NOTES DE COURS POUR LE COURS MATHÉMATIQUES DISCRÈTES MAT1500

ABRAHAM BROER

Références

[R] Kenneth H. Rosen, *Mathématiques discrètes, Édition révisée* Chenelière McGraw-Hill, 2002.

1. But à long terme : Développer un bon sens critique

Même si vous voulez devenir un actuaire ou un statisticien, il faut bien comprendre comment les mathématiques fonctionnes. Il ne faut pas penser qu'il est possible de bien utiliser les mathématiques sans en avoir une comprehension fonctionnelle. Chaque résultat en mathématiques vient avec une preuve ou une explication pourquoi le résultat soit vrai. Pas seulement le *Comment* compte mais aussi le *Pourquoi*, la comprehension.

Aussi il faut comprendre pourquoi on passe du concret à l'abstraction. Oui, les exemples restent toujours importants ; mais la reflection sur ce qui est en commun dans beaucoup de problèmes, l'abstraction, restera toujours important. Aussi dans la vraie vie on le fait tout le temps, mais presque toujours implicitement. Il faut développer la capacité de voir qu'un genre de solution, naturelle pour un genre de problèmes, peut s'appliquer aussi à d'autres problèmes qui ne semblent pas du tout semblables.

C'est ça que nous voulons commencer de faire ce premier trimestre : nous allons moins insister sur le *Comment* et plus insister sur le *Pourquoi* ; on va essayer de développer votre sens critique et votre comprehension de certains abstractions.

Dans le cours de MAT1600 on va commencer à montrer encore une fois comment résoudre un système d'équations linéaires, ce qui est très pratique dans beaucoup de situations déjà. Mais après on donne des abstractions moins et moins évidentes, par exemples d'opérateurs linéaires et vecteurs propres. En MAT1400 on va expliquer, encore une fois, c'est quoi un "dérivé" et un "intégral", et puis calculer des exemples. Mais ici aussi, les preuves et les abstractions seront de plus en plus importants.

C'est naturel de penser : "Calcul et algèbre linéaire ? J'ai vu tout ça déjà au cégep ; et l'abstraction : ça ne m'intéresse passe et est inutile pour un actuaire, statisticien, ou économe. Je suis déjà content si je sais comment calculer quelque chose, si le prof dit que je l'ai fait correctement, ça me suffit."

Certainement, les enseignants ne sont pas d'accord. Il faut développer un bon sens critique, si on veut ou pas. Et ça commence par vouloir comprendre les subtilités des *Pourquoi* et l'abstraction. Et de résoudre des exercices soi-même ou avec un petit peu d'aide. Et de développer le réflexe que si

Date: 11 janvier 2016.

on fait une erreur (ce qui arrivera régulièrement et est normal !), d'aller chercher *soi-même* l'erreur dans l'argument. Ça peut prendre des heures de temps, de temps en temps, oui et c'est normal et cela arrive aux meilleurs mathématiciens au monde. (Remarque : Selon les normes de l'université, pour bien réussir un cours de 4 crédits, il faux en moyenne dépenser $3 * 4 = 12$ heures de votre temps et concentration par semaine sur la matière de ce cours !) Le processus d'apprentisage est lent, ça prend du temps et un effort soutenu. Mais c'est certain que si vous réussissez votre bacc en math avec une moyenne raisonnable vous aurez développé très considérablement votre esprit critique. Les diplômés d'un baccalauréat ont la réputation enviable d'être capable de bien analyser et de résoudre des problèmes de façon efficace.

Comprendre *plus ou moins* ne suffit plus dans le monde : pas en mathématiques, ni dans le monde de la haute finance, de l'assurance, de la technologie, et cetera. Mais si vous avez un bon sens critique en mathématique, très probablement vous avez aussi un bon sens critique dans d'autres domaines scientifique. Malheureusement pas nécessairement dans tous les situations sociales (en questions d'amour par exemple), car la "*logique*" utilisée dans une telle situation est différente. Il faut travailler sur l'esprit critique sociale aussi : mais les cours de mathématiques ne vont pas aider grandement.

De MAT1400 et MAT1600 vous connaissez déjà *plus ou moins* la matière ; donc c'est le moment pour vous habituer à faire de plus d'attention aux définitions, contre-exemples et preuves et abstractions. Ça va vous aider grandement dans les cours d'analyse mathématique abstraite MAT1000 et MAT2050, qui posent beaucoup de problèmes aux étudiants qui ne sont pas suffisamment (mathématiquement) adulte.

Exemple 1.1. On a une collection de sept objets, dont deux d'une couleur et les cinq autres d'une autre couleur. Question : En combien de façons *différents* peut-on en choisir trois ?

Vous donnez peut-être tout de suite donnez une réponse, en utilisant une formule que vous connaissez ! Mais ce sera trop vite répondu. Car il manque d'information, ou de l'information restée implicite.

Qu'est-ce que veut dire "différents". L'ordre du choix importe ? Choisir avec remise ? Dans les vrai vie on peut toujours distinguer des objets, mais ce n'est pas ça ce qui importe. Est-ce qu'on *veut* distinguer tous les sept objets ? Ou veut-on que tous les objets sont considérés comme distincts. Ou veut-on que la seule distinction entre ces objets est la couleur. Sans préciser on ne peut pas répondre, car la réponse dépend de ces conditions.

$(1, 3, 4, \frac{7\cdot 6\cdot 5}{3\cdot 2\cdot 1}, 7 \cdot 6 \cdot 5, 7^3, \ldots$ sont tous des réponses correctes, dépendant de ce que veut dire "différents". Pouvez vous trouvez des conditions qui correspondent à ces solutions ?)

1.1. **Le cours MAT1500, les mathématiques discrètes.** Le cours de mathématiques discrètes n'est pas une version approfondie d'un cours suivi par tout le monde au collège. Ce sera un peu de nouveau pour vous. Mais de l'autre côté : la matière n'est pas nouvelle du tout. On a rencontré déjà les concepts, mais souvent seulement de façon implicit.

Sans doute vous avez déjà rencontré les ensembles, leurs éléments, et leurs sous-ensembles. Puis les applications (ou fonctions) d'un ensemble dans un autre ensemble. Mais quand-même, nous allons en discuter au début.

Pour donner, ou critiquer, des arguments mathématiques il faut avoir un certain idée de quel genre d'arguments est acceptable, et de quel genre d'arguments ne l'est pas. On va expliciter les règles de la logique sous-jacentes. Aussi la rédaction d'une preuve d'une proposition mathématique utilise des règles de la logique. Par exemple, une *preuve par contradiction* , c'est quoi et est-ce que c'est valide ?

Il y a une méthode de preuve qui utilise de l'induction ("C'est vrai si on prend $n = 1$, $n = 2$ et $n = 3$ ..., donc c'est vrai pour tout n."), est-ce que c'est acceptable ? Oui, une version d'induction est acceptée (d'autres ne le sont pas). L'induction *mathématique* est basée sur les propriétés des nombres entiers. Nous allons rendre explicit ces propriétés élémentaires. Vous "connaissez" déjà la plupart de ces propriétés, mais il s'agit ici aussi de fournir des preuves.

Après nous allons *compter* le nombre d'éléments de certains ensembles, comme dans la théorie des probabilités. On va établir plusieurs principes de comptage de base. Et appliquer ces principes dans les situations concrètes, et faire reconnaître quel principe s'applique. Car la différence est subtile à saisir pour un débutant avec un sens critique encore faible. On va expliquer pourquoi deux problèmes, qui semblent différent à la première vue, peuvent avoir la même réponse (avec la notion de bijection). Si on comprend seulement *plus ou moins* la théorie, on va facilement faire des erreurs, et pire, insister qu'on avait raison plus ou moins ("ma réponse mérite plus de points dans la correction").

2. Ensembles

2.1. **Ensembles et éléments.** [1] *Ensembles* et leurs *éléments* sont une modélisation mathématique de l'idée de collections de différents objets de la vraie vie. Un *ensemble* E est une collection d'objets, appelé les *éléments* de E. On écrit

$$x \in E,$$

si x est un élément de E et $x \notin E$ sinon. L'ensemble sans éléments, l'*ensemble vide*, est noté $\emptyset$.

Si un ensemble E a seulement un nombre fini n d'éléments différents, on dit que c'est un ensemble fini et n est la *taille* ou la *cardinalité* de E. On écrit

$$|E| = n \text{ (ou aussi comme } \#E = n).$$

Soient $e_1, e_2, \ldots, e_n$ les éléments différents de E, alors on écrit

$$E = \{e_1, e_2, \ldots, e_n\}$$

Par exemple l'ensemble "Chiffres" des chiffres décimales :

$$\text{Chiffres} := \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\},$$

et l'ensemble vide peut s'écrire comme $\emptyset = \{\}$. On utilise le symbole ":=" pour indiquer c'est une égalité par définition. Ou l'ensemble des lettres dans l'alphabet français

$$\text{Alphabet} := \{a, b, c, d, \ldots, x, y, z\}.$$

On utilise "..." s'il est clair au lecteur ce qu'il faut écrire pour compléter.

1. Voir aussi [R, §1.4].

Deux ensembles E_1 et E_2 sont considérés comme égaux si les deux ensembles ont les mêmes éléments. En particulier, le même ensemble peut avoir plusieurs noms. Aussi un même élément donné peut avoir plusieurs noms. Il existe seulement un ensemble vide. Aussi

$$\{0,1,2,3,4,5,6,7,8,9\} = \{4,3,2,1,0,9,5,6,7,8\};$$

car l'ordre de l'énumération des éléments n'importe pas. Normalement on fait une énumération des éléments sans répétitions, mais on a le droit de répéter dans une liste définissant un ensemble même élément plusieurs fois, mais ça reste le même ensemble. Par exemple

$$\{0,1,2,3,4,5,6,7,8,9\} = \{0,1,2,2,3,3,3,4,4,4,5,5,5,5,6,6,6,6,6,7,8,9\}.$$

a dix éléments (différents).

Remarque. Dans les mathématiques on utilise surtout des ensembles. Mais de temps en temps on utilise aussi le concept de "ensemble-avec-multiplicités", appelé *multi-ensemble*. C'est comme un ensemble, mais chaque élément vient avec une multiplicité fixée. Par exemple $\{a,b,b,c,c,c,c\} = \{a^1,b^2,c^4\}$ représente un multi-ensemble basé sur l'ensemble {a,b,c}, où par exemple c apparaît avec la multiplicité 4, ou l'élément c "apparaît" exactement quatre fois dans ce multi-ensemble.

Supposons qu'on a une boîte qui contient 7 objets ; un de type a, deux de type b et quatre de type c. L'ensemble des types différents est $\{a,b,c\}$. Si on ne veut pas distinguer deux objets du même type (même si on peut distinguer !), on va modéliser par le multi-set $\{a^1,b^2,c^4\}$. Par contre si on veut (et peut) différencier les deux objets de type b, disons b_1 et b_2, et les quatre objets de type c, disons c_1,c_2,c_3,c_4 on peut modéliser par l'ensemble (ordinaire) de sept éléments $\{a,b_1,b_2,c_1,c_2,c_3,c_4\}$.

Ça dépend du problème qu'on veut résoudre quel ensemble (ou multi-ensemble) on utilise :

$$\{a,b,c\}, \{a^1,b^2,c^4\} \text{ ou } \{a,b_1,b_2,c_1,c_2,c_3,c_4\}?!$$

Ça dépend !

On discutera les multi-ensembles un peu plus tard, car il sont utiles pour certains problèmes de comptage. Pour le moment il suffit de savoir que le concept de élément-répété existe dans les multi-ensembles, mais pas dans les ensembles : dans un ensemble le même élément apparaît exactement une fois.

2.2. **Sous-ensembles.** Soient F et E deux ensembles. Si chaque élément de F est aussi un élément de E, on dit que F est un *sous-ensemble*, et on écrit $F \subseteq E$. On a $F \subseteq E$ et $E \subseteq F$ si et seulement si $E = F$:

Lemme 2.1 (Sandwich)**.** *Soient F et E deux sous-ensembles d'un ensemble U. Si $F \subseteq E \subseteq F$ alors $F = E$.*

Démonstration. $F \neq E$ est seulement le cas si (i) il existe un $e \in E$ tel que $e \notin F$ ou (ii) il existe un $f \in F$ tel que $f \notin E$.

Mais le cas (i) est impossible, car $E \subseteq F$ (ce qui veut dire par définition de "sous-ensemble" que pour chaque $e \in E$ on a $e \in F$). Et le cas (ii) est aussi impossible, car $F \subseteq E$.

Donc ce n'est pas vrai que $F \neq E$. IL suit que nécessairement $F = E$. □

Soit E un ensemble et P une propriété qu'un élément de E peut avoir. Alors

$$\{e \in E; e \text{ a propriété } P\} \quad \text{ou} \quad \{e \in E | \ e \text{ a propriété } P\}$$

est par définition le sous-ensemble de E des éléments e de E qui ont la propriété P. Il faut que ce soit claire : chaque $e \in E$ a cette propriété, ou ne l'a pas. Pas de zone grise.

Disons E l'ensemble de tous les femmes étudiantes à l'université de Montréal et P la propriété d'être nées avant le 1 janvier 1990. Alors $\{e \in E; e \text{ a propriété } P\}$ est l'ensemble des femmes étudiantes à l'Université de Montréal nées avant le 1 janvier 1990.

Remarque. Dans la vrai vie on utilise seulement *une* notion d'appartenir à une collection. Aux mathématiques on utilise deux notions. L'un est "être élément de", et l'autre est "être sous-ensemble de". Soit $a \in A$ un élément. Alors le sous-ensemble de A qui contient seulement a, $\{a\}$, est un sous-ensemble de A et n'est pas un élement de A. Nous distinguons entre $a \in A$ et $\{a\} \subset A$, mais dans la vraie vie on pense peut-être : "C'est la même chose, non ?". En effet, NON, pas en mathématique.

Et c'est bon comme ça, ça évitera beaucoup de confusion plus tard ! Il faut s'habituer à cette distinction tout de suite.

Remarque. Dans la réalité pas chaque "sous-collection" est tout de suite un sous-ensemble, car la définition d'appartenance pourrait être trop vague. Par exemple, considérons la collection P des personnes et la "sous-collection" A des adultes. Et prenons une personne, disons Adrien. Alors Adrien $\in P$. Il devrait avoir *deux* possibilités seulement : soit Adrien$\in A$ soit Adrien $\notin A$ (pas les deux simultanément). Mais ce n'est pas clair : oui, il est adulte physiquement, mais non, il n'est pas adulte mentalement. Qu'est-ce qu'on décide ? Il faut avoir un critère stricte. Pas de zone grise pour définir les (sous-)ensembles. Si vous voulez modéliser des (sous-)collections par la théorie mathématique des (sous-)ensembles il faut être précis dans vos définitions.

Remarque. Nous avons défini l'alphabet français comme

$$\text{Alphabet} := \{a, b, c, d, \ldots, x, y, z\}.$$

C'est clair j'espère ? Je ne suis pas si certain. Il y a beaucoup de symboles semblables, mais légèrement différents :

a, a, a, A, $\mathbf{a}$, A, A, A, A, ...

Nous avons fait une abstraction sophistiquée dans la vraie vie : nous considérons que tous ces symboles représentent le même élément $a \in$ Alphabet, sans répétition. L'élément $a \in$ Alphabet est vraiment "une classe d'équivalence de symboles" similaires d'un certain façon (en langue mathématique encore à expliquer).

C'est une des abstractions que les bêtes ont une plus grande difficulté de faire que les humains. Ce n'est pas si facile, notre définition de l'ensemble Alphabet. La réalité est dur à comprendre, car il y a tellement beaucoup d'abstractions non-explicites et des sous-entendus ! Les mathématiques sont beaucoup plus simples, car les règles sont plus claires. Ce qui est difficile est de décider de comment d'utiliser les mathématiques dans les problèmes de la vraie vie.

2.3. **Union, intersection et complément.** [2]

2. Voir aussi [R, §1.5]

Soient E et F deux sous-ensembles d'un ensemble U. *L'intersection* $E \cap F$ est l'ensemble des éléments $u \in U$ qui sont simultanément éléments de E et de F. Deux ensembles sont *disjoints* si leur intersection est l'ensemble vide.

L'union $E \cup F$ est l'ensemble des éléments $u \in U$ qui sont éléments de E ou de F (c'est permis d'être élément des deux simultanément aussi).

Souvent on s'imagine implicitement un (très grand) ensemble U (l'ensemble *universel* pour la discussion) contenant comme éléments tous les objects on peut imaginer ou construire. On imagine que chaque ensemble est sous-ensemble de cet ensemble universel. Dans ce cas on définit $E \cup F$ comme réunion dans cet ensemble U.

La *différence* de E et F, notée $E - F$ (où $E \backslash F$) est l'ensemble de tous les éléments de E qui ne sont pas élément de F. Si $E \subseteq F$ est un sous-ensemble, alors on définit le *complément* $\overline{E} = F - E$ (ce qui dépend de F), est l'ensemble de tous les éléments de F qui ne sont pas élément de E. Alors $\overline{\overline{E}} = E$.

Par exemple :

$$\{1,2,3,4,5\} \cap \{4,5,6,7\} = \{4,5\}, \{1,2,3,4,5\} - \{4,5,6,7\} = \{1,2,3\}$$

et

$$\{1,2,3,4,5\} \cup \{4,5,6,7\} = \{1,2,3,4,5,4,5,6,7\} (= \{1,2,3,4,5,6,7\}).$$

Il y a quelques propriétés, pour la plupart évidentes.

Proposition 2.1. *Soient A, B et C trois sous-ensemble de l'ensemble U.*
(i) $A \cup \emptyset = A$; $A \cap U = A$ ("Identité") ;
(ii) $A \cup U = U$; $A \cap \emptyset = \emptyset$ ("Domination") ;
(iii) $A \cup A = A = A \cap A$ ("Idempotence") ;
(iv) $\overline{(\overline{A})} = A$ ("Complémentarité") ;
(v) $A \cap B = B \cap A$; $A \cup B = B \cup A$ ("Commutativité") ;
(vi) $A \cup (B \cup C) = (A \cup B) \cup C$; $A \cap (B \cap C) = (A \cap B) \cap C$ ("Associativité") ;
(vii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ("Distributivité") ;
(viii) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$, $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ ("Lois de De Morgan").

Démonstration. La vérité de la plupart des propositions est facile à vérifier. Nous avons fait ainsi en classe. Essayez encore une fois de vous convaincre de cela.

(vii) On veut montrer que $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Soit $u \in U$ tel que $u \in A \cap (B \cup C)$. Alors par définition de l'intersection nécessairement $u \in A$ et $u \in (B \cup C)$. Alors par définition de l'union $u \in B$ ou $u \in C$ (ou u est dans tous les deux). Donc ($u \in A$ et $u \in B$) ou ($u \in A$ et $u \in C$). Donc $u \in A \cap B$ ou $u \in A \cap C$. Donc $u \in (A \cap B) \cup (A \cap C)$. Donc chaque élément u de $A \cap (B \cup C)$ est aussi un élément de $(A \cap B) \cup (A \cap C)$. Nous avons donc montré que $A \cap (B \cup C)$ est un sous-ensemble de $(A \cap B) \cup (A \cap C)$.

Soit maintenant $u \in U$ tel que $u \in (A \cap B) \cup (A \cap C)$. Par définition de $\cup$ ça veut dire que $u \in (A \cap B)$ ou $u \in (A \cap C)$ (ou dans tous les deux). Mais $u \in (A \cap B)$ veut dire que $u \in A$ et $u \in B$. Et $u \in (A \cap C)$ veut dire que $u \in A$ et $u \in C$. Il suit que certainement $u \in A$ mais aussi que $u \in B$ ou $u \in C$, i.e., $u \in B \cup C$. Donc $u \in A \cap (B \cup C)$ et nous avons montré que chaque

élément de $(A \cap B) \cup (A \cap C)$ est aussi un élément de $A \cap (B \cup C)$. Donc nous avons montré que $(A \cap B) \cup (A \cap C)$ est un sous-ensemble de $A \cap (B \cup C)$.

En utilisant le lemme du sandwich, lemme 2.1, on conclut : $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$.

Montrer (viii) est un exercice aux tp. □

2.4. **Constructions d'ensembles à partir d'ensembles donnés.** Nous pouvons construire beaucoup d'autres ensembles à partir des ensembles déjà donnés.

Définition 2.1. *Soit E un ensemble. L'ensemble des sous-ensembles (ou la* puissance*) d'un ensemble E est noté $P(E)$* [3].

Donc un *élément* de $P(E)$ est par définition un sous-ensemble de E. Vous comprenez ?

On va voir que pour chaque ensemble E on a $|P(E)| = 2^{|E|}$; en particulier $|P(\emptyset)| = 1$ (=exercice de compréhension).

Exemple 2.1. Si $E = \{a, b, c\}$, alors $P(E) = \{\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Il faut bien comprendre : on peut maintenant considérer $\{a, b\}$ comme sous-ensemble de E, mais aussi comme élément de $P(E)$. Et $\{\{a, b\}\}$ comme sous-ensemble de $P(E)$ et comme élément de $P(P(E))$.

La réunion $E \cup P(E)$ a 11 éléments différents :

$$E \cup P(E) = \{a, b, c, \{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

C'est comme ça ; dans la théorie d'ensembles on a décidé de voir a et $\{a\}$ comme deux éléments différents de $E \cup P(E)$. Et

$$E \cap P(E) = \emptyset.$$

En particulier :

$$E \cap P(E) \neq \{\emptyset\}$$

(vous comprenez la différence ? !).

Remarque. En pratique on voudrait peut-être de temps en temps "identifier a avec $\{a\}$". C'est possible de faire ainsi avec une construction dans la théorie d'ensembles avec la notion de "relation d'équivalence" et "classe d'équivalence", ce qui viendra plus tard. La théorie d'ensembles vous force d'être précis. Si vous voulez "identifier a avec $\{a\}$" vous devez *le dire*, car ce n'est pas automatique (c.a.d. il faut définir une relation d'équivalence, et prendre les classes d'équivalence pour construire un nouveau ensemble, et tout ce tralala).

Définition 2.2. *Soient E et F deux ensembles. Le* produit cartésien *de E et F noté $E \times F$ est l'ensemble de tous les couples ordonnées (e, f) où $e \in E$ et $b \in F$* [4] *:*

$$E \times F = \{(e, f); e \in E \text{ et } f \in F\}.$$

Par exemple, si $E = \{1, 2, 3\}$ et $F = \{1, 2\}$ alors

$$E \times F = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}$$

a $3 \times 2 = 6$ éléments En particulier $(2, 3) \notin E \times F$.

L'exemple $\mathbb{R} \times \mathbb{R}$ est le plan ordinaire $\mathbb{R}^2$.

3. Voir aussi [R, p. 38].

4. Voir aussi [R, p. 39]

Remarque. Si E et F sont des ensembles finis, alors

$$|E \times F| = |E| \times |F|.$$

(Vous voyez pour quoi ?)

Exemple 2.2. Beaucoup de situations dans la vraie vie sont (implicitement) de ce type. Par exemple, un packet de 52 cartes de jeu.

$$\text{Valeurs} := \{2, 3, 4, 5, 6, 7, 8, 9, 10, V, D, R, A\}$$

(V= valet, D=dame, R=roy, A=as).

$$\text{Enseignes} := \{\heartsuit, \clubsuit, \diamondsuit, \spadesuit\}$$

$\heartsuit$ = coeur (hearts), $\clubsuit$ = trèfle (clubs),$\diamondsuit$ = carreau (diamonds), $\spadesuit$ = pique (spades).

Essentiellement :

$$\text{Jeu de Cartes} = \text{Valeurs} \times \text{Enseignes}.$$

Exemple : $2\heartsuit$ et $A\clubsuit$ sont deux éléments de Jeu de Cartes.

Exemple 2.3. On peut répéter et obtenir le produit cartésien de trois (ou plus) d'ensembles. Par exemple, soit

$$\begin{aligned} \text{Heures} &:= \{00, 01, 02, \ldots, 23\}, \\ \text{Minutes} &:= \{00, 01, 02, \ldots, 59\}, \\ \text{Secondes} &:= \{00, 01, 02, \ldots, 59\}. \end{aligned}$$

Et

$$\text{Montre} := \text{Heures} \times \text{Minutes} \times \text{Secondes}.$$

Par exemple $(10h : 35m : 29s) \in \text{Montre}$.

Exemple 2.4. Soient E et F deux ensembles. On pourrait aussi considérer l'ensemble de tous les ensembles $\{e, f\}$ où $e \in E$ et $b \in F$. Dans se cas $\{e, f\} = \{f, e\}$ et on obtient quelque chose essentiellement différente de $E \times F$, si $E \cap F \neq \emptyset$, mais beaucoup moins utile que le produit cartésien.

Par exemple, si $E = \{1, 2, 3\}$ et $F = \{1, 2\}$ alors on obtiendrais par définition.

$$\{\{1,1\},\{1,2\},\{2,1\},\{2,2\},\{3,1\},\{3,2\}\} = \{\{1\},\{1,2\},\{2\},\{3,1\},\{3,2\}\},$$

si on enlève les répétitions il reste 5 éléments !

Vous comprenez la différence avec $E \times F$?

Définition 2.3. *Soit E un ensemble et $n > 0$ un entier. On définit E^n comme l'ensemble des suites ordonnées $(e_1, e_2, \ldots, e_n)$ de longueur n d'éléments de E.*

Ici : l'ordre des coefficients importe, et des répétitions sont permises ! Par exemple, $(1, 2, 2) \in \mathbb{N}^3$ et $(1, 2, 2) \neq (2, 1, 2) \neq (1, 2)$.

(Comparez avez les sous-ensembles de $\mathbb{N}$ définis par ces suites $\{1, 2, 2\} \subseteq \mathbb{N}$ et $\{1, 2, 2\} = \{2, 1, 2\} = \{1, 2\}$.)

Exemples :

$$\{0,1\}^3 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$$

and

$$\{a,b,c\}^2 = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\}.$$

Remarque. Si E est un ensemble fini et $n > 0$ un entier. Alors

$$|E^n| = |E|^n.$$

Vous voyez pourquoi ?

2.5. **Fonctions.** Dans les mathématiques modernes les fonctions entre les ensembles sont au moins aussi importantes que les ensembles soi-mêmes, sinon plus importantes !

Définition 2.4. *Soient A et B deux ensembles. Une fonction F de A dans B,*

$$F : A \to B,$$

est l'affectation d'exactement un élément de B, noté $F(a) \in B$, attribué par F à $a \in A$, et ça pour chaque $a \in A$. [5]

On dit aussi "application" à la place de "fonction".

Définition 2.5. *Soit $F : A \to B$ une fonction.*

(i) Alors A est appelé le domaine *de F, et B le* codomaine *de F.*

*(ii) Soit $a \in A$ et posons $b := F(a) \in B$. Alors b est appelé "l'image de a par F" et a est "*une *préimage de b".*

(iii) Le sous-ensemble de B formé des images des éléments de A est appelé l'image (ou la portée) de F, $\operatorname{Im} F$.

Donc F est une règle que définit pour chaque $a \in A$ une (seule !) image dans B. Mais pas chaque b a une préimage, et il peut exister plusieurs préimages pour un $b \in B$ donné ou aucune.

On peut définir une fonction par un formule. Vous avez l'habitude. Par exemple la fonction :

$$F : \mathbb{N} \to \mathbb{N},\ F(m) = m^2 + 1.$$

On peut aussi définir une fonction F "élément par élément" : Par exemple, on définit la fonction

$$F : \text{Chiffres} \to \text{Alphabet},$$

par $F(0) = a, F(1) = b, F(2) = a, F(3) = z, F(4) = y, F(5) = c, F(6) = a, F(7) = x, F(8) = t, F(9) = o$. Nous allons une notation plus claire et plus compacte, mais qui donne la même information :

$$F = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ a & b & a & z & y & c & a & x & t & o \end{pmatrix}$$

Ici, la première ligne donne une liste de tous les éléments du domaine de la fonction. La deuxième ligne donne les images correspondantes.

5. Voir [R, p. 54].

Remarquez :

$$\begin{aligned} F &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ a & b & a & z & y & c & a & x & t & o \end{pmatrix} \\ &= \begin{pmatrix} 9 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 0 \\ o & b & a & z & y & c & a & x & t & a \end{pmatrix} \end{aligned}$$

Tous les éléments de Chiffres apparaissent dans la première ligne, mais pas tous les éléments de Alphabet dans la deuxième. Et $\{2, 6, 0\}$ est le sous-ensemble de tous les préimages de a : $F(2) = F(6) = F(0) = a$. Mais q n'a aucun préimage.

Permis ? Permis !

2.6. **Composition de fonctions.** Si le codomaine d'une fonction est égal au domaine d'une autre fonction, on peut composer ces deux fonctions.

Définition 2.6. *Soit $F : A \to B$ et $G : B \to C$ deux fonctions.*

Alors la composition est la fonction

$$G \circ F : A \to C$$

définie par

$$(G \circ F)(a) = G(F(a)).$$

Donc $G \circ F$ est d'abord appliquer F et puis appliquer G !

Exemple 2.5. Soit $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $C = \mathbb{N}$. Et $F : A \to B$ donnée par

$$F := \begin{pmatrix} a & b & c \\ 3 & 2 & 4 \end{pmatrix};$$

$G : B \to C$ donnée par

$$G := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 13 & 23 & 33 & 4344 \end{pmatrix}.$$

Alors $G \circ F : \{a, b, c\} \to \mathbb{N}$:

$$G \circ F = \begin{pmatrix} a & b & c \\ 33 & 23 & 4344 \end{pmatrix}$$

Par exemple

$$(G \circ F)(c) = G(F(c)) = G(4) = 4344.$$

Exemple 2.6. Soit $F : \mathbb{N} \to \mathbb{N}$, $F(n) = n^2 + 1$ et $G : \mathbb{N} \to \mathbb{N}$, $G(n) = n^3 + n$. Alors $F \circ G : \mathbb{N} \to \mathbb{N}$ et $G \circ F : \mathbb{N} \to \mathbb{N}$ sont données par :

$$(F \circ G)(n) = F(G(n)) = F(n^3 + n) = (n^3 + n)^2 + 1$$

et

$$G \circ F(n) = G(F(n)) = G(n^2 + 1) = (n^2 + 1)^3 + (n^2 + 1).$$

Exercice 2.1. Soient $F_1 : A \to B$, $F_2 : B \to C$ et $F_3 : C \to D$ trois fonctions. Montrer que $F_3 \circ (F_2 \circ F_1) = (F_3 \circ F_2) \circ F_1$ comme fonctions de A dans D.

2.7. **Quelques exemples de fonctions.**

Exemple 2.7. Est-ce que

$$F : \mathbb{N} \to \mathbb{N},\ F(m) = \frac{m(m+1)(m+5)}{3}$$

est une fonction ? On a des doutes, car $\frac{m(m+1)(m+5)}{3}$ semble être une fraction, et pas un nombre naturel. Mais nous allons montrer que le numérateur de cette fraction est toujours divisible par 3, donc après division il reste un nombre naturel, comme on voulait. Donc c'est une fonction.

Lemme 2.2. *Si* $m \in \mathbb{N}$ *alors* $F(m) = \frac{m(m+1)(m+5)}{3} \in \mathbb{N}$.

Démonstration. Soit $m \in \mathbb{N}$. Il y a trois cas possibles : existe un nombre naturel a tel que (i) $m = 3a$ ou (ii) $m = 3a + 1$ ou (iii) $m = 3a + 2$.

En cas (i) : on a

$$F(m) = F(3a) = \frac{3a(3a+1)(3a+5)}{3} = a(3a+1)(3a+5) \in \mathbb{N};$$

en cas (ii) on a

$$F(m) = F(3a+1) = \frac{(3a+1)(3a+2)(3a+6)}{3} = (3a+1)(3a+2)(a+2) \in \mathbb{N};$$

et en cas (iii) on a

$$F(m) = F(3a+2) = \frac{(3a+2)(3a+3)(3a+7)}{3} = (3a+2)(a+1)(3a+7) \in \mathbb{N}.$$

Dans tous les cas $F(m) \in \mathbb{N}$. □

Exemple 2.8. Soit A un ensemble. La *fonction identité* est la fonction $1_A : A \to A$ où

$$1_A(a) = a$$

pour chaque $a \in A$.

Soit $A \subseteq B$ un sous-ensemble. La *fonction inclusion* est la fonction $\iota : A \to B$:

$$\iota(a) = a$$

pour chaque $a \in A$.

Si

$$A = \{a, 1, \heartsuit, \pi, \emptyset\},\ B = \{a, b, c, 1, 2, 3, \heartsuit, \clubsuit, \pi, \emptyset, \}$$

alors

$$1_A = \begin{pmatrix} a & 1 & \heartsuit & \pi & \emptyset \\ a & 1 & \heartsuit & \pi & \emptyset \end{pmatrix}$$

et

$$\iota_A = \begin{pmatrix} a & 1 & \heartsuit & \pi & \emptyset \\ a & 1 & \heartsuit & \pi & \emptyset \end{pmatrix}.$$

La *différence* entre 1_A et ι est le codomaine (mais la portée et la formule sont les mêmes).

Remarque. Soit $F : A \to B$ et $G : D \to C$ deux fonctions et $B \subset D$. On peut quand-même définir la composition, en utlisant $\iota : B \to D$, comme la composition $G \circ (\iota \circ F)$. Est-ce que c'est ça qu'on voudrait Oui.

2.8. **L'ensemble des fonctions entre deux ensembles.** Soient A et B deux ensembles. Nous notons

$$\text{Fonctions}(A,B) \text{ (ou aussi } B^A),$$

pour l'ensemble de toutes les fonctions différentes de A dans B. Donc un élément de $\text{Fonctions}(A,B) = B^A$ est par définition une fonction de A dans B.

Exemple :

$$\begin{aligned}\text{Fonctions}(\{1,2\},\{a,b,c\}) &= \{F_1 = \begin{pmatrix}1 & 2\\ a & a\end{pmatrix}, F_2 = \begin{pmatrix}1 & 2\\ a & b\end{pmatrix}, F_3 = \begin{pmatrix}1 & 2\\ a & c\end{pmatrix} F_4 = \begin{pmatrix}1 & 2\\ b & a\end{pmatrix}, F_5 = \begin{pmatrix}1 & 2\\ b & b\end{pmatrix},\\ &\quad F_6 = \begin{pmatrix}1 & 2\\ b & c\end{pmatrix}, F_7 = \begin{pmatrix}1 & 2\\ c & a\end{pmatrix}, F_8 = \begin{pmatrix}1 & 2\\ c & b\end{pmatrix}, F_9 = \begin{pmatrix}1 & 2\\ c & c\end{pmatrix}\}\end{aligned}$$

Remarque. Si A et B sont deux ensembles finis, alors

$$|\text{Fonctions}(A,B)| = |B^A| = |B|^{|A|}.$$

Vous voyez pourquoi ? Ça devrait expliquer l'alternatif de notation un peu étrange :

$$\text{Fonctions}(A,B) = B^A.$$

2.9. **Injectivité, surjectivité et bijectivité.** Une fonction peut avoir des propriétés. Les suivantes sont les plus importantes.

Définition 2.7. *Soit $F : A \to B$ une fonction. On dit que*

(i) F est injective si $F(a_1) = F(a_2)$ seulement si $a_1 = a_2$.

(ii) F est surjective si chaque élément de B est l'image d'un élément de A.

(iii) F est bijective si chaque élément de B est l'image d'un seul élément de A.

Conclusion : F est bijective si et seulement si F est injective et surjective. Par exemple, la fonction inclusion ι est injective, et la fonction identité 1_A est bijective.

Proposition 2.2. *Soit la fonction $F : A \to B$ donnée par la notation "deux-lignes" (sans répétitions dans la première ligne), disons*

$$F = \begin{pmatrix}a_1 & a_2 & a_3 & \dots & a_n\\ f_1 & f_2 & f_3 & \dots & f_n\end{pmatrix}.$$

Alors la fonction est

(i) injective si et seulement si chaque élément de B se trouve au maximum une fois sur la 2-ième ligne ;

(ii) surjective si et seulement si chaque élément de B se trouve au minimum une fois sur la 2-ième ligne ;

(iii) bijective si et seulement si chaque élément de B se trouve exactement une fois sur la 2-ième ligne.

Démonstration. (i) Supposons que chaque élément de B se trouve au maximum une fois sur la deuxième ligne. Montrons par une *preuve directe* que F est injective .

Soient a et a' des éléments de A tels que $b = F(a) = F(a')$. Ces deux éléments a et a' se trouvent sur la première ligne, c'est à dire ils existent i et j tels que $a = a_i$ et $a' = a_j$ et donc $F(a) = F(a_i) = f_i$, $F(a') = f(a_j) = f_j$. Nous avons que $b = f_i = f_j$. Mais b se trouve au maximum une fois sur la 2-ième ligne. Ça veut dire $i = j$ et donc $a = a_i = a_j = a'$. Alors nous avons montré que F est injective (si chaque élément de B se trouve au maximum une fois sur la deuxième ligne).

Supposons F est injective. Nous allons montrer par une *preuve indirecte* que chaque élément de B se trouve au maximum une fois sur la deuxième ligne.

Supposons $b \in B$ se trouve au moins deux fois sur la 2-ième ligne, disons à positions i et j ($i \neq j$). Donc $b = f_i = f_j$. Mais $f_i = F(a_i)$ et $f_j = F(a_j)$, alors $F(a_i) = F(a_j)$ et $a_i \neq a_j$. Donc F n'est pas injective. On conclut la preuve indirecte que si F est injective alors chaque élément de B se trouve au maximum une fois sur la deuxième ligne.

Ça finit la preuve de (i).

(ii) et (iii) : exercices. □

2.10. **Taille et bijectivité.**

Exemple 2.9. Soit $A := \{a, b, c\}$ et $B := \{1, 2, 3, 4\}$.

$F_1 : A \to B$ définie par $F_1 := \begin{pmatrix} a & b & c \\ 3 & 2 & 1 \end{pmatrix}$ est injective,

$F_2 : B \to A$ définie par $F_2 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ a & b & c & a \end{pmatrix}$ est surjective. Il n'existe pas de fonction de A dans B qui est surjective et il n'existe pas de fonction de B dans A qui est injective. Vous voyez pourquoi ?

Cet exemple est motivation pour la proposition suivante et sa preuve.

Proposition 2.3. *Soient A et B deux ensembles finis.*

(i) Il existe une fonction injective $F : A \to B$ si et seulement $|A| \leq |B|$.

(ii) Il existe une fonction surjective $F : A \to B$ si et seulement si $|A| \geq |B|$.

(iii) Il existe une fonction bijective $F : A \to B$ si et seulement si $|A| = |B|$.

Démonstration. Avant de commencer les preuves, fixons une suite ordonnée *sans répétitions* des éléments de A, disons

$$A = \{a_1, a_2, \ldots, a_n\}$$

où $n = |A|$. Il y a beaucoup de façons, mais fixons une manière.

Et fixons aussi une suite ordonnée sans répétitions des éléments de B, disons

$$B = \{b_1, b_2, \ldots, b_m\}$$

où $m = |B|$.

(i) Supposons il existe une fonction injective $F : A \to B$. Nous voulons montrer $|A| \leq |B|$. Montrons d'abord par une *preuve par l'absurde* que dans la suite ordonnée $(F(a_1), F(a_2), \ldots, F(a_n))$ il n'y a pas de répétition.

Sinon, il y a $i \neq j$ tels que $F(a_i) = F(a_j)$. Par la définition d'injectivité il suit que $a_i = a_j$. Mais dans la suite choisie des a_k's il n'y a pas de répétions. Donc $i = j$. et au même temps $i \neq j$.

Ce qui est absurde. Donc en effet, dans la suite ordonnée $(F(a_1), F(a_2), \ldots, F(a_n))$ il n'y a pas de répétitions.

Il suit que le sous-ensemble

$$\mathrm{Im}(F) = \{F(a_1), F(a_2), \ldots, F(a_n)\} \subseteq B$$

a $n = |A|$ éléments différents. Et le fait que $\mathrm{Im}(F) \subseteq B$ implique que $|A| = |\mathrm{Im}(F)| \leq |B|$.

Nous venons de montrer que s'il existe une fonction injective $F : A \to B$ alors $|A| \leq |B|$..

Deuxième partie de la preuve de (i). Supposons $|A| \leq |B|$. Il faut montrer qu'il existe une fonction injective $F : A \to B$.

Définition d'une telle fonction, à l'aide de nos deux suites ordonnées choisies :

$$F(a_i) := b_i$$

pour chaque $1 \leq i \leq n = |A|$. Ou en notation "deux-lignes"

$$F := \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}.$$

Ça fait du sens, car $n \leq m = |B|$! C'est une fonction injective, car la deuxième ligne il n'y a pas de répétitions, prop. 2.2(ii). Donc en effet si $|A| \leq |B|$, alors il existe une fonction injective $F : A \to B$.

La preuve de (i) est complète.

(iii) Si on a montré (i) et (ii), alors (iii) en suit tout de suite.

La preuve de (ii) est une exercice. □

C'est surtout (iii) qui sera utilisé.

Remarque. On dit que deux ensembles, fini ou pas, A et B sont de même *cardinalité* s'il existe une bijection de A dans B, voir [R, p.71]. Par la proposition, si les deux ensembles sont finis, alors ils sont de même cardinalité si et seulement si $|A| = |B|$.

Si un ensemble A et l'ensemble $\mathbb{N}$ sont de même cardinalité on dit que A est *dénombrable*.

L'ensemble des nombres entiers, l'ensemble des fractions et l'ensemble des nombres premiers sont tous dénombrable. Mais l'ensemble des nombres réels n'est pas dénombrable.

2.11. **Fonction inverse.**

Théorème 2.1. *Soit $F : A \to B$ une fonction. Alors F est bijective* si et seulement si *il existe une fonction $G : B \to A$ telle que $F \circ G = 1_B$ et $G \circ F = 1_A$.*

Dans cette situation cette fonction G est unique, appelée la *fonction inverse* et notée

$$G = F^{-1}.$$

En fait, parce que F est bijective, pour chaque $b \in B$ il existe un unique $a \in A$ tel que $F(a) = b$. Alors $F^{-1}(b) = a$. Une fonction inverse existe seulement si la fonction est bijective.

Démonstration. (Supposons $F : A \to B$ est bijective. Définition d'une fonction $G : B \to A$: Soit $b \in B$, il existe un unique $a \in A$ tel que $F(a) = b$. Posons $G(b){:=}a$. Pour chaque $a \in A$ on a :

$$(G \circ F)(a) = G(F(a)) = G(b) = a.$$

Donc $G \circ F = 1_A$. Et pour chaque $b \in B$:

$$(F \circ G)(b) = F(G(b)) = F(a) = b.$$

Donc $F \circ G = 1_B$.

De l'autre côté, supposons qu'il existe une fonction $G : B \to A$ telle que $F \circ G = 1_B$ et $G \circ F = 1_A$. Soit $b \in B$. Définissons $a := G(b) \in A$. Alors

$$F(a) = F(G(b)) = (F \circ G)(b) = 1_B(b) = b.$$

Donc a est un préimage de b pour F. Nous avons montré que F est surjective.

Supposons $a_1, a_2 \in A$ tels que $F(a_1) = F(a_2)$. Donc

$$a_1 = 1_A(a_1) = (G \circ F)(a_1) = G(F(a_1)) = G(F(a_2)) = (G \circ F)(a_2) = a_2.$$

Donc F est aussi injective. On conclut la preuve, car une fonction surjective et injective est automatiquement bijective. □

Preuve du commentaire après le théorème. Supposons $F : A \to B$ est injective. Supposons $G : B \to A$ et $G' : B \to A$ telles que $G \circ F = 1_A$ et aussi $G' \circ F = 1_A$. Soit $b \in B$. Parce que F est bijective il existe un $a \in A$ tel que $F(a) = b$. Alors

$$G(b) = G(F(a)) = (G \circ F)(a) = 1_A(a) = (G' \circ F)(a) = G'(F(a)) = G'(b$$

Donc pour chaque $b \in B$ on a $G(b) = G'(b)$, c.-à-d., $G = G'$. □

Exemple 2.10. Soit $\mathbb{R}_{>0}$ l'ensemble des nombres réels strictement positifs.

L'application $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ est bijectif. Sa fonction inverse est $\ln : \mathbb{R}_{>0} \to \mathbb{R}$.

Exemple 2.11. Nous donnons un exemple d'une fonction bijective un peu plus compliqué à comprendre, mais la preuve n'est pas difficile.

Théorème 2.2. *Soient A et B deux ensembles non-vides. Supposons $n = |A|$ est fini. Il existe une fonction bijective ϕ : Fonctions$(A, B) \to B^n$.*

Ce théorème explique :

Corollaire 2.1. *Soient A et B deux ensembles finis non-vides. Posons $n = |A|$. On a*

$$|\text{Fonctions}(A, B)| = |B^n|.$$

Le corollaire est une conséquence directe du théorème et prop.2.3(iii).

Démonstration. Fixons une liste ordonnée des éléments de A, sans répétitions, disons $A = \{a_1, a_2, \ldots, a_n\}$. Posons $\phi : \text{Fonctions}(A, B) \to B^n$ par

$$\phi\left(F = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix}\right) := (b_1, b_2, b_3, \ldots, b_n) \in B^n.$$

La fonction inverse de ϕ est la fonction $\psi : B^n \to \text{Fonctions}(A, B)$

$$\psi((b_1, b_2, \ldots, b_n)) := F = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix}$$

Vous comprenez ces notations et pourquoi ψ est en effet l'inverse de ϕ ? Sinon, essayer de comprendre mot par mot, et compléter les détails. □

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA