Introduction générale aux mathématiques: théorie des ensembles, logique booléenne, structures algébriques, et théorie des catégories

Tristan Duquesne

February 1, 2021

Prérequis: Aucun; mais vous pouvez (ou devriez) vous servir des fiches fournies sur différents espaces mathématiques importants pour travailler des cas concrets pour les concepts abstraits présentés ici. Certaines choses vous aurez déjà vues, et seront mieux recontextualisées ici.

Objectif: Le but de ce document est de présenter une vision assez générale des constructions fondamentales des mathématiques; sans aller trop loin dans l'érudition et la démonstration. Voyez-le comme une première étape pour se figurer du vocabulaire mathématique riche et inter-relié, ainsi que la place et l'utilité des mathématiques que ce langage décrit. Le but n'est pas de tout comprendre ce qui est présenté ici du premier coup (bravo si vous y arrivez), mais il vaut mieux avoir lu toute cette section afin de mieux préparer comment structurer, travailler et intégrer tout le reste des mathématiques selon un cadre commun unifié. Vous êtes encouragés à souvent revenir à ce document par la suite: cela vous sera très utile pour faire les liens nécessaires entre les concepts.

Méthode: Ce texte ignore beaucoup des conventions d'une introduction aux mathématiques "classique", *first-and-foremost* à peu près toutes les démonstrations qui passent à la trappe. Notez qu'un mathématicien instruit reconnaîtra sûrement certaines démonstrations classiques dans la façon d'aborder un problème, même quand il s'agit juste de le décrire, lui et les éléments qui le composent.

Cependant, l'objectif principal de ce texte est l'appréhension du vocabulaire des mathématiques modernes de manière écosystémique (inter-reliée et bien fondée), et de le faire vite, pour un public moyennement adepte mais qui doit quand même se confronter aux mathématiques au quotidien. Nous opérons par l'intuition géométrique avant tout, et les liens de cette intuition géométrique avec son expression en langage formel, et en langage vernaculaire (en français ici). Nous avons choisi cette problématique afin que le lecteur puisse s'approprier rapidement beaucoup de réflexes de la pensée d'un mathématicien en pratique (à nager dans les analogies et les définitions) et puisse poursuivre ses recherches de manière autonome.

Pour cela, *il ne faut pas avoir peur de lire avec un papier, de noter chaque nouveau concept, et de relire souvent.*

REVENEZ TOUJOURS A LA DEFINITION: Je ne peux pas assez vous répéter cette idée. Qu'est-ce qu'une définition, en mathématiques ? D'une part, la description abstraite et formelle; d'autre part, des exemples et contre-exemples concrets. C'est ça définir. Si vous ne faites pas ce travail, vous divaguerez dans votre lecture car les mots n'accrocheront pas, à force que le texte devienne plus technique ! Vous voyez quand vous essayez de lire un passage, divaguer, s'en rendre compte, revenir au dernier moment dont on se souvient, relire, redivaguer... et n'aller nulle part ? J'appelle cela "l'illusion de lecture" (au sens d'illusion d'optique). Faites ce travail de revenir à la définition, et vous verrez que cette illusion de lecture ne se produira plus. Mieux, si vous vous rendez compte qu'elle arrive, sachez qu'elle indique que vous avez lu un mot que vous ne comprenez pas ! Ce bug mental peut être dompté pour devenir l'un de vos outils d'apprentissage les plus efficaces.

Ce format court semblait alors plus efficace, sans pour autant sacrifier les vrais clefs de compréhension, qui tiennent plus de brasser large tout en liant constamment l'intuition au formalisme, que l'un ou l'autre seuls, ou les détails techniques du travail de mathématicien: l'art de la démonstration qui s'apprend par le problème et la pratique.

Je prie donc aux mathématiciens professionnels de m'excuser pour mon hérésie bienveillante !

1 Introduction, ou pourquoi on commencerait avec des sujets "abstraits"

Au fondement de tout, il y a l'algèbre. L'algèbre, dans son sens premier (le plus utilisé aujourd'hui du moins), c'est le champ des mathématiques qui s'intéressent à la représentation et à l'étude des espaces mathématiques d'un point de vue de symboles et procédés formels. C'est les mathématiques symbolique, et leurs règles. "Al-jabr", dans son sens originel, c'est la "méthode de réunion/d'équilibre/d'équivalence des quantités", aujourd'hui, c'est plus clairement "ce qu'on a le droit de faire avec des mathématiques sans risquer d'avoir tort". L'algèbre, c'est la branche des mathématiques qui essaye d'établir "quelles sont les propriétés de tel ensemble, et qu'est-ce que cela implique ?" ou plus bêtement "j'ai le droit de faire quoi, avec cet objet/structure mathématique, si je pars de ceci ?".

Par exemple sur "l'espace des entiers avec l'addition, la soustraction et la multiplication" (une de ces "structures mathématiques"), il y a la "division euclidienne", que vous connaissez (vous savez, c'est la "division avec reste"). Mais saviez-vous que sur des polynômes (contenus dans une autre structure avec ses propres règles, très similaires), on peut aussi construire une forme de division euclidienne ? Par exemple, $4x^4 + 7x^3 - 4x^2 + 3x + 12$ divisé par le polynôme $x + 2$ ça donne :

```
  4x^4 + 7x^3 - 4x^2 + 3x + 12 = A(x) | x + 2 = B(x)
- 4x^4 - 8x^3                         +-------
-------------                         | 4x^3 - x^2 - 2x + 7 = Q(x)
    0  -  x^3 - 4x^2 + 3x + 12        |
       +  x^3 + 2x^2                  |
         -----------                  |
            0 - 2x^2 + 3x + 12        |
              + 2x^2 + 4x             |
               ----------             |
                   0 + 7x + 12        |
                     - 7x - 14        |
                      --------        |
                         0 - 2        |
```

Il n'y a pas de moyen de faire tenir $x + 2$ dans -2: cela veut dire que $R(x) = -2$

Ici, le reste de la division euclidienne est $R(x) = -2$ (une constante considérée comme un "polynôme constant"), et le quotient est $Q(x) = 4x^3 - x^2 - 2x + 7$, et on retrouve bien $A(x) = B(x) \times Q(x) + R(x)$ comme la division euclidienne normale (ex: 51 divisé par 10 est égal 5 et il reste 1 correspond à $a = b \times q + r \Rightarrow 51 = 10 \times 5 + 1$).

Remarquez notamment que chaque nouveau monôme rajouté à $Q(x)$ à chaque étape est multiplié à $B(x)$ puis soustrait à $A(x)$, comme dans la méthode que vous connaissez, sauf que les monômes ici présents sont d'habitude des chiffres rajoutés à un seul nombre q que l'on construit progressivement. Notez aussi que si $R(x) = 0$, le polynôme nul, alors on dit que le polynôme $A(x)$ est divisible par le polynôme $B(x)$, comme on ferait pour les entiers.

Voici un petit tableau récapitulatif :

$A(x)$	$4x^4 + 7x^3 - 4x^2 + 3x + 12$	a	51
$B(x)$	$x + 2$	b	10
$Q(x)$	$4x^3 - x^2 - 2x + 7$	q	5
$R(x)$	-2	r	1
$A(x) = B(x) \times Q(x) + R(x)$	Verify by yourself.	$a = b \times q + r$	$51 = 10 \times 5 + 1$

Pas besoin de maîtriser cet exemple parfaitement pour l'instant, la suite du texte vous permettra de relier tout ceci avec ce que vous comprenez déjà : comprenez juste que des structures mathématiques complexes, souvent, vont se "comporter" comme des structures plus simples. Cette idée fondamentale est le sujet de la première partie de ce texte. Nous nous en servirons pour explorer les polynômes de manière assez approfondie (pour une introduction brève en seulementquelques pages).

Ajoutez à cela le fait que **pour tout espace algébrique, on peut construire une géométrie sous-jacente qui fonctionne comme les calculs (manipulations algébriques de symboles) dans cet espace**, et vous avez le fer de lance de la recherche mathématique moderne: **mieux comprendre des listes de symboles compliquées qui révèle l'univers pour nous (mais que nos cerveaux ont du mal à gérer sans les bons réflexes), en revenant à des concepts géométriques simples**.

Des points communs aussi fondamentaux entre des structures qui paraissent pourtant si différentes ont mis les mathématiciens du XIXe et du XXe siècle sur la piste de quelque chose de très profond, sur une manière plus ab-

straite de comprendre les mathématiques, en analysant les structures ("`structures algébriques`") et leurs propriétés, leur fonctionnement, plutôt que s'attarder sur les éléments. Avec un tel outil, mieux comprendre les entiers naturels ou relatifs permet de mieux comprendre les polynômes, en partant de quelque chose de plus simple, mais similaire. Cela permet de traduire les outils entre différentes branches des mathématiques. C'est très utile comme réflexion, pour toute la science et notamment en informatique : ça nous permet de trouver la branche des mathématiques la plus intéressante pour régler efficacement un problème de calcul/code/modélisation donné, tout en offrant la possibilité de simplifier cette branche par une autre, équivalente, sans perte de généralité.

2 Quelques idées-clefs sur les ensembles et le langage formel pour les débutants

2.1 Un petit mot pour se figurer les "ensembles" mathématiques

Désolé de vous faire faux-bond dès le départ, mais malheureusement, un "ensemble", c'est un peu indéfinissable de manière formelle comme concept (du moins sans se référer au concept d'ensemble lui-même, ou à quelque chose analogue lui-même mal défini). Ce qui pose quelques problème niveau fondements. On dit par exemple dans les manuels "les objets fondamentaux sont les ensembles" mais ça n'explique rien. Depuis que la question se pose, beaucoup de progrès ont lieu - mais c'est un autre sujet, dont on parlera rapidement dans ce cours.

Du coup, comme un "ensemble" c'est un concept un peu ambigu pour certains cas litigieux, on va parler de quelques trucs basiques à garder en tête quand on se figure les ensembles, afin de pouvoir mieux les manipuler :

– un ensemble est en gros **une *collection d'éléments* tous différents**, qu'on exprime comme une "idée entre accolades" ou alors comme une "le dessin d'une patate avec des trucs dedans", un "sac" abstrait avec un nom. Ces éléments peuvent être des nombres entiers, des vecteurs, des giraffes, peu importe.

– une sous-collection d'éléments d'un ensemble est appelé un sous-ensemble, et est un ensemble à part entière.

– cette collection d'éléments **peut être vide, finie ou infinie**, et il existe différents types et **différentes tailles d'infinis** (*infini discret vs. infini continu* pour la distinction la plus importante en pratique). L'ensemble vide est noté $\emptyset$.

– **il existe des ensembles qui peuvent contenir d'autres ensembles** (ensemble des parties (des sous-ensembles) d'un ensemble (*powerset* en anglais), tribu (aussi appelée sigma-algèbre), topologie (aussi appelé "ensemble des ouverts")) ; **mais on n'a pas le droit de faire un ensemble qui se contient lui-même** (ou alors vous jouez vraiment avec le feu), ni un "ensemble de tous les ensembles", souvent, même pas "un ensemble de tous les ensembles d'un certain type". [Gérer ce problème-là au niveau des fondements est une des multiples raisons de l'intérêt porté à la théorie des catégories, la vision moderne la plus populaire d'un framework abstrait pour la totalité des maths, comme l'était la théorie des ensembles pour le XXe

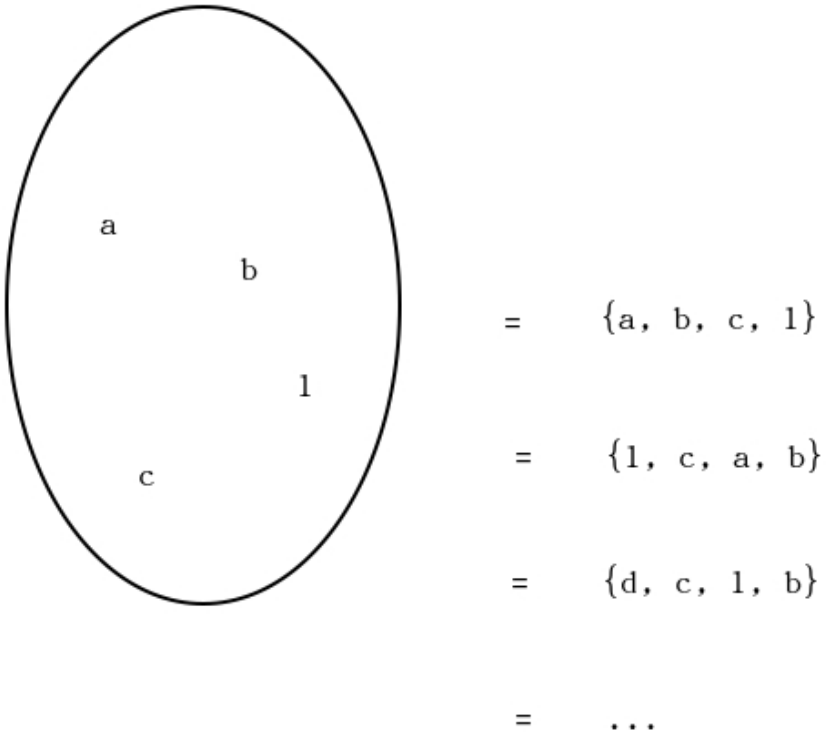


Figure 1: Un ensemble sous-forme de patate/sac, et sous-forme d'objets entre accolades. NB: l'ordre des éléments n'importe pas.

siècle.]

— on se place en général dans le contexte d'un ensemble englobant, au sein duquel des opérations ont lieu. Notez que même si deux ensembles ont des opérations similaires, voire "identique", on ne mélange pas les éléments de deux ensembles différents au niveau des opérations internes à l'ensemble. Si l'on veut faire "communiquer" des ensembles entre eux, il existe une multitude de constructions différentes "entre deux ensembles" pour parvenir au résultat souhaité. Vu que "savoir où se trouve quoi" est un sujet *fondamental* et un peu souvent ignoré dans les intrdouctions, nous mettons l'accent dessus à travers tout ce texte.

NB: Sauf pour quelques mathématiciens qui s'intéressent vraiment au sujet, l'absence d'une définition absolument rigoureuse pour les ensembles ne pose pas vraiment problème en pratique, vu qu'on manipule en général des ensembles finis ou des ensembles d'un type d'infini qu'on maîtrise bien (discret et continu). [Vous entendrez sûrement parler de "l'axiome du choix" (ou une de ses version équivalentes comme le "lemme de Zorn") à travers votre pratique des mathématiques, mais c'est sûrement le seul des problèmes des fondements à lequel vous risquez un jour d'être confronté.] On pourra donc simplifier l'apprentissage et conserver notre définition d'un ensemble comme une "patate d'éléments", ou "liste d'éléments", ou un "sac d'éléments" différents ! Ça convient très bien comme image pour réfléchir.

Notez seulement que c'est aussi une pratique habituelle de décrire les ensembles "conceptuellement", une idée entre accolades, du style "les objets de telle forme — qui vérifie telle contrainte". Par exemple :

$$B = \{2^i \mid i \in [[0, 10]]\}$$

veut dire "B est l'ensemble des nombres de la forme "2 puissance i" tel que i est un nombre compris entre 0 et 10, inclus", ou en clair :

$$B = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024\}$$

La partie à gauche de la barre "$\mid$" décrit la forme des éléments de l'ensemble ("forme", comme "formule" ou "formellement", càd la "façon d'écrire proprement et rigoureusement avec des symboles"). La partie de droite exprime les conditions que ces éléments doivent respecter. Et la barre verticale (parfois c'est une virgule) entre les deux parties se lit "tel que". Les avantages de "l'idée entre accolades" sont multiples: elle peut représenter une infinité d'éléments respectant un certain motif, elle peut expliciter le motif partagé

de divers éléments, elle est souvent plus courte à noter, et souvent, c'est la seule manière d'exprimer les choses à la fois clairement et rigoureusement.

2.2 Quelques ensembles importants

Comme exemples ensembles classiques et/ou auxquels vous aurez droit dans ces textes, vous avez:

- $\mathbb{N}$, ensemble des entiers naturels, $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$
- $\mathbb{Z}$, ensemble des entiers relatifs, $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$
- $\mathbb{Q}$, ensemble des fractions, des nombres rationnels (comme un "ratio"), $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z} \text{ et } b \in \mathbb{N}^*\}$
- $\mathbb{R}$, ensemble des nombres réels, défini comme l'ensemble des limites de suites de rationnels; souvent représenté comme la "droite réelle". Dit grossièrement, $\mathbb{R}$ "bouche les trous" laissés par les nombres qui ne peuvent pas être adéquatement représentés comme des fractions (comme $\sqrt{2} = 1.4142\dots$ ou $\pi = 3.1415\dots$)
- $\mathbb{C}$, ensemble des nombres complexes, une version bidimensionnelle de $\mathbb{R}$, muni d'une multiplication particulière qui généralise celle de $\mathbb{R}$ à un plan en 2 dimensions.
- $\mathbb{R}^n$, espace vectoriel de dimension n sur $\mathbb{R}$
- $\mathbb{C}^n$, espace vectoriel de dimension n sur $\mathbb{C}$
- $\mathbb{R}[X]$, espace des polynômes à une indéterminée sur $\mathbb{R}$
- $\mathbb{C}[X]$, espace des polynômes à une indéterminée sur $\mathbb{C}$
- $\mathbb{R}(X)$, espace des fonctions rationnelles (polynômiales; parfois appelées "fractions rationnelles") à une indéterminée sur $\mathbb{R}$
- $\mathbb{C}(X)$, espace des fonctions rationnelles (polynômiales; parfois appelées "fractions rationnelles") à une indéterminée sur $\mathbb{C}$
- $\mathbb{R}^{\mathbb{N}}$, espace des suites numériques à valeurs réelles, c'est-à-dire l'espace des fonctions de $\mathbb{N}$ dans $\mathbb{R}$
- $\mathbb{R}^{\infty}$, espace des suites numériques à valeurs réelles, nulle à partir d'un certain rang, sous-ensemble du précédent.
- $\mathbb{C}^{\mathbb{N}}$, espace des suites numériques à valeurs complexes, c'est-à-dire l'espace des fonctions de $\mathbb{N}$ dans $\mathbb{C}$
- $\mathbb{C}^{\infty}$, espace des suites numériques à valeurs complexes, nulle à partir d'un certain rang, sous-ensemble du précédent.
- $\mathbb{R}^{\mathbb{R}}$, espace des fonctions de $\mathbb{R}$ dans $\mathbb{R}$

- $\mathcal{L}(\mathbb{R}, \mathbb{R})$, espace des fonctions linéaires de $\mathbb{R}$ dans $\mathbb{R}$, sous-ensemble du précédent

- $\mathbb{C}^{\mathbb{C}}$, espace des fonctions de $\mathbb{C}$ dans $\mathbb{C}$

- $\mathcal{L}(\mathbb{C}, \mathbb{C})$, espace des fonctions linéaires de $\mathbb{C}$ dans $\mathbb{C}$, sous-ensemble du précédent

NB: la raison derrière le terme "d'espace" plutôt "qu'ensemble" au-dessus est liée à celle de "structure algébrique" que nous voyons plus bas. Techniquement, ce n'est qu'une question de point de vue: "l'espace" (ou de même "la structure algébrique") c'est l'ensemble avec en plus un choix des propriétés sur le fonctionnement de cet ensemble. Par abus de langage, les structures plus complexes ont tendances à être qualifiées "d'espace" plus fréquemment, car on les retrouve plus souvent dans des contextes où du langage algébrique avancé est nécessaire (et aussi, la physique et les mathématiques ont évolué symbiotiquement à travers l'histoire humaine).

NB: *Le discret, c'est ce qu'on compte, le continu, c'est ce qu'on mesure.* L'infini discret correspond à un "cardinal" (nombre d'éléments dans un ensemble) noté $\aleph_0$ (aleph zéro). C'est l'ordre de grandeur infini de $\mathbb{N}$, de $\mathbb{Z}$ et de $\mathbb{Q}$. Avec $\aleph_0$, on peut faire une "liste infinie" (l'exemple de l'hôtel de Hilbert, sur lequel je vous conseille de vous renseigner). Cet infini est strictement plus petit que $\aleph_1$, le cardinal de $\mathbb{R}$ et $\mathbb{C}$, l'infini continu. Cet infini continu est trop gros et trop dense pour être mis en liste. Une bonne illustration: il y a plus d'infini dans les nombres entre 0 et 0.001 dans les réels que dans l'entièreté des nombres rationnels de $-\infty$ à $+\infty$. La preuve de cette bizarrerie est appelée "l'argument diagonal de Cantor". Le fait qu'il y ait des infinis de nature et tailles différentes a des ramifications très intéressantes sur beaucoup de distinctions importantes entre le discret et le continu.

2.3 Un petit mot sur la lecture du langage mathématique symbolique

Voici les symboles et concepts fondamentaux du langage de la théorie ensembles (et en réalité, du langage mathématique général):

– une déclaration qui peut être vrai ou fausse, mais pas les deux, s'appelle une **proposition**. Par exemple, "il neige", et "2 est un nombre impair" sont des propositions; mais "pourquoi ai-je faim ?" n'en est pas une. La phrase précédente est aussi une proposition. La plupart des idées en mathématiques (notamment les théorèmes) s'expriment sous forme de propositions.

– "$\in$" se lit "appartient à/appartenant à" et signifie que l'élément représenté par la lettre/valeur à gauche est dans l'ensemble représenté par la lettre à droite (ex : $a \in A$). C'est une relation d'un élément à un ensemble. Cela s'applique aussi à l'appartenance d'un ensemble à son *powerset*. À noter, $a \in A$ est une proposition.

– "$\subset$" se lit "(est) inclus dans" et signifie que tous les éléments de l'ensemble de gauche se trouvent aussi dans l'ensemble de droite (ex. $A \subset B$). C'est une relation entre ensembles. C'est une "relation d'ordre" (ça fonctionne comme $\leq$). De manière équivalente, on dit que A est inclus dans B "si et seulement si (ssi)" $\forall x \in A, x \in B$ (tous les éléments de A sont aussi dans B). Graphiquement, A est une patate qui est englobée par la patate de B. Deux ensembles A et B sont égaux ssi ("A est inclus dans B" ET "B est inclus dans A"). Il est clair géométriquement que si deux patates s'englobent mutuellement, elles sont la même patate. Formellement, on peut noter cela $A = B \Leftrightarrow A \subset B \cap B \subset A$. Ex : $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

– $\forall$ qui se lit "pour tout". Il est appelé quantificateur universel. "$\forall x \in E$" se lit "pour tout x appartenant à E" et signifie "on peut prendre n'importe quel élément x (tous doivent convenir !) de notre ensemble E, et la suite de la formule marchera pour x". Ex : Si $\mathbb{N}$ est l'ensemble des entiers naturels $\{0, 1, 2, 3, \dots\}$ alors $\forall x, y \in \mathbb{N}, x + y = y + x$ est une propriété de $\mathbb{N}$ (cette formule est vraie pour toute paire d'éléments choisis au hasard ou au choix dans $\mathbb{N}$). [Par ailleurs, cette propriété s'appelle "commutativité de l'addition dans $\mathbb{N}$".]

– $\exists$ qui se lit "il existe". Il est appelé quantificateur existentiel. $\exists x \in E$ signifie "on peut trouver au moins un élément x de notre ensemble E qui convienne pour que la suite de la formule marche". Ex : Si n n'est pas premier, alors il existe b, élément de $\mathbb{N}$ différent de 0 et 1, tel que b est un diviseur de n. Cela s'écrirait:

$$n \in \mathbb{N}, n \text{ non-premier } \Rightarrow \exists b \in \mathbb{N}, b \geq 2, b \neq n, b|n$$

– "$\exists!$" se lit "il existe un unique"/"il existe un et un seul". L'unicité est un sujet important en mathématique. $\exists! x \in E$ signifie "on peut trouver exactement un seul élément x de notre ensemble E tel que la suite de la formule marche pour x".

— si une variable est déclarée dans une formule mais n'a ni $\forall$ ni $\exists$ la précédant, il faut comprendre qu'il s'agit d'une constante fixée (qui est en réalité juste un $\forall$ caché, mais qui se comprend plus intuitivement si on le comprend comme un cas fixé; c'est un choix de style).

— "ssi" se lit "si et seulement si" et correspond au symbole $\Leftrightarrow$, c'est-à-dire l'**équivalence** logique. Cela signifie une synonymie au niveau des idées; qu'une idée n'existe pas sans l'autre. L'idée de "carré" est équivalente à l'idée de "figure à quatre sommets au côtés de longueur égale avec au moins un angle droit" ou encore à l'idée de "figure à quatre sommets chacun faisant un angle de 90 degrés, avec au moins deux côtés consécutifs de même longueur". Ceci est à contraster avec l'**implication** $\Rightarrow$, qui transcrit l'idée que "tous les pouces sont des doigts, mais tous les doigts ne sont pas forcément des pouces". En clair, "carré $\Rightarrow$ quadrilatère" $\Leftrightarrow$ "tous les carrés sont des quadrilatères, mais tous les quadrilatères ne sont pas forcément des carrés" $\Leftrightarrow$ "si c'est même pas un quadrilatère, impossible que ce soit un carré".

NB: ne pas confondre ces symboles et notations ! Quand vous travaillerez les ensembles d'ensembles (multiset, hypergraphes, powerset, tribu, topologie) vous risquez de vous tromper sinon. On peut noter soit "$a \in A$", soit (de manière équivalente) "$\{a\} \subset A$", où $\{a\}$ est un ensemble appelé **singleton** contenant un seul élément : a. Mais on ne note pas "$a \subset A$" car c'est changer de niveau de "contenance" de manière inappropriée. C'est un peu comme oublier de déréférencer un pointeur en C dans un appel de fonction. Soit le compilateur grogne, soit ça segfault.

NB: l'ordre des termes est important dans une formule ! Exemple :

$$\forall x \in A, \exists y \in B, y = f(x)$$

$$\exists y \in B, \forall x \in A, y = f(x)$$

Dans le premier cas, on est en train de dire que A est l'ensemble de définition approprié de la fonction f car pour "tout x au départ, on peut trouver une image y à l'arrivée de la fonction" (ie : il n'y aura pas de cas de bug en input de votre fonction). Dans le deuxième cas, on est en train de dire que f est une fonction constante qui à tout x associe la valeur y, car "il existe un y de l'ensemble d'arrivée B tel que tous les x de A donnent ce même y qu'on peut choisir précisément". Comprenez bien cet exemple, c'est un des cas de lecture les plus utiles pour se donner une idée de comment lire le langage mathématique dans le bon ordre.

NB: La règle pour maintenir le sens d'une formule mathématique est que les quantificateurs sont intervertibles avec des quantificateurs du même type uniquement (c'est-à-dire universel avec universel, existentiel avec existentiel, mais jamais d'échange). La justification de ce principe se trouve dans la théorie des catégories, en logique formelle et dans la théorie des types. Donc

il est vrai que $\forall x \forall y \exists z = \forall y \forall x \exists z$, mais par contre $\forall x \forall y \exists z$, $\forall x \exists z \forall y$ et $\exists z \forall x \forall y$ ont tous un sens différent. J'essaierai de rajouter les "tel que" aux bons endroits dans les formules de la suite, mais il faut ABSOLUMENT être capable de faire cette "lecture" des formules mathématiques tout seul, ça demande de s'entraîner, de prendre le temps de déchiffrer au départ ! Mais cela est très important pour pouvoir comprendre de nouvelles idées abstraites rapidement. C'est aussi important que l'intuition géométrique, je pense, ce qui est dire! En effet, si "un bon dessin vaut mille paroles", alors "une formule bien comprise vaut une *infinité* de dessins". Notez quand même qu'il vaut mieux ne pas se priver de la géométrie, au départ, pour comprendre les formules ! Partout, l'intuition et le formalisme se complètent et s'enrichissent mutuellement.

3 Opérations sur les ensembles et logique booléenne

Il existe des opérations que l'on peut effectuer sur des ensembles, qui donnent de nouveaux ensembles ou expriment certaines propriétés de ces ensembles. Par ailleurs, la plupart de ces opérations trouvent une expression équivalente en logique. Voici les plus importantes. (Notez que dans ce qui suit, on se situe dans un ensemble E servant d'univers englobant toutes les possibilités.)

3.1 Liste générale des opérateurs sur les ensembles

— $A \setminus B$, ou $A - B$, appelé **soustraction** de A par B, et lu "A privé de B", est l'ensemble des éléments appartenant à A et pas à B. Formellement, $A \setminus B = \{x \in A \parallel x \notin B\}$. Cet opérateur peut aussi être défini à l'aide des opérateurs ci-dessous comme $A \setminus B = A \cap \overline{B}$.

— $\neg A$, ou $\overline{A}$, appelé la **négation**, ou le **complémentaire**, de A, et lu "non-A" est l'ensemble des éléments de E, l'univers englobant, n'appartenant pas à A. Formellement, $\overline{A} = \{x \in E \parallel x \notin A\} = E \setminus A$.

— $A \cap B$, appelé **intersection** (ou, rarement, "meet") de A et B, et lu "A inter B", ou "A et B", est l'ensemble des éléments communs à A et B (le '&&' en langage de programmation C pour sa version logique).

— $A \cup B$, appelé **union** (ou, rarement, "join") de A et B, et lu "A union B", ou "A ou (inclusif) B" est l'ensemble des éléments soit dans A, soit dans B, soit dans les deux, en ne gardant qu'un seul exemplaire de doublon s'il y en a (le "||" en langage de programmation C, pour sa version logique).

— $A\Delta B$ (ou plus rarement $A \oplus B$ ou $A \otimes B$), appelé la **différence symmétrique** de A et B, et lu "A xor B" ou "A delta B" ou "A ou (exclusif) B", correspond aux éléments qui appartiennent à soit A, soit B, mais pas aux deux. Formellement, $A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A) = (A \cap \overline{B}) \cup (B \cap \overline{A})$.

3.2 Diagrammes de Venn

Tout ceci n'est pas très intuitif à ce stade, sans exemple concrets ni visualisations. C'est pourquoi on va maintenant faire les liens avec la logique avec un outil extrêmement utile pour se figurer les ensembles et leurs opérations. C'est la version "propre" de notre intuition des "ensembles comme patates". Il s'agit d'un des outils les plus bêtes et pourtant les plus prolifiques des mathématiques: les diagrammes de Venn. Vous les rencontrerez sous leur forme simple surtout en théorie des ensembles, en logique, ou en probabilités (théorie de la mesure); mais vous pourriez argumenter que des branches comme la géométrie algébrique c'est juste des diagrammes de Venn complexifiés. En voici un exemple explicatif.

Le principe est simple non ? Chaque patate/cercle est un ensemble, et les différents régions découpées vont nous permettre d'analyser le comportement des opérateurs.

Maintenant, ce qui est intéressant c'est de se poser la question de ce que ces ensembles peuvent représenter, concrètement. Surtout en logique. Alors prenons des exemples concrets.

$$A = \{\text{Ensemble des ordinateurs pouvant lancer Linux}\}$$

$$B = \{\text{Ensemble des ordinateurs pouvant lancer Windows}\}$$

$p = \{$"Il pleut", ensemble des 'univers' ou cette idée est vraie, par exemple$\}$

$$q = \{\text{"Je porte un manteau", idem}\}$$

Vous pouvez penser p comme A et q comme B, ou inversement. Je donne juste des noms différents pour être plus clair, et pour rester dans les conventions d'écriture respectives à chaque domaine (théorie des ensembles *vs* logique booléenne). La plupart des opérations sont commutatives

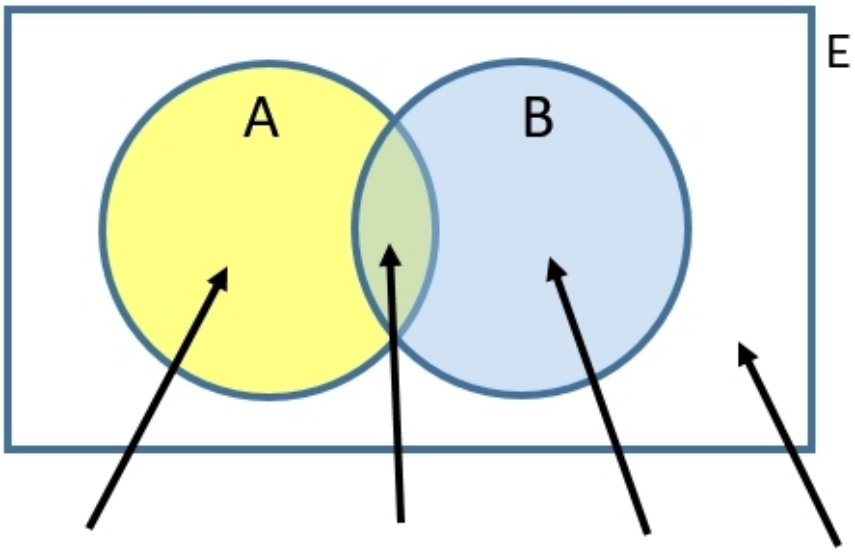


Figure 2: Deux ensembles A et B, dans un ensemble englobant E — sous forme de diagramme de Venn.

(symétriques, comme $5+3$ qui est égal à $3+5$) de toute façon, donc comment vous mettez vos lettres sur le diagramme importe peu tant que vous captez l'intuition géométrique du truc.

Pour approfondir ce qui suit, ces pages Wikipédia sont très bien et les articles détaillés vers lesquels elles renvoient le sont aussi:

https://fr.wikipedia.org/wiki/Table_de_vérité

https://fr.wikipedia.org/wiki/Algèbre_des_parties_d'un_ensemble

Je leur vole leurs diagrammes d'ailleurs.

Dans la suite, A est la patate de gauche, B celle de droite. Le coloriage rouge veut dire "vrai", "T", ou "1", le blanc veut dire "faux", "F" ou "0". Le coloriage rouge veut aussi dire "résultat de l'opération ensembliste que l'on vient d'effectuer".

p	$id(p)$	$\neg p$	$\top$	$\bot$
F	F	T	T	F
T	T	F	T	F

p	q	$p \cap q$	$p \cup q$	$p \Delta q$	$p \cap \neg q$	$p \Rightarrow q$	$p \Leftrightarrow q$
F	F	F	F	F	F	T	T
F	T	F	T	T	F	T	F
T	F	F	T	T	T	F	F
T	T	T	T	F	F	T	T

3.2.1 Ensemble vide ($\emptyset$); constante "FAUX" (F, 0, $\bot$)

L'ensemble vide est l'ensemble ne contenant aucun élément. C'est aussi la représentation d'une proposition p qui est toujours fausse, généralement noté F, ou 0, parfois $\bot$. On appelle une telle proposition une "négalogie" ou "contradiction".

3.2.2 Ensemble total (ici appelé E); constante "VRAI" (V, T, 1, $\top$)

L'ensemble total est l'ensemble contenant tous les éléments (du contexte dans lequel on se place). C'est aussi la représentation d'une proposition p qui est toujours vraie; généralement notée, V, T (pour "true"), 0, et parfois $\top$. On appelle une telle proposition une "tautologie" ou un "théorème (de logique)".

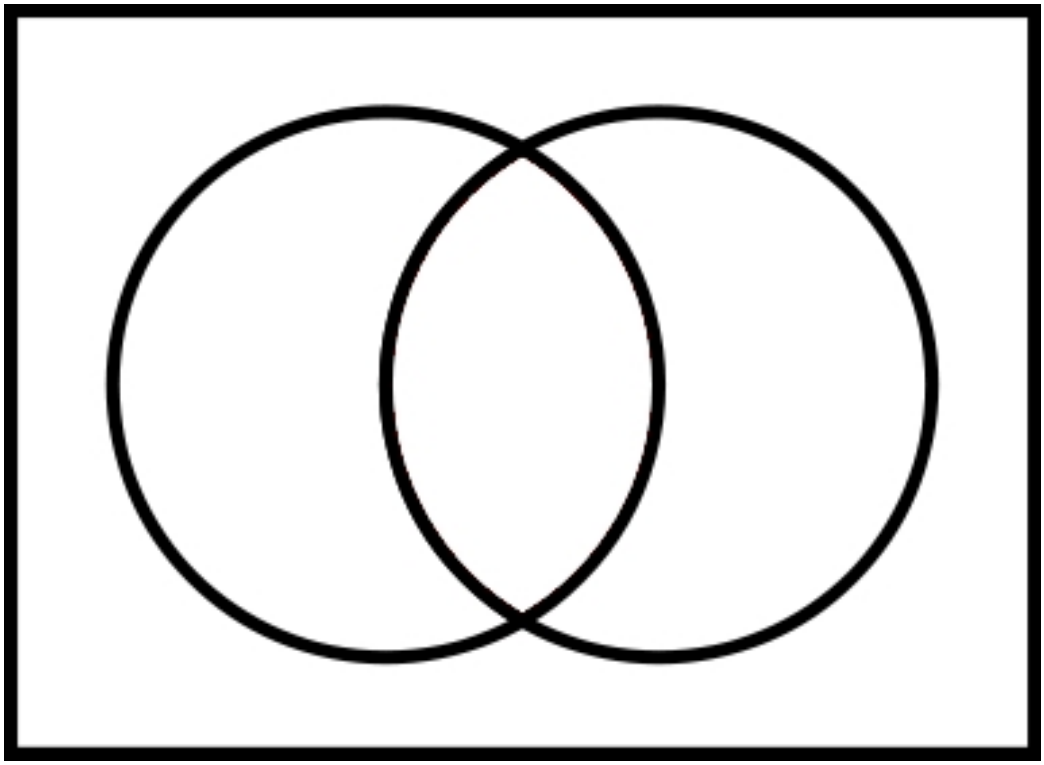


Figure 3: Ensemble vide, ne contenant aucun élément.

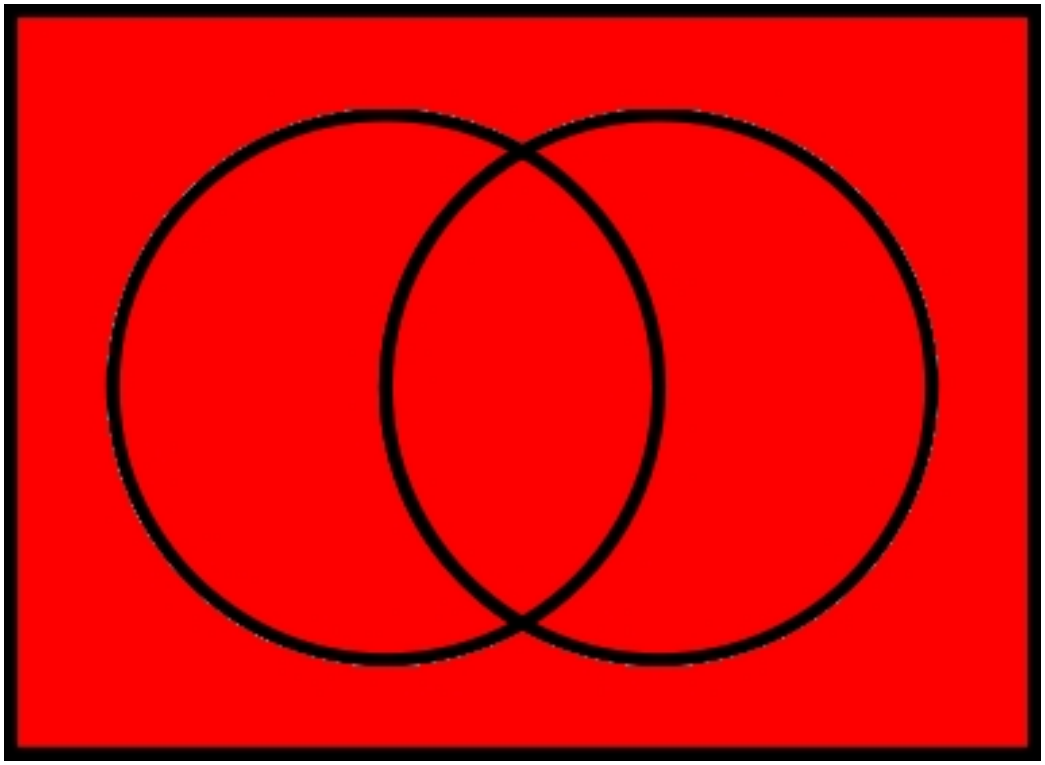


Figure 4: Ensemble total, contenant tous les éléments.

[TODO: add "ID" identity/no change operator on A for the sake of exhaustivity ? Or is it overkill ?]

3.2.3 "NON/NOT/NEG" : la complémentarité, la négation ($\neg$, !)

La négation est un opérateur unaire : elle ne s'applique qu'à un ensemble à la fois, ici, A. La zone en rouge est $\overline{A}$ (pour la notation ensembliste) ou $\neg p$ (pour sa notation en logique). En informatique, on verra généralement le symbole "!".

Si A est l'ensemble des ordinateurs Linux, alors $\overline{A}$ est l'ensemble des ordinateurs qui ne sont aucunement Linux. Cela veut dire un ordi soit Windows (la patate B), soit Mac (un troisième cercle qu'on pourrait imaginer), mais sans "dual-boot avec Linux" (c'est-à-dire qu'un ordi contenant à la fois une installation de Linux et d'un autre système d'exploitation). Un dual-boot Windows-Linux serait un ordi qui appartient la zone centrale commune à A et B. Du coup, il n'appartiendrait pas à $\overline{A}$. Si p est la proposition "il pleut", alors $\neg p$ est la proposition "il ne pleut pas".

3.2.4 "ET/AND" : l'intersection, la conjonction ($\cap$, $\wedge$, &&)

L'intersection est un opérateur binaire : elle s'applique à deux ensembles, ici, A et B.

Si A représente les Linux, et B les Windows, alors la zone rouge $A \cap B$ correspond aux ordis à la fois Linux et Windows, c'est-à-dire les dual-boots Linux+Windows.

En logique, $p \cap q$ signifie que "p ET q"" est vrai uniquement quand "p est vrai" ET "q est vrai". Par exemple, si on reprend p = "Il pleut" et q = "J'ai un manteau sur mon dos", alors $p \cap q$ correspond à la situation où "il pleut et j'ai un manteau sur mon dos", vraie uniquement si p est vrai et q est vrai.

Un exemple typique en info : on veut s'assurer qu'un nombre n soit compris entre 0 et 10 avant de continuer dans notre code. Alors on écrit la condition "$0 \leq n \cap n \leq 10$" – une autre façon d'exprimer "$0 \leq n \leq 10$" mais avec des opérateurs binaires qui servent de blocs de base ($\leq$ et $\cap$). Généralement, en programmation, "$\cap$" est écrit "&&", et a une version bitwise "&".

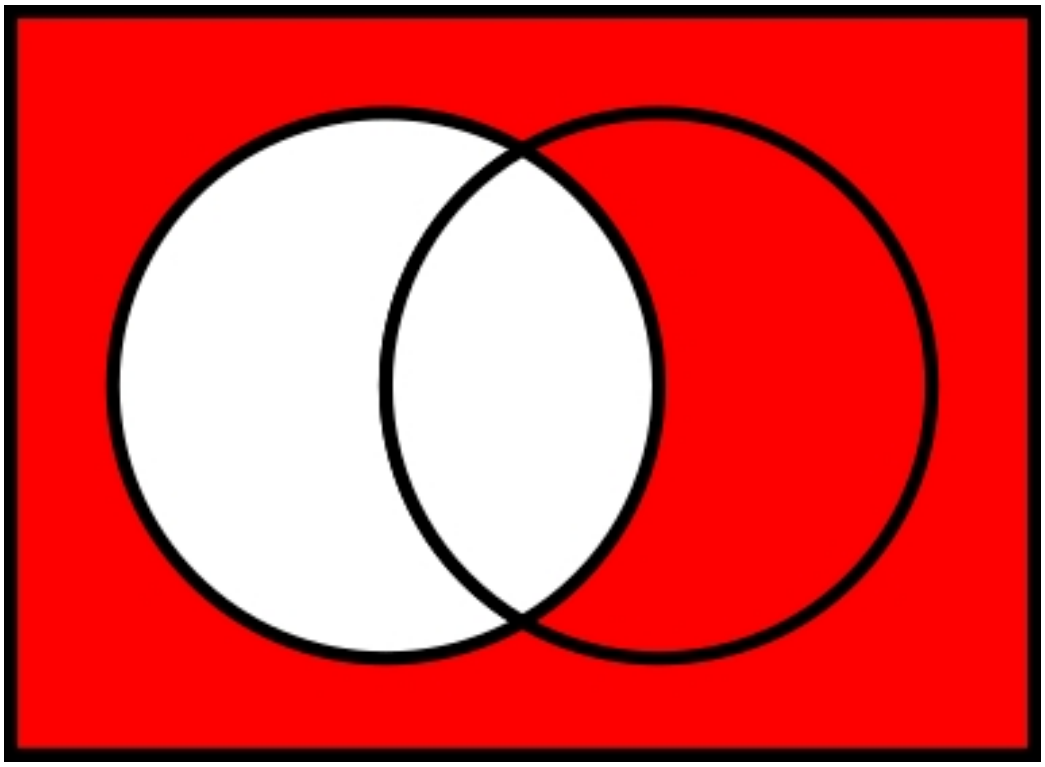


Figure 5: Ensemble $\overline{A}$: ensembles de tous les éléments qui ne sont pas dans A

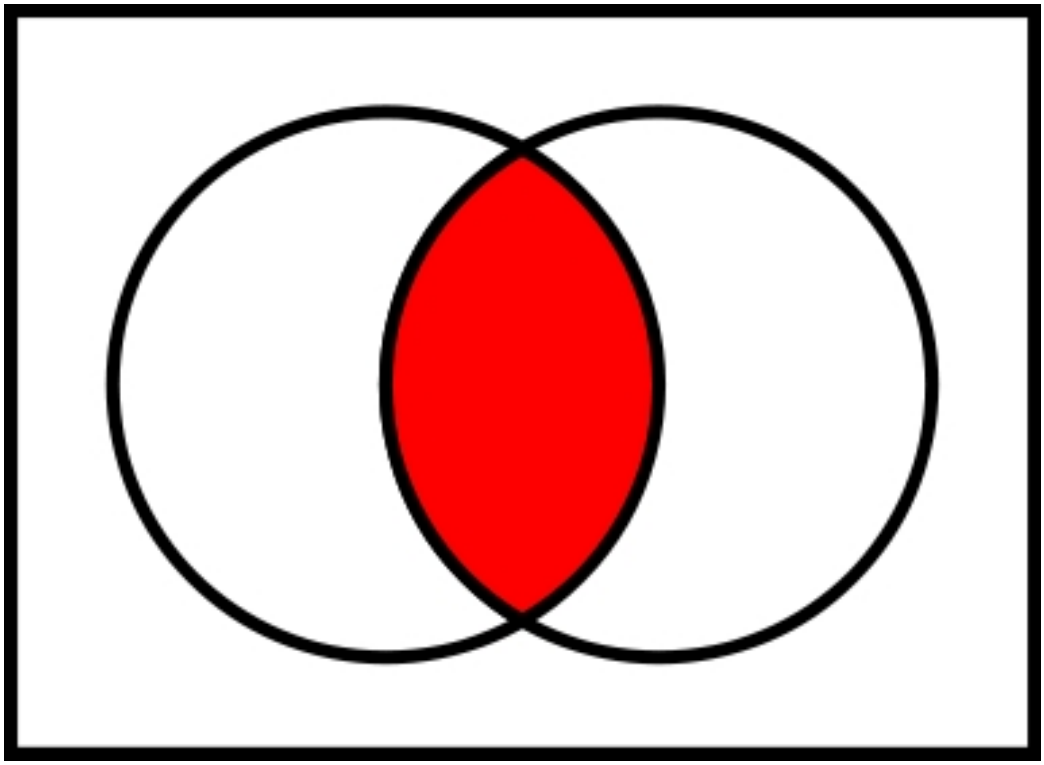


Figure 6: Set $A \cap B$: set of all elements both in A and B

3.2.5 "OU/OR": l'union, la disjonction (inclusive) ($\cup$, $\vee$, $||$)

L'union est un opérateur binaire, il prend en input deux ensemble A et B et renvoie un ensemble $A \cup B$.

Le OU logique n'est pas le "ou" usuel du français qui est en général le XOR (juste après). Le OU logique est dit "OU inclusif". Si A et B représentent les ordis Linux et Windows respectivement, alors $A \cup B$ représente l'ensemble des ordis soit Linux, soit Windows, soit les deux (dual-boots). On utilise souvent "et/ou" dans le langage commun pour signifier la disjonction.

Pour faire la distinction: - ou inclusif: "on peut devenir millionaire en gagnant au loto ou en montant son entreprise"; rien n'empêche les deux de fonctionner en même temps - ou exclusif: "tu as le choix: prends un bonbon ou un caramel"; c'est l'un ou l'autre, mais pas les deux.

La justification de l'importance du OU inclusif se voit surtout en logique. $A \cup B$ est vrai si A est vrai ou si B est vrai. L'un seul des deux peut convenir. Si on dit "il pleut ou j'ai un manteau sur mon dos", soit il pleut, soit j'ai un manteau sur mon dos, soit les deux. Dès que l'un des deux est vrai, ça marche. C'est fondamental en informatique. Par exemple, si l'on veut que le code se termine, mais qu'il y a plusieurs conditions de fin possible (par exemple échec et mat, ou pat, ou abandon d'un joueur aux échecs), l'une OU l'autre de ces conditions convient pour faire que le jeu s'arrête (lancer le protocole "fin de partie") à la fin d'un tour.

3.2.6 "XOR" : la différence symétrique, l'union disjonctive, la disjonction (exclusive) (Δ, $\veebar$, $\oplus$, $\otimes$)

Le XOR, notre "OU eXclusif" habituel du français ("je peux te donner un chocolat XOR un bonbon, au choix"), est un opérateur binaire. Il est surtout utile en électronique, un peu en cryptographie, pas si fréquent en logique. On aurait plus tendance à faire $((A \cup B) \setminus (A \cap B))$, où l'opérateur "$\setminus$" est l'opérateur de soustraction ensembliste, juste en dessous. La notation de l'opérateur XOR varie beaucoup parce qu'il est peu utilisé. On conseille la notation Δ (ensembliste) ou $\veebar$ (logique), car $\oplus$ est souvent réservé à la somme directe d'espaces vectoriels, et $\otimes$ au produit tensoriel; même si la probabilité de tomber sur un exemple où vous devez gérer une différence symétrique et une somme directe/produit tensoriel d'espaces vectoriels est faible, mieux vaut éviter.

Si A est l'ensemble des Linux, et B est l'ensemble des Windows, alors

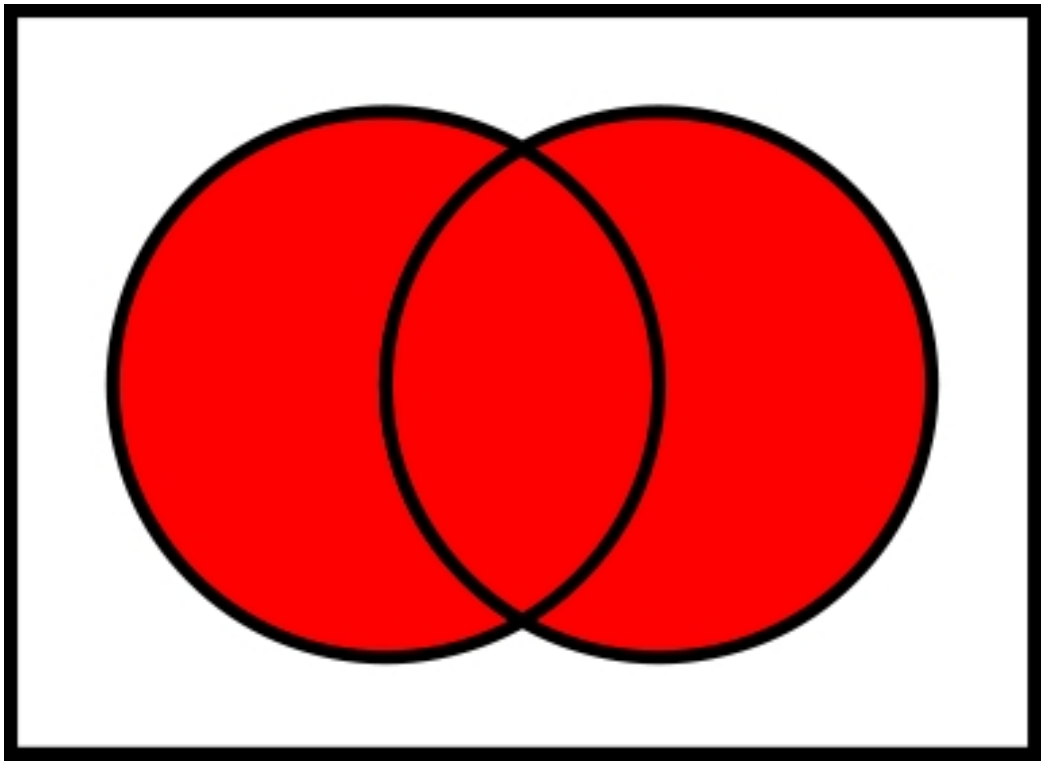


Figure 7: $A \cup B$: ensemble de tous les éléments de A, de B, ou des deux

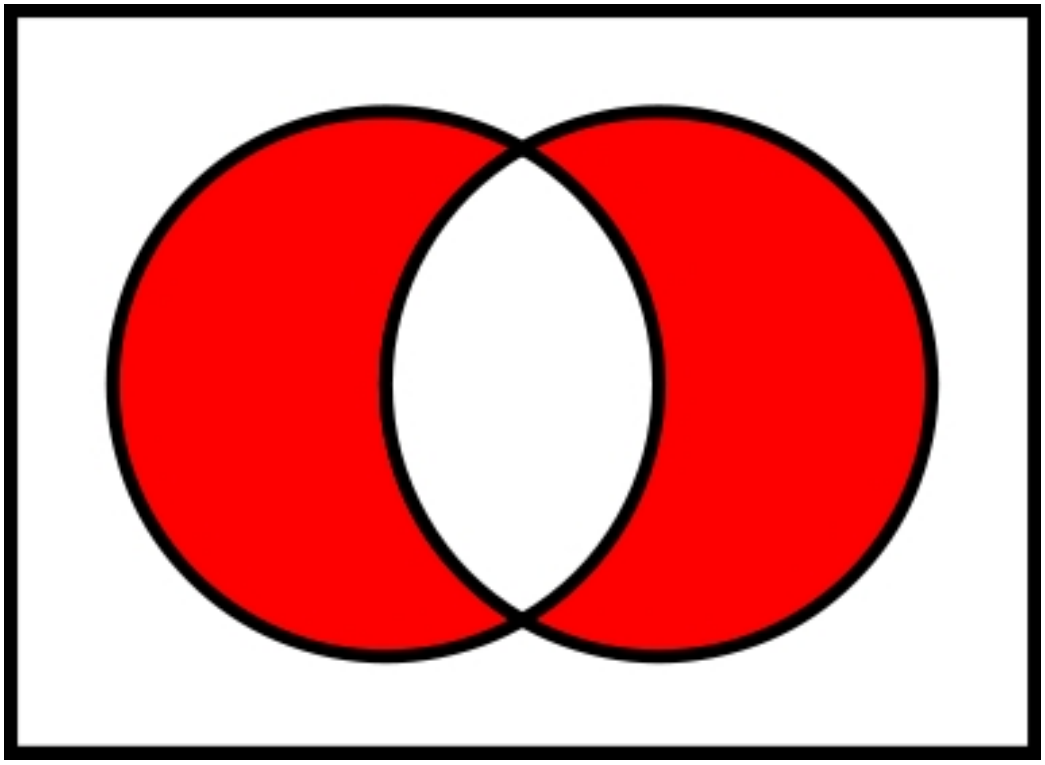


Figure 8: $A\Delta B$: ensemble de tous les éléments de soit A, soit B, mais n'appartenant pas aux deux

$A\Delta B$ est l'ensemble des ordinateurs qui sont soit Linux-pur, soit Windows-pur : c'est-à-dire pas de dual-boot.

En logique, il est assez rare que quelque chose qui marche quand A est vrai et quand B est vrai ne marche plus quand les deux sont vrais, donc XOR est assez utilisé, mais ça arrive. J'en donne un exemple très important plus bas, car il est une des premières étapes de l'informatique, en faisant la traduction d'un monde mathématique/logique à un monde physique avec des courants électriques. Il existe d'ailleurs une version bitwise du XOR, en général notée avec l'opérateur circonflexe ˆ.

3.2.7 "A (AND) NOT B", soustraction ensembliste, $A \setminus B$

Voici la représentation de l'opérateur binaire (entre 2 ensembles) de soustraction d'ensembles, $\setminus$. A est le disque de gauche, B le disque de droite, $A \setminus B$

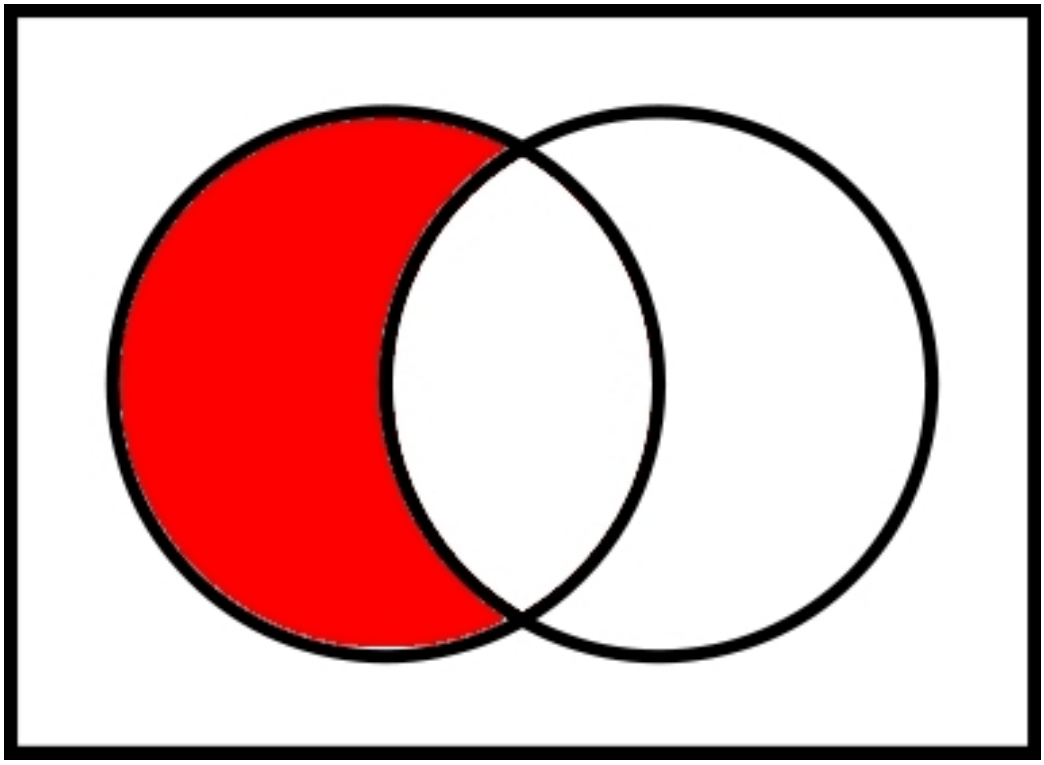


Figure 9: Ensemble $A \setminus B$, résultat du fait de prendre un ensemble A et d'en retirer les éléments de B.

la zone rouge. On lit "A privé de B".

Si p est la proposition "il pleut", et q est la proposition "je porte un manteau", alors $p \setminus q$ signifie "il pleut et je ne porte pas un manteau". Il s'écrirait en logique $p \cap \neg q$, en général.

3.2.8 "Si ..., alors ..." : l'implication ($\Rightarrow$)

Nous en venons à l'opération qui est peut-être la plus compliquée de toutes en logique, mais celle que l'on utilise le plus souvent intuitivement sans comprendre son formalisme. On n'a pas vraiment de symbole ensembliste pour la représenter, mais ce n'est pas grave car on peut construire la même idée avec d'autres symboles ensemblistes de base (cf. l'exercice en bas de cette section). On la trouve assez peu en informatique (à part si vous faites de la logique pure pour des logiciels de démonstration ou des systèmes critiques,

genre logiciel pour centrale nucléaire, par exemple). Par contre, c'est peut-être la plus importante dans le langage de tous les jours et en mathématiques. Il s'agit de l'implication, $p \Rightarrow q$, lue "p implique q", ou "si p, alors q", ou encore "pour que p, il faut que q".

En particulier, pour comprendre la bizarrerie, regardez le résultat quand p est faux et q est vrai dans la table de vérité ci-dessus, $p \Rightarrow q$ reste vrai. Mais quand p est vrai et q est faux, là $p \Rightarrow q$ est faux. Ca paraît étrange non ? Le problème avec l'implication, c'est qu'on la symbolise avec une flèche, comme si elle n'allait que dans un sens, mais ce serait mal la comprendre. Le lien logique qu'exprime l'implication est vraiment "entre p et q", et pas uniquement "de p à q".

Aussi, il faut noter que cette idée "$p \Rightarrow q$" est une proposition indépendante, à part entière, avec ses propre valeurs de vérités etc. On pourrait l'appeler r et la définir comme $r := (p \Rightarrow q)$ pour montrer qu'il s'agit de sa propre proposition ("assertion logique"). C'est aussi le cas pour $\neg p$ qui est sa propre proposition, pour $p \cap q$ qui est sa propre proposition, etc. C'est important car parfois, vous connaitrez (les valeurs de vérité) de p et q, mais pas (celle de) $p \Rightarrow q$. Parfois q et $p \Rightarrow q$, mais pas p, etc.

Si $p \Rightarrow q$ est vrai, on dit que : – p est une **condition suffisante** pour q – q est une **condition nécessaire** pour p

Disons que si $p :=$ cet objet est un pouce et $q :=$ cet objet est un doigt (et donc que $p \Rightarrow q$ est l'idée que "si un objet est un pouce, alors cet objet est un doigt"), alors, de la manière la plus basique que je puisse expliquer les bizarreries techniques de l'implication est cette idée que "tous les pouces sont des doigts, mais que tous les doigts ne sont pas forcément des pouces". Si c'est un pouce, alors c'est un doigt. Remplacez "pouce" par "carré" et "doigt" par "quadrilatère" ; ou "pouce" par "situation où il pleut" et "doigt" par "situation où j'ai un manteau sur mon dos", etc : vous aurez les exemples équivalents pour d'autres propositions p et q.

Il est "suffisant" d'être un pouce pour être sûr qu'on est un doigt ; il est "nécessaire" d'être déjà un doigt pour même pouvoir envisager être un pouce. Dire que quelque chose est un pouce mais n'est pas un doigt n'a pas de sens, vu comment on définit "pouce" et "doigt" ici. Avec "pouce $= p = A =$ vrai" et "doigt $= q = B =$ faux" (on est dans A, mais pas dans B : croissant de gauche), ce cas qui n'a pas de sens est la zone blanche dans notre diagramme. Mais par contre, le fait que certains doigts ne sont pas des pouces (la partie $B \setminus A$, croissant de droite) n'empêche aucunement le fait que "tous les pouces sont des doigts", donc devient zone

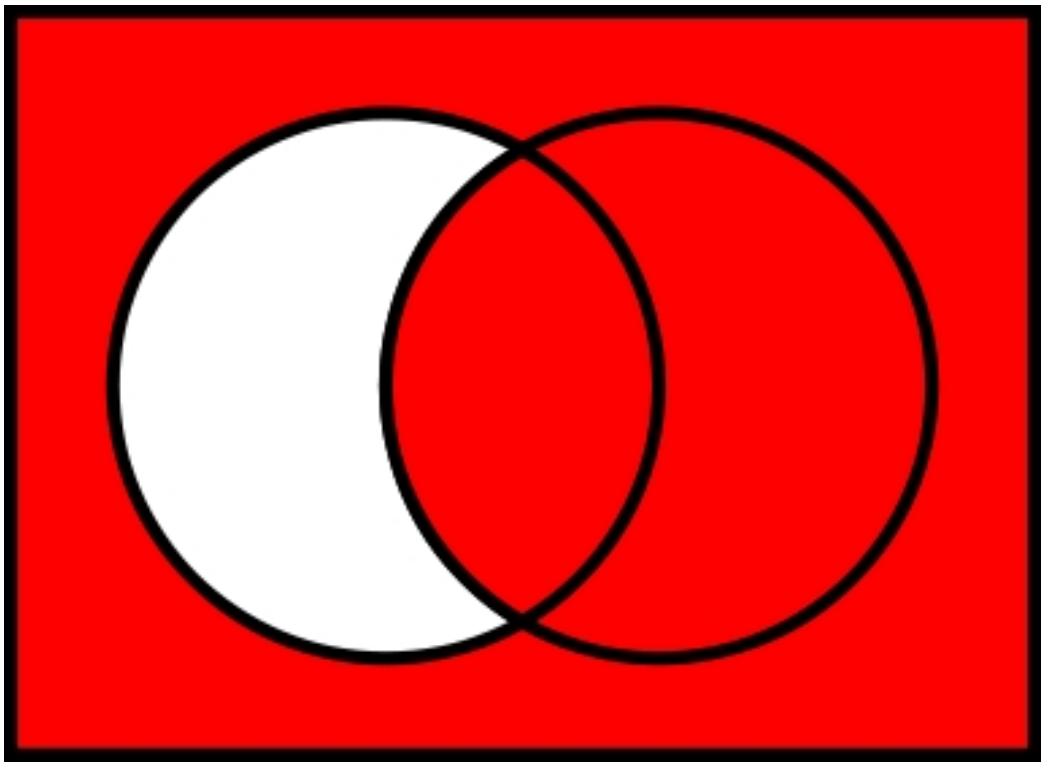


Figure 10: $A \Rightarrow B$: ensemble de tous les éléments répresentant "si A alors B" comme étant vrai

rouge (vraie) dans le diagramme. Donc quand A (ou p) est faux, mais B (ou q) est vrai, $p \Rightarrow q$ reste vrai.

L'exemple du manteau sur le dos peut paraître bizarre, mais le monde mathématique est beaucoup plus pur et rigide dans sa structure que ne l'est la réalité et le langage humain qui la décrit. C'est pourquoi on va l'utiliser comme exemple pour construire une traduction entre la pureté mathématique et le langage humain afin de mieux comprendre tout ça.

Disons qu'on est sûr du fait que $r := p \Rightarrow q$ soit vrai, on est sûr que "p implique q" est vrai. Mais on ne connait la valeur de vérité ni de p ni de q. p est une condition suffisante de q. Dès qu'on a p vrai, on sait (on peut déduire) que q est vrai. Si p est faux, on ne peut rien dire sur q. Peut-être qu'il est vrai, peut-être qu'il est faux. Imaginez que j'ai un super pouvoir: dès qu'il pleut, même si je ne le veux pas, j'ai un manteau qui apparaît sur mes épaules. Ce super-pouvoir représente notre $p \Rightarrow q$. p est vrai : il pleut. Pof, j'ai pas le choix, le manteau apparaît, et reste tant qu'il pleut. Par contre, même quand il ne pleut pas (p faux), rien ne m'empêche de quand même porter un manteau. Ou pas. Rien n'empêche l'un ou l'autre scénario. On peut simplement déduire que s'il pleut, alors Tristan aura un manteau sur le dos, mais ça reste limité: il faut p et $p \Rightarrow q$ tous deux vrais pour déduire quelque chose sur q (que q est vrai).

Maintenant (toujours en supposant que $p \Rightarrow q$ est vrai), on dit que q est une condition nécessaire de p. Et c'est là que l'on se rend compte que la relation va dans les deux sens ; non seulement avec p et $p \Rightarrow q$ on peut faire des déductions à propos de q comme on vient de le voir, mais aussi avec q et $p \Rightarrow q$ on peut déduire certaines choses sur p. On sait que j'ai ce pouvoir ($p \Rightarrow q$), mais maintenant on connait q, et on veut savoir si p est vrai ou pas. Si q est faux, tu es SÛR que p est faux (parce que dès que p est vrai, q est vrai). Par contre si q est vrai, tu ne peux rien déduire. p peut être vrai ou être faux, ça n'influence pas la vérité du lien entre p et q, de l'implication.

Pour en revenir à notre scénario: imaginez que quelqu'un vous dise "j'ai vu Tristan en T-shirt hier" (q est faux, je ne porte pas de manteau); vous savez que j'ai mon pouvoir ($p \Rightarrow q$): vous pouvez être sûr qu'il ne pleuvait pas (p est faux), autrement il aurait été impossible (contradictoire!) de me voir sans mon manteau. Par contre, si on vous dit qu'on m'a vu avec un manteau (q est vrai), il pouvait très bien juste faire froid et ne pas pleuvoir (p=?). On peut simplement déduire que si Tristan n'a pas son manteau, alors il ne pleuvait pas, mais ça reste limité: il faut q faux et $p \Rightarrow q$ vrai, pour déduire quelque chose sur p (que p est faux).

Ces pistes pour les démonstrations aident à expliquer la bizarrerie: c'est juste le "fonctionnement" de l'implication; on utilise une flèche pour l'illustrer, mais c'est juste un "lien" logique entre deux idées. Ça nous dit quel rapport existe entre des idées, quels motifs/patterns on peut dessiner entre nos idées, lesquels seront forcément vrais, lesquels seront forcément faux, et ceux dont on ne peut rien savoir. Les F et les T sont organisés tels qu'ils sont dans la table de vérité, même si ça paraît étrange, pour que ton langage logique puisse fonctionner et décrire ce phénomène de lien entre l'idée du carré et du quadrilatère, du pouce et du doigt, qui n'est ni une équivalence ni une indépendance totale.

Aussi, de manière ensembliste, être "sûr que $p \Rightarrow q$" (supposer "$p \Rightarrow q$"), c'est vraiment très simple ! C'est juste avoir $q \subset p$ vrai (l'ensemble des pouces est contenu dans l'ensemble des doigts).

BONUS : On en arrive à une conséquence marrante : une tautologie (théorème de logique; une formule logique qui reste vraie quoique que soient les valeurs des atomes p, q, etc qui la composent) est impliquée par toutes les idées de ta theorie (ta tautologie est forcément vraie, donc il faut l'avoir dans ta théorie pour que ta théorie tienne debout; elle est condition nécessaire de toutes les autres idées!). Une contradiction (ou "négalogie", une idée forcément fausse quelque soit la valeur des atomes qui la composent) au contraire, implique toutes les idées de ta théorie (elle est forcément fausse, donc ne pose aucun problème, n'affecte la valeur de vérité d'aucune implication) ! C'est sur cette idée que repose le principe d'explosion (aussi appelé la loi de non-contradiction), qui est probablement l'une des lois les plus importantes de l'épistémologie (l'étude de la méthode scientifique rationnelle). Si dans une théorie, on prouve une contradiction (comme vraie), une seule, alors la théorie entière s'écroule.

Exercice : montrer avec des diagrammes de Venn, une table de vérité et par calcul logique que: $(A \Rightarrow B) \Leftrightarrow \neg(A \setminus B)$ et que $(p \Rightarrow q) \Leftrightarrow ((\neg p) \cup q)$

3.2.9 "Si et seulement si", "XNOR" : l'équivalence logique, ($\Leftrightarrow$, $\triangleq$)

L'équivalence est une forme de synonymie logique entre deux propositions. $p \Leftrightarrow q$ est vrai si et seulement si p et q ont la même valeur de vérité. Montrer une équivalence mathématique, c'est montrer que on ne peut pas avoir p sans q – ni q sans p – ni $\neg q$ sans $\neg p$ – ni $\neg p$ sans $\neg q$. Les deux idées, p et q, sont fondamentalement liées et viennent forcément ensemble dans votre

paradigme, votre système de connaissances. Elles y sont soit toutes deux présentes, soit toutes deux absentes.

En pratique on démontre souvent $p \Leftrightarrow q$ en montrant $(p \Rightarrow q) \cap (q \Rightarrow p)$, d'où la notation.

Notez que les définitions cache souvent un "si et seulement si" même quand on utilise la formule "On dit que ... est un(e)... si...". Pourquoi ? Parce qu'une définition est quelque chose d'axiomatique, d'arbitraire. On décide que cette implication entre l'expression usuelle et le langage formel soit réciproque, que ces deux entités soit "mathématiquement synonymes". On choisit arbitrairement un mot, en étant très formel sur ce qu'il décrit, afin de le manipuler avec le langage humain, qui est un des points forts de notre cerveau. Une définition en maths, c'est un travail de traduction d'un concept du langage mathématique pour l'utiliser en langage visuel ou vernaculaire.

D'un point de vue ensembliste, être sûr que $p \Leftrightarrow q$ (supposer $p \Leftrightarrow q$), c'est avoir $p = q$, tout simplement (car on a $p \subset q$ et $q \subset p$, par implications réciproques).

Exercice bonus: réfléchissez et essayez de voir en quoi l'équivalence logique est un isomorphisme (cf plus bas).

3.2.10 Pratique de la logique booléenne: tables de vérité, calcul logique et théories logiques

[Commencer avec les tables, puis expliquer la notion de tautologie, voir le principe de non-contradition d'un point de vue formel.] [TODO : lois de De Morgan ; lois d'absorption; propriétés des algèbres d'ensembles (associativité, commutativité, distributivité dans les deux sens) ? mettre des diagrammes commutatifs ?] [TODO : parler de modèles; parler rapidement des logiques multivaluées, logiques non-standards (notamment modales), opération "nand" qui est totipotente et donc "génère" automatiquement les autres opérateurs; eletronique, réduction à forme dis/conjonctive, tables de Karnaugh ?]

3.2.11 Quelques exercices

Exercice: avec une table de vérité et par calcul logique, montrez l'idée intuitive que si deux choses s'impliquent mutuellement, elles sont équivalentes. Formellemment : montrer que $(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \cap (q \Rightarrow p))$ est une tautologie. Notez l'usage des parenthèses pour ceux qui utiliseraient cet outil de manière intuitive sans conscientiser ce processus intellectuel : ce qu'il y

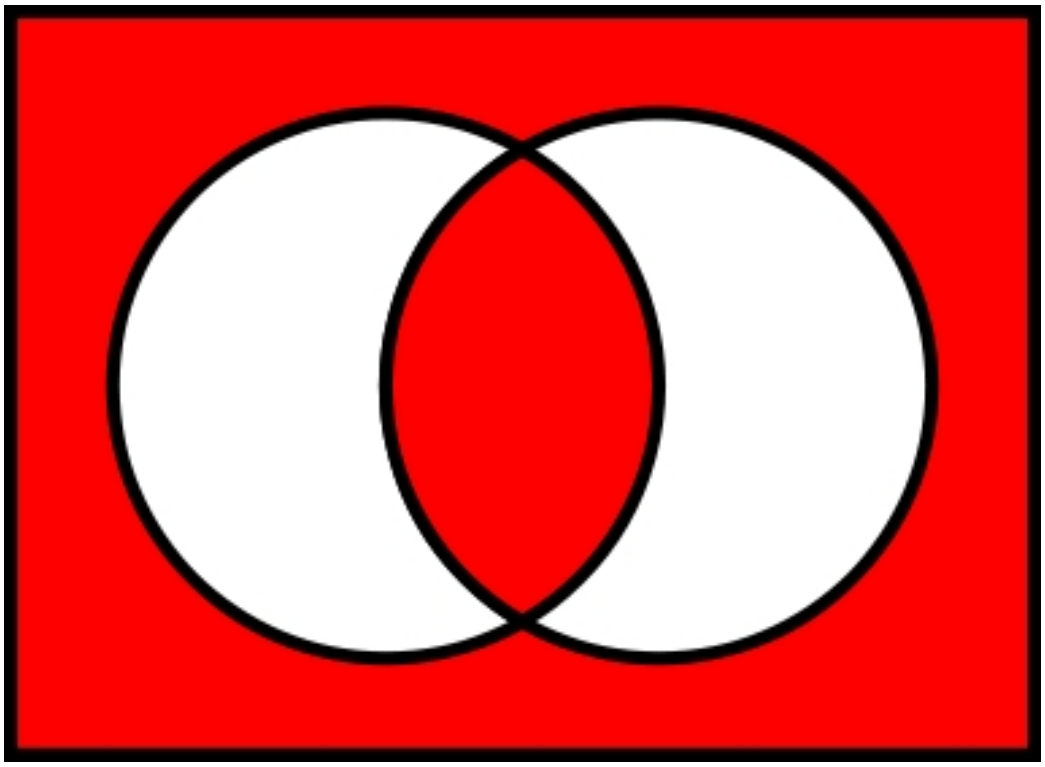


Figure 11: $A \Leftrightarrow B$: ensemble de tous les éléments répresentant "A équivalent à B" comme étant vrai

a le plus à l'intérieur se fait d'abord (je sais que certains peuvent se perdre dans leurs 'if' programmatiques, ce qui en général cause des bugs évitables et du temps perdu, donc c'est pas mal de s'entraîner à toutes ces petites manipulations logiques...).

Exercice: Recherchez en ligne "forme normale conjonctive/disjonctive" et faites la négation d'un exemple. Vérifiez vous-mêmes avec une table de vérité, ou éventuellement des ensembles, même si dans ce cas-là je conseillerais de s'amuser à le coder. Entraînez-vous aussi à exprimer vos 'if' plus intelligemment avec la négation (il y a souvent une optimisation à trouver sur des mix de ET et OU un peu complexes quand des négations interviennent).

Exercice bonus: essayez de dessiner (ou de représenter dans votre tête) $A \star B \star C$ avec des diagrammes de Venn, où $\star$ représente dans chaque cas soit l'intersection, soit l'union, soit la différence symétrique. Indice : AND, OR et XOR sont associatifs et commutatifs (cf plus bas pour la définition), donc l'ordre n'est pas important, et la notation sans parenthèse est légitime. On peut toujours donner un nouveau nom à un ensemble qu'on obtient par un calcul compliqué pour en faire un raccourci dans les calculs suivants (ah, douces variables).

Exercice bonus: Pour quels opérateurs logiques l'absence de parenthèses est-elle ambiguë, voire contradictoire ?

Exercice bonus: même question, mais en analysant les combinaisons d'opérateurs.

[TODO: add Venn diagram web applet here]

3.2.12 Pour aller plus loin

1) Trouvez une liste de tautologies à démontrer.

2) Essayez de designer un calculateur binaire basique, un "Full Adder". Car si vous connaissez le binaire, vous êtes enfin en mesure de savoir comment un ordinateur "pense", au fond. Comment on passe de la logique à l'arithmétique. Tout repose sur le binaire. Vrai ou Faux. 1 ou 0. Quand vous faites une somme en binaire, si vous vous concentrez sur une seule colonne des inputs de votre addition, vous n'avez que quatre cas possibles : 0 ET 0, 0 ET 1, 1 ET 0, 1 ET 1. Remplaçons les ET par des +. On obtient "$0+0=0$", "$0+1=1$", "$1+0=1$, et "$1+1=10$", sachant que $[10]_2$ est la représentation en binaire du nombre $[2]_10$ dans notre base décimale usuelle. Votre "retenue" dans l'addition n'est pas à dix, mais à deux, et à chaque puissance de deux (qui s'écrivent $[10]_2 = [2]_10$, $[100]_2 = [4]_10$, $[1000]_2 = [8]_10$,

etc, parce que, oui, les bases c'est intéressant).

Maintenant regardez la colonne des unités. Quand vos nombres en input sont identiques, le chiffre des unités de l'output est 0, quand ils sont différents, c'est 1. Voici l'addition : une porte logique XOR sur du binaire. La retenue, si elle est là (reconnue par une porte ET, on a une retenue que si 1 ET 1 sur les mêmes input de courant), est envoyée vers un bloc identique qui fera le même boulot pour les "2-aines", puis les "4-aines", puis les "8-aines", comme nous faisons avec nos dizaines et centaines depuis le CP. Voici, en un mot, l'informatique: *Through logic, we have tricked rocks into thinking.*

Optimisez votre design électronique de Full Adder avec des tables de Karnaugh. Google/Duckduckgo/Etc (+Images) Full Adder, Substractor, etc.

4 Théorie des ensembles

4.1 Vocabulaire préliminaire, rappels

On appelle l'**ensemble vide**, et l'on note $\emptyset$ (ou $\{\}$), l'unique ensemble sans élément. L'ensemble vide est toujours inclus dans tous les ensembles.

On dit que deux ensemble A et B sont **disjoints** si leur intersection est vide (les deux patates ne se touchent même pas). Formellement, $A et B disjoints \Leftrightarrow A \cap B = \emptyset \Leftrightarrow \neg(\exists x \in A, x \in B)$

Soit E un ensemble. On appelle **ensemble des parties** de E, et on note $\mathcal{P}(E)$, l'ensemble de tous les sous-ensembles de E. Par exemple, si $A = \{a, b, c, d\}$, alors

$$\begin{aligned}\mathcal{P}(A) = \{&\emptyset, \{a\}, \{b\}, \{c\}, \{d\},\\ &\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\},\\ &\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\}\end{aligned}$$

NB: $\mathcal{P}(\emptyset) = \emptyset$

On appelle **partition** d'un ensemble une division de cet ensemble en sous-ensembles disjoints. Exemple : $A = \{1, 2, 7, 12, 15, 21\}$, un ensemble de nombres, alors (A_1, A_2, A_3), où $A_1 = \{1, 2\}$, $A_2 = \{15\}$ et $A_3 = \{7, 12, 21\}$, est une partition de A.

On appelle **cardinal** d'un ensemble E, noté $card(E)$ ou $\#(E)$, le nombre d'éléments contenus dans E. Ex: $card(\{1, 2, 7, 10\}) = 4$

NB :

– $card(\mathbb{N}) = card(\mathbb{Z}) = card(\mathbb{Q}) = \aleph_0$, aussi appelé "infini discret" (lu "aleph zéro" ou "aleph nul")

– $card(\mathbb{R}) = card(\mathbb{C}) = card(\mathbb{R}^n) = \aleph_1$, aussi appelé "infini continu"

Rappel:

– $\mathbb{N}$ est l'ensemble des entiers naturels $\{0, 1, 2, 3, 4, 5, 6 \dots\}$. $\mathbb{N}^*$ c'est $\mathbb{N}$ sans 0.

– $\mathbb{Z}$ est l'ensemble des entiers relatifs $\{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}$

– $\mathbb{Q}$ est l'ensemble des nombres rationnels (=fractions) $\{\frac{a}{b} \parallel a \in \mathbb{Z} \text{ et } b \in \mathbb{N}^*\}$. On parle de "rationnels" car toute fraction exprime un rapport de proportion, un "ratio", entre deux nombres.

– $\mathbb{R}$ est l'ensemble des nombres réels; en gros, si l'on fait des suite $(u_n)_{n\in\mathbb{N}}$ à valeurs (d'output) dans $\mathbb{Q}$, alors l'ensemble de toutes les limites de suites possibles construit la droite réelle ; on remplit les "trous" entre les rationnels pour faire une droite bien nette. La racine carré de 2 ou le nombre π sont des "irrationels", des exemples de nombres qui sont réels mais pas exprimables comme un rationnel, uniquement comme une suite de rationnels qui s'approchent de plus en plus d'eux, à l'infini. Le nombre π, par exemple, peut-être écrit : $3/1+1/10+4/100+1/1000+5/10000\ldots$, et être approximé par la suite $(u_n)_{n\in\mathbb{N}} = (3, 3.1, 3.14, 3.141, 3.1415, \ldots)$

– $\mathbb{C}$ décrit l'ensemble des nombres complexes (aussi appelés imaginaires ou plus rarement transversaux, même si ç'aurait été un bien meilleur nom, ça représente mieux ce que c'est); il s'agit d'une $\mathbb{R}$-algèbre (vous verrez cela plus bas) construite sur $\mathbb{R}^2$ avec comme base les vecteurs $\{1, i\}$ et comme propriété multiplicative $i^2 = -1$. Tous nombre de $\mathbb{C}$ peut s'exprimer $x + i * y$ avec x et y deux nombres réels.

NB: on a $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. L'ensemble des nombres décimaux est un sous-ensemble de $\mathbb{Q}$ (cf. aussi nombre p-adiques).

NB: remarquez la bizarrerie ici : il y a autant d'entiers naturels (positifs) que d'entiers relatifs, et autant que de fractions. Mais par contre, il y a tellement plus de réels "non-fraction", irrationnels, que ça en devient un infini "plus grand"... mais qui reste le même, même en l'étendant à n dimensions! Nous verrons en quoi plus bas en travaillant la notion de bijection.

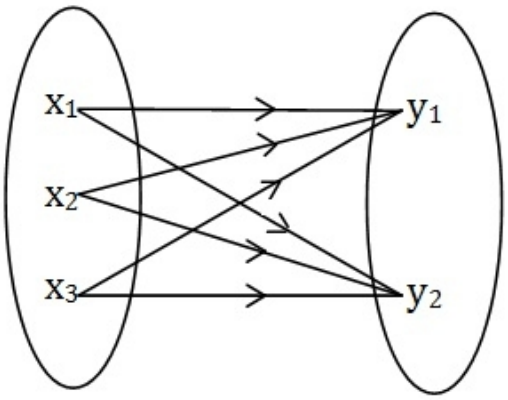
[TODO: a gif which shows the evolution of N to C ?]

4.2 Relations entre ensembles

On appelle le **produit cartésien** de deux ensembles A et B, et l'on note $A \times B$, l'ensemble contenant toutes les paires d'éléments de A et B (où l'ordre compte et l'élément de A est d'abord). Ces "paires ordonnées" sont appelées "**couples**", et les vecteurs 2D en sont un cas particulier.

Par exemple: $A = \{a, b\}$ un ensemble à 2 éléments, et $B = \{1, 2, 3\}$ un ensemble à 3 éléments. Alors $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$, un ensemble à $2 \times 3 = 6$ éléments.

On peut enchaîner les produits cartésiens. $A \times B \times C \times A \times E \times F$ est un ensemble de "sextuplets" (6-uplet ; array/liste de taille 6) chacun avec en première position un élément de A; en deuxième, un élément de B; en



$$A=\{x_1, x_2, x_3\} \quad B=\{y_1, y_2\}$$

$$A*B=\{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_2), (x_3, y_1), (x_3, y_2)\}$$

Figure 12: Exemple de produit cartésien de deux ensembles

troisième, de C; en quatrième, de A; en cinquième, de E et enfin en sixième position, de F.

Pour $A \times A$, on peut noter A^2, idem pour A^n en général (pour la suite de produits cartésiens succcessifs faisant intervenir n fois l'ensemble A). En général pour préciser qu'on choisit n éléments d'un ensemble A, on préfère écrire qu'on choisit un élément de son n-produit cartésien avec lui-même, A^n. On appelle les éléments de A^n des n-uplets, ou n-tuples. Les 2-uplets sont souvent appelés "couples", les 3-uplets "triplets".

NB : si vous faites de la théorie des catégories, $\|\mathbb{R}^n\|$ désigne l'ensemble sous-jacent l'espace vectoriel de dimension n basé sur les réels, $\mathbb{R}^n$. En termes informatiques, on peut penser $\mathbb{R}^n$ est l'ensemble de tous les arrays imaginables de float de taille n (même si l'ordinateur doit se contenter d'une approximation de cet espace mathématique pur). Si vous codez du jeu vidéo, ou que vous faites des sprites 2D ou des modèles 3D, vous avez travaillé (peut-être sans le savoir) sur une version informatique approximative de $\mathbb{R}^2$ ou de $\mathbb{R}^3$.

Exercice: Parfois les ensembles ont un nombre infini d'éléments. C'est le cas des intervalles réels. Si l'on prend l'intervalle $[0, 1]$ (tous les x tels que "$0 \leq x \leq 1$") et l'intervalle $[4, 6]$, quel est un bon moyen de visualiser $[0, 1] \times [4, 6]$, l'ensemble de tous les couples avec comme première coordonnée un élément de $[0, 1]$ et comme deuxième coordonnée un élément de $[4, 6]$? Indice : On a deux intervalles réels... Utiliser $\mathbb{R}^2$, le plan réel! Bonus : comment cette visualisation peut-elle s'étendre à des dimensions supérieures ?

Une "**relation** entre deux ensembles A et B" est un ensemble contenant un choix de couples d'éléments dont le premier membre de chaque couple provient A et le deuxième membre de chaque couple provient de B. Une autre façon de le voir: une relation $\mathcal{R}$ entre deux ensembles est tout simplement un sous-ensemble de leur produit cartésien.

Une relation d'un ensemble E, à E lui-même, est dite "binaire" (rien à voir avec le binaire en informatique, attention). Toute relation binaire est un sous-ensemble de E^2.

Une relation binaire $\mathcal{R}$ peut être:

– **réfléxive** : $\forall x \in A$, on a: $x\mathcal{R}x$ (ex: $=$, $\geq$ et $\leq$ sont réfléxives, car par exemple "$x \leq x$" est toujours vrai)

– **irréfléxive** : $\forall x \in A$, on a "$\neg(x\mathcal{R}x)$". (ex: $<$ et $>$ sont irréfléxives, car "$x < x$" est toujours faux; $\neg$ se lit "non-...")

– **symétrique** : $\forall (x, y) \in A^2$, on a $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ (ex: l'égalité, car $x = 2 \Rightarrow 2 = x$)

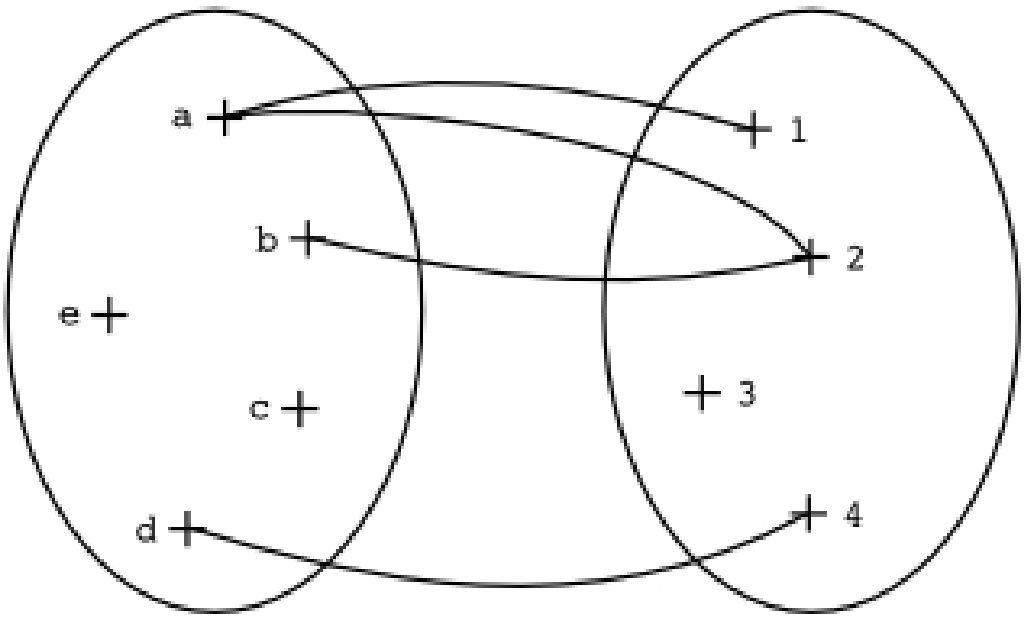


Figure 13: Dans le diagramme ci-dessus, on a deux ensembles $A = \{a, b, c, d, e\}$ et $B = \{1, 2, 3, 4\}$. Le couple $(a, 1)$ peut être compris comme le lien entre $\{a\}$ et $\{1\}$. Du coup, si on devait exprimer l'ensemble $\mathcal{R}$ des liens dans le diagramme au-dessus, on aurait $\mathcal{R} = \{(a, 1), (a, 2), (b, 2), (d, 4)\}$.

– **antisymétrique** :

$$\forall (x,y) \in A^2, \text{ on a: } \begin{cases} x\mathcal{R}y \\ \\ y\mathcal{R}x \end{cases} \Rightarrow x = y$$

– **transitive** :

$$\forall (x,y) \in A^2, \text{ on a: } \begin{cases} x\mathcal{R}y \\ \\ y\mathcal{R}z \end{cases} \Rightarrow x\mathcal{R}z$$

NB : $=, \geq, \leq, >, <$ et le parallélisme // sont transitives, la perpendicularité $\perp$ ne l'est pas.

NB: pour la définition de la symétrie d'une relation, remarquez qu'on a dans cette formule une implication "$\Rightarrow$" qui a l'air de n'aller que dans un seul sens, mais que comme on vérifie cette propriété pour tous les couples de A^2, c'est vrai aussi dans le sens inverse si on commence avec le couple (y, x), on aurait $2 = x \Rightarrow x = 2$, et donc qu'il s'agit en fait aussi d'une équivalence ("$\Leftrightarrow$") évidente ! Mais c'est toujours plus propre de garder la version qui fait le moins de suppositions.

NB: pour la définition de l'antisymétrie d'une relation, l'idée, c'est que le SEUL cas où ça peut aller dans les deux sens ($x\mathcal{R}y$ ET $y\mathcal{R}x$) c'est le cas EVENTUEL d'égalité (ex: $\leq$ est antisymétrique car si "$x \leq y$ ET $y \leq x$" alors nécessairement "$x = y$"). Cela ne veut pas dire que ce cas d'égalité existe !! Juste que si on voit $x\mathcal{R}y$ et $y\mathcal{R}x$ avec une relation qu'on sait être antisymétrique, on peut en déduire qu'il s'agit du cas d'égalité (ex: $<$ et $>$ sont antisymétriques mais sont quand même irréfléxives donc n'ont aucun cas d'égalité, donc vous auriez atteint une contradiction en cas de ($x\mathcal{R}y$ ET $y\mathcal{R}x$) où R est une 'relation d'ordre stricte').

On appelle une **relation d'équivalence** toute relation : **réflexive, symétrique, transitive** (exemples : égalité, congruence modulo n, parallélisme). Celles-ci jouent un rôle pratique fondamental dans les mathématiques à haut niveau, mais moins en informatique, à part si vous voulez poussez loin votre programmation fonctionnelle (ça en vaut la peine).

Si $\sim$ est une relation d'équivalence quelconque, on note $[x]$, et on appelle "classe d'équivalence d'un élément x modulo la relation $\sim$" l'ensemble des

éléments qui sont "égaux" à x si l'on considère que cette relation est une forme d'égalité, c'est-à-dire tous les y tels que $x \sim y$. Par exemple, pour le parallélisme, si x est une droite horizontale, toutes les autres droites horizontales (qu'on nommerait $y_1, y_2, \dots$) sont "égales" à x car elles sont parallèles à x. La "classe d'équivalence de la droite x modulo la relation de parallélisme $//$" est l'ensemble de toutes les droites dont la direction est horizontale. N'importe quelle droite peut servir pour illustrer cette direction : on dit que x est un représentant de la classe $[x]$ et n'importe quel élément (soit x, soit y_1, soit y_2,...) convient pour être un représentant de sa classe (ici, classe des droites d'une certaine direction).

NB : Le représentant x se trouve dans l'espace avec les droites de départ (nommons le E), ainsi que les droites y_i. Par contre, $[x]$ se trouve dans un autre espace, appelé "espace quotient de E par la relation d'équivalence $\sim$", et noté $E/\sim$. Pour qu'un tel "quotientage par une relation d'équivalence" (construction de l'espace où on réduit des éléments équivalents en un seul élément) soit autorisé, il faut juste vérifier que les mêmes objets d'une classe d'équivalence ont bien le même rôle, fonctionnent parfaitement identiquement, dans l'ensemble d'arrivée. Un bon exemple, sur une horloge à 12 heures, avancer de 16 heures et avancer de 4 heures donne le même résultat. Le mot "modulo" pour les relations d'équivalence fait d'ailleurs référence à l'opérateur de "congruence modulo n", utilisé dans le quotientage à partir duquel on définit les maths de l'horloge, mais il ne faut pas confondre les usages.

On appelle une **relation d'ordre (large)** et (on note en général "$\leq$") toute relation : **réfléxive, antisymétrique, transitive** ($\geq$, $\leq$, ou encore, l'inclusion $\subset$ entre ensembles, sont des relations d'ordre). On distingue les relations d'ordre partielles des relations d'ordre totales: dans une relation d'ordre totale, toute pair d'éléments de notre ensemble sont liées par la relation (ex: $\leq$ and $\geq$ sont des ordres totaux sur $\mathbb{R}$, mais pas sur $\mathbb{C}$).Les relations d'ordre jouent un rôle important dans les fondements de l'informatique théorique, notamment pour la définition de la récursion. En effet, comment définir un cas "tout en bas" traitable en temps réel, si l'on n'a pas de notion de ce qui est le "bas" d'une structure de données ?

On appelle relation d'ordre strict toute relation : irréfléxive, antisymétrique, transitive (ex: $<$ et $>$). Les ordres stricts sont beaucoup plus rares, en général les ordres larges sont plus efficaces pour construire des choses pertinentes, au point où si vous entendez "relation d'ordre" sans préciser, c'est qu'on parle

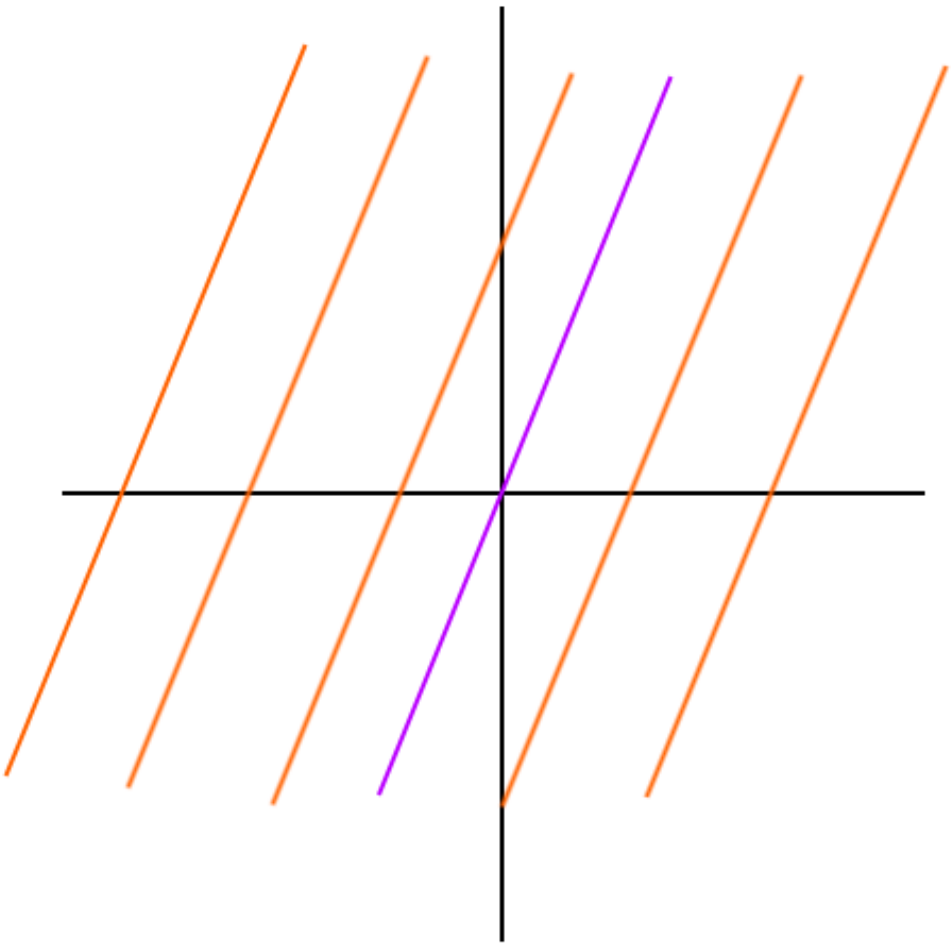


Figure 14: Exemple d'un quotient d'espace par la relation d'équivalence correspondant au parallélisme, partie 1. On a $E = \{ax + by = c \parallel (a, b, c) \in \mathbb{R}^3 \text{et}(a, b, c) \neq (0, 0, 0)\}$, l'ensemble des droites du plan (notez qu'une même droite peut avoir plusieurs façon d'être representé sous forme d'équation; précisément, une droite d_1 définie par l'équation $ax + by = c$ est égale à une droite d_2 définie par $Ax + By = C$ ssi $\exists k \in \mathbb{R}^*, A = ak, B = bk, C = ck$). Dans la figure ci-dessus, on a différents membres d'une même classe d'équivalence pour la relation d'équivalence représentant le parallélisme. Ces droites d_i parallèles ne diffèrent algébriquement que sur leur paramètre c_i respectif. La relation d'équivalence du parallélisme pourrait donc ici s'exprimer algébriquement comme $d_1 \sim d_2 \Leftrightarrow \exists k \in \mathbb{R}^*, a_1 = ka_2 \text{et} b_1 = k * b_2$. On choisit un seul représentant de la classe d'équivalence: la droite violette.

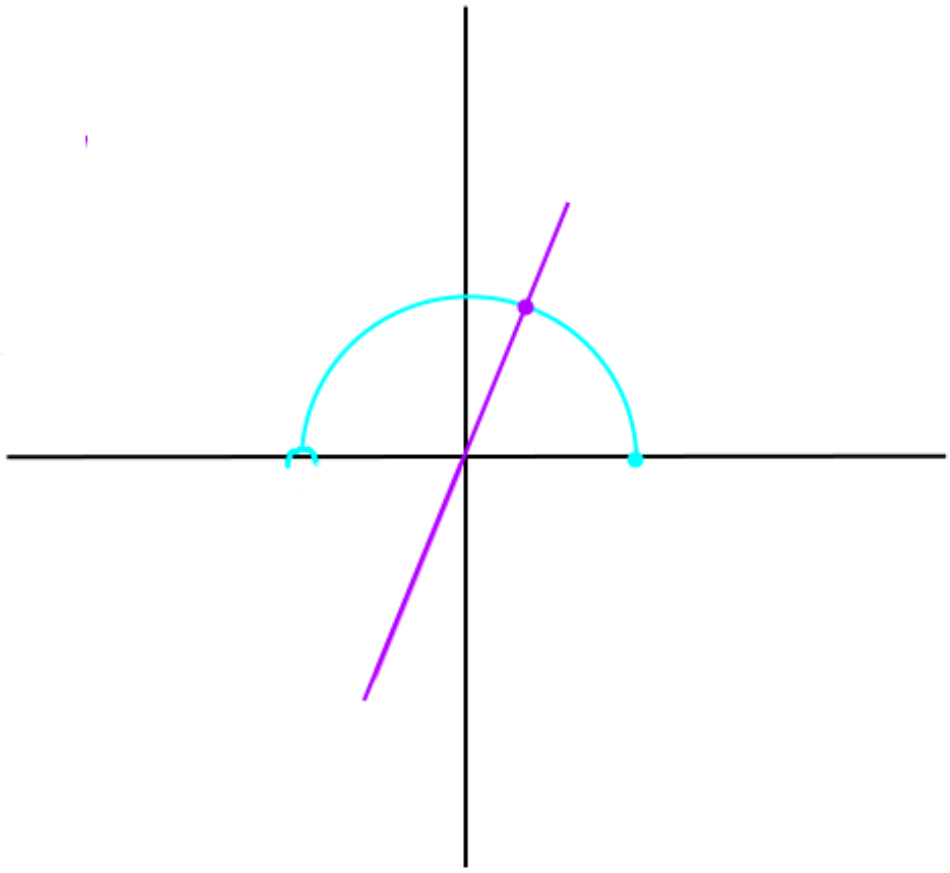


Figure 15: Exemple d'un quotient d'espace par la relation d'équivalence correspondant au parallélisme, partie 2. On peut faire ce qu'on a fait dans la partie 1 de l'exemple pour toute direction possible. Si, pour toutes les directions, on réduit chaque classe d'équivalence à un seul élément (choisir la droite violette parmi les droites oranges), et qu'on représente chaque élément comme un seul point (le point violet), on obtient un espace quotient (le demi-cercle cyan, avec un bord inclus, un bord exclu), qui est l'ensembles de tous les points ainsi obtenus. Il y a précisément autant de points sur le demi-cercle cyan que de directions distinctes que peuvent prendre nos droites, et chaque point de ce demi-cercle correspond à une et une seule direction. Notez que l'on pourrait choisir d'autres représentants/points pour l'espace quotient; cette représentation géométrique de l'espaec quotient n'est pas la "vérité", mais juste un représentant de celle-ci. Les propriétés et le comportement réel de l'espace quotient (et donc quelle représentation de celui-ci il vaut mieux choisir) dépendra de "où" ce quotient a lieu; mais pour expliquer cela, nous devrons expliquer les notions de "structure algébrique" et de "catégorie".

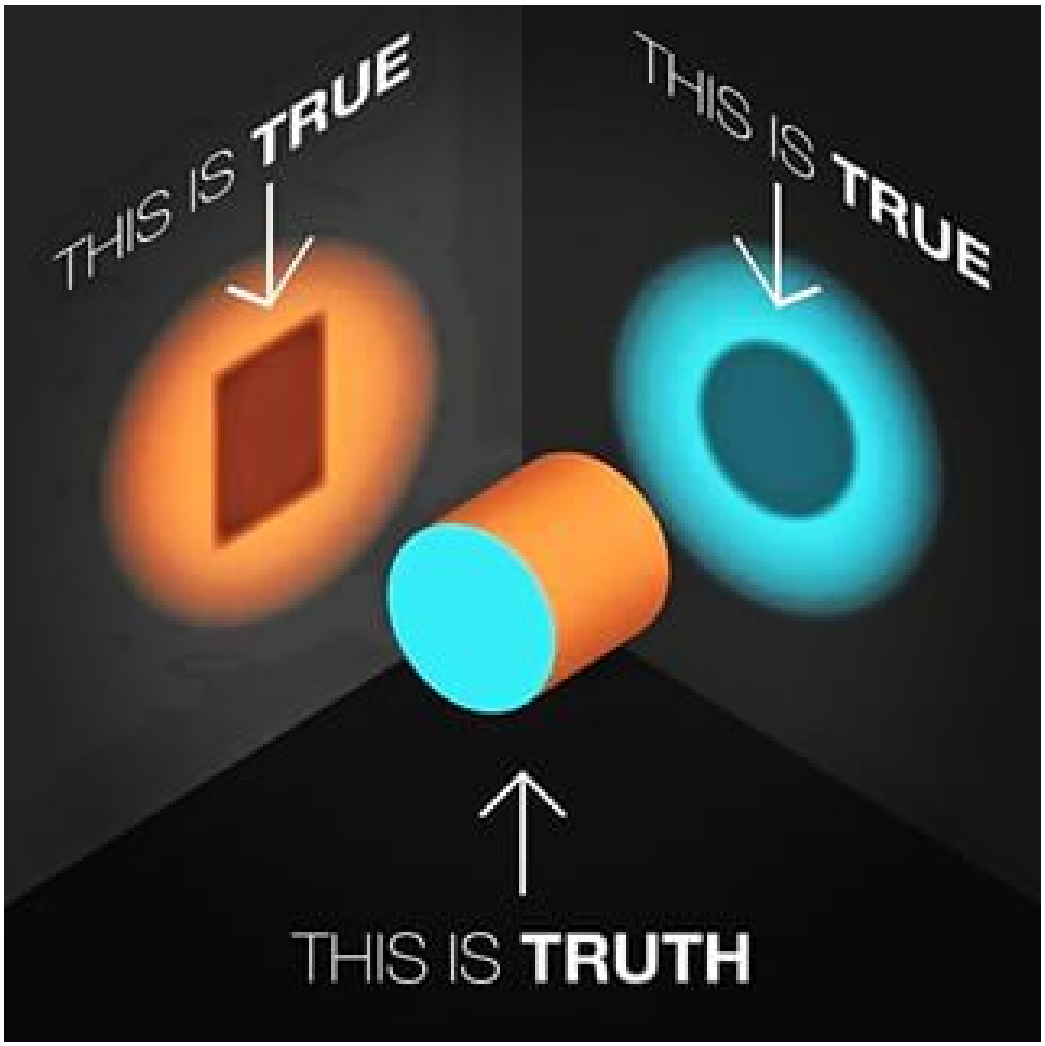


Figure 16: Distinction entre une représentation "vraie", et la "vérité" qu'elle représente. Une représentation est en général un "choix de point de vue", et il y a souvent des points de vue qui seront plus adaptés dans certains cas et pas dans d'autres.

d'un ordre large. On précisera par contre si l'ordre est total ou partiel.

NB : Beaucoup de relations n'ont pas de caractérisation particulière (ex: la perpendicularité qui est irréfléxive et symétrique; d'autres relations quelconques).

On appelle **poset** ou **ensemble partiellement ordonné** le couple $(X, \leq)$ d'un ensemble X muni d'une relation d'ordre sur ses éléments (poset pour *partially ordered set*). Un ordre est **total** sur X si tout élément de X peut-être ordonné avec tout ordre, c'est-à-dire si $\forall (x, y) \in X^2, x \leq y$ ou $y \leq x$.

Exercice : $\leq$, $\geq$ sont des ordres totaux sur $\mathbb{R}$, mais qu'en est-il de l'ensemble $\mathbb{C}$ des complexes ou de $\mathbb{R}^n$? Pourquoi ? Essayez d'inventer un ordre total sur $\mathbb{C}$ – il y a une infinité de bonnes réponses possible ! [Un exemple classique est l'ordre lexicographique.]

NB : L'inclusion "$\subset$" est un ordre partiel. Si l'on prend $E = \{1, 2\}$, on a $\{1\} \subset E$ et $\{2\} \subset E$, mais on n'a ni $\{1\} \subset \{2\}$, ni $\{2\} \subset \{1\}$. Exercice : dessinez le poset représentant l'inclusion dans $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$, l'ensemble des parties (=sous-ensembles) de $\{a, b, c\}$. On peut cependant définir une inclusion 'stricte' des ensembles. On parle alors de "sous-ensemble propre".

NB : les posets, que l'on peut représenter comme des graphes acycliques orientés, jouent un rôle important en théorie des catégories, car ils sont une manière d'analyser les catégories et leur comportement.

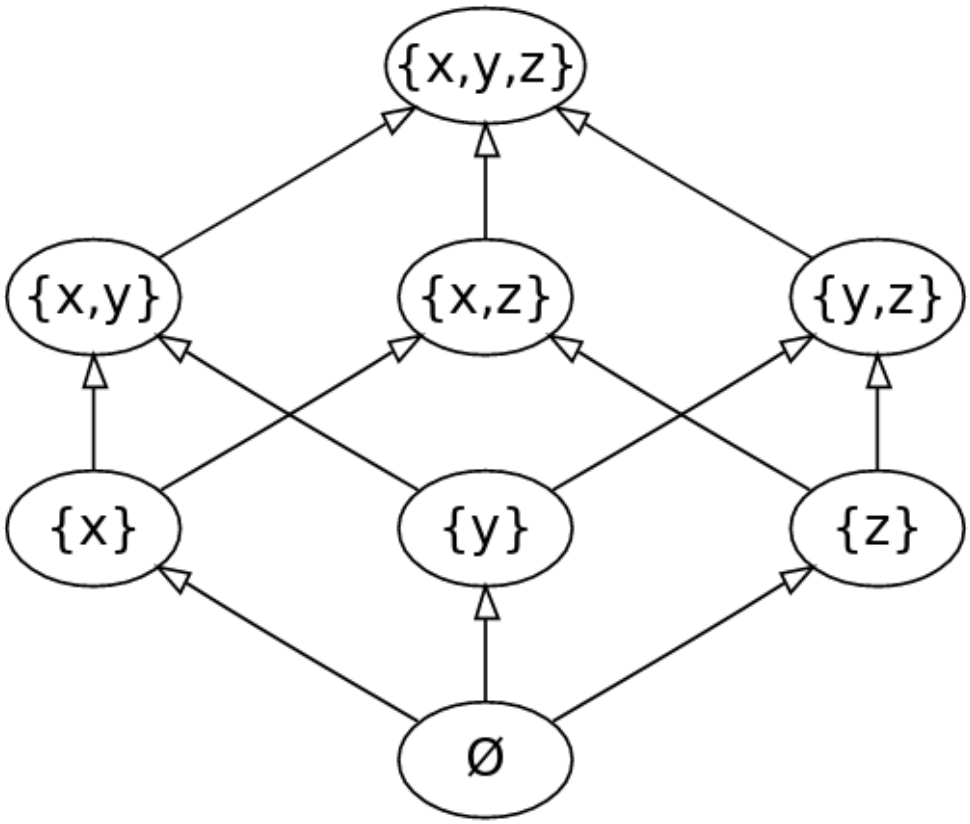


Figure 17: Exemple du diagramme de Hasse de $\mathcal{P}(\{x, y, z\})$, représentant le poset de l'ordre partiel d'inclusion par un graphe orienté acyclique.

4.3 Fonctions

La caractéristique définissante des fonctions ensemblistes, *a contrario* d'une fonction informatique comme "rand()", est qu'elle ne sont pas ambigües: un 4 en input qui donne une fois un 16 en output donnera toujours un 16 en output. Si votre fonction est fixée/définie, vous n'aurez pas un 4 en input qui donne un 16 une fois, et un -21 à un autre moment. Du moins pas avec ce qu'on appelle une "fonction" dans la théorie des ensembles.

Techniquement, une fonction (ensembliste) est juste un type de relation particulier entre deux ensembles A et B. Dans ce contexte, l'élément de A, appelé **antécédent**, joue le rôle d'input; celui de B, appelé **image**, joue celui d'output. A est appelé le **domaine** de f, ou ensemble de définition, et B le codomaine. Formellement, on dit que F "une **fonction** de l'ensemble A dans l'ensemble B" si F est une relation entre A et B telle que :

$$\forall(a_1, a_2) \in A^2, \forall(b_1, b_2) \in B^2, (a_1 F b_1 \text{ ET } a_2 F b_2 \text{ ET } a_1 = a_2) \Rightarrow b_1 = b_2$$

ou plus simple, dans une autre notation équivalente:

$$\forall(x, y) \in A^2, x = y \Rightarrow F(x) = F(y)$$

NB: si F possède le couple (a, b) (a est l'antécédent, et $b = F(a)$ l'image) alors, de manière équivalente, on peut écrire aFb. C'est juste que $a \to F(a)$ est une notation plus explicite par rapport au rôle que jouent les fonctions, qui est de transformer un objet en un autre selon un protocole fixé. De plus, $[a]F[F(a)]$ c'est lourd.

NB: si vous voyez le terme **"application"** ("map" en anglais), vous pouvez le comprendre comme "fonction". La distinction technique est qu'une fonction est une application ssi elle possède une image pour tous les éléments de A (son ensemble de définition $dom(f) = A$). Par exemple, $x \to \frac{1}{x}$ est une fonction qu'on peut définir sur $\mathbb{R}$, mais une application uniquement sur $\mathbb{R}^*$ car 0 n'est pas inversible. Nous ne ferons en général pas la distinction, sauf si vraiment nécessaire.

4.3.1 Image, préimage d'un ensemble par une fonction

Si vous voyez $f(x)$, où x est un élément, alors $f(x)$ est un élément de l'ensemble d'arrivée. Si par contre vous voyez $f(E)$ avec E un ensemble, alors $f(E)$ est aussi un ensemble, appelé **ensemble image** (parfois tout simple "l'image") de E par la fonction f. Cet ensemble contient les éléments

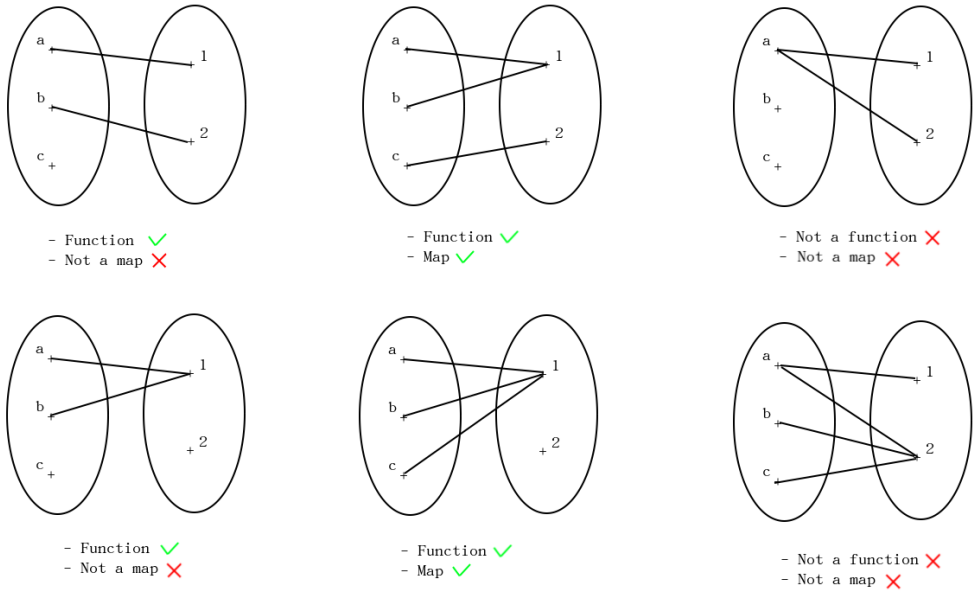


Figure 18: Exemples de relations entre ensembles qui sont ou des fonctions, ou des fonctions et des applications, ou ni l'un ni l'autre. Remarquez bien le diagramme critique en haut à droite: si un argument peut avoir plusieurs images, ce qu'on a n'est pas une fonction.

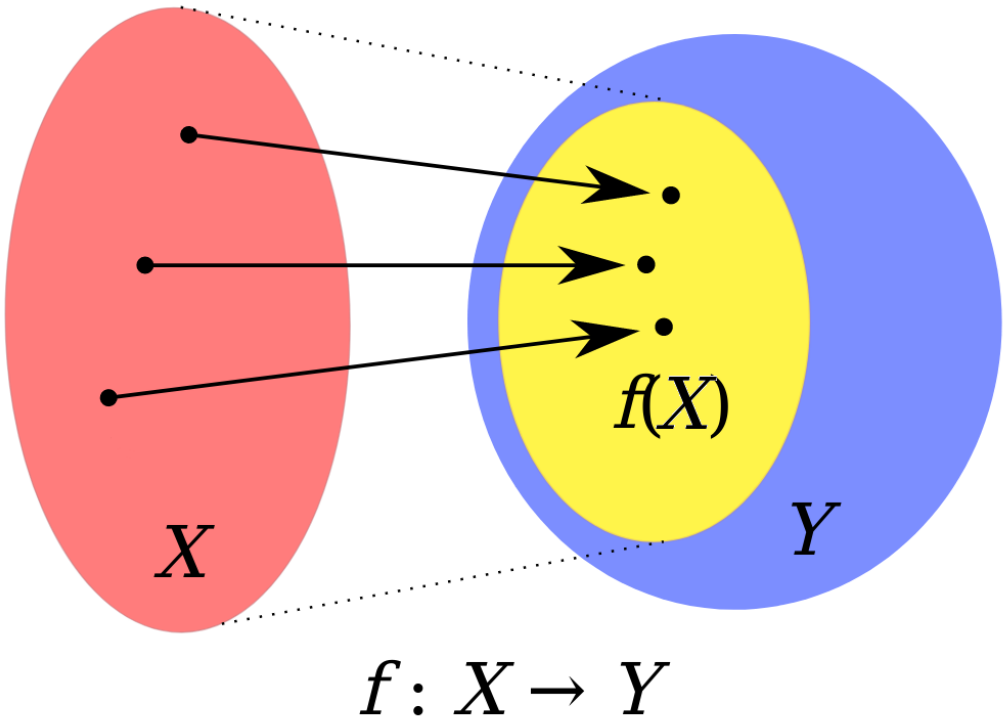


Figure 19: Visualisation de l'image $f(X)$ (incluse dans un codomaine Y) d'un ensemble X. L'image est définie par $f(X) = \{y \in Y \parallel \exists x \in X, f(x) = y\}$, ou de manière équivalente, $f(X) = \{f(a) \in Y \parallel a \in X\}$

de l'ensemble d'arrivée qui ont un antécédent par la fonction f (le champ des résultats "possibles" de votre fonction f, en gros). Il existe aussi un concept qui correspond à "tous les arguments possibles pour un ensemble d'images donné", appelé **préimage** ou **image réciproque**.

4.3.2 Composition de fonctions

Soit f une fonction de A dans B et g une fonction de B dans C, alors il existe une fonction h (notée $h = g \circ f$) de A dans C telle que $\forall a \in A, h(a) = g(f(a))$ Attention, je vous ai un peu simplifié la définition, techniquement, il faut en plus que g soit bien définie au moins en tout point de $f(A)$ au cas où $f(A)$ est un sous-ensemble de B distinct de B tout entier. Pour les codeurs, il faut qu'on puisse donner tous les retours de f en argument à g sans que

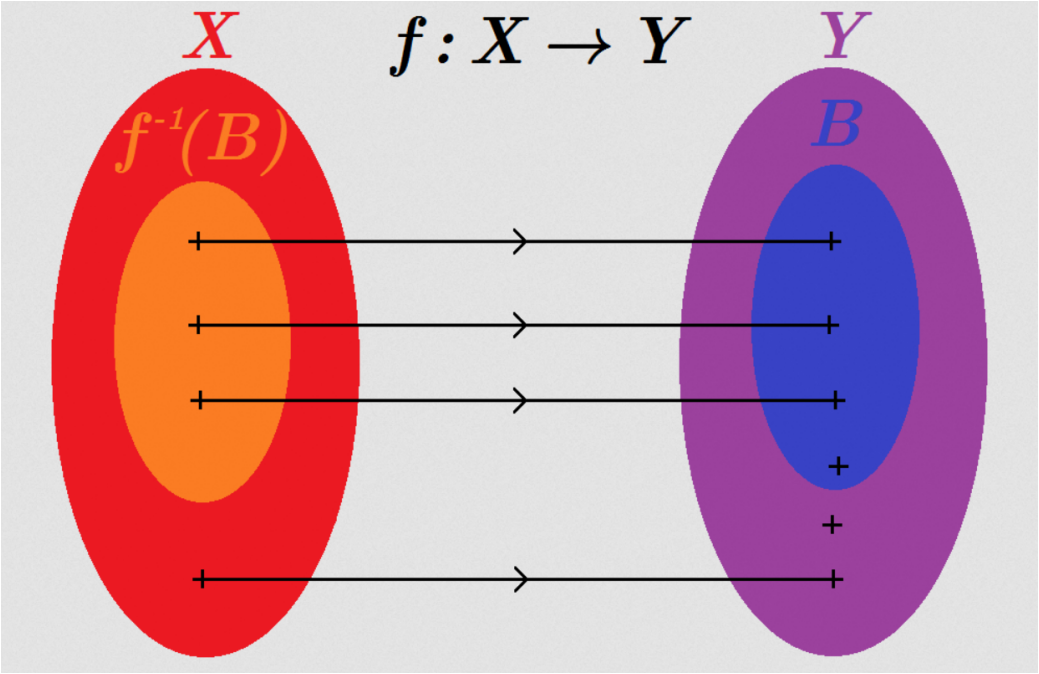


Figure 20: Visualisation de la préimage $f^{-1}(B)$ (incluse dans un domaine X) d'un ensemble B (inclus dans un codomaine Y). La préimage est définie par $f^{-1}(B) = \{x \in X \parallel f(x) \in B\}$.

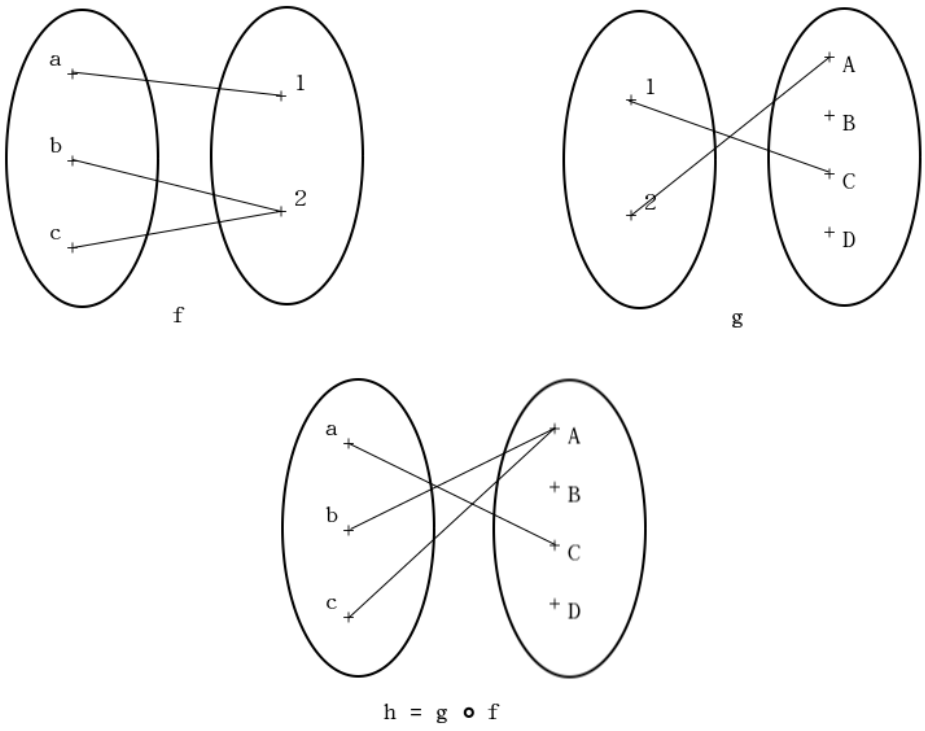


Figure 21: Visualisation d'une composition de fonctions $h = g \circ f$ sur des ensembles simples.

.

g renvoie une erreur. Je rappelle que $f(A)$ est un ENSEMBLE. Pour la définition concrète, l'ensemble de définition de h consiste en le plus grand sous-ensemble A' de A tel que $f(A')$ est inclus dans l'ensemble de définition de g. Autrement dit, $A' = f^{-1}(g^{-1}(C))$, la préimage de la préimage du codomaine final.

4.3.3 Ensemble de fonctions

On note F^E, ou $E \to F$, ou plus rarement $\mathcal{F}(E, F)$, l'ensemble des fonctions de E dans F. Ex: comme les suites réelles $(u_n)_{n\in\mathbb{N}}$ sont les fonctions de $\mathbb{N} \to \mathbb{R}$, on peut donc noter $\mathbb{R}^{\mathbb{N}}$ cet ensemble des suites à valeurs réelles. NB: la notation F^E s'explique par le fait que dans le cas où E et F sont finis, $card(F^E) = card(F)^{card(E)}$

4.3.4 Injectivité, surjectivité, bijectivité

Voici 3 notions fondamentales sur les fonctions. Une application f de A dans B est dite :

– **injective** ssi

$$\forall (x, y) \in A^2, f(x) = f(y) => x = y$$

NB: c'est l'implication en sens inverse de la définition d'une fonction, en gros. **Une fonction est injective si on n'a aucune image aui a plusieurs arguments possibles. TOUT élément de l'ensemble d'arrivée a AU PLUS une flèche/un lien qui arrive vers lui.** Il peut quand même y avoir des éléments de l'ensemble d'arrivée qui n'ont pas d'antécédent, bien sûr. Cette notion est utile pour pouvoir retrouver l'antécédent à partir de l'image. C'est en particulier la raison pour laquelle on choisit que "la racine carrée d'un nombre est toujours sa racine positive" vu que sinon on aurait toujours deux antécédents possibles (un positif et un négatif), sauf pour 0. Intuitivement, une injection va d'un ensemble "plus petit" dans un ensemble "plus grand" (voir NB en bas, il faut se méfier de ce que veut dire "plus petit/grand" à cause des différents types d'infini et des dimensions dans les espaces vectoriels, mais ça reste un bon moyen mnémotechnique, de penser à une piqûre pour "l'injection" : petit dans grand).

– **surjective** ssi

$$\forall y \in B, \exists x \in A, f(x) = y$$

NB: cela veut dire que **TOUT élément de l'ensemble d'arrivée a AU MOINS une flèche qui arrive vers lui**. En général, on peut considérer qu'une surjection est une fonction d'un ensemble "plus grand" dans un ensemble "plus petit" (voir NB en bas, penser au mot "surplomber" : tout est couvert).

– **bijective** ssi

$$\forall y \in B, \exists! x \in A \textbf{tel que} f(x) = y$$

NB : f est bijective $\Leftrightarrow$ f est injective ET surjective. Cela veut dire que **tous les éléments de l'ensemble de départ ont UN SEUL lien avec l'ensemble d'arrivée, et vice-versa**. Pour cette raison, une fonction bijective peut-être considérée comme une "application" dans les deux sens (vu qu'aucune des deux patates n'a de double-branche), et donc on peut définir une fonction dite **réciproque** notée f^{-1}.

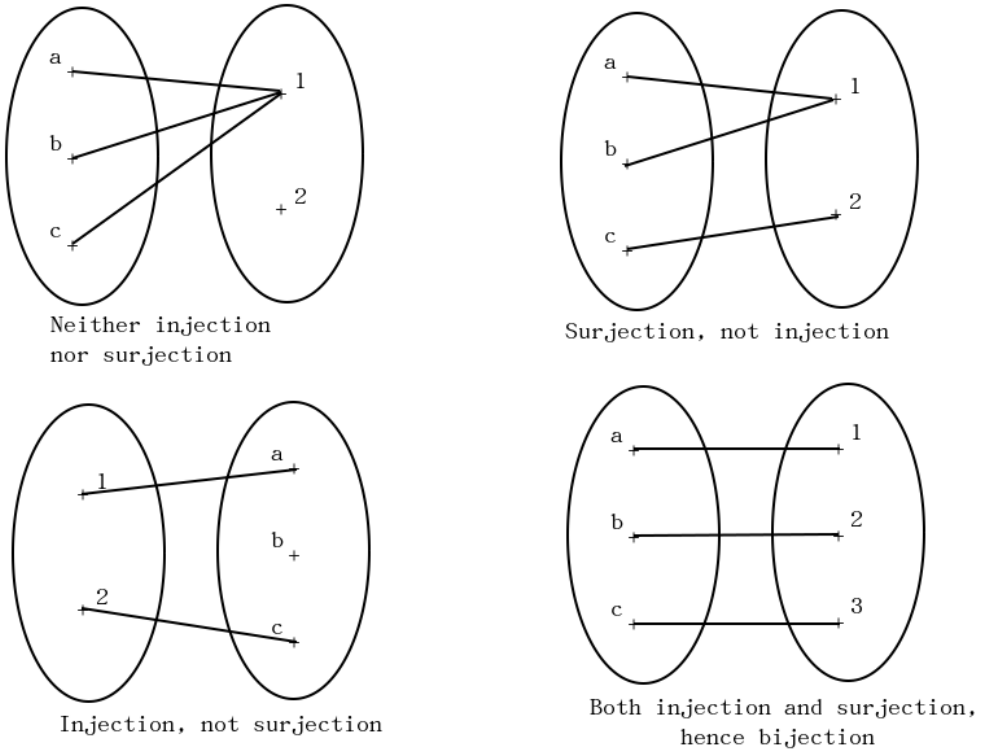


Figure 22: Exemple de fonction injective, surjective, bijective, ou rien.

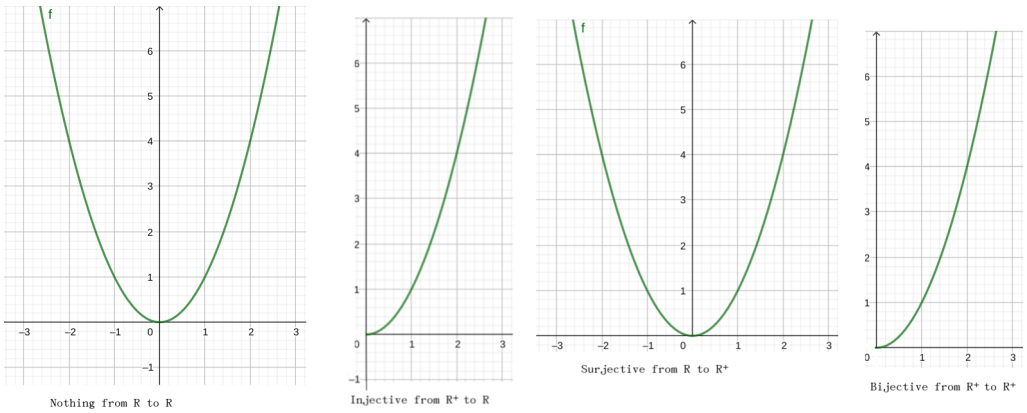


Figure 23: Exemple d'une même fonction étant injective, surjective, bijective, ou rien, selon le contexte (son domaine et son codomaine).

NB: CES NOTIONS DÉPENDENT COMPLETEMENT DE L'ENSEMBLE DE DÉPART (DOMAINE) ET D'ARRIVÉE (CODOMAINE). UNE MÊME FONCTION PEUT ÊTRE OU NE PAS ÊTRE INJ/SUR/BIJ SELON LE CONTEXTE ! Exemple très important: en notant $\mathbb{R}^+ = [0, +\infty[$ et avec $f = x \to x^2$, on voit que f est :

– surjective de $\mathbb{R}$ dans $\mathbb{R}^+$, mais pas injective

– injective de $\mathbb{R}^+$ dans $\mathbb{R}$, mais pas surjective

– bijective de $\mathbb{R}^+$ dans $\mathbb{R}^+$

NB : "ensemble plus petit" et "ensemble plus grand" prend un sens très particulier ici qui a à voir avec la notion de cardinal d'un ensemble et avec les différentes formes d'infini. On dit qu'un ensemble (fini ou infini) F est **discret si il existe une injection de cet ensemble dans** $\mathbb{N}$, ensemble des entiers naturels (il est alors "égal en taille ou plus petit que les entiers naturels", F dans $\mathbb{N}$, petit dans grand). Dans ce cas, si F est discret, et en plus infini, alors ce rapport est non seulement injectif mais aussi bijectif "F est d'un infini aussi grand que $\mathbb{N}$". $\mathbb{Z}$, ensemble des entiers relatifs, et $\mathbb{Q}$, ensemble des nombres rationnels (ensemble de toutes les fractions), sont dans ce type de bijection avec $\mathbb{N}$, donc sont aussi grands que $\mathbb{N}$ (aussi étrange que cela puisse paraître, c'est quelque chose qui fait complètement sens et est une des raisons majeures pour lesquelles on a adopté la théorie des ensembles: elle a permis de mieux comprendre le fonctionnement de l'infini, en démontrant qu'il y en avait différents types et en permettant leur

analyse). Par contre, il n'existe pas d'injection de $\mathbb{R}$ dans $\mathbb{N}$, donc $\mathbb{R}$ est un infini strictement plus grand! **On appelle l'infini de $\mathbb{R}$ infini "continu"**. En gros, **le discret c'est ce qu'on compte, le continu c'est ce qu'on mesure**. Si ces digressions vous intéressent, recherchez le 1er problème de Hilbert: l'hypothèse du continu.

Maintenant, pour vraiment vous faire péter un câble : il existe une bijection entre tout intervalle de $\mathbb{R}$ et $\mathbb{R}$ tout entier (exemple, $]-\pi/2, \pi/2[$ en bijection avec $\mathbb{R}$ par la fonction tangente ($tan(x)$) ! Cela veut dire qu'il y a strictement "plus d'infini" sur $[0, 1]$ qu'il n'y a "d'infini d'entiers naturels" ; et "autant d'infini" dans $[0, 1]$ que "d'infini dans $\mathbb{R}$". C'est fou, non ? Pourtant c'est vrai. Ou du moins, avec ces principes-là on a fait des maths solidement applicables à la physique (et autres domaines), ce qui est assez impressionnant et intriguant.

4.3.5 Famille d'ensembles

On appelle $\mathcal{F}$ une **famille** si $\mathcal{F}$ est une collection indexée (d'ensembles ou d'éléments) sur un ensemble I servant d'index. Par exemple, une liste de n nombres réels peut s'écrire $\{x_i \in \mathbb{R} \parallel i \in I\}$ où $I = [[1; n]]$.

4.4 Opérateurs

4.4.1 Opérateur binaire

On appelle **opérateur binaire** une fonction qui prend deux argument en input, et renvoie un seul retour en output (rien à voir avec le binaire informatique, c'est juste l'idée que ton opérateur prend 2 inputs, un opérateur ternaire en prendrait 3, etc). Formellement, on dit que $\star : A \times B \to C$, c'est-à-dire $\star$ (étoile) est une fonction du produit cartésien de A et B dans un ensemble C.

NB: La choix du symbole $\star$ comme notation, c'est pour avoir un opérateur abstrait, capable d'en représenter plein d'autres. Comme c'est un symbole que vous ne connaissez pas, ça devient plus simple d'éviter les erreurs liées aux réflexes et suppositions habituels. On utilisera aussi le symbole $\perp$ ('perp') pour un second opérateur quand on aura besoin d'exprimer les liens entre 2 opérateurs différents, comme l'addition et la multiplication.

Vous en connaissez plein, des opérateurs binaires ! $+, -, \times, \div, \hat{}$, modulo $(\%), \cap, \cup, \&\&, ||, \Rightarrow, \Leftrightarrow, \leq$ ($\leq$ peut-être un opérateur pour construire des

propositions logiques, donc une application de $(A^2 \to \{Vrai, Faux\})$, on le voit souvent en info), etc. Mais attention, le même symbole peut faire référence à différents opérateurs, tout dépend du contexte !! La multiplication des matrices ne fonctionne pas comme la multiplication normale qu'on s'imaginerait (elle est un assortiment de produits scalaires) - l'addition des matrices non plus, même si ça ressemble un peu plus à ce à quoi on "s'attendrait". Même, la soustraction dans $\mathbb{N}$ n'est pas la même que la soustraction dans $\mathbb{Z}$, vous verrez pourquoi plus bas.

Maintenant, pourquoi comprendre cela comme deux inputs, un output ? En gros parce que tout élément de $A \times B$, appelés "couple", fonctionnent comme deux éléments.

Exemples :

– $12 + 5 = 17$, on peut aussi le noter $+(12, 5) = 17$ ou $add(12, 5) = 17$ ou $f(12, 5) = 17$ pour comprendre le lien avec l'informatique : deux arguments en input (12 et 5), que l'on peut considérer comme un couple, avec ici un élément de un argument en output (17). Ici, $+ : N \times N \to N$

– Dans un $\mathbb{K}$-espace vectoriel E, le produit scalaire de deux vecteurs u et v, noté $\langle u|v\rangle$, est un opérateur de $E \times E \to K$.

– Soient $x \in E$ et $f \in F^E$ [aussi écrit $(E \to F)$], ensemble des fonctions de E dans F. On note $\circ$ l'opérateur d'évaluation d'une fonction, tel que :

$$\circ : \begin{array}{ccc} \big((E \to F) \times E\big) & \to & F \\ (f, x) & \to & f(x) \end{array}$$

c'est-à-dire, $\circ(f, x) = f \circ x = f(x)$ $\circ$ est aussi appelé opérateur de composition de fonctions.

– On prend l'alphabet binaire $A_b = \{0, 1\}$ et l'alphabet latin $A_l = \{a, b, c, ..., y, z\}$. Soient L_b un langage sur A_b et L_l un langage sur A_l. Un langage est un défini comme un ensemble de mots sur un alphabet. Un mot est défini comme un string (une chaînes de symboles) sur un alphabet. Par exemple L_l pourrait être l'ensemble des mots qui ne contiennent que des groupes de 5 lettres, et donc "aaaaaaaaaauuuuucccccc" est un mot de L_l. On note "+" l'opérateur représentant la concaténation de mots ("0101" + "*chien*" = "0101*chien*"), qui est non-commutatif. Alors $+ : L_b \times L_l \to L_a$, où $L_a = +(L_b \times L_l)$ est un langage, ensemble image de (à spécifier) sur l'alphabet $A_a = \{0, 1, a, b, c, \ldots, y, z\} = A_b \cup A_l$.

Exercice bonus : Comment décririez-vous ce que représente $+(L_b \times L_l) = L_a$, l'image de l'ensemble $L_b \times L_l$ par la fonction de concaténation notée $+$, en

fonction des langages L_b et L_l ? Est-ce que ce langage L_a est égal au langage L sur l'alphabet A_a tel que $L = A_a^*$ = tous les mots possibles sur l'alphabet A_a, ou l'image L_a est-elle un sous-ensemble propre de L (c'est-à-dire inclus dans L mais différent de L) ?

NB : l'étoile de Kleene A^* est un opérateur unaire qui transforme un alphabet en l'ensemble de tous les mots possible sur cet alphabet. Il joue un rôle très important dans la théorie des catégories quand on s'intéresse aux monoïdes (cf plus bas) : c'est le "foncteur libre" de la catégorie Set des ensembles vers la catégorie Mon des monoïdes (un outil pour transformer n'importe quel ensemble en un monoïde fonctionnel).

4.4.2 Opérateur n-aire

On appelle opérateur n-aire un opérateur qui répète la même opération binaire $n-1$ fois d'affilée sur un ensemble à n-éléments. Pour l'addition, l'opérateur n-aire est généralement noté Σ ("sigma", pour "somme"); pour la multiplication Π ("pi", pour produit). La partie en-dessous du symbole définit le point de départ de l'index, la partie au-dessus sa condition d'arrêt; si rien d'autre n'est pas précisé, on considère que les valeurs de l'index augmente par 1 à chaque valeur.

- somme des 2 puissance i pour i allant de 0 à 5:

$$\sum_{i=0}^{i=5} 2^i = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = 63$$

- produit des $2+i$ pour i allant de 0 à n (le point d'exclamation représente ici la "factorielle", un opérateur unaire représentant la multiplication des entiers successifs):

$$\prod_{i=0}^{i=n} 2 + i = (2+0) \times (2+1) \times (2+2) \times \cdots \times (2+n) = \frac{(n+2)!}{1!} = (n+2)!$$

- intersection de 3 ensembles, en employant en ensemble indexeur $I = \{1, 2, 3\}$:

$$A_1 = \{a, b, c\}, A_2 = \{a, c\}, A_3 = \{a, b\}, \bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 = \{a\}$$

On peut avoir des index multiples sur des opérateurs n-aires. Souvent, quand on a plusieurs index, il vaut mieux visualiser le déroulement d'un opérateur n-aire comme un objet avec autant de dimensions qu'on a de variables servant d'index. Donc, par exemple pour deux index, un truc rectangulaire:

$$\begin{aligned}\sum_{i=0,j=7}^{i=2,j=10} i*j = {} & 0*7+0*8+0*9+0*10+ \\ & 1*7+1*8+1*9+1*10+ \\ & 2*7+2*8+2*9+2*10\end{aligned}$$

On peut aussi avoir des schémas d'indexation un peu plus compliqués. Par exemple:

$$\sum_{i=0,\ j=0}^{i=4,\ 2j\leq i} a_{i,j}$$

peut être lu

$$\begin{aligned}&a_{0,0}+\\ &a_{1,0}+\\ &a_{2,0}+a_{2,1}+\\ &a_{3,0}+a_{3,1}+\\ &a_{4,0}+a_{4,2}+a_{4,4}\end{aligned}$$

NB: l'opération "fold" (aussi appelé "reduce") sur un type liste/array en informatique revient en général à appliquer un opérateur n-aire.

4.4.3 Stabilité d'un opérateur

Une dernière chose *très* importante pour la partie suivante. On appelle "opérateur binaire **stable**" ou "**loi de composition interne**" tout opérateur de $E \times E \to E$. C'est-à-dire un opérateur qui donne toujours un résultat dans le même ensemble que ses inputs. Cette notion de stabilité ("closure" en anglais, rester dans le même ensemble après une opération donnée) est extrêmement importante en mathématiques. *Elle est une condition nécessaire au fonctionnement de la plupart des propriétés des structures algébriques.*

Nous en venons au point sûrement le plus intéressant de ce cours: les structures algébriques.

5 Construction hiérarchique des structures algébriques fondamentales

L'idée ici, c'est de faire une "cartographie" de la colonne vertébrale, du tronc des mathématiques. D'avoir une organisation des outils qu'on a développés pour faire sens de ce système inter-relié auto-constructeur que sont les mathématiques. Le sujet est assez hiérarchisé, et offre les clefs pour explorer l'écosystème des maths.

5.1 Structures algébriques

Tous les exemples non-développés dans la suite sont à vérifier par vous-même: c'est comme ça que vous comprendrez les notions abstraites, en les comparant à ce que vous connaissez mieux. Les contre-exemples sont aussi très importants. N'hésitez pas à en chercher vous-même.

Tous les cas suivants sont à comprendre, ceux à "comprendre le mieux par coeur", ceux que vous devez pouvoir reconnaître aussi bien que vous reconnaissez la différence entre deux droites parallèles et deux droites sécantes, sont "**groupe abélien**" et "**corps**", car ils interviennent dans la définition d'un espace vectoriel. Eventuellement "**monoïde**" parce qu'il est simple, et pour son rôle en théorie des langages et en théorie des catégories. Enfin "**anneau**" et "**algèbre**" car ils seront importants pour les polynômes.

Ceci dit, le reste du vocabulaire est quand même très, très utile pour se créer une cartographie du bestiaire des maths et se donner une idée des interactions entre structure algébriques de types différents. Ces intéractions entre structures sont un sujet on-ne-peut-plus fondamental pour comprendre les maths à un plus haut (si ça vous rend curieux, voici un bon article introductif sur le Lemme de Yoneda http://www.math3ma.com/mathema/2017/8/30/the-yoneda-perspective). Autre que vous aider à dompter votre pensée, et vous créer une machette pour explorer la jungle mathématique, c'est utile notamment pour certains protocoles en programmation fonctionnelle de haut niveau, notamment tous les questions de démonstration automatique (notamment de l'infaillibilité d'un module de code, ce qui commence à devenir important en sécurité informatique) qui s'inspirent de la théorie des types.

Une structure algébrique, ou un "espace" dans le sens général du terme, est un ensemble muni de propriétés fixées.

1. – Magma

   On appelle magma un couple $(E, \star)$ où E est un ensemble et $\star$ est une loi de composition interne sur E. Ex :

   – $(\mathbb{N}, +)$ est un magma, car $+$ est stable dans $\mathbb{N}$.

   – $(\mathbb{N}, -)$ n'est pas un magma, car la soustraction n'est pas stable dans $\mathbb{N}$ (ex: $7 \in \mathbb{N}$ et $12 \in \mathbb{N}$ mais $7 - 12 = -5$ et $-5 \notin \mathbb{N}$)

   – $(\mathbb{Z}, -)$ est un magma

   – $(\mathbb{Z}, \div)$ n'est pas un magma

   – $(\mathbb{N}, \times)$ est un magma

   – $(\mathbb{R}, \times)$ est un magma

   – $(\mathbb{R}^*, \div)$ est un magma, mais pas $(\mathbb{R}, \div)$ (car il faut que l'opérateur soit une application, pas juste une fonction, et $a \div 0$ est indéfini pour tout réel a).

   NB: le magma est un peu le bloc de base "sans rien", de la théorie des structures algébriques (l'algèbre abstraite). "Sans rien", à part la stabilité de l'opérateur, qui "va de soi" parce que le fondement de la théorie des structures algébriques est bien de "construire le langage mathématique autour de l'isolation des structures pour mieux les analyser"; pas étonnant alors que le bloc de base ait une propriété comme la stabilité de son opérateur.

2. – Monoïde

   Soit E un ensemble, $\star$ un opérateur. On dit que $(E, \star)$ est un **monoïde** ssi il vérifie les propriétés suivantes:

   – $(E, \star)$ est un magma

   – $\star$ est **associative** :

   $$\forall (x, y, z) \in E^3,\ (x \star y) \star z = x \star (y \star z)$$

   – existence d'un **élément neutre** (aussi appelé **identité**, comme "identique") (noté e) pour $\star$:

   $$\exists e \in E, \forall x \in E,\ x \star e = e \star x = x$$

Ex:

– $(\mathbb{N}, +)$ est un monoïde (c'est en plus un monoïde commutatif).

– $(\mathbb{N}^*, +)$ n'est pas un monoïde

– $(\mathbb{Z}, -)$ n'est pas un monoïde (car la soustraction n'est pas associative)

– $(\mathbb{N}*, \times)$ est un monoïde.

– Tout langage muni de la concaténation stable et du mot vide (=string vide) est un monoïde.

NB :

— dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, l'élément neutre pour l'addition est 0, le neutre pour la multiplication est 1.

— Le vecteur nul $(0, 0, 0, ..., 0)$ à n coordonnées (=de dimension n) est le neutre pour l'addition de $\mathbb{R}^n$.

— Dans les espaces de fonctions, le neutre pour l'addition, s'il existe, est la fonction "identiquement nulle" de cet espace (la constante $(x \to 0)$, la matrice nulle, etc). Le neutre pour la multiplication (si celle-ci est l'extension point-par-point de la multiplication basique) est la fonction constante $(x \to 1)$. Le neutre pour la composition de fonctions (opérateur $\circ$) est en général la fonction $Id = (x \to x)$.

— Dans les espaces de matrices, vu que les matrices sont des fonctions (applications linéaires) et que leur produit fonctionne comme la composition, la fonction identité est la matrice I_n avec des 1 sur la diagonale principale et des 0 partout ailleurs.

— Le neutre pour la concaténation est le string vide ("", aussi noté ϵ).

— Le neutre pour l'union d'ensembles est l'ensemble vide, le neutre pour l'intersection est l'ensemble "maximal" dans lequel on se place.

NB: Certains neutres ne sont neutres que d'un côté, par exemple 1 est neutre à droite pour l'opérateur puissance "$\hat{}$" $(a^1 = a)$, mais n'est pas neutre à gauche $(1^a = 1 \neq a$, dans le cas général où $a \neq 1)$.

NB: Si un neutre existe, il est UNIQUE (exercice: démontrer l'unicité; exemple super classique, supposer qu'il existe deux neutres différents et montrer qu'ils sont forcément égaux).

NB: Notez l'ordre dans la formule pour l'élément neutre. Exercice : expliquer la différence si on alterne le "il existe e" et le "pour tout x".

3. – Groupe

   On dit que $(E, \star)$ est un **groupe** ssi il vérifie les propriétés suivantes:

   – $(E, \star)$ est un monoïde

   – existence d'**éléments symétriques** pour $\star$:

   $$\forall x \in E, \exists sym(x) \in E, x \star sym(x) = sym(x) \star x = e$$

   On dit que $(E, \star)$ est un **groupe abélien** (ou **groupe commutatif**) ssi :

   – $(E, \star)$ est un groupe

   – $\star$ est **commutative** :

   $$\forall (x, y) \in E^2, x \star y = y \star x$$

   NB : un groupe abélien a donc 5 propriétés : stabilité de l'opérateur, associativité de l'opérateur, élément neutre pour l'opérateur, symétrie des éléments par rapport à l'opérateur, commutativité de l'opérateur.

   NB : pour l'addition, on note $-x$ le symétrique d'un élément x et on l'appelle "**opposé**" ; pour la multiplication, on le note $\frac{1}{x}$ ou x^{-1} en général, et on l'appelle "**inverse**" ; pour la composition de fonctions, on le note en général f^{-1} et on l'appelle "**réciproque**". Généralement, on emploie la même notation que la multiplication quand on parle d'un seul opérateur abstrait comme $\star$.

   NB : le fait que la soustraction et la division ne soient pas associatives explique cette construction : on se base sur $+$ et $\times$ qui marchent bien, et on étend les notations de ces opérateurs à $-$ et $\div$ si les éléments symétriques sont présents (*"soustraire c'est additioner par l'opposé, diviser c'est multiplier par l'inverse"*).

   NB : la fonction $x \to sym(x)$ est une involution: cela veut dire que si on l'applique deux fois de suite, on revient de là où on est parti. Formellement, $x \to sym(sym(x)) = Id = x \to x$. Cela veut dire que les éléments symétriques viennent toujours en paires (et rarement,

sont couplés à eux-mêmes, comme -1 pour multiplication). D'ailleurs, l'élément neutre est aussi toujours son propre symétrique pour l'opérateur duquel il est le neutre.

Ex:

– $(\mathbb{N}, +)$ n'est pas un groupe

– $(\mathbb{Z}, +)$ est un groupe abélien

– $(\mathbb{R}_+^*, \times)$, qu'on peut aussi noter $(]0, +\infty[, \times)$, est un groupe abélien. C'est aussi le cas pour $(\mathbb{R}^*, \times) = (]\infty, 0[\cup]0, +\infty[, \times)$.

— l'ensemble des symétries du carré est un groupe non-abélien, appelé $D4$. https://www.cs.umb.edu/∼eb/d4/index.html

– $(bij(\mathbb{R}^{\mathbb{R}}), \circ)$ l'ensemble des fonctions bijectives de $\mathbb{R}$ dans $\mathbb{R}$, muni de l'opérateur de composition, est un groupe non-abélien.

— le cercle des nombres complexes de module (=rayon) 1 est un groupe abélien pour la multiplication, nommé groupe unitaire, il est noté $U(1)$ et est isomorphe (pareil) à l'espace des rotations d'un cercle, appelé $SO(2)$. https://groupprops.subwiki.org/wiki/Circle_group

— la théorie des groupes est vaste et fondamentale à beaucoup des mathématiques modernes. Un exemple, la mécanique quantique: les groupes de rotations et symétries sont utilisés pour simplifier énormément le langage des possibilités de transformation dans les espaces vectoriels, notamment les espaces vectoriels complexes et les espaces vectoriels topologiques complexes, dont les objets sont par exemples les fonctions continues complexes.

4. – Anneau

   Soit $(E, \star, \perp)$ un ensemble muni de deux opérateurs binaires stables (je ne sais pas si ça a un nom, on pourrait appeler cela un "bimagma" par exemple; inventer de nouveaux concepts n'est certainement pas interdit en mathématiques, tant que leur définition est claire et rigoureuse).

   On dit que $(E, \star, \perp)$ est un **anneau** ssi il vérifie les propriétés suivantes:

   – $(E, \star)$ est un groupe abélien

   – $\perp$ est associative

– $\perp$ possède son propre élément neutre, noté e'

– $\perp$ est **distributive des deux côtés** sur $\star$, càd :

$$\forall(x,y,z) \in E^3, x \perp (y \star z) = (x \perp y) \star (x \perp z)$$

$$\forall(x,y,z) \in E^3, (y \star z) \perp x = (y \perp x) \star (z \perp x)$$

On dit que E est un **anneau commutatif** si $\perp$ est en plus commutative.

NB: en général, $\star$ correspond à l'addition et $\perp$ à la multiplication, ou alors on peut faire des rapprochements qui s'y ressemblent pas mal. Pour cette raison, quand il y a deux types de symétriques différents, on a tendance à reprendre la notation $-x$ pour $\star$ et $x^{-1} = \frac{1}{x}$ pour $\perp$ et de noter 0_E le neutre de $\star$ et 1_E le neutre de $\perp$. Vous verrez aussi d'autres auteurs qui utilisent par défaut $+$ et $\times$ plutôt que $\star$ et $\perp$, et il faut comprendre que c'est pas forcément $+$ et $\times$ dans les réels. Donc en gros, un *anneau c'est une structure avec addition, soustraction et multiplication (pas forcément commutative) mais pas division généralisée* (on ignore la division euclidienne qui existe même dans les entiers). On peut avoir des anneaux où CERTAINS inverses existent, mais pas pour tous les éléments, comme les anneaux de matrices ou de fonctions.

NB: un **pseudo-anneau** est un anneau sans le neutre multiplicatif. La nomenclature des anneaux varie beaucoup, surtout selon la nationalité des auteurs, ou leur période historique. Certains diront "anneau" pour vouloir dire "pseudo-anneau" et par contre préciseront "anneau unitaire" pour les cas où il existe un neutre multiplicatif. Donc faites attention si jamais vous avez un doute sur comment un auteur donné définit un concept spécifique.

NB: certains opérateurs ne sont distributifs que d'un côté, ou encore distributifs de manière bizarre (notamment en algèbre sesquilinéaire, dans le cadre des espaces vectoriel sur $\mathbb{C}$, il y a de la géométrie pète-crâne et magnifique là-dedans, et l'analyse de Fourier qui en dépend est l'outil fondamental du traitement des signaux à haut niveau).

NB: dans certains cas, la distributivité peut marcher dans les deux sens, comme pour $\cap$ et $\cup$ (union et intersection) où $\cap$ est distributive sur $\cup$ et $\cup$ est aussi distributive sur $\cap$. Dans les anneaux c'est en général à sens unique, c'est-à-dire $\times$ sur $+$, ou $\perp$ sur $\star$. Comprendre la distributivité

dans les deux sens vous sera essentiel en logique, surtout si vous voulez comprendre la composition et l'optimisation de circuits électroniques logiques.

NB : La définition de l'anneau peut aussi être résumée ainsi : $(E, \star)$ est un groupe abélien, $(E, \perp)$ est un monoïde, et $\perp$ est distributive sur $\star$.

Ex :

– $(\mathbb{Z}, +, \times)$ est un anneau (c'est l'exemple basique d'un anneau intègre commutatif (et d'autres classes d'anneaux); voir section suivante).

– $(\mathbb{R}[X], +, \times)$, noté simplement $\mathbb{R}[X]$, est l'anneau des polynômes à valeurs réelles.

– $(\mathcal{M}_n(R), +, \times)$ ensemble des matrices carrées de taille $n \times n$ à coefficients réels muni de l'addition et de la multiplication matricielle est un anneau non-commutatif.

5. – Anneau intègre

   On dit qu'un élément x de E est un **diviseur de 0** ssi :

$$\begin{cases} x \neq 0 \\ \exists y \in E, y \neq 0, \text{ tel que } x \perp y = 0_E \text{ ou } y \perp x = 0_E \end{cases}$$

   NB : attention $\perp$ représente la multiplication mais 0_E le neutre de l'addition notée $\star$!

   Exemple : – Soient deux fonctions f et g dans l'espace de fonctions $E = \mathbb{R} \to \mathbb{R}$, f étant nulle sur $\mathbb{R}$ - mais pas sur $\mathbb{R}_+$, et g nulle sur $\mathbb{R}_+$ mais pas sur $\mathbb{R}_-$ sont diviseurs de 0 pour l'opérateur de multiplication "point-par-point" car $f \times g = g \times f = 0_E$, ici la fonction nulle (neutre pour l'addition de fonctions).

   – $A = [1, 0; 0, 0]$ et $B = [0, 0; 0, 1]$ deux matrices de taille 2×2, sont des diviseurs de zéro, car $AB = 0_{\mathcal{M}_2(\mathbb{R})}$, la matrice nulle (neutre pour l'addition de matrices). Plus généralement, toute matrice avec un déterminant nul est un diviseur de zéro.

   NB : les diviseurs de zéros sont importants car il s'agit précisément des éléments non-inversibles pour la multiplication.

On dit que $(E, \star, \perp)$ est un **anneau intègre** ssi :

– $(E, \star, \perp)$ est un anneau

– $(E, \star, \perp)$ n'est pas l'anneau nul (ie, $(E, \star, \perp)$ possède au moins les DEUX éléments neutres, 0_E et 1_E)

– E ne possède pas de diviseur de zéro

NB : Anneau intègre commutatif se dit *integral domain* en anglais [par abus, on dit aussi *domain* tout court...], vous risquez pas de le voir si vous faites pas des maths pures, mais c'est bien à savoir qu'il faut faire attention, car *domain* est aussi utilisé pour dire "ensemble de départ d'une fonction"! C'est un des rares cas où la nomenclature française est nettement meilleure à mon goût.

NB: cette notion est utile pour créer des systèmes où l'on peut résoudre des équations dans lesquelles il faut traiter des cas en zéro, c'est-à-dire la base de la vaste majorité des équations qui interviennent dans pleeeein de branches des maths. Pourquoi ? Généralement, on peut remplacer une équation entre deux éléments $f = g$ par une formule équivalente $f - g = 0$, et ainsi se concentrer sur l'étude souvent plus simple des cas où $h = f - g$ est nul. Cette notion est aussi utile pour pouvoir définir la division rigoureusement, ce que nous voyons tout de suite.

6. – Corps

   On note souvent E^* l'ensemble E privé de ses éléments non-inversibles (sauf dans le contexte des espaces vectoriels où l'étoile est souvent réservée pour le dual). Si E est un anneau intègre, le seul élément non-inversible (par lequel on ne peut pas diviser) est le neutre pour l'addition (or $\star$), noted 0_E.

   On dit qu'un ensemble $(E, \star, \perp)$ est un **corps** ssi :

   – $(E, \star, \perp)$ est un anneau intègre

   – $\perp$ est commutative

   – $\forall x \in E^*$, x possède un symétrique pour $\perp$ noté x^{-1}, appelé inverse.

   Ex:

   – $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, munis de l'addition et la multiplication usuelles, sont des corps. La lettre choisie pour référer à un corps (généralement $\mathbb{R}$ et $\mathbb{C}$)

est $\mathbb{K}$ en français (pour *Körper*, en allemand, vu que la lettre 'c' est occupée pour le corps des nombres complexes) et $\mathbb{F}$ en anglais (pour *(algebraic) Field*). Notez qu'en anglais, il ne faut pas confondre à ne pas confondre avec "*field*" comme "champ" en physique, *magnetic field*, etc, qui sont en général des "champs vectoriels", des espaces vectoriels où on chaque vecteur (chaque point de l'espace) se trouve affixé d'un autre vecteur (une flèche pour voir le sens du mouvement à ce point-là si l'on veut).

– $(\mathbb{R}(X), +, \times)$ ensemble des fractions rationnelles (nomenclature bizarre, mais, bon, il s'agit des fractions avec des polynômes au numérateur et au dénominateur) est un corps.

– $(bij(M_n(\mathbb{R})), +, \times)$ l'ensemble des matrices carrées de taille $n \times n$ inversibles n'est pas un corps car sa multiplication n'est pas commutative, et que l'addition n'est pas stable.

– Les seuls corps au cardinal fini sont les $\mathbb{Z}/p\mathbb{Z}$ (aussi notés $\mathbb{K}_p$, ou $\mathbb{F}_p$ en anglais; ou GF_p pour "**Galois field**") où p est un nombre premier. Ils sont appelés "ensemble des classes d'équivalence sur $\mathbb{Z}$ modulo p". [Techniquement on devrait dire "modulo la relation de 'congruence modulo p' " mais ça fait lourd.] Pensez à une horloge avec un nombre premier d'heures et où il n'y a que les heures, pas de minutes. Vous avez le droit de faire vos multiplications, additions, mais vous devez rester sur l'horloge.

Exercice : Pour comprendre la division dans un tel ensemble, revenir à la définition d'éléments symétriques : définir chaque inverse et multipliez par l'inverse. Les horloges avec un nombre n d'heures où n n'est pas premier contiennent des diviseurs de zéro.

Exercice : sur votre horloge classique à 12h, si vous vous coucher à 10h du soir, et que vous dormer 9 heures, vous vous levez à 7h du matin. Donc $10 + 9 \equiv 7[12]$. Question: 12 n'est pas premier, donc $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. Mais est-il au moins un anneau intègre ? Pourquoi, ou pourquoi pas ?

– La notation "$(\mathbb{Z}/n\mathbb{Z})^*$" est utilisée pour désigner le groupe multiplicatif pour les $\mathbb{Z}/n\mathbb{Z}$ où n n'est pas premier. Cela signifie de ne garder que les éléments de l'horloge possédant un inverse. Donc parfois le symbole "puissance l'étoile" c'est pas juste enlever 0_E, comme dans $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. Il y a des contextes où on l'utilise pour désigner les éléments

inversibles d'un anneau, et construire son sous-groupe multiplicatif à partir de son monoïde multiplicatif.

NB : En gros, un corps c'est une structure sur laquelle on peut utiliser $+$, $-$, $\times$ et $/$, selon les règles habituelles (pas de division par 0).

NB : en résumé, **un corps $\mathbb{K}$ c'est une structure où $(\mathbb{K}, +)$ et $(\mathbb{K}^*, \times)$ sont des groupes abéliens et $\times$ est distributive sur $+$.**

7. – Espace vectoriel

   Rappel : par "$\mathbb{K}$", on entend en général $\mathbb{R}$, les nombres réels, ou $\mathbb{C}$, les nombres complexes. Cependant la définition s'applique aussi $\mathbb{Q}$, à des corps finis comme les $\mathbb{Z}/p\mathbb{Z}$ (sauf $\mathbb{Z}/2\mathbb{Z}$ qui est bizarre apparemment, je pense parce que dedans on a $-1 \equiv 1$), ou d'autres exemples plus complexes (corps de fractions polynomiales). Si vous avez déjà l'habitude des vecteurs à valeurs réelle (c'est peut-être le cas à ce stade!), comme $\mathbb{R}^2$, essayez de visualiser ce que ça donnerait avec des coefficients dans un corps fini, comme $(\mathbb{Z}/5\mathbb{Z})^2$ par exemple.

   Soit $\mathbb{K}$ un corps, $(E, +)$ un groupe abélien. On munit $K \times E$ d'un opérateur dans E nommé "loi externe" ou "loi scalaire" noté comme la multiplication (càd avec $\times$, un point centré "$\cdot$", ou sans notation, juste en collant les lettres). En clair, $\cdot : K \times E \to E$.

   On dit alors que $(E, +, \cdot)$, ou E tout court, est un **$\mathbb{K}$-espace vectoriel** ssi il possède les propriétés suivantes:

   – Pseudo-distributivité sur les vecteurs :

   $$\forall \lambda \in \mathbb{K}, \forall (x, y) \in E^2, \lambda(x + y) = \lambda x + \lambda y$$

   – Pseudo-distributivité sur les scalaires :

   $$\forall (\lambda, \mu) \in \mathbb{K}^2, \forall x \in E, (\lambda + \mu)x = \lambda x + \mu x$$

   – Pseudo-associativité multiplicative de la loi scalaire :

   $$\forall (\lambda, \mu) \in \mathbb{K}^2, \forall x \in E, (\lambda\mu)x = \lambda(\mu x)$$

   – Compatibilité du neutre multiplicatif du corps avec la loi scalaire :

   $$\forall x \in E, 1_{\mathbb{K}} x = x$$

NB: on appelle les éléments de $\mathbb{K}$ les **scalaires**, qu'on note avec des lettres grecques, et les éléments de E les **vecteurs**, qu'on note avec des lettres latines (par convention).

NB: la "loi scalaire" n'a pas vraiment de nom sympa en français, et même l'usage du terme "loi scalaire" n'est pas très répandu. En anglais, j'ai déjà vu *scaling product*, à ne pas confondre avec le "produit scalaire (euclidien)", qui lui est le *dot product*. Le "produit vectoriel" (un outil assez pathologique n'existant que dans $\mathbb{R}^3$ mais dont l'usage est répandu à cause du choix du langage mathématique créé par Gibbs plutôt que celui créé par Clifford au début du XXe siècle) se dit *cross product*. Le produit vectoriel est une variation d'un produit plus important, et mieux construit, appelé "produit extérieur", qui intervient dans le domaine de l'algèbre tensorielle (étude des espaces tensoriels; l'étape qui suit l'algèbre linéaire, elle-même l'étude des espaces vectoriels).

NB: si E est un $\mathbb{K}$-ev, on note en général 0_E son neutre additif, le fameux "vecteur nul". Vous avez des détails supplémentaires dans la section sur les moboïdes plus haut.

NB: la loi scalaire est commutative, mais en pratique, on note les scalaires à gauche (ex : $\frac{1}{3}v$)

NB: **IL N'Y A PAS DE MULTIPLICATION ENTRE VECTEURS DANS UN ESPACE VECTORIEL BASIQUE. Le sujet de la multiplication entre vecteurs est traité juste après avec la notion de "$\mathbb{K}$-algèbre" en tant que structure algébrique.**

Exemples :

– $\mathbb{K}[X]$, ensemble des polynômes à valeurs dans $\mathbb{K}$ est un $\mathbb{K}$-espace vectoriel (c'est aussi une algèbre, cf. plus bas).

– $\mathbb{K}^n$ est un $\mathbb{K}$-ev (c'est l'exemple fondamental en dimension finie, car si on se limite à la structure d'espace vectoriel, c'est-à-dire sans la multiplication d'une $\mathbb{K}$-algèbre, tout espace vectoriel de dimension n est isomorphe à $\mathbb{K}^n$, donc qu'on peut par exemple se dire "Ah, mais si on se limite à l'addition des matrices, sans la multiplication des matrices, $\mathbb{R}^{m\times n}$ c'est la même chose que $\mathcal{M}_{m,n}(\mathbb{R})$!").

– $(F^E, +) = ((E \to F), +)$, un groupe abélien additif de fonctions peut toujours être transformé en $\mathbb{K}$-espace vectoriel (d'où l'idée que toute

fonction est un vecteur dans un contexte donné; notez que pour une raison différente, tout vecteur est aussi une fonction). Certains de ces espaces seront plus intéressants que d'autres.

Exercice : si l'on considère le groupe abélien $(E, \times)$ des dimensions physiques (E est généré par multiplications ou divisions successives par éléments de son sous-ensemble générateur, sa "base", $B = \{m, kg, s, mol, cand, ^\circ K, A\}$ et l'opération d'inversion, par exemple $m^3 * kg * s^{-2}$ est un élément de E). E est-il un espace vectoriel sur R, sur C ? Pourquoi, ou pourquoi pas ?

Exercice : Visualisez $f = (x \to x^2)$ et $g = (x \to 3x)$, par exemple sur Geogebra, ou mieux, dans votre tête. Que donnerait la fonction (aussi bien visuellement qu'en tant que formule algébrique): $h_1 = f + g$? et $h_2 = 4f$? et $h_3 = 3h_1$? et $h_4 = 3f + 3g$? Quelle conclusion en tirez-vous ?

Les fonctions qui conservent la structure d'espace vectoriel (les "morphismes" d'espaces vectoriels, cf théorie des catégories plus bas) s'appellent **applications linéaires** (ou fonctions linéaires).

Soient E et F deux $\mathbb{K}$-ev. On dit que $f : E \in F$ est **linéaire** ssi :

– $\forall (x, y) \in E^2, f(x +_E y) = f(x) +_F f(y)$

– $\forall \lambda \in \mathbb{K}, \forall x \in E, f(\lambda x) = \lambda f(x)$

Cela signifie que les applications linéaires sont commutatives (au sens des diagrammes de la théorie des catégories) avec l'addition et la loi scalaire. Cela signifie qu'on peut soit faire l'addition dans le domain d'abord, puis appliquer la fonction au résultat, soit appliquer la fonction aux opérandes, et additionner dans le codomaine: on arrivera au même résultat.

NB: On note $\mathcal{L}(E, F)$ ou $Hom_{Vec_\mathbb{K}}(E, F)$ l'ensemble des applications linéaire de E dans F.

NB : $\mathcal{L}(E, F)$, en tant qu'ensemble de morphismes d'espaces vectoriels, est un espace vectoriel. Exercice : démontrer que $\mathcal{L}(E, F)$ est un $\mathbb{K}$-ev.

NB : en théorie des catégories, on le note $Hom_{Vec_\mathbb{K}}(E, F)$ ou juste $Hom(E, F)$ s'il n'y a pas d'ambigüité sur le fait que E et F sont des ev sur le même corps.

NB : on note $\mathcal{L}(E)$ plutôt que $\mathcal{L}(E, E)$ l'ensemble des endomorphismes sur E.

NB : attention, il faut se méfier, la notation pour $\mathcal{L}(E, F)$ varie selon les sources. On note souvent $L(E, F)$ l'ensemble des applications linéaires continues, qui sont elles les morphismes des "espaces vectoriels topologiques". Mais parfois vous verrez la notation inverse: L pour les applications linéaires et $\mathcal{L}$ pour les applications linéaires continues, donc méfiez-vous...

NB : on note $(\mathcal{GL}(E), \circ)$ ou plutôt $\mathcal{GL}(E)$ l'ensemble des automorphismes (morphismes bijectifs) sur E, munis de l'opérateur de composition, appelé "groupe linéaire". Exercice : démontrer que c'est un groupe. Pour ceux qui ont un peu exploré la représentation géométrique des espaces vectoriels : ce groupe linéaire correspond à toutes les matrices inversibles, c'est-à-dire tous les changements de base valides de notre espace vectoriel.

8. – Algèbre

En gros, une algèbre (ou $\mathbb{K}$-algèbre, ou "algèbre sur un corps $\mathbb{K}$", à ne pas confondre avec la branche des mathématiques appelée "algèbre"), c'est un *espace vectoriel auquel on rajoute une forme de multiplication entre les vecteurs*. Cette multiplication est un troisième opérateur binaire, noté aussi comme la multiplication (ou comme la composition de fonction), appelé en général "troisième loi", parfois "multiplication vectorielle". Ici, j'ai choisi de reprendre l'opérateur $\perp$ qu'on avait pour la multiplication sur les anneaux. On l'utilise ici comme une loi de composition interne (c'est-à-dire que $\perp: E \times E \to E$ est une multiplication sur les vecteurs, et est en plus une multiplication stable, qui rend un vecteur; je précise car le produit scalaire euclidien renvoie un scalaire, élément de $\mathbb{K}$, en output).

Formellement, un ensemble $(E, +, \cdot, \perp)$ est appelé une **$\mathbb{K}$-algèbre** ssi :

– $(E, +, \cdot)$ est un espace vectoriel sur $\mathbb{K}$

– $\perp: E^2 \to E$

– $\perp$ est bilinéaire (linéaire pour chaque argument ; comparez avec la distributivité) :

– $\forall (x, y, z) \in E^3, \perp (x + y, z) = \perp (x, z) + \perp (y, z)$

– $\forall(x,y,z) \in E^3, \perp (x, y+z) = \perp (x,y) + \perp (x,z)$

– $\forall\lambda \in \mathbb{K}, \forall(x,y) \in E^2, f(\lambda x, y) = \lambda f(x,y)$

– $\forall\lambda \in \mathbb{K}, \forall(x,y) \in E^2, f(x, \lambda y) = \lambda f(x,y)$

=> si la troisième loi possède un neutre, l'algèbre est dite unitaire (ou unifère)

=> si la troisième loi est associative, l'algèbre est dite associative

=> si la troisième loi est commutative, l'algèbre est dite commutative

=> je ne suis pas sûr de comment qualifier les algèbres avec éléments symétriques ("algèbre inversible" n'a pas l'air d'exister, mais je l'utiliserai), mais je sais qu'il en existe (par exemple, les algèbres de fractions rationnelles (polynômiales), qui fonctionnent comme des corps, sont ainsi inversibles).

NB : les algèbres ressemblent beaucoup aux anneaux, mais sont plus riches. Elles sont comme un anneau de vecteurs (éventuellement sans associativité et neutre pour la multiplication) avec un corps de scalaires si l'on veut. Les polynômes en sont en très bon exemple. On peut y faire de la division euclidienne et de la multiplication scalaire. Nous en parlons dans la section suivante.

NB : Souvent, vous verrez "algèbre" pour vouloir dire "algèbre associative unitaire", car une algèbre associative unitaire est un anneau, et donc est un exemple typique d'algèbre qu'on va beaucoup manipuler – attention à cet abus de langage.

NB : Les algèbres de Lie sont un exemple d'algèbres non-associatives (leur troisième loi, appelée commutateur, respecte à la place une propriété appelée l'identité de Jacobi).

NB : Si une algèbre est associative, unitaire, commutative, ne possède pas de diviseurs de zéro (diviseurs du neutre pour l'addition vectorielle, le vecteur nul, pour la multiplication vectorielle propre à l'algèbre), et possède un inverse pour tous les éléments sauf le vecteur nul, alors elle fonctionne en quelque sorte comme un "corps vectoriel sur un corps scalaire". C'est le cas des espaces de fractions rationnelles (polynomiales).

NB : Pour A et B deux $\mathbb{K}$-algèbres, les morphismes d'algèbre sont les applications $f \in Hom(A,B)$. Elles vérifient la linéarité ($\forall(x,y) \in$

$E^2, f(x +_A y) = f(x) +_B f(y)$ et $\forall \lambda \in \mathbb{K}, \forall x \in E, f(\lambda x) = \lambda f(x)$) et la préservation de la troisième loi ($\forall (x, y) \in E^2, f(x \perp_A y) = f(x) \perp_B f(y)$). Pour les morphismes d'algèbres unitaires, on rajoute la condition $f(1_A) = 1_B$, où 1_A (resp. 1_B) est le neutre pour la troisième loi de A (resp. B), même si certains considèrent cela redondant vu que c'est impliqué par la préservation de la troisième loi, tant qu'un neutre multiplicatif non-nul existe dans B (c'est-à-dire dès que $B \neq (\{0_E\}, +, \cdot, \perp)$, l'anneau/l'algèbre nul/le). On rajoute souvent des conditions sur les morphismes quand la structure devient plus riche et complexe : renseignez-vous toujours sur le type de morphisme pour votre structure !

NB : On peut considérer des algèbres dans lesquelles on a un choix de plusieurs multiplications possibles. Les algèbres géométriques de Hestenes / algèbres de Clifford possèdent un produit fondamental, appelé produit géométrique, et ce produit est la composition de plusieurs sous-produits qui chacun encodent des informations différentes. C'est un exemple de ce qu'on pourrait éventuellement qualifier une "algèbre polymultiplicative". Un autre exemple serait des espaces de fonctions munis à la fois d'un produit de multiplication "point-par-point", et d'une "convolution".

Exemples :

– $\mathbb{R}$ peut-être considéré comme une algèbre unitaire, associative, commutative, avec éléments symétriques (inversibles), en choisissant la multiplication usuelle à la fois comme la loi scalaire et comme la troisième loi.

– $\mathbb{C}$ est une $\mathbb{R}$-algèbre unitaire, associative, commutative, inversible, avec pour troisième loi la multiplication complexe ($\times(z_1, z_2) = z_1 z_2 = (x_1 + iy_1) \times (x_2 + iy_2) = (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1)$). Sa structure restreinte à l'espace vectoriel (en ignorant la multiplication) est isomorphe à $\mathbb{R}^2$.

– $\mathbb{R}^n$ muni du produit de Schur (*point-wise product*) est une algèbre associative, commutative, unitaire (le vecteur $[1, 1, 1, ..., 1, 1]$ de taille n), non-inversible (cet espace a des diviseurs de zéro: trouvez-en une paire!).

– $\mathbb{R}^3$ muni du produit vectoriel (*cross product*) est une algèbre anticommutative (ie, $\forall (a, b) \in (\mathbb{R}^3)^2, a \times b = -b \times a$), mais pas unitaire,

ni associative. Le produit vectoriel ne peut être défini que comme un opérateur $(n-1)$-aire dans un espace de dimension n. Le seul cas d'opérateur binaire est donc le produit vectoriel de $\mathbb{R}^3$.

– $\mathbb{K}[X]$ muni de la multiplication $[P \times Q = P(x) \times Q(x)$ pour tous polynômes P et $Q]$ est une $\mathbb{R}$-algèbre associative, unitaire, commutative.

– $\mathcal{M}_n(\mathbb{R})$ munie de la multiplication matricielle est une $\mathbb{R}$-algèbre unitaire, associative.

– Par isomorphisme d'algèbres $\mathcal{M}_n(\mathbb{R}) \cong \mathcal{L}(\mathbb{R}^n)$. Cela signifie aussi que $\mathcal{L}(\mathbb{R}^n)$ (muni en troisième loi de la composition de fonctions "rond $\circ$" sur les applications linéaires) est aussi une $\mathbb{R}$-algèbre unitaire, associative (donc un anneau non-commutatif de vecteurs sur un corps scalaire).

9. — Sous-structures

Une dernière définition utile avant de pouvoir passer aux anneaux/algèbres (et donc aux polynômes). Elle sera néanmoins sûrement plus claire en ayant aussi lu la partie suivante.

On dit que F est une **sous-structure** de E si F et E appartiennent à la même catégorie $\mathcal{C}$ (cela revient à dire qu'il s'agit du même type de structure algébrique) et que F est inclus dans E. On peut revenir à démontrer la stabilité de la sous-structure pour les différents opérateurs pour justifier que E et F sont dans la même catégorie.

Par exemple :

Soit $(G, \star)$ un groupe, on dit que H est un sous-groupe de G ssi :

– $H \subset G$, H est inclus dans G

– $\forall x \in H, sym_G(x) \in H$ (ie, H est un sous-ensemble stable pour l'automorphisme sym_G d'inversion)

– $\forall (x, y) \in H^2, x \star y \in H$ (ie, H est un sous-ensemble stable de G pour $\star$)

Autre exemple : F est un sous-espace vectoriel (sev) de E ssi F est un espace vectoriel inclus dans E et F est stable pour $+_E$ et la loi scalaire, càd ssi :

– $F \subset E$, F est inclus dans E

– $0_E \in F$

– $\forall (x, y) \in F^2, x +_E y \in F$ (stabilité pour l'addition vectorielle)

– $\forall \mu \in \mathbb{K}, \forall x \in F, \mu x \in F$ (stabiité pour la multiplication scalaire)

NB : Si les trois propriétés précédentes sont vérifiées, F est un $\mathbb{K}$-ev, indépendant et propre. Ses opérateurs $(+_F, \cdot_F)$ sont juste la restriction de ceux de E aux éléments de F. C'est souvent utile de montrer que F est un sev d'un autre $\mathbb{K}$-ev connu pour montrer que F est un $\mathbb{K}$-ev tout court (qu'il a les bonnes propriétés, pour ensuite pouvoir s'en servir).

NB : Un sous-groupe est un de même un groupe en soi (ie, il respecte les mêmes propriétés que tous les autres groupes). De fait, c'est le cas pour toute sous-structure. Ceci est un composant clef de la théorie des catégories.

NB : Un groupe inclus dans un autre est forcément un sous-groupe. Ces notions s'étendent aux autres structures; ex : $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, et $\mathbb{R}$ est un sous-corps de $\mathbb{C}$. Et montrer que $\mathbb{Q}$ est un sous-corps peut se faire en sachant que $\mathbb{R}$ est un corps et en montrant que $\mathbb{Q}$ est stable pour $+$, $\times$, l'opérateur de symétrie additive et celui de symétrie multiplicative (sauf 0), etc.

NB : On parle de sous-structure "propre" quand F est une sous-structure "strictement incluse" dans E, c'est-à-dire si F est inclus dans E et F est différent de E. Rappelez-vous que l'inclusion est une relation d'ordre !

NB: L'inverse d'une sous-structure est une extension de structure. Par exemple, $\mathbb{C}$ est une extension de corps de $\mathbb{R}$. Un exemple plus intéressant est de prendre $\mathbb{Q}$, et les éléments $\sqrt{2}$ et $\sqrt{3}$ de $\mathbb{R}$, et de faire toutes les combinaisons d'opérations possibles afin d'en faire de nouveau un ensemble stable. Ceci nous donne $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid (a, b, c, d) \in \mathbb{Q}^4\}$, qui est une extension de corps propre de $\mathbb{Q}$ et un sous-corps propre de $\mathbb{R}$. Ce genre d'espace intervient dans la théorie de Galois.

Bon. On a déjà fait du bon travail à ce stade. On a ignoré quelques structures algébriques classiques mais moins fréquentes (semigroupes: un magma associatif, sans l'élément neutre qui en ferait un monoïde), ou avec un brin de complexité qui leur est propre (modules; qui est ce qui se passerait si

on prenait un anneau A plutôt qu'un corps $\mathbb{K}$ comme ensemble des scalaires, et qu'on essayait de faire un espace vectoriel avec: c'est surtout la non-commutativité potentielle de l'anneau qui complique les choses, car multiplier par un scalaire à droite ou à gauche ne donne pas forcément le même résultat). Libre à vous de vous renseigner plus à leur sujet !

6 Théorie des catégories

6.1 Introduction

L'intérêt principal de la théorie des catégories c'est que c'est une excellente théorie unificatrice de l'algèbre abstrait. Elle offre un framework général pour parler de tous types de structures algébriques avec un langage commun à toutes, et explique clairement leur interrelations. Elle permet de manipuler les structures algébriques en elles-mêmes, d'ignorer complètement les éléments d'un ensemble mais plutôt de regarder comment sa structure dicte le fonctionnement des éléments. En gros, on appelle "catégorie" la totalité de toutes les structures d'un type donné. Rappelez-vous qu'on ne peut pas avoir "d'ensemble de tous les ensembles", c'est ce problème que permet de régler la notion de catégorie : elle est assez "grande" pour pouvoir construire des "catégories de tous les ensembles d'un certain type" mais assez "petite" pour ne pas tomber dans les contradictions des ensembles qui se contiennent eux-mêmes. Ainsi, la théorie des catégories nous permet de faire des opérations entre des collections d'ensembles massives (les catégories) qui ont quand même rigoureusement du sens.

Donc en gros, chaque élément d'une catégorie est une structure algébrique, ou peut être interprété comme une structure même si ce n'est pas la conception "habituelle" du problème (ex: chaque *proposition logique* peut être comprise comme *l'espace des modèles logiques dans lesquels cette proposition peut être démontrée comme vraie*). On peut aller plus loin (plus général ou plus précis) avec les catégories – par exemple décider d'analyser une seule structure comme une catégorie – mais en général les catégories les plus intéressantes et qui reviennent fréquemment sont ces *catégories de structures algébriques* (aussi appelées "**catégories concrètes**" ; un théorème dit que toute catégorie est isomorphe à au moins une catégorie concrète). Cela implique que la théorie des catégories va plus loin que l'algèbre abstraite dans ce qu'elle peut exprimer; mais elle la contient quand même dans son entièreté.

À son coeur, la théorie des catégories est un essai grandiose pour comprendre la notion de "fonction" de la manière la plus pure, la plus abstraite, et la plus générale possible. Cela peut sembler n'être pas grand chose, mais étant donné l'ubiquité du concept de fonction dans les mathématiques, les sciences, la cognition... cela fait de la théorie des catégories l'un des plus profonds accomplissements du savoir humain.

Des exemples de catégories concrètes:

– Set, catégorie des ensembles munie des fonctions ensemblistes comme morphismes

– Rel, catégorie des ensembles munie des relations entre ensembles comme morphismes

– Fld, catégorie des corps,

– Mon, catégorie des monoïdes,

– Grp, catégorie des groupes,

– Ab, catégorie des groupes abéliens,

– Rng, catégorie des pseudo-anneaux (anneau sans élément neutre pour la multiplication),

– Ring, catégorie des anneaux,

– $Vect_{\mathbb{K}}$, ou K-**Vect**, catégorie des espaces vectoriels sur le corps $\mathbb{K}$

– $Alg_{\mathbb{K}}$, ou K-**Alg**, catégorie des algèbres sur le corps $\mathbb{K}$.

– Top, catégorie des espaces vectoriels topologiques

– Mod_A, ou A-**Mod**, catégorie des modules à droite sur un anneau ou une algèbre A

– Beaucoup d'autres.

Formellement, on dit que $\mathcal{C}$ est une catégorie si $\mathcal{C}$ consiste des propriétés suivantes:

– $\mathcal{C}$ possède une collection d'objets A, B, C... notée $|\mathcal{C}|$

– Pour toute paire (A, B) d'objets de $|C|$ il existe un objet de $\mathcal{C}$ noté $A \to B$, contenant les morphismes (les flèches, les transformations, notés f, g, etc.) de A vers B. Si $f : A \to B$, alors on note $dom(f) = A$ l'objet de départ de f, et $cod(f) = B$ son objet d'arrivée.

– Pour tout couple de flèches (f, g) tel que $f : A \to B$ et $g : B \to C$, il existe un morphisme $h : A \to C$ tel que $h = g \circ f$, qui consiste à appliquer d'abord f, puis g.

– La loi de composition ainsi générée est associative, c'est-à-dire pour tout triplet de morphismes (f, g, h) avec des domaines et codomaines compatibles ($cod(f) = dom(g)$ et $cod(g) = dom(h)$, on a $h \circ (g \circ f) = (h \circ g) \circ f$.

– Pour tout objet A de $|\mathcal{C}|$, il existe un morphisme identité $1_A := A \to A$ tel que pour tout f tel que $cod(f) = A$, on a $1_A \circ f = f$ et pour tout g tel que $dom(g) = A$, on a $g \circ 1_A = g$.

Ces catégories sont souvent qualifiées de "catégories monoïdales" car leurs flèches se comportent plus ou moins comme les éléments d'un monoïde.

Une catégorie $\mathcal{C}$ peut donc être décrite comme une collection de points

(appelés objets, qui sont en général les structures) et de flèches (appelés [homo]morphismes, qui correspondent à des transformations des objets qui maintiennent la structure/les propriétés, c'est-à-dire des transformations stables dans la catégorie). Juste des objets et des flèches. Notez que la racine grecque "homo" veut dire "similaire" et "morphè" veut dire "forme".

NB: la collection d'objets et les collections de morphismes ne sont pas forcément "assez petites" pour être des ensembles. Une catégorie dont toutes les collections sont des ensembles "classiques" est dite "petite". Les catégories dans lesquelles la collection d'objet est plus "grande" (ou auto-référente) qu'un ensemble ne peut l'être, mais dans laquelle tous les homset (ses collections de morphismes, les "$Hom(A, B) = (A \to B)$") sont assez petits pour être des ensembles classiques, est dite "localement petite". Pour la plupart des cas traités ici, on est dans un contexte de catégories localement petites.

En quelques sortes, la théorie des catégories c'est l'étude des structures algébriques et des fonctions qui maintiennent la structure. "Fonction" est ici utilisé au sens large, il ne s'agit pas forcément de "fonctions ensemblistes" même si beaucoup d'entre elles le sont quand même, à cause de l'importance des catégories concrètes – celles dont les objets sont des structures algébriques.

Cette "fonction abstraite", généralisée, en théorie des catégorie (le "morphisme") est définie comme "un lien entre les objets d'une catégorie, et ce lien vérifie trois propriétés : stabilité, associativité et existence d'un morphisme identité pour l'opération de composition pour chaque objet".

La stabilité par composition c'est juste l'idée que si f et g sont dans une même catégorie (genre dans la catégorie des fonctions injectives) et que $cod(f) = dom(g)$, alors $g \circ f$ existe et est du même type que f et g (donc injective).

L'associativité de la composition, vous connaissez :

$$(h \circ g) \circ f = h \circ (g \circ f)$$

L'identité, c'est que pour tout objet A de notre catégorie, on a une fonction identité de A dans A qui ne change rien et est du même type que les autres morphismes (ex : injective). Formellement:

$$\forall A, B \in |\mathcal{C}|, \exists 1_A \in (A \to A), \exists 1_B \in (B \to B), \forall f \ : A \to B, f \circ 1_A = f = 1_B \circ f$$

Si un de ces points coince, on n'est pas dans une catégorie, ça ne fonctionne pas. Par contre, tout groupe de "fonctions" qui vérifie ceci en étant

bien défini pour une collection d'objets donnée peut être considéré comme un choix possible de "morphismes" pour cette collection afin d'en faire une catégorie donnée. Par exemple, les fonctions injectives, les fonctions ensemblistes et les relations entre ensembles sont toutes des choix de morphismes valides, et chacun de ces choix donne naissance à une catégorie différente sur les ensembles.

Exercice bonus : explorez ces concepts en essayant de vous donner une idée de comment la catégorie Set des ensembles muni des fonctions ensemblistes diffère de la catégorie Rel des ensembles muni des relations entre ensembles.

Tout ça étant bien sûr très abstrait, expliquons en prenant l'exemple de Grp.

Soient $(G, \star)$ et $(H, \perp)$ deux groupes. On appelle un "morphisme de groupes" une fonction $f : G \to H$ telle que :

$$\forall (x, y) \in G^2, f(x \star y) = f(x) \perp f(y)$$

Intuitivement, un morphisme de groupe transforme tout simplement un opérateur en un autre en gardant le même lien entre les éléments de départ. Ou plus précisément, en faisant en sorte que l'on puisse choisir d'abord opérateur puis fonction ($\star$ puis f) ou d'abord fonction puis opérateur (f puis $\perp$) et on tombera quand même sur le même résultat.

Vous connaissez sûrement deux morphismes de groupes, déjà : exp et ln. ln est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$ et inversement pour exp, car :

$$\forall (x, y) \in \mathbb{R}_+^*, \ln(a \times b) = \ln(a) + \ln(b)$$

$$\forall (x, y) \in \mathbb{R}, \exp(a + b) = \exp(a) \times \exp(b)$$

Un morphisme de groupe transforme un opérateur en un autre, tout simplement.

Un des trucs les plus fous de la théorie des catégories c'est le fait que l'ensemble des morphismes entre deux structures d'une catégorie $\mathcal{C}$ est aussi en général un objet de $\mathcal{C}$. Dans notre exemple, l'ensemble des morphismes de groupes de G à H, noté $Hom(G, H)$ (pour **hom**omorphisme qui veut dire morphisme), est lui-même un groupe.

Un autre exemple, $\mathcal{L}(E, F)$, ensemble des applications linéaires de E dans F deux $\mathbb{K}$-espaces vectoriels (les applications linéaires sont les "morphismes

d'espaces vectoriels") : $\mathcal{L}(E, F)$ est lui-même un espace vectoriel sur le même corps $\mathbb{K}$.

Le diagramme commutatif est un outil fondamental en théorie des catégories. Il est "commutatif", parce qu'en partant de A, on peut décider de partir à vers B par la fonction f puis vers D par h, ou alors d'aller vers C par la fonction g, puis de finir en D par k, et on aura nécessairement le même résultat en D une fois le point de départ en A fixé. En clair, le diagramme commute ssi $h \circ f = k \circ g$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ C & \xrightarrow{k} & D \end{array}$$

Ici, en notant à gauche les lettres du diagramme et à droite les éléments de notre exemple sur les morphismes de groupes : on note $A := G^2, f := \star, B := G, h := f, D := H, g := f, C := H^2, k :=\perp$.

$$\begin{array}{ccc} G \times G & \xrightarrow{\star} & G \\ \downarrow{\scriptstyle (f,f)} & & \downarrow{\scriptstyle f} \\ H \times H & \xrightarrow{\perp} & H \end{array}$$

L'idée de "conservation des structures" renvoie fondamentalement à la commutativité des diagrammes définissant les morphismes dans une catégorie donnée. La commutativité de diagrammes catégoriques, c'est ce fait qu'on puisse choisir par quelles flèches on passe, et qu'on peut rester sûr d'arriver au même résultat (la commutativité d'un diagramme donné se démontre). Voici par exemple la définition des applications linéaires dans un espace vectoriel, avec le langage de la théorie des catégories (les diagrammes commutatifs). Les morphismes dans $Vec_{\mathbb{K}}$ (représentés par l'exemple des morphismes de $Hom(E, F)$, où E et F sont des $\mathbb{K}$-ev quelconques) sont définis comme faisant commuter les diagrammes suivants :

$$\begin{array}{ccc} E \times E & \xrightarrow{(f,f)} & F \times F \\ \downarrow{\scriptstyle +_E} & & \downarrow{\scriptstyle +_F} \\ E & \xrightarrow{f} & F \end{array}$$

$$\begin{array}{ccc} K \times E & \xrightarrow{(id_{\mathbb{K}}, f)} & K \times F \\ \downarrow{\scriptstyle *_E} & & \downarrow{\scriptstyle *_F} \\ E & \xrightarrow{\quad f \quad} & F \end{array}$$

où + est l'addition vectorielle et $*$ la loi scalaire dans E et F, respesctivement, et $id_{\mathbb{K}}$ la fonction $id_{\mathbb{K}} = (x \to x)$ dans $Hom(\mathbb{K}, \mathbb{K})$.

Cette conservation des structures peut être très utile, par exemple, si l'on sait que $(G, \star)$ est un groupe et que $\forall (x, y) \in G^2, f(x \star y) = f(x) \perp f(y)$ est vraie, et que $f(G) = H$, alors on peut déduire que $(H, \perp)$ est forcément un groupe, car f est un morphisme de groupe appliqué à un groupe G, donc appliquer f à G maintient la structure de groupe, donc $f(G) = H$ est un groupe (et son neutre est $e_H = f(e_G)$, où e_G est le neutre de G).

Un contrexemple : E un $\mathbb{K}$-espace vectoriel et $f = (x \to x^2)$. Comme $f(E)$ n'est plus un espace vectoriel (on perd les bonnes propriétés sur les éléments d'un $\mathbb{K}$-ev / on perd la commutativité des diagrammes), $x \to x^2$ n'est pas un morphisme d'espaces vectoriels.

Trois notions importantes sur les morphismes. Soient E et F deux structures; deux objets d'une même catégorie $\mathcal{C}$:

– un morphisme de E dans E s'appelle un **endomorphisme** ("endo" = interne)

– un morphisme de E dans F bijectif s'appelle un **isomorphisme** ("iso" = identique, pareil)

– un morphisme de E dans E bijectif s'appelle un **automorphisme** ("auto" = soi-même)

– s'il existe un isomorphisme entre E et F, on dit que E et F sont isomorphes et on note $E \cong F$

NB : *LA NOTION D'ISOMORPHISME EST UNE DES PLUS IMPORTANTES DES MATHEMATIQUES CONTEMPORAINES.* Avec celle-ci, et notamment la notion "d'isomorphisme naturel", qui est en gros une bijection structurelle sans même passer par les éléments, on peut remarquer deux structures qui fonctionnent de la même manière, et démontrer qu'elles fonctionnent de la même manière au sein d'une catégorie $\mathcal{C}$ donnée. L'isomorphisme est l'outil pour démontrer la synonymie entre les structures – l'outil pour démontrer que même si on a utilisé un langage différent, on est en train de parler du même objet mathématique. Cela permet par exemple au mathématicien de voir avec certitude "AAAH, mais en fait, mes applications linéaires finies

et mes matrices c'est LA MÊME CHOSE !!!"; permettant de réduire la complexité d'un objet d'étude complexe en l'exprimant sous la forme équivalence d'un objet isomorphe et plus intuitif.

Par ailleurs, Cat, la catégorie des catégories, est elle-même une catégorie. On appelle ses morphismes les "**foncteurs**". Ceux-ci jouent un rôle incroyable en mathématiques. Par exemple dans les démonstrations : ils permettent de passer d'une catégorie à une autre, de "transporter" des démonstrations d'un domaine où elles sont évidentes à un domaine où elles sont galères. Ou encore, de créer des structures complexes à partir de structures simples (free functor, foncteur libre) et de s'en servir comme bloc de marbre pour sculpter des structures plus précises et utiles de manière abstraite, "par le haut" (construction de l'algèbre tensorielle à partir des élements du produit cartésien de deux espaces vectoriels en utilisant la technique du quotient algébrique pour y injecter les propriétés souhaitées, créant ainsi l'algèbre extérieur et l'algèbre symétrique). Ou l'inverse, de revenir à une structure plus simple à partir d'une structure complexe (forgetful functor, foncteur "oublieur", celui par lequel on obtient $|U|$, l'ensemble des vecteurs d'un espace vectoriel U, pris isolés et sans rapport les uns aux autres, comme un ensemble basique sans propriété ni opérateur; un objet de Set).

6.2 Algèbre abstraite avec le langage de la théorie des catégories

https://tex.stackexchange.com/questions/115783/how-to-draw-commutative-diagrams#115835 https://tikzcd.yichuanshen.de/

[TODO: - present all relevant previous formulae as commutative diagrams: associativity, commutativity, identity, composition, inversion, distributivity, linearity, bilinearity... - présenter rapidement les catégories correspondantes à toutes les structures algébriques vues plus haut (notamment leur morphismes, associateur, commutateur, multiplicateur, identité, etc)]

6.3 Eléments de théorie des catégories "pure"

[TODO: epis, monos, functors, monads, diagram chasing, example categories; some typed lambda calculus ? monoidal, symmetric, etc categories. Forgetful functor, free functor]

[For the curious that want more category theory right now, read Emily Riehl's *Category Theory in Context*.]