Jedidi Med Aziz
Mathématiques pour l'intelligence artificielle
Mardi 06 septembre 2022

Notes de cours 1 : Notions de bases sur les preuves

1. Différents types de preuves

1.1. **Preuve directe.**

Cette technique consiste simplement à supposer que P est vrai puis à faire des déductions logiques à partir de cette hypothèse jusqu'à parvenir à montrer que Q est vrai.

1.1.1. *Exemple.*

Prouver que la somme de deux nombre entiers impairs est paire.

Proof. Soient n_1, $n_2 \in \mathbb{Z}^2$ impairs, donc $\exists k_1, k_2 \in \mathbb{Z}^2$ tels que :

$$n_1 = 2k_1 + 1$$
$$n_2 = 2k_2 + 1$$

alors :

$$\begin{aligned} n_1 + n_2 &= (2k_1 + 1) + (2k_2 + 1) \\ &= 2k_1 + 1 + 2k_2 + 1 \\ &= 2k_1 + 2k_2 + 2 \\ &= 2(k_1 + k_2 + 1) \end{aligned}$$

Posons $K = k_1 + k_2 + 1$, la somme d'entiers est un entier donc $K \in \mathbb{Z}$.

Ainsi, $\exists K \in \mathbb{Z} : n_1 + n_2 = 2K$ et par suite $n_1 + n_2$ est pair. QUOD ERAT DEM■

1.2. **Preuve par disjonction des cas.**

Cette technique consiste simplement à traiter tout les cas possibles. Dans notre cas, nous allons expliciter le cas où n est paire puis celui où n est impaire.

1.2.1. *Exemple.*

Prouver que pour tout nombre entier n, $n^2 + n$ est pair..

Proof. Soit $n \in \mathbb{Z}$, montrons que $n + n^2$ est un nombre pair. Procédons par disjonction des cas :

Cas 1 (n paire) :

Supposons que n est pair, $\exists k \in \mathbb{Z}$ tel que $n = 2k$ Ainsi :

$$\begin{aligned} n^2 + n &= (2k)^2 + 2k \\ &= 4k^2 + 2k \\ &= 2(k^2 + k) \end{aligned}$$

Posons $K = k^2+k$, la somme et le carré d'entiers est un entier donc $K \in \mathbb{Z}$. Ainsi : $\exists K \in \mathbb{Z} : n+n^2 = 2K$ Donc pour n paire : $n + n^2$ est également paire.

Cas 2 (n impair) : Maintenant supposons que n est impair, $\exists k \in \mathbb{Z}$ tel que $n = 2k + 1$ Ainsi :

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

Posons $K = (2k+1)(k+1)$, la somme et le carré d'entiers est un entier donc $K \in \mathbb{Z}$. Ainsi : $\exists K \in \mathbb{Z}$: $n + n^2 = 2K$ Donc pour n paire : $n + n^2$ est également paire.

Ainsi que n soit pair ou impair, $n^2 + n$ est pair.

QUOD ERAT DEM■

1.3. **Preuve par récurrence.**

On peut envisager la récurrence lorsque l'on désire montrer une affirmation mathématique P(n) dépendant d'un certain paramètre naturel n . On procède alors en deux étapes :

1) L'initialisation : on montre que P(1) est vrai.
2) L'induction : on suppose que P(k) est vrai pour un certain naturel k , et on montre que P(k+1) est alors également vrai.

1.3.1. *Exemple.*

Montrer que pour tout entier n, $2^{3n+1} + 5$ *est un multiple de* 7.

Proof. Posons la propriété P : $\forall n \in \mathbb{N}, \exists kin\mathbb{Z} : 2^{3n+1} + 5 = 7k$.

1) Initialisation : Si n $= 0$, $2^{3*0+1} + 5 = 7 * 1$. La propriété P est donc vraie au rang 0 avec $k = 1$.
2) Hérédité : Supposons la propriété P vraie au rang n quelconque et montrons qu'elle est également vraie au rang $n + 1$:

$$\begin{aligned} 2^{3*(n+1)+1} + 5 &= 2^{3n+4} + 5 \\ &= 2^{3*(n+1)+1}.2^3 + 5 \\ &= (7k5)2^3 + 5 \\ &= (56k40) + 5 \\ &= 56k35 \\ &= 7(8k5) \end{aligned}$$

3) Conclusion : La propriété est vraie au rang 0. En supposant la propriété vraie au rang n elle est encore vraie au rang suivant avec $k_{n+1} = 8k - 5$.

   Par conséquent, par le principe de récurrence faible : $\forall n \in \mathbb{N}, \exists kin\mathbb{Z} : 2^{3n+1} + 5 = 7k$.

QUOD ERAT DEM■

1.4. **Preuve par l'absurde.**

1.4.1. *Exemple.*

Soit a un nombre rationnel et b un nombre irrationnel. Prouver que $a + b$ *est irrationnel.*

Proof. Par l'absurde, supposons que $a \in \mathbb{Q}$ et $b \notin \mathbb{Q}$ et $a + b \in \mathbb{Q}$:

Donc $\exists p_1, q_1 \in \mathbb{Z} \times \mathbb{N}^\star$ tels que : $a = \frac{p_1}{q_1}$

Donc $\exists p_2, q_2 \in \mathbb{Z} \times \mathbb{N}^\star$ tels que : $a + b = \frac{p_2}{q_2}$

donc $a + b - a = \frac{p_2}{q_2} - \frac{p_1}{q_1}$

donc $b = \frac{p_2 q_1 - p_1 q_2}{q_1 q_2}$

or $q_2 q_1 \in \mathbb{N}^\star$ et $(p_2 q_1 - p_1 q_2) \in \mathbb{Z}$ donc $b \in \mathbb{Q}$
c'est absurde car nous avions supposé que $b \notin \mathbb{Q}$

QUOD ERAT DEM■

1.5. **Preuve par contraposition.**

En logique propositionnelle, la proposition $P \implies Q$ est équivalente à sa contraposée $\neg Q \implies \neg P$. Une preuve par contraposition consiste à démontrer que l'on a $\neg Q \implies \neg P$ et donc par équivalence $P \implies Q$.

1.5.1. *Exemple.*

Montrer que si n est un nombre entier et n^2 est impair, alors n est impair.

Proof. Soit n un entier. Posons $P(n) : \exists k \in \mathbb{Z} : n^2 = 2k + 1$ et $Q(n) : \exists k \in \mathbb{Z} : n = 2k + 1$
La contraposée serait : $\neg P(n) : \exists k \in \mathbb{Z} : n^2 = 2k$ et $\neg Q(n) : \exists k \in \mathbb{Z} : n = 2k$
Soit $\neg P(n)$ vraie, montrons que $\neg Q(n)$ est vraie. Soit n un entier pair, ainsi $\exists k \in \mathbb{Z} : n = 2k$:

$$\begin{aligned} &\exists k \in \mathbb{Z} : n^2 = (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2) \end{aligned}$$

Ainsi $\exists K \in \mathbb{Z} : n^2 = 2K$ avec $K = 2k^2$ et $K \in \mathbb{Z}$ car K produit d'entiers donc un entier.
Ainsi la contraposée est vraie donc pour n entier, si n^2 est impair, alors n est impair.

QUOD ERAT DEM■

2. Algèbre linéaire

2.1. **Fonction linéaire.**

Soit la fonction :

$$\begin{aligned} F:\mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (x,y) &\longmapsto (x+y, x-y) \end{aligned}$$

Prouvons que f est une fonction linéaire :

Soient $\alpha, \beta \in \mathbb{R}^2$ et soient $(u,v) \in \mathbb{R}^2 \times \mathbb{R}^2$.

Notons $u = (u_1, u_2)$ et $v = (v_1, v_2)$ alors :

$\alpha u + \beta v = (\alpha(u_1) + \beta v_1, \alpha u_2 + \beta v_2)$

donc :

$f(\alpha u + \beta v) = (\alpha u_1 + \beta v_1 + \alpha u_2 + \beta v_2, \alpha u_1 + \beta v_1 - \alpha u_2 - \beta v_2)$

d'autre part :

$\alpha f(u) + \beta f(v) = \alpha(u_1 + u_2, u_1 - u_2) + \beta(v_1 + v_2, v_1 - v_2)$

Ainsi : $f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$

Nous avons prouvé que f est une fonction linéaire.

2.2. **Caractérisation d'une famille libre (Famille finie/infinie).**

Soient E un espace vectoriel et K son corps. Une famille (finie ou infinie) $(v_i)_{i\in I}$ de vecteurs de E est dite libre (constituée de vecteurs linéairement indépendants), si la seule combinaison linéaire des vecteurs viv_i égale au vecteur nul 0_E est celle dont tous les coefficients sont nuls (autrement dit : si toute combinaison linéaire des viv_i à coefficients non tous nuls est différente du vecteur nul).

- Pour une famille finiede vecteurs, $(v_i)_{1\leqslant i\leqslant v}$, la caractérisation s'énonce ainsi :
  $\forall (a_1, \ldots, a_n) \in K^n, \quad (a_1 v_1 + \cdots + a_n v_n = 0_E \Rightarrow a_1 = a_2 = \cdots = a_n = 0_K)\,.$

2.3. **Théorème (existence et unicité de la décomposition).**

Étant donné une base $V = (v_i)_{i\in I}$ de E, tout vecteur $v \in E$ peut-être décomposé sur cette base et cette décomposition est unique. Autrement dit :

$\forall vinE : \exists!(\lambda_1, \lambda_2, ..., \lambda_n) \in \mathbb{R}^n : f(v) = \sum_{i=1}^{n} \lambda_i w_i$

Aix-Marseille Université