Partie A

Résultats algébriques

Chapitre 0

Préliminaires

Introduction

Ce chapitre passe en revue la théorie algébrique de base des dioïdes. Les résultats présentés sont classiques, à l'exception des questions d'inversibilité d'applications linéaires et de quelques raffinements sur les familles génératrices minimales. L'idée qui est à l'œuvre dans cette théorie est qu'à la différence des demi-anneaux généraux, les dioïdes peuvent être munis d'une structure ordonnée canonique. Il devient alors possible (i): d' étudier les inéquations de type

$$x \succeq ax \oplus b \tag{0.0.a}$$

à l'aide de techniques de point fixe, et (ii): d'étudier les inéquations de type

$$x \oplus a \succeq b, \tag{0.0.b}$$

$$ax \preceq b \tag{0.0.c}$$

à l'aide de la théorie de la résiduation. L'étude des inéquations de type (i) est l'un des plus anciens résultats connus sur ces structures [47]. L'opération "$*$" (étoile de Kleene) est introduite à cette occasion, ainsi que la notion de rationalité. L'interprétation de l'étoile en termes d'algèbre de chemins est brièvement rappelée. Elle jouera un rôle central dans la dernière partie (optimisation des ressources). L'étude des inéquations de type (ii) est une application assez directe de la théorie de la résiduation, dite aussi théorie des correspondances de Galois dans les structures ordonnées. On applique cette théorie au cas des dioïdes, définissant les opérations résiduées des lois de structure, i.e. les différences et quotients résidués, dont on établit le formulaire. Ce formulaire est obtenu en spécialisant la théorie des demi-groupes résidués généraux, qui remonte à Dubreil [30]. Nous ferons dans la suite un usage constant de ces outils (étoile et opérations résiduées). Signalons enfin que ces techniques permettent de résoudre à peu près exclusivement les équations et inéquations de type (0.0.a), (0.0.b) ou (0.0.c) (ainsi que leur duales). L'étude des équations générales du type $ax \oplus b = cx \oplus d$ requiert une théorie de la symétrisation qui sera développée dans les chapitres suivants.

1 Demi-anneaux et dioïdes

1.0.1 Définition (demi-anneau) *On appelle demi-anneau un ensemble $\mathcal{D}$ muni d'une loi associative (notée additivement "$\oplus$"), commutative, d'élément neutre ε, et d'une loi associative (notée multiplicativement "$\otimes$"), d'élément neutre e, telles que:*

(i) $\forall a, b, c \in \mathcal{D},\ (a \oplus b) \otimes c = (a \otimes c) \ \oplus\ (b \otimes c)$

(ii) $\forall a, b, c \in \mathcal{D},\ c \otimes (a \oplus b) = (c \otimes a) \ \oplus\ (c \otimes b)$

(iii) $\forall a \in \mathcal{D}, a \otimes \varepsilon = \varepsilon \otimes a = \varepsilon.$

Si en outre $\oplus$ vérifie

$$a \oplus a = a \tag{1.0.a}$$

alors $\mathcal{D}$ est dit *demi-anneau idempotent*, ou *dioïde*. Si $(\mathcal{D}\backslash\{\varepsilon\}, \otimes)$ est un groupe, on qualifie $(\mathcal{D}, \oplus, \otimes)$ de *demi-corps*. Un demi-corps dont l'addition vérifie (1.0.a) sera dit *idempotent*. Un demi-anneau ou demi-corps sera dit *commutatif* lorsque le produit est commutatif. Un demi-anneau tel que

$$\begin{array}{l}(a \neq \varepsilon \text{ et } \ ax = ay) \implies x = y \\ (a \neq \varepsilon \text{ et } \ xa = ya) \implies x = y\end{array} \tag{1.0.b}$$

(i.e. les homothéties à gauche et à droite sont injectives) sera dit *intègre*. On notera ordinairement le produit $a \otimes b$ par $a.b$ ou ab.

1.0.2 Exemple (dioïde des booléens) L'ensemble $\mathbb{B} := \{\varepsilon, e\}$, muni des lois $\oplus$ et $\otimes$ définies ci dessous est un dioïde commutatif, dit dioïde des booléens.

$\oplus$	ε	e
ε	ε	e
e	e	e

$\otimes$	ε	e
ε	ε	ε
e	ε	e

On notera que tout dioïde admet $\mathbb{B}$ comme sous-dioïde.

1.0.3 Exemple (algèbre $(\max, +)$) L'ensemble $\mathbb{R} \cup \{-\infty\}$, muni du max (noté additivement) et de l'addition usuelle (noté multiplicativement) est un demi-corps idempotent (on convient que $x + (-\infty) = x$ pour tout x). On a dans cette structure $1 \otimes 1 = 2$, $1 \otimes 0 = 1$, $2 \oplus 3 = 3$. On notera $\mathbb{R}_{\max}$ ce demi-corps idempotent, traditionnellement[1] appelé "algèbre $(\max, +)$".

1.0.4 Exemple (algèbre $(\min, +)$) L'ensemble $\mathbb{R} \cup \{+\infty\}$, muni du min (noté additivement) et de l'addition usuelle (noté multiplicativement) est un demi-corps idempotent, isomorphe à $\mathbb{R}_{\max}$, que l'on notera $\mathbb{R}_{\min}$.

1.0.5 Exemple (dioïde des parties de $\mathbb{R}$) L'ensemble des parties de $\mathbb{R}$, muni de l'union et de la somme vectorielle est un dioïde.

1.0.6 Exemple (dioïde libre et dioïde des langages) Rappelons qu'étant donné un ensemble de k lettres $A = \{a_1, \ldots, a_k\}$ (alphabet), le *monoïde libre* formé sur A est l'ensemble des mots formés d'un nombre fini de lettres de A, y compris le mot vide noté "_", muni du produit de concaténation noté ".". Etant données deux parties X, Y de A^* (deux *langages*), on définit le produit $X.Y := \{x.y \mid (x, y) \in X \times Y\}$. On a les deux dioïdes suivants:

1/ $(\mathcal{P}_{\text{finies}}(A^*), \cup, .)$, dioïde des langages finis (parties finies de A^*) formés sur l'alphabet A,

[1]le terme "algèbre est à prendre au sens général (un ensemble muni d'une famille d'opérations [9]), et n'a rien à voir avec les algèbres au sens usuel [12]

2/ $(\mathcal{P}(A^*), \cup, .)$, dioïde des langages quelconques formés sur l'alphabet A.

Le dioïde $\mathcal{P}(A^*)$ admet $\emptyset$ pour zéro et $\{\_\}$ pour unité. Il a $\mathcal{P}_{\text{finies}}(A^*)$ pour sous-dioïde. On posera $\alpha_i := \{a_i\}$. L'intérêt de $\mathcal{P}_{\text{finies}}(A^*)$ est d'être une réalisation du *dioïde libre* engendré par $\alpha_1, \ldots, \alpha_k$. Précisément, on a la propriété universelle suivante:

1.0.7 Proposition *Pour tout dioïde $\mathcal{D}$ et tout k-uplet $(x_1, \ldots, x_k) \in \mathcal{D}^k$, il existe un unique morphisme de dioïde $\phi : \mathcal{P}_{\text{finies}}(A^*) \to \mathcal{D}$, tel que pour tout $i \in \{1, \ldots, k\}$, $\phi(\alpha_i) = x_i$.*

Preuve de 1.0.7. ϕ est nécessairement donné par

$$\begin{aligned} \phi(\{\_\}) &= e \\ \phi(\{a_{i_1} \ldots a_{i_k}\}) = \phi(\{a_{i_1}\}) \ldots \phi(\{a_{i_k}\}) &= \phi(\alpha_{i_1}) \ldots \phi(\alpha_{i_k}) = x_{i_1} \ldots x_{i_k} \\ \phi(\{w_1, \ldots, w_r\}) &= \phi(\{w_1\}) \oplus \ldots \phi(\{w_r\}) \end{aligned} \tag{1.0.c}$$

ce qui définit bien un morphisme de dioïde. ∎

1.0.8 Exemple (Dioïde des séries formelles, dioïde des polynômes) Soient A un alphabet comme ci-dessus et $\mathcal{D}$ un dioïde. On appelle dioïde des séries formelles à coefficients dans $\mathcal{D}$ en les indéterminées non commutatives a_i l'ensemble des applications s du monoïde libre A^* dans $\mathcal{D}$, muni des deux lois suivantes:

$$(s \oplus s')(w) := s(w) \oplus s'(w), \quad (s \otimes s')(w) := \bigoplus_{w_1 w_2 = w} s(w_1) \otimes s(w_2) \ .$$

On notera $\mathcal{D}\langle\langle A \rangle\rangle$ ce dioïde. En identifiant a_i et l'application $\delta_{a_i} : \delta_{a_i}(w) = e$ si $w = a_i$ et ε sinon, on écrit formellement

$$s = \bigoplus_{w \in A^*} s(w) w \ .$$

On appelle polynôme une séries s telles que $s(w) = \varepsilon$ sauf peut-être pour un nombre fini de mots. L'ensemble des polynômes forme un sous-dioïde de $\mathcal{D}\langle\langle A \rangle\rangle$, que l'on notera $\mathcal{D}\langle A \rangle$. On observe que le dioïde des polynômes à coefficients booléiens $\mathbb{B}\langle A \rangle$ vérifie la propriété universelle 1.0.7 avec $\alpha_i = a_i$. Il est donc isomorphe à $(\mathcal{P}_{\text{finies}}(A^*), \cup, .)$ défini en 1.0.6. L'isomorphisme n'est autre que l'application support:

$$(\mathbb{B}\langle A \rangle, \oplus, \otimes) \to (\mathcal{P}_{\text{finies}}(A^*), \cup, .), \quad s \mapsto \text{supp} s := \{w \in A \mid \ s(w) \neq \varepsilon\} \ .$$

Si l'on remplace A^* par le monoïde commutatif libre engendré par A, on obtient les dioïdes des polynômes et séries à indéterminées commutatives, que l'on notera respectivement $\mathcal{D}[A]$ et $\mathcal{D}[[A]]$.

1.0.9 Exemple ($\mathbb{N}_{\text{pgcd}}, \mathbb{N}_{\text{ppcm}}$) L'ensemble $\mathbb{N}^* \cup \{\infty\}$, muni du pgcd et du produit est un demi-anneau idempotent (on convient que $\text{pgcd}(x, \infty) = x$ et $x.\infty = \infty$). On notera $\mathbb{N}_{\text{pgcd}}$ cette structure. Si l'on considère les deux lois ppcm et $\times$, il faut adjoindre à $\mathbb{N}^*$ un élément ε vérifiant $\varepsilon \times x = \varepsilon$ et $\varepsilon \oplus x = x$ (et qui n'est donc ni 0 ni ∞), pour obtenir un dioïde. On notera $\mathbb{N}_{\text{ppcm}}$ cette structure.

1.0.10 Exemple (parties convexes de $\mathbb{R}^2$) On considère l'ensemble des parties convexes de $\mathbb{R}^2$, muni des deux opérations suivantes:

$$\begin{aligned} A \oplus B &= \text{conv}(A \cup B) \\ A \otimes B &= A + B \qquad \text{(somme vectorielle)}, \end{aligned}$$

où conv(U) désigne l'enveloppe convexe d'une partie U. On prétend qu'il s'agit d'un dioïde. La seule propriété non triviale à vérifier est la distributivité, i.e.:

$$\mathrm{conv}(A \cup B) + C = \mathrm{conv}[(A + C) \cup (B + C)] \ . \tag{1.0.d}$$

Commençons par noter le fait suivant:

$$V \text{ convexe } \Rightarrow \text{ pour toute partie } U, \mathrm{conv}(U + V) = \mathrm{conv}(U) + V \ . \tag{1.0.e}$$

En effet, conv$(U) + V$ est un convexe contenant $U + V$, donc conv$(U) + V \supset$ conv$(U + V)$. Inversement, tout élément w de conv$(U) + V$ s'écrit $w = \sum_{i=1}^{n} \alpha_i u_i + v$ avec $\alpha_i \geq 0, \sum_{i=1}^{n} \alpha_i = 1, u_i \in U, v \in V$, d'où $w = \sum_{i=1}^{n} \alpha_i (u_i + v) \in \mathrm{conv}(U + V)$, ce qui montre (1.0.e). On a donc $\mathrm{conv}(A \cup B) + C = \mathrm{conv}((A \cup B) + C) = \mathrm{conv}((A + C) \cup (B + C))$, d'où (1.0.d). On notera $\mathrm{conv}\mathcal{P}(\mathbb{R}^2)$ le dioïde des convexes de $\mathbb{R}^2$.

1.0.11 Exemple (convexes compacts) L'ensemble des convexes compacts de $\mathbb{R}^2$ forme un sous-dioïde de $\mathrm{conv}\mathcal{P}(\mathbb{R}^2)$, que l'on notera $\mathrm{conv}\mathcal{P}_c(\mathbb{R}^2)$. Le dioïde $\mathrm{conv}\mathcal{P}_c(\mathbb{R}^2)$ est intègre. Soit en effet l'application *support* définie par

$$\delta_A^\star(p) = \sup_{x \in A} \langle p, x \rangle \qquad \text{pour } p \in \mathbb{R}^2$$

qui, par compacité de A, est finie. On a $\delta_{A+B}^\star = \delta_A^\star + \delta_B^\star$ (vérification immédiate), et l'on rappelle que les convexes fermés sont caractérisés par leur support. Si $A + B = C$, B est l'unique convexe de fonction support $\delta_B^\star = \delta_C^\star - \delta_A^\star$. Il s'ensuit donc que l'application $B \mapsto A + B$ est injective, et donc que $\mathrm{conv}\mathcal{P}_c(\mathbb{R}^2)$ est intègre.

1.0.12 Exemple (Dioïde des relations) Soit E un ensemble et $\mathcal{R}(E)$ l'ensemble des relations sur E. $\mathcal{R}(E)$, muni des deux lois suivantes:

$$R \oplus R' : \quad x\ (R \oplus R')\ y \text{ ssi } x\ R\ y \ \text{ ou } \ x\ R'\ y,$$
$$R \otimes R' : \quad x\ (R \otimes R')\ y \text{ ssi } \exists z \in E\ x\ R\ z \ \text{ et } \ z\ R'\ y$$

est un dioïde.

1.0.13 Avertissement La traduction anglaise de demi-anneau (resp. demi-corps) est "semiring" (resp. "semifield").

1.0.14 Note historique Kuntzmann ainsi que Gondran & Minoux [47], à qui le terme "dioïde" doit sa fortune, appellent en réalité dioïdes les demi-anneaux généraux. A la suite de Cohen, Dubois, Quadrat et Viot [17], nous préférons réserver le terme de dioïde aux demi-anneaux vérifiant $a \oplus a = a$, tout d'abord pour ne pas faire double emploi avec le terme "demi-anneau" ou "semiring", et ensuite parce que l'idempotence permet d'ordonner les dioïdes et produit une théorie spécifique plus riche que celle des demi-anneaux.

2 Dioïdes et structures ordonnées

2.1 L'ordre naturel d'un dioïde

Dans un dioïde $(\mathcal{D}, \oplus, \otimes)$, on définit la relation d'ordre naturelle $\preceq$ par:

$$a \preceq b \Leftrightarrow a \oplus b = b \ . \tag{2.1.a}$$

Cette relation d'ordre est compatible avec les lois de structure de $\mathcal{D}$, i.e.:

$$a \preceq b \Rightarrow a \oplus c \preceq b \oplus c$$
$$a \preceq b \Rightarrow ac \preceq bc \ .$$

$(\mathcal{D}, \preceq)$ est ainsi un demi-treillis dans lequel la borne-sup est donnée par $\oplus$ ($a \oplus b$ est le plus petit majorant de a, b), où ε est le plus petit élément.

2.1.1 Exemple Dans $\mathbb{R}_{\max}$ (cf. 1.0.3), la relation $\preceq$ coïncide avec l'ordre coutumier. Dans $\mathbb{R}_{\min}$ (cf. 1.0.4), on a $x \preceq y$ ssi $\min(x, y) = y$, et donc $\preceq$ est l'ordre dual de l'ordre usuel (par exemple, $2 \succeq 3$).

2.1.2 Remarque Les deux propriétés 1.0.1,(i) et (ii) expriment que $(\mathcal{D}, \otimes)$ est un demi-groupe demi-réticulé.

2.1.3 Définition (Ensemble ordonné complet) *On dit que l'ensemble ordonné $(\mathcal{D}, \preceq)$ est complet si toute partie A de $\mathcal{D}$ admet une borne-sup, que l'on notera indifféremment*

$$\bigvee A \quad \text{ou} \quad \bigvee_{a \in A} a \ .$$

Lorsque $(\mathcal{D}, \vee, \wedge)$ est un treillis, on dira que $\mathcal{D}$ est un treillis complet lorsque toute partie admettra une borne-sup et une borne-inf.

On notera $\top = \bigvee \mathcal{D}$ le plus grand élément de $\mathcal{D}$.

Lorsque qu'il s'agit de l'ordre naturel d'un dioïde, on notera la borne-sup $\bigoplus$ au lieu de $\bigvee$.

2.1.4 Définition (ensembles descendants, idéaux, filtres) *On dira que l'ensemble $S \subset \mathcal{D}$ est descendant*[2] *si $x \in S$ et $y \preceq x$ entraînent $y \in S$. Si en outre, pour tous $a, b \in S$, $a \oplus b \in S$, on dira que S est un idéal. Si S est un idéal pour l'ordre dual, on dira que S est un filtre.*

Etant donné une partie P, on notera

$$\downarrow(P) = \{x \in \mathcal{D} \mid \ \exists p \in P, \ x \preceq p\} = \bigcup_{p \in P} \downarrow(\{p\}) \ .$$

Il s'agit du plus petit ensemble descendant contenant P. Les ensembles descendants de $\mathcal{D}$, muni de l'union et de l'intersection forment clairement un treillis complet.

2.1.5 Treillis des idéaux L'ensemble des idéaux, muni des deux lois

$$I \wedge J = I \cap J, \quad I \vee J = \bigcap_{K \ \text{idéal}, \ K \supset I, J} K \ , \tag{2.1.b}$$

est un treillis complet. On note que pour $x \in \mathcal{D}$, $\downarrow(\{x\})$ est un idéal. Les idéaux de cette forme seront appelés principaux. On les notera plus simplement $\downarrow(x)$.

[2] le terme anglais est "lower set", cf. [43]

2.1.6 Définition (Dioïde complet) *Le dioïde $\mathcal{D}$ est* complet *s'il est complet en tant qu'ensemble ordonné par (2.1.a) et s'il vérifie les deux propriétés suivantes, dites de "distributivité infinie":*

$$\forall A \subset \mathcal{D}, \quad \forall b \in \mathcal{D}, \quad \begin{array}{l} (\bigoplus_{a\in A} a)b = \bigoplus_{a\in A} ab \\ b(\bigoplus_{a\in A} a) = \bigoplus_{a\in A} ba \ . \end{array}$$

Il en résulte immédiatement que

$$(\bigoplus_{a\in A} a)(\bigoplus_{b\in B} b) = \bigoplus_{(a,b)\in A\times B} ab \ . \tag{2.1.c}$$

2.1.7 Exemple (dioïde complété de $\mathbb{R}_{\max}$) $\mathbb{R}\cup\{\pm\infty\}$, muni du max et du $+$, avec la convention $(+\infty)+(-\infty)=-\infty$, est un dioïde complet que l'on notera $\overline{\mathbb{R}}_{\max}$.

2.1.8 Exemple L'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}\cup\{\pm\infty\}$, muni du max point par point et du produit de sup-convolution défini par:

$$(f\otimes g)(t) = \sup_{x\in\mathbb{R}}[f(t-x)+g(x)]$$

(avec $(+\infty)+(-\infty)=-\infty$) est un dioïde complet que l'on notera $\overline{\mathbb{R}}_{\max}^{\mathbb{R}}$. L'élément neutre pour le produit est la fonction e donnée par $e(t)=-\infty$ si $t\neq 0$ et $e(0)=0$.

2.1.9 Exemple (ordre des relations) Pour le dioïde $\mathcal{R}(E)$ des relations sur E défini en 1.0.12, on a $R\preceq R'$ ssi xRy entraîne $xR'y$, i.e. ssi R est plus *fine* que R'.

2.1.10 Remarque Un demi-corps idempotent non trivial n'a pas de plus grand élément, et en particulier n'est pas complet. Soit en effet ∞ plus grand élément d'un demi-corps idempotent $\mathcal{D}$. On a $\infty.\infty \succeq \infty.e = \infty$, et en simplifiant $\infty = e$. Ainsi, tout x non nul vérifie

$$x \preceq e \tag{2.1.d}$$

D'où en passant aux inverses $x^{-1}\succeq e$. L'autre inégalité s'obtient en appliquant (2.1.d) à x^{-1}, d'où $x=e$ et $\mathcal{D}=\{\varepsilon, e\}$.

2.1.11 Intégration idempotente de Maslov On notera, à la suite de Maslov [67],

$$\oint_{i\in I} a_i := \bigoplus_{i\in I} a_i$$

par analogie avec l'intégrale usuelle. On a en particulier la règle de Fubini:

$$\oint_{\cup_{k\in I}\{k\}\times J(k)} a_{ij} = \oint_{i\in I}\oint_{j\in J(i)} a_{ij}$$

qui n'est autre que l'associativité de la borne sup. L'infinie distributivité du produit se réécrit

$$c\otimes\left(\oint_{i\in I} a_i\right) = \oint_{i\in I} c\otimes a_i \ .$$

2.2 Inf-dioïdes

2.2.1 Définition *Le dioïde $\mathcal{D}$ est un* inf-dioïde *si pour tous éléments $a, b \in \mathcal{D}$, a et b admettent une borne-inf pour l'ordre naturel (notée $a \wedge b$).*

En d'autres termes, l'ensemble ordonné sous jacent à un inf-dioïde est un treillis. Les deux faits suivants sont bien classiques:

2.2.2 Proposition *Un demi-corps idempotent est un inf-dioïde.*

Preuve On vérifie en effet que la borne-inf est donnée par $a \wedge b = b(a \oplus b)^{-1}a$. ∎

2.2.3 Proposition *Un dioïde complet est un inf-dioïde.*

Preuve La loi $\wedge$, donnée par

$$a \wedge b = \bigvee \{x \mid x \preceq a \text{ et } x \preceq b\},$$

fait alors de $(\mathcal{D}, \vee, \wedge)$ un treillis complet. ∎

2.2.4 Exemple Le dioïde $\mathbb{B}[X]$ des polynômes à coefficients booléiens en une indéterminée X est un exemple d'inf-dioïde qui n'est ni complet (considérer $\bigoplus_{k \in \mathbb{N}} X^k \notin \mathbb{B}[X]$), ni un demi-corps idempotent (par exemple, $(e \oplus X)(e \oplus X^2) = (e \oplus X)(e \oplus X \oplus X^2)$, ce qui montre que le produit n'est pas simplifiable).

2.2.5 Remarque Dans le cas d'un demi-corps idempotent, on a en outre (cf. [30, 8]) que la borne-inf distribue par rapport au produit:

$$(a \wedge b)c = ac \wedge bc, \quad c(a \wedge b) = ca \wedge cb \ . \tag{2.2.a}$$

Le groupe $(\mathcal{D} \setminus \{\varepsilon\}, \otimes)$ est donc réticulé.

2.2.6 Note Nous avons choisi le terme "inf-dioïde" plutôt que "dioïde réticulé", car on n'exige *pas* que la borne-inf distribue par rapport au produit, ce qui est le cas dans un "demi-groupe réticulé".

2.2.7 Note Le lecteur pourrait se demander pourquoi ci-dessus et dans la suite, on considère des dioïdes non complets, ce qui oblige à introduire la classe des inf-dioïdes et complique légèrement le discours. Il est en fait essentiel pour les développements algébriques ultérieurs de prendre en compte des dioïdes non complets (typiquement des demi-corps). En particulier, les résultats de symétrisation exigent que la structure multiplicative soit "presque" un groupe, ce qui est incompatible avec la complétion.

2.3 Continuité

2.3.1 Définition (Fonctions croissantes continues) *Soit f une application croissante $(E, \leq) \to (F, \leq)$. f est* continue *si pour toute partie $X \subset E$ admettant une borne-sup, on a:*

$$f\Big(\bigvee_{x \in X} x\Big) = \bigvee_{x \in X} f(x) \tag{2.3.a}$$

Pour une application croissante, il est trivial que $f(\bigvee_{x \in X} x) \geq \bigvee_{x \in X} f(x)$. Ainsi, (2.3.a) est équivalente à:

$$f(\bigvee_{x \in X} x) \leq \bigvee_{x \in X} f(x) \ . \tag{2.3.b}$$

2.3.2 Remarque Pour une fonction croissante $\mathbb{R} \to \overline{\mathbb{R}}$, la continuité au sens de 2.3.1 n'est autre que la semi-continuité inférieure usuelle. En effet, pour f croissante, on a

$$\liminf_{x \to x_0} f(x) = \sup_{x \leq x_0} f(x)$$

et donc (2.3.b) est équivalent à $f(x_0) \leq \liminf_{x \to x_0} f(x)$.

2.3.3 Remarque Dans [43], on examine sous quelles conditions la notion de continuité 2.3.1 relève d'une topologie, dite topologie de Scott.

2.3.4 Remarque Les lois de structure d'un dioïde complet sont continues. En effet, la condition d'infinie distributivité (2.1.c) n'est rien d'autre que la continuité du produit. La somme dans un dioïde complet est trivialement continue.

2.3.5 Exemple (Dioïde complet libre à k générateurs) Le dioïde des langages $(\mathcal{P}(A^*), \cup, .)$ sur un alphabet $A = \{a_1, \ldots, a_k\}$ (cf. 1.0.6) est le dioïde complet libre à k générateurs $\alpha_1 = \{a_1\}, \ldots, \alpha_k = \{a_k\}$, i.e. l'unique dioïde complet (à un isomorphisme *continu* près) tel que pour tout dioïde complet $\mathcal{D}'$ et tout k-uplet $(x_1, \ldots, x_k)$, on ait un unique morphisme continu $\phi : \mathcal{P}(A^*) \to \mathcal{D}'$ avec $\phi(\alpha_i) = x_i$. La preuve est analogue à celle de 1.0.7 en remarquant que ϕ est défini par continuité de manière unique pour les langages infinis.

2.3.6 Remarque Le dioïde des séries formelles à coefficients booléiens $\mathbb{B}\langle\langle A \rangle\rangle$ défini en 1.0.8 vérifie la propriété universelle caractéristique du dioïde complet libre énoncée ci-dessus. Il est donc isomorphe à $(\mathcal{P}(A^*), \cup, .)$, l'isomorphisme étant l'application support (cf. 1.0.8).

3 Moduloïdes

3.1 Généralités

3.1.1 Définition (Demi-module, moduloïde) *Soit $\mathcal{D}$ un demi-anneau. On appelle demi-module (à gauche) sur $\mathcal{D}$ un demi-groupe additif $(V, \oplus)$ muni d'une loi de composition externe "." $\mathcal{D} \times V \to V$ vérifiant:*

(i) $(\lambda\mu).u = \lambda.(\mu.u)$

(ii) $(\lambda \oplus \mu).u = \lambda.u \oplus \mu.u$

(iii) $\lambda.(u \oplus v) = \lambda.u \oplus \lambda.v$

(iv) $\varepsilon_{\mathcal{D}}.u = \varepsilon_V$

(v) $e.u = u \quad .$

Un demi-module sur un dioïde est appelé moduloïde.

On notera comme de coutume λu pour $\lambda.u$. On observe que (iv) entraîne $\lambda.\varepsilon_V = \lambda\varepsilon_{\mathcal{D}}.u = \varepsilon_{\mathcal{D}}.u = \varepsilon_V$, pour tout $\lambda \in \mathcal{D}$.

3.1.2 Proposition *L'addition d'un moduloïde est idempotente.*

Preuve $u \oplus u = eu \oplus eu = (e \oplus e)u = eu = u$ ∎

On peut donc ordonner canoniquement un moduloïde par $u \preceq v \Leftrightarrow u \oplus v = v$. Un moduloïde est dit *complet* si l'ensemble ordonné sous-jacent est complet et si en outre les propriétés de distributivité (ii) et (iii) s'étendent aux sommes infinies.

3.1.3 Remarque La condition de distributivité infinie est équivalente à

$$\mathcal{D} \times V \to V, \;\; (\lambda, u) \mapsto \lambda u \;\; \text{continue.}$$

3.1.4 Définition (Application Linéaire) *Soient V, V' deux $\mathcal{D}$-demi-modules, et $f : V \to V'$. L'application f est dite* linéaire à gauche *si*

(i) $f(u \oplus v) = f(u) \oplus f(v)$,

(ii) $f(\lambda u) = \lambda f(u)$.

On notera $\mathsf{L}(V, V')$ l'ensemble de ces applications.

Une application linéaire vérifie donc

$$f(\varepsilon) = \varepsilon \;\;,$$

comme il résulte de (ii) avec $\lambda = \varepsilon$ et u quelconque. L'ensemble des applications linéaires d'un moduloïde V dans lui même, muni de la somme et du produit de composition est un dioïde. On le notera $\mathsf{L}(V)$. Si V est un moduloïde complet, l'ensemble des applications linéaires continues de V dans V est lui même un dioïde complet. On le notera $\mathcal{L}(V)$.

3.1.5 Exemple (Fonctions réelles) L'ensemble des fonctions de $\mathbb{R}$ dans $\mathbb{R} \cup \{-\infty\}$, muni du max point par point et de la loi de composition externe $\mathbb{R}_{\max} \times V \to V$ définie par $\forall t \in \mathbb{R}, \;\; (\lambda u)(t) = \lambda + u(t)$ est un moduloïde sur $\mathbb{R}_{\max}$. On le notera $\mathbb{R}_{\max}^{\mathbb{R}}$.

3.1.6 Exemple (Applications croissantes) L'ensemble des applications croissantes de $\mathbb{R}$ dans $\mathbb{R} \cup \{-\infty\}$ est un sous-moduloïde de $\mathbb{R}_{\max}^{\mathbb{R}}$.

3.1.7 Exemple (Fonctions concaves scs) L'ensemble des fonctions concaves de $\mathbb{R}$ dans $\overline{\mathbb{R}}$ est un sous-moduloïde complet de $\overline{\mathbb{R}}_{\min}^{\mathbb{R}}$ (l'inf de fonctions concaves est concaves, idem pour les fonctions scs).

3.1.8 Familles génératrices, familles libres, bases Etant donnée une famille $\{u_i\}_{i \in I}$ de vecteurs d'un $\mathcal{D}$-moduloïde V, on notera $\mathrm{vect}\langle u_i \rangle_{i \in I}$ le moduloïde des vecteurs combinaisons linéaires d'un nombre fini de u_i. Si $\mathrm{vect}\langle u_i \rangle_{i \in I} = V$, la famille est dite génératrice. Un moduloïde est dit *de type fini* s'il admet une famille génératrice finie. Si un vecteur $v \in \mathrm{vect}\langle u_i \rangle$ s'écrit de manière unique comme $\sum_i \lambda_i u_i$, la famille est dite *libre*. Une famille libre et génératrice est une *base*.

3.1.9 Contre exemple (Moller, [72]). Voici un sous moduloïde de $\mathbb{R}^2_{\max}$ qui n'est pas de type fini:

$$M = \{(x,y) \mid \ x \prec y\} \cup \{(\varepsilon,\varepsilon)\} \ .$$

3.1.10 Contre exemple Soit le sous moduloïde de $\mathbb{B}^2$

$$V = \mathrm{vect}\langle u_1, u_2\rangle \quad \text{où} \quad u_1 = \begin{bmatrix} e \\ e \end{bmatrix}, \quad u_2 = \begin{bmatrix} e \\ \varepsilon \end{bmatrix} \ .$$

La famille $\{u_1, u_2\}$ est génératrice minimale (i.e. toute sous famille stricte engendre un sous moduloïde strict). Cependant, on a $eu_1 \oplus eu_2 = eu_1$, ce qui montre que la famille $\{u_1, u_2\}$ n'est pas libre.

Cet exemple suggère que l'existence de bases est un phénomène "rare" dans les moduloïdes. Cette rareté sera précisée ultérieurement par l'étude des matrices inversibles (cf. §6).

3.2 Familles génératrices minimales

3.2.1 Définition (Redondance) *Le vecteur u_j de la famille $\{u_i\}_{i\in I}$ est dit* redondant *si*

$$u_j \in \mathrm{vect}\langle u_i\rangle_{i\neq j} \ .$$

Une famille dont un vecteur est redondant est dite redondante.

3.2.2 Définition (Base faible) *On appelle base faible de V une famille génératrice minimale.*

Il est clair qu'une famille génératrice est minimale ssi elle est non redondante. En outre, étant donné une famille génératrice *finie*, on obtient une famille génératrice minimale après suppression éventuelle de vecteurs redondants. En résumé:

3.2.3 Observation Tout moduloïde de type fini admet une famille génératrice minimale.

On peut calculer cette famille génératrice minimale pour peu que l'on sache déterminer les vecteurs redondants. Nous aurons besoin pour cela de certains résultats de résiduation, et nous reportons l'étude à la section §5.5 de ce chapitre.

4 Equations implicites linéaires dans les dioïdes complets

4.1 Généralités

Dans les dioïdes complets, les équations linéaires du type $x = ax \oplus b$ se résolvent trivialement:

4.1.1 Proposition *L'inéquation $x \succeq ax \oplus b$ dans un dioïde complet admet une plus petite solution, égale à a^*b, où a^* est définie par:*

$$a^* = \bigoplus_{n\in\mathbb{N}} a^n \ .$$

En outre, $x = a^*b$ réalise l'égalité dans $x \succeq ax \oplus b$.

Preuve On a par une induction immédiate

$$x \succeq (e \oplus a \oplus \ldots \oplus a^n)b \oplus a^{n+1}x, \qquad (4.1.a)$$

d'où $x \succeq (e \oplus a \oplus \ldots \oplus a^n)b$ pour tout n, d'où $x \succeq a^*b$. L'égalité résulte de la propriété de distributivité infinie 2.1.6. ∎

4.1.2 Application L'ensemble des endomorphismes continus d'un moduloïde complet V, muni de la somme et du produit forme un dioïde complet. Soit $f \in \mathcal{L}(V)$. La plus petite solution de

$$g \succeq f \circ g \oplus \mathrm{Id}$$

est donnée par $g = f^*$

4.1.3 Généralisation Soit f un endomorphisme continu d'un moduloïde complet V. Le plus petit vecteur $x \in V$ solution de $x \succeq f(x) \oplus b$ est donné par $x = f^*(b)$ et satisfait l'égalité.

4.1.4 Exemple Soit $f(x) := axb$. Il résulte immédiatement de 4.1.2 que la plus petite solution de $x \succeq axb \oplus c$ est donnée par $x = a^*cb^* = f^*(c)$.

4.1.5 Notation L'opération "plus" dérivée de l'étoile sera utile:

$$a^+ := a \oplus a^2 \oplus \ldots \oplus a^n \oplus \ldots = aa^* = a^*a \ . \qquad (4.1.b)$$

On a

$$e \oplus a^+ = a^* \ . \qquad (4.1.c)$$

Nous établissons ci-après les propriétés de base des opérations étoile et plus.

4.1.6 Proposition *Dans un dioïde complet $\mathcal{D}$, on a:*

(i) $(a^*)^* = a^*$,

(ii) $(a^+)^* = a^*$,

(iii) $(a \oplus b)^* = (a^*b)^*a^*$,

(iv) $(a \oplus b)^* = b^*(ab^*)^*$,

(v) $a^* = a^*a^*$.

(vi) $(ab^*)^+ = a(a \oplus b)^*$

(vii) $(ab^*)^* = e \oplus a(a \oplus b)^*$

En outre, lorsque $\mathcal{D}$ est commutatif:

(viii) $(a \oplus b)^* = a^*b^*$

Preuve (i).$x \succeq ax \oplus e$ entraîne $x \succeq a(ax \oplus e) \oplus e \succeq a^2x \oplus e$ et plus généralement $x \succeq a^nx \oplus e$, soit en sommant $x \succeq a^*x \oplus e$. On en déduit que la plus petite solution de $x \succeq ax \oplus e$, i.e. a^*, est plus grande que la plus petite solution de $x \succeq a^*x \oplus e$, i.e. $(a^*)^*$. Par ailleurs, trivialement, $a^* \preceq (a^*)^*$, d'où l'égalité.

(ii): $a^* \preceq (a^+)^* \preceq (a^*)^* = a^*$ (par (i)).
(iii),(iv): par 4.1.1, les propositions suivantes sont équivalentes:

$$\begin{aligned} x &\succeq (a \oplus b)^* \\ x &\succeq ax \oplus bx \oplus e \\ x &\succeq a^*bx \oplus a^* \\ x &\succeq (a^*b)^*a^* \quad . \end{aligned}$$

La formule (iii) en résulte. (iv) s'obtient dualement en remplaçant $ax \oplus bx$ par $xa \oplus xb$ dans la preuve ci-dessus.
(v): par (iii), $a^* = (a \oplus a)^* = (aa^*)^*a^* = (a^+)^*a^* = a^*a^*$ (par (ii)).
(vi) Via (iv), $a(a \oplus b)^* = ab^*(ab^*)^* = (ab^*)^+$.
(vii): résulte de (vi) et de la formule (4.1.c) ci-dessus.
(viii): On a alors pour $k \geq 1$: $(a^*b)^k = (a^*)^k b^k = a^*b^k$ (par (v)). D'où $(a \oplus b)^* = (a^*b)^*a^* = (e \oplus \bigoplus_{k\geq 1} a^*b^k)a^* = a^* \oplus \bigoplus_{k\geq 1} a^*b^k = a^*b^*$. ■

4.1.7 Exemple Dans $\overline{\mathbb{R}}_{\max}$, on a $a^* = +\infty$ si $a > 0$ et $a^* = 0$ sinon.

4.1.8 Exemple Dans le dioïde des relations défini en 1.0.12, on a $R^* = e \oplus R \oplus R^2 \oplus \ldots$. Il s'agit de la fermeture réflexive transitive de R (i.e. la plus fine relation réflexive et transitive plus grossière que R).

4.1.9 Exemple Soit A un alphabet, et $l \in A$. Dans $\mathcal{P}(A^*)$, on a $\{l\}^* = \{\_, l, ll, lll, \ldots\}$. On observera que la notation A^* pour le monoïde libre formé sur A est consistante (on a $A^* = \{\_\} \cup A \cup A.A \cup \ldots$). A^* s'interprète comme l'ensemble des mots formés sur A, et A^+ comme l'ensemble des mots de longueur au moins 1.

4.2 Equations implicites matricielles et interprétation combinatoire

La Proposition 4.1.1 s'étend au cas matriciel ($A \in \mathcal{D}^{n\times n}$ et $b \in \mathcal{D}^{n\times p}$). Classiquement, le calcul des étoiles de matrices se réduit aux calcul d'étoiles de scalaires via une élimination de Gauss. On a par exemple l'algorithme suivant, fort simple (cf. Backhouse & Carre [4], Gondran & Minoux [47]):

4.2.1 Algorithme (de Jordan) *Soit A une matrice $n \times n$ à coefficients dans un dioïde complet, et $A^{(0)}, \ldots, A^{(n)}$ les matrices définies par:*

$$\begin{aligned} & A^{(0)} = A \\ \text{pour } i,j = 1,\ldots,n \qquad & A^{(k)}_{ij} = A^{(k-1)}_{ij} \oplus A^{(k-1)}_{ik}(A^{(k-1)}_{kk})^* A^{(k-1)}_{kj} . \end{aligned} \tag{4.2.a}$$

On a $A^{(n)} = A^+$.

Le terme $A^{(k-1)}_{kk}$ sera qualifié de k-ième *pivot* par analogie avec l'algorithme de Gauss usuel.

Preuve Soient a_{ij} n^2 lettres. Nous introduisons la matrice générique

$$\mathfrak{A} : \quad \mathfrak{A}_{ij} = a_{ij} \quad .$$

Il suffit de montrer le résultat pour la matrice générique en raisonnant dans le dioïde complet libre $\mathbb{B}\langle\!\langle a_{ij} \rangle\!\rangle$ engendré par les lettres a_{ij}. (cf. 2.3.5). La preuve repose sur l'interprétation des séries en termes d'ensembles de chemins du graphe associé à la matrice $\mathfrak{A}$ (voir aussi [85]).

4.2.2 Définition (Chemin) *On appelle* chemin de longueur k de j à i *un mot de la forme*

$$p = a_{i_1 i_2} a_{i_2 i_3} \dots a_{i_{k-1} i_k}$$

avec[3] $i_i = i$ *et* $i_k = j$.

On dira que le chemin passe éventuellement par I si $i_2, \dots, i_{k-1} \in I$ (mais tous les $i \in I$ ne sont pas forcément atteints). Le coefficient a_{ij} s'interprète comme le chemin de longueur 1 allant de j à i. nous renvoyons le lecteur à [4, 47] pour une preuve algébrique de l'algorithme de Jordan. Nous le déduisons d'une interprétation combinatoire de l'élimination de Gauss, qui nous sera utile dans la suite.

4.2.3 Lemme $\mathfrak{A}^{(k)}_{ij}$ *est égal à la somme des chemins de longueur au moins 1 de j à i passant éventuellement par les sommets* $1, \dots, k$.

Preuve par récurrence. Dans (4.2.a), le second terme $\mathfrak{A}^{(k-1)}_{ik}(\mathfrak{A}^{(k-1)}_{kk})^* \mathfrak{A}^{(k-1)}_{kj}$ s'interprète comme la somme des chemins de j à k puis de k à k, puis de k à i, ces chemins passant par ailleurs éventuellement par $1, \dots, k-1$, soit la somme des chemins de j à i passant au moins une fois par k et éventuellement par $1, \dots, k-1$. Les chemins ne passant pas par k ont été déjà énumérés dans le premier terme de (4.2.a). La récurrence en résulte. ■

Finalement, $\mathfrak{A}^{(n)}_{ij}$ est égal à la somme des chemins de longueur au moins 1 de j à i, i.e. $\mathfrak{A}^{(n)}_{ij} = \mathfrak{A}^{+}_{ij}$. Cela achève la preuve de 4.2.1. ■

On a les deux conséquences immédiates suivantes:

4.2.4 Corollaire *L'étoile du k-ième pivot* $\mathfrak{A}^{(k-1)}_{kk}$ *est égale à la somme des circuits passant par k et éventuellement par les sommets* $1, \dots, k-1$.

4.2.5 Corollaire *La somme des étoiles des pivots est égale à la somme des circuits du graphe. La somme des pivots est supérieure aux circuits élémentaires de longueur au moins 1.*

4.2.6 Exemple (Enumération des chemins) On illustre l'algorithme de Jordan 4.2.1 sur le graphe à 2 sommets représenté sur la Figure 0.1. Soit

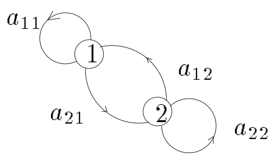

Figure 0.1: Enumération des chemins

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

[3] Noter que le chemin se lit de la droite vers la gauche.

la matrice A^+ représente alors les chemins non triviaux du graphe. On a en appliquant 4.2.1:

$$X = A^+ = \begin{bmatrix} a_{11}^+ \oplus a_{11}^* a_{12}(a_{22} \oplus a_{21}a_{11}^* a_{12})^* a_{21} a_{11}^* & a_{11}^* a_{12}(a_{22} \oplus a_{21} a_{11}^* a_{12})^* \\ (a_{22} \oplus a_{21} a_{11}^* a_{12})^* a_{21} a_{11}^* & (a_{22} \oplus a_{21} a_{11}^* a_{12})^+ \end{bmatrix}, \tag{4.2.b}$$

et en développant A_{22}^+

$$A_{22}^+ = a_{22} \oplus a_{21}a_{12} \oplus a_{21}a_{11}a_{12} \oplus a_{22}a_{21}a_{12} \oplus a_{21}a_{12}a_{22} \oplus \dots$$

ce qui est bien l'ensemble des chemins de 2 à 2.

La notion suivante nous sera utile dans la suite.

4.2.7 Chemins commutatifs Nous dirons que $p \in \mathbb{B}[[a_{ij}]]$ est un chemin commutatif de j à i si c'est l'image commutative d'un chemin $p' \in \mathbb{B}\langle\langle a_{ij} \rangle\rangle$. Définition analogue pour les circuits. Par exemple, $a_{12}a_{13}a_{21}$ est un chemin commutatif de 1 à 3 car $a_{12}a_{21}a_{13}$ est un chemin de 1 à 3. L'intérêt d'un chemin commutatif tient au fait immédiat suivant:

4.2.8 Lemme *Un chemin p commutatif de j à i se factorise sous la forme*

$$p = p' c_1^{n_1} \dots c_l^{n_l} \enspace ,$$

où p est un chemin élémentaire de j à i et les c_i sont des circuits élémentaires.

4.2.9 Exemple Le chemin non commutatif de 7 à 6, $p = a_{61}a_{12}a_{24}a_{41}a_{13}a_{32}a_{21}a_{17}$ peut s'écrire $p = p'c_1c_2$, avec $p' = a_{61}a_{17}$ et $c_1 = a_{12}a_{24}a_{41}$, $c_2 = a_{13}a_{32}a_{21}$ ou bien $p = p'c_1'c_2'$, avec $c_1' = a_{12}a_{21}$ et $c_2' = a_{24}a_{41}a_{13}a_{32}$.

5 Résiduation

Une référence de base est Blyth et Janowitz [11]. Les applications résiduables sont parfois appelées *correspondances de Galois* (cf. Remarque 5.1.9 ci-dessous).

5.1 Applications résiduables

5.1.1 Proposition *Soient E et F deux ensembles ordonnés, et $f : E \to F$ une application croissante. Les deux propositions suivantes sont équivalentes:*

(i) *il existe $g : F \to E$ croissante, telle que $f \circ g \leq \mathrm{Id}_E$ et $g \circ f \geq \mathrm{Id}_F$,*

(ii) *pour tout y appartenant à F, l'ensemble $\{t \in E \mid f(t) \leq y\}$ admet un plus grand élément.*

Preuve Supposons (i). Si $f(t) \leq y$, $t \leq g \circ f(t) \leq g(y)$. De plus, $f \circ g(y) \leq y$ ce qui montre que $g(y)$ est le plus grand élément de $\{t \in E \mid f(t) \leq y\}$. Réciproquement, l'application $g : y \mapsto \max\{t \in E \mid f(t) \leq y\}$ vérifie (i). ∎

5.1.2 Définition *Une application croissante f est dite résiduable si et seulement si elle vérifie les conditions de la proposition 5.1.1. L'application $f^\uparrow$ ainsi définie:*

$$y \mapsto f^\uparrow(y) = \max\{t \in E \mid f(t) \leq y\} \tag{5.1.a}$$

est appelée application résiduée de f.

On note $\mathsf{Res}^{\uparrow}(E,F)$ l'ensemble des applications résiduables de E dans F. On dira que f, croissante, est *dualement résiduable* si elle vérifie les deux conditions équivalentes:

(iii) Il existe $g : E \to F$ croissante, telle que $f \circ g \geq \mathrm{Id}_E$ et $g \circ f \leq \mathrm{Id}_F$

(iv) Pour tout y appartenant à F, l'ensemble $\{t \in E \mid f(t) \geq y\}$ admet un plus petit élément.

L'on notera alors

$$f^{\downarrow}(y) = \min\{t \in E \mid f(t) \geq y\}, \tag{5.1.b}$$

appelée résiduée duale de f. L'ensemble des applications dualement résiduables de E dans F sera noté $\mathsf{Res}^{\downarrow}(E,F)$.

5.1.3 Proposition *L'application $f \mapsto f^{\uparrow}$ est un bijection décroissante de $(\mathsf{Res}^{\uparrow}(E,F),\leq)$ dans $(\mathsf{Res}^{\downarrow}(F,E),\leq)$.*

Preuve En comparant (i) et (iii), il est clair que f est la résiduée duale de $f^{\uparrow}$. ∎

Voici quelques exemples bien connus d'applications résiduées:

5.1.4 Exemple (image réciproque) Etant donné une application $f : A \to B$, l'application associée $\varphi_f : (\mathcal{P}(A),\subset) \to (\mathcal{P}(B),\subset), \varphi_f(X) = f(X)$ est résiduable. On a $\varphi_f^{\uparrow}(Y) = f^{-1}(Y)$ (image réciproque de Y par f).

5.1.5 Exemple (conjuguée convexe) La transformée de Fenchel

$$\mathcal{F} : \left((\mathbb{R}\cup\{\pm\infty\})^{\mathbb{R}},\geq\right) \to \left((\mathbb{R}\cup\{\pm\infty\})^{\mathbb{R}},\leq\right), \mathcal{F}f(p) = \sup_{x\in\mathbb{R}}[px - f(x)],$$

est résiduable (noter le renversement de l'ordre entre les ensembles de départ et d'arrivée), et l'on a $\mathcal{F}^{\uparrow} = \mathcal{F}$.

5.1.6 Exemple (partie entière) L'injection canonique $(\mathbb{Z},\leq) \to (\mathbb{R},\leq)$ est résiduable. Elle admet pour résiduée l'application “partie entière”.

5.1.7 Exemple (orthogonal) Munissons $\mathbb{R}^n$ du produit scalaire usuel. L'application

$$(\mathcal{P}(\mathbb{R}^n),\subset) \to (\mathcal{P}(\mathbb{R}^n),\supset), \quad X \mapsto X^{\perp} = \{y \in \mathbb{R}^n \mid \forall x \in X,\ x.y = 0\}$$

est résiduable.

Un certain nombre de propriétés s'établissent immédiatement:

5.1.8 Proposition *Pour toutes $f, f_i, g \in \mathsf{Res}^{\uparrow}(E,F)$, on a:*

(i) $f \circ f^{\uparrow} \circ f = f$

(ii) $f^{\uparrow} \circ f \circ f^{\uparrow} = f^{\uparrow}$

(iii) $(f \circ g)^{\uparrow} = g^{\uparrow} \circ f^{\uparrow}$

(iv) $(f \vee g)^{\uparrow} = f^{\uparrow} \wedge g^{\uparrow}$.

(v) *Si E et F sont des treillis complets, on a $(\bigvee_i f_i)^{\uparrow} = \bigwedge_i f_i^{\uparrow}$.*

Preuve (i): $f = f \circ \mathrm{Id}_E \leq f \circ (f^{\uparrow} \circ f) = (f \circ f^{\uparrow}) \circ f \leq \mathrm{Id}_F \circ f = f$. Démonstration analogue pour (ii).
(iii): $(f \circ g) \circ (g^{\uparrow} \circ f^{\uparrow}) = f \circ (g \circ g^{\uparrow}) \circ f^{\uparrow} \leq f \circ \mathrm{Id} \circ f^{\uparrow} \leq \mathrm{Id}$. L'autre égalité de 5.1.1,(i) se montre de manière analogue.
(iv): on décompose $t \mapsto f(t) \vee g(t)$ comme le produit des applications suivantes:

$$\begin{array}{lll} E \overset{\varphi_1}{\rightarrow} E^2 & E^2 \overset{\varphi_2}{\rightarrow} F^2 & F^2 \overset{\varphi_3}{\rightarrow} F \\ t \mapsto (t,t) & (u,v) \mapsto (f(u), g(v)) & (x,y) \mapsto x \vee y \end{array}$$

et l'on applique (iii) en remarquant que les applications résiduées associées à cette décomposition sont données par:$\varphi_1^{\uparrow}((x',y')) = x' \wedge y'$, $\varphi_2^{\uparrow}(u',v') = (f^{\uparrow}(u'), g^{\uparrow}(v'))$, $\varphi_2^{\uparrow}(t') = (t',t')$. On a ainsi: $(f \vee g)^{\uparrow} = (\varphi_3 \circ \varphi_2 \circ \varphi_1)^{\uparrow} = \varphi_1^{\uparrow} \circ \varphi_2^{\uparrow} \circ \varphi_3^{\uparrow} = f^{\uparrow} \wedge g^{\uparrow}$. Preuve identique pour (v). ∎

5.1.9 Remarque Il faut bien noter ici le renversement de l'ordre entre les ensembles de départ et d'arrivée dans 5.1.7. Certains auteurs [43] appellent correspondances de Galois les applications résiduables générales, d'autres plus classiques, comme Ore [78], réservent cette dénomination à la donnée de deux applications décroissantes $f : E \to F$ et $g : F \to E$ telles que $f \circ g \geq \mathrm{Id}$ et $g \circ f \geq \mathrm{Id}$, ce qui est une généralisation immédiate de la correspondance de Galois usuelle [90]. La notion de correspondance de Galois au sens de Ore et la notion d'application résiduable coïncident donc à un renversement de l'ordre près sur l'un des deux ensembles. L'intérêt de ce renversement est manifeste dans la formule (iii) ci-dessus: la composée de deux applications croissantes est croissante, et l'on peut donc composer les applications résiduables, ce qui n'est pas le cas pour des correspondances de Galois.

5.1.10 Proposition *Soient $(E, \leq)$ et $(F, \leq)$ deux ensembles ordonnés complets de plus petits éléments respectifs ε_E et ε_F. Une application croissante $f : (E, \leq) \to (F, \leq)$ est résiduable si et seulement f est continue et $f(\varepsilon_E) = \varepsilon_F$.*

Preuve Si f est résiduable, l'ensemble $\{x \mid f(x) \leq \varepsilon\}$ admet un plus grand élément x_0 et par croissance de f, $f(\varepsilon) \leq f(x_0) \leq \varepsilon$. L'autre inégalité est triviale. Montrons que f est alors continue. On a pour toute partie X de E $f(\bigvee_{x \in X} x) \geq \bigvee_{x \in X} f(x)$ (par croissance de f). En outre:

$$f(\bigvee_{x \in X} x) \leq f(\bigvee_{x \in X} f^{\uparrow} \circ f(x)) \leq f \circ f^{\uparrow}(\bigvee_{x \in X} f(x)) \leq \bigvee_{x \in X} f(x),$$

ce qui montre que f est continue. Réciproquement, si $f(\varepsilon) = \varepsilon$, pour tout $y \in F$, l'ensemble $X = \{x \mid f(x) \leq y\}$ est non vide. En outre, par continuité de f, $f(\bigvee_{x \in X} x) = \bigvee_{x \in X} f(x)$ et donc X admet un plus grand élément, ce qui satisfait la condition 5.1.1,(ii). ∎

5.1.11 Définition *On appelle fermeture une application croissante $\phi : E \to E$, telle que $\phi \circ \phi = \phi$ et $\phi \geq \mathrm{Id}$.*

5.1.12 Proposition *Une fermeture résiduable ϕ vérifie* (i)*: $\phi = \phi^{\uparrow} \circ \phi$ et* (ii)*: $\phi = \phi \circ \phi^{\uparrow}$.*

Preuve $\phi = \mathrm{Id} \circ \phi \geq \phi \circ \phi^{\uparrow} \circ \phi \geq \phi^{\uparrow} \circ \phi = \phi^{\uparrow} \circ \phi \circ \phi \geq \mathrm{Id} \circ \phi$. Preuve duale pour (ii). ∎

5.1.13 Définition (Fermés) *Si f est résiduable, $f^{\uparrow} \circ f$ est une fermeture, et l'on appelle* fermés *les éléments de la forme $f^{\uparrow} \circ f(x)$.*

On définit de manière analogue une fermeture duale, et l'on constate que f est une bijection de l'ensemble des fermés sur l'ensemble des fermés duaux.

5.1.14 Exemple Pour les exemples déjà traités, les fermés sont respectivement 5.1.5: les fonctions convexes sci ne prenant jamais la valeur $-\infty$ ou la prenant identiquement (cf. [2]), 5.1.6: les nombres entiers, 5.1.7: les sous espaces vectoriels de $\mathbb{R}^n$.

5.1.15 Lemme (de projection) *Soit E un ensemble ordonné complet et F un sous ensemble complet de E contenant l'élément minimal de E, ε. L'injection $\imath\ :\quad F\ \rightarrow\ E$ est résiduable. L'application résiduée $\mathsf{pr}_F = \imath^\uparrow$ vérifie:*

(i) $\mathsf{pr}_F \circ \mathsf{pr}_F = \mathsf{pr}_F$,

(ii) $\mathsf{pr}_F \leq \mathrm{Id}_E$,

(iii) $x \in F \Leftrightarrow \mathsf{pr}_F(x) = x$.

Preuve La résiduabilité de $\imath$ résulte de 5.1.10. (i): $\imath^\uparrow \circ \imath^\uparrow = (\imath \circ \imath)^\uparrow = \imath^\uparrow$. (ii): $\mathsf{pr}_F = \imath \circ \mathsf{pr}_F = \imath \circ \imath^\uparrow \leq \mathrm{Id}$. (iii): si $x \in F$, alors $x = \imath(x)$, donc $\mathsf{pr}_F(x) = \mathsf{pr}_F \circ \imath(x) \geq x$. L'autre inégalité est donnée par (ii). La réciproque est triviale. ∎

Les propriétés (i) et (ii) affirment que pr_F est une fermeture duale, la propriété (iii) affirme que les fermés duaux sont les éléments de F.

5.1.16 Exemple Soit $E = \mathbb{R}^{\overline{\mathbb{R}}}$, $F = \mathsf{Croiss}(\mathbb{R}, \overline{\mathbb{R}})$ sous ensemble complet des fonctions croissantes. Par application de 5.1.15 au sous ensemble complet des fonctions croissantes, pour tout $u \in \mathbb{R}^{\overline{\mathbb{R}}}$, Il existe une plus grande fonction croissante $\overline{u}$ plus petite que u. On montrera en V,3.3.1 que $\overline{u}$ est donnée par

$$\overline{u}(t) = \inf_{\tau \geq t} u(\tau),$$

ce qui se voit aussi de manière élémentaire.

5.1.17 Exemple En appliquant le dual de 5.1.15 à l'exemple précédent, on a l'existence d'une plus petite fonction croissante $\underline{u}$ plus grande que u, donnée par

$$\underline{u}(t) = \sup_{\tau \leq t} u(\tau) \quad .$$

5.2 Dioïdes additivement résidués

On étudie maintenant l'équation $a \oplus x = b$ dans un dioïde. Si $a \succ b$, on a $a \oplus x \succeq a \succ b$ et donc l'équation $a \oplus x = b$ n'a pas de solution. Cependant, l'inéquation $a \oplus x \succeq b$ admet toujours la solution triviale $x = b$. On est ainsi conduit à considérer les inéquations de type (0.0.b).

5.2.1 Définition *Le dioïde $\mathcal{D}$ est* additivement résidué *si pour tout $a \in \mathcal{D}$, l'application $\tau_a : x \mapsto x \oplus a$ est dualement résiduable.*

En d'autres termes, $\mathcal{D}$ est additivement résidué si pour tous a et $b \in \mathcal{D}$, l'inéquation

$$a \oplus x \succeq b \tag{5.2.a}$$

admet une plus petite solution. On notera $b \boxminus a (= \tau_a^\downarrow(b))$ cette plus petite solution, et on lira "b moins-résidué a".

5.2.2 Définition *$\mathcal{D}$ est un dioïde* inf-complet distributif *si et seulement si:*

(i) *toute partie X de $\mathcal{D}$ admet une borne-inf pour l'ordre naturel,*

(ii) $(\bigwedge_{x\in X} x)\oplus y = \bigwedge_{x\in X}(x\oplus y)$

5.2.3 Proposition *Un dioïde inf-complet distributif est additivement résidué.*

Preuve On note que $b \in \{x \mid \tau_a(x)\succeq b\}\neq\emptyset$. Cet ensemble admet un plus petit élément car τ_a est dualement continue. ∎

5.2.4 Remarque Le treillis sous-jacent à un dioïde inf-complet distributif n'est autre que le dual d'une "algèbre complète de Heyting" ([43], Chapitre 0).

Les propriétés principales de l'opération moins-résidué sont:

5.2.5 Proposition *Pour tout $u, v, w \in \mathcal{D}$ ($\mathcal{D}$ additivement résidué), on a*

(i) $x\mapsto x\boxminus u$ *croissante*

(ii) $x\mapsto u\boxminus x$ *décroissante*

(iii) $u\boxminus u=\varepsilon$

(iv) $(u\boxminus v)\boxminus w = u\boxminus(v\oplus w)$

(v) $(u\oplus v)\boxminus w=(u\boxminus w)\oplus(v\boxminus w)$

(vi) $u\oplus v=(u\boxminus v)\oplus v$

(vii) $(u\boxminus v)w\succeq uw\boxminus vw$ *(égalité si w inversible)*

(viii) $u\boxminus(u\boxminus v)\preceq v$.

En outre, lorsque $\mathcal{D}$ est inf-complet distributif:

(ix) $w\boxminus(u\wedge v)=(w\boxminus u)\oplus(w\boxminus v)$

(x) $u=(u\boxminus v)\oplus(u\wedge v)$.

Preuve : (i),(ii),(iii): immédiates.
(iv) se réécrit $\tau_w^{\downarrow}[\tau_v^{\downarrow}(u)]=(\tau_v\circ\tau_w)^{\downarrow}(u)$, qui n'est autre que 5.1.8,(iii).
(v): exprime que $\tau_w^{\downarrow}$ est un $\oplus$-morphisme, ce qui est vrai, car $\tau_w^{\downarrow}$ est résiduable, donc continue (cf. 5.1.10).
(vi): provient de ce que τ_a est une fermeture, $\tau_a\circ\tau_a=\tau_a$ et $\tau_a\geq \mathrm{Id}$ (cf. 5.1.12).
(vii): résulte de ce que $vw\oplus(u\boxminus v)w=(v\oplus(u\boxminus v))w\succeq uw$. En obtient l'égalité en notant que $(uw\boxminus vw)w^{-1}\succeq u\boxminus v$ lorsque w est inversible.
(viii): résulte de $(u\boxminus v)\oplus v\succeq u$.
(ix): si la borne-inf distribue par rapport au $\oplus$, on a $\tau_{u\wedge v}=\tau_u\wedge\tau_v$, et par le dual de 5.1.8,(iv), on a $\tau_{u\wedge v}^{\downarrow}=\tau_u^{\downarrow}\oplus\tau_v^{\downarrow}$, soit (ix).
(x): ce fait est spécifique à l'opération $\boxminus$. On a $(u\boxminus v)\oplus(u\wedge v)=((u\boxminus v)\oplus u)\wedge((u\boxminus v)\oplus v)=u\wedge(u\oplus v)=u$. ∎

5.2.6 Exemple Le dioïde des parties de $\mathbb{R}$ munies de l'union et de la somme vectorielle est additivement résidué, et $A\boxminus B=A\setminus B$ (différence ensembliste). On a $\mathbb{R}^+\boxminus\{0\}=\mathbb{R}^{+*}$ mais $(\mathbb{R}^+ +\mathbb{R})\boxminus(\{0\}+\mathbb{R})=\mathbb{R}\boxminus\mathbb{R}=\emptyset$, ce qui montre que l'inégalité dans 5.2.5,(vii) peut être stricte.

5.2.7 Exemple Dans $\mathbb{R}_{\max}$, on a $x \boxminus y = \varepsilon$ si $x \leq y$ et $x \boxminus y = x$ sinon.

5.2.8 Contre exemple Le dioïde des parties compactes convexes de $\mathbb{R}^2$ (cf. 1.0.11) n'est ni inf-complet distributif, ni additivement résidué. On a

$$\mathrm{conv}((A \cap B) \cup C) \subset \mathrm{conv}(A \cup C) \cap \mathrm{conv}(B \cup C), \text{ i.e. } (A \cap B) \oplus C \subset (A \oplus C) \cap (B \oplus C) \ ,$$

mais l'égalité est en général fausse (même en dimension 1, considérer dans $\mathbb{R}$ les parties $A = \{1\}, B = \{2\}, C = \{0\}$), de sorte que la propriété de distributivité 5.2.2 est déjà en défaut pour des inf finis. Sur la Figure 0.2, on a représenté deux élément minimaux non comparables X_0 et X_1 de l'ensemble des solutions de $X \oplus B \supset A$.

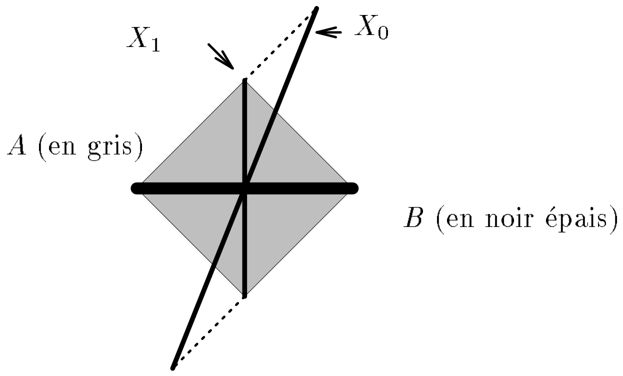

Figure 0.2: Un dioïde non additivement résidué

5.3 Dioïdes multiplicativement résidués

On considère maintenant l'équation $ax = b$. Dans la mesure où l'ensemble des sous solutions est non vide (il contient ε), on introduit naturellement l'inéquation (0.0.c).

5.3.1 Définition *Le dioïde $\mathcal{D}$ est* multiplicativement résidué *si pour tout $a \in \mathcal{D}$, les homothéties à gauche et à droite, respectivement $\lambda_a : x \mapsto ax$ et $\rho_a : x \mapsto xa$, sont résiduables.*

On notera

$$a \backslash x = \lambda_a^{\sharp}(x) = \max\{x \mid ax \preceq b\}$$
$$x / a = \rho_a^{\sharp}(x) = \max\{x \mid xa \preceq b\} \ .$$

5.3.2 Proposition *Un dioïde complet est multiplicativement résidué.*

Preuve résulte immédiatement de 5.1.10. ∎

Les propriétés suivantes sont élémentaires:

5.3.3 Proposition *Pour tout $(u, v, w) \in \mathcal{D}^3$, ($\mathcal{D}$ dioïde multiplicativement résidué), on a*

(i) $x \mapsto u \backslash x$ *croissante*

(ii) $x \mapsto x \backslash u$ *décroissante*

(iii) *si u inversible,* $u\backslash v = u^{-1}v$

(iv) $w\backslash(v\backslash u) = (vw)\backslash u$

(v) $(u\backslash v)/w = u\backslash(v/w)$.

(vi) $(u\backslash v)w \preceq u\backslash(vw)$ *(égalité si w inversible)*

(vii) $w\backslash(u \oplus v) \succeq w\backslash u \oplus w\backslash v$ *(égalité si w inversible)*

(viii) $(v/w)\backslash u \succeq w(v/u)$ *(égalité si w inversible).*

En outre, lorsque $\mathcal{D}$ est un inf-dioïde:

(ix) $w\backslash(u \wedge v) = w\backslash u \wedge w\backslash v$ *et* $w\backslash(\bigwedge_i u_i) = \bigwedge_i w\backslash u_i$ *pour une famille infinie* $\{u_i\}$ *si $\mathcal{D}$ est complet,*

(x) $(u \oplus v)\backslash w = (u\backslash w) \wedge (v\backslash w)$ *et* $(\bigoplus_i u_i)\backslash w = \bigwedge_i(u_i\backslash w)$ *pour une famille infinie* $\{u_i\}$ *si $\mathcal{D}$ est complet,*

(xi) $(u \wedge v)\backslash w \succeq u\backslash w \oplus v\backslash w$

Formulations duales pour les quotients à droite.

Preuve (i),(ii),(iii): immédiates.
(iv): résulte de 5.1.8,(iii).
(v): se réécrit $\lambda_u^{\uparrow}\circ\rho_w^{\uparrow}(v) = \rho_w^{\uparrow}\circ\lambda_u^{\uparrow}(v)$. Or $\lambda_u\circ\rho_w = \rho_w\circ\lambda_u$, d'où par 5.1.8,(iii), $\rho_w^{\uparrow}\circ\lambda_u^{\uparrow} = \lambda_u^{\uparrow}\circ\rho_w^{\uparrow}$.
(vi): on a $u(u\backslash v)w \preceq vw$, d'où $(u\backslash v)w \preceq u\backslash(vw)$. Si w est inversible, $(u\backslash v)w \succeq (u\backslash(vww^{-1}))w \succeq (u\backslash vw)$, d'où l'égalité.
(vii): argument analogue pour l'inégalité. L'égalité résulte de (iii).
(viii): on a $(v/w)w(v\backslash u) \preceq v(v\backslash u) \preceq u$, d'où l'inégalité. Si w est inversible, on a:

$$\begin{aligned}(v/w)\backslash u &= (vw^{-1})\backslash u && \text{(dual de (iii))}\\ &= w^{-1}\backslash(v\backslash u) && \text{(via (iv))}\\ &= w(v\backslash u) && \text{(via (iii)).}\end{aligned}$$

(ix): l'application $\lambda_w^{\uparrow}$ est dualement résiduable, donc dualement continue (5.1.10).
(x): résulte de 5.1.8,(iv),(v).
(xi): clair. ∎

5.3.4 Exemple Le dioïde $\mathbb{Q} \cup \{\pm\infty\}$, muni du max et du $+$, est un inf-dioïde additivement et multiplicativement résidué, mais n'est pas complet.

5.3.5 Exemple Dans $\overline{\mathbb{R}}_{\max}$, le quotient est donné par:

$$\begin{aligned}a\backslash b &= b - a && \text{si } a \text{ et } b \text{ sont finis}\\ a\backslash(+\infty) &= (+\infty) && \text{pour tout } a\\ a\backslash\varepsilon &= \varepsilon && \text{pour tout } a \text{ fini}\\ \varepsilon\backslash a &= (+\infty) && \text{pour tout } a\\ (+\infty)\backslash a &= \varepsilon && \text{pour } a \neq (+\infty).\end{aligned}$$

Il faut bien voir que $(+\infty) \otimes \varepsilon =$"$(+\infty) + (-\infty)$"$= \varepsilon = -\infty$ alors que $\varepsilon/\varepsilon =$"$-\infty - (-\infty)$"$= +\infty$, de sorte que la notation "$a - b$" est ambiguë pour des valeurs infinies des paramètres.

5.4 Résiduation matricielle

Le résultat suivant est du à Blyth [10]:

5.4.1 Proposition *Si $\mathcal{D}$ est un inf-dioïde multiplicativement résidué et $A \in \mathcal{D}^{n\times p}$ alors les applications $\lambda_A : \mathcal{D}^{p\times k} \to \mathcal{D}^{n\times k}$, $X \mapsto AX$ et $\rho_A : \mathcal{D}^{q\times n} \to \mathcal{D}^{q\times p}$, $X \mapsto XA$, sont résiduables, et l'on a:*

$$(\lambda_A^{\natural}(B))_{ij} = \bigwedge_{l=1}^{k} A_{li}\backslash B_{lj} \tag{5.4.a}$$

$$(\rho_A^{\natural}(B))_{ij} = \bigwedge_{l=1}^{q} B_{il}/A_{jl} \ . \tag{5.4.b}$$

Preuve Les propositions suivantes sont équivalentes:

$$\begin{gathered} AX \preceq B \\ \forall i,j, \quad \bigoplus_k A_{ik}X_{kj} \preceq B_{ij} \\ \forall i,j,k, \quad A_{ik}X_{kj} \preceq B_{ij} \\ \forall i,j,k, \quad X_{kj} \preceq A_{ik}\backslash B_{ij} \\ \forall j,k, \quad X_{kj} \preceq \bigwedge_i A_{ik}\backslash B_{ij} \ . \end{gathered}$$

D'où (5.4.a). ∎

L'on notera $A\backslash B$ pour $\lambda_A^{\natural}(B)$ et B/A pour $\rho_A^{\natural}(B)$. L'on vérifie que le formulaire 5.3.3 s'étend aux cas matriciel pourvu que les dimensions des matrices soient compatibles.

5.4.2 Remarque On notera que $A\backslash B$ a la même dimension que $A^{\mathrm{T}}B$ et que B/A a la même dimension que BA^{T}.

5.4.3 Exemple Dans $\mathbb{N}_{\mathrm{ppcm}}$ (cf 1.0.9), on considère le système d'inéquations:

$$\begin{cases} \mathrm{ppcm}(2x_1, 3x_2) \leq 12 \\ \mathrm{ppcm}(5x_1, 2^2x_2) \leq 240, \end{cases} \tag{5.4.c}$$

i.e.:

$$\begin{bmatrix} 2 & 3 \\ 5 & 2^2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \preceq \begin{bmatrix} 2^2 \times 3 \\ 2^4 \times 3 \times 5 \end{bmatrix} = \begin{bmatrix} 12 \\ 240 \end{bmatrix}. \tag{5.4.d}$$

On a par application de (5.4.a):

$$\begin{gathered} x_1 = (2^2 \times 3)/2 \wedge (2^4 \times 3 \times 5)/5 = 2 \times 3 = 6 \\ x_2 = (2^2 \times 3)/3 \wedge (2^4 \times 3 \times 5)/2^2 = 2^2 = 4. \end{gathered}$$

On vérifie que $[x_1, x_2]^{\mathrm{T}}$ est solution de (5.4.d) (et satisfait même l'égalité).

5.4.4 Cas des demi-corps idempotents On a vu en 2.1.10 qu'un demi-corps idempotent non trivial $\mathcal{D}$ n'admettait pas de plus grand élément. En conséquence, l'inéquation scalaire $\varepsilon.x \preceq \varepsilon$ n'admet pas de solution maximale, et $\mathcal{D}$ n'est pas multiplicativement résidué. Cependant, les homothéties $\lambda_a : x \mapsto ax$ non triviales (i.e. $a \neq \varepsilon$) sont résiduées, et l'on a $\lambda_a^{\natural}(b) = a^{-1}b$. Dans le cas matriciel, les homothéties non dégénérées s'avèrent également résiduables, et l'on a l'extension suivante de 5.4.1:

5.4.5 Proposition *Soit $\mathcal{D}$ un demi-corps idempotent, $A \in \mathcal{D}^{n\times p}$. L'application $\lambda_A : \mathcal{D}^{p\times k} \to \mathcal{D}^{n\times k}, X \mapsto AX$ est résiduable si et seulement si A n'a pas de colonne nulle. $A\backslash B$ est donné par la formule (5.4.a), où l'inf est restreint aux l tels que $A_{li} \neq \varepsilon$.*

5.4.6 Autre point de vue On retrouve 5.4.5 en adjoignant au demi-corps idempotent $\mathcal{D}$ un élément ∞ vérifiant $x \oplus \infty = \infty$ et $x \otimes \infty = \infty \otimes x = \infty$ pour $x \neq \varepsilon$. On constate que le dioïde $\mathcal{D} \cup \{\infty\}$ ainsi obtenu est un inf-dioïde multiplicativement résidué, dans lequel la théorie précédente s'applique.

Le résultat suivant est une généralisation immédiate de 5.4.1 en dimension infinie.

5.4.7 Quotient résidé du produit de sup-convolution Dans $\overline{\mathbb{R}}_{\max}^{\mathbb{R}}$ (cf.2.1.8), l'opération résiduée du produit de sup-convolution est donné par

$$(f\backslash g)(x) = \bigwedge_{t\in\mathbb{R}} [f(t-x)\backslash g(t)] \tag{5.4.e}$$

où $\backslash$ dans le membre de droite dénote le quotient de $\overline{\mathbb{R}}_{\max}$. Pour des valeurs finies de f et g, on a avec des notations plus familières:

$$(f\backslash g)(x) = \inf_{t\in\mathbb{R}} [-f(t-x) + g(t)] \ . \tag{5.4.f}$$

5.5 Caractérisation des familles génératrices minimales

On examine ici comment, étant donné un moduloïde de type fini, on obtient une famille génératrice minimale.

5.5.1 Hypothèse *$\mathcal{D}$ est un dioïde additivement résidué tel que les homothéties de rapport non nul soient résiduables, et:*

(i) $\forall u, \lambda \in \mathcal{D},\ \lambda \prec e \Rightarrow u \boxminus \lambda u = u$,

(ii) $\forall u \neq \varepsilon,\ u/u = e$.

En particulier, un dioïde intègre (cf. §1,(1.0.b)) totalement ordonné vérifie l'hypothèse 5.5.1(i) et vérifie (ii) dès que u/u est bien défini. On verra plus loin que le dioïde $\mathbb{R}_{\max}[X]$ vérifie également ces hypothèses.

5.5.2 Lemme *Sous l'hypothèse 5.5.1, on a:*

(i) $u \neq \varepsilon$ *et* $u = \alpha u \ \Rightarrow\ \alpha = e$,

(ii) $u_1 \oplus \ldots \oplus u_n = e \ \Rightarrow\ \exists i \in \{1,\ldots,n\},\ u_i = e$,

(iii) $\alpha \prec e$ *et* $u = \alpha u \oplus v$ *entraîne* $u = v$.

Preuve (i): On a $e = u/u = (\alpha u)/u \succeq \alpha(u/u) = \alpha$. Si $\alpha \prec e$, on a d'après 5.5.1,(i) $u = \alpha u \Rightarrow u \boxminus (\alpha u) = u = (\alpha u) \boxminus (\alpha u) = \varepsilon$: absurde.
(ii): On a si $\forall i, u_i \prec e$, $e = e \boxminus u_1 = (u_2 \boxminus u_1) \oplus \ldots \oplus (u_n \boxminus u_n)$, comme $u_i \boxminus u_1 \preceq u_i \prec e$, on obtient après une récurrence immédiate une absurdité.
(iii): Trivialement, $u \succeq v$. On a d'après l'hypothèse 5.5.1,(i), $u = u \boxminus (\alpha u) = (\alpha u \oplus v) \boxminus (\alpha u) = [(\alpha u) \boxminus (\alpha u)] \oplus [v \boxminus (\alpha u)] = \varepsilon \oplus [v \boxminus (\alpha u)] \preceq v$. ∎

Le résultat suivant est du à Moller [72] et Wagneur [97, 99], à un raffinement près des hypothèses.

5.5.3 Théorème *Soit L un ensemble et V un sous moduloïde de type fini de $\mathcal{D}^L$. Sous l'hypothèse 5.5.1, deux familles génératrices minimales $\{u_i\}_{i\in I}$ et $\{v_j\}_{j\in J}$ de V sont reliées de la manière suivante:*

$$\exists \lambda \in (\mathcal{D}\setminus\{\varepsilon\})^I,\ \exists\sigma \ \text{ bijection } I\to J,\quad \forall i\in I,\quad v_i=\lambda_i v_{\sigma(i)}\ .$$

En outre, les scalaires λ_i sont inversibles dans $\mathcal{D}$.

5.5.4 Définition (Dimension faible) *Sous l'hypothèse 5.5.1, on appellera* dimension faible *d'un sous-moduloïde V de type fini le cardinal d'une famille génératrice minimale de V. Lorsque V n'est pas de type fini, on le dira de dimension faible infinie.*

Le Théorème 5.5.3 affirme "l'unicité" de la base faible (à l'ordre des vecteurs de bases et à une "dilatation" près de ceux-ci).

Preuve Les familles $\{u_i\}$ et $\{v_j\}$ étant génératrices, on a des relations de la forme:

$$u_i=\bigoplus_{j\in J}\lambda_{ij}v_j,\quad v_j=\bigoplus_{k\in I}\mu_{jk}u_k\ .$$

En remplaçant v_j dans le premier membre, on obtient

$$u_i=\bigoplus_{j\in J,\,k\in I}\lambda_{ij}\mu_{jk}u_k\ . \tag{5.5.a}$$

En projetant (5.5.a) sur une coordonnée non nulle de u_i, on obtient

$$u_i^l\succeq\bigoplus_{j\in J,}\lambda_{ij}\mu_{ji}u_i^l\ .$$

Il résulte de l'hypothèse 5.5.1,(ii) que $\bigoplus_{j\in J,}\lambda_{ij}\mu_{ji}\preceq u_i^l/u_i^l=e$. On obtient l'égalité par application du Lemme 5.5.2,(iii): on contredirait la non redondance de la famille. On a donc

$$\bigoplus_{j\in J,}\lambda_{ij}\mu_{ji}=e\ .$$

D'après le Lemme 5.5.2,(ii), il existe $j_i\in J$ tel que $\lambda_{ij_i}\mu_{j_ii}=e$, d'où

$$u_i\succeq\lambda_{ij_i}v_{j_i}\succeq\lambda_{ij_i}\mu_{j_ii}u_i=u_i\ ,$$

et l'égalité $u_i=\lambda_{ij_i}v_{j_i}$, ainsi que par 5.5.2,(i), $\lambda_{ij_i}\mu_{j_ii}=e$. L'application $i\mapsto\sigma(i):=j_i$ est clairement une bijection de I dans J. ∎

5.5.5 Algorithme *Soit $V=\mathrm{vect}\langle u_i\rangle_{1\leq i\leq p}$ un sous moduloïde de $\mathcal{D}^n$. Via 5.5.3, on obtient une famille génératrice minimale de V de la manière suivante: 1/ si aucun vecteur n'est redondant, $\{u_i\}$ est une base faible de V. 2/ si l'on trouve un vecteur redondant, on le supprime de la famille $\{u_i\}$, et on recommence en 1/.*

Ainsi, la détermination d'une famille génératrice minimale exige seulement de savoir vérifier la redondance d'un vecteur, ou plus généralement de déterminer si un vecteur v appartient à $\mathrm{vect}\langle u_j\rangle_{j\in J}$. Soit U la matrice obtenue en concaténant les vecteurs u_j. On a

$$v\in\mathrm{vect}\langle u_j\rangle\quad\Leftrightarrow\quad v=U(U\backslash v)\ .$$

Ainsi, le problème est ramené au calcul du quotient résidué d'un vecteur par une matrice. Quitte à supprimer les vecteurs nuls de la famille u_i, on pourra supposer que U n'a pas de colonne nulle et appliquer 5.4.5.

5.5.6 Exemple Soit V le sous moduloïde de $\mathbb{R}^3_{\max}$ engendré par les trois vecteurs suivants:

$$u_1 = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}, \ u_2 = \begin{bmatrix} 3 \\ 3 \\ 1 \end{bmatrix}, \ u_3 = \begin{bmatrix} 4 \\ 4 \\ 4 \end{bmatrix} .$$

On a:

$$[u_1, u_2]([u_1, u_2]\backslash u_3) = \begin{bmatrix} 1 & 3 \\ 2 & 3 \\ 3 & 1 \end{bmatrix} \left(\begin{bmatrix} 1 & 3 \\ 2 & 3 \\ 3 & 1 \end{bmatrix} \backslash \begin{bmatrix} 4 \\ 4 \\ 4 \end{bmatrix} \right) = \begin{bmatrix} 1 & 3 \\ 2 & 3 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 4 \\ 4 \end{bmatrix} = u_3,$$

d'où l'on déduit que u_3 est redondant. Les vecteurs u_1 et u_2 n'étant pas proportionnels, la famille $\{u_1, u_2\}$ n'est pas redondante et constitue donc une famille génératrice minimale de V.

5.5.7 Remarque On notera qu'étant donnée un moduloïde V engendré par une famille infinie $\{v_i\}_{i\in I}$ il est équivalent de dire que V est de type fini et qu'il existe une sous famille finie extraite de $\{v_i\}$ engendrant V. Soit en effet une famille finie $\{w_1, \ldots, w_k\}$ engendrant V. Chaque w_j s'exprime comme combinaison linéaire finie des v_i soit $w_j = \bigoplus_{l\in I_j} \lambda_l v_l$, donc la sous famille finie de $\{v_i\}_{i\in I_1\cup\ldots I_k}$ est génératrice.

5.5.8 Idéaux de type fini de $\mathbb{R}_{\max}[X]$
$\mathbb{R}_{\max}[X]$ est naturellement muni d'une structure de $\mathbb{R}_{\max}[X]$ moduloïde. On appellera ici *idéaux* (resp. idéaux de type fini) (par analogie avec l'algèbre usuelle et non avec la théorie des treillis) les sous-moduloïdes de $\mathbb{R}_{\max}[X]$ (resp. de type fini). Notons que $\mathbb{R}_{\max}[X]$ vérifie l'hypothèse 5.5.1, le point (ii) étant non trivial.

5.5.9 Lemme *Pour tout polynôme $u \in \mathbb{R}_{\max}[X]$, on a $u\backslash u = e$.*

Preuve Soit $u = \bigoplus_{i=0}^p u_i X^i$. D'abord, si $bX^r \neq \varepsilon$, on a

$$(bX^r)\backslash u = \bigoplus_{r\leq i\leq p} b^{-1} u_i X^{i-r} \ ,$$

comme il résulte d'une vérification immédiate. On a ensuite par $\wedge$-distributivité:

$$\begin{aligned} u\backslash u &= \bigwedge_{k=0}^{p} (u_k X^k)\backslash \left(\bigoplus_{i=0}^{p} u_i X^i \right) \\ &= \bigwedge_{0\leq k\leq p,\ u_k\neq\varepsilon} \ \bigoplus_{k\leq i\leq p} u_k^{-1} u_i X^{i-p} \end{aligned} \tag{5.5.b}$$

En considérant le terme $k = p$ ($u_p \neq \varepsilon$), on trouve que $u\backslash u$ est majoré par $u_p^{-1} u_p = e$. L'autre inégalité est immédiate. ∎

Ainsi, le Théorème 5.5.3 s'applique, et un idéal de type fini de $\mathbb{R}_{\max}[X]$ admet une unique famille génératrice minimale (à une permutation et une dilatation près des vecteurs de base). Soit par exemple I l'idéal engendré par les trois polynômes suivants:

$$P = e \oplus X^2, \quad Q = e \oplus X, \quad R = e \oplus X^2 \oplus X^4 \oplus X^8 \oplus X^9 \ .$$

On a:

$$\begin{aligned} R/P &= (e \oplus X^2 \oplus X^4 \oplus X^8 \oplus X^9) \wedge (e \oplus X^2 \oplus X^4 \oplus X^8 \oplus X^9)/X^2 = e \oplus X^2 \\ R/Q &= \ldots = X^8 \ . \end{aligned}$$

On constate que $R = (R/P)P \oplus (R/Q)Q$, ce qui montre que R est redondant. Finalement, $\{P, Q\}$ est une famille génératrice minimale de l'idéal I.

6 Matrices inversibles dans les demi-anneaux positifs

On étudie ici les matrices inversibles. On introduit une classe de demi-anneaux dits positifs qui couvrent typiquement le cas du cône positif d'un anneau ordonné sans diviseurs de zéro ou le cas d'un dioïde sans diviseur de zéro. On montre que les matrices rectangulaires inversibles à gauche contiennent une sous matrice monomiale de taille maximale (produit d'une matrice diagonale à coefficients diagonaux non nuls par une matrice de permutation). Dans un demi-corps, cette condition est suffisante, ce qui généralise un Théorème bien connu sur les matrices de Boole. On étendra dans la section suivante ces résultats aux applications linéaires inversibles.

6.1 Préliminaires

6.1.1 Définition *Le demi-anneau $\mathcal{P}$ est positif s'il est sans diviseurs de zéro et si de plus*

$$a \oplus b = \varepsilon \Rightarrow a = \varepsilon \text{ et } b = \varepsilon \ . \tag{6.1.a}$$

Si $\mathcal{P}$ est ordonné, la condition suivante entraîne (6.1.a).

$$\forall a, b \in \mathcal{P}, \qquad a \oplus b \succeq a \ . \tag{6.1.b}$$

Il résulte qu'un dioïde sans diviseurs de zéro est positif, ainsi que le cône positif d'un anneau intègre ordonné. La caractéristique majeure des demi-anneaux positifs est d'être homomorphes au demi-anneau de boole $\mathbb{B}$.

6.1.2 Observation Le demi-anneau $\mathcal{P}$ est positif si et seulement si l'application π, $\mathcal{P} \to \mathbb{B}$,

$$\pi(a) = \begin{cases} \varepsilon & \text{si } a = \varepsilon \\ e & \text{sinon} \end{cases}$$

est un homomorphisme de demi-anneaux.

On étend π aux matrices en posant $(\pi(A))_{ij} = \pi(A_{ij})$ et l'on a alors pour des matrices de tailles compatibles: $\pi(A \oplus B) = \pi(A) \oplus \pi(B)$, $\pi(AB) = \pi(A)\pi(B)$.

6.1.3 Définition (Matrices monomiales) *Les matrices de la forme DP où D est une matrice diagonale à coefficients diagonaux non nuls et P une matrice de permutation sont dites monomiales.*

6.1.4 Lemme *A est monomiale si et seulement si $\pi(A)$ est une matrice de permutation.*

Preuve Si $A = DP$, alors $\pi(A) = \pi(D)\pi(P) = \mathrm{Id}P = P$. Réciproquement, si $P = \pi(A)$ est une matrice de permutation, alors $D = AP^{-1}$ est diagonale (car $\pi(D) = \pi(A)\pi(A)^{-1} = \mathrm{Id}$), et donc $A = DP$. ∎

Il résulte de la preuve du lemme que l'écriture $A = DP$ est unique. En notant que $DP = P(P^{-1}DP)$, on voit qu'il est équivalent de définir les matrices monomiales comme des matrices de la forme PD'.

6.2 Matrices inversibles

On dira qu'une matrice A est inversible à gauche s'il existe une matrice B telle que $BA = \mathrm{Id}$. Le résultat suivant généralise un fait bien connu pour les matrices de Boole carrées (Théorème de Wedderburn, Rutherford [100, 88]). L'argument est adapté de Berman et Plemmons [6] qui donnent le résultat pour des matrices à coefficients dans $\mathbb{R}^+$.

6.2.1 Théorème *Une matrice de Boole A de taille $n \times p$ est inversible à gauche ssi l'on peut extraire de A une matrice de permutation de taille $p \times p$.*

Preuve Notons δ_{ij} le booléien valant e si $i = j$ et ε sinon. De

$$\bigoplus_{k=1}^{p} B_{ik} A_{kj} = \delta_{ij}$$

on tire une application $\{1, \ldots, p\} \to \{1, \ldots, n\}$, $j \mapsto \varphi(j)$ telle que $B_{i\varphi(j)} = e$, $A_{\varphi(j)j} = e$ et $A_{\varphi(j)l} = \varepsilon$ pour $l \neq j$. Autrement dit, la ligne $\varphi(j)$ de la matrice A a un seul élément non nul sur la colonne j, donc φ injecte $\{1, \ldots, p\}$ dans $\{1, \ldots, n\}$ et la matrice formée des lignes d'indices $\varphi(1), \ldots, \varphi(p)$ est une matrice de permutation de taille p. ∎

Plus généralement:

6.2.2 Théorème *Une matrice carrée A à coefficients dans un demi-anneau positif $\mathcal{P}$ est inversible à gauche si et seulement si elle est monomiale ($A = DP$), les coefficients diagonaux de D étant inversibles à gauche.*

Preuve Si A est inversible à gauche, alors $\pi(A)$ est inversible à gauche dans $\mathbb{B}^{n\times n}$, donc par 6.2.1, $\pi(A) = P$ (matrice de permutation), d'où l'on déduit via le lemme 6.1.4 que $A = DP$ est monomiale. A est inversible à gauche si et seulement si D est inversible à gauche, i.e. si tous les coefficients diagonaux de D sont inversibles à gauche. ∎

6.2.3 Remarque La décomposition $A = DP$ est l'analogue dans un demi-anneau positif de la décomposition polaire (décomposition de Cartan) des matrices complexes non dégénérées, qui affirme qu'une telle matrice s'écrit de manière unique comme produit d'une matrice symétrique (en l'occurrence D) et d'une matrice orthogonale (en l'occurrence P telle que $P^{-1} = P^T$). On constate ainsi que le groupe linéaire d'un demi-anneau positif est réduit à ses éléments triviaux.

6.2.4 Théorème *Une matrice A de taille $n \times p$ à coefficients dans un demi-corps positif est inversible à gauche si et seulement si il existe une sous matrice de A de taille $p \times p$ monomiale.*

Preuve $\pi(A)$ est alors inversible à gauche dans $\mathbb{B}^{n\times n}$ et via 6.2.1, on a une sous matrice de permutation:

$$\pi(A)_{[K|} = P,$$

et donc par 6.1.4, $A_{[K|} = DP$. ∎

6.2.5 Remarque Dans le cas d'un demi-anneau positif commutatif, on trouve en dualisant le théorème 6.2.2 que A est inversible à droite si et seulement si $A = PD$ pour une matrice diagonale D inversible à droite, donc inversible, et l'on conclut que les matrices carrées sur un demi-anneau positif commutatif sont inversibles à gauche si et seulement si elles sont inversibles à droite, ce qui est un cas particulier d'un résultat prouvé généralement pour les demi-anneaux commutatifs par Reutenauer et Straubing [86].

7 Inversibilité d'applications linéaires

Etant donnés E et F deux moduloïdes, $f \in L(E,F)$, on a l'équivalence des deux propriétés suivantes:

(i) f est injective

(ii) il existe $g \in L(\operatorname{Im} f, E)$, telle que $g \circ f = \mathrm{Id}$

Cela n'implique pas l'inversibilité à gauche de f (ce qui serait $g \circ f = \mathrm{Id}$ avec $g \in L(F,E)$). Dans le cas particulier où $E = \mathcal{D}^n$ et $F = \mathcal{D}^p$, on souhaiterait se ramener au Théorème 6.2.4 relatif aux matrices inversibles à gauche. Il faut pour cela montrer que l'application linéaire $g \in L(\operatorname{Im} f, \mathcal{D}^n)$ se prolonge en une application linéaire $\tilde{g} \in L(\mathcal{D}^p, \mathcal{D}^n)$.

7.1 Prolongement d'applications linéaires

Le résultat suivant généralise un résultat donné par Kim [55] pour $\mathbb{B}^n$:

7.1.1 Théorème *Soit $\mathcal{K}$ un demi-corps idempotent, V un sous-moduloïde de type fini de $\mathcal{K}^n$, $f \in L(V, \mathcal{K}^p)$. f admet un prolongement linéaire à $\mathcal{K}^n$.*

Preuve On est dans la situation suivante:

$$\begin{tikzcd}
\mathcal{K}^n \arrow[dr, "\tilde{f}"] & \\
\cup & \\
V \arrow[r, "f"'] & \mathcal{K}^p
\end{tikzcd}$$

Soit i l'injection canonique de V dans $\mathcal{K}^n$. On peut voir l'équation $f = \tilde{f} \circ i$ comme un problème de résiduation.

7.1.2 Lemme (résiduabilité de la composition) *Soit $h \in L(V, \mathcal{K}^n)$, et $\mathcal{V}$ une partie finie génératrice de V. Les deux assertions suivantes sont équivalentes:*

(i) *Pour tout j, l'ensemble $P(j) = \{v \in \mathcal{V} \mid h(v)_j \neq \varepsilon\}$ est non vide.*

(ii) *L'application $\varphi : L(\mathcal{K}^n, \mathcal{K}^p) \to L(V, \mathcal{K}^p)$, $g \mapsto g \circ h$ est résiduable.*

Preuve du Lemme. Supposons (i) et montrons que l'application résiduée est donnée par:

$$(\varphi^{\sharp}(f))(e_j) = \bigwedge_{v \in P(j)} (h(v)_j)^{-1} f(v) \ ,$$

où e_j désigne le j-ième vecteur de la base canonique. Les propositions suivantes sont équivalentes:

$$\begin{array}{rrcl}
 & f & \succeq & g \circ h \\
\forall v \in \mathcal{V}, & f(v) & \succeq & g \circ h(v) \\
\forall v \in \mathcal{V}, & f(v) & \succeq & g\left(\bigoplus_{j=1}^{n} h(v)_j e_j\right) \\
\forall v \in \mathcal{V}, & f(v) & \succeq & \bigoplus_{j=1}^{n} h(v)_j g(e_j) \\
\forall j \in \{1, \dots, n\}, & \bigwedge_{v \in P(j)} (h(v)_j)^{-1} f(v) & \succeq & g(e_j)
\end{array}$$

ce qui montre que (i)$\Rightarrow$(ii). La réciproque est claire. ∎

On considère maintenant le cas où h est l'injection canonique de V dans $\mathcal{K}^n$. En supprimant éventuellement des composantes, on peut supposer la propriété 7.1.2,(i) réalisée. Il faut voir que $\varphi\circ\varphi^\uparrow(f) = f$. On a $(\varphi\circ\varphi^\uparrow)(f) = \varphi^\uparrow(f)\circ i$. Montrons que $(\varphi^\uparrow(f))(v) = f(v)$ pour tout $v \in \mathcal{V}$. On a

$$\begin{aligned}
(\varphi^\uparrow(f))(v) &= \bigoplus_{j=1}^{n} v_j(\varphi^\uparrow(f))(e_j) \\
&= \bigoplus_{j=1}^{n} v_j \left(\bigwedge_{w\in P(j)} w_j^{-1} f(w) \right) \\
&= \bigwedge_{\delta\in\{1,\dots,n\}^{P(j)}} \bigoplus_{j=1}^{n} v_j(\delta(j)_j)^{-1} f(\delta(j)) \\
&= \bigwedge_{\delta\in\{1,\dots,n\}^{P(j)}} f\left(\bigoplus_{j=1}^{n} v_j(\delta(j)_j)^{-1}\delta(j) \right) \ .
\end{aligned}$$

Or, pour toute application $\delta \in \{1,\dots,n\}^{P(j)}$,

$$\bigoplus_{j=1}^{n} v_j(\delta(j)_j)^{-1}\delta(j) \succeq v$$

(projeter sur la q-ième coordonnée et prendre $j = q$), et donc $\varphi\circ\varphi^\uparrow(f) \succeq f$. L'autre sens résultant de la définition de l'application résiduée $\varphi^\uparrow$, le Théorème est prouvé. ∎

7.1.3 Corollaire *Toute application linéaire d'un sous moduloïde de type fini de $\mathcal{K}^p$ dans $\mathcal{K}^n$ est représentable par une matrice.*

Preuve Une telle application se prolonge en une application $f : \mathcal{K}^p \to \mathcal{K}^n$, qui s'écrit:

$$f(x) = \bigoplus_{i=1}^{n} x_i.f(e_i)$$

laquelle formule n'est autre que le produit du vecteur ligne $[x_1,\dots,x_p]$ par la matrice formée des colonnes $f(e_i)$ (on remarquera qu'une application linéaire à gauche se représente par un produit de matrice à droite). ∎

7.2 Applications linéaires injectives

7.2.1 Définition *Le demi-anneau positif $\mathcal{P}$ est dit faiblement archimédien s'il vérifie la propriété suivante:*

$$\forall x,y \in (\mathcal{P}\setminus\{\varepsilon\})^2,\quad \exists\lambda,\mu,\lambda',\mu' \in (\mathcal{P}\setminus\{\varepsilon\})^2,\qquad \lambda x \preceq \mu y,\quad \lambda' y \preceq \mu' x\ . \tag{7.2.a}$$

7.2.2 Remarque D'ordinaire, on appelle archimédien un monoïde ordonné où pour tout y, on a pour $x \succ e$ un naturel n tel que $x^n \succeq y$. Cohen, Moller, Quadrat et Viot [23] appellent archimédien un dioïde $\mathcal{D}$ où

$$x \neq \varepsilon \Rightarrow \exists\lambda \in \mathcal{D},\ \lambda x \succeq y \tag{7.2.b}$$

La notion 7.2.1 est plus faible. Par exemple, $\mathbb{B}[X]$ est faiblement archimédien mais n'est pas archimédien au sens de [23] ni au sens classique. Soient en effet $P = X$ et $Q = e$. Il n'existe pas de polynôme R tel que $PR \succeq Q$ (considérer la valuation de PR) ce qui contredit (7.2.b). En considérant $P = e \oplus X^2 \succ e$ et $Q = X$, on constate que l'on n'a pas $P^n \succeq Q$, ce qui montre que $\mathbb{B}[X]$ n'est pas archimédien au sens usuel.

7.2.3 Hypothèse *$\mathcal{P}$ est un demi-anneau positif faiblement archimédien vérifiant (6.1.b).*

L'intérêt de cette hypothèse tient au fait suivant.

7.2.4 Proposition *Soit $\mathcal{P}$ vérifiant l'hypothèse 7.2.3, $\mathcal{V}$ un sous-moduloïde de $\mathcal{P}^p$. Pour toute application linéaire f de $\mathcal{V}$ dans $\mathcal{P}^n$, il existe une application linéaire $F : \pi(\mathcal{V}) \to \mathbb{B}^n$ telle que le diagramme suivant commute.*

$$\begin{tikzcd}
\mathcal{P}^p \supset \mathcal{V} \arrow[r, "f"] \arrow[d, "\pi"'] & \mathcal{P}^n \arrow[d, "\pi"] \\
\mathbb{B}^p \supset \pi(\mathcal{V}) \arrow[r, dashed, "F"] & \mathbb{B}^n
\end{tikzcd}$$

7.2.5 Lemme *Sous l'hypothèse 7.2.3, on a pour tous $u, v \in \mathcal{P}^n$:*

$$\pi(u) \preceq \pi(v) \Leftrightarrow \quad \exists \lambda, \mu \neq \varepsilon, \quad \lambda u \preceq \mu v$$

Preuve $\Leftarrow$: Cela résulte de $\pi(\lambda v) = \pi(v)$ pour $\lambda \neq \varepsilon$.

$\Rightarrow$: Si $n = 1$, c'est la définition même d'un demi-anneau faiblement archimédien. Pour $n = 2$, on peut supposer toute les composantes de u et v non nulles. On a

$$\lambda_1 u_1 \preceq \mu_1 v_1, \quad \lambda_2 u_2 \preceq \mu_2 v_2 \ .$$

Si $\mathcal{P}$ est commutatif, on écrit $\lambda_1\lambda_2 u \preceq (\lambda_2\mu_1 \oplus \lambda_1\mu_2)v$ et le résultat est acquis. Si $\mathcal{P}$ n'est pas commutatif, c'est à peine plus compliqué. En utilisant (7.2.a), on a $\lambda_3, \mu_3 \neq 0$ tels que $\lambda_3\lambda_1 \preceq \mu_3\lambda_2$, et donc

$$\begin{array}{l} \lambda_3\lambda_1 u_2 \preceq \mu_3\lambda_2 u_2 \preceq \mu_3\mu_2 v_2 \\ \lambda_3\lambda_1 u_1 \preceq \lambda_3\mu_1 v_1 \ , \end{array}$$

d'où une inégalité du type $\lambda u \preceq \mu v$, avec $\lambda = \lambda_3\lambda_1$ et $\mu = \mu_3\mu_2 \oplus \lambda_3\mu_1$. Le cas général résulte d'une récurrence immédiate. Le lemme 7.2.5 est prouvé. ■

Preuve de la Proposition 7.2.4. Prenons $X = \pi(u)$ avec $u \in \mathcal{V}$. Il faut vérifier que $F(X) = \pi(f(u))$ ne dépend pas du choix de u. Si $\pi(u) = \pi(v)$, alors par 7.2.5, $\lambda u \preceq \mu v$, et donc $\pi(f(u)) = \pi(f(\lambda u)) \preceq \pi(f(\lambda v)) = \pi(f(v))$, et égalité par symétrie, ce qui montre que F est bien défini. On a

$$F(\pi(u) \oplus \pi(v)) = F \circ \pi(u \oplus v) = \pi \circ f(u \oplus v) = \pi \circ f(u) \oplus \pi \circ f(v) = f \circ \pi(u) \oplus f \circ \pi(v) = F(u) \oplus F(v)$$

ce qui montre que F est additive. Trivialement, $F(\alpha X) = \alpha F(X)$ (à ne vérifier que pour $\alpha = e$ et ε). ■

7.2.6 Lemme *Sous l'hypothèse 7.2.3, pour qu'une application linéaire $f : \mathcal{P}^p \to \mathcal{P}^n$ soit injective, il est nécessaire que la matrice de f contienne une sous matrice monomiale de taille p.*

Preuve Soit $h \in \mathsf{L}(\mathrm{Im}\, f, \mathcal{P}^p)$ telle que $h \circ f = \mathrm{Id}$. On a en passant aux Booléiens via la Proposition 7.2.4 des applications F et H telles que $\pi \circ f = F \circ \pi$ et $\pi \circ h = H \circ \pi$. On peut écrire

$$\begin{aligned} h \circ f &= \mathrm{Id} \\ \pi \circ h \circ f &= \pi \\ H \circ \pi \circ f &= \pi \\ H \circ F \circ \pi &= \pi \end{aligned}$$

et il résulte de la surjectivité de π que $H \circ F = \mathrm{Id}_{\mathbb{B}^p}$. D'après le Théorème de prolongement, l'application linéaire H se représente par une matrice. On peut donc appliquer le Théorème 6.2.1 qui montre que la matrice F_0 associée à F contient une matrice monomiale de taille p. Notons f_0 la matrice associée à f. On a $F_0 = \pi(f_0)$ ce qui montre le Lemme. ∎

7.2.7 Théorème *Sous l'hypothèse 7.2.3, une application linéaire à gauche $f : \mathcal{P}^n \to \mathcal{P}^n$ est injective si et seulement si elle se représente sous la forme $X \mapsto XDP$, P étant une matrice de permutation et la matrice diagonale D étant telle que les applications $\mathcal{P} \to \mathcal{P}$, $x \mapsto xD_{ii}$ soient injective.*

Preuve Le Lemme ci-dessus montre que f se représente par une matrice monomiale. Les conditions d'injectivité de l'application $X \mapsto DPX$ sont claires. ∎

La proposition suivante résulte immédiatement du Lemme 7.2.6.

7.2.8 Proposition *Soit $\mathcal{K}$ un demi-corps idempotent. Une application linéaire de $\mathcal{D}^n$ dans $\mathcal{D}^p$ est injective ssi sa matrice dans la base canonique contient une sous matrice monomiale de taille p.*

7.2.9 Corollaire *Les seuls éléments intègres de $\mathbb{R}_{\max}[X]$ sont les monômes.*

Preuve Cherchons à quelle condition l'endomorphisme $\lambda_P : \; Q \mapsto PQ$, de $\mathbb{R}_{\max}[X]$ est injectif. En considérant la restriction de $\lambda_P : \mathbb{R}_n[X] \to \mathbb{R}_p[X]$, où $p = n + \deg P$ et $\mathbb{R}_q[X]$ dénote le moduloïde des polynômes de degré au plus q, on constate que la matrice de P dans la base canonique contient une matrice monomiale de taille n, ce qui n'est possible que si P est de la forme aX^k. ∎