Raisonnement mathématique

Septembre 2019 - v1 - non relue sérieusement

La notion de preuve (appelée aussi démonstration) est centrale en mathématiques : un théorème est un énoncé mathématique qui admet une preuve. Un étudiant en mathématiques doit être capable de produire des preuves, ne serait-ce que parce que c'est ce qui lui est demandé dans quasiment tous les exercices. Pour cela, il doit être capable de vérifier lui-même si ce qu'il produit est ou non une preuve. Pour cette vérification, il doit avoir au moins une compréhension pragmatique de ce qu'est une preuve.

L'objectif de ces notes est de rassembler quelques éléments pour aider les étudiants à acquérir cette compréhension pragmatique. Ce n'est ni un cours de logique ni un cours de théorie de la démonstration. En particulier, je ne définirai pas ce qu'est une preuve. Le critère pragmatique suivant me semble suffisant : vous détenez une preuve (sauf erreur d'inattention) lorsque vous n'avez plus aucun doute sur aucune étape de votre raisonnement (que ce soit sur la définition d'un objet, le sens d'une phrase, un enchaînement, ...).

Cette version est préliminaire. Merci pour toute remarque ou correction !

1 Présentation naïve de la logique

1.1 Assertions

Vocabulaire. Une assertion est un énoncé mathématique qui est vrai ou faux.

Remarques. Je n'ai pas écrit « définition » car ce n'est pas une définition : c'est beaucoup trop vague ! Des subtilités sont par ailleurs cachées. J'en cache quelques autres plus loin. Je rappelle que j'adopte un point de vue pragmatique. Les exemples qui suivent seront sans doute plus éclairants.

Premiers exemples.

- P : « $0 = 1$ ». L'assertion P est fausse.
- Q : « $(4+5)^2 \leq 100$ ». L'assertion Q est vraie.
- R : « $\{1,2\} \cap \{2,3\} \subset \{2,4\}$ ». L'assertion R est vraie.

D'un point de vue pratique, on demande ainsi à une assertion d'avoir un sens mathématique et d'être vraie ou fausse.

1.2 Connecteurs

Les connecteurs permettent de construire de nouvelles assertions à partir d'assertions données.

1.2.1 Non : connecteur de négation

Si P est une assertion, on définit une nouvelle assertion notée (non P) de la manière suivante :

- Lorsque P est vraie, (non P) est fausse.
- Lorsque P est fausse, (non P) est vraie.

Par exemple « (non $(0 = 1)$) » est vraie.

1.2.2 ... et ... : connecteur de conjonction

Si P et Q sont deux assertions, on définit une nouvelle assertion notée (P et Q) de la manière suivante :

- Lorsque P et Q sont vraies, (P et Q) est vraie.
- Dans tous les autres cas, (P et Q) est fausse.

On résume souvent cela sous la forme d'une table de vérité :

P	Q	P et Q
V	V	V
V	F	F
F	V	F
F	F	F

Les quatre dernières lignes correspondent aux quatre cas possibles. L'avant dernière ligne indique par exemple que, lorsque P est fausse et Q est vraie, l'assertion (P et Q) est fausse.

1.2.3 ... ou ... : connecteur de disjonction

Si P et Q sont deux assertions, on définit une nouvelle assertion notée (P ou Q) que je décris par sa table de vérité :

P	Q	P ou Q
V	V	V
V	F	V
F	V	V
F	F	F

Remarques. Ce n'est pas un « ou exclusif ».

1.2.4 Si ... alors ... : connecteur d'implication

Si P et Q sont deux assertions, on définit une nouvelle assertion notée ($P \Rightarrow Q$) qui se lit « P implique Q » ou « si P alors Q ». Je la décris par sa table de vérité :

P	Q	$P \Rightarrow Q$
V	V	V
V	F	F
F	V	V
F	F	V

Remarque.

- $(P \Rightarrow Q)$ est en particulier vraie lorsque P est fausse.
- Quand on affirme que $(P \Rightarrow Q)$ est vraie, on n'affirme pas que P est vraie, on n'affirme pas que Q est vraie et on n'affirme pas non plus qu'il y a un lien de causalité (ou de temporalité ou autre) entre P et Q.
- $(P \Rightarrow Q)$ peut être vraie sans que $(Q \Rightarrow P)$ soit vraie.
- Le connecteur d'implication n'est a priori pas plus compliqué que les connecteurs « et » et « ou » : il y a quatre cas pour les valeurs de vérité de P et de Q ; $(P \Rightarrow Q)$ prend une certaine valeur dans chacun de ces cas. Un étudiant qui fait l'effort d'étudier la définition et de l'utiliser ne devrait donc pas avoir de difficultés. L'expérience montre cependant que ce connecteur pose plus de problèmes que les autres aux étudiants :
  - Peut-être parce que certains ont une idée a priori sur le sens que devrait avoir un connecteur appelé « implication » et « si ... alors ... », que ce sens ne correspond pas à celui donné en mathématiques et qu'ils refusent d'utiliser le sens mathématique quand ils font des mathématiques.
  - Peut-être parce que certains confondent l'assertion $(P \Rightarrow Q)$ avec le bout de preuve « P est vraie donc Q est vraie » qui n'est pas du tout la même chose (voir plus loin le sens de « donc » dans une preuve en mathématiques).
  - Peut-être parce que certains pensent que, pour montrer $(P \Rightarrow Q)$, il faut nécessairement « prouver Q en supposant P ». Dans les exemples ci-dessous, il suffit pourtant d'obtenir la valeur de vérité de P et de Q et de lire le résultat dans la table de vérité ci-dessus.

Exemples. Les valeurs de vérité de ces implications se lisent sur la table de vérité ci-dessus (il suffit de regarder dans quel cas nous nous trouvons).

- « $(0 = 1) \Rightarrow (\{1, 2, 3, 4\} \subset \{1, 2\})$ » est vraie.
- « $(0 = 1) \Rightarrow (\{1\} \subset \{1, 2, 3\})$ » est vraie.
- « $(\{1\} \subset \{1, 2, 3\}) \Rightarrow (0 = 1)$ » est fausse.

1.2.5 ... si et seulement si ... : connecteur d'équivalence

Si P et Q sont deux assertions, on définit une nouvelle assertion notée $(P \Leftrightarrow Q)$ qui se lit « P est équivalent à Q » ou « P si seulement si Q ». Je la décris par sa table de vérité :

P	Q	$P \Leftrightarrow Q$
V	V	V
V	F	F
F	V	F
F	F	V

Autrement dit : $(P \Leftrightarrow Q)$ est vraie exactement lorsque P et Q ont la même valeur de vérité.

1.3 Assertions tautologiquement équivalentes

Considérons l'exemple suivant. Si P et Q sont deux assertions, alors

$$P \Rightarrow Q$$

et

$$Q \text{ ou } (\text{non } P)$$

sont deux nouvelles assertions. Dressons leur table de vérité :

P	Q	$P \Rightarrow Q$	Q ou (non P)
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

On constate qu'elles ont toujours la même valeur de vérité, quelles que soient les valeurs de vérité de P et Q. On dit dans ce cas que l'assertion $(P \Rightarrow Q)$ et l'assertion $(Q$ ou (non $P))$ sont tautologiquement équivalentes. On note cela ainsi :

$$(P \Rightarrow Q) \equiv (Q \text{ ou } (\text{non } P)).$$

Des assertions peuvent être composées de trois assertions ou davantage, comme par exemple $(P$ ou $(Q \Rightarrow R))$ qui est composée de P, Q et R[1]. Pour deux telles assertions, on dit similairement qu'elles sont tautologiquement équivalentes lorsqu'elles ont toujours la même valeur de vérité, quelles que soient les valeurs de vérité des assertions qui les composent.

Exemples importants. Voici quelques équivalences tautologiques, dans lesquelles P, Q et R sont des assertions :

1. $P \equiv$ (non (non P)).
2. $(P$ et $Q) \equiv (Q$ et $P)$.
3. $(P$ ou $Q) \equiv (Q$ ou $P)$.
4. $((P$ et $Q)$ et $R) \equiv (P$ et $(Q$ et $R))$.
5. $((P$ ou $Q)$ ou $R) \equiv (P$ ou $(Q$ ou $R))$.
6. $(P \Rightarrow Q) \equiv$ ((non P) ou Q).
7. $(P \Leftrightarrow Q) \equiv ((P \Rightarrow Q)$ et $(Q \Rightarrow P))$.
8. (non $(P$ et $Q)) \equiv$ ((non P) ou (non Q)).
9. (non $(P$ ou $Q)) \equiv$ ((non P) et (non Q)).
10. (non $(P \Rightarrow Q)) \equiv (P$ et (non Q)).
11. $(P \Rightarrow Q) \equiv$ ((non Q) $\Rightarrow$ (non P)).

Toutes ces équivalences tautologiques sont importantes pour bâtir des preuves. Ils est important d'y réfléchir calmement jusqu'à les trouver intuitives. Vérifier qu'elles sont vraies peut par contre se faire de manière mécanique en dressant simplement les tables de vérité.

1.4 Prédicats

Vocabulaire. Un prédicat est un énoncé dépendant de variables tel que, si on remplace ces variables par des éléments d'un certain ensemble[2], on obtienne une assertion.

Remarque. Un prédicat est ainsi un énoncé dont la valeur de vérité peut dépendre de la valeur de certaines variables. Une nouvelle fois, c'est très vague, ce n'est que du vocabulaire et mieux vaut sans doute considérer des exemples.

1. Elle est aussi composée de P et $(Q \Rightarrow R)$.
2. Il est trop restrictif de se limiter à des ensembles, mais je cache également cette subtilité.

Exemples.

- Le prédicat $A(n)$ défini par « n est pair » où n est un entier positif. C'est un prédicat à une variable, n, représentant un élément de l'ensemble des entiers positifs. Si on remplace n par l'entier positif 2 on obtient l'assertion $A(2)$: « 2 est pair ». Si on remplace n par l'entier positif 3 on obtient l'assertion $A(3)$: « 3 est pair ». On note que l'assertion $A(2)$ est vraie tandis que l'assertion $A(3)$ est fausse.
- Le prédicat $B(x, y)$ défini par « $(x+y)^2 = x^2+2xy+y^2$ » où x et y sont des nombres réels. C'est un prédicat à deux variables, x et y, représentant chacune un élément de l'ensemble des nombres réels. Si on remplace x par le réel 3 et y par le réel 5 on obtient l'assertion $B(3, 5)$: « $(3 + 5)^2 = 3^2 + 2 * 3 * 5 + 5^2$ ». Si on remplace x par le réel -1 et y par le réel 2 on obtient l'assertion $B(-1, 2)$: « $(-1 + 2)^2 = (-1)^2 + 2 * (-1) * 2 + 2^2$ ». On note que ces deux assertions sont vraies. D'ailleurs, on obtient une assertion vraie quel que soit le choix que l'on fait pour le réel x et le réel y.

1.5 Quantificateurs et prédicats à une variable

Si $A(x)$ est un prédicat à une variable x représentant un élément d'un ensemble E, on lui associe les deux assertions suivantes :

- L'assertion « l'assertion $A(x)$ est vraie pour tout élément x de l'ensemble E ». Elle se note : $\forall x \in E,\ A(x)$.
- L'assertion « l'assertion $A(x)$ est vraie pour au moins un élément x de l'ensemble E ». Elle se note : $\exists x \in E,\ A(x)$.

Le symbole $\forall$ est appelé quantificateur universel. Le symbole $\exists$ est appelé quantificateur existentiel.

Exemples. La valeur de vérité de ces assertions est, je l'espère, intuitivement claire. Les preuves sont-elles simples ?

- L'assertion « $\forall n \in \mathbb{N}$, n est un entier pair » est fausse.
- L'assertion « $\exists n \in \mathbb{N}$, n est un entier pair » est vraie.

Remarques.

- Les assertions « $\forall x \in E,\ A(x)$ » et « $\exists x \in E,\ A(x)$ » ne dépendent pas de x.
- L'assertion « $\forall x \in E,\ A(x)$ » peut également s'écrire par exemple « $\forall y \in E,\ A(y)$ ».

Négation. Réfléchir aux équivalences tautologiques suivantes jusqu'à les trouver intuitives.

- non $(\exists x \in E,\ A(x)) \equiv (\forall x \in E,\ \text{non } A(x))$.
- non $(\forall x \in E,\ A(x)) \equiv (\exists x \in E,\ \text{non } A(x))$.

Existence et unicité. L'assertion « l'assertion $A(x)$ est vraie pour un et un seul élément x de l'ensemble E » se note ainsi : « $\exists! x \in E,\ A(x)$ ».

1.6 Quantificateurs et prédicats à plusieurs variables

Si $A(x, y)$ est un prédicat à deux variables représentant des éléments de E et F, on peut lui associer des assertions parmi lesquelles :

– Les assertions tautologiquement équivalentes :

$$\forall x \in E,\ (\forall y \in F,\ A(x,y)) \text{ et } \forall y \in F,\ (\forall x \in E\ A(x,y)).$$

Explicitons davantage le sens de l'assertion de gauche : on définit tout d'abord le prédicat à une variable

$$B(x) : \forall y \in F,\ A(x,y)$$

puis l'assertion

$$\forall x \in E,\ B(x).$$

– Les assertions tautologiquement équivalentes :

$$\exists x \in E,\ (\exists y \in F,\ A(x,y)) \text{ et } \exists y \in F,\ (\exists x \in E,\ A(x,y)).$$

– Les assertions non tautologiquement équivalentes (du moins pas en toute généralité) :

$$\exists x \in E,\ (\forall y \in F,\ A(x,y)) \text{ et } \forall y \in F,\ (\exists x \in E,\ A(x,y)).$$

On peut naturellement généraliser davantage. On omet souvent les parenthèses (en gardant en tête que cela se lit de gauche à droite). Il faut par contre prendre bien garde à l'ordre des quantificateurs quand on n'obtient pas deux assertions tautologiquement équivalentes en intervertissant l'ordre des quantificateurs. Lorsque $E = F$ on écrit par ailleurs souvent (par exemple) $\forall x, y \in E$ pour $\forall x \in E,\ \forall y \in E$.

Voici deux exercices. J'ai trouvé plus naturel de les mettre ici mais, pour les faire, il est nécessaire de savoir bâtir une preuve, chose dont je parle plus loin.

Exercices.

1. Les assertions suivantes sont-elles vraies ou fausses ?
   (a) $\forall x, y \in \mathbb{R},\ (x+y)^2 = x^2 + 2xy + y^2$.
   (b) $\forall a \in \mathbb{N},\ \forall b \in \mathbb{N},\ a+b$ est pair.
   (c) $\exists a \in \mathbb{N},\ \exists b \in \mathbb{N},\ a+b$ est pair.
   (d) $\exists a \in \mathbb{N},\ \forall b \in\ \mathbb{N},\ a+b$ est pair.
   (e) $\exists b \in \mathbb{N},\ \forall a \in\ \mathbb{N},\ a+b$ est pair.
   (f) $\forall a \in \mathbb{N},\ \exists b \in\ \mathbb{N},\ a+b$ est pair.
   (g) $\forall b \in \mathbb{N},\ \forall a \in \mathbb{N},\ a+b$ est pair.
2. Soit $(u_n)_{n\in\mathbb{N}}$ une suite de nombre réels. Considérons l'assertion P suivante :

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ (n \geq N \Rightarrow |u_n| \leq \varepsilon).$$

   (a) L'assertion P est-elle vraie lorsque $(u_n)_n$ est la suite constante égale à 1 ?
   (b) Même question lorsque la suite u_n est la suite définie par $u_n = 1/(n+1)$?
3. Mêmes questions avec l'assertion Q suivante :

$$\forall \varepsilon > 0,\ \forall n \in \mathbb{N},\ \exists N \in \mathbb{N},\ (n \geq N \Rightarrow |u_n| \leq \varepsilon).$$

1.7 Convention.

Par défaut, lorsque l'on énonce une assertion, on affirme que cette assertion possède la valeur de vérité "vraie".

2 Théorèmes et preuves.

2.1 Théorie et raisonnement mathématiques : description rapide et naïve

Une théorie mathématique est décrite par :

1. Une définition précise de la notion d'assertion.
2. Une liste d'assertions que l'on considère comme vraies (les axiomes de la théorie).
3. Une liste de règles de démonstration permettant de déduire, à partir d'assertions vraies, de nouvelles assertions vraies.

Une preuve (ou démonstration) d'une assertion est une manière d'établir que cette assertion est vraie. La preuve utilise des assertions que l'on sait être vraies et des règles de démonstrations. Chaque étape de la preuve consiste donc en l'utilisation de règles précises et d'assertions précises : il n'y aucune place pour le doute. Je ne définirai pas plus précisément dans ce document ce qu'est une preuve. Le critère pragmatique suivant me semble suffisant : vous détenez une preuve (sauf erreur d'inattention) lorsque vous n'avez plus aucun doute sur aucune étape de votre raisonnement (que ce soit sur la définition d'un objet, le sens d'une assertion, un enchaînement, ...).

2.2 Quelques remarques sur la rédaction

Il ne faut pas confondre « preuve » et « rédaction d'une preuve ».

Il existe des logiciels (par exemple le logiciel Coq) qui permettent de vérifier qu'une preuve est correcte. Cela nécessite de rédiger la preuve de manière complètement détaillée dans un langage particulier. Rédiger ainsi des preuves nécessite des compétences spécialisées et beaucoup de temps.

Lorsqu'un mathématicien rédige une preuve dans article de recherche, il ne donne en général que les grandes étapes de la preuve. Il laisse au lecteur (humain) le soin de détailler lui-même les étapes qui l'intéressent (c'est-à-dire toutes les étapes si le lecteur veut vérifier que la preuve est correcte).

Lorsqu'un étudiant rédige une preuve dans un devoir, il n'a en général pas le temps de tout détailler. Il doit alors également choisir les grandes étapes de la preuve. C'est facile lorsqu'il a une preuve complète en tête. Dans le cas contraire, l'important est d'être intellectuellement honnête : on peut admettre un passage que l'on ne sait pas démontrer (en le précisant), on peut ne démontrer qu'un résultat partiel (en précisant ce que l'on démontre) etc. Autrement dit, il s'agit de ne pas s'abuser soi-même (en ignorant un doute) et de ne pas chercher à abuser le lecteur (en faisant semblant de ne pas avoir de doutes).

L'objectif d'un étudiant doit absolument être l'obtention (dans sa tête) de preuves complètement détaillées, autrement dit, l'obtention de certitudes. De son côté, le correcteur va chercher à déterminer, sur la base de ce qu'il lit, si l'étudiant avait réellement obtenu une preuve ou, à défaut, s'il avait obtenu une preuve partielle, si l'étudiant a compris ce qu'est une preuve, s'il est intellectuellement honnête etc.

2.3 Théorèmes, corollaires, propositions, lemmes, ...

Un théorème est une assertion qui admet une preuve. On pourrait se contenter de ce terme. Cependant, si on veut rendre lisible un texte de mathématiques, il est très utile de hiérarchiser les principaux théorèmes rencontrés. Traditionnellement,

- on appelle « théorèmes » les théorèmes les plus importants du texte ;

- on nomme « propositions » des théorèmes d'importance secondaire ;
- on qualifie de « corollaires » les conséquences simples des théorèmes que l'on a appelé « théorèmes » ;
- on appelle « lemmes » les théorèmes intermédiaires utiles dans la preuve d'un autre théorème.

Tout ceci est peut-être un peu confus à première vue. Le point important est que tous ces termes désignent des théorèmes (même si on ne les appellent pas ainsi) c'est-à-dire des assertions prouvées.

2.4 Quelques schémas de preuves

Une compréhension parfaite des connecteurs logiques, des quantificateurs et des définitions des objets manipulés doit permettre de trouver seul des schémas de preuves. Voici quelques exemples.

2.4.1 Prouver une assertion composée.

Prouver $A \Rightarrow B$. Distinguons deux cas.

- A est fausse. Dans ce cas $(A \Rightarrow B)$ est vraie (cela se lit sur la table de vérité) et c'est terminé.
- A est vraie. Dans ce cas, pour établir que $(A \Rightarrow B)$ est vraie, il reste à montrer que B est vraie.

Le seul cas où il y a quelque chose à faire est le deuxième cas. Cela nous fournit le schéma de preuve suivant pour prouver $(A \Rightarrow B)$:

« Supposons que A est vraie. Montrons que B est vraie [...]. »

C'est un schéma très naturel quand on a compris le sens de $(A \Rightarrow B)$.

Prouver $A \Rightarrow B$. On sait que $(A \Rightarrow B) \equiv ((\text{non } B) \Rightarrow (\text{non } A))$. Le paragraphe précédent nous amène alors au schéma suivant pour prouver $(A \Rightarrow B)$:

« Supposons que B est fausse. Montrons que A est fausse [...]. »

À nouveau, c'est un schéma très naturel (et différent du précédent) quand on a compris le sens de $(A \Rightarrow B)$.

Prouver $(A$ ou $B) \Rightarrow C$. On peut vérifier que l'on a

$$((A \text{ ou } B) \Rightarrow C) \equiv ((A \Rightarrow C) \text{ et } (B \Rightarrow C)).$$

Cela nous amène au schéma suivant (un schéma parmi d'autres) pour prouver $((A \text{ ou } B) \Rightarrow C)$:

« Montrons $(A \Rightarrow C)$ [...]. Montrons $(B \Rightarrow C)$ [...]. »

Pour chacune de ces deux preuves, on peut utiliser l'un des deux schémas précédents pour la preuve d'une implication. On aurait aussi pu appliquer directement, par exemple, le premier schéma : cela nous aurait amené à supposer $(A$ ou $B)$ vraie puis à chercher à montrer C ; on aurait distingué deux cas etc.

Prouver que $(A \Rightarrow B)$ **est fausse.** Il s'agit de prouver que (non $(A \Rightarrow B)$) est vraie. Or

$$(\text{non } (A \Rightarrow B)) \equiv (A \text{ et } (\text{non } B)).$$

Cela nous amène au schéma suivant (à nouveau, un parmi d'autres) :

« Montrons A [...]. Montrons que B est fausse [...]. »

Etc. La compréhension des connecteurs logiques doit vous permettre de déterminer des schémas de preuves pour toute assertion composée.

2.4.2 Prouver une assertion quantifiée.

Je considère un prédicat $A(x)$ où x est une variable appartenant à l'ensemble E.

Prouver $\forall x \in E,\ A(x)$**.** Voici un schéma de preuve :

« Soit $x \in E$. Montrons $A(x)$ [...]. »

La preuve de $A(x)$ doit être valable pour n'importe quel élément x de E.

Prouver $\exists x \in E,\ A(x)$**.** Dans certain cas, on peut prouver cette assertion en exhibant un élément x de E pour lequel $A(x)$ est vraie. Voici par exemple une preuve complète de $\exists n \in \mathbb{N},\ n$ est pair : posons $n = 10$; on a $n \in \mathbb{N}$; l'assertion « n est pair » est vraie.

Dans d'autres cas, on peut prouver l'existence d'un x de E pour lequel $A(x)$ est vraie sans être capable de l'exhiber (cela arrive par exemple lorsque l'on applique le théorème des valeurs intermédiaires, lorsque l'on utilise des arguments de compacité, ...).

Prouver que $(\forall x \in E,\ A(x))$ **est fausse.** Il s'agit de prouver (non $(\forall x \in E,\ A(x))$. Or :

$$(\text{non } (\forall x \in E,\ A(x)) \equiv (\exists x \in E,\ (\text{non } A(x)).$$

Nous sommes ainsi ramenés à l'un des cas précédents.

Prouver que $(\exists x \in E,\ A(x))$ **est fausse.** Il s'agit de prouver (non $(\exists x \in E,\ A(x))$. Or :

$$(\text{non } (\exists x \in E,\ A(x)) \equiv (\forall x \in E,\ (\text{non } A(x)).$$

Nous sommes à nouveau ramenés à l'un des cas précédents.

2.5 Raisonnement par l'absurde.

C'est un raisonnement particulier. On cherche à prouver qu'une assertion A est vraie. Le raisonnement par l'absurde consiste à supposer que A est fausse et à en déduire une contradiction. On peut alors en conclure que A est vraie.

2.6 Raisonnement par récurrence.

Soit $H(n)$ un prédicat où n est un élément de l'ensemble des entiers naturels. Pour montrer

$$\forall n \in \mathbb{N},\ H(n),$$

il suffit de montrer

$$H(0) \text{ et } (\forall n \in \mathbb{N},\ (H(n) \Rightarrow H(n+1))).$$

Les paragraphes précédents fournissent un schéma de preuve naturel pour montrer l'assertion ci-dessus.

3 Un exemple de preuve

Commençons par rappeler quelques définitions.

Définitions. Soit E un ensemble. Soit $f : E \to E$ une application [3].

- On dit que f est une involution si, pour tout $x \in E$,

$$f(f(x)) = x. \tag{1}$$

- On dit que f est une injection (ou que f est injective) si

$$\forall x, x' \in E, f(x) = f(x') \Rightarrow x = x'.$$

- On dit que f est une surjection (ou que f est surjective) si

$$\forall y \in E, \exists x \in E : f(x) = y.$$

- On dit que f est une bijection (ou que f est bijective) si f est à la fois une injection et une surjection.

Voici un théorème très simple.

Théorème 1 *Soit E un ensemble. Pour toute application $f : E \to E$, si f est une involution alors f est une bijection.*

Je donne dans la suite une preuve détaillée et commentée. Il est clair qu'il serait pénible de toujours détailler et commenter une preuve comme je le fais ici (pour le rédacteur comme pour le lecteur). La preuve est en caractères gras. Les commentaires sont en caractères maigres.

Dans cette preuve élémentaire, la structure de la preuve (qui occupe ici une grande partie de la preuve) se construit de manière mécanique à partir de la propriété que l'on cherche à prouver.

Cette preuve doit être totalement limpide pour tout étudiant en fin de L1 : il doit comprendre chaque étape et comprendre pourquoi c'est effectivement une preuve de la propriété annoncée (comme pour toute preuve qu'il propose lui-même et comme pour toutes les preuves de difficulté raisonnable qu'il voit en cours ou en TD). Tout étudiant en fin de L1 doit par ailleurs être capable de mettre en place seul toute la structure de cette preuve, quitte à ne pas avoir les quelques idées nécessaires pour conclure.

Une structure de preuve est indispensable pour toute preuve et elle facilite par ailleurs la recherche des idées permettant de conclure (c'est la recherche de ces idées ou de structures de preuves originales qui est intéressante pour le mathématicien, mais ce n'est pas ce sur quoi je veux insister ici).

Preuve. Nous voulons montrer que, dès que l'on se donne un ensemble E, la propriété « pour toute application $f : E \to E$, si f est une involution alors f est une bijection » est vraie. Nous utilisons le schéma de preuve naturel suivant : on se donne un ensemble E ; on montre ensuite la propriété évoquée.

- **Soit E un ensemble.** Nous sommes ramenés à montrer que pour toute application $f : E \to E$, la propriété « si f est une involution alors f est une bijection » est vraie. Nous utilisons le même schéma de preuve que ci-dessus.

3. Connaissez-vous la définition d'une application ?

- **Soit $f : E \to E$ une application.** Nous sommes ramenés à montrer que f vérifie la propriété « si f est une involution alors f est une bijection ». Il s'agit d'une implication. Nous utilisons le schéma de preuve naturel suivant : nous supposons « f est une involution » ; nous montrons ensuite « f est une bijection ».
  - **Supposons que f est une involution.** Nous sommes ramenés à montrer que f est une bijection. Mais « f est une bijection » signifie que les deux propriétés « f est injective » et « f est surjective » sont vraies. Nous utilisons le schéma de preuve naturel suivant : nous montrons « f est injective » ; nous montrons « f surjective ».
    - Montrons que f est injective. La propriété « f injective » signifie

      $$\forall x, x' \in E, f(x) = f(x') \Rightarrow x = x'.$$

      Nous utilisons le même schéma de preuve que précédemment dans cette situation.
      - **Soient $x, x' \in E$.** Nous sommes amenés à montrer

        $$f(x) = f(x') \Rightarrow x = x'.$$

        C'est à nouveau une implication. Nous utilisons le même schéma de preuve que précédemment dans cette situation.
        - **Supposons $f(x) = f(x')$.** Nous sommes ramenés à montrer $x = x'$. C'est le premier instant où nous avons besoin d'une idée. Tout ce qui précédait était mécanique, nous avons utilisé les schémas de preuve les plus naturels pour montrer les propriétés du type « pour tout ... on a ... » et « si ... alors ... ». À ce stade, nous disposons de E, f, x et x', nous savons que f est une involution et que $f(x) = f(x')$. Il s'agit de combiner convenablement ces propriétés. La manière la plus simple d'exploiter le fait que f est une involution est de considérer $f(f(x)), f(f(x'))$ et d'espérer que cela mène à une preuve... **Comme f est une involution, en appliquant (1) pour x et pour x' on obtient**

          $$f(f(x)) = x \tag{2}$$

          et

          $$f(f(x')) = x'. \tag{3}$$

          Mais de $f(x) = f(x')$ on déduit également

          $$f(f(x)) = f(f(x')). \tag{4}$$

          De (2) et (4) on déduit

          $$x = f(f(x')). \tag{5}$$

          De (3) et (5) on déduit $x = x'$.

          Conclusion de ce paragraphe : $x = x'$.

        Conclusion de ce paragraphe : $f(x) = f(x') \Rightarrow x = x'$.

      Conclusion de ce paragraphe : $\forall x, x' \in E, f(x) = f(x') \Rightarrow x = x'$. Autrement dit f est injective.

– Montrons que f est surjective. La propriété « f surjective » signifie

$$\forall y \in E, \exists x \in E : f(x) = y.$$

Nous utilisons le même schéma de preuve que précédemment dans cette situation.

– **Soit $y \in E$.** Nous sommes amenés à montrer

$$\exists x \in E : f(x) = y.$$

Nous arrivons à nouveau à un stade où il faut une idée. À ce stade, nous disposons de E, f et y et nous savons que f est une involution. À nouveau, il s'agit de combiner habilement ces propriétés. La manière la plus simple d'exploiter le fait que f est une involution est de considérer $f(f(y))$ et d'espérer que cela mène à une preuve. **Comme f est une involution, en appliquant (1) pour y on obtient**

$$f(f(y)) = y.$$

Posons $x = f(y)$. On a alors bien $x \in E$. De $f(x) = f(f(y))$ et de $f(f(y)) = y$ on déduit $f(x) = y$. Conclusion de ce paragraphe : $\exists x \in E : f(x) = y$.

Conclusion de ce paragraphe : $\forall y \in E, \exists x \in E : f(x) = y$. Autrement dit, f est surjective.

Conclusion de ce paragraphe : f est bijective.

Conclusion de ce paragraphe : si f est une involution alors f est bijective.

Conclusion de ce paragraphe : pour toute application $f : E \to E$, si f est une involution alors f est bijective.

Conclusion : pour tout ensemble E, pour toute application $f : E \to E$, si f est une involution alors f est bijective. Autrement dit, le théorème est prouvé. □

Voici la même preuve sans les commentaires et avec une structure moins explicite. Je trouve cela plus lisible mais ce n'est qu'une autre rédaction plus concise de la même preuve. Un étudiant en fin de L1 doit être capable, à la lecture de cette preuve, d'expliciter complètement sa structure.

Preuve. Soit E un ensemble. Soit $f : E \to E$ une involution. Soient $x, x' \in E$ tels que $f(x) = f(x')$. Comme f est une involution, on a $f(f(x)) = x$ et $f(f(x')) = x'$. Comme $f(x) = f(x')$ on a $f(f(x)) = f(f(x'))$. Ainsi $x = f(f(x)) = f(f(x')) = x'$ et f est injective. Soit $y \in E$. Posons $x = f(y) \in E$. Comme f est une involution on a $y = f(f(y)) = f(x)$. Ainsi f est également surjective. □

Voici pour conclure une autre preuve. Elle utilise le lien entre l'existence d'une application réciproque et la bijectivité. Exercice : donner un énoncé du théorème utilisé ; donner une preuve de ce théorème.

Preuve. Comme $f \circ f$ est l'identité de E, f est bijective (et sa réciproque est f). □

4 Remarques diverses

Introduire les objets et éviter les conflits. Voici un texte dans lequel les [...] représentent de longs développements.

> [...] Il existe donc n tel que [propriété compliquée 1]
> [...] Il existe donc n tel que [proprieté compliquée 2]
> [...]
> Comme n vérifie [propriété compliquée 1] on a [...]
> [...]
> Comme n vérifie [propriété compliquée 2] on a [...]
> [...]

Voyez-vous le problème ? Le même nom « n » a été donné à deux objets a priori différents. Il n'y a en effet aucune raison qu'il existe n vérifiant les deux propriétés compliquées. Voici la même erreur sur un exemple caricatural.

> Il existe n un entier pair.
> Il existe n un entier impair.
> Comme n est pair et impair, il existe un entier pair et impair.

J'espère que cet exemple vous convaincra d'introduire convenablement les objets et de vérifier qu'il n'y a pas de conflits de notation (même nom pour différents objets).

A **donc** B**.** Cela signifie en général que l'on vient de montrer A, que l'on sait par ailleurs que $A \Rightarrow B$ est vraie, et que l'on déduit de tout cela B. Le mot « donc » est en particulier un mot qui sert à décrire un enchaînement logique dans la preuve. Il est souvent confondu avec le mot « implique » qui est un connecteur logique et qui sert donc à décrire une assertion. La phrase « A donc B » (qui décrit une partie de la preuve) n'a pas du tout le même sens que l'assertion « $A \Rightarrow B$ » (qui est un énoncé mathématique ; revoir si besoin la définition de l'implication).