BULLETIN DE LA S. M. F.

D. PONASSE

Anneaux monadiques rationnels

Bulletin de la S. M. F., tome 99 (1971), p. 143-170

<http://www.numdam.org/item?id=BSMF_1971__99__143_0>

Bull. Soc. math. France,
99, 1971, p. 143 à 170.

ANNEAUX MONADIQUES RATIONNELS

PAR

DANIEL PONASSE

[Yaoundé, Cameroun.]

0. Introduction.

Précisons tout d'abord les notations utilisées pour un anneau booléien A; si p, q sont des éléments de A, les opérations habituelles seront notées : pq (produit, ou conjonction, ou borne inférieure), $p \vee q$ (disjonction, ou borne supérieure), $\neg p$ (négation, ou complément), $p + q$ (somme, ou différence symétrique, ou disjonction exclusive). La relation d'ordre $p \leq q$ s'exprime par $pq = p$ (ou de façon équivalente, $p \vee q = q$). On rappelle les formules usuelles :

$$\neg p = p + 1, \qquad p \vee q = p + q + pq,$$
$$p + q = (p . \neg q) \vee (\neg p . q) = (p \vee q) . (\neg p \vee \neg q).$$

Une *algèbre monadique* [3] est une structure $(A, \exists)$ définie par la donnée d'un anneau booléien A et d'un opérateur $\exists$ (quantificateur existentiel) vérifiant les trois axiomes :

$$\exists\, 0 = 0, \qquad p \leq \exists\, p, \qquad \exists\,(p . \exists\, q) = \exists\, p . \exists\, q.$$

On sait que l'ensemble $B = \exists(A)$ est alors un sous-anneau booléien de A, il sera appelé la *charpente* de A.

Soit A un anneau booléien, et soit G une partie quelconque de A, on appellera *monôme booléien* en G tout élément de A qui est, soit égal à 1, soit égal à un produit fini $g_1 . g_2, \ldots, g_n$ d'éléments de G. Un *polynôme booléien* en G sera toute somme finie de monômes booléiens en G. En pratique, un polynôme booléien sera écrit à l'aide de coefficients

appartenant au sous-anneau $\mathbf{U} = \{0, 1\}$, par exemple un polynôme booléien en p, q a pour forme générale $ap + bq + cpq + d$, où $a, b, c, d \in \mathbf{U}$. Notons que l'ensemble des polynômes booléiens en G n'est autre que le sous-anneau booléien A_G de A engendré par G.

D'une façon analogue, dans un anneau monadique A, nous définirons un *polynôme monadique* en G comme étant un polynôme booléien en $G \cup \exists(G) \cup \forall(G)$ [l'opérateur $\forall$ est défini par $\forall p = \neg \exists (\neg p)$]. Par exemple, un polynôme monadique en p, en tenant compte des inégalités $\forall p \leq p \leq \exists p$, aura comme forme générale :

$$ap + b \exists p + c \forall p + d, \qquad \text{avec} \quad a, b, c, d \in \mathbf{U},$$

et un polynôme monadique en p, q sera du type :

$$\alpha q + \beta \exists q + \gamma \forall q + \delta,$$

où α, β, γ, δ sont des polynômes monadiques en p (ce qui donne *a priori* 2^{16} polynômes monadiques en p, q).

Le problème initial que nous avons envisagé est le suivant : dans tout anneau monadique on peut exprimer, sous forme de polynômes monadiques, les quantités

$$\exists(\neg p) = \forall p + 1 \qquad \text{et} \qquad \exists(p \vee q) = \exists p \vee \exists q,$$

par contre, il n'en est pas de même en général de $\exists(pq)$. Nous avons pu caractériser de façon très simple les anneaux où $\exists(pq)$ s'exprime « rationnellement » (c'est-à-dire sous forme d'un polynôme monadique en p, q), et il se trouve que cette étude est étroitement liée à celle des automorphismes involutifs d'un anneau booléien. On verra également que l'on peut obtenir des renseignements intéressants en ce qui concerne les constantes et la richesse de tels anneaux « rationnels ».

Avant d'aborder la notion de rationalité d'un anneau monadique, nous étudierons, dans les deux premiers paragraphes, d'une part la construction d'un certain type d'algèbres monadiques définies par un anneau booléien et un idéal quelconques, d'autre part les propriétés générales de certains opérateurs monadiques. Le plan adopté est le suivant :

1. Anneaux monadiques $B[\Gamma]$;
2. Opérateurs monadiques m et γ et notion de centre monadique;
3. Caractérisation des anneaux monadiques rationnels;
4. Constantes et richesse des anneaux monadiques rationnels;
5. Généralisation : notion de dimension monadique.

1. Anneaux monadiques $B[\Gamma]$.

Soient B un anneau booléien quelconque, et Γ un idéal booléien quelconque de B.

Définissons sur l'ensemble produit $B\times\Gamma$ deux lois de composition (addition et multiplication) par

$$(p, q) + (p', q') = (p + p', q + q'),$$
$$(p, q).(p', q') = (pp', pq' + p'q + qq').$$

On vérifie sans peine (il suffit d'écrire) que ces opérations définissent une structure d'anneau booléien que nous désignerons dans toute la suite par $B[\Gamma]$.

Les éléments neutres sont

(o, o) pour l'addition,
(1, o) pour la multiplication.

La négation est définie par

$$\neg(p, q) = (\neg p, q)$$

et la disjonction par

$$(p, q)\vee(p', q') = (p\vee p', q\vee q' + pq' + p'q).$$

On peut immerger l'anneau booléien B dans $B[\Gamma]$; en effet, l'application $f: B\rightarrowtail B[\Gamma]$ définie par $f(p) = (p, o)$ est un monomorphisme booléien :

f est évidemment injective,
$f(p + p') = (p + p', o) = (p, o) + (p', o) = f(p) + f(p')$,
$f(pp') = (pp', o) = (p, o).(p', o) = f(p).f(p')$.

On pourra donc identifier B à un sous-anneau booléien de $B[\Gamma]$ en identifiant p à (p, o).

1.1. Cas particulier.

Supposons que Γ soit un idéal principal : $\Gamma = \theta B (\theta\in B)$.
Si $q\in\Gamma$: $q\leq\theta$, donc

$$(o, \theta).(q, o) = (o, q\theta) = (o, q),$$

donc tout élément (p, q) de $B[\Gamma]$ se décompose sous la forme

$$(p, q) = (p, o) + (o, q) = (p, o) + (o, \theta).(q, o),$$

soit, en posant $\zeta = (o, \theta)$ et en utilisant l'identification précédente,

$$(p, q) = p + \zeta q,$$

et cette décomposition est évidemment unique. On a donc, dans ce cas particulier,

$$B[\Gamma] = B \oplus \zeta\Gamma.$$

Comme cas extrêmes, nous aurons

$B[o] = B$,

$B[B] = B \oplus \zeta B$, avec $\zeta = (o, 1)$, c'est-à-dire l'anneau des polynômes booléiens à une indéterminée ζ et à coefficients dans B.

1.2. **Structure monadique sur** $B[\Gamma]$.

Γ est ici un idéal quelconque, définissons l'opérateur $\exists$ par

$$\exists (p, q) = (p \vee q, o) = p \vee q.$$

$\exists$ est un quantificateur monadique existentiel, en effet :

$\exists (o, o) = (o, o)$,

$(p, q) \leq \exists (p, q)$, car

$(p, q).(p \vee q, o) = (p.(p \vee q), q.(p \vee q)) = (p, q)$,

$\exists ((p, q).\exists (p', q')) = \exists (p, q).\exists (p', q')$, car

$$(p, q).\exists (p', q') = (p.(p' \vee q'), q.(p' \vee q')),$$

$$\exists ((p, q).\exists (p', q')) = (p.(p' \vee q')) \vee (q.(p' \vee q')) = (p \vee q).(p' \vee q').$$

Lorsque nous parlerons de l'anneau monadique $B[\Gamma]$, il s'agira toujours de la structure ainsi définie.

Le quantificateur universel associé est

$$\forall (p, q) = \neg \exists (\neg p, q) = \neg p.q.$$

La charpente de $B[\Gamma]$ n'est autre que l'anneau booléien B, car $\exists (p, q) \in B$, et pour tout $p \in B$, $\exists (p, o) = (p, o) = p$.

1.3. **Richesse des anneaux** $B[\Gamma]$.

Rappelons qu'une *constante* d'un anneau monadique est tout endomorphisme c tel que $c\,\exists = \exists$ et $\exists\, c = c$, l'anneau est dit *riche* si, pour tout élément p, il existe une constante c (dite témoin de p) telle que $\exists\, p = cp$.

Pour un anneau $B[\Gamma]$, on peut associer à chaque $\lambda \in B$ une constante c_λ définie par

$$c_\lambda(p, q) = (p + \lambda q, o) = p + \lambda q;$$

en effet, on vérifie :

c_λ est un endomorphisme :

$$\begin{aligned} c_\lambda((p, q)(p', q')) &= c_\lambda(pp', qq' + pq' + p'q) = pp' + \lambda(qq' + pq' + p'q) \\ &= (p + \lambda q)(p' + \lambda q') = c_\lambda(p, q) + c_\lambda(p', q'), \end{aligned}$$

$$c_\lambda((p, q) + (p', q')) = (p + p') + \lambda(q + q') = c_\lambda(p, q) + c_\lambda(p', q'),$$

$$c_\lambda \exists (p, q) = c_\lambda(p \vee q, o) = (p \vee q, o) = \exists (p, q),$$

$$\exists\, c_\lambda(p, q) = \exists (p + \lambda q, o) = (p + \lambda q, o) = c_\lambda(p, q).$$

Tout élément (p, q) possède un témoin; en effet, il suffit de déterminer λ de telle sorte que

$$\exists (p, q) = c_\lambda(p, q),$$

soit $p \vee q = p + \lambda q$, d'où $\lambda q = q + pq$.

Il suffit alors de prendre, par exemple, $\lambda = p + 1$. Ainsi tout anneau $B[\Gamma]$ est riche.

1.4. **Cas particulier.**

Revenons au cas où Γ est un idéal principal engendré par θ, dans ce cas : $B[\Gamma] = B \oplus \zeta\Gamma$; un homomorphisme booléien f de $B[\Gamma]$ dans B est donc entièrement caractérisé par :

— sa restriction f' à B;

— la valeur $f(\zeta) = \lambda$

et on a alors : $f(p, q) = f'(p) + \lambda f'(q)$, λ pouvant être choisie arbitrairement dans B, et f' étant un endomorphisme quelconque de B.

Pour qu'une telle application f soit une constante, il est alors nécessaire et suffisant que f' soit l'identité de B. Donc, dans ce cas particulier, on obtient toutes les constantes de $B[\Gamma]$ par la formule

$$c_\lambda(p, q) = p + \lambda q, \qquad \lambda \in B.$$

En outre, chacune de ces constantes a un noyau principal (nous dirons que c'est une *constante principale*) en effet : soit $(p, q) \in \ker(c_\lambda) : p = \lambda q$,

$$(p, q) = (\lambda q, q) = (\lambda\theta q, \theta q) \qquad (q \in \Gamma, \text{ donc } \theta q = q),$$
$$(p, q) = q(\lambda\theta, \theta),$$

donc $(p, q) \leq (\lambda\theta, \theta)$, et on a bien $c_\lambda(\lambda\theta, \theta) = \lambda\theta + \lambda\theta = 0$.

Donc $\ker(c_\lambda)$ est l'idéal principal engendré par $(\lambda\theta, \theta)$.

1.5. Remarque.

Nous démontrerons plus loin (dans un cadre plus général) la réciproque suivante :

Si un anneau $B[\Gamma]$ a au moins une constante principale, alors Γ est un idéal principal.

2. Sur certains opérateurs monadiques.

Nous considérons dans ce paragraphe une algèbre monadique $(A, \exists)$ absolument quelconque, nous désignerons toujours par B sa charpente.

2.1. Fonction moyenne.

Un anneau booléien peut être considéré comme un treillis distributif complémenté, on sait qu'il est alors relativement complémenté, avec unicité du complément relatif [1].

Soit $p \in A$, on a $\forall p \leq p \leq \exists p$, donc p possède un complément relatif q dans l'intervalle $[\forall p, \exists p]$; q est défini par

$$\begin{cases} p.q = \forall p, \\ p \vee q = \exists p. \end{cases}$$

Le calcul de q est simple : $pq + p \vee q = \exists p + \forall p$,

soit $p + q = \exists p + \forall p$,

d'où $q = p + \exists p + \forall p$.

Nous définirons alors la fonction moyenne m de l'anneau monadique $(A, \exists)$ par $mp = p + \exists p + \forall p$.

Cette fonction m permet donc de définir les deux quantificateurs par les formules

$$\exists p = p \vee mp \qquad \text{et} \qquad \forall p = p.mp.$$

2.2. Propriétés de la fonction moyenne.

On a, par un calcul simple,

$$mp = (\neg p . \exists p) \vee \forall p = (\neg p \vee \forall p)\ \exists p,$$
$$\exists m = m \exists = \exists \qquad \text{et} \qquad \forall m = m \forall = \forall,$$

car

$$\exists mp = \exists (\neg p . \exists p) \vee \exists \forall p$$
$$= (\exists (\neg p)\ \exists p) \vee \forall p = (\neg \forall p . \exists p) \vee \forall p = \exists p \vee \forall p = \exists p,$$
$$m \exists p = \exists p + \exists \exists p + \forall \exists p = \exists p + \exists p + \exists p = \exists p,$$

de même pour $\forall$.

$p \in B \Leftrightarrow mp = p$, car

$$p \in B \Leftrightarrow \exists p = \forall p,$$

$m(\neg p) = \neg mp$, car

$$m(\neg p) = \neg p + \exists (\neg p) + \forall (\neg p)$$
$$= \neg p + \neg \forall p + \neg \exists p = \neg (p + \exists p + \forall p),$$

$mmp = p$, car

$$mmp = mp + \exists mp + \forall mp = mp + \exists p + \forall p = p.$$

La fonction moyenne est donc *involutive*, c'est donc notamment une bijection de A sur lui-même.

— Si A' est un sous-anneau monadique de A, la fonction moyenne m' de A' est la restriction de m à A'.

— Si I est un idéal monadique de A et $(\overline{A}, \overline{\exists})$ l'anneau monadique quotient de A par I, la fonction moyenne $\overline{m}$ de $\overline{A}$ est définie par $\overline{m}\,\overline{p} = \overline{mp}$, où p est un représentant quelconque de la classe $\overline{p}$.

En effet, si $p \equiv q\ (I)$, on sait que $\exists p \equiv \exists q\ (I)$ et $\forall p \equiv \forall q\ (I)$, d'où $mp \equiv mq\ (I)$,
on peut donc passer au quotient.

— Si $(A, \exists)$ est l'anneau monadique produit d'une famille $(A_i, \exists_i)$, en désignant par m_i la fonction moyenne de chaque A_i, la fonction moyenne m de A est alors définie par

$$m((p_i)) = (m_i p_i).$$

— Soient $(A, \exists)$ et $(A', \exists')$ deux anneaux monadiques de fonctions moyennes respectives m et m', et soit f un homomorphisme monadique de A dans A', alors, pour tout $p \in A$,

$$f(mp) = m' f(p).$$

2.3. **Fonction centrale.**

Nous définirons un autre opérateur monadique, très proche de la fonction moyenne, qui sera appelé fonction centrale, et défini par

$$\begin{aligned} \gamma p &= \exists p + \forall p \\ &= p + mp. \end{aligned}$$

Notons que γ est en fait une application de A dans sa charpente B.

On vérifie immédiatement

$$\gamma p = \neg \forall p . \exists p = \exists p . \exists (\neg p) = \exists (p + \exists p) = \exists (p + \forall p).$$

On appellera *centre monadique* de A le sous-ensemble de B : $\Gamma = \gamma(A)$. On peut remarquer que

$$\Gamma = \exists \forall^{-1}((o)),$$

$$\text{car } \gamma p = \exists (p . \neg \forall p), \text{ avec } \forall (p . \neg \forall p) = o.$$

2.4. **Exemple.**

Considérons un anneau monadique $B[\Gamma]$ étudié précédemment

$$\exists (p, q) = (p \vee q, o) = (p + q + pq, o),$$
$$\forall (p, q) = (p . \neg q, o) = (pq + p, o),$$

d'où $\gamma(p, q) = (q, o) = q$ (avec la convention d'identification).

Le centre monadique est donc précisément l'idéal Γ de B.

La fonction moyenne est ici définie par $m(p, q) = (p + q, q)$.

2.5. **Propriétés de la fonction centrale et du centre monadique.**

$p \in B \Leftrightarrow \gamma p = o$,

$\gamma(\neg p) = \gamma p$,

$\gamma(bp) = b \gamma p$ pour tout $b \in B$, car

$$\exists (bp) = b \exists p \qquad \text{et} \qquad \forall (bp) = b \forall p,$$

$\gamma(b + p) = \gamma p$ pour tout $b \in B$.

En effet :

$$\begin{aligned}\exists(b+p) = \exists(b.\neg p)\vee\exists(\neg b.p) &= (b.\exists(\neg p))\vee(\neg b.\exists p)\\ &= b.\exists(\neg p)+\neg b.\exists p\\ &= b.\neg\forall p+\neg b.\exists p,\\ \forall(b+p) = \forall(b\vee p).\forall(\neg b\vee\neg p) &= (b\vee\forall p).(\neg b\vee\forall(\neg p))\\ &= (b.\forall(\neg p))\vee(\neg b.\forall p)\\ &= b.\forall(\neg p)+\neg b.\forall p\\ &= b.\neg\exists p+\neg b.\forall p\end{aligned}$$

d'où $\gamma(b+p) = b.\gamma p+\neg b.\gamma p = \gamma p$.

Le centre monadique Γ est toujours un *idéal* (éventuellement impropre) de B.

En effet :

— si $b\in\Gamma$ et $b'\in B$: $b = \gamma p$,

$$b'b = b'\gamma p = \gamma(b'p)\in\Gamma;$$

— si $b\in\Gamma$ et $b'\in\Gamma$: $b = \exists p$, avec $\forall p = 0$,

$$b' = \exists q, \quad \text{avec} \quad \forall q = 0;$$

posons alors

$$r = (\neg p.\exists p.\neg\exists q)\vee(\neg q.\exists q.\neg\exists p),$$

on a

$$\exists r = (\exists(\neg p).\exists p.\neg\exists q)\vee(\exists(\neg q).\exists q.\neg\exists p)$$

or $\exists(\neg p) = \neg\forall p = 1$, $\exists(\neg q) = \neg\forall q = 1$,

$$\begin{aligned}\exists r &= (\exists p.\neg\exists q)\vee(\exists q.\neg\exists p)\\ &= \exists p+\exists q = b+b'.\end{aligned}$$

Par ailleurs :

$$\begin{aligned}r &\leq (\exists(\neg p).\exists p.\neg\exists q)\vee(\neg q.\exists q.\neg\exists p)\\ &= (\exists p.\neg\exists q)\vee(\neg q.\exists q.\neg\exists p),\end{aligned}$$

donc

$$\forall r\leq(\exists p.\neg\exists q)\vee(\forall(\neg q).\exists q.\neg\exists p) = \exists p.\neg\exists q,$$

et, de même,

$$\begin{aligned}r &\leq (\neg p.\exists p.\neg\exists q)\vee(\exists(\neg q).\exists q.\neg\exists p)\\ &= (\neg p.\exists p.\neg\exists q)\vee(\exists q.\neg\exists p),\end{aligned}$$

donc

$$\forall r\leq(\forall(\neg p).\exists p.\neg\exists q)\vee(\exists q.\neg\exists p) = \exists q.\neg\exists p,$$

par suite :

$$\forall r \leq (\exists p . \neg \exists q) . (\exists q . \neg \exists p),$$

donc $\forall r = 0$ et $b + b' = \exists r$, donc $b + b' \in \Gamma$.

2.6. Application de γ à l'étude des constantes.

Rappelons les résultats suivants ([3], [4]) pour un anneau monadique quelconque :

— Une constante c est entièrement caractérisée par son noyau I (idéal de A), plus précisément, pour qu'un idéal I soit un noyau de constante, il faut et il suffit que $A = B \oplus I$, la constante c associée à I est alors la projection sur B.

— Un noyau de constante principale est ainsi caractérisé : $I = A . \neg \varpi$, où ϖ est un élément minimal de $\exists^{-1}(1)$, ou, ce qui revient au même,

$$\begin{cases} \exists \varpi = 1 \\ \exists (p . \varpi) . \exists (\neg p . \varpi) = 0 \quad \text{pour tout } p \in A. \end{cases}$$

Un tel élément ϖ sera dit un *élément principal* (appelé aussi « partition monadique » dans [4]). La constante principale associée est définie par

$$cp = \exists (p . \varpi) \quad \text{(cette constante } c \text{ est l'unique témoin de } \varpi).$$

— Nous introduirons également la notion d'*élément singulier* : tout élément $s \in A$ tel que $\exists s = 1$ et $\forall s = 0$.

Remarque. — Dans l'algébrisation du calcul des prédicats classique [5], il n'y a aucun élément singulier. Cela est dû à la non-complétude syntaxique, c'est-à-dire au fait que tout énoncé du type $\exists x [f^x] \to \forall x [f^x]$ est compatible.

Dans un anneau monadique simple, tout élément différent de 0 et de 1 est singulier.

Un élément singulier peut être défini de différentes façons équivalentes :

$$\exists s = \exists (\neg s), \qquad \text{car alors} \quad \exists s = \exists s \vee \exists (\neg s) = 1,$$
$$\text{ou} \qquad ms = \neg s, \qquad \text{ou} \qquad \gamma s = 1,$$

ce qui montre que si s est singulier, tout élément $s + b$ avec $b \in B$ est également singulier. En outre, puisque le centre monadique est $\Gamma = \gamma(A)$, on a la caractérisation suivante :

$$\text{(il existe des éléments singuliers)} \iff (\Gamma = B).$$

On obtient alors les résultats suivants :

PROPOSITION 2.6.1. — *Si c est une constante, alors* $\Gamma = \exists(\ker(c))$.

En effet, soit $I = \ker(c)$, $A = B \oplus I$,

— si $q \in \Gamma : q = \gamma p$, $p = b + i$, avec $b \in B$ et $i \in I$,
donc :

$$q = \gamma i = \exists i, \qquad \text{car} \quad \forall i \leq ci = o,$$

— si $q = \exists i$, avec $i \in I$, $q \in \Gamma$, car $\forall i = o$.

COROLLAIRE 1. — *Si A possède au moins une constante principale, alors Γ est un idéal principal de B. En outre, pour tout élément principal, la quantité $\forall \varpi$ est invariante, et $\neg \forall \varpi$ est le générateur de Γ.*

En effet, si $q \in \Gamma : q = \exists i$,

$$i \in \ker(c), \quad \text{soit } \varpi \text{ l'élément principal associé à } c : i \leq \neg \varpi,$$

donc $q \leq \exists(\neg \varpi) = \neg \forall \varpi$.

COROLLAIRE 2. — *Si A possède au moins un élément singulier, alors tout élément principal est singulier.*

Car $\Gamma = B$, donc $\neg \forall \varpi = 1$, soit $\forall \varpi = o$.

Remarque. — Il peut exister des éléments singuliers sans qu'il y ait des éléments principaux (exemple : anneau monadique simple sans atome).

On est alors conduit à généraliser la notion d'élément singulier, en considérant le cas où le centre monadique Γ serait un idéal principal quelconque (au lieu de $\Gamma = B$). Dans ce cas, soit $t \in A$ tel que γt engendre Γ. Pour tout $b \in B$, on a

$$\gamma(b + t) = \gamma t,$$

or

$$\exists(b + t) = \neg b . \exists t + b . \neg \forall t = b(\exists t + \forall t + 1) + \exists t,$$

on peut donc toujours déterminer b de telle sorte que $\exists(b + t) = 1$, en prenant par exemple : $b = \exists t + 1 + t$.

Ceci nous conduit à poser la définition suivante : on appellera *élément quasi-singulier*, tout élément t tel que

$$\begin{cases} \exists t = 1, \\ \gamma t \text{ engendre } \Gamma, \text{ i. e. : } \gamma p \leq \gamma t \text{ pour tout } p \in A. \end{cases}$$

L'existence de tels éléments équivaut donc au fait que Γ est principal.

PROPOSITION 2.6.2. — *Tout élément principal est un élément quasi-singulier.*

En effet, si ϖ est un élément principal, Γ est l'idéal principal engendré par

$$\neg \forall \varpi = \forall \varpi + 1 = \gamma \varpi,$$

donc ϖ est quasi-singulier.

3. **Anneaux monadiques rationnels.**

Revenons au problème posé en introduction, nous définirons alors :

— *Quantificateur rationnel :* si la fonction de deux variables $\exists(pq)$ est un polynôme monadique en p, q, c'est-à-dire

$$\exists(pq) = \alpha q + \beta \exists q + \gamma \forall q + \delta,$$

où α, β, γ, δ sont des polynômes monadiques en p, donc du type

$$\alpha = ap + b \exists p + c \forall p + d, \qquad \ldots,$$

les 16 coefficients a, b, c, d, ... étant des éléments de $\mathbf{U} = \{ 0, 1 \}$ (indépendants de p et q).

— *Anneau monadique rationnel* $(A, \exists)$: si le quantificateur $\exists$ est rationnel.

Un exemple trivial d'anneaux monadiques rationnels est celui des anneaux monadiques discrets ($\exists p = p$).

Nous verrons qu'il est possible de caractériser de façon simple les anneaux monadiques rationnels, et qu'il existe un procédé permettant de les construire tous.

Lemme 3.0. — *On suppose que $\exists$ n'est pas le quantificateur discret. Soient a, b, c, d, a', b', c', $d' \in \mathbf{U}$. Si*

$$ap + b \exists p + c \forall p + d = a'p + b' \exists p + c' \forall p + d' \quad \textit{pour tout } p \in A,$$

alors

$$a = a', \qquad b = b', \qquad c = c' \qquad d = d'.$$

En effet, on peut se ramener à l'égalité

$$ap + b \exists p + c \forall p + d = 0 \quad \text{pour tout } p;$$

— pour $p = 0$, on obtient $d = 0$;

— pour $p = 1$, on obtient $a + b + c = 0$;

— en remplaçant p par $\neg p = p + 1$, avec

$$\exists(\neg p) = \forall p + 1 \qquad \text{et} \qquad \forall(\neg p) = \exists p + 1,$$

on obtient alors

$$ap + b\,\forall p + c\,\exists p = 0.$$

D'où

$$(b+c)(\exists p + \forall p) = 0 \quad \text{pour tout } p,$$

soit

$$\exists p + \forall p \leq \neg(b+c).$$

$\neg(b+c) \in \mathbf{U}$, si $\neg(b+c) = 0 : \exists p = \forall p$, le quantificateur serait discret.

Donc $\neg(b+c) = 1$, soit $b = c$; par suite, $a = 0$.

Alors $b(\exists p + \forall p) = 0$ pour tout p, donc comme précédemment, $b = 0$. On a donc bien $a = b = c = d = 0$.

THÉORÈME 3.1. — *Si* $\exists$ *est un quantificateur* rationnel, *alors quels que soient* p *et* q,

$$\exists(pq) = (\exists p + \forall p)q + (p + \exists p + \forall p)\exists q + (p + \exists p)\forall q.$$

Démonstration. — Si $\exists$ est le quantificateur discret, on vérifie trivialement cette formule.

On suppose donc que $\exists$ n'est pas discret.

$$\exists(pq) = \alpha q + \beta\exists q + \gamma\forall q + \delta, \tag{1}$$

où α, β, γ, δ sont eux-mêmes des polynômes monadiques en p.

— Pour $q = 0$, on obtient $\delta = 0$ pour tout p, donc tous les coefficients de δ sont nuls.

— Pour $q = 1$, on obtient $\alpha + \beta + \gamma = \exists p$, pour tout p.

— Pour $q = \neg p$, on obtient alors

$$\alpha p + \beta\forall p + \gamma\exists p = \exists p. \tag{2}$$

— Et pour $q = p$:

$$\alpha p + \beta\exists p + \gamma\forall p = \exists p. \tag{3}$$

En multipliant (2) et (3) par p

$$\alpha p + \beta\forall p + \gamma p = p, \tag{4}$$

$$\alpha p + \beta p + \gamma\forall p = p. \tag{5}$$

Or $p = p.\exists p = p(\alpha + \beta + \gamma)$, de (4) on tire alors

$$\beta\forall p = \beta p$$

et de (5)

$$\gamma \forall p = \gamma p;$$

β et γ sont des polynômes monadiques en p, posons

$$\left.\begin{aligned} \beta &= ap + b \exists p + c \forall p + d \\ \gamma &= a'p + b' \exists p + c' \forall p + d' \end{aligned}\right\} \text{ les coefficients étant dans } \mathbf{U},$$

alors

$$\alpha = \beta + \gamma + \exists p = (a + a')p + (b + b' + 1) \exists p + (c + c') \forall p + d + d'$$

Pour $p = 0$ dans (1) (avec $\delta = 0$) :

$$(d + d')q + d \exists q + d' \forall q = 0 \quad \text{pour tout } q,$$

donc, d'après le lemme : $d = d' = 0$.

Pour $p = 1$ dans (1) :

$$\begin{aligned} \exists q = {} & (a + b + c + a' + b' + c' + 1)q \\ & + (a + b + c)q + (a' + b' + c') \forall q \quad \text{pour tout } q. \end{aligned}$$

Donc, d'après le lemme :

$$\left\{\begin{aligned} a' + b' + c' &= 0, \\ a + b + c &= 1, \end{aligned}\right.$$

$$\beta \forall p = \beta p, \quad \text{soit} \quad a \forall p + b \forall p + c \forall p = ap + bp + c \forall p,$$

$$\gamma \forall p = \gamma p, \quad \text{soit} \quad a' \forall p + b' \forall p + c' \forall p = a'p + b'p + c' \forall p,$$

donc, d'après le lemme :

$$\begin{aligned} a + b &= 0, \\ a' + b' &= 0, \end{aligned}$$

d'où $a = b$, $c = 1$, $a' = b'$, $c' = 0$.

Ainsi :

$$\left\{\begin{aligned} \beta &= ap + a \exists p + \forall p, \\ \gamma &= a'p + a' \exists p, \\ \alpha &= (a + a')p + (a + a' + 1) \exists p + \forall p. \end{aligned}\right.$$

On peut alors écrire (1) sous la forme :

$$\exists (pq) = \alpha' p + \beta' \exists p + \gamma' \forall p,$$

avec

$$\left\{\begin{aligned} \alpha' &= (a + a')q + a \exists q + a' \forall q, \\ \beta' &= (a + a' + 1)q + a \exists q + a' \forall q, \\ \gamma' &= q + \exists q. \end{aligned}\right.$$

En utilisant la formule symétrique

$$\beta' \forall q = \beta' q.$$

Soit

$$(a + a' + 1) \forall q + a \forall q + a' \forall q = (a + a' + 1) q + aq + a' \forall q,$$

on obtient : $a' = 1$.

Enfin, en ajoutant (2) et (3) :

$$(\beta + \gamma)(\exists p + \forall p) = 0,$$

soit $(a + 1) p + (a + 1) \exists p = 0$, d'où $a = 1$.

Finalement :

$$\begin{cases} \alpha = \exists p + \forall p, \\ \beta = p + \exists p + p, \\ \gamma = p + \exists p. \end{cases}$$

Remarques :

1° Dans un anneau monadique rationnel, si $f(p_1, \ldots, p_n)$ est un polynôme booléien (ou un polynôme monadique), alors $\exists f(p_1, \ldots, p_n)$ et $\forall f(p_1, \ldots, p_n)$ sont des polynômes monadiques.

Ceci se démontre par une récurrence simple à partir du formulaire suivant :

$$\exists (\neg p) = \forall p + 1,$$

$$\exists (p \vee q) = \exists p \vee \exists q,$$

$$\exists (pq) = \exists p \ \exists q + p \exists q + q \exists p + p \exists q + q \forall p + \exists p \forall q + \exists q \forall p,$$

$$\exists (p + q) = \exists p + \exists q + p \exists q + q \exists p + p \forall q + q \forall p$$

[on utilise la formule : $p + q = (p \ \neg q) \vee (q \ \neg p)$]

$$\forall (\neg p) = \exists p + 1,$$

$$\forall (pq) = \forall p \ \forall q,$$

$$\forall (p \vee q) = \forall p \vee \forall q + p \forall q + q \forall p + p \exists q + q \exists p + \forall p \exists q + \forall q \exists p,$$

$$\forall (p + q) = \forall p + \forall q + p \exists q + q \exists p + p \forall q + q \forall p.$$

2° Si $(A, \exists)$ est un anneau monadique rationnel, et si G est une partie quelconque de A, alors le sous-anneau monadique M_G engendré par G n'est autre que l'ensemble des polynômes monadiques en G.

Ceci résulte de la remarque précédente.

THÉORÈME 3.2. — *Soit* $(A, \exists)$ *un anneau monadique, de fonction moyenne* m *et de fonction centrale* γ. *Les assertions suivantes sont équivalentes :*

1° $\exists$ *est un quantificateur rationnel,*

2° m *est multiplicative,*

3° m *est un automorphisme (involutif) de* A,

4° m *est croissante,*

5° γ *est additive,*

6° γ *est une application linéaire du* B*-module* A *dans* B.

Démonstration. — Pour l'équivalence entre 1° et 2°, il suffit de remarquer que la formule du théorème 3.1 s'écrit

$$\exists (pq) = (p + \exists p + \forall p)(q + \exists q + \forall q) + pq + \forall p . \forall q,$$

soit $m(pq) = mp . mq$.

L'équivalence entre 2° et 3° est triviale, car on a toujours $m(\neg p) = \neg mp$.

L'équivalence entre 3° et 4° résulte du fait que m est bijective avec $m^{-1} = m$, et que tout isomorphisme d'ordre est un isomorphisme booléien.

3° implique 5° trivialement, car : $\gamma p = p + mp$ avec m additive.

5° implique 4°, en effet : soient p, q, r trois éléments deux à deux disjoints : $pq = qr = rp = 0$

$$\gamma p . \gamma q . \gamma r = \exists p . \exists q . \exists r . \neg \forall p . \neg \forall q . \neg \forall r,$$

or $p \leq \neg q$, donc $\exists p \leq \exists (\neg q)$, d'où $\exists p \leq \neg \forall q$.

De même, $\exists q \leq \neg \forall r$ et $\exists r \leq \neg \forall p$, on a donc

$$\gamma p . \gamma q . \gamma r = \exists p . \exists q . \exists r$$

(ceci est général, pour toute suite finie d'éléments deux à deux disjoints).

Soient maintenant p, q deux éléments disjoints, les trois éléments p, q et $\neg p . \neg q$ sont deux à deux disjoints, donc

$$\gamma p . \gamma q . \gamma (\neg p . \neg q) = \exists p . \exists q . \exists (\neg p . \neg q),$$

soit

$$\gamma p . \gamma q . \gamma (\neg (p \vee q)) = \exists p . \exists q . \exists (\neg (p \vee q)),$$

soit

$$\gamma p . \gamma q . \gamma (p + q) = \exists p . \exists q . (\neg (p \vee q))$$

si γ est additive,

$$\gamma p.\gamma q.\gamma(p+q) = \gamma p.\gamma q.(\gamma p + \gamma q) = o,$$

donc

$$\exists p.\exists q.(\neg(p \vee q)) = o \quad \text{lorsque } p \text{ et } q \text{ sont disjoints.}$$

Montrons enfin que m est croissante : soient p et q deux éléments tels que $p \leq q$, p et $\neg q$ sont disjoints, donc

$$\exists p.\exists(\neg q).\exists(\neg p.q) = o, \qquad \neg p.q = p+q,$$

d'où $\exists p.\exists(p+q) \leq \forall q$, *a fortiori* $mp.m(p+q) \leq mq$,

or m est aussi additive (car $mp = p + \gamma p$), donc

$$mp.(mp + mq) \leq mq,$$

soit

$$mp + mp.mq = o, \qquad \text{d'où} \quad mp \leq mq.$$

L'équivalence entre 5° et 6° est triviale, car on a toujours $\gamma(bp) = b\gamma p$ pour $b \in B$.

THÉORÈME 3.3. — *Soient A un anneau booléien et m un automorphisme involutif de A, alors l'opérateur $\exists$ défini par $\exists p = p \vee mp$ est un quantificateur sur A, et le quantificateur universel associé est $\forall p = p.mp$. Pour cette structure, A est un anneau monadique rationnel et sa fonction moyenne est m.*

En effet, on vérifie aisément les trois axiomes des quantificateurs :

$\exists o = o$: trivial,

$p \leq \exists p$: trivial,

$$\exists(p.\exists q) = (p\,\exists q) \vee m(p\,\exists q) = (p\,\exists q) \vee (mp.\exists q),$$

car $m\,\exists q = mq \vee mmq = \exists q$,

$$= (p \vee mp)\,\exists q = \exists p.\exists q.$$

En outre,

$$\forall p = \neg\exists(\neg p) = \neg(\neg p \vee m(\neg p)) = p.mp.$$

On a ainsi caractérisé les anneaux monadiques rationnels, ils sont tous obtenus par le procédé du théorème 3.3.

Si A est un anneau booléien, il y a donc correspondance bijective entre les automorphismes involutifs de A et les quantificateurs rationnels sur A.

Remarque. — Si un polynôme monadique en p est un endomorphisme, ce ne peut être que p ou mp.

Supposons que $f(p) = ap + b\,\exists\, p + c\,\forall\, p + d (a, b, c, d \in \mathbf{U})$ soit un endomorphisme.

— Pour $p = 0$: $d = 0$,

— Pour $p = 1$: $a + b + c = 1$,

$$f(\neg p) = ap + b\,\forall\, p + c\,\exists\, p + a + b + c = ap + b\,\forall\, p + c\,\exists\, p + 1,$$
$$\neg f(p) = ap + b\,\exists\, p + c\,\forall\, p + 1,$$

d'où

$$b\,\exists\, p + c\,\forall\, p = b\,\forall\, p + c\,\exists\, p \quad \text{pour tout } p,$$

donc $b = c$, alors $a = 1$.

Si $b = c = 0$, on a la fonction $f(p) = p$.

Si $b = c = 1$, on a la fonction $f(p) = mp$.

3.4. Exemples d'anneaux monadiques rationnels.

1° *Les anneaux* $B[\Gamma]$ *sont rationnels.* En effet, $\gamma(p, q) = (q, 0)$, donc γ est additive.

2° *Tout anneau monadique discret est rationnel,* avec $m(p) = p$.

3° *Le seul anneau monadique simple, non discret, rationnel, est l'anneau à quatre éléments.*

En effet :

— Si A est simple, pour $p \neq 0$ et $p \neq 1$:

$$m(p) = p + \exists\, p + \forall\, p = p + 1 = \neg p,$$

par ailleurs $m(0) = 0$ et $m(1) = 1$.

— Si A est l'anneau à quatre éléments $\{ 0, p, \neg p, 1 \}$, m est bien alors un automorphisme, car elle est croissante.

— Réciproquement, si m est un automorphisme : soient p et q deux éléments différents de 0 et 1, si $pq \neq 0$:

$$m(pq) = \neg(pq) = \neg p \vee \neg q \leq m(p) = \neg p,$$

donc $\neg p \vee \neg q = \neg p$, soit $\neg q \leq \neg p$; de même, $\neg p \vee \neg q = \neg q$, soit $\neg p \leq \neg q$, donc $p = q$.

De même, si $p \vee q \neq 1$, on a $p = q$.

Donc si $q \neq p$, on a $pq = 0$ et $p \vee q = 1$, soit $q = \neg p$.

Donc $A = \{ 0, p, \neg p, 1 \}$.

4° *Cas des anneaux atomiques :* Supposons que A soit un anneau atomique, et soit $\mathfrak{A}$ l'ensemble de ses atomes. Soit m un automorphisme involutif de A, et soit μ sa restriction à $\mathfrak{A}$: alors μ est une permutation (involutive) de $\mathfrak{A}$, en effet : soit $a \in \mathfrak{A}$, supposons $p \leq m(a)$, alors $m(p) \leq a$ donc $m(p) = 0$ ou $m(p) = a$.

Soit $p = 0$ ou $p = m(a)$, donc $m(a) \in \mathfrak{A}$.

Donc μ est une application de $\mathfrak{A}$ dans $\mathfrak{A}$, et elle est involutive.

Remarquons que m est entièrement définie par μ : soit $p \in A$, soit $\mathfrak{A}_p$ l'ensemble des atomes $\leq p$, on sait que $p = \bigvee_{\mathfrak{A}_p} a$, et m étant un automorphisme, on aura

$$m(p) = \bigvee_{\mathfrak{A}_p} m(a) = \bigvee_{\mathfrak{A}_p} \mu(a).$$

Réciproquement, si on se donne une permutation involutive μ de $\mathfrak{A}$, peut-on la prolonger en un automorphisme involutif m de A ? D'après ce qui précède, si un tel prolongement existe, il est unique, et il est donné par la formule

$$m(p) = \bigvee_{\mathfrak{A}_p} \mu(a).$$

La condition nécessaire et suffisante de possibilité est donc :

(I) *Pour tout p, l'ensemble $\mu(\mathfrak{A}_p)$ possède une borne supérieure.*

Cette condition sera notamment réalisée dans tout anneau atomique achevé (i. e. l'anneau des parties d'un ensemble), en particulier dans tout anneau fini. Lorsque la condition précédente est réalisée, il est facile de vérifier que le prolongement m est bien un automorphisme involutif (c'est-à-dire, plus simplement, une involution croissante).

5° *Cas des anneaux finis :* La recherche des quantificateurs rationnels sur un anneau booléien fini (et plus généralement sur un anneau du type $\mathfrak{P}(X)$) est donc ramenée à la recherche des permutations involutives de l'ensemble $\mathfrak{A}$ de ses atomes.

Toute permutation involutive de $\mathfrak{A}$ est une fonction composée d'échanges d'atomes deux à deux.

Par exemple, dans l'anneau à huit éléments construit avec trois atomes p, q, r, il y a quatre automorphismes involutifs : l'application identique et les échanges de deux des trois atomes p, q, r. Notons qu'il y a au total six automorphismes (toutes les permutations des atomes) et cinq quantificateurs (toutes les partitions de l'ensemble des atomes), seul le quantificateur simple n'est pas rationnel.

Remarque. — Dans un anneau atomique quelconque, toute fonction composée d'une nombre *fini* d'échanges d'atomes vérifie la condition (I) :

considérons simplement l'échange de deux atomes :

$$\mu(a) = b, \qquad \mu(b) = a,$$
$$\mu(c) = c \quad \text{ailleurs};$$

— si a et $b \notin \mathfrak{a}_p$: $\mu(\mathfrak{a}_p) = \mathfrak{a}_p$,
— si a et $b \in \mathfrak{a}_p$: $\mu(\mathfrak{a}_p) = \mathfrak{a}_p$,
— si $a \in \mathfrak{a}_p$ et $b \notin \mathfrak{a}_p$: $\mu(\mathfrak{a}_p) = (\mathfrak{a}_p - \{ a \}) \cup \{ b \} = \mathfrak{a}_q$, avec $q = (p . \neg a) \vee b$.

Dans tous les cas : $\bigvee \mu(\mathfrak{a}_p)$ existe.

3.5. **Représentation topologique des anneaux monadiques rationnels.**

Désignons par (X, R) l'espace monadique dual de l'anneau monadique $(A, \exists)$, c'est-à-dire :

X : espace de Stone de A (ensemble des ultrafiltres de A), la topologie étant celle engendrée par les ofs (ouverts-fermés) :

$$\sigma(p) = \{ x \in X : p \in x \}.$$

R : relation booléienne d'équivalence duale de $\exists$ ([3], [6]) définie par

$$xRy \Leftrightarrow x \cap B = y \cap B.$$

Dans le cas d'un anneau rationnel, m est un automorphisme de A, on pourra donc définir sa fonction continue duale $m^* : X \frown X$:

$$m^*(x) = m^{-1}(x),$$

soit, tout simplement, $m^*(x) = m(x)$.

Par abus de notations, on continuera à noter m au lieu de m^* cette fonction duale, qui est donc une involution continue de X.

Réciproquement, à partir de toute involution continue de X, on peut définir dualement un automorphisme involutif de A.

On a la formule de dualité habituelle : $\sigma(mp) = m(\sigma(p))$ pour tout $p \in A$. Notons aussi :

$$p \in m(x) \iff mp \in x$$

et

$$\sigma(\exists p) = \sigma(p \vee mp) = \sigma(p) \cup \sigma(mp) = \sigma(p) \cup m(\sigma(p)) = \operatorname{sat} \sigma(p).$$

Désignons par $\tilde{x}$ la classe modulo R d'un ultrafiltre x.

Soit $y \in \tilde{x}$, et supposons $y \neq x$: il existe $q \in y$, $q \notin x$; soit alors $p \in y$:

$pq \in y$, $\exists\,(pq) \in y$, donc $\exists\,(pq) \in x$,

or

$$\exists\,(pq) = (pq) \vee (mp.mq) = (p \vee mp).(q \vee mq).(q \vee mp),$$

donc $q \vee mp \in x$, or $q \notin x$, donc $mp \in x$, soit $p \in m(x)$.

Donc $y \subset m(x)$, et par suite $y = m(x)$. Ainsi

$$\tilde{x} = \{ x, m(x) \}.$$

On obtient donc une partition de X en classes ayant au plus deux éléments [on peut avoir $x = m(x)$].

Réciproquement, soit $(A, \exists)$ un anneau monadique tel que toutes les classes modulo R de son espace dual possèdent au plus deux éléments. Montrons que A est un anneau monadique rationnel.

Soit m^* l'application de X dans X définie par

$$m^*(x) = x \quad \text{si} \quad \tilde{x} = \{ x \},$$
$$m^*(x) = y \quad \text{si} \quad \tilde{x} = \{ x, y \}, \quad \text{avec} \quad y \neq x,$$

m^* est une involution de X;

m^* est continue; en effet, nous allons vérifier que

$$m^*(\sigma(p)) = \left(\bigcap \sigma(p) \cup \sigma(\forall\, p) \right) \cap \sigma(\exists\, p) \quad \text{(qui sera un of).}$$

En effet :

— si $y \in m^*(\sigma(p))$, par définition $y \in \operatorname{sat} \sigma(p)$, soit $y \in \sigma(\exists\, p)$, et

$$\text{ou bien } y \notin \sigma(p) : \quad y \in \bigcap \sigma(p),$$
$$\text{ou bien } y \in \sigma(p), \quad \text{alors} \quad \tilde{y} \subset \sigma(p),$$

donc $y \notin \operatorname{sat} \bigcap \sigma(p)$, soit $y \in \bigcap \operatorname{sat} \bigcap \sigma(p) = \sigma(\forall\, p)$.

— Réciproquement, si $y \in \left(\bigcap \sigma(p) \cup \sigma(\forall\, p) \right) \cap \sigma(\exists\, p)$, $y \in \operatorname{sat} \sigma(p)$, donc il existe $x \in \sigma(p)$ tel que $y \in \check{x}$,

si $y \notin \sigma(p)$: $y \neq x$, donc $\tilde{x} = \{ x, y \}$ et $y = m^*(x) \in m^*(\sigma(p))$,

si $y \in \sigma(p)$, alors $y \in \sigma(\forall\, p)$, donc $y \notin \operatorname{sat} \bigcap \sigma(p)$,

donc $\tilde{y} \cap \bigcap \sigma(p) = \emptyset$, soit $\tilde{y} \subset \sigma(p)$,

si $\tilde{y} = \{y\}$: $y = m^*(y) \in m^*(\sigma(p))$,
si $\tilde{y} = \{x, y\}$ avec $x \neq y$: $y = m^*(x) \in m^*(\sigma(p))$.

Ainsi m^* est bien une involution continue de X, il lui correspond un automorphisme dual m de A, défini par

$$\sigma(mp) = m^*(\sigma(p)) = \sigma((\neg p \vee \forall p).\exists p),$$

m n'est autre que la fonction moyenne, $(A, \exists)$ est donc un anneau monadique rationnel. On peut donc énoncer :

THÉORÈME 3.6. — *Soit $(A, \exists)$ un anneau monadique, d'espace monadique dual (X, R), il y a équivalence entre :*

1° *$(A, \exists)$ est un anneau monadique rationnel.*

2° *les classes* modulo R *dans X ont au plus deux éléments.*

4. Constantes et richesse des anneaux monadiques rationnels.

Dans tout ce paragraphe, $(A, \exists)$ désigne un anneau monadique rationnel, de charpente B et de centre Γ, on rappelle que m est alors un automorphisme involutif, et γ une application B-linéaire.

PROPOSITION 4.1. — *$\exists$ est injective sur tout idéal $I \subset \forall^{-1}(0)$.*

En effet, si $\exists p = \exists q$ avec $p, q \in I$: $\forall p = \forall q = 0$, donc $\gamma p = \gamma q$, soit $\gamma(p + q) = 0$, donc $p + q \in B$, or $p + q \in I$, donc $p + q = \forall (p + q) = 0$ soit $p = q$.

COROLLAIRE 1. — *$\exists$ est injective sur tout noyau de constante, car si c est une constante,*

$$\ker(c) \subset \forall^{-1}(0) \qquad (\forall p \leq cp).$$

COROLLAIRE 2. — *Pour toute constante c, $\exists$ est une bijection de* $\ker(c)$ *sur Γ, car $\Gamma = \exists$ (*$\ker(c)$*), et on applique le corollaire* 1.

COROLLAIRE 3. — *Il y a équivalence entre :*

(*a*) *il existe une constante,*

(*b*) *il existe un idéal de A : $I \subset \forall^{-1}(0)$ tel que $\Gamma = \exists I$ (I* est alors un noyau de constante).

En effet :

$(a) \Rightarrow (b)$: en prenant $I = \ker(c)$, où c est une constante.

$(b) \Rightarrow (a)$: soit $p \in A$, $\gamma p \in \Gamma$, donc $\gamma p = \exists\, i$ avec $i \in I$ (i unique), alors

$$\gamma(p + i) = \gamma p + \gamma i = \exists\, i + \exists\, i = 0,$$

donc $p + i = b \in B$; soit $p = b + i$, d'où

$$A = B \oplus I,$$

donc I est un noyau de constante.

THÉORÈME 4.2. — *Pour qu'un anneau monadique rationnel possède au moins une constante, il faut et il suffit qu'il soit isomorphe à un anneau monadique $B[\Gamma]$. Il est alors riche.*

Démonstration. — On sait déjà que tout anneau $B[\Gamma]$ est rationnel riche.

Réciproquement, soit $(A, \exists)$ un anneau rationnel admettant au moins une constante c, définissons l'application $\varphi : A \rightharpoonup B[\Gamma]$ par

$$\varphi(p) = (cp, \gamma p),$$

φ est *injective* : si $cp = cq$ et $\gamma p = \gamma q$, alors $c(p + q) = 0$ et $\gamma(p + q) = 0$, donc $p + q \in B \cap \ker(c)$, donc $p = q$.

φ est *surjective* : soit $(b, q) \in B[\Gamma]$, $q \in \Gamma$, donc $q = \exists\, i$ avec $i \in \ker(c)$, et nous savons que i est unique, soit alors $p = b + i$, on a bien $cp = b$,

$$\gamma p = \gamma i = \exists\, i = q,$$

donc $(b, q) = \varphi(p)$.

φ est un *homomorphisme booléien* :

$$\begin{aligned}
\varphi(\neg p) &= (c(\neg p), \quad \gamma(\neg p)) = (\neg cp, \gamma p) = \neg \varphi(p) \\
\varphi(pq) &= (c(pq), \gamma(pq)) \\
&= (cp.cq, pq + mp.mq) \qquad (\text{car } \gamma p = p + mp), \\
\varphi(p).\varphi(q) &= (cp.cq, \gamma p.\gamma q + cp.\gamma q + cq.\gamma p),
\end{aligned}$$

on remarque

$$\begin{aligned}
cp.\gamma q + cq.\gamma p &= c(p.\gamma q + q.\gamma p), \qquad \text{car } \gamma p, \gamma q \in B \\
&= c(p(q + mq) + q(p + mp)), \\
&= c(p.mq + q.mp),
\end{aligned}$$

or $m(p.mq + q.mp) = p.mq + q.mp$, soit $p.mq + q.mp \in B$, donc

$$cp.\gamma q + cq.\gamma p = p.mq + q.mp$$

et

$$\gamma p.\gamma q = pq + mp.mq + p.mq + q.mp,$$

d'où $\varphi(p).\varphi(q) = (cp.cq,\ pq + mp.mq) = \varphi(pq)$.

Enfin, φ est un *isomorphisme monadique :*

$$\varphi(\exists p) = (c\exists p,\ \gamma\exists p) = (\exists p,\ o),$$
$$\exists\varphi(p) = (cp \vee \gamma p,\ o),$$

or

$$cp \vee \gamma p = cp \vee (\exists p + \forall p) = cp + \exists p + \forall p + cp.\exists p + cp.\forall p = \exists p.$$

Nous avons ainsi entièrement caractérisé les anneaux monadiques rationnels riches (ou possédant une constante).

Corollaire. — *Les anneaux monadiques rationnels qui ont au moins un élément principal sont riches, et toutes leurs constantes sont principales*

En effet, Γ est alors un idéal principal.

Nous allons voir que la réciproque est exacte : si Γ est principal, l'anneau rationnel possède au moins un élément principal.

Proposition 4.3. — *Dans un anneau monadique rationnel, il y a équivalence entre élément principal et élément quasi-singulier.*

En effet : soient p et q deux éléments quelconques,

$$\exists(pq) = (pq) \vee (mp.mq) = (p \vee mp).(q \vee mq).(p \vee mq).(q \vee mp),$$

de même,

$$\exists(\neg p.q) = (\neg p \vee \neg mp).(q \vee mq).(\neg p \vee mq).(p \vee \neg mp),$$

donc

$$\begin{aligned}\exists(pq).\exists(\neg p.q) &= (p + mp).(q \vee mq).mq.q \\ &= (p + mp).\exists q.\forall q \\ &= (p + mp).\forall q \\ &= \gamma p.\forall q.\end{aligned}$$

Supposons que q soit quasi-singulier : $\gamma q = \forall q + 1$ et $\gamma p \leq \gamma q$, donc

$$\exists(p.q).\exists(\neg p.q) = \gamma p.(\gamma q + 1) = o \quad \text{pour tout } p \in A,$$

donc q est un élément principal.

Par ailleurs, la réciproque est vraie dans tout anneau monadique. On en déduit le résultat suivant.

THÉORÈME 4.4. — *Pour un anneau monadique rationnel* $(A, \exists)$, *il y a équivalence entre :*

1° *A possède au moins une constante principale :*

2° *le centre* Γ *est un idéal principal.*

Dans ce cas, l'anneau est riche, et toutes ses constantes sont principales.

Un anneau monadique rationnel à centre principal sera dit *rationnel principal.*

THÉORÈME 4.5. — *Si A est un anneau monadique rationnel principal, de charpente B et de centre* Γ, *alors pour tout élément principal* ϖ :

$$A = B \oplus \Gamma.\varpi.$$

Autrement dit, tout élément $p \in A$ *s'écrit de façon unique* $p = a + b\varpi$ *avec* $a, b \in B$ *et* $b \leq \neg \forall \varpi$.

On a alors : $\exists\, p = a \vee b$, $\forall\, p = a.\neg\, b$, $\gamma p = b$.

En effet, ceci résulte immédiatement du théorème 4.2 et de l'isomorphisme φ de A sur $B[\Gamma]$:

$$\varphi(p) = (cp, \gamma p), \qquad c, \text{ constante principale définie par } \varpi.$$

Soit

$$\begin{aligned} \varphi(p) &= (cp, o) + (o, \gamma p), \qquad \text{or} \quad (o, \gamma\varpi).(\gamma p, o) = (o, \gamma p) \\ &= (cp, o) + (\gamma p, o).(o, \gamma\varpi), \\ &= \varphi(cp) + \varphi(\gamma p).\varphi(\neg\varpi), \qquad \text{car} \quad c(\neg\varpi) = o, \end{aligned}$$

soit $p = cp + \gamma p.(\neg\varpi) = cp + \gamma p + \gamma p.\varpi$, donc $a = cp + \gamma p$ et $b = \gamma p$.

Réciproquement, si $p = a + b\varpi$ avec $a, b \in B$ et $b \leq \gamma\varpi$, on a

$$\begin{aligned} \gamma p &= b\gamma\varpi = b, \\ p.\varpi &= (a+b)\varpi, \end{aligned}$$

donc $cp = \exists\,(p.\varpi) = a + b$, d'où $a = cp + \gamma p$.

5. Introduction à la notion de dimension monadique.

Soit $(A, \exists)$ un anneau monadique quelconque, de charpente B, pour toute partie $G \subset A - B$, nous noterons $\langle B, G \rangle$ le sous-anneau booléien de A engendré par $B \cup G$, notons que c'est aussi le sous-anneau monadique de A engendré par $B \cup G$ (car il contient la charpente de A). En particulier, si G est réduit à un seul élément q, on pourra parler del'anneau monadique $\langle B, q \rangle$, et dans ce cas, nous savons qu'il est formé par tous

les éléments $a + bq$, avec $a, b \in B$ (cette écriture n'étant pas nécessairement unique).

Le théorème 4.5 ci-dessus peut alors s'exprimer de la façon suivante :

Si A est un anneau monadique rationnel principal non discret, alors pour tout élément principal ϖ :

$$A = \langle B, \varpi \rangle.$$

On peut obtenir une réciproque de cette propriété.

THÉORÈME 5.1. — *Soit $(A, \exists)$ un anneau monadique quelconque, non discret, alors pour tout élément $q \in A - B$, $\langle B, q \rangle$ est un anneau monadique rationnel principal.*

Démonstration. — Soit $p \in \langle B, q \rangle$: $p = a + bq$ avec $a, b \in B$, d'où $\gamma p = b \gamma p$.

Il en résulte trivialement que γ est additive sur $\langle B, q \rangle$, $\langle B, q \rangle$ est donc un sous-anneau rationnel de A.

En outre, $\gamma p \leq \gamma q$, donc le centre Γ' de $\langle B, q \rangle$ est l'idéal principal de B engendré par γq.

N. B. — q n'est pas nécessairement un élément principal de $\langle B, q \rangle$, mais on peut construire un élément principal (ou quasi-singulier) ϖ, en prenant simplement $\varpi = \exists q + 1 + q = q \vee \neg \exists q$. On a alors $\langle B, q \rangle = \langle B, \varpi \rangle$, mais cette fois avec la décomposition canonique du théorème 4.5.

On en déduit :

COROLLAIRE. — *Pour qu'un anneau monadique A de charpente B soit rationnel principal, il faut et il suffit qu'il existe un élément q tel que $A = \langle B, q \rangle$.*

On est ainsi conduit à définir la notion de *dimension monadique* pour un anneau monadique A de charpente B : le plus petit cardinal α tel qu'il existe $G \subset A - B$, avec card $G = \alpha$ et $A = \langle B, G \rangle$. On a donc obtenu les caractérisations suivantes :

Anneau de dimension $0 \Leftrightarrow$ Anneau monadique discret,

Anneau de dimension $1 \Leftrightarrow$ Anneau monadique rationnel principal, non discret.

Dans le cas des anneaux rationnels, on peut préciser la dimension :

THÉORÈME 5.2. — *Un anneau monadique rationnel, non discret, est soit de dimension 1 (et cela équivaut à dire qu'il est principal), soit de dimension infinie.*

En effet :

— Considérons d'abord le cas d'un anneau rationnel du type $A = \langle B, q, r \rangle$. Soit $p \in A$: $p = a + bq + cr + dqr$, $a, b, c, d \in B$, d'où

$$\gamma p = b\gamma q + c\gamma r + d\gamma(qr),$$

or

$$\gamma(qr) = qr + mq.mr = qr + (q + \gamma q)(r + \gamma r) = \gamma q.\gamma r + r.\gamma q + q.\gamma r,$$

alors

$$\gamma p.\gamma q = b.\gamma q + c\gamma q\gamma r + d\gamma q\gamma r + dr\gamma q + dq.\gamma q\gamma r,$$

$$\gamma p + \gamma r = b\gamma q\gamma r + c\gamma r + d\gamma q\gamma r + dr\gamma r\gamma q + dq\gamma r,$$

$$\gamma p.\gamma q.\gamma r = b\gamma q\gamma r + c\gamma q\gamma r + d\gamma q\gamma r + dr\gamma q\gamma r + dq\gamma r\gamma q,$$

d'où

$$\gamma p(\gamma q \vee \gamma r) = b\gamma q + c\gamma r + d\gamma q.r + dr\gamma q + dq\gamma r = \gamma p,$$

donc $\gamma p \leq \gamma q \vee \gamma r$: le centre Γ est donc principal, et A est de dimension 1.

— Soit maintenant $A = \langle B, G \rangle$ avec G fini, montrons par récurrence sur le cardinal de G que A est de dimension 1 : si $G = q_1, \ldots, q_n, q_{n+1}$, en posant $H = q_1, \ldots, q_n$, il suffit de remarquer que

$$A = \langle B, G \rangle = \langle \langle B, H \rangle, q_{n+1} \rangle,$$

$\langle B, H \rangle = \langle B, r \rangle$ par hypothèse de récurrence

$$A = \langle \langle B, r \rangle, q_{n-1} \rangle = \langle B, r, q_{n-1} \rangle,$$

de dimension 1 d'après le cas étudié précédemment.

Remarques :

1° Il existe évidemment des anneaux rationnels de dimension infinie ($B[\Gamma]$ avec Γ non principal). On peut d'ailleurs montrer [2] que, pour tout cardinal infini α, il existe des anneaux rationnels de dimension α.

2° Un anneau monadique non rationnel peut être de dimension finie quelconque (et également de dimension infinie), par exemple un anneau monadique simple, ayant 2^{2^n} éléments, est de dimension n.

3° Une étude générale des anneaux (non rationnels) de dimension finie ou dénombrable a été faite par J.-L. Coulon [2], on obtient toujours des anneaux riches.

4° On peut construire des anneaux rationnels sans constante (un exemple m'a été communiqué par un de mes élèves, J.-C. Carrega).

BIBLIOGRAPHIE.

[1] BIRKHOFF (G.). — *Lattice theory.* 3rd edition. — Providence, American mathematical Society, 1967 (*American mathematical Society, Colloquium Publications*, 25).

[2] COULON (J. L.). — *Notion de dimension dans les anneaux monadiques* (Thèse 3e cycle, Math., Fac. Sc. Lyon).

[3] HALMOS (P. R.). — *Algebraic logic.* — New York, Chelsea Publishing Company, 1962.

[4] LE BLANC (N.). — *Introduction à la logique algébrique.* Cours polycopié, Montréal, 1963.

[5] PONASSE (D.). — *Logique mathématique.* — Paris, Office central de Librairie, 1967.

[6] PONASSE (D.). — Quelques catégories de la logique, *Bol. Soc. mat. São Paulo*, t. 16, 1965, p. 91-102.

(Texte reçu le 10 septembre 1970.)

Daniel PONASSE,
Faculté des Sciences de Yaoundé,
Département de Mathématiques,
B. P. nº 812,
Yaoundé (Cameroun).