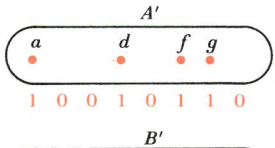
# Mathématique et organisation

Parmi les innombrables applications des mathématiques au monde concret, nous ne citerons pas celles qui, depuis si longtemps, ont trait à la physique, l'architecture, la mécanique, etc., car elles sont bien connues et donnent du mathématicien une image trop reliée au métier d'ingénieur classique. Loin de nous l'idée de mépriser une contribution aussi fondamentale ; mais notre but, ici, est plutôt de faire découvrir des aspects mal connus, souvent parce que relativement récents, de notre science. Aussi avons-nous choisi, non sans arbitraire, des applications relativement peu classiques qui apporteront, à certains lecteurs, des vues inhabituelles de l'activité du mathématicien, par exemple dans le domaine des sciences sociales.

## La politique en fiches

Etudions les opinions politiques d'une population donnée. A chaque individu on distribue une liste d'une vingtaine de questions auxquelles il faut répondre par oui ou par non et qui sont censées représenter les principaux tests politiques envisageables. On obtient ainsi des « mots » de 20 lettres que nous représenterons par une suite de 20 chiffres égaux à 1 (oui) ou à 0 (non) : nous appellerons opinion un tel mot.




A (10010110) est associé $A' = \{ a, d, f, g \}$.
A (10110011) est associé $B' = \{ a, c, d, g, h \}$.
Il y a accord pour les chiffres numérotés 1, 2, 4, 5, 7 et désaccord pour 3, 6 et 8. D'ailleurs $A' \triangle B' = \{ c, f, h \}$ est formé des éléments $c$ (n° 3), $f$ (n° 6) ; $h$ (n° 8). On peut les obtenir en ajoutant, dans $F_2$ (donc sans retenue) les nombres

$$\begin{array}{r} 10010110 \\ + \ 10110011 \\ \hline = \ 00100100 \end{array}$$

Remarque : on a toujours
$C' \triangle C' = \varnothing$ et $A' \triangle \varnothing = A'$, d'où
$A' \triangle B' = A' \triangle (C' \triangle C') \triangle B'$
$= (A' \triangle C') \triangle (B' \triangle C') \subset (A' \triangle C') \cup (B' \triangle C')$.

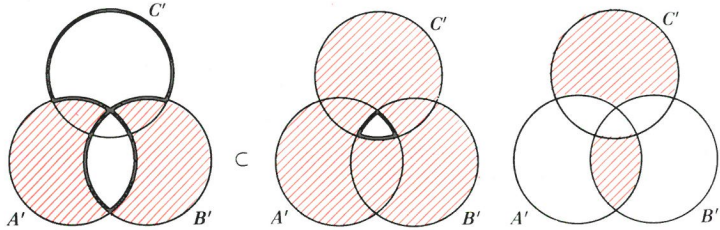
Nous savons comment associer un ensemble à une telle suite ; partant d'un ensemble à 20 éléments (les lettres de *a* à *t* par exemple), on fait correspondre au mot (11000 01001 10001 11011) l'ensemble { *a*, *b*, *g*, *j*, *k*, *o*, *p*, *q*, *s*, *t* } obtenu en répondant par oui (1) ou par non (0) aux questions « faut-il prendre *a* ? faut-il prendre *b* ?, etc. ».

Il est naturel de rechercher un test de voisinage entre deux opinions. Nous dirons que la *distance* des opinions $A$ et $B$ est égale au nombre de questions où la réponse est différente dans $A$ et dans $B$. Cette distance, notée $AB$ comme en géométrie, satisfait aux propriétés suivantes :

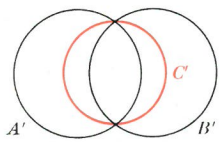
$$\left\{ \begin{array}{l} AB \text{ est positive ou nulle ;} \\ AB = 0 \text{ équivaut à } A = B ; \\ AB = BA. \end{array} \right.$$

De plus, comme en géométrie, les distances entre trois opinions $A$, $B$ et $C$ obéissent à l'inégalité $AB \leqslant AC + BC$. Pour démontrer ceci, nous pourrions observer que la distance des ensembles $A'$ et $B'$, associés aux opinions $A$ et $B$, n'est autre que le cardinal de la différence symétrique $(A' \Delta B')$ puisqu'elle est égale au nombre d'éléments de $A'$ ne figurant pas dans $B'$ augmenté du nombre d'éléments de $B'$ ne figurant pas dans $A'$. C'est alors une simple question d'arithmétique de cardinaux que de démontrer l'inégalité considérée.

En géométrie élémentaire, un point $C$ est *entre* deux points $A$ et $B$ si l'on a $AB = AC + CB$ (ce qui entraîne notamment l'alignement de $A$, $B$ et $C$). Nous dirons de même qu'une opinion $C$ est intermédiaire entre $A$ et $B$ si $AB = AC + CB$. On peut voir assez facilement que ceci est équivalent à la condition suivante : $C$ est entre $A$ et $B$ si les réponses de




Pour avoir égalité il faut et il suffit que les ensembles hachurés ci-dessus soient vides, ce qui donne la figure ci-dessous et la relation :




$(A' \cap B') \subset C' \subset (A' \cup B')$.


la liste de $C$ figurent toutes dans $A$ ou dans $B$. En particulier, si $A$ et $B$ sont d'accord sur un point pour y répondre par oui ou par non, $C$ doit reproduire leur réponse commune sur ce point. Traduit en langage ensembliste, cela signifie que l'ensemble $C'$ contient $(A' \cap B')$ (qui correspond aux réponses positives communes) mais est inclus dans $(A' \cup B')$ (il ne peut y avoir de réponse positive dans l'opinion $C$ là où $A$ et $B$ ont répondu ensemble négativement).

## Les opinions intermédiaires

Donnons quelques propriétés de cette relation (ternaire) d'opinion intermédiaire entre deux autres, que nous noterons $C \in AB$ :

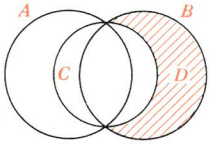
– $C \in AB \Rightarrow C \in BA$ (cf. axiome 10 d'Hilbert) ;

– étant donné deux opinions $A$ et $B$, il existe au moins une opinion $C$ et une opinion $D$ telles que $C \in AB$ et $B \in AD$ (cf. Hilbert, n° 11) ; de plus on a $B \in CD$ et $C \in AD$ (ce sont des théorèmes de géométrie euclidienne).

– Si $C \in AB$ et $D \in AB$, toute opinion intermédiaire entre $C$ et $D$ est intermédiaire entre $A$ et $B$.


$C \in AB$ et $B \in AD$


$(C \in AB)$ et $(D \in AB)$ et $(X \in CD) \Rightarrow X \in AB$



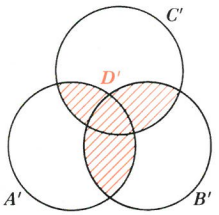


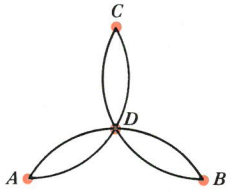
Bien que l'on ait ici $C$ entre $A$ et $B$ et $B$ entre $C$ et $D$ ($D$ est l'ensemble hachuré $B$–$C$) ; on ne peut trouver de relation « entre » qui relie $ACD$, pas davantage que pour $ABD$.

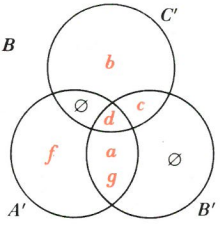

$ACB$ alignés et $ADB$ alignés n'impliquent pas nécessairement que $ACD$ sont alignés (ceci peut se produire seulement dans une géométrie non euclidienne ; notons néanmoins que tout point de $CD$ est aligné avec $A$ et $B$).

Toutes ces propriétés sont celles de la relation « entre » qui est définie en géométrie. Le parallélisme ne se poursuit pourtant pas. On peut en effet montrer que si $C$ et $D$ sont entre $A$ et $B$, il ne s'ensuit pas nécessairement que $D$ est égal à $C$, que $D$ est entre $A$ et $C$ ou que $C$ est entre $A$ ou $D$, ce qui serait normal pour des points alignés en géométrie : on ne peut donc généraliser la notion de droite à une famille d'ensembles (ou d'opinions), puisque bien que $ABC$ et $ABD$ soient « alignés », il n'en est pas de même en général de $ACD$[1].

Voici encore un résultat différent de ce que l'on peut constater en géométrie, mais qui possède un grand intérêt. Considérons trois opinions $A$, $B$, $C$ non alignées (aucune d'elle n'est entre les deux autres). Il existe alors une opinion $D$, unique, qui est à la fois intermédiaire entre $A$ et $B$, $B$ et $C$ et $C$ et $A$. Cette opinion « moyenne » est obtenue par une règle très simple : sur une question où il y a désaccord, on prendra l'opinion... de la majorité (trois étant impair, cette

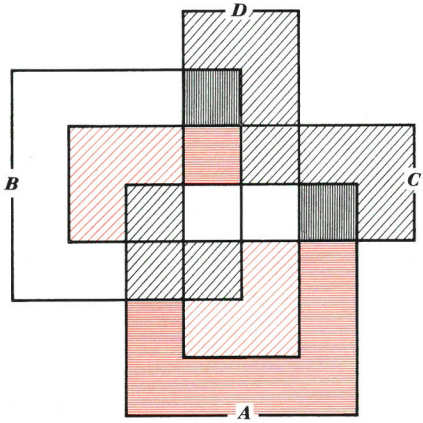



L'ensemble $D'$ correspondant à l'opinion « moyenne » de $(A, B, C)$ est hachuré à gauche.
Exemple :

d'où $A = (10010110)$ $A' = \{ a, d, f, g \}$
$B = (10110011)$ $B' = \{ a, c, d, g, h \}$
$C = (01110000)$ $C' = \{ b, c, d \}$
d'où $D = (10110010)$ $D' = \{ a, c, d, g \}$.




Supposons que $C$ soit entre $A$ et $B$ : on en déduit les égalités $A \cap B \cap \overline{C} = \overline{A} \cap \overline{B} \cap C = \varnothing$. $D$ entre $A$ et $B$ implique également $A \cap B \cap \overline{D} = \overline{A} \cap \overline{B} \cap D = \varnothing$. Sur le diagramme d'Euler ci-dessus nous avons hachuré de noir les ensembles vides résultant de $(C \in AB)$ et $(D \in AB)$. Pour que l'on ait $C$ entre $A$ et $D$, il faudrait que soient vides en outre

$$A \cap \overline{B} \cap \overline{C} \cap D \text{ et } \overline{A} \cap B \cap C \cap \overline{D}$$

(hachurés de rouge) ce qui n'est pas en général. De même $(D \in CA)$ impliquerait : $A \cap \overline{B} \cap C \cap \overline{D} = \overline{A} \cap B \cap \overline{C} \cap D = \varnothing$ (ensembles hachurés verticalement) et $(A \in CD)$ impliquerait

$$\overline{A} \cap B \cap C \cap D = A \cap \overline{B} \cap \overline{C} \cap \overline{D} = \varnothing$$

(ensembles hachurés horizontalement). $A$, $C$, $D$ ne sont donc pas « alignés » en général, pas plus d'ailleurs que $B$, $C$, $D$.

majorité existe toujours). En langage ensembliste, ce résultat signifie qu'on gardera les éléments qui figurent dans deux au moins des trois ensembles $A'$ $B'$ et $C'$ qui forment donc l'ensemble

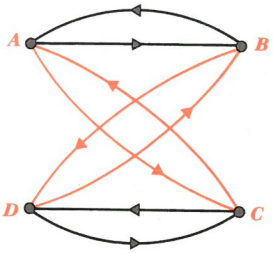
$$(A' \cap B') \cup (B' \cap C') \cup (C' \cap A')$$
$$= (A' \cup B') \cap (B' \cup C') \cap (C' \cup A').$$

Philosophiquement consolant, ce résultat ne s'étend malheureusement pas à plus de trois opinions... On sait d'ailleurs tous les avatars que l'on rencontre en voulant, à partir d'une liste de désirs de plusieurs individus, cohérents chacun avec eux-mêmes, construire mathématiquement (par la règle de la majorité ou une autre) une liste « moyenne » : celle-ci peut comporter des incohérences inévitables [2].

---

1. Un autre résultat négatif est le suivant : si $C$ est entre $A$ et $B$ et si $B$ est entre $C$ et $D$, il ne s'ensuit pas nécessairement que $BAD$ soient alignés (en géométrie, on aurait alors $B$ entre $A$ et $D$) ; de même pour $CAD$.

2. C'est le fameux « effet Condorcet ». Voir par exemple *les Nombres et leurs Mystères*, pp. 28 à 32.




Graphe des applications $f$ (tout homme de $X$ peut épouser une femme de $f(X)$) et $g$ (tout membre de $g(Y)$ est un enfant d'une femme de $Y$).

## De curieux mariages

Une des applications les plus célèbres des mathématiques aux problèmes de l'organisation du monde et des sociétés est celle que M. Lévi-Strauss a rapportée dans son livre *les Structures élémentaires de la parenté* (P. U. F.), qui a marqué le début de l'ère structuraliste. Le mathématicien André Weil – l'un des pères de Bourbaki – en a dégagé le contenu mathématique. La société Kariéra est divisée en quatre sous-populations ou clans, que nous noterons $A$, $B$, $C$ et $D$. Un homme du clan $X$ ne peut épouser qu'une femme d'un clan bien déterminé noté $f(X)$. L'application $f$ est définie par le tableau :

| $X$ | $A$ | $B$ | $C$ | $D$ | (clan de l'époux) |
|---|---|---|---|---|---|
| $f(X)$ | $C$ | $D$ | $A$ | $B$ | (clan de l'épouse). |

Quand un enfant naît, on l'attribue au clan $g(Y)$, où $Y$ est le clan de sa mère, $g$ étant définie par le tableau :

| $Y$ | $A$ | $B$ | $C$ | $D$ | (clan de la mère) |
|---|---|---|---|---|---|
| $g(Y)$ | $B$ | $A$ | $D$ | $C$ | (clan de l'enfant). |

$f$ et $g$ doivent être surjectives, pour que les femmes de tous les clans puissent prendre époux et pour qu'aucun clan ne dépérisse faute de se voir renouvelé par l'attribution d'enfants. Dans ce cas particulier, $f$ et $g$ sont d'ailleurs involutives (les produits $f \circ f$ et $g \circ g$ sont l'identité : si un homme de $X$ épouse une femme de $Y = f(X)$, un homme de $f(X)$ peut alors épouser une femme de $f(f(X)) = X$ ; si une fille d'une femme de $Y$ appartient au clan $g(Y)$, ses filles appartiendront au clan $g(g(Y)) = Y$. Les fonctions $f \circ g$ et $g \circ f$ sont identiques ; les enfants d'un homme de $X$ appartiennent au clan $g(f(X))$, qui est aussi le clan des brus possibles d'une

| $\circ$ | $e$ | $f$ | $g$ | $h$ |
|---|---|---|---|---|
| $e$ | $e$ | $f$ | $g$ | $h$ |
| $f$ | $f$ | $e$ | $h$ | $g$ |
| $g$ | $g$ | $h$ | $e$ | $f$ |
| $h$ | $h$ | $g$ | $f$ | $e$ |

5 sous-groupes : $\{ e \}$, $\{ ef \}$, $\{ eg \}$, $\{ eh \}$ (et lui-même).

Les applications $e, f, g, f \circ g = g \circ f = h$ forment un groupe de Klein.

femme du clan $X$, c'est-à-dire $f(g(X))$. Les produits engendrés par les applications $f$ et $g$ sont au nombre de 4 : $f$, $g$, $e$ (l'identité) et $h = f \circ g = g \circ f$. Elles forment un groupe isomorphe au groupe de Klein (voir page 103).

Chaque individu a un type de mariage : son clan s'il est masculin, celui d'un époux possible s'il est féminin. Il existe quatre types fondamentaux dans la structure Kariéra, déterminés par le clan du père ; à partir de celui-ci, noté $X$, on peut calculer le clan de la mère $f(X)$, celui des enfants $g(f(X)) = g \circ f(X)$ et celui des beaux-enfants (gendre et bru) $f(g(f(X))) = f \circ g \circ f(X)$. Le tableau des différents types de mariage détermine entièrement les fonctions $f$ et $g$, donc la structure nuptiale.

| Père | Mère | Enfants | Beaux-enfants |
|---|---|---|---|
| $A$ | $C$ | $D$ | $B$ |
| $B$ | $D$ | $C$ | $A$ |
| $C$ | $A$ | $B$ | $D$ |
| $D$ | $B$ | $A$ | $C$ |
| $(X)$ | $[f(X)]$ | $[g \circ f(X)]$ | $[f \circ g \circ f(X)]$ |

**Les quatre types de mariage Kariéra**

Il existe de nombreuses structures possibles. Parmi celles qui sont effectivement employées dans des tribus primitives, nous donnons ci-contre les graphes des applications $f$ et $g$, les types de mariage et les groupes engendrés par ces fonctions (ainsi que leurs sous-groupes) dans les cas des sociétés Tarau, Ambrym et Aranda, respectivement définis par les applications :

*Tarau* :

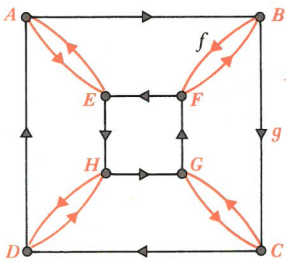
| $X$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $f(X)$ | $D$ | $A$ | $B$ | $C$ |
| $g(X)$ | $B$ | $C$ | $D$ | $A$ |

*Ambrym* :

| $X$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ |
|---|---|---|---|---|---|---|
| $f(X)$ | $D$ | $E$ | $F$ | $A$ | $B$ | $C$ |
| $g(X)$ | $B$ | $C$ | $A$ | $F$ | $D$ | $E$ |

*Aranda* :

| $X$ | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ |
|---|---|---|---|---|---|---|---|---|
| $f(X)$ | $E$ | $F$ | $G$ | $H$ | $A$ | $B$ | $C$ | $D$ |
| $g(X)$ | $B$ | $C$ | $D$ | $A$ | $H$ | $E$ | $F$ | $G$ |



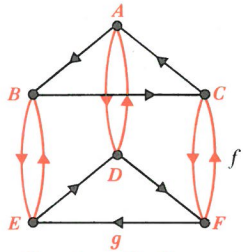

**Structure Aranda**

| $o$ | $e$ | $g^2$ | $g$ | $g^3$ | $f$ | $fg^2$ | $fg$ | $gf$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $g^2$ | $g$ | $g^3$ | $f$ | $fg^2$ | $fg$ | $gf$ |
| $g^2$ | $g^2$ | $e$ | $g^3$ | $g$ | $fg^2$ | $f$ | $gf$ | $fg$ |
| $g$ | $g$ | $g^3$ | $g^2$ | $e$ | $gf$ | $fg$ | $f$ | $fg^2$ |
| $g^3$ | $g^3$ | $g$ | $e$ | $g^2$ | $fg$ | $gf$ | $fg^2$ | $f$ |
| $f$ | $f$ | $fg^2$ | $fg$ | $gf$ | $e$ | $g^2$ | $g$ | $g^3$ |
| $fg^2$ | $fg^2$ | $f$ | $gf$ | $fg$ | $g^2$ | $e$ | $g^3$ | $g$ |
| $fg$ | $fg$ | $gf$ | $fg^2$ | $f$ | $g^3$ | $g$ | $e$ | $g^2$ |
| $gf$ | $gf$ | $fg$ | $f$ | $fg^2$ | $g$ | $g^3$ | $g^2$ | $e$ |

Groupe du carré ($f^2 = g^4 = e, fg^3 = gf$)

| Père | Mère | Enfants | Beaux-enfants |
|---|---|---|---|
| $A$ | $E$ | $H$ | $D$ |
| $B$ | $F$ | $E$ | $A$ |
| $C$ | $G$ | $F$ | $B$ |
| $D$ | $H$ | $G$ | $C$ |
| $E$ | $A$ | $B$ | $F$ |
| $F$ | $B$ | $C$ | $G$ |
| $G$ | $C$ | $D$ | $H$ |
| $H$ | $D$ | $A$ | $E$ |

(Le groupe du carré est isomorphe au groupe des isométries conservant le carré $ABCD$ : il suffit de prendre, pour $f$, la symétrie par rapport à la droite $AC$ (avant tout déplacement du carré), et pour $g$ la rotation de centre $(AC \cap BD)$ et d'angle droit dans le seńs positif : on peut alors vérifier les relations $f^2 = g^4 = e$ et $fg^3 = gf$ qui permettent de reconstruire la table du groupe.)

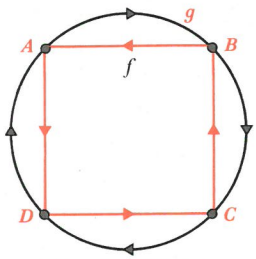



**Structure Ambrym**

| $o$ | $e$ | $g$ | $g^2$ | $f$ | $fg$ | $gf$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $g$ | $g^2$ | $f$ | $fg$ | $gf$ |
| $g$ | $g$ | $g^2$ | $e$ | $gf$ | $f$ | $fg$ |
| $g^2$ | $g^2$ | $e$ | $g$ | $fg$ | $gf$ | $f$ |
| $f$ | $f$ | $fg$ | $gf$ | $e$ | $g$ | $g^2$ |
| $fg$ | $fg$ | $gf$ | $f$ | $g^2$ | $e$ | $g$ |
| $gf$ | $gf$ | $f$ | $fg$ | $g$ | $g^2$ | $e$ |

Groupe du triangle équilatéral
($f^2 = g^3 = e, fg^2 = gf$)

| Père | Mère | Enfants | Beaux-enfants |
|---|---|---|---|
| $A$ | $D$ | $F$ | $C$ |
| $B$ | $E$ | $D$ | $A$ |
| $C$ | $F$ | $E$ | $B$ |
| $D$ | $A$ | $B$ | $E$ |
| $E$ | $B$ | $C$ | $F$ |
| $F$ | $C$ | $A$ | $D$ |




**Structure Tarau**

| $o$ | $e$ | $f^2$ | $f$ | $g$ |
|---|---|---|---|---|
| $e$ | $e$ | $f^2$ | $f$ | $g$ |
| $f^2$ | $f^2$ | $e^2$ | $g$ | $ef$ |
| $f$ | $f$ | $g$ | $f^2$ | $e$ |
| $g$ | $g$ | $f$ | $e$ | $f^2$ |

Groupe $(\mathbf{Z}_4, +)$
($f^4 = e, g = f^3$)

| Père | Mère | Enfants | Beaux-enfants |
|---|---|---|---|
| $A$ | $D$ | $A$ | $D$ |
| $B$ | $A$ | $B$ | $A$ |
| $C$ | $B$ | $C$ | $B$ |
| $D$ | $C$ | $D$ | $C$ |

## Une axiomatique ethnologique

Toutes ces structures obéissent aux propriétés suivantes :

– le clan du père détermine ceux de la mère, des enfants et des beaux-enfants ;

– le genre de parenté qui relie un homme et une femme permet, à lui seul, de déterminer si un mariage entre eux est possible ou non ;

– deux garçons dont les pères appartiennent à des clans différents sont attribués à des clans différents (en d'autres termes, l'application $g \circ f$ est injective ce qui implique que $f$ est injective : sinon l'existence d'un $X$ et d'un $Y$ tels que $f(X) = f(Y)$ impliquerait $g \circ f(X) = g \circ f(Y)$, et les fils d'hommes de $X$ et de $Y$ appartiendraient au même clan) ;

– un homme ne peut épouser sa sœur (il n'existe aucun $X$ tel que $f(X) = X$) ;

– deux individus quelconques ont toujours des descendants qui peuvent convoler.

Seul le dernier axiome est un peu complexe à utiliser. Les autres impliquent que $f$ est bijective, puisque le nombre de clans est fini ; on peut en déduire la même propriété pour $g$, égale à $(g \circ f) \circ f^{-1}$ et bijective comme produit de bijections. L'application $f$ n'admet aucun invariant $X$ tel que $f(X) = X$ ; il en est de même pour toute combinaison [1] (autre que l'identité) de fonctions $f$, $g$, $f^{-1}$ et $g^{-1}$.

Ceci montre qu'une structure telle que celle que définiraient les applications :

| $X$ | $A$ | $B$ | $C$ |
|---|---|---|---|
| $f(X)$ | $B$ | $C$ | $A$ |
| $g(X)$ | $A$ | $C$ | $B$ |

1. Ceci est une conséquence de l'axiome selon lequel le genre de parenté entre un homme et une femme permet, à lui seul, de déterminer si leur mariage est possible. Supposons en effet qu'il existe une application $h$ engendrée à partir de $f$ et de $g$ (par exemple $h = f^2g^{-1}fgf$ ; nous avons supprimé les signes $\circ$ trop lourds à manier) et un clan $Y$ tel que $h(Y) = Y$. $Y$ est l'image par $f$ d'un certain clan $X = f^{-1}(Y)$ tel que $Y = f(X)$, d'où l'égalité :

$$Z = k(X) = h(f(X)) = f(X).$$

Un homme du clan $X$ peut donc épouser une femme du clan $k(X)$. Mais cette égalité, vraie pour un clan particulier $X$, doit être vraie pour tous les clans, puisque $k = hf$ est une application respectant un certain genre de parenté (par exemple $f^{-1}g^{-1}$ définit le clan du père d'un individu, $fgf$ celui de sa bru ou de son gendre, etc.) On en déduit donc l'égalité de $k$ et de $f$, et $h$ doit être l'application identique.

(pour laquelle $g$ admettrait l'élément invariant $A$) n'est pas recevable ; en effet le fils d'un membre du clan $A$ peut y épouser la sœur de son père, ce qui est refusé aux fils de membres de $B$ ou de $C$.

## Un processus monotone

Le dernier exemple de ce chapitre, consacré à l'organisation en ensembles remarquables d'éléments mathématiques (ou d'origine plus concrète) a trait à un certain type de questions se rencontrant en *informatique*. On sait que les machines travaillent généralement en système binaire, c'est-à-dire traitent de suites de symboles 0 ou 1. Elles ne sont que d'imparfaits modèles d'une machine idéale, imaginée par le mathématicien Turing, qui sert notamment à démontrer les théorèmes de Gödel et de Church (voir p. 138). Imaginons que notre machine ait reçu l'ordre suivant : considérer le dernier triplet $T$ $(xyz)$ inscrit, et marquer à sa suite le résultat de l'addition

$$t = x + z,$$

addition effectuée dans le corps $F_2$ (c'est-à-dire telle que $1 + 1 = 0$). La machine écrit donc $(t)$ et, si on a maintenu l'ordre initial, elle calculera ensuite

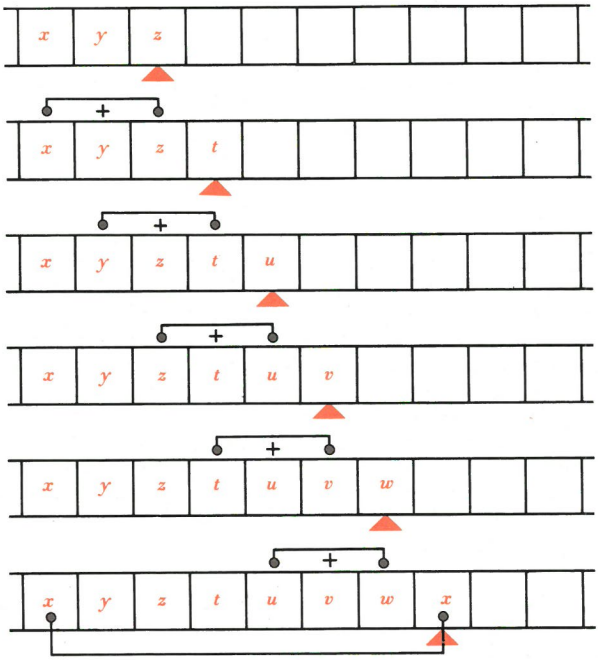
$$u = y + t,$$

inscrira $(u)$, calculera $v = z + u$, $w = t + v$, $s = u + w$, $r = v + s$, etc., ce qui donne la suite infinie

$$(xyztuvwsr...)$$

Si l'on part du triplet (000), il est clair que tous les chiffres marqués sont des 0. Sinon, on obtient un résultat assez remarquable. Le nombre de triplets possibles étant limité (8 en tout dont 000), il est fatal que l'on retombe un moment donné sur le triplet initial $(xyz)$. Les mêmes causes produisant les mêmes effets, la suite va donc finir par se reproduire exactement à la manière d'un motif de tapisserie. Ce qui n'est pas évident par contre, c'est qu'un triplet distinct de (000) redonne, par ce processus, les six autres triplets non nuls. En d'autres termes, les chiffres $(sr...)$ reproduisent exactement la suite fondamentale $(xyztuvw)$, que l'on peut déduire explicitement de $(xyz)$ par les formules (dans $F_2$) :

$$t = y + z,\ u = x + y + z,\ v = x + y,$$
$$w = y + z\ (s = x,\ r = y,\ \text{etc.})$$




Partant du triplet (*xyz*) non nul, la machine de Turing (ou l'ordinateur) qui ont reçu la consigne « sommez le dernier chiffre écrit et celui qui en est séparé par une case » inscrivent successivement *t*, *u*, *v*, *w* puis de nouveau *x*, *y*, *z*, etc. Partant de n'importe quel triplet distinct de (000) on obtient une suite contenant (... 001 110 100 111 010 011 101 001 110 1 ...)

Essayons à partir de (001) : on obtient la suite

(0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 ...)

où le motif principal est souligné. Cherchons tous les triplets (*xyz*), (*yzt*), (*ztu*), (*tuv*), (*uvw*), (*vws*) = (*vwx*), (*wsr*) = (*wxy*) : on obtient (001), (011), (111), (110), (101), (010) et (100), c'est-à-dire les sept triplets autres que (000).

Un mathématicien américain, S. K. Stein, a raconté [1] l'histoire de cette suite et de ses généralisations (roues à mémoire, codes à enchaînement ou réguliers, etc.). Sans

1. Notamment dans un numéro du *Scientific American* (mai 1961) et dans son livre *les Mathématiques, ce monde que créa l'homme* (Dunod), pp. 122 à 134.

reprendre son exposé, nous voudrions montrer ici quelques coïncidences étranges (pour le profane, non pour le spécialiste de l'informatique ou de la théorie des nombres qui les a déjà rencontrées) nées de ce processus élémentaire.

## Des égalités matricielles remarquables

Le passage du triplet $(x, y, z)$ au triplet

$$(y, z, t) = (y, z, x + z)$$

peut évidemment s'écrire sous forme matricielle :

$$T' = A \times T = \begin{pmatrix} y \\ z \\ t \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ (dans } F_2\text{).}$$

La matrice $A$ satisfait à l'égalité

$$A^3 = I + A^2.$$

Ses puissances $I = A^0$, $A$, $A^2 = A \times A$, $A^3 = A^2 \times A$, $A^4$, $A^5$ et $A^6$ sont toutes distinctes et forment un groupe multiplicatif commutatif, la septième puissance $A^7$ étant égale à l'élément neutre $I$. Elles représentent les passages de $(xyz)$

| $O$ | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ | $A^6$ | $A^7$ | $A^8$... |
|---|---|---|---|---|---|---|---|---|---|
| 000 | 100 | 010 | 001 | 101 | 111 | 110 | 011 | 100 | 010 ... |
| 000 | 010 | 001 | 101 | 111 | 110 | 011 | 100 | 010 | 001 ... |
| 000 | 001 | 101 | 111 | 110 | 011 | 100 | 010 | 001 | 101 ... |
| | | | | | | | | $(=I)$ | $(=A)$ |

Eléments du corps $\{ O, I, A, A^2, A^3, A^4, A^5, A^6 \}$ isomorphe à $F_8$.
Pour passer de $A^n$ à $A^{n+1}$ on peut remarquer que les deux dernières lignes de $A^n$ sont les premières de $A^{n+1}$, la 3e colonne de $A^n$ est la première de $A^{n+1}$, etc...

à tous les triplets de la suite (par exemple $A^3$ le transforme en $(tuv)$ ). Leurs dernières colonnes, lues de haut en bas, reproduisent exactement tous les triplets (001) (011) (111) (110) (101) (010) (100). Chacune d'entre elles peut s'exprimer, d'une façon et d'une seule, sous la forme $(pI + qA + rA^2)$, où $p$, $q$ et $r$ sont 3 nombres non tous nuls du corps $F_2 = \{ 0, 1 \}$. Si on ajoute à cet ensemble à sept éléments la matrice nulle dont tous les éléments sont des 0, on obtient un espace vectoriel (de dimension 3 sur $F_2$ dont une base est $\{ I, A, A^2 \}$) mais surtout un corps : le corps de Galois $F_8$.

**ADDITION**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $O$ | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ | $A^6$ |
| $I$ | $O$ | $A^5$ | $A^3$ | $A^2$ | $A^6$ | $A$ | $A^4$ |
| $A$ | $A^5$ | $O$ | $A^6$ | $A^4$ | $A^3$ | $I$ | $A^2$ |
| $A^2$ | $A^3$ | $A^6$ | $O$ | $I$ | $A^5$ | $A^4$ | $A$ |
| $A^3$ | $A^2$ | $A^4$ | $I$ | $O$ | $A$ | $A^6$ | $A^5$ |
| $A^4$ | $A^6$ | $A^3$ | $A^5$ | $A$ | $O$ | $A^2$ | $I$ |
| $A^5$ | $A$ | $I$ | $A^4$ | $A^6$ | $A^2$ | $O$ | $A^3$ |
| $A^6$ | $A^4$ | $A^2$ | $A$ | $A^5$ | $I$ | $A^3$ | $O$ |

**MULTIPLICATION**

| | | | | | | |
|---|---|---|---|---|---|---|
| $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ | $A^6$ |
| $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ | $A^6$ | $I$ |
| $A^2$ | $A^3$ | $A^4$ | $A^5$ | $A^6$ | $I$ | $A$ |
| $A^3$ | $A^4$ | $A^5$ | $A^6$ | $I$ | $A$ | $A^2$ |
| $A^4$ | $A^5$ | $A^6$ | $I$ | $A$ | $A^2$ | $A^3$ |
| $A^5$ | $A^6$ | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ |
| $A^6$ | $I$ | $A$ | $A^2$ | $A^3$ | $A^4$ | $A^5$ |

**Tables du corps $F_8$**

$O = 0I + 0A + 0A^2$ $\quad I = 1I + 0A + 0A^2$ $\quad A = 0I + 1A + 0A^2$

$A^2 = 0I + 0A + 1A^2$ $\quad A^3 = 1I + 0A + 1A^2$ $\quad A^4 = 1I + 1A + 1A^2$

$A^5 = 1I + 1A + 0A^2$ $\quad A^6 = 0I + 1A + 1A^2$.

Les coordonnées de $I$, $A$, $A^2$, $A^3$, $A^4$, $A^5$, $A^6$ dans la base $\{ I, A, A^2 \}$ sont les triplets (100) (010) (001) (101) (111) (110) (011) c'est-à-dire les lignes de la matrice $H$ du bas de cette page.

Cet exemple est très riche. En fait, il exhibe une *représentation matricielle* d'un groupe (le groupe multiplicatif des sept matrices non nulles), représentation qui ramène un groupe abstrait fini à un ensemble de matrices sur lesquelles on peut agir avec toute la puissance du calcul linéaire (on emploie couramment de telles représentations en physique nucléaire et dans de nombreux domaines des mathématiques appliquées) ; il montre de plus comment construire un corps fini à $p^n$ éléments ($p$ étant premier), à partir du corps $F_p$ et d'une équation, comme $A^3 = I + A^2$, qui est de degré $n$ et n'a pas de solutions dans $F_p$ mais en reçoit si l'on considère des matrices à éléments dans $F_{p^n}$. Une telle méthode est très voisine de l'adjonction algébrique que nous avons décrite brièvement page 159 : en fait elle n'en diffère pas fondamentalement.

## Encore le codage

Nous pouvons observer encore d'autres résultats intéressants. Considérons le passage du triplet $(xyz)$ au 7-plet $(xyztuvw)$ ; il peut également s'écrire matriciellement, sous la forme :

$$S = H \times T = \begin{bmatrix} x \\ y \\ z \\ t \\ u \\ v \\ w \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Les lignes (123) de la matrice $H$ forment la matrice $I$, les lignes (234) forment $A$, (345) forment $A^2$, (456) forment $A^3$, etc., et les lignes (671) forment $A^5$, (712) forment $A^6$. La dernière colonne de $H$ est donc notre suite (0011101) qui « engendrait » tous les triplets non nuls : $H$ « engendre » de même les puissances de $A$. On obtient d'ailleurs la ligne $(n + 3)$ de $H$ en ajoutant les lignes $(n)$ et $(n + 2)$, ce qui redonne bien notre processus.

Appliquons la matrice $H$ à tous les triplets (000), (001) et ceux qui s'en déduisent par $A$, $A^2$, $A^3$, etc. On obtient ainsi un tableau à 8 lignes et 7 colonnes :

| $x$ | $y$ | $z$ | $t$ | $u$ | $v$ | $w$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 1 | 0 |

On peut constater que la distance entre deux lignes quelconques, distance définie (cf. page 164) par le nombre de colonnes où les chiffres correspondants sont distincts, est égale à 4 quelque soit le choix de la paire de lignes (distinctes) : il y a deux « 1 » et un « 0 » qui coïncident, les autres signes différent. Ceci permet d'employer les huit lignes pour coder huit signes (par exemple pour coder des nombres écrits en système octal, qui utilise huit chiffres : 0, 1, 2, 3, 4, 5, 6 et 7) ; la distance entre deux « mots » du code étant grande et régulière, celui-ci est particulièrement sûr. Voici comment l'utiliser : on y effectue quatre tests après avoir reçu un « mot » de 8 signaux, les tests $T$ (vérifier $t = x + z$), $U$ (vérifier $u = x + y + z$), $V$ (vérifier $v = x + y$) et $W$ (vérifier $w = y + z$). Si la ligne de transmission n'est pas trop défectueuse, on admettra volontiers qu'il n'y a pas eu plus de trois erreurs commises dans ce message de 7 bits (unités d'information) ; dans ces conditions, si les quatre tests sont favorables, on peut être certain que le mot a été bien transmis (on dit que le code détecte 3 erreurs au plus). Un nombre impair de tests défaillant prouve la présence de 1 ou de 3 erreurs, un nombre pair démontrant celle de 2 er-

reurs. De plus, si l'on admet (ce qui est encore assez probable) qu'une erreur double a de fortes chances de s'être produite sur deux chiffres voisins, on dispose d'une règle de correction pour une erreur simple ou une erreur double entre chiffres consécutifs. Un tableau donne en effet, d'après les tests défaillants, les corrections à apporter.

| tests défaillants | colonne (s) à corriger |
|---|---|
| $T$ | $t$ |
| $U$ | $u$ |
| $V$ | $v$ |
| $W$ | $w$ |
| $TU$ | $tu$ |
| $TV$ | $tvyz$ |
| $TW$ | $txy$ |
| $UV$ | $uv$ |
| $UW$ | $zt$ |
| $VW$ | $vw$ |
| $TUV$ | $x$ |
| $TUW$ | $z$ |
| $UWW$ | $y$ |

**Tableau de correction d'erreurs** (une simple ou une double portant sur deux chiffres voisins).
Mais la défaillance simultanée de $T$ et de $U$ peut également provenir d'erreurs sur $x$ et $v$, ou sur $z$ et $w$ ; la défaillance simultanée de $T$, $U$ et $V$ peut également provenir d'erreurs sur $(y, z, u)$, $(y, t, w)$, $(z, t, w)$ ou $(t, u, v)$, etc...

Otons la première ligne (0000000) du tableau de la p. 175. Il reste une matrice carrée symétrique (la n-ième colonne est formée des chiffres de la n-ième ligne). Si l'on en lit les lignes comme des nombres écrits en système binaire, on s'aperçoit qu'il s'agit des nombres 29, 58, 116, 105, 83, 39 et 78. On passe d'un tel nombre au suivant en le doublant (mais en en soustrayant 127 si le total est supérieur à 127 : ceci tient à ce que 127 est le nombre qui s'écrit 1111111 en système binaire). La démonstration de ce résultat curieux est simple ; il suffit en effet d'observer que l'on passe de la ligne $(n)$ à la ligne

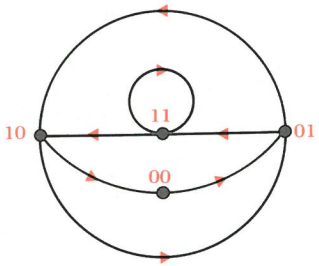
| | | |
|---|---|---|
| $(n)$ | 0011101 | |
| $(n + 1)$ | 0111010 | Passage de la ligne $(n)$ à la ligne $(n + 1)$. |

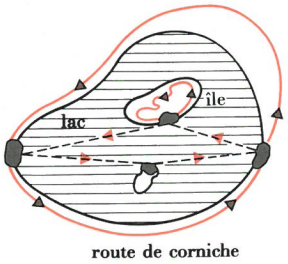
0011101
0111010
1110100
1101001
1010011
0100111
1001110

Cette écriture décalée du tableau montre bien les recouvrements de la suite fondamentale (0011101).

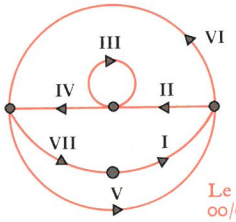
suivante en en enlevant le terme d'extrême gauche pour le porter à sa droite : chaque ligne se déduit de la précédente par une permutation dite circulaire, ou une translation vers la gauche d'une unité (compensée aux extrémités). Cette translation est la conséquence logique de la propriété selon laquelle deux triplets tels que $(xyz)$ et $(yzt)$ de la suite (0011101001110 1...) se recouvrent partiellement, la fin $(yz)$ du premier étant identique au début du second.

Ceci suggère une approche concrète (due à Good) du problème consistant à trouver des suites « à mémoire » telles que (0011101) qui redonnent tous les $n$-uplets possibles formés avec $n$ éléments de $F_2$. Nous l'exposerons pour $n = 3$ : le schéma ci-dessous est un graphe orienté reliant des sommets




**Le graphe de Good et son interprétation dans Disneyland.**




7

Le mot (001110100) correspond au circuit 00/01/11/11/10/01/10/00.

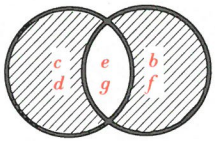
qui sont les doublets (00) (01) (10) (11) de $F_2 \times F_2$. Un arc entre $(xy)$ et $(tz)$ signifie que les extrémités $y$ et $t$ sont confondues et représente le triplet $(xyz)$ (il existe des boucles comme celle qui relie (11) à lui-même et représente (111) ; nous n'avons pas figuré de boucle en (00) car nous ne nous intéressons pas à (000)). On peut imaginer que ce graphe représente un lac, le long duquel est instauré un sens unique, avec un service régulier de bateaux qui assure (toujours en tournant dans le sens inverse des aiguilles d'une montre, comme il sied en mathématiques !) l'abordage dans une île où il faut absolument suivre un trajet particulièrement pittoresque et l'accostage sur un îlot. Le problème consistant à trouver une suite telle que (0011101001101...) peut s'exprimer sur le graphe de la page précédente : déterminer un itinéraire permettant de partir d'un point quelconque, faire le tour du lac, visiter l'île et toucher l'îlot sans suivre deux fois le même chemin. Nous retrouverons un problème analogue plus loin (voir page 182).

Notre sujet n'est pas encore épuisé : considérez les lignes du tableau comme représentant des sous-ensembles à 4 éléments de l'ensemble $E = \{ a, b, c, d, e, f, g \}$ (cf. page 167). Vous constaterez que la différence symétrique de deux d'entre eux est encore dans l'ensemble, qu'une intersection quelconque (resp. une réunion) est de cardinal 2 (resp. 6) et qu'on peut réengendrer ainsi $E$ entier ! Nous l'abandonnerons néanmmoins pour explorer la topologie.

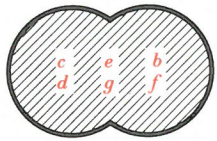
**Sous-ensembles de $E = \{ a, b, c, d, e, f, g \}$ associés aux mots du code**

| 0000000 | 0011101 | 0111010 | 1110100 |
|---|---|---|---|
| $\varnothing$ | $\{ cde\ g \}$ | $\{ bcd\ f \}$ | $\{ abc\ e \}$ |

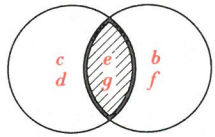
| 1101001 | 1010011 | 0100111 | 1001110 |
|---|---|---|---|
| $\{ ab\ d\ g \}$ | $\{ a\ c\ fg \}$ | $\{ b\ efg \}$ | $\{ a\ def \}$ |




Exemple :
- $\{ c, d, e, g \} \triangle \{ b, e, f, g \} = \{ b, c, d, f \}$
  $(0011101) + (0100111) = (0111010)$

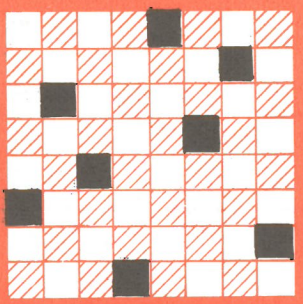



- $\{ c, d, e, g \} \cup \{ b, e, f, g \} = \{ b, c, d, e, f, g \}$

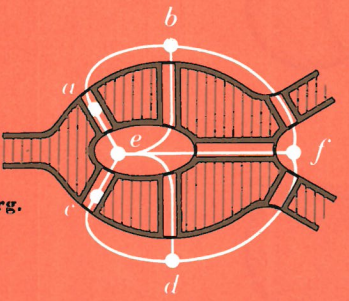



- $\{ c, d, e, g \} \cap \{ b, e, f, g \} = \{ e, g \}$

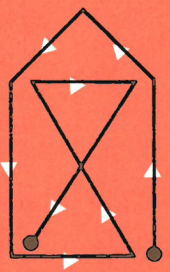
On peut reconstituer entièrement $\mathcal{P}(E)$ par de telles opérations :
par exemple :
- $\{ a \} = \{ a, b, c, e \} \cap \{ a, b, d, g \} \cap \{ a, c, f, g \}$,
- $\{a, b, c \} = \{ a \} \cup \{ b, c, d, f \} \cap \{ a, b, c, e \})$
- $E = \{ a \} \cup \{ c, d, e, g \} \cup \{ b, e, f, g \}$, etc.



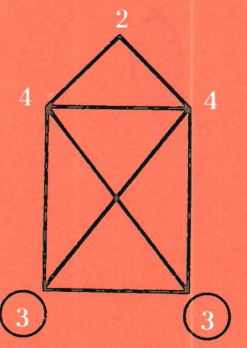
L'une des 92 solutions du problème de la dame aux échecs : aucune des 28 droites joignant deux pièces n'est ni horizontale, ni verticale, ni à 45 degrés.




**Les ponts de Königsberg.**



**La guérite ou l'enveloppe.**
Une chaine eulérienne possible.



# De la théorie des graphes à la topologie

Le lecteur profane lui-même n'aura pu manquer de remarquer quelle place tiennent, dans les présentations modernes de problèmes parfois très anciens, les diagrammes et les représentations figurées qui symbolisent l'effort de structuration de la mathématique. En logique par exemple, ou dans toute partie d'un exposé où interviennent des démonstrations un peu complexes, l'établissement d'un graphe rend évidentes les implications et les équivalences établies dans les pages qu'il illustre. L'aspect très élémentaire de ces représentations fait illusion ; si certaines d'entre elles sont effectivement triviales et sont employées depuis des siècles (sans apparaître toutefois dans les livres anciens où elles n'auraient guère paru sérieuses), le concept même de graphe n'a rien d'évident.

## L'analysis situs

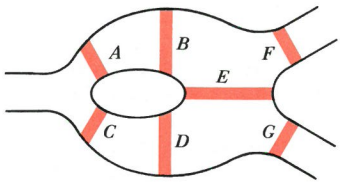
L'étude de ces figures où comptent des relations telles que « être entre tel et tel point », « être relié à tel point », « être d'un seul tenant », etc., est une partie de la *topologie*. L'origine de celle-ci est bien connue ; nous la reprendrons néanmoins une fois de plus car elle est particulièrement intéressante. D'un problème fameux traité pour la première fois par Euler en 1735, est né une branche particulière des mathématiques appelée alors *analysis situs* (analyse des positions), illustrée par d'autres questions étudiées par Euler lui-même (les trente-six officiers), Gauss (le problème des

huit dames aux échecs qui ne se mettent pas mutuellement en échec), Lucas (le problème des ménages placés autour d'une table ronde sans que deux époux soient côte à côte), etc. Toutes ces questions ressortissent aujourd'hui à la combinatoire qui fait grand usage de la notion de *graphe*. Celle-ci, issue directement du problème d'Euler que nous allons rappeler, a connu un grand développement assez récemment sous l'influence de l'informatique naissante. L'analysis situs est à l'origine de la création de la topologie générale, dont l'importance ne saurait être sous-estimée aujourd'hui, la mathématique contemporaine étant née de la collaboration entre l'algèbre et la topologie.

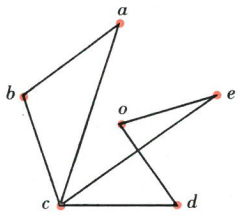
Partons donc de Königsberg, où la rivière Pregel entoure deux îles. L'île de Kneiphof est reliée à chaque rive par deux ponts (*A* et *B*, *C* et *D*) ; un cinquième l'unit à une presqu'île elle-même connectée à chaque rive. Le problème des bourgeois désœuvrés du dimanche consistait à trouver un itinéraire empruntant, une fois et une seule, chacun de ces ponts. Euler prouva l'impossibilité de ce programme. Le problème se pose de la façon suivante : étant donné un certain nombre de chemins reliant différents points, existe-t-il un chemin « eulérien », c'est-à-dire une suite de tronçons qui permette de les décrire tous mais sans répétition (il est permis de passer plusieurs fois au même endroit, mais à condition d'y arriver et d'en repartir par des itinéraires différents). Posons-le en termes de graphes (voir page 71), que nous prendrons non orientés pour simplifier [1]. Un certain nombre de sommets sont reliés par des arêtes [2]. Le degré d'un sommet est le nombre d'arêtes y aboutissant. Une chaîne est une suite d'arêtes que l'on peut tracer d'un trait continu ; elle est simple si aucune arête n'est utilisée deux fois, et eulérienne si elle est simple et utilise toutes les arêtes. Un cycle est une chaîne fermée (qui revient à son point de départ). Une chaîne est élémentaire si aucun sommet n'est utilisé deux fois, et hamiltonienne si elle est élémentaire et utilise tous les sommets. (Pour des graphes orientés, arête devient arc, chaîne se traduit par chemin, et cycle par circuit.)

1. Le graphe de Good du chapitre précédent est orienté ; les différences entre les deux sortes de graphes, pour le problème eulérien, sont minimes.

2. En principe il n'existe qu'une arête au plus entre deux sommets. Si cela n'était pas (comme dans le problème de Königsberg) on créerait artificiellement autant de sommets qu'il est nécessaire pour obéir à cette règle simplificatrice.




**Les ponts de Königsberg**

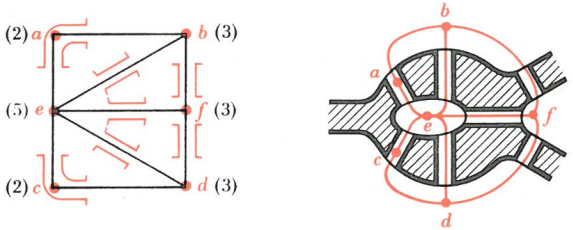



**Graphe non orienté.**
(Sommets *o*, *a*, *b*, *c*, *d*, *e* ;
arêtes *od*, *oe*, *ab*, *ac*, *bc*, *cd*, *ce*.)

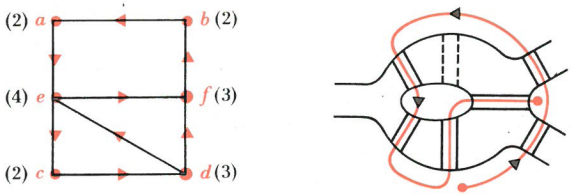
## Le problème d'Euler

Le théorème d'Euler repose sur la remarque banale suivante : quel que soit le sommet où l'on arrive, il faut en repartir, ce qui donne en tout sommet d'une chaîne simple un nombre égal d'arêtes utilisées pour y arriver et d'arêtes pour en repartir (ceci pouvant toutefois être faux aux deux extrémités de la chaîne). S'il existe une chaîne eulérienne dans le graphe, tout sommet du graphe est de degré pair ; ceci est entièrement exact si la chaîne est un cycle. Si elle n'est pas fermée, seuls les degrés des extrémités sont impairs.

Dans le problème de Königsberg, il existe quatre sommets de degrés impairs : aucune chaîne ne permet donc d'effectuer




**Le graphe de Königsberg.** Les degrés sont écrits à côté des sommets. Le schéma ci-dessus montre comment extraire ce graphe abstrait de la figure réelle (il a fallu créer deux sommets supplémentaires *a* et *c* pour distinguer les deux routes menant de *b* à *c*, et celles qui joignent *d* et *e*).




**Problème de Königsberg modifié.** En supprimant le pont *B*, on peut trouver une chaîne eulérienne ; ses extrémités sont alors nécessairement les sommets de degrés impairs.

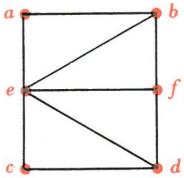
sans hélicoptère le trajet des sept ponts. Dans un problème assez connu qui occupe parfois les écoliers fatigués d'écouter leur maître (celui qui consiste à dessiner à la manière eulérienne une guérite de soldat – une enveloppe si l'on est antimilitariste), il existe deux sommets de degré impair : s'il existe une chaîne eulérienne, elle doit nécessairement partir et revenir en ces deux points. Si l'on supprime au hasard un pont à Königsberg, l'étude des degrés montre immédiatement d'où il faut partir et où il faut arriver (à une symétrie près dans la description du trajet trouvé [1]).

## Le voyageur de commerce

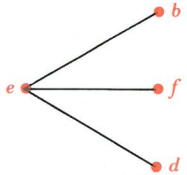
Le théorème d'Euler est même un théorème constructif, ce qui est assez rare en mathématiques. Non seulement il donne une condition nécessaire d'existence, mais il prouve que cette condition est suffisante en exhibant une méthode pour trouver la chaîne eulérienne. On a longtemps recherché un théorème analogue pour les chaînes (et plus généralement les chemins dans un graphe orienté) hamiltoniennes : c'est le célèbre « problème du voyageur de commerce ». Ce dernier doit visiter un certain nombre de villes (les sommets du graphe). Pour des raisons économiques évidentes, il recherche un chemin qui ne passe qu'une fois par chaque ville en les atteignant toutes ; parmi ces chemins il recherche le trajet le plus court.

La similitude des définitions laisserait espérer une solution aussi simple que celle du problème d'Euler. Il n'en est rien ; si tout chemin élémentaire est simple, il est inexact que tout graphe admettant un chemin hamiltonien admette un chemin eulérien (l'inverse est également faux). Le problème resta sans solution, autre qu'une énumération plus ou moins déguisée (et absolument impraticable même par un ordinateur), de 1859 à 1963. Une équipe américaine, sous la direction de J. D. C. Little, mit au point un algorithme

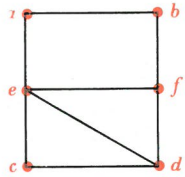
1. Nous n'avons, jusqu'à présent, donné qu'une réponse négative : dans certains cas (ceux où il existe plus de deux sommets de degré impair), il n'existe pas de chaîne eulérienne. Mais le théorème d'Euler est beaucoup plus riche. Il affirme en effet que s'il n'existe que deux sommets de degré impair, on peut toujours trouver une chaîne eulérienne les reliant ; qu'il est impossible qu'il n'existe qu'un seul sommet de degré impair ; enfin que si tous les degrés sont pairs, il existe un cycle eulérien. On pourra vérifier ce théorème sur des graphes pris au hasard (par exemple sur un hypercube à quatre dimensions, page 122).



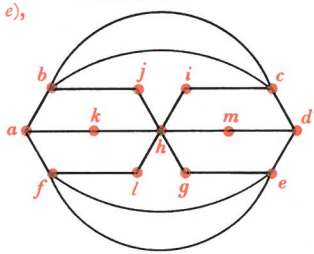

Hamiltonien (*a b f d c e*), non eulérien.




Ni hamiltonien, ni eulérien.




Hamiltonien et eulérien.




Eulérien (*a b c d e f e g h i c b j h k a f l h m d*), non hamiltonien.

effectivement réalisable pour le résoudre (méthode de séparation et d'évaluation progressive, ou *branch and bound*). Cette méthode est complexe [1] et ne comporte pas de condition nécessaire et suffisante aussi simple que celle d'Euler. Il est douteux qu'un braconnier, désirant limiter au maximum le risque d'être pris en relevant ses collets, ou une ménagère recherchant le meilleur chemin pour faire son marché puissent l'appliquer sans une étude préalable par un bureau de recherche opérationnelle! Mais enfin elle existe, et on a pu l'appliquer, après aménagements, à une foule d'autres problèmes analogues, comme ceux consistant à affecter des ouvriers à certaines tâches en rendant minimums le coût ou le temps de l'opération totale, aux problèmes d'ordonnancement (qui tiennent compte de certaines contraintes obligeant à réaliser certaines affectations après d'autres : on ne peut construire le toit d'une maison, par exemple, avant d'en avoir creusé les fondations, etc.) et en général à tous les problèmes d'*optimisation*. Elle vient donc s'ajouter à la liste déjà longue des méthodes plus ou moins partielles (méthode du simplexe, méthode Pert, etc.) qui forment l'arsenal des chercheurs spécialisés, dont la science est très prisée des planificateurs et des entreprises importantes.

1. Elle est exposée, avec un grand nombre de propriétés combinatoires très intéressantes, dans l'*Introduction à la combinatorique en vue des applications* de Arnold Kaufmann, (Dunod), pp. 377 et sq.

## La topologie

Les problèmes de graphes ne constituent qu'une retombée de l'analysis situs. Les recherches sur les formes des surfaces, sont centrées sur des propriétés relatives au nombre de points d'intersection de courbes, à la relation « il existe une courbe reliant tel et tel point », aux concepts de déformation continue comme celles qui transforment un cube en une sphère, une tasse avec anse en un tore, etc. D'une manière un peu vague, on peut dire que la topologie est née des relations issues de la géométrie où les notions de distance, de parallèle et même de ligne droite ne sont pas utilisées : elle se consacre à la structure même des ensembles ponctuels auxquels on laisse une liberté maximum quand aux déplacements relatifs qui ne mettent pas en cause les « positions » relatives de ces points.

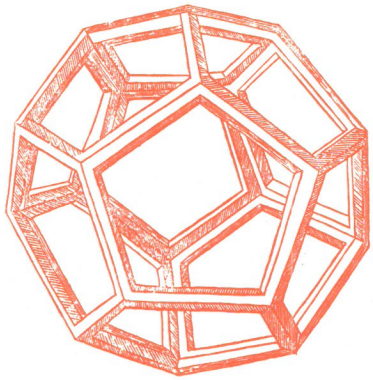
L'étude de la *continuité* était restée longtemps l'apanage de la seule analyse, par le biais des fonctions continues définies sur des nombres réels ou complexes. C'est d'ailleurs un problème d'analyse pure (sur les séries trigonométriques) qui avait amené Cantor à étudier le concept d'ensemble, concept dont Lebesgue fit un grand usage dans sa généralisation de la notion d'intégrale. C'est pourquoi la théorie naissante des ensembles, loin d'être d'abord appliquée aux structures algébriques comme aujourd'hui dans les livres scolaires élémentaires, apparaissait il y a peu encore dans les ouvrages d'analyse. Or voici que la topologie, par exemple par ses déformations continues, mettait en évidence des concepts clés tels que celui de *voisinage*, celui de point d'accumulation (essentiel dans la construction des nombres réels). En quelques années, la topologie conquit à son tour l'analyse quand on put en dégager les structures fondamentales.

## La mathématique est une

Voici comment, d'une façon très grossière, on pourrait imaginer l'unité actuelle de la mathématique. D'une part les *structures algébriques* étudient les opérations, les relations, les applications : en un certain sens, ces structures algébriques sont bien les filles abstraites du calcul. A cet ensemble statique, les *structures topologiques* apportent la notion dynamique de *limite* (au sens du verbe « tendre vers ») : les groupes, les espaces vectoriels topologiques sont des groupes, des vectoriels où les procédés issus de l'analyse classique, voire

du calcul différentiel et intégral, permettent un enrichissement considérable des modèles étudiés par l'introduction des phénomènes de convergence. Il n'y a guère de structure mathématique importante (en dehors naturellement des grandes familles de base) qui ne mêle l'algèbre et la topologie. Le meilleur exemple en est certainement la *géométrie*. Non seulement celle-ci n'est pas morte, mais elle reste un secteur très vivant, apportant son langage et son capital d'intuition très apprécié. Seulement elle s'est dégagée depuis longtemps des problèmes très particuliers de la géométrie euclidienne et des fastidieuses énumérations de courbes et de surfaces remarquables. Elle atteint sa plus grande généralité quand on lui donne les systèmes d'axiomes les plus divers : on considère, par exemple, des géométries sur des nombres finis de points de dimensions diverses, des géométries dans des espaces fonctionnels (où les points sont des fonctions) ; on voit que le processus de « contestation » inauguré en banissant le postulat d'Euclide pour construire les géométries non euclidiennes a porté des fruits bien plus riches encore qu'on n'aurait pu le croire il y a seulement un siècle. Cette généralité se paye par le fait qu'il n'y a plus aucune frontière distincte entre les domaines dont on essaie de tracer les limites pour la commodité de l'esprit. Comment dissocier l'algébrique et le topologique (donc le géométrique) dans telle théorie, comme celle des distributions ? Cela n'est ni possible, ni intéressant en soi : l'essentiel est de ramener toute structure mathématique à un petit nombre de combinaisons-clés dont l'origine est indifférente, tant les siècles et les travaux les plus divers (arithmétique, géométrie euclidienne, calcul algébrique, combinatoire, physique théorique, mécanique) ont contribué collectivement à en dégager la puissance et la pureté.

Si tentant qu'il aurait pu être d'emmener notre lecteur dans la véritable topologie (dont ce qui précède ne donne que le point de départ historique, et pas du tout l'aspect actuel), dans la géométrie rénovée, il faut s'arrêter sagement et conclure. Notre seul espoir est, qu'en dépit de la mauvaise foi de l'auteur (qui a souvent feint de croire que ce qu'il racontait était nécessairement à la portée de tous!), les pages qu'on vient de lire ont pu donner une vue au moins approximative des méthodes, voire de l'esprit des mathématiques éternelles d'aujourd'hui. Le prochain rendez-vous est à prendre pour les mathématiques modernes de demain.



# Bibliographie

Parmi les très nombreux livres de langue française traitant de tout ou partie des sujets abordés dans cet ouvrage, on peut isoler (arbitrairement) :

## Livres généraux

F. Le Lionnais (sous la direction de), *les Grands Courants de la pensée mathématique*, (Blanchard) : recueil de textes écrits par des mathématiciens sur leur science.

I. Adler, *Initiation à la mathématique, d'aujourd'hui*, (O.C.D.L.) ainsi que de nombreux livres de Revuz, Dienes, etc., : les mathématiques modernes vues par des éléments enthousiastes, novateurs en pédagogie.

S. K. Stein, *les Mathématiques, ce monde que créa l'homme*, (Dunod) : recueil (très clair) de dissertations sur certains problèmes assez classiques expliqués par un mathématicien.

P. Rosenstiehl et J. Mothes, *les Mathématiques de l'action*, (Dunod) : un classique de l'application des mathématiques finies aux sciences économiques, à la probabilité, etc.

H. Rademacher et O. Tœplitz, *Plaisir des mathématiques*, (Dunod) : articles (déjà un peu anciens) consacrés à des questions particulières mais traitées avec un art consommé de la vulgarisation pertinente des méthodes mathématiques.

J.-L. Boursin, *les Structures du hasard*, (Seuil : même collection) : introduction classique au calcul des probabilités.

A. Warusfel, *les Nombres et leurs Mystères*, (Seuil : même collection) : exposé élémentaire des différents ensembles de nombres usuels et de certaines de leurs applications.

Outre ces ouvrages généraux, on pourra consulter les livres plus spécialisés suivants, classés en deux niveaux :

## Niveau d'un baccalauréat scientifique

P. R. Halmos, *Introduction à la théorie des ensembles*, (Gauthier-Villars et Mouton) : exposé complet bien qu'autonome des principaux résultats de cette théorie ; très accessible.

K. Kuratowski, *Théorie des ensembles et topologie*, (L'enseignement mathématique) : exposé beaucoup plus riche, dont une partie déborde largement le niveau annoncé, mais contenant tout ce que connaît, en général, un mathématicien non spécialiste de ces questions.

J. Chauvineau, *la Logique moderne*, (P.U.F., « Que sais-je ? ») : abrégé des éléments de la logique mathématique.

L. Chambadal, *Éléments d'algèbre*, (Dunod) : exemple réussi d'exposé moderne de l'essentiel de l'algèbre (linéaire y compris) pour des non-spécialistes (élèves préparant H.E.C.).

A. Warusfel, *Dictionnaire raisonné de mathématiques*, (Seuil) : tentative, sous la forme d'un dictionnaire aux articles étendus, de regroupement des principales notions et propriétés élémentaires des mathématiques classiques et modernes.

G. Casanova, *l'Algèbre de Boole*, (P.U.F., « Que sais-je ? ») : l'essentiel sur une structure fondamentale en informatique.

J. Itard, *Arithmétique et Théorie des nombres*, (P.U.F., « Que sais-je ? ») : la naissance de l'algèbre abstraite à travers les problèmes passionnants que posent les nombres entiers.

## Niveau d'une propédeutique scientifique

N. Bourbaki, *Éléments d'histoire des mathématiques*, (Hermann) : l'évolution actuelle décrite par un orfèvre.

P. Dubreil et M.-L. Dubreil-Jacotin, *Leçons d'algèbre moderne*, (Dunod) : le développement de l'algèbre générale, avec les principales structures (treillis par exemple).

D. Ponasse, *Logique mathématique*, (O.C.D.L.) : exposé complet où se mêlent les structures algébriques, topologiques pour l'étude des différents calculs.

A. Kaufmann, *Introduction à la combinatorique en vue des applications*, (Dunod) : recueil de méthodes de dénombrement et d'énumération employées notamment en recherche opérationnelle.

G. Cullmann, *Codes détecteurs et correcteurs d'erreurs*, (Dunod) : avec une première partie consacrée à l'algèbre moderne.

C. Berge, *La théorie des graphes et ses applications*, (Dunod) : la première référence française en ce domaine récent.

A. Warusfel, *les Corps finis* (en préparation) : sur un sujet limité, les théorèmes et les méthodes fondamentales de l'algèbre abstraite.

# Index

Parmi les deux cents mots ou expressions définis dans ce livre (que l'on reconnaît à ce qu'ils sont en italique), on peut retenir les suivants avec l'indication de la page où ils sont introduits :



# Illustrations


Archives A. W. : pp. 4, 98, 188. - Keystone : pp. 32, 132b, 132c. - Roger Viollet : p. 66. - Express : p. 132e. - D. R. : pp. 132a, 132d. - Schémas Ed. du Seuil/Ho Tham Kouie : p. 1 de cv, pp. 2, 9, 12, 13, 14, 15, 16, 17, 18, 24, 31, 38, 40, 42, 45, 46, 47, 48, 49, 51, 54, 55, 56, 57, 58, 59, 60, 61, 62, 64, 68, 69, 70, 71, 73, 75, 76, 77, 79, 81, 82, 84, 86, 89, 92, 96, 101, 103, 104, 105, 107, 108, 109, 118, 119, 120, 121, 122, 123, 124, 125, 140, 141, 143, 144, 148, 151, 152, 153, 156, 160, 162, 163, 164, 165, 166, 168, 169, 172, 177, 179, 180, 183, 185.

collections microcosme

## PETITE PLANÈTE

1 Autriche
2 Suède
3 Italie
4 Hollande
5 Irlande
6 Grèce
7 Allemagne
8 Tunisie
9 Suisse
10 Espagne
11 Turquie
12 Chine
13 Iran
14 Israël
15 Danemark
16 Portugal
17 Tahiti
18 Belgique
19 Inde
20 Brésil
21 Japon
22 Sahara
23 URSS
24 Grande-Bretagne
25 Yougoslavie
26 Finlande
27 Norvège
28 Madagascar
29 Venezuela
30 Égypte
31 Maroc
32 Pologne
33 Australie
34 Mexique
35 Tchécoslovaquie
36 Argentine
37 Canada
38 Afrique des Grands Lacs
39 Liban
40 Chypre

## SOLFÈGES

1 Couperin
2 Schumann
3 Ravel
4 Schubert
5 Chopin
6 Haydn
7 Honegger
8 Mozart
9 Jazz
10 Verdi
11 Tchaïkovski
12 Stravinsky
13 Falla
14 Monteverdi
15 Liszt
16 Prokofiev
17 Wagner
18 Rameau
19 Bach
20 Puccini
21 Moussorgsky
22 Debussy
23 Beethoven
24 Bartok
25 Brahms
26 Mahler
27 Franck
28 Vivaldi
29 Berlioz
30 Schönberg

* Ouverture pour une discothèque

## ÉCRIVAINS DE TOUJOURS

1 Hugo *par lui-même*
2 Stendhal
3 Montaigne
4 Flaubert
5 Colette
6 Pascal
7 Zola
8 Giraudoux
9 Baudelaire
10 Montesquieu
11 Proust
12 Malraux
13 Diderot
14 Mauriac
15 Saint-Simon
16 Laclos
17 Montherlant
18 Corneille
19 Michelet
20 Apollinaire
21 Bernanos
22 Shakespeare
23 Gorki
24 Anatole France
25 Barrès
26 Marivaux
27 Gœthe
28 Voltaire
29 Sartre
30 Tchekhov
31 Romain Rolland
32 Giono
33 Balzac
34 Saint-Exupéry
35 Virginia Woolf
36 Descartes
37 Jules Renard
38 Machiavel
39 Joyce
40 Molière
41 Cocteau
42 Horace
43 Homère
44 Melville
45 M^me^ de La Fayette
46 Hemingway
47 Virgile
48 Rabelais
49 Edgar Poe
50 Ronsard
51 Beaumarchais
52 Cicéron
53 Rousseau
54 Rimbaud
55 La Fontaine
56 Maïakovski
57 Dostoïevski
58 Teilhard de Chardin
59 Kierkegaard
60 Aristophane
61 Maupassant
62 André Gide
63 Paul Claudel
64 Camus
65 Faulkner
66 Pasternak
67 Mallarmé
68 Nerval
69 Vigny
70 Érasme
71 Chateaubriand
72 Verlaine
73 Pouchkine
74 Lautréamont
75 M^me^ de Sévigné
76 Julien Green
77 Bergson
78 Benjamin Constant
79 Paul Eluard
80 Hegel
81 Kafka
82 Freud
83 Beckett
84 Sophocle
85 Tacite

collections microcosme

## LE RAYON DE LA SCIENCE

1 L'électronique
2 La conquête des fonds marins
3 Les nuages
4 La vie sur les planètes
5 Le cerveau et la conscience
6 La vie sociale des animaux
7 Le pétrole
8 Le cancer
9 Les nombres et leurs mystères
10 L'énergie nucléaire
11 La connaissance de l'univers
12 Introduction à la géologie
13 L'astronautique
14 L'alimentation
15 La vie de la cellule à l'homme
16 L'optique
17 L'oreille et le langage
18 L'archéologie préhistorique
19 La métallurgie
20 Le froid
21 L'évolution botanique
22 La spéléologie scientifique
23 La médecine chinoise
24 Les structures du hasard
25 Physique de l'océan
26 La vie dans l'océan
27 Les origines de la vie
28 Histoire des mammifères
29 Les médicaments
30 Les mathématiques modernes
31 L'informatique

## MAITRES SPIRITUELS

1 Mahomet et la tradition islamique
2 Saint Augustin et l'augustinisme
3 Saint Jean-Baptiste et la spiritualité du désert
4 George Fox et les Quakers
5 Saint Paul et le mystère du Christ
6 Le Bouddha et le bouddhisme
7 Maître Eckhart et la mystique rhénane
8 Moïse et la vocation juive
9 Socrate et la conscience de l'homme
10 Saint François d'Assise et l'esprit franciscain
11 Fénelon et le pur amour
12 Jean Calvin et la tradition calvinienne
13 David et les psaumes
14 Confucius et l'humanisme chinois
15 Charles de Foucauld et la fraternité
16 Saint Serge et la spiritualité russe
17 Saint Thomas d'Aquin et la théologie
18 Râmakrishna et la vitalité de l'hindouisme
19 Saint Benoît et la vie monastique
20 Saint Grégoire Palamas et la mystique orthodoxe
21 Saint Vincent de Paul et la charité
22 Saint Jean de la Croix et la nuit mystique
23 Saint Ignace de Loyola et la Compagnie de Jésus
24 Isaïe et le prophétisme
25 Saint-Cyran et le jansénisme
26 Rabbi Siméon bar Yochaï et la Cabbale
27 Patañjali et le Yoga
28 Luther et l'Église confessante
29 Saint François de Sales et l'esprit salésien
30 Saint Bonaventure et la sagesse chrétienne
31 Bérulle et l'École française
32 Râmânuja et la mystique vishnouite
33 Épictète et la spiritualité stoïcienne
34 Lao tseu et le taoïsme
35 Zarathushtra et la tradition mazdéenne
36 Saint Bernard et l'esprit cistercien

## LE TEMPS QUI COURT

GROUPES SOCIAUX

2 Les instituteurs
3 Les intellectuels au Moyen Age
4 Les marchands au XVIe siècle
5 Les stars
6 Les prêtres de l'ancienne Égypte
7 Les juges
8 Les officiers
9 Les grandes dames romaines
10 Les templiers
11 Les bâtisseurs de cathédrales
16 Les alchimistes
19 Les Francs-Maçons
22 Les courtisans
23 Les troubadours
25 Les explorateurs au Moyen Age
31 Les prêtres
35 Les Conquistadores
36 Les communards
39 Les premiers chrétiens

CIVILISATIONS

1 Les Gaulois
12 Les Étrusques
24 Les Assyriens
26 Les Incas
30 Les Byzantins
32 Les Hébreux
33 Les Khmers

BIOGRAPHIES

13 César
14 Napoléon
15 Lénine
17 Jeanne d'Arc
18 Christophe Colomb
20 Hitler
21 Robespierre
27 La reine Victoria
28 Catherine II
29 Gengis Khan
34 Pétain
37 Lincoln
38 De Gaulle

ACHEVÉ D'IMPRIMER EN 1969 PAR L'IMPRIMERIE TARDY A BOURGES
D. L. 3e trim. 1969 - No 2331.3 (5793)