UNIVERSITÉ BORDEAUX 1

Leçons de mathématiques d'aujourd'hui

Jeudi 5 juin 1997

La théorie de la démonstration, du programme de Hilbert à la logique linéaire[1]

Jean-Yves GIRARD

(Institut de mathématiques de Luminy, Université de Marseille)

---

[1] Rédigé par Pierre CASTÉRAN et Éric CHARPENTIER.

Table des matières

1 La « crise des fondements »

1.1 La théorie naïve des ensembles : grandeur et décadence

On va remonter très loin dans le passé : jusqu'à la « crise des fondements ».

Cantor, vers 1880, a inventé la théorie des ensembles —pour des tas de raisons, qui peuvent nous sembler un peu étranges, notamment l'étude des *ensembles d'exception* pour les séries trigonométriques. . .[2]

La théorie des ensembles permet pour la première fois d'envisager une idée bizarre, l'*unité* des mathématiques : il est théoriquement pensable qu'il n'y ait qu'une seule mathématique, je dis bien : *théoriquement*. On peut donc, en principe, combiner librement tous les aspects du raisonnement mathématique. Ce qui contraste agréablement avec —disons— la physique, constituée d'îlots réunis par des passerelles hasardeuses : on ne sait pas trop pourquoi un problème est du ressort de la mécanique quantique plutôt que de la théorie des champs —enfin, c'est tout un sujet.

L'unité des mathématiques nous permet d'aborder le même problème de théorie des nombres par la théorie analytique ou la théorie algébrique, qui appartiennent pourtant à des univers mathématiques *a priori* éloignés, voire incompatibles. Cela dit, il n'est pas vrai qu'un nombre réel —même de nos jours— soit devenu ce que la théorie des ensembles voudrait en faire, c'est-à-dire essentiellement un ensemble d'entiers —vous savez, les rationnels se réduisent à des couples de nombres relatifs, lesquels se réduisent à des couples de nombres positifs ; ensuite, un réel c'est une (classe d'équivalence d'une) suite de rationnels, une suite se réduit à un ensemble, donc finalement on trouve qu'un réel est un ensemble (d'ensembles d'ensembles. . .) d'entiers : si on prend ça au pied de la lettre, c'est une ânerie : essayez donc de résoudre une équation du second degré au moyen d'ensembles d'entiers ! C'est absurde. Mais enfin, ce qui est intéressant, c'est la *possibilité*, à travers des machines —qu'on commence d'ailleurs à activer avec des logiciels de vérification formelle— de « tout mettre dans le même système ».

L'ingrédient de base de cette théorie des ensembles est ce qu'on appelle le *schéma de compréhension*, qui dit que « toute propriété définit un ensemble » : étant donné une propriété P, on considère la collection des a qui vérifient $P[a]$, et ça définit un ensemble x, autrement dit : $\exists x \, \forall a \;\; (a \in x \Leftrightarrow P[a])$.

Évidemment, on peut définir énormément de choses comme ça, on peut en faire tout ce qu'on veut, à tel point qu'en 1897, un monsieur qui s'appelait Burali-Forti[3] —et dont on se souvient d'ailleurs uniquement pour cette raison— trouve un paradoxe (et même, en fait, une contradiction)[4]. Un peu plus tard (en 1901), Bertrand Russell —bien connu pour avoir fait par la suite de la philosophie et de la politique— trouve un paradoxe analogue mais encore plus

---

[2] Cf. la Leçon de G. Godefroy, dans ce volume. (N.d.r.)

[3] Voir [Burali-Forti, 1897a, Burali-Forti, 1897b]. (N.d.r.)

[4] Il y a plus qu'une nuance : la « courbe » de Peano qui passe par tous les points d'un carré est paradoxale en ce qu'elle contredit notre intuition quant à la continuité ; mais il ne s'agit pas d'une contradiction formelle.

simple[5]. Le paradoxe de Russell surgit quand on considère l'ensemble X des ensembles qui ne s'appartiennent pas à eux-mêmes, c'est-à-dire $X = \{a; a \notin a\}$, obtenu en appliquant le schéma de compréhension à la propriété $P[a] : a \notin a$. On voit que : $X \in X \Leftrightarrow X \notin X$ et, en bonne logique, on obtient une contradiction (du moins en logique classique ; maintenant il y a des nouveautés avec la *logique linéaire allégée* [Girard, 1998], mais je n'aurai pas le temps de vous en parler).

Quand on le regarde de près, on voit que le paradoxe de Russell est un recyclage d'un argument mathématique, la diagonalisation de Cantor, qui est lui même le recyclage d'un vieux truc des philosophes, le paradoxe du menteur : c'est l'histoire du Crétois Épiménide qui disait que les Crétois sont menteurs, ou plutôt, si on veut une vraie contradiction, c'est Eubulide qui dit : « je mens ». Alors, s'il dit la vérité, il ment, puisque c'est ce qu'il affirme : contradiction. Et s'il ment en disant « je mens », c'est qu'il ne ment pas : encore une contradiction.

La diagonalisation de Cantor a servi par exemple à démontrer que l'ensemble des parties de $\mathbb{N}$ n'est pas dénombrable. Tout simplement, si vous prenez une famille dénombrable $\{X_n\}$ de parties de $\mathbb{N}$, vous définissez la relation $n \ R \ m \ : n \in X_m$, et vous prenez l'ensemble $\{n; \neg(nRn)\}$; cette partie-là n'appartient pas à la famille $\{X_n\}$. (Supposez que c'est X_m : si $m \in X_m$, on a donc $m \notin X_m$, et réciproquement.) Donc l'ensemble $\mathcal{P}(\mathbb{N})$ des parties de $\mathbb{N}$ n'est pas dénombrable, puisque pour toute famille dénombrable $\{X_n\}$ l'argument donne une partie de $\mathbb{N}$ qui n'est pas dans cette famille. Et c'est amusant : c'est l'argument de Cantor qui a été utilisé (par Russell) pour démolir la théorie de Cantor !

1.2 Une crise de quoi ?

Quand sont apparus, vers 1900, ces paradoxes, on a parlé de *crise des fondements* ; est-ce que c'était vraiment une crise ? En regardant cela avec un peu de distance : est-ce que ça engageait vraiment les mathématiques ? On pouvait sûrement continuer à travailler sur les fonctions analytiques, ou en algèbre, sans se poser ce genre de problème ; ça ne concernait premièrement que les *liens* entre diverses parties des mathématiques —liens assurés par la théorie des ensembles— et deuxièmement des choses somme toute expérimentales et marginales (si on peut faire la différence entre ces deux mots). Le schéma de compréhension était utilisé dans des cas très simples, par exemple pour définir la paire formée de deux ensembles, l'union, le produit cartésien : des choses extrêmement pratiques. Mais pourquoi pousser ce truc à l'extrême ? Les mathématiques existaient, elles n'attendaient pas la théorie des ensembles, elles n'étaient pas vraiment concernées par le problème. On savait bien qu'au pire on aurait *jeté* la théorie des ensembles.

Et puis, en 1908, le grand logicien Zermelo a produit une nouvelle version de la théorie des ensembles [Zermelo, 1908], basée sur une restriction du schéma de compréhension. Essentiellement, au lieu d'écrire « l'ensemble des a qui vérifient P », on écrit « l'ensemble des a qui vérifient P *et qui sont déjà dans un ensemble donné* x_0 » : $\forall x_0 \ \ \exists x \ \ \forall a \ \ (a \in x \Leftrightarrow a \in x_0 \wedge P[a])$.

Voilà la nuance : on a seulement le droit de construire des ensembles *plus petits* qu'un ensemble (quelconque) qu'on a déjà. Pour fabriquer des ensembles *plus grands*, il faut ajouter aussi quelques nouveaux axiomes, qui garantissent l'existence de l'ensemble des entiers et de l'ensemble des parties d'un ensemble, et on obtient la théorie dite de Zermelo (il y a eu ensuite la version plus complète dite de Zermelo-Fraenkel, mais dans la pratique on ne se sert que de Zermelo). Et depuis, il n'y a jamais eu de problème. Par exemple, le « paradoxe de Russell »

---

[5] Publié dans [Russell, 1903]. (N.d.r.)

appliqué à $x = \{y \in x_0, y \notin y\}$ devient simplement une preuve que x n'est pas un élément de x_0. Mais la « crise » avait traumatisé deux ou trois personnes et on a eu droit au fameux « programme de Hilbert ».

2 Le programme de Hilbert

2.1 Un chevalier blanc et une ontologie

Hilbert s'est manifesté deux fois là-dessus. La première fois, dans les années 1900 : il y a eu d'abord sa conférence au Congrès International de Mathématiques à Paris, en 1900, où il a énoncé une liste de 23 problèmes qui lui semblaient cruciaux pour l'avenir des mathématiques (les deux premiers problèmes concernaient les fondements[6]) —voir aussi sa conférence au congrès de Heidelberg 4 ans plus tard [Hilbert, 1905]. La deuxième fois, c'était autour de 1925, et là il s'est vraiment beaucoup excité : voir [Hilbert, 1926]. Hilbert se présentait carrément comme le chevalier blanc qui allait sauver les mathématiques menacées par le sida, le cancer du paradoxe. C'était assez délirant, et c'est vraiment à rapprocher d'Edgar Hoover, le fondateur du F.B.I. qui a « sauvé » les États-Unis du communisme en instrumentalisant un prétendu danger. Le *Programme de Hilbert* de fondement des mathématiques est un programme philosophique à mettre en œuvre par des moyens entièrement mathématiques ; une tentative de *prouver mathématiquement une opinion philosophique*, ce qui est une première et —on l'espère— une dernière.

Au fond, dit Hilbert, le seul problème, c'est le *statut de l'infini.* Tout est arrivé parce qu'on a manipulé des infinis de plus en plus douteux : on est passé du dénombrable au continu, puis à des ensembles de fonctions, et puis au bout d'un moment, à l'ensemble des ensembles qui ne s'appartiennent pas à eux-mêmes : on ne sait plus du tout de quelle taille c'est. Donc, c'est bien cela : il faut clarifier le *statut de l'infini.* Et alors Hilbert dit une chose toute simple : « L'infini, ça n'existe pas ». Ce qui est sûr avec un tel « statut » c'est qu'il n'est pas ambigu !

On va diviser l'ontologie de Hilbert en trois cases :

1. ce qui existe, ou n'existe pas ;
2. ce qui signifie, ou ne signifie pas ;
3. ce qui convainc, ou ne convainc pas.

	Existant	Signifiant	Convaincant
oui	Entiers, constructions finies.	Propriétés récessives, $a^n + b^n \neq c^n$ ($abc \neq 0$, $n \geq 3$).	Maths du lycée, récurrence simple.
non	Nombres réels, espaces de Hilbert, bases de $\mathbb{R}$ sur $\mathbb{Q}$.	Propriétés expansives.	Compréhension, Axiome du choix.

Qu'est-ce qui existe ? Eh bien c'est facile, ce sont les entiers, les constructions finies... Les informaticiens ajouteront les listes, les arbres finis, les choses comme ça. Ça a l'air d'une bêtise, car on sait que les listes, les arbres finis, sont codables par des entiers. Mais il est vrai que dans la pratique ce n'est pas la même chose : un entier comme suite de bâtons, ou en

---

[6] Le premier problème était l'Hypothèse du continu de Cantor ; le second était celui de la compatibilité des axiomes de l'arithmétique. On trouvera le texte de la conférence de Hilbert au Congrès de Paris, traduit en anglais, à l'URL : `http ://aleph0.clarku.edu/~djoyce/hilbert/problems.html`. (N.d.r.)

représentation binaire, ça fait une grosse différence. Bon, mais *fondamentalement* —c'est-à-dire dans une problématique fondamentaliste, où on réduit tout à des idées simples— les seules choses qui existent sont les entiers. Comme disait Kronecker : « Dieu a fait les entiers, et l'homme a fait le reste ».

Ce qui n'existe pas : les nombres réels (!), les espaces de Hilbert (!), les bases de $\mathbb{R}$ sur $\mathbb{Q}$ (utilisation de l'axiome du choix), les choses non mesurables au sens de Lebesgue : voilà des objets de moins en moins plausibles.

Maintenant, qu'est ce qui fait sens ? Évidemment, pour qu'une propriété soit signifiante, il faut qu'elle ne parle que d'objets qui existent. Par exemple, vous ne pouvez rien dire de signifiant sur les anges si les anges n'existent pas, d'accord ? Parce qu'alors chacun peut en dire ce qu'il veut : il n'y a pas la contrainte du réel, on parle dans le vide. Les propriétés signifiantes doivent donc être des propriétés des entiers. Hilbert demande qu'elles soient de plus *récessives*[7], i.e., ne mentionnant l'infini que sous la forme d'une quantification universelle sur les entiers, typiquement $A = \forall n \ P[n]$. Une telle propriété peut s'« approximer » au moyen de vérifications systématiques, soit par $\forall n \leq N \ P[n]$; quand N augmente, l'approximation s'affine et peut devenir fausse (et le reste alors dans les approximations ultérieures) : c'est en cela que la propriété « régresse ». C'est le type de propriété qu'on ne pourra jamais vérifier dans son intégralité, mais dont on verra des segments arbitrairement grands. L'exemple type en est le théorème de Fermat, que vous connaissez tous, évidemment (on en a beaucoup parlé récemment) ; ou les identités algébriques : $(n+1)^2 = n^2 + 2n + 1$. Ce sont des choses qu'on vérifie *cas par cas* sans en épuiser la liste. Le cas le plus simple de non-signifiant selon Hilbert, ce sont les énoncés purement existentiels —donc les négations d'énoncés récessifs— et qu'on appellera donc « expansifs », vu qu'ils sont de plus en plus vrais quand l'approximation s'affine.

Et enfin, qu'est-ce qui convainc ? Ce sont les maths du lycée, math sup, math spé au mieux ; tout ce qu'on a pu traduire en termes d'entiers (même si on parle de fonctions, du moment qu'on a pu les approximer par des objets finis) ; bref, tout ce qu'on peut faire par des manipulations d'entiers, purement mécaniques, et par des récurrences. Et je parle de récurrences simples (parce qu'il y a aussi des récurrences doubles : on peut « récurrer » sur deux arguments, avec un argument principal et un argument secondaire ; sans parler des récurrences transfinies dont la récurrence double est le cas le plus simple !)...

Alors, qu'est ce qui ne nous convaincrait pas ? Eh bien c'est le schéma de compréhension, et bien sûr tout ce qui utilise l'Axiome du Choix, par exemple la démonstration de Zermelo que les nombres réels peuvent être bien ordonnés, i.e., énumérés dans une liste transfinie.

Et voilà, c'est toute l'ontologie de Hilbert. Elle a d'ailleurs été reprise par un épigone fameux : Karl Popper, qui avait sa division du monde entre les propriétés qu'il appelait falsifiables et les autres, infalsifiables. Les propriétés falsifiables, c'est tout ce qu'on peut approximer : une loi physique, vous l'avez vérifiée sur un certain nombre de cas, ou à un certain degré de précision près ; et vous pouvez dire : « Pour tout degré de précision, pour tous les cas que j'ai examinés, j'ai rencontré P ». Ou encore : « Jusqu'ici, ça va ». C'est bien l'idée d'une *approximation.* Comme je l'ai dit, je préfère parler de propriété « récessive », i.e., qui s'amenuise avec les vérifications, les propriétés duales —existentielles— étant appelées « expansives ». Ce qui intéresse Hilbert, c'est le récessif, les propriétés du genre « l'équation n'a pas de solution » ; tout comme Popper considère que les seules énoncés scientifiques ayant un sens sont les énoncés « falsifiables ».

---

[7] Cette terminologie me semble meilleure que « falsifiable » ou « approximable ».

2.2 Le programme : un principe de conservation

Prenons une propriété récessive, et supposons qu'on l'ait démontrée avec de « mauvaises » méthodes, c'est-à-dire avec les mathématiques habituelles : de l'infini, l'axiome du choix, les pires trucs que vous pouvez imaginer. Il s'agit de montrer qu'elle a aussi une démonstration « politiquement correcte »; donc qu'on peut la démontrer avec les mathématiques du lycée, avec les maths de papa ou de grand papa. Ce qu'on veut donc montrer, c'est un résultat de conservation : à savoir *qu'on ne montre rien de plus avec les méthodes infinies qu'avec les méthodes finies, au sens le plus étroit du terme.* Bien sûr, c'est nier la complexité des mathématiques.

Mais, si vous voulez être vraiment convaincant, vous ne pouvez pas montrer cette propriété de conservation avec n'importe quelles mathématiques, il faut la démontrer avec les *vraies* mathématiques, les maths du lycée. Parce que les maths du lycée, au moins, il ne peut rien leur arriver, elles sont sûres, elles sont parfaites, elles n'ont pas de problème de fondation, n'est-ce pas ? Les « mathématiques élémentaires » interviennent donc deux fois dans le programme, puisqu'elles doivent servir à établir une propriété *qui les concerne*, à savoir qu'il n'est rien hors d'elles, qu'elles sont en quelque sorte *complètes*.

Voilà donc le programme de Hilbert : démontrer le résultat de conservation avec les « bonnes » méthodes. Mais comment peut-on démontrer une telle chose, qu'est-ce que Hilbert avait en tête ? Je vous donne un exemple. On veut démontrer que l'équation $f(x) = f^3(x)$, où $f^3(x)$ signifie $f(f(f(x)))$, *n'implique pas* celle-ci : $f^4(x) = f^3(x)$. On pourrait dire : *soyons concret, je vous sors une fonction* f *qui vérifie* $f(x) = f^3(x)$ *et qui ne vérifie pas* $f^4(x) = f^3(x)$. OK, on peut le faire, parce que j'ai pris un exemple extraordinairement simple. Mais dans les problèmes compliqués, comment trouver les contre-exemples ? Sûrement pas par l'axiome du choix ! Ce serait comme si on n'avait rien fait, du point de vue de Hilbert. Et puis la recherche de contre-exemples pose des tas de problèmes de *statut* des objets mathématiques, d'objectivité : il y a quelque chose qui est extérieur à nous, on ne sait pas ce que c'est, on ne va pas y toucher.

Alors que proposerait Hilbert, pour cet exemple ? Eh bien on peut remarquer que quand on joue avec l'équation pour en tirer de nouvelles, il y a un phénomène de parité entre les deux membres : *la différence entre le nombre d'occurrences de* f *dans les deux membres* de l'équation et de toutes celles qu'on peut en déduire, *est toujours un nombre pair.* Et ça, on peut le montrer par une récurrence toute bête. Donc, si vous me présentez une équation où cette différence est un nombre impair, eh bien je suis sûr que cette équation ne découle pas de $f(x) = f^3(x)$. Or, c'est le cas de $f^4(x) = f^3(x)$: CQFD.

C'est exactement ce genre de preuves que Hilbert a en tête : regarder le formalisme et trouver, derrière, un principe de régularité, par exemple : « tout énoncé démontrable a un nombre pair de symboles ». C'est aussi naïf que ça ! Et si en plus je constate qu'une absurdité (comme $1 = 0$) a un nombre impair de symboles, alors je prouve du même coup que dans ma théorie je ne peux pas démontrer n'importe quoi. Ce qui me permet de réaliser le programme de Hilbert sous sa forme la plus connue : « *donner une démonstration élémentaire de la cohérence des mathématiques* ». Prenez la théorie des ensembles, celle que vous voulez, ou l'arithmétique de Peano ; voici le genre de recette dont rêve Hilbert pour démontrer, avec les méthodes élémentaires, qu'il n'y a pas de contradiction dans votre théorie : classez les formules en deux couleurs, de manière toute bête, par exemple en regardant le nombre de connecteurs, en multipliant par 3, en retenant 2, les chiffres et les lettres,... et hop ! en rouge ce qui est démontrable, en vert ce qui est réfutable, et on constate que $1 = 0$ est vert, donc la théorie n'est pas contradictoire. Un truc comme ça, quoi ! Un truc tout à fait élémentaire. On peut en rire, tellement ça paraît stupide, mais quand même il y a quelque chose. Le formalisme, on va s'en apercevoir à la fin de l'exposé, ce n'est pas n'importe quoi, il y a des propriétés très profondes. Mais, en attendant, ça ne donne pas ce que c'était censé donner d'après Hilbert (ça va même donner le contraire, en un sens). Hilbert était très convaincu par son programme, il l'a annoncé en 1925 comme un résultat imminent ; d'ailleurs, dans le même article sur l'infini, il annonçait aussi qu'il avait résolu l'hypothèse du continu —avec une démonstration qui est complètement fausse, bien sûr. Mais il s'est cassé la figure : c'est la chute, la chute de la Maison Hilbert.

3 La chute

3.1 Immersion

L'originalité de Hilbert, c'est qu'il a immergé la réflexion *sur* les mathématiques *dans* les mathématiques. Cette idée est très profonde, ça n'a l'air de rien mais quand on dit « ce système est logiquement cohérent » c'est *aussi* une formule de mathématiques. Et Hilbert qui —comme tous les scientistes— était un peu fanatique, n'était pas idiot. Il s'est donné un outil pour *démontrer* quelque chose. Ce qui s'est passé, c'est que cet outil a servi au contraire à *réfuter* tout son programme formaliste. Hilbert a forgé un outil tellement tranchant qu'il s'est coupé avec ! Voyons cela.

Gödel, en 1931, commence par compléter le programme de Hilbert, en construisant explicitement l'immersion dont rêvait Hilbert, et qui va permettre de faire de l'énoncé « la théorie T est cohérente » un énoncé de pure arithmétique. D'abord, qu'est-ce que la cohérence d'une théorie T ? Prenez pour T la théorie que vous voulez, assez puissante quand même pour pouvoir y faire de la bonne vieille arithmétique à papa —ça peut être la théorie des ensembles de Zermelo, ou le système que vous imaginez quand vous faites des mathématiques. L'immersion de Gödel, et donc le théorème qui va suivre, s'appliqueront à tous ces systèmes-là. Une démonstration, dans T, c'est un assemblage fini de propositions, qui s'enchaînent selon les règles d'inférence en vigueur, en commençant par des axiomes. En utilisant astucieusement l'existence et l'unicité de la décomposition des entiers en facteurs premiers[8], Gödel attribue un nombre entier aux constantes, aux variables, aux parenthèses, etc. puis aux formules, puis aux démonstrations elles-mêmes[9]. Ce qui fait que la propriété « π *est une démonstration de* A » se traduit par un énoncé de pure arithmétique $P(\ulcorner \pi \urcorner, \ulcorner A \urcorner)$, qui exprime une relation entre les nombres $\ulcorner \pi \urcorner, \ulcorner A \urcorner$ associés à π et A. La cohérence de T dit qu'aucune démonstration π n'aboutit à l'absurdité : $\perp$. En formules :

$$\forall p \ \neg P(p, \ulcorner \perp \urcorner)$$

C'est un énoncé de T, et il est récessif : c'est fantastique, la seule chose qui intéresse Hilbert, c'est-à-dire la cohérence, fait partie des énoncés auxquels il concède une signification !

3.2 Le(s) théorème(s) d'incomplétude de Gödel

Et alors Gödel casse la baraque. D'abord, une remarque : on vient de voir que la cohérence de T s'exprime par un énoncé de T : $\forall p \ \neg P(p, \ulcorner \perp \urcorner)$. Ce « couronnement » du programme de Hilbert suffit à l'anéantir : car dans une théorie T *contradictoire*, on peut tout prouver, y compris la non-contradiction —si on peut la formuler dans T : une *preuve de non-contradiction*

---

[8] En réalité, le « théorème du Chinois ».

[9] Cf. par exemple [Girard, 1987b]. (N.d.r.)

dans la théorie elle-même est donc *a priori* au moins aussi inquiétante —pensez aux sectes— que rassurante, et en tout cas elle ne prouve rien. Et ce que Gödel va prouver, maintenant, c'est que si T est cohérente, une preuve de cohérence dans T n'est pas possible, *un point c'est tout !* C'est ce que nous disent ses théorèmes d'incomplétude, ou *le* théorème d'incomplétude, si vous voulez : c'est plutôt un théorème qui a deux formes.

Ce qu'on appelle le *premier* théorème d'incomplétude, c'est la diagonalisation, la même technique que chez Cantor et Russell, appliquée à la démonstrabilité. En fait, persistait à l'époque une confusion entre *vrai* et *démontrable* : on pensait que toutes les propriétés vraies étaient démontrables (c'est flagrant, on ne voit pas la distinction dans la littérature). Et je pense que Gödel a vraiment cherché à fabriquer une absurdité, une formule qui dise « je ne suis pas vraie ». Une version du paradoxe du menteur dans les mathématiques : une catastrophe ! Il l'a trouvée à partir de la démonstrabilité, et il a dû vraiment croire un moment qu'il avait une absurdité. Mais au bout d'un instant, il s'est dit : « *minute papillon, le truc ne fonctionne que si* vrai *et* démontrable *sont la même chose* ». D'où le théorème d'incomplétude. C'est comme ça que ça a dû se passer, c'est complètement évident. Ce que va —finalement— prouver Gödel, c'est que contrairement à la vérité, *la démonstrabilité ne commute pas avec la négation* : si A n'est pas démontrable, ça ne veut pas dire que $\neg A$ est démontrable. Donc il existe des propositions qui sont *indécidables.*

Voici comment Gödel fait sa diagonalisation. Énumérez tous les énoncés à une variable. (On peut énumérer tous les énoncés, qui ne sont que des suites finies de symboles pris dans un alphabet fini : l'énumération se fait comme dans le dictionnaire, à ceci près qu'on commence avec les expressions comportant un symbole, puis celles qui en ont deux, puis celles qui en ont trois. . .) On applique la diagonale de Cantor à la démonstrabilité, plus précisément à « l'énoncé numéro n appliqué à m est démontrable », ce qu'on exprime par

$$\exists p\ P[p, \ulcorner A_n[m] \urcorner]$$

Diagonalisez là-dessus. C'est-à-dire, considérez l'énoncé qui dit : l'énoncé numéro n, pris en n, n'est pas démontrable :

$$\forall p\ \neg P[p, \ulcorner A_n[n] \urcorner]$$

C'est une formule à une variable n. Elle a donc un numéro : disons que c'est la formule n^o N, c'est $A_N[n]$. Appliquez-la à $n = N$: vous obtenez la formule $A_N[N]$ (notons-la A), qui est :

$$\forall p\ \neg P[p, \ulcorner A_N[N] \urcorner]$$

Donc, A dit exactement : « je ne suis pas démontrable » ! Dès lors, les conséquences sont immédiates. Supposez que votre théorie soit cohérente, et que vous puissiez y *démontrer* cet énoncé A. Alors A serait forcément vrai, n'est-ce pas ? Car si je peux démontrer un énoncé récessif dans une théorie cohérente, il est forcément vrai ; parce que —c'est là qu'arrive l'informatique— s'il était faux, il y aurait quelque part un contre-exemple. Le contre-exemple, c'est le calcul à la main. Par exemple, le théorème de Fermat est faux pour l'exposant 2. Si vous l'aviez énoncé pour tous les entiers à partir de 2, vous auriez ce contre-exemple : $3^2 + 4^2 = 5^2$. Et cette égalité est forcément démontrable : tout ce qui est vérifiable à la main est démontrable (le calcul constitue la meilleure démonstration). Donc, si un énoncé récessif pouvait être démontré tout en étant faux, on aurait à la fois une preuve de cet énoncé et une preuve du contraire : ça ne peut pas arriver dans une théorie cohérente (c'est la définition même de la cohérence !) Donc —je reviens à mon énoncé A— si A est démontrable, il est vrai. Mais A, c'est exactement : « je ne suis pas démontrable », donc s'il est vrai, il n'est pas démontrable, puisque c'est ce qu'il dit !

Et d'ailleurs *il est forcément vrai* : parce que s'il était faux, comme c'est l'énoncé : « je ne suis pas démontrable », c'est qu'il serait démontrable —et donc il serait vrai ! Absurdité ! Il n'y a donc qu'une seule possibilité : A est vrai, mais pas démontrable ! (Évidemment c'est seulement dans une théorie cohérente que tout cela marche.)

Vous obtenez donc le premier théorème d'incomplétude : *il existe un énoncé A, qui est vrai, et qui n'est pas démontrable.* Et ce théorème réfute la première forme du programme de Hilbert, le « résultat de conservation » (selon lequel *les méthodes finitistes peuvent prouver tout ce qu'on peut prouver autrement*). Car, mine de rien, on a prouvé que A est vraie, tout en prouvant qu'elle est indémontrable *dans la théorie formelle*, qui contient les maths de papa.

Le second théorème (qui va réfuter la deuxième forme du programme de Hilbert : la preuve de la non-contradiction) consiste à formaliser le premier théorème. Formaliser, c'est extrêmement difficile à faire, c'est fastidieux. Quand j'ai écrit un gros bouquin de théorie de la démonstration [Girard, 1987b], je ne l'ai pas fait dans le détail. Pourtant ça ne présente aucune difficulté, puisqu'à partir du moment où on a quelque chose de parfaitement rigoureux —et le raisonnement qui a conduit au premier théorème l'est— ça peut toujours se formaliser : il suffit d'y mettre le prix. Donc on peut écrire formellement le premier théorème, et ça donne une démonstration (dans les maths du lycée) que la cohérence de T implique A. Comme A n'est pas démontrable, la cohérence de T ne l'est pas non plus ! C'est le deuxième théorème d'incomplétude de Gödel : la cohérence de T s'exprime par un énoncé récessif $\forall p\ \neg P(p, \ulcorner\bot\urcorner)$, qui est sans doute vrai (en tout cas on peut le montrer par des méthodes non élémentaires), mais qui n'est pas démontrable dans T. C'est la fin des illusions fondamentalistes. On ne peut faire de la fondation que sous forme de spirale, on se fonde toujours sur plus que soi, et ça c'est absolu. Pensez à Dupond et Dupont dans le désert, trouvant une piste, bientôt rejointe par une seconde piste... C'est ça les fondements ! Mais, vous savez, le fondamentalisme, c'est très dur à extirper, ça résiste ; c'est à peine croyable, j'ai toujours des discussions avec des fondamentalistes : ils veulent continuer le programme de cohérence, alors que ça a été réfuté en 1931[10] !

4 L'obstination

4.1 Gentzen

Donc on s'obstine, car les vrais croyants ne se découragent jamais. Et il y a eu un vrai croyant, particulièrement remarquable, qui est Gentzen. Encore une fois, je ne ris qu'à moitié, car Gentzen est le plus grand théoricien de la démonstration, sans aucun doute, et il s'est énormément obstiné. En 1936, il a démontré la cohérence de l'arithmétique de Peano, par récurrence transfinie jusqu'à l'ordinal ε_0. Je ne sais pas si vous savez ce que c'est que les ordinaux (ou *nombres transfinis*) : c'est quand on compte *après* les entiers. Le cœur de l'arithmétique de Peano, c'est le principe de récurrence : si une propriété P est vraie sur 0, et si sa vérité passe de n à $n+1$ (c'est-à-dire si $P[n] \Rightarrow P[n+1]$), alors elle est vraie pour tous les entiers. Mais vous pouvez vous amuser à continuer. Quand vous avez épuisé tous les entiers : $0, 1, 2, \ldots$, pour dire que vous avez terminé, vous écrivez ω : ce n'est pas le « dernier entier » (il n'y en a pas), c'est la *totalité* des entiers. Quand j'écris $0, 1, 2, \ldots, n$, j'ai tous les entiers jusqu'à n ; quand

---

[10] Note de l'auteur : je ne pouvais imaginer qu'en l'an 2000 certains collègues allaient proposer... le Programme de Hilbert —vaguement « relooké »— comme le défi logique du nouveau siècle. Comme quoi le « millenium bug » n'a pas frappé que les machines !

j'écris $0, 1, 2, \ldots, \omega$, j'ai *tous* les entiers. Et je recommence à compter : $\omega + 1, \omega + 2, \ldots$, etc. et ça donne :

$$0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega.2, \omega.2 + 1, \ldots \omega^2, \omega^2 + 1, \ldots, \nearrow \varepsilon_0$$

(ε_0, c'est $\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$: une tour de Pise à une infinité d'étages.) Il y a encore des ordinaux après ε_0 : $\varepsilon_0 + 1$, $\varepsilon_0 + 2$,...(ça ne s'arrête jamais), mais Gentzen n'en a pas besoin, alors arrêtons-nous là.

Que fait Gentzen ? Il démontre, par une récurrence jusqu'à ε_0, la validité des récurrences ordinaires (donc la cohérence de l'arithmétique de Peano). Donc ce qu'il fait n'est pas une *réduction* aux maths les plus élémentaires, et on peut poser la question : ça convainc qui ? Tous ces trucs-là, ça ne peut convaincre que les convaincus. Ce type de théorie de la démonstration, qui n'est pas sans qualités, surtout quand ça commence avec Gentzen (on va beaucoup parler de Gentzen, par la suite), a continué un temps en suivant une pente déclinante, surtout en Allemagne, avec par exemple Schütte, un épigone de Gentzen, qui a travaillé pendant les années 1950-1960... Il y a eu des théories de plus en plus monstrueuses, par la suite, mais c'est toujours le même « machin » : on fonde un truc sur un truc un peu plus gros, qui se fonde lui-même sur un truc un peu plus gros... C'est une vis sans fin dans l'abstraction, une spirale : au bout d'un moment les Dupondt en sont à leur dixième piste superposée, et il sont tout autant perdus qu'au début. De toute façon, comme disait Kreisel —paraphrasant Kant— « *les doutes quant à la cohérence sont encore plus douteux que la cohérence elle-même* ».

Un bémol, toutefois : il y a une boutade célèbre selon laquelle « Gentzen est le rigolo qui a prouvé le principe de récurrence jusqu'à ω, par une récurrence jusqu'à ε_0 »! Comme le faisait remarquer Kreisel, ce jugement cruel (d'un célèbre mathématicien français : André Weil) mérite d'être nuancé : Gentzen montre par *une seule récurrence jusqu'à* ε_0, portant sur des formules élémentaires (sans quantificateurs), la validité de toutes les récurrences ordinaires —aussi emmêlées soient-elles— et portant sur des énoncés de complexité logique arbitraire ; les quantificateurs dans les récurrences ordinaires sont remplacés par des exponentielles ordinales dans la récurrence de Gentzen ; le détour par les ordinaux transfinis permet, d'une certaine manière, d'y voir plus clair dans les situations élémentaires les plus embrouillées. Depuis Kreisel (dans les années 1950-1960) on cherche dans les démonstrations de cohérence, non un motif de *croire* en la cohérence, mais des *informations* sur la *structure logique* des théories. Et là, ça devient vraiment intéressant : à la question stérile et prétentieuse du « *pourquoi* » vient se substituer la question plus modeste mais féconde du « *comment* ».

4.2 Avatars du théorème de Gödel

Je voudrais mentionner en passant, parmi les sous-produits du théorème de Gödel, quelque chose qui n'a pas tellement de rapport avec la suite de l'exposé : le problème de la décidabilité. C'est un problème de nature algorithmique, un sous-produit technique du théorème d'incomplétude, basé sur des analogies qui sont assez exactes (pourvu qu'on se donne la peine d'écrire les choses précisément), à savoir : *prouver* c'est comme *connaître*, et ce n'est pas très loin de *calculer*. Dans la plupart des questions algorithmiques, dans la plupart des questions que vous pouvez vous poser, il s'agit de savoir si un objet vérifie ou non telle ou telle propriété ; et quand on regarde ce qu'on peut *prouver*, ou ce qu'on peut *calculer*, on obtient des limites, comme dans le théorème de Gödel, et pour la même raison : à cause de l'argument de diagonalisation.

Il y a fondamentalement trois catégories : à un bout, ce qu'on peut démontrer (les théorèmes) ; à l'autre bout, ce qu'on peut réfuter (les antithéorèmes) ; et, au milieu, un énorme trou, la catégorie la plus importante : l'indécidable.

Je sais que oui.	Je ne sais pas.	Je sais que non.

Prenez un algorithme qui répond par oui ou par non. Vous avez les cas où l'algorithme va vous dire oui, les cas où il va vous dire non, et les cas où il ne va pas répondre, où il va se planter, ou bien il va mouliner, mouliner, mouliner, ... et cette zone-là, la zone « je ne sais pas », est à peine compressible. On peut éventuellement changer d'algorithme, et améliorer certaines réponses ; la zone centrale peut être grignotée, mais pas comblée, et plus on veut grignoter plus il faut le payer cher : c'est la traduction du théorème d'incomplétude. L'exemple typique est celui des algorithmes « être prouvable », ou « être réfutable ». C'est l'exemple souche, le problème d'arrêt d'un programme.

Comment grignoter la zone centrale ? C'est simple : si la Vierge Marie vous a dit « Je sais que ce cas-là est vrai », alors vous pouvez le rajouter à l'algorithme. Au cas où c'est contrôlable, je sais que c'est vrai. On peut faire ça pour un nombre fini de cas. Mais il restera toujours une infinité de gens dans la zone centrale.

Pour faire une analogie avec les mathématiques habituelles, considérez les opérateurs non bornés dans un espace de Hilbert (ce n'est pas démesurément abstrait : on les utilise en relation avec la physique) : ils sont définis sur des parties denses ; on demande qu'ils aient un graphe fermé (comme ça, si la partie dense est tout l'espace, ils sont continus, c'est-à-dire bornés[11]). En général, ces opérateurs ne sont pas totaux : c'est-à-dire qu'on ne peut pas les prolonger continûment à tout l'espace. C'est comme ça. Eh bien ici, c'est pareil : l'algorithme associe (correctement) à certains énoncés la valeur *vrai* et à d'autres la valeur *faux* ; il se trouve qu'on ne peut pas prolonger l'algorithme, de façon à toujours donner des réponses —correctes ou non !— (l'analogue de la continuité, ici, c'est qu'un algorithme procède d'un calcul fini). *Ce n'est ni plus ni moins mystérieux que pour les opérateurs.*

On retrouve des limitations analogues (même si elles sont techniquement différentes) dans de nombreux problèmes d'algorithmique. Par exemple, le 10ème problème de Hilbert —de la fameuse liste de 1900— s'énonce : « *Étant donné une équation diophantienne —i.e., une équation* $P[x_1, \ldots, x_n] = 0$ *où* P *est un polynôme à coefficients entiers—, trouver un processus (un algorithme) permettant de déterminer en un nombre fini d'opérations si l'équation a des solutions entières.* » Tout algorithme prétendant répondre à la question sera soit incomplet (il y aura des cas où il ne saura pas trancher) soit fautif, comme l'a montré Matijasevich en 1970.[12]

Et c'est encore la même chose en intelligence artificielle : dans les années 1980, des rigolos se sont émus qu'on ne sache pas toujours répondre *oui* ou *non* à toute question ; ils se sont dit : « *quand je ne sais pas, je fais ci, je répond ça, et je vais bien finir par boucher les trous* ». Le problème c'est *qu'on ne peut pas savoir qu'on ne sait pas.* Et ils ont proposé —modestement— de « *compléter la logique* » de façon à répondre à tout coup, en contradiction complète avec le théorème de Gödel et ses corollaires. On a eu droit à tout : une « logique non monotone », une « logique des défauts », etc., toutes écloses *ex nihilo*, complètement dépourvues de notion cohérente de *preuve* (ce qui fait qu'elles méritent difficilement le nom de *logiques* !), et qui se maintiennent en vie artificiellement, du fait du nouveau scientisme ambiant, selon lequel l'ordinateur serait capable de répondre à toutes les questions...

---

[11] L'usage est de parler d'opérateurs bornés, mais bien sûr cela signifie qu'ils sont bornés *sur la boule unité.* Un opérateur (linéaire) ne peut évidemment pas être borné sur tout l'espace, donc il n'y a pas de confusion possible. (N.d.r.)

[12] Cf. la Leçon de G. Godefroy, dans ce volume, et l'exposé de J. P. Azra au Séminaire Bourbaki de novembre 1970 (exposé n^o 383). (N.d.r.)

5 Le *Hauptsatz*

5.1 Toutes les mauvaises idées ne sont pas à jeter

Après avoir dit beaucoup de mal de l'obstination, il faut quand même remarquer que toutes les mauvaises idées ne sont pas à jeter. C'est très important, en sciences, d'avoir de mauvaises idées, pourvu que les gens qui les mettent en œuvre soient bons. En particulier, cette idée de s'obstiner sur le programme de Hilbert a été extrêmement fructueuse, dès qu'on a cessé de vouloir l'appliquer à l'arithmétique et qu'on l'a transposé à la logique pure (le *calcul des prédicats*) : là, le programme marche !

C'est, en substance, ce que disent le théorème de Herbrand [Herbrand, 1930], dont je n'ai pas parlé (et je n'en parlerai plus), et celui (essentiellement équivalent) de Gentzen [Gentzen, 1969a] (dont je vais parler). Ces deux logiciens sont morts assez jeunes : Herbrand à 23 ans, en 1931, dans un accident de montagne à La Bérarde ; Gentzen à 36 ans, en 1945, à Prague (où il était *dozent* depuis 1943[13]). L'Histoire a surtout retenu le *Hauptsatz* de Gentzen, plutôt que le « théorème fondamental » d'Herbrand, mais les deux résultats pêchent dans les mêmes eaux. (Soit dit en passant, admirez l'imagination, sans doute liée à l'époque : Herbrand appelle son résultat « théorème fondamental », ce qui ne veut pas dire grand chose, et Gentzen appelle le sien « *Hauptsatz* », ce qui veut dire à peu près pareil —donc pas grand chose non plus !)

Alors qu'est-ce que Gentzen a trouvé avec son *Hauptsatz* ? C'est d'abord une formulation symétrique de la logique, qui rappelle un peu la formulation hamiltonienne de la mécanique : comme celle-ci, elle repose fondamentalement sur la recherche et l'exploitation des symétries ; elle a le même défaut : c'est une formulation tellement artificielle qu'elle est mal adaptée aux problèmes concrets, du moins pour les humains —les machines s'en accommodent beaucoup mieux. Elle a aussi la même qualité : une hauteur de vue inégalée dans les autres approches. Bref, cette formulation a été inventée plutôt pour *étudier la structure générale des preuves* que pour écrire telle ou telle preuve particulière. (Ce n'est que beaucoup plus tard qu'on s'est rendu compte que ça pouvait aussi être un outil pour la recherche ou la vérification automatique de preuves.)

Ce point de vue s'applique à la logique, et non aux mathématiques : c'est une remarque importante, parce que le théorème de Gödel, lui, s'applique aux mathématiques, c'est-à-dire à ce qu'on peut faire dès qu'on a un petit peu d'arithmétique. Il ne s'applique pas à la logique pure. L'arithmétique, c'est un système basé sur les entiers. C'est une structure un peu spécifique, avec sa récurrence. La logique, c'est vraiment ce qu'on peut faire sur les structures arbitraires, quand on ne sait rien. Le théorème de Gödel suppose un petit peu d'entiers, parce qu'il faut les entiers pour pouvoir coder la syntaxe (il faut parler d'entiers, de suites d'entiers, de démonstrations). Alors que là, on parle de la logique, on va enlever tout principe non logique, donc on n'a même pas la récurrence de l'école secondaire. On n'a que le calcul des prédicats —la logique classique : c'est comme ça qu'on appelle la logique d'autrefois ; comme toujours quand vient un hérésiarque, qui dit « non, ça ne marche pas comme ça », l'idéologie ou la science ambiante prend un adjectif ; c'est comme ça qu'on a eu l'Église catholique, et plus récemment —quand Brouwer a proposé l'intuitionnisme— la logique classique.

---

[13] Nazi de cœur, il n'avait pas voulu abandonner une « ville allemande ». Interné dans un camp par l'Armée Rouge, il fut victime de jets de pierres : la population se vengeait bien dérisoirement des horreurs de l'occupation. C'est ainsi que Gentzen est mort de faim : blessé, il ne put disputer sa pitance à ses codétenus.

5.2 Les séquents

Les séquents sont la grande invention de Gentzen. Il s'agit de suites de formules, Γ et Δ, séparées par le symbole $\vdash$:

$$\Gamma \vdash \Delta \quad \textit{(lire : « } \Gamma \textit{ thèse } \Delta \textit{ »)}$$

$A_1, \ldots, A_n \vdash B_1, \ldots, B_m$, signifie que la conjonction des A_i implique la disjonction des B_i.

Et ça reste vrai quelque soit le sens (raisonnable) qu'on donne à « implique », « conjonction », « disjonction ». Et tant mieux, parce que ce sens n'est pas clair du tout. En tout cas, ce n'est certainement pas ce que vous croyez ; mais si vous l'interprétez comme ce que vous croyez, vous ne vous tromperez pas : vous serez seulement très en deçà du sens précis qu'on peut donner à cette implication, cette conjonction, cette disjonction. Bref, pour suivre ce que je vais vous en raconter, pensez que ça veut simplement dire : « si toutes les A_i sont vraies, alors au moins une des B_i est vraie ». C'est une lecture possible, quoique très réductrice.

Il y a quelques cas particuliers : $\vdash B_1, \ldots B_m$ signifie que l'une au moins des formules $B_1, \ldots B_m$ est vraie, et cela indépendamment de toute hypothèse. Donc $\vdash A$ signifie A (« j'affirme A »). $A_1, \ldots, A_n \vdash$ signifie que sur la base des hypothèses $A_1, \ldots, A_n$ aucune possibilité ne reste ouverte, c'est-à-dire que ces hypothèses sont incompatibles. Donc $A \vdash$ signifie $\neg A$ (« A n'est pas tenable ») ; le séquent vide $\vdash$ dit que sans aucune hypothèse on a déjà une impossibilité : si ce séquent est démontrable, la théorie est nécessairement contradictoire. Le séquent $\vdash$ représente donc l'absurdité. On va voir d'ailleurs que, par transitivité —la règle de coupure, voir *infra*—, de $\vdash A$ et $A \vdash$ résulte $\vdash$, ce qui veut dire que $\vdash$ est le résultat de A et $\neg A$. Ce symbole : $\vdash$ veut dire « implique », ou du moins il est appelé à se transformer en « implique »; mais l'astuce de Gentzen, c'est de faire en sorte qu'on ne soit pas obligé d'écrire « implique » ($\Rightarrow$) quand on n'en a pas besoin trop tôt.

Gentzen a écrit des règles : le logicien normal est un bureaucrate qui passe son temps avec du papier, une règle, il trace des traits ; au-dessus de chaque trait, et en dessous, il met des formules. Quand ces formules obéissent à certaines contraintes, eh bien il est content : c'est ça le calcul des séquents. Il y a trois groupes de règles :

Le groupe identité : « A est A » et réciproquement !

$$\frac{}{A \vdash A}\ \text{(axiome d'identité)} \qquad \frac{\Gamma \vdash A, \Delta \qquad \Gamma', A \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ \text{(coupure)}$$

Le groupe « identité », dit que « A est A » et réciproquement ! En effet, la règle de gauche, qui s'appelle « l'axiome d'identité », dit que si j'ai A comme prémisse, je l'ai *de fait* comme conclusion (autrement dit, « A implique A ») ; et l'autre règle, la coupure, dit : inversement, si j'ai obtenu A en conclusion, je peux m'en servir maintenant comme prémisse. C'est absolument fondamental. Je pense connaître beaucoup de logique, mais je pense qu'on n'a pas terminé la compréhension de ça. Quand je dis : « A est A, et réciproquement », je ne me moque pas du monde, c'est très compliqué à comprendre. Je peux faire 4 heures de cours sur l'interprétation de ces deux machins-là. Par rapport à ça, le reste n'est rien du tout !

La coupure, c'est le *Modus Ponens* de nos grand-mères : si on a A, et si on a $A \Rightarrow B$, alors on a B. Il y a une autre version : si on a $A \Rightarrow B$ et $B \Rightarrow C$, alors on a $A \Rightarrow C$. Sous cette forme (en mettant juste les deux prémisses dans l'ordre inverse), on reconnaît le bon vieux syllogisme, du genre : « tous les hommes sont mortels, or Socrate est un homme, donc Socrate est mortel ».

Vous savez, il y a deux principes qu'on utilise en mathématiques : le syllogisme et la récurrence. La récurrence, c'est le principe « de $P[0]$ et de $\forall n(P[n] \Rightarrow P[n+1])$ déduire $\forall n\ P[n]$ »; ce principe peut se justifier informellement par une suite infinie de *Modus Ponens* —on démontre $P[1]$, puis $P[2]$... Mais, malheureusement, les règles de déduction sont finies et la récurrence ne fait pas partie de la logique élémentaire ; ainsi pour établir la cohérence de l'arithmétique, Gentzen sera obligé de passer à une sorte de « logique infinie », ce qui soulève de graves problèmes. Résumons-nous : en logique, il n'y a que le syllogisme. Tout le reste n'est là que parce qu'il faut bien nommer les évidences, mais fondamentalement, on ne fait que du syllogisme.

Le syllogisme n'est pas très différent du *Modus Ponens*, et il est aussi dans la coupure : la coupure contient tous les cas de transitivité de l'implication. C'est la règle fondamentale, celle qui permet d'*activer* les lemmes, qui permet d'utiliser un théorème dont on ne connaît pas la démonstration : on le trouve dans un article, l'auteur est un type sérieux, on peut lui faire confiance... Alors on le prend et on l'applique : eh bien en faisant cela on utilise la coupure ! Alors, vous voyez donc, c'est fondamental, la coupure. C'est une règle extrêmement mal nommée, parce que c'est la règle de communication, de sociabilité. Si on appelle « coupure » la règle de sociabilité, on est parti pour être un peu schizophrène. C'est d'ailleurs ce qui va arriver.

Le groupe structurel : ce qui va de soi

Voici maintenant le groupe structurel (σ désigne une permutation) :

$$\frac{\Gamma \vdash \Delta}{\sigma(\Gamma) \vdash \Delta}\ \text{(échange à gauche de } \vdash) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \sigma(\Delta)}\ \text{(échange à droite de } \vdash)$$

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{(affaiblissement à gauche de } \vdash) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ \text{(affaiblissement à droite de } \vdash)$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ \text{(contraction à gauche de } \vdash) \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ \text{(contraction à droite de } \vdash)$$

Le calcul est complètement symétrique : à toute règle à gauche du $\vdash$ correspond la règle analogue pour la droite. Ce groupe a été appelé « structurel » par Gentzen, parce qu'il va de soi. Ce sont des règles qu'il ne vaut même pas la peine de discuter (!).

L'échange à gauche dit que l'ordre des hypothèses n'a aucune importance ; l'échange à droite dit que l'ordre des conclusions n'a aucune importance. Ça va de soi.

L'affaiblissement à gauche, ça veut dire que vous pouvez ajouter des hypothèses inutiles (vous n'êtes pas obligé d'utiliser toutes les hypothèses) ; et l'affaiblissement à droite, que vous pouvez affaiblir les conclusions : qui peut le plus peut le moins ! Ça aussi, ça va de soi.

La contraction à gauche dit que si vous avez une hypothèse, c'est comme si vous l'aviez deux fois : vous pouvez l'utiliser et la réutiliser, autant de fois que vous le voulez ; et la contraction à droite, que si vous avez un éventail de choix, il suffit d'énoncer chacun d'eux une seule fois[14]. Bon, tout ça va de soi !

Et le point essentiel, c'est que ces règles réussissent à exprimer les propriétés de la conjonction et de la disjonction sans en introduire les symboles.

---

[14] En fait la contraction droite cache le *raisonnement par l'absurde*, voir *infra*.

Le groupe logique : introduction des connecteurs et des quantificateurs
Et enfin voici le groupe logique, ainsi dénommé parce qu'il dit comment introduire les connecteurs logiques $\wedge$, $\vee$, $\neg$, $\Rightarrow$, et les quantificateurs. Commençons par la conjonction $\wedge$:

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}(g\wedge \vdash) \quad \frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}(d\wedge \vdash) \qquad : \text{introduction du } \wedge \text{ à gauche de } \vdash$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'} \ (\vdash \wedge) \qquad : \text{introduction du } \wedge \text{ à droite de } \vdash.$$

Une règle binaire introduit la conjonction à droite de $\vdash$ (pour démontrer $A \wedge B$, on démontre A, et on démontre B), deux règles unaires l'introduisent à gauche. La notation entre parenthèses $(g\wedge \vdash)$, $(d\wedge \vdash)$, $(\vdash \wedge)$ est une façon condensée de nommer la règle (dans les démonstrations, il est recommandé d'indiquer à chaque étape la règle qu'on applique) ; le g dans $(g\wedge \vdash)$ signifie *gauche* : il signale que la formule A qui se trouvait au-dessus de la barre va se retrouver, après introduction du $\wedge$, à gauche du $\wedge$ (on a $A \wedge B$, et non $B \wedge A$) ; de même, dans la règle $(d\wedge \vdash)$, la formule initiale B se retrouve à droite du $\wedge$. Cette distinction évite de présupposer la commutativité du $\wedge$ —en fait, elle l'exprime. (Il existe des logiques —forcément linéaires— où $\wedge$ n'est pas commutatif, mais je n'en parlerai pas.)

Il y a un certain arbitraire dans la *présentation* des règles. Par exemple, dans le dernier séquent de la règle $\vdash \wedge$, j'aurais pu écrire le $A \wedge B$ à droite des contextes Δ, Δ', plutôt qu'à leur gauche. Bien sûr, on passe d'une présentation à l'autre par la règle d'échange, donc quand on utilise la règle $\vdash \wedge$, on ne fait pas attention à ce genre de détails : on met le $A \wedge B$ là où on veut le trouver. Voici maintenant les règles du $\vee$:

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'}(\vee \vdash) \qquad : \text{introduction du } \vee \text{ à gauche de } \vdash$$

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta}(\vdash g\vee) \quad \frac{\Gamma \vdash B, \Delta}{\Gamma \vdash A \vee B, \Delta}(\vdash d\vee) \qquad : \text{introduction du } \vee \text{ à droite de } \vdash$$

Ces règles de la disjonction sont l'image miroir de celles de la conjonction ($\vdash$ joue le rôle du miroir). La symétrie profonde qui fait passer des unes aux autres opère encore dans les règles de la négation :

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}(\neg \vdash) \quad \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}(\vdash \neg) \qquad : \text{introductions du } \neg.$$

Ces règles permettent à une formule de franchir le « *miroir* » $\vdash$; l'image miroir de A est $\neg A$, autrement dit, la négation exprime l'échange gauche/droite. J'insiste là-dessus, parce qu'en logique linéaire, ce seront ces aspects *géométriques* de la logique qui seront fondamentaux.

L'implication est régie par les règles suivantes :

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \Rightarrow B \vdash \Delta, \Delta'}(\Rightarrow\vdash) \qquad : \text{introduction du } \Rightarrow \text{ à gauche,}$$

$$\frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta}(\vdash\Rightarrow) \quad : \text{introduction du } \Rightarrow \text{ à droite.}$$

Quand on fait de la théorie de la démonstration fondamentaliste, les quantificateurs (et donc les règles qui permettent de les introduire) jouent un rôle essentiel, vu que c'est là-dessus que se posent les problèmes de cohérence. Voici les règles correspondantes :

$$\frac{\Gamma, A[t] \vdash \Delta}{\Gamma, \forall x A[x] \vdash \Delta}(\forall\vdash) \quad \frac{\Gamma \vdash A[y], \Delta}{\Gamma \vdash \forall x A[x], \Delta}(\vdash\forall) \quad : \text{introductions du } \forall.$$

$$\frac{\Gamma, A[y] \vdash \Delta}{\Gamma, \exists x A[x] \vdash \Delta}(\exists\vdash) \quad \frac{\Gamma \vdash A[t], \Delta}{\Gamma \vdash \exists x A[x], \Delta}(\vdash\exists) \quad : \text{introductions du } \exists.$$

Dans ces règles, y désigne une variable (qui n'apparaît pas dans le contexte, c'est-à-dire dans Γ et Δ), et t désigne un terme (une variable, une constante...). Dans toutes les règles logiques, la formule qui contient le connecteur ou le quantificateur introduit par la règle s'appelle la *formule principale*. Les autres formules (Γ, Γ' et Δ, Δ') forment le *contexte* : c'est une espèce de paquet, c'est livré avec les hypothèses, ou comme conclusions alternatives.

Il est à noter que le choix des règles logiques est unique à quelques variantes près (qui sont d'ailleurs équivalentes modulo les règles structurelles).

Les démonstrations

On construit les démonstrations en appliquant successivement les règles précédentes. La conclusion d'une démonstration est un séquent. Voici par exemple une démonstration, aussi courte que possible, du séquent $A \Rightarrow B, A \Rightarrow C, (B \wedge C) \Rightarrow D \vdash A \Rightarrow D$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \vdash A} \quad \dfrac{}{B \vdash B}}{A, A \Rightarrow B \vdash B}(\Rightarrow\vdash) \quad \dfrac{\dfrac{}{A \vdash A} \quad \dfrac{}{C \vdash C}}{A, A \Rightarrow C \vdash C}(\Rightarrow\vdash)}{A, A \Rightarrow B, A \Rightarrow C \vdash B \wedge C}(\vdash\wedge) \quad \dfrac{}{D \vdash D}}{A \Rightarrow B, A \Rightarrow C, (B \wedge C) \Rightarrow D, A \vdash D}(\Rightarrow\vdash)}{A \Rightarrow B, A \Rightarrow C, (B \wedge C) \Rightarrow D \vdash A \Rightarrow D}(\vdash\Rightarrow)$$

Cette démonstration est légèrement incorrecte : les règles structurelles qui font passer de
$A, A \Rightarrow B, A, A \Rightarrow C \vdash B \wedge C$ à $A, A \Rightarrow B, A \Rightarrow C \vdash B \wedge C$ et de
$A, A \Rightarrow B, A \Rightarrow C, (B \wedge C) \Rightarrow D \vdash D$ à $A \Rightarrow B, A \Rightarrow C, (B \wedge C) \Rightarrow D, A \vdash D$
n'ont pas été indiquées.

Le but ultime étant de démontrer des formules, on dira qu'une démonstration de A est une démonstration du séquent $\vdash A$. Par exemple —à partir de la démonstration précédente— on peut produire une démonstration de $((A \Rightarrow B) \wedge (A \Rightarrow C)) \Rightarrow (((B \wedge C) \Rightarrow D) \Rightarrow (A \Rightarrow D))$.

5.3 L'élimination des coupures (le *Hauptsatz*)

Le *Hauptsatz* de Gentzen dit que toute preuve peut être remplacée par une preuve sans coupure : la règle de coupure est, d'un point de vue fondamental, inutile. C'est un beau paradoxe :

la coupure (c'est-à-dire l'enchaînement, l'utilisation de lemmes) est la seule règle vraiment utile en pratique ; et c'est précisément la règle qu'on peut éliminer, et qu'on va éliminer de toutes les preuves. Et ça, c'est très surprenant. Je ne suis pas capable, et je vous mets au défi, de faire une démonstration non triviale (une vraie démonstration de mathématiques) sans utiliser cette règle : c'est vraiment impossible. Un humain n'en est pas capable (sauf bien sûr pour des tautologies d'une ligne, comme celle de l'exemple précédent).

La règle de coupure est le passage du général au particulier ; or, c'est dans les propriétés générales que se trouvent toutes les idées d'une preuve, tous les fils directeurs, tout ce qui rend la preuve compréhensible quand on la lit ; ce sont elles qui permettent de condenser les démonstrations ; les longueurs des démonstrations croissent en général plus qu'exponentiellement quand on élimine les coupures. Les seules preuves qu'on puisse comprendre (donc aussi les seules qu'on puisse trouver) font forcément intervenir des propriétés générales et, donc, utilisent la règle de coupure, car il faut bien à un moment passer du général au particulier. Et pourtant, cette règle est éliminée : *la seule règle utile est éliminée !* Cette *tension*, entre le fait d'être une règle essentielle, qui concentre l'intelligence, et en même temps une règle qu'on peut éliminer, est à la base de toute la théorie de la démonstration.

L'élimination des coupures traduit une dynamique. Il y a là toute une thématique de la théorie de la démonstration, que je vais essayer de développer par la suite, et qu'on peut orienter, soit comme on l'a trop fait, vers un fondamentalisme rétrograde (les fondements, le pourquoi du pourquoi, etc.), soit vers quelque chose de beaucoup plus excitant (la dynamique sous-jacente, le *comment* plutôt que le *pourquoi*). En particulier, les démonstrations sans coupures (ou avec peu de coupures) sont intéressantes, car elles exhibent des informations effectives, donnent des bornes explicites, etc.[15].

Dans une coupure, un A positif et un A négatif s'annihilent pour ne garder que le contexte global ; mais, du fait des symétries cachées entre règles gauches et droites, il est possible de « simplifier[16] » la situation jusqu'à disparition des coupures.

5.4 Idée de la preuve

La démonstration du théorème de Gentzen se fait par une récurrence sur la taille —i.e., le nombre de symboles logiques— des coupures, où on remplace chaque coupure sur une formule A par des coupures sur des sous-formules strictes de A (c'est-à-dire des sous-formules autres que A elle-même). Une sous-formule de A est définie de manière à peu près évidente, par récurrence sur le nombre de connecteurs et de quantificateurs : si A est de l'une des formes $B \vee C$, $B \wedge C$, une sous-formule de A est une sous-formule de B ou de C ; si A est de la forme $\neg B$, une sous-formule de A est une sous-formule de B ; si A est de la forme $\forall x\, B[x]$ ou $\exists x\, B[x]$, une sous-formule de A est une sous-formule d'une $B[t]$ où t est un *terme* (c'est-à-dire une valeur, qui peut être une autre variable, qu'on substitue à la variable x)... La récurrence de Gentzen ramène toutes les coupures à des coupures ne portant que sur des formules sans connecteur ni quantificateur, et ces coupures-là sont faciles à éliminer.

---

[15] On trouvera un exemple concret d'élimination des coupures (sur une vraie propriété mathématique, non tautologique) dans le livre [Girard, 1987b] de J.-Y. Girard, annexe 4.A, p. 237-251 : Girard part d'une preuve courte, mais ne donnant (en l'état) aucune borne effective, d'un théorème de Van der Waerden selon lequel dans toute partition finie de ℕ, l'une des parties contient des progressions arithmétiques arbitrairement longues ; et par élimination des coupures, il en fait une preuve plus longue mais donnant des bornes effectives. (N.d.r.)

[16] Au prix d'une complexification de la structure globale !

Les cas clé

Il s'agit donc de réduire la coupure à des coupures sur des sous-formules. Le cas de figure le plus simple est celui où les deux occurrences de la formule qu'on coupe sont des formules principales de règles logiques : on appelle cela les *cas clé*.

Voici un premier exemple de cas clé (introduction d'un connecteur et coupure) :

$$\dfrac{\dfrac{\Gamma \vdash A, \Delta \quad \Gamma \vdash B, \Delta}{\Gamma \vdash A \wedge B, \Delta} \qquad \dfrac{\Gamma', B \vdash \Delta'}{\Gamma', A \wedge B \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Il contient une coupure sur $A \wedge B$. On peut la remplacer par

$$\dfrac{\Gamma \vdash B, \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

qui contient une coupure sur la sous-formule B. On a bien sûr les analogues obtenus en remplaçant $A \wedge B$ par $A \vee B$ ou par $A \Rightarrow B$...

Voici un autre exemple de cas clé (introduction d'une négation et coupure) :

$$\dfrac{\dfrac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \qquad \dfrac{\Gamma' \vdash A, \Delta'}{\Gamma', \neg A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

qui contient une coupure sur $\neg A$, peut être remplacé par

$$\dfrac{\Gamma' \vdash A, \Delta' \quad \Gamma, A \vdash \Delta}{\Gamma', \Gamma \vdash \Delta', \Delta}$$

qui contient une coupure sur A, et il n'y a plus qu'à appliquer la règle de permutation (échange) pour retrouver en conclusion $\Gamma, \Gamma' \vdash \Delta, \Delta'$.

Voici enfin l'exemple d'un cas clé avec quantificateur :

$$\dfrac{\dfrac{\Gamma \vdash A[y], \Delta}{\Gamma \vdash \forall x A[x], \Delta} \qquad \dfrac{\Gamma', A[t] \vdash \Delta'}{\Gamma', \forall x A[x] \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

qui contient une coupure sur $\forall x A[x]$, peut être remplacé par

$$\dfrac{\Gamma \vdash A[t], \Delta \quad \Gamma', A[t] \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

qui contient une coupure sur $A[t]$.

N.B. t est un terme, y désigne une variable, ce qui fait que la substitution du terme t pour y dans $\Gamma \vdash A[y], \Delta$ donne $\Gamma \vdash A[t], \Delta$, i.e., n'altère pas le contexte.

La possibilité de simplifier les cas clé traduit la symétrie la plus profonde du système : elle suppose un certain équilibre entre les règles gauches et droites d'un même connecteur (ou d'un même quantificateur).

Commutations de règles
En général, il n'y a pas de raison que les occurrences de A dans une coupure soient des formules principales. Mais dans ce cas on peut toujours faire « remonter » la coupure en permutant l'ordre des règles. Par exemple, à partir de :

$$\dfrac{\dfrac{\vdash B, A}{\vdash B \vee C, A} \qquad \dfrac{A, E \vdash}{A, D \wedge E \vdash}}{D \wedge E \vdash B \vee C}$$

je peux aussi bien faire d'abord la coupure et ensuite introduire le $\wedge$ et le $\vee$:

$$\dfrac{\dfrac{\dfrac{\vdash B, A \quad A, E \vdash}{E \vdash B}}{D \wedge E \vdash B}}{D \wedge E \vdash B \vee C}$$

La commutation des règles d'introduction de $\wedge$ et de coupure modifie le contexte : c'est la *raison d'être* des contextes dans la formulation des règles. Bien sûr, j'aurais tout aussi bien pu introduire le $\vee$ avant le $\wedge$. Les deux procédures sont aussi légitimes l'une que l'autre, bien qu'elles conduisent à des preuves différentes, du point de vue du calcul des séquents. Autrement dit, le calcul des séquents n'est pas déterministe, il y a des choix arbitraires à faire. Est-ce un arbitraire profond ou n'y a-t-il là que des maladresses de formulation ? Je reviendrai sur ce point.

Cas des règles structurelles
La situation est un peu moins simple quand on coupe sur une formule qui provient d'un affaiblissement ou d'une contraction. La première idée, évidemment, est de simplifier une telle coupure par un effacement ou une duplication. Par exemple,

$$\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\Gamma' \vdash \Delta'}{\Gamma', A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

peut être remplacé par des affaiblissements itérés de $\Gamma' \vdash \Delta'$ (d'abord en $\Gamma, \Gamma' \vdash \Delta'$ puis en $\Gamma, \Gamma' \vdash \Delta, \Delta'$, et avec bien sûr les permutations nécessaires), qui font disparaître la coupure. De même :

$$\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\Gamma', A, A \vdash \Delta'}{\Gamma', A \vdash \Delta'}}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

peut être remplacé par deux coupures successives

$$\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\Gamma \vdash \Delta, A \quad \Gamma', A, A \vdash \Delta'}{\Gamma, \Gamma', A \vdash \Delta'}}{\Gamma, \Gamma, \Gamma' \vdash \Delta, \Delta'}$$

suivies de contractions pour obtenir $\Gamma, \Gamma' \vdash \Delta, \Delta'$. La première coupure a eu lieu avant la contraction. On peut ainsi faire remonter la coupure jusqu'à retomber dans les cas clé. Mais, dans ce processus, la contraction induit une duplication du morceau se terminant avec $\Gamma \vdash \Delta, A$. Ce qui fait que la procédure ne converge pas si les deux occurrences de A sont obtenues par des contractions, chacune induisant une duplication de l'autre ! Il y a plusieurs façons de s'en sortir. On peut utiliser la technique dite des « coupures croisées » de Gentzen, dont je ne parlerai pas ici —c'est trop technique ; ça marche, mais l'algorithme d'élimination des coupures est tellement compliqué... que personne ne l'a jamais vraiment compris, voir aussi 11.3 !

Une autre possibilité est de modifier les règles du calcul des séquents, en imposant des restrictions qui empêchent cette situation de se produire. Ce sera le cas, par exemple, en logique intuitionniste où, comme on le verra, il n'y a pas de règles structurelles droites. Ce sera le cas aussi, de façon plus élégante (car la symétrie gauche/droite n'y sera pas brisée) en logique linéaire.

L'algorithme
En combinant les cas précédents et en itérant adéquatement, les coupures finissent par disparaître. Mais, ce faisant, la taille des démonstrations a tendance à augmenter, à cause de la contraction. C'est une algorithmique absolument non triviale :

- La complexité de l'algorithme —dans le cas étudié ici— est énorme : le temps de calcul est une tour d'exponentielles, dont la hauteur dépend de la « taille » —i.e., le nombre de symboles— de la coupure à éliminer.
- De plus c'est un algorithme universel, dans un sens à préciser.

6 Corollaires du *Hauptsatz*

6.1 La cohérence de l'arithmétique de Peano

Rappelons-nous que le séquent vide $\vdash$ représente l'absurdité. Or il est facile de voir que la seule règle pouvant mener à ce séquent est la coupure ; en l'absence de coupure pas de séquent vide ! Le *Hauptsatz* implique donc la cohérence.

On applique cela à l'arithmétique ; il faut bien sûr étendre l'élimination des coupures pour tenir compte de l'induction, par exemple en introduisant une espèce de calcul des prédicats infinis. Tout fonctionne de la même façon, à ce détail près que l'algorithme d'élimination des coupures devient d'une telle complexité que sa *convergence* nécessite une induction transfinie —jusqu'à ce fameux ordinal ε_0. C'était prévisible du fait du second théorème d'incomplétude et les arguties de certains rescapés du jurassique ne convaincront jamais personne : le résultat de Gentzen ne fonde pas plus l'arithmétique que la piste suivie par les Dupondt dans le désert ne mène à la ville...

Gentzen considérait son travail de 1934 (l'introduction du calcul des séquents) comme une simple préparation à son travail de 1936 – 1938 [Gentzen, 1969c, Gentzen, 1969b] (sa preuve de la cohérence de l'arithmétique), alors que maintenant on se fiche un peu du résultat de 1936, et que celui de 1934, pour nous, est beaucoup plus intéressant. Alors que la tradition fondamentaliste ne s'intéresse qu'à l'étude en force —démontrer la convergence de l'algorithme de Gentzen pour des systèmes comme l'arithmétique— (une étude en force bloquée par le théorème d'incomplétude), il est possible de travailler aussi en finesse... Et là, ça devient beaucoup plus excitant !

6.2 La propriété de la sous-formule, et la programmation logique

Regardez n'importe quelle règle : ce qu'il y a au-dessus d'un séquent, c'est toujours des sous-formules, c'est toujours des choses plus simples. Par exemple, ici :

$$\frac{\Gamma \vdash A, \Delta}{\Gamma \vdash A \vee B, \Delta},$$

au-dessus de $A \vee B$, vous avez A : il y a un connecteur de moins, c'est plus simple. Dans les règles d'introduction des quantificateurs, vous avez par exemple $\forall x\ A[x]$ dans la conclusion et $A[t]$ dans la prémisse : là encore, c'est plus simple, du moins si on néglige la taille du terme t. Et dans le cas d'une règle structurelle, la conclusion est obtenue à partir de la prémisse au moyen d'une permutation, d'un effacement ou d'une duplication, donc les formules sont les mêmes.

En fait, la seule règle qui ne marche pas « à la sous-formule », c'est la coupure —puisque la formule de coupure disparaît. Elle seule fait que la démonstration contient en général des formules plus complexes que celles qui interviennent dans la conclusion. Et c'est là qu'est toute la difficulté des mathématiques : pour démontrer un énoncé simple, le plus court chemin, et en fait tous les chemins compréhensibles, passent par des idées générales et pas forcément prévisibles. Mais le *Hauptsatz* nous apprend que si on a une démonstration de $\Gamma \vdash \Delta$, il en existe aussi une démonstration sans coupures, et donc, *pour démontrer* $\Gamma \vdash \Delta$*, on peut se restreindre aux sous-formules des formules de* Γ *et* Δ : c'est ce qu'on appelle la « *propriété de la sous-formule* ».

Vous voyez, on passe très près d'un *algorithme de décision* : il s'en faut d'un cheveu que la recherche de démonstration ne soit décidable. Car une (éventuelle) démonstration de $\vdash A$ se trouve forcément parmi les sous-formules de A : l'espace de recherche devient ainsi tout petit, presque fini. Sans le *Hauptsatz*, on serait obligé de chercher parmi les démonstrations avec coupure, les démonstrations « réelles », où le théorème A est l'aboutissement d'un enchaînement de lemmes assemblés par le *Modus Ponens*; et ces lemmes (qui contiennent les idées) sont imprévisibles : si je vous donne la conclusion d'une coupure, vous n'avez aucun moyen de retrouver la formule qu'on a coupée.

Ce « presqu'algorithme » de décision a des applications pratiques : il permet d'envisager la démonstration automatique. *Par principe*, ça ne convergera pas à tous les coups, sinon on pourrait *décider* la prouvabilité, ce qu'interdisent le théorème de Gödel et ses corollaires. Mais, *en pratique*, ça peut s'avérer efficace. C'est ce qui s'est produit avec une activité dont il faut malheureusement parler au passé : la *programmation logique* —qu'on peut résumer par le slogan : « Vous posez le problème logiquement, et `PROLOG` fera le reste ». Une fois le problème converti en formule logique, il n'y avait plus qu'à tenter de le démontrer automatiquement —ce qui est plausible grâce à la propriété de la sous-formule; de plus l'aspect logique garantit contre toute erreur. Une bonne idée, donc, mais qui avait trois défauts. Premièrement, comme je viens de le dire, l'algorithme ne peut pas toujours converger. Deuxièmement, et c'est beaucoup plus grave, on a voulu vendre cette idée comme une panacée, alors qu'évidemment, les véhicules tous terrains, c'est commode, mais ça ne va très vite nulle part : un algorithme générique, universel, ne vaudra jamais un algorithme spécialisé, basé sur une idée spécifique. (Cela dit, il y a quand même des situations où les algorithmes génériques sont les meilleurs; il aurait fallu confiner `PROLOG` à des problèmes de type « exploration », et il aurait pu être vendu pour gérer de grosses bases de données, par exemple des fichiers de police...) Troisièmement, on a voulu mettre des moustaches à la logique, en ajoutant des *instructions de contrôle* —soi-disant pour améliorer la rapidité— permettant au programmeur d'utiliser son astuce... et on n'a plus rien « contrôlé » du tout : le « machin » faisait exactement le contraire de ce qu'il était supposé faire. En tout cas, il est intéressant de se rappeler que tout ce qu'il y avait de bon dans `PROLOG` (c'est-à-dire sa partie logique) nous vient du résultat de Gentzen : c'est la recherche d'une démonstration sans coupures (la « méthode de résolution » sur laquelle est basé `PROLOG` est une variante du *Hauptsatz*).

6.3 La contraction coupable !

Au fait, comment le rate-t-on, cet algorithme de décision ? Eh bien ça se passe au niveau de la règle de contraction, qui était déjà responsable de la complexité du *Hauptsatz.* Je vous ai déjà fait remarquer que dans toutes les règles (je ne parle pas de la coupure, puisqu'on l'a éliminée), ce que vous avez au-dessus de la barre est toujours plus simple qu'en dessous (*c'est* la propriété de la sous-formule). S'il n'y avait pas la règle de contraction, on pourrait trouver une grandeur qui *diminuerait toujours* dans la recherche d'une démonstration. Mais avec la règle de contraction, ça ne diminue pas. Dans :

$$\frac{\vdash A, A}{\vdash A} \tag{1}$$

en bas, vous avez un A, en haut vous en avez deux : ça double l'espace de recherche. S'il y a des quantificateurs, ça devient impossible à borner. Car, par exemple, en faisant autant de copies que vous voulez de $\forall x\, A[x]$, et en substituant dans chaque occurrence de A une valeur différente pour x, vous pouvez obtenir $A[1]$, $A[2]$, etc. Ça vous donne, potentiellement, une infinité de formules, qui vont apparaître au gré des contractions : la contraction, en fait, c'est l'infini ![17]

La règle de contraction est pourtant bien utile. Elle intervient par exemple dans la preuve de la formule $A \vee \neg A$ (propriété du « tiers exclu ») :

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \vdash A}}{\vdash \neg A, A}\ \vdash \neg}{\vdash \neg A, A \vee \neg A}\ \vdash g\vee}{\vdash A \vee \neg A, A \vee \neg A}\ \vdash d\vee}{\vdash A \vee \neg A}\ (\text{contr.}) \tag{2}$$

Si on abandonne la règle de contraction pour supprimer les problèmes qu'elle crée, on risque de perdre le tiers exclu (du moins, sous cette forme classique). Et c'est ce qui va arriver dans un premier temps, avec la logique intuitionniste. Plus tard, la logique linéaire évitera la contraction tout en restaurant le tiers exclu (cf. p. 32).

7 La logique intuitionniste

7.1 Don Camillo contre Peppone

En face du scientisme formaliste d'un Hilbert, on trouve très tôt des positions « intuitionnistes », pensons à Poincaré (*Science et Méthode*, 1908). Mais c'est Brouwer[18] qui devait

---

[17] En l'absence de contraction, la recherche devient décidable, quantificateurs ou pas.

[18] *Sur les fondements des mathématiques* [Brouwer, 1907] ; *le caractère incertain des principes de la logique* [Brouwer, 1908]. (N.d.r.)

—au nom d'un idéalisme touchant parfois au mysticisme de bazar— attacher son nom à cette expression. Brouwer contre Hilbert, Don Camillo contre Peppone…

Pour Hilbert, l'intuition du mathématicien lui sert uniquement à gagner un peu de temps par rapport à une manipulation aveugle des symboles —c'est une sorte de court-circuit : une fois la route tracée, un robot peut la suivre pas à pas, mécaniquement, en comblant tous les fossés que l'intuition avait sautés —sans coupures, dirait Gentzen. La vraie réalité mathématique, c'est le formalisme, et son seul critère, la *non-contradiction*.

Brouwer met au contraire l'intuition au centre de l'activité du mathématicien —du « *creative subject* ». Du coup, « l'existence » et « la vérité » sont bien autre chose que la non-contradiction : une théorie inexacte, dirait Brouwer, même si elle est exempte de contradiction, n'en est pas moins inexacte —de même qu'un voleur qui ne se fait pas prendre n'en est pas moins un voleur. La vérité mathématique, comme l'éthique, est *indéfinissable*, mais nous en avons tous *l'expérience intérieure*. Rien à voir, donc, avec d'arbitraires « règles du jeu », qu'on peut énoncer en quelques mots. Une preuve de non-contradiction est alors doublement inutile : parce qu'elle ne prouve pas l'existence ou la vérité, qui est la seule vraie question, et parce que de toute façon ce qui est intuitivement vrai est évidemment non contradictoire : ça va de soi.

L'ontologie hilbertienne est très mesquine, mais en contrepartie, elle donne un statut à toutes les mathématiques : celui d'une *façon de parler*. Une fois le programme réalisé, on ne court pas plus de risque avec les méthodes non élémentaires qu'avec les méthodes élémentaires. Pour comprendre : l'Axiome de Zermelo —l'Axiome du Choix— qui permet de construire des ensembles de réels non mesurables… a toujours été considéré comme douteux par de nombreux mathématiciens. Or, en 1938, Gödel a démontré[19] qu'on pouvait l'éliminer des démonstrations de propriétés suffisamment élémentaires : c'est tout bonus, d'une part on peut s'en servir, d'autre part il est inoffensif. Ce résultat —tout à fait dans l'esprit du programme de Hilbert— nous permet de soutenir que l'Axiome du Choix est complètement faux… tout en en libéralisant l'usage.

Pour Brouwer, les objets mathématiques sont des *constructions mentales*, forgées *dans* et *par* mon intuition, en suivant des lois « *évidentes* » et « *naturelles* ». Il donne ainsi un sens à une grande partie des mathématiques, en évitant l'hypocrisie : cette histoire de *façon de parler*, c'est quoi ? Si quelque chose est utile, il a forcément un statut… Brouwer s'attache donc à donner un statut —dont on peut dire qu'il est hautement non trivial— aux *artefacts* mathématiques. Il n'a pas toujours eu la main heureuse, sa refondation de l'analyse —qui élimine les fonctions non continues, mais pas la courbe de Peano— n'intéresse plus guère que les historiens[20] ; par contre son explication des opérations logiques tient toujours la route. *Grosso modo* il insiste sur l'effectivité.

Par exemple, la logique classique —et donc Hilbert, à titre de *façon de parler*— admet des paradoxes du genre (étant donné une propriété arithmétique $P[n]$) « il existe un entier N tel que si $P[n]$ est vraie pour tout $n \leq N$, alors elle est vraie pour tout entier n » : il suffit de prendre pour N une exception à P s'il y en a une, n'importe quoi sinon[21]. Pour Brouwer, c'est de la poudre de perlimpinpin : ce « théorème » ne donne aucune information effective ; d'ailleurs, j'ai pu l'énoncer (et le prouver) sans rien savoir de P. Brouwer demande à une démonstration digne

---

[19] Résultats complétés par ceux de Cohen en 1963.

[20] Le débat de l'époque était tout sauf courtois : en 1928, Hilbert expulse Brouwer des *Mathematische Annalen* ; marginalisé, Brouwer ne devait plus jamais retrouver la même « pêche ».

[21] Cet exemple ne doit pas nous faire sourire : les grands théorèmes de théorie des nombres —par exemple celui de Siegel sur $L(1,\chi)$— utilisent ce type de principe ; ce n'est pas ce qu'il y a de plus malin dans la preuve, mais c'est ça qui la rend non effective.

de ce nom de *montrer* l'objet dont elle entend prouver l'existence. Ce qui l'amène à rejeter la règle du tiers exclu $A \vee \neg A$ —qui est la clé de la « non-construction » précédente[22]. Vous me dites qu'un tel entier N existe, combien vaut-il donc ? Silence embarrassé...

7.2 Le *Hauptsatz* et la propriété de la disjonction

Malgré l'allergie de Brouwer au formalisme, l'intuitionnisme a donné lieu a une formalisation —due à son élève Heyting. Mieux, la logique intuitionniste apparaît comme une restriction simple et naturelle du calcul des séquents : la restriction à des séquents de la forme $\Gamma \vdash A$, i.e., avec exactement une formule à droite, les règles restant les mêmes. Observons que les règles structurelles droites disparaissent (en effet aucune ne fait sens quand premisse et conclusion ont une seule formule à droite) ; la négation devient impraticable ; qu'à cela ne tienne, on *définit* $\neg A$ comme $A \Rightarrow \mathtt{f}$, où $\mathtt{f}$ est une constante pour l'absurdité. Pour des raisons presque évidentes, le *Hauptsatz* persiste pour ce système restreint. Mais il a des conséquences beaucoup plus spectaculaires...

Supposons que la formule $A \vee B$ soit démontrable, i.e., que $\vdash A \vee B$ soit démontrable. On peut supposer la démonstration sans coupures et chercher sa dernière règle ; il se trouve qu'on n'a le choix qu'entre ($\vdash g\vee$) et ($\vdash d\vee$)... ce qui veut dire qu'une démonstration de $A \vee B$ sans coupures contient une démonstration de A ou une démonstration de B. C'est la *propriété de la disjonction* : *si le séquent* $\vdash A \vee B$ *est démontrable, l'un des séquents* $\vdash A$, $\vdash B$ *l'est.*

Ce n'était pas le cas dans le calcul des séquents classique, où la dernière règle était presque toujours une *contraction*, voir l'exemple (2), p. 23 : la clé de la *propriété de la disjonction* est l'absence de règles structurelles à droite du $\vdash$. Et si ces règles sont absentes, c'est pour la raison contingente qu'on ne veut qu'une formule à droite : la symétrie est explicitement *brisée*. Mais essayons de passer outre : si A est à droite —dans cette zone politiquement correcte où les règles structurelles sont interdites— on peut le faire transiter à gauche : il devient $\neg A = (A \Rightarrow \mathtt{f})$ (règle ($\Rightarrow\vdash$)) ; là on peut librement appliquer les règles structurelles, essentiellement des contractions sur $\neg A$... Finalement, au moyen d'une règle ($\vdash\Rightarrow$), A peut réintégrer la zone droite. Mais en fait il s'appelle maintenant $\neg\neg A$, et le préfixe $\neg\neg$ trahit son escapade ! Ce qui nous amène aux réflexions suivantes :

- Un préjugé vulgaire voudrait que la logique intuitionniste soit « plus faible » que la logique classique. C'est faux, puisqu'en saturant les énoncés de doubles négations, on obtient une simulation de la logique classique.
- Ce passage de A (déguisé en $\neg A$) sur la gauche, c'est la contraposition (raisonnement par l'absurde). En logique classique, quand on a obtenu une contradiction sous l'hypothèse $\neg A$ (en général utilisée plusieurs fois grâce à la contraction), on déduit A. Ici, on n'a que $\neg\neg A$. La logique intuitionniste refuse le raisonnement par l'absurde, i.e., l'involutivité de la négation, tout simplement parce que les zones droite et gauche ont des gestions différentes, donc la négation, qui correspond à la traversée du miroir, ne peut pas être involutive[23].
- Pourquoi donc brider la déduction, en se refusant le raisonnement par l'absurde ? Tout simplement parce qu'en compensation on obtient la propriété de la disjonction qui est fausse en logique classique (elle démontre $A \vee \neg A$ sans aucune hypothèse sur A). Ce qui est sûr, c'est que plus un formalisme est laxiste, plus il est facile à utiliser et moins il a de

---

[22] Ou du raisonnement par l'absurde $\neg\neg A \Rightarrow A$ qui produit le même effet.

[23] On voit aussi que le raisonnement par l'absurde n'est rien d'autre que la contraction à droite.

bonnes propriétés... et réciproquement plus un formalisme a de bonnes propriétés plus son utilisation est délicate... Mais on ne peut pas avoir le beurre et l'argent du beurre !

- Toutes ces remarques s'appliqueront à la logique linéaire ; *mutatis mutandis* puisque la négation linéaire sera involutive.

7.3 La lecture moderne de l'intuitionnisme

Tout comme le formalisme a ses dinosaures fondamentalistes, il y a de nombreuses sectes constructivistes qui réclament l'exclusivité de l'héritage de Brouwer. Laissons ces braves gens à leurs scissions, et relisons l'intuitionnisme hors de toute idéologie.

La propriété de la disjonction me dit « une démonstration de $A \vee B$, c'est une démonstration de A ou une démonstration de B. ». Levons quelques ambiguïtés de ce slogan ressassé :

- D'abord, à moins d'être masochiste —ou tenu par le secret défense—, personne n'énonce $A \vee B$ s'il a démontré B, c'est évident[24]. Pour être correct, il faut se restreindre à des démonstrations sans coupures qui sont, nous l'avons vu, des vues de l'esprit ou des créations des machines : c'est seulement après élimination des coupures qu'une démonstration d'une disjonction devient démonstration d'un des membres. Il faut donc rajouter « c'est *implicitement...* ».
- La démonstration d'une disjonction $A \vee B$ peut donc représenter —entre autres— un booléen, `vrai` ou `faux`, suivant qu'elle contient (après élimination des coupures) une démonstration de A ou une démonstration de B. Pour revenir sur le point précédent, un booléen qu'on calcule, ce n'est jamais `vrai` ou `faux`, c'est un problème dont la réponse est `oui` ou `non`, et dont on obtient la réponse en exécutant un algorithme.
- Quel algorithme ? Typiquement l'élimination des coupures. Par exemple, j'ai une démonstration que tout entier est pair ou impair $n \in \mathbb{N} \vdash P[n] \vee I[n]$; en coupant avec une démonstration de $\vdash 37 \in N$, j'obtiens $\vdash P[37] \vee I[37]$, qui, après élimination des coupures se révèle comme venant d'une démonstration de $\vdash I[37]$. La propriété de la disjonction (et plus généralement la propriété d'existence) cache donc une algorithmique qui pourrait bien être universelle.
- Pour des raisons de bon goût mathématique, on est amené à faire $A = B$ dans le cas précédent. Ça continue à fonctionner, car une démonstration de $A \vee A$ continue à représenter —implicitement— un booléen : bien sûr il ne s'agit plus de distinguer entre une démonstration de A et... une démonstration de A, mais entre les dernières règles $(\vdash g\vee)$ et $(\vdash d\vee)$. « Implicitement » —qui réfère à l'élimination des coupures— suppose que le *bit* $(\vdash g\vee)/(\vdash d\vee)$ ne varie pas arbitrairement au gré des commutations de règles.

8 L'interprétation fonctionnelle

8.1 La sémantique des preuves

Si on donne le premier rôle aux preuves, aux constructions, plutôt qu'aux formules elles-mêmes, une formule n'est plus qu'une étiquette qu'on appose sur ses démonstrations pour spécifier qu'elles démontrent la même chose. Autrement dit, une formule *s'identifie* à l'ensemble de ses preuves. C'est le principe de la *sémantique des preuves*, proposée par Heyting —et

---

[24] C'est un peu moins net pour la propriété jumelle d'*existence* : je peux par exemple énoncer $\exists n\ A[n]$ sans éprouver le besoin de donner mon témoin $A[N]$, par exemple parce que N peut être difficile à décrire !

indépendamment par Kolmogorov— dans les années 1930. Essayons de préciser ce qu'est une « preuve »[25] :

Pour une formule « atomique », c'est-à-dire sans connecteur ni quantificateur, il n'y a pas d'ambiguïté : une preuve, c'est une vérification à la main, par exemple le calcul qui établit que $27 \times 37 = 999$.

Une preuve de $A \wedge B$ est la donnée simultanée, sous forme d'un couple (π, π'), d'une preuve π de A et d'une preuve π' de B ; si on identifie une formule à l'ensemble de ses démonstrations, $A \wedge B$ correspond donc au *produit cartésien* $A \times B$.

Une preuve de $A \vee B$ est, comme on l'a dit, une preuve de A ou une preuve de B, avec une étiquette qui précise si elle prouve A ou B ; autrement dit, c'est un couple (i, π), avec $i = 0$ et π une preuve de A, ou $i = 1$ et π une preuve de B. $A \vee B$ correspond donc à la *somme disjointe* $A \oplus B$. Cette explication n'est convaincante que si « preuve » veut dire « preuve explicite », i.e., « sans coupures ».

Une preuve de $\forall x\ A[x]$ est une fonction Φ qui à tout point a du domaine de définition de A associe une preuve $\Phi(a)$ de la proposition $A[a]$. Une preuve de $\exists x A[x]$ est une paire (a, π), où a est un point du domaine de définition de A, et π une preuve de la proposition $A[a]$.

Une démonstration de $A \Rightarrow B$[26] est une fonction (calculable) Φ qui à une preuve π de A associe une preuve $\Phi(\pi)$ de B. En effet, étant donné une (vraie) preuve de $A \Rightarrow B$, le *Modus Ponens* —la coupure— permet de transformer toute preuve de A en une preuve de B ; en fait comme on essaye —nous venons de le voir— d'interpréter les démonstrations sans coupures, encore faut-il éliminer cette coupure. Par exemple, l'axiome d'identité $A \Rightarrow A$ induit la fonction identique de A dans A.

Cette interprétation est largement fautive, car il y a beaucoup plus de « preuves » au sens de Heyting que de « vraies » preuves sans coupures ; cela est dû principalement à l'interprétation de l'implication : la plupart des fonctions de A dans B —calculables ou non— ne correspondent en aucune façon à une espèce de démonstration. Cela dit, bien que laxiste, i.e., non fidèle, cette interprétation reste correcte. Il est vrai que les démonstrations de $A \Rightarrow B$ sont *des* fonctions de A dans B, que la coupure correspond à l'application, et plus généralement à la composition des fonctions. C'est ce qui va permettre l'interprétation fonctionnelle.

8.2 Le λ-calcul typé et l'isomorphisme de Curry-Howard

Au même moment (début des années 1930), Church avait l'idée hautement saugrenue de construire une théorie *naïve* des fonctions : le « λ-calcul »[27]. On allait bien sûr retrouver les problèmes de la théorie naïve des ensembles : il suffit de remplacer les ensembles par leurs fonctions caractéristiques ! De fait, le paradoxe de Russell —qui est essentiellement la construction d'un point fixe pour la négation— se transpose sans problème au λ-calcul et fournit un point fixe pour toute fonction (c'est le $n$ième avatar de l'argument diagonal de Cantor). Mais on n'obtient pas de contradiction : dans un cas « délicat » comme $a = a(a) = (a(a))(a(a)) = \ldots$, l'égalité n'est que le signe d'un calcul *divergent*, et en fait on peut voir l'objet a comme non-défini. En fait le λ-calcul est une théorie simple et souple des algorithmes partiels.

---

[25] Il ne faut pas donner à cette expression son sens formel usuel.

[26] La négation $\neg A$ est traitée comme $A \Rightarrow \mathtt{f}$, où $\mathtt{f}$ est une proposition sans preuve possible —bref : $\mathtt{f} = \emptyset$.

[27] Le nom provient d'une notation : si $(x, y) \mapsto f(x, y)$ est une fonction, on note $\lambda x \cdot f(x, y)$ la fonction $g(y) : x \mapsto f(x, y)$. λ se manipule avec les précautions en usage pour les quantificateurs ; ainsi la variable x est-elle « muette » dans $\lambda x \cdot f(x, y)$. (N.d.r.)

La notion de « *type* » fut inventée par Russell[28] pour sortir la théorie naïve des ensembles de ses contradictions : Russell partait d'objets de « type » 0, considérés comme des données naturelles ; les ensembles d'objets de « type » 0 ou, ce qui revient au même, les propriétés de ces objets, sont de « type » 1, et ainsi de suite. Avec cette hiérarchisation des objets mathématiques, le paradoxe de Russell disparaît : l'axiome de compréhension permet seulement de définir l'ensemble des *a de type n* qui vérifient une certaine propriété, et cet ensemble étant de type $n+1$, le cercle est brisé. La solution de Russell n'a pas été retenue (c'est Zermelo qui a eu le dernier mot), mais elle constitue le second ingrédient d'une formalisation de l'approche de Heyting : si l'on injecte le typage dans le λ-calcul, on élimine —non pas la contradiction, il n'y en a pas—, mais la non-terminaison.

C'est ainsi qu'apparaît le λ-calcul « typé ». On part des types atomiques puis, si A et B sont des types, $A \times B$ et $A \to B$ $(= B^A)$ sont des types. L'implication entre deux types de données $A \Rightarrow B$ est le type des algorithmes totaux envoyant des entrées A sur des sorties B. Les formules logiques jouent bien le rôle de spécifications : quel type de donnée est accepté, qu'en advient-il ? Les types garantissent l'absence de boucle, donc la terminaison. À remarquer que les « types de données », e.g., les booléens, les entiers, les listes, les arbres finis, etc. correspondent à des types, du moins dans la version du second ordre du λ-calcul typé, le *système* $\mathbb{F}$ dont nous ne parlerons pas, voir par exemple [Girard et al., 1990].

L'*isomorphisme de Curry-Howard* traduit les preuves dans un λ-calcul typé. Une formule A devient un type, et une preuve de $\vdash A$ devient un terme clos —i.e., sans variable libre— du λ-calcul typé, de type A. Plus généralement, une démonstration de $\Gamma \vdash A$ devient un terme de type A contenant des variables (libres) dont les types sont dans Γ. Pour comprendre : l'axiome d'identité $A \vdash A$ est le terme x de type A (qui contient la variable libre x du même type), alors que la démonstration de $\vdash A \Rightarrow A$ qu'on en déduit est le terme clos $\lambda x.x$ de type $A \Rightarrow A$. Bien que nous n'ayons pas vraiment introduit de formalisme, donnons l'interprétation fonctionnelle du fragment $\wedge, \Rightarrow$ du calcul des séquents, elle se comprend facilement ; comme d'habitude le crochet $t[x]$ signifie que la variable libre x est susceptible d'apparaître dans le terme t ; y_1, y_2 sont les deux projections d'une paire ordonnée y (et donc $y = (y_1, y_2)$) :

$$\frac{}{x \mapsto x}\ \text{(identité)} \qquad \frac{\vec{x} \mapsto f[\vec{x}] \qquad \vec{x'}, y \mapsto g[\vec{x'}, y]}{\vec{x}, \vec{x'} \mapsto g\big[\vec{x'}, f[\vec{x}]\big]}\ \text{(coupure : substitution)} \tag{3}$$

$$\frac{\vec{x} \mapsto f[\vec{x}]}{\vec{y} \mapsto f\big[\sigma[\vec{y}]\big]}\ \text{(échange)} \qquad \frac{\vec{x} \mapsto f[\vec{x}]}{\vec{x}, y \mapsto f[\vec{x}]}\ \text{(affaiblissement : dépendance fictive)} \tag{4}$$

$$\frac{\vec{x}, y, z \mapsto f[\vec{x}, y, z]}{\vec{x}, y \mapsto f[\vec{x}, y, y]}\ \text{(contraction : identification)} \qquad \frac{\vec{x} \mapsto f[\vec{x}] \quad \vec{x} \mapsto g[\vec{x}]}{\vec{x} \mapsto \big(f[\vec{x}], g[\vec{x}]\big)}\ (\vdash \wedge\ \text{ : paire}) \tag{5}$$

$$\frac{\vec{x}, y \mapsto f[\vec{x}, y]}{\vec{x}, y \mapsto f[\vec{x}, y_1]}\ (g\wedge \vdash\ \text{ : projection gauche}) \qquad \frac{\vec{x}, y \mapsto f[\vec{x}, y]}{\vec{x}, y \mapsto f[\vec{x}, y_2]}\ (d\wedge \vdash\ \text{ : projection droite}) \tag{6}$$

$$\frac{\vec{x} \mapsto f[\vec{x}] \qquad \vec{x'}, y \mapsto g[\vec{x'}, y]}{\vec{x}, \vec{x'}, \psi \mapsto g\Big[\vec{x'}, \psi\big(f[\vec{x}]\big)\Big]}\ (\Rightarrow\vdash\ \text{ : application}) \qquad \frac{\vec{x}, y \mapsto f[\vec{x}, y]}{\vec{x} \mapsto \lambda y \cdot f[\vec{x}, y]}\ (\vdash\Rightarrow\ \text{ : }\lambda\text{-abstraction})$$

---

[28] Voir [Russell, 1908], [Whitehead and Russell, 1910]. (N.d.r.)

8.3 Le paradigme de programmation fonctionnelle

On aboutit au paradigme de *programmation fonctionnelle* : les coupures sont codées par la *composition* des fonctions, l'exécution (l'élimination des coupures) c'est *l'évaluation* des fonctions.

Le paradigme de programmation fonctionnelle contraste avec le paradigme dominant de programmation *impérative* qui utilise des instructions comme `del` (ou `rm`) indiquant les actes à effectuer (ici, effacer un registre)... Il diffère aussi de la *programmation logique*, où on cherche des preuves sans coupures pour que l'espace de recherche soit raisonnablement limité, alors que dans la *programmation fonctionnelle*, on part d'une preuve (avec des coupures) considérée comme un programme qui s'exécuterait par élimination des coupures : dans le premier cas, le *Hauptsatz* garantit qu'on ne perd rien en limitant l'espace de recherche, dans le second cas il garantit que le programme s'arrêtera. Il s'agit là de deux postérités bien distinctes du *Hauptsatz*[29].

La programmation fonctionnelle est mise en application dans des sytèmes comme `Automath` et dans le « calcul des constructions » de Coquand [Coquand and Huet, 1988] : on démontre *l'existence* d'une solution à un problème, et on transforme la démonstration en algorithme de calcul, qui va nous *fournir* une solution (voire toutes). Par exemple, soit $\mathbb{P}$ l'ensemble des nombres premiers ; considérons l'énoncé général et, classiquement, tautologique :
$\forall n\, n \in \mathbb{P} \vee \exists m(m \notin \{1, n\} \wedge m|n)$. ($m|n$ signifie que m divise n.) Par coupure on en tire l'énoncé particulier : $N_0 \in \mathbb{P} \vee \exists m(m \notin \{1, N_0\} \wedge m|N_0)$. N_0 est l'entrée. L'élimination des coupures conduit à l'énoncé : $N_0 \in \mathbb{P}$ ou bien fournit un diviseur m de N_0.

L'avantage de cette méthode est évidemment qu'elle produit des programmes *prouvés corrects*, puisque issus de démonstrations mathématiques ! Mais sa mise en œuvre, quand elle est possible, est délicate ; ainsi, les programmes obtenus sont rarement efficaces : si je démontre la connexité de la France continentale par le fait qu'elle est étoilée par rapport à Paris, le programme que j'obtiens est le réseau SNCF que nous connaissons... Rien ne remplace une vraie idée algorithmique et Jean-Louis Krivine, notamment, a donc proposé de partir d'un algorithme obtenu au *feeling*, puis de *démontrer* qu'il répond à la question, et d'appliquer alors la démarche ci-dessus *à cette preuve*. Le λ-terme final est une sorte de compilation certifiée de l'algorithme de départ. Je ne vais pas m'étendre davantage sur ces questions. (Pour ceux qui voudraient en savoir plus sur les liens entre le lambda-calcul typé et la théorie de la démonstration, cf. par exemple [Girard et al., 1990].)

9 La nature des fonctions

9.1 Une interprétation linéaire

Le λ-calcul typé, auquel nous ramène l'isomorphisme de Curry-Howard, n'est qu'un calcul fonctionnel *formel* : il n'a pas d'assise *concrète*, sur laquelle l'intuition puisse vraiment avoir prise. Il a bien une interprétation ensembliste, mais elle fait intervenir des ensembles monstrueux sans rapport avec l'idée sous-jacente.

On a essayé, dès les années 1960 (travaux de Scott et d'Ershov : voir e.g. [Scott, 1976]), de diminuer la taille des interprétations —en particulier celle de l'espace de fonctions B^A qui répond de l'implication logique. L'idée était de munir les espaces d'une structure topologique,

---

[29] C'est seulement avec la ludique, voir 12.2, p. 42, qui réalise l'équivalence entre l'élimination des coupures et une recherche (interactive) de preuves, que ces deux aspects sont réconciliés.

de façon à considérer non plus *toutes* les fonctions de A dans B, mais toutes les fonctions *continues*. Ce type d'interprétation a réussi à simplifier l'approche, mais ce ne fut qu'un demi-succès, car comme vous le savez sûrement, il y a plusieurs topologies possibles sur un espace de fonctions —par exemple convergence simple, convergence uniforme— et Scott ne peut les faire coïncider qu'au moyen d'acrobaties qui vont à l'encontre de l'esprit de la topologie : par exemple les espaces ne vérifient pas la propriété de séparation de Hausdorff, toute fonction séparément continue en deux variables est continue…

Pour remédier aux limitations de l'approche topologique on a cherché d'autres structures. Je vais vous parler ici d'une interprétation linéaire ; pour fixer les idées on commencera par des espaces vectoriels (complexes) de dimension finie pour éviter tout problème. Supposons donc que les formules $A, B, C \ldots$ représentent en fait de tels espaces vectoriels ; une démonstration du séquent $\vdash C$ devient alors un vecteur de l'espace C, une démonstration du séquent $B \vdash C$ devient une application linéaire de B dans C, et en général un séquent devient une application multilinéaire, e.g., une démonstration de $A, B \vdash C$ est une application bilinéaire de $A \times B$ dans C. Cette interprétation accepte le groupe identité (fonction identité, composition d'application multilinéaires). Elle accepte aussi la règle d'échange ; par contre elle est rétive à l'affaiblissement et à la contraction : l'affaiblissement introduit des fonctions affines, e.g., $f(x) = y_0$ tandis que la contraction introduit des fonctions quadratiques, e.g., à partir de $f(x, y) = x.y$ de $\mathbb{C} \times \mathbb{C}$ dans $\mathbb{C}$ elle construit $f(x) = x^2$ de $\mathbb{C}$ dans $\mathbb{C}$ qui n'est pas précisément linéaire ! Mais oublions ce détail et résignons-nous pour le moment à n'interpréter qu'un morceau de logique sans affaiblissement ni contraction, ce que nous appellerons *logique linéaire* pour des raisons évidentes.

Que devient l'implication ? Elle devient l'espace des fonctions linéaires de A dans B, « en tant qu'espace vectoriel », ce que nous noterons $A \multimap B$ (implication *linéaire*) : le changement de notation nous rappelle qu'il y a en plus des fonctions affines, quadratiques, etc. dans la « vraie » implication $A \Rightarrow B$. Les règles logiques de l'implication sont validées par cette interprétation.

Venons-en à la conjonction ; les espaces vectoriels nous offrent en fait deux conjonctions, à savoir la somme directe d'espaces vectoriels, que nous noterons $A \& B$ (A *avec* B) (de dimension $\dim(A) + \dim(B)$) et le produit tensoriel, que nous noterons $A \otimes B$ (A *fois* B) (de dimension $\dim(A).\dim(B)$). Ces deux interprétations valident les règles de la conjonction, pourvu d'être soigneux quant à la gestion du contexte, voir *infra*.

De plus une nouvelle opération apparaît, la *négation linéaire* $A^{\perp}$, qui correspond à l'espace dual ; sa principale qualité est d'être involutive. En particulier, chaque opération logique induit une opération duale, ainsi on définit la disjonction *plus* au moyen de $A \oplus B = (A^{\perp} \& B^{\perp})^{\perp}$, et la disjonction *par* au moyen de $A \parr B = (A^{\perp} \otimes B^{\perp})^{\perp}$.

À vrai dire tout ça n'est qu'à moitié convaincant, car notre explication identifie chaque opération à son dual. Cela devient plus satisfaisant si on ajoute les contraintes suivantes :

- On considère des espaces normés (espaces de Banach) ; cela suffit à différencier les espaces de leurs duaux. Ainsi, la conjonction $A \& B$ est munie de la norme ℓ^{∞} : $\|x + y\| = \sup(\|x\|, \|y\|)$, tandis que la disjonction $A \oplus B$ est munie de la norme ℓ^1 : $\|x + y\| = \|x\| + \|y\|$.
- À cause des fonctions analytiques (voir *infra*), on doit passer à des Banach de dimension infinie ; il se pose des problèmes techniques liés au fait que le bidual d'un Banach est rarement égal à l'espace lui-même, mais on peut sans trop de difficulté résoudre la question, en « spécifiant » le dual. On trouvera les détails dans l'article [Girard, 1999].

Il reste à régler le cas de l'affaiblissement et de la contraction, qui introduisent des dépendances « polynomiales » ; la forme la plus générale d'une telle dépendance est celle d'une fonction analytique bornée définie sur une boule ouverte de rayon 1, et c'est d'ailleurs ainsi qu'apparaissent les espaces de dimension infinie. On a donc deux notions d'implication, $A \Rightarrow B$ et $A \multimap B$, que faire ? Une technique standard de linéarisation nous permet d'exprimer $A \Rightarrow B$ comme un espace de fonctions linéaires *pourvu de changer l'espace-source*. Donnons un exemple : une fonction analytique d'une variable se développe au voisinage de l'origine en $f(z) = \sum a_n z^n$. Si elle est définie pour tout z de module < 1, on peut essayer de définir une fonction F sur l'espace des suites $Z = (z_0, z_1, z_2, \dots)$ de nombres complexes au moyen de $F(Z) = \sum a_n z_n$; cette définition a un sens pour les suites $\mathbf{z} = (1, z, z^2, \dots)$ $(|z| < 1)$, on a alors $F(\mathbf{z}) = f(z)$; elle s'étend naturellement à l'espace vectoriel engendré par les $\mathbf{z}$ $(|z| < 1)$. Cet espace peut être naturellement muni d'une norme, et on considère son complété $!A$ (lire « bien sûr ») : c'est sur cet espace que F est défini et la construction est parfaitement générale. À toute fonction analytique f correspond une fonction linéaire bornée F et réciproquement : les « coefficients » sont les mêmes, seul le domaine change. On a ainsi $A \Rightarrow B \simeq (!A) \multimap B$; la nouvelle opération $!A$ a un dual $?A$ (lire « pourquoi pas »).

Outre les espaces de Banach cohérents [Girard, 1999] —interprétation assez tardive—, il y a d'autres types d'espaces linéaires donnant lieu à la même analyse, celle qui mène à la logique linéaire, mentionnons les *espaces cohérents*, voir e.g., [Girard, 1987a], les *hypercohérences* [Ehrhard, 1995].

9.2 Le calcul des séquents linéaire

Les nouveautés que nous venons de découvrir —refus de l'affaiblissement et de la contraction en tant que règles structurelles—, nouveaux connecteurs… amènent à la *logique linéaire*, qui se présente comme un calcul des séquents. Du fait de la présence d'une négation involutive, le côté gauche du $\vdash$ est redondant : on peut mettre tout à droite, c'est-à-dire écrire $\vdash {A_1}^\perp, {A_2}^\perp, \dots, {A_n}^\perp, \Delta$ au lieu de $A_1, A_2, \dots, A_n \vdash \Delta$ —ce qui rend la symétrie entrées/sorties complètement manifeste, puisque conclusions et hypothèses sont du même côté ! Du coup, on n'a même plus besoin de parler de la négation, elle disparaît en tant que donnée primitive de la théorie : on peut la retrouver en la *définissant* comme symétrie par rapport au « miroir » $\vdash$; on spécifie aussi que $\otimes$ et $\parr$, $\oplus$ et $\&$, $!$ et $?$, $\forall$ et $\exists$ sont respectivement duaux, c'est-à-dire images l'un de l'autre dans le « miroir » $\vdash$; en d'autres termes la négation est *définie* par $(A \otimes B)^\perp = A^\perp \parr B^\perp$, etc.[30] Les règles se divisent toujours en trois groupes :

Le groupe identité

$$\frac{}{\vdash A^\perp, A}\ \text{(axiome d'identité)} \qquad \frac{\vdash \Gamma, A \qquad \vdash A^\perp, \Gamma'}{\vdash \Gamma, \Gamma'}\ \text{(coupure)}$$

Le groupe structurel

$$\frac{\vdash \Gamma}{\vdash \sigma(\Gamma)}\ \text{(échange)}$$

---

[30] De sorte que, par exemple, la règle du « Par » de la version « droite » (cf. *infra*) induit dans une version gauche/droite les deux règles $\dfrac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, A \parr B}$ $(\vdash \parr)$ et $\dfrac{\Gamma, A, B \vdash \Delta}{\Gamma, A \otimes B \vdash \Delta}$ $(\otimes \vdash)$. (N.d.r.)

Ce principe exprime la commutativité de la logique[31]. Par contre, les deux autres règles structurelles (affaiblissement et contraction) disparaissent en logique linéaire, parce qu'elles reviennent à dire que $A \otimes B \vdash A$ et $A \vdash A \otimes A$, respectivement : dans l'une on voit une fonction affine, dans l'autre une fonction quadratique, ce n'est pas linéaire. Ces règles réapparaîtront comme règles *logiques* du ? et du !…*Cet abandon des règles structurelles n'est pas un simple artifice technique* : on va voir dans un instant (n^o 10) que la logique linéaire est une « logique des actions », et que dans une telle logique il *faut* renoncer à ces règles. De plus, contrairement à ce qui se passait en logique intuitionniste, ici les règles structurelles sont interdites de façon symétrique (la logique linéaire peut être vue comme une logique intuitionniste symétrisée) : on cumule bien les avantages des logiques classique et intuitionniste.

Le groupe logique

Les connecteurs logiques se répartissent en trois groupes[32] :

1. Les connecteurs *additifs* $\oplus, \&$, qui correspondent à des sommes d'espaces.

   $$\frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \,\&\, B}\ (\&), \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, A \oplus B}\ (g\oplus), \qquad \frac{\vdash \Gamma, B}{\vdash \Gamma, A \oplus B}\ (d\oplus)$$

   Le connecteur « Plus » $\oplus$ est très proche de la disjonction intuitionniste ; en particulier il vérifie la propriété de la disjonction. Le connecteur « Avec » & *est* la conjonction intuitionniste. Observez que les deux prémisses de la règle du « Avec » ont le même contexte : c'est la seule façon de préserver la contrainte de multilinéarité.

2. Les connecteurs *multiplicatifs* $\otimes, \parr$, qui correspondent à des produits tensoriels. Il y a un troisième connecteur multiplicatif, $A \multimap B$, mais on peut se dispenser de l'écrire, car on le définit par $A^\perp \parr B$.

   $$\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \parr B}\ (\parr) \qquad \frac{\vdash \Gamma, A \quad \vdash \Delta, B}{\vdash \Gamma, \Delta, A \otimes B}\ (\otimes)$$

   Le connecteur « Par » $\parr$ est très proche de la disjonction classique ; on s'amusera ainsi à démontrer $A \parr A^\perp$; remarquez que la virgule du calcul tient lieu de « Par » non écrit. Le connecteur « Fois » $\otimes$ est nouveau : remarquez que les contraintes de multilinéarité imposent un partage du contexte dans les prémisses.

3. Les connecteurs *exponentiels*, !, ?, qui tirent leur nom d'un isomorphisme très important $!(A \,\&\, B) \simeq !A \otimes !B$.

   $$\frac{\vdash ?\Gamma, A}{\vdash ?\Gamma, !A}\ (\text{promotion}) \qquad \frac{\vdash \Gamma, A}{\vdash \Gamma, ?A}\ (\text{déréliction})$$

   $$\frac{\vdash \Gamma}{\vdash \Gamma, ?A}\ (\text{affaiblissement}) \qquad \frac{\vdash \Gamma, ?A, ?A}{\vdash \Gamma, ?A}\ (\text{contraction})$$

   Remarquons que la contraction et l'affaiblissement sont toujours présents en logique linéaire, mais maintenant comme *règles logiques*. C'est donc le connecteur « Pourquoi

---

[31] Il existe depuis peu une logique non commutative, voir [Abrusci and Ruet, 2000], basée sur le refus —ou plutôt le contrôle— de l'échange.

[32] On n'écrira pas les règles des quantificateurs, qui offrent d'ailleurs peu de surprises.

> pas »? qui en contrôle l'usage. On pourra d'ailleurs s'amuser à démontrer les séquents $!(A \& B) \vdash !A \otimes !B$ et $!A \otimes !B \vdash !(A \& B)$ qui expriment l'isomorphisme $!(A \& B) \simeq !A \otimes !B$; une de ces démonstrations utilise l'affaiblissement, l'autre la contraction. En fait l'isomorphisme exprime la validité de ces règles structurelles dans le cas exponentiel.

Faisons une pause : introduire une nouvelle logique est un acte grave. La première chose à vérifier est qu'on ne perd pas ce qu'on avait déjà, typiquement ce qu'on pouvait exprimer classiquement ou intuitionistiquement. En fait, si on traduit $A \Rightarrow B$ par $!A \multimap B$, $A \wedge B$ par $A \& B$, etc. et le séquent intuitionniste $A_1, \ldots, A_n \vdash B$ par $\vdash ?A_1{}^{\perp}, \ldots, ?A_n{}^{\perp}, B$, cette traduction s'étend en une traduction des démonstrations —traduction fidèle. Le symbole ? devant les hypothèses niées sert précisément à autoriser contraction et affaiblissement « à gauche ». On peut procéder de même avec la logique classique, au moyen du préfixe ?!, qui joue le rôle de double négation.

On n'a rien perdu ; reste à savoir si l'on y a vraiment gagné !

10 Interprétation intuitive des connecteurs linéaires

Nous allons voir maintenant que les connecteurs de la logique linéaire expriment des nuances qui existent dans la vie courante, mais que la logique avait jusque-là complètement négligées. Cela leur donne une interprétation utile, parce qu'intuitivement parlante. Mais il ne faut pas chercher dans ces illustrations le « véritable sens » de ces connecteurs : si ce « véritable sens » existe, on ne le trouvera pas dans un univers qui leur est extérieur, il ne peut résider que dans la combinaison des démonstrations entre elles, et dans leur *harmonie interne*.

Une logique des actions : l'implication linéaire $\multimap$

Les mathématiques manipulent des vérités éternelles : on utilise une formule A pour obtenir B par $A \Rightarrow B$, mais ça n'use pas A, elle est toujours là, on pourra la réutiliser : c'est le principe *d'inoxydabilité des formules* ! Toute la logique classique sort de là. Dans les sciences autres que les mathématiques, et dans la vie courante, on ne s'intéresse pas tant aux déductions $A \Rightarrow B$ entre des vérités éternelles qu'aux *transformations* $A \rightarrow B$ entre des états passagers : « *A se change en B (ou est échangé contre B)* ». C'est de cette façon qu'il faut interpréter l'implication linéaire $A \multimap B$. Cette implication est liée à l'idée de *payer* : je paye avec A pour avoir B, et du coup, je n'ai plus A. Et ce n'est pas un simple avatar de l'implication classique $\Rightarrow$. Par exemple, on ne peut pas remplacer $A \multimap B$ par la formule classique $A \Rightarrow (B \wedge \neg A)$, dont on voit tout de suite qu'elle équivaut à $\neg A$: ce n'est pas du tout ce qu'on voulait exprimer ! Il s'agit réellement d'un nouveau connecteur, et d'une nouvelle logique —une logique des *actions*, et des *réactions* qu'elles appellent inévitablement : *j'agis* sur mon environnement pour avoir B, mon environnement *réagit* en me prenant A.

La conjonction de faits indépendants : la conjonction multiplicative $\otimes$

Supposons qu'un café et un déca soient au même prix, disons 5F ; je note A la pièce de 5F, B un café, C un déca ; si vous préférez manipuler des propositions logiques plutôt que des objets, vous pouvez considérer que A signifie « j'ai 5F », B signifie « j'ai un café » et C « j'ai un déca »... Le fait qu'avec 5F je peux avoir un café s'écrit $A \multimap B$; de même : $A \multimap C$. Bien sûr, je ne peux pas écrire $A \Rightarrow B$, $A \Rightarrow C$, car d'abord ça ne correspond pas à la signification usuelle du symbole $\Rightarrow$, et ensuite parce que j'en déduirais aussitôt $A \Rightarrow B \wedge C$, ce qui tendrait à signifier qu'avec 5F je peux avoir un café *et* un déca : ce serait la ruine de l'économie libérale !

La conjonction « Fois », $\otimes$, exprime que deux actions sont effectuées de façon « indépendantes », typiquement $B \otimes C$ signifie (boire) un café et un déca (pensons à deux buveurs distincts). $\multimap$ et $\otimes$ ne se manipulent pas comme leurs analogues classiques $\Rightarrow$ et $\wedge$: de $A \multimap B$ et $A \multimap C$ les règles logiques ne nous permettent pas de déduire $A \multimap B \otimes C$. Par contre, elles permettent de déduire $A \otimes A \multimap B \otimes C$, c'est-à-dire que si j'ai *deux* pièces de 5F je peux avoir un café *et* un déca. On voit bien sur cet exemple que dans la vie de tous les jours *la conjonction n'est pas idempotente* —contrairement à $A \wedge A = A$, on n'a pas $A \otimes A = A$: avoir 5F *et* 5F, ce n'est pas la même chose qu'avoir simplement 5F ! *En logique linéaire, comme dans la vie courante, la duplication est payante.*

Un autre exemple est celui des réactions chimiques. Si A désigne une molécule $\mathtt{H_2}$, B une molécule $\mathtt{O_2}$ et C une molécule $\mathtt{H_2O}$, la synthèse de l'eau s'écrit : $A \otimes A \otimes B \multimap C \otimes C$. On retrouve de manière évidente le fait que, dans les phénomènes d'interaction, la conjonction n'est pas idempotente : si on remplace $A \otimes A$ par A et $C \otimes C$ par C, on perd une information essentielle, celle des *proportions des mélanges*. On remarque aussi un autre phénomène important : si on désigne par D une autre molécule (par exemple une molécule de fer, `Fe`), on ne peut pas déduire de $A \otimes A \otimes B \multimap C \otimes C$ que $A \otimes A \otimes B \otimes D \multimap C \otimes C$ car la molécule D qui se trouve à gauche doit nécessairement donner quelque chose à droite —ne serait-ce que de la fumée. Elle ne peut pas disparaître purement et simplement. Ce *principe de conservation* remplace, en logique linéaire (du moins, tant qu'on n'utilise pas les connecteurs exponentiels), le *principe d'inoxydabilité des formules* qui était valable en logique classique, et il est l'explication intuitive de la *linéarité* de $\multimap$. En logique linéaire, supprimer est payant, tout comme dupliquer.

La conjonction & : coexistence des éventualités

On peut traduire $A \,\&\, B$ par « avoir le choix entre A *et* B. » Dans l'exemple du café et du déca, j'ai $A \multimap B \,\&\, C$, c'est-à-dire qu'avec 5F j'ai la *possibilité* d'acheter un café, *et* (simultanément) la *possibilité* d'acheter un déca. Il s'agit d'une potentialité, et au moment de passer à l'acte, je devrai choisir entre B et C : & désigne donc la superposition de deux actions potentielles, un peu comme la superposition de deux états quantiques. Si je regarde dans une vitrine de magasin, je vois pour le même prix (disons 100F) un objet A *et* un objet B, ils sont là tous les deux devant moi : c'est bien une conjonction ! Mais avec mes 100F je n'aurai qu'un des deux : c'est un peu comme la réduction du paquet d'onde.

Les deux conjonctions sont donc profondément différentes : $A \,\&\, B$ signifie que j'ai le choix entre le beurre et l'argent du beurre, il n'en résulte pas que je peux avoir le beurre *et* l'argent du beurre ($A \otimes B$)... On voit bien, sur les règles logiques du calcul des séquents (dans la version gauche/droite, plus parlante), la différence entre les deux conjonctions & et $\otimes$:

$$\cfrac{\cfrac{A \vdash B \quad A \vdash C}{A, A \vdash B \otimes C}}{A \otimes A \vdash B \otimes C} \qquad \frac{A \vdash B \quad A \vdash C}{A \vdash B \,\&\, C} \qquad \text{(les deux conjonctions)}$$

On cherchera d'ailleurs en vain à démontrer les séquents $A \otimes B \vdash A \,\&\, B$ ou $A \,\&\, B \vdash A \otimes B$, sans aucune hypothèse sur A ou B : il faudrait l'affaiblissement pour obtenir le premier, la contraction pour le second. Bien entendu, dans une conception ringarde de la logique-comme-système-déductif, rien ne s'oppose à l'existence d'une démonstration indirecte : par exemple, on pourrait invoquer un « détour » via une autre formule C pour permettre les contractions ou affaiblissements nécessaires... Mais c'est là qu'intervient l'élimination des coupures dans toute sa majesté ! Ce détour, ça s'appelle une coupure ; ça revient à démontrer $A \,\&\, B \vdash C$ et $C \vdash A \otimes B$ pour en déduire $A \,\&\, B \vdash A \otimes B$, mais le *Hauptsatz*, toujours valable en logique linéaire[33] nous ramène aux seules démonstrations sans coupures, et donc… *no way* !

Micro-actions/macro-actions : connecteurs exponentiels

La logique classique décrivait des *situations*, la logique linéaire décrit des *actions*. La différence entre une *action* et une *situation*, c'est qu'une situation est statique : elle ne rencontre aucune opposition, n'entraîne aucune *réaction*, *elle ne coûte rien*. Vous pouvez utiliser $2 + 2 = 4$ à volonté, ça sera toujours là, c'est comme s'il y en avait un stock inépuisable. La logique linéaire rend compte de ce cas limite par le symbole « ! », qui signale que les ressources sont, au moins *en pratique*, inépuisables —et donc la réaction (*pratiquement*) négligeable. Autrement dit, « $!A$ » signifie « A *ad libitum* ». M. Rockefeller ne compte plus ses pièces, il peut écrire $!A$; et de $!A \multimap B$, $!A \multimap C$, il peut déduire $!A \multimap B \otimes C$. Les logiques intuitionniste et classique apparaissent comme des *logiques des macro-actions* (la gestion des grandes quantités, comme en macro-économie), tandis que la logique linéaire est la logique des micro-actions, des quantités limitées (comme en micro-économie). Celles-là ne sont donc que des cas limites de celle-ci —un peu comme la thermodynamique est un cas limite de la mécanique, et comme la mécanique classique est un cas limite de la mécanique quantique.

L'interprétation des règles de déréliction, affaiblissement et contraction en termes de « ! » (p. 32) est claire. Pour comprendre l'interprétation de « ? », on peut prendre l'exemple des mémoires des machines [Lafont, 1990] : $!A$ signifie que A est stocké dans la mémoire d'une machine et qu'on peut l'y appeler autant de fois qu'on le veut ; $?A^{\perp}$ consiste alors à *activer cette potentialité*, ce qui peut se faire suivant trois modes fondamentaux :

- *lecture* (= *déréliction*) ;
- *effacement* (= *affaiblissement*) ;
- *duplication* (= *contraction*).

La règle de *promotion* correspond donc à un *stockage* ; sa forme spéciale (le contexte doit être de la forme $?\Gamma$) s'explique par l'impossibilité de stocker une donnée qui dépendrait de données (contexte) susceptibles de variations.

La disjonction $\oplus$: le choix subi

$A \oplus B$ signifie « faire A ou faire B ». Mais, contrairement à $A \,\&\, B$, qui exprime la *conjonction* de deux *possibilités* qui me sont offertes simultanément, donc un choix que j'ai à faire, $A \oplus B$ est pour moi un choix subi, une alternative sur laquelle je n'ai pas prise : il va faire beau ou il va pleuvoir —on verra bien, je n'ai pas le choix. & était une conjonction, $\oplus$ exprime vraiment une *disjonction* : j'ai le choix entre A *et* B ($A \,\&\, B$), mais je vais rencontrer C *ou* D ($C \oplus D$). Cette nuance existe réellement dans la vie de tous les jours, c'est la distinction entre le choix qu'on fait et le choix qu'on subit ; entre l'indéterminisme interne et l'indéterminisme externe, etc. Pour bien comprendre cette nuance, voici un exemple quotidien, proposé par Yves Lafont :

Un menu gastronomique :

```
Prix : FF 380
Entrée : Huîtres ou Melon suivant arrivage ;
Plat principal : Hamburger et son cortège de frites à volonté ;
```

---

[33] C'est une évidence *a priori* : la logique linéaire a été construite *autour* d'une analyse fine de ce résultat. La moindre des choses est qu'elle le préserve !

`Sortie : Fromage ou Dessert ;`
`Boisson : carafe d'eau à volonté.`

Pour le prix donné j'ai tout un menu : $\mathtt{Prix} \multimap \mathtt{Entrée} \otimes \mathtt{Principal} \otimes \mathtt{Sortie} \otimes \mathtt{Boisson}$. Si on détaille :

$$\mathtt{FF\ 380} \multimap (\mathtt{Huîtres} \oplus \mathtt{Melon}) \otimes \mathtt{Hamburger} \otimes {!\mathtt{Frites}} \otimes (\mathtt{Fromage}\ \&\ \mathtt{Dessert}) \otimes {!\mathtt{Eau}}$$

$\mathtt{Huîtres} \oplus \mathtt{Melon}$ signifie que je n'ai pas le choix entre Huîtres ou Melon : c'est suivant l'arrivage, ce n'est pas à moi de choisir. Par contre, c'est moi qui choisis entre Fromage et Dessert, c'est pourquoi je note $\mathtt{Fromage}\&\mathtt{Dessert}$, et non $\mathtt{Fromage} \oplus \mathtt{Dessert}$.

Dualité action/réaction : négation linéaire
Ce qui différencie une action d'une situation, c'est qu'on ne peut pas l'itérer. Pourquoi ? Parce que toute action provoque une *réaction* qui la détuit, i.e., s'oppose à son itération. Les possibilités dynamiques sont jaugées par un acteur : « je » veux avoir B, mais ça va « me » coûter A ; « j'ai » le choix entre A *et* B, mais « je » vais rencontrer C *ou* D. L'acteur agit sur le reste du monde, qui lui oppose une résistance ; à chaque action, une réaction. Mais pour le reste du monde (du moins pour la partie qui est concernée par notre acteur, c'est-à-dire celle qui lui réagit), le point de vue est inversé : ce que « je » vois de l'intérieur, « il » le voit de l'extérieur, et vice versa. Des actions décrites par moi comme « donner », « choisir », seront décrites par lui comme « recevoir », « subir » — c'est-à-dire comme des réactions. Cette inversion du point de référence correspond à une dualité :

Moi/le Monde
Action/Réaction

Son expression en logique linéaire est la *négation linéaire* : $A/A^{\perp}$. La négation linéaire ne correspond en aucune façon à l'idée de s'abstenir d'une action, il faut la rapprocher de l'idée d'espace orthogonal : en géométrie, ce n'est pas le complémentaire d'une droite qui a de l'importance, c'est le plan orthogonal.
La dualité est à l'œuvre dans le cas des exponentielles —lire (et ses variantes, effacer, dupliquer)/écrire. Elle est aussi à l'œuvre dans le cas additif : dans notre menu, adoptons un instant le point de vue du restaurateur (et plus généralement du monde externe au consommateur) : il a le choix entre les huîtres et le melon, pour lui, c'est un « Avec », alors qu'il est sans pouvoir sur l'alternative fromage/dessert, pour lui c'est un « Plus », soumis à l'arbitraire du client. Il est par contre plus difficile de rendre compte de la dualité entre « Fois » et « Par » : on commence à arriver au point où les métaphores s'épuisent, où les mathématiques seules peuvent parler. Mais essayons tout de même…

La disjonction $\parr$: vases communicants, concommitance
Considérons deux vases communiquants fermés par des pistons $\mathcal{P}$ et $\mathcal{Q}$. Si j'appelle A l'action de tirer $\mathcal{P}$ de dix centimètres, et B l'action d'abaisser $\mathcal{Q}$ de dix centimètres, ce sont pour moi deux aspects complémentaires d'une même action, qui consiste à déshabiller Pierre pour habiller Paul. Bien sûr, les deux phénomènes A et B vont survenir, et quelqu'un qui observerait la scène sans voir que les vases communiquent, dirait : *je constate que* $\mathcal{P}$ *remonte* et *($\otimes$) que* $\mathcal{Q}$ *descend*, il aura l'illusion d'un « Tenseur » d'actions, i.e., une *conjonction* de deux événements indépendants. Mais il déchantera vite, par exemple quand il voudra abaisser simultanément les deux pistons. On a donc affaire à des événements *concommitants*, mais non indépendants, ce qui est le sens du connecteur « Par ». L'exemple emblématique de « Par » est le principe $\vdash A, A^{\perp}$

(ou encore $A \parr A^{\perp}$), dont la métaphore la plus exacte est celle d'une rallonge, e.g., les actions concommitantes donner 220V/accepter 220V.

Machines abstraites

Tout cela, bien que très amusant, doit se traduire en théorèmes. Ces exemples informels peuvent se traduire en termes de manipulations de piles, de choix déterministes ou non, d'utilisation de la mémoire pour les machines abstraites de votre choix, etc. Les résultats sont tous de la forme : par rapport à la machine $\mathcal{M}$ fixée, la configuration b est accessible à partir de la configuration a *si et seulement si* l'implication $A \otimes M \multimap B$ entre les propositions (formules sans quantificateurs qui représentent a, $\mathcal{M}$ et b de façon adéquate) est démontrable en logique linéaire. On mesure alors le pouvoir expressif énorme de la logique linéaire par rapport aux systèmes existants, ce qui confirme nos intuitions[34]. Les complexités algorithmiques des principaux *fragments* propositionnels (morceaux de logique n'utilisant qu'une partie des connecteurs, *sans changer les règles*) s'établit comme suit[35] :

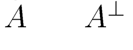
– *Fragment multiplicatif :* `NP`-complet ;
– *Fragment multiplicatif/additif :* `Pspace`-complet ;
– *Fragment multiplicatif/exponentiel :* inconnu, mais au moins celui de l'accessibilité des réseaux de Petri.
– *Fragment complet multiplicatif/additif/exponentiel :* indécidable.

Voir les articles [Lincoln et al., 1990] et [Kanovitch, 1991].

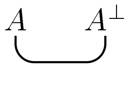
11 Les réseaux de démonstration

11.1 Réseaux

Hors de toute idéologie, la raison principale du remplacement de la logique classique par la logique intuitionniste réside dans une amélioration du *Hauptsatz* : le λ-calcul typé, voir *supra* permet, moyennant une asymétrie entre gauche (*les* arguments) et droite (*le* résultat), d'obtenir un bon calcul fonctionnel : la logique intuitionniste se représente par des λ-termes qui peuvent se voir comme des arbres dont les feuilles sont les formules gauches du séquents (hypothèses, variables) et la racine la formule droite (conclusion, résultat). La réintroduction de la symétrie à travers la négation linéaire détruit cet aspect fonctionnel : tout est argument, ou tout est résultat, comme on veut... On est amené à considérer des « termes à plusieurs résultats », qui se présenteront sous forme de graphes, les *réseaux de démonstration*. Dans ce qui suit nous nous retreindrons au fragment multiplicatif $(\otimes, \parr)$ de la logique. L'idée est de revenir au calcul des séquents, *mais en oubliant le contexte*, ce qui se traduit par des *liens* graphiques entre les formules. Ainsi le groupe identité donne-t-il lieu aux liens :



(lien axiome)



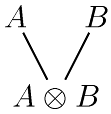
(lien coupure)

---

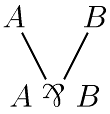
[34] Rappelons, pour les initiés, que le calcul propositionnel est `coNP`-complet dans le cas classique, et `Pspace`-complet dans le cas intuitionniste.

[35] On se restreint aux fragments contenant les connecteurs multiplicatifs, car pour avoir un système déductif intéressant, il faut au moins disposer de l'implication linéaire, qui est multiplicative.

Nous verrons que le lien axiome est une rallonge et le lien coupure un branchement. Les règles logiques donnent lieu à cette représentation banale :



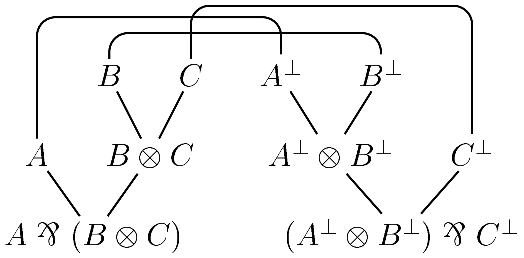
(lien Tenseur)



(lien Par)

Finalement, la règle d'échange ne donne lieu à rien en termes de graphe ; à remarquer cependant, que du point de vue planaire, l'échange introduit des croisements de liens axiomes. Voici quelques exemples de réseaux de démonstration, corrects ou non (voir *infra*) :

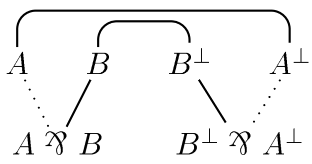
(7)

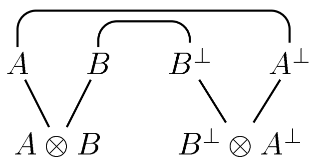


(8)

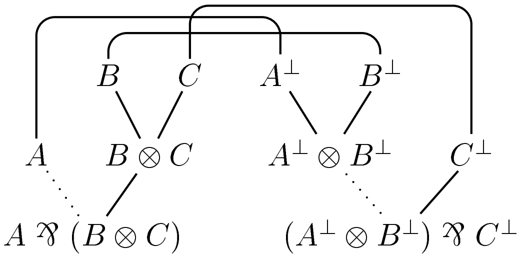
11.2 Le critère de correction

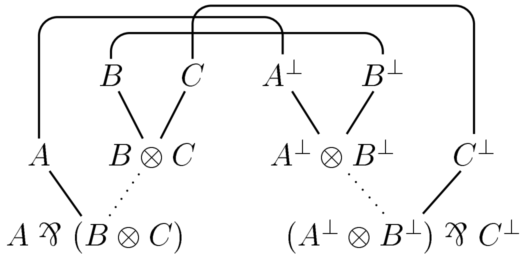
En face de tels graphes, la première question qui se pose est la suivante : nous avons oublié toute séquentialité, i.e., l'ordre dans lequel les règles logiques ont été appliquées. Y-a-t-il un moyen de le retrouver, ou, du moins —ce qui est plus raisonnable, puisque le but des réseaux est précisément d'enlever toute séquentialité— de caractériser parmi de tels graphes, ceux qui sont *sequentialisables*, i.e., qui « proviennent » du calcul des séquents. La réponse est le résultat principal de [Girard, 1987a] ; je présente ici la version simplifiée due à Danos et Regnier, [Danos and Regnier, 1989]. L'idée est de sélectionner, pour chaque lien « Par », une des deux prémisses `g` ou `d` (ce qu'on appelle un positionnement d'interrupteurs), et on ne garde que l'arête correspondant au choix. Ainsi, les deux réseaux (7) nous donnent-ils, par exemple :





Celui de gauche (on a positionné un « Par » sur `d`, l'autre sur `g` ; les arêtes manquantes sont figurées en pointillé) n'est pas connexe. Quand à celui de droite —où il n'y a pas de « Par »— il a un cycle. Par contre le réseau (8) est connexe et acyclique quelque soit le positionnement des interrupteurs, par exemple

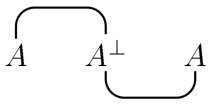


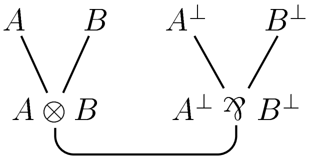


Cela tombe bien, car les réseaux (7) ne sont pas *séquentialisables*, i.e., ne viennent pas d'une démonstration, alors que (8) l'est. D'ailleurs le *théorème de séquentialisation* stipule qu'un réseau est séquentialisable si et seulement si, quelque soit le positionnement d'interrupteurs $\mathcal{S}$, le graphe induit est connexe/acyclique. À noter que ce critère demande *a priori* un nombre exponentiel de vérifications ; mais Guerrini a récemment démontré [Guerrini, 1999] que cette condition peut se vérifier en temps linéaire.

11.3 Normalisation des réseaux

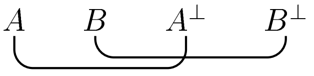
Les réseaux ne sont pas là pour être contemplés, mais pour être *normalisés* : une coupure apparaît nécessairement au sein d'une des deux configurations :





qui se simplifient respectivement en :

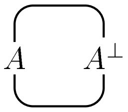
A



On observe que :

1. Cette procédure, bien que non-déterministe, est « confluente », i.e. que le résultat ne dépend pas vraiment de l'ordre dans lequel on a appliqué les simplifications. C'est ce qui a inspiré Lafont pour ses *réseaux d'interaction* : voir [Lafont, 1995].
2. Cette procédure converge, car à chaque étape, le nombre total de liens diminue strictement...

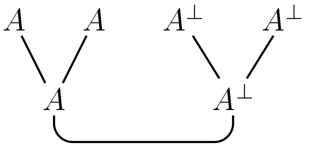
Illusion graphique que dément une analyse rigoureuse ; en effet la configuration axiome/coupure de gauche ne se simplifie que si les deux « A » sont distincts, j'ai négligé le cas suivant :



(9)

Cette structure —qui correspond à une rallonge branchée sur elle-même— contient un cycle et ne vérifie donc pas le critère de correction. Le critère de correction nous assure donc qu'une étape de « simplification » diminue toujours la taille d'un réseau : il ne reste qu'à démontrer que, de plus, le réseau simplifié vérifie encore le critère ; nous y reviendrons.

La normalisation des réseaux nous permet de comprendre quel est le vrai problème de la logique classique : on peut facilement fabriquer des réseaux « classiques » —pour l'essentiel il suffit d'ajouter un lien pour la contraction, géré exactement comme un lien « Par »— mais ça n'avance guère, car il n'y a pas de façon générale de simplifier les configurations de coupures contenant ce lien, typiquement une coupure entre deux contractions :



qui correspond aux « coupures croisées » de Gentzen. La normalisation suppose des duplications, or chacun veut dupliquer l'autre, ce qui s'annonce mal..., de plus les dupliqueurs se mettraient-ils d'accord que se poserait un problème de localisation, car on ne voit pas comment procéder sans invoquer la totalité de la structure. Ça ne dit peut-être pas que la logique classique est fausse, mais ça montre en quoi elle est hautement problématique.

11.4 Analogie électrique

L'interprétation de la logique linéaire en termes de réseaux conduit assez naturellement à une analogie où les objets de base sont les modules électriques : ce sont des boîtes noires d'où sortent un certain nombre de prises. Pour assembler des modules, on lit l'étiquette qui donne le mode d'emploi de chaque prise, par exemple : « sortie 220V ». Si on assimile ces modes d'emplois à des propositions, la combinaison des modules entre eux est une sorte de logique.

On note $A = B^\perp$, ou $B = A^\perp$, pour dire qu'une prise étiquetée A peut physiquement être branchée sur une prise étiquetée B. Autrement dit, la négation correspond à la complémentarité mâle/femelle. Si π est un module dont sortent des prises $A_1, \ldots, A_n$, on note : $\pi \vdash A_1, \ldots, A_n$. On note Γ, Δ,... des suites de prises. Et on va retrouver tout notre cher calcul des séquents :

l'axiome d'identité dit qu'on dispose des rallonges formées de deux prises complémentaires A et $A^\perp$. La coupure dit qu'on peut utiliser ces rallonges dans les branchements : si $\pi \vdash \Gamma, A$ et si $\pi' \vdash A^\perp, \Delta$, alors ces deux modules peuvent être branchés de façon à former $\pi'' \vdash \Gamma, \Delta$. Dans cette interprétation, l'élimination des coupures est simplement le raccourcissement d'un chemin, ce que d'ailleurs nous avons fait dans le cas Axiome/Coupure ! Brancher une rallonge sur elle-même, comme dans (9), serait complètement idiot, *ça ne peut pas faire partie d'une procédure d'installation !*

La règle d'*échange* est évidente : on peut brancher les prises dans l'ordre qu'on veut. Les autres règles structurelles n'ont pas de sens électrique : d'abord, la règle d'*affaiblissement* permettrait de remplacer $\pi \vdash \Gamma$ par $\pi \vdash \Gamma, A$, donc d'ajouter une prise factice, sur laquelle on écrirait quelque chose comme « sortie 220V » alors qu'il n'y a rien derrière : on ne peut pas faire de branchement avec ça ! La règle de *contraction* permettrait de remplacer $\pi \vdash \Gamma, A, A$ par $\pi \vdash \Gamma, A$, donc de regrouper deux prises d'étiquettes identiques. Superposer les deux sorties « haut-parleur » d'un amplificateur est physiquement réalisable, et revient à brancher les deux prises sur un seul haut-parleur. Peu importe que le système fonctionne encore ou explose, en tout cas, il ne fonctionnera plus de la même façon —et ce montage « classique » n'est pas couvert par la garantie ! L'unique prise ainsi créée devra porter une nouvelle étiquette, ce ne sera plus A (ce sera $A \parr A$).

Justement, cela nous amène aux règles logiques : elles décrivent la création de nouvelles prises à partir de prises existantes. Par exemple, $A \otimes B$ est formée en réunissant deux prises qui sortent de deux modules différents : si j'avais $\pi \vdash \Gamma, A$ et $\pi' \vdash \Delta, B$, j'obtiens un module $\pi'' \vdash \Gamma, \Delta, A \otimes B$. Par contre, $A \parr B$ est formée en réunissant deux prises qui sortent d'un *même* module (et donc qui communiquent à *l'intérieur* de ce module : on retrouve là l'idée de communication cachée, de vase communiquant). Les règles logiques pour $\otimes$ et $\parr$ sont immédiatement justifiées par cette interprétation. La dualité entre $\otimes$ et $\parr$ est aussi transparente : $A^\perp \parr B^\perp = (A \otimes B)^\perp$ exprime qu'on peut faire un branchement (une coupure). Bien sûr, on pourrait aussi bien faire deux coupures, l'une entre A et $A^\perp$, l'autre entre B et $B^\perp$, plutôt que le branchement de la prise composée $A \otimes B$ sur la prise composée $A^\perp \parr B^\perp$ (on retrouve l'algorithme de normalisation des réseaux, voir *supra*).

L'interprétation « électrique » s'étend à toute la logique linéaire, c'est la *Géométrie de l'Interaction*, [Girard, 1989] ; les modules s'écrivent au moyen de matrices entrée/sortie, et pour pouvoir gérer les exponentielles, il est nécessaire de passer en dimension infinie, i.e., à des opérateurs sur l'espace de Hilbert.

12 Des règles de la logique à la logique des règles

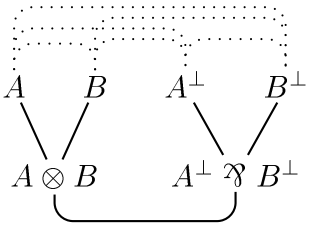
12.1 La dualité

Revenons encore au critère de correction des réseaux, et demandons-nous à quoi il sert... Notre motivation originelle était de respecter les règles —la séquentialisation— mais au fait pourquoi donc faudrait-il respecter les règles, simplement parce qu'elles sont écrites dans un grand livre ? Et si on écrit autre chose dans le livre, les règles vont se mettre à changer... balivernes[36] ! Au lieu d'une pseudo-explication *dualiste* (la logique comme *syntaxe* reflétant une *sémantique* préexistante), on peut tenter une explication *moniste*, i.e., sans ce recours à un

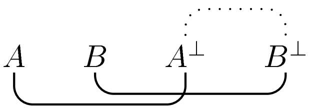
---

[36] Ce type d'ânerie est sanctifié par cette expression *méta*, qui est toujours utilisée pour faire des tours de passe-passe.

Deus ex machina externe à la logique. Pour cela, rappelons-nous que le critère de correction sert à la normalisation —il exclut le cycle (9)— mais qu'en contrepartie, il faut démontrer la préservation du critère lors des simplifications. En particulier, considérons une configuration Coupure/Tenseur/Par, et positionnons les interrupteurs au moyen de $\mathcal{S}$ sur tous les autres liens « Par », ce qui nous laisse deux possibilités quant à $A \parr B$; $\mathcal{S}$ induit un graphe :



où les pointillés entre deux formules indiquent la possibilité de « voyager par en dessus » d'une formule à une autre ; bien entendu, la plupart de ces chemins en pointillés sont impossibles. Par exemple, le pointillé entre A et B correspond à un cycle dans notre réseau, le pointillé entre A et $A^\perp$ produit un cycle si on positionne $A \parr B$ sur « gauche »... Finalement, le seul pontillé plausible est celui entre $A^\perp$ et $B^\perp$, et il est d'ailleurs nécessairement présent pour des raisons de connexité. Le critère de correction est préservé : lorsque je simplifie la coupure, le graphe



est bien connexe et acyclique.
Finalement, le critère de correction, qui exclut cinq des six trajets en pointillés, peut être vu comme une anticipation de l'élimination des coupures. En particulier, les deux arêtes qui lient A, B à $A \otimes B$ anticipent la vraie liaison qui se produira à travers une coupure et le trajet pointillé entre $A^\perp$ et $B^\perp$; de même le fait qu'on ne trace qu'une arête (au choix) entre $A^\perp$ ou $B^\perp$ et $A^\perp \parr B^\perp$ anticipe le fait que la coupure n'introduira aucune nouvelle liaison entre $A^\perp$ et $B^\perp$. Les arêtes anticipent donc les preuves de la négation, et on arrive finalement à l'identification de principe :

Positionnement d'interrupteur sur A = ***Démonstration de*** $A^\perp$

12.2 La ludique

Ce qui veut dire que la logique ne s'articule plus autour d'une opposition *démonstrations de A/modèles de* $\neg A$ (dualiste, démonstrations contre modèles) mais d'une opposition *démonstrations de A/démonstrations de* $A^\perp$ (moniste, un seul type d'objets, les démonstrations). Il faut évidemment réviser notre idée de démonstration, mais nous y étions un peu préparés depuis Heyting, de façon à en avoir suffisamment pour étayer la dualité. Ceci est le programme *ludique*, qui explique la logique comme une interaction entre deux partenaires égaux, une sorte de jeu sans arbitre. Cela nous emmenerait trop loin que de parler de ce programme déjà réalisé dans ses plus grandes lignes, voir [Girard, 2001].

12.3 Le pourquoi et le comment

Revenons à notre point de départ, le temps de Hilbert. En ce temps-là les règles des mathématiques, de la logique, plus ou moins tombées du ciel, devaient être justifiées à tout prix, par des démonstrations de cohérence. C'était le temps du *pourquoi*, une interrogation qui n'a rien produit du tout... Sauf des sous-produits de nature antagoniste à l'interrogation de départ : à partir de Gentzen, mais surtout à la fin du siècle, la question du *comment*, de la structure des règles hors de toute justification —qui finit toujours dans un peu glorieux appel au « méta »— est devenue envahissante. On découvre une possibilité extravagante : la logique est non pas la logique de cette improbable réalité préexistante, mais celle de sa propre géométrie, sa propre structure :

Disjonction : Faire la règle A ou faire la règle B, prouver A ou prouver B... La disjonction, vue comme disjonction des règles, doit avoir... la propriété de la disjonction, comme en logique intuitionniste ou linéaire.

Négation : Dans le calcul des séquents la négation apparaît comme l'échange gauche/droite, le miroir. On finit par interpréter la négation comme une dualité du genre « orthogonalité », ce qui n'a aucun rapport immédiat avec l'idée habituelle de négation.

Connecteurs multiplicatifs : On a vu que le « Tenseur », c'est « deux composantes connexes », le « Par », c'est une seule composante. On ne voit pas directement de conjonction ou de disjonction et pourtant quand on essaye de manipuler des configurations du point de vue des composantes connexes, des cycles possibles, on retrouve les règles des connecteurs multiplicatifs.

C'est ce passage des règles de la logique à la logique des règles qui me semble le plus emblématique du nouveau siècle.

Références

[Abrusci and Ruet, 2000] Abrusci, V. M. and Ruet, P. (2000). **Non-commutative logic I : the multiplicative fragment**. *Annals of Pure and Applied Logic*, 101 :29 – 64.

[Brouwer, 1907] Brouwer, L. E. J. (1907). **Over de grondslagen der wiskunde**. *Maas and van Suchtelen.*

[Brouwer, 1908] Brouwer, L. E. J. (1908). **De onbetrouwbaarheid der logische principes**. *Tijdschrift voor wisjbegeerte*, 2 :152 – 158.

[Burali-Forti, 1897a] Burali-Forti, C. (1897a). **Sulle classi ben ordinate**. *Rend. Circ. mat. Palermo*, 11 :260. English translation in *From Frege to Gödel*, ed. van Heijenoort, Harvard University Press, 1967.

[Burali-Forti, 1897b] Burali-Forti, C. (1897b). **Una questione sui numeri transfiniti**. *Rend. Circ. mat. Palermo*, 11 :154 – 164. English translation in *From Frege to Gödel*, ed. van Heijenoort, Harvard University Press, 1967.

[Coquand and Huet, 1988] Coquand, T. and Huet, G. (1988). **The calculus of constructions**. *Information and Computation*, 76 :95 – 120.

[Danos and Regnier, 1989] Danos, V. and Regnier, L. (1989). **The structure of multiplicatives**. *Archive for Mathematical Logic*, 28 :181 – 203.

[Ehrhard, 1995] Ehrhard, T. (1995). **Hypercoherences : a strongly stable model of linear logic**. In Girard, Lafont, and Regnier, editors, *Advances in Linear Logic*, pages 83 – 108, Cambridge. Cambridge University Press.

[Gentzen, 1969a] Gentzen, G. (1969a). **Investigations into logical deduction**. In Szabo, M. E., editor, *The collected works of Gehrard Gentzen*, pages 68 – 131, Amsterdam. North-Holland.

[Gentzen, 1969b] Gentzen, G. (1969b). **New version of the consistency proof for elementary number theory**. In Szabo, M. E., editor, *The collected works of Gehrard Gentzen*, pages 252 – 286, Amsterdam. North-Holland. SBN 7204-2254-X.

[Gentzen, 1969c] Gentzen, G. (1969c). **The consistency of elementary number theory**. In Szabo, M. E., editor, *The collected works of Gehrard Gentzen*, pages 132 – 213, Amsterdam. North-Holland.

[Girard, 1987a] Girard, J.-Y. (1987a). **Linear logic**. *Theoretical Computer Science*, 50 :1 – 102.

[Girard, 1987b] Girard, J.-Y. (1987b). **Proof-theory and logical complexity I**. Bibliopolis, Napoli.

[Girard, 1989] Girard, J.-Y. (1989). **Geometry of interaction I : interpretation of system** *F*. In Ferro, Bonotto, Valentini, and Zanardo, editors, *Logic Colloquium '88*, pages 221 – 260, Amsterdam. North-Holland.

[Girard, 1998] Girard, J.-Y. (1998). **Light Linear logic**. *Information and Computation*, 143 :175 – 204.

[Girard, 1999] Girard, J.-Y. (1999). **Coherent Banach Spaces : a continuous denotational semantics**. *Theoretical Computer Science*, 227 :275 – 297.

[Girard, 2001] Girard, J.-Y. (2001). **Locus Solum**. *Mathematical Structures in Computer Science.* Version électronique à l'URL `http ://iml.univ-mrs.fr/~girard/Articles.html`.

[Girard et al., 1990] Girard, J.-Y., Lafont, Y., and P.Taylor (1990). **Proofs and types**, volume 7 of *Cambridge tracts in theoretical computer science.* Cambridge University Press, Cambridge.

[Guerrini, 1999] Guerrini, S. (1999). **Correctness of multiplicative proof-nets is linear**. In *14th Annual IEEE Symposium on Logic in Computer Science (LICS '99*, pages 454 – 463. IEEE Computer Society Press.

[Herbrand, 1930] Herbrand, J. (1930). **Recherches sur la théorie de la démonstration**. Thèse à l'Université de Paris. English translation in *From Frege to Gödel*, ed. van Heijenoort, Harvard University Press, 1967.

[Hilbert, 1905] Hilbert, D. (1905). **Uber die Grundlagen der Logik und die Arithmetik**. *Verhandlungen des Dritten Internationalen Mathematiker-Kongresses in Heidelberg.*

[Hilbert, 1926] Hilbert, D. (1926). **Über das Unendliche**. *Mathematische Annalen*, 95 :161 – 190. English translation in *From Frege to Gödel*, ed. van Heijenoort, Harvard University Press, 1967.

[Kanovitch, 1991] Kanovitch, M. (1991). **The multiplicative fragment of linear logic is NP-complete**. Technical report, Institute for language, logic and information, Amsterdam.

[Lafont, 1990] Lafont, Y. (1990). **The linear abstract machine**. *Theoretical Computer Science*, 59 :95 – 108.

[Lafont, 1995] Lafont, Y. (1995). **From proof-nets to interaction nets**. In Girard, Lafont, and Regnier, editors, *Advances in Linear Logic*, Cambridge. Cambridge University Press.

[Lincoln et al., 1990] Lincoln, P., Mitchell, J. C., Shankar, J. C., and Scedrov, A. (1990). **Decision problems for propositional linear logic**. In *Proceedings of 31st IEEE symposium on foundations of computer science, volume 2*, pages 662 – 671. IEEE Computer Society Press.

[Russell, 1903] Russell, B. (1903). **The principles of Mathematics**, volume 1. Cambridge University Press.

[Russell, 1908] Russell, B. (1908). **Mathematical Logic as Based on the Theory of Types**. *American Journal of Mathematics*, 30 :222–262.

[Scott, 1976] Scott, D. (1976). **Data types as lattices**. *SIAM Journal of computing*, 5 :522 – 587.

[Whitehead and Russell, 1910] Whitehead, A. N. and Russell, B. (1910). **Principia Mathematica**. Cambridge University Press.

[Zermelo, 1908] Zermelo, E. (1908). **Untersuchungen über die Grundlagen der Mengenlehre I**. *Mathematiche Annalen*, 65 :261 – 281. English translation in *From Frege to Gödel*, ed. van Heijenoort, Harvard University Press, 1967.