Chapitre 1

Preuves

Définition : Une *démonstration* est une vérification d'une *proposition* par une séquence de *déductions logiques* à partir d'un ensemble d'*axiomes*.

Propositions

Définition : Une *proposition* est un énoncé qui est *soit vrai*, *soit faux*.

Exemples :

- $2 + 3 = 5$. Proposition vraie.
- $(\forall n \in \mathbb{N})\ n^2 + n + 41$ est un nombre premier. Proposition fausse : pour $n = 40$, on a $n^2 + n + 41 = 40^2 + 40 + 41 = 41^2$.
- (Conjecture d'Euler, 1769) $a^4 + b^4 + c^4 = d^4$ n'a pas de solution quand $a, b, c, d \in \mathbb{N}^+$. Proposition fausse (Elkies, 1988). Contre-exemple : $a = 95800, b = 217519, c = 414560, d = 422481$.
- $(\exists a, b, c, d \in \mathbb{N}^+)\ a^4 + b^4 + c^4 = d^4$. Proposition vraie.

- $(\forall n \in \mathbb{Z})\ (n \geq 2) \Rightarrow (n^2 \geq 4)$. Proposition vraie.
- $1 = 0 \Rightarrow (\forall n \in \mathbb{N})\ n^2 + n + 41$ est un nombre premier. Proposition vraie.
- $(\forall n \in \mathbb{Z})\ (n \geq 2) \Leftrightarrow (n^2 \geq 4)$. Proposition fausse.

Axiomes

- Définition : Un *axiome* est une proposition qui est *supposée vraie*.
- Exemple : $(\forall a, b, c \in \mathbb{Z})\ (a = b \text{ et } b = c) \Rightarrow (a = c)$.
- Un ensemble d'axiomes est *consistant* s'il n'existe pas de proposition dont on peut démontrer qu'elle est *à la fois vraie et fausse*.
- Un ensemble d'axiomes est *complet* si, pour toute proposition, il est possible de démontrer qu'elle est vraie ou fausse.
- Théorème d'incomplétude de Gödel (1931) : tout ensemble consistant d'axiomes pour l'arithmétique sur les entiers est nécessairement incomplet.
- Dans ce cours, on considérera comme axiomes les notions des mathématiques de base.

Autres types de proposition

- Un *théorème* est une proposition qui peut être démontrée
- Un *lemme* est une proposition préliminaire utile pour faire la démonstration d'autres propositions plus importantes
- Un *corrolaire* est une proposition qui peut se déduire d'un théorème en quelques étapes logiques
- Une *conjecture* est une proposition pour laquelle on ne connaît pas encore de démonstration mais que l'on soupçonne d'être vraie, en l'absence de contre-exemple. Exemple : tout entier paire plus grand que 2 est la somme de deux nombres premiers (Conjecture de Golbach).

Déductions logiques

- Définition : Les *règles de déductions logiques*, ou *règles d'inférence*, sont des règles permettant de combiner des axiomes et des propositions vraies pour établir de nouvelles propositions vraies.
- Exemple : $\boxed{\dfrac{\begin{array}{c} P \\ P \Rightarrow Q \end{array}}{Q}}$ (modus ponens).

  Le modus ponens est fortement lié à la proposition $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$, qui est une *tautologie*.
  (= une proposition qui est toujours vraie quelles que soient les valeurs de ses variables)

Exemples de démonstrations

Théorème : La proposition suivante est une tautologie :

$$(X \Rightarrow Y) \Leftrightarrow (\neg Y \Rightarrow \neg X).$$

Démonstration : Montrons que $(X \Rightarrow Y)$ est logiquement équivalent à sa *contraposée* $(\neg Y \Rightarrow \neg X)$, quelles que soient les valeurs booléennes des variables X et Y.

X	Y	$X \Rightarrow Y$	$\neg Y \Rightarrow \neg X$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

La proposition $(X \Rightarrow Y) \Leftrightarrow (\neg Y \Rightarrow \neg X)$ est donc vraie dans tous les cas, ce qui implique qu'elle est une tautologie. $\square$

Les deux règles suivantes sont donc des règles d'inférence.

$$\frac{P \Rightarrow Q}{\neg Q \Rightarrow \neg P} \qquad\qquad \frac{\neg Q \Rightarrow \neg P}{P \Rightarrow Q.}$$

Théorème : $(\forall a \in \mathbb{Z})$ (a est pair) $\Leftrightarrow$ (a^2 est pair).

Démonstration : Soit a un entier quelconque.

$\boxed{a \text{ est pair } \Rightarrow \ a^2 \text{ est pair}}$ Supposons que a soit pair. On a donc $a = 2b$, avec $b \in \mathbb{Z}$. Dès lors, on obtient $a^2 = (2b)^2 = 4b^2 = 2(2b^2)$. Le nombre a^2 est donc pair.

$\boxed{a^2 \text{ est pair } \Rightarrow \ a \text{ est pair}}$ Par le théorème précédent, il suffit de démontrer que a est impair $\Rightarrow$ a^2 est impair. Supposons que a soit impair. On a donc $a = 2b + 1$, avec $b \in \mathbb{Z}$. Dès lors, on obtient $a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1$. Le nombre a^2 est donc impair. $\square$

Démonstrations par l'absurde

Principe :

- On veut démontrer qu'une proposition P est vraie.
- On suppose que $\neg P$ est vraie, et on montre que cette hypothèse conduit à une *contradiction*.
- Ainsi, $\neg P$ est fausse, ce qui implique que P est vraie.

Règle d'inférence correspondante :

$$\frac{\neg P \Rightarrow \text{faux}}{P}$$

Exemple

Théorème : $\sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$.

Démonstration : Par l'absurde, supposons que $\sqrt{2} \in \mathbb{Q}$. On a donc

$$\sqrt{2} = \frac{a}{b},$$

où $a, b \in \mathbb{Z}$, $b \neq 0$ et où cette fraction est réduite. Cela implique $2 = \frac{a^2}{b^2}$, et donc

$$2b^2 = a^2.$$

Par conséquent, le nombre a^2 est pair, ce qui implique que a est lui-même pair.

Il existe donc $a' \in \mathbb{Z}$ tel que $a = 2a'$. On a donc $a^2 = 4a'^2$. Donc, on a $2b^2 = 4a'^2$, ce qui implique que

$$b^2 = 2a'^2.$$

Dès lors, b^2 est pair, et donc b est lui-même pair. Il existe donc $b' \in \mathbb{Z}$ tel que $b = 2b'$. La fraction

$$\frac{a}{b} = \frac{2a'}{2b'}$$

n'est donc pas réduite. C'est une contradiction. Par conséquent, l'hypothèse selon laquelle $\sqrt{2} \in \mathbb{Q}$ est fausse. Donc, on a $\sqrt{2} \in \mathbb{R} \backslash \mathbb{Q}$. $\square$

Écrire de bonnes démonstrations

En plus d'être logiquement correcte, une bonne démonstration doit être *claire*.

Conseils pour l'écriture de bonnes démonstrations :

- Expliquez la manière dont vous allez procéder (par l'absurde, contraposition, induction, ...) ;
- Donnez une explication séquentielle ;
- Expliquez votre raisonnement (passages d'une étape à l'autre, arithmétique, induction, ...) ;
- N'utilisez pas trop de symboles ; utiliser du texte lorsque c'est possible ;
- Simplifiez ;

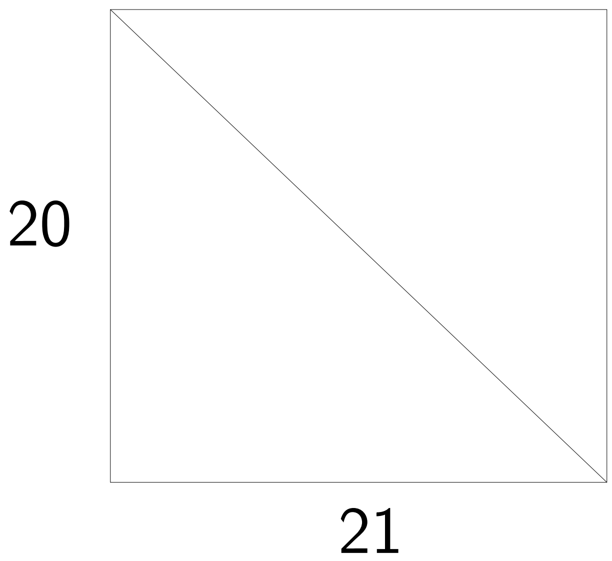
- Introduisez des notations judicieusement, en prenant soin définir leur signification ;
- Si la démonstration est trop longue, structurez-la (par exemple établissez à l'aide de *lemmes* les faits dont vous aurez souvent besoin) ;
- N'essayez pas de camoufler les passages que vous avez du mal à justifier ;
- Terminez en expliquant à quelles conclusions on peut arriver.

Un faux théorème

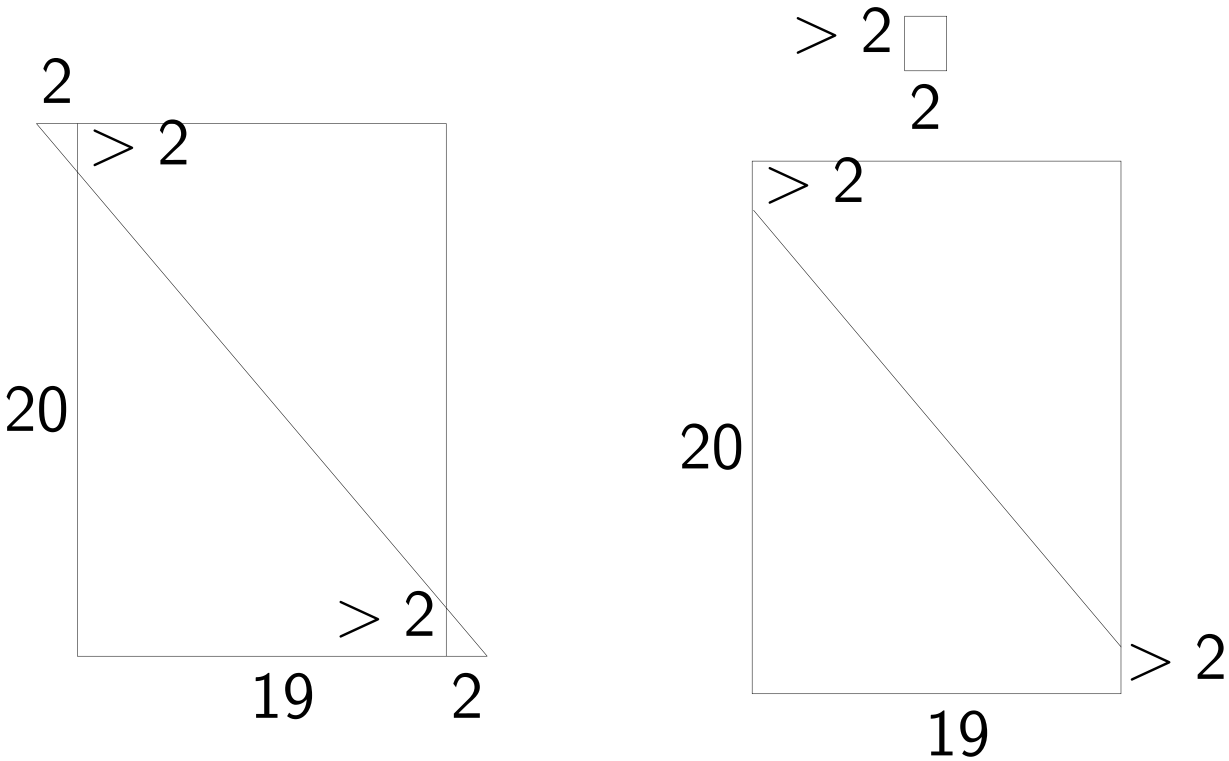
Quelle est l'erreur dans la démonstration suivante ?

Faux théorème : $420 > 422$.

Démonstration erronée : Démonstration géométrique. Soit un rectangle de dimension 20×21. Son aire vaut donc 420.



Découpage + glissement de 2 unités vers la gauche :



- Aire du petit rectangle : > 4.
- Aire du grand rectangle : $> (20 + 2) \times 19 = 418$.
- $\Rightarrow$ Aire totale : > 422. Par conservation d'aire, on a donc $420 > 422$. $\square$