Méthodologie : des quantificateurs à la preuve

1er mars 2024

Le but de cette fiche est de revenir sur une partie de ce qui a été vu au premier semestre concernant la logique et les différents types de raisonnement, et de voir comment cela peut s'appliquer concrètement pour démontrer des propositions simples d'algèbre linéaire.

1 Énoncés universels

1.1 Exemples

Considérons les propriétés suivantes, qui n'ont a priori pas grand chose de commun entre elles :

1. l'ensemble A est inclus dans l'ensemble B, noté $A \subset B$;
2. l'application $\varphi : E \to F$ entre $\mathbb{K}$-espaces vectoriels est une application linéaire ;
3. les vecteurs $x_1, \dots, x_n$ appartenant à E forment une famille libre.

Les énoncés formels définissant ces propriétés sont les suivants :

1. $\forall x \in A,\ x \in B$;
2. $\forall u \in E,\ \forall v \in E,\ \forall \lambda \in \mathbb{K},\ \varphi(u + \lambda v) = \varphi(u) + \lambda\varphi(v)$;
3. $\forall (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n,\ (\sum_{i=1}^n \lambda_i x_i = 0 \implies (\lambda_1, \dots, \lambda_n) = (0, \dots, 0))$.

Ce sont tous des énoncés commençant par le quantificateur universel $\forall$ et ne faisant pas intervenir d'autres quantificateurs. On peut aussi écrire ces énoncés en français, cela prend plus de place mais c'est souvent préférable :

1. tout x appartenant à A appartient à B ;
2. pour tous vecteurs u et v appartenant à E, pour tout scalaire λ appartenant à $\mathbb{K}$, on a
$$\varphi(u + \lambda v) = \varphi(u) + \lambda\varphi(v).$$
3. etc..

Remarque 1 *Tout énoncé commençant par $\forall x \in \emptyset$ est vrai, car l'ensemble vide n'a aucun élément. On peut facilement le prouver par l'absurde. En effet la négation d'un tel énoncé commence par $\exists x \in \emptyset$, ce qui est faux par définition.*

Exercice 1 *Nombres de propriétés définies en cours sont des énoncés universels. Par exemple : pour F un sous-ensemble d'un espace vectoriel E, les propriétés "F est stable pour l'addition" et "F est stable pour la multiplication". Définir en français ces propriétés puis les traduire en énoncés formels. Donner un exemple où F est stable pour l'addition et la multiplication mais n'est pas un sous-espace vectoriel.*

1.2 Comment utiliser un tel énoncé ?

En général cela ne pose pas de problèmes et se fait sans trop y penser. Au cours d'une preuve, ces énoncés universels peuvent être appliqués à n'importe quelle instance des variables quantifiées. Cette instance peut-être une valeur "concrète", comme le nombre réel 0 par exemple, ou n'importe quelle variable qui a été **introduite** auparavant. Voici un exemple (sans intérêt en lui même) d'utilisation de la linéarité d'une application.

Exemple 1 *Soient $\varphi : \mathbb{R}^2 \to \mathbb{R}^3$ une application linéaire et x un nombre réel. Alors par linéarité de φ on a*

$$\varphi(2;3) = \varphi(1;2) + \varphi(1;1)$$

et de plus

$$\varphi(x,x) = x\varphi(1,1).$$

On retiendra qu'il faut toujours **introduire** les variables qu'on utilise et faire attention au "**type**" des éléments qu'on manipule. Par exemple $(1;2)$ et $(x;x)$ sont bien des éléments de $\mathbb{R}^2$, car on a pris soin d'introduire x en tant que nombre réel auparavant. Il est donc légitime de leur appliquer l'application φ.

1.3 Comment prouver un tel énoncé ?

Le premier point à retenir vaut de manière générale : les preuves doivent être rédigées en **français** et non dans un langage formel. Il s'agit d'écrire un raisonnement mathématique destiné à un humain. Cela signifie par exemple qu'on n'utilisera pas les quantificateurs $\forall$ et $\exists$ dans une preuve [1]. Ces derniers sont réservés aux énoncés formels. De même on n'utilisera pas les symboles logiques $\wedge, \vee, \implies$ [2].

Deuxièmement, dans la grande majorité des cas, la méthode pour prouver un énoncé commençant par "pour tout" consiste à **introduire** un élément arbitraire du type souhaité et à raisonner sur cet élément pour arriver à la conclusion voulue.

Plus concrètement voici à quoi pourrait ressembler le début d'une preuve dans nos trois exemples.

1. Soit x appartenant à A. Montrons que x appartient à B.
2. Soient u et v des vecteurs de l'espace vectoriel E. Soit λ appartenant à $\mathbb{K}$. Montrons que
$$\varphi(u + \lambda v) = \varphi(u) + \lambda\varphi(v).$$

1. à moins qu'on veuille écrire un énoncé formel, par exemple pour définir un ensemble, mais cela n'est pas si fréquent.
2. à l'exception éventuellement de $\Rightarrow$ et $\Leftrightarrow$ dans les résolutions d'équations

3. Soient $\lambda_1, \ldots, \lambda_n$ appartenant à $\mathbb{K}$ des scalaires. Supposons que

$$\sum_{i=1}^{n} \lambda_i x_i = 0.$$

Montrons que pour tout entier i compris entre 1 et n on a $\lambda_i = 0$.

Quelques remarques :

— l'usage de la locution "*Montrons que*" ou d'un équivalent permet d'organiser la preuve et de la rendre compréhensible pour le lecteur ;
— encore une fois toutes les variables qui apparaissent doivent avoir été introduites (ici on suppose que A, B, φ, E, $\mathbb{K}$, $(x_i)_{1\leq i\leq n}$ nous sont donnés, i.e. ont été introduits auparavant) ;
— dans le troisième exemple pour démontrer une implication on pose l'hypothèse et on cherche à démontrer la conclusion.

Bien sûr il n'est pas possible d'aller plus loin dans la preuve si l'on n'en sait pas plus sur les ensembles/applications/vecteurs à l'étude. Pour des exemples concrets de preuves de linéarité d'application on peut se référer au TD 3 exercices 1 et 2. Pour des preuves de liberté d'une famille de vecteurs on peut se référer au devoir encadré, exercices 2, 3 et 4. Noter que le nom donné aux variables ainsi que leur numérotation varie d'un exercice à l'autre, mais que le canevas de la preuve varie peu.

Exercice 2 *Refaire (sans recopier) une ou plusieurs des preuves du cours que certains sous-ensembles sont des sous-espaces vectoriels. On a le choix parmi : la somme ou l'intersection de deux sous-espaces vectoriels, l'image directe ou réciproque d'un sous-espace vectoriel par une application linéaire, $\mathcal{L}(E,F) \subset F^E$.*

2 Énoncés existentiels

2.1 Exemples

On s'intéresse maintenant à des énoncés commençant par "Il existe"/$\exists$ et ne faisant intervenir aucun autre quantificateurs. Les premiers exemples sont donnés par les négations des énoncés de la section précédentes. Ainsi formellement la négation de la propriété de linéarité est l'énoncé :

$$\exists u \in E,\ \exists v \in E,\ \exists \lambda \in \mathbb{K},\ \varphi(u+\lambda v) \neq \varphi(u) + \lambda\varphi(v)$$

Comme vu en cours, la linéarité équivaut à la compatibilité avec l'addition et la multiplication. Ainsi pour les espaces vectoriels l'énoncé précédent équivaut à :

$$(\exists u \in E,\ \exists v \in E,\ \varphi(u+v) \neq \varphi(u) + \varphi(v))$$

$$\vee\, (\exists u \in E,\ \exists \lambda \in \mathbb{K},\ \varphi(\lambda u) \neq \lambda\varphi(u))$$

Exercice 3 *Écrire la négation des deux autres énoncés de la section précédente ; en français ou comme un énoncé formel au choix.*

On peut aussi donner un exemple plus direct. Ainsi considérons $f : A \to B$ une application entre ensembles. Alors par définition l'image de f est :

$$\mathrm{Im}(f) = \{y \in B \mid \exists x \in A,\ f(x) = y\}.$$

La propriété "appartenir à l'image de f" est donc un énoncé existentiel (existence d'un antécédent).

2.2 Comment utiliser un tel énoncé ?

Là encore c'est assez intuitif. Si on sait qu'un énoncé d'existence est vérifié alors on est autorisé à introduire un élément vérifiant la propriété considérée. Concrètement voici ce que cela donne avec l'exemple précédent.

Exemple 2 *Supposons qu'au cours d'une preuve on soit amené à considérer un élément y appartenant à l'image d'une application f. On pourra alors rencontrer l'argument suivant :*

"L'élément y est dans l'image de f. ***Soit donc*** *x appartenant à A tel que $f(x) = y$."*

Il n'arrive par contre à peu près jamais qu'on soit amené à utiliser des propriétés du type "telle application n'est pas linéaire", ou "tel sous-ensemble n'est pas un sous-espace vectoriel" dans une preuve. En effet cela apporte très peu d'informations.

2.3 Comment prouver un tel énoncé ?

Pour prouver un énoncé d'existence, il faut exhiber une valeur vérifiant la propriété. Concrètement, voici à quoi cela peut ressembler :

"Posons $u_0 = \ldots$ et $\lambda_0 = \ldots$ et montrons que $\varphi(\lambda_0 u_0) \neq \lambda_0 \varphi(u_0)$."

Dans le cas particulier où il s'agit de mettre en défaut une propriété telle que la linéarité d'une application, on dit qu'on exhibe un contre-exemple à la propriété (cf. TD 3 exercices 1 et 2).

Cependant tester des valeurs aléatoires ne sera pas une stratégie viable dans de nombreux cas. Une des solutions consiste à raisonner par analyse-synthèse pour comprendre quelle valeur va fonctionner. La rédaction prendra donc la forme suivante :

On cherche x vérifiant [insérer la propriété].

Analyse. Supposons donc que x est tel que [insérer la propriété]. Alors, nécessairement..

Synthèse. Posons donc x =[insérer une des valeurs possibles obtenues], et vérifions que x convient.

Remarque 2 *Si dans la phase d'analyse on montre qu'il y a une unique valeur de x possible, alors on aura démontré à la fin de la preuve à la fois l'existence et l'unicité.*

3 Un exemple

Beaucoup d'énoncés mathématiques utilisent les deux quantificateurs. Il faut alors combiner ce qu'on a vu dans les deux sections précédentes. Comme exemple, nous allons redémontrer différemment la conclusion de l'exercice 6 du TD 3.

Soit $n \leq 1$ un entier. On rappelle que si $A = (a_{i,j})_{1 \leq i,j \leq n}$ est une matrice de $\mathcal{M}_n(\mathbb{R})$ on définit sa transposée A^T par :

$$A^T := (a_{j,i})_{1 \leq i,j \leq n}.$$

Autrement dit, cela revient à échanger lignes et colonnes, ou encore à prendre le symétrique de la matrice par rapport à la diagonale. Par exemple la transposée de la matrice

$$\begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}$$

est la matrice

$$\begin{pmatrix} 1 & 0 \\ 2 & 4 \end{pmatrix}.$$

On voit que la transposée est une application linéaire de $\mathcal{M}_n(\mathbb{R})$ dans lui-même et que pour toute matrice A on a $(A^T)^T = A$.

On définit maintenant deux sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{R})$, nommés respectivement le sous-espace des matrices symétriques et celui des matrices antisymétriques de $\mathcal{M}_n(\mathbb{R})$.

$$\mathcal{S}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) | A^T = A\}$$

$$\mathcal{A}_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) | A^T = -A\}$$

Exercice 4 *Démontrer que $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont supplémentaires dans $\mathcal{M}_n(\mathbb{R})$.*

Comment aborder cet exercice ? On commence par comprendre et expliciter ce que l'on veut démontrer. Ici on souhaite montrer que pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$, il existe d'uniques matrices B et C telles que :
— $A = B + C$;
— $B^T = B$;
— $C^T = -C$.

Soit donc $A \in \mathcal{M}_n(\mathbb{R})$. On va raisonner par analyse synthèse pour trouver B et C convenables. Au passage on démontrera aussi l'unicité.

Analyse. Supposons donc que B et C *sont* des matrices appartenant à $\mathcal{M}_n(\mathbb{R})$ telles que :
— $A = B + C$;
— $B^T = B$;
— $C^T = -C$.
On va utiliser ces équations pour exprimer B et C en fonction de A. Appliquer la transposée à la première équation implique par linéarité de la transposition :

$$A^T = B^T + C^T.$$

Les deux équations restantes impliquent alors :

$$A^T = B - C$$

Mais alors nécessairement :

$$A + A^T = 2B.$$

Finalement on obtient :

$$B = \frac{1}{2}(A + A^T);$$
$$C = \frac{1}{2}(A - A^T).$$

Ceci démontre l'unicité sous réserve d'existence.

Synthèse. *Posons*

$$B := \frac{1}{2}(A + A^T)$$
$$C := \frac{1}{2}(A - A^T)$$

et *vérifions* que B et C conviennent.

Tout d'abord :

$$\begin{aligned} B + C &= \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T) \\ &= A. \end{aligned}$$

Ensuite par linéarité de la transposition :

$$\begin{aligned} B^T &= \frac{1}{2}(A^T + (A^T)^T) \\ &= \frac{1}{2}(A^T + A) \\ &= B \end{aligned}$$

De même :

$$\begin{aligned} C^T &= \frac{1}{2}(A^T - (A^T)^T) \\ &= \frac{1}{2}(A^T - A) \\ &= -C. \end{aligned}$$

Finalement on a bien prouvé l'existence et l'unicité d'une décomposition convenable de A. On conclut que $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont supplémentaires dans $\mathcal{M}_n(\mathbb{R})$.

Remarque 3 *Finalement le seul endroit dans la preuve où il y a besoin de réfléchir se situe dans le calcul de B et C en fonction de A dans la phase d'analyse.*

L'énoncé formel que l'on a démontré est le suivant :

$$\forall A \in \mathcal{M}_n(\mathbb{R}), \exists!(B, C) \in \mathcal{S}_n(\mathbb{R}) \times \mathcal{A}_n(\mathbb{R}), A = B + C.$$

On voit que la structure de la preuve reflète la structure de l'énoncé. Nul besoin cependant de faire apparaître cet énoncé formel ! Il vaut mieux écrire en français comme on l'a fait ici au tout début de la preuve.

4 Mémo

Quelques locutions essentielles à employer dans la rédaction :
— "*Montrons que...*", "*On va...*" : pour **annoncer** ce que l'on va démontrer, afin que le raisonnement soit compréhensible ;
— "*Soit x...*", "*Posons x...*" : pour **introduire les variables** ;
— les connecteurs logiques habituels.

Quelques canevas élémentaires de démonstration, selon le type d'énoncé qu'on veut démontrer :
— $\forall x \in A,\ P(x)$: "Soit $x \in A$. Montrons $P(x)$."
— $\exists x \in A,\ P(x)$: "Posons $a := \ldots$. Montrons $P(a)$."
— $P \Rightarrow Q$: "Supposons que P est vraie. Montrons que Q est vraie."
— $P \Leftrightarrow Q$: on raisonne par double implication.
— $P \vee Q$: "Supposons que P est fausse. Montrons que Q est vraie.".

Ne pas oublier le raisonnement par analyse-synthèse (lorsque l'on cherche quelle valeur poser dans une preuve), ou encore le raisonnement par l'absurde (par exemple si on n'a pas réussi autrement).

Ne pas hésiter à bien **expliciter** le résultat que l'on veut démontrer et à procéder pas à pas pour y arriver. Dans la plupart des cas, cela rend évident quel calcul il faut poser (par exemple un système linéaire à résoudre) ou quel théorème du cours il faut invoquer (par exemple le théorème de la base incomplète).

Enfin, il faut acquérir certains réflexes propres à l'algèbre linéaire. Par exemple les arguments de dimension sont omniprésents et permettent d'économiser des calculs pour montrer qu'une famille de vecteurs est une base, que deux sous-espaces vectoriels coïncident ou au contraire sont supplémentaires.