NOTE I

# Monoïdes

***Définition :***

(1) On appelle *monoïde* tout ensemble muni d'une loi de composition associative. Si M est un monoïde, et si on note $\times$ sa loi de composition, on a donc

$$[x, y \in \mathrm{M}] \Rightarrow [x \times y \in \mathrm{M}]$$
$$[x, y, z \in \mathrm{M}] \Rightarrow [x \times y] \times z = x \times [y \times z]$$

(2) Une partie M′ d'un monoïde est un *sous-monoïde* si

$$[x, y \in \mathrm{M}'] \Rightarrow [x \times y \in \mathrm{M}'].$$

Il est clair que la loi $\times$ induit alors une structure de monoïde sur M′.

— Un élément $e$ d'un monoïde M est dit *neutre* si

(3) $$[x \in \mathrm{M}] \Rightarrow [e \times x = x \times e = x]$$

⫰ Le nombre d'éléments neutres d'un monoïde est 0 ou 1.

(4) — Si $\mathrm{M}_0$ est un monoïde sans élément neutre, on peut ajouter à $\mathrm{M}_0$ un élément $e$, et prolonger l'opération $\times$ à l'ensemble $\mathrm{M} = \mathrm{M}_0 \cup \{e\}$ par la règle (3) ; ⫰ M est alors un monoïde, qui possède l'élément neutre $e$.

***Exemples de monoïdes :***

(5) — Les groupes, les recueils sont des monoïdes.

(6) — Soit E un ensemble ; on appellera *mot* de E tout symbole

$$x_1 x_2 \ldots x_n$$

dont les « lettres » $x_1, x_2, \ldots x_n$ sont des éléments de E (l'entier $n$ s'appelle *longueur* du mot) ; les mots de longueur 1 sont identifiés aux éléments correspondants de E.

On définit le produit de deux mots

$$m = x_1 x_2 \ldots x_n \quad \text{et} \quad m' = x'_1 x'_2 \ldots x'_{n'}$$

comme le mot

$$mm' = x_1 \ldots x_n x'_1 \ldots x'_{n'}$$

obtenu en écrivant les mots $m$ et $m'$ l'un au bout de l'autre.

ó L'ensemble M des mots de E est alors un monoïde ; on l'appelle *monoïde libre* engendré par E.

— Ce monoïde M n'admet pas d'élément neutre ; si on lui en ajoute un par la construction (4), on obtient le *monoïde libre avec élément neutre* engendré par E ; il est commode de considérer cet élément neutre comme le « mot de longueur nulle ».

## Homomorphismes de monoïdes.

Une application $f$ d'un monoïde M dans un monoïde M′ s'appelle un *homomorphisme* si elle vérifie

$$f(x \times y) = f(x) \times f(y)$$

(7) ó l'ensemble val $(f)$ est alors un sous-monoïde de M′ ; si M possède un élément neutre $e$, val $(f)$ possède un élément neutre $f(e)$ ; si M est un groupe, val $(f)$ est un groupe.

- Un homomorphisme régulier s'appelle un *isomorphisme* (de def $(f)$ sur val $(f)$) ; son inverse est alors un isomorphisme.



***Théorème :***

ó (8) Soit E un ensemble ; $\varphi$ une application de E dans un monoïde M′ ; M le monoïde libre engendré par E,

Il existe alors un seul prolongement $f$ de $\varphi$ qui soit un homomorphisme de M dans M′.

— On voit immédiatement que l'on a, pour tout mot $x_1 x_2 \ldots x_n$ :

(9) $$f(x_1 x_2 \ldots x_n) = \varphi(x_1) \times \varphi(x_2) \times \ldots \varphi(x_n).$$

## Noyaux.

***Théorème :***

Soit M un monoïde, $f$ un homomorphisme de M dans un monoïde M′ ; on appellera *noyau* de $f$ l'ensemble N des éléments $\begin{pmatrix} x \\ y \end{pmatrix}$ de M² tels que $f(x) = f(y)$ ; on a

ó (10) ♡
$$\left\{\begin{array}{lcl} [x \in \mathrm{M}] & \Rightarrow & \begin{pmatrix} x \\ x \end{pmatrix} \in \mathrm{N} \\ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{N} & \Rightarrow & \begin{pmatrix} y \\ x \end{pmatrix} \in \mathrm{N} \\ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{N},\ \begin{pmatrix} y \\ z \end{pmatrix} \in \mathrm{N} & \Rightarrow & \begin{pmatrix} x \\ z \end{pmatrix} \in \mathrm{N} \\ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{N},\ \begin{pmatrix} x' \\ y' \end{pmatrix} \in \mathrm{N} & \Rightarrow & \begin{pmatrix} x \times x' \\ y \times y' \end{pmatrix} \in \mathrm{N}. \end{array}\right.$$

(11) — Réciproquement, soit M un monoïde, N une partie de M² qui vérifie les propriétés (10, ♡) ; associons à chaque élément $x$ de M l'ensemble $f(x)$ défini par

$$[y \in f(x)] \Leftrightarrow \left[\begin{pmatrix} x \\ y \end{pmatrix} \in \mathrm{N}\right]$$

ó on peut alors définir, *d'une seule façon*, une opération associative X sur l'ensemble M′ = val $(f)$, de sorte que $f$ soit un homomorphisme de M sur M′ ayant N pour noyau ; M′ s'appelle *monoïde* *quotient* de M par N ; on pourra le noter M/N ; $f$ s'appelle *homomorphisme canonique* de M sur M/N.

— En utilisant le théorème (6.10), on établit le théorème :

(12) Soient M, $M_1$, $M_2$ trois monoïdes ; $f_1$ et $f_2$ des homomorphismes de L dans $M_1$ et $M_2$, de noyaux $N_1$ et $N_2$ respectivement. Alors :

$$[N_2 \subset N_1] \Leftrightarrow [f_1 \text{ est multiple de } f_2] \Rightarrow \begin{bmatrix} f_1/f_2 \text{ est un homorphisme de} \\ \text{val}\,(f_2) \text{ sur val}\,(f_1) \end{bmatrix}$$

(13) — Soit M un monoïde ; une partie N de $M^2$ s'appelle un noyau de M si elle est le noyau d'un homomorphisme, c'est-à-dire si elle vérifie les axiomes (10, ♡) ; ♂ toute intersection de noyaux est encore un noyau.

Soit donc K une partie quelconque de $M^2$ ; il existe des noyaux contenant K (par exemple $M^2$) ; leur intersection $N_K$ est encore un noyau ; c'est donc le plus petit noyau qui contienne K ; on l'appellera *noyau engendré* par K, Le monoïde quotient $M/N_K$ pourra aussi s'appeler quotient de M par K et se noter, sans ambiguïté, M/K.

— Par application de (12), ♂ on a le théorème :

(14) Soit M un monoïde ; $f$ un homomorphisme défini sur M ; K une partie de $M^2$ ; $f_K$ l'homomorphisme canonique de M sur M/K. Alors :

$[K \subset$ noyau de $f] \Leftrightarrow [$Il existe un homomorphisme $g$ tel que $f = g.f_K]$

***Exemple :***

(15) Soit E un ensemble ; A une application de E sur E, telle que $A^2 = 1_E$.

Soit M le monoïde libre avec élément unité $1\!\!1_M$ engendré par E ; K l'ensemble des couples $\begin{bmatrix} 1\!\!1_M \\ xA(x) \end{bmatrix}$ $[x \in E]$ ; ♂ le monoïde quotient M/K est un *groupe ;* on l'appelle *groupe libre* lorsque il n'y a pas de point $x$ tel que $x = A(x)$. On peut montrer que tout groupe est isomorphe à un quotient d'un groupe libre.