Chapitre I

Rudiments de logique et théorie naïve des ensembles

Si la mathématique repose sur la logique et la théorie des ensembles, il semble difficile de commencer un cours de base avec des notions issues de ces disciplines : l'abstraction dont il faut faire preuve pour les aborder rebuterait plus d'un novice. Heureusement, tout un chacun possède un minimum de sens logique. Nous ne ferons ici que donner quelques rappels afin de familiariser le lecteur avec nos conventions. En ce qui concerne la théorie des ensembles proprement dite, nous ne ferons qu'effleurer le sujet. Les développements donnés ici sont largement suffisants pour une première approche et sont proches des idées intuitives des mathématiciens du XIX^e siècle. Il est toutefois à noter que cette manière de voir les choses n'est pas mathématiquement correcte, comme nous l'évoquerons. Elle ne donne cependant aucune mauvaise habitude, ce qui fait que nous adopterons cette approche sans hésitation. Le lecteur intéressé par la logique pourra, par exemple, consulter [22, 5, 6, 17] ; en ce qui concerne la théorie des ensembles, [3, 4, 11, 13, 14] sont des références communes.

I.1 Logique

Toute théorie mathématique est basée sur des axiomes : ce sont des formulations de propriétés jugées comme évidentes concernant des objets auxquels on désire appliquer les mathématiques. Une manière, certainement restrictive, d'aborder une théorie mathématique consiste en la voir comme une collection d'objets mathématiques et de relations vraies entre ces objets. Les objets mathématiques sont par exemple les nombres, les fonctions, *et cætera*. Les relations sont des assertions (qui peuvent être vraies ou fausses) que l'on peut formuler entre ces objets. Les vraies, appelées théorèmes, sont celles qu'on démontre, c'est-à-dire que l'on déduit logiquement d'un certain nombre d'axiomes.

I.1.1 Quelques locutions et symboles

Nous allons nous contenter ici d'introduire le vocabulaire de base de la logique mathématique, ainsi que les règles basiques concernant son utilisation.

Une *relation* entre objets mathématiques est une propriété, vérifiée ou pas, entre certains de ces objets. Un exemple de relation est « 5 est strictement inférieur à 6 » ; cette relation est vraie. Par contre, la relation « 5 est strictement inférieur à 5 » est fausse.

Le principe de *non-contradiction*[1] affirme qu'une relation ne peut être vraie et fausse à la fois. Le principe du *tiers exclu*[2] affirme quant à lui que si une relation n'est pas vraie, alors elle est fausse et que si une relation n'est pas fausse, alors elle est vraie.

À partir de deux relations R et S, on peut en définir de nouvelles.

— La *négation* de R est désignée par $\neg R$. Une relation est fausse si sa négation est vraie ; elle est vraie si sa négation est fausse.

— La relation « R ou S », souvent notée $R \vee S$, est une relation vraie si l'une au moins des relations R, S est vraie. Il convient donc de remarquer que le « ou mathématique » est toujours pris au sens non disjonctif : si R et S sont vrais, alors $R \vee S$ est vrai.

D'autres méthodes de construction peuvent être introduites à partir des précédentes :

— La relation « R et S », souvent notée $R \wedge S$, est une relation vraie si les deux relations R, S sont vraies. En fait $R \wedge S$ est défini comme suit :

$$\neg(\neg R \vee \neg S),$$

où, comme à l'accoutumée, les parenthèses servent à indiquer la priorité des opérations.

— La relation « R implique S », notée $R \Rightarrow S$, est la relation

$$S \vee \neg R.$$

— Enfin, la relation « R si et seulement si S », notée $R \Leftrightarrow S$, est la relation

$$(R \Rightarrow S) \wedge (S \Rightarrow R).$$

Deux relations R et S sont *logiquement équivalentes* si elles sont simultanément vraies et simultanément fausses, c'est-à-dire si la relation $R \Leftrightarrow S$ est vraie. On peut exprimer que deux relations R et S sont logiquement équivalentes en affirmant que l'on a :

— R si et seulement si S (noté $R \Leftrightarrow S$ ou R ssi S),

— pour que R, il faut et il suffit que S,

— une condition nécessaire et suffisante pour que R est S,

— R équivaut à S (noté $R \equiv S$).

---

1. Ce principe n'est pas toujours vérifié dans la vie courante. Ainsi, le *paradoxe du menteur*, cité par Paul de Tarse, en est-il un exemple : Épiménide, un crétois, dit : « tous les Crétois sont des menteurs ». S'il dit la vérité, Épiménide ment puisqu'il est crétois. A contrario, s'il ment, il dit effectivement la vérité. Il s'agit d'une relation contradictoire.

2. Selon David Hilbert, « priver le mathématicien du *tertium non datur* serait enlever son télescope à l'astronome, son poing au boxeur ».

Dans un théorème, lorsqu'on peut lire $R \Leftrightarrow S$, il faut comprendre que les relations R et S sont logiquement équivalente.

Remarque. Nous ne ferons pas la distinction entre l'« équivalence » et le « si et seulement si ». Bornons-nous à dire qu'en logique, la relation d'équivalence est en général notée « $\equiv$ », la notation « $\Leftrightarrow$ » étant plutôt réservée aux connecteurs.

Donnons deux exemples.

Exemples I.1.1. Soit R et S deux relations.
- Si R est la relation « 5 est strictement inférieur à 6 » et S est la relation « 5 est égal à 6 », la relation $R \vee S$ est la relation « 5 est inférieur ou égal à 6 »,
- si R est la relation « x est un multiple de deux » et S est la relation « x est un multiple de trois », la relation $R \wedge S$ est la relation « x est un multiple de six ».

I.1.2 Tables de vérité

Les tables de vérités facilitent la comparaison de relations.

Une *table de vérité* permet de comparer deux relations. On considère d'abord les relations de base comme des variables, qui peuvent prendre soit la valeur « vraie », soit la valeur « fausse » ; une table de vérité contient une colonne par relation, les lignes reflétant toutes les occurrences possibles des variables. La dernière colonne représente les valeurs de la relation construite à partir des relations de base en fonction des valeurs possibles de ces relations. Par exemple, la table de vérité du « et » logique est la suivante :

R	S	$R \wedge S$
v	v	v
v	f	f
f	v	f
f	f	f

,

ce qui permet de constater que $R \wedge S$ est vrai si et seulement si R et S sont simultanément vrais. Il est parfois utile d'insérer des colonnes intermédiaires.

Deux expressions sont équivalentes si elles ont la même table de vérité. À titre d'application, montrons que $R \Rightarrow (S \vee T)$ est équivalent à $\neg T \Rightarrow (\neg R \vee S)$. De fait, on a

R	S	T	$S \vee T$	$R \Rightarrow (S \vee T)$
v	v	v	v	v
v	v	f	v	v
v	f	v	v	v
v	f	f	f	f
f	v	v	v	v
f	v	f	v	v
f	f	v	v	v
f	f	f	f	v

et

R	S	T	$\neg T$	$\neg R \vee S$	$\neg T \Rightarrow (\neg R \vee S)$
v	v	v	f	v	v
v	v	f	v	v	v
v	f	v	f	f	v
v	f	f	v	f	f
f	v	v	f	v	v
f	v	f	v	v	v
f	f	v	f	v	v
f	f	f	v	v	v

,

ce qui suffit, les dernières colonnes présentant les mêmes valeurs.

Exercice I.1.2. Montrer que l'expression $\neg(R \wedge S)$ est équivalente à $\neg R \vee \neg S$.

Exercice I.1.3. Montrer que l'expression $\neg(R \vee S)$ est équivalente à $\neg R \wedge \neg S$.

Exercice I.1.4. Montrer que l'expression $R \Rightarrow S$ est équivalente à $\neg S \Rightarrow \neg R$.

Exercice I.1.5. Montrer que l'expression R est équivalente à $\neg R \Rightarrow (S \wedge \neg S)$.

Exercice I.1.6. Montrer que l'expression $\neg(R \Rightarrow S)$ est équivalente à $R \wedge \neg S$.

Exercice I.1.7. Montrer que l'expression $R \Rightarrow (S \vee T)$ est équivalente à $(R \wedge \neg S) \Rightarrow T$ et $(R \wedge \neg T) \Rightarrow S$.

Exercice I.1.8. Montrer que l'expression $(R \vee S) \Rightarrow T$ est équivalente à l'expression $(R \Rightarrow T) \wedge (S \Rightarrow T)$.

I.1.3 Types de démonstration

Une *démonstration* est un raisonnement permettant (à partir d'axiomes) d'établir qu'une relation est vraie. Une démonstration repose sur la logique mais utilise également des éléments de langage naturel, en essayant d'éviter toute ambiguïté. Une relation démontrée est un *théorème*. Une fois démontré, un théorème peut être utilisé pour démontrer la véracité d'autres relations. Une relation qui est tenue pour vraie mais qui n'a pas encore été démontrée est appelée une *conjecture*.

La *démonstration directe* consiste à démontrer une relation en partant des hypothèses pour arriver à la conclusion par une suite d'implications logiques.

Exemple I.1.9. Pour tout nombre naturel[3] n, considérons le nombre

$$P(n) = n^2 + 7n + 12$$

et montrons qu'il n'existe pas de nombre naturel n tel que $\sqrt{P(n)}$ soit un nombre naturel. De fait, on a toujours

$$n^2 + 6n + 9 < n^2 + 7n + 12 < n^2 + 8n + 16,$$

3. On parle aussi d'entier naturel, c'est-à-dire un nombre entier positif ou nul.

pour tout nombre naturel n, de sorte que l'on a

$$(n+3)^2 < P(n) < (n+4)^2,$$

pour tout nombre naturel n. Il vient alors

$$n+3 < \sqrt{P(n)} < n+4.$$

Ainsi, $\sqrt{P(n)}$ est toujours strictement compris entre deux nombres naturels consécutifs, ce qui suffit.

Exercice I.1.10. Montrer que pour tout nombre naturel n, on a

$$1+2+\cdots+n = \frac{n(n+1)}{2}$$

(*suggestion* : poser $S = 1+\cdots+n$ et considérer le nombre $2S$).

Exercice I.1.11. Montrer que si p/q et p'/q' sont deux nombres rationnels égaux, alors on a

$$\frac{p+p'}{q+q'} = \frac{p}{q} = \frac{p'}{q'}.$$

Suggestion. De fait, on a

$$\begin{aligned}\frac{p+p'}{q+q'} = \frac{p}{q} &\Leftrightarrow (p+p')q = p(q+q')\\ &\Leftrightarrow (pq)+(p'q) = (pq)+(pq')\\ &\Leftrightarrow p'q = pq'\\ &\Leftrightarrow \frac{p'}{q'} = \frac{p}{q},\end{aligned}$$

ce qui suffit.

Pour une *démonstration par la contraposée*, on cherche à prouver la relation $R \Rightarrow S$ en prouvant la relation équivalente $\neg S \Rightarrow \neg R$.

Exemple I.1.12. Montrons que, pour tout nombre naturel n, si n^2 est impair, alors n l'est également. Il suffit de prouver que si n est pair (non-impair), alors n^2 l'est également. De fait, si n est pair, il s'écrit $n = 2m$ pour un nombre naturel m. Il vient alors $n^2 = 4m^2 = 2(2m^2)$, ce qui permet de conclure.

Exercice I.1.13. Montrer que si x est un nombre réel tel que $x^3+x^2-2x < 0$, alors on a $x < 1$.

Exercice I.1.14. Montrer que si x et y sont deux nombres réels tels que $x+y$ est irrationnel, alors x ou y est irrationnel[4].

Pour une *démonstration par l'absurde*, on suppose que la relation à démontrer est fausse et on montre que l'on aboutit nécessairement à une contradiction.

4. L'ensemble des nombres rationnels forme un corps commutatif.

Exemple I.1.15. Montrons que le nombre $\sqrt{2}$ n'est pas rationnel ; autrement dit, il n'existe pas deux nombres naturels non nuls p et q tels que $\sqrt{2} = p/q$. Supposons que $\sqrt{2}$ est un nombre rationnel ; il existe donc deux nombres naturels non nuls m et n tels que $\sqrt{2} = m/n$. Soit p et q deux nombres naturels non nuls premiers entre eux tels que $\sqrt{2} = p/q$; *i.e.* on choisit p et q tels que q soit le plus petit des nombres naturels satisfaisant la relation précédente. Ainsi on a $(p/q)^2 = 2$ et donc $p^2 = 2q^2$. Il s'ensuit que p^2 est pair, ce qui est équivalent à affirmer que p est pair. Il existe donc un nombre naturel non nul p' tel que $p = 2p'$. Par conséquent, on obtient la relation $4p'^2 = 2q^2$, c'est-à-dire $2p'^2 = q^2$. Ceci montre que q est pair ; il existe ainsi un nombre naturel non nul q' tel que $q = 2q'$. On a ainsi montré la relation $p/q = p'/q'$, avec $q' < q$, ce qui contredit la minimalité de q.

Exercice I.1.16. Montrer que le nombre $\sqrt{3}$ n'est pas rationnel.

Exercice I.1.17. Montrer qu'il existe un nombre infini de nombres premiers [5].

Suggestion. Si n est un nombre naturel et $p_1, \dots, p_n$ sont tous les nombres premiers, soit m le produit de ces nombres. Bien entendu, $m+1$ ne peut être premier ; de plus, ce nombre n'est divisible par aucun nombre premier. De fait, s'il existait un nombre naturel d tel que $m + 1 = dp_1$, on pourrait écrire

$$1 = p_1(d - p_2 \cdots p_n),$$

ce qui est absurde. Soit q le plus petit diviseur de $m + 1$ strictement supérieur à un. Tout diviseur de q étant un diviseur de $m + 1$, q est nécessairement premier. Cependant, par définition de $m+1$, q est différent de p_j quel que soit j $(1 \leqslant j \leqslant n)$.

On peut cependant modifier cette démonstration pour en faire une démonstration directe.

Remarque I.1.18. En modifiant légèrement la démonstration de l'exercice précédent, on peut montrer que $m + 1$ est un nombre premier ; il ne peut par conséquent y avoir de plus grand nombre premier. Qui plus est, la preuve d'Euclide permet de montrer que le n-ième nombre premier est inférieur ou égal à 2^{2^n} [20].

La *démonstration par récurrence* ou *par induction* repose sur le principe suivant. Soit $R(k)$ une relation dépendant du nombre entier k. Si l'assertion $R(k_0)$ est vraie pour le nombre entier k_0 (ancrage) et si l'implication $R(k) \Rightarrow R(k+1)$ est vraie pour chaque nombre entier k tel que $k \geqslant k_0$ (hérédité), alors l'assertion $R(k)$ est vraie pour tout $k \geqslant k_0$. Une démonstration par récurrence peut donc toujours être décomposée en deux étapes : le cas de base, où l'on montre que $R(k_0)$ est vrai (initialisation) et la récurrence proprement dite, où l'on démontre que si $R(k)$ est vrai avec $k \geqslant k_0$ (hypothèse de récurrence), alors $R(k + 1)$ l'est également.

Exemple I.1.19. Démontrons l'*inégalité de Bernoulli* : pour tout nombre x tel que $x \geqslant -1$ et tout nombre naturel non nul n, on a $(1 + x)^n \geqslant 1 + nx$. Soit $R(n)$ la relation $(1+x)^n \geqslant 1+nx$. L'assertion $R(1)$ est trivialement vraie. Si la relation $R(n)$

5. Il s'agit du théorème d'Euclide sur les nombres premiers.

est vraie, on a

$$\begin{aligned}(1+x)^{n+1} &= (1+x)(1+x)^n \\ &\geqslant (1+x)(1+nx) \\ &= 1+(n+1)x+nx^2 \\ &\geqslant 1+(n+1)x,\end{aligned}$$

ce qui prouve que $R(n+1)$ est vrai.

Exercice I.1.20. Montrer que pour tout nombre naturel n, on a

$$1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Exercice I.1.21. Montrer que pour tous nombres naturels $n \geqslant 2$ et $j \neq 0$, on a

$$\frac{1}{n}+\frac{1}{n^2}+\cdots+\frac{1}{n^j} = \frac{1}{1-1/n}\left(\frac{1}{n}-\frac{1}{n^{j+1}}\right).$$

Suggestion. On a bien entendu

$$\frac{1}{1-1/n}\left(\frac{1}{n}-\frac{1}{n^2}\right) = \frac{1}{1-1/n}\,\frac{1}{n}\left(1-\frac{1}{n}\right) = \frac{1}{n-1}\,\frac{n-1}{n} = \frac{1}{n},$$

ce qui prouve que la formule est vraie pour $j=1$. Si la formule a été vérifiée pour $1,\ldots,j$, il vient

$$\begin{aligned}\frac{1}{n}+\frac{1}{n^2}+\cdots+\frac{1}{n^j}+\frac{1}{n^{j+1}} &= \frac{1}{1-1/n}\left(\frac{1}{n}-\frac{1}{n^{j+1}}\right)+\frac{1}{n^{j+1}} \\ &= \frac{1}{n-1}\left(1-\frac{1}{n^j}\right)+\frac{1}{n-1}\,\frac{n-1}{n^{j+1}} \\ &= \frac{1}{n-1}\left(1-\frac{1}{n^j}+\frac{n-1}{n^{j+1}}\right) \\ &= \frac{1}{n-1}\left(1-\frac{1}{n^{j+1}}\right) = \frac{1}{1-1/n}\left(\frac{1}{n}+\frac{1}{n^{j+2}}\right),\end{aligned}$$

ce qui permet de conclure par récurrence.

Exercice I.1.22. Montrer que pour tout nombre naturel n, $n(n+1)(n+2)$ est divisible par 6.

Exercice I.1.23. Montrer que pour tout nombre naturel n, 7^n+2 est divisible par 3.

Exercice I.1.24. Montrer que pour tout nombre naturel n, n^5-n est un multiple de 5.

Remarque I.1.25. Logiquement, l'exercice I.1.4 justifie la technique de démonstration par contraposition et l'exercice I.1.5 la démonstration par l'absurde. L'exercice I.1.8 permet quant à lui de simplifier une démonstration par disjonction des cas. L'exercice I.1.6 permet de montrer qu'une relation est fausse en fournissant un contre-exemple. Enfin, l'exercice I.1.7 permet éventuellement de modifier l'énoncé du théorème à démontrer. La technique de démonstration par récurrence repose sur une propriété des nombres naturels [18].

I.1.4 Une application : le binôme de Newton

Comme application, nous allons introduire la fonction factorielle, les coefficients binomiaux et la formule du binôme de Newton.

Si f est une fonction[6] définie sur les nombres entiers $m, m+1, \ldots, n$, on écrit $\sum_{j=m}^{n} f(j)$ pour représenter l'expression

$$\sum_{j=m}^{n} f(j) = f(m) + f(m+1) + \cdots + f(n).$$

Bien entendu, on a $\sum_{j=m}^{n} f(j) = \sum_{k=m}^{n} f(k)$. Pour une définition rigoureuse, on peut poser $\sum_{j=m}^{m} f(j) = f(m)$ et, si $\sum_{j=m}^{k} f(j)$ a été défini,

$$\sum_{j=m}^{k+1} f(j) = f(k+1) + \sum_{j=m}^{k} f(j).$$

De même, on introduit

$$\prod_{j=m}^{n} f(j) = f(m)f(m+1)\cdots f(n).$$

On pose $0! = 1$ et

$$(j+1)! = (j+1)j! = \cdots = (j+1)j(j-1)\cdots 2 \cdot 1,$$

pour tout nombre naturel j. Le nombre $j!$ est appelé[7] la *factorielle*[8] de j.

Remarque I.1.26. Étant donné un nombre naturel j, $j!$ représente le nombre de manières de permuter les éléments d'un ensemble de taille j. En effet, étant donné j éléments $a_1, \ldots, a_j$, on peut choisir un premier élément de j façons différentes (on sélectionne donc un élément a_k, avec $1 \leqslant j \leqslant k$). Ensuite, un élément ayant déjà été choisi, il reste à choisir parmi les $j-1$ éléments restants. Ainsi, à l'étape k, il reste le choix entre $j-k+1$ éléments. Au total, on a bien

$$j(j-1)\cdots 2 \cdot 1 = j!$$

permutations possibles.

Étant donné deux nombres naturels n et j tels que $n \geqslant j$, le *coefficient binomial* $\binom{n}{j}$ (parfois noté[9] C_n^j dans d'anciens ouvrages francophones) est le nombre

$$\binom{n}{j} = \frac{n!}{j!(n-j)!}.$$

6. On peut pour l'instant voir $f(j)$ comme une expression mathématique dépendant de j et faisant intervenir des nombres et des opérations.

7. Cette notation a été introduite en 1808 par Christian Kramp.

8. Il s'agit d'une fonction : $\mathbb{N} \to \mathbb{N} \quad j \mapsto j!$.

9. Nous privilégions systématiquement les notations préconisées par une norme ISO. La notation pour le coefficient binomial en pays francophones a changé il y a quelques années pour s'adapter à la norme anglo-saxonne préconisée par la norme ISO 31.