Théorème de Schmüdgen

Richard Leroy

Séminaire de DEA

Résumé

On donne ici une démonstration algébrique du théorème de Schmüdgen. On étudiera donc certains liens entre polynômes positifs et sommes de carrés de polynômes, et on donnera au passage une réponse au 17e problème de Hilbert.

Table des matières

1 Positivstellentsatz

La première partie de ce document vise à démontrer le Positivstellensatz, apportant ainsi une réponse au 17e problème de Hilbert.

1.1 Préordres

Dans ce document, A sera un anneau commutatif unitaire. On sera amené à considérer les sommes de carrés d'éléments de A :

$$\sum A^2 := \{\sum_{finie} a_i^2 / a_i \in T\}$$

Définition 1.1.1 *Un préordre sur A est un sous-ensemble $T \subseteq A$ vérifiant :*

$$\begin{cases} T+T \subseteq T \\ TT \subseteq T \\ \forall a \in A, a^2 \in A \end{cases}$$

Exemple : $\sum A^2$ est un préordre de A, tel que pour tout préordre $T \subseteq A$, on ait $\sum A^2 \subseteq T$: c'est le plus petit préordre de A pour l'inclusion.

Exemple : Si T est un préordre de A, le préordre de A engendré par $S = \{g_1, ..., g_s\}$ sur T est :

$$T[S] = \sum_{e \in \{0,1\}^s} Tg^e = \left\{ \sum_{e \in \{0,1\}^s} t_e g^e / \ \forall e \in \{0,1\}^s, t_e \in T \right\}$$

où l'on a noté $g^e = g_1^{e_1} ... g_s^{e_s}$ pour $e = (e_1, ..., e_s)$.

- si $S = \{g\}$, $T[S] = T[g] = T + Tg$
- si $S = \{g, h\}$, $T[S] = T[g, h] = T + Tg + Th + Tgh$
- si $T = \sum A^2$, $\sum A^2[S] = \left\{ \sum_{e \in \{0,1\}^s} \sigma_e g^e / \ \forall e \in \{0,1\}^s, \sigma_e \in \sum A^2 \right\}$.

Ce préordre est appelé préordre de A engendré par S, et c'est le plus petit préordre de A contenant S.

1.2 Positivstellentsatz

On note $\mathbb{R}[X] = \mathbb{R}[X_1, ..., X_n]$. Soit $S = \{g_1, ..., g_s\} \subset \mathbb{R}[X]$.

On pose $K = K_S = \{x \in \mathbb{R}^n / \ \forall i \in \{1, ..., s\}, g_i(x) \geq 0\}$.

Soit $T = T_S = \sum \mathbb{R}[X]^2[S]$ le préordre sur $\mathbb{R}[X]$ engendré par S.

Théorème 1.2.1 (Positivstellensatz) *(Stengle,1974)*
Soit $S = \{g_1, ..., g_s\} \subset \mathbb{R}[X]$, $K = K_S$ et $T = T_S$ définis comme ci-dessus. Alors, pour tout $f \in \mathbb{R}[X]$, on a :

(i) $f > 0$ *sur* $K_S \Leftrightarrow \exists p, q \in T_S, pf = 1 + q$

(ii) $f \geq 0$ *sur* $K_S \Leftrightarrow \exists m \in \mathbb{N}, \exists p, q \in T_S, pf = f^{2m} + q$

(iii) $f = 0$ *sur* $K_S \Leftrightarrow \exists m \in \mathbb{N}, -f^{2m} \in T_S$

Corollaire 1.2.2 (17e problème de Hilbert)
Soit $f \in \mathbb{R}[X] = \mathbb{R}[X_1, ..., X_n]$ tel que $f \geq 0$ sur $\mathbb{R}^n$.
Alors $f \in \sum \mathbb{R}(X)^2$, ie f est la somme de carrés de fractions rationnelles réelles.

Preuve :
On peut supposer $f \neq 0$.
D'après le Positivstellensatz (ii) appliqué avec $S = \emptyset$ (on a alors $K = \mathbb{R}^n$, $T = \sum \mathbb{R}[X]^2$) : $\exists m \in \mathbb{N}$, $pf = \underbrace{f^{2m} + q}_{\neq 0 \ car \ f \neq 0}$ avec $p, q \in \sum \mathbb{R}[X]^2$.
Par conséquent, $p \neq 0$, donc $f = \frac{1}{p}(f^{2m} + q) = \underbrace{\frac{1}{p^2} p(f^{2m} + q)}_{\in \sum \mathbb{R}(X)^2}$ ■

1.3 Preuve du Positivstellensatz

On va démontrer le (i), puis l'implication $(i) \Rightarrow (ii)$.

1.3.1 Preuve du (i)

On va avoir besoin de deux lemmes.

Lemme 1.3.1 *Soit A un anneau commutatif unitaire.*
On suppose que P est un préordre de A maximal pour la condition « $-1 \notin P$». Alors :
(i) $P \cup -P = A$
(ii) $\mathcal{P} = P \cap -P$ est un idéal premier de A

Preuve :

• (i) Supposons $P \cup -P \neq A$. Soit $g \in A \backslash (P \cup -P)$.
Alors par maximalité de P, on a :
$\begin{cases} -1 \in P + gP \\ -1 \in P - gP \end{cases}$
donc $-1 = s_1 + gt_1 = s_2 - gt_2$ avec les $s_i, t_i \in P$.
On a alors :
$\begin{cases} -gt_1 = s_1 + 1 \\ gt_2 = s_2 + 1 \end{cases}$
$\Rightarrow -g^2 t_1 t_2 = (s_1 + 1)(s_2 + 1) = 1 + s_1 + s_2 + s_1 s_2$
$\Rightarrow -1 = g^2 t_1 t_2 + s_1 + s_2 + s_1 s_2 \in P$
Contradiction !
Par conséquent, $P \cup -P = A$.

• (ii) Soit $\mathcal{P} = P \cap -P$.
Alors clairement :
$$\begin{cases} 0 \in \mathcal{P} \\ \mathcal{P} + \mathcal{P} \subset \mathcal{P} \\ -\mathcal{P} \subset \mathcal{P} \\ P\mathcal{P} \subset \mathcal{P} \end{cases}$$
d'où $A\mathcal{P} = (P \cup -P)\mathcal{P} \subset P\mathcal{P} \cup -P\mathcal{P} \subset \mathcal{P}$: $\mathcal{P}$ est un idéal de A.
Montrons qu'il est premier.
Soient $g, h \notin \mathcal{P}$ tels que $gh \in \mathcal{P}$. Quitte à remplacer g, h par $-g, -h$, on peut supposer $g, h \notin P$ (car $A = P \cup -P$).
Alors, par maximalité de P, il vient :
$$\begin{cases} -1 \in P + gP \\ -1 \in P + hP \end{cases}$$
donc $-1 = s_1 + gt_1 = s_2 + ht_2$ avec les $s_i, t_i \in P$
$\Rightarrow ght_1t_2 = (1 + s_1)(1 + s_2) = 1 + s_1 + s_2 + s_1s_2$
$\Rightarrow -1 = s_1 + s_2 + s_1s_2 - ght_1t_2 \in P$: contradiction !
Par conséquent, $\mathcal{P}$ est un idéal premier de A. ■

Lemme 1.3.2 *Soit A un anneau commutatif unitaire.*
On suppose que P est un préordre de A tel que
• $A = P \cup -P$
• $\mathcal{P} := P \cap -P$ *est un idéal premier de A.*
Alors P induit un unique ordre sur $F = Frac(A/\mathcal{P})$ tel que

$$\frac{\bar{g}}{\bar{h}} \geq 0 \Leftrightarrow gh \in P \ (avec\ \bar{h} \neq 0).$$

Preuve :
Laissée au lecteur. ■

On peut maintenant démontrer le (i) du Positivstellensatz.

Soit donc $f \in \mathbb{R}[X]$ tel que $f > 0$ sur K_S.
Supposons qu'il n'existe pas $p, q \in T_S$ tels que $pf = 1 + q$, ie $-1 = q - fp$.
Alors $-1 \notin T_S - fT_S$.
Le lemme de Zorn assure l'existence d'un préordre P de $\mathbb{R}[X]$ tel que $T_S - fT_S \subset P$, maximal pour la condition $-1 \notin P$.
Du lemme 1.3.1, on déduit que $\mathbb{R}[X] = P \cup -P$ et que si l'on pose $\mathcal{P} = P \cap -P$, alors $\mathcal{P}$ est un idéal premier de $\mathbb{R}[X]$.
D'après le lemme 1.3.2, P induit un ordre sur $F = Frac(\mathbb{R}[X]/\mathcal{P})$ via :

$$\frac{\bar{g}}{\bar{h}} \geq 0 \Leftrightarrow gh \in P.$$

Le morphisme composé $\mathbb{R} \hookrightarrow \mathbb{R}[X] \to \mathbb{R}[X]/\mathcal{P} \hookrightarrow F$ montre que F est une extension de $\mathbb{R}$, dont l'ordre étend l'unique ordre de $\mathbb{R}$.
D'autre part, il existe $x = (x_1, ..., x_n) \in F^n$ tel que

$$\begin{cases} \forall i \in \{1, ..., s\}, g_i(x) \geq 0 \\ f(x) \leq 0 \end{cases}$$

En effet, posons $x_i = \bar{X}_i = X_i + \mathcal{P}$.
Alors : $\forall g \in \mathbb{R}[X],\ g = \sum a_k X_1^{k_1} ... X_n^{k_n},\ \bar{g} = \sum a_k x_1^{k_1} ... x_n^{k_n} = g(x)$.
Reste à vérifier que $\bar{g_i} \geq 0$ et que $\bar{f} \leq 0$.
$\bar{g_i} \geq 0$ car $g_i \in T_S \subset T_S - fT_S \subset P$.
$\bar{f} \leq 0$ car $-f \in T_S - fT_S \subset P$.
On peut donc appliquer le principe de transfert de Tarski ; on obtient alors l'existence de $y \in \mathbb{R}^n$ (et non plus dans F^n) tel que

$$\begin{cases} \forall i \in \{1, ..., n\}, g_i(y) \geq 0\ (ie\ y \in K_S) \\ f(y) \leq 0 \end{cases}$$

ce qui entre en contradiction avec l'hypothèse $f > 0$ sur K_S ■

1.3.2 Preuve du (ii)

On suppose $f \geq 0$ sur K_S. Le principe est de passer à une dimension supérieure. On note $(x, y) = (x_1, ..., x_n, y) \in \mathbb{R}^{n+1}$ et $\mathbb{R}[X, Y] = \mathbb{R}[X_1, ..., X_n, Y]$.
On pose $S' = \{g_1, ..., g_s, Yf - 1, -Yf + 1\}$.
Alors $K_{S'} = \{(x, y) \in \mathbb{R}^{n+1} / \ \forall i = 1, ..., s,\ g_i(x) \geq 0,\ yf(x) = 1\}$.
Par conséquent, sur $K_{S'}$, $f(x, y) = f(x) > 0$, donc d'après le (i),

$$\exists p', q' \in T_{S'},\ p'(X, Y)f(X) = 1 + q'(X, Y).$$

En remplaçant Y par $1/f(X)$ dans cette égalité et en chassant les dénominateurs en multipliant de chaque côté par $f(X)^{2m}$ pour m suffisamment grand, on obtient :

$$p(X)f(X) = f(X)^{2m} + q(X)$$

avec

$$p(X) = f(X)^{2m} p'(X, \frac{1}{f(X)})$$

$$q(X) = f(X)^{2m} q'(X, \frac{1}{f(X)})$$

Pour finir la preuve, il suffit de vérifier que $p, q \in T_S$ pour m suffisamment grand. Par définition de $T_{S'}$, $p'(X, Y)$ est une somme de termes de la forme

$$\sigma(X, Y) g_1(X)^{e_1} ... g_s(X)^{e_s} (Yf(X) - 1)^{e_{s+1}} (-Yf(X) + 1)^{e_{s+2}}$$

où $e_i = 0$ ou 1, $\sigma(X,Y) \in \sum \mathbb{R}[X,Y]^2$, disons $\sigma(X,Y) = \sum h_j(X,Y)^2$.
En remplaçant Y par $1/f(X)$, les termes pour lesquels $e_{s+1} = 1$ ou $e_{s+2} = 1$ sont nuls. Pour les termes restants, on multiplie par $f(X)^{2m}$, où m est supérieur à la plus grande puissance de Y apparaissant dans les $h_j(X,Y)$.
Si on écrit $h_j(X,Y) = \sum_{i=0}^{l} h_{ij}(X)Y^i, l \leq m$, alors :

$$f(X)^m h_j(X, \frac{1}{f(X)}) = \sum_{i=0}^{l} h_{ij}(X) f(X)^{m-i} \in \mathbb{R}[X]$$

et donc $f(X)^{2m}\sigma(X, \frac{1}{f(X)}) = \sum_j [\underbrace{f(X)^m h_j(X, \frac{1}{f(X)})}_{\in R[X]}]^2 \in \sum R[X]^2$.
L'argument pour q est le même. ■

2 Théorème de Kadison-Dubois

Dans cette section, A désignera un anneau commutatif unitaire contenant $\mathbb{Q}$.

2.1 Prépremiers

Définition 2.1.1
• *Un sous-ensemble $T \subseteq A$ est un prépremier de A (en anglais preprime) si*

$$\begin{cases} T + T \subseteq T \\ TT \subseteq T \\ \mathbb{Q}^+ \subseteq T \end{cases}$$

• *Un prépremier T de A est dit archimédien si*

$$\forall a \in A, \exists n \in \mathbb{N}^*, n \pm a \in T.$$

• *Un prépremier T de A est dit générateur si $T - T = A$.*

Remarque :
(i) $T - T$ est un sous-anneau de A. Cela vient des identités :

$$(t_1 - t_2) + (t_3 - t_4) = (t_1 + t_3) - (t_2 + t_4)$$

$$(t_1 - t_2)(t_3 - t_4) = (t_1 t_3 + t_2 t_4) - (t_1 t_4 + t_2 t_3)$$

(ii) $\mathbb{Q}^+$ est le plus petit prépremier de A. Il n'est générateur que si $A = \mathbb{Q}$ ($\mathbb{Q}^+ - \mathbb{Q}^+ = \mathbb{Q}$).

(iii) T est archimédien $\Rightarrow$ T est générateur $(a = (n+a) - n)$
(iv) T est un préodre de $A \Rightarrow$ T est un prépremier générateur de A :
• D'une part, l'égalité $\frac{m}{n} = (\frac{1}{n^2})(mn) = \underbrace{(\frac{1}{n^2}) + ... + (\frac{1}{n^2})}_{mn\ termes}$ montre que $\mathbb{Q}^+ \subset T$.
• D'autre part, l'égalité $a = (\frac{1+a}{2})^2 - (\frac{1-a}{2})^2$ montre que T est générateur.

2.2 T-modules

Définition 2.2.1 *Soit T un prépremier de A.*
(i) $M \subseteq A$ est un $T-$module de A si :

$$\begin{cases} M + M \subseteq M \\ TM \subseteq M \\ 1 \in M \ (ie\ T \subseteq M) \end{cases}$$

(ii) Un $T-$module M de A est dit archimédien si

$$\forall a \in A, \exists n \geq 1, n \pm a \in M.$$

Remarque :
(i) T est un $T-$module
(ii) T archimédien $\Rightarrow$ tout $T-$module M est archimédien (car $T \subseteq M$).

Notation : Si M est un $\sum A^2-$module, on définit H_M par :
$H_M = \{a \in A/\ \exists n \geq 1, n \pm a \in M\}$

Proposition 2.2.2 *Soit M est un $\sum A^2-$module. Alors :*
(i) H_M est un sous-anneau de A contenant $\mathbb{Q}$
(ii) M est archimédien $\Leftrightarrow$ $H_M = A$
(iii) $a^2 \in H_M \Rightarrow a \in H_M$
(iv) $\sum_{i=1}^{k} a_i^2 \in H_M \Rightarrow \forall i \in \{1, ..., k\}, a_i \in H_M$

Preuve :

(i) : Clairement, H_M est un sous-groupe de A contenant $\mathbb{Q}$.
Puisque $ab = \frac{1}{4}[(a+b)^2 - (a-b)^2]$, il suffit, pour prouver la stabilité par multiplication, de montrer que $a \in H_M \Rightarrow a^2 \in H_M$. Ceci se démontre comme suit. Supposons que $n \pm a \in M$. Alors $n^2 + a^2 \in M$ et

$$\begin{aligned} n^2 - a^2 &= \tfrac{1}{2n}[(n+a)(n^2-a^2) + (n-a)(n^2-a^2)] \\ &= \tfrac{1}{2n}[(n+a)^2(n-a) + (n-a)^2(n+a)] \in M \end{aligned}$$

(ii) : clair
(iii) : Si $n - a^2 \in M$, alors $n \pm a = \frac{1}{n}[(n-1) + (n-a^2) + (a \pm 1)^2] \in M$
(iv) : Si $n - \sum a_i^2 \in M$, alors $n - a_i^2 = (n - \sum a_i^2) + \sum_{j \neq i} a_j^2 \in M$,
donc, par (iii), $n \pm a_i \in M$, *ie* $a_i \in H_M$. ■

Corollaire 2.2.3 *Soit M un $\sum \mathbb{R}[X]^2-$module de $\mathbb{R}[X]$ tel que :*

$$\exists k \geq 1, k - \sum_{i=1}^{n} X_i^2 \in M.$$

Alors M est archimédien.

Preuve :
Comme tout élément de $\mathbb{R}^+$ est un carré, on a l'inclusion $\mathbb{R}^+ \subseteq M$, donc $\mathbb{R} \subseteq H_M$ (prendre, pour $x \in \mathbb{R}$, $n = |E(x)| + 1$). La démonstration du (iv) prouve alors que $X_1, ..., X_n \in H_M$. Par conséquent, H_M (qui est un sous-anneau de $\mathbb{R}[X]$ contenant $\mathbb{R}, X_1, ..., X_n$) est égal à $\mathbb{R}[X]$, et le (ii) implique le résultat. ■

2.3 Théorème de Kadison-Dubois

Dans cette section, on étudiera en particulier les morphismes d'anneaux de A dans $\mathbb{R}$.

Notation :
• On pose $\chi = Hom(A, \mathbb{R})$. Pour $a \in A$, on définit $\hat{a} : \begin{cases} \chi \to \mathbb{R} \\ \alpha \mapsto \alpha(a) \end{cases}$
• Si $S \subset A$, on note χ_S le sous-ensemble de χ formé des morphismes d'anneaux $\alpha : A \to \mathbb{R}$ tels que $\alpha(S) \subset \mathbb{R}^+$.

On aura tout d'abord besoin de deux lemmes.

Lemme 2.3.1 *Soit T un prépremier générateur et Q un $T-$module maximal pour la condition $-1 \notin Q$.*
Alors $Q \cup -Q = A$.

Preuve :
Supposons qu'il existe $a \in A \backslash (Q \cup -Q)$.
Alors, par maximalité de Q,

$\begin{cases} -1 \in Q + aT \\ -1 \in Q - aT \end{cases}$
donc $\begin{cases} -1 = s_1 + at_1 \\ -1 = s_2 - at_2 \end{cases}$ $(avec\ s_i \in Q, t_i \in T)$
$\Rightarrow t_1 + t_2 + t_2 s_1 + t_1 s_2 = t_1(1 + s_2) + t_2(1 + s_1) = t_1 t_2 a - t_1 t_2 a = 0$
$\Rightarrow -t_1 = t_2 + t_2 s_1 + t_1 s_2 \in Q$.
Soient $t_3, t_4 \in T$ tel que $a = t_3 - t_4$ (T est générateur).
Alors $-1 = s_1 + t_1 a = s_1 + t_1(t_3 - t_4) = s_1 + t_1 t_3 + t_4(-t_1) \in Q$,
ce qui fournit la contradiction recherchée. ■

Lemme 2.3.2 *Soit T un prépremier générateur et Q un $T-$module tel que $-1 \notin Q$.*
Alors $\mathbb{Q} \cap Q = \mathbb{Q}^+$.

Preuve :

$\supseteq$: Par définition, $\mathbb{Q}^+ \subseteq T \subseteq Q$.
$\subseteq$: Soit $r \in \mathbb{Q} \cap Q$, et supposons que $r < 0$.
Alors $\forall k \geq 1, kr \in Q$
donc $\forall k \geq 1, kr + \mathbb{Q}^+ \subseteq Q$
donc $\underbrace{\bigcup_{k \geq 1} (kr + \mathbb{Q}^+)}_{=\mathbb{Q}} \subseteq Q$
donc $\mathbb{Q} \subseteq Q$: contradiction ! En effet, $-1 \notin Q$. ■

Théorème 2.3.3 *Soit T un prépremier générateur et Q un $T-$module maximal pour la condition $-1 \notin Q$. On suppose de plus Q archimédien.*
Alors il existe un unique morphisme d'anneaux $\alpha : A \to \mathbb{R}$ tel que $Q = \alpha^{-1}(\mathbb{R}^+)$.

Preuve :
• Le lemme 2.3.1 implique que $Q \cup -Q = A$.
• Pour $a \in A$, on pose :

$$\mathcal{U}(a) = \{r \in \mathbb{Q} / \ r - a \in Q\}$$
$$\mathcal{L}(a) = \mathbb{Q} \backslash \mathcal{U}(a)$$

Alors ($\mathcal{L}(a)$,$\mathcal{U}(a)$) est une coupure non triviale de $\mathbb{Q}$, *ie* :

$(i)\ \mathcal{U}(a), \mathcal{L}(a) \subseteq \mathbb{Q}$
$(ii)\ \mathcal{L}(a) \cup \mathcal{U}(a) = \mathbb{Q}$
$(iii)\ \mathcal{L}(a) < \mathcal{U}(a)$

(i) et (ii) sont claires. Montrons (iii).
Soient $u \in \mathcal{U}(a)$ et $l \in \mathcal{L}(a)$. Alors
$u - a \in Q$
$l - a \notin Q$
donc, puisque $A = Q \cup -Q$, $-(l-a) \in Q$
donc $u - l = (u-a) - (l-a) \in Q$
donc $u - l \in \mathbb{Q} \cap Q = \mathbb{Q}^+$. $\diamond$
• $\mathcal{U}(a) \neq \emptyset$:
Q est archimédien, donc $\exists n \geq 1, n - a \in Q$
• De plus, $\mathcal{L}(a) \neq \emptyset$:
Puisque Q est archimédien, $\exists m \geq 1, m + a \in Q$.
Supposons que $-(m+1) - a \in Q$.
Alors $-1 = [-(m+1) - a] + [m + a] \in Q$: contradiction !
Donc $-(m+1) - a \notin Q$, et donc $\mathcal{L}(a) \neq \emptyset$.
• Soit $\alpha : \begin{cases} A \to \mathbb{R} \\ a \mapsto Inf(\mathcal{U}(a)) \end{cases}$
Alors α est un morphisme d'anneaux (laissé au lecteur : considérer la construction de $\mathbb{R}$ par les coupures de Dedekind).
• De plus, α est unitaire :

$$\begin{aligned} \mathcal{U}(1) &= \{r \in \mathbb{Q} / r - 1 \in Q\} \\ &= \{r \in \mathbb{Q} / r - 1 \in \mathbb{Q} \cap Q = \mathbb{Q}^+\} \\ &= [1, +\infty[\cap \mathbb{Q}^+ \diamond \end{aligned}$$

• $\alpha(Q) \subset \mathbb{R}^+$:
On a $\mathcal{U}(q) = \{r \in \mathbb{Q} / r - q \in Q\}$;
Mais les deux conditions $r - q \in Q$ et $r \in \mathbb{Q}$ impliquent

$$r = (r-q) + q \in Q \cap \mathbb{Q} = \mathbb{Q}^+$$

donc $\mathcal{U}(q) \subset \mathbb{Q}^+$, et $Inf(\mathcal{U}(q)) \geq 0$.
• Soit $Q' = \alpha^{-1}(\mathbb{R}^+)$. Q' est un T-module contenant Q et satisfaisant $-1 \notin Q'$ (car $\alpha(-1) = -\alpha(1) = -1$).
Par maximalité de Q, $Q' = Q$.

• **unicité :**
Soit β un autre morphisme d'anneaux de A dans $\mathbb{R}$ tel que

$$\beta^{-1}(\mathbb{R}^+) = \alpha^{-1}(\mathbb{R}^+).$$

Supposons que $\alpha \neq \beta$. Soit donc $a \in A$ tel que $\alpha(a) \neq \beta(a)$, disons $\alpha(a) < \beta(a)$. Alors il existe $r \in \mathbb{Q}$ tel que $\alpha(a) < r < \beta(a)$, d'où $a - r \notin \alpha^{-1}(\mathbb{R}^+)$, mais $a - r \in \beta^{-1}(\mathbb{R}^+)$: contradiction. ■

Corollaire 2.3.4 *Soit M un T-module archimédien, où T est un prépremier générateur.*
Les conditions suivantes sont équivalentes :
(i) $\chi_M \neq \emptyset$
(ii) $-1 \notin M$

Rappel : $\chi_M = \{\alpha : A \to \mathbb{R} / \ \alpha(M) \subset \mathbb{R}^+\}$.

Preuve :

• $(i) \Rightarrow (ii)$: Si $\alpha \in \chi_M$, alors $\alpha(-1) = -1 < 0$, donc $-1 \notin M$.
• $(ii) \Rightarrow (i)$: Supposons que $-1 \notin M$.
Le lemme de Zorn fournit l'existence d'un T-module Q contenant M (donc lui aussi archimédien) et maximal pour la condition $-1 \notin Q$.
Le théorème précédent assure alors l'existence d'un morphisme $\alpha : A \to \mathbb{R}$ tel que $Q = \alpha^{-1}(\mathbb{R}^+)$.
Par conséquent, $M \subset Q = \alpha^{-1}(\mathbb{R}^+)$, et donc $\alpha(M) \subset \mathbb{R}^+$, ie $\alpha \in \chi_M$. ■

On en arrive maintenant au théorème que l'on voulait démontrer dans cette section :

Théorème 2.3.5 (Théorème de Kadison-Dubois, version faible)
Soit M un T-module , où T est un prépremier archimédien.
Alors, pour tout $a \in A$,

$$\hat{a} > 0 \ sur \ \chi_M \Rightarrow a \in M.$$

Remarque : La condition $\hat{a} > 0$ *sur* χ_M équivaut à :

$$\forall \alpha \in \chi_M, \ \alpha(a) > 0$$

Preuve :
Soit $a \in A$ et $M_1 = M - aT$.
La condition $\forall \alpha \in \chi_M, \ \alpha(a) > 0$ implique $\chi_{M_1} = \emptyset$ (car $-a = 0 - a * 1 \in M_1$ et $\alpha(-a) = -\alpha(a) < 0$), et donc, d'après le corollaire précédent, $-1 \in M_1$.
-1 s'écrit alors $-1 = s - at$, avec $s \in M, \ t \in T$,
d'où $at - 1 = s \in M$.
Soit $\Sigma = \{r \in \mathbb{Q} / \ r + a \in M\}$.
Puisque T est archimédien, il existe $n \geq 1$ tel que $n + a \in T$.
$T \subset M \Rightarrow n \in \Sigma$, donc $\Sigma \neq \emptyset$.
Fixons $r \in \Sigma, \ r \geq 0$ et $k \geq 1$ tel que $k - t \in T$.

Alors

$$kr - 1 + ka = \underbrace{\underbrace{(k-t)}_{\in T}\underbrace{(r+a)}_{\in M}}_{\in M} + \underbrace{(ta-1)}_{\in M} + \underbrace{rt}_{\in M} \in M$$

d'où $r - \frac{1}{k} + a = \frac{1}{k}(kr - 1 + ka) \in M$ (car $\frac{1}{k} \in \mathbb{Q}^+ \subset T$)
ie $r - \frac{1}{k} \in \Sigma$.
En itérant, on trouvera un $r \in \Sigma$ vérifiant $r < 0$. On aura alors
$a = \underbrace{(a+r)}_{\in M} + \underbrace{(-r)}_{\in \mathbb{Q}^+ \subset T \subset M} \in M$. ■

3 Théorème de Schmüdgen

On en arrive finalement à la démonstration du théorème de Schmüdgen.

Fixons $S = \{g_1, ..., g_s\} \subset \mathbb{R}[X]$. Posons $T = \sum \mathbb{R}[X]^2$ et reprenons les notations $K = K_S$ et $T = T_S$:
$K = K_S = \{x \in \mathbb{R}^n / \ \forall i \in \{1, ..., s\}, g_i(x) \geq 0\}$
$T = T_S = \sum \mathbb{R}[X]^2[S]$ le préordre sur $\mathbb{R}[X]$ engendré par S.

Théorème 3.0.6 *On a l'équivalence suivante :*
T_S est archimédien $\Leftrightarrow$ K_S est compact.

Remarque : T_S est un préordre, donc est un prépremier. L'hypothèse T_S archimédien signifie que T_S est un préordre supposé archimédien en tant que prépremier.

Preuve :
• Le sens direct ($\Rightarrow$) est laissé au lecteur.
• Réciproquement, supposons K_S compact. Alors K_S est borné, donc

$$\exists k \geq 1, \ k - \sum_{i=1}^{n} X_i^2 > 0 \ sur \ K_S.$$

Le Positivstellensatz implique : $\exists p, q \in T, \ p(k - \sum_{i=1}^{n} X_i^2) = 1 + q$

donc $(1+q)(k - \sum_{i=1}^{n} X_i^2) = \underbrace{p}_{\in T} \underbrace{(k - \sum_{i=1}^{n} X_i^2)^2}_{\in T} \in T.$

Soit $T' = T[k - \sum_{i=1}^{n} X_i^2] = T + (k - \sum_{i=1}^{n} X_i^2)T$. Du corollaire 2.2.3, on déduit

que T' est archimédien
$\Rightarrow \forall a \in \mathbb{R}[X],\ \exists m \geq 1,\ m-a \in T'$
$\Rightarrow m-a = t_1 + (k - \sum_{i=1}^{n} X_i^2)t_2$ (avec les $t_i \in T$)
$$\Rightarrow (m-a)(1+q) = (m-a)p(k-\sum_{i=1}^{n} X_i^2) = \underbrace{t_1(1+q)}_{\in T} + \underbrace{p(k-\sum_{i=1}^{n} X_i^2)^2 t_2}_{\in T} \in T$$

En particulier, pour $a = q$, $\exists m \geq 1,\ m-q \in T'$, et donc
$(m-q)(1+q) \in T$.
D'où :

$$\begin{cases} (m-q)(1+q) = mq - q^2 + m - q \in T\ (L_1) \\ \underbrace{\left(\frac{m}{2} - q\right)^2}_{\in T} = \frac{m^2}{4} - mq + q^2 \in T\ (L_2) \end{cases}$$

$$L_1 + L_2 \Rightarrow m + \frac{m^2}{4} - q \in T$$

$$k(L_1+L_2) + \underbrace{(1+q)(k-\sum_{i=1}^{n} X_i^2)}_{\in T} + \underbrace{q\sum_{i=1}^{n} X_i^2}_{\in T}$$

$$\Rightarrow km + \frac{km^2}{4} - kq + (1+q)(k-\sum_{i=1}^{n} X_i^2) + q\sum_{i=1}^{n} X_i^2 \in T$$

$$\Rightarrow km + \frac{km^2}{4} + k - \sum_{i=1}^{n} X_i^2 \in T$$

$$\Rightarrow k(\frac{m}{2}+1)^2 - \sum_{i=1}^{n} X_i^2 \in T$$

Le corollaire 2.2.3 montre alors que T est archimédien : il suffit de choisir k suffisamment grand pour qu'en plus de la majoration $k - \sum_{i=1}^{n} X_i^2 > 0$ *sur* K_S, on ait $k(\frac{m}{2}+1)^2 \in \mathbb{N}^*$. ■

Théorème 3.0.7 (Schmüdgen) *On suppose que K_S est compact. Alors, pour tout $f \in \mathbb{R}[X]$, on a l'implication :*

$$f > 0 \text{ sur } K_S \Rightarrow f \in T_S.$$

Preuve :
K_S est compact donc T_S est archimédien (d'après le théorème précédent).
D'après le théorème 2.3.5, pour tout $f \in \mathbb{R}[X]$,

$$\hat{f} > 0 \ sur \ \chi_{T_S} = \chi_S \Rightarrow f \in T_S.$$

Mais $\hat{f} > 0 \ sur \ \chi_S$
$\Leftrightarrow \forall \alpha \in \chi_S, \ \alpha(f) > 0$
$\Leftrightarrow \forall x \in K_S, f(x) > 0$ ■

Références

[Mar] Murray Marshall, *Positive polynomials and sums of squares*, Université de Pise.

[PD] A. Prestel, C. N. Deltzell, *Positive polynomials*, Springer.