Top. Géo. Dif., vol.XIII-2, 1972, pp.407-516.

[5] R. Guitart et C. Lair, *Calcul syntaxique des modèles et calcul des formules internes*, Diagrammes, vol.4, 1980, 106 p.

[6] R. Guitart et C. Lair, *Existence de diagrammes localement libres, I et II*, Diagrammes, vol.6, 1981, 13 p., et vol.7, 1982, 4 p.

[7] R.Guitart, *On the geometry of computation, I et II*, Cahiers Top. Géo. Dif. Cat., vol.XXVII,4, p.107-136, (1986), et vol.XXIX,4, p.297-326, (1988).

René Guitart, UFR de Maths, tours 45-55, 5e étage,Université Paris VII,

2 Place Jussieu, 75005 Paris, France