Le triomphe de l'algèbre

L'algèbre a pris, en mathématiques, la première place. Des deux types de *structures* qui engendrent presque toute cette science, les structures algébriques sont les plus simples et les plus fondamentales. Nous avons déjà fait connaissance avec les groupes ; un groupe $(G, \circ)$ est un couple formé d'un ensemble G et d'une opération interne $\circ$ définie dans G, satisfaisant aux trois axiomes d'associativité

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

d'existence d'un élément neutre e (tel que $a \circ e = e \circ a = a$ pour tout a dans G) et d'existence d'un inverse a' pour tout élément a de G (tel que $a \circ a' = a' \circ a = e$). Nous avons vu qu'il existait des groupes très différents les uns des autres, quand ce ne serait que parce que certains d'entre eux sont commutatifs et d'autres non. (Un groupe $(G, \circ)$ est commutatif si l'opération $\circ$ est *commutative*, c'est-à-dire si l'on a l'égalité $a \circ b = b \circ a$ pour toutes les paires $\{ a, b \}$.) Nous bornant aux groupes finis, nous pouvons définir ceux-ci par leurs *tables de Pythagore*.

Le groupe Z_3

Nous avons par exemple affirmé que l'ensemble $A = \{ e, a, b \}$ était un groupe si on le munissait de l'opération[1] $\circ$

1. On dit aussi *loi de composition* au lieu d'opération.

définie par certaines égalités (voir p. 19). Pour écrire de façon commode tous les « produits » $x \circ y$ où x et y sont des éléments quelconques de A, on a l'habitude de les écrire dans une matrice carrée, où la ligne marquée u contient tous les produits de la forme $u \circ x$ où x est variable, la colonne v contenant au contraire tous les produits du type $y \circ v$ où y décrit A tout entier. Ainsi le produit $u \circ v$ est à l'intersection de la ligne u et de la colonne v ; nous connaissons bien cette disposition, qui est celle que l'on donne souvent à la table de Pythagore pour le produit des nombres de 1 à 10 qui se trouve au dos des cahiers d'écolier. Pour notre groupe $(A, \circ)$ la table est la suivante :

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

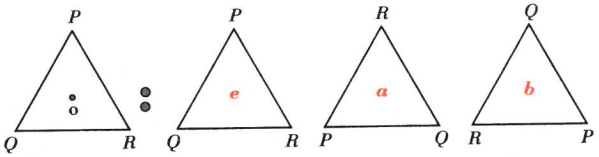
ex. :

$\circ$	a
b	$b \circ a$

On y vérifie sans peine que e est bien un élément neutre. Dans les tables de groupe, on supprime souvent la première ligne et la première colonne qui sont dès lors inutiles, puisqu'elles répètent exactement la ligne e et la colonne e ; il suffit de poser comme convention de toujours placer l'élément neutre en tête du groupe. On lit également avec clarté sur la table quels sont les inverses des éléments de A : $e' = e$ (e est son propre inverse), $a' = b$ et $b' = a$, car

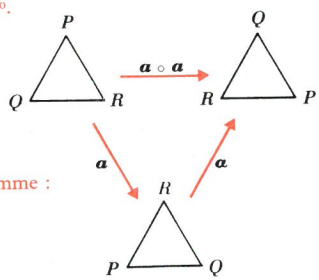
$$a \circ b = b \circ a = e.$$

Pour l'associativité, il n'existe rien de simple : il faut a priori envisager les 27 égalités à vérifier. Nous nous en dispenserons, car il existe ici un autre moyen d'y parvenir. Notre groupe n'est pas né de notre seule intuition, mais d'une idée géométrique. Considérons en effet un point O dans un plan, et les trois transformations de ce plan (c'est-à-dire les trois applications du plan dans lui-même) définies de la façon suivante : e est la transformation identique, qui a tout point m du plan associe m lui-même ; a est la rotation de centre O et d'angle 120^0 (ou encore $2\pi/3$ radians) dans le sens trigonométrique ; b est enfin la rotation de même centre et d'angle opposé. Reste à définir l'opération $\circ$. Celle-ci agit sur des applications ; c'est le *produit* d'applications. Le calcul d'une expression telle que sin (x^2) montre de quoi il s'agit ; partant de x, on forme d'abord $f(x) = x^2 = y$,

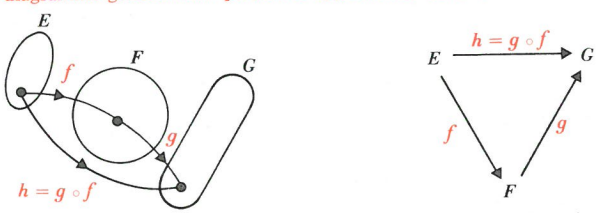


Un triangle équilatéral et ses images dans les trois transformations e, a et b du groupe $(A, \circ)$: la première le laisse inchangé, la seconde et la troisième sont des rotations d'angles + 120° et — 120°.

On peut vérifier simplement une égalité telle que $a \circ a = b$, par le diagramme :



Le diagramme général d'un produit d'applications est le suivant :



puis $g(y) = \sin y$. Le résultat est bien une application qui transforme x en $g(y) = g(f(x))$. Cette application est notée $g \circ f$, puisque c'est dans cet ordre qu'apparaissent, dans l'écriture, les lettres f et g de l'égalité $\sin(x^2) = g(f(x))$. Ce produit redonne facilement les éléments de notre table de Pythagore. Mais, ce qui est immédiat, cette interprétation de notre groupe abstrait montre que l'opération $\circ$ est associative et que $(A, \circ)$ est un groupe. On le notera ici $(\mathbf{Z}_3, +)$.

A la recherche des petits groupes

Il est assez facile de déterminer toutes les tables des groupes ayant un, deux, trois, quatre ou cinq éléments. On décide, évidemment, de n'écrire qu'une seule table si deux groupes sont isomorphes, car une traduction (qui revient à une transformation des lettres figurant dans le premier groupe en

celles qui figurent dans le second) permet alors de passer immédiatement de l'un à l'autre groupe. Ces tables figurent ci-dessous ; on a omis volontairement d'y faire figurer la première ligne et la première colonne comme il en a été convenu plus haut. Le groupe à un élément voit ainsi sa table réduite... à une seule lettre, puisque ce groupe est tout entier décrit par la seule égalité $e \circ e = e$.

e

(1)

e	a
a	e

(2)

e	a	b
a	b	e
b	e	a

(3)

e	a	b	c
a	b	c	e
b	c	e	a
c	e	a	b

(4)

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

(5)

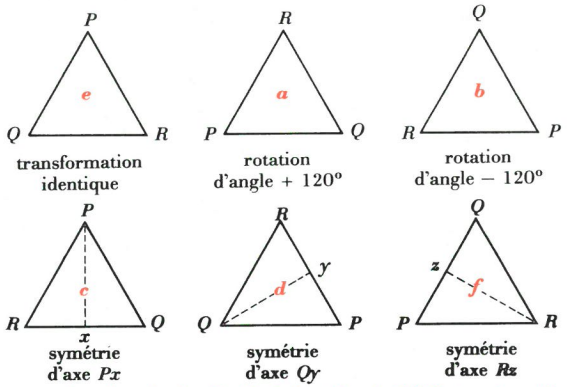
e	a	b	c	d
a	b	c	d	e
b	c	d	e	a
c	d	e	a	b
d	e	a	b	c

(6)

Il existe deux groupes vraiment distincts à quatre éléments : (4) et (5). Le second, appelé *groupe de Klein*, est très important. Nous donnerons plus loin une interprétation des cinq autres groupes ci-dessus. Remarquons simplement que ces six groupes sont tous commutatifs. Pour six éléments, ce n'est plus exact. On trouve bien encore un groupe commutatif qui ressemble bien à celui que nous avons ci-dessus avec cinq éléments (et dont on aperçoit facilement le mode de formation), mais il en existe un second, dont voici la table :

e	a	b	c	d	f
a	b	e	f	c	d
b	e	a	d	f	c
c	d	f	e	a	b
d	f	c	b	e	a
f	c	d	a	b	e

Ce groupe, connu sous le nom de groupe du triangle équilatéral, est étudié dans de nombreux livres, même élémentaires. (On peut l'interpréter comme le groupe des rotations et

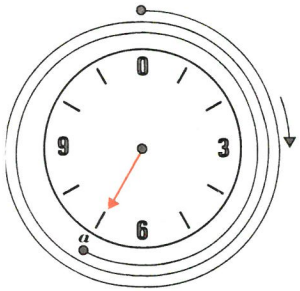


Le groupe du triangle équilatéral. Le triangle PQR et ses transformés par les six transformations de ce groupe. L'égalité $f = a \circ c$ peut se symboliser par la formule : $\begin{matrix} P & c & P & a & Q \\ QR & \smile & RQ & \smile & PR \end{matrix}$ équivalente à : $\begin{matrix} P & b & Q \\ QR & \smile & PR \end{matrix}$.

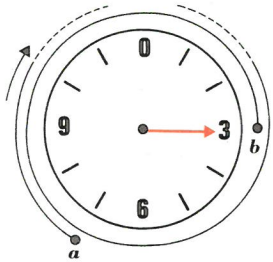
des symétries qui transforment un triangle équilatéral donné en lui-même.) Nous ne signalerons simplement que sa non-commutativité (puisque $f = a \circ c \neq c \circ a = d$), et la présence, dans le coin supérieur gauche, de la table du groupe à trois éléments $(A, \circ)$ déjà étudié. On dit alors que $(A, \circ)$ est un *sous-groupe* du groupe du triangle équilatéral, c'est-à-dire un sous-ensemble qui est lui-même un groupe pour la même opération. Le groupe de Klein peut également être considéré comme un groupe de transformations (par exemple celles qui conservent les longueurs et transforment un rectangle donné en lui-même, c'est-à-dire les symétries par rapport à deux droites perpendiculaires et leurs produits). Il possède lui aussi des sous-groupes, comme $(\{ e, a \}, \circ)$ ou $(\{ e, b \}, \circ)$, etc.

L'arithmétique de l'horloge

Montrons qu'il existe au moins un groupe commutatif à 12 éléments ; la méthode serait valable pour n'importe quel nombre naturel, et fournit les modèles des groupes (1), (2), (3), (4) et (6). Considérons une pendule ayant perdu sa petite aiguille et ne nous intéressons qu'aux multiples de cinq minutes, durée que nous prendrons comme unité (indivisible) de temps. Commençons une certaine expérience lorsque la grande aiguille est devant le 3. Supposons qu'à la fin de l'expérience elle se trouve devant le 7. Combien l'expérience a-t-elle duré ? La réponse n'est évidemment pas bien déterminée, mais on sait néanmoins quelque chose :



En 31 fois cinq minutes, la grande aiguille a effectué 2 tours complets et $\frac{7}{12}$ de tour.



En 44 fois cinq minutes, la grande aiguille a effectué 3 tours complets et $\frac{8}{12}$ de tour.

En (31 + 44) fois cinq minutes, la grande aiguille a effectué 6 tours complets et 3/12 de tour. Donc $31 = 7$, $44 = 8$ et $7 + 8 = 3$ dans $\mathbf{Z}_{12}$.

la durée, calculée en multiples de 5 minutes, est exprimée par l'un des nombres suivants :

$$4, 16, 28, 40, 52, \ldots, 124, \ldots$$

c'est-à-dire l'un des nombres de la forme $(12n + 4)$, puisqu'il est impossible de distinguer, avec la seule pendule, des durées qui diffèrent de 12 unités (une heure). Pour la pendule, toutes ces durées sont équivalentes, et la relation « les durées d et d' diffèrent d'un multiple de 12 » est justement une relation d'équivalence.

Notre horloge est, en quelque sorte, un additionneur qui confond des durées équivalentes, au sens que nous venons de donner à ce mot. Son arithmétique est la suivante : partant de 0, pour ajouter deux durées d et d' l'aiguille tourne un certain nombre de fois (que nous ignorons), passe devant le nombre a, correspondant à ce qui reste de la durée d après en avoir ôté le plus grand nombre possible d'heures, (prenons par exemple $d = 31$, d'où $a = 31 - 2 \times 12 = 7$), tourne encore quelques heures et s'immobilise sur le nombre b ; si la seconde durée était $d' = 44$, on peut calculer b, puisque la durée totale $(d + d')$, égale à $44 + 31 = 75$ unités, peut se décomposer en 72 unités (six heures) et 3 unités, d'où $b = 3$.

Mais on aurait pu procéder autrement : pour notre pendule, la durée d est absolument équivalente à $a = 7$; la durée d' est équivalente à $a' = 44 - 3 \times 12 = 8$; $d + d'$ est donc équivalente à $a + a' = 7 + 8 = 15$, donc à $b = 15 - 1 \times 12 = 3$. En d'autres termes, *dans ses additions, notre horloge annule tous les multiples de 12 qu'elle peut trouver*. Dans son arithmétique, elle écrit : $7 + 8 = 3$.

Les groupes Z_n

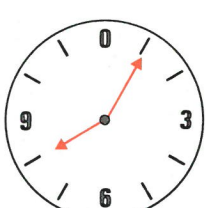
Il n'est pas très difficile de montrer que cette opération particulière permet de munir l'ensemble

$$G = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 \}$$

d'une structure de groupe commutatif, d'élément neutre 0, où l'inverse de x est le nombre $(12 - x)$ (sauf pour $x = 0$, dont l'inverse est naturellement 0). On pourrait en dresser la table : sa structure, très régulière, est celle que nous avons déjà trouvée dans quelques groupes ci-dessus :

0	1	2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10	11	0
2	3	4	5	6	7	8	9	10	11	0	1
3	4	5	6	7	8	9	10	11	0	1	2
4	5	6	7	8	9	10	11	0	1	2	3
5	6	7	8	9	10	11	0	1	2	3	4
6	7	8	9	10	11	0	1	2	3	4	5
7	8	9	10	11	0	1	2	3	4	5	6
8	9	10	11	0	1	2	3	4	5	6	7
9	10	11	0	1	2	3	4	5	6	7	8
10	11	0	1	2	3	4	5	6	7	8	9
11	0	1	2	3	4	5	6	7	8	9	10

Cette « arithmétique de l'horloge » fait fureur, notamment dans les livres scolaires américains, ce qui explique que certains assimilent désormais les « new maths » à ce jeu et



En se bornant aux multiples de cinq minutes, une horloge complète est un modèle de $\mathbf{Z}_{144}$, puisqu'il existe 144 positions distinctes sur le cadran : $\mathbf{Z}_{144}$ est donc, en un certain sens, le produit $\mathbf{Z}_{12} \times \mathbf{Z}_{12}$.

La colonne de droite d'un totalisateur de kilomètres est un additionneur de l'arithmétique $\mathbf{Z}_{10}$: pour lui par exemple $8 + 7 = 5$ car $15 = 10 + 5$. Il se contente donc d' « ignorer » les retenues.

au calcul en système binaire [1]! En fait, elle remonte à Gauss, pour sa formalisation complète, mais date du jour où un homme a remarqué, le premier, une périodicité dans le temps et en a déduit le premier calendrier, car nous aurions pu également prendre comme exemple les jours de la semaine, les mois de l'année, etc. D'ailleurs la théorie des congruences – son nom officiel – est à la base des curiosités que sont la règle de Gauss pour la détermination du jour de Pâques ou le calendrier perpétuel, qui permet de savoir quel jour était le 14 juillet 1789.

Cette arithmétique nous permet de construire pour tout nombre naturel n un groupe $(\mathbf{Z}_n, +)$ commutatif à n éléments [2] : une horloge avec ses deux aiguilles donnerait un groupe à 144 éléments, celui de la colonne de droite du totalisateur kilométrique d'une voiture conduit à un groupe à dix éléments, un semainier à un groupe à sept éléments, etc.

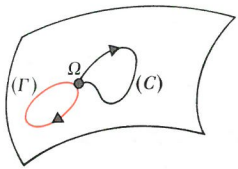
En jouant sur une surface

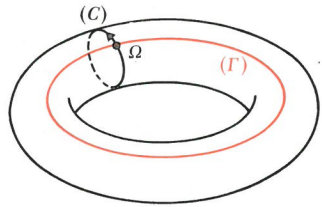
Les groupes infinis, quant à eux, ont une structure encore plus complexe. Indiquons rapidement comment définir, en un point d'une surface, un groupe très important qui fait intervenir des notions d'analyse (et, naturellement, de géométrie). Considérons, sur cette surface, une courbe continue permettant de partir du point Ω et d'y revenir de façon continue pendant une unité de temps. Toute courbe ayant la même propriété et pouvant être obtenue à partir de la précédente par une déformation continue est dite équivalente à la première : considérons l'ensemble des classes d'équivalence ainsi formées [3]. En munissant ces classes

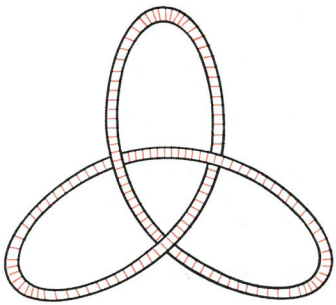
1. Voir *les Nombres et leurs Mystères*, même collection, pp. 18-23.

2. Il est très difficile d'obtenir tous les groupes finis ayant un nombre d'éléments donné (sauf si ce nombre est premier : il n'existe alors qu'un seul groupe). On connaît néanmoins une famille de groupes finis (les groupes de substitutions) qui permet théoriquement d'atteindre tous les groupes finis comme sous-groupes particuliers. L'étude complète des groupes finis mène à des résultats très importants pour la physique et la chimie nucléaire, notamment, ainsi qu'en arithmétique supérieure, en calcul matriciel, etc.

3. Techniquement, une courbe et sa description par le mobile considéré sont définis par la donnée d'une application continue de l'ensemble des nombres réels compris entre 0 et 1 sur la surface, de telle façon qu'elle passe bien en Ω pour les valeurs 0 et 1 du paramètre (le temps) ; une courbe équivalente (on dit : un lacet) est telle qu'il existe une fonction continue à deux variables, le temps et un autre paramètre x, dont les restrictions pour $x = 0$ et $x = 1$ donnent exactement les deux lacets équivalents.







Sur la surface de gauche, les deux chemins C et Γ sont équivalents (on suppose par exemple que C et Γ sont décrits de manière uniforme). Il n'en serait pas de même sur le tore de droite (un tore est une surface géométrique inspirée de la forme d'une chambre à air gonflée), car on ne peut pas déformer, de façon continue, C pour le transformer en Γ. La topologie peut permettre de démontrer qu'on ne peut déformer, de façon continue le « nœud de trèfle » ci-contre en un simple cercle sans trancher la corde, ce qui introduirait une discontinuité dans le processus.

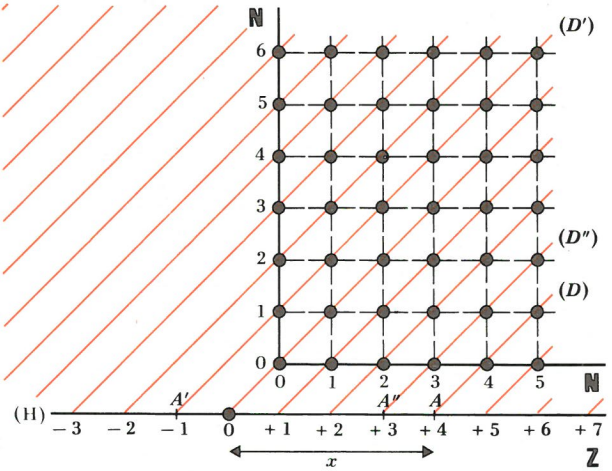
d'équivalence d'un produit approprié on obtient un groupe, appelé *groupe fondamental* de la surface au point Ω qui permet d'étudier les particularités de celle-ci au voisinage de Ω ; si la surface est une tasse à deux anses, le groupe n'est pas commutatif. Citons un résultat curieux, que l'on peut atteindre par la considération des groupes fondamentaux : le nœud de trèfle, dessiné ci-dessus, ne peut pas être déformé de façon continue jusqu'à devenir un cercle [1]!

Qu'est-ce qu'un entier relatif ?

L'algèbre a dépassé depuis longtemps le cadre étroit du calcul sur les nombres. Pourtant ceux-ci sont bien, historiquement et mathématiquement, les principaux bénéficiaires de l'algèbre, au moins de l'algèbre élémentaire. Montrons comment, à partir de l'ensemble **N**, fabriquer deux groupes très importants, que chacun de nous connaît depuis toujours. La figure montre certaines droites tracées sur le diagramme représentant une partie du produit cartésien $\mathbf{N} \times \mathbf{N}$. Considérons l'ensemble de ces droites ; on peut lui donner une structure de groupe additif commutatif de la manière suivante : pour définir la somme D'' des deux droites D et D', recherchons les points d'intersections A et A' des droites

1. D'après une conférence de M. J.-P. Serre (1957).

Construction de Z à partir du produit N × N



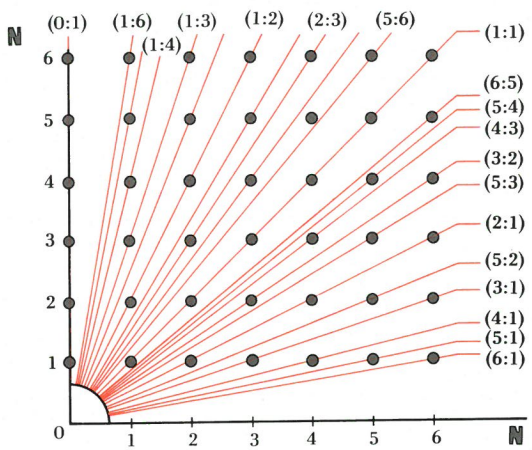
D et D' avec la droite marquée H. Nous construirons A'' sur H de façon que les segments OA'' et AA' aient même milieu ; la droite D'' est alors la droite de la famille passant par A'', et on peut montrer que l'opération ainsi définie munit nos droites d'une structure de groupe. Ce groupe n'est naturellement pas différent du groupe (**Z**, +), que nous avons déjà rencontré (groupe additif des nombres entiers relatifs), ou plus exactement il lui est isomorphe [1]. En effet, il suffit d'associer à toute droite D son intersection A avec H, et à A le nombre x dont la valeur absolue mesure, avec une unité de longueur appropriée, la distance OA, son signe étant positif ou négatif suivant que A est à droite ou à gauche de O : on aura reconnu en x l'abscisse de A. Le fait que OA'' et AA' aient même milieu traduit simplement l'égalité

$$x'' = x + x'.$$

1. La méthode ci-dessus, convenablement formalisée, est d'ailleurs celle qui permet de construire **Z** à partir de **N** par une méthode ensembliste. Disons simplement que l'on considère, dans l'ensemble des couples (a, b) de **N** × **N**, la relation d'équivalence définie par l'égalité $a + b' = a' + b$; les classes sont les ensembles de points de **N** × **N** situés sur les droites telles que D. L'ensemble de ces classes (l'ensemble-quotient) est alors muni d'une addition convenable, « héritée » de celle de **N**. On peut confondre pratiquement **N** et un sous-ensemble de **Z** : celui des droites rencontrant H à droite de O ; ceci revient à confondre les nombres $+ n$ et n, où n est un nombre naturel.

Les rationnels positifs

Otons maintenant, du produit $\mathbf{N} \times \mathbf{N}$, la ligne du bas (ce qui revient à ne considérer que les couples (a, b) où b est différent de 0, donc à se restreindre au produit $\mathbf{N} \times \mathbf{N}^*$ où l'ensemble $\mathbf{N}^*$ est l'ensemble $\mathbf{N} - \{ 0 \}$). Nous y construisons, cette fois-ci, toutes les droites passant par O (qui n'appartient pas au diagramme) et par les points de $\mathbf{N} \times \mathbf{N}^*$. Ces droites peuvent former un groupe. Nous appellerons « produit » des droites D et D' la droite D'' construite de la façon suivante. Si D passe par le point (a, b) et D' par le point (a', b'), D'' passe par le point (aa', bb'). On peut se convaincre facilement que d'autres choix de points sur D ou D' ne modifieraient pas D''. Ce que nous venons de construire est un groupe multiplicatif ; l'élément neutre est la droite passant par le point (1, 1), et l'inverse de la droite passant par (a, b) passe par (b, a). A dire vrai, il nous faut évidemment exclure la droite verticale, qui contient tous les couples (0, b), car elle n'admet aucune inverse. Le groupe obtenu est celui des fractions à éléments positifs : il suffit d'associer, à la droite passant par (a, b), la fraction $(a : b)$ elle-même, et toutes les fractions qui lui sont « égales » dans le langage



On obtient, cette fois-ci, l'ensemble des rationnels positifs ou nuls.

courant [1]. La construction de D'' traduit simplement cette règle bien connue : le produit de $(a : b)$ par $(a' : b')$ est la fraction $(aa' : bb')$. Modifions un peu notre procédé, en partant cette fois-ci du produit cartésien $\mathbf{Z} \times \mathbf{Z}^*$ (c'est-à-dire $\mathbf{Z} \times \mathbf{Z} - \{ 0 \}$). Cela revient, géométriquement, à ajouter de nouveaux points à notre diagramme, ainsi que de nouvelles droites, symétriques des précédentes. On obtient ainsi un ensemble [2] très intéressant, celui des *nombres rationnels*, définis par des fractions à éléments entiers positifs ou négatifs. Cet ensemble, noté $\mathbf{Q}$ (comme quotient) est encore un groupe multiplicatif si l'on enlève la droite verticale contenant la fraction nulle. Mais c'est aussi un groupe additif, dont cette droite est justement l'élément neutre, si on définit l'addition de manière à respecter la règle classique de la « réduction au même dénominateur » :

$$(a : b) + (a' : b') = (ab' : bb') + (a'b : b'b) = (ab' + a'b : bb').$$

Qu'est-ce qu'un corps ?

On peut inclure de force $\mathbf{Z}$ et $\mathbf{N}$ dans notre ensemble $\mathbf{Q}$, en confondant volontairement n, $+ n$, et $(n : 1)$. On peut effectuer alors tous les calculs classiques ne faisant intervenir que les quatres opérations. On appelle *corps* tout triplet $(K, +, \times)$ où l'on peut additionner, soustraire, multiplier et diviser (sauf par 0) de la manière habituelle : $\mathbf{Q}$ est le corps des nombres rationnels. De façon rigoureuse, un corps $(K, +, \times)$ est un triplet où :

– $(K, +)$ est un groupe commutatif, d'élément neutre 0, où l'inverse x' de x est noté $(- x)$ (et appelé *opposé* de x) ;

– $(K^*, \times)$, où K^* représente l'ensemble $K - \{ 0 \}$, est un groupe que nous supposerons généralement commutatif, d'élément neutre 1 où l'inverse de x est noté x^{-1} ou $1/x$;

1. Il s'agit en fait d'une équivalence : les fractions (1 : 2) et (2 : 4) ne sont pas identiques, puisque la première est irréductible et non l'autre !

2. La construction formelle se trouve aujourd'hui dans un grand nombre de manuels scolaires (et figurait déjà dans des manuels beaucoup plus anciens, sous une forme évidemment non ensembliste, sans relations d'équivalence, mais identique quant au fond : tout n'est pas nouveau sous le soleil). Elle ressemble beaucoup à la construction de $\mathbf{Z}$: définition d'une relation, démonstration du caractère d'équivalence de celle-ci, définition de l'ensemble-quotient, définitions adéquates de l'addition et de la multiplication dans cet ensemble, reconnaissance des deux structures de groupe annoncées.

– l'addition $+$ et la multiplication $\times$ sont liées par les relations de *distributivité* :

$$a(b + c) = ab + ac \quad \text{et} \quad (a + b)c = ac + bc\ ^{1}.$$

Il existe de très nombreux corps, dont le corps des nombres réels, qui est celui le plus couramment employé, celui des nombres complexes, et celui des *quaternions*, qui sont des généralisations successives de **Q**. Le dernier de ces corps, découvert par Hamilton au siècle dernier, est l'ensemble des nombres de la forme $(x + yi + zj + tk)$, où x, y, z, t, sont réels, et où les produits des nombres $(i, -i, j, -j, k, -k)$ entre eux sont donnés par la table suivante (la distributivité permet de calculer tous les autres produits) :

1	-1	i	$-i$	j	$-j$	k	$-k$
-1	1	$-i$	i	$-j$	j	$-k$	k
i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	i	1	-1	$-k$	k	j	$-j$
j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	j	k	$-k$	1	-1	$-i$	i
k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	k	$-j$	j	i	$-i$	1	-1

Cette table est d'ailleurs celle d'un groupe à huit éléments, non commutatif : c'est que la multiplication des quaternions est non commutative ; ces nombres forment un corps non commutatif.

Parmi les très nombreux autres corps, étudions très rapidement les corps finis commutatifs ; on les connaît explicitement. Si le nombre n possède plusieurs diviseurs premiers, il n'existe pas de corps à n éléments. Si n est de la forme $n = p^m$, où p est un nombre premier, il existe un corps unique de cardinal n. Dans ce corps, noté $\mathbf{F}_n$ et appelé « *corps de*

1. Nous avons vu que ces relations étaient vérifiées lorsque l'on considérait la réunion (à la place de $\times$) et l'intersection (à la place de $+$) de deux ensembles (voir p. 61) ; mais elles sont également vérifiées si l'on échange réunion et intersection, ce qui est une différence importante de l'algèbre des ensembles et de celle des nombres, où l'on n'a pas $a + bc = (a + b)(a + c)$.

Galois d'ordre n », on a l'égalité suivante, particulièrement choquante :

$$\underbrace{1 + 1 + \ldots + 1}_{p \text{ fois}} = 0$$

On traduit ceci en disant qu'un tel corps est de caractéristique p : le fait d'ajouter à lui-même p fois un élément quelconque du corps, comme 1, donne toujours 0. Comme on peut montrer (Wedderburn, 1909) que tout corps fini est commutatif, les corps de Galois épuisent tous les corps finis.

Les corps F_p

Une horloge où une heure serait divisée en un nombre premier d'intervalles égaux (trois, par exemple), nous a déjà permis de construire un groupe commutatif. On peut enrichir sa structure en définissant une multiplication convenable pour lui donner la structure de corps. Pour définir l'arithmétique de l'addition dans l'ensemble { 0, 1, 2 } il suffisait en effet d'ajouter normalement les éléments, puis de prendre, pour définition de $x + y$, le reste dans la division par 3 de la somme habituelle. Ceci donnait la table d'addition (que nous dessinons complètement, cette fois-ci) :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(on y a remplacé systématiquement 3 par 0 et 4 par 1). Ceci donne l'idée d'agir de façon semblable avec la multiplication : opérer le produit ordinaire de x et de y, puis en prendre le reste dans la division par 3 comme définition de xy, ce qui donne la table :

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

On y constate bien que l'ensemble { 1, 2 }, muni de cette multiplication, est un groupe commutatif. Comme les vérifi-

cations des distributivités sont immédiates (compte tenu de ce que ces propriétés sont vérifiées dans **N**), nous avons bien un corps : c'est F_3 Nous connaissons déjà le corps F_2, présenté page 62 sous son aspect d'anneau de Boole. L'ensemble $\{ p, i \}$ (pair/impair) est en effet le plus simple de tous les corps, avec les tables

$+$	p	i
p	p	i
i	i	p

$\times$	p	i
p	p	p
i	p	i

(y remplacer p par 0, reste dans la division par 2 des nombres pairs, et i par 1, reste des nombres impairs, permet de raccrocher immédiatement ce corps à nos arithmétiques d'horloges). D'une manière plus générale, on peut transformer l'ensemble

$$\{ 0, 1, 2, 3, \ldots\ldots, p\text{-}1 \}$$

(où p est un nombre premier) en un corps, en y remplaçant somme et produit ordinaires par leurs restes dans la division par p. Ceci fournit tous les corps de Galois de la forme F_p, puisque nous avons dit que tous les corps de Galois [1] de même cardinal étaient isomorphes (et donc pratiquement confondus, à une copie conforme près).

Les anneaux

Bien entendu, il est tentant de définir également une multiplication dans l'ensemble

$$\{ 0, 1, 2, 3, \ldots\ldots, n\text{-}1 \}$$

(où n n'est pas premier). Nous y connaissons déjà une addition qui le transforme en un groupe additif (le groupe $\mathbf{Z}_n$ ou $\mathbf{Z}/n$). Mais la multiplication donne ici une structure moins riche. Prenons par exemple $n = 10$. Calculer dans cette arithmétique est immédiat : il suffit d'oublier systématiquement d'effectuer toutes les retenues! Ainsi $7 + 8 = 5$ et non 15, $7 \times 8 = 6$ et non 56. Nous y constatons que $2 \times 5 = 0$. Or, dans un corps, le produit de deux éléments non nuls est lui-même non nul : par suite $\mathbf{Z}_{10}$ n'est pas un corps. Il en possède toutes les

→ 116

1. Les autres corps, de cardinaux p^m (où m est égal au moins à 2), sont plus compliqués ; ils sont construits en ajoutant, à F_p, un nouvel élément soigneusement choisi et en en considérant toutes les combinaisons possibles (additions et multiplications) avec les éléments de F_p, qui est toujours un sous-corps (le plus petit) de $F_p{}^m$.

Une application au codage du calcul dans l'arithmétique finie

$$\mathbf{Z}_5 = \{ 0, 1, 2, 3, 4 \}.$$

Cet ensemble est un corps, défini par les tables :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Il peut servir au codage. Soit en effet un texte composé uniquement de lettres. On le transforme en une suite de nombres de $\mathbf{Z}_5$, en utilisant le tableau suivant :

	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	V	W	X	Z

(ex. : C = 02, Q = 31, Y = I = 13, etc.)

La phrase VIVE BOURBAKI devient ainsi le nombre

41 13 41 04 01 24 40 32 01 00 20 13.

On le regroupe en triplets (complétant donc au besoin par un ou deux chiffres arbitraires) :

411 341 040 124 403 201 002 013.

Chaque triplet (x, y, z) est transformé en un triplet (x', y', z') défini par les égalités :

$$\begin{cases} s = x + y + z \\ x' = s + z \quad (= x + y + 2z) \\ y' = s + y \quad (= x + 2y + z) \\ z' = s + x \quad (= 2x + y + z) \end{cases}$$

les calculs étant évidemment effectués dans $\mathbf{Z}_5$.
Exemple : codons VIV = 411 341.
Pour 411, il vient $s = 6$, $x' = 2$ (car $7 = 5 + 2$), $y' = 2$, $z' = 0$ (car $10 = 5 + 5$).
Pour 341, il vient $s = 3$ (car $8 = 5 + 3$), $x' = 4$, $y' = 2$, $z' = 1$.
Donc 411 341 se transforme en 220 421 = 22 04 21, et VIV est codé en MEL.

VIVE BOURBAKI devient ainsi

220 421 434 143 021 430 422 204

soit :

22 04 21 43 41 43 02 14 30 42 22 04

d'où :

M E L X V X C J P W M E

• Ce code est construit de telle façon que le décodage soit identique au codage : si l'on code le message chiffré de la façon indiquée ci-dessus, il se retrouve en clair.
Exemple : MEL = 220 421.
Pour 220, il vient $s = 4$, $x' = 4$, $y' = 1$, $z' = 1$.
Pour 421, il vient $s = 2$, $x' = 3$, $y' = 4$, $z' = 1$.
MEL devient donc 411 341 = 41 13 41 = VIV.
Il n'utilise que la structure de groupe additif de $\mathbf{Z}_5$, la multiplication n'intervenant pas si l'on calcule d'abord s. Un autre code plus simple encore est défini par les égalités $x' = z$, $y' = y$, $z' = x$.
Un autre code, utilisant cette fois explicitement la multiplication, est défini par les formules dans le corps $F_5 = (\mathbf{Z}_5, +, \times)$:

$$\begin{cases} x' = 2x + 4y + z \\ y' = 4x + y + 3z \\ z' = x + 3y + z \end{cases}$$

• Donnons encore un exemple de code, pouvant transmettre des chiffres et un point, défini sur l'anneau

$(\mathbf{Z}_6, +, \times)$ $(\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\})$

	0	1	2	3	4	5
0	A	B	C	D	E	F
1	G	H	I	J	K	L
2	M	N	O	P	Q	R
3	S	T	U	V	W	X
4	Y	Z	1	2	3	4
5	5	6	7	8	9	•

Le tableau ci-contre donne la clé de la première transformation d'une phrase en nombres de $\mathbf{Z}_5$ ex. : A = 00, C = 02, • = 55 (le point représente les espacements, O est à la fois la lettre O et le chiffre 0).

On groupe ensuite par triplets (xyz), après avoir ajouté au besoin une ou deux lettres arbitraires, et on transforme par les formules (dans $\mathbf{Z}_5$) suivantes :

$$x' = 2y + 3z,\ y' = 2x + 3y,\ z' = 3x + 2z.$$

Il ne reste plus qu'à récrire en lettres et chiffres le message codé que l'on décode ensuite de la même façon (Un défaut de ce code est qu'il laisse invariant certains groupes, comme ISA, s'il constitue une tranche de 3 signes).
Exemple : 13 AOUT 17 H (il n'y a pas besoin d'espacement ici). 42 44 00 22 32 31 42 52 11 devient 424 400 223 231 425 211, puis 422 020 140 312 124 512 ou 42 20 20 14 03 12 12 45 12, c'est-à-dire

1MMKDII4I

propriétés sauf une : un élément non nul n'a pas forcément d'inverses (1, 3, 7 et 9 ont des inverses, respectivement égaux à 1, 7, 3 et 9 ; 2, 4, 5, 6, et 8 n'en ont pas). La structure de $\mathbf{Z}_{10}$ est celle d'un *anneau* commutatif unitaire. Un anneau est un triplet $(A, +, \times)$ tel que $(A, +)$ soit un groupe commutatif, la multiplication étant associative et vérifiant les deux conditions de distributivité. Il est commutatif si la multiplication est commutative ; il est unitaire s'il existe un élément neutre pour la multiplication. Il existe de nombreuses variétés d'anneaux ; certains, comme $\mathbf{Z}_n$ où n n'est pas premier, possèdent des diviseurs de zéro (par exemple, $2 \times 5 = 0$ dans $\mathbf{Z}_{10}$) ; d'autres, comme $(\mathbf{Z}, +, \times)$ ne possèdent aucun diviseur de zéro, c'est-à-dire que la règle classique « le produit de deux facteurs n'est nul que si l'un d'entre eux au moins est nul » y est valable comme dans un corps. Pourtant ce ne sont pas nécessairement des corps ; dans $\mathbf{Z}$, seuls 1 et (-1) possèdent des inverses : de tels anneaux sont dits intègres. Citons les anneaux principaux, noethériens, euclidiens, de Lie, artiniens, etc. [1].

Des algèbres d'ensembles

Une structure assez voisine de celle d'anneau est la structure d'*algèbre* de Boole. C'est un triplet $(A, \circ, \times)$ tel que les deux opérations $\circ$ et $\times$ soient commutatives, associatives, et distributives l'une par rapport à l'autre (ce qui fait quatre propriétés de distributivité). D'autre part, les opérations [2] $\circ$ et $\times$ ont chacune un élément neutre, noté par exemple 0 et 1, tel qu'à tout élément a de A on puisse associer au moins un élément noté a' tel que $a \circ a' = 1$ et $a \times a' = 0$.

On n'aura pas manqué de reconnaître ici une généralisation des propriétés des sous-ensembles d'un ensemble donné U : il suffit de remplacer $\circ$ et $\times$ par $\cup$ et $\cap$, a' par $\bar{a} = U - a$,

---

1. Certains auteurs appellent encore anneaux des ensembles $(A, +, \times)$ où la multiplication n'est pas associative, comme celui de Cayley.

2. Il suffit en fait de huit axiomes, qui sont indépendants, à savoir :
$\left.\begin{array}{l} a \circ b = b \circ a,\ a \times b = b \times a,\ a \circ (b \times c) = (a \circ b) \times (a \circ c), \\ a \times (b \circ c) = (a \times b) \circ (a \times c),\quad a \circ 0 = a,\quad a \times 1 = a, \\ a \circ a' = 1 \text{ et } a \times a' = 0. \end{array}\right.$
L'associativité $(a \circ (b \circ c) = (a \circ b) \circ c)$ et $(a \times (b \times c) = (a \times b) \times c)$ peut s'en déduire, ainsi que d'autres propriétés telles que l'unicité de a' et les formules :
$a = a \circ a = a \times a = a \circ (a \times b) = a \times (a \circ b)$, $(a')' = a$, et
$(a \circ b)' = a' \times b'$, $(a \times b)' = a' \circ b'$ (formules de Morgan).

o par $\varnothing$ et 1 par U. Le théorème de Stone affirme que toute algèbre de Boole est isomorphe à un sous-ensemble de parties $\mathscr{P}(U)$ muni des opérations ci-dessus ; toute algèbre finie est isomorphe à un certain ensemble $\mathscr{P}(U)$ tout entier et possède 2^n éléments. Notre exemple d'algèbre de Boole est donc, en quelque sorte, l'algèbre de Boole la plus générale.

On sait que l'on peut considérer $(\mathscr{P}(U), \Delta, \cap)$ comme un anneau (voir page 61). Il suffit de même, pour une algèbre de Boole abstraite, de remplacer l'opération $\circ$ (la réunion) par la somme $+$, définie par

$$a + b = (a \times b') \circ (a' \times b)$$

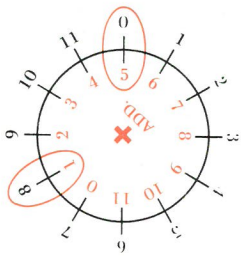
d'où $a \circ b = (a + b) + (a \times b)$. On montre alors facilement que $(A, +, \times)$ est un anneau commutatif unitaire à diviseur de zéro. C'est par exemple le cas de $\mathbf{Z}_4$.

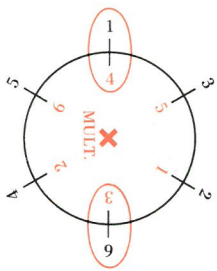
Une structure moins connue : le treillis

Les algèbres de Boole sont des cas particuliers de ce que l'on appelle des *treillis*, qui introduisent des relations d'ordre. Jusqu'ici, nous n'avons pas considéré de telles relations, qui permettent d'enrichir considérablement les structures de groupe, anneau, corps. (Nous avons tous, de nos souvenirs d'école, des notions sur les inégalités et les inéquations, donc une idée approximative des conséquences de l'introduction de l'ordre dans des structures définies, jusqu'ici, uniquement à l'aide d'opérations internes). Un treillis est un ensemble T dans lequel est définie une relation d'ordre que nous noterons $\leqslant$. Cette relation possède la propriété suivante : si a et b sont deux éléments quelconque de T, il existe un élément c de T tel que l'on ait $a \leqslant c$ et $b \leqslant c$; de plus, tout élément d de T tel que l'on ait $a \leqslant d$ et $b \leqslant d$ satisfait à l'inégalité $c \leqslant d$. Cet élément c se nomme le sup de a et de b ; il est évidemment unique ; nous le noterons $c = a \circ b$. Il existe de même, par définition d'un treillis, pour tout couple (a, b) un élément f de T (le inf de a et b) tel que l'on ait $f \leqslant a$ et $f \leqslant b$, tel que tout élément g satisfaisant à $g \leqslant a$ et $g \leqslant b$ soit relié à f par la relation $g \leqslant f$. Nous noterons $f = a \times b$. En d'autres termes, parmi les majorants communs à a et à b (c'est-à-dire des éléments d supérieurs ou égaux à la fois à a et b), il en existe un qui est inférieur ou égal à tous les autres : c'est $c = a \circ b$. De même, parmi les minorants communs, il en existe un $(f = a \times b)$ qui est supérieur ou égal à tous les autres. Les → 120

Les règles à calcul dans les corps finis F_p (p, premier)

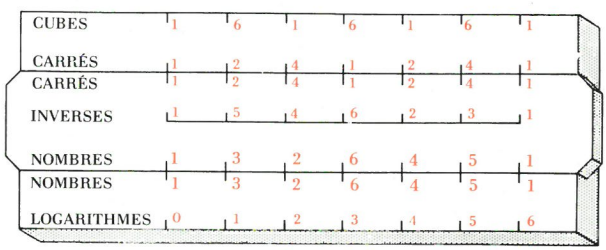
• Les horloges qui nous ont permis de définir les groupes additifs $\mathbf{Z}_n$ sont des cercles à calcul naturels de l'addition. La figure ci-contre montre comment additionner 5 et 8 dans le groupe $(\mathbf{Z}_{12}, +)$ à l'aide de deux cadrans de pendule : ayant fait coïncider le 5 et le 0, on lit le résultat 1 sous le 8. ($5 + 8 = 1$, car $13 = 12 + 1$).



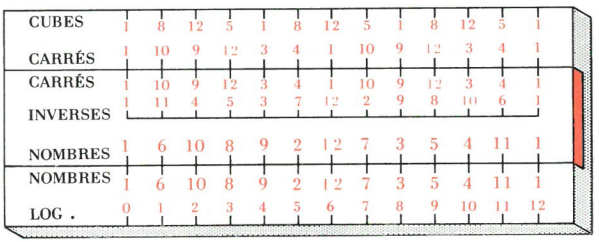


Si n est un nombre premier, $(\mathbf{Z}_n, +, \times)$ est un corps de Galois (F_n). On peut y construire des cercles à calcul pour la multiplication. Dans F_7, on peut ainsi multiplier 4 par 6 (0 ne figure pas sur le cercle). Ayant fait coïncider le 4 et le 1, on lit le résultat 3 sous le 6. ($4 \times 6 = 3$, car $24 = 3 \times 7 + 3$) (remarquer que, cette fois-ci, les nombres { 1, 3, 2, 6, 4, 5 } ne sont pas dans l'ordre naturel : celui-ci ne conviendrait pas).

• On peut aussi, pour la seule multiplication dans un tel corps, dessiner des règles à calcul qui ont exactement l'aspect des règles usuelles. Ainsi pour le corps F_7, peut-on obtenir l'instrument suivant :



• Voici l'une des 4 règles possibles pour le calcul dans le corps F_{13} :

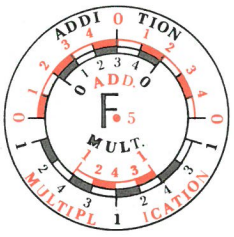


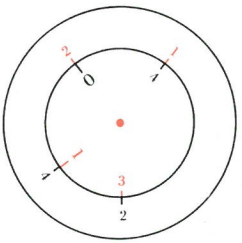
(On peut naturellement placer au dos une règle pour les additions, etc.) La construction de cette règle repose sur le fait que tout élément x non nul de F_{13} peut s'écrire sous la forme $x = 6^y$ (y est le « logarithme » de x). On aurait pu remplacer 6 par 2, 7 ou 11.
Le mot logarithme ne doit pas faire illusion : il est exact que le logarithme du produit xy est bien la somme des logarithmes de x et de y, mais calculée dans $\mathbf{Z}_{12}$ et non dans F_{13} ! Ce résultat paradoxal est valable pour tous les corps finis, et est une conséquence de l'implication :

$$(x \in F_n) \Rightarrow (x^n = x) \Rightarrow (x = 0 \text{ ou } x^{n-1} = 1).$$

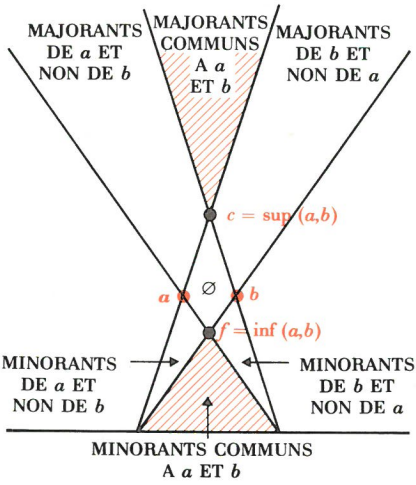
• Le cercle à calcul que voici permet, dans le corps $F_5 = \{0, 1, 2, 3, 4\}$, de calculer pratiquement la somme, la différence, le produit et le quotient suivants :

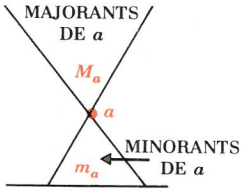
$$2 + 4 = 1, \qquad 1 - 4 = 2,$$
$$4 \times 3 = 2, \qquad 2 : 3 = 4.$$





Il peut servir à coder et à décoder suivant la méthode indiquée page 115.

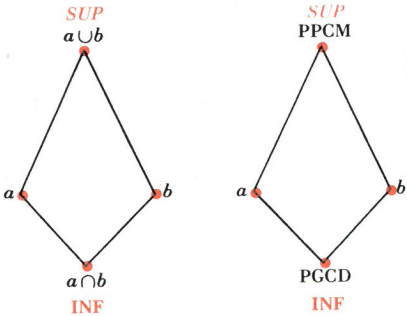




Treillis : Considérons un élément a, l'ensemble M_a de ses majorants ($x \in M_a$ équivaut à $a \leqslant x$) et l'ensemble m_a de ses minorants ($x \in m_a$ équivaut à $x \leqslant a$). Réunissant deux éléments a et b, l'ensemble $M_a \cap M_b$ possède un élément minimum c, qui est inférieur ou égal à tous les majorants communs à a et à b. De même $m_a \cap m_b$ a un élément maximum f, supérieur ou égal à tous les minorants communs à a et à b. On note souvent :

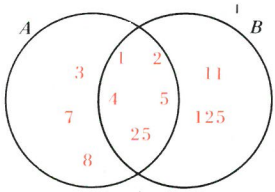
$\begin{cases} c = \sup(a, b) = a \circ b = a \vee b \\ f = \inf(a, b) = a \times b = a \wedge b. \end{cases}$

opérations $\circ$ et $\times$ possèdent certaines propriétés des opérations de même nom d'une algèbre de Boole (mais pas les distributivités, du moins en général). Un ensemble de parties est donc un treillis : la relation d'ordre est ici, naturellement, la relation d'inclusion. Donnons encore deux exemples. Le premier a trait à l'arithmétique : à toute paire d'entiers naturels $\{ a, b \}$ on peut associer leur PGCD (plus grand commun diviseur), qui joue le rôle de inf, et leur PPCM (plus petit commun multiple) qui est le sup, la relation d'ordre étant cette fois-ci la divisibilité. Une définition qui rattache ces opérations très connues à l'algèbre des ensembles repose sur la considération des « diviseurs primaires » d'un nombre, c'est-à-dire des diviseurs de ce nombre qui sont des puissances exactes d'un seul nombre premier. Les diviseurs primaires de $4\,200 = 2^3 \times 3 \times 5^2 \times 7$ sont donc les nombres { 1, 2, 4, 8, 3, 5, 25, 7}. Ceux du nombre $5\,500 = 2^2 \times 5^3 \times 11$ sont les nombres { 1, 2, 4, 5, 25, 125, 11 }. Leur réunion est l'ensemble des diviseurs primaires du nombre $231\,000 = 2^3 \times 3 \times 5^3 \times 7 \times 11$, qui est bien un multiple commun des deux nombres ($231\,000 = 55 \times 4\,200 = 42 \times 5\,500$), et même le plus petit possible, en est donc le PPCM. Inversement, le nombre $100 = 2^2 \times 5^2$ a pour diviseurs primaires l'intersection des deux ensembles considérés, soit {1, 2, 4, 5, 25 } ; c'est un diviseur commun des deux nombres, et même le plus grand. On voit comment ces notions traditionnelles illustrent les concepts ensemblistes ; le fait même que a

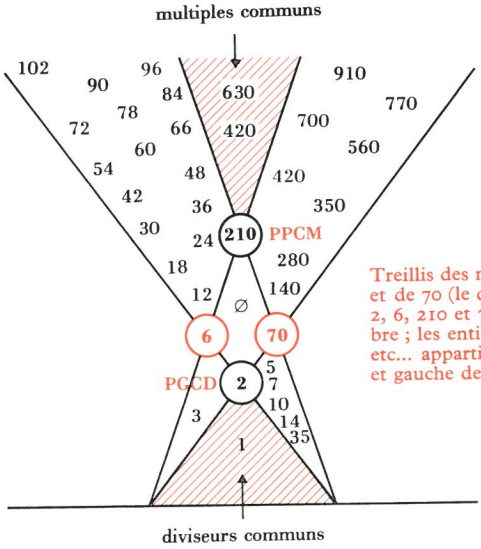


Treillis fondamentaux :
($\mathcal{P}(U)$, $\cup$, $\cap$), (div n, PPCM, PGCD).

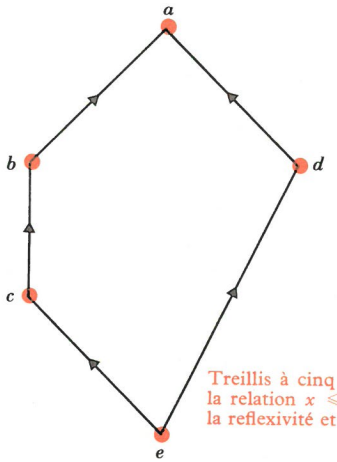
divise b peut s'exprimer dans ce langage (il est nécessaire et suffisant que l'ensemble des diviseurs primaires de a soit inclus dans celui de b) et cette remarque fait que presque toute la théorie des nombres peut être exprimée en termes d'ensembles.

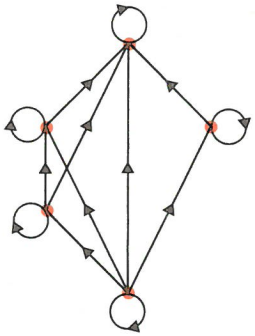


A = { diviseurs primaires de 4 200 }
B = { diviseurs primaires de 5 500 }
$4\,200 = 2^3 \times 3^1 \times 5^2 \times 7^1 \times 11^0$.
$5\,500 = 2^2 \times 3^0 \times 5^3 \times 7^0 \times 11^1$.
PPCM : $231\,000 = 2^2 \times 3^1 \times 5^3 \times 7^1 \times 11^1$.
PGCD : $100 = 2^2 \times 3^0 \times 5^2 \times 7^0 \times 11^0$.
A $\cup$ B : diviseurs primaires de 231 000
A $\cap$ B : diviseurs primaires de 100
Pour calculer les PPCM, on peut prendre A $\cup$ B et effectuer le produit des plus grandes puissances de 2, 3, 5, 7 et 11 qui y figurent. Pour calculer le PGCD, opérer de même dans A $\cap$ B. On peut déduire immédiatement de ce processus que l'opération PPCM est associative, commutative, distributive par rapport au PGCD, etc.



Treillis des multiples et diviseurs de 6 et de 70 (le quadrilatère compris entre 2, 6, 210 et 70 ne contient aucun nombre ; les entiers 4, 8, 9, 11, 13, 15, 19, etc... appartiennent aux parties droite et gauche de la figure).





Treillis à cinq éléments. Un arc fléché $\overrightarrow{xy}$ représente la relation $x \leqslant y$. Ce graphe est incomplet ; usant de la reflexivité et de la transitivité on obtient la figure ci-dessus.

Retour aux algèbres de Boole

Le second exemple est celui du plus petit treillis qui n'obéisse pas aux relations de distributivité. Il est constitué de cinq éléments $\{ a, b, c, d, e \}$. Le diagramme ci-dessus permet de définir la relation d'ordre. x est inférieur ou égal à y, sur de tels diagrammes, s'il existe un chemin, partant de x et aboutissant à y, allant uniquement de bas en haut (sans s'incurver). On en déduit par exemple les relations

$$e \leqslant c \leqslant b \leqslant a, \text{ et } e \leqslant d \leqslant a$$

ainsi que les conséquences que l'on peut en tirer par transitivité (comme $c \leqslant a$). Dressons les deux tables de la loi sup ($\circ$) et de la loi inf ($\times$) :

$\circ$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	b	a	b
c	a	b	c	a	c
d	a	a	a	d	d
e	a	b	c	d	e

$\times$	a	b	c	d	e
a	a	b	c	d	e
b	b	b	c	e	e
c	c	c	c	e	e
d	d	e	e	d	e
e	e	e	e	e	e

Chacune de ces lois a un élément neutre (e et a respectivement), est associative et commutative ; on peut aussi y vérifier les égalités $a \circ a = a \times a = a$, etc. Mais les distributivités n'y sont pas vraies. Par exemple :

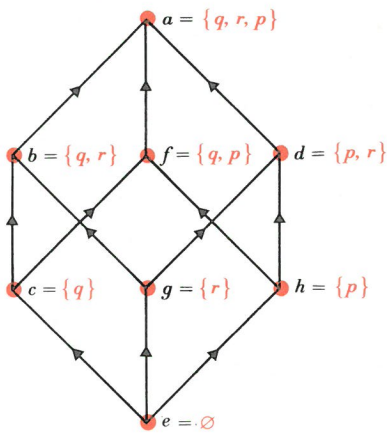
$$b \times (c \circ d) = b \times a = b,$$
$$(b \times c) \circ (b \times d) = c \circ e = c \neq b.$$

Notre treillis est en fait un extrait d'une algèbre de Boole simple : celle des sous-ensemble de l'ensemble $a = \{ p, q, r \}$. Il suffit de poser $b = \{ q, r \}$, $c = \{ q \}$, $d = \{ p, r \}$ et $e = \varnothing$. La relation. est bien celle d'inclusion, et l'opération $\circ$ correspond à la réunion. L'opération $\times$ est confondue avec l'intersection sauf pour $b \times d = e$, puisque l'intersection de b et de d, qui est l'ensemble $\{ r \}$, a été exclu de $\mathscr{P}(a)$.

Convenablement complété par les trois ensembles $f = \{ p, q \}$, $g = \{ r \}$ et $h = \{ p \}$, l'ensemble des parties de a est susceptible d'une représentation remarquable. Nous avons placé ses huit éléments aux sommets d'un cube (représenté dans une perspective particulière), dont les côtés symbolisent les relations d'inclusion les plus importantes. Les représenter toutes n'aurait pas rendu lisible notre graphe orienté : c'est pourquoi on s'est borné à celles qui suffisent à entraîner les autres par transitivité. La lecture attentive du graphe révèle l'existence de six sous-treillis particulièrement simple (les « faces » du cube) et, parmis eux, trois ensembles de parties (les trois faces ayant $e = \varnothing$ pour sommet, qui représentent les ensembles $\mathscr{P}(b)$, $\mathscr{P}(d)$ et $\mathscr{P}(f)$).

Voyage dans la quatrième dimension

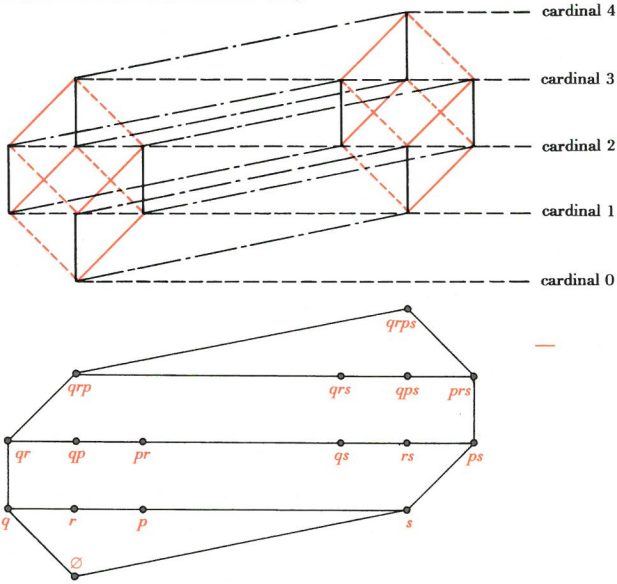
De même que des points bordent des segments, que des segments bordent des carrés, que des carrés bordent des cubes (ce sont des représentations d'ensembles $\mathscr{P}(U)$ de cardinaux 0, 1, 2, 3), des cubes bordent des ... *hypercubes* à quatre dimensions, graphes de l'ensemble des parties d'un ensemble à 4 éléments ordonné par l'inclusion. On reconnait sur la figure de cet hypercube (p. 125), à ses deux extrémités,



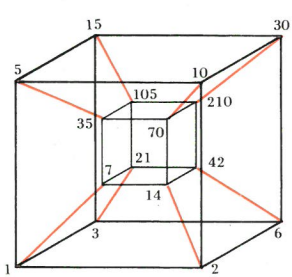
Graphe orienté de la relation d'inclusion dans l'ensemble $\mathscr{P}(a)$. Un arc fléché $\overrightarrow{xy}$ signifie « x est inclus dans y » (on n'a représenté que les principales inclusions, mais ni $a \subset a$, ni $e \subset b$ par exemple, qui sont des conséquences immédiates des propriétés des relations d'ordre). Deux sous-ensembles symétriques par rapport au centre du cube sont complémentaires.

L'hypercube à quatre dimensions

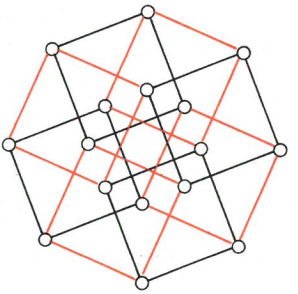
Ses seize sommets sont associés chacun à un sous-ensemble de l'ensemble $u = \{ p, q, r, s \}$. Dans le schéma du bas, ont été écrits (sans accolades ni virgules), les éléments de ces seize ensembles. Sur une même horizontale, ne figurent que des sous-ensembles de même cardinal. (D'après P. Rosenstiehl et J. Mothes, *les Mathématiques de l'action*, Dunod éd.)

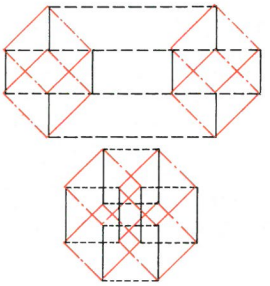


• Une autre représentation de l'hypercube permet d'en construire un « modèle » euclidien, à l'aide de tiges rigides et de câbles. On aperçoit nettement les huit cubes qui servent d'« hyperfaces » à l'hypercube : deux d'entre eux sont représentés fidèlement (aux dimensions près) les six autres ont leurs bases empruntées aux deux précédents comme le cube 1 — 3 — 6 — 2 — 7 — 21 — 42 — 14. (D'après D. Hilbert.)

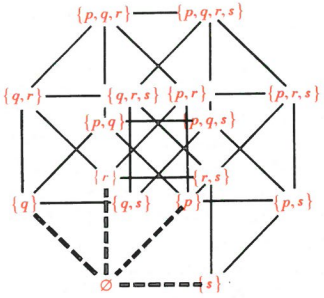


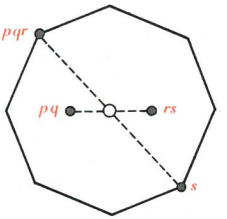
• Cette représentation est plus symétrique que la précédente mais se laisse lire moins facilement. On peut comprendre sa construction en imaginant deux cubes se pénétrant mutuellement. (*op. cit.*)





• Sur ce nouveau schéma, nous avons placé les sous-ensembles de $\{ p, q, r, s \}$ en les explicitant. Si l'on appelle $\vec{p}, \vec{q}, \vec{r}, \vec{s}$ les vecteurs d'origine $\varnothing$ aboutissant aux singletons $\{ p \}, \{ q \}, \{ r \}, \{ s \}$, les sommets de l'hypercube sont les extrémités des vecteurs $\alpha \vec{p} + \beta \vec{q} + \gamma \vec{r} + \delta \vec{s}$, où les lettres grecques prennent les valeurs 0 ou 1 : ceci nous ramène à la représentation en arbre de l'ensemble $\mathscr{P}(\{ p, q, r, s \})$. Deux ensembles symétriques par rapport au centre de la figure sont complémentaires comme $\{ p, q, r \}$ et $\{ s \}$, ou $\{ p, q \}$ et $\{ r, s \}$.





les cubes « ordinaires » qui sont les « hyperfaces » de l'hypercube (il y en a d'ailleurs beaucoup d'autres, déformés par la perspective). Voici comment interpréter ce graphe. Partant d'un point donné, représentant un ensemble z, on lui ajoute l'élément p en s'élevant vers la droite ; on lui ajoute q en s'élevant vers la gauche ; on lui ajoute r en s'élevant verticalement ; enfin on lui ajoute l'élément s en s'éloignant vers la droite en « pente douce ». Le tout donne une image saisissante de l'ensemble des parties de

$$u = \{ p, q, r, s \}.$$

Une légère déformation permet d'obtenir une représentation très symétrique (et décorative) de cet hypercube sous la forme de deux octogones réguliers. A propos de cette figure, indiquons au passage qu'il est possible de la dessiner d'un seul coup de crayon sans interrompre le trait ni repasser sur une ligne déjà tracée. Nous retrouverons plus loin ce genre de problèmes, moins anodins qu'il ne semble (voir page 182).

Le panier de la ménagère

Dans notre catalogue de structures algébriques, de groupes et treillis (et encore n'avons-nous pu passer en revue que quelques vedettes solitaires, en oubliant la piétaille), nous avons considéré exclusivement des opérations internes. Or la structure algébrique la plus importante, après celle de groupe, fait intervenir une opération externe ; c'est celle d'*espace vectoriel*. Imaginons une ménagère se rendant au marché. Dans son panier s'accumulent divers produits A, B, C, etc., dont le prix unitaire est respectivement noté $\bar{a}$, $\bar{b}$, $\bar{c}$ et ainsi de suite. Si elle achète x unités de A, y unités de B, z unités de C, le prix payé est :

$$\bar{p} = x\bar{a} + y\bar{b} + z\bar{c} + \ldots$$

($\bar{a}$, $\bar{b}$, $\bar{c}$,... $\bar{p}$) sont des sommes d'argent ; (x, y, z,..) sont des nombres entiers. Pourtant on peut combiner entre eux ces éléments d'origine différente. Élargissons notre modèle un peu simpliste en un modèle économique plus complexe, où les quantités peuvent prendre des valeurs non entières, rationnelles par exemple. Ceci impose en particulier que l'on prenne en considération des achats négatifs, symbolisés par des nombres $x < 0$: de tels achats sont simplement des ventes. Autorisons-nous également des prix unitaires négatifs : certains produits seront donc donnés avec de l'argent (les

économistes sont assez subtils pour nous trouver une interprétation plausible d'un tel comportement). Nous sommes prêts désormais à apprendre ce qu'est un espace vectoriel. Notre matériel se compose d'un ensemble E de sommes d'argent, positives ou négatives, muni d'une addition pour laquelle $(E, +)$ est un groupe commutatif. Dans notre exemple, E est simplement $\mathbf{Z}$, ensemble des nombres entiers relatifs. D'autre part nous disposons d'un ensemble K (les quantités, positives et négatives) qui possède une structure de corps ; dans notre exemple $K = \mathbf{Q}$, corps des rationnels. Aux trois opérations que nous connaissons (addition dans E, addition et multiplication dans K) ajoutons l'opération externe qui, à tout couple $(x, \bar{p})$ de $K \times E$, associe leur produit qui est l'élément de E noté $x\,\bar{p}$: dans notre modèle, pour une quantité donnée x d'une marchandise de prix unitaire $\bar{p}$, le produit $x\bar{p}$ est le prix qu'il faut payer pour acquérir x unités de cette marchandise. Cette opération est notée comme une multiplication par simple juxtaposition des deux lettres [1].

Les vectoriels

Posons enfin les axiomes qui munissent le sextuplet formé des deux ensembles K, E et des quatre opérations de la structure d'espace vectoriel :

- $(E, +)$ est un groupe commutatif (4 axiomes),
- $(K, +, \times)$ est un corps commutatif (9 axiomes),
- l'opération externe obéit aux propriétés suivantes :

$$\begin{cases} x\,(y\bar{p}) = (xy)\,\bar{p} \\ x\,(\bar{p} + \bar{q}) = (x\bar{p}) + (x\bar{q}) \\ (x + y)\,\bar{p} = (x\bar{p}) + (y\bar{p}) \\ 1\,\bar{p} = \bar{p}. \end{cases}$$

Certains de ces axiomes sont surabondants, mais le dernier, en dépit de son « évidence », est nécessaire.

L'archétype de cette structure est celle de l'ensemble E des vecteurs libres (ou translations) de l'espace ou du plan et du

1. Bien que ce ne soit théoriquement pas justifié, nous écrirons avec le même signe $(+)$ les deux additions (dans K et dans E), et avec la même convention (juxtaposition) les deux multiplications (dans K et dans $K \times E$), le contexte permettant toujours de décider. Pour la même raison, les deux zéros (de K et de E) sont parfois confondus ; nous ne le ferons pas ici, réservant 0 à K et $\overline{0}$ à E. Les deux « inverses » (c'est-à-dire opposés) pour les additions seront notés respectivement $(-x)$ et $(-\bar{p})$.

corps $\mathbf{R}$ des nombres réels. L'axiome $x(\overline{p} + \overline{q}) = x\overline{p} + x\overline{q}$ n'est autre que le célèbre théorème de Thalès. C'est pourquoi les éléments de E, même dans le cas général, sont appelés des vecteurs (et souvent notés p), les éléments de K étant les scalaires ; on dit que E est un espace vectoriel sur le corps K (un espace vectoriel rationnel, réel ou complexe, si K est l'un des corps $\mathbf{Q}$, $\mathbf{R}$ ou $\mathbf{C}$). Nous verrons les espaces vectoriels à l'œuvre en algèbre linéaire. Signalons simplement le résultat fondamental de toute la théorie, que l'on peut démontrer à l'aide de l'axiome du choix : pour tout espace vectoriel E, il existe un sous-ensemble B de E tel que tout vecteur de E puisse s'écrire d'une façon et d'une seule comme somme d'un nombre fini de produits d'éléments de K par des vecteurs de B. B s'appelle une *base* de E. S'il existe une base finie de cardinal n, toutes les bases ont même cardinal, et ce nombre est la *dimension* de E ; les espaces de dimension finie sont beaucoup plus simples que les autres. Parmi ces derniers, citons l'ensemble des fonctions continues, ou même $\mathbf{R}$, qui est un espace vectoriel sur $\mathbf{Q}$ [1].

Les espaces de dimension finie sont bien connus : l'espace euclidien (qui est de dimension 3), le plan euclidien (dimension 2), la droite euclidienne (dimension 1), le point (dimension 0), le corps de Galois $F_p{}^m$ (dimension m sur le corps F_p), les suites $f(n)$, c'est-à-dire les applications de $\mathbf{N}$ dans $\mathbf{R}$, telles que $f(n + 2) = f(n) + f(n + 1)$ comme la fameuse suite de Fibonacci [2] (dimension 2), les fonctions de la forme $\sin(x - a)$ (dimension 2, dont une base est : $\{\sin x, \cos x\}$) [3], etc.

Qu'est-ce qu'un nombre réel ?

Nous avons souvent parlé de l'ensemble des *nombres réels* $\mathbf{R}$, sans toutefois jamais le définir explicitement. Cette construction est assez délicate et nous ne la tenterons pas. Une idée naïve, suffisante jusqu'à un certain point, consiste à définir

1. Notons que l'on ne connaît pas explicitement de base de $\mathbf{R}$ sur $\mathbf{Q}$. Si l'on en connaissait une, il serait alors facile de construire une fonction $f(x)$ telle que $f(x + y) = f(x) + f(y)$ qui ne soit pas de la forme triviale $f(x) = kx$.

2. Voir *les Nombres et leurs Mystères*, pp. 92-97.

3. Si l'on supposait que K n'est pas un corps, mais seulement un anneau commutatif unitaire (comme $\mathbf{Z}$), on obtiendrait un K-module, structure plus générale mais plus complexe, indispensable à l'étude de certains phénomènes.

les nombres réels par une suite infinie de décimales : le nombre (− 0,12345678910111213 14... 100101102...) est un nombre réel. Une définition rigoureuse par ce moyen est possible mais pénible [1].

Signalons enfin un théorème très important, peut-être la meilleure introduction à cet ensemble fondamental dont la théorie rigoureuse remonte au siècle dernier seulement. Il existe une infinité de groupe $(G, +)$, commutatifs, munis d'une relation d'ordre total vérifiant l'implication

$$x \leqslant y \Rightarrow a + x \leqslant a + y \qquad \text{(ex. : } \mathbf{Q}, \mathbf{Z}\text{)}.$$

Supposons de plus qu'entre deux éléments distincts de G, il en existe au moins un troisième distinct des deux précédents : on obtient une classe assez large de tels groupes, dont $\mathbf{Q}$ (mais non $\mathbf{Z}$: entre 0 et 1, il n'existe aucun autre élément de $\mathbf{Z}$). Supposons enfin que tout sous-ensemble A non vide majoré de G possède une borne supérieure, c'est-à-dire que s'il existe un nombre M (un majorant) supérieur ou égal à tous les éléments de A, il existe alors un nombre B (la borne supérieure) qui est à la fois un majorant ($x \in A \Rightarrow x \leqslant B$) et le plus petit de ces majorants (y majorant de $A \Rightarrow x \leqslant y$). (Cette condition, analogue à une condition de treillis, n'est pas vérifiée dans $\mathbf{Q}$: considérer en effet l'ensemble des rationnels x tels que $x^2 < 2$ qui n'a pas de borne supérieure). Notre théorème affirme que tous les groupes satisfaisant à ces conditions sont isomorphes entre eux, et permet d'en construire un exemplaire contenant $\mathbf{Q}$ comme sous-ensemble. Cet exemplaire est le groupe $(\mathbf{R}, +)$ des nombres réels munis de l'addition et de la relation d'ordre habituelle. Il est alors facile de définir une multiplication qui confère à $\mathbf{R}$ la structure de corps. Il n'y a peut-être pas de meilleur objet d'étude de l'algèbre, cette science des relations et des opérations, que $\mathbf{R}$, à la fois groupe, anneau, corps, treillis, espace vectoriel de dimension infinie (sur $\mathbf{Q}$) et de dimension 1 (sur lui-même), dont la richesse est à la base du prodigieux développement des mathématiques pures et appliquées.

1. Une autre définition est la suivante : on appelle nombre réel tout sous-ensemble S (non vides et distincts de $\mathbf{Q}$) de nombres rationnels, satisfaisant à la propriété suivante : si x est inférieur ou égal à un élément de S, alors x appartient à S (S est appelée section commençante de $\mathbf{Q}$, nommée ainsi bien qu'elle n'ait pas de commencement, mais quelquefois une fin...).

Quelques problèmes relatifs au codage

Dans la transmission d'un message, en morse, il faut trois signaux élémentaires : le point (·), le tiret (—) et l'espacement ; ce dernier est nécessaire pour séparer les lettres. Sans lui on pourrait confondre L (· — · ·) et AI (· — / · ·). Soit { ·, —, / } l'ensemble de base de l'alphabet morse : pour transmettre l'alphabet, il faut associer à chaque lettre un message comportant au moins deux signaux (E = · /) et au plus cinq (L = · — · · /), l'espacement intervenant une fois seulement, en dernière position : ceci permet de comprendre une partie d'un message, tronqué par un défaut de transmission. Si l'on décidait de donner à toutes les lettres une traduction par un nombre *fixe n* de signaux, l'espacement deviendrait inutile. On peut ainsi traduire, à l'aide de 2 signaux élémentaires (·, —) toute lettre du sous-alphabet { A, B, C, D, E, F, G, H } par des triplets :

$$\begin{cases} A = \cdot\,\cdot\,\cdot, B = \cdot\,\cdot — , C = \cdot — \cdot, D = \cdot — — , \\ E = — \cdot\,\cdot, F = — \cdot — , G = — — \cdot, H = — — — . \end{cases}$$

A condition d'être certain d'avoir bien reçu le premier signal du message, une suite formée de $3n$ signaux élémentaires ne peut-être décodée que d'une façon unique ; ex :

· — · — — — · · — · · · · — · = CHBAC.

Un message tronqué tel que

· — · — —

peut aussi bien provenir de BD (· · · — · — —),FD (— · — · — —), CG (· — · — — ·) ou CH (· — · — — —), voire même de messages plus longs tels que AFF = · · · — · — — · —

Le risque, en transmissions radio notamment, de perte de l'information est donc très grand.

• Il existe pourtant des codes évitant cet inconvénient si grave. Adoptons pour notre alphabet restreint le code à trois signaux élémentaires (· — /) :

$$\begin{cases} A = \cdot\,/\,/ , B = \cdot\,/\,\cdot, C = \cdot\,/\,— , D = — \,/\,/, \\ E = — \,/\,\cdot, F = — \,/\,— , G = — \cdot\,\cdot, H = — \cdot — \end{cases}$$

Un signal tronqué tel que

· / / — / — · /

ne peut provenir que d'un message contenant les lettres AFA, AFB ou AFC : la transmission défectueuse n'a pas altéré les lettres AF ; ceci tient à ce que la juxtaposition de deux blocs $(\alpha\beta\gamma)$ (uvw) du code est telle que ni $(\beta\gamma u)$ ni (γuv) n'y appartiennent eux-mêmes.

• Certains codes permettent de déceler, voire parfois de corriger, certaines erreurs de transmission. Notre sous-alphabet peut-être codé, avec des blocs de 8 signaux écrits avec des (·) et des (—), de la manière suivante : associant à A, B, C... les nombres n = 0, 1, 2,...., on calcule $m = 19\,n + 61$ et on écrit les 8 derniers chiffres de m (en binaire). Il ne reste plus qu'à remplacer 0 par · et 1 par —.

Exemple : D → 4 ; $19 \times 4 + 61 = 137$.

$137 = 2^7 + 2^3 + 2^0 (= 128 + 8 + 1)$.

D sera donc codé par le bloc

10001001 ou (— · · · — · · —)

(7) (3) (0)

On peut vérifier que les 8 blocs obtenus sont très différents les uns des autres, et que, pour transmettre exactement un bloc du code à la place d'un autre, il a fallu commettre au moins trois erreurs. (D'après G. Cullmann, *Codes détecteurs et Correcteurs d'erreurs*, Dunod.)

• Le code suivant (en système binaire) :

A = 000000, B = 001110, C = 010101, D = 011011,

E = 100011, F = 101101, G = 110110, H = 111000,

permet de détecter et de corriger une erreur simple (Hamming). Il est en effet construit de façon que les trois premiers chiffres (xyz) représentent les nombres 0, 1, 2, ..., 7 en système binaire, et que les trois derniers (uvw) soient choisis de façon que

$$u + y + z, \quad v + z + x, \quad w + x + y$$

soient pairs.

On reçoit un message, tel que 110010 : un ordinateur peut effectuer les tests de parité en calculant

$u + y + x = 0 + 1 + 0 = 1$ (non correct)

$v + z + x = 1 + 0 + 1 = 2$ (correct)

$w + x + y = 0 + 1 + 1 = 2$ (correct)

Admettant qu'il n'y ait eu qu'une seule erreur de transmission commise, il suffit de se reporter au tableau suivant qui donne le numéro de la colonne ou a été commise une erreur d'après les réponses aux 3 tests :

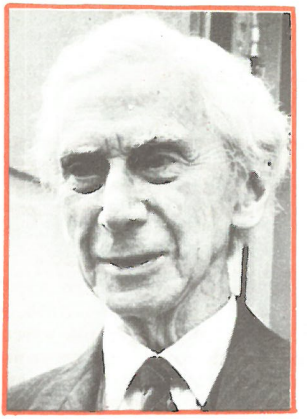
1° test	oui	oui	oui	oui	non	non	non
2° test	oui	oui	non	non	oui	oui	non
3° test	oui	non	oui	non	oui	non	oui
colonne fausse	—	6	5	3	4	1	2

(3 réponses négatives ne peuvent provenir que de deux erreurs au moins).

Ainsi le message 110010 était-il faux dans sa quatrième colonne ; en fait c'était 110110, c'est-à-dire G, qu'il fallait lire.

Deux erreurs sont peu probables (même si la fiabilité de la voie de transmission est si mauvaise que la probalilité d'une erreur sur un chiffre donné soit 1/10, celle pour qu'il existe une erreur dans un groupe de six chiffres est 0,354, tandis que la probabilité descend à 0,098 pour deux erreurs). Elles ne sont pas corrigibles, ni même détectables, par ce code : ainsi des erreurs sur la 3e et la 5e colonne donnent 110010 au lieu de 111000 = H.

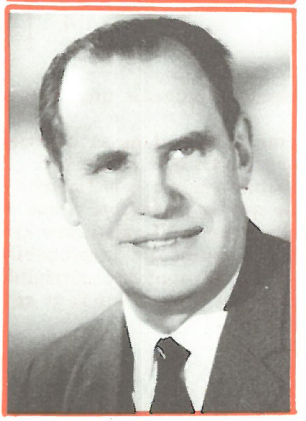
Cartan



Russell

Schwartz

Dieudonné



Lichnerowicz