NOTES DE COURS
MAT1500
MATHÉMATIQUES DISCRÈTES
AUTOMNE 2018

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

Chaque scientifique doit bien comprendre comment les mathématiques fonctionnent. Il est inpossible de bien utiliser les mathématiques sans en avoir une comprehension qui est au moins fonctionnelle. Chaque résultat en mathématiques vient avec une preuve ou au moins une explication pourquoi le résultat soit vrai. Pas seulement le *Comment* compte mais aussi le *Pourquoi*, c.-à-d. la comprehension.

Il faut aussi comprendre pourquoi on passe du concret à l'abstraction (et vice versa), et comment. Et faire la réflection sur ce qui est en commun dans beaucoup de problèmes. Dans la vraie vie on le fait tout le temps aussi, bien que souvent seulement implicitement. Il faut développer la capacité d'observer qu'un genre de solution, naturelle pour un genre de problèmes, peut s'appliquer aussi à d'autres problèmes qui semblent être très différents.

C'est ça que nous voulons commencer de faire ce 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. En particulier, nous allons insister au moins que chaque preuve soit comprise.

Dans le cours de MAT1600 on commence 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 exemple les opérateurs linéaires et les vecteurs propres. En MAT1400 on continue à discuter le *dérivé* et *l"intégral*, dans le cas où il y a plusieurs variables impliquées. Mais ici aussi, les preuves et les abstractions seront de plus en plus importantes. Dans le trimestre suivant le cours MAT1000 on refait les notions de limite, dérivé corrrectement et abstraitement : il faut avoir déjà une certaine maturité pour saisir les subtilités.

C'est naturel de penser : "Calcul et algèbre linéaire ? J'ai vu tout ça déjà au cégep. Et l'abstraction : c'est trop dur et ne m'intéresse pas trop. Ça me semble inutile pour un actuaire,

Date: 3 septembre 2018.

un statisticien, ou un économe. Je serai déjà content si je saurai comment calculer quelque chose de pratique. Si le prof me dit que je le fais correctement, ça me suffit. Je vais sauter, comme au cégep, toutes les preuves."

Certainement, les enseignants ici à l'université ne sont plus d'accord avec une telle approche. Il faut développer un bon sens critique, si on le veut ou pas. Et ça commence par *vouloir* comprendre au fond les subtilités des *Pourquoi* et de saisir la raison des abstractions.

Ce sens critique est développé le plus vite (mais quand-même lentement) si on essaie toujours de résoudre les exercices soi-même ou sinon avec peu d'aide. Et de développer vite le réflexe que si on fait une erreur (ce qui arrivera souvent et est normal !), d'aller chercher *soi-même* l'erreur dans l'argument. Ça prendra possiblement des heures de votre temps, mais c'est normal et cela arrive tout le temps, même aux meilleurs mathématiciens au monde.

Une remarque à propos de ce sujet, ce qui est aussi une différence avec l'expeerience au cégep. Selon les normes de l'université, pour bien réussir un cours de 4 crédits, comme MAT1500, il faut dépenser $3 * 4 = 12$ heures de votre temps et votre concentration en *moyenne* par semaine sur la matière de ce cours ! Un effort cégepien ne suffira plus. Donc si vous dépensez beaucoup de temps : c'est normal et nécessaire !

Le processus d'apprentissage est lent ; ça prend du temps et un effort soutenu. Mais il est certain que quand vous réussissez votre baccalauréat en mathématiques avec une moyenne raisonnable vous aurez développé très considérablement votre esprit critique. Les diplômés d'un baccalauréat en mathématiques 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 scientifiques.

Malheureusement ce n'est pas nécessairement vrai dans toutes les situations sociales, disons en questions d'amour par exemple. Car la *"logique"* utilisée dans une situation *sociale* est différente. C'est important de travailler sur *l'esprit critique sociale* aussi : mais les cours de mathématiques ne vont pas aider grandement.

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

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

Qu'est-ce que veut dire *"différents"*. Est-ce que l'ordre du choix importe ? Choisir avec remise ? Dans la vrai vie on peut toujours distinguer des objets, mais est-ce que ça importe dans ce problème ? Est-ce qu'on *veut* distinguer tous les sept objets ? Ou veut-on que la seule

distinction relevante entre ces objets soit la couleur. Sans préciser on ne peut pas répondre (ni correctement ni incorrectement), 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, mais sont dépendantes de ce qu'on veut dire avec "différents". Pouvez vous trouvez des conditions qui correspondent à ces solutions ? Et autres réponses raisonnables ? À rediscuter en détail plus tard dans le cours.)

1.1. **Le cours MAT1500, les mathématiques discrètes.** Le cours des 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 : une grande partie de la matière n'est pas nouvelle du tout. On a rencontré déjà les concepts, mais souvent seulement d'une façon implicite.

Sans doute vous avez déjà rencontré les *ensembles*, leurs *éléments*, et leurs *sous-ensembles*. Puis les *fonctions* (ou applications) d'un ensemble dans un autre ensemble. Mais quand-même, nous allons en discuter au début. De nouveau pour vous, peut-être, sera la notion de *relation d'équivalence* avec l'ensemble de ses classes d'équivalence.

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*, souvent utilisée par les Grecs antiques comme Platon et Euclide, c'est quoi et est-ce que c'est encore accepté comme une preuve valide ? En fait, oui.

Il y a une méthode de preuve, super utile, qui utilise 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 naturels. Nous allons rendre explicit ces propriétés élémentaires. Vous "connaissez" déjà la plupart de ces propriétés, mais il s'agit ici aussi de fournir les preuves. Nous donnerons plusieurs preuves de ce type.

Ensuite, pour généraliser les notions de *pair* et *impair*, nous allons introduire la relation d'équivalence *modulo* n avec ses classes d'équivalence. Et va calculer un peu avec ses classes, comme "*impair* fois *impair* = *impair*".

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).

À la fin du cours nous allons résoudre quelques problèmes des mathématiques discrètes par les méthode de calcul et algèbre linéaire. Car en mathématiques tout est lié.

Le manuel de Rosen [R] n"est pas obligatoire pour le cours. Tout sera inclu dans ses notes de cours (et les transparents fournis et les exercices).. Mais le manuel est quand-même recommandé pour de la lecture indépendante. Dans les notes de cours les sections relevant du manuel sont indiquées. Le livre donne plus d'exemples, entre autres, mais ne donne pas toutes les preuves.

Et dans ce cours on doit insister sur toutes les preuves : c'est la raison d'être de ce cours, et les notes de cours.

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. Pour chaque objet x, il y a exactement deux possibilités : soit $x \in E$, soit $x \notin E$ (et donc jamais moitié-moitié).

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

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

Si l'ensemble E n'a pas un nombre fini d'éléments on écrit $|E| = \infty$.

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

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

(on écrit une liste de tous les éléments entre deux accolades).

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

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

Commentaire : on a utilisé le symbole ":=" ici pour indiquer que "la partie à la droite de := est la définition de la partie à la gauche".

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 devrait écrire pour compléter.

Remarque. Nous venons de définir l'alphabet français comme

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

C'est clair j'espère ? Mais ....

Il y a beaucoup de symboles semblables, mais légèrement différents :

1. Voir aussi [R, §1.4].

a, a, a, A, **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 millions d'abstractions que font les humains intuitivement. Philosophiquement notre définition de l'ensemble Alphabet n'est pas si facile. La réalité est souvent dur à comprendre de façon précise, car il y a tellement beaucoup d'abstractions non-explicites et aussi tellement beaucoup de sous-entendus ! Les mathématiques sont beaucoup plus simples, car les règles sont plus claires. Ce qui est difficile est de décider de comment utiliser les mathématiques dans les problèmes de la vraie vie.

Définition 2.1. *Deux ensembles E_1 et E_2 sont considérés comme égaux si les deux ensembles ont exactement les mêmes éléments. On écrit $E_1 = E_2$.*

Par exemple si $E_1 := \{1, 2, 3\}$ et $E_2 = \{3, 2, 1\}$, alors $E_1 = E_2$, c'est à dire E_1 et E_2 sont deux noms pour ce même ensemble de trois éléments. Donc le même ensemble peut avoir plusieurs *noms*.

Aussi un même objet peut porter plusieurs noms.

Mais $\{1, 2, 3\} \neq \{a, b, c\}$, parce que $1 \in \{1, 2, 3\}$, mais $1 \neq \{a, b, c\}$. Il y a beaucoup d'ensembles de trois éléments.

Un ensemble sans élément s'appelle un *ensemble vide*. Peuvent-t-ils exister deux ensembles vides différents. Mais non. Voici un premier résultat avec preuve, de quelque chose fort évidente ! C'est une conséquence de la définition.

Proposition 2.1. *Il existe un seul ensemble vide.*

Démonstration. Définissons $V := \{\}$. C'est un ensemble avec zero elements, donc au moins un ensemble vide existe !

Supposons V_1 est aussi un ensemble vide et x un objet quelconque. Alors on n'a jamais $x \in V$ et on n'a jamais $x \in V_1$, parce que V et V_1 n'ont pas d'élément. En particulier :

L'objet x est un élément de V *si et seulement si* x est un élément de V_1. Donc par la *définition d'égalité d'ensembles* on conclut que $V = V_1$. □

Nous adoptons la *notation* suivante pour l'ensemble vide : $\emptyset := \{\}$.

Un premier exercice, aussi évident. Mais donner les arguments au complet.

Exercice 2.1. Soient A et B deux ensembles finis. Vrai ou faux (donner vos argument !)

(i) Si $A = B$, alors nécessairement $|A| = |B|$?

(ii) Si $|A| = |B|$,alors nécessairement $A = B$?

(ii) Si $|A| = |B| = 0$, alors nécessairement $A = B$?

2.1.1. *L'ordre des éléments dans un ensemble n'importe pas.* On a

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

parce que les deux ensembles ont les mêmes éléments. L'*ordre de l'énumération* des éléments n'importe pas. Normalement on fait une énumération des éléments sans répétition, mais on a le droit de répéter dans une liste définissant un ensemble un même élément plusieurs fois, mais ça reste le même ensemble.

Et c"est souvent très pratique !

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 exactement dix éléments différents.

2.1.2. *Multi-ensembles vs. ensembles.* 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-ensemble $\{a^1,b^2,c^4\}$. Par contre si on veut (et si on 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 ils 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.** La définition de sous-ensemble.

Définition 2.2. *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 *de E, et on écrit $F \subset E$ (ou $E \supset F$).*

Exemple 2.1. Si $E = F$ alors nécessairement $E \subset F$ (et $F \subset E$). Parce que, par définition $E = F$ veut dire que E et F ont les mêmes éléments, donc en particulier chaque élément de E est aussi un élément de F.

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, c.-a-d. $\{a\}$, 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 mathématiques.

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

2.2.1. *Définir des sous-ensembles par des propriétés de ces éléments.* Soit E un ensemble et P une propriété qu'un élément de E peut avoir ou pas. 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 née 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 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 V de vêtements, avec la "sous-collection" R des vêtements rouges. Et prenons un T-shirt originalement rouge mais lavé trop souvent et devenu un genre de rose. Est ce qu'on le met encore dans le sous-collection de vêtements rouge R ou pas ? Il ne faut pas avoir de zone grise pour définir les (sous-)ensembles ou les éléments. Si vous voulez modéliser des (sous-)collections par la théorie mathématique des (sous-)ensembles il faut être précis dans vos définitions.

2.2.2. *Dire la même chose de différents façons.* On peut dire des choses en français courant de plusieurs façons, mais aussi en mathématiques.

Exercice 2.2. (a) Soient E et F deux ensembles. Est-ce que c'est dire la même chose :

(i) On a $F \subset E$ si pour chaque objet x c'est vrai que *si x est un élément de F alors x est nécessairement aussi un élément de E.*

(ii) On a $F \subset E$ si pour chaque objet x c'est vrai que *x est nécessairement un élément de E si x est un élément de F.* (Et si x n'est pas un élément de F ?).

(iii) On a $F \subset E$ si pour chaque objet x c'est vrai que *si x n'est pas un élément de E alors nécessairement x n'est pas un élément de F.*

(iv) On a $F \subset E$ si pour chaque objet x c'est vrai que *x est un élément de F seulement si aussi x un élément de E.* (Et si $x \in E$?)

(b) Et si pour chaque objet x c'est vrai que *$x \in E$ seulement si $x \in F$* ? Et si pour chaque objet x c'est vrai que *$x \in F$ si $x \in E$* ?

(c) Argumenter pourquoi : $F \subset E$ et $E \subset F$ sont simultanément vraies si pour chaque objet x on a "$x \in E$ *si et seulement si* $x \in F$".

C'est un problème des mathématiques (ou de la logique), et pas seulement de la langue française.

Nous allons encore souvent utiliser les bouts de phrase : "seulement si", "si" et "si et seulement si", donc il sera très utile de bien comprendre cet exercice !

2.2.3. *Le théorème du sandwich.* Voici un deuxième résultat évident, mais souvent utilisé. Si $E = F$ alors nécessairement $E \subset F$ et $F \subset E$) (par exemple 2.1). Mais aussi si $F \subset E$ et $E \subset F$ alors nécessairement $E = F$ (voir aussi exercice 2.2(c)).

Théorème 2.1 (Le théorème du Sandwich)**.** *Soient F et E deux ensembles. Si $F \subset E \subset F$ alors $F = E$.*

Démonstration. Supposons F et E sont deux ensembles tels que $F \subset E$ et $E \subset F$.

Et supposons temporairement aussi, par contre, que $F \neq E$. Par la définition d'égalité d'ensemble ça veut dire que ce n'est pas vrai que E et F ont les mêmes éléments. Donc

(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, parce qu'on suppose $E \subset F$ (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 $F \subset E$.

Donc (sous les hypthèses que $F \subset E$ et $E \subset F$) ce n'est pas vrai que $F \neq E$.

Il suit que (sous les hypothèses que $F \subset E$ et $E \subset F$) nécessairement $F = E$. Ce qui était à montrer. □

C'est une preuve valide, mais il y en a d'autres qui sont valides aussi. C'est une question de goût. Mais n'importe, vous devez être capable de valider cette preuve, même si vous ne l'aimez pas !

Voici une autre preuve, un peu plus directe, qui est aussi valide (mais, en fait les deux preuves sont logiquement équivalentes comme nous allons voir plus tard) :

Démonstration. Supposons F et E sont deux ensembles, tels que (i) $F \subset E$ et (ii) $E \subset F$.

Par définition de sous-ensembles on obtient

(i) Si $x \in F$ alors aussi $x \in E$;

(ii) Si $x \in E$ alors aussi $x \in F$.

Sous ces hypothèses nous voulons montrer que $E = F$.

Il faut montrer que E et F ont les mêmes éléments. Soit x un objet. Si $x \in E$ alors par l'hypothèse (ii) on a aussi $x \in F$, et si $x \in F$ alors par l'hypothèse (i) on a aussi $x \in E$. (C'est aussi possible que x n'est ni un élément de E, ni de F : mais dans ce cas nous n'avons rien à vérifier.)

En autre mots E et F ont les mêmes éléments (ou $x \in E$ si et seulement si $x \in F$).

Il suit que $F = E$, ce qui était à montrer. $\square$

On avoue, le théorème du sandwich est évident. Mais c'est plutôt la logique utilisée dans les preuves qu'il faut comprendre. On en discutera encore.

2.3. **Définitions de l'union, de l'intersection, de la différence et du complément.** [2]
Soient E et F deux sous-ensembles d'un ensemble U. Commençons par donner quelques définitions.

L'intersection $E \cap F$ est par définition le sous-ensemble de U des éléments $u \in U$ qui sont simultanément éléments de E et de F.

On dit que deux ensembles sont *disjoints* si leur intersection est l'ensemble vide.

L'union $E \cup F$ est par définition 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).

La *différence* de E et F, notée $E - F$ (où $E \backslash F$) est par définition l'ensemble de tous les éléments de E qui ne sont pas élément de F.

Si $E \subset F$ est un sous-ensemble, alors on définit le *complément* $\overline{E} = F - E$ (ce qui dépend de F), comme le sous-ensemble de tous les éléments de F qui ne sont pas élément de 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

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

Remarque. Souvent dans les mathématiques, on s'imagine implicitement un (très, 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.

Il y a quelques propriétés de base, pour la plupart évidentes.

Proposition 2.2. *Soient A, B et C trois sous-ensembles 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").

2. Voir aussi [R, §1.5]

Démonstration. La vérité de la plupart des propositions est facile à vérifier et à montrer. Nous avons fait ainsi en classe. Voici une preuve de (vii).

(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 $u \in C$ (possiblement u est dans tous les deux). Donc on a deux possibilités : ($u \in A$ et $u \in B$) ou ($u \in A$ et $u \in C$). Donc, par la définition de l'intersection, $u \in A \cap B$ ou $u \in A \cap C$. Donc, par la définition de l'union, $u \in (A \cap B) \cup (A \cap C)$. Nous venons de montrer que chaque élément u de $A \cap (B \cup C)$ est aussi un élément de $(A \cap B) \cup (A \cap C)$, donc par la définition de sous-ensemble, nous avons ainsi 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 $u \in (A \cap C)$ (possiblement u est dans tous les deux). Mais, par la définition de l'intersection, $u \in (A \cap B)$ 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 $u \in C$, c.à-d., $u \in B \cup C$, par la définition de l'union. Donc $u \in A \cap (B \cup C)$, par la définition de l'intersection. Nous avons ainsi montré que chaque élément de $(A \cap B) \cup (A \cap C)$ est aussi un élément de $A \cap (B \cup C)$. Donc, par la définition de sous-ensemble, nous avons montré que $(A \cap B) \cup (A \cap C)$ est un sous-ensemble de $A \cap (B \cup C)$.

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

Exercice 2.3. Montrer vous-même au moins (viii).

2.4. **Constructions d'ensembles à partir d'ensembles donnés.** Nous pouvons construire beaucoup d'autres ensembles à partir des ensembles déjà donnés. La possibilité de faire des constructions est la raison pourquoi les ensembles sont tellement importants : on peut construire presque n'importe quoi en mathématique en commençant disons avec les nombres naturels ! Nous donnons les deux constructions les plus importantes. Avec ces deux constructions et $\cap, \cup, ..$ nous pouvons déjà beaucoup faire.

Définition 2.3. *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 2.2. 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 $P(P(E))$.

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

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 des ensembles en utilisant la notion de "relation d'équivalence" et "classe d'équivalence", ce qui viendra plus tard. La théorie d'ensembles nous 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 2.4. *Soient E et F deux ensembles non-vides. 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 $f \in F$* [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 $\mathbb{R}^2$.

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

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

(Vous voyez pour quoi ?)

Exemple 2.3. 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).

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

4. Voir aussi [R, p. 39]

$\heartsuit$ = 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 2.4. 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 2.5. Soient E et F deux ensembles. On pourrait aussi considérer l'ensemble de tous les ensembles $\{e, f\}$ où $e \in E$ et $f \in F$. 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 2.5. *Soit E un ensemble non-vide et $n > 0$ un entier. On définit E^n comme l'ensemble des* suites ordonnées $(e_1, e_2, \ldots, e_n)$ *d'éléments de E de longueur n.*

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 $\{1, 2, 2\} \subset \mathbb{N}$ 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 2.6. *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". Donc une fonction $F : A \to B$ est une manière d'associer à chaque élément $a \in A$ un certain élément de B, noté $F(a)$.

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

(i) 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, appelé la notation deux-lignes, 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 2.8. *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 2.6. 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 2.7. 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 2.4. 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 2.8. 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 2.1. *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 2.9. 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 $A \subset B$ 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 : l'ensemble $\text{Fonctions}(\{1, 2\}, \{a, b, c\})$ est

$$\{F_1 = \begin{pmatrix} 1 & 2 \\ a & a \end{pmatrix}, F_2 = \begin{pmatrix} 1 & 2 \\ a & b \end{pmatrix}, F_3 = \begin{pmatrix} 1 & 2 \\ a & c \end{pmatrix} F_4 = \begin{pmatrix} 1 & 2 \\ b & a \end{pmatrix}, F_5 = \begin{pmatrix} 1 & 2 \\ b & b \end{pmatrix},$$

$$F_6 = \begin{pmatrix} 1 & 2 \\ b & c \end{pmatrix}, F_7 = \begin{pmatrix} 1 & 2 \\ c & a \end{pmatrix}, F_8 = \begin{pmatrix} 1 & 2 \\ c & b \end{pmatrix}, F_9 = \begin{pmatrix} 1 & 2 \\ c & c \end{pmatrix} \}$$

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 2.9. *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 2.3. *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. □

Exemple 2.10. Soient E et F deux ensembles non-vides avec produit cartésien $E \times F$. Il y a deux *projections*, souvent utilisées : $\pi_E : E \times F \to E$ et $\pi_F : E \times F \to F$ définies par

$$\pi_E((e, f)) := e \quad \text{et} \quad \pi_F((e, f)) := f,$$

où $(e, f) \in E \times F$. Ce sont deux fonctions surjectives.

2.10. **Taille et bijectivité.**

Exemple 2.11. 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 2.4. *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 serait 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

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

a $n = |A|$ éléments différents. Et le fait que $\mathrm{Im}(F) \subset B$ 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 $F : A \to B$.

Nous allons construire une telle fonction F, à l'aide de nos deux suites ordonnées choisies. Posons :

$$F(a_i) := b_i$$

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

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

Ça fait du sens, car $n \leq m = |B|$. C'est une fonction injective, car sur la deuxième ligne il n'y a pas de répétitions, prop. 2.3(ii). Donc en effet si $|A| \leq |B|$, alors il existe au moins 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. **Sur l'existence d'une fonction inverse.**

Théorème 2.2. *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 si F est bijective, pour chaque $b \in B$ il existe un *unique* $a \in A$ tel que $F(a) = b$. Alors $F^{-1}(b) = a$.

Mais si F n'est pas bijective, une fonction inverse n'existe pas et $F^{-1} : B \to A$ n'est pas définie.

Démonstration. (i) 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 $F \circ G = 1_B$.

(ii) 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 2.12. 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 2.13. Nous donnons un exemple d'une fonction bijective un peu plus compliqué à comprendre, mais la preuve n'est pas difficile.

Théorème 2.3. *Soient A et B deux ensembles non-vides. Supposons $n = |A|$ est fini. Il existe une fonction bijective $\phi : \mathit{Fonctions}(A, B) \to B^n$.*

Ce théorème explique :

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

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

Le corollaire est une conséquence directe du théorème et prop.2.4(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