Les **structures algébriques**

INDISPENSABLES

Les structures algébriques regroupent un grand nombre de concepts fondamentaux en mathématiques. L'importance des structures algébriques est telle que sans elles, les mathématiques n'existeraient quasiment pas. Sans structures, effectuer de simples opérations telles que des additions serait impossible. Les structures algébriques ont toutes en commun le fait de permettre de définir des opérations dans des ensembles.
Par exemple, l'addition et la multiplication des nombres entiers sont des opérations que l'on apprend dès le plus jeune âge. Néanmoins, ces deux opérations n'ont pas les mêmes propriétés. L'étude des structures algébriques permet de créer des opérations plus complexes que de simples additions, d'étudier leurs propriétés, et d'unifier dans une théorie unique toutes les opérations.

LES LOIS DE COMPOSITIONS INTERNES

Les mathématiques adoptent un vocabulaire précis pour désigner une opération. On utilise le terme de loi de composition interne.
Dans un ensemble, noté E, une loi de composition interne de E, notée par exemple *, est une opération qui permet d'associer, à deux éléments quelconques x et y de E, un troisième élément noté x*y.
Ainsi, si E désigne l'ensemble des entiers naturels N, c'est-à-dire l'ensemble des nombres entiers positifs {0 ; 1 ; 2 ; 3…} et que l'on choisit d'étudier l'addition (notée +), à deux éléments de E, 3 et 4 par exemple, on associe l'entier 3+4, c'est-à-dire 7.
En mathématiques, on n'appelle donc plus cela une opération, mais une loi et cette loi est dite interne car à deux éléments de E, elle associe encore un élément de E. Autrement dit, on se place toujours dans le même ensemble.
Cependant, toutes les lois n'ont pas les mêmes propriétés. Suivant les propriétés de la loi choisie, il est possible de définir des structures algébriques différentes. Les plus utilisées en mathématiques sont le groupe, l'anneau, le corps et l'espace vectoriel.

Un peu de vocabulaire

• Si $x*y=y*x$ alors la loi * est dire commutative.
C'est le cas de l'addition. En effet, pour tout nombre a et b, a+b = b+a.
Cependant, il existe des lois non commutatives comme la division : 1 divisé par 3 est différent de 3 divisé par 1.
• La loi * sera dite associative si lorsque l'on prend trois éléments x, y et z dans E, on a la relation $x*(y*z)=(x*y)*z$. En d'autres termes, l'ordre des opérations n'a pas d'importance. C'est le cas de l'addition. Effectuer x+(y+z) ou (x+y)+z donne le même résultat. Pour cette raison, le plus souvent, les parenthèses sont oubliées.
• S'il existe deux lois de composition internes sur E, notées * et #, on dit que * est distributive à gauche par rapport à # si $x*(y\#z)=(x*y)\#(x*z)$. De même, on dit que * est distributive à droite par rapport à # si $(y\#z)*x=(y*x)\#(z*x)$.
En général, on parle de distributivité sans autre précision, il s'agit alors de distributivité à droite et à gauche.
Par exemple, la multiplication est distributive par rapport à l'addition :

$$\begin{cases} x\times(y+z)=(x\times y)+(x\times z) \\ (y+z)\times x=(y\times x)+(z\times x) \end{cases}$$

Les lois de composition internes courantes

• L'addition, +, dans N, Z, Q, R ou C.
• La soustraction, –, dans les mêmes ensembles.
• La multiplication, dans les mêmes ensembles.
• La division, /, dans Q^*, R^* ou C^*.
• La composition des fonctions, ∘, dans l'ensemble des applications de E dans E.

LES GROUPES

Soit E un ensemble muni d'une loi de composition interne *.
(E,*) forme un groupe si les trois propriétés suivantes sont réunies :
• * est associative.
• * possède un élément neutre noté « e » : pour x dans E, e*x=x et x*e=x. Dans le cas de l'addition, l'élément neutre est 0. En effet, pour tout x, x+0 = x et 0+x = x.
• Tout élément de E possède un inverse pour *. Cela signifie que pour tout élément x de E, il existe un élément y de E tel que x*y = e. Dans le cas de l'addition l'inverse de x est ce que l'on a l'habitude de noter –x car x+(-x) = 0 et 0 est bien l'élément neutre.
Il faut cependant faire attention à notre instinct qui nous pousse à penser en premier lieu à des opérations telles que l'addition ou la multiplication. Un groupe ne possède que ces trois propriétés et écrire x*y = y*x est faux en général !
Un groupe dans lequel cette relation est vérifiée est dit commutatif ou abélien.
Il suffit de penser à la division : x divisé par y est le plus souvent différent de y divisé par x.
Il faut également faire attention à l'ensemble dans lequel les opérations sont effectuées. Une loi de composition interne peut très bien définir un groupe dans un certain ensemble sans que cela soit le cas dans un autre ensemble.
Par exemple, (Z,+) où Z est l'ensemble des entiers relatifs, c'est-à-dire positifs et négatifs, est un groupe.
Dans Z, on a bien x+(y+z) ou (x+y)+z.
0 est neutre : pour tout x, x+0 = x et 0+x = x.
Tout nombre x a un inverse : -x.
Cependant (N,+) où N est l'ensemble des entiers naturels n'est pas un groupe car on ne peut trouver d'inverse pour tous les nombres. L'inverse de 3 devrait être -3, mais N ne contient pas les nombres négatifs !
Un groupe est donc formé par deux objets mathématiques : un ensemble et une loi de composition interne vérifiant les trois propriétés ci-dessus. On dit que la loi confère à l'ensemble une structure de groupe.

Quelques propriétés des groupes

À partir de la définition, les propriétés suivantes peuvent être démontrées :
• L'élément neutre est unique. Ceci est important car la définition affirme son existence mais non son unicité.
• L'inverse de l'élément neutre est l'élément neutre lui-même.
• L'inverse d'un élément est unique.
Examinons le cas de la multiplication dans R^* (l'ensemble des nombres réels privé de 0) : on constate que $(R^*, \times)$ est un groupe et que ces propriétés sont vérifiées.
L'élément neutre est 1 car pour tout x de R^*, $X\times 1 = x$ et $1\times x = x$. À part 1, aucun autre nombre ne vérifie cette équation.
L'inverse d'un élément x est 1/x. Par exemple, l'inverse de 3 est 1/3 car $3\times 1/3 = 1/3\times 3 = 1$ et aucun autre nombre à part 1/3 ne vérifie cette équation.
La force des structures apparaît ici. Que l'on considère l'addition, ou bien la multiplication ou n'importe quelle autre loi faisant d'un certain ensemble un groupe, les propriétés ci-dessus, démontrées dans le cas général, seront toujours vérifiées.

Morphismes de groupes

• Soient (G, *) et (H, T) deux groupes. Une application de G dans H est un « morphisme de groupes » lorsque pour tout x, y éléments de G, f(x*y) = f(x) T f(y).
• Si G = H et * = T, on parle d'endomorphisme.
• Si f est bijective, on parle d'isomorphisme.
• Si f est un endomorphisme bijectif, on parle d'automorphisme.

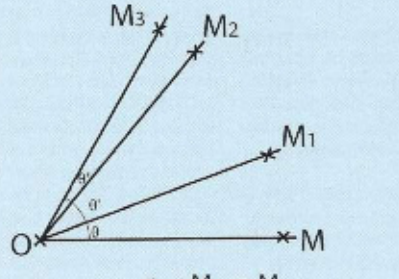
Exemples

• $x \to 2^x$ réalise un isomorphisme de $(R, +)$ sur $(R^*, \times)$;
• $x \to 2x$ réalise un automorphisme de (R, +) ;
• $x \to 3\ln(x)$ réalise un isomorphisme de $(R^*, *)$ sur (R, +) ;
• $z \to |z|$ réalise un morphisme de $(C^*, \times)$ dans $(R^*, \times)$.
L'idée de morphisme vient du fait que pour certaines applications (appelées alors des morphismes), les opérations effectuées sur des éléments ont lieu également sur leurs images. De cette constatation découlent les propriétés suivantes.

Propriétés élémentaires des morphismes de groupes

Soient (G, *) et (H, T) deux groupes et f un morphisme de (G, *) dans (H, T).
• Si on note « e » le neutre de G

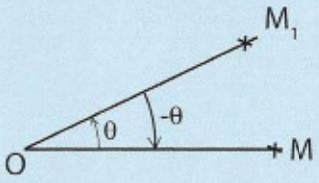
Un exemple : le groupe de rotaton simple



$r_\theta : M \to M_1$
$r_{\theta'} : M_1 \to M_2$
$r_{\theta''} : M_2 \to M_3$
$r_{\theta'} \circ r_\theta : M \to M_1 \to M_2$

1. La composée, notée ∘, est une loi de composition interne.
$r_\theta \circ r_{\theta'} = r_{\theta+\theta'}$

2. La composition ∘ est une loi associative.
$r_{\theta''} \circ (r_{\theta'} \circ r_\theta) = (r_{\theta''} \circ r_{\theta'}) \circ r_\theta$



$r_\theta \circ r_{-\theta} : M \to M_1 \to M$
$r_\theta \circ r_{-\theta} = r_0$

3. L'élément neutre est la rotation r_θ d'angle nul.

2. L'inverse de la rotation r_θ est la rotation $r_{-\theta}$.

Les chiffres algébriques

1825

Niels Abel introduit la notion de nombre algébrique.

1829

Évariste Galois introduit la théorie des groupes.

1830

Augustin Cauchy introduit la notion de groupe de permutation.

0

Élément neutre pour l'addition et la soustraction et absorbant pour la multiplication.

1

Élément neutre pour la multiplication.

Magma

$(\mathbb{N},+)$

Structure avec **1** seule loi de composition interne

La structure **la plus simple**

alors f(e) est le neutre de H.
• Pour x dans G, si on note x-1 l'inverse de X dans G alors $f(x^{-1})$ est l'inverse de f(x) dans H. Autrement dit, l'inverse de l'image est égal à l'image de l'inverse : $(f(x))^{-1} = f(x^{-1})$
En résumé, les groupes sont des ensembles dans lesquels il existe une opération appelée loi de composition interne possédant des propriétés particulières et ces groupes englobent une grande partie des opérations que l'on utilise chaque jour. Cependant, la structure de groupe possède une faiblesse. Dans un groupe, une seule loi est disponible alors que l'on est souvent amené en mathématiques à manipuler plusieurs lois à la fois. Les concepts d'anneaux et de corps permettent de pallier cette faiblesse.

LES ANNEAUX

Les structures d'anneau et de corps sont des enrichissements de la structure de groupe. Un anneau (ou un corps) est un groupe muni d'une deuxième loi interne. Cette deuxième loi n'aura généralement pas, pour la structure d'anneau, toutes les propriétés de la première. Il lui manquera en particulier l'existence d'un inverse pour chacun des éléments de l'anneau. La seconde loi d'un corps possèdera, quant à elle, toutes les propriétés de la première. La structure d'anneau sera le plus souvent rencontrée sur des ensembles de fonctions ou de matrices. Celle de corps, beaucoup plus rare, est celle des ensembles Q, R et C munis de leurs lois additives et multiplicatives. Par analogie avec l'addition et la multiplication, les deux lois d'un anneau sont souvent notées + et x. Cela permet de manipuler des symboles familiers. Il faut néanmoins faire attention car, en règle générale, il ne s'agit pas de l'addition ni de la multiplication classiques des nombres ! La définition d'un anneau est la suivante. Un anneau est un ensemble muni de deux lois internes + et x telles que :
• (A, +) est un groupe commutatif de neutre noté 0_A (par analogie avec l'addition).
• La loi x est une loi de composition interne sur A associative et distributive à gauche et à droite par rapport à +.
• La loi x admet un neutre différent de 0_A, note 1_A (par analogie avec la multiplication).
Si la loi x est commutative, l'anneau est dit commutatif ou abélien.

UN PREMIER EXEMPLE

Soit F l'ensemble des fonctions numériques réelles.
Pour deux fonctions, f et g de F, on définit la somme f+g de la façon suivante.
f+g est la fonction qui à un x associe f(x)+g(x). Autrement dit $(f+g) : x \to f(x)+g(x)$. Faire la somme de deux fonctions, revient à faire la somme de leur image.
De même, la multiplication de deux fonctions se définit par $(f \times g) : x \to f(x) \times g(x)$.
Il convient de noter que, même si ces deux notions peuvent paraître naturelles, on vient de définir de façon complète deux opérations sur l'ensemble des fonctions. Il aurait été possible de définir une addition et une multiplication différemment !
Il faut garder en tête les définitions de ce que sont l'addition et la multiplication dans l'ensemble considéré et que + et x ne sont que des symboles.
L'ensemble (F, +, x) ainsi construit est un anneau.
Par exemple la fonction nulle, c'est-à-dire $x \to 0$ qui à tout nombre associe 0 est l'élément neutre de F pour l'addition définie ci-dessus. En effet, ajouter la fonction nulle à une autre ne modifie pas la fonction de départ. Ainsi $0_F = x \to 0$.
De même, le neutre pour la multiplication est la fonction identiquement égale à $1_F = x \to 1$ car multiplier une fonction par une autre valant toujours 1 ne la modifie pas.
De plus, toute fonction f de F possède un inverse pour l'addition, à savoir (-f) : $x \to -f(x)$ car f+(-f) est la fonction $x \to f(x)+(-f(x))$ à savoir $x \to 0$ qui est le neutre pour +.
On peut remarquer que pour la multiplication, toutes les fonctions ne possèdent pas un inverse.
En effet, si f ne s'annule jamais, on remarque que $1/f = x \to 1/f(x)$ est l'inverse de f pour x car $f \times 1/f = f(x) \times 1/f(x)$ c'est-à-dire $f \times 1/f = x \to 1$. Mais si f s'annule en au moins un point, écrire cela devient impossible car cela reviendrait à diviser par 0.

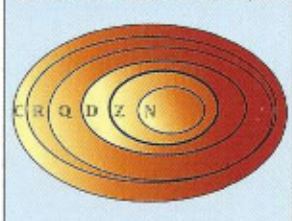
DES ANNEAUX CLASSIQUES

• (Z,+, .), (Q,+, .), (R,+, .) et (C,+, .).
• L'ensemble des matrices carrées muni de la somme et de la multiplication des matrices.
Tout comme dans les groupes, on a des morphismes de groupes, on dispose également de morphisme d'anneaux.

MORPHISMES D'ANNEAUX

Soient (A,+, .) et (B,+, .) deux anneaux (on note de la même façon les lois de A et de B). Un morphisme d'anneaux de A vers B est une application de A vers B telle que :
• $f(1_A) = 1_B$;
• Pour tout x, y éléments de A, $f(x + y) = f(x) + f(y)$ et $f(x \times y) = f(x) \times f(y)$.
Autrement dit, un morphisme d'anneaux est une application compatible avec les lois de l'anneau.

LES ENSEMBLES MATHÉMATIQUES



N : entiers naturel
Z : entiers relatifs
D : nombres décimaux
Q : nombres rationnels
R : nombres réels
C : nombres complexes

LES CORPS

Dans un anneau, les éléments sont inversibles pour l'addition mais rien n'est dit quant à leur inversibilité par rapport à la multiplication.
De cette remarque naît l'idée d'inventer une nouvelle structure : le corps.
Un corps est un anneau dans lequel tout élément non-nul, c'est-à-dire différent de l'élément neutre pour l'addition, est inversible pour la multiplication.
Si l'anneau est commutatif (sous entendu « pour la multiplication », car un anneau est toujours commutatif pour l'addition d'après sa définition) alors le corps est dit commutatif.
Si l'anneau n'est pas commutatif, on parle de corps gauche.

DES CORPS CONNUS

Z est un anneau commutatif mais non un corps car les éléments autres que 1 n'ont pas d'inverse pour la multiplication.
Par exemple, l'inverse de 3 est 1/3 et 1/3 n'est pas dans Z.
Pour établir un corps à partir de Z, on doit ajouter à Z des éléments tels que 1/3 ainsi que le produit de tels éléments avec ceux de Z. Ce nouvel ensemble est Q, l'ensemble des nombres rationnels, c'est-à-dire l'ensemble des nombres qui peuvent s'écrire sous la forme p/q avec p et q des nombres entiers relatifs.
Il existe des corps plus grands que Q, à savoir R, ensemble des réels ou même C, ensemble des complexes.

POURQUOI DES STRUCTURES ?

On dispose à présent de trois structures fondamentales qui sont le groupe, l'anneau et le corps. Mais pourquoi construire de tels objets mathématiques ? La réponse est tellement simple que nous l'avons sous nos yeux sans la voir.
Prenons l'exemple des nombres tels que nous les connaissons.
Lorsque l'on est enfant, on apprend à compter : 1, 2, 3, etc. On construit ainsi, sans même sans apercevoir, l'ensemble N des entiers naturels, c'est-à-dire des entiers positifs.
N est un ensemble très utile pour compter mais présente un défaut majeur : on ne dispose pas des nombres négatifs. Les nombres négatifs sont non seulement utiles dans la vie courante, par exemple pour caractériser une température inférieure à 0 °C, mais aussi et surtout pour résoudre des équations.
En effet, pour résoudre x+3 = 0, on doit ajouter -3 aux deux membres de l'équation afin d'éliminer 3 à gauche du signe égale.
Éliminer 3 signifie que l'on ne veut plus que ce nombre apparaisse à gauche du signe « = ». Mais comment a-t-on fait ?
En ajoutant -3 dans chaque membre de l'équation, on utilise sans le savoir les propriétés des lois de composition internes !
On ajoute -3 tout simplement parce que -3 est l'inverse de 3 pour l'addition et que donc 3+(-3) = 0. On obtient ainsi le neutre qui par définition vérifie x+0 = x.
Dans le cas d'une loi de composition interne notée *, pour résoudre l'équation x*y = z d'inconnue x, on compose à droite par l'inverse de y. Ainsi on obtient $(x*y)*y^{-1} = z*y^{-1}$. Si la loi est associative, on peut écrire $(x*y)*y^{-1} = x*(y*y^{-1})$. Or, comme par définition $y*y^{-1} = e$, on obtient $x*e = z*y^{-1}$, c'est-à-dire $x = z*y^{-1}$.
On a ainsi résolu notre équation !
Ainsi l'ensemble N des entiers naturels ne permet pas de résoudre des équations faisant intervenir des sommes car on ne dispose pas des inverses des nombres dans cet ensemble. Il faut pour cela inventer la structure de groupe.
L'ensemble Z des entiers relatifs possède une structure de groupe pour l'addition et permet ainsi de résoudre des équations faisant intervenir des additions. Cependant, la plupart des équations font à la fois intervenir des additions et des multiplications. Il est alors nécessaire d'adopter une structure d'anneau.
$(Z,+,*)$ est bien un anneau mais un problème similaire à celui de N se pose. Il n'existe pas d'inverse pour la multiplication dans Z. Un nouvel ensemble doit alors être créé : un corps. Le corps Q des nombres rationnels permet de pallier ceci. Ainsi, lorsque l'on passe de structure en structure, on gagne des propriétés tout en restant dans un cadre très général permettant de traiter un grand nombre de problèmes différents.
Par exemple, les équations faisant intervenir + et x peuvent être résolues dans un corps. Après avoir montré que l'ensemble des matrices de déterminant non nul forme un corps, il sera possible de résoudre sans problème les équations faisant intervenir des sommes et des produits matriciels.

UNE DERNIÈRE STRUCTURE

Comme vu ci-dessus, les structures algébriques permettent de résoudre des équations. Mais les structures permettent de faire beaucoup d'autres choses. La géométrie en est un exemple. Lorsque l'on souhaite représenter des vecteurs et effectuer des opérations sur ceux-ci, on fait appel à une nouvelle structure : l'espace vectoriel. Il s'agit ici de pouvoir effectuer des opérations telles que la somme de deux vecteurs ainsi que de multiplier un vecteur par un nombre (appelé scalaire). Il est donc nécessaire de définir un ensemble qui constituera ce que l'on appellera les vecteurs ainsi qu'un autre contenant les nombres (scalaires) que l'on utilisera pour les multiplier aux vecteurs. Comme vu ci-dessus, la structure la plus complète pour les nombres est le corps. On prendra donc toujours les scalaires dans un corps. Soit alors K un corps. On appelle espace vectoriel sur K, un ensemble E muni d'une loi de composition interne notée + conférant à E la structure de groupe commutatif et d'une loi dite externe notée par un point qui à un scalaire de K et à un vecteur de E associe le produit de ces deux éléments. Ainsi, à un vecteur x et un scalaire λ, on associe le vecteur λ.x.
Par exemple, si le corps choisi est R l'ensemble des nombres réels, et E l'ensemble des vecteurs du plan pouvant s'écrire $\begin{pmatrix} a \\ b \end{pmatrix}$ avec a et b deux nombres réels correspondants aux coordonnées du vecteur, $\lambda\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \lambda \times a \\ \lambda \times b \end{pmatrix}$.

Par ailleurs, la loi notée point doit vérifier les axiomes suivants, x et y désignant des éléments (vecteurs) de E, a et b désignant des scalaires :
• $a(x+y) = ax+ay$;
• $(a+b)x = ax+bx$;
• $a(b \times x) = ab \times x$;
• $1x = x$.

LES SYMÉTRIES DE LA NATURE ET LES GROUPES

Lorsque l'on observe le monde physique, on ne peut que remarquer l'importance des symétries. Ces dernières structurent l'univers à notre échelle, mais aussi, comme le prouve la physique moderne, l'univers de l'infiniment grand et celui de l'infiniment petit. Mathématiquement, les symétries d'un système physique permettent de faire baisser le nombre de paramètres inconnus décrivant ce système.
Il a fallu cependant attendre le XIXe siècle pour disposer d'un bon support conceptuel au sujet des symétries. Même si, historiquement, la notion de groupe n'est pas née avec comme objectif celui de traiter des symétries, c'est cette notion qui permit de les modéliser complètement et de les étudier dans toute leur généralité.

Le génieur premier de la théorie des groupes fut ***Évariste Galois***. Il introduisit cette notion afin d'étudier la possibilité de résoudre les équations polynomiales de degré supérieur ou égal à cinq par radicaux. Il remarqua une symétrie dans l'écriture des racines des polynômes de degré inférieur à 5, puis construisit un groupe correspondant à ces symétries (groupe de permutation). Il montra les liens entre certaines des propriétés mathématiques de ce groupe et le fait que les racines du polynôme correspondant soient exprimables par radicaux. Il montra finalement que ces propriétés mathématiques n'étaient pas vérifiées si le degré du polynôme considéré était supérieur ou égale à 5.

LA FORMULE DU BINÔME DE NEWTON

Soient a, b deux éléments d'un anneau, tels que a et b commutent, c'est à dire avec ab = ba. Soit n un entier naturel, on a alors la formule du binôme de Newton :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$$

avec

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Cette formule, pour n=2, n'est autre que l'une des fameuses identités remarquables que les lycéens doivent apprendre par cœur :
$(a+b)^2 = a^2+2ab+b^2$
De même, on dispose d'une autre formule très utile dans un anneau dont deux éléments x et y commettants.

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}$$

Dans le cas n=2, on retrouve une autre identité remarquable :
$x^2-y^2 = (x-y)(x+y)$.