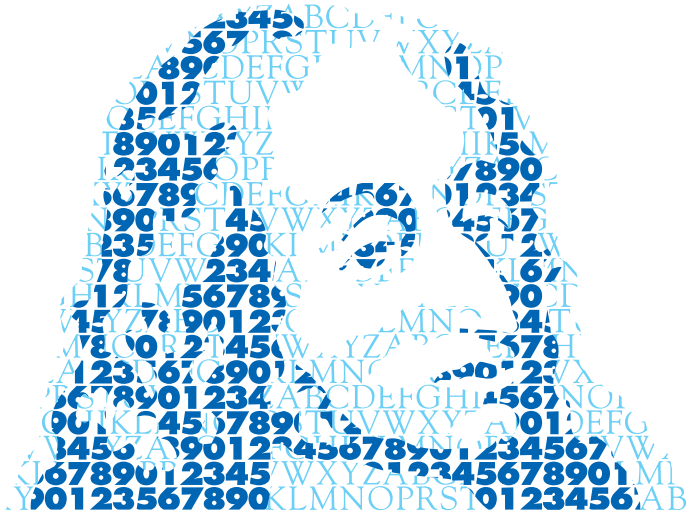
ANNALES MATHÉMATIQUES



BLAISE PASCAL

Dominique Castella

Algèbres de polynômes tropicaux

Volume 20, n° 2 (2013), p. 301-330.

<http://ambp.cedram.org/item?id=AMBP_2013__20_2_301_0>

Publication éditée par le laboratoire de mathématiques de l'université Blaise-Pascal, UMR 6620 du CNRS Clermont-Ferrand — France

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Annales mathématiques Blaise Pascal **20**, 301-330 (2013)

Algèbres de polynômes tropicaux

Dominique Castella

Résumé

Nous continuons dans ce second article, l'étude des outils algébrique de l'algèbre de la caractéristique 1 : nous examinons plus spécialement ici les algèbres de polynômes sur un semi-corps idempotent. Ce travail est motivé par le développement de la géométrie tropicale qui apparaît comme étant la géométrie algébrique de l'algèbre tropicale. En fait l'objet algébrique le plus intéressant est l'image de l'algèbre de polynôme dans son semi-corps des fractions. Nous pouvons ainsi retrouver sur les bons semi-corps l'analogue des correspondances classiques entre polynômes, fonctions polynomiales et ensemble de zéros... Par exemple, nous montrons que l'algèbre des fonctions polynomiales sur une hypersurface tropicale associée à un polynôme P, est comme dans le cas classique, le quotient de l'algèbre de polynômes par le radical de l'idéal engendré par P et nous retrouvons ainsi, de façon purement algébrique la description complète de cet idéal (i.e. une nouvelle démonstration du Tropical Nullstellensatz obtenu par Izhakian, Shustin et Rowen). Ces méthodes devraient permettre d'obtenir des algorithmes de factorisation pour les polynômes tropicaux.

Tropical polynomial algebras

Abstract

We continue, in this second article, the study of the algebraic tools which play a role in tropical algebra. We especially examine here the polynomial algebras over idempotent semi-fields. This work is motivated by the development of tropical geometry which appears to be the algebraic geometry of tropical algebra. In fact, the most interesting object is the image of a polynomial algebra in its semi-field of fractions. We can thus obtain, over good semi-fields, the analog of classical correspondences between polynomials, polynomial functions and varieties of zeros... For example, we show that the algebras of polynomial functions over a tropical curve associated to a polynomial P, is, as in classical algebraic geometry, the quotient of the polynomial algebra by the radical of the ideal generated by P and we give a purely algebraic complete description of this ideal (i. e. a new demonstration of the Tropical Nullstellensatz obtained previously by Izhakian, Shustin et Rowen).

Mots-clés : Algèbre polynomiale, algèbre tropicale, semi-corps idempotent, géométrie tropicale.

Classification math. : 55B20, 14A05, 16Y60.

1. **Introduction**

Nous avons défini dans un premier article [5] un cadre formel incluant à la fois l'algèbre classique et l'algèbre tropicale, c'est à dire l'algèbre sur les semi-corps idempotents, qui apparaissent en fait comme les « corps » de caractéristique 1.
Ceci nous a permis de généraliser la notion de zéro (les points de non différentiabilité des polynômes à plusieurs variables pouvant ainsi être vus comme les zéros de ces polynômes) et de développer de nouveaux outils algébriques pour l'étude de ces courbes (anneaux quotients par un idéal, polynômes rationnels...).
Ce travail est motivé par l'essort de la géométrie tropicale qui, développée comme "limite" et déformation de la géométrie habituelle, apparaît aussi maintenant comme la géométrie algébrique de l'algèbre tropicale (c.f. les travaux de O. Viro [21], J. Richter, D. Speyer et B. Sturmfels [17], I. Itenberg, G. Mikhalkin, E. Shustin [8], [15], ou encore L. Rowen et Z. Izhakian, [11], et bien d'autres...), et peut être relié d'autre part aux nombreux travaux sur la caractéristique 1 autour des idées de J. Tits, C. Solé, A. Connes, même si les points de vue sont, a priori, différents (voir par exemple [13]).
Si la géométrie tropicale classique est essentiellement celle du semi-corps tropical $(\mathbb{R} \cup \{-\infty\}, \max, +)$, des travaux récents, par exemple ceux de F. Aroca et S. Banerjee [2], [3], suggèrent l'intérêt de développer ces outils algébriques dans le cadre plus large des semi-corps idempotents.

Les semi-anneaux de polynômes étant intègres mais non simplifiables, ils admettent bien un semi-corps des fractions mais ne s'y injectent pas...

L'objet algébrique adéquat pour l'étude des fonctions polynomiales est alors le polynôme rationnel qui est l' image d'un polynôme dans le semi-corps des fractions rationnelles, ou de façon équivalente la classe des polynômes ayant même image.
Le lien entre les polynômes et les fonctions polynomiales a évidemment déjà été longuement étudié et caractérisé (V. P. Maslov [12], Z. Izhakian, L. Rowen [9], [11], D. Grigoriev [6], etc...), et il est bien connu qu'il n'y a pas injectivité et que deux polynômes distincts peuvent donner la même fonction. Nous montrons ici que le bon objet algébrique est bien l'algèbre des polynômes rationnels en obtenant pour ces polynômes un théorème

d'isomorphisme avec les fonctions polynomiales, valable sur les bons semi-corps idempotents, en particulier sur le semi-corps des réels max-plus. De plus nous retrouvons ainsi une bonne correspondance entre les ensembles de zéros et l'arithmétique de ces polynômes. Ceci nous permet d'associer à la variété tropicale définie par un polynôme P son algèbre de fonctions polynomiales, qui est encore le quotient de l'anneau des polynômes par le radical de l'idéal engendré par P.
Nous caractérisons par ailleurs complètement ce radical, à partir de l'hypersurface définie par le polynôme, donnant ainsi une nouvelle démonstration plus directe du "Tropical Nullstellensatz" démontré précédemment par E. Shustin et Z. Izhakian [18] Théorème 2.1 ou encore par Z. Izhakian et L. Rowen (Th. 7.17) [11].
De plus ces méthodes permettent la détermination explicite des décompositions d'une hypersurface en réunion d'hypersurfaces irréductibles et ouvrent la voie à des algorithmes de factorisation pour les polynômes tropicaux.
Rappelons pour commencer quelques définitions classiques ou provenant de l'article précédent ([5]) et quelques propriétés bien connues (voir les nombreux travaux de G.L. Litvinov ou de l'équipe Max-plus sur les semi-anneaux idempotents, par exemple [14], [1]) :

2. **Définitions**

Rappelons qu'un monoïde est un ensemble muni d'une loi interne associative, admettant un élément neutre.

Deux éléments x et y d'un monoïde $(G, *)$ sont *orthogonaux* (notation : $x \perp y$) si $x * z = x$ et $y * z = y$ implique $z = e$, où e désigne l'élément neutre de G. On dira que $(x_1, x_2) \in G^2$ est une *décomposition orthogonale* de $x \in G$ si $x = x_1 * x_2$ et $x_1 \perp x_2$. Dans le cas commutatif on notera $x = x_1 \bigoplus x_2$ pour indiquer que (x_1, x_2) est une décomposition orthogonale de x.

Un semi-anneau $(A, +, \times)$ est un monoïde commutatif $(A, +)$ muni d'une seconde loi $\times$, associative et distributive par rapport à la première,

+, et telle que l'élément neutre de + est absorbant pour cette multiplication. On dira qu'il est idempotent (ou encore de caractéristique 1 [5]) si, pour tout $a \in A$, $a + a = a$.

Si A est un semi-anneau, l'ensemble $A[X_i]_{i\in I}$ des polynômes à coefficients dans A est aussi un semi-anneau.
Un semi-anneau est *simplifiable à droite* si $\forall (x, y, z) \in A^3$, $x \times z = y \times z \Longrightarrow x = y$.

Un semi-corps est un semi-anneau dont les éléments non nuls sont inversibles.

Remarque 2.1. Même si K est un semi-corps, le semi-anneau de polynômes $K[X]$ n'est pas en général simplifiable : si K est idempotent,
$(X + 1)(X^2 + 1) = (X + 1)(X^2 + X + 1)$.
En particulier, il ne peut donc pas se plonger dans un semi-corps des fractions.

Exemple 2.2. Nous utiliserons plus particulièrement dans la suite les deux semi-corps idempotents suivants :

Le semi-corps à deux éléments, $F_1 = \{0, 1\}$, muni de l'addition, telle que 0 soit élément neutre et $1+1 = 1$, et de la multiplication habituelle, est un semi-corps de caractéristique 1, isomorphe à l'ensemble des parties d'un singleton, muni de la réunion et de l'intersection. Il est facile de vérifier que c'est le seul semi-corps fini de caractéristique 1...

Le semi-corps des réels max-plus, T, sous la version utilisée dans la plupart des applications, $\mathbb{R} \cup \{-\infty\}$ muni de la loi max comme addition et de la loi + comme multiplication, ou dans sa version, plus pratique pour conserver des notations algébriques générales (et plus facile à suivre par des non-spécialistes) $\mathbb{R}_+$ muni de la loi max comme addition et de la multiplication usuelle...

Dans un semi-anneau idempotent simplifiable, on utilisera souvent la propriété classique :

Proposition 2.3. *Si A est un semi-anneau idempotent, simplifiable à droite, pour tout couple $(x, y) \in A^2$ tel que $xy = yx$, et tout entier n, on a :*

$$(x + y)^n = x^n + y^n.$$

Un semi-anneau idempotent est ordonné par la relation : $a \leq b$ si $a+b = b$.

Un cas particulier très important est celui des semi-corps idempotents dont l'ordre associé est total. C'est en effet le cas de tous les semi-corps introduits en algèbre et géométrie tropicale. On parlera alors de semi-corps totalement ordonnés.

Réciproquement, tout groupe totalement ordonné apparaît comme le groupe multiplicatif d'un semi-corps idempotent, l'addition étant donnée par $a + b = \max(a, b)$. Il suffit en fait que le groupe ait une structure de treillis.

Un *module à droite* sur un semi-anneau A est un triplet $(M, +, .)$ où $(M, +)$ est un semi-groupe, et . une loi externe de $A \times M$ dans M, vérifiant les propriétés suivantes :
$\forall a \in A$, $\forall b \in A$, $\forall m \in M$, $\forall n \in M$, $(m.a).b = m.a \times b$, $m.(a + b) = m.a + m.b$, $(m + n).a = m.a + n.a$, $m.1 = m$ et $m.0_A = 0_M$, $0_M.a = 0_M$.

Les notions de sous-modules, d'idéaux, de morphismes et isomorphismes de semi-anneaux et de modules, se définissent de façon naturelle ; on dit encore que la famille (e_i) d'éléments d'un module M en est une base si tout élément m de M s'écrit de manière unique comme combinaison linéaire des e_i. Un module est libre s'il admet une base.

Par exemple, un F_1-module libre, de base E, est isomorphe à l'ensemble des parties finies de E, l'addition étant la réunion, et la loi externe triviale ici.

Si M est un module libre de base $B = (e_i)$, si x et y appartenant à M ont des supports (relativement à B) disjoints, ils sont orthogonaux. Réciproquement, si le semi-anneau A est idempotent et totalement ordonné, les supports de deux éléments orthogonaux sont nécessairement disjoints. Il suffit en fait pour avoir cette réciproque, que deux éléments non nuls de A ne puissent être orthogonaux, ce qui est vrai sur tout semi-corps idempotent, puisque $\inf(a, b) = (a^{-1} + b^{-1})^{-1}$ pour a et b non nuls, dans un tel corps.

On appellera encore racine d'un idéal I d'un semi-anneau A commutatif, l'idéal $\sqrt{I} = \{x \in A \ / \ \exists n \in \mathbb{N} \ x^n \in I\}$.

2.1. **Points singuliers, *singuliers et zéros**

Si f est un morphisme d'un semi-anneau idempotent A dans un semi-groupe commutatif B, on peut définir deux notions duales généralisant la notion de zéro.

On dira que u appartenant à A est un point *singulier* de f, ou que f est singulier en u, s'il existe une décomposition orthogonale de f dans $Mor(A, B)$, $f = f_1 \bigoplus f_2$, telle que $f_1(u) = f_2(u)$.

On dira que u appartenant à A est un zéro, ou un point **singulier* de f, ou que f est *singulier en u, s'il existe une décomposition orthogonale de u dans E, $u = u_1 \bigoplus u_2$, telle que $f(u_1) = f(u_2)$.

Exemple 2.4. Soit A le semi-anneau $\mathbb{Q}_+[X, Y]$ des polynômes à deux variables (avec les lois usuelles) sur $\mathbb{Q}_+$; les applications degré en X, $\deg_X$, degré en Y, $\deg_Y$ et leur somme, $d = \max(d_X, d_Y)$, de A dans le semi-anneau idempotent $(\mathbb{N} \cup \{-\infty\}, \max, +)$ sont des morphismes ; $X + Y$ est *singulier pour d puisque $d(X) = d(Y)$, mais d n'a pas de décomposition orthogonale non triviale et donc $X + Y$ ne peut être singulier pour d : si $d = f \bigoplus g$, on a $1 = \max(f(X), g(X))$ et aussi, comme f et g sont orthogonaux, $\inf(f(X), g(X)) = -\infty$; de même pour Y ; si la décomposition n'est pas triviale, on obtient donc, à l'ordre près, $f(X) = g(Y) = 1$, $f(Y) = g(X) = -\infty$, ce qui contredit $1 = d(XY) = f(X)f(Y) + g(X)g(Y)$.

On dira de même que $x = (x_i) \in A^{(I)}$ est un *zéro* d'un polynôme $P \in A[X_i]_{i \in I}$, sur un semi-anneau idempotent commutatif A, si P est un zéro (i.e. un point *singulier) pour le morphisme d'évaluation en x, $P \longmapsto P(x)$ (i.e. si l'on peut écrire $P = P_1 \bigoplus P_2$, avec $P_1(x) = P_2(x)$).

Il en découle immédiatement que si A est un semi-corps idempotent et totalement ordonné (comme le semi-corps tropical T), x est un zéro de $P = \sum \lambda_\alpha X^\alpha$ (où les $\alpha = (\alpha_i)$ appartiennent à $\mathbb{N}^n$ et $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$) si et seulement si P contient deux monômes distincts, maximaux en x (i.e. tels que $P(x) = \lambda_\alpha x^\alpha = \lambda_{\alpha'} x^{\alpha'}$).

On retrouve bien ainsi la définition usuelle des zéros (ou points de non-dérivabilité) en géométrie tropicale.

En particulier $0 \in K^n$ est un zéro de $P \in K[X_i]$ si et seulement si le terme constant de P est nul.

Cette définition s'étend sans difficulté à un point de $B^{(I)}$, où B est une extension de A, dont tous les éléments commutent avec ceux de A.

Exemple 2.5. Soient K un semi-corps idempotent commutatif et totalement ordonné et $M_n(K)$ le semi-anneau des matrices d'ordre n sur K (les définitions habituelles s'étendent sans difficulté) ; on peut considérer le polynôme $P = \sum_{\sigma \in S_n} X_{1,\sigma(1)} \cdots X_{n,\sigma(n)}$ et, comme K est totalement ordonné, les zéros de ce "déterminant tropical" sont les matrices $A = (a_{i,j})$, telles qu'il existe $\sigma \neq \tau$ avec : $a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = a_{1,\tau(1)} \cdots a_{n,\tau(n)} = P(A)$ (c.f. par exemple [5] ou [10]).

Les zéros d'un polynôme à une variable $P \in A[X]$, seront encore appelés *racines* de ce polynôme P.

Si $x \in A$ est un point singulier de l'application polynomiale P, x est une racine de $P \in A[X]$, mais la réciproque est fausse, deux applications polynomiales P_1 et P_2 correspondant à deux polynômes orthogonaux, n'étant pas, en général, orthogonales (sur F_1 par exemple, les applications polynomiales définies par X et par X^2 sont égales).

Cependant, sur le corps des réels (max,+), on peut voir facilement que ces deux notions coïncident : il suffit de voir que l'inf de deux applications définies par des monômes distincts non nuls est l'application nulle, c'est à dire que les applications monômes sont bien deux à deux orthogonales : pour cela, on peut remarquer, si $i \neq j$, que $\sum \alpha_i x^i \leq a_k x^k$ pour tout $x \in \mathbb{R}$ implique $a_i = 0$, pour tout $i \neq k$ (si $i < k$, on obtient $a_i/a_k \leq x^{k-i}$ pour tout $x \in \mathbb{R}_+$et donc $a_i = 0$ et on a de même, si $i > k$, $a_i/a_k x^{i-k} \leq 1$ pour tout $x \in \mathbb{R}_+$, ce qui donne encore $a_i = 0$).

3. **Quotients et localisations**

A tout morphisme de semi-anneaux de A dans B est associé de la manière habituelle une relation d'équivalence compatible avec les lois du semi-anneau, et donc une structure quotient. Ces relations ne sont par contre

pas toutes obtenues à partir d'un idéal du semi-anneau (il faut considérer des sous-modules convenables de A^2). Par contre on peut encore, à partir d'un idéal d'un semi-anneau commutatif construire un semi-anneau quotient, et ce cas particulier va nous permettre de généraliser les notions de corps des racines d'un polynôme et d'extension algébrique.
Plus généralement, on peut définir le quotient d'un module par un sous-module (voir par exemple [7]).

Dans cette section nous supposerons pour alléger le texte que tous les semi-anneaux considérés sont commutatifs.

3.1. **Quotient d'un module par un sous-module**

Soit M un module à droite sur un semi-anneau A et N un sous-module de M.
On notera $[M, N]$ l'idéal $\{a \in A \ / \ M.a \subset N\}$.
Pour $m \in N$, on pose $E_m = \{r \in M \ / \ m + r \in N\}$.
On définit une relation R sur M^2 par :
$\forall (m, n) \in M^2$, mRn si $(m+N) \cap (n+N) \neq \emptyset$ et $\forall a \in [M, N]$, $E_{ma} = E_{na}$.
R s'appelle la *congruence modulo* N (notation $x \equiv y(N)$ pour xRy).

Proposition 3.1. *R est une relation d'équivalence compatible avec les lois de M. On notera M/N l'ensemble quotient qui est donc muni d'une structure de module à droite.*

Démonstration. D'abord, R est bien une relation d'équivalence :
La reflexivité et la symétrie étant évidentes, il suffit de vérifier la transitivité et plus précisemment que si $(m+N) \cap (n+N) \neq \emptyset$ et $(n+N) \cap (p+N) \neq \emptyset$, pour $p \in M$, alors $(m + N) \cap (p + N) \neq \emptyset$:
Soient donc r, s, t, u dans N tels que $m + r = n + s$ et $n + t = p + u$; on a $m + r + t = n + s + t = p + u + s$ d'où le résultat puisque N est stable par $+$.

Maintenant soient m, m', n et n' dans M tels que mRm' et nRn'. Il est encore clair que $(m + n + N) \cap (m' + n' + N) \neq \emptyset$, et il suffit donc de montrer que $E_{(m+n)a} = E_{(m'+n')a}$, pour tout $a \in [M, N]$:

Si $(m + n)a + u$ appartient à N, $m'a + (na + u)$, puis $n'a + (m'a + u)$ appartiennent aussi à N, par hypothèse.

Ceci montre bien la compatibilité avec l'addition. Pour la loi externe, c'est immédiat. □

Remarque 3.2. Dans le cas des modules la relation R est la relation habituelle, la première condition impliquant la seconde.

3.2. **Quotient d'un semi-anneau commutatif par un idéal**

Proposition 3.3. *Dans le cas d'un semi-anneau commutatif A, le quotient par un idéal I est muni d'une structure de semi-anneau appelé semi-anneau quotient de A par I.*
Si I est propre ce quotient A/I n'est pas trivial.

Démonstration. On peut d'abord remarquer qu'ici la définition se simplifie (légèrement) car A étant unitaire, $[A, I] = I$; pour le premier point, il suffit de voir que la relation est compatible avec la multiplication, ce qui est immédiat.

De plus si 1 est congru à 0 modulo I, il existe un $i \in I$ tel que $1 + i$ appartienne à I, et la deuxième condition implique alors $1 \in I$. □

Proposition 3.4. *Soit K un semi-corps et L une extension de K. On suppose K de caractéristique 1 et que L est totalement ordonnée (par la relation $x \leq y$ si $x + y = y$).*
a) Si $A = K[X]$, I_x, l'ensemble des polynômes ayant $x \in L$ comme racine, est un idéal et le semi-anneau quotient est isomorphe au sous-semi-anneau $K[x]$ de L.
b) Plus généralement, si $A = K[X_1, \ldots, X_n]$, l'ensemble des polynômes dont $x \in L^n$ est un zéro, est un idéal I_x et si R_x est la relation définie par cet idéal on a PR_xQ si et seulement si $P(x) = Q(x)$.

Démonstration. Il suffit de montrer le b) dont le a) est un cas particulier :
Montrons d'abord que I_x est un idéal :
Supposons que P et Q appartiennent à I_x :
- si $P(x) \neq Q(x)$ il est clair que $P + Q$ est encore singulier en x.
- si $P(x) = Q(x)$, soient $P = P_1 \bigoplus P_2$, $Q = Q_1 \bigoplus Q_2$ des décompositions orthogonales de P et Q, telles que $P_1(x) = P_2(x)$ et $Q_1(x) = Q_2(x)$.

Dans notre cas d'un semi-corps totalement ordonné, on peut supposer que P_1 et Q_1 sont des monômes :
- si $P_1 \neq Q_1$, on peut écrire $P + Q = P_1 \bigoplus Q_1 \bigoplus R$ avec $P_1(x) = Q_1(x) = (P + Q)(x)$ et $P + Q$ a bien un zéro en x.
- si $P_1 = Q_1$, $P + Q = P_1 \bigoplus (P_2 + Q_2)$ et le résultat est immédiat.

De plus si $P \in I_x$ il est facile de voir que, pour tout Q, le polynôme PQ a un zéro en x.

Soient P et Q deux polynômes tels que $P(x) \neq Q(x)$; vérifions que P et Q ne sont pas congrus modulo I_x :
si I_x est l'idéal réduit à 0, $(P + I_x) \cap (Q + I_x) = \emptyset$.
sinon soit U non nul dans I_x ; $U(x)$ est donc aussi non nul : on peut supposer $P(x) < Q(x)$ et poser $R = Q(x)U(x)$.
$PU + R$ n'est pas dans I_x alors que $QU + R$ y est...

Supposons maintenant $P(x) = Q(x)$: Si $x = (0, \ldots, 0)$, $I_x = \sum X_i A$ et $P + Q$ appartient à la fois à $P + I_x$ et $Q + I_x$; de plus $PXU + R$ (resp. $QXU + R$), appartient à I_x si et seulement si $R(x) = 0$...
Si $x \neq (0, \ldots, 0)$, pour un $\alpha \in \mathbb{N}^n$ n'appartenant pas au support de $P+Q$ et tel que $x^\alpha \neq 0$, $P + Q + \frac{X^\alpha}{x^\alpha}(P + Q)$ appartient à $(P + I_x) \cap (Q + I_x)$.

D'autre part, pour $U \in I_x$, $PU + R$ appartient à I_x si et seulement si $R \in I_x$ ou $R(x) \leq P(x)U(x)$. La condition $P(x) = Q(x)$ implique donc bien l'équivalence demandée. □

On dira qu'un idéal I d'un semi-anneau commutatif idempotent A est *fermé* si pour tout $a \in A$, $(a + I) \cap I \neq \emptyset \Longrightarrow a \in I$.

On dira qu'il est *dense* si, pour tout $a \in A$, $(a + I) \cap I \neq \emptyset$.
Pour tous a, b de A, on a alors $(a + I) \cap (b + I) \neq \emptyset$.

Si I est un idéal d'un semi-anneau idempotent A, il est facile de vérifier que :
$\overline{I} = \{x \in A \ / \ (x + I) \cap I \neq \emptyset\}$ est un idéal fermé, la *clôture* de I.

De même il est facile de vérifier que le *cœur* de I :
$C(I) = \{x \in \overline{I} / \ \forall \alpha \in I, \forall r \in A, x\alpha + r \in I \Longrightarrow r \in I\}$ est un idéal de A.
Il est clair que I est fermé si et seulement si $\overline{I} = I$.

Proposition 3.5. *Soit A un semi-anneau commutatif idempotent et I un idéal de A. La classe de 0 modulo I est égale au cœur de I et est un idéal fermé de A.*

En particulier si I est fermé, la classe de 0 modulo I est I.

Démonstration. Soit $x \in A$: on a par définition $x \equiv 0(I)$ si $(x+I) \cap I \neq \emptyset$ et si pour tout $\alpha \in I$, $x\alpha + r \in I \Longrightarrow r \in I$, c'est à dire exactement si $x \in C(I)$.

Comme la congruence modulo I est compatible avec la structure d'anneau, si $x \equiv 0(I)$ et $x + y \equiv 0(I)$ on a nécessairement $y \equiv 0(I)$, ce qui montre que la classe de 0 est bien fermée.

Si I est fermé, il est clair que $I = C(I)$. □

Remarque 3.6. Si A est un anneau, tout idéal est fermé.
Si $A = K[X]$ est un semi-anneau de polynômes sur un semi-corps commutatif de caractéristique 1, l'idéal $PK[X]$ des multiples d'un polynôme non nul P est dense si et seulement si $P(0) \neq 0$; si $P = X$ il est fermé.
(si $P(0) \neq 0$, pour tout polynôme Q, $Q \leq PQ/P(0)$ et donc $Q + PQ/P(0)$ appartient à $I \cap (Q + I)$; réciproquement $(1 + I) \cap I \neq \emptyset$ implique que I n'est pas contenu dans $XK[X]$).

3.3. **Semi-corps de fractions d'un semi-anneau commutatif intègre**

La localisation des monoïdes commutatifs (c.f. Bourbaki, Algèbre ch I, par exemple) s'applique au monoïde A^*, où A est un semi-anneau intègre, et il est facile de vérifier que comme dans le cas classique, on obtient ainsi un semi-corps $B = Frac(A)$, que nous appellerons *semi-corps des fractions* de A et un morphisme i (non injectif en général) de A dans B, tels que B ne contienne que les produits d'éléments de $i(A)$ et de leurs inverses.

Plus précisément, on a $i(a) = i(b)$ si et seulement s'il existe $z \in A^*$ tel que $za = zb$.

i est donc injectif si et seulement si A est simplifiable et $i(A)$ est donc toujours un semi-anneau simplifiable. De plus tout morphisme de A dans un semi-anneau simplifiable C se factorise en un morphisme de $i(A)$ dans C.

On dira donc que $i(A)$ est *l'enveloppe simplifiable* de A.

Ceci s'applique en particulier aux semi-anneau $A[X]$ de polynômes sur un semi-anneau intègre A. Le semi-corps des fractions $Frac(A[X])$ sera donc isomorphe au semi-corps des fractions $Frac(K[X])$, où K est le semi-corps des fractions de A.

Nous noterons dans la suite $A\{X\}$ l'enveloppe simplifiable du semi-anneau des polynômes $A[X]$ et $K(X)$ le semi-corps des fractions de $K[X]$,

que nous appellerons le *semi-corps des fractions rationnelles* à coefficients dans le semi-corps K.

Dans le cas des anneaux, nous retrouvons bien entendu les notions usuelles et on peut identifier un anneau commutatif intègre avec son enveloppe simplifiable.

Dans la suite nous appellerons *polynômes rationnels* les éléments de $A\{X\}$, puisqu'ils s'identifient aux fractions rationnelles dont le dénominateur est constant. Deux polynômes P et Q définissent donc le même polynôme rationnel si et seulement s'il existe un polynôme non nul R tel que $RP = RQ$. Par exemple, on a, dans $A\{X\}$, $(X+1)^n = X^n + 1$, ce qui n'est bien sûr pas vrai dans $A[X]$.

Le point crucial pour la suite est que la notion de zéro est conservée :

Proposition 3.7. *Si $P \in K[X_1, \ldots, X_n]$, où K est un semi-corps commutatif idempotent totalement ordonné, admet un zéro $x = (x_i) \in K^n$ et si, pour*
$Q \in K[X_1, \ldots, X_n]$, il existe $R \neq 0$ dans $K[X_1, \ldots, X_n]$ tel que
$RP = RQ$, x est aussi un zéro de Q.

Démonstration. Supposons d'abord $R(x) \neq 0$ et $P(x) \neq 0$; il est facile de voir que, s'il y a exactement k monômes de R prenant la valeur $R(x)$, le nombre de monômes de RP prenant la valeur maximale est au moins $k+1$, ce qui implique que Q est singulier en x.

Si $R(x) \neq 0$ et $P(x) = 0$, on a bien nécessairement $Q(x) = 0$.

Supposons maintenant $R(x) = 0$. Pour $n = 1$, le résultat est immédiat par simplification.

On procède donc par récurrence sur n :

On peut écrire dans ce cas :

$R = \sum X_i^{l_i} R_i$, $R_i \in K[X_1, \ldots X_{i-1}, X_{i+1}, \ldots, X_n]$ et si $R_i \neq 0$, on doit avoir $x_i = 0$. Il existe au moins un i tel que $x_i = 0$ et quitte à renommer les variables, on peut supposer $x_1 = 0$.

En écrivant $R = R_0 + X_1 R_1$, $P = P_0 + X_1 P_1$ et $Q = Q_0 + X_1 Q_1$, R_1, P_1, Q_1 appartenant à $K[X_2, \ldots X_n]$, il vient $R_0 P_0 = R_0 Q_0$; comme P_0 est nécessairement singulier en $(x_2, \ldots, x_n)$, l'hypothèse de récurrence donne alors que Q_0 est singulier en $(x_2, \ldots, x_n)$ et donc que Q l'est en x. □

Ceci permet donc de définir les *racines d'un polynôme rationnel* $P \in K\{X\}$, comme étant les racines d'un des représentants et plus généralement, la notion de zéro d'un polynôme rationnel. On peut aussi clairement parler du degré d'un tel polynôme.

4. **Polynômes et fonctions polynomiales**

K désigne dans la suite un semi-corps idempotent (ou semi-corps de caractéristique 1) totalement ordonné.

Il est bien connu qu'un polynôme de degré n a au plus n racines et que la fonction polynomiale sur le semi-corps des réels tropicaux se factorise en produit de facteurs du premier degré (voir par exemple [19]). L'étude qui suit permet de préciser ce qui se passe pour une variable, la situation étant bien sûr nettement plus compliquée dans le cas général.

4.1. **Extensions de Semi-corps**

Le but de cette section est de construire une extension d'un semi-corps de caractéristique 1, totalement ordonnée, L, contenant une racine d'un polynôme donné de $K[X]$.

Pour ceci nous allons montrer que $K\{X\}/(X^n + a)$ est un semi-corps de caractéristique 1, totalement ordonné, contenant une racine n-ième de a, la classe de X.

On dira qu'un semi-corps idempotent K est *algébriquement clos* si tout polynôme de $K[X]$, non constant, admet au moins une racine dans K. Le semi-corps idempotents T des réels tropicaux est clairement algébriquement clos. Il est d'autre part facile de voir que le semi-corps idempotent à deux éléments F_1 est le seul semi-corps fini algébriquement clos.

Théorème 4.1. *Soit K un semi-corps totalement ordonné de caractéristique 1.*
a) L'ensemble des polynômes admettant x comme racine est l'idéal : $J = \sum_k (X^k + x^k)$.
b) L'ensemble des polynômes rationnels de $A = K\{X\}$ admettant $x \in K$ comme racine est l'idéal de A engendré par $X + x$.

Démonstration. a) Supposons que $P \in K[X]$ admet x comme racine et soient $a_i X^i$ et $a_j X^j$ deux monômes distincts, $i < j$, tels que $P(x) = a_i x^i = a_j x^j$: on a donc pour tout k, $a_k x^k \leq P(x)$ et $P_1 = a_j X^j +$

$a_iX^i = a_jX^i(X^{j-i}+x^{j-i})$ appartient à J ; posons $R_k = a_kx^{k-i}X^i$; puisque $a_kx^{k-i} \leq a_i$ par hypothèse, on a $R_k \leq P$ et donc $P = P + R_k$.
Si $k < i$, $a_kx^{k-i}X^i + a_kX^k = a_kx^{k-i}X^k(X^{i-k} + x^{i-k})$ appartient à J.
De même, si $k > i$, $a_kX^k + a_kx^{k-i}X^i = a_kX^i(X^{k-i} + x^{k-i})$ appartient à J.
On obtient ainsi que $\sum(P + R_k) = P$ appartient à J.
La réciproque est claire.

b) Il en découle aussi que tout multiple de $X+x$ admet x comme racine. Réciproquement il suffit de montrer que tous les $X^k + x^k$ sont multiples de $X + x$; ceci vient de l'égalité

$$(X + x)^k(X^k + x^k) = \sum_0^{2k} x^i X^{2k-i} = (X + x)^{2k}$$

qui implique dans $K\{X\}$, l'égalité $(X + x)^k = X^k + x^k$. □

En raisonnant par récurrence sur le degré on retrouve ainsi facilement le résultat bien connu :

Corollaire 1. *a) Si K est un semi-corps totalement ordonné de caractéristique 1, et $P \in K[X]$ un polynôme de degré n, P a au plus n racines dans K.*
b) Si K est de plus algébriquement clos, tout polynôme rationnel de degré n se factorise en produit de polynômes du premier degré.

Proposition 4.2. *Soit K un semi-corps totalement ordonné et $a \in K$, $a \neq 0$, $n \in \mathbb{N}^*$;*
$L = K\{X\}/(X^n + a)$ est un semi-corps totalement ordonné contenant K et la classe x de X dans L vérifie $x^n = a$. De plus, pour tout $y \in L$, y^n appartient à K.

Démonstration. Considérons l'application linéaire ϕ de $K[X]$ dans $E = K + KX + KX^2 + \ldots + KX^{n-1}$ définie par $\phi(X^m) = a^qX^r$ si $m = nq + r$ avec $0 \leq r < n$. On note θ le morphisme canonique de $K[X]$ dans $K\{X\}$. Comme le degré est indépendant du représentant, $F = \theta(E)$ est l'ensemble des polynômes rationnels de degré inférieur ou égal à $n - 1$.

Lemme 1. *$P \in K[X]$ est *singulier pour ϕ si et seulement si :*
$P \in J = \sum_k(X^{nk} + a^k)$:

Démonstration. Tout polynôme P peut s'écrire de façon unique $P = \sum_0^{n-1} P_iX^i$ les P_i étant des polynômes en $Y = X^n$, et on a alors $\phi(P) =$

$\sum_0^{n-1} P_i(a)X^i$.
P est *singulier pour ϕ si et seulement chacun des polynômes P_i est *singulier en a, ou encore si a est une racine de P_i.

Or, d'après la proposition précédente, P_i admet une racine en a si et seulement si $P_i \in I = \sum_k (Y^k + a^k)$, ce qui donne bien le résultat annoncé. □

Lemme 2. *Si P et Q ont même image par ϕ, ils sont congrus modulo J :*

Démonstration. Comme, pour tout $m = nq + r$, $X^m + \phi(X^m) = (X^{nq} + a^q)X^r$, appartient à J, on a, pour tout $P \in K[X]$, $P + \phi(P) \in J$ et donc $P + \phi(P) + Q = P + \phi(Q) + Q \in (P + J) \cap (Q + J)$, qui est donc bien non vide.

Il suffit donc de voir que si $\phi(P) = \phi(Q)$ alors, pour tout $U \in J$ et pour tout $V \in K[X]$, $PU + V$ est *singulier pour ϕ si et seulement si $QU + V$ l'est ; or ϕ est *singulier en $PU + V$ si et seulement s'il existe une décomposition orthogonale de V, $V = V_1 + V_2$ telle que ϕ soit *singulier en V_2 et $\phi(V_1) \leq \phi(PU)$. L'équivalence annoncée provient alors de ce que $\phi(PU) = \phi(\phi(P)\phi(U)) = \phi(QU)$. □

On en déduit immédiatement que dans $A = K[X]/J$ la classe de X^n est égale à la classe de a et que K s'injecte dans A. De plus A est intègre, car le coeur de J est réduit à $\{0\}$ (si $P \neq 0$, il existe un monôme non nul V, tel que $V \leq P(X^n + a)$ et $P(X^n + a) + V \in J$, alors que V n'appartient pas à J).

On vérifie de plus bien aisément que K s'injecte alors dans le semi-corps des fractions L de A et l'image x de X y est naturellement une racine n-ième de a.

Pour tout $c \in L$ et tout entier k, on a $(c + x^k)^n = c^n + \cdots + x^{kn} = c^n + x^{kn}$ et si $c^n \leq a^k$, $(x^k)^n \geq c(x^k)^{n-1}$ et donc $x^k \geq c$; de même si $a^k \leq c^n$, on a $c \geq x^k$. En particulier $x \geq 1$ si $a \geq 1$ et $x \leq 1$ si $a \leq 1$.

Il est donc clair que A et L sont totalement ordonnés ; pour $P \in K[X]$, $P(x)$ est alors égal au monôme dominant évalué en x, $a_i x^i$ qui est inversible dans A puisque x l'est. Ceci montre qu'en fait A est un corps et donc égal à L.

Soit ψ le morphisme de $K[X]$ dans L, $P \longmapsto P(x)$: J est l'ensemble des éléments *singuliers pour ψ et $(X^n + a)$ est l'idéal des polynômes rationnels *singuliers pour le morphisme quotient Ψ de $K\{X\}$ dans L. On obtient ainsi un morphisme surjectif de $K[X]$ dans $K\{X\}/(X^n + a)$

qui se factorise en un isomorphisme de A dans $K\{X\}/(X^n + a)$ On peut ainsi sans inconvénient identifier ces deux quotients. □

On retrouve ainsi facilement que :

Proposition 4.3. *Tout semi-corps idempotent totalement ordonné se plonge dans un semi-corps algébriquement clos totalement ordonné.*

Démonstration. En effet, si $x \in L$, totalement ordonné, est une racine d'un polynôme P à coefficients dans un sous-corps K, l'égalité de deux monômes implique qu'une puissance de x est dans K. Les extensions "algébriques" sont donc ici radicielles. En considérant, comme dans le cas classique, les extensions radicielles totalement ordonnées de K, contenues dans un ensemble Ω de cardinal strictement supérieur à celui de K, on obtient un ensemble clairement inductif. Soit donc L un élément maximal : si L n'était pas algébriquement clos, il existerait donc, d'après la proposition précédente, une extension radicielle totalement ordonnée, de la forme $F = L[X]/(X^n - a)$, $a \in L$; mais celle-ci serait alors plongeable dans $\Omega - L$ (dont le cardinal est supérieur), ce qui contredit la maximalité de L. (Comme dans le cas classique, $cardF = cardL = cardK$, sauf si K est fini, mais ici cela implique égal à F_1 et algébriquement clos). □

4.2. **Polynômes rationnels et fonctions polynomiales sur** K^n

On définit, comme dans le cas d'une variable, le semi-anneau simplifiable des polynômes rationnels à n variables sur K, $K\{X_1, \ldots, X_n\}$, comme étant l'image de $K[X_1, \ldots, X_n]$ dans son corps des fractions.

Pour un polynôme $P \in K\{X_i\}_{i\in\mathbb{N}}$ on notera $V(P)$ l'ensemble des zéros de P dans K^n, c'est à dire l'hypersurface tropicale définie par P. Pour $x \in K^n$ on notera I_x l'ensemble $\{Q \in K\{X_i\} \ / \ x \text{ est un zéro de } Q\}$, des polynômes rationnels dont x est un zéro.

Pour une partie V de K^n, on notera $I(V)$ l'idéal $\cap_{x\in V} I_x$, des polynômes dont tous les points de V sont des zéros (i.e. donc "nuls" sur V).

On a immédiatement, pour $V = V(P)$, $V(I(V)) = V$. Une telle partie V n'est cependant pas en général une variété au sens usuel de la géométrie tropicale... Nous dirons que c'est un ensemble t-algébrique.

On dira que l'hypersurface définie par P, $V(P)$ est irréductible si elle n'est pas réunion de deux hypersurfaces strictement incluses.

Soit $P \in K[X_1, \ldots, X_n]$, $P = \sum_I \lambda_\alpha X^\alpha$, où I est une partie finie de $\mathbb{N}^n$.

On dira que P est *convexe* si, pour tout $j \in \mathbb{N}^n$ appartenant à l'enveloppe convexe de $I_j = I - \{j\}$ et toute écriture $j = 1/m(\sum_{I_j} j_i i)$, (avec pour tout $i \in I_j$, $j_i \in \mathbb{N}$, $m = \sum J_i$), on a : $\lambda_j^m \geq \Pi \lambda_i^{j_i}$.

Si K est algébriquement clos, tout élément admet des racines de tout ordre ce qui permet de définir les puissances rationnelles : comme il est supposé totalement ordonné, la racine d'ordre n d'un élément est en effet unique (par stricte croissance des fonctions puissances).

On appellera *enveloppe convexe* de P le plus petit polynôme convexe supérieur à P : comme il suffit de considérer un nombre fini de monômes correspondant à l'enveloppe convexe du support I de P dans $\mathbb{N}^n$, on obtient un polynôme convexe supérieur à P et nécessairement plus petit que tous les autres, en ajoutant à P tous les monômes de la forme $\Pi_{I_j} \lambda_i^{\frac{j_i}{m}} X^j$, avec les notations ci-dessus. On notera $conv(P)$ cette enveloppe convexe.

On dira qu'un monôme $\lambda_\alpha X^\alpha$ de P est extrémal si l'enveloppe convexe du polynôme obtenu en supprimant ce monôme est strictement inférieure à celle de P. Il est clair que l'enveloppe convexe de P est égale à l'enveloppe convexe de la somme de ses monômes extrémaux.

Ces définitions correspondent, dans le cas des réels tropicaux, aux définitions habituelles (même si elles sont, en général, formulées à partir de l'enveloppe convexe du graphe de la transformation de Legendre :
$(i, j) \longmapsto -\ln(\lambda_{i,j})$, pour des raisons historiques... Voir par ex. [16]).

Pour un polynôme P de $K[X_1, \ldots, X_n]$, on notera $\overline{P}$ le polynôme rationnel et $\tilde{P}$ la fonction polynomiale associés.

Exemple 4.4. Soit $P = 1 + X + 2XY + 9X^2 + X^3 + 8Y^3 \in T[X, Y]$ (avec donc ici $T = \mathbb{R}_+$, $+ = \max$ et la multiplication usuelle).
Il est clair que X n'est pas extrémal, mais moins que $2XY$ non plus : il est facile de voir que l'enveloppe convexe de $X^3 + 8Y^3 + 1$ est en fait $(X + 2Y + 1)^3$.
On a de plus, dans $T\{X, Y\}$, $9X^2 + 4Y^2 = (3X + 2Y)^2 = 9X^2 + 6XY + 4Y^2$ ce qui donne : $\overline{P} = 1 + X + 2Y + 9X^2 + 6XY + 4Y^2 + 2X^2Y + 4XY^2 + X^3 + 8Y^3$.

On peut voir que l'on a aussi, dans $T[X,Y]$ cette fois :
$conv(P) = 1 + X + 2Y + 9X^2 + 6XY + 4Y^2 + 2X^2Y + 4XY^2 + X^3 + 8Y^3$.

On a alors le lemme (déjà connu lorsque K est le semi-corps des réels max-plus) :

Lemme 3. *Soit K est un semi-corps idempotent algébriquement clos infini.*

a) La fonction polynomiale définie par P et celle définie par son enveloppe convexe sont les mêmes.

b) Les fonctions polynomiales $\tilde{P}$ et $\tilde{Q}$ sont égales si et seulement si les enveloppes convexes de P et Q sont égales.

Démonstration. a) Soit $P = \sum_I \lambda_\alpha X^\alpha$, où I est une partie finie de $\mathbb{N}^n$.

On dira que le monôme $\lambda_\alpha X^\alpha$ est localement dominant si
$A_\alpha = \{x \in K^n \ / \ \lambda_\alpha x^\alpha > \lambda_\beta x^\beta, \forall \beta \in I - \{\alpha\} \}$ est non vide.

Il suffit donc de voir que les monômes localement dominant sont exactement les monômes extrémaux pour obtenir le résultat.

Il est clair qu'un monôme non extrémal ne peut être dominant. Il reste donc à voir que si $\lambda_\alpha X^\alpha$ est extrémal il est localement dominant. On peut distinguer deux cas :

- soit α n'est pas dans l'enveloppe convexe des $\beta \in I$, $\beta \neq \alpha$.

On peut alors trouver une $\mathbb{Q}$-forme linéaire sur , l, telle que $l(\gamma) \in \mathbb{Z}$ pour tous les γ appartenant à I et telle que $l(\alpha) > 0$, $l(\beta) < 0$ pour tous les $\beta \neq \alpha$ de I. Si $l((\gamma_1, \ldots, \gamma_n)) = \sum c_i \gamma_i$, il suffit de choisir $x = (y^{c_1}, \ldots, y^{c_n})$, où $y \in K$ est suffisamment grand, ce qui est possible car K est infini et totalement ordonné et ne peut donc avoir de plus grand élément.

- soit α est dans l'enveloppe convexe des $\beta \in I$, $\beta \neq \alpha$ et il existe avec $m \in \mathbb{N}$, et des $c_\beta \in \mathbb{N}$, tels que : $m\alpha = \sum_{I-\{\alpha\}} c_\beta \beta$; comme le monôme est lui extrémal, on a nécessairement $\lambda_\alpha^m > \Pi \lambda_\beta^{c_\beta}$; $x = (1, \ldots, 1)$ convient alors.

b) Si les enveloppes convexes sont différentes, $conv(P+Q) > conv(P)$ ou $conv(P+Q) > conv(Q)$. Il existe donc un monôme extrémal de $conv(P+Q)$ n'apparaissant pas, par exemple, dans $conv(P)$. Or ce monôme est localement dominant ; soit x pour lequel ce monôme domine, $(P+Q)(x)$ ne peut donc être égal à $P(x)$ ce qui prouve bien que $\tilde{P} \neq \tilde{Q}$.

La réciproque est immédiate. □

On peut en déduire qu'il y a une bonne correspondance entre les fonctions polynomiales et les polynômes rationnels :

Théorème 4.5. *Si K est un semi-corps algébriquement clos idempotent infini, l'application naturelle de $K\{X_1, \ldots, X_n\}$ dans les fonctions polynomiales de K^n dans K, est un isomorphisme de semi-anneaux.*

Démonstration. Considérons l'application Φ de $K[X_1, \ldots, X_n]$ dans l'ensemble des fonctions polynomiales sur K^n, $Pol_n(K)$, $P \longmapsto (x \mapsto P(x))$. Si R est un polynôme non nul et $x \in K^n$ est tel que $R(x) \neq 0$, $R(x)P(x) = R(x)Q(x)$ implique $P(x) = Q(x)$. Supposons $R(x) = 0$, avec $x = (x_i) \in K^n$; on peut alors écrire $R = \sum_I X_i^j R_i$ où I est inclus dans l'ensemble des $i \in [1, n]$ tels que $x_i = 0$ et $j \geq 1$ est tel que $R_i(x) \neq 0$.

Choisissons un $i \in I$: en dérivant j fois par rapport à X_i, on obtient $R_i(x)P(x) = R_i(x)Q(x)$ et donc bien $P(x) = Q(x)$.
(La dérivée P' d'un polynôme $\sum a_i Y^i \in K[Y]$ est le polynôme $\sum a_i Y^{i-1}$ et $P \longmapsto P'$ est encore une dérivation).

On peut donc bien considérer l'application Ψ de $K\{X_1, \ldots, X_n\}$ dans $Pol_n(K)$ qui associe à un polynôme rationnel la valeur de l'un de ses représentants en x et Ψ est clairement un morphisme surjectif de semi-anneaux.

Il reste donc à montrer l'injectivité de ce morphisme.

Or celle-ci découle de la proposition suivante, déja bien connue (voir les travaux de Maslov par exemple [12]), mais que nous redémontrons ici de façon purement algébrique :

Proposition 4.6. *Soient P et Q deux polynômes sur un semi-corps K idempotent et totalement ordonné, infini et algébriquement clos.*
Les propositions suivantes sont équivalentes :
a) P et Q définissent les mêmes polynômes rationnels.
b) P et Q ont même enveloppe convexe.
c) P et Q définissent les mêmes fonctions polynomiales.

On a vu ci-dessus l'équivalence entre les assertions b) et c) et que a) implique c).

Il reste donc à voir que b) implique a) ce qui revient en fait à montrer que $\overline{conv(P)} = \overline{P}$, c'est à dire que les classes dans $K\{X_1, \ldots, X_n\}$ de P et de son enveloppe convexe sont les mêmes.

Soit donc $P = \sum_I \lambda_\alpha X^\alpha$, où I est une partie finie de $\mathbb{N}^n$.

Soit J l'enveloppe convexe de I dans N^n. Pour chaque $\gamma \in J - I$, il existe des entiers γ_i et m_γ tels que $\gamma = 1/m_\gamma(\sum_I \gamma_i i)$, et on peut poser $\lambda_\gamma = \Pi\lambda_i^{\frac{\gamma_i}{m_\gamma}}$.

On obtient, en développant P^{m_γ}, $(\lambda_\gamma X^\gamma)^{m_\gamma} \leq P^{m_\gamma}$ et ceci montre que, pour $m = \max(m_\gamma)$:

$\overline{P^m} \geq \overline{conv(P)^m} = \overline{\sum_J \lambda_\beta^m X^{m\beta}}$; ceci donne donc l'égalité :

$\overline{P}^m = \overline{P^m} = \overline{conv(P)^m} = \overline{conv(P)}^m$, car l'autre inégalité est évidente.

Le lemme suivant termine alors la démonstration :

Lemme 4. *Soient P et Q deux polynômes rationnels. S'il existe $m > 0$ tel que $P^m = Q^m$, alors $P = Q$.*

Démonstration. On peut supposer P et Q non nuls. On a $P^m = P^m + Q^m = (P+Q)^m$ et donc $(P+Q)^{2m} \geq P^{2m} + P^{2m-1}Q \geq P^{2m}$ donne $P^{2m} = P^{2m-1}(P+Q)$ d'où finalement $P = P+Q$, après simplification. □

□

Remarque 4.7. Un polynôme rationnel P admet donc deux représentants particuliers, l'un maximal, l'enveloppe convexe commune de ses représentants, l'autre minimal, la somme des monômes extémaux de l'un de ses représentants.

5. Variété des zéros d'un polynôme de $T\{X_1, \cdots, X_n\}$

On peut, du moins sur le semi-corps T des réels max-plus, retrouver le lien habituel entre "variété des zéros" et divisibilité.

5.1. Variété des zéros d'un polynôme et diviseurs

Nous allons démontrer dans ce paragraphe que :
si P et Q appartiennent à $T\{X_i\}_{i\in\mathbb{N}}$, $V(Q) \subset V(P)$ si et seulement si Q divise une puissance de P.

Pour ceci nous considérerons les parties suivantes de K^n associées à un polynôme rationnel $P = \sum_I \lambda_\alpha X^\alpha \in T\{X_1, \ldots, X_n\}$:
$A_\alpha(P) = \{x \in T^n \ / \ \lambda_\alpha x^\alpha > \lambda_\beta x^\beta, \forall \beta \in I - \{\alpha\} \}$.

$B_\alpha(P) = \{x \in T^n \ / \ \lambda_\alpha x^\alpha \geq \lambda_\beta x^\beta, \forall \beta \in I - \{\alpha\} \ \}$.
$B_{\alpha,\beta} = B_\alpha \cap B_\beta$, pour $(\alpha, \beta) \in I^2$.

On peut remarquer que $V(P)$ est la réunion des $B_{\alpha,\beta}$ non vides.

Les deux lemmes suivants donnent la correspondance bien connue entre la subdivision du polytope de Newton induite par un polynôme tropical et la décomposition de $\mathbb{R}^n$ induite par l'hypersurface tropicale définie par ce polynôme, mais nous les reformulons ici avec nos notations pour la commodité de la lecture, le graphe considéré étant ici le 1-squelette de cette subdivision :

Lemme 5. *1) a) V(P) est la réunion des $B_{\alpha,\beta}$ non vides pour les α et β tels que A_α et A_β soient eux mêmes non vides.*
b) Les A_α non vides sont connexes par arcs.
c) Le graphe Γ dont les sommets sont les α tels que A_α soit non vide et les arêtes (α, β) tels que $B_{\alpha,\beta}$ de codimension 1, est connexe.
On notera $s(\Gamma)$ l'ensemble des sommets et $a(\Gamma)$ l'ensemble des arêtes de ce graphe.
2) Si $V(P) = V(Q)$, $\{A_\alpha(P) \neq \emptyset\} = \{A_\beta(Q) \neq \emptyset\}$ et les graphes associés sont isomorphes.
On peut donc numéroter les monômes extrémaux de P et de Q de sorte que $A_{\alpha_i}(P) = A_{\beta_i}(Q) = A_i$ pour tout i.

Démonstration. 1) a) Ceci découle de ce que pour tout élément $x \in V(P)$ est adhérent à au moins deux A_α distincts...
b) Ce sont même des convexes sur le corps des réels max-plus...
c) Si $x \in A_\alpha$ et $y \in A_\beta$, le segment $[x, y]$ a une intersection non vide avec une suite finie de A_{α_i} et coupe nécessairement les $B_{\alpha_i,\alpha_{i+1}}$; quitte à prendre une succession de segments pour joindre x à y, on peut supposer que ce chemin ne rencontre que des $B_{\alpha_i,\alpha_{i+1}}$ de codimension 1. Ceci fournit alors bien un chemin dans le graphe entre les sommets α et β.
2) Soient $x, y \in A_\alpha(P)$ tels que $x \in A_\beta(Q)$ et $y \in A_\gamma(Q)$: si $\beta \neq \gamma$, il existe un chemin continu ϕ de x à y dans $\{A_\alpha(P)\}$ et ce chemin rencontre nécessaire $V(Q)$, ce qui est contradictoire avec la définition de $\{A_\alpha(P)\}$ et l'hypothèse $V(P) = V(Q)$.
On trouve donc pour chaque α un β tel que $A_\alpha(P) = A_\beta(Q)$ et par symétrie, en utilisant le a) du lemme précédent, on obtient bien une bijection entre les sommets du graphe qui respecte les arêtes... □

Lemme 6. *Soit $V = V(P) \subset T^n$, où $P = \sum_I \lambda_\alpha X^\alpha \in T\{X_1, \ldots, X_n\}$:*

1) On peut donc associer à V une famille de parties ouvertes connexes disjointes de T^n, $(A_1, \ldots, A_k)$, où k est le nombre de monômes extrémaux de P, telles que $T^n - V = \cup A_i$.
On a alors pour $Q = \sum \mu_\beta X^\beta \in T\{X_i\}_{1\leq i\leq n}$, $V(Q) \subset V(P)$ si et seulement si pour chaque A_i il existe β, nécessairement unique, appartenant au support de Q tel que $A_i \subset A_\beta(Q)$.

2) Soient les fractions rationnelles $L_{i,j} = \frac{\lambda_{\alpha_i}}{\lambda_{\alpha_j}} X^{\alpha_i - \alpha_j}$ et $M_{i,j} = \frac{\mu_{\beta_i}}{\mu_{\beta_j}} X^{\beta_i - \beta_j}$.
Si $B_{i,j}(P)$ est de codimension 1, il existe un rationnel positif $q_{i,j}$ tel que $M_{i,j} = L_{i,j}^{q_{i,j}}$.

Démonstration. 1) En effet, si $V(Q) \subset V$, on a $A_i \subset T^n - V \subset T^n - V(Q) = \cup A_\alpha(Q)$ et le résultat par connexité.
Réciproquement on a immédiatement $T^n - V = \cup A_i \subset \cup A_\alpha = T^n - V(Q)$ et donc bien $V(Q) \subset V$.

2) Dans le cas des réels max-plus, B_i, l'adhérence de A_i, est un convexe défini par le système d'inéquations affines (à coefficients entiers), pour tout $r \neq i$, $L_{i,r}(x) \geq 1$.
Si $\beta_i \neq \beta_j$, $B_{i,j}(P) \subset B_{i,j}(Q)$ et chacune des équations $L_{i,j}(x) = 1$ et $M_{i,j}(x) = 1$ définit un hyperplan contenant l'intersection $B_i(P) \cap B_j(P)$; mais cet hyperplan est unique si $B_{i,j}$ est de dimension $n-1$ et il en découle dans ce cas que ces deux équations sont proportionnelles, ce qui donne, en notation algébrique, l'existence d'un rationnel $k_{i,j}$ tel que $L_{i,j} = M_{i,j}^{k_{i,j}}$. Ce rationnel est nécessairement strictement positif car A_i est inclus dans le demi-plan positif pour les deux équations. □

Lemme 7. *1) On peut, d'après le lemme précédent, associer à tout polynôme $Q = \sum \mu_\beta X^\beta \in T\{X_i\}_{1\leq i\leq n}$, tel que $V(Q) \subset V$, la famille $S(Q) = (\beta_1, \ldots, \beta_k)$, appartenant à $(\mathbb{N}^n)^k$, telle que pour chaque i, $A_i \subset A_{\beta_i}(Q)$.*
L'ensemble $\{S(Q) \ / \ V(Q) \subset V\}$ est un sous-monoïde de $(\mathbb{N}^n)^k$.
2) En notant $e_{i,j}$ le pgcd des composantes de $(\alpha_i - \alpha_j)$ et $n_{i,j}$ le k-uplet $(\alpha_i - \alpha_j)/e_{i,j}$, il existe une famille d'entiers positifs $r_{i,j}$ telle que : $\beta_i - \beta_j = r_{i,j} n_{i,j}$.

Démonstration. 1) Ceci découle immédiatement de $S(Q^r) = rS(Q)$ pour $r \in \mathbb{N}$ et du fait que, pour chaque i, si $A_i \subset A_{\alpha_i}(Q_1)$ et $A_i \subset A_{\beta_i}(Q_2)$, on a $A_i \subset A_{\alpha_i+\beta_i}(Q_1 Q_2)$, d'où $S(Q_1 Q_2) = S(Q_1) + S(Q_2)$.
2) Le lemme précédent prouve que, pour tout $Q = \sum \mu_\beta X^\beta$, tel que $V(Q) \subset V(P)$, il existe une famille de rationnels positifs $r_{i,j}$ telle que

$\beta_i - \beta_j = r_{i,j} n_{i,j}$, et cette famille est nécessairement composée d'entiers par définition des $n_{i,j}$. □

Lemme 8. *Soit $Q = \sum \mu_\beta X^\beta \in T\{X_i\}_{1 \leq i \leq n}$, tel que $V(Q) \subset V$:*
pour chaque arête $(i,j) \in a(\Gamma)$ liant les sommets α_i et α_j de Γ, il existe d'après les lemmes précédents un entier positif $r_{(i,j)}(Q)$ tel que :
$\beta_i - \beta_j = r_{(i,j)}(Q) n_{i,j}$:
1) $V(Q)$ est strictement inclus dans $V(P)$ si et seulement si l'un des $r_{(i,j)}(Q)$ est nul.
2) $r(Q) = (r_{(i,j)}(Q)) \in \mathbb{N}^{a(Q)}$ est solution du système d'équations linéaires à coefficients entiers, $\Sigma(V) = \{\sum_{s \in \gamma} r_s n_s = 0 \ / \gamma \in C(\Gamma)\}$ où $C(\Gamma)$ est l'ensemble des circuits contenus dans Γ.
3) Réciproquement si $r = (r_s) \in \mathbb{N}^{a(Q)}$ est solution du système d'équations linéaires $\Sigma(V)$, il existe Q tel que $V(Q) \subset V(P)$ et $r(Q) = r$.
$V(Q)$ est la réunion des $B_{i,j}$ tels que $r_{i,j}(Q) \neq 0$.
4) Si $r(Q_1) = r(Q_2)$ il existe $\delta \in \mathbb{Z}^n$ tel que $Q_2 = X^\delta Q_1$.

Démonstration. 1) En effet l'inclusion entre $V(Q)$ et $V(P)$ est stricte si et seulement si il existe i et j tels que $\beta_i = \beta_j$, c'est à dire que les ouverts A_i et A_j (composantes connexes de $T^n - V$) soient inclus dans le même $A_\beta(Q)$.

2) C'est la condition classique de $V(P)$ vu comme graphe équilibré...

3) Là aussi c'est la construction classique [16] : en se fixant une valeur suffisamment grande de β_1 (pour éviter de trouver ensuite des exposants négatifs. Mais on peut bien sûr corriger ensuite...) sur A_1, on obtient les valeurs des exposants sur les ouverts contigus A_i par $\beta_i - \beta_1 = r_{(i,1)} n_{i,1}$, en notant $(i,1)$ l'arête correspondante, puis de proche en proche, sur tous les A_i, la compatibilité de ces choix étant justement assurée par le fait que r est solution du système $\Sigma(V)$.
Il est clair que l'arête de Γ sera une arête du graphe associé à Q si et seulement si $\beta_i \neq \beta_j$, c'est à dire $r_{i,j} \neq 0$.

4) Le seul choix est en fait celui de l'exposant sur A_1... d'où le passage de l'une à l'autre solution... □

Lemme 9. *1) Si $V = V(P)$, $R(V) = \{r(Q) \ / \ V(Q) \subset V\}$ est un sous-monoïde de $\mathbb{N}^{a(P)}$. Le $\mathbb{Z}$-module engendré $T(V)$ est donc libre de rang fini.*
2) $T(V) \cap \mathbb{N}^{a(P)} = R(V)$.

Démonstration. 1) On a vu ci-dessus que l'ensemble des

$$\{S(Q) = (\beta_1, \ldots, \beta_k) \ / \ V(Q) \subset V\}$$

est un sous-monoïde de $(\mathbb{N}^n)^k$. On en déduit aisément qu'il en est de même pour $R(V)$. Il s'ensuit classiquement que le sous $\mathbb{Z}$-module engendré, sous module d'un $\mathbb{Z}$-module libre de type fini, est lui-même libre de type fini.
2) Si $r = (r_a) \in T(V)$, c'est la différence de deux éléments de $R(V)$ et donc une solution du système d'équation $\Sigma(V)$. Il résulte du 3) du lemme précédent que si les r_a sont tous positifs, il existe bien Q tel que $r = r(Q)$ et r appartient bien à $R(V)$. □

Nous pouvons maintenant démontrer le résultat annoncé :

Théorème 5.1. *Soit T le semi-corps des réels max-plus.*
Si P et Q appartiennent à $T\{X_i\}_{i\in\mathbb{N}}$, $V(Q) \subset V(P)$ si et seulement si Q divise une puissance de P.
On a donc $I(V(Q)) = \sqrt{(Q)}$.

Démonstration. Avec les notations précédentes, il existe $k \in \mathbb{N}$ tel que $kr(P) \geq r(Q)$. Comme $kr(P) - r(Q)$ appartient à $R(V)$ d'après le lemme précédent, par définition de $R(V)$ il existe U tel que : $V(U) \subset V$ et $r(U) = kr(P) - r(Q)$; on a alors immédiatement $P^k = QU$. □

Remarque 5.2. Nous retrouvons bien le résultat de E. Shustin et Z. Izhakian ([10], Th 2.1) : ils caractérisent les éléments P de la racine de l'idéal engendré par un polynôme Q par la même condition $V(Q) \subset V(P)$, mais comme ils ne considèrent que les zéros dans $(T^*)^n$, ils ajoutent (de ce fait) une autre condition (énoncée en termes de dérivées partielles qui, avec les notations ci-dessus, se traduit par : si $A_\alpha(P) \subset A_\beta(Q)$ alors $\alpha_i \neq 0$ dès que $\beta_i \neq 0$).

Il est cependant facile de voir que, si le terme constant de P n'est pas nul, celui de Q ne peut l'être (sinon l'origine serait dans $V(Q)$) et que donc de proche en proche, la condition supplémentaire donnée découle bien dans ce cas de la condition $r(Q) \leq r(P)$ qui est conséquence de la première condition $V(Q) \subset V(P)$ (qui est, dans ce cas, la même que la nôtre).

Par contre en excluant les zéros appartenant aux axes, il est clair que la première condition n'est plus suffisante (X_iP ne divisant pas une puissance de P si P n'est pas déjà multiple de X_i).

5.2. **Décomposition de V en hypersurfaces irréduciblles**

Nous dirons qu'une hypersurface est irréductible si elle n'est pas la réunion d'hypersurfaces strictement incluses.

Nous allons appliquer les résultats précédents pour trouver les décompositions d'une hypersurface en réunion d'hypersurfaces irréductibles et préciser les décompositions associées du polynôme définissant cette hypersurface.

On appellera support de $r = (r_a) \in \mathbb{N}^{a(P)}$ (notation $supp(r)$) l'ensemble des $a \in a(P)$ tels que $r_a \neq 0$, si bien que W est égal à V si et seulement si le support de $r(Q)$ est égal à $a(P)$ tout entier.
On notera dans la suite $\Lambda = \Lambda(V)$ l'ensemble $\{supp(r(Q)) \ / \ V(Q) \subset V\}$.

Proposition 5.3. *Soit $Q = \sum \mu_\beta X^\beta \in T\{X_i\}_{1 \leq i \leq n}$, tel que $V(Q) = W \subset V$:*
1) W est irréductible si et seulement si $supp(r(Q))$ est minimal pour l'inclusion dans Λ.
En particulier V est réductible si et seulement s'il contient strictement un $V(Q)$.
2) V est irréductible si et seulement si $T(V)$ est de rang 1.
Il existe alors un polynôme R tel que $V(R) = V(P)$ et pour tout Q vérifiant $V(Q) = V(P)$, il existe un entier l tel que $Q = R^l$.
3) Il existe une famille finie d'irréductibles distincts, $V_1, \ldots, V_p$ tels que $V = V_1 \cup \cdots \cup V_p$.

Démonstration. 1) Si W n'est pas irréductible, il contient un $V(S)$ strictement plus petit et le support de $r(S)$ est aussi strictement plus petit que celui de $r(Q)$.
Si $supp(r(S))$ est contenu strictement dans $suppr(r(Q))$, il existe $m \in \mathbb{N}^*$ tel que $r(S) \leq mr(Q)$ (i.e. $r_a(S) \leq mr_a(Q)$ pour tous les $a \in a(\Gamma)$). On peut alors trouver deux entiers p et q tels que $qr(Q) - pr(S)$ soit positif, avec un support strictement inférieur à celui de $r(Q)$, mais contenant nécessairement $supp(r(Q)) - supp(r(S))$... (soit c= s/t, l'inf des rapports $mr_a(Q)/r_a(S)$, pour $r_a(S) \neq 0$, $tmr(Q) - sr(S)$ convient). Il existe donc d'après le lemme précédent, un polynôme S' tel que $supp(r(S)) \cup supp(r(S')) = supp(r(Q))$ et on a alors $V(S) \cup V(S') = W$, qui n'est donc pas irréductible.

2) Si V n'est pas irréductible, comme ci-dessus, il est clair que $R(V)$ contient deux éléments non colinéaires...

Réciproquement si $R(V)$ contient deux éléments non colinéaires on peut comme précédemment en construire un troisième dont le support est strictement plus petit... et V ne peut être irréductible...
Le reste découle de ce que, dans ce cas, un générateur de $T(V)$ peut être pris dans $R(V)$, puisque si r est un générateur de $T(V)$, r (ou $-r$) appartient à $R(V)$.

3) En itérant le procédé utilisé au 1, le support de V peut s'écrire comme réunion de supports minimaux... □

Remarque 5.4. Il est bien connu que cette décomposition n'est pas nécessairement unique !
On a par exemple $(X+1)(Y+1)(X+Y) = (X+Y+1)(X+Y+XY)$.

Lemme 10. *Soit $Q = \sum \mu_\beta X^\beta \in T\{X_i\}_{1\leq i\leq n}$, tel que $V(Q) = W \subset V$: Q est irréductible si et seulement si $r(Q)$ est minimal dans $R(V)$.*

Démonstration. S'il existe $r \in R(V)$, $r < r(Q)$, $r = r(U)$ et U divise Q...
La réciproque est évidente. □

Rappelons que W est irréductible si $supp(r(Q))$ est minimal dans Λ, ce qui est a priori, plus fort. Si Q est irréductible et $V(Q)$ aussi, on dira donc que Q est *fortement irréductible.*

Théorème 5.5. *Soit $V = V(P)$. Il existe une famille finie de polynômes fortement irréductibles $P_1, \ldots, P_t$ telle que les $V(P_i)$ forment une décomposition de V en hypersurfaces irréductibles et telle que :*

$$I(V) = \sqrt{(P_1 \cdots P_t)} = \sqrt{(P)}$$

(où $\sqrt{I} = \{Q \in T\{X_1, \cdots, X_n\} \ / \ \exists k \in \mathbb{N},\ Q^k \in I\}$).

Démonstration. D'après la proposition précédente, on peut décomposer V en une réunion d'hypersurfaces irréductibles distinctes V_i, $1 \leq i \leq k$, et choisir pour chaque i un P_i irréductible ($r(P_i)$ étant minimal) tel que $V(P_i) = V_i$.

Le reste en découle car d'une part $supp(r(P)) = supp(r(P_1 \cdots P_k)$ et donc, $\sqrt{(P_1 \cdots P_t)} = \sqrt{(P)}$; d'autre part si Q appartient à $I(V)$, en changeant les rôles, il existe un $s \in \mathbb{N}$ tel que P divise Q^s. □

Remarque 5.6. S'il est vraisemblable qu'irréductible n'implique pas fortement irréductible, la question reste ouverte.

On peut donner une condition nécessaire et suffisante pour que P engendre $I(V)$ (cette condition est beaucoup plus forte que "sans facteurs multiples" et $I(V)$ n'est pas en général principal). Nous dirons que P est *primitif* si tous les $r_a(P)$ sont égaux à 1.

Proposition 5.7. *$I(V(P)) = (P)$ si et seulement si P est primitif.*

Démonstration. Il découle de ce qui précède que l'on peut, pour un polynôme donné P, définir un graphe $\Gamma(V(P)) = (s(V(P)), a(V(P)))$ tel que $V(Q) \subset V(P)$ si et seulement si $\Gamma(V(Q))$ est un sous graphe de $\Gamma(V(P))$ et un graphe pondéré (qui est le polygone de Newton de P),
$G(P) = (s(V(P)), a(V(P)), r(P))$ tel que Q divise P si et seulement si $G(Q) \leq G(P)$ (i.e. $G(Q)$ est un sous-graphe de $G(P)$ et $r(Q) \leq r(P)$, $r_a(Q)$ valant 0 pour les arêtes n'appartenant pas à $G(Q)$).

Si P est primitif et U est dans $I(V)$, $V(P) \subset V(U)$ et nécessairement $r(P) \leq r(U)$ et donc P divise bien U.

Réciproquement, il existe un polynôme primitif $R \in I(V)$, et si P n'est pas lui-même primitif, il ne peut pas diviser R : si $P = \sum_i \lambda_i X^{\alpha_i}$ et $V(P) = \cup_{(i,j)\in a(V)} B_{i,j}$, le polynôme $R = \Pi_{(i,j)\in a(V)}(\lambda_i X^{\alpha_i} + \lambda_j X^{\alpha_j})$ est bien primitif, tel que :
$V(R) = \cup_{(i,j)\in a(V)} V(\lambda_i X^{\alpha_i} + \lambda_j X^{\alpha_j})$, et on a bien $V(P) \subset V(R)$. □

Exemple 5.8. Soit $T = (R_+, max, +)$:
a) $X + Y + 1$, polynôme fortement irréductible et primitif, divise bien $(X + Y + a)(X + 1)(Y + 1)$, pour $0 \leq a \leq 1$...
b) Par contre $X^2 + Y + 1$, fortement irréductible mais non primitif ne divise pas le polynôme de $I(V)$, $(X + Y + a)(X + 1)(Y + 1)$, $0 \leq a \leq 1$ (mais divise bien son carré)... ni d'ailleurs $1 + X + X^2Y + Y^2$ qui est aussi dans $I(V)$.
Ceci montre d'ailleurs que $I(V(X^2 + Y + 1))$ n'est pas monogène...

Remarque 5.9. Les méthodes utilisées dans les démonstrations précédentes peuvent donner lieu à des algorithmes : les décompositions d'une hypersurface $V = V(P)$ en réunion d'hypersurfaces irréductibles et la détermination de générateurs de $I(V)$ se ramènent à la recherche de solutions minimales en entier, $r = (r_\alpha)$, d'un système d'équations linéaires, dès lors que l'on a explicitement une description complète de V (arêtes et poids ou polygone de Newton de P)... On en déduit alors aisément les factorisations du polynôme tropical (rationnel) P en produit de polynômes irréductibles...

5.3. **Algèbre des fonctions polynomiales sur** $V(P)$

L'algèbre des fonctions polynomiales sur une hypersurface $V = V(P) \subset K^n$ peut se définir, de même que dans le cas classique, comme étant l'algèbre des restrictions à V des fonctions polynomiales sur K^n.

On peut alors énoncer le :

Théorème 5.10. *Soient T le semi-corps des réels max-plus, P un polynôme rationnel appartenant à $T\{X_1, \ldots, X_n\}$ et*
$I = \sqrt{(P)} = \{Q \in T\{X_1, \ldots, X_n\} \ / \ \exists k \in \mathbb{N},\ Q^k \in I\}$ la racine de l'idéal engendré :
a) I est égal à l'intersection $I(V)$ de tous les $Ker\ \epsilon_x$ pour $x \in V(P)$, où ϵ_x est le morphisme d'évaluation en x, $P \longmapsto P(x)$.
b) Si les classes de deux polynômes A et B de $T\{X_1, \ldots, X_n\}$ sont égales modulo I, alors $A(x) = B(x)$ pour tous les $x \in V(P)$.
c) Si P ne s'annule pas et si $A(x) = B(x)$ pour tous les $x \in V(P)$, alors A et B sont congrus modulo I .
d) Si P ne s'annule pas, l'algèbre quotient $T\{X_1, \ldots, X_n\}/I(V)$ est donc isomorphe à l'algèbre des fonctions polynomiales sur V.

Démonstration. a) x est un zéro de P si et seulement si ϵ_x est singulier en P...
b) En effet, A et B sont congrus modulo I si et seulement si, pour tout couple $(U, R) \in I \times T\{X_1, \ldots, X_n\}$, $AU + R \in I \Leftrightarrow BU + R \in I$ et $(A + I) \cap (B + I) \neq \emptyset$.
$APU + R$ appartient à I si et seulement si $V(P) \subset V(APU + R)$, c'est à dire si et seulement si, pour chaque $x \in V(P)$, R est singulier en x ou $R(x) \leq APU(x)$.
En prenant $R \in T$, on obtient que pour tout $x \in V(P)$ tel que $P(x) \neq 0$, $R \leq AP(x)$ si et seulement si $R \leq BP(x)$ ce qui implique bien $A(x) = B(x)$. Si $P(x) = 0$, l'autre condition implique encore $A(x) = B(x)$.
c) Dans ce sens, si A et B coïncident sur $V(P)$ on a donc que :
$AU + R \in I \Leftrightarrow BU + R \in I$. De plus si le terme constant p_0 de P n'est pas nul, pour tout polynôme A il existe U tel que $A \leq PU$, et $A + I$ ne peut être disjoint de $B + I$ ($A \leq PA/p_0$). □

Remarque 5.11. On peut donc constater que si les classes de A et B sont égales modulo I, les fonctions définies par A et B sont bien égales sur $V(P)$, sans la condition que P ne s'annule pas. Par contre, il est aisé de donner des contre-exemples qui montrent que la réciproque est fausse :

pour $P = X^2 + Y^3$, et $A = X + Y + X^3$, $B = Y + X^3$, on a $(A + I) \cap (B + I) = \emptyset$ car la valuation en X d'un élément de $B + I$ ne peut être égale à 1(deux représentants du même polynôme rationnel ont les mêmes valuations car les monômes extrémaux sont les mêmes) ; par contre sur $V(P)$, soit $x^3 \geq x \geq y \geq 1$ et $A(x, y) = x^3 = B(x, y)$, soit $1 \geq y \geq x \geq x^3$ et $A(x, y) = y = B(x, y)\ldots$

Références

[1] M. Akian, R. Bapat & S. Gaubert – « Max-plus algebras, chapter 25 in the handbook of linear algebra, », in *Discrete Mathematics and Its Applications, Volume 39,*, Chapman and Hall, 2007.

[2] F. Aroca – « Krull-tropical hypersurfaces », *Annales de la faculté des sciences de Toulouse* (2010), p. 525–538.

[3] S. Banerjee – « Tropical geometry over higher dimensional local fields », *arXiv : 1105.5873 v2* (2012).

[4] D. Castella – « L'algèbre tropicale comme algèbre de la caractéristique 1 : Polynômes rationnels et fonctions polynomiales », *arXiv : 0809.0231* (2008).

[5] ———, « Eléments d'algèbre linéaire tropicale », *Linear Algebra and Its Applications* **432** (2010), p. 1460–1474.

[6] D. Grigoriev – « On a tropical dual Nullstellensatz », *Adv. Appl. Math.* **48** (2012), p. 457–464.

[7] U. Hebisch & H. Weinert – *Semirings. algebraic theory and application in computer sciences*, World scientific, Singapore, 1998.

[8] I. Itenberg, G. Mikhalkin & E. Shustin – *Tropical algebraic geometry*, second éd., Oberwolfach Seminars, vol. 35, Birkhäuser Verlag, Basel, 2009.

[9] Z. Izhakian – « Tropical algebraic sets ideals and an algebraic Nullstellensatz », *IJAC* **18(6)** (2008), p. 1067–1098.

[10] Z. Izhakian & L. Rowen – « The tropical rank of a tropical matrix », *Comm. in Algebra* **37** (2009), p. 3912–3927.

[11] ———, « Supertropical algebra », *Adv. in Math.* **225** (2010), p. 2222–2286.

[12] V. N. Kolokoltsov & V. P. Maslov – *Idempotent analysis and its applications*, Kluver academic publishers, Dordrecht, 1997.

[13] P. Lescot – « Absolute algebra II ideals and spectra », *J. of Pure and Applied Algebra* **215(7)** (2011), p. 1782–1790.

[14] G. L. Litvinov & V. P. Maslov – « Idempotent mathematics and mathematical physics », in *Number 377*, Contemp. Math. Amer. Math. Soc., 2005.

[15] G. Mikhalkin – « Amoebas of algebraic varieties and tropical geometry », in *Different faces of geometry* (v. Int. Math. Ser.(N.Y.), éd.), Kluwer/Plenum, NewYork, 2004, p. 257–300.

[16] ———, « Decomposition into pairs-of-plants for complex algebraic hypersurfaces », *Topology* **43(5)** (2004), p. 1035–1065.

[17] J. Richter-Gebert, B. Sturmfels & T. Theobland – « First steps in tropical geometry », *Contemporary Mathematics* **377** (2005), p. 289–317.

[18] E. Shustin & Z. Izhakian – « A tropical Nullstellensatz », *Proc. Amer. Math. Soc.* **135 (12)** (2007), p. 3815–3821.

[19] D. Speyer & B. Sturmfels – « Tropical mathematics », *Mathematics Magazine* **82 (3)** (2009), p. 163–173.

[20] L. Tabera – « Tropical resultants for curves and stable intersection », *Rev. Mat. Iberoam* **24** (2008), p. 941–961.

[21] O. Viro – « Dequantization of real algebraic geometry on logarithm », in *European Congress of Mathematics, Vol. I, Barcelone* (P. M. 201, éd.), Birkhäuser, 2001, p. 135–146.

Dominique Castella
Laboratoire d'Informatique et de Mathématiques
Université de la Réunion
Pôle Technologique Universitaire
Bâtiment 2, 2 rue Joseph Wetzell
97490 Sainte Clotilde,
France
dominique.castella@univ-reunion.fr