MATHÉMATIQUES ET SCIENCES HUMAINES

M. EYTAN
G. TH. GUILBAUD

Présentation de quelques monoïdes finis (initiation à l'algèbre)

Mathématiques et sciences humaines, tome 7 (1964), p. 3-10
<http://www.numdam.org/item?id=MSH_1964__7__3_0>

PRESENTATION DE QUELQUES MONOIDES FINIS

(Initiation a l'Algèbre)

par M. EYTAN,
et G.Th. GUILBAUD

1. Parmi les structures algébriques, celle de monoïde, que nous définissons plus loin, est une des plus fondamentales. Elle est une abstraction d'une construction très souvent utilisée dans les systèmes formels. On se donne au départ un alphabet (A), ensemble de signes (ou symboles). A partir des signes de l'alphabet on construit des mots en juxtaposant un certain nombre (arbitraire mais fini) de signes conformément à certaines règles (orthographe); l'ensemble des mots est le lexique (L). On étend la juxtaposition, définie jusqu'à présent pour les signes de l'alphabet (A), aux mots du lexique (L), cette opération consistant à écrire les deux mots de (L) l'un à la suite de l'autre. On a ainsi une loi de composition interne sur (L) qui à tout couple (x, y) de mots de (L), associe le mot $x * y$ (juxtaposé de x et y). On vérifie que cette opération est associative: $(x * y) * z$ et $x * (y * z)$ sont un seul et même mot de (L).

Soit, pour fixer les idées, l'alphabet:

$$A = \{0, 1, 2\}$$

et le lexique comprenant tous les assemblages qui ne commencent pas par 0, soit:

$$L = \{1, 2, 10, 11, 12, 20, 21, 22, 100, 101, \text{etc....}\}$$

le mot: $x = 21$, et le mot: $y = 100$, se composent pour donner le mot:

$$z = x * y = 21100$$

qui aurait aussi bien résulté de la composition des mots: 2 et 1100. Par contre le mot 2000 est indécomposable.

2. La définition suivante est donc naturelle: un monoïde est la structure algébrique définie par la donnée de:

1) un ensemble quelconque E,

2) une loi de composition interne associative (notée $*$) sur E, c'est-à-dire une application associant au couple (x, y) d'éléments de E l'unique élément $x * y \in E$, et telle que:

$$x * (y * z) = (x * y) * z$$

On démontre alors que dans la formule: $x_1 * x_2 * \ldots * x_n$ on peut disposer les parenthèses de n'importe quelle façon, l'élément obtenu est toujours le même, c'est le composé des n éléments x_i.

Un monoïde fini est un monoïde (E, $*$) tel que le cardinal de E soit fini.

Un élément $e \in E$ est dit neutre si:

$$x * e = e * x = x \qquad \text{pour tout } x \in E$$

Si E admet un élément neutre, il est unique car e' étant un autre élément neutre, on a:

$$e = e * e' = e'$$

La première égalité résultant de ce que e' est neutre, la seconde de ce que e est neutre.

Remarque: certains auteurs exigent, dans la définition d'un monoïde, l'existence d'un élément neutre. Il est toujours possible d'ajouter à un monoïde un élément e tel que e soit neutre. On supposera cette adjonction faite dans la suite.

Dans une réalisation concrète, l'élément neutre sera figuré (si l'on ose dire) par le"mot vide" c'est-à-dire par rien du tout.

Etant donné un monoïde, il peut être commode de chercher un ensemble de <u>générateurs</u>: c'est un ensemble d'éléments sélectionnés qui permettent de reconstruire tous les autres par composition.

Ainsi, pour la composition multiplicative, les nombres premiers permettent de construire tous les nombres entiers naturels.

Examinons, à titre d'exercice, le cas d'un seul générateur que nous appellerons g.

Les mots sont donc g, g * g, g * g * g, etc...

Il est commode d'abréger ces désignations en:

$$g,\ g^2,\ g^3,\ g^4,\ \text{etc....}$$

Si l'on admet que tous les éléments de cette suite sont distincts, on obtient alors un monoïde libre: il s'agit tout simplement de la suite des entiers naturels et du mécanisme de l'addition.

Mais on peut construire aussi des monoïdes non-libres en imposant quelques égalités. Voici deux exemples:

1°) $g^3 = g^2$, il en résulte $g^4 = g^3$ (en "multipliant" par g) d'où (transitivité de l'égalité): $g^4 = g^2$, d'où de la même façon $g^5 = g^3 = g^2$ et ainsi de suite. Ce qui montre qu'alors notre Monoïde ne comporte que <u>deux</u> éléments à savoir g et $g^2 = g^3 = g^4 =$ etc... que nous noterons h. Pour apprendre les règles de calcul dans ce monoïde, il suffit de retenir que

$$g*g = h*g = g*h = h*h = h$$

ou bien sous forme de Table (dite de Cayley, ou parfois de Pythagore);

*	g	h
g	h	h
h	h	h

ou encore donner des noms imagés:

g = "singulier"
h = "pluriel"

2°) $g^3 = g$; comme dans le précédent exemple, il est facile d'en déduire d'autres égalités:

$$g^4 = g^2,\ g^5 = g^3 = g,\ \text{etc...}$$

Ici encore deux éléments distincts seulement

$$g = g^3 = g^5 = g^7 = \ldots \quad \text{(impair)}$$
$$f = g^2 = g^4 = g^6 = \ldots \quad \text{(pair)}$$

et la loi de composition sous la forme de table:

$*$	g	f
g	f	g
f	g	f

ou si l'on préfère

$*$	pair	impair
pair	pair	imp.
impair	imp.	pair

L'élément f(pair) sera dit <u>neutre</u> car les composés:

$$f * x \quad \text{ou} \quad x * f$$

sont toujours identiques à x, quel que soit l'élément x.

L'élément g(impair) est dit <u>involutif</u> (ou encore: de périodicité égale à deux) parce que le composé par répétition:

$$g * g$$

donne l'élément neutre.

Il sera facile (exercice recommandé au lecteur) d'étudier par des méthodes toutes semblables, les trois petits monoïdes engendrés par g, seul générateur, et définis respectivement par:

1°) $g^4 = g$

2°) $g^4 = g^2$

3°) $g^4 = g^3$

On pourra aussi s'exercer aux cas (plus difficiles) de deux générateurs.

4. Un monoïde est <u>commutatif</u> si:

$x * y = y * x$ pour tous les couples (x, y) de E.

L'ordre dans lequel on effectue l'opération $*$ sur x et y est donc indifférent. On démontre que dans un monoïde commutatif on peut modifier l'ordre des éléments dans la formule $x_1 * x_2 * \ldots * x_n$ sans que change l'élément qu'elle désigne.

Un élément x est dit <u>involutif</u> si l'on a: $x * x = e$. Autrement dit, la composition de x à lui-même équivaut à rien.

Notons que l'élément neutre est toujours involutif.

<u>Prop.1</u> : un monoïde dont tous les éléments sont involutifs est nécessairement commutatif.

En effet $x * y$ étant un élément de E, il est involutif, et l'on peut écrire:

$$(x * y) * (x * y) = e \qquad (1)$$

Multiplions l'égalité (1) par y à droite. On a :

$$(x * y) * (x * y) * y = e * y$$

soit $$(x * y) * x * \underbrace{(y * y)}_{e} = y \qquad \text{(associativité de } *)$$

d'où $$(x * y) * x = y \qquad (2)$$

Multiplions (2) à droite par x:

$$(x * y) * \underbrace{(x * x)}_{e} = y * x$$

soit $x * y = y * x$, quels que soient x et y.

Désormais nous utiliserons, pour les monoïdes commutatifs et involutifs que nous voulons étudier, la notation + au lieu de * (comme il est de tradition) et 0 (zéro) au lieu de e. Ainsi $x * x = e$ s'écrira:

$$x + x = 0$$

Dans tout ce qui suit on se bornera aux monoïdes finis.

5. Nous allons engendrer les monoïdes étudiés par des familles finies, (les monoïdes en question l'étant aussi) de générateurs. On verra que le cardinal de G (nombre de ses éléments) détermine complètement E.

<u>card G = 1</u> : $G = \{0\}$. Le monoïde E_1 engendré ne contient que le zéro. Comme $0+0=0$, on a bien un monoïde.

<u>card G = 2</u> : $G = \{0, a\}$. Le monoïde engendré E_2 contient 0 et a.

De plus $$\begin{cases} 0 + a = a \\ a + a = 0 \\ 0 + 0 = 0 \end{cases}$$

Dressons la table d'addition qui détermine complètement E_2 :

+	0	a
0	0	a
a	a	0

Ce monoïde est très répandu. On l'a déjà rencontré plus haut (pair, impair). Pour en donner un autre exemple, considérons la "règle des signes": "plus par plus égale plus", "plus par moins égale moins" etc...

Dénotant "plus" par p, "moins" par m, "égale" par =, "par" par +, on obtient la table suivante:

+	p	m
p	p	m
m	m	p

On reconnait que c'est la table d'un monoïde qui ne diffère de E_2 que par la dénomination de ses éléments, p représentant 0 et m représentant a.

card G = 3 : soit G = $\{0, a, b\}$ $a \neq b$, on a

$$\begin{cases} a + 0 = 0 + a = a \\ b + 0 = 0 + b = b \end{cases}$$ et les 3 équations d'involution.

Reste à déterminer a + b. Cet élément ne peut être ni 0, ni a, ni b. En effet:

- si l'on avait a + b = 0, en ajoutant a aux deux membres, on trouverait:

$$\underbrace{a + a}_{0} + b = a \quad \text{d'où } b = a, \text{ ce qui n'est pas,}$$

- si a + b = a, on obtient en ajoutant a aux deux membres

$$\underbrace{a + a}_{0} + b = \underbrace{a + a}_{0} \quad \text{soit } b = 0, \text{ impossible.}$$

- si a + b = b, ajoutons b aux deux membres:

$$a + \underbrace{b + b}_{0} = \underbrace{b + b}_{0} \quad \text{soit } a = 0, \text{ impossible.}$$

Donc a + b est un nouvel élément c distinct de 0, de a et de b. Le monoïde E_4 engendré par G a quatre éléments. On construit facilement la table ci-dessous:

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$$\begin{cases} c + a = a + c = a + (a + b) = (a + a) + b = b \\ c + b = b + c = b + (a + b) = (b + b) + a = a \end{cases}$$

Dans cette dernière table on distingue les trois parties suivantes:

0	a
a	0

0	b
b	0

0	c
c	0

que l'on peut considérer comme les tables de Cayley (pour la même opération + que dans E_4) des monoïdes E_2 (a), E_2 (b), E_2 (c) engendrés respectivement par $\{0, a\}$, $\{0, b\}$, $\{0, c\}$.

Ces parties de E_4 contiennent donc le zéro $0 \in E_4$ et sont des monoïdes, c'est-à-dire contiennent x + y dès qu'elles contiennent x et y (l'opération + étant la même que dans E_4). Ce sont des sous-monoïdes de E_4. Un sous-monoïde d'un monoïde E est, de façon générale, un sous-ensemble F de E qui contient l'élément neutre de E et le composé, pour l'opération de E, de tout couple d'éléments de F.

On montre que dans un monoïde quelconque toute intersection non vide de sous-monoïdes est un sous-monoïde.

Revenons maintenant au monoïde E_4 et à sa table d'addition. Supposons que l'on confonde (par une sorte de daltonisme) les objets a et b d'une part, les objets 0 et c d'autre part. Autrement dit, on considère a et b comme <u>équivalents</u> à un même objet m, 0 et c comme <u>équivalents</u> à un même objet p. Remplaçons alors a et b par m et 0 et c par p dans la table qui devient:

+	p	m	m	p
p	p	m	m	p
m	m	p	p	m
m	m	p	p	m
p	p	m	m	p

Regroupons les éléments de façon à éliminer les répétitions. Il reste:

+	p	m
p	p	m
m	m	p

On reconnait là le monoïde de la règle des signes (p. 6), isomorphe à E_2. Le monoïde ainsi obtenu est dit <u>monoïde quotient de E_4</u>. On dira de façon générale qu'on a un monoïde quotient Q d'un monoïde E si on a partitionné E en un certain nombre de classes et si l'extension de la composition dans E aux classes de Q (le composé de deux classes étant la classe du composé de deux éléments quelconques des deux classes en question) munit Q d'une structure de monoïde. Autrement dit, si f est l'application qui à un élément x de E associe sa classe $f(x) \in Q$, le composé de f(x) et de f(y) est l'image par f du composé de x et de y :

$$f(x) * f(y) = f(x * y),$$

ou bien, en notation additive:

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

Une telle application est un <u>homomorphisme</u> du monoïde E dans le monoïde Q.

Puisque dans l'exemple de E_4 ci-dessus on a

$$f(a) = f(b) = m, \qquad f(0) = f(c) = p$$

et que

$$f(a + c) = f(b) = m = p + m = f(a) + f(c)$$

... etc...

on voit que l'application f qui à $x \in E$ associe sa classe $f(x) \in Q$ est un homomorphisme.

Lorsqu'un homomorphisme f est une bijection (tout f(x) provient d'un seul x, et tout élément de l'arrivée de f peut s'écrire sous la forme f(x)), on dit que f est un <u>isomorphisme</u>.

Ainsi les monoïdes dont les tables de Cayley suivent sont isomorphes:

+	0	a
0	0	a
a	a	0

+	p	m
p	p	m
m	m	p

L'isomorphisme f est donné par la table ci-dessous:

x	f(x)
0	p
a	m

On vérifie sans peine qu'on a bien un isomorphisme.

Nous allons maintenant reconstituer le monoïde E_4 à partir de deux exemplaires (isomorphes) du monoïde E_2. Autrement dit, on va se servir du "langage" E_2 pour expliciter E_4. Soient donc E'_2 et E''_2 les deux monoïdes isomorphes à E_2 dont les tables sont:

+	p	m	m	p
p	p	m	m	p
m	m	p	p	m
m	m	p	p	m
p	p	m	m	p

E'_2

+	q	q	n	n
q	q	q	n	n
q	q	q	n	n
n	n	n	q	q
n	n	n	q	q

E''_2

E'_2 est le monoïde quotient de E_4 obtenu en identifiant a et b à m, 0 et c à p. De même E''_2 est le monoïde quotient de E_4 obtenu en identifiant 0 et a à q, b et c à n. Superposons les tables de E'_2 et E''_2:

	p q	m q	m n	p n
p q	p q	m q	m n	p n
m q	m q	p q	p n	m n
m n	m n	p n	p q	m q
p n	p n	m n	m q	p q

On vérifie facilement que c'est la table du monoïde de E'_4 isomorphe à E_4 par l'application f donnée ci-dessous:

x	f(x)
0	p q
a	m q
b	m n
c	p n

Chaque élément de E'_4 est le "produit" (ou juxtaposé) de deux éléments, l'un appartenant à E'_2, l'autre à E''_2, et cela de façon unique. On dit que E'_4 est le produit direct de E'_2 et de E''_2.

Bien entendu il n'est pas nécessaire que les deux monoïdes quotient E'_2 et E''_2 soient distincts. Il suffira, si l'on prend un même monoïde quotient, de distinguer l'ordre des termes dans les éléments du produit direct.

Par exemple, supposons que E'_2 et E''_2 sont tous deux engendrés par $G = \{0, i\}$ mais que les identifications soient faites des deux manières distinctes suivantes:

	E'_2	E''_2
0	0	0
a	1	0
b	1	1
c	0	1

L'isomorphisme f entre E_4 et E'_4 sera donné par:

x	f(x)
0	0 0
a	1 0
b	1 1
c	0 1

On voit de quelle manière procéder: la première "coordonnée" d'un élément f(x) est l'élément auquel on identifie x pour obtenir E'_2; la deuxième "coordonnée" de f(x) est l'élément auquel on identifie x pour obtenir E''_2 (cf table ci-dessus).

7. Ce que nous venons de faire à l'aide de monoïdes - quotients peut également se faire avec des sous-monoïdes (et cela essentiellement à cause de l'isomorphisme entre monoïdes-quotients et sous-monoïdes de E_4): soient $E_2(a)$ et $E_2(b)$ les sous-monoïdes dont les tables sont respectivement:

0	a
a	0

et

0	b
b	0

Tout élément de E_4 pourra s'exprimer (de façon unique) comme "somme" de deux éléments, l'un appartenant à $E_2(a)$, l'autre à $E_2(b)$. C'est évident pour $0 = 0 + 0$, $a = a + 0$, $b = 0 + b$, mais encore pour $c = a + b$.

On dit que E_4 est somme directe de $E_2(a)$ et $E_2(b)$ ce que l'on note parfois $E_4 = E_2 \oplus E_2$.

Généralisation: On montre que tout monoïde involutif fini E possède 2^n éléments, (n étant le nombre des générateurs). Ce monoïde est le produit direct de n monoïdes-quotients isomorphes à E_2 et en même temps somme directe de n sous-monoïdes isomorphes à E_2.

Remarque: Le lecteur connaissant la théorie des groupes finis n'aura pas manqué de s'apercevoir que les monoïdes étudiés sont des groupes abéliens (de caractéristique 2) ce qui explique leur structure comme somme ou produit directs.