Delphine Massenet

L'ARITHMÉTIQUE EN PRATIQUE

De la division au chiffrement de messages secrets

ellipses

Chapitre I

Les mots clefs de la logique mathématique

1 Hypothèse, proposition, proposition réciproque, contraposée, théorème

Une *hypothèse* est un énoncé supposé vrai.
Une *proposition* P est un énoncé mathématique qui a une unique valeur : vraie ou fausse.
La *négation* d'une proposition P est la proposition qui est vraie quand P est fausse. Elle se note $\neg P$ et se lit *non* P.
$P \Rightarrow Q$ est une proposition qui dit que si P est vraie, alors Q est vraie.
$\Rightarrow$ est un symbole qui signifie *implique*.
La *contraposée* de la proposition $P \Rightarrow Q$ (ou proposition contraposée) est la proposition $\neg Q \Rightarrow \neg P$.
La proposition $P \Rightarrow Q$ et sa contraposée $\neg Q \Rightarrow \neg P$ sont *équivalentes*, ce qui signifie qu'elles sont soit vraies simultanément, soit fausses simultanément.
Cela se note : $(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P)$.
$\iff$ est un symbole qui signifie : *si et seulement si*, c'est-à-dire *équivalent à*. Il exprime le fait que l'on peut intervertir hypothèse et conclusion : les implications fonctionnent dans les deux sens. Quand on écrit $P \iff Q$, cela signifie que $P \Rightarrow Q$ est vraie et que la réciproque $Q \Rightarrow P$ l'est également. Par exemple, on a, pour tout n entier : $n > 0 \iff n \geq 1$ car les implications sont vraies dans les deux sens. Si $n > 0$, alors $n \geq 1$ car n est nombre entier. Et si $n \geq 1$, alors $n > 0$ car $1 > 0$.
Quand on écrit une proposition dans l'autre sens, en inversant hypothèse et conclusion, on appelle cela une *proposition réciproque* ou *réciproque*. Ce n'est pas parce qu'une proposition est vraie que sa réciproque est vraie. Voici un exemple de proposition dont la réciproque est fausse. Si $n > 5$, alors $n > 1$ est vraie mais la réciproque : si $n > 1$, alors $n > 5$ est fausse car, par exemple, c'est faux pour $2 : 2 > 1$ mais $2 < 5$. 2 est un *contre-exemple*.

Voici un autre exemple de proposition, en français, qui ne fonctionne pas non plus dans les deux sens : « S'il pleut, alors je prends mon parapluie. » ne fonctionne pas dans l'autre sens : « Si je prends mon parapluie, alors il pleut » n'est pas toujours vraie !

2 Condition nécessaire, condition suffisante

Il y a un lien entre *implication*, *condition suffisante* et *condition nécessaire*, comme le montre la définition qui suit.

Définition 1
$P \Rightarrow Q$ se lit : si P est vraie, alors Q est vraie. On dit alors que Q est une *condition nécessaire* de P et que P est une *condition suffisante* de Q.

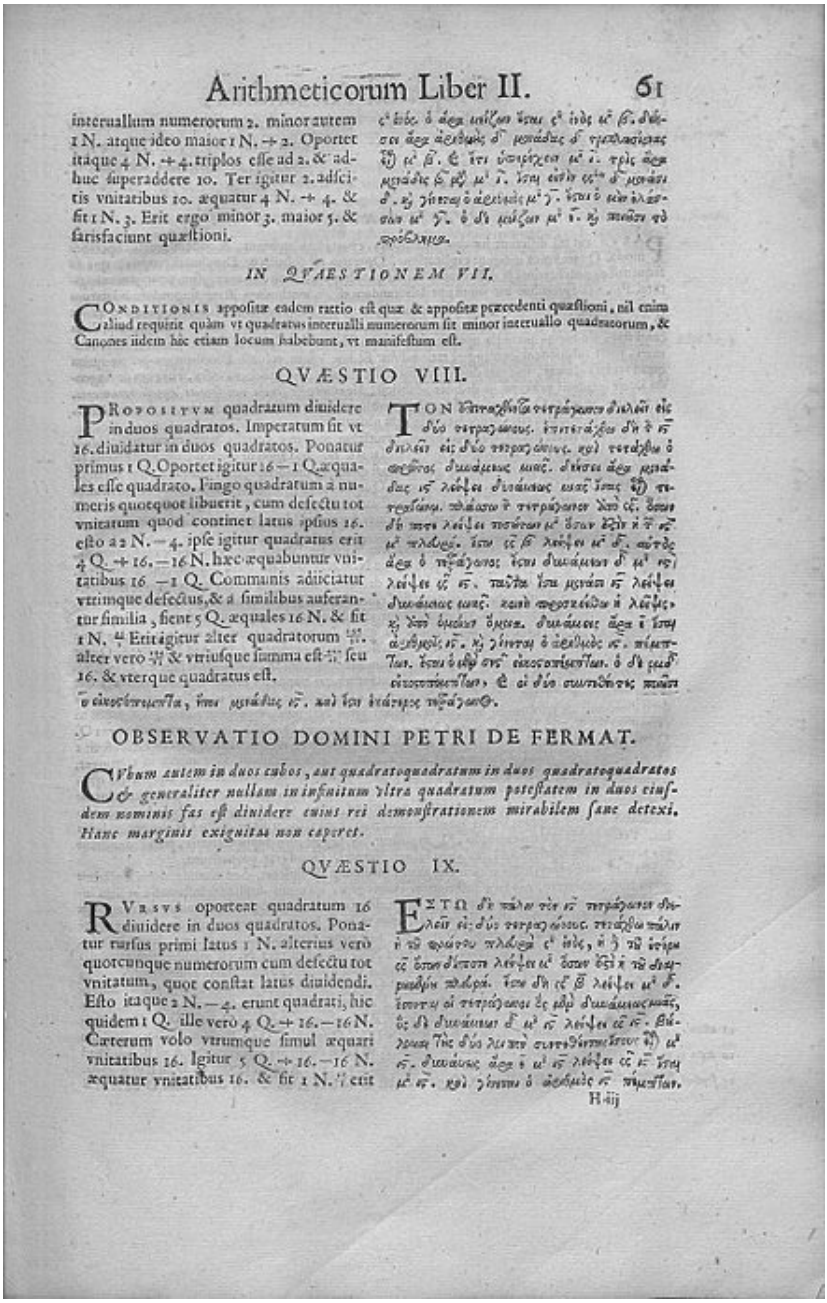
Voici un exemple non mathématique, pour illustrer cette notion : dans l'énoncé « si une personne va courir trois fois par semaine, alors elle est sportive », « elle est sportive » est une condition nécessaire. C'est une conséquence de « une personne va courir trois fois par semaine ». Ce n'est pas une condition suffisante car « elle est sportive » n'implique pas forcément la pratique de la course. Cela ne suffit pas à prouver que cette personne « va courir trois fois par semaine ». De même, dans l'énoncé « si je suis un être humain, alors je suis mortel », « je suis mortel » est une condition nécessaire de « je suis un être humain » mais ne suffit pas prouver que « je suis un être humain » car les chats, par exemple, sont aussi mortels.
Pour savoir si une condition nécessaire est suffisante, il faut inverser le sens de la proposition et regarder si l'énoncé obtenu est également vrai. Si c'est le cas, la condition est aussi une condition suffisante, sinon, ce ne l'est pas.
De même, il existe des conditions suffisantes qui ne sont pas nécessaires. Et pour savoir si une condition suffisante est nécessaire, on procède de la même manière, on inverse le sens de la proposition et on regarde si l'énoncé obtenu est vrai. Reprenons l'exemple plus haut : si $x > 5$, alors $x > 1$.
$x > 5$ est une condition suffisante de $x > 1$ mais n'en est pas une condition nécessaire car, en inversant le sens, la proposition devient : si $x > 1$, alors $x > 5$ et cet énoncé mathématique est faux car, comme nous l'avons déjà vu, 2 est supérieur à 1 mais pas à 5.
Remarquons que les définitions fonctionnent toujours dans les deux sens, puisqu'elles expriment des synonymes, mais on écrit plutôt « si » ou « quand » que « si et seulement si ». C'est une exception. Nous verrons d'autres exemples de conditions nécessaires ou suffisantes dans les exercices 7, 11, 17 du chapitre 5, et 5 du chapitre 7 .

3 Conjecture, théorème, proposition

Une *conjecture* est un énoncé dont on pense qu'il est vrai, mais sans en avoir encore la preuve. Dès qu'il est démontré, il porte le qualificatif de *théorème* ou de *proposition*, la différence entre les deux tenant à l'importance du résultat. Le mot proposition, ici, désigne un énoncé mathématique vrai. Son sens dépend donc du contexte, de pure logique, comme dans les paragraphes 1 et 2 ou de résultat.

Une célèbre conjecture maintenant prouvée

En mathématiques, un énoncé très court peut faire couler beaucoup d'encre. La démonstration de la conjecture de Pierre de Fermat (1607-1665), magistrat et mathématicien surnommé « le prince des amateurs », a été établie seulement en 1994 par Andrew Wiles (1953 -), mathématicien britannique, et comporte plus de mille pages de mathématiques.
Fermat possédait un exemplaire du livre II d'*Arithmetica*, œuvre de Diophante, mathématicien qui vivait à Alexandrie autour du III^{e} siècle après J.-C. Dans la marge du problème 8, diviser un carré en deux carrés, Fermat a écrit : « Diviser un cube en deux cubes, une puissance 4 en deux puissance 4 ou une puissance quelconque en deux puissances de même dénomination, est impossible. J'ai trouvé une démonstration de cette proposition, mais je ne peux l'écrire dans cette marge car elle est trop longue. » Etant donné les domaines mathématiques mis en jeu dans la preuve de Wiles, il semble impossible que Fermat ait pu établir cette preuve et il est très probable qu'il se soit trompé. L'énoncé de sa conjecture, en latin, figure dans le livre de Diophante qu'il a annoté (voir la figure I.1), sous le titre "OBSERVATIO DOMINI PETRI DE FERMAT".



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adsciti vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVÆSTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 — 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto 2 2 N. — 4. ipse igitur quadratus erit 4 Q. + 16. — 16 N. hæc æquabuntur vnitatibus 16 — 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{4}{5}$. Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sanè detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. — 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. — 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. — 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{4}{5}$ erit

Figure I.1 : *Arithmetica* de Diophante, réédité en 1670 par le fils de Pierre de Fermat, augmenté des annotations de son père - Livre II, problème 8, page 61.

Cette conjecture, qui est maintenant prouvée, s'appelle aujourd'hui le grand théorème de Fermat et s'énonce comme suit.

Théorème 1
(Grand théorème de Fermat)
Il n'existe pas d'entier n supérieur ou égal à 3 et d'entiers a, b et c tels que $a^n + b^n = c^n$.

4 Généralités sur les démonstrations

En mathématiques, un seul exemple, appelé contre-exemple, suffit à montrer qu'une proposition est fausse, tandis qu'il faut une démonstration générale pour montrer qu'une proposition est vraie.
Il y a des démonstrations tout au long de ce livre, qui montrent comment procéder en pratique. Elles peuvent être sautées en première lecture mais pour progresser davantage, il est nécessaire de les lire et de savoir les refaire soi-même.

5 Démonstration par récurrence

On effectue une démonstration par récurrence quand on doit montrer qu'une propriété est vérifiée pout tout nombre entier naturel n.
Il existe deux types de démonstration par récurrence.

- Dans une démonstration par récurrence dite *faible* :
  - on initialise en montrant que la propriété est vraie pour $n = 0$
  - et on montre que si elle est vraie pour l'entier n, alors elle est vraie pour $n + 1$.
- Dans une démonstration par récurrence dite *forte* :
  - on initialise en montrant que la propriété est vraie pour $n = 0$
  - et on montre que si elle est vraie pour tous les nombres inférieurs ou égaux à n, alors elle est vraie pour $n + 1$.

Remarque : si la propriété est à démontrer pour les entiers supérieurs ou égaux à un entier n_0, on effectue l'initialisation pour n_0 au lieu de 0.

Ce type de démonstration est basé sur le fait que pour obtenir tous les éléments de l'ensemble $\mathbb{N}$ (voir le rappel au chapitre 3), on ajoute 1 à 0, puis on ajoute 1 à l'entier obtenu 1, et ainsi de suite. Tous les entiers sont obtenus en ajoutant 1, de proche en proche, et il en est de même des propriétés dépendant de n.

6 Démonstration par l'absurde

Pour montrer qu'une proposition est vraie, on est parfois amené à effectuer un raisonnement par l'absurde : on suppose que la proposition est fausse et on montre qu'il y a une contradiction avec un des éléments dont on dispose, une absurdité. Ce procédé porte le nom de *démonstration par l'absurde*.

Chapitre II

Rappels sur les techniques de calcul

Tout au long de ce livre, vous allez avoir besoin de quelques techniques de calcul, que je rappelle ici.

1 Calcul littéral

Le *calcul littéral* est le calcul d'expressions mathématiques comportant des lettres. Une lettre représente un nombre.
La *factorisation* et le *développement* sont appris au collège.

Définition 1
Factoriser, c'est transformer une somme en un produit. Et *développer*, c'est transformer un produit en une somme.

1.1 Simple développement

Proposition 1
Soient k, a et b des nombres.

$$k\,a + k\,b = k\,(a + b)$$

Dans l'expression $k\,a + k\,b$, k est appelé le *facteur commun*.
Quand on écrit l'expression $k\,(a + b)$, on dit qu'on a *factorisé* ou qu'*on a mis k en facteur*.
En lisant cette égalité de droite à gauche, on *développe* :

$$k\,(a + b) = k\,a + k\,b$$

$k\,(a+b)$ signifie $k \times (a+b)$, $k\,a$ et $k\,b$ signifient $k \times a$ et $k \times b$. On omet le $\times$ pour alléger les notations.
Ici, c'est du *simple développement* car il n'y a que k à gauche de $(a+b)$.

Définition 2
Réduire une expression, c'est calculer tout ce que l'on peut pour qu'elle soit la plus courte possible.

Par exemple, s'il y a plusieurs termes avec x, on met x en facteur et on termine le calcul :
$2x + 3 - 5x - 1 + 12x = (2 - 5 + 12)x + 3 - 1 = 9x + 2$

Interprétation géométrique
Cette formule s'explique, pour des nombres positifs, grâce à la géométrie (voir la figure II.1).
L'aire d'un rectangle est *largeur* $\times$ *longueur*.
Considérons le grand rectangle ci-dessous. Sa largeur est k et sa longueur est $a+b$. Son aire vaut : $k\,(a+b)$. Ce rectangle peut être divisé en deux rectangles d'aires $k \times a$ et $k \times b$. On a donc : $k\,(a+b) = k\,a + k\,b$.

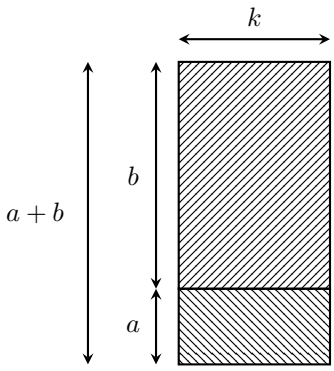


Figure II.1 : Simple développement et aires de rectangles

Exemple : Factorisons les expressions suivantes.
$A = 2x + 7x$: quand on cherche à factoriser, on peut lire à voix haute. Ici, on entend deux fois x : c'est donc x que l'on va mettre en facteur.
$A = (2+7)x = 9x$
On met toujours en facteur le plus d'expressions communes possibles.
Par exemple, $B = 2x - 4x^2 = 2x \times 1 - 2x \times 2x = 2x(1 - 2x)$
$C = 7x - 3x + 5x + 4 - 2x$. On met x en facteur. $C = (7-3+5-2)x + 4 = 7x + 4$
$D = 3a + 5 - 2b + 4a - 3b$. On met a et b en facteur.
$D = (3+4)a + 5 + (-2-3)b = 7a + 5 - 5b = 7a - 5b + 5$
$E = 3x^2 - 7x^2 + 8x^2$. On met x^2 en facteur.