Chapitre 1

Techniques de preuves

Plan

1. Définitions
2. Techniques de preuves simples
3. Principe du bon ordre
4. Induction
5. Principe d'invariant

Lectures conseillées : MCS : chapitres 1, 2, et 5.

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.

Prédicats

Définition : Une proposition dont la valeur de vérité dépend de la valeur d'une ou plusieurs variables

Exemples :

- "n est un carré parfait" : vrai pour $n = 4$ mais faux pour $n = 10$
- Souvent noté $P(n) =$"n est un carré parfait". $P(4)$ est vrai. $P(5)$ est faux.

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 pair strictement 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 : $\boxed{\dfrac{P \qquad P \Rightarrow Q}{Q}}$ (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. □

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

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

Schémas de preuves classiques

Quelques schémas de preuves classiques :

- Implication
- Equivalence (si et seulement si)
- Preuve par cas
- Preuve par contradiction (ou par l'absurde)
- Principe du bon ordre
- Induction faible
- Induction forte
- Principe d'invariant

Une preuve complexe requière la plupart du temps la combinaison de plusieurs de ces techniques

Implications

Deux méthode pour prouver que P implique Q (noté $P \Rightarrow Q$)

1. Supposez que P est vrai et montrez que Q vrai en découle.

Théorème : Si $0 \leq x \leq 2$, alors $-x^3 + 4x + 1 > 0$

Démonstration :

- Supposons que $0 \leq x \leq 2$.
- Alors x, $2 - x$ et $2 + x$ sont tous non négatifs et leur produit l'est également.
- Ajouter 1 à ce produit donne un nombre strictement positif :

$$x(2 - x)(2 + x) + 1 > 0$$

- En multipliant les termes, on obtient :

$$-x^3 + 4x + 1 > 0$$

□

Implications

Deux méthode pour prouver que P implique Q (noté $P \Rightarrow Q$)

2. On démontre la *contraposée*. Régle d'inférence : $\dfrac{\neg Q \Rightarrow \neg P}{P \Rightarrow Q}$

Théorème : Si r est irrationnel, alors $\sqrt{r}$ est aussi irrationnel

Démonstration :

- Par contraposition, il suffit de démontrer que si $\sqrt{r}$ est rationnel, alors r est rationnel.
- Supposons que $\sqrt{r}$ est rationnel. Il existe alors des entiers m et n tels que :

$$\sqrt{r} = \frac{m}{n}$$

- En mettant au carré les deux côtés de l'équation, on obtient :

$$r = \frac{m^2}{n^2}$$

- Etant donné que m^2 et n^2 sont des entiers, on a montré que r était rationnel. □

Si et seulement si

Deux méthodes :

1. Chaînage de si et seulement si

$$\frac{P \Leftrightarrow R, R \Leftrightarrow Q}{P \Leftrightarrow Q}$$

2. Preuve des implications dans les deux sens

$$\frac{P \Rightarrow Q, Q \Rightarrow P}{P \Leftrightarrow Q}$$

Si et seulement si : exemple

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 contraposition, 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. □

Preuve par cas

Décomposer la preuve en différents cas qui seront traités séparément

Exemple :
Théorème : Toute ensemble de 6 personnes inclut un groupe de 3 personnes qui se sont déjà rencontrées ou un groupe de 3 étrangers.

Démonstration La preuve se fait par une analyse de cas. Soit x une des 6 personnes. Il y a deux cas possibles :

- Parmi les 5 autres personnes du groupe, au moins 3 connaissent x.
- Parmi les 5 autres personnes du groupe, au moins 3 ne connaissent pas x.

En effet, si on divise le groupe des 5 personnes en deux groupes, ceux qui connaissent x et ceux qui ne le connaissent pas, un des deux groupes doit contenir au moins la moitié des 5 personnes.

Preuve par cas

On va traiter les deux cas séparément.
Cas 1 : Au moins 3 personnes connaissent x. Ce cas peut se diviser en deux sous-cas :

- **Cas 1.1 :** Aucun de ces 3 personnes ne se connaissent et ils forment donc un groupe de 3 étrangers
- **Cas 1.2 :** Deux personnes parmi les 3 se connaissent et avec x, ils forment un groupe de 3 personnes qui se connaissent.

Dans les deux cas, le théorème est vérifié et donc il l'est dans le cas 2.
Cas 2 : Au moins 3 personnes ne connaissent pas x. Ce cas peut aussi se diviser en deux sous-cas :

- **Cas 1.1 :** Ces 3 personnes se connaissent.
- **Cas 1.2 :** Deux personnes parmi les 3 ne se connaissent pas et avec x, ils forment un groupe de 3 étrangers.

Dans les deux cas, le théorème est vérifié et donc il l'est dans le cas 1.
Le théorème est donc vrai dans tous les cas. □

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 (a et b n'ont pas de facteur commun). 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 $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$. □

Écrire de bonnes démonstrations

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

Conseils pour l'écriture de bonnes démonstrations :

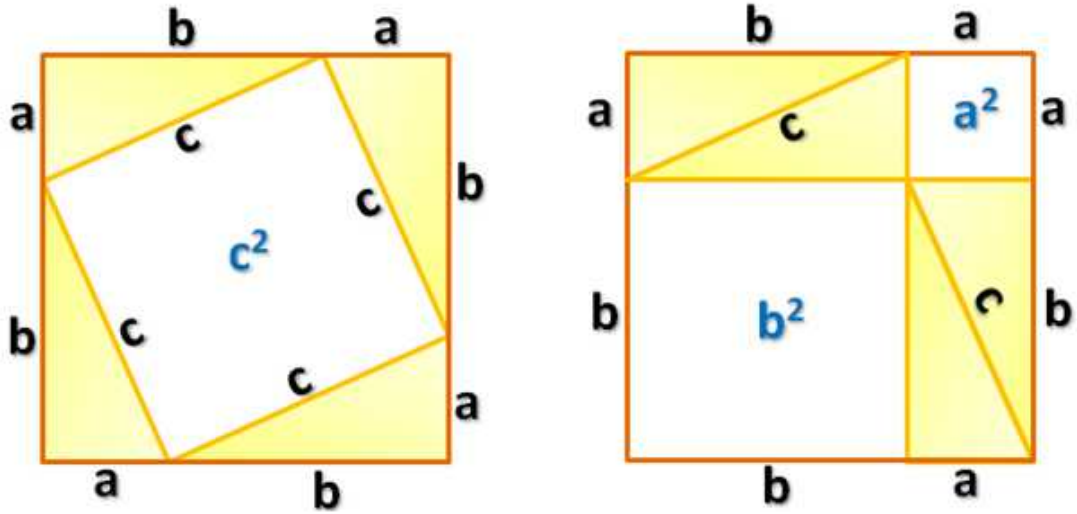
- Expliquez la manière dont vous allez procéder (par l'absurde, contraposition, induction . . .) ;
- Donnez une explication séquentielle ;
- Expliquez votre raisonnement (passages d'une étape à l'autre, arithmétique, induction, . . .) ;
- N'utilisez pas trop de symboles ; utiliser du texte lorsque c'est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

Une preuve sans mot

Théorème de Pythagore : Dans un triangle rectangle, le carré de la longueur de l'hypothénuse est égal à la somme des carrés des longueurs des deux autres côtés.

Démonstration :



Source :

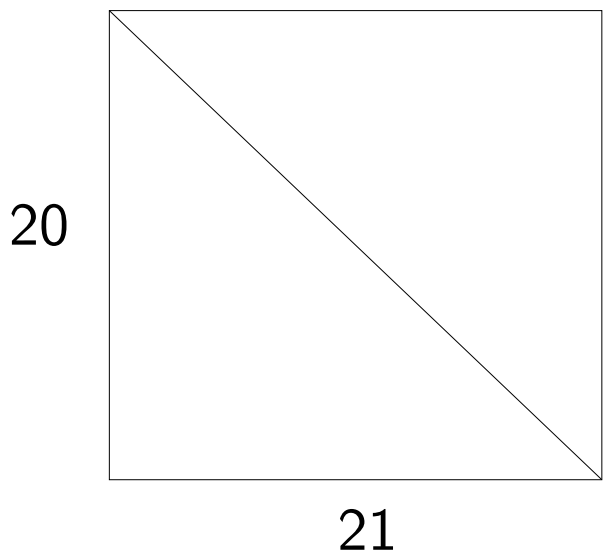
`http://mathandmultimedia.com/2012/06/01/mathematical-proof-without-words/`

Un faux théorème

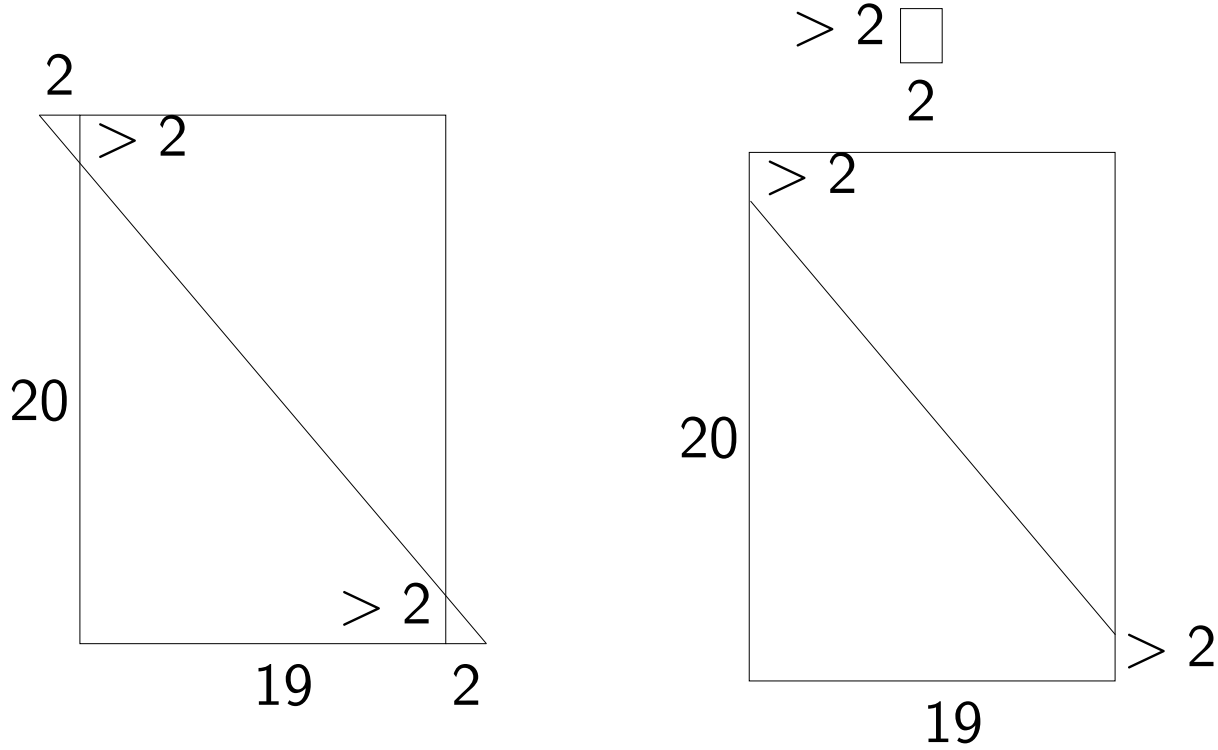
Quelle est l'erreur dans la démonstration suivante ?

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 $420 > 422$.

Plan

Principe du bon ordre

Le principe du bon ordre (sur les naturels) s'énonce comme suit :

> *tout ensemble non vide d'entiers non-négatifs possède un plus petit élément.*

Principe évident mais à la base de nombreuses preuves.

Principe du bon ordre

Exemple dans une précédente preuve :

> *...$\sqrt{2}$ peut s'écrire $\frac{a}{b}$ où on suppose que a et b n'ont pas de facteur commun...*

Montrons que c'est toujours possible par le principe du bon ordre :

- Soit l'ensemble suivant : $C = \{a \in \mathbb{N} | \exists b \in \mathbb{N} : \sqrt{2} = \frac{a}{b}\}$.
- Par le principe du bon ordre, il existe un plus petit élément a' dans C. Soit $b' \in \mathbb{N}$ tel que $\sqrt{2} = \frac{a'}{b'}$.
- Supposons que a' et b' aient un facteur commun $c' > 1$. On a alors $\sqrt{2} = \frac{a'/c'}{b'/c'}$ et donc a'/c' appartient à C.
- Or $a'/c' < a'$, ce qui amène une contradiction puisque a' est le plus petit élément de C.
- On a donc $\sqrt{2} = \frac{a'}{b'}$ où a' et b' n'ont pas de facteur commun.

Schéma de preuve par le principe du bon ordre

Pour prouver qu'un prédicat $P(n)$ est vrai pour tout $n \in \mathbb{N}$:

- Définir l'ensemble $C = \{n \in \mathbb{N} | P(n) \text{ est faux}\}$.
- Supposer que C est non vide comme base pour une preuve par contradiction
- Par le principe du bon ordre, il y a un plus petit élément, n, dans C
- Atteindre une contradiction, souvent en utilisant n pour trouver un autre élément de C plus petit que n.
- Conclure que C doit être vide et donc que $P(n)$ est vrai pour tout n.

Exemple

Théorème : Pour tout $n \in \mathbb{N}$, on a

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Démonstration : Par l'absurde. Supposons que le théorème soit faux et définissons C comme suit :

$$C = \{n \in \mathbb{N} | \sum_{i=1}^{n} i \neq \frac{n(n+1)}{2}\}.$$

Si le théorème est faux, C est non vide et par le principe du bon ordre, il contient un élément minimum. Soit c cet élément.
Par définition de c, le théorème est vrai pour tout $n < c$. Or, il est vrai pour $n = 0$ et donc on a $c > 0$. $c - 1$ est donc un entier non négatif et comme $c - 1 < c$, le théorème est vrai pour $c - 1$.

On en déduit que :

$$\sum_{i=1}^{c-1} i = \frac{(c-1)c}{2}.$$

En ajoutant c des deux côtés, on obtient

$$\sum_{i=1}^{c-1} i + c = \sum_{i=1}^{c} i = \frac{(c-1)c}{2} + c = \frac{c(c+1)}{2},$$

ce qui veut dire que le théorème est vérifié pour c.

On arrive donc à une contradiction, ce qui nous permet de conclure que le théorème est vrai pour tout $n \in \mathbb{N}$. □

Un autre exemple

Théorème : Tout nombre entier positif plus grand que 1 peut s'écrire comme un produit de nombres premiers

Démonstration :

- La preuve utilise le principe du bon ordre.
- Soit C l'ensemble des entiers supérieurs à 1 qui ne peuvent pas être factorisés comme un produit de premiers. Supposons que C soit non vide et montrons que nous arrivons à une contradiction.
- Soit n le plus petit élément de C, par le principe du bon ordre. n ne peut pas être premier, car un premier est un produit de premiers (de taille 1) et donc n serait alors dans C.
- n est donc le produit de deux entiers a et b tels que $1 < a, b < n$.

- Puisque a et b sont plus petits que n, ils ne peuvent pas appartenir à C et donc a peut s'écrire comme un produit de premiers $p_1 p_2 \dots p_k$ et b comme un produit de premiers $q_1 q_2 \dots q_l$.
- En conséquence, $n = p_1 \dots p_k q_1 \dots q_l$ peut s'écrire comme un produit de premiers, ce qui contredit $n \in C$. □

Ensembles bien ordonnés

On peut généraliser le principe du bon ordre à d'autres ensembles.

Définition : Un ensemble est *bien ordonné* si tous ses sous-ensembles possèdent un élément minimal.

Théorème : Pour tout entier non négatif, n, l'ensemble des entiers supérieurs ou égaux à $-n$ est bien ordonné

Démonstration : Soit S un sous-ensemble non vide d'entiers $\geq -n$, montrons que S possède un élément minimum. Ajoutons n à chaque élément de S et appelons ce nouvelle ensemble $S + n$. $S + n$ est une sous-ensemble non vide d'entiers non-négatifs, donc, par le principe du bon ordre, il a un élément minimum m. Il est facile de se convaincre que $m - n$ est l'élément minimum de S. □

Un ensemble bien ordonné plus complexe

Soit l'ensemble $To1$ des fractions suivantes :

$$\frac{0}{1}, \frac{1}{2}, \frac{2}{3}, \ldots, \frac{n}{n+1}, \ldots$$

$To1$ est bien ordonné, le minimum d'un sous-ensemble étant la fraction de ce sous-ensemble avec le numérateur le plus petit (qui existe par le principe du bon ordre).

Soit $\mathbb{N} + To1$ l'ensemble de tous les nombres $n + f$ où n est un entier non négatif et f est un élément de $To1$.

Théorème : $\mathbb{N} + To1$ est bien ordonné.

Démonstration :
Soit un sous-ensemble non vide, S, de $\mathbb{N} + To1$. Soit l'ensemble de tous les entiers non négatifs, n, tels que $n + f$ est dans S pour un $f \in To1$. Cet ensemble est une sous-ensemble non vide d'entiers non négatifs et par le principe du bon ordre, il a donc un élément minimum. Notons le n_S.

Soit l'ensemble des fractions f tels que $n_S + f$ soit dans S. Par définition de n_S, cet ensemble est un sous-ensemble non vide de $To1$ et $To1$ étant bien ordonné, il possède donc un élément minimum. Soit f_S cet élément.

Étant donné que toute fraction de $To1$ est inférieure à 1 et non négative, il est facile de vérifier que $n_S + f_S$ est l'élément minimum de S. □

Plan

Principe d'induction

Principe d'induction :

Soit $P(n)$ un prédicat. Si

- $P(0)$ est vrai, et si
- pour tout $n \in \mathbb{N}$, $P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$.

$$\frac{P(0), \forall n : P(n) \Rightarrow P(n+1)}{\forall n : P(n)}$$

Variante :

Soit $P(n)$ un prédicat et $k \in \mathbb{N}$. Si

- $P(k)$ est vrai, et si
- pour tout $n \geq k$, $P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \geq k$.

$$\frac{P(k), \forall n \geq k : P(n) \Rightarrow P(n+1)}{\forall n \geq k : P(n)}$$

Un modèle pour les démonstrations par induction

1. Annoncer que la démonstration utilise une induction ;
2. Définir un prédicat approprié $P(n)$;
3. Démontrer que $P(0)$ est vrai (**“cas de base”**) ;
4. Démontrer que $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$ (**“‘cas inductif”**) ;
5. Invoquer l'induction (cette étape est souvent implicite).

Illustration

Théorème : Pour tout $n \in \mathbb{N}$, on a

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Démonstration :

La démonstration fonctionne par induction.

Soit $P(n)$ le prédicat qui est vrai si et seulement si $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Cas de base : $P(0)$ est vrai car $\sum_{i=1}^{0} i = 0 = \frac{0(0+1)}{2}$.

Cas inductif : Supposons que $P(n)$ soit vrai, où n est un nombre naturel quelconque, et démontrons que cette hypothèse implique la validité de $P(n+1)$. On a

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1).$$

Comme $P(n)$ (l'"hypothèse d'induction") est vraie, cette expression est égale à $\dfrac{n(n+1)}{2} + (n+1)$. On obtient donc

$$\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}.$$

Dès lors, par induction, $P(n)$ est vrai quel que soit le nombre naturel n, et le théorème est démontré. □

Un théorème de divisibilité

Définition : Un nombre entier a *divise* un nombre entier b si b est un multiple de a. Lorsque a divise b, on écrit $a \mid b$.

Exemple : On a $3 \mid (5^3 - 5)$ car $5^3 - 5 = 120$ est un multiple de 3.

On souhaite démontrer par induction que, quel que soit $n \in \mathbb{N}$, on a $3 \mid (n^3 - n)$.

Soit $P(n)$ le prédicat "$3 \mid (n^3 - n)$".

Le cas de base $P(0)$ est immédiat. Pour démontrer le cas inductif, il faut supposer que $3 \mid (n^3 - n)$ et en déduire que $3 \mid ((n+1)^3 - (n+1))$.

On a

$$\begin{aligned}(n+1)^3-(n+1) &= n^3+3n+2n \\ &= (n^3-n)+(3n^2+3n).\end{aligned}$$

Comme 3 divise (n^3-n) par hypothèse d'induction, et que $3n^2+3n$ est un multiple de 3, la somme $(n^3-n)+(3n^2+3n)$ est un multiple de 3.

Réorganisons ce raisonnement dans une démonstration claire.

Théorème : $(\forall n \in \mathbb{N})\ 3 \mid (n^3-n)$.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n)$ la proposition $3 \mid (n^3 - n)$.
- *Cas de base :* $P(0)$ est vrai car $3 \mid (0^3 - 0)$.
- *Cas inductif :* Supposons que $P(n)$ soit vrai, où $n \in \mathbb{N}$. On a

$$\begin{aligned} 3 \mid (n^3 - n) &\Rightarrow 3 \mid ((n^3 - n) + 3(n^2 + n)) \\ &\Rightarrow 3 \mid (n^3 + 3n^2 + 3n + 1 - n - 1) \\ &\Rightarrow 3 \mid ((n+1)^3 - (n+1)). \end{aligned}$$

  Première implication : $3(n^2 + n)$ est divisible par 3.
  Autres implications : réécriture de l'expression de droite.
  On a prouvé que $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$.
- Dès lors, par induction, $P(n)$ est vrai quel que soit $n \in \mathbb{N}$, et le théorème et démontré. □

Une démonstration par induction erronée

Faux théorème : Tous les chevaux ont la même couleur.

Démonstration erronée : *(Où est l'erreur ?)*

- La démonstration fonctionne par induction.
- $P(n)$: "pour tout ensemble de n chevaux, tous ces chevaux ont la même couleur".
- *Cas de base :* $P(1)$ est vrai car tous les chevaux dans un ensemble de 1 cheval ont la même couleur.
- *Cas inductif :* Supposons que $P(n)$ soit vrai. Soit un ensemble de $n+1$ chevaux :

$$c_1, c_2, \ldots, c_n, c_{n+1}.$$

Par hypothèse, les n premiers chevaux ont la même couleur. Il en est de même pour les n derniers :

$$\underbrace{c_1, c_2, \ldots, c_n}_{\text{même couleur}}, c_{n+1}.$$

$$c_1, \underbrace{c_2, \ldots, c_n, c_{n+1}}_{\text{même couleur}}.$$

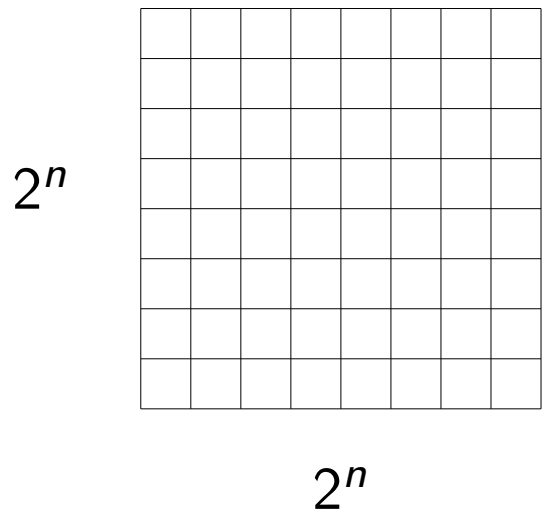
Dès lors, les chevaux $c_1, c_2, \ldots, c_{n+1}$ ont la même couleur, i.e., $P(n+1)$ est vrai. Donc, $P(n)$ implique $P(n+1)$.

- Par induction, $P(n)$ est vrai pour tout $n \geq 1$. Le théorème est un cas particulier de ce résultat : celui où n vaut le nombre total de chevaux dans le monde. □

Dallage

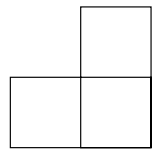
On souhaite créer une terrasse de dimension $2^n \times 2^n$ à la place de la pelouse située au centre du bâtiment B28.

Photo : ©ULg - M. Houet

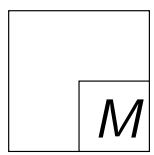


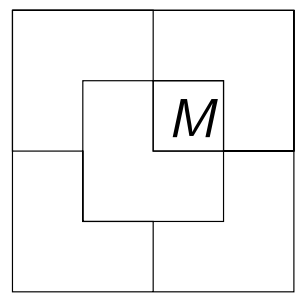
Contraintes :

- Sur un des emplacements situés au centre de la terrasse, on doit ériger une statue de Georges Montefiore (M).
- Tous les autres emplacements doivent être couverts par des dalles en "L", sans que ces dalles ne se recouvrent.



Remarque : Pour $n = 0$, $n = 1$ et $n = 2$, un dallage existe :





On demande de démontrer qu'un tel dallage existe quelle que soit la valeur $n \in \mathbb{N}$.

Problème : Choisir $P(n) =$ "il existe un dallage d'une terrasse $2^n \times 2^n$ avec M au centre" n'est pas adéquat : un dallage pour une terrasse de dimension $2^n \times 2^n$ ne permet pas de construire facilement un dallage pour une terrasse de dimension $2^{n+1} \times 2^{n+1}$.

Solution : Choisir une hypothèse d'induction *plus générale*.

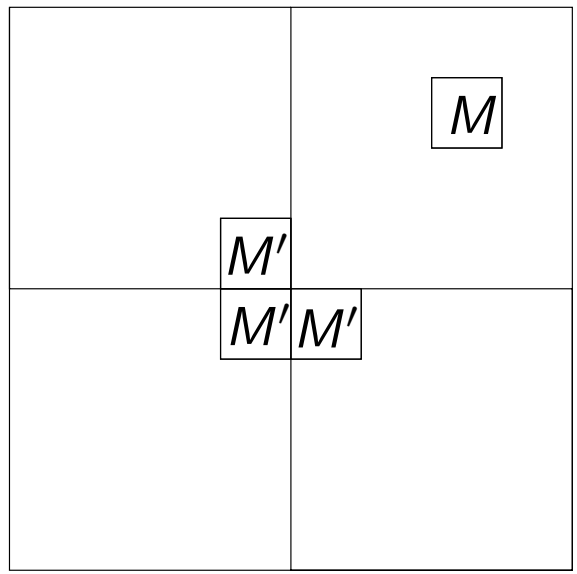
$P(n) =$ "Pour *tout* emplacement de M sur une terrasse de dimension $2^n \times 2^n$, il y a une possibilité de dallage pour le reste de la terrasse."

Théorème : Pour tout $n \in \mathbb{N}$, il existe un dallage d'une terrasse de dimension $2^n \times 2^n$ avec M au centre.

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n) =$ "Pour *tout* emplacement de M sur une terrasse de dimension $2^n \times 2^n$, il y a une possibilité de dallage pour le reste de la terrasse."
- *Cas de base :* $P(0)$ est vrai car M couvre toute la terrasse.
- *Cas inductif :* Supposons que $P(n)$ soit vrai pour un $n \in \mathbb{N}$.
  Soit une terrasse de dimension $2^{n+1} \times 2^{n+1}$, et supposons que M se trouve sur un quelconque emplacement de celle-ci.

Divisons la terrasse en 4 quadrants, chacun de dimension $2^n \times 2^n$. Un d'entre-eux contient M. Plaçons un M temporaire (M' sur le schéma) sur chacun des 3 emplacements centraux situés dans les 3 autres quadrants.



Par l'hypothèse d'induction, chacun des 4 quadrants admet un dallage. Remplacer les 3 emplacements de M' par une dalle en "L" permet de terminer le travail. Donc $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$.

- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. Le théorème en est un cas particulier. $\square$

Induction forte

Principe d'induction forte :

Soit $P(n)$ un prédicat. Si

- $P(0)$ est vrai, et si
- pour tout $n \in \mathbb{N}$, $P(0) \wedge P(1) \wedge \cdots \wedge P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \in \mathbb{N}$.

$$\frac{P(0), \forall n : (\forall k \leq n : P(k)) \Rightarrow P(n+1)}{\forall n : P(n)}$$

Variante :

Soit $P(n)$ un prédicat, et soit $k \in \mathbb{N}$. Si

- $P(k)$ est vrai, et si
- pour tout $n \geq k$, $P(k) \wedge P(k+1) \wedge \cdots \wedge P(n)$ implique $P(n+1)$,

alors $P(n)$ est vrai pour tout $n \geq k$.

Application : jeu de dépilage

Règles du jeu :

- On commence avec une pile de n boîtes.
- A chaque étape, on divise une pile en deux piles non vides.
- Le jeu s'arrête lorsque l'on obtient n piles, chacune contenant une seule pile.
- Une division où l'on transforme une pile de hauteur $a + b$ en deux piles d'hauteurs a et b permet d'obtenir ab points.

Exemple :

hauteurs des piles										score
10										
5	5									25 points
5	3	2								6
4	3	2	1							4
2	3	2	1	2						4
2	2	2	1	2	1					2
1	2	2	1	2	1	1				1
1	1	2	1	2	1	1	1			1
1	1	1	1	2	1	1	1	1		1
1	1	1	1	1	1	1	1	1	1	1
									score total =	45 points

Est-il possible de trouver une meilleure stratégie ?

Théorème : Toute manière de dépiler n blocs conduit à un score de $n(n-1)/2$ points.

Démonstration :

- La démonstration fonctionne par induction forte.
- Soit $P(n) =$ "Toute manière de dépiler n blocs conduit à un score de $n(n-1)/2$ points".
- *Cas de base :* $P(1)$ est vrai car une pile de 1 bloc est déjà dépilée. Le score est donc de $0 = 1(1-1)/2$.
- *Cas inductif :* Supposons que $P(1)$, $P(2)$, ..., $P(n)$ soient vrais, avec $n \geq 1$, et supposons que nous disposions d'une pile de $n+1$ blocs.
  - Premier mouvement : divise la pile initiale en deux piles de tailles k et $n+1-k$, avec $1 \leq k < n+1$.

- On obtient :

$$\begin{aligned}
\text{s. total} &= \text{score du premier mouvement} \\
&\quad + \text{score du dépliage de } k \text{ blocs} \\
&\quad + \text{score du dépliage de } n+1-k \text{ blocs} \\
&= k(n+1-k) + \frac{k(k-1)}{2} + \frac{(n+1-k)(n-k)}{2} \\
&= \frac{2kn + 2k - 2k^2 + k^2 - k + n^2 - kn + n - k - kn + k^2}{2} \\
&= \frac{(n+1)n}{2}
\end{aligned}$$

- La conjonction $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$ implique donc $P(n+1)$ quel que soit $n \geq 1$.
- Par induction forte, on a donc $P(n)$ pour tout $n \geq 1$. □

Factorisation en nombres premiers

Redémontrons le théorème suivant par induction forte :

Théorème : Tout nombre entier positif plus grand que 1 peut s'écrire comme un produit de nombres premiers

Démonstration :

- La démonstration fonctionne par induction forte.
- $P(n) =$ "n s'écrit comme un produit de nombres premiers".
- *Cas de base :* $P(1)$ est vrai car il s'écrit comme le produit d'un ensemble vide de nombres premiers.
- *Cas inductif :* Supposons $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$.
  - Si $n+1$ est premier, $P(n+1)$ est vrai.
  - Sinon, $n+1 = ab$, avec $2 \leq a, b \leq n$.
  - Par induction, a et b sont des produits de nombres premiers. Donc, $P(n+1)$ est vrai.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}_0$. □

Remarques :

- Tout théorème qui peut être démontré par induction forte peut aussi être démontré par induction simple.
  - Supposons que $P(0)$ et $\forall n : (\forall k \leq n : P(k)) \Rightarrow P(n+1)$ soient vraies.
  - On peut montrer par induction simple que

$$Q(n) = "\forall 0 \leq k \leq n : P(k)"$$

    est vraie pour tout n.
  - Et donc en déduire que $P(n)$ est vraie pour tout n.
- Utiliser l'induction forte rend parfois les preuves plus simples.
- Cependant, si $P(n)$ permet de démontrer facilement que $P(n+1)$ est vrai, alors, par soucis de simplicité, il est préférable d'utiliser l'induction simple.

Equivalence entre bon ordre et induction

Tout ce qui peut se démontrer par induction peut également se démontrer par le principe du bon ordre.

Si on suppose qu'un de ces principes est un axiome, on peut en déduire l'autre.

Théorème : Soit un prédicat $P(n)$. Si $P(0)$ est vraie et $P(n) \Rightarrow P(n+1)$ est vraie pour tout $n \geq 0$, alors $P(n)$ est vraie pour tout $n \geq 0$.

Démonstration :

- Supposons $P(0)$ et $\forall n \geq 0 : P(n) \Rightarrow P(n+1)$ vraies.
- Soit l'ensemble $C = \{n | P(n) \text{ fausse}\}$.
- Si le théorème est faux, C est non vide et par le principe du bon ordre, il contient un plus petit élément. Soit m cet élément.
- Puisque $P(0)$ est vraie, on a $m > 0$ et donc $m - 1 \geq 0$.
- $P(m-1) \Rightarrow P(m)$ est vraie et donc $P(m)$ doit être vraie, ce qui contredit le choix de m.
- $P(n)$ est donc vraie pour tout $n \geq 0$. □

Plan

L'énigme du Taquin (Sam Lloyd, ±1870)

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

→

1	2	3	4
5	6	7	8
9	10	11	12
13	15		14

→

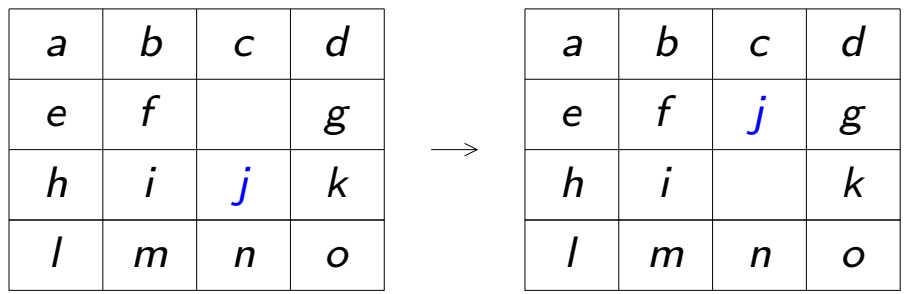
1	2	3	4
5	6	7	8
9	10		12
13	15	11	14

Existe-t-il une séquence de mouvements qui permet d'échanger les pièces 15 et 14 de la configuration de gauche, sans modifier l'emplacement des autres pièces ?

Principe de la démonstration :

- Nous allons établir un propriété de la grille qui est toujours vraie, quelle que soit la façon dont les pièces sont déplacées.
- Nous montrerons ensuite que la grille recherchée viole cette propriété et n'est donc pas atteignable

- Deux types de mouvements : mouvement de ligne et mouvement de colonne.
- Lemme 1 : Un mouvement de ligne ne modifie pas l'ordre des pièces.
  Démonstration : C'est immédiat. □
- Lemme 2 : Un mouvement de colonne modifie l'ordre relatif d'exactement 3 paires de pièces.



Démonstration : Faire glisser une pièce vers le bas la déplace après les 3 pièces suivantes. Faire glisser une pièce vers le haut la déplace avant les 3 pièces précédentes. □

- Lemme 3 : Un mouvement de ligne ne modifie jamais la parité du nombre d'inversions. Un mouvement de colonne modifie toujours la parité du nombre d'inversions.

  Démonstration : Par le lemme 1, un mouvement de ligne ne modifie pas l'ordre des pièces. En particulier, il ne modifie pas le nombre d'inversions.

  Par le lemme 2, un mouvement de colonne modifie l'ordre relatif d'exactement 3 paires de pièces. Donc, un nombre pair d'inversions devient impair, et vice-versa. □

- Lemme 4 : Dans toute configuration accessible à partir de la configuration ci-dessous, la parité du nombre d'inversions est différente de la parité du numéro de la ligne contenant la case vide.

ligne 1	1	2	3	4
ligne 2	5	6	7	8
ligne 3	9	10	11	12
ligne 4	13	15	14	

Démonstration :

- La démonstration fonctionne par induction.
- Soit $P(n)$ = "Après n mouvements, la parité du nombre d'inversions est différente de la parité du numéro de la ligne contenant la case vide".
- *Cas de base :* $P(0)$ est vrai, car, initialement, le nombre d'inversions vaut 1, tandis que le numéro de la ligne contenant la case vide vaut 4.

- *Cas inductif :* Supposons que $P(n)$ soit vrai pour un $n \in \mathbb{N}$.
  - Si le mouvement $n+1$ est un mouvement de ligne, alors $P(n+1)$ est vrai car, la ligne contenant la case vide n'a pas changé, et par le lemme 3 la parité du nombre d'inversions n'est pas modifiée.
  - Si le mouvement $n+1$ est un mouvement de colonne, alors, par le lemme 3, la parité du nombre total d'inversions a été modifiée. De plus, la parité du numéro de la ligne contenant la case vide a été modifiée également. Donc, $P(n+1)$ est vrai.
- Dès lors, $P(n)$ implique $P(n+1)$ pour tout $n \in \mathbb{N}$.
- Par induction, $P(n)$ est vrai pour tout $n \in \mathbb{N}$. □

- Théorème : Aucune séquence de mouvements de permet d'obtenir la configuration de droite à partir de la configuration de gauche :

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Démonstration : Dans la configuration de droite, le nombre total d'inversions est de 0, tandis que la case vide est dans la ligne 4. Par le lemme 4, cette configuration n'est pas accessible. □