Ce qui n’est plus dans le programme de mathématiques du lycée.

Ce qui n'est plus dans le programme de mathématiques du lycée

Structures

Préface

Ce texte est la suite de l'ouvrage « ensembles ». On y introduit l'étape suivante dans la construction des « idées mathématiques », les structures. Les structures abordées dans cet ouvrage étaient enseignées dans les programmes du lycée des filières mathématiques (et même du collège) il y a 40 ans, et *permettaient d'appréhender l'universalité de certaines notions mathématiques* qui étaient préalablement vues concrètement sur une construction particulière. Effectivement, le parcours de l'élève au lycée doit lui faire constater que dans les mathématiques, il y a beaucoup de choses qui se ressemblent, sans être exactement les mêmes. La notion de structure permet de comprendre de façon plus abstraite la cause de ces ressemblances, et permet donc, de « structurer » le vaste domaine des mathématiques. *Dans la mesure où le programme actuel du lycée ne nécessite pas la compréhension de la notion de structure pour être compris, c'est quand-même une façon de prendre du recul vis-à-vis des notions apprises*. La notion d'espace vectoriel était la culmination des structures algébriques vues au lycée, notion dont il serait dommage de ne pas la connaître au regard de l'enseignement des matrices en spécialité mathématique. Mais aussi en dehors de cet enseignement de spécialité, la notion de « combinaison linéaire » de nombres, vecteurs, fonctions numériques etc. est si universelle, qu'il est judicieux de comprendre, justement, la structure d'espace vectoriel.

Il est évident que ce texte est fortement inspiré des « maths modernes » qui étaient au programme il y a 60 – 40 ans. Il est

sans-doute vrai que ce programme n'a pas plu à certaines personnes, et c'est sans-doute la raison pour laquelle ce programme a été abandonné. Cependant, ce même programme a ouvert des horizons pour beaucoup d'autres personnes (y compris moi-même et certains de mes camarades). Alors, pourquoi priver les personnes pour qui cela peut être bénéfique ? Cet ouvrage veut contribuer à redonner cette possibilité à ceux qui en peuvent tirer profit (comme c'était le cas de beaucoup d' élèves à l'époque).

Cela dit, répétons-nous, les notions abordées dans cet ouvrage, « structures », ne sont pas nécessaires pour comprendre le programme du lycée d'aujourd'hui ; ceci contrairement aux notions abordées dans « ensembles ». Le texte est peut-être aussi un peu plus dur à assimiler que le texte « ensembles », car le niveau d'abstraction monte d'un cran. Cependant, autant que je crois que la notion d'ensemble est essentielle, la notion de structure est optionnelle mais très bénéfique dans la compréhension du programme du lycée, et était parfaitement assimilable il y a 40 ans.

Patrick Van Esch

Table des matières

Introduction aux structures

Une structure est une forme d'abstraction en mathématiques qui est inspirée par le fait que des objets mathématiques différents **se comportent de la même façon** et nous voulons étudier cette « façon de se comporter », sans se lier à un objet mathématique spécifique.

Par exemple, l'addition de nombres naturels, l'addition de nombres rationnels, et l'addition de nombres réels se ressemblent. L'addition de vecteurs ressemble à l'addition des nombres réels. L'union d'ensembles ressemble à l'addition des nombres naturels. Il y a des « règles de calcul » qui s'appliquent à toutes ces additions. Mais il y a aussi des différences, et un vecteur n'est pas un nombre naturel. Cependant, si nous voulons étudier ce qui est universel à cette notion d' « opération d'addition », nous voulons faire abstraction des objets spécifiques (nombres entiers, nombres réels, vecteurs…) qui sont additionnés afin d'*étudier la notion d'addition de façon abstraite*.

La notion de « plus petit que » parmi les nombres, et la notion « est sous-ensemble de » impliquent tous les deux une propriété d'ordre qu'on veut pouvoir étudier de façon abstraite sans se fixer sur des nombres ou des ensembles spécifiques.

La notion de «convergence» qui est introduite avec des suites numériques, est bien plus universelle que sa seule application dans les suites numériques.

L'idée de structure est de retenir ce qui est essentiel et universel dans *le comportement* certaines notions, indépendamment de leur incarnation dans un système spécifique : c'est de se demander ce qui est « universel » dans l'addition, indépendamment si on considère l'addition de nombres naturels, de nombres rationnels, ou de vecteurs. En d'autres termes, **on essaie d'isoler le comportement essentiel de certaines idées mathématiques en faisant abstraction de leur nature précise.**

Par exemple, dans une addition, on peut toujours changer l'ordre des termes : si on fait 5 + 3 + 9, c'est égal à 9 + 3 + 5. Si on fait la somme des vecteurs u, v et w, on a que $u + v + w = w + u + v$. C'est un comportement universel d'une addition, qu'elle soit une addition de nombres, de vecteurs ou d'autres choses. Dans une addition, il y a toujours un élément qui fait que l'addition avec cet élément ne fait rien : un « zéro ». Une addition implique aussi l'existence d'une « multiplication avec un nombre naturel ». Effectivement, si on peut écrire $a + a + a + a$, il n'y a pas de raison de ne pas écrire cela comme $4.a$, même si la multiplication n'est pas définie. Et alors on obtient aussi tout de suite que $4.a + 5.a = 9.a$. C'est inévitable quand nous avons une addition, *même si on ne sait pas exactement ce que sont les choses qu'on est en train d'ajouter.*

Mais on peut aller plus loin. Les multiplications ressemblent aussi aux additions. Si on fait 5×3×9 c'est égal à 9×3×5. Il y a aussi un élément qui fait que la multiplication ne fait rien : un « un ». Une multiplication implique aussi une « puissance avec

un nombre naturel ». Si on peut écrire $a \times a \times a$, on peut aussi écrire a^3.

Comme nous voulons parler de façon abstraite de « choses à additionner » et « d'addition », nous allons pouvoir mettre à profit le fait *que toute chose en mathématiques est un ensemble*. Ainsi, les « choses à additionner » vont faire partie d'un ensemble. Et l'addition même sera aussi un autre ensemble (une relation), qui aura un lien avec le premier ensemble. Ainsi, *une structure mathématique sera donc un jeu d'ensembles et des liens entre ces ensembles*.

Pour faire une structure qui étudie la notion d'addition (et en même temps, notion de multiplication, d'union...), nous avons donc un ensemble E avec des éléments « inconnus » et une « opération » (qui est une application de $E \times E$ en E) qui possède quelques propriétés qu'on estime justement « universel » dans les additions, multiplications, unions... On donnera un nom bizarre à cette « chose », qui est donc une structure : un *monoïde commutatif*. Nous allons, par axiome, introduire des propriétés, les comportements, de cette opération (et peut-être quelques propriétés de l'ensemble E). En suite, en utilisant la méthode axiomatique, nous allons voir ce qu'on peut déduire de ces axiomes sans utiliser des informations d'une construction particulière des éléments sur lesquels ces axiomes ont application, donc sans dire que E, c'est l'ensemble des nombres réels, ou l'ensemble des vecteurs dans le plan Euclidien : *nous faisons abstraction de la nature des éléments auxquels l'addition sera appliquée*. Ainsi, ces éléments sont

axiomatiquement postulés d'exister sans que l'on précise leur nature ou leur construction.

Si nous avons, ailleurs, *construit* un ensemble (par exemple, l'ensemble des nombres rationnels) et que nous avons construit une application et nous constatons que cette application satisfait toutes les exigences de notre «opération abstraite », alors nous savons que cette addition aura aussi toutes les propriétés que nous avions déduites pour notre opération abstraite dans notre structure. Notre addition « concrète » peut avoir des propriétés en plus, qui sont spécifiques à sa construction mais qui, justement, ne font pas partie de la notion universelle d'addition/multiplication/opération.

Pour définir des structures, on s'inspire de systèmes existants, pour ensuite, essayer d'oublier le « cas particulier » qui nous a inspiré pour définir la structure en question. Nous sommes donc en plein exercice d'abstraction…

Une structure consiste d'un système d'axiomes qui postule l'existence de quelques ensembles, dont au moins un ensemble de base, et qui ont des liens particuliers. Souvent certains de ces ensembles sont des relations sur les ensembles de base de la structure. Les axiomes postulent les propriétés particulières de ces ensembles et de ces liens. Le nombre des objets postulés est restreint, et le nombre de propriétés est souvent une liste relativement petite. Les axiomes ne disent rien sur une possible construction des éléments des ensembles de base.

Une structure peut être **réalisée** par une construction existante, ce qui prouve la cohérence de la structure. La construction des nombres rationnels, par exemple, réalise l'addition abstraite par l'addition des nombres rationnels.

On peut classifier les structures les plus courantes en trois grandes familles:

- **structures algébriques** : tout ce qui concerne les calculs, les opérations...
- **structures topologiques** : tout ce qui concerne des limites, la continuité…
- **structures d'ordre** : tout ce qui concerne des relations de « plus grand que »

et puis, toutes **les combinaisons de ces structures**.

On peut, à partir de structures existantes, considérer de nouvelles structures « plus petites » ou « plus grandes ».

Certaines structures sont si universelles, qu'on leur donne un nom. Ce nom est souvent assez bizarre, comme « groupe », « monoïde », « anneau », « corps » et on ne voit pas toujours ce que ce nom (qui a une signification dans le langage courant) voudrait bien inspirer concernant la structure en question.

Nous écrivons une structure simplement par les noms du ou des ensembles de base, et les symboles représentant les ensembles structurels ou relations axiomatiques, séparés par des virgules, ou des point-virgules.

Comme c'est presque toujours le cas dans les exercices d'abstraction, les structures abstraites sont fortement inspirées par des constructions existantes, dont on a voulu « extraire l'essentiel ».

Révision

Ensembles

Nous rappelons que tout objet mathématique est un ensemble, et qu'un ensemble est défini dès qu'on peut déterminer si un élément (un autre objet mathématique) appartient à cet ensemble ou non. Pour se protéger contre des contre-sens, il faut quand-même que l'ensemble existe. S'il y a un petit nombre d'éléments dont il est déjà avéré qu'ils existent, l'ensemble fait par énumération de ces éléments, existe aussi.

Donc, **on peut toujours définir un ensemble avec une énumération d'éléments existants**.

Dans la théorie naïve des ensembles, on peut, par axiome, décider que certains objets mathématiques sont « atomiques » et ne sont pas des ensembles eux-mêmes (faisant exception à la règle que tout objet mathématique est un ensemble), mais seulement des éléments d'un ensemble postulé d'exister. Souvent, on prend les nombres naturels comme « pré-existants ». Mais dans une approche plus rigoureuse, cela n'est pas fait et ces objets sont aussi construits à partir de l'ensemble vide. Si, d'une façon ou d'une autre, nous supposons que les nombres naturels existent, on peut donc fabriquer des petits ensembles en écrivant, par exemple :

$A = \{1,6,8,115\}$

Cet ensemble existe et est bien défini.

A partir d'ensembles existants, on peut construire d'autres ensembles qui existent alors :

- En prenant des unions, intersections et différences d'ensembles existants
- En prenant le produit de deux ensembles existants
- En prenant l'ensemble des parties d'un ensemble existant

A partir d'un ensemble existant, on peut définir un sous-ensemble en utilisant un prédicat sur l'ensemble existant.

Ceci se fait en écrivant :

$$A = \{x \in U | F(x)\}$$

Ceci définit l'ensemble *A*, sous-ensemble de l'ensemble existant *U*, contenant les éléments *X* pour lesquels *F(X)* est une proposition vraie.

Relations et fonctions

Un sous-ensemble du produit $A \times B$ est une **relation** de *A* en *B* : il contient des couples *(a,b)*. Une relation est un ensemble, et peut donc être défini comme tel. Quand *A* et *B* sont le même ensemble, on parle d'**une relation interne à *A***.

Une **fonction** est une relation avec une propriété particulière : qu'aucun élément de *A* n'apparaît dans plus qu'un couple de la relation comme premier élément. Une fonction associe donc au plus un seul élément de *B* à un élément de *A*.

Des fonctions spéciales sont des surjections, des injections, et des bijections.

Des relations internes à un seul ensemble peuvent avoir des propriétés comme la réflexivité, la symétrie ou l'anti-symétrie, et la transitivité.

Une relation interne qui est en même temps réflexive, symétrique et transitive est une relation d'équivalence. Elle a la propriété qu'elle engendre une partition sur l'ensemble dans lequel elle est définie. Cette partition s'appelle **l'ensemble quotient** de l'ensemble d'origine et de la relation d'équivalence.

Une **partition** *S* d'un ensemble *A* est un ensemble de parties de cet ensemble *A*, tel que :

- chaque élément de *A* appartient à exactement un élément de *S*
- l'ensemble *{}* n'est pas un élément de *S*

L'ensemble-quotient existe si l'ensemble d'origine existe et si la relation d'équivalence existe. C'est la formalisation du processus d'abstraction, et les ensembles de nombres entiers, les nombres rationnels et les nombres réels sont construits de cette façon à partir de l'ensemble des nombres naturels.

Structures algébriques

Monoïde

Opération interne

Quand nous avons un ensemble E, on peut définir une « opération interne » sur cet ensemble. C'est **une application de $E \times E$ en E**, ce qui veut dire que deux éléments de E (un couple) sont associés « au résultat de l'opération » qui est aussi un élément de cet ensemble E.

L'exemple qui nous inspire, bien sûr, c'est l'addition et un ensemble de nombres. Un couple de nombres de l'ensemble donne lieu à « leur somme » :

$$+ : E \times E \rightarrow E : (a,b) \rightarrow a + b$$

Il peut être judicieux d'écrire l'addition dans sa notation fonctionnelle : $+(a,b)$, car la notation standard implique déjà des propriétés qu'il faut établir.

Il y a un autre exemple qui peut nous inspirer, et c'est la multiplication de nombres : un couple de nombres de l'ensemble donne lieu à « leur produit » :

$$. : E \times E \rightarrow E : (a,b) \rightarrow a.b$$

Comme nous voulons parler d'une opération « en général », il nous faut introduire de nouveaux symboles qu'on n'associe pas tout de suite à une addition ou une multiplication existante.

$\clubsuit : E \times E \rightarrow E : (a,b) \rightarrow a\clubsuit b$

Nous pouvons introduire la notation fonctionnelle standard :

$\clubsuit(a,b)$

Monoïde

Les axiomes d'un monoïde sont :

***E*, ♣ est un monoïde, si :**

1. **L'opération ♣ est une *application* sur $E \times E$**
2. **L'opération ♣ est *associative* : $\clubsuit(\clubsuit(a,b),c) = \clubsuit(a,\clubsuit(b,c))$**
3. **Il existe un *élément neutre e* en E : $\clubsuit(e,a) = \clubsuit(a,e) = a$**

E est l'ensemble de base. Notez qu'*on ne dit rien concernant cet ensemble*. **On postule qu'il existe et qu'il a des éléments, sans qu'on dise ce que sont ces éléments**. C'est justement l'essentiel d'une structure, qu'on ne spécifie rien concernant la nature des éléments du ou des ensembles de base.

Le premier axiome indique que le domaine de ♣ est bien tout $E \times E$ (il n'y a aucun couple (a,b) auquel on ne pourrait pas appliquer l'opération ♣). Souvent, quand on définit une opération, ceci est déjà implicitement supposé, mais on le dit explicitement dans les axiomes.

L'associativité veut dire qu'il ne faut pas tenir compte de l'ordre dans lequel on calcule des opérations imbriquées. Pour une addition, ceci revient à dire que si on veut faire la somme de 3, 5 et 9, il n'est pas important si on ajoute d'abord 3 et 5, pour

obtenir 8, et ensuite, d'ajouter 9, pour obtenir le résultat de 17 ; ou si on ajoute d'abord 5 et 9, pour obtenir 14, et ensuite faire la somme de 3 et de 14, pour obtenir 17.

On l'écrit mieux comme ceci :

$(a \clubsuit b) \clubsuit c = a \clubsuit (b \clubsuit c) = a \clubsuit b \clubsuit c$

L'associativité veut dire que l'opération sur plus que 2 éléments de *E* est bien définie sans qu'on ait à se soucier de l'ordre dans lequel on applique l'opération binaire.

L'écriture classique d'une opération même **avec le symbole entre les deux opérandes** (comme 5 + 8) au lieu de la notation fonctionnelle (comme +(5,8)) implique quelque part l'associativité.

L'élément neutre est un élément qui fait que « l'opération ne fait rien ». Pour l'addition, c'est 0 : 0 + 5 = 5. Faire une addition avec 0 ou ne pas faire cette addition, ne change rien. Pour la multiplication, c'est 1. Multiplier par 1 ou ne rien faire donne le même résultat.

Il ne peut y avoir qu'un seul élément neutre pour une opération donnée, car s'il y en a deux, disons, *e* et *f*, alors $\clubsuit(e,f) = e$ car *f* est neutre, mais $\clubsuit(e,f) = f$ car *e* est neutre, et donc $e = f$.

Des exemples de monoïdes sont :

- L'addition sur les ensembles de nombres naturels, entiers, rationnels et réels.

- La multiplication sur ces mêmes ensembles avec ou sans zéro.

Le monoïde permet d'introduire une opération externe : **la multiplication avec un nombre naturel** :

$. : \mathbb{N} \times E \rightarrow E : (n,a) \rightarrow .(n,a) = a \clubsuit a \clubsuit \ldots. \clubsuit a$ (n fois)

Pour $n = 0$, on définit : $.(0,a) = e$, l'élément neutre.

Si on voit ♣ plutôt comme une multiplication, alors notre opération externe est un « exposant ».

Dans le cas tout à fait particulier du monoïde de l'addition dans les nombres naturels, cette opération externe est, en fait, interne, et permet d'introduire la multiplication sur les nombres naturels. En école primaire, on apprend que la multiplication est une « addition répétée ». C'est exactement de cela qu'on parle ici, sauf que cela peut aussi s'appliquer à d'autres monoïdes que l'addition des nombres naturels.

Il y a une propriété qui semble naturelle pour toute opération, mais qui ne l'est pas automatiquement : c'est la **commutativité**. Une opération ♣ est dite commutative, si $a \clubsuit b = b \clubsuit a$; en notation fonctionnelle : si $\clubsuit(a,b) = \clubsuit(b,a)$. L'addition et la multiplication des nombres sont des opérations commutatives. Mais il existe des opérations qui ne sont pas commutatives.

Si une opération d'un monoïde est aussi commutative, on dit que nous avons **un monoïde commutatif**.

Il faut comprendre ce qu'un monoïde représente: c'est une opération qui peut se faire sur *un nombre de termes* (donc c'est

essentiellement une opération sur *n* éléments, et non seulement sur 2 éléments de *E grâce* à l'associativité), et où on peut ajouter *des « termes bidon »* (l'élément neutre). Si en plus, l'ordre des éléments n'a pas d'importance, nous avons notre monoïde commutatif. En d'autres termes, le monoïde nous permet d'avoir une opération $a \clubsuit b \clubsuit c \clubsuit d \ldots \clubsuit z$ sur *n* éléments de *E*, avec la possibilité de faufiler *m* éléments supplémentaires bidon dedans si on le souhaite, à partir d'une opération de base sur 2 éléments. C'est ce qui caractérise de façon la plus générale les opérations comme l'addition et la multiplication et c'est pour cela que nous avons la notation avec le + ou le . « entre les termes ».

Nous voici donc riche de notre première structure, et nous allons en apercevoir autour de nous… Il y en a partout !

Exemple de monoïde : *P(A)* ; ∪

Considérons un ensemble quelconque, *A*. Considérons l'ensemble des parties de *A*, *P(A)*. Si on considère l'union de deux ensembles comme une opération dans *P(A)*, c'est à dire que :

$\cup : P(A) \times P(A) \rightarrow P(A) : (x,y) \rightarrow x \cup y$

U est bien une opération interne à *P(A)* : l'union de deux parties d'un ensemble *A* est bien une partie de *A* ; et cette opération est bien une application : on peut prendre l'union de chaque couple de parties de *A*.

L'union est une opération associative :

$(x \cup y) \cup z = x \cup (y \cup z) = x \cup y \cup z$,

car pour qu'un élément a de A appartienne à ceci, il faut simplement que a appartienne à x, y ou z.

Il y a un élément neutre : l'ensemble $\{\}$. Effectivement :

$x \cup \{\} = \{\} \cup x = x$.

Notez que l'ensemble $\{\}$ appartient toujours à $P(A)$.

Ainsi, $P(A)$; $\cup$ est bien un monoïde.

Comme $x \cup y = y \cup x$, c'est **un monoïde commutatif.**

On peut remarquer que la « multiplication avec un nombre naturel » (ou l'exposant, si on veut) ne fait pas grand-chose dans ce monoïde : $x^3 = x \cup x \cup x = x$.

Exemple de monoïde : $P(A)$; $\cap$

L'intersection forme aussi **un monoïde commutatif** dans $P(A)$. Les arguments sont très similaires aux arguments pour le monoïde $P(A)$; $\cup$. La différence principale est que l'élément neutre est A cette fois, à la place de $\{\}$ pour l'union. De la même façon, l'exposant ne fait pas grand-chose dans ce monoïde.

Exemple de monoïde : composition

Considérez l'ensemble des fonctions internes à un ensemble A, $F(A)$. Dans cet ensemble de fonctions, on peut considérer l'opération « composition de fonctions» comme opération interne :

$\circ : F(A) \times F(A) \rightarrow F(A) : (f,g) \rightarrow f \circ g$

La composition est bien une **application** sur $F(A) \times F(A)$: toute fonction peut être composée avec toute autre fonction interne à A.

La composition est **associative** :

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

On peut facilement s'en convaincre, car $h \circ g \circ f\ (a) = h(g(f(a)))$. Pour finir la démonstration, il faut vérifier les domaines des fonctions.

Il y a bien **un élément neutre** : la permutation identique I sur A, tel que $I(a) = a$ pour tout a de A. La permutation identique est la permutation qui contient tous les couples (a,a).

Effectivement, $f \circ I = I \circ f = f$.

Ainsi, $F(A)$; $\circ$ est bien un monoïde.

Mais $\circ$ n'est pas commutatif. Pour s'en rendre compte, on peut s'imaginer la fonction $f(x) = 2\ x$ et $g(x) = x + 1$ dans l'ensemble des nombres naturels. $g(f(x)) = 2\ x + 1$; $f\ (g(x)) = 2\ x + 2$ par contre.

L'exposant de la composition est bien utile dans ce monoïde :

$f^3 = f \circ f \circ f$ par exemple.

Si $f(x) = 2x+1$, alors $f^2(x) = 2(2x+1) + 1 = 4x+3$ et $f^3(x) = 2(4x+3) + 1 = 8x + 7$. Attention : souvent, quand on écrit $f^3(x)$, on ne veut pas dire « l'exposant dans le monoïde de composition », mais simplement $(f(x))^3$ dans le monoïde de la

multiplication de nombres. A force d'avoir des monoïdes partout, on pourrait se tromper sur lequel on veut utiliser avec des notations abusées.

Effectivement, si on considère le monoïde de composition, $f^3(x)$ veut bien dire $f(f(f(x)))$, mais si on considère le monoïde de la multiplication des nombres, et l'image $f(x)$ en fait partie, alors il faudrait écrire $(f(x))^3$ et non $f^3(x)$, mais souvent, on le fait quand-même, et par cette dernière notation, on veut donc dire $f(x).f(x).f(x)$.

Contre-exemple : la soustraction des entiers

Un contre-exemple, pour illustrer ce qui n'est pas un monoïde, est la soustraction des entiers. La soustraction des entiers est bien une opération interne (elle existe pour tous les couples d'entiers : on peut soustraire n'importe quel entier de n'importe quel entier), mais c'est une opération qui est ni associative, ni commutative. Elle possède un élément neutre « à droite » mais pas « à gauche » : 5 – 0 = 5 ; mais 0 – 5 n'est pas 5.

5 – 3 – 8 pose problème de son interprétation : (5 – 3) – 12 n'est pas la même chose que 5 – (3 – 12). Par convention, on opère « de gauche à droite », mais alors que cette convention n'est pas nécessaire dans un monoïde, elle l'est pour la soustraction. La « soustraction à n éléments » n'existe pas vraiment : on va soustraire les $n-1$ derniers éléments du premier, qui a donc un statut particulier. La soustraction sépare le premier élément de tous les autres.

S’entraîner

1. Considérez l'ensemble des nombres naturels, avec comme opération sur deux nombres, le maximum des deux nombres. C'est à dire, max(2,5) = 5 ; max(8,3) = 8. ℕ,max, est-il un monoïde ? Un monoïde commutatif ? Que fait la « multiplication avec un nombre naturel » dans ce monoïde ?

2. Même question, mais avec «le minimum des deux nombres ». Est-ce un monoïde ? Un monoïde commutatif ?

3. Considérez l'ensemble des nombres naturels sans 0, avec comme opération : le plus petit multiple commun. Est-ce un monoïde ? Peut-on inclure le zéro dans l'ensemble de base ?

4. Quel est le plus petit monoïde que vous pouvez vous imaginer ? Suggestion : {} n'est pas un monoïde ! (pourquoi?) Quel est l'ensemble de base et quelle est l'opération (vue comme ensemble de couples) ? Est-ce que ce monoïde est commutatif ?

Groupe

Élément inverse

Nous rappelons que les nombres naturels avec l'addition forment un monoïde. Ce qui nous avait inspiré pour introduire les nombres entiers, était le fait que « l'opération inverse » de l'addition ne fonctionnait pas toujours avec l'addition des nombres naturels. Quand on fait une addition, 5 + 3 = 8, on peut se poser la question :« quel est le nombre qu'il faut ajouter à 5 pour obtenir 8 ? », et on écrit cette question : 8 – 5. Ceci

introduit donc une nouvelle opération : -, **la soustraction**, qui va de $\mathbb{N} \times \mathbb{N}$ vers $\mathbb{N}$: - (8,5) = 3, de la même façon que +(2,4) = 6. Mais, contrairement à +, - n'est pas une application, mais une fonction. Car -(5,8) n'existe pas. Il n'y a pas de nombre naturel, qu'on peut additionner à 8, pour obtenir 5. Pour que cette fonction devienne une application, nous avons inventé les nombres entiers : -(5,8) existe bel et bien dans les entiers, c'est -3. Le nombre qu'il faut ajouter à 8 pour obtenir 5, est -3.

On pourrait croire qu'il faut avoir une « solution de la soustraction » pour tout *couple* de nombres, mais les propriétés de monoïde font en sorte qu'**il suffit d'avoir une soustraction de l'élément neutre**. Effectivement, si nous avons le nombre qu'il faut ajouter à 8 pour obtenir 0, on peut, en même temps, obtenir le nombre qu'il faut ajouter à 8 pour obtenir 5 :

$x + 8 = 0$

alors

$5 + (x + 8) = 5 + 0 = 5$

$(5 + x) + 8 = 5$

$5+x$ est donc le nombre que nous cherchons, qui, ajouté à 8, donne 5. Si nous avons x, alors nous pouvons bien sûr trouver $5+x$. Ce qu'il fallait démontrer. Notez que nous avons utilisé les propriétés de monoïde (associativité, élément neutre, et le fait que 5+x existe si x existe), mais que nous n'avons pas utilisé la commutativité.

Il suffit donc d'avoir une solution pour toute équation $x + a = 0$, pour avoir une solution pour toute soustraction.

Quand nous généralisons cela à un monoïde en général, nous introduisons « l'élément inverse » par axiome :

***x* est l'élément inverse de *a* dans un monoïde *A*, ♣ si :**

a* ♣ *x* = *e* = *x* ♣ *a

où *e* est l'élément neutre ; on le note aussi : *-a*.

Si un élément inverse de *a* existe, il est unique (exercice).

Groupe

Les axiomes du groupe sont :

Un groupe est un monoïde dont tout élément a un inverse.

Un groupe commutatif, ou groupe Abélien, est un monoïde commutatif, dont tout élément a un inverse.

Des exemples de groupes Abéliens sont :

- Les nombres entiers et l'addition
- Les nombres rationnels, et l'addition
- Les nombres réels, et l'addition
- Les nombres rationnels sans zéro, et la multiplication
- Les nombres réels sans zéro et la multiplication

Notez qu'il faut exclure zéro des ensembles de nombres si on veut considérer la multiplication dans un groupe, car zéro n'a pas d'inverse pour la multiplication.

Nous avons vu que le monoïde caractérise l'idée générale de « opération sur *n* éléments ». Le groupe, lui, caractérise *la*

réversibilité de l'opération. Contrairement à un monoïde en général, où ce n'est pas toujours possible « d'aller partout et de revenir », avec un groupe, *on peut aller de n'importe quel élément à n'importe quel autre élément (et revenir si on veut)*.

L'addition des nombres naturels, ou l'union d'ensembles, ne permet pas « de revenir en arrière » : c'est un monoïde. Ajouter un nombre naturel est « irréversible » ; faire l'union de deux ensembles est « irréversible ». Par contre, dans un groupe, on peut donc « faire marche arrière ». Aussi, on ne peut pas aller de 8 à 5 avec une addition naturelle par exemple. On ne peut pas aller d'un ensemble à 2 éléments vers l'ensemble vide avec une union. Dans un groupe, par contre, on peut aller « n'importe où ».

Le groupe a deux grandes applications : la résolution d'équations, et les opérations de symétrie. Allons à la découverte de groupes autour de nous...

Exemple de groupe : permutations

Considérez un ensemble existant, *A*. Considérez l'ensemble *G* des permutations sur *A*. Cet ensemble existe, car c'est une partie de l'ensemble de toutes les fonctions de *A* en *A*.

L'ensemble *G* et *l'opération de composition* ◦ est un groupe, et ce n'est pas un groupe Abélien. Le groupe des permutations (et les sous-groupes ; on y viendra) est une notion très riche en mathématiques.

Prenez comme exemple : $A = \{1,2,3\}$. Il y a 6 permutations sur cet ensemble :

p1 = {(1,1),(2,2),(3,3)}

p2 = {(1,2),(2,3),(3,1)}

p3 = {(1,3),(2,1),(3,2)}

p4 = {(1,3),(2,2),(3,1)}

p5 = {(1,2),(2,1),(3,3)}

p6 = {(1,1),(2,3),(3,2)}

p1 est l'élément neutre, et *p2* est l'inverse de *p3*. Les permutations *p4*, *p5*, et *p6* sont des involutions (leurs propres inverses).

L'ensemble *G* est *{p1, p2, p3, p4, p5, p6}*. *G* avec la composition est bien un groupe.

Il est intéressant de remarquer que ces 6 permutations correspondent aux **6 opérations de symétrie** qu'on peut appliquer à un triangle équilatéral dont les sommets s'appellent 1, 2 et 3. Par exemple, *p2* représente une rotation de 120 dégrées, et *p3* représente la rotation dans l'autre sens. Les permutations *p4*, *p5* et *p6* représentent une réflexion dans un axe de symétrie ; *p4* par exemple représente la réflexion dans l'axe qui passe par le sommet numéro 2.

Les opérations de symétrie de n'importe quel objet forment toujours un groupe avec la composition.

Sous-groupe

Si *E ;* ♣ est un groupe, et *A* est une partie de *E*, et *A ;* ♣ est aussi un groupe, alors on dit que *A ;* ♣ est un sous-groupe de *E ;* ♣

Quelques exemples de sous-groupes : Les nombres entiers avec l'addition sont un sous-groupe des nombres rationnels avec l'addition et sont aussi un sous-groupe des nombres réels avec l'addition. Les nombres rationnels avec l'addition sont un sous-groupe des nombres réels avec l'addition.

Le groupe *{p1,p5}* avec la composition est un sous-groupe du groupe de permutations que nous avons vu dans la précédente sous-section, ainsi que le groupe *{p1,p2,p3}*.

Si *E*, ♣ est un groupe, *e* est son élément neutre et *a* est un autre élément quelconque, alors il est toujours possible de construire **un sous-groupe commutatif généré par *a***. Considérons l'ensemble :

$$A = \{x \in E | \exists n \in \mathbb{N} : x = n.a \vee x = n.(-a)\}$$

Nous avons utilisé ici la « multiplication induite » dans un monoïde, où par exemple, *5.a* veut dire *a* ♣ *a* ♣ *a* ♣ *a* ♣ *a*. Notez que *0.a = e*.

En d'autres termes, l'ensemble *A* est l'ensemble de toutes les opérations possible de *a* avec lui-même, ou de toutes les opérations de l'élément inverse de *a* avec lui-même.

Il est facile d'établir que *A*,♣ est un groupe. Que c'est un monoïde est facile à établir. L'associativité est établie, et si

nous avons deux éléments x et y, alors $x \clubsuit y$ appartient aussi à A, car :

$x = n.a$ ou $x = n.(-a)$

$y = m.a$ ou $y = m.(-a)$

Premier cas :

$x = n.a$ et $y = m.a$, alors $x \clubsuit y = (n+m).a$

Deuxième cas :

$x = n.(-a)$ et $y = m.(-a)$, alors $x \clubsuit y = (n+m).(-a)$

Troisième cas :

$x = n.a$ *et* $y = m.(-a)$ et $n > m$, alors $x \clubsuit y = (n - m).a$

Quatrième cas :

$x = n.a$ et $y = m.(-a)$ et $n < m$, alors $x \clubsuit y = (m - n).(-a)$

etc.

La commutativité est aussi facile à établir, de la même façon d'ailleurs. Finalement, tout élément de A a son inverse dans A.

Il se peut qu'une certaine répétition de a est égale à l'élément neutre : qu'il existe un nombre naturel, N, tel que $N.a = e$. Nous avons alors aussi que $N.(-a) = e$.

Dans ce cas, **le groupe est dit cyclique**.

Considérons notre groupe de permutations. Si nous choisissons comme élément générateur, $p2$, nous avons que :

$1.p2 = p2$

2.p2 = p3

3.p2 = p1 (élément neutre)

-p2 = p3

2.(-p2) = p2

3.(-p2) = p1 (élément neutre)

Ce groupe est cyclique et contient 3 éléments : *{p1, p2, p3}*.

Notez que même si le groupe des permutations n'est pas un groupe commutatif, ce sous-groupe est bien commutatif, car c'est un groupe généré par un seul élément.

Un autre exemple : considérez le groupe des entiers avec l'addition. L'élément neutre est 0. Considérez maintenant l'élément 5. Le groupe commutatif généré par 5 n'est rien d'autre que l'ensemble des multiples de 5. Cet ensemble de multiples de 5, avec l'addition, est aussi un groupe commutatif. On le note $5\mathbb{Z}\ ;\ +$.

Encore un autre exemple : considérez le groupe des fractions sans zéro, et la multiplication. L'élément neutre est 1. Prenez l'élément 7. Le groupe commutatif généré par 7 est l'ensemble des puissances de 7 et de 1/7.

S’entraîner

1. Démontrez que dans un groupe non-commutatif *G,**, nous avons : 1 */(u * v) = 1/v * 1/u* (dans cet ordre). Appliquez cela au groupe des permutations de l'ensemble {1,2,3} comme dans

le texte précédemment, et vérifiez que l'inverse de *(p4 ◦ p2)* suit bien cette propriété.

2. Démontrez qu'un élément d'un groupe ne peut avoir qu'un seul élément inverse. Suggestion : *v* u = u*v = 1 = u*w = w*u* ; multipliez *u*v = u*w* à gauche avec *v*.

3. Démontrez la commutativité d'un groupe généré par *a*.

4. Est-ce que, dans le groupe des fractions sans zéro et la multiplication standard, le groupe généré par 49 est un sous-groupe du groupe généré par 7 ?

5. Quel est le plus petit groupe que vous pouvez vous imaginer ? Est-ce que ce groupe est commutatif ?

Anneau et corps

Les structures que nous avons vues jusqu'ici, monoïde, groupe, et leurs versions commutatives, consistent d'un ensemble et *d'une* opération interne. Nous allons maintenant considérer des structures avec un ensemble et *deux opérations internes*. Les opérations ne sont pas « interchangeables », il y a une première opération, dite « additive », et une deuxième, dite « multiplicative ». Nous allons noter la structure : *E,*♣,♠

Distributivité

Les deux opérations sont dites « distributives », si :

a ♠ *(b* ♣ *c) = (a* ♠ *b)* ♣ *(a* ♠ *c)*

et

(b ♣ c) ♠ a= (b ♠ a) ♣ (c ♠ a)

Notez que si les opérations sont commutatives, ces deux propriétés sont les mêmes. Il faut noter que *c'est la deuxième opération, l'opération « multiplicative » qui se distribue » sur la première, l'opération « additive »*. L'inverse n'est pas demandée.

C'est bien sûr l'équivalent abstrait de la propriété de distributivité dans les nombres : 5.(3+9) = 5.3 + 5.9.

L'addition et la multiplication des nombres est distributive.

Notez aussi que, dans l'ensemble des parties de *A*, *P(A)*, l'union et l'intersection sont distributives :

$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

Anneau

Les axiomes de l'anneau sont :

Un anneau est une structure qui consiste d'un ensemble *E*, et deux opérations ♣ (additive) et ♠ (multiplicative), tel que :

1. ***E*, ♣ est un groupe Abélien (groupe commutatif)**
2. ***E*, ♠ est un monoïde**
3. **♣,♠ sont des opérations distributives**

Si *E*, ♠ est un monoïde commutatif, on dit que l'anneau est un anneau commutatif.

Dans un anneau, l'élément neutre de la première opération s'appelle **l'élément nul ou zéro,** et l'élément neutre de la deuxième opération s'appelle **l'élément unité**. Il n'y a qu'un seul anneau dans lequel l'élément nul et l'élément unité sont le même : c'est l'anneau trivial avec un seul élément {0}.

L'anneau (commutatif) le plus connu est l'anneau des nombres entiers, avec l'addition et la multiplication standard.

La structure de l'anneau est introduite, car il y a tellement de constructions mathématiques qui correspondent à cette structure que son étude en général est utile. Par exemple, le calcul des matrices carrées est un anneau (non-commutatif). *Presque partout*[1] *où on a la combinaison de quelque chose qui est « une addition » et quelque chose qui est « une multiplication », on obtient un anneau.*

Un anneau *commutatif* engendre la plupart des règles de calcul algébriques qu'on connaît des nombres, et en particulier, l'existence des *polynômes*. **L'ensemble des polynômes même, équipé d'une addition et une multiplication, sera d'ailleurs aussi un anneau commutatif.** Cet anneau de polynômes est noté *A[X]*, si *A* était le nom de l'ensemble de base de l'anneau de départ. Par exemple, $\mathbb{Z}[X]$ est l'anneau des polynômes sur

1 En réalité, il y a une structure moins exigeante que l'anneau qui incarne mieux la notion « basique » du binôme « addition - multiplication », le demi-anneau. Effectivement, l'addition et la multiplication des nombres naturels ne forme pas un anneau, mais un demi-anneau. L'union et l'intersection forment aussi un demi-anneau. Nous devons nous limiter dans ce texte, cependant, à un nombre limité de structures et nous ne traiterons donc pas le demi-anneau, mais essentiellement, c'est un anneau, où la première exigence de groupe commutatif change en monoïde commutatif.

les entiers (avec, donc, des coefficients entiers). On peut quelque part dire que l'anneau et les polynômes, même combat.

Anneau des entiers modulo *n*

Un anneau très important est celui des nombres entiers modulo *n*. L'ensemble de base consiste en les nombres 0, 1, 2, … *n – 1*. L'addition est définie comme l'addition traditionnelle, modulo *n*. **Modulo *n*** veut dire : on prend le reste quand on fait la division Euclidienne par *n*. 9 modulo 8 est 1. 3 modulo 8 est 3. 50 modulo 8 est 2. Notez que cela marche aussi pour les entiers négatifs : -2 modulo 8 est 6, car le plus grand multiple de 8 qui est plus petit que -2, est -8, et il reste donc 6. « modulo *n* » donne toujours un résultat de 0 à *n* – 1.

Par exemple, si nous prenons *n* = 8, alors 2 + 4 est bien 6 comme l'addition traditionnelle ; par contre 5 + 6 devient 3, car 5 + 6 est 11, et 11 modulo 8 est 3. De la même façon, la multiplication est comme la multiplication traditionnelle, modulo *n*. Ainsi, 5 . 6 est 6, car 5 . 6 est 30, et 30 modulo 8 est 6.

On peut facilement constater que l'addition modulo *n* forme un groupe commutatif sur notre ensemble avec *n* éléments. C'est un exercice pour le lecteur. La multiplication modulo *n* forme un monoïde commutatif sur cet ensemble, comme le lecteur pourra prouver. La distributivité de l'addition et la multiplication reste valable aussi quand on prend le résultat « modulo ».

Ainsi, l'ensemble {0, 1, … *n*-1}, et l'addition et la multiplication « modulo *n* », forment un anneau commutatif.

Corps

Un corps est un « anneau amélioré » ; les axiomes d'un corps sont :

Un corps est une structure qui consiste d'un ensemble *E*, et deux opérations ♣ (additive) et ♠ (multiplicative), tel que :

1. ***E*, ♣ est un groupe Abélien (groupe commutatif) avec 0 comme élément neutre**
2. ***E* \ {0}, ♠ est un groupe**
3. **♣,♠ sont des opérations distributives**

Si *E* \ {0}, ♠ est un groupe *commutatif*, on dit que le corps est un corps *commutatif*.

Un corps est donc un anneau, où la deuxième opération a un élément inverse pour tout élément sauf l'élément nul. Il y a donc une soustraction et une division (sauf par zéro) dans un corps.

Le corps est la structure algébrique qui permet de résoudre l'équation linéaire : $a.x+b = 0$. Par extension, **c'est la structure qui permet de résoudre un jeu d'équations linéaires en *n* inconnus**.

Les corps commutatifs les plus connus sont l'ensemble des nombres rationnels, avec l'addition et la multiplication, et celui

des nombres réels. Les nombres complexes forment aussi un corps commutatif.

Dans un corps commutatif, toutes les règles d'algèbre (les techniques pour résoudre des équations – tant qu'elles n'utilisent que les 4 opérations de base, les produits remarquables, ...) qu'on connaît d'habitude, sont valables.

Cependant, il faut faire attention à ne pas trop généraliser : il y a des règles de calcul dont nous avons l'habitude de les utiliser, et qui ne sont pas liées aux axiomes du corps, mais qui dépendent des détails des nombres utilisés. La solution de l'équation quadratique en est un exemple. Nous allons regarder cela d' un peu plus près pour les trois corps commutatifs qu'on connaît bien au lycée : les nombres rationnels, les nombres réels, et les nombres complexes.

Considérons l'équation du deuxième degré :

$$a\,x^2+bx+c=0$$

La solution « algébrique » est :

$$x_1=\frac{-b+\sqrt{b^2-4\,a\,c}}{2\,a} \quad \text{et} \quad x_2=\frac{-b-\sqrt{b^2-4\,a\,c}}{2\,a}$$

Ici, le symbole « racine carrée » veut dire que ce nombre, multiplié avec lui-même, donne ce qui se trouve sous le symbole. *Le corps ne garantit pas une solution à ce problème*. Par contre, dans l'hypothèse où ce nombre existe, alors la solution est algébriquement correcte.

Considérons l'équation $4\,x^2+5\,x+1=0$

Nous avons que $b^2 - 4ac = 25 - 4.4.1 = 25 - 16 = 9$.

Dans les nombres rationnels, aussi bien que dans les nombres réels ou complexes, il y a une solution pour la racine carrée de 9 : c'est 3. Ainsi, dans les nombres rationnels, réels, et complexes, notre équation quadratique possède deux solutions : 1/4 et -1.

Mais considérons maintenant l'équation $5x^2+5x+1=0$

Maintenant, nous avons : $b^2 - 4ac = 25 - 4.5.1 = 25 - 20 = 5$

Dans les nombres rationnels, 5 n'a pas de racine carrée. Il n'y a aucun nombre rationnel dont la multiplication avec lui-même donne 5 comme résultat. Cette équation quadratique n'a donc pas de solution dans les nombres rationnels. Par contre, 5 a bien une racine carrée dans les nombres réels (et donc aussi dans les nombres complexes). Il y a donc bien deux solutions dans les nombres réels et complexes.

Finalement, nous considérons l'équation $5x^2+4x+1=0$

Cela donne : $b^2 - 4ac = 16 - 4.5.1 = 16 - 20 = -4$

Cette fois, la racine carrée de -4 n'existe pas, ni dans les nombres rationnels, ni dans les nombres réels. Par contre, elle existe dans les nombres complexes. Nous n'avons donc pas de solution de notre équation quadratique dans les nombres rationnels, ni dans les nombres réels, mais on a nos deux solutions dans les nombres complexes.

Ainsi, les solutions d'une équation quadratique dépendent de l'existence, dans l'ensemble en question, de la racine carrée

d'un nombre, et cette existence n'est pas déterminée par la structure du corps (commutatif), mais par des spécificités autres de la construction mathématique en question. Par contre, si cette racine carré existe, alors ce sont les règles de calcul du corps commutatif qui dictent la forme des solutions. Il ne peut pas y avoir un corps commutatif où la solution d'une équation quadratique aurait une autre formule que celle qu'on vient d'énoncer et qui en est la solution classique, car cette solution est obtenue par des manipulations algébriques (c.a.d. avec les 4 opérations de base : +, -, . et /). Mais cette solution dépend de l'existence (ou non) d'une racine carrée et cette solution n'est pas garantie par la structure d'un corps commutatif et dépend donc des autres propriétés de la construction mathématique en question (ici, donc, si on utilise des nombres rationnels, réels ou complexes).

Un autre exemple très important, est le corps commutatif « modulo *p* ». **L'anneau commutatif « modulo *n* » devient un corps commutatif si *n* est un nombre premier *p*.**

La preuve est basée sur *le théorème de Bezout*, qui dit que le plus grand diviseur commun *pgdc(a,b)* de deux nombres naturels, *a*, et *b*, peut s'exprimer par une combinaison des nombres *a* et *b* :

$pgdc(a,b) = s.a + r.b$

avec *s* et *r* des nombres entiers.

Si nous acceptons ce théorème sans preuve, il en suit que si *p* est un nombre premier, alors chaque nombre de 1 à $p - 1$ a un réciproque sous la multiplication modulo *p*. Effectivement,

prenons un nombre quelconque x entre 1 et $p - 1$. Comme p est un nombre premier, le plus grand diviseur commun de x et de p est 1. En appliquant le théorème de Bezout :

$1 = s \, . \, x + r. \, p$

Si nous utilisons les opérations « modulo p », le dernier terme n'a pas d'importance, et nous obtenons, modulo p, que $1 = s.x$. En d'autres termes, s est bien le réciproque de x. Ainsi, tout nombre de 1 à p-1 aura un réciproque pour la multiplication modulo p, et donc, nous avons bien un corps (commutatif).

On peut d'ailleurs étudier l'équation quadratique dans un tel corps. Considérons par exemple l'équation quadratique :

$x^2 + x + 1 = 0$

Comme nous avons un corps commutatif, les solutions classiques sont toujours valables, à condition que la racine carrée existe. Ici, le discriminant $D = b^2 - 4 \, a \, c = (-3) \bmod p$. Si p est 3, alors $D = 0$ et il a une racine carrée : 0. Les deux solutions se confondent. Si $p = 5$, $D = 2$ et on peut vérifier qu'il n'y a pas de racine carrée : $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$. Les seuls nombres avec $p = 5$ qui ont des racines carrées sont donc 0, 1 et 4. 2 n'a pas de racine carrée. Par contre, pour $p = 7$, nous avons que $D = 4$, et on peut vérifier que $2^2 = 4$, donc que 2 est bien une racine carrée de D : il y aura donc 2 solutions. Nous voyons de nouveau clairement que, pour des corps différents (des valeurs de p différents), une même équation peut avoir des solutions ou non, mais que la forme algébrique (la formule) de la solution est fixée par la structure du corps.

S'entraîner

1. Démontrez que l'ensemble des polynômes sur un anneau commutatif $A,+,*$, avec une addition et multiplication naturelle, forme bien un anneau commutatif.

2. Considérez l'ensemble $F(\mathbb{R})$ des fonctions internes à $\mathbb{R}$ (donc les fonctions numériques réelles). Est-ce qu'on peut considérer une addition et une multiplication de ces fonctions tel que F, avec ces opérations, forme un anneau (commutatif) ? (suggestion : pensez élément inverse pour l'addition) Et si on se limitait à des applications ?

3. Considérez un ensemble X quelconque, et considérez $A,+,*$ un anneau. Considérez l'ensemble des applications $F(X \to A)$ de X en A, et équipez cet ensemble d'une addition et une multiplication de la façon suivante :

$(f+g)(x) = f(x) + g(x)$ et le domaine de $f+g$ est l'intersection des domaines de f et de g ;

$(f*g)(x) = f(x)*g(x)$ et le domaine de $f*g$ est l'intersection des domaines de f et de g.

Alors, vérifiez que $F(X \to A),+,*$ est un anneau.

Espace vectoriel

Un espace vectoriel est une structure qui contient deux ensembles de base : K (les **scalaires**) et V (les **vecteurs**), et qui possède 4 opérations. Une de ces opérations est une opération externe : la multiplication scalaire.

L'espace vectoriel est bien sûr inspiré des vecteurs dans la géométrie Euclidienne. D'une certaine façon, *on peut dire que la géométrie Euclidienne est remplacée dans les mathématiques contemporaines, par l'espace vectoriel*. Les « scalaires » seront les nombres réels, et les « vecteurs » seront les vecteurs du plan Euclidien. La multiplication scalaire n'est alors rien d'autre que la multiplication d'un nombre avec un vecteur : cela change sa longueur (et éventuellement son sens si le nombre est négatif), mais ne change pas sa direction.

Mais l'utilité de la structure de l'espace vectoriel dépassera largement celle de la géométrie Euclidienne et formera la base de toute une branche des mathématiques : **l'algèbre linéaire**.

Opération externe

Une opération *interne* était une application de $E \times E$ en E. Une opération *externe* sera une application où les ensembles ne sont pas tous les mêmes. Dans le cas du produit *externe* qui nous intéresse pour les espaces vecteurs, c'est : $E \times V$ en V.

Espace vectoriel : axiomes

Un espace vectoriel est une structure qui a :

1. Un corps K, avec son addition + et sa multiplication *
2. Un groupe commutatif V, avec son addition +
3. Une **multiplication scalaire** « . »de $E \times V$ en V, tel que :
    1. pour a,b en K, et pour v en V : $a.(b.v) = (a*b).v$

2. pour 1 dans K, et pour v en V : $1.v = v$
3. pour a en K, et u, v en V : $a.(u + v) = a.u + a.v$
4. pour a et b en K, et u en V : $(a+b).u = a.u + b.u$

Souvent, mais pas nécessairement, le corps K est commutatif.

L'espace vectoriel est la structure qui décrit « la combinaison linéaire », c.a.d. des objets qu'on peut non seulement additionner, mais aussi « changer de taille » avec un « coefficient ». C'est effectivement ce qu'on entend par « un vecteur » : un truc qu'on peut additionner à un autre, mais aussi, qu'on peut « agrandir », c.a.d. multiplier avec un coefficient. La « multiplication avec un coefficient » est, justement, la multiplication scalaire.

La définition ancestrale de « vecteur » est une flèche, c.a.d. « un truc avec une direction et une longueur ». La multiplication scalaire peut changer la longueur, mais ne peut pas changer la « direction ». *C'est ce qui distingue un espace vectoriel d'un corps* : dans un corps, la multiplication peut « modifier » n'importe quel élément du corps (sauf zéro) en n'importe quel autre élément du corps. La multiplication scalaire dans un espace vectoriel est plus restreinte : elle ne peut modifier que « la longueur », mais ne peut pas changer n'importe quel vecteur en n'importe quel autre vecteur. Alors, les vecteurs en V ont bien quelque chose qui leur est « propre », ce qu'on peut voir comme une généralisation de la notion de « direction » qui n'est pas modifiable par la multiplication scalaire. La partie « modifiable » par la multiplication scalaire sera donc la généralisation de leur « longueur ». **Nous voyons**

donc que la structure de l'espace vectoriel a généralisé cette idée de la combinaison de « longueur » et de « direction ».

Il est clair que la première application de l'espace vectoriel est **dans la géométrie Euclidienne**. Les vecteurs sont les « flèches » qui vont de l'origine à tous les « points de l'espace », donc les vecteurs du style $\overline{OA}$. On peut considérer l'espace comme le plan Euclidien, ou l'espace tri-dimensionnel. L'ensemble de ces flèches forment un groupe commutatif sous l'opération de composition de vecteurs par la règle du parallélogramme. Mais on peut multiplier ces vecteurs avec un coefficient qui est un nombre réel, et que le résultat est aussi un vecteur. Ainsi, une droite qui passe par l'origine, c'est l'ensemble de toutes les flèches qui sont tous les multiples réels d'une flèche donnée : $k.\overline{OA}$. Ce sont, en fait, l*es vecteurs qui ont la même direction,* mais des longueurs différentes. Une droite quelconque, c'est une droite qui passe par l'origine, plus un autre vecteur $k.\overline{OA} + \overline{OB}$. Un plan qui passe par l'origine, c'est tous les vecteurs qui sont, justement, la somme d'un multiple d'un vecteur et le multiple d'un autre vecteur : $k.\overline{OA} + l.\overline{OB}$. Un plan quelconque, c'est un plan qui passe par l'origine, plus un autre vecteur : $k.\overline{OA} + l.\overline{OB} + \overline{OC}$.

Mais cette idée de « combinaison linéaire » est bien plus riche que juste cette application de géométrie. Effectivement, considérons les applications d'un ensemble A dans les nombres réels. L'ensemble de ces applications forme un groupe sous l'addition réelle : si f et g sont des applications de A en $\mathbb{R}$, alors $f + g$ est aussi une application de A en $\mathbb{R}$. Il en est de même

pour une multiplication avec un nombre réel *a* : *a.f* est aussi une application de *A* en $\mathbb{R}$. Ainsi, les applications de *A* en $\mathbb{R}$ forment un espace vectoriel sur le corps $\mathbb{R}$. Les applications prennent ici la place des « vecteurs ». Si *A* est l'ensemble des nombres naturels, alors ces applications sont les suites réelles. Les suites réelles forment donc un espace vectoriel sur le corps des nombres réels. Si *A* est l'ensemble des nombres réels, alors nous parlons des applications numériques, et ces applications numériques forment donc un espace vectoriel sur le corps réel. Nous constatons donc qu'il y a beaucoup d'espaces vectoriels autour de nous, et que c'est une notion qui va bien au-delà de l'utilisation dans la géométrie Euclidienne : *partout où on peut faire des « combinaisons linéaires », c.a.d. des sommes avec des coefficients, nous avons un espace vectoriel.*

Si on a un corps *K*,+,* avec son groupe additif, *K*,+ (partie de la définition du corps), alors *K* (comme corps) et *K* (comme groupe commutatif) forment toujours un espace vectoriel.

Par exemple : nous pouvons considérer le corps des nombres rationnels. Mais ce corps possède un groupe commutatif : les nombres rationnels et l'addition. Si on considère ce groupe comme le « groupe des vecteurs », alors la multiplication traditionnelle peut faire office aussi de multiplication scalaire entre un nombre rationnel (du corps) et un nombre rationnel (vecteur). On peut se demander à quoi bon. Effectivement, il n'y a rien qu'on peut faire dans cet espace vectoriel, qu'on ne pouvait pas déjà faire dans le corps en question. La raison c'est

que cette étape prépare une notion bien plus utile : l'espace vectoriel des coordonnées.

Espace vectoriel : espace coordonnées

La construction « triviale » de l'espace vectoriel par un corps et son propre groupe commutatif peut être étendue de la manière suivante. Au lieu de considérer le groupe commutatif $K,+$ du corps tout seul, on peut considérer le groupe commutatif produit :

$K \times K, +$

Le produit de deux groupes commutatifs est défini comme :

$(A, +) \times (B, +)$, devient $A \times B$, + avec une nouvelle addition de couples :

$(a,b) + (c,d) = (a+c,b+d)$.

On peut facilement constater que $A \times B$, + est un groupe commutatif en soi.

Par exemple, l'associativité :

$[(a,b) + (c,d)] + (e, f) = ([a + c] + e , [b + d] + f)$

Ceci devient, par l'associativité dans les deux groupes :

$(a + [c + e] , b + [d + f])$ ce qui n'est rien d'autre que :

$(a,b) + [(c,d) + (e,f)]$

et donc, l'associativité dans le groupe produit est prouvée.

L'élément neutre est le couple *(e,E)*, où le premier *e* est celui du groupe *A*,+ et le deuxième *E* est celui du groupe *B*,+.

Pour revenir à notre espace vectoriel, nous avons donc que :

$K \times K$, +

est un groupe commutatif, et **il peut former un espace vectoriel** avec le corps *K*, +, *

La multiplication scalaire devient la multiplication du corps, appliquée aux deux termes du couple :

*a. (u,v) = (a*u, a*v)*

La multiplication à gauche du signe = est la multiplication scalaire ; les deux multiplications à droite, à l'intérieur du couple, est la multiplication dans le corps.

C'est l'espace de coordonnées à deux dimensions sur le corps *K*.

Prenons comme exemple le corps (commutatif) des nombres réels. Alors, l'ensemble des vecteurs sera $\mathbb{R} \times \mathbb{R}$, l'ensemble des couples de nombres réels. Cet ensemble est bien un groupe commutatif sous l'addition :

(5, 3.3) + (-2, 1.4) = (3, 4.7) sera l'addition des couples et cette addition forme un groupe commutatif.

La multiplication scalaire 5.(2,3) donnera :

(5*2 , 5*3) = (10,15)

Cet espace vectoriel des couples réels, sur le corps commutatif des nombres réels, sera **l'espace de coordonnées Euclidiens**

en deux dimensions. Cet espace de coordonnées est parfaitement « équivalent » (nous y reviendrons) à l'espace vectoriel du plan Euclidien dont nous avions parlé avant, mais a l'avantage d'être une représentation purement « numérique ». C'est l**a géométrie Cartésienne**, équivalente à la géométrie Euclidienne.

Nous pouvons étendre cette notion. Au lieu de considérer $K \times K$, nous pouvons considérer :

$K \times K \times K \ldots \times K, +$

Pour cela, nous introduisons **la notion de n-tuple** :

$(a,b,c,...d)$

qui est une généralisation de la notion de couple. Il est bien sûr trivial de définir un n-tuple comme une « succession de couples imbriquées » :

$(a,b,c) = ((a,b) ,c)$

$(a,b,c,d) = ((a,b,c) , d)$

etc.

mais en général, on ne s'amuse pas à écrire toutes ces parenthèses.

$K \times K \times K$ est donc $(K \times K) \times K$

$K \times K \times K \times K$ est $((K \times K) \times K) \times K$

etc.

Ainsi, nous pouvons considérer : $K \times K \times \ldots \times K$, + où il y a N fois l'apparition de K. On peut démontrer facilement que ceci est un groupe commutatif avec l'addition des n-tuples :

$(a,b,c,\ldots. d) + (u,v,w, \ldots, z) = (a+u, b+v, c+w, \ldots., d+z)$

C'est laissé comme un exercice pour le lecteur.

Ce groupe commutatif avec des N-tuples peut former un espace vectoriel avec le corps K,+,. d'origine. C'est **l'espace de coordonnées à *N* dimensions sur le corps *K*.**

Appliqué au corps des nombres réels, nous obtenons des N-tuples de nombres réels. Cet espace vectoriel est **l'espace de coordonnées Euclidiens en *N* dimensions.**

L'essentiel de la géométrie Euclidienne en mathématiques contemporaines est faite par l'étude de cet espace de coordonnées Euclidiens en N dimensions. Ceci remplace donc l'axiomatique d'Euclide, et la généralise à N dimensions.

Mais cet espace de coordonnées aura bien d'avantage des applications, dans les espaces vectoriels qui ne sont pas directement associés à une situation géométrique. La représentation par des coordonnées sera l'outil le plus important dans l'utilisation de la structure d'espace vectoriel dans bien des applications, au-delà de la géométrie.

Illustration : espace réel à deux dimensions

L'espace vectoriel de coordonnées Euclidiens en deux dimensions est le système qui représente la géométrie Cartésienne dans le plan, dans un repère orthonormal. Les

éléments sont les couples de nombres réels qui représentent des vecteurs dans le plan. Un vecteur est par exemple (2.3 ; 3.1). Le produit scalaire est la multiplication de ce vecteur avec un nombre réel, par exemple : 2.5 . (2.3 ; 3.1) ce qui nous fait un vecteur, 2.5 fois plus long que le premier, et dans la même direction : (5.75 ; 7.75). Deux vecteurs sont parallèles, si l'un est un multiple sous une multiplication scalaire, de l'autre. Ainsi, les vecteurs (2.3 ; 3.1) et (5.75 ; 7.75) sont des vecteurs parallèles. La somme de deux vecteurs est illustrée par la somme de (2.1 ; 3.1) et (3.1 ; -0.6) : (2.1 ; 3.1) + (3.1 ; -0.6) = (5.2 ; 2.5). Cela correspond bien à la somme de vecteurs que nous connaissons dans la géométrie Cartésienne.

Illustration : sinusoïde à fréquence donnée

Considérons un « sinus », une onde, à une fréquence donnée, par exemple, 1 Hz. Il s'agit des fonctions : $f(t) = A \sin(2.\pi.t + \theta)$, où A est l'amplitude et θ est la phase de début. Ce sont tous les « sinus » de fréquence 1 Hz si t est le temps en secondes.

On peut démontrer que ces fonctions sont aussi données par :

$f(t) = u \,.\, \cos(2.\pi.t) + v.\sin(2.\pi.t)$

Ainsi, cet ensemble de fonctions est un espace vectoriel sur les nombres réels qui sera équivalent à l'espace de coordonnées Euclidiens à deux dimensions. Effectivement, chaque $f(t)$ de notre ensemble peut être représenté par le couple (u,v). Si $f(t)$ est représenté par (u,v) et $g(t)$ est représenté par (p,q), alors $f(t) + g(t)$ est représenté par $(u+p,v+q) = (u,v) + (p,q)$, et $r.f(t)$ est

représenté par *(r.u, r.v) = r.(u,v)*. La somme du groupe, et le produit scalaire sont donc préservés.

Cette équivalence entre un « sinus à fréquence donnée » et l'espace Euclidien en 2 dimensions (c.a.d. le plan) est d'ailleurs utilisé en ingénierie électrique est s'appelle un « phaseur » : un vecteur dans le plan représente une tension, ou un courant alternatif (en France et en Europe, à 50 Hz).

Variations de nomenclature

Malheureusement, les mathématiciens ne sont pas toujours d'accord sur la nomenclature exacte des structures. Sur la notion de monoïde, tout le monde semble être d'accord, ainsi que sur la notion de groupe.

Par contre, en se qui concerne l'anneau, il y a deux écoles. Il y a des mathématiciens qui incluent, dans la définition d'un anneau, l'élément neutre multiplicatif. Nous avons choisi de suivre cette définition.

Mais il y a aussi des mathématiciens, qui définissent un anneau sans cette exigence d'un élément neutre multiplicatif ; et ils appellent « notre » anneau, un anneau **unitaire**.

Structures semblables

Introduction

Nous avons étudié différentes structures algébriques. Les axiomes de chaque structure garantissent des propriétés, mais ne définissent pas un système unique. Par exemple, il y a beaucoup de groupes différents. $\mathbb{Z},+$ et $\mathbb{Q}_0,*$ sont deux groupes commutatifs, mais ce ne sont pas les mêmes objets mathématiques. Pas tous les groupes sont les mêmes – *on peut d'ailleurs se poser ce qu'on entend exactement, par « les mêmes » dans ce contexte.*

Effectivement, jusque là, les objets mathématiques que nous avions construits étaient des ensembles et il était facile de décider si deux ensembles étaient identiques : il fallait qu'ils contiennent exactement les mêmes éléments (et ces éléments sont les mêmes, s'ils sont les mêmes éléments atomiques – en théorie naïve des ensembles de Cantor – ou sont, de façon récursive, aussi des ensembles identiques). Mais quand, justement, nous voulons faire abstraction de la construction spécifique d'objets mathématiques (ensembles), alors cette façon de comparer des objets ne marche plus. Bien sûr, pour toute construction et réalisation spécifique d'une structure, cela reste valable, mais justement, nous voulons « oublier » ces différences « superficielles ». Considérons l'ensemble A={1,2,3}, et le groupe de permutations sur A. Considérons l'ensemble B = {8,9,10} et le groupe de permutations sur B. Ces deux groupes, comme « jeux d'ensembles », sont

différents, car *A* et *B* sont des ensembles différents. Par exemple, l'élément « 3 »appartient à *A*, et n'appartient pas à *B*. La permutation {(1,2), (2,3), (3,1)} appartient au groupe de permutations de *A*, et pas au groupe de permutations de *B*. Mais nous voyons qu'en remplaçant 1 par 8, 2 par 9 et 3 par 10, on peut changer la première structure en la deuxième. Ce ne sont donc que les « noms des éléments de base » qui distinguent ces deux structures, et, justement, nous voulions faire abstraction de cela. Nous allons donc considérer que d'une certaine façon, ces deux structures sont bien « les mêmes », et c'est cette notion que nous voulons creuser dans ce qui suit. Cette notion de « ce sont les mêmes » s'appellera un **isomorphisme**, car nous ne pouvons pas appeler cela une vraie égalité.

A partir de ce constat, on peut se poser la question quel peut être le lien entre différents groupes ; cette question se généralise **: quel est le lien entre deux structures du même type ou de type semblable ?**

Mais avant d'attaquer la question de l'équivalence de structures « séparées », regardons déjà le lien qui peut y avoir entre des structures « à partir du même ensemble de base », où cette question ne se pose donc pas. Il y a deux façons d'obtenir des nouvelles structures «à partir du même ensemble de base » : on peut regarder **des sous-ensembles,** et on peut construire des **ensembles-quotients**.

Sous-structures

Sous-groupe, sous-anneau, sous-espace

Une structure est une sous-structure d'une autre structure de même type, si tous les ensembles dont est faite la première structure sont des sous-ensembles des ensembles correspondants de la deuxième structure et que les propriétés de la structure en question sont satisfaites.

Nous avons déjà rencontré cette idée avec la notion de **sous-groupe**.

Si G, ● est un groupe, et H,♦ est un autre groupe, alors G, ● est un sous-groupe de H,♦ si et seulement si:

1. G, ● est bien un groupe
2. H,♦ est bien un groupe
3. G est un sous-ensemble de H
4. ● est un sous-ensemble de ♦

Cette idée se généralise.

Par exemple, G,●,♦ est **un sous-anneau** de H,○,□ si :

1. G,●,♦ est bien un anneau
2. H,○,□ est bien un anneau
3. G est un sous-ensemble de H
4. ● est un sous-ensemble de ○
5. ♦ est un sous-ensemble de □

Par exemple, $\mathbb{Z},+,\times$ est bien un sous-anneau de $\mathbb{Q},+,.$.

Effectivement, $\mathbb{Z}$ est un sous-ensemble de $\mathbb{Q}$ (avec la bonne inclusion, on se souvient), le + dans $\mathbb{Z}$ est bien un sous-ensemble du + en $\mathbb{Q}$ (tout couple qui appartient au + de $\mathbb{Z}$ appartient aussi au + de $\mathbb{Q}$), et le × dans $\mathbb{Z}$ est bien un sous-ensemble du . en $\mathbb{Q}$ (tout couple qui appartient au × de $\mathbb{Z}$ appartient aussi au . de $\mathbb{Q}$).

Notez que l'anneau $\mathbb{Z}$ modulo p, +, * n'est pas un sous-anneau de $\mathbb{Z},+,*$, bien que $\mathbb{Z}$ modulo p est un sous-ensemble de $\mathbb{Z}$, mais les opérations du premier anneau ne sont pas des sous-ensembles des opérations du deuxième anneau. Par exemple, pour $p = 5$, la première addition contient ((2,3),0) tandis que la deuxième addition ne contient pas ce couple (il contiendra ((2,3), 5)).

Cette règle est légèrement modifiée pour un sous-espace vectoriel. Effectivement, si nous considérons $K,+,*$; $V,+$; . comme espace vectoriel, nous considérons un autre espace vectoriel comme un sous-espace **seulement si le corps *K* est le même pour les deux**.

Donc : $K,+,*$; $W,+$; . est **un sous-espace vectoriel** de $L,+,*$; $V,+$; . si :

1. $K,+,*$; $W,+$; . est un espace vectoriel
2. $L,+,*$; $V,+$; . est un espace vectoriel
3. $K,+,*$ et $L,+,*$ sont les mêmes corps
4. $W,+$ est un sous-groupe de $V,+$

5. La multiplication scalaire . du deuxième espace est un sous-ensemble de la multiplication scalaire . du premier.

On ne compare en fait jamais des espaces vectoriels avec des corps différents.

Un exemple de sous-espace vectoriel est le suivant. Dans l'espace de coordonnées Euclidiens en deux dimensions, nous considérons l'ensemble :

$D = \{(k, 2.3k) \in \mathbb{R} \times \mathbb{R} | k \in \mathbb{R}\}$

Ceci est géométriquement la droite passant par 0 avec un coefficient directeur de 2.3. On peut facilement constater que *D* est lui-même un espace vectoriel sur les nombres réels, et donc que *D* est un sous-espace vectoriel de l'espace de coordonnées Euclidiens en deux dimensions.

D'autres exemples géométriques sont : les droites passant par l'origine dans l'espace 3-dimensionnel sont des sous-espaces de l'espace 3-dimensionnel. Les plans passant par l'origine dans l'espace 3-dimensionnel sont des sous-espaces de l'espace 3-dimensionnel.

Dans l'espace des applications numériques réelles (dont nous avons vu qu'ils formaient un espace vectoriel sur le corps des nombres réels), nous pouvons considérer les polynômes. Les polynômes forment un sous-espace vectoriel de l'espace vectoriel des applications numériques réelles.

Idéal

Jusqu'ici, nous avons considéré comme sous-structure, la *même* structure que la structure-mère : le sous-groupe était un groupe, le sous-anneau était un anneau, le sous-espace vectoriel était un espace vectoriel.

Mais il peut aussi être judicieux **de définir des sous-structures qui sont différentes des structures-mères, quand ces sous-structures ont une relation particulière avec la structure-mère.** Nous allons voir un peu plus loin pourquoi ces sous-structures peuvent être utile, quand nous allons considérer les structures-quotients.

C'est le cas de sous-structures d'un anneau, qu'on appelle, des **idéaux**. La théorie des idéaux est vaste, et il y a au moins une dizaine de différents types d'idéaux, mais nous allons nous limiter à un seul cas :

Un anneau commutatif avec un idéal bilatéral.

Étant donné un anneau commutatif $A, +, *$, un idéal (bilatéral) G de cet anneau est un sous-ensemble de A tel que:

1. $G,+$ est un sous-groupe de $A,+$
2. Pour tout x en A et y en G, $x * y$ est dans G

Il faut noter que la condition 2 est plus sévère que celle des sous-structures habituelles ; Il faut que $x * y$ soit dans G, même pour des éléments x en-dehors de G.

Par contre, un idéal n'est pas toujours un sous-anneau[2], car il ne contient pas toujours l'élément neutre pour la multiplication. D'ailleurs, il ne peut pas (sauf pour l'idéal trivial qui est *A* lui-même) : si 1 fait partie de *G* alors *x* * 1 = *x* n'est pas dans *G* si *x* n'est pas dans *G*.

Par exemple, dans l'anneau $\mathbb{Z}$,+, *, l'ensemble {…,-15, -10, -5, 0, 5, 10, 15….} est un idéal, mais comme cet ensemble ne contient pas 1, selon notre définition d'anneau, ce n'est pas un sous-anneau.

Sous-groupe normal

G,* est un groupe. *H*,* est un sous-groupe *normal* de *G*,*, si :

1. *H*,* est un sous-groupe de *G*,*
2. Pour tout élément *x* de *G*, et pour tout élément *y* de *H*, nous avons que *x * y * (1/x)* appartient à *H*.

Il va de soi que pour tout groupe commutatif, chaque sous-groupe est aussi un sous-groupe normal, car

*x * y * (1/x) = x * 1/x * y = 1 * y = y* qui est bien dans *H*.

La notion de sous-groupe normal ne prend tout son sens que pour des groupes non-commutatifs.

2 Ceci vient de notre définition d'anneau qui contient l'exigence d'élément neutre pour la multiplication ; si nous avions utilisé l'autre définition, sans cette exigence, alors tout idéal est un sous-anneau (mais pas tout sous-anneau est nécessairement un idéal).

S'entraîner

1. Considérez le groupe commutatif d'addition modulo 8 en {0,1,2,3,4,5,6,7}. Est-ce que {0,4},+ est un sous-groupe de ce groupe ? Et {0,2,4,6},+ ?

2. Considérez le groupe des permutations d'un ensemble A = {1,2,3}, qui consiste des permutation {*p1*,*p2*,*p3*,*p4*,*p5*,*p6*} et la composition comme opération. Est-ce que {*p1*,*p2*,*p3*} est un sous-groupe normal ? Et {*p1*,*p5*}, est-ce un sous groupe normal ?

3. Considérez le groupe des permutations d'un ensemble B = {1,2,3,4}. Combien de permutations y a-t-il ? Trouvez un sous-groupe de ce groupe, et vérifiez s'il est un sous-groupe normal ou non.

4. Vérifiez que dans un anneau commutatif A, +, *, avec un élément s dans A, l'ensemble suivant

$$\{x \in A | \exists r \in A : x = r * s\}$$

forme un idéal. On l'appelle l'idéal principal généré par s. Un cas spécifique est l'idéal de $\mathbb{Z}$,+,* fait de multiples d'un nombre entier.

Structures quotient

Si nous avons une structure avec un ensemble de base V et une sous-structure avec un ensemble de base W qui est donc une partie de V, alors nous pouvons parfois définir une structure-quotient : cette structure-quotient est une structure basée sur

l'ensemble-quotient qui vient d'une relation d'équivalence dont les classes d'équivalence sont :

$[a] = \{x \in V | x - a \in W\}$

Ici, *la différence est prise par rapport à une opération de groupe*. Si la structure est un groupe, cette opération est évidemment celle du groupe. Si la structure est un anneau, l'opération en question est celle du groupe additif. Si la structure est un espace vectoriel, l'opération est celle du groupe commutatif des vecteurs.

Les opérations « héritées » sont celles qui s'appliquent aux éléments des classes d'équivalence, si on peut démontrer que le choix de l'élément représentant sa classe est indifférent.

Ainsi, nous obtenons :

- **le groupe-quotient** : il faut que la sous-structure soit un groupe normal.
- **L'anneau-quotient** : il faut que la sous-structure soit un idéal.
- **l'espace vectoriel-quotient** : il faut que la sous-structure soit un sous-espace vectoriel.

Le groupe-quotient

Nous allons démontrer que **le groupe-quotient est bien un groupe**, et nous allons nous rendre compte pourquoi la sous-structure doit être un groupe normal et pas un simple sous-groupe arbitraire.

Considérons le groupe *V*,* comme le « grand » groupe, et *W*,* le groupe par lequel nous « divisons ». Ainsi, les classes sont :

[y] = $\{x \in V | x * (1/y) \in W\}$

[z] = $\{u \in V | u * (1/z) \in W\}$

*[y*z]* = $\{a \in V | a * (1/(y * z)) \in W\}$

y' est aussi un élément de *[y]* si *y'/y = w* est dans *W*.

z' est aussi un élément de *[z]* si *z'/z = w'* est dans *W*.

Il faut maintenant qu'il y ait un *w''* tel que *(y'*z')/(y*z) = w''* dans *W*.

Nous voyons que pour un groupe commutatif, cela est évident :

*(y'*z')/(y*z) = (y' / y) * (z'/z) = w * w' = w''* dans *W*.

Mais si le groupe n'est pas commutatif ?

Nous pouvons écrire que *y' = w * y* et *z' = w' * z*.

Alors : *(y'*z')/(y*z) = (w*y*w'*z)/(y*z)*

Dans un groupe non-commutatif, *1/(y*z) = (1/z)*(1/y)* ; ainsi :

*(y'*z')/(y*z) = w*y*w'*z*(1/z)*(1/y) = w*(y*w'*(1/y))*.

L'expression entre parenthèses sera membre de *W* si *W* est un sous-groupe *normal*, car c'est la propriété qui distingue un sous-groupe normal d'un sous-groupe quelconque. Le produit de *w* et de cet élément de *W* sera aussi un élément de *W*. Ainsi, nous trouvons bien que *(y'*z')/(y*z)* appartient à *W*, et donc, que *(y'*z')* et *(y*z)* appartiennent à la même classe d'équivalence. Ainsi, nous avons démontré que le choix de

l'élément spécifique d'une classe ne joue pas de rôle et que le produit de deux classes d'équivalence est donc correctement définie.

Mais nous avons aussi vu que la propriété de sous-groupe normal est essentielle pour que cette opération soit définie dans le groupe-quotient.

Un premier exemple est le groupe additif des entiers $\mathbb{Z}$. Considérons le sous-groupe des multiples de 5:

{…,-15,-10,-5,0,5,10,15….}, +

On peut facilement se convaincre que c'est bien un groupe, et donc un sous-groupe de $\mathbb{Z}$,+. Comme c'est un groupe commutatif, il est automatiquement un sous-groupe normal.

Le groupe-quotient contiendra 5 différentes classes d'équivalence : { [0], [1], [2],[3], [4]} car on peut facilement constater que [-15] = [5] = [0], que [-4] = [6] = [1] etc.

Le groupe-quotient n'est rien d'autre que le groupe additif modulo 5.

L'anneau-quotient

Pour **l'anneau-quotient** le raisonnement est comparable, et c'est aussi la raison pour laquelle il faut diviser par un idéal, et non par un sous-anneau. Pour l'opération additive, il n'y a pas de problème comme le groupe additif est commutatif, mais pour que la multiplication soit bien définie, nous avons besoin de la propriété de l'idéal de la même façon que nous avions

besoin de la propriété de groupe normal pour le groupe-quotient.

L'espace-vectoriel quotient

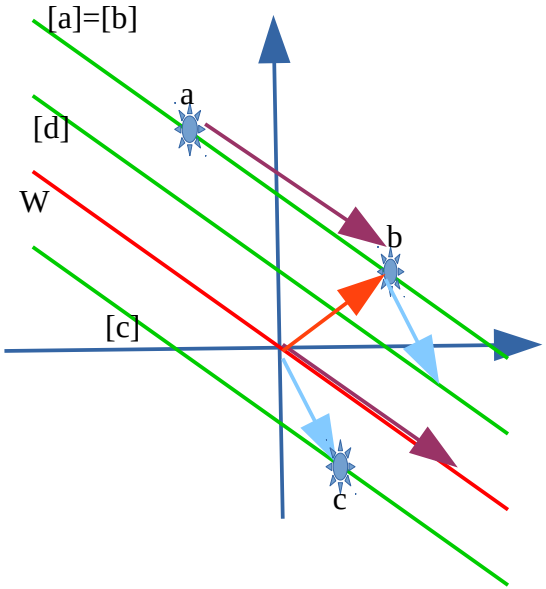
On s'imagine le mieux l'espace-vectoriel quotient, comme *l'ensemble des « objets parallèles » au sous-espace par lequel on « divise »*. Par exemple, dans l'espace de coordonnées Euclidiens à deux dimensions, une droite passant par l'origine est un sous-espace. Si on considère l'espace vectoriel quotient, c'est l'ensemble des droites parallèles à cette droite passant par l'origine. Effectivement, chaque élément de l'espace vectoriel quotient est une classe d'équivalence contenant un jeu de vecteurs qui sont « mis en relation » entre eux par un vecteur appartenant au sous-espace, c.a.d. par la droite passant par l'origine. Il est intéressant de remarquer que cet ensemble de droites est un espace vectoriel, qu'on peut ajouter deux droites parallèles, et qu'on peut multiplier une droite parallèle avec un nombre réel. **Les droites parallèles sont, dans cet espace-quotient, elles-mêmes des vecteurs** !

En trois dimensions, l'espace-quotient de la division de l'espace total par une droite passant par l'origine, est l'ensemble des droites parallèles à cette droite. C'est un espace à deux dimensions. Par contre, l'espace-quotient de la division de l'espace total par un plan passant par l'origine, est l'ensemble des plans parallèles à ce plan. C'est un espace à une dimension.

Ceci peut paraître étrange, qu'un ensemble de droites est un espace à deux dimensions, et qu'un ensemble de plans est un espace à une dimension ; mais ce n'est pas la nature des

éléments qui détermine le nombre de coordonnées, mais le « nombre » d'éléments dans l'ensemble. Il y a « plus » de droites parallèles que de plans parallèles.

Illustration 1: Illustration géométrique d'espace-quotient



La ligne rouge représente le sous-espace par lequel on divise, et les lignes vertes (et la ligne rouge) sont les éléments de l'espace-quotient. Les points *a* et *b* appartiennent à la même classe d'équivalence car *b-a*, le vecteur violet, appartient au sous-espace rouge. Nous avons donc que *[a] = [b]*. L'espace-quotient étant un espace vectoriel lui-même, nous pouvons

considérer l'addition de *[b]* et de *[c]*, ce qui nous donne *[d]*, car un représentant de *[b]* (le vecteur orange) plus un représentant de *[c]* (le vecteur bleu-clair) est un représentant de *[d]*.

L'espace-vectoriel quotient est la « projection » de l'espace total par l'espace par lequel on divise. **C'est un peu l'idée générale de structure-quotient : c'est une généralisation de la notion de « projection ».**

Cette idée est la plus nette dans sa forme géométrique dans l'espace vectoriel-quotient, mais l'idée y est aussi dans le groupe-quotient et dans l'anneau-quotient.

On peut voir une « projection » comme « une partition en choses parallèles », où on peut voir « des choses parallèles » comme des choses « qui sont faites de points dont les différences ont les mêmes directions ». On se rapproche très fortement de la définition formelle de structure-quotient ! Si on considère que la sous-structure est l'ensemble des points « de la même direction », alors les « choses parallèles » sont les parties dont les éléments ont des différences qui appartiennent à cette sous-structure. Ces « choses parallèles » sont alors justement, les projections « selon cette direction » comme donnée par la sous-structure en question.

On peut effectivement voir que la « projection » des entiers « selon les multiples de 5 » donne une « projection » qui consiste en les 5 « différentes versions parallèles » des multiples de 5 : celle qui passe par l'origine (donc $[0]_5$), et les 4 autres, qui y sont « parallèles » , donc $[1]_5$, $[2]_5$, $[3]_5$ et $[4]_5$.

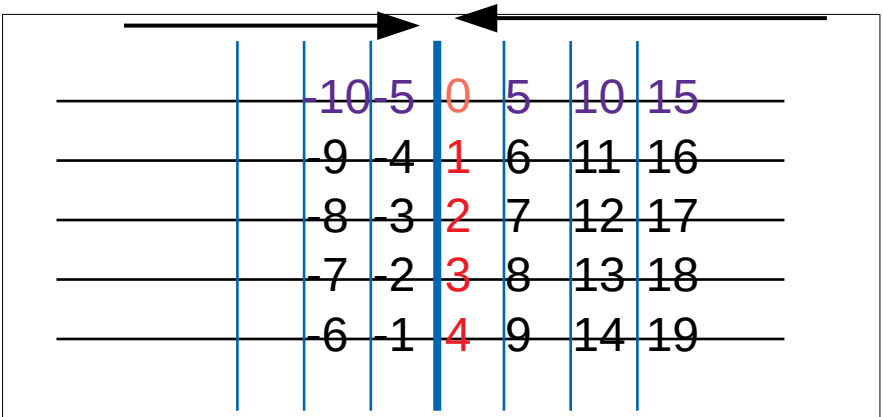


Illustration 2: Groupe-quotient comme projection: on projette les entiers le long des multiples de 5, et on obtient 5 parties « parallèles ».

S'entraîner

1. Considérez le groupe *P* des permutations de l'ensemble {1,2,3} avec la précédente notation. {*p1*,*p2*,*p3*} est un sous-groupe normal. Quel est le groupe-quotient ?

2. Vérifiez que l'anneau-quotient d'un anneau commutatif divisé par un idéal bilatéral est bien un anneau. Utilisez l'exemple de ℤ,+,* divisé par les multiples de 5 pour vous inspirer.

3. Vérifiez que l'espace-vectoriel quotient d'un espace de coordonnées Euclidiens à deux dimensions, par l'axe *X*, est un espace vectoriel à une dimension.

Homomorphismes et isomorphismes

Définitions

De façon informelle, un homomorphisme est une application d'une structure algébrique en une autre structure algébrique de nature semblable, *de telle façon que l'image sous l'application d'une expression algébrique dans la première structure, devient l'expression algébrique dans la deuxième structure, des images*.

Si nous avons une structure algébrique avec une seule opération, par exemple, un groupe : A, ▲ et une deuxième structure algébrique semblable, donc aussi avec une seule opération : B, ■ ; alors, l'application f de A en B est un homomorphisme si :

$f(a \blacktriangle b) = f(a) \blacksquare f(b)$.

Pour une structure avec deux opérations internes, A, +, * et une structure semblable (donc aussi avec deux opérations internes) B, ■, ▲ l'homomorphisme devra satisfaire :

$f(a + b * c) = f(a) \blacksquare f(b) \blacktriangle f(c)$

Notez qu'un homomorphisme n'est pas nécessairement injectif, ni surjectif. Si un homomorphisme est aussi une bijection, on dit qu'on a un **isomorphisme** entre les deux structures.

Un isomorphisme dit en fait que les deux structures, en *ce qui concerne la structure algébrique*, sont identiques.

Nous tenons là, enfin, notre notion de « ce sont les mêmes structures » que nous cherchions. Pour tout ce qui concerne la structure algébrique, qu'on le fasse dans la première structure, ou dans la deuxième, c'est la même chose. Il se peut bien sûr que les deux ensembles possèdent des propriétés supplémentaires qui font que les deux ensembles se distinguent, mais en ce qui concerne la structure algébrique, les deux sont la « même chose ». Si un isomorphisme existe entre deux structures algébriques, on dit qu'elles sont **isomorphes**.

Un exemple d'isomorphisme est : la fonction exponentielle entre le groupe additif $\mathbb{R}$, + et le groupe multiplicatif $\mathbb{R}^+_0$,*.

Qu'on fasse des additions dans $\mathbb{R}$,+, ou des multiplications dans $\mathbb{R}^+_0$,*, en ce qui concerne la loi de composition, c'est identique. C'était la grande découverte des tables logarithmiques par **John Napier** au 17ieme siècle.

Nous sentons que *la notion d'isomorphisme introduit une nouvelle couche d'abstraction* : celle des structures algébriques. Étudier une structure algébrique, ou une « autre » structure algébrique avec laquelle, la première est isomorphe, est la même étude. Nous nous retrouvons un peu dans le cas comparable d'abstraction, que nous avons rencontré en fin d'école maternelle : « deux pommes », « deux bonbons », et « deux camarades », c'est la notion de « deux » qui est retenue pour tout ce qui concerne « compter ». Bien sûr, on ne mange pas une pomme de la même façon qu'on mange un camarade ! Deux pommes n'est pas la même chose que deux camarades pour tout, mais, pour ce qui concerne « compter », c'est la même chose. On peut illustrer l'addition 3 + 2 = 5 aussi bien

en ajoutant deux pommes à trois pommes, qu'en ajoutant deux camarades à trois camarades, pour compter, respectivement, 5 pommes, ou 5 camarades.

Pour tout ce qui concerne l'algèbre avec les opérations de deux structures algébriques isomorphes, on peut le faire dans l'une, ou dans l'autre, c'est la même chose. C'est dans ce sens-là que des structures algébriques isomorphes sont « les mêmes ». La question qui devient intéressante alors, est : « quelles sont les structures non-identiques qui existent ? ». Par exemple, quels sont les différents groupes possibles ? Combien de groupes différents avec 7 éléments sont possibles ? *Combien de corps commutatifs différents avec n éléments sont possibles ?* C'est **Évariste Galois** qui a traité cette dernière question au 19ième siècle, qui s'avère extrêmement importante en théorie des nombres, et la réponse est remarquable :

- si *n* est une puissance d'un seul nombre premier, alors, la réponse est 1.
- si *n* n'est pas une puissance d'un seul nombre premier, alors la réponse est 0.

Il n'existe donc pas de corps commutatif qui contient, disons, 48 éléments. Il existe un seul corps commutatif qui contient 49 éléments (49 est 7^2), *à un isomorphisme près*.

Par contre, nous voyons qu'il y a plus de variation dans les groupes. Par exemple, le groupe avec 6 éléments *{p1, p2, p3, p4, p5, p6}* qui étaient les permutations d'un ensemble de 3 éléments, est un groupe qui ne peut pas être isomorphe avec le

groupe cyclique $\mathbb{Z}_6$,+, car le premier groupe n'est pas commutatif, alors qu'un groupe cyclique est toujours commutatif. Il existe donc au moins 2 groupes différents avec 6 éléments.

La branche des mathématiques qui étudie de façon systématique la notion abstraite qui résulte des isomorphismes, s'appelle **la théorie des catégories**, mais cela dépasse trop largement le cadre de cet ouvrage. Il faut juste retenir qu'un isomorphisme rend deux structures algébriques identiques en ce qui concerne leur algèbre.

Un homomorphisme n'est pas aussi strict qu'un isomorphisme, et nous pouvons avoir des homomorphismes entre structures qui ne sont pas identiques.

Un homomorphisme d'une structure en elle-même (l'application est donc une transformation) s'appelle un **endomorphisme**. Un isomorphisme d'une structure en elle-même (l'application est donc une permutation) s'appelle un **automorphisme**. Tout automorphisme est automatiquement un endomorphisme bien sûr, mais l'inverse n'est pas vrai.

Notez que toute structure a bien sûr un automorphisme : la permutation identique. Mais beaucoup de structures ont aussi des automorphismes non-triviales. Nous connaissons l'ensemble de toutes les permutations d'un ensemble. Cet ensemble de permutations, équipé de l'opération « composition », forme un groupe, comme nous avons vu. De la même façon, **l'ensemble de tous les automorphismes d'une structure donnée, équipé de l'opération**

« composition », forme d'ailleurs aussi un groupe (un sous-groupe du groupe des permutations).

Homomorphisme de groupe

Un homomorphisme de groupe est un homomorphisme concernant des groupes. Si *A*,* et *B*,. sont deux groupes, et si *f* est un homomorphisme de groupe entre *A* et *B*, alors, par définition, nous avons que *f(a*b) = f(a) . f(b)* pour tout *a* et *b* de *A*.

Un homomorphisme de groupe a des propriétés importantes. La première est que **l'image de *f*, notons-la *f(A)*, est un sous-groupe de *B*,.**

La deuxième est : **si *C*,* est un sous-groupe de *A*,*, alors l'image de *C* sous *f*, notons-la *f(C)* est un sous-groupe de *f(A)*, .**

La troisième est : **L'image de l'élément neutre est l'élément neutre de l'autre groupe.**

Notez cependant, comme *f* ne doit pas être injectif, que *A*,* et *f(A)*,. ne sont pas nécessairement isomorphes.

Un exemple est l'homomorphisme entre $\mathbb{Z}$,+ et $\mathbb{Z}_3$, + :

f(n) = n mod 3.

Notez que cette application n'est pas un homomorphisme de $\mathbb{Z}$, + en $\mathbb{Z}$,+ comme on pourrait le croire. Effectivement, *f(5) = 2* et *f(4) = 1*, mais *f(5 + 4) = f(9) = 0* et ceci n'est pas égal à *f(5)*

$+ f(4) = 2 + 1 = 3$ dans $\mathbb{Z},+$. Par contre, dans $\mathbb{Z}_3$,+, l'égalité 2 + 1 = 0 vaut, et donc notre exigence pour *f* marche bien.

Un autre exemple : l'homomorphisme entre $\mathbb{Z},+$ et $\mathbb{Z}_6$, + avec $f(n) = n$ mod 6. Quand nous considérons le sous-groupe des nombres pairs de $\mathbb{Z},+$, à savoir $2\mathbb{Z}$, +, l'image de ce sous-groupe $2\mathbb{Z},+$ sous notre homomorphisme donne : {0,2,4}. Le groupe {0,2,4},+ est bien un sous-groupe de $\mathbb{Z}_6$, + comme on peut vérifier (exercice).

Rappelons que nous avions introduit un générateur de groupe : un élément *a*, tel que le groupe consiste de toutes les puissances entières a^n. *Il s'avère que tous les groupes qui ont un générateur, sont isomorphes à* $\mathbb{Z}$, + *s'ils ne sont pas cycliques, et sont isomorphes à* $\mathbb{Z}_n$, + *s'ils sont cycliques d'ordre n.* L'isomorphisme, est exactement : $f(n) = a^n$. Tous les groupes cycliques avec *n* éléments sont donc « les mêmes », et tous les groupes avec un seul générateur qui ne sont pas cycliques sont « le même groupe », à savoir le groupe additif des entiers.

Nous définissons **le noyau d'un homomorphisme de groupe,** comme l'ensemble des éléments du premier groupe, qui ont pour image, l'élément neutre du deuxième groupe. On note cet ensemble : *Ker f.*

$$Ker\, f = \{ x \in G | f(x) = 1_{G'} \}$$

Le théorème fondamental de l'homomorphisme de groupes est le suivant :

Considérons un homomorphisme *f* de *G*,* en *G'*,. Alors :

1) *Ker f* est un sous-groupe normal de *G*

2) Le groupe-quotient *G / Ker f* est isomorphe à l'image de *G* sous *f*.

Quelque part, on peut « sentir » ce théorème : si tous les éléments de *Ker f* sont projetés sur l'élément neutre, alors chaque « tranche parallèle » à *Ker f* dans le groupe d'origine sera projetée sur un seul élément du groupe d'arrivée. Cette « tranche parallèle » est exactement un élément du groupe-quotient *G / Ker f*.

Dans notre exemple de l'homomorphisme $f(x) = x$ mod 6 du groupe $\mathbb{Z}$, + en $\mathbb{Z}_6$, +, nous constatons que *Ker f* est l'ensemble des multiples de 6 (les multiples de 6 sont portés sur 0, l'élément neutre). Les multiples de 6 sont un sous-groupe normal de $\mathbb{Z}$, + (ici, c'est le cas parce que $\mathbb{Z}$, + est un groupe commutatif, et tout sous-groupe est un sous-groupe normal dans un groupe commutatif). Ainsi, le théorème nous dit que l'image de $\mathbb{Z}$ sous *f*, à savoir $\mathbb{Z}_6$. est isomorphe au groupe-quotient de $\mathbb{Z}$ par les multiples de 6. Nous avions effectivement déjà constaté que le groupe « addition modulo 6 » était (isomorphe au) groupe-quotient de $\mathbb{Z}$ par les multiples de 6.

Les multiples de 6 forment *Ker f*. Les multiples de 6, plus 1, une « tranche parallèle » aux multiples de 6, seront projetés sur 1. Les multiples de 6, plus 2, une autre « tranche parallèle » aux multiples de 6, seront projetés sur 2. Etc...

Nous voyons ici d'ailleurs cet effet de « c'est le même groupe ». A strictement parler, l'ensemble qui contient les

nombres {0,1,2,3,4,5}, et l'ensemble qui contient les classes d'équivalence {[0], [1], [2], [3], [4], [5]} des nombres entiers par la relation d'équivalence « x mod 6 = y mod 6 », ne sont pas les mêmes ensembles. Mais les deux groupes formés par l'addition modulo 6 sont isomorphes, et on considère donc que les deux groupes sont « les mêmes ». On fait abstraction de la construction détaillée de chaque élément (de la même façon qu'on faisait abstraction du fait que les objets qu'on comptait étaient des bananes ou des copains de classe) ; tout en admettant que le nombre « 5 » n'est pas la même chose que la classe d'équivalence [5], qui contient le nombre 5.

La notion d'isomorphisme introduit un nouvel outil d'abstraction en mathématiques.

Homomorphisme d'anneaux et de corps

Un homomorphisme de l'anneau A,+,* en l'anneau B, +, * est un application de A en B tel que :

$f(a+b) = f(a) + f(b)$

$f(a*b) = f(a) * f(b)$

Mais en plus, on exige une propriété supplémentaire :

$f(1) = 1$.

Dans les homomorphismes de groupe, cette exigence n'était pas nécessaire, car c'était une propriété (la troisième propriété que nous avions énoncée). Mais comme ceci ne suit pas des deux premières exigences dans un anneau, il faut l'exiger explicitement.

Pour illustrer la nécessité de cette condition *f(1) = 1*, considérons l'application *f(x) = 4 x* de $\mathbb{Z}_6$,+,* en $\mathbb{Z}_6$,+,*. Il va de soi que *f(x+y) = f(x) + f(y)*, car *4*(x+y) = 4*x + 4*y*. Il est aussi vrai que *f(x*y) = f(x) * f(y)* car f*(x) * f(y) = 4 * x * 4 * y = 16 * x * y = 4 * x * y = f(x*y)*, car 16 mod 6 = 4. Cependant, *f(1) = 4*, et n'est pas 1. Ainsi, pour préserver toute la structure d'anneau (y compris, donc, l'élément unitaire), il faut exiger *f(1) = 1* car ça ne suit pas automatiquement des deux autres exigences.

Il faut noter qu'un homomorphisme d'anneaux est automatiquement aussi un homomorphisme pour les groupes additifs, et donc les propriétés des homomorphismes de groupe s'appliquent. Mais en outre, il y a la propriété suivante :

Si *A*, +, * et *B*, +, * sont des anneaux, et *f* est un homomorphisme d'anneaux de *A* en *B*, alors l'image de *A* est un sous-anneau de *B*.

Pour un corps, l'homomorphisme est comme l'homomorphisme d'anneaux et l'image d'un corps par un homomorphisme est aussi un sous-corps.

Homomorphisme d'espace vectoriel

On appelle les homomorphismes des espaces vectoriels : **des applications linéaires**. On ne les considère qu'entre espaces vectoriels sur le même corps. La définition d'une application linéaire est la définition « standard » d'homomorphisme :

f(a x + b y) = a f(x) + b f(y)

L'étude des applications linéaires est une branche très développée des mathématiques : **l'algèbre linéaire**.

S'il y a un isomorphisme entre un espace vectoriel *V* sur le corps *K*, et l'espace de coordonnées de dimension *n* sur le corps *K*, **on dit que l'espace vectoriel *V* est de dimension *n*.** Comme c'est toujours le cas pour un isomorphisme, l'étude de l'espace vectoriel *V* se réduit alors à l'étude de l'espace de coordonnées sur le corps *K*. Mais il y a aussi des espaces vectoriels qui ne sont pas isomorphes à un espace de coordonnées, et qui n'ont donc pas de dimension finie.

Quand un espace vectoriel est de dimension *n*, **toute transformation linéaire pourra alors être représentée par un tableau d'éléments de *K*, de taille *n x n*, qu'on appelle une matrice.**

Effectivement, considérons le vecteur $e_1 = (1, 0, \dots , 0)$. Sous la transformation linéaire, $f(e_1) = (a_1, a_2 \dots a_n)$. De la même façon, $e_2 = (0, 1, 0, \dots 0)$ et $f(e_2) = (b_1, b_2, \dots b_n)$. On continue la série, et finalement, nous avons $f(e_n) = (z_1, \dots z_n)$.

Conventionnellement, nous écrivons une matrice, un tableau de nombres (éléments de *K*), comme le tableau qui a comme première colonne, $a_1, a_2 \dots a_n$, comme deuxième colonne : $b_1, b_2, \dots b_n$ etc.… et comme dernière colonne : $z_1, \dots z_n$.

Ce tableau suffit pour calculer l'image de n'importe quel vecteur. Effectivement, imaginons que nous voulons calculer l'image du vecteur $x = (x_1, x_2, \dots x_n)$. On peut bien sûr écrire :

$x = x_1.e_1 + x_2.e_2 + \dots x_n.e_n$

f étant une transformation linéaire (un endomorphisme de l'espace vectoriel), nous avons :

$f(x) = x_1.f(e_1) + x_2.f(e_2) + \ldots x_n.f(e_n)$

Ainsi, $f(x)$ est un vecteur $(y_1, y_2, \ldots y_n)$ et nous avons :

$y_1 = x_1 .a_1 + x_2.b_1 + \ldots + x_n.z_1$

$y_2 = x_1 .a_2 + x_2.b_2 + \ldots + x_n.z_2$

…

$y_n = x_1 .a_n + x_2.b_n + \ldots + x_n.z_n$

Nous voyons que, pour calculer l'image d'un vecteur quelconque *x* sous l'application linéaire, nous avons besoin du tableau de nombres (éléments de *K*), la matrice, et rien d'autre.

Nous avons déjà rencontré un cas dégénéré de cette notion d'application linéaire : quand nous considérons un espace de coordonnées de dimension 1. Effectivement, une application linéaire dans l'espace de coordonnées de dimension 1 (qui n'est rien d'autre que l'axe réel, ici l'axe « *X* »), la « matrice » prend la forme d'un « tableau » de dimensions *1 x 1* : c'est donc juste un seul nombre : **le « coefficient directeur ».**

L'application linéaire de l'espace Euclidien de dimension 1 en lui-même, s'écrit :

$y = f(x) = a.x$

C'est la forme la plus simple de l'expression générale d'une application linéaire.

En géométrie plane, nous avons déjà compris que le plan est isomorphe à un espace Euclidien de dimension 2. Alors toutes les transformations linéaires seront représentées par un tableau de 2 x 2 nombres. Par exemple, le tableau :

1	0
0	0

Représente une projection du plan sur l'axe *X*. Effectivement, l'image d'un vecteur arbitraire *(x,y)*, aura comme image, *(x,0)*, ce qui est bien sa projection sur l'axe *X*.

Le tableau :

1	0
0	-1

Représente une réflexion dans l'axe *X*. Effectivement, l'image d'un vecteur arbitraire *(x,y)* aura comme image, *(x, -y)*, ce qui est bien sa réflexion dans l'axe *X*.

Une application linéaire d'un espace vectoriel *V* de dimension *n*, dans un autre espace vectoriel *W* de dimension *m*, sera, de la même façon, représenté par un tableau, cette fois rectangulaire, de taille *n* × *m*. Le raisonnement est exactement le même que pour une transformation linéaire, sauf que y aura cette fois, *m* coordonnées *y* à calculer.

Nous voyons qu'**il y a un lien très intime entre des systèmes d'équations du premier ordre et des applications linéaires.** Effectivement, l'expression d'une application linéaire n'est rien d'autre qu'un système de *m* équations en *n* variables. C'est une des principales applications de l'algèbre linéaire : d'utiliser les techniques dans les espaces vectoriels pour étudier/résoudre des systèmes d'équations linéaires.

L'algèbre linéaire est un vaste domaine d'étude, mais nous voulons terminer sur une propriété simple et remarquable : **Si *V* est un espace vectoriel de dimension *n*, et *f* est une application linéaire dans un espace vectoriel *W*, alors :**

- **le noyau de *f* (la partie de *V* qui a comme image, sous *f*, l'élément neutre de *W*), *Ker f*, est un sous-espace vectoriel de *V***
- **l'image de *f*, *Im f*, est un sous-espace vectoriel de *W***
- ***n* = *dim Ker f* + *dim Im f***

où *dim Ker f* est la dimension de *Ker f*, et *dim Im f* est la dimension de *Im f*.

Notez que la dimension de *W* ne rentre pas dans les considérations, sauf pour le fait que *dim Im f* ne peut, bien sûr, ne pas être supérieur à la dimension de *W*.

S'entraîner

1. Considérez l'ensemble *A* de toutes les puissances positives et négatives entières du nombre 7, qui est un sous-ensemble de $\mathbb{Q}$, l'ensemble des fractions. Est-ce que cet ensemble, équipé de la

multiplication, forme un groupe ? Est-ce qu'on peut établir un isomorphisme entre ce groupe, et $\mathbb{Z}$, + ? Si oui, quel est cet isomorphisme ?

2. Considérez un homomorphisme entre un groupe cyclique *A* avec *n* éléments, et un autre groupe cyclique *B*, de *m* éléments. Que peut-on dire de *n* et de *m* ?

3. Considérez une application linéaire surjective de l'espace Euclidien 3-dimensionnel en un plan (donc 2-dimensionnel). Que peut-on dire concernant la dimension du noyau de cette application ? Un exemple est une projection sur un plan. Considérez une autre application linéaire surjective de l'espace Euclidien 3-dimensionnel sur une droite. Que peut-on dire cette fois concernant la dimension du noyau ?

Structures non-algébriques

Jusqu'ici nous avons étudié des structures algébriques, c'est à dire, des structures qui consistent d'ensembles, équipés d' applications qui sont des opérations (internes ou externes), et dont la structure postule des propriétés de ces opérations. Mais il existent d'autres structures, qui ne sont pas basées sur des opérations. Nous allons voir des structures d'ordre, des structures topologiques, et des structures métriques.

Structures d'ordre

Définitions et notions de base

Une structure d'ordre consiste en un ensemble de base *A*, et une relation d'ordre *R* dans cet ensemble.

La structure d'ordre est une généralisation et une abstraction de la notion de « plus petit que », que nous connaissons dans les nombres.

Il y a différents types de relation d'ordre, ce qui donne lieu à différentes structures d'ordre.

Il y a d'abord **la relation d'ordre totale** : C'est une relation de *A* en *A*, tel que :

1. la relation est **réflexive** (tout *(a,a)* est dans *R*)
2. la relation est **anti-symétrique** (si *(a,b)* avec *a* différent de *b*, est dans *R*, alors *(b,a)* n'est pas dans *R*)

3. la relation est **transitive** (si *(a,b)* et *(b,c)* sont dans *R*, alors *(a,c)* est dans *R*)

4. la relation est **totale** : pour tout *a* et *b* de *A*, *(a,b)* ou *(b,a)* est dans *R*

L'exemple-type est la relation « plus petit ou égal » dans les nombres (réels, rationnels, entiers, naturels). **Notez que l'inverse d'une relation d'ordre totale, est aussi une relation d'ordre totale.** L'inverse de « plus petit ou égal » est « plus grand ou égal » dans les nombres[3].

Nous pouvons comprendre les exigences d'une relation d'ordre comme une généralisation de la notion « plus petit ou égal ». Effectivement, tout élément est « plus petit ou égal » à lui-même (réflexivité) ; quand deux éléments sont différents, nous ne pouvons pas avoir qu'un élément soit plus petit ou égal à l'autre, et en même temps, plus grand où égal (anti-symétrie). Finalement, si *a* est plus petit ou égal à *b*, et *b* est plus petit ou égal à *c*, alors *a* est plus petit ou égal à *c* (transitivité).

L'exigence de totalité veut dire que *tous les éléments sont comparables* : nous ne pouvons pas avoir le cas de deux éléments qui ne sont pas comparables (c.a.d. où *a* n'est pas plus petit ou égal à *b* mais *b* n'est pas plus petit ou égal à *a* non plus).

3 Il ne faut pas confondre la « relation inverse » et la « négation logique ». Nous parlons de la relation inverse ici ; la négation logique de « a est plus petit ou égal à b » serait « a est strictement plus grand que b », mais la relation inverse contient le couple (b,a) au lieu du couple (a,b).

Une relation d'ordre (non-totale) est une relation d'ordre sans la quatrième condition. Cela veut dire que *nous acceptons des éléments qui ne sont pas comparables à d'autres éléments*. Ceci est une notion qui généralise beaucoup la notion de « plus petit que ». Un exemple est le suivant : considérons comme ensemble de base *A*, un ensemble qui contient des sous-ensembles d'un autre ensemble (disons, *B*). En d'autres termes, *A* est une partie de *P(B)*. La relation « est un sous-ensemble de » est une relation d'ordre dans *A*, mais n'est pas nécessairement une relation d'ordre totale. Effectivement, considérons l'ensemble $B = \{a,b,c,d\}$, et l'ensemble $A = \{\{\}, \{a\}, \{b\}, \{a,b\}, \{c, d\}, \{a,b,c,d\} \}$.

$\{a\}$ est bien un sous-ensemble de $\{a,b\}$, et de $\{a,b,c,d\}$. $\{b\}$ aussi. Mais $\{a\}$ n'est pas un sous-ensemble de $\{b\}$, et $\{b\}$ n'est pas un sous-ensemble de $\{a\}$ non plus.

C'est donc vrai que d'une certaine façon, « est un sous-ensemble de » a des propriétés similaires que « est plus petit que », mais elle n'a pas la propriété de totalité, ce qui rend cette relation d'ordre différente.

Notez qu'au lieu d'exiger la réflexivité, nous pouvons aussi exiger l'**anti-réflexivité.** Alors nous avons **une relation d'ordre stricte**. Notez que, contrairement à ce que le nom implique, une relation d'ordre stricte, n'est pas une relation d'ordre.

A **toute relation d'ordre, correspond une relation d'ordre stricte, et vice versa.** Il suffit d'enlever tous les couples (a,a) de la relation d'ordre, pour en faire une relation d'ordre stricte,

et il suffit d'ajouter tous les couples *(a,a)* à un ordre strict, pour en faire une relation d'ordre.

L'exemple est bien sûr : « est plus petit ou égal » est une relation d'ordre ; « est strictement plus petit que » est une relation d'ordre stricte.

Pour la plus-part des applications, c'est une question de goût de travailler avec des relations d'ordre ou des relations d'ordre strictes.

Éléments maximaux et autres

Considérons une structure d'ordre *A, R*

Si *B* est un sous-ensemble de *A*, il peut avoir :

- des éléments maximaux (ou non)
- un plus grand élément (ou non)
- des majorants (ou non)
- une borne supérieure (ou non)
- des éléments minimaux (ou non)
- un plus petit élément (ou non)
- des minorants (ou non)
- une borne inférieure (ou non)

L'élément *m* est **un élément maximal** d'un ensemble *B* si *m* est un élément de *B*, tel qu'aucun élément *b* de *B* est plus grand que *m*. Si la relation *R* n'est pas totale, cela ne veut pas dire

que *m* est plus grand que *b* : il se peut que *m* et *b* ne sont pas comparables (que ni *(b,m)*, ni *(m,b)* sont dans *R*). *Si la relation d'ordre n'est pas totale, un sous-ensemble B peut avoir plusieurs éléments maximaux.*

L'élément *m* est **un plus grand élément** de *B*, par contre, si *m* appartient à *B* et *m* est plus grand que tout élément *b* de *B*. Cela veut dire que *m* doit être comparable à tous les éléments de *B*. *Il peut y avoir au plus un seul plus grand élément.*

Pour un ordre total, le plus grand élément, et l'élément maximal sont les mêmes notions. Pour un ordre qui n'est pas total, les deux notions sont différentes.

L'élément *m* est **un majorant de *B***, si *m* est plus grand que tout élément de *B*. Notez qu'il n'est pas exigé, contrairement à un élément maximal, que *m* appartienne à *B*. *Un sous-ensemble peut posséder plusieurs majorants.* S'il existe au moins un majorant, on dit que **le sous-ensemble *B* est majoré**.

Il va de soi quelles sont les définitions de : **élément minimal, plus petit élément et minorant.**

Finalement, **une borne supérieure est le plus petit élément de l'ensemble des majorants de *B*.** Comme c'est un plus petit élément, qui est unique s'il existe, *il ne peut y avoir qu'une seule borne supérieure.*

Automatiquement, **une borne inférieure est le plus grand élément de l'ensemble des minorants de *B***.

Si un sous-ensemble possède un plus grand élément, alors cet élément est aussi la borne supérieure. La borne supérieure est

le plus grand élément si elle appartient au sous-ensemble (ce qui n'est pas nécessairement le cas).

On peut conclure :

- La notion la plus forte est « le plus grand élément »
- Une notion moins forte est « borne supérieure »
- Une notion moins forte que « le plus grand élément », est « élément maximal » ; qui ne se distingue que dans le cas d'un ordre qui n'est pas total
- Une notion moins forte que « borne supérieure » est « majorant ».
- Un ensemble peut très bien ne pas avoir ni de majorant (et donc de facto ni de borne supérieure) ; ni d'élément maximal (et donc de facto ni de plus grand élément).

Considérons d'abord un exemple avec un ordre total, l'ordre des nombres rationnels. Nous parlons donc de la structure ordonnée totale : $\mathbb{Q}, <$.

Dans cette structure, nous considérons le sous-ensemble B des nombres de la forme de $-1/n$, où n est un nombre naturel (dans $\mathbb{N}\backslash\{0\}$), donc $B = \{-1, -1/2, -1/3, -1/4 \ldots\}$.

L'ensemble B possède un plus petit élément : c'est -1. Par contre, l'ensemble B ne possède pas un plus grand élément. Effectivement, imaginons que $-1/m$ soit ce plus grand élément. Alors, $-1/(m+1)$ appartient aussi à B, et est plus grand que $-1/m$, donc $-1/m$ ne pouvait pas être ce plus grand élément. Tous les nombres rationnels positifs sont des majorants. Il y a bien un

plus petit élément de l'ensemble des nombres rationnels positifs : l'élément zéro. 0 est donc la borne supérieure de notre ensemble B ; mais nous voyons que cette borne supérieure n'appartient pas à B même (il n'y a aucun nombre naturel n, tel que $-1/n = 0$).

Nous voyons donc que l'ensemble B possède un plus petit élément : -1, et une borne supérieure, 0.

Considérons maintenant un autre sous-ensemble des nombres rationnels : les nombres entiers, $\mathbb{Z}$. $\mathbb{Z}$ n'a pas de plus grand élément, ni de plus petit élément. $\mathbb{Z}$ n'a pas de majorant non plus : aucun nombre rationnel est plus grand que chaque nombre entier. De la même façon, $\mathbb{Z}$ n'a pas de minorant. Alors $\mathbb{Z}$ n'a pas de borne supérieure, ni de borne inférieure.

En suite, nous allons considérer un ordre qui n'est pas total : la relation « est diviseur de » dans les nombres naturels non-zéro. Il faut peut-être se convaincre que cette relation est bien un ordre, c'est laissé comme exercice. Il faut vérifier que cette relation est réflexive, anti-symétrique et transitive.

Considérons l'ensemble des nombres naturels de 1 à 15. On peut vérifier que 1 est le plus petit élément de cet ensemble. Effectivement, 1 divise tous les nombres de l'ensemble. Par contre, il n'y a pas de plus grand élément : il n'y a pas de nombre dans cet ensemble qui est divisé par tous les nombres de l'ensemble. Mais il y a des éléments maximaux : il y a des éléments qui ne divisent rien d'autre. Ce sont 8, 9, 10, 11, 12, 13, 14 et 15. Il y a des majorants, ce sont tous les nombres naturels qui ont comme diviseurs, tous les éléments de

l'ensemble. La borne supérieure est alors le plus petit multiple commun, à savoir $2^3\ 3^2\ 5\ 7\ 11\ 13 = 360\ 360$.

Applications entre structures d'ordre

Une application *f* d'une structure d'ordre *A*, ≤ en *B*, ≤ tel que, si $a \leq b$ alors $f(a) \leq f(b)$ est appelé **une application croissante**. La composition de deux applications croissantes est une application croissante.

Une application croissante garantit la préservation du plus grand et plus petit élément et la préservation de la notion de majorant et minorant. Par contre, elle ne garantit pas la préservation des notions d'élément maximal et de borne supérieure (ou inférieure), car il se peut que dans la structure d'ordre *B*, $f(x)$ et $f(y)$ sont comparables, tandis que x et y ne le sont pas.

Par exemple, l'application identique de $\mathbb{N}$ en $\mathbb{N}$ est une application croissante entre $\mathbb{N}, |$ et $\mathbb{N}, \leq$ (où l'on entend par |, « est diviseur de », ce qui est un ordre partiel). Si $x \mid y$, alors $f(x) \leq f(y)$ (c.a.d. $x \leq y$, car c'est l'application identique). Par contre, dans les nombres de 1 à 15, les éléments de 8 à 15 étaient des éléments maximaux pour |, mais ne le sont pas pour ≤. Les majorants (multiples de 360 360) pour | sont bien des majorants pour ≤ aussi, mais il y en a pleins d'autres (15, 16, 17, … par exemple), et la borne supérieure qui était 360 360 pour |, est 15 pour ≤.

Pour que toutes les notions liées à la structure d'ordre se transmettent, il faut que l'application soit bijective et « croissante dans les deux sens », c.a.d. :

$x \leq y$ si et seulement si $f(x) \leq f(y)$

Nous parlons, dans ce cas, d'**un isomorphisme d'ordre**.

Comme d'habitude, un isomorphisme d'ordre entre deux structures d'ordre rend les deux structures identiques, pour ce qui concerne l'ordre.

S'entraîner

1. Vérifiez que la relation « est un sous-ensemble de » dans un sous-ensemble de $P(A)$, est une relation d'ordre.

2. Vérifiez que la relation « est un diviseur de » dans les nombres naturels non-nuls est une relation d'ordre.

3. Considérez l'ensemble A des sous-ensembles de $\mathbb{Q}$: $\{x \in \mathbb{Q} | x < 1/n\}$ pour tous les n naturels non-nuls, et considérez la structure d'ordre $P(Q)$ et « est un sous-ensemble de ». Est-ce qu'il y a un plus petit élément dans A ? Est-ce qu'il y a des minorants de A ? Est-ce qu'il y a une borne inférieure à A ? Est-ce qu'il y a un plus grand élément dans A ? Est-ce qu'il y a des majorants de A ? Est-ce qu'il y a une borne supérieure à A ?

Structures topologiques

Notions d'union et d'intersection

Nous connaissons la notion d'union de deux ensembles et d'intersection de deux ensembles. Mais nous allons élargir ces notions à la notion d'union et d'intersection d'un ensemble de sous-ensembles.

Considérons Z qui est une partie de *P(A)*, c'est à dire : *Z* est un ensemble de sous ensembles de *A*. Nous définissons l'union de *Z* :

$$\cup Z = \{x \in A | \exists W \in Z : x \in W\}$$

c'est à dire : $\cup Z$ est un sous ensemble de *A*, tel qu'il contient les éléments de *A* qui appartiennent à au moins un ensemble dans *Z*.

Nous avons immédiatement que cette nouvelle notion d'union se réduit à l'ancienne quand nous avons deux sous ensembles de *A* : $\cup \{B,C\} = B \cup C$.

Notez que cette union comme nous l'avons introduite existe toujours, car il s'agit de la définition correcte d'un sous ensemble de *A* : le prédicat « il existe un *W* de *Z* tel que *x* appartient à *W* » est un prédicat en *x*, bien défini sur *A*.

Il y a une notion équivalente pour l'intersection :

$$\cap Z = \{x \in A | \forall W \in Z : x \in W\}$$

Quelques exemples peuvent illustrer ces notions. Considérez les intervalles $]x-1,x+1[$, qui sont des sous-ensembles de $\mathbb{R}$.

L'ensemble de toutes ces intervalles pour toutes les valeurs *x* s'appellera *Z*. Alors, l'union de *Z* sera ℝ en entier.

Considérez maintenant toutes les intervalles *]-1/n,1/n[* qui sont des sous-ensembles de ℝ. L'ensemble de toutes ces intervalles pour toutes les valeurs de *n* (nombre naturel non-zéro) s'appellera *W*. L'intersection de *W* sera {0}. Effectivement, 0 est le seul élément qui appartient à toutes ces intervalles. C'est une propriété remarquable : nous avons un ensemble d'intervalles ouvertes, et l'intersection de deux intervalles ouvertes est toujours une intervalle ouverte. Mais l'intersection d'un ensemble infini d'intervalles ouvertes donne lieu à un seul point, qui n'est forcément pas une intervalle ouverte. Cette observation sera très importante.

Définition de topologie

Une structure topologique, qui s'appelle aussi **un espace topologique**, est une structure qui consiste d'un ensemble de base *A*, et une partie *T* de *P(A)*, qui s'appelle **une topologie sur *A***. Un espace topologique se distingue donc des autres structures par le fait qu'il ne contient pas de relation, mais un ensemble de sous-ensembles.

Une topologie, *T*, partie de *P(A)*, sur *A*, doit satisfaire les exigences suivantes :

1. **{} doit appartenir à *T***
2. ***A* doit appartenir à *T***

3. **Si *U* et *V* appartiennent à *T*, alors l'intersection *U* ∩ *V* doit appartenir à *T***
4. **Si *X* est une partie de *T*, alors l'union de tous les éléments de *X*, ∪ *X*, doit appartenir à *T***

C'est une liste bien étrange. Mais on peut comprendre un peu plus cette définition quand on pense à une situation géométrique, et **on appelle les éléments de *A*, des « points », et les éléments de *T*, des « ouverts ».**

L'intersection de deux ouverts est bien un ouvert ; l'union d'autant d'ouverts qu'on veut est aussi un ouvert. La notion de structure topologique est inspirée par les parties « ouvertes » (c.a.d. sans bord) de la géométrie.

La notion qu'une structure topologique veut introduire, est la notion de « infiniment proche », sans nécessairement vouloir dépendre d'une « mesure quantitative » de la proximité. En d'autres termes, une structure topologique veut être la notion la plus abstraite de la notion d'infiniment proche (et les notions associés de limite, continuité, bord, intérieur et autres). Pour cela, une structure topologique introduit la notion de « jeux de voisinages d'un point ». *Si quelque chose se passe « dans tous les voisinages d'un point » alors on dit que cela se passe « infiniment proche de ce point ».* **Une structure topologique permet de définir ce que l'on entend par « jeu de voisinages d'un point ».**

***V*, sous-ensemble de *A*, est un *voisinage* du point *x*, s'il existent des éléments de *T* qui contiennent *x* et qui sont un sous-ensemble de *V*.**

L' *environnement* d'un point *x* dans une structure topologique *A, T,* noté *B(x),* est l'ensemble de tous les voisinages du point *x*. *B(x)* est une partie de *P(A).*

Souvent, il suffit de travailler avec un jeu de voisinages restreint. C'est ce que nous avions utilisé dans le premier volume, « Les ensembles », quand nous avions introduit la notion de limite.

Une base d'environnement d'un point *x* *E(x)* dans une structure topologique *A, T,* est une partie de l'environnement *B(x)*, tel que pour tout *V* de *B(x)*, il existe un *W* de *E(x)*, qui est un sous ensemble de *V*.

La plupart des notions topologiques (dont la limite, et la continuité) nécessitent seulement que cela se passe dans une base d'environnement d'un point ; il en suit alors que cela se passe aussi dans tout l'environnement.

Les topologies « normales » ont une propriété supplémentaire qui est la séparabilité. Une topologie **séparable** s'appelle aussi une topologie **Hausdorff**. Il s'agit de la propriété suivante : **si *x* et *y* sont deux points différents de *A*, alors il existe des voisinages de *x* et il existe des voisinages de *y* qui sont disjoint (leur intersection est nulle).**

Intuitivement, une topologie Hausdorff « sépare » chaque point d'un autre. Si la topologie n'est pas Hausdorff, il y a des points qui ne peuvent pas être séparés, même si on les regarde de façon infiniment proche.

Exemples

Il y a deux topologies « bizarres » sur tout ensemble : la topologie triviale, et la topologie discrète.

La topologie triviale sur *A*, est *{ {}, A}*. On peut vérifier que c'est bien une topologie. Tous les environnements de tous les points sont { *A* }. On ne peut pas faire grand-chose avec cette topologie, mais elle existe.

Notez que la topologie triviale n'est pas Hausdorff.

La topologie discrète sur *A*, est *P(A)*. Une base topologique d'un point *x*, est { {*x*} }. On ne peut pas faire grand-chose non plus avec cette topologie, mais elle existe. La topologie discrète est Hausdorff.

La structure topologique standard des nombres réels est l'ensemble de tous les sous-ensembles de nombres réels ouverts. Par exemple, toutes les intervalles de type *]a,b[* font partie de cette topologie ; mais aussi toutes les combinaisons possibles : *]a,b[* ∪ *]c,d[* ∪ *]e,f[*.

Un sous-ensemble ouvert standard sur les nombres réels *O* est normalement défini comme un ensemble de nombres réels, tel que pour chaque élément x de cet ensemble, il existe une intervalle ouverte *]a,b[* contenant *x*, tel que *]a,b[* est une partie de *O*. C'est pour cela qu'un sous-ensemble ouvert standard ne peut pas contenir « un bord » car ce bord ne peut jamais être inclus dans une intervalle *]a,b[*, tel que cette intervalle fasse partie de l'ensemble en question.

Il faut noter que la topologie standard contient des sous-ensembles qui peuvent sembler bizarre. Par exemple, l'ensemble des nombres réels qui ne sont pas des nombres entiers est un élément de la topologie standard. Par contre, l'ensemble des nombres réels qui ne sont pas des nombres rationnels, n'en fait pas partie (exercice : pourquoi?).

L'environnement d'un élément réel *x*, contient tout sous-ensemble de nombres réels, tel qu'il contient une intervalle *]a,b[* qui contient lui-même, le point *x*. Notez que l'environnement contient beaucoup d'ensembles de réels qui ne sont pas des ensembles ouverts eux-mêmes.

Une base d'environnement d'un nombre réel est ce que nous avions introduit précédemment dans le volume « ensembles » :

C'est l'ensemble des intervalles $]x - 1/n, x+1/n[$ (pour n un nombre naturel non-nul) que nous avions appelé par abus de langage, *l'environnement*, au lieu de *base d'environnement*. Aussi, nous l'avions introduit comme une suite ; strictement parlé, ce n'est que l'ensemble (l'image de la suite) qui est la base d'environnement.

Intérieur, bord, ensemble fermé…

Un espace topologique introduit plusieurs propriétés d'ensembles et de relations entre points et ensembles. Si *A,T* est un espace topologique, et *X* est un sous-ensemble de *A*, alors on dit qu'**un point *x* est un point intérieur à *X*, si *X* est un voisinage de *x***.

Cela vient à exiger qu'il y ait un ouvert (dans *T*) qui contient *x*, et qui est un sous-ensemble de *X*. On peut définir **l'intérieur d'un ensemble *X*, comme tous les points intérieurs de *X***.

Dans la topologie discrète, tout point appartenant à *X* est « un point intérieur à X », et l'intérieur de tout ensemble *X*, est *X* lui-même.

Un point *x* est adhérent à l'ensemble *X*, si tout voisinage de *x* contient des points de *X*. Notez que *x* ne doit pas nécessairement appartenir à *X*. Forcément, si *x* appartient à *X*, *x* est aussi un point adhérent à *X*, mais ce qui nous intéresse surtout, ce sont les points qui n'appartiennent pas à *X*, mais qui y sont adhérents. **L'ensemble de tous les points adhérents à *X*, s'appelle *la fermeture de X*. *X* est une sous-partie de sa fermeture.** Il faut imaginer la fermeture comme « ajouter le bord ». Dans une topologie discrète, tout ensemble est sa propre fermeture. Dans la topologie triviale, la fermeture de tout ensemble non-vide est l'ensemble de base *A* en entier.

Un point *x* se trouve sur le bord (ou la frontière) d'un ensemble *X*, si *x* est adhérent à *X* mais ne fait pas partie de son intérieur. L'ensemble des points sur le bord, est le bord de *X*. On peut le définir comme **la fermeture de *X* moins l'intérieur de *X*.**

Un ensemble fermé est le complément d'un ensemble ouvert (c.a.d. un élément de la topologie). *X* est fermé, si $A \setminus X$ est un élément de *T*. Le bord d'un ensemble est toujours fermé. Notez qu'un ensemble fermé peut aussi être ouvert en même

temps : il suffit que cet ensemble et son complément sont tous les deux des éléments de *T*.

Une illustration simple dans la topologie standard de $\mathbb{R}$:

Les intervalles]-2,3],]-2,,3[, [-2,3] et [-2,3[ont le même intérieur : l'intervalle]-2,3[ouverte. Ils ont tous aussi la même fermeture : l'intervalle [-2,3]. Finalement, ils ont tous le même bord : {-2, 3} (donc deux points).

Dans la topologie standard sur $\mathbb{R}$, si on considère $\mathbb{Q}$ (l'ensemble des nombres rationnels), alors :

- $\mathbb{Q}$ n'a pas de points intérieurs. L'intérieur de $\mathbb{Q}$ est {}.
- La fermeture de $\mathbb{Q}$ est $\mathbb{R}$.
- Le bord de $\mathbb{Q}$ est $\mathbb{R}$.

Dans la topologie standard sur $\mathbb{R}$, si on considère *X* l'ensemble des fractions *1/n* avec *n* un nombre naturel non nul, alors *X* n'a pas de points intérieurs. La fermeture de *X* est $X \cup \{0\}$, et c'est aussi son bord. Effectivement, le point 0 est bien un point adhérent à *X*, mais n'appartient pas à *X*, car tout voisinage de 0 contient bien un *1/n* avec *n* suffisamment grand.

Dans la topologie triviale, tous les points sont adhérents à tous les autres points, la fermeture de toute partie de *A* est *A* même, et l'intérieur de tout sous-ensemble de *A*, sauf *A* même, est {}. L'intérieur de *A* est *A*. Ainsi, a part *A*, aucun sous-ensemble de *A* n'a de point intérieur. Ainsi, le bord de tout sous-ensemble, sauf *A* même, est *A*. Le bord de *A*, par contre, est {}.

Limite de suite

Une suite dans un espace topologique est une application des nombres naturels dans l'ensemble de base : $n \rightarrow a_n$

Une suite est dite « convergente vers *a* » si, pour tout voisinage de *a*, il existe un *N*, tel que tout a_n appartient à ce voisinage, si $n > N$.

Il suffit d'exiger cela non pas pour tous les voisinages, mais pour tous les voisinages qui font partie d'une base d'environnement. Effectivement, tout voisinage contient un voisinage dans la base d'environnement ; si la propriété est valide pour ce dernier, forcément elle est aussi valide pour le voisinage contenant ce dernier avec la même valeur de *N*.

Il est souvent plus facile de prouver cette propriété pour une base d'environnement que pour l'environnement même.

Bien sûr, il se peut qu'une suite n'ait pas de limite dans un espace topologique.

Si la topologie est Hausdorff, alors une limite est unique : il ne peut pas y avoir deux éléments différents tel que la même suite ait les deux éléments comme limite.

Par contre, dans une topologie qui n'est pas Hausdorff, ceci est parfaitement possible. En fait, *dans la topologie triviale, toute suite converge vers tous les éléments de A !*

On peut démontrer cela facilement. Considérons n'importe quel élément a de *A*. Le voisinage de *a* est { *A* }. Pour tout voisinage (à savoir, pour *A*), on peut choisir un nombre *N*,

disons, 1, tel que, pour tout $n > N$, a_n appartient à A. C'est le cas, car la suite est une application dans A, donc tous les a_n appartiennent à A.

Dans la topologie discrète, une suite converge seulement, si elle est constante à partir d'un certain N. Effectivement, admettons que a soit la limite de la suite. Comme $\{a\}$ appartient à l'environnement de a (topologie discrète), la seule façon pour que la suite converge vers a, est que, pour un certain N, si $n > N$, alors $a_n = a$.

Fonction continue, homéomorphisme

Une fonction *f* d'un espace topologique dans un autre est continue en *a*, point de son domaine, si pour tout voisinage *W* de *f(a)*, il existe un voisinage *V* de *a*, tel que l'image de *V* sous *f* est un sous-ensemble de *W*.

Notez que la continuité dépend de *deux* espaces topologiques. Toute fonction *dans* un espace topologique trivial est continue en tout point. Toute fonction *à partir d*'un espace topologique discret est continue en tout point (exercice pour le lecteur).

Une fonction qui est continue en tout point de son domaine est une fonction continue.

Un homéomorphisme entre deux espaces topologiques est :

- **une bijection entre les deux ensembles de base**
- **qui est continue**
- **dont l'inverse est continue**

Si un homéomorphisme existe entre deux espaces topologiques, alors pour tout ce qui concerne la topologie, les deux structures sont identiques. L'homéomorphisme est à l'espace topologique, ce que l'isomorphisme est à la structure algébrique.

S'entraîner

1. Considérez l'ensemble $A = \{1,2,3\}$. $T = \{ \{\},\{1,2\}, \{2,3\}, \{1,2\}, \{1,2,3\}\}$. Est-ce que A,T est un espace topologique ?

2. Considérez $A = \{1,2,3\}$. $T = \{\{\},\{1,2\},\{1,2,3\} \}$. Est-ce que A,T est un espace topologique ? Est-ce que cet espace est Hausdorff ?

3. a) Prenez l'espace topologique de l'exercice 2. Considérez la suite suivante : si n est pair, alors $a_n = 1$; si n est impair, alors $a_n = 2$. Est-ce que cette suite converge dans A, T ? Quelle est la limite ou quelles sont les limites de cette suite ?

3. b) Même questions, mais maintenant, la suite est : si n est pair, alors $a_n = 3$; si n est impair, alors $a_n = 2$.

4. Démontrez que si V,T est un espace topologique, et W,S est un espace topologique, et f est un homéomorphisme de V,T en W,S, alors : si a_n est une suite qui converge vers a en V,T, alors $b_n = f(a_n)$ est une suite qui converge vers $f(a)$ en W,S.

Espaces métriques

Notions, définition

Un espace métrique est une généralisation et une abstraction de l'idée de « distance » dans la géométrie Euclidienne. On a distillé les propriétés essentielles de ce qui fait de la distance Euclidienne une notion de « distance », et on est arrivé à la liste suivante :

1. Une distance est un nombre réel positif
2. Quand la distance entre deux points *x* et *y* est 0, alors ce sont les deux mêmes points.
3. La distance « aller » est la même que la distance « retour ».
4. La distance « par un détour » est toujours plus longue que la distance directe, c.a.d. la distance entre *x* et *y* plus la distance entre *y* et *z* est une somme plus grande que la distance directe entre *x* et *z*.

De cela, on a fabriqué une structure abstraite : l'espace métrique. Un espace métrique est un ensemble de base, *V*, équipé d'une application distance *d* :

$d : V \times V \rightarrow \mathbb{R}^+ : (x,y) \rightarrow d(x,y)$

qui satisfait les propriétés suivantes :

- $d(x,y) = 0 \Rightarrow x = y$
- $d(x,y) = d(y,x)$

- $d(x,y) + d(y,z) \geq d(x,z)$

L'exemple-type est bien sûr la distance Euclidienne dans $\mathbb{R}^n$, qui a inspiré cette notion. Dans $\mathbb{R}$ même, $d(x,y) = |x - y|$ est une distance qui fait de $\mathbb{R}$ un espace métrique.

Mais on peut introduire d'autres distances dans $\mathbb{R}^n$. Par exemple, la « métrique taxi », inspirée par la distance parcouru par un taxi dans une ville Américaine au plan de rue quadrillé :

$$d(x,y) = |x_1 - y_1| + |x_2 - y_2| + \ldots + |x_n - y_n|$$

C'est laissé comme exercice de vérifier que cette fonction est bien une distance.

Topologie induite par une structure métrique

Une des propriétés les plus importantes d'une structure métrique, c'est qu'elle définit automatiquement une topologie Hausdorff sur l'ensemble de base.

Il suffit de reconnaître que **les « boules ouvertes » autour d'un point *x*, c'est à dire, les ensembles de points *y* tel que $d(x,y) < 1/n$, forment une base d'environnement pour le point *x*.**

On peut effectivement démontrer qu'a partir de ces bases d'environnements, on peut construire une topologie unique : la topologie induite par la distance $d(x,y)$.

Le point important est que la topologie induite par une distance donne lieu aux notions de convergence et de continuité.

Quelque part, il n’est pas nécessaire de passer par une topologie et on peut définir les notions de convergence et de continuité avec des « jeux de boules ouvertes » ; c’est en fait une abstraction plus poussée de ces notions qui sont à la base de l’idée d’espace topologique. La notion de continuité et de convergence dans un espace topologique est plus générale et plus abstraite que la notion de continuité et de convergence avec des boules ouvertes.

On peut démontrer que la métrique Euclidienne, et la métrique taxi, donnent lieu à la même topologie (standard) sur $\mathbb{R}^n$, cela veut dire que l’ensemble des ouverts est la même.

Ainsi, toute forme de convergence ou de limite pour la distance standard Euclidienne, est aussi une forme de convergence et de limite pour la distance taxi, et vice versa.

Épilogue

Cet ouvrage est la suite de l'ouvrage « Les ensembles », mais l'esprit en est différent. Là où je suis convaincu qu'il est impossible de comprendre correctement le programme du lycée sans les notions abordées dans « les ensembles », il n'en est pas de même pour « les structures ». On peut parfaitement assimiler le programme du lycée sans ces notions. Seulement, les notions dans cet ouvrage étaient bien enseignées au lycée il y a 40 ans. A quoi servaient-ils alors ? Les structures donnent une vision plus profonde sur les mathématiques enseignés au lycée, et permettent de prendre du recul, d'avoir une vision structurée de la matière, et de comprendre ce qui est essentiel dans les notions apprises ; c'est d'ailleurs pour cela qu'elles ont été inventées par les mathématiciens.

Ainsi, les mathématiques sont bien plus vastes que les notions abordées au lycée, mais ces notions abordées au lycée contiennent déjà beaucoup de notions plus générales que pourrait paraître dans la mise en œuvre au lycée ; c'est justement ces notions plus générales qui sont distillées par les structures, inspirées par les objets mathématiques abordées au lycée.

Ainsi, *les structures font sortir le vaste potentiel de l'investissement fait par les apprentissages au lycée et permettent d'en ouvrir la profondeur*. En d'autres termes, une fois qu'on a vu des notions topologiques, on ne regarde plus une intervalle ouverte de la même façon, on a une compréhension plus profonde de la notion d'ouvert. Une fois

qu’on a vu la notion de groupe, on ne regarde plus aucune opération de la même façon. Une fois qu’on a vu un espace vectoriel, on ne regarde plus une matrice ou un système d’équations linéaires de la même façon. On comprend ces notions élémentaires de façon beaucoup plus profonde maintenant. On en a saisi l’essentiel. On les a placé dans le cadre des mathématiques.

Les structures distillent donc de façon abstraite, des notions mathématiques essentielles qui étaient présentes « par hasard » dans les objets mathématiques étudiés au lycée, mais ayant une importance qui va bien au-delà de ces objets mathématiques et qui sont donc bien plus universelles. Elles permettent donc d’en approfondir la compréhension. On se défait du superflu des notions concrètes du lycée, pour mieux voir l’essentiel dans ces notions et ne pas embrouiller sa pensée par ce qui nous distrait : *c’est l’exercice d’abstraction même, et le cœur des mathématiques*.

Il y a 40 ans, un bon élève d'une filière mathématique n'avait pas trop de problèmes à assimiler la notion de structure, et avait donc ce recul sur les mathématiques qu'il avait appris ; il n'y a pas de raison de priver le bon lycéen d'aujourd'hui de ce même recul.