Introduction aux structures algébriques, aux polynômes et aux séries

Tristan Duquesne *

Avril 2019

Prérequis: Juste quelques vagues souvenirs du lycée (sur lesquels on reviendra un peu) suffiront pour vous épauler (notamment polynômes de degré 2, suites numériques, nombres complexes, dérivation, intégration).

Objectif: Présenter une vision assez générale du rôle de ce qu'on appelle les "anneaux" et "algèbres" en 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.

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. (Ceux qui sont passés par Monier reconnaîtront aussi ce que je lui dois, même si c'est la théorie des catégories qui m'a permis d'explorer le reste.)

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

*pour 42 AI

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 les nouveaux concepts, et de relire.*

REVENEZ TOUJOURS A LA DEFINITION: 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 !

Ce format court semblait alors plus efficace, sans pour autant sacrifier les vrais clefs de compréhension, qui tiennent plus de l'intuition liée au formalisme, que l'un ou l'autre seuls, ou les détails techniques du travail de mathématicien: 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

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. "Al-jabr", c'est la "méthode", "ce qu'on a le droit de faire 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 naturels avec l'addition et la multiplication mais pas de soustraction" (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), on peut aussi construire une forme de division euclidienne ? Genre $4x^4 + 7x^3 - 4x^2 + 3x + 12$ 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 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 $B(x)$.

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
$A(x) = B(x) \times Q(x) + R(x)$	Vérifiez vous-mêmes.	$a = b \times q + r$	$51 = 10 \times 5 + 1$

Pas besoin de maîtriser parfaitement pour l'instant, la suite du texte vous permettra de tout relier 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 abstraite 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.

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

NB: Vous pouvez sauter cette section si vous vous sentez à l'aise.

2.1 Un petit mot pour se figurer les ensembles

Désolé de vous faire faux-bond dès le départ, mais malheureusement, un ensemble, c'est un peu indéfinissable de manière formelle. Ce qui pose pas mal 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 :

– 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.

– 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 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 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 intorductions, 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). 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 de gauche de la barre "|" décrit la forme des éléments de l'ensemble ("forme", comme "formule" ou "formellement", càd la "façon d'écrire proprement et rigoureusement"), 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".

Il y a plein d'autres choses à dire sur les ensembles, notamment sur les diagrammes de Venn et la logique, mais on en restera là. Juste rappelez vous que: - $A \cap B$, appelé **intersection** de A et B, est l'ensemble des éléments communs à A et B (votre '&&' en langage C pour sa version logique). - $A \cup B$, appelé **union** de A et B, est l'ensemble des éléments soit dans A, soit dans B, sans jamais garder les doublons s'il y en a (votre "||" en langage C pour sa version logique).

Comme ensembles classiques et/ou auxquels vous aurez droit dans ce texte, 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, $\mathbb{Q} = \{\frac{a}{b} | a \in \mathbb{Z} \text{et} b \in \mathbb{N}^*\}$
- $\mathbb{R}$, ensemble des nombres réels, ensemble des limites de suites de rationnels
- $\mathbb{C}$, ensemble des nombres complexes
- $\mathbb{R}^n$, 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 fractions (fonctions) rationnelles (polynômiales) à une indéterminée sur $\mathbb{R}$
- $\mathbb{C}(X)$, espace des fractions (fonctions) rationnelles (polynômiales) 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 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.

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 $\aleph_0$, 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). 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"; mais a des ramifications très intéressantes sur beaucoup de distinctions importantes entre le discret et le continu.

2.2 Un petit mot sur la lecture du langage mathématique

Comme symboles et concepts fondamentaux du langage des ensembles (ou plutôt du langage mathématique en général):

– "$\in$" se lit "appartient à" et signifie que l'élément représenté par la lettre/valeur à gauche est dans la patate représentée par la lettre à droite (ex : $a \in A$), c'est une relation d'un élément à un ensemble.

– "$\subset$" se lit "est inclus" et signifie que tous les éléments de la patate de gauche sont 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 $\forall x \in A, x \in B$ (tous les éléments de A sont aussi dans B). Géométriquement, 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. 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 patate 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 $\mathbb{N}$). [Il s'agit de la "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 patate 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:

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

– "$\exists!$" 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 patate 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 1 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 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.

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"; il faut quand même mieux de la géométrie, d'abord, pour comprendre les formules !

3 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.

3.1 Relations

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.

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. 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.

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 $x = 2 \Rightarrow 2 = x$)

– **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 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 (xRy ET yRx) 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 (xRy ET yRx) 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). 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 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, 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 $\mathbb{R}^n$? 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.

3.2 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.

Une fonction (ensembliste) est juste un type de relation particulier. Dans ce contexte, l'élément de A, appelé **antécédent**, joue le rôle d'input; celui de B, appelé **image**, joue celui d'output. 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:

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

[TODO: ajouter un diagramme commutatif pour illustrer ?]

Notez que 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.

Notez que 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** de E par la fonction f. Cet ensemble contient les éléments de l'ensemble d'arrivée qui ont un antécédent par la fonction f (le champ des résultats "possibles" de votre fonction f, en gros).

Notez que si vous voyez le terme "application", 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.

[TODO: Petit topo sur injectivité, surjectivité et bijectivité pour les morphismes ?]

3.3 Opérateurs

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 notation $\star$ 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 $\perp$ (poteau ? '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 ! $+, -, \times, \div,$' 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 $< u|v >$, 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, $\circ(f, x) = f \circ x = f(x)$

– 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).

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.

3.4 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.

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 vois

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 N.

   – $(\mathbb{N}, -)$ n'est pas un magma, car la soustraction n'est pas stable dans 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. "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** (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.

– $(\mathbb{N}^*, +)$ 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 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 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 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 ($1^a = 1 \neq a$).

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**".

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 à $-$ et $\div$ si les éléments symétriques sont présents (*"soustraire c'est additioner par l'opposé, diviser c'est multiplier par l'inverse"*).

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.

— 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 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).

   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 un 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. Certains diront "anneau" pour vouloir dire "pseudo-anneau" et par contre préciseront "anneau unitaire" pour les cas où il existe un neutre multiplicatif. 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 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)).

– $(\mathbb{R}[X], +, \times)$, 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 :

– Deux fonctions f et g dans un espace de fonctions E, f nulle sur 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).

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, 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. Elle l'est aussi pour pouvoir diviser correctement, 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 ($\star$) 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) 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 française 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.

– Les seuls corps de cardinal fini sont les $\mathbb{Z}/p\mathbb{Z}$ (aussi notés $\mathbb{K}_p$, ou $\mathbb{F}_p$ en anglais) 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.

– 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 le sous-groupe 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), ou d'autres exemples plus complexes. Essayez de visualiser ce que ça donnerait.

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 :

– 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 temre "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*.

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

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.

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, 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 "loi scalaire" (en anglais *scaling product*). Ici, j'ai choisi de reprendre l'opérateur $\perp$ qu'on avait pour la multiplication sur les anneaux. Cette fois-ci c'est

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.

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 : 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 : 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. Sa partie 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), inversible. – $\mathbb{R}^3$ 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 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 loi de composition "rond $\circ$" sur les applications linéaires) est aussi une 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 E est une **sous-structure** de F si E et F appartiennent à la même catégorie $\mathcal{C}$ (cela revient à dire qu'il s'agit du même type de structure algébrique) et E est inclus dans F. On peut revenir à démontrer la stabilité de la sous-structure pour justifier que E et F sont dans la même catégorie.

Par exemple :

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

– $H \subset G$

- $\forall x \in H, sym_G(x) \in H$ (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 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 groupe en soi (ie, il respecte les mêmes propriétés que tous les autres groupes). C'est le cas pour toute sous-structure.

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 E est une sous-structure "strictement incluse" dans F, c'est-à-dire si E est inclus dans F et E est différent de F. Rappelez-vous que l'inclusion est une relation d'ordre ! NB: L'inverse d'une sous-structure est une extension de structure. $\mathbb{C}$ est une extension de corps de $\mathbb{R}$.

3.5 Un mot sur la théorie des catégories

L'intérêt 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 albébriques avec un langage commun à toutes. 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 et arriver à faire des opérations entre catégories qui ont 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).

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.

Des exemples:

– 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,

– $Vec_{\mathbb{K}}$, catégorie des espaces vectoriels sur le corps $\mathbb{K}$

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

– Top, catégorie des espaces vectoriels topologiques

- Mod_A, catégorie des modules 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 $g \circ 1_A = g$.

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 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. 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.

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

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

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

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 se démontre). Voici par exemple la définition des applications linéaires dans un EV d'un point de vue de la théorie des catégories. 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 :

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

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

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 et mes matrices c'est LA MÊME CHOSE !!!"

Par ailleurs, Cat, la catégorie des catégories, est elle-même une catégorie. On appelle ses morphismes les "**foncteurs**". Ceux-ci jouent un rôle incroyable 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. De créer des structures complexes à partir de structures simples (free functor, foncteur libre) et de s'en servir comme bloc de marbre pour construire 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 pour y injecter les propriétés souhaitées). Ou l'inverse, de revenir à une structure plus simple à partir d'une structure complexe (forgetful functor, foncteur "oublieur", comme $|U|$, l'ensemble des vecteurs de d'un espace vectoriel U, pris isolés et sans rapport les uns aux autres, comme un ensemble/patate basique sans propriété ni opérateur).

4 Théorie des anneaux et anneaux de polynômes

Pour recapituler, nous avons vu qu'en gros, un anneau c'était une structure avec addition et soustraction classiques (groupe abélien) et une multiplication (pas forcément commutative, comme la composition de fonctions ou la multiplication des matrices carrées de rang n), mais pas (forcément) de division.

Je vais pas vous mentir, la théorie des anneaux c'est vaste et complexe. Après, comme toute chose vaste et complexe en maths, ça offre du vocabulaire et des visualisations pour gérer plus simplement des objets encore plus complexes, en jouant sur les analogies avec des objets plus simples. Mieux vaut comprendre les nombres complexes que mémoriser le formulaire énorme de la trigonométrie !

La théorie des anneaux est un peu un des "gros" sujets mathématiques de la fin du XIXe et début du XXe (et ça a eu des influences dans beaucoup d'autres domaines). Vous voyez les diviseurs de zéros ? C'est la surface de l'iceberg. Il y a énormément d'outils qui ont été développés pour évaluer "à quel point mon anneau/mon algèbre avec une structure plus riche et complexe se comporte ou non comme l'arithmétique et/ou les polynômes, ou pas". Il y a toute une hiérarchie (voire un écosystème...) des propriétés progressivement respectées par vos types d'espaces.

Nous allons donc continuer notre approche sur le vocabulaire et les visualisations, plutôt que les preuves, pour faire un peu sens de tout cela.

La clef de compréhension est qu'on peut construire des relations d'équivalence (appelées **congruences**) et une relation d'ordre (appelée **divisibilité**) particulières sur les membres de certains anneaux (et quelques autres structures à deux opérateurs). Celles-ci donnent naturellement naissance à des comportements qui émergent naturellement, et sont extrêmement profonds (quant à la nature de notre univers et leur utilité pratiqu). Ces relations jouent respectivement le rôle des sous-espaces vectoriels et de l'inclusion entre sous-espaces vectoriels; et vous ne le savez peut-être pas, mais les sous-espaces vectoriels sont un outil fondamental pour expliquer les rapports des espaces vectoriels entre eux. En plus abstrait, le principe général des classes d'équivalence et d'ordre "naturelles" permet de construire des structures à partir d'autres au sein d'une même catégorie, et c'est un outil d'ingénierie mathématique sur lequel se fonde de plus en plus les mathématiques en général.

Dans un premier temps, avec l'exemple de $\mathbb{Z}$, nous verrons le théorème

fondamental de l'arithmétique, et la question des nombres premiers. Par la suite, avec les polynômes, on verra le théorème fondamental de l'algèbre, ainsi que l'analogie avec l'idée de 'polynômes premiers' et des racines des polynômes dans $\mathbb{R}$ et $\mathbb{C}$. Enfin, nous parlerons d'applications concrètes des polynômes, notamment les séries.

4.1 Exemple fondamental: l'arithmétique dans $\mathbb{N}$ et $\mathbb{Z}$

[Notez qu'une structure de demi-anneau suffit pour faire la construction de la division euclidienne. Un demi-anneau est un anneau sans les éléments symétriques pour l'addition. Ne pas confondre avec pseudo-anneau non plus, je parle bien de: https://fr.wikipedia.org/wiki/Demi-anneau]

Quand on parle de $\mathbb{Z}$, on parle en général de $(\mathbb{Z}, +, \times)$ l'anneau des entiers relatifs munis de l'addition, la soustraction et la multiplication (commutative) classiques. Vous remarquerez l'absence de division (façon division dans les corps).

On peut cependant définir une relation d'ordre, appelé **divisibilité**, qui permette de reconstruire une forme de division euclidienne (division avec reste) sur un anneau.

Divisibilité: On dit que "a divise b", et on note "$a|b$", en parlant de la relation suivante entre deux éléments de $\mathbb{Z}$:

$$\forall (a,b) \in \mathbb{Z}^2, (a|b \Leftrightarrow \exists k \in \mathbb{Z}^*, b = ka)$$

On laisse en exercice le fait de montrer que $|$ est une relation d'ordre. On dit que **a est un diviseur de b**, et **b un multiple de a**.

Congruence: Pour tout élément n de $\mathbb{Z}$, on peut munir $\mathbb{Z}$ d'une relation d'équivalence appelée "congruence modulo n", qu'on notera "$a \equiv_n b$"" ou "$a \equiv b[n]$". Cela se lit "a est congru (équivalent) à b modulo n". On définit cette relation de la manière suivante:

$$n \in \mathbb{Z}, \forall (a,b) \in \mathbb{Z}^2, (a \equiv_n b \Leftrightarrow \exists q \in \mathbb{Z}, b = qn + a)$$

De même, pas très compliqué de vérifier que c'est bien une relation d'équivalence.

Division euclidienne: Même si a ne divise pas b, il existe un protocole pour trouver l'entier q tel que aq est aussi proche de b qu'il puisse être sans le dépasser. C'est un des premiers algorithmes que vous ayez appris de votre

vie, un des premiers de l'histoire des maths, et un beaucoup moins anodin qu'il n'y paraît. On pourrait même caricaturer une bonne partie de la fin de ce cours comme "comprendre les ramifications de la division euclidienne sur l'ensemble des maths". On définit la division euclidienne de b par a ainsi:

$$\forall (a,b) \in (\mathbb{N}^*)^2, a \leq b, \exists (q,r) \in \mathbb{N}^2, 0 \leq r < a \text{ et } b = aq + r$$

Pour tout couple d'éléments non-nuls a (le dénominateur) et b (le numérateur) de $\mathbb{N}$ tels que $a \leq b$, il existe deux éléments de $\mathbb{N}$, q (le **quotient**) et r (le **reste**), tels que q groupes de a unités, et un groupe de r unités (pas assez nombreuses pour faire un groupe de taille a), correspondront à une taille initiale de b unités au total.

NB: Pour $\mathbb{Z}$, rien ne change à part un éventuel facteur -1 pour q, et le choix de comment le reste d'un négatif est choisi (si on prend le reste positif pour avoir une valeur absolue de notre nombre, ou "l'opposé du quotient plus le reste positif" pour garder plutôt le signe ET la congruence du résultat).

Résumé des trois définitions précédentes en beaucoup plus intuitif: — a divise b ssi le reste de la division euclidienne est nul. — a est congru à b modulo n ssi le reste r_a de la division euclidienne de a par n et r_b, le reste de b par n, sont égaux. — Exemple qui deviendra plus concret par la suite: prenez une horloge à n heures. n divise a ssi avancer de a heures fait retomber l'horloge sur le même nombre que celui duquel elle est partie. a est congru à b ssi avancer de a ou b heures arrive sur le même résultat (pas forcément le même qu'au départ).

Nombres premiers: On ignore les nombres négatifs dont tout le comportement peut-être expliqué en ajoutant juste le nombre -1 aux les nombres premiers. En se limitant donc sur $\mathbb{N}$, on dit qu'un nombre p est premier s'il n'a comme diviseur que p et 1 (si on faisait la définition sur $\mathbb{Z}$, tout ce qui changerait serait qu'on aurait aussi $-p$ et -1 à considérer). On rajoute comme condition d'ignorer le neutre multiplicatif 1 dans la liste des nombres premiers, afin de simplifier l'expression du théorème fondamental de l'arithmétique.

Une définition équivalente utile pour la suite: imaginez la version "ordre strict" de la divisibilité (a n'est plus un diviseur de a, tout simplement), qu'on pourrait noter $|_{\neq}$ par exemple. Alors un nombre p est premier si et seulement s'il est strictement plus grand que 1, et qu'on ne peut pas trouver ("il n'existe pas") un nombre m entre 1 et p tel que $1|_{\neq}m|_{\neq}p$.

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$$

Théorème fondamental de l'arithmétique

Tout nombre entier ($n \in \mathbb{N}$) peut être exprimé comme un produit de facteurs premiers, et ce produit est unique à l'ordre des facteurs près.

Ce théorème recèle plus qu'il n'en a l'air. L'idée, déjà, est la suivante: si on essaye de décomposer un nombre entier, soit il est premier, soit il est composé. S'il est composé, on peut trouver ses diviseurs, et l'exprimer comme un produit de ces diviseurs. Au bout d'un moment, on arrive toujours à une liste de nombres premiers. On a $2|20$ et du coup, le quotient est 5 et le reste est nul. On peut alors écrire 2×10 puis $2 \times 2 \times 5$ plutôt que 20 en gros.

De plus, ce produit est "unique à l'ordre des facteurs près". On tombe forcément sur les mêmes nombres premiers au final. Après, il faut considérer que la commutativité de la multiplication te permet de dire que l'ordre de ces facteurs premiers n'importe pas.

La raison pour laquelle on ignore 1 (et -1) est parce que la liste pourrait très bien avoir de multiples 1 et -1 dans le produit sans changer son "rôle" arithmétique, qui est de donner une description exacte d'un nombre comme un produit de nombres premiers; une décomposition naturelle en plusieurs facteurs plus petits.

Cette décomposition d'un nombre entier que permet le théorème fondamental de l'arithmétique signifie qu'il y a deux façons de voir les nombres entiers. Une comme une somme, une comme un produit; et que ces façons sont uniques au niveau des nombres premiers.

$$1024 = (1 \times 1000) + (0 \times 100) + (2 \times 10) + (4 \times 1)$$
$$1024 = 2^{10}$$

Cette décomposition en blocs plus simples est la raison de l'importance des nombres premiers. Si l'on considère $\mathbb{P}$, ensemble des nombres premiers inclus dans $\mathbb{N}$, alors l'image de $(\{0, 1\} \cup \mathbb{P})^2$ par la fonction de multiplication est $\mathbb{N}$ tout entier, et les nombres premiers (avec les neutres) génèrent $\mathbb{N}$ par multiplication, sans trou ni problème. Rajoutez la possibilité de multiplier par -1 à l'union précédente, et cela génère $\mathbb{Z}$.

Un phénomène similaire se passe dans les anneaux de polynômes. On parle "d'**anneau factoriel**" pour les anneaux dans lesquels il existe une analogie du théorème fondamental de l'arithmétique et des nombres premiers. Les anneaux de polynômes en sont un exemple, ce qui en soit est assez fascinant.

4.2 Anneaux/algèbres de polynômes

Soit $\mathbb{K}$ un corps; ici on se concentrera sur les cas de $\mathbb{R}$ et $\mathbb{C}$.

NB: On peut définir des structures similaires aux algèbres avec d'autres choses que des corps pour les scalaires (même des trucs plus restreints, style "modules (algébriques)"). On peut définir le fait que la variable x (la partie vecteur) soit à valeurs dans autre chose que dans un corps. On peut avoir plusieurs indéterminées $x, y, z, w, \dots$. On peut faire plein de choses. Pour l'instant on se concentre d'abord sur $\mathbb{C}$ et on expliquera les bizarreries qui se passent sur $\mathbb{R}$ ensuite. Le reste sera pour un autre document.

On appelle **suite numérique à valeurs dans** $\mathbb{K}$ un élément de $\mathbb{K}^{\mathbb{N}} = (\mathbb{N} \to \mathbb{K})$, c'est-à-dire une fonction de $\mathbb{N}$ dans $\mathbb{K}$.

$\mathbb{K}^{\mathbb{N}}$ est un espace vectoriel sur $\mathbb{K}$. Il existe un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$ notable, celui des suites nulles à partir d'un certain rang ($\exists n \in \mathbb{N}, \forall i \geq n, u_i = 0_{\mathbb{K}}$) que l'on note $\mathbb{K}^{\infty}$. Les deux sont de dimension infinie.

Ex:

— la suite définie par la fonction $(n \to 2^n)$, qui pourrait s'écrire $(u_n)_{n\in\mathbb{N}} = (1, 2, 4, 8, 16, 32, 64, 128, 256, \dots)$. C'est un élément de $\mathbb{K}^{\mathbb{N}}$ mais pas de $\mathbb{K}^{\infty}$.

— la suite $(1, 2, 1, 0, 0, 0, 0, \dots)$ est un élément de $\mathbb{K}^{\infty}$ et donc aussi de $\mathbb{K}^{\mathbb{N}}$.

On appelle **monôme** une expression de la forme μx^n, où x est une variable de $\mathbb{K}$ (un nombre pas fixé), n est un entier naturel, et μ est une constante de $\mathbb{K}$ (un nombre fixé). Le nombre n s'appelle le **degré** du monôme. L'objet x s'appelle l'**indéterminée**, ou la **variable**. Le nombre μ s'appelle le **coefficient** du monôme. Un monôme est dit **unitaire** si son coefficient est égal à 1.

NB: Un monôme de degré 0 est un scalaire, un monôme de degré 1 est dit "linéaire", de degré 2 "quadratique", de degré 3 "cubique", de degré 4 "quartique". Si vous voyez "non-linéaire" quelque part, en général vous avez le droit à des monômes/polynômes de degré 2 ou plus (voire tous le temps en

cherchant bien, ie, en faisant artificiellement le lien le plus rapide jusqu'aux polynômes par la théorie des catégories).

On appelle P un **polynôme** si c'est une somme généralisée (une somme sur n élément plutôt que juste 2) de monômes dont le degré va de 0 à n. Les coefficients du polynôme sont choisis comme un élément de $\mathbb{R}^\infty$, par isomorphisme de $\mathbb{K}$-espaces vectoriels. Formellement:

$$P(x) := \sum_{i=0}^{i=n} a_i x^i = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n, \text{ où } (a_n)_{0 \leq n \leq deg(P)} \in \mathbb{K}^\infty$$

Ex: $(1, 2, 1, 0, 7, 0, \dots) = 1 + 2x + x^2 + 7x^4$

NB: Le nombre n porte aussi le nom de **degré** $deg(P)$ du polynôme. Un polynôme dont le monôme de degré maximal a pour coefficient 1 est appelé un polynôme unitaire.

On munit cet espace vectoriel des polynômes, qui est une copie par isomorphisme de $\mathbb{K}^\infty$, d'une multiplication appelée **convolution**, qui est une extension naturelle de la multiplication usuelle/de la distributivité/de la bilinéarité (et qui revient sous beaucoup de formes différentes dans plein d'endroits des maths). Cet espace résultant, noté $\mathbb{K}[X]$, est appelé l'anneau, ou l'algèbre, des polynômes sur $\mathbb{K}$ à une indéterminée (ou "polynôme univarié"). C'est une $\mathbb{K}$-algèbre. L'ensemble des monômes unitaires $(\{1, x, x^2, x^3, x^4, \dots\})$ est une base de $\mathbb{K}[X]$, la plus simple, appelée base canonique. $\mathbb{K}[X]$ est une $\mathbb{K}$-algèbre associative, unitaire, commutative et intègre. NB: $(0, 0, 0, 0, \dots)$ est le neutre additif; $(1, 0, 0, 0, \dots)$ est le neutre multiplicatif.

La convolution, c'est le $(a+b)(c+d) = (ac) + (ad) + (bc) + (bd)$ que vous connaissez depuis le collège, mais où $(a + b)$ et $(c + d)$ par deux polynômes P et Q, et le résultat $(ac) + (ad) + (bc) + (bd)$ est un nouveau polynôme S. Formellement:

$$\forall (P, Q) \in \mathbb{K}[X], (P \times Q)(x) = (\sum_{i=0}^{i=deg(P)} p_i x^i)(\sum_{j=0}^{j=deg(Q)} q_j x^j) = \sum_{i+j=0}^{i+j=deg(P)+deg(Q)} p_i q_j x^{i+j}$$

Ex:

$$(3x + 2)(x^{20} + 3x^{10} + 1) = 3x^{21} + 2x^{20} + 9x^{11} + 6x^{10} + 3x + 2$$

NB: En général, on note P le polynôme abstrait, celui qui est isomorphe à une suite numérique, le $P = (1, 2, 1, 0, 0, 0, \dots)$. On note $P(x) = 1 + 2x + x^2$

pour les "fonctions polynômiales" de $\mathbb{K}$ dans $\mathbb{K}$. Vous verrez des conflations des deux, même si on peut techniquement les distinguer.

On appelle **racine** d'un polynôme toute valeur de x pour laquelle $P(x) = 0$. Ex: $P(x) = x^2 - 1 = (x-1)(x+1)$ s'annule ssi $x = 1$ ou $x = -1$.

On remarque que tout polynôme non-unitaire (avec un monôme de degré maximal dont le coefficient, qu'on nomme $\lambda = a_{deg(P)}$ est différent de 1) peut être multiplié par $\frac{1}{\lambda}$ pour donner un polynôme unitaire avec *les mêmes racines*. $\frac{1}{\lambda}$ est sûr d'exister puisque $\mathbb{K}$ est un corps, et λ est non-nul, sans quoi le degré de P serait plus petit. Ceci dresse une relation d'équivalence, la colinéarité sur $\mathbb{K}[X]$, définie par:

$$P \sim Q \Leftrightarrow \exists \lambda \in \mathbb{K}, \lambda P = Q$$

Cette relation d'équivalence nous permet d'ignorer les polynômes non-unitaire pour ce qui suit, car ils sont identiques à un polynôme unitaire, à multiplication par un scalaire près. Et les polynômes unitaires sont légèrement plus simples à gérer. C'est à peu près la même chose que nous avions fait plus tôt pour ignorer les nombres négatifs dans le théorème fondamental de l'arithmétique. Le paramètre λ dans $\mathbb{R}[X]$ joue le rôle que jouait le nombre -1 dans $\mathbb{Z}$.

On dit qu'un corps $\mathbb{K}$ est dit **algébriquement clos** ssi toutes les racines de tous les polynômes appartiennent aussi à $\mathbb{K}$. Ex: — $\mathbb{C}$ est algébriquement clos. — $\mathbb{R}$ n'est pas algébriquement clos. En effet, le polynôme $x^2+1 = (x-i)(x+i)$ a pour racines i et $-i$, deux nombres complexes (appartenant à une "extension de corps" des réels), malgré le fait que le polynôme (dans sa forme additive) a bien des coefficients réels. Vous remarquerez que les coefficients du polynôme étant dans $\mathbb{N}$, il n'existe pas de structure algébriquement close avant $\mathbb{C}$ dans la hiérarchie classique.

Théorème fondamental de l'algèbre

Tous les polynômes unitaires sur les corps algébriquement clos sont scindés, c'est-à-dire qu'il peuvent être exprimés comme un produit de polynômes unitaires de degré 1. De plus, ce produit est unique à l'ordre des facteurs près, et chaque facteur est de la forme $(x - x_i)$, où x_i est une racine du polynôme.

Cela implique que tout polynôme a exactement autant de racines que son degré.

Similairement au théorème fondamental de l'arithmétique, le théorème fondamental de l'algèbre nous apprend que nos objets, ici non plus des nombres mais des polynômes, possèdent tous une forme additive, et une forme multiplicative, et qu'il y a bijection entre les deux: toutes les polynômes viennent par paires de formules uniques.

$$\forall P \in \mathbb{C}[X], deg(P) = n, a_n = 1, P(x) = \sum_{i=0}^{i=n} a_i x^i = \prod_{j=0}^{j=n} (x - x_j), \forall k \in [[0, n]], P(x_k) = 0$$

NB: Un polynôme a *toujours autant de racines que son degré*, au sens où la somme des multiplicités des facteurs de P dans sa décomposition doit être égale à $deg(P)$.

NB: pour tout polynôme de degré 2, c'est-à-dire de la forme $ax^2 + bx + c$, on peut retenir les élégantes égalités suivantes:

$$\begin{aligned} ax^2 + bx + c &= a(x^2 + \tfrac{b}{a}x + \tfrac{c}{a}) \\ &= a(x^2 - Sx + P) \\ &= a(x^2 - (x' + x")x + (x'x")) \\ &= a(x - x')(x - x") \end{aligned}$$

Où $S = -\frac{b}{a} = x' + x"$ est la somme des racines, et $P = \frac{c}{a} = x'x"$ est le produit des racines. Remarquez bien la présence cachée des effets du théorème fondamental de l'algèbre.

Le sujet des solutions aux équations polynômiales (trouver les racines) est très important, car énormément de problèmes dépendent des racines des polynômes (ou d'une version de ce concept). (La jordanisation est un tel problème.)

Dans $\mathbb{C}[X]$, c'est-à-dire que vos coefficients et variables peuvent être des nombres complexes, les racines existent toujours. Cependant, il n'existe pas forcément de moyen de les exprimer algébriquement (avec une formule bien définie en fonction des coefficients): dans certains cas, on ne pourra qu'au mieux approximer les racines, ce qui peut causer beaucoup de problème. L'analyse numérique est le champ des maths qui cherche à gérer ce genre d'erreurs d'approximation, et leur conséquence sur un problème, pour évaluer la fiabilité de nos machines de calcul scientifique.

Jusqu'au degré 4, il existe toujours une solution algébrique dans $\mathbb{C}$ (les polynômes de degré 2 avec $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, de degré 3 avec la méthode de Cardan,

de degré 4 avec la méthode de Ferrari). Pour les équations polynômiales de degré ¿ 4, il n'existe en général pas de solution algébriques.

https://fr.wikipedia.org/wiki/Théorème_d'Abel_(algèbre) (à ne pas confondre avec le théorème d'Abel pour les séries, mentionné plus bas)

Deux exceptions notables sont les polynômes du type $x^n - c$: les racines sont alors les n racines complexes de l'unité ($\sqrt[n]{1_{\mathbb{C}}}$, où $\sqrt[n]{x} \to (e^{\frac{k}{n}2\pi i})_{k\in[[0,n[[}$ est une fonction de $(\mathbb{C} \to \mathbb{C}^n)$), toutes valeurs de $U(1) \cong SO(2)$) (le groupe cyclique continu) et les polynômes qui peuvent être réduits à un (ou plusieurs) problème de degré 2, 3 ou 4 par symétrie ou extraction algébrique de racines évidentes (un tel cas: si la somme des coefficients est égale à 0, alors 1 est une racine évidente du polynôme).

Dans $\mathbb{R}[X]$, c'est-à-dire que vos coefficients et valeurs sont bien limités aux réels, il arrive que des racines soient complexes. Vous pouvez trouver les racines d'un polynôme de degré 4 par le même procédé que dans $\mathbb{C}$: votre forme multiplicative n'est pas sûre d'utiliser uniquement des nombres $\mathbb{R}$ par contre. Mais ce sera toujours dans le cas particulier d'un polynôme de degré 2 qui est un produit de deux polynômes unitaires de degré 1, dont les constantes respectives sont deux nombres complexes conjugués (ce qui permet à leur produit de redevenir un nombre réel).

Cela veut dire que la décomposition en facteurs d'un polynôme unitaire dans $\mathbb{R}[X]$ sera un produit de blocs $(x-x_i)$ où chaque x_i est une racine réelle du polynôme, et de blocs $(x-z_{j_1})(x-z_{j_2}) = (x^2-2\Re(z_j)x+|z_j|^2)$ où z_j est un "représentant" d'une des deux racines complexes conjuguées du polynômes. Il n'y a pas d'ambigüité ici vu que les deux racines d'un polynôme de degré 2 à coefficients réels, si $\Delta = b^2 - 4ac < 0$, seront deux nombres complexes conjugués (pour que leur somme et leur produit aient un résultat réel). Ils ont nécessairement la même partie réelle et la même norme, et c'est tout ce qui intervient ici dans la version "additive" de notre nombre.

[TODO: Mention rapide de l'espace des fractions rationnelles, la décomposition en éléments simples en utilisant la division euclidienne de K[X] pour l'intégration ? parler déjà de K[XY] avec les monômes multivariés et la distinction de leur notion de degré, parler des polynômes homogènes ?]

4.3 Propriétés des anneaux

Idéal : il existe des **sous-ensembles stables pour les DEUX opérateurs dans un anneau** qui s'appellent les **idéaux** de cet anneau. Mais ces sous-

structures ne conservent pas toutes les propriétés des anneaux (notamment le neutre multiplicatif), donc ne sont pas des sous-structures au sens catégorique du terme, et donc on leur donne ce nom particulier "d'idéal".

En réalité, par distributivité et factorisation (par bilinéarité), une structure stable pour la multiplication l'est en général aussi pour l'addition. Maintenant vous avez quand même le droit à des additions et multiplications plutôt bizarres (et fascinantes et profondes) au bout d'un moment en maths. Par contre, à part l'idéal généré par l'élément neutre (qui est juste l'anneau lui-même inchangé), les idéaux ne sont PAS des sous-anneaux.

Concrètement, un idéal dans $\mathbb{Z}$ c'est *l'ensemble de tous les multiples d'un nombre donné.*

Une autre façon de voir un idéal est de multiplier ses éléments aux éléments de la structure de départ et de prendre l'ensemble de tous les résultats. Dans un anneau non-commutatif, un idéal n'est un "vrai" idéal que quand il génère la même structure quand on le multiplie à gauche et à droite de la structure de départ. Cependant, la question des idéaux à gauche et à droite est traité dans la littérature (pensez au cas d'un anneau de matrice carrées "non-commutatives pour le produit matriciel" par exemple): nous n'aborderons pas le sujet ici, vu que la multiplication (convolution) des polynômes à laquelle nous arrivons est commutative.

– L'ensemble des nombres pairs $\{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$ est un sous-groupe additif de $(\mathbb{Z}, +)$ et est stable pour la multiplication, c'est donc un idéal de $\mathbb{Z}$, noté $2\mathbb{Z}$, généré par 2, c'est à dire en prenant tout élément de $\mathbb{Z}$ et en le multipliant par 2. C'est un abus de notation d'étendre la multiplication dans un ensemble à l'ensemble lui-même, mais il se comprend bien. Comme $\mathbb{Z}$ est un anneau intègre commutatif, l'ensemble des nombres pairs est un idéal des deux côtés.

– L'ensemble des nombres impairs $\{\dots, -5, -3, -1, 1, 3, 5, \dots\}$ est stable par multiplication, mais pas par addition. Il n'a pas le neutre pour l'addition non plus. C'est un sous-monoïde multiplicatif de $(\mathbb{Z}, \times)$ (car contenant le neutre 1 ! et pas d'inverses) mais pas un idéal.

Tout idéal de $\mathbb{Z}$ peut s'écrire $n\mathbb{Z}$ où $n \in \mathbb{N}$ ou $n \in \mathbb{Z}$ (ça revient au même), et est l'ensemble des multiples de n.

$$n\mathbb{Z} = \{a \in \mathbb{Z} \mid n \text{ divise } a\}$$

Ex: $7\mathbb{Z} = \{\dots, -14, -7, 0, 7, 14, 21, \dots\} = \{z \in \mathbb{Z} \mid 7 \text{ divise } z\} = \{z \in \mathbb{Z} \mid z \equiv 0[7]\} = \{z \in \mathbb{Z} \mid z\%7 = 0\}$

Les idéaux sur l'anneau des polynômes sont similairement les ensembles de la forme $P \times \mathbb{R}[X]$ où $\mathbb{R}[X]$ est l'ensemble des polynômes à valeurs réelles, $P \in \mathbb{R}[X]$ est polynôme quelconque, et $P \times \mathbb{R}[X]$ est l'ensemble de tous les polynômes de $\mathbb{R}[X]$ chacun multipliés par P. Si vous vous souvenez du commentaire sur la division euclidienne dans les polynômes faite plus haut, $P \times \mathbb{R}[X] = \{Q \in \mathbb{R}[X] \mid P \text{ divise } Q\}$.

Exemple: l'ensemble E des polynômes de la forme $(x^2 + x - 1) \times Q(x)$ (où $Q(x)$ est un polynôme quelconque de $\mathbb{R}[X]$ et la multiplication est la multiplication usuelle étendue aux polynômes, la convolution) est l'idéal dans $\mathbb{R}[X]$ contenant les polynômes divisibles par $(x^2 + x - 1)$. C'est un idéal des deux côtés, par commutativité de la convolution.

PGCD (Plus Grand Commun Dénominateur)

Le PGCD de deux nombres a et b est le plus grand nombre qui divise à la fois a et b.

$$\forall (a, b) \in \mathbb{Z}^2, PGCD(a, b) = max\{n \in \mathbb{N} \mid n \text{ divise } a \text{ ET } n \text{ divise } b\}$$

C'est aussi le produit des facteurs communs à chacune de leur décomposition; leur zone de rencontre dans leur forme multiplicative. Dans le langage des idéaux, le PGCD est le nombre qui génère l'idéal le plus précis (le $n\mathbb{Z}$ le plus grand) qui contient les idéaux générés par a et b.

$$\forall (a, b) \in \mathbb{Z}^2, PGCD(a, b) = max\{n \in \mathbb{N} \mid a\mathbb{Z} \subset n\mathbb{Z} \text{ et } b\mathbb{Z} \subset n\mathbb{Z}\}$$

L'algorithme pour calculer le PGCD (sans passer par la décomposition en nombres premiers) s'appelle l'algorithme d'Euclide, je vous laisse vous renseigner sur son fonctionnement et sa définition formelle. Vous l'avez normalement déjà employé au collège.

Ex:

$$180 = 2^2 3^2 5^1$$

$$24 = 2^3 3^1$$

$$PGCD(24, 60) = 12 = 2^2 3^1$$

$$P(x) = (x - 1)^2 (x + \pi)$$

$$Q(x) = (x - 1)(x - 2)(x + 12.5)$$

$$R(x) = PGCD(P(x), Q(x)) = (x - 1)$$

et il n'existe aucun nombre n strictement supérieur à 12 pour lequel la propriété suivante est vérifiée:

$$180\mathbb{Z} \subset n\mathbb{Z} \text{ et } 24\mathbb{Z} \subset n\mathbb{Z}$$

ni aucun polynôme S de degré strictement supérieur à $deg(R)$ (ni aucun de même degré que R, autre que R lui-même à l'ordre des facteurs près) pour lequel:

$$P\mathbb{R}[X] \subset S\mathbb{R}[X] \text{ et } Q\mathbb{R}[X] \subset S\mathbb{R}[X]$$

NB: la puissance à laquelle s'élève un facteur premier donné dans la décomposition d'un nombre composé s'appelle sa **multiplicité**.

PPCM (Plus Petit Commun Multiple)

Le PPCM de deux nombres a et b est le plus petit nombre qui soit divisible par a et par b.

$$\forall (a,b) \in \mathbb{Z}^2, PPCM(a,b) = min\{n \in \mathbb{N} \mid a \text{ divise } n \text{ ET } b \text{ divise } n\}$$

C'est aussi le produit des facteurs combinés (sans doublon) de chacune des décomposition de a et b; leur extension combinée. Dans le langage des idéaux, le PPCM est le nombre qui génère le plus grand idéal

$$\forall (a,b) \in \mathbb{Z}^2, PPCM(a,b) = min\{n \in \mathbb{N} | n\mathbb{Z} \subset a\mathbb{Z} \text{ et } n\mathbb{Z} \subset b\mathbb{Z}\}$$

Notez ici que $PPCM(a,b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$

Ex:

$$180 = 2^2 3^2 5^1$$
$$24 = 2^3 3^1$$
$$PPCM(24,60) = 360 = 2^3 3^2 5^1$$

$$P(x) = (x-1)^2(x+\pi)$$
$$Q(x) = (x-1)(x-i)(x+12.5)$$
$$R(x) = PPCM(P(x),Q(x)) = (x-1)^2(x+\pi)(x-i)(x+12.5)$$

Dans toute structure E dans laquelle on peut définir une analogie du PGCD et du PPCM (comme les anneaux de polynômes ou les algèbres géométriques), on a comme théorème:

$$\forall (a,b) \in E, PGCD(a,b) \times PPCM(a,b) = a \times b$$

Nombres premiers entre eux Deux nombres sont dits premiers entre eux si leur PGCD est égal au neutre multiplicatif.

NB: à travers tout le passage précédent, le terme "nombre" peut en général être compris comme "élément d'un espace qui fonctionne (au moins) comme un anneau factoriel".

[TODO: Anneaux gradués ? Anneaux noethériens ? Distinction technique entre anneau factoriel et anneau principal ? Théorème de Bézout ?]

5 Applications des polynômes: séries, développements limités et anneaux de polynômes de fonctions

5.1 Convergence et séries entières

Convergence

On dit qu'une suite numérique est **convergente** si lorsque n se rapproche de $+\infty$, le résultat renvoyé en output par la suite "s'approche" d'une valeur donnée de $\mathbb{K}$. "S'approcher" peut avoir plusieurs définitions techniques selon le contexte (surtout quand on s'intéresse aux suites de fonctions; et aux différents types de convergence sur espaces de fonctions). Une introduction à l'analyse/la topologie serait nécessaire pour définir adéquatement les différentes formes de continuité et de convergence, et se créer une intuition bien distincte pour chacune. Nous en resterons à celles dont nous avons strictement besoin.

L'idée de la définition de la convergence en une valeur d'input autour d'une valeur d'output (que ce soit convergence en $+\infty$ d'une suite ou en une valeur de $\mathbb{K} \cup \{\infty\}$ pour une fonction continue par morceaux), est que s'approcher de la valeur d'input en laquelle la limite a lieu, implique de s'approcher aussi de la valeur limite en output. La valeur d'output vers laquelle tend l'élément est appelé la **limite** de l'objet mathématique en la valeur d'input par la fonction qu'on lui applique. Nous donnons la définition pour la convergence d'une suite.

Formellement, on dit qu'une suite $(u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ est **convergente vers une limite** $u \in \mathbb{K}$ ssi la propriété suivante est vérifiée:

$$\exists u \in \mathbb{K}, \forall \epsilon \in \mathbb{R}_+^*, \exists N \in \mathbb{N}, \forall i \in \mathbb{N}, (i \geq N \Rightarrow |u_i - u| < \epsilon)$$

On peut alors noter: $u = \lim_{n\to+\infty} u_n$

C'est-à-dire que pour toute distance strictement positive ϵ, qu'on peut prendre aussi petite (aussi proche de 0 côté positif) que l'on souhaite; il existe un certain rang N de notre suite à partir duquel toute valeur (les u_i où $i \geq N$) est au moins "ϵ-proche" de la valeur limite u (c'est-à-dire $|u_i - u| < \epsilon$).

Si cette limite u n'existe pas (ou qu'elle correspond à ∞), on dit que la suite **diverge**, et on précisera son comportement à l'approche de l'infini.

En une dimension, "a est ϵ-proche de b" veut dire $a \in]b-\epsilon, b+\epsilon[$; dans des dimensions supérieures, on définit un "bloc topologique de base" selon comment la distance se calcule dans cet espace, en général, c'est ligne, carré, cube, hypercube... centré en u, ou alors ligne, disque, boule, hyperboule... centré en u. C'est la notion de **voisinage** en topologie.

Pour l'exemple simple qui concrétise le tout: la convergence d'une valeur dans $\mathbb{C}$, si l'on trace les points $u_0, u_1, \dots$ sur le plan complexe, ressemble à la trajectoire d'un objet qui est happé par la gravitation d'un point u: il entre en orbite spirale en s'approchant indéfiniment. Aussi petit que l'on choisisse ϵ, le rayon du cercle centré en u, il y aura un rang N à partir duquel toutes les étapes suivantes de la suite (les $u_N, u_{N+1}, \dots$) seront à l'intérieur du cercle.

Séries

Il existe un endomorphisme de $\mathbb{R}^{\mathbb{N}}$ qui à chaque suite $(u_n)_{n\in\mathbb{N}}$ fait correspondre une suite $(S_n)_{n\in\mathbb{N}}$, appelée **série (numérique) de terme général** $(u_n)_{n\in\mathbb{N}}$, définie par l'équation suivante:

$$\forall n \in N, S_n = \sum_{i=0}^{i=n} u_i = u_0 + u_1 + \cdots + u_n$$

Si celle-ci existe, on appelle la limite, somme ou résultat, et on note S, l'élément défini par:

$$S = \lim_{n\to\infty} S_n = \sum_{i=0}^{i=+\infty} u_i = u_0 + u_1 x + u_2 + u_3 + \dots, \text{ où } (u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$$

Dans le cas où cette limite n'existe pas (ou qu'elle est infinie), on dit que la série **diverge**.

On appelle le terme S_n, pour un n fixé, la **somme partielle**de la série. On définit le **reste** de la série comme:

$$R_n = S - S_n = (\sum_{i=def(P)+1}^{i=+\infty} a_i x^i)$$

Exemple 1:

$$\forall n \in \mathbb{N}, u_n = 1$$

$$u = \lim_{n\to\infty} u_n = +\infty$$

$$\forall n \in \mathbb{N}, S_n = n$$

$$\forall n \in \mathbb{N}, R_n = +\infty$$

$$(S_n)_{n\in\mathbb{N}} = (1, 2, 3, 4, 5, ...)$$

$$(R_n)_{n\in\mathbb{N}} = (\infty, \infty, \infty, ...)$$

$$S = +\infty$$

Exemple 2:

$$\forall n \in \mathbb{N}, u_n = \frac{1}{n!}$$

$$u = lim_{n\to\infty} u_n = 0$$

$$\forall n \in \mathbb{N}, S_n = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}$$

$$\forall n \in \mathbb{N}, R_n =$$

$$(S_n)_{n\in\mathbb{N}} = (1, 2, 2.5, 2.666, \dots)$$

$$(R_n)_{n\in\mathbb{N}} = (e - 1, e - 2, e - 2.5, e - 2.666, \dots)$$

$$S = e \simeq 2.71828182846$$

NB: Pour que cette limite de la somme existe, il faut déjà que que la suite correspondant au terme général tende vers 0. Non seulement ça, mais en plus elle doit tendre vers 0 assez vite pour répondre à certains critères, sans quoi la somme diverge. R_n sert à simplifier l'analyse technique de ce comportement à l'infini. L'idée intuitive c'est que le terme général doit converger "strictement plus vite vers 0 que ne le fait $\frac{1}{x}$". C'est-à-dire que "$\sum_{i=0}^{\infty} \frac{1}{x}$" ne converge pas, mais que "$\sum_{i=0}^{\infty} \frac{1}{x^d}$" converge dès que $d > 1$ (avec un petit supplément de technicité à rajouter pour un terme général $\frac{1}{x^a(\ln(x))^b}$ si $a = 1$, "série/intégrale de Bertrand"). On peut aussi noter l'exception de certaines séries alternées qui peuvent converger avec un terme général plus grand).

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

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

NB: Le symbole $\sum$ (sigma) est choisi pour la somme discrète, le symbole intégral $\int$ (s) pour la somme continue. La somme partielle est l'équivalent discret d'une intégrale de a à b continue. La série est l'équivalent discret de l'intégrale avec une borne infinie continue. Si vous n'en avez jamais vu,

cela veut dire la limité d'une intégrale de a à x avec a fixé et x tendant vers l'infini. Formellement:

$$\int_a^{+\infty} f(t)dt = \lim_{x \to +\infty} \int_a^x f(t)dt$$

On retrouve plusieurs critères de convergence. La somme partielle (de $i = a$ à $i = b$) correspond à une intégrale discrète de a à b.

https://fr.wikipedia.org/wiki/Comparaison_série-intégrale

NB: Une bonne partie de l'analyse générale des séries consiste à trouver une formule plus sympathique pour la somme partielle. Par exemple, la série définie comme la somme progressive de tous les nombres entiers jusqu'à n peut s'écrire:

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

Séries entières

Il existe, pour tout corps $\mathbb{K}$, un foncteur de $Vec_{\mathbb{K}}$ dans $Alg_{\mathbb{K}}$ qui renvoie chaque suite numérique $(a_n)_{n \in \mathbb{N}}$ de $\mathbb{K}^{\mathbb{N}}$ vers une *suite de polynômes*, notée $S_n(x) \in (\mathbb{K}[X])^{\mathbb{N}}$, appelée **série entière de terme général** $a_n x^n$. Celle-ci est définie de la manière suivante:

$$\forall n \in \mathbb{N}, S_n(x) = a_i x^i = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n, \text{où} (a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$$

Si celui-ci existe, on appelle la valeur, limite, somme ou résultat, et on note $S(x)$, le polynôme défini par:

$$S(x) = \sum_{i=0}^{i=+\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots, \text{où} (a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$$

NB: vous verrez en général x comme indéterminée pour les séries sur $\mathbb{R}$, et z sur $\mathbb{C}$.

NB: Pour faciliter l'analyse, on décompose ici aussi souvent une série entière en deux morceaux, un morceau $S_n(x)$, appelé "somme partielle" et un morceau $R(x)$, appelé "reste" tels que

$$S(x) = S_n(x) + R_n(x) = (\sum_{i=0}^{i=deg(P)} a_i x^i) + (\sum_{i=deg(P)+1}^{i=+\infty} a_i x^i)$$

NB: le critère de convergence est ici plus riche; vu qu'on a un x variable, il y aura en général des valeurs pour lesquelles la série converge (dans une zone pour x appelée "rayon de convergence", un cercle/voisinage/etc autour de 0 en gros), et d'autres valeurs de x pour lesquelles la série entière diverge.

[TODO: Critères de convergence d'Abel, de Cauchy, de d'Alembert + Raabe-Duhamel. Ouverture sur les polynômes à plusieurs indéterminées de K[XY] et la question de la multiplication non-commutative ? intro pour la géométrie algébrique ? Séries dérivées et convergence vers la dérivée ? Dérivées discrètes ? Distinction techniques des convergences: absolue, normale, uniforme...]

5.2 Théorème d'approximation de Stone-Weierstrass

Un brin de topologie

Ce serait mieux de vous faire faire un peu de topologie avant de passer directement à Stone-Weierstrass, pour bien comprendre l'expression technique du théorème, ou plutôt la notion de "densité" qui le rend compréhensible sans compréhension technique parfaite. Si vous avez relativement tout compris jusqu'à ce stage, on devrait quand même pouvoir vous en donner une bonne idée avec des exemples. N'ayez pas peur si vous ne comprenez pas tout pour l'instant, ça se veut une introduction rudimentaire.

Une **topologie**, comme nous l'avons mentionné rapidement plus haut, est une construction qui est "un ensemble d'ensembles" représentant "une structure choisie pour gérer sur les sous-ensembles d'un ensemble donné". Si ces sous-ensembles respectent certaines propriétés entre eux (typiquement sur la stabilité dans la topologie de différents degrés d'intersection et d'union d'ensemble finis ou infinies), on les qualifie "d'ouvert" et de "fermé".

Un **ouvert** c'est la généralisation d'un intervalle réel ouvert (ie, $]a, b[= \{x \in \mathbb{R} \mid a < x < b\}$, notez que $a < b$ par transitivité, donc les deux nombres sont différents), un **fermé** d'un intervalle fermé (ie, $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$, notez que cela peut-être un singleton, contrairement aux ouverts, à cause de l'ordre large). Cette généralisation s'opère de la même manière que celle des "hyperboules" ou "hypercubes" centrés autour d'un point décrite plus haut. A la différence près qu'une union (même infinie continue) d'ouverts est un ouvert, et une intersection finie (jusquà n fixé) de fermés un fermé; donc on peut s'amuser à faire d'autres formes que des hypercubes ou hyperboules.

Le rôle fondamental d'une topologie (au sens de "organisation des parties d'un ensembles selon certaines propriétés, notamment par rapport à l'union et l'intersection de zones", qui fait la différence entre un "espace vectoriel" et un "espace vectoriel topologique") est de permettre de définir un "voisinage" pour chaque point. Le **voisinage** en topologie est une façon technique de décrire "dans un ensemble englobant, l'ensemble des sous-ensembles qui contiennent un point". Cela permet d'exprimer des informations importantes sur la structure d'un espace en observant les comportements locaux.

Soit A un sous-ensemble d'un espace vectoriel topologique. On appelle "**adhérence**", et on note $\overline{A}$, la "complétion fermée" d'un ensemble. On appelle "**intérieur**", et on note $\overset{\circ}{A}$ la "plus grand partie ouverte" d'un ensemble. On appelle "frontière" de A (et on note δA) la partie qui appartient à l'adhérence de A mais pas à son intérieur.

NB: certains ensembles peuvent être simultanément ouverts et fermés ("clopen" ssi l'intérieur est égal à l'adhérence). C'est le cas de l'ensemble vide et de l'ensemble englobant, pour toute topologie.

NB: Frontière = adhérence - interieur (au sens de la soustraction d'ensembles).

$$\delta A = \overline{A} - \overset{\circ}{A}$$

NB: *Un ensemble est fermé ssi il est égal à son adhérence. Un ensemble est ouvert ssi il est égal à son intérieur. Un ensemble est ouvert et fermé ssi sa frontière est nulle.*

Ex:

— En 1D, pour un intervalle $]a, b]$ avec $a < b$, son adhérence est $[a, b]$, son intérieur est $]a, b[$, et sa frontière est $\{a, b\}$

— En 2D, notre exemple basique est un disque de rayon 1, avec éventuellement un peu du cercle de rayon 1 qui appartient aussi à notre ensemble (exemple, l'ensemble $M = \{z \in \mathbb{C} | (|z| < 1) \text{ ou } ((|z| = 1) \text{ et } (\Re(z) > 0))\}$, qui contient le disque entier, et la partie du cercle à droite de l'axe des imaginaires purs, mais pas la partie du cercle à gauche de cet axe. La frontière du disque δM est le cercle de rayon 1 tout entier ($\delta M = \{z \in \mathbb{C}, |z| = 1\}$), son intérieur est le disque sans le cercle ($\overset{\circ}{M} = \{z \in \mathbb{C}, |z| < 1\}$), son adhérence est l'union du disque avec le cercle ($\overline{M} = \{z \in \mathbb{C}, |z| \leq 1\}$)

— le cas nD ressemble au cas 2D, avec "hyperboule" remplaçant "disque", et "hypersphère" remplaçant "cercle".

NB: la façon technique de penser l'adhérence est "si on imagine des suites à valeurs dans un ouvert U, quel sera l'ensemble de mes limites possibles ?". Dans $]a, b]$, on peut approximer a par la droite $(a + 0.00\ldots001)$, donc a peut être la limite d'une suite de $(\mathbb{N} \to]a, b])$, donc $\{a\}$ appartient à l'adhérence de $]a, b]$. On voit bien alors en quoi les suites à valeurs dans un disque peuvent converger vers une limite à la frontière, sur le cercle.

NB: Les éléments discrets d'un espace continu sont en général tous des "fermés" de mesure nulle pour la plupart topologies classiques. Selon le choix de la topologie, ceci peut-être faux. Le choix d'une topologie consiste en gros un niveau de "détail" que l'on choisit pour les voisinages. Ce "détail" revient à des questions de sous-ensembles imbriqués.

(cf. https://en.wikipedia.org/wiki/Comparison_of_topologies)

En général, pour des usages pratiques, on choisit des ouverts donnant naissance à la "mesure de Lebesgue" (concept assez simple: Lebesgue dimension 1 = longueur; Lebesgue dimension 2 = aire; Lebesgue dimension 3 = volume; etc.), qui joue (en plus abstrait) le rôle en mathématiques du "mètre" en physique (d'où le nom de "mesure"). Votre déterminant de matrice est techniquement une mesure de Lebesgue de dimension n pour une matrice de taille $n \times n$.

Densité de $\mathbb{Q}$ dans $\mathbb{R}$

Nous en venons à la raison pour laquelle j'ai fait ce détour avant de passer à Stone-Weierstrass, la notion de **densité**. On dit que A est "dense" dans B ssi l'adhérence de A est égale à B.

L'exemple du cercle et du disque est très utile pour comprendre les notions d'intérieur et d'adhérence, mais il cache un certain type de comportement qui revient souvent, dont le cas de $\mathbb{Q}$ dans $\mathbb{R}$ est l'exemple typique.

La "densité" de $\mathbb{Q}$ dans $\mathbb{R}$ est particulière, parce que $\mathbb{Q}$ couvre bien toute l'étendue de $\mathbb{R}$ (de $-\infty$ à $+\infty$; et à chaque niveau infinitésimal). Pour tout x réel, on peut toujours trouver une infinité (discrète) d'éléments de $\mathbb{Q}$ qui sont "ϵ-proches" de x ! Autre façon de le voir, dans toute intervalle réel (un intervalle à intérieur (ouvert) non-nul; pas un singleton ou une liste de singletons), il existe une infinité de rationnels.

Cependant, par rapport à $\mathbb{R}$, $\mathbb{Q}$ est bourré de "trous". Sur la droite réelle, il existe plein de valeurs, comme π, comme $\sqrt{2}$, comme e, comme le nombre d'or, qui ne peuvent pas être exprimées comme une fraction $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, et qu'on appelle "irrationnels" (car ratio = fraction). Cela peut paraître contre-intuitif, mais ces nombres irrationnels sont tellement plus

nombreux (l'ensemble $\mathbb{R}-\mathbb{Q}$ d'un cardinal infini plus grand), que la mesure de $\mathbb{Q}$ dans $\mathbb{R}$ est nulle, alors que la mesure de $\mathbb{R}-\mathbb{Q}$ est égale à celle de $\mathbb{R}$ tout entier !

En gros, les éléments de $\mathbb{Q}$ fonctionnent comme des points ultra-fréquents et zoomables à l'infini sur une droite. Les éléments de $\mathbb{R}-\mathbb{Q}$ fonctionnent comme des micro-segments "entre" chacun de ces points. Du moins c'est ce qui semble être le cas par intégration (l'intégrale en un point ou sur une liste de points est toujours nulle, sauf cas particulier bien spécifiques où les points fonctionnent comme des singularité, style masse de Dirac). Cependant, cette intuition a un problème fondamental, qui est que pour chaque "micro-segment" qu'on essayerait de construire, il y a une infinité d'élements de $\mathbb{Q}$ pour le re-découper quand on zoome.

C'est pourquoi on a utilisé les notions de convergence, de voisinage et d'adhérence pour expliquer ces ramifications infinies et bizarres de $\mathbb{Q}$ dans $\mathbb{R}$. En gros, on a dit "on prend les suites à valeurs dans $\mathbb{Q}$, et on considère l'ensemble des limites de ces suites, comme ça c'est un peu comme si on faisait des cercles de rayon infiniténisimal ϵ autour de chaque point". Cet ensemble de toutes les limites est $\mathbb{R}$, car les cercles infinitésimaux comblent tous les trous; couvrent tous les irrationnels.

En clair: **La densité de $\mathbb{Q}$ dans $\mathbb{R}$ signifie que tout nombre réel peut-être approximé comme la limite d'une suite de rationnels.**

NB: l'intérieur de $\mathbb{Q}$ dans $\mathbb{R}$ pour les topologies classiques est l'ensemble vide: cela implique une mesure de Lebesgue nulle pour la tribu des boréliens. NB: l'injection canonique de $\mathbb{Q}$ dans $\mathbb{R}$ (output 1 si $x \in \mathbb{Q}$ sinon output 0) est un exemple de fonction "continue nulle part". NB: $\mathbb{Q} \oplus i\mathbb{Q}$ est dense dans $\mathbb{C}$. NB: pour comprendre adhérence et intérieur, bien se souvenir de l'exemple du disque à demi-frontière et l'exemple de $\mathbb{Q}$ dans $\mathbb{R}$ vus ici. L'essentiel de ces concepts se résume avec ces deux exemples.

Explication du théorème de Stone-Weierstrass: Densité de $\mathbb{R}[X]$ dans $\mathcal{C}^0(\mathbb{R}^{\mathbb{R}})$

Soient E et F deux ensemble quelconques.

On note $\mathcal{C}^0(F^E)$ l'espace des fonctions continues de E dans F.

On note $\mathcal{C}^1(F^E)$ l'espace des fonctions dérivables à dérivée continue de E dans F.

On note $\mathcal{C}^n(F^E)$ l'espace des fonctions n fois dérivables de E dans F, dont la n-ième dérivée est continue.

On note $\mathcal{C}^\infty(F^E)$ l'espace des fonctions lisses de E dans F, c'est-à-dire les fonctions infiniment dérivables.

NB: On rappelle que toute fonction est forcément continue là où elle est dérivable:

$$\forall(n,m) \in \mathbb{N}^2, n < m, \mathcal{C}^m \subset \mathcal{C}^n$$

Ex:

— La valeur absolue $(x \to |x|)$ est de classe $\mathcal{C}^0$ sur $\mathbb{R}$.

— La fonction $(x \to x \times |x|)$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}$.

— $\exp, \ln, \cos, \tan, \sin$ et les polynômes sont de classe $\mathcal{C}^\infty$.

Théorème de Weierstrass

Soit A un intervalle fermé de $\mathbb{R}$, et f une fonction continue de $(A \to \mathbb{R})$. Alors, il existe une suite de polynômes $(P_n(x))_{n\in\mathbb{R}}$ de $(\mathbb{N} \to \mathbb{R}[X])$ telle que $(P_n(x))_{n\in\mathbb{R}}$ converge uniformément vers f sur A.

L'idée fondamentale ici est que "tout comme on peut approximer tout réel par une suite de rationnels, on peut aussi approximer toute fonction continue de $\mathbb{R}$ dans $\mathbb{R}$ par une série entière".

NB: la convergence uniforme est une version de la convergence sur les espaces de suites de fonctions $(f_n)_{n\in\mathbb{N}}$ (ici $\in (\mathbb{N} \to \mathbb{K}^{\mathbb{K}})$, nécessaire à certaines démonstrations. En gros, la convergence simple c'est une convergence "point-par-point" vérifiée par une fonction, mais tous les points ne convergeront pas tout à fait "ensemble/en commun" vers . La convergence uniforme est une version de la convergence où la convergence "point-par-point ET en commun" a lieu. C'est une condition plus forte de convergence.

L'expression du théorème selon Stone est une généralisation puissante de la version Weierstrass, mais je me vois mal vous la faire comprendre dans son détail sans de meilleures bases en analyse et en topologie que le rudiment fourni ici. L'idée est qu'il généralise le résultat de Weierstrass en transformant d'une part l'intervalle fermé en l'idée de "compact" (un ensemble "fermé" avec de bonnes propriétés topologiques supplémentaires, typiquement d'aider à transformer une propriété vraie "au voisinage de chaque point" au compact entier); et d'autre part, en élargissant le cas de $\mathbb{R}$ à toute une classe d'algèbres de fontions (appelées algèbres de Banach). Consultez ici si vous êtes curieux:

https://fr.wikipedia.org/wiki/Théorème_de_Stone-Weierstrass .

Séries de Taylor/Maclaurin

Autre que l'interpolation polynômiale, l'application la plus importante du théorème de Stone-Weierstrass est l'idée de série de Taylor et les approximations de fonction par développement limité.

Une fonction $f = (x \to f(x)) \in \mathcal{C}^{n+1}(F^E)$ (avec $n \in \mathbb{N} \cup \{\infty\}$), dérivable donc en tout point a, possède une expression sous la forme d'une série (appelée **développement de Taylor d'ordre** n ou **développement limité d'ordre** n) et d'un reste intégral, qui est négligeable lorsque x tend vers a (notée $\epsilon(x-a)$). Cette formule permet d'approximer $f(x)$ au voisinage du point a à l'aide d'un polynôme.

$$\forall x \in E, f(x) = (\sum_{i=0}^{i=n} \frac{f^{(i)}(a)}{i!}(x-a)^i) + \epsilon(x-a)$$

où les $f^{(i)}$ signifie la i-ème dérivée de f, et f elle-même peut-être considérée comme la 0-ième dérivée. Aussi, on indique la simplification faite:

$$\epsilon(x-a) = \frac{1}{n!}\int_a^x (x-t)^n f^{(n+1)}(t)dt$$

NB: $n!$ se lit "n factorielle", et est défini comme le produit des n premiers nombres entiers:$\forall n \in \mathbb{N}, n! = \prod_{i=1}^{i=n} i = 1 \times 2 \times \cdots \times n$ Dans les ordres de vitesse de divergence, vous avez: logarithmique $<$ linéaire $<$ polynomial $<$ exponentiel $<$ factoriel. Ca croît très, très vite la factorielle.

NB: en général, on parle plus de série de Taylor pour le cas $n = \infty$, quand la fonction approximée est infiniment dérivable.

NB: Si $a = 0$, on parle aussi de "série de Maclaurin". La plupart des développements limités sont donnés en tant que série de Maclaurin.

Je vous invite vivement à consulter ceci et à comprendre les images:
https://en.wikipedia.org/wiki/Taylor_series
http://www.h-k.fr/publications/data/adc.ps__annexes.maths.pdf

NB: le développement limité est très souvent utilisé en physique pour des approximations rapides (par exemple, un cosinus en 0 remplacé par les 3 premiers termes de sa série de Taylor, $\cos(x) \simeq 1 + \frac{x^2}{2!}$).

NB: l'exponentielle d'une matrice carrée A est définie comme la série de Maclaurin de l'exponentielle où l'on remplace l'indéterminée x par la matrice A.

NB: les plupart des fonctions classiques en mathématiques ($\ln, \exp, \cos, \sin, \dots$) sont implémentables, et efficaces, par série de Taylor/approximations et convergences. Vous devriez à ce stade en être tout à fait capable (il faut juste faire attention aux vitesses de convergence selon l'input et la fonction choisie; le développement $\ln(1+x)$ converge mal autre part qu'autour de $x = 0$, mais il y a des techniques pour trouver un résultat hors de la zone de converge grâce à un résultat trouvé dans la zone de convergence).

NB: les séries/les transformées de Fourier (forme série/discrète et forme intégrale/continue) sont un sujet très, très utile à maîtriser en tant qu'informaticien et en tant que mathématicien. Fondamentalement, c'est une autre façon de faire "une approximation de fonction par densité topologique" que Weierstrass/Taylor. Avec une maîtrise correcte des intégrales et des nombres complexes, et une meilleure compréhension des convergences que celle présentée rapidement dans ce texte, vous avez toutes les clefs en main pour vous y intéresser à ce stade.

6 Anneau de fonctions, de matrices, de fonctions continues, espace vectoriels normés, espaces de Banach, analyse numérique

[TODO]

7 Bonus: Quotientage de structure algébrique par classe d'équivalence

7.1 Anneau quotient $\mathbb{Z}/n\mathbb{Z}$

Les idéaux peuvent devenir très intéressant sur les $\mathbb{K}$-algèbres, en employant les quotients d'algèbres. Quotienter une algèbre par une relation d'équivalence sur un de ses idéaux est le seul moyen de maintenir la stabilité des *deux* opérateurs internes (et donc la structure d'algèbre) dans l'espace quotient.

Travaillons l'exemple de l'horloge à n heures. On peut considérer $\mathbb{Z}$ comme une algèbre; $5\mathbb{Z}$ comme un idéal. Les ensembles de translations (appelé **espaces affines**) possibles modulo 5 sont les 5Z + m où $m \in [[0, 4]]$. (ex: 5Z + 1 = ...,-9,-4,1,6,11,.... En effet, 5Z + 1 est le même ensemble que 5Z + 6, etc.

On considère que deux éléments sont équivalents dans l'espace quotient Z/5Z ssi ils appartiennent au même espace affine 5Z + m dans Z. Ainsi, l'espace quotient Z/5Z est l'ensemble des classes d'équivalence de Z modulo 5. $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ où $-5 = 0 = 5 = 10 = 15$ etc., où $-4 = 1 = 6 = 11$ etc., où $-3 = 2 = 7 = 12$, etc. Comme une horloge à 5 heures : après 4, on revient à 0. Sur cette horloge, si je me couche à 4 heures et que je dors 12 heures, je me réveille à 1 heure, donc $4 + 12 = 16 = 1$ dans ce système. En informatique (4 + 12) % 5 == 1.

On dit que la relation d'équivalence est "bien-fondée" car elle mène à un espace quotient dans lequel les représentant d'une même classe d'équivalence (par exemple les $-3 = 2 = 7 = 12$) ont tous le même rôle arithmétique et géométrique sur l'horloge à 5 heures.

Exercice : montrer que $\mathbb{Z}/5\mathbb{Z}$ est un corps.

NB : quand vos types unsigned en C overflowent (vous dépassez le max du type *unsigned int* par exemple), ils ont ce même comportement cyclique. En quelque sorte, "unsigned char" désigne ce même genre "d'horloge avec juste les heures", cette fois-ci à 256 heures, représentée en mémoire en binaire sur 8 bits.

NB : les $\mathbb{Z}/p\mathbb{Z}$ (aussi notés $\mathbb{K}_p$ ou $\mathbb{F}_p$) où p est un nombre premier sont les seuls corps finis (plus précisément, si un corps est fini, alors il est isomorphe à un $\mathbb{Z}/p\mathbb{Z}$). On appelle p (le nombre le plus petit, différent de zéro, qui par multiplication renvoie tout autre élément à zéro) la **caractéristique** du corps. Si un tel nombre n'existe pas, le corps est dit **de caractéristique**

0. La caractéristique de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ est donc 0. Seuls les corps finis ont une caractéristique non-nulle.

https://en.wikipedia.org/wiki/Linear_subspace (image de F_5^2 géniale, pour montrer qu'on peut bien créer un espace vectoriel sur un corps fini)

Exercice : faire une construction similaire pour $\mathbb{R}/\mathbb{Z} \cong U(1) \cong SO(2)$ (le groupe unitaire).

7.2 Problème final: quotients d'espaces vectoriels

Pour terminer ce document, je vous propose un problème qui vous intéressera et vous creusera les méninges, de quoi travailler plusieurs outils acquis ici. Le travail de prendre conscience des outils dont il faudra se servir, et ignorer ceux dont on n'a pas besoin dans ce cas, est fondamental à la recherche mathématique. Je défends même souvent d'avoir plus appris sur les maths en jouant à *The Legend of Zelda* qu'en cours, rien que pour cet exercice là: une nouvelle salle, un nouveau puzzle, une nouvelle façon de combiner les outils dans notre sac... C'est fondamentalement ça la recherche en maths, quand il n'y a d'autorité pour vous donner "la réponse au fonds du bouquin".

Soit F un sev de E. On note $(F + v) = \{v + w \in E | v \in E, w \in F\}$ les espaces affines parallèles au sev F dans E. Différentes valeurs de v peuvent donner le même espace affine. On munit donc E d'une relation d'équivalence $\sim_F$ telle que $v \sim_F v' \Leftrightarrow (v - v') \in F$. Finir la construction de l'espace quotient (déjà bien entamée) $E/\sim_F$ (aussi noté E/F par convention). Expliquer la géométrie des espaces affines, l'intuition géométrique des formules au-dessus, et la géométrie de E/F. Vérifiez que E/F est bien un sev, précisez sa dimension en fonction de celles de E et F. Prenez par exemple $E = \mathbb{R}^3$ et F le sev de dimension 1 généré par le vecteur $w_0 = e_3 = (0, 0, 1)$

[TODO: parler des quotients d'ev et des foliations pour les solutions d'équadiff ?]

[TODO: Parler des suites récurrentes $u_(n + 1) = f(u_n)$, et du fait qu'il s'agisse fondamentalement d'une équation différentielle discrète ?]