UNIVERSIDAD DE BUENOS AIRES

Facultad de Ciencias Exactas y Naturales

Departamento de Matemática

Tesis de Licenciatura

Estados puros y certificados de no negatividad

Paula Micaela Escorcielo

Director: Daniel Perrucci

Marzo de 2015

Agradecimientos

A Daniel, por haber aceptado que trabaje a su lado, por haberme presentado y ayudarme a entender el mundo de los estados puros, por su paciencia y dedicación, ¡GRACIAS!

A todos los docentes que se cruzaron en mi camino y lograron que me enamore de la matemática cada vez un poquito más.

A mamá, papá y Ale, por su apoyo incondicional.

A mis amigos, porque sin ellos el mundo sería un lugar mucho más triste.

Índice general

Introducción

Un certificado de positividad o de no negatividad es una identidad algebraica que torna evidente la positividad o la no negatividad de un polinomio multivariado con coeficientes reales en una cierta región. El origen del estudio de los certificados de positividad y de no negatividad se encuentra en el Problema 17 de Hilbert, presentado a principios del siglo XX, que plantea si un polinomio multivariado con ceoficientes reales que toma siempre valores no negativos es necesariamente una suma de cuadrado de funciones racionales. La respuesta afirmativa a este problema llegó con Emil Artin en los años '20 ([1]), dando un gran impulso inicial a la teoría que actualmente se conoce como geometría algebraica real.

Tiempo después, se enuncia y demuestra uno de los certificado de no negatividad que ha tenido mayor repercusión en el área, el Positivstellensatz ([8], [16], [2, Theorem 4.4.2]). En su versión generalizada, dado un sistema de ecuaciones e inecuaciones polinomiales que no admite solución, el Positivstellensatz asegura la existencia de una identidad algebraica que torna evidente este hecho. Existen varios refinamientos de este resultado para casos particulares, entre ellos, los Schmüdgen y Putinar Positivstellensätze ([15], [13]).

En los últimos años ha surgido un interés renovado por el estudio de certificados de no negatividad debido en parte a su estrecha relación con la teoría de optimización ([9], [10]).

El objetivo principal de este trabajo es estudiar nuevas demostraciones, más conceptuales, de los siguientes conocidos certificados de no negatividad: Teorema de Pólya ([11]), Teorema de Reznick ([14]), los antes mencionados Schmüdgen y Putinar Positivstellensätze y un certificado de no negatividad para el caso de poliedros compactos ([7]). Para dicho objetivo estudiamos el trabajo:

S. Burgdorf, C. Scheiderer, M. Schweighofer, Pure States, Nonnegative Polynomial and Sums of Squares. *Comment. Math. Helv.* 87, 2012,

en donde se desarrolla la teoría de estados puros y se obtienen, como aplicación de dicha teoría, nuevas demostraciones de los ya mencionados certificados de no negatividad, así como también nuevos resultados que exceden al propósito de esta tesis.

La presente tesis está estructurada de la siguiente manera. El capítulo 1 está dedicado a enunciar y demostrar el Teorema de Krein-Milman, que garantiza la existencia de puntos extremales de un conjunto bajo ciertas hipótesis. En el capítulo 2 se definen los conceptos de estádo puro y unidad de orden y se estudia la relación entre ellos. En el capítulo 3 se estudia el caso particular en el que los estádos puros están definidos sobre un anillo. El capítulo consta de dos secciones en cada una de las cuales se estudian los estádos puros bajo distintas hipótesis. En ambos casos se muestra que lo estádos puros resultan morfismos de anillos. Finalmente, en el capítulo 4 se encuentran las demostraciones de los certificados de no negatividad utilizando la teoría de estados puros desarrollada en los capítulos anteriores.

Capítulo 1

Teorema de Krein-Milman

Como el nombre del capítulo lo indica, el objetivo es demostrar el Teorema de Krein-Milman que utilizaremos en el Capítulo 2. La referencia principal para este capítulo es [5, Chapter V]; aunque en dicha referencia este resultado se prueba con mayor generalidad para espacios localmente convexos, y aquí lo demostraremos para el espacio $\mathbb{R}^I$ con topología producto, siendo I un conjunto no vacío.

Empecemos recordando el Teorema de Hahn-Banach, un conocido resultado de análisis funcional.

Definición 1.1 *Decimos que $q : \mathbb{R}^I \to \mathbb{R}$ es **sublineal** si:*

(i) $q(x+y) \leq q(x) + q(y)$ *para todo* $x,\ y \in \mathbb{R}^I$,

(ii) $q(\alpha x) = \alpha q(x)$ *para todo* $x \in \mathbb{R}^I$, $\alpha \in \mathbb{R}_{\geq 0}$.

Teorema 1.2 (Hahn-Banach) *Sea $\mathfrak{X}$ un espacio vectorial sobre $\mathbb{R}$ y $q : \mathfrak{X} \to \mathbb{R}$ función sublineal. Dado $\mathfrak{Y} \subseteq \mathfrak{X}$ subespacio y $f : \mathfrak{Y} \to \mathbb{R}$ funcional lineal tal que $f(x) \leq q(x)\ \forall x \in \mathfrak{Y}$, existe $F : \mathfrak{X} \to \mathbb{R}$ funcional lineal tal que $F|_{\mathfrak{Y}} \equiv f$ y $F(x) \leq q(x)\ \forall x \in \mathfrak{X}$.*

Demostración: Ver [5, Theorem 6.2]. ▫

A continuación vamos a ver algunos lemas técnicos que serán de utilidad más adelante.

Lema 1.3 *Dada $f : \mathbb{R}^I \to \mathbb{R}$ lineal y continua. Son equivalentes:*

(i) $f \equiv 0$.

(ii) *Existe* $V \subseteq \mathbb{R}^I$ *abierto,* $0 \in V$ *tal que* $f|_V \equiv 0$.

Demostración: Es claro que *(i)* implica *(ii)*. Para la otra implicación, tomemos $x \in \mathbb{R}^I$ y veamos que $f(x) = 0$. Consideremos $h : \mathbb{R} \to \mathbb{R}^I$ definida por $h(t) = tx$. Dado que h es continua, $h^{-1}(V) \subseteq \mathbb{R}$ es abierto y $0 \in h^{-1}(V)$, entonces existe $\epsilon > 0$ tal que $(-\epsilon, \epsilon) \subseteq h^{-1}(V)$. En particular, $\frac{\epsilon}{2}x \in V$ y por lo tanto $f(\frac{\epsilon}{2}x) = 0$, por linealidad de f se tiene que $f(x) = 0$. □

Lema 1.4 *Sea* $f : \mathbb{R}^I \to \mathbb{R}$ *lineal y continua, no idénticamente nula. Si* $A \subseteq \mathbb{R}^I$ *es abierto convexo, entonces* $f(A) \subseteq \mathbb{R}$ *es un intervalo abierto.*

Demostración: Como A es convexo, $f(A) \subseteq \mathbb{R}$ es convexo y dado que los únicos convexos en $\mathbb{R}$ son los intervalos, tenemos que $f(A)$ es un intervalo. Para ver que es abierto, dado $a \in A$, tenemos dos posibilidades:

- Si $f(a) \neq 0$, consideremos $h : \mathbb{R} \to \mathbb{R}^I$ definida por $h(t) = ta$, $h^{-1}(A) \subseteq \mathbb{R}$ es abierto y $1 \in h^{-1}(A)$, entonces existe $\epsilon > 0$ tal que $(1-\epsilon, 1+\epsilon) \subseteq h^{-1}(A)$ y por lo tanto $(1-\epsilon, 1+\epsilon)f(a) \subseteq f(A)$.
- Si $f(a) = 0$, consideremos $V = A - a \subseteq \mathbb{R}^I$ abierto y $0 \in V$, por el Lema 1.3, $f|_V$ no es idénticamente nula, es decir, existe $x \in V$ tal que $f(x) \neq 0$, consideremos $h : \mathbb{R} \to \mathbb{R}^I$ definida por $h(t) = tx$, $h^{-1}(V) \subseteq \mathbb{R}$ es abierto y $0 \in h^{-1}(V)$, entonces existe $\epsilon > 0$ tal que $(-\epsilon, \epsilon) \subseteq h^{-1}(V)$ y por lo tanto $(-\epsilon, \epsilon)f(x) \subseteq f(V)$. Para terminar basta observar que $f(V) = f(A)$.

□

Lema 1.5 *Si* $A \subseteq \mathbb{R}^I$ *es convexo, entonces:*

(i) $\overline{A}$ *es convexo.*

(ii) *Si* $x \in A^\circ$ *e* $y \in \overline{A}$, *entonces* $[x, y) := \{ty + (1-t)x \mid 0 \leq t < 1\} \subseteq A^\circ$.

Demostración: (i) Sean x, $y \in \overline{A}$ y $t \in [0, 1]$, veamos que $tx + (1-t)y \in \overline{A}$. Sean $\{x_\lambda\}_{\lambda\in\Lambda}$ e $\{y_\gamma\}_{\gamma\in\Gamma}$ redes en A tal que $x_\lambda \longrightarrow x$ e $y_\gamma \longrightarrow y$. Consideremos $\Lambda \times \Gamma$ con el orden parcial definido por: $(\lambda_1, \gamma_1) \leq (\lambda_2, \gamma_2)$ si $\lambda_1 \leq \lambda_2$ y $\gamma_1 \leq \gamma_2$. Entonces $\Lambda \times \Gamma$ es un conjunto dirigido y podemos considerar la red $\{(x_\lambda, y_\gamma)\}_{(\lambda,\gamma)\in\Lambda\times\Gamma}$ en $\mathbb{R}^I \times \mathbb{R}^I$.

Por otro lado, sea $f : \mathbb{R}^I \times \mathbb{R}^I \to \mathbb{R}^I$ definida por $f(z, w) = tz + (1-t)w$. Dado que f es continua y $(x_\lambda, y_\gamma) \longrightarrow (x, y)$ se tiene que:

$$f((x_\lambda, y_\gamma)) \longrightarrow f((x, y)),$$

y como $f((x_\lambda, y_\gamma)) \in A$ tenemos que $f((x, y)) \in \overline{A}$ como queríamos.
(ii) Tomemos $0 < t < 1$ y llamemos $z = ty + (1-t)x$. Veamos que existe un entorno abierto de z que está contenido en A. Como $x \in A^\circ$ existe $U \subseteq \mathbb{R}^I$ abierto tal que $x \in U \subseteq A$, consideremos $V := U - x$, V es abierto y $0 \in V$, entonces para cada $w \in A$, tenemos que:

$$\begin{aligned} tw + (1-t)U &\subseteq A, \\ tw + (1-t)(x+V) &\subseteq A, \\ tw - ty + ty + (1-t)(x+V) &\subseteq A, \\ t(w-y) + z + (1-t)V &\subseteq A. \end{aligned}$$

Llamemos $W := t(w-y) + (1-t)V$. Observemos que si existe $w \in A$ tal que $0 \in W$, tenemos que $z \in z + W \subseteq A$ y es claro que $z + W$ es abierto pues V lo es. Entonces, basta ver que existe $w \in A$ tal que $0 \in W$. En efecto, como $0 \in V$, $y \in y - \frac{1-t}{t}V$ y, como $y \in \overline{A}$, existe $w \in (y - \frac{1-t}{t}V) \cap A$, es decir, $w = y - \frac{1-t}{t}v$, para algún $v \in V$ y por lo tanto $W = t(w-y) + (1-t)V = -(1-t)v + (1-t)V$, es claro que $0 \in W$. ▫

Veamos ahora una consecuencia del Teorema de Hahn-Banach:

Proposición 1.6 *Sea $G \subseteq \mathbb{R}^I$ abierto convexo tal que $0 \in G$. Definimos $q : \mathbb{R}^I \to \mathbb{R}$, $q(x) := \text{ínf}\{t \in \mathbb{R} \mid t \geq 0 \text{ y } x \in tG\}$. Entonces q es sublineal, no negativa y $G = \{x \in \mathbb{R}^I \mid q(x) < 1\}$.*

Demostración: Empecemos observando que, para cada $x \in \mathbb{R}^I$, se tiene que:

$$\{t \in \mathbb{R} \mid t \geq 0 \text{ y } x \in tG\} \neq \varnothing.$$

En efecto, como $0 \in G$, existe $U \subseteq G$ abierto básico con $0 \in U$ y podemos suponer que:

$$U = \prod_{i \in I} U_i$$

con $U_i = \mathbb{R}$ para todo $i \in I - I_0$ y $U_i = (-\epsilon, \epsilon)$ para todo $i \in I_0$, $I_0 \subseteq I$ finito. Consideremos $\widetilde{U} := kU$ con $k \in \mathbb{N}$ tal que $k > \frac{|x_i|}{\epsilon}$ para todo $i \in I_0$. Entonces, $x \in \widetilde{U}$ (pues $|x_i| < k\epsilon$ para todo $i \in I_0$), es decir, $k \in \{t \in \mathbb{R} \mid t \geq 0 \text{ y } x \in tG\}$.
Es claro que q es no negativa ya que el ínfimo se toma sobre $t \geq 0$. Veamos que q es sublineal:

- $q(\alpha x) = \alpha q(x)$ para todo $\alpha \geq 0$: Si $\alpha = 0$, basta observar que $q(0) = 0$. Si $\alpha > 0$ tenemos la siguiente cadena de igualdades:

$$q(\alpha x) = \text{ínf}\{t \in \mathbb{R} \mid t \geq 0 \text{ y } \alpha x \in tG\} = \text{ínf}\{t \in \mathbb{R} \mid t \geq 0 \text{ y } x \in \frac{t}{\alpha}G\} =$$
$$= \text{ínf}\{\alpha s \in \mathbb{R} \mid s \geq 0 \text{ y } x \in sG\} = \alpha \ \text{ínf}\{s \in \mathbb{R} \mid s \geq 0 \text{ y } x \in sG\} = \alpha q(x)$$

- $q(x + y) \leq q(x) + q(y)$: Sean $t, s \geq 0$ tales que $x \in tG$ e $y \in sG$, es decir, existen g, $h \in G$ tales que $x = tg$ e $y = sh$, entonces:

$$x + y = tg + sh = (t + s)\left(\frac{t}{t+s}g + \frac{s}{t+s}h\right),$$

y, como G es convexo y $\frac{t}{t+s} + \frac{s}{t+s} = 1$, se tiene que $x+y \in (t+s)G$. Por lo tanto $(t + s) \geq q(x + y)$. Si dejamos s fijo y tomamos ínfimo sobre t tenemos que $q(x)+s \geq q(x+y)$, finalmente tomamos ínfimo sobre s y tenemos $q(x)+q(y) \geq q(x + y)$.

Por último veamos que $G = \{x \in \mathbb{R}^I \mid q(x) < 1\}$: Sea $x \in \mathbb{R}^I$ tal que $q(x) < 1$, entonces existe $0 \leq t < 1$ tal que $x \in tG$. Como G es convexo se tiene que $tG + (1 - t)G \subseteq G$ luego, como:

$$x = x + 0 \in tG + (1 - t)G,$$

tenemos que $x \in G$ como queríamos. Recíprocamente, si $x \in G$, es claro que $q(x) \leq 1$. Basta observar que dado que G es abierto existe $t \in (0, 1)$ tal que $x \in tG$ y por lo tanto $q(x) < 1$. ▫

Proposición 1.7 *Sea $G \subseteq \mathbb{R}^I$ abierto, convexo y no vacío tal que $0 \notin G$. Entonces existe $f : \mathbb{R}^I \to \mathbb{R}$ funcional lineal y continuo, no idénticamente nulo tal que si $\mathfrak{M} = \ker(f)$, entonces $\mathfrak{M} \cap G = \varnothing$.*

Demostración: Sea $x_0 \in G$ y consideremos $H = x_0 - G \subseteq \mathbb{R}^I$ abierto convexo (pues G lo es) y $0 \in H$, entonces por la Proposición 1.6 existe $q : \mathbb{R}^I \to \mathbb{R}$ sublineal y no negativa tal que $H = \{x \in \mathbb{R}^I \mid q(x) < 1\}$. Sea $\mathfrak{Y} \subseteq \mathbb{R}^I$ el subespacio generado por x_0, es decir, $\mathfrak{Y} = \{\alpha x_0 \mid \alpha \in \mathbb{R}\}$ y $f_0 : \mathfrak{Y} \to \mathbb{R}$ definida por $f_0(\alpha x_0) := \alpha q(x_0)$. Veamos que $f_0(\alpha x_0) \leq q(\alpha x_0)$ para todo $\alpha \in \mathbb{R}$:

- Si $\alpha \geq 0$: $f_0(\alpha x_0) = \alpha q(x_0) = q(\alpha x_0)$.

- Si $\alpha < 0$: Como $q(x) \geq 0$ para todo $x \in G$ tenemos que:

$$f_0(\alpha x_0) = \alpha q(x_0) \leq 0 \leq q(\alpha x_0).$$

Entonces por el Teorema 1.2 existe $f : \mathbb{R}^I \to \mathbb{R}$ funcional lineal tal que $f|_{\mathfrak{Y}} \equiv f_0$ y $f(x) \leq q(x)\ \forall x \in \mathbb{R}^I$. Veamos que f es continua. Observemos que para todo $x \in H$ se tiene que $f(x) \leq q(x) < 1$. Veamos que esto implica que $|f(x)| < 1$ para todo x en un entorno de 0. En efecto, como $0 \in H$, existe un abierto básico U con $0 \in U \subseteq H$ que podemos suponer simétrico, es decir, de la forma:

$$U = \prod U_i$$

con $U_i = \mathbb{R}$ para todo $i \in I - I_0$ y $U_i = (-\epsilon, \epsilon)$ para todo $i \in I_0$, I_0 finito. Supongamos que existe $x \in U$ tal que $f(x) < -1$, entonces, por linealidad de f, $f(-x) > 1$, pero, por simetría de U, $-x \in U$ y, dado que $U \subseteq H$, se tiene un absurdo. Por lo tanto, para todo $x \in U$ se tiene que $-1 < f(x) < 1$. Finalmente, para concluir que f es continua basta observer que para todo abierto $V \subseteq \mathbb{R}$, dado $x \in f^{-1}(V)$, existe $\eta > 0$ tal que $(f(x) - \eta, f(x) + \eta) \subseteq V$ y en consecuencia $x \in x + \eta U \subseteq f^{-1}(V)$. Luego, tomamos $\mathfrak{M} = \ker(f)$. Para terminar veamos que $\mathfrak{M} \cap G = \varnothing$: Sea $x \in G$, entonces $x_0 - x \in H$ y por lo tanto $q(x_0 - x) < 1$. Por otro lado,

$$f(x_0) - f(x) = f(x_0 - x) \leq q(x_0 - x) < 1.$$

En consecuancia:

$$f(x) > f(x_0) - 1,$$

y como $f(x_0) = f_0(x_0) = q(x_0) \geq 1$, resulta $f(x) > 0$. En particular, se deduce que $\mathfrak{M} \cap G = \varnothing$. ▫

En lo que sigue vamos a introducir la noción de abiertos estrictamente separados y veremos algunas propiedades relacionadas con estos conjuntos.

Definición 1.8 *Un conjunto $S \subseteq \mathbb{R}^I$ es un* ***semiespacio abierto*** *si existe $f : \mathbb{R}^I \to \mathbb{R}$ funcional lineal y continuo, no idénticamente nulo, tal que $S = \{x \in \mathbb{R}^I \mid f(x) > \alpha\}$ para algún $\alpha \in \mathbb{R}$.*

Definición 1.9 *Sean A, $B \subseteq \mathbb{R}^I$, decimos que A y B están* ***estrictamente separados*** *si están contenidos en semiespacios abiertos disjuntos.*

Veamos una caracterización de abiertos estrictamente separados que necesitaremos más adelante.

Proposición 1.10 *Dados A, $B \subseteq \mathbb{R}^I$, son equivalentes:*

(i) A y B están estrictamente separados.

(ii) Existen $f : \mathbb{R}^I \to \mathbb{R}$ funcional lineal y continuo y $\alpha \in \mathbb{R}$ tales que:

$$A \subseteq \{x \in \mathbb{R}^I \mid f(x) > \alpha\} \text{ y } B \subseteq \{x \in \mathbb{R}^I \mid f(x) < \alpha\}.$$

Demostración: Es claro que *(ii)* implica *(i)*. Recíprocamente, si existen U, V semiespacios abiertos y disjuntos tales que $A \subseteq U$ y $B \subseteq V$, supongamos:

$$U = \{x \in \mathbb{R}^I \mid f(x) > \alpha\},$$
$$V = \{x \in \mathbb{R}^I \mid g(x) > \beta\}$$

donde f, $g : \mathbb{R}^I \to \mathbb{R}$ funcionales lineales y continuos, no idénticamente nulos, y α, $\beta \in \mathbb{R}$. Observemos primero que para todo $x \in \mathbb{R}^I$, si $f(x) = 0$, entonces $g(x) = 0$. En efecto, supongamos que $g(x) \neq 0$, y tomemos $y \in \mathbb{R}^I$ tal que $f(y) \neq 0$, entonces, para todo s, $t \in \mathbb{R}$, se tiene que:

$$f(tx + sy) = sf(y),$$
$$g(tx + sy) = tg(x) + sg(y).$$

Como $f(y) \neq 0$, podemos tomar $s \in \mathbb{R}$ tal que $tx + sy \in U$ (basta tomar $sf(y) > \alpha$) y, fijado s, como $g(x) \neq 0$, podemos tomar $t \in \mathbb{R}$ tal que $tx + sy \in V$ (basta tomar $tg(x) + sg(y) > \beta$), con lo cual tenemos que $tx + sy \in U \cap V$, lo cual es absurdo. Análogamente, se prueba que si $g(x) = 0$, entonces $f(x) = 0$. A continuación vamos a ver que, dado que $U \cap V = \varnothing$, existe $\gamma < 0$ tal que $f = \gamma g$. Por lo probado previamente, basta mostrar la igualdad cuando $f(x)$, $g(x) \neq 0$. Tomemos $x_0 \in \mathbb{R}^I$ tal que $g(x_0) \neq 0$ y llamemos $\gamma = \frac{f(x_0)}{g(x_0)}$. Sea $x \in \mathbb{R}^I$ tal que $g(x) \neq 0$, entonces:

$$0 = g(x) - g(x) = g(x) - \frac{g(x)}{g(x_0)} g(x_0) = g\left(x - \frac{g(x)}{g(x_0)} x_0\right),$$

Luego,

$$f\left(x - \frac{g(x)}{g(x_0)} x_0\right) = 0,$$

y, usando la linealidad de f, tenemos que $\frac{f(x)}{g(x)} = \frac{f(x_0)}{g(x_0)} = \gamma$ como queríamos. Finalmente, observemos que si $\gamma > 0$, tenemos que

$$U = \{x \in \mathbb{R}^I \mid g(x) > \frac{\alpha}{\gamma}\},$$

y en este caso U y V no pueden ser disjuntos (basta tomar x tal que $g(x) > \text{máx}\{\frac{\alpha}{\gamma}, \beta\}$). Para concluir, como $\gamma < 0$ se tiene que

$$U = \{x \in \mathbb{R}^I \mid g(x) < \frac{\alpha}{\gamma}\}.$$

Como $U \cap V = \varnothing$ se tiene que $\frac{\alpha}{\gamma} \leq \beta$ y por lo tanto existe $\eta \in \mathbb{R}$ tal que $\frac{\alpha}{\gamma} \leq \eta \leq \beta$, entonces

$$U \subseteq \{x \in \mathbb{R}^I \mid g(x) < \eta\},$$
$$V \subseteq \{x \in \mathbb{R}^I \mid g(x) > \eta\}.$$

□

Proposición 1.11 *Sean A, $B \subseteq \mathbb{R}^I$ abiertos convexos no vacíos tales que $A \cap B = \varnothing$. Entonces A y B están estrictamente separados.*

Demostración: Veamos que $G = A - B$ cumple las hipótesis de la Proposición 1.7:

- G es abierto pues:
$$G = \bigcup_{b \in B} A - b.$$
- G es convexo pues A y B lo son.
- $G \neq \varnothing$ y $0 \notin G$ pues $A \cap B = \varnothing$.

Entonces existe $f : \mathbb{R}^I \to \mathbb{R}$ funcional lineal y continuo, no idénticamente nulo tal que si $\mathfrak{M} = \ker(f)$ se tiene que $\mathfrak{M} \cap G = \varnothing$. Por otro lado, como G convexo y f es lineal, $f(G) \subseteq \mathbb{R}$ es convexo y $f(x) > 0$ para todo $x \in G$ ó $f(x) < 0$ para todo $x \in G$. Si $f(x) > 0$ para todo $x \in G$, entonces $f(a) > f(b)$ para todo $a \in A$, $b \in B$, y por lo tanto se tiene que:

$$\text{ínf}\{f(a) \mid a \in A\} \geq \sup\{f(b) \mid b \in B\}.$$

Sea $\alpha \in \mathbb{R}$ tal que:

$$\text{ínf}\{f(a) \mid a \in A\} \geq \alpha \geq \sup\{f(b) \mid b \in B\}.$$

Luego $f(a) \geq \alpha$ para todo $a \in A$ y $f(b) \leq \alpha$ para todo $b \in B$. Finalmente basta observar que las desigualdades son estrictas dado que como A y B son abiertos convexos, entonces $f(A)$ y $f(B)$ son intervalos abiertos en $\mathbb{R}$ por el Lema 1.4. Si $f(x) < 0$ para todo $x \in G$ se procede de manera análoga. ▫

Lema 1.12 *Sea $K \subseteq \mathbb{R}^I$ compacto y $V \subseteq \mathbb{R}^I$ abierto tal que $K \subseteq V$, entonces existe $U \subseteq \mathbb{R}^I$ abierto tal que $0 \in U$ y $K + U \subseteq V$.*

Demostración: Consideremos $\mathfrak{U} = \{U \subseteq \mathbb{R}^I \mid U \text{ es abierto y } 0 \in U\}$, queremos ver que existe un elemento U de $\mathfrak{U}$ tal que $K+U \subseteq V$. Supongamos que no, entonces para todo $U \in \mathfrak{U}$ existen $x_U \in K$, $y_U \in U$ tal que $x_U + y_U \in \mathbb{R}^I - V$. Si consideramos en $\mathfrak{U}$ el orden parcial dado por la inclusión al revés, $\mathfrak{U}$ resulta un conjunto dirigido y por lo tanto $\{x_U\}_{U\in\mathfrak{U}}$, $\{y_U\}_{U\in\mathfrak{U}}$ son redes. Como K es compacto existe $\{x_{U_\gamma}\}_{\gamma\in\Gamma}$ subred convergente a un elemento $x \in K$. Por otro lado, veamos que $\{y_U\}_{U\in\mathfrak{U}}$ converge a 0. En efecto, dado W abierto con $0 \in W$, para todo $U \in \mathfrak{U}$ tal que $U \subseteq W$ se tiene que $y_U \in U \subseteq W$. Entonces $x_{U_\gamma} + y_{U_\gamma} \longrightarrow x + 0 = x$ y como $\mathbb{R}^I - V$ es cerrado, se tiene que $x \in \mathbb{R}^I - V$, lo cual es absurdo dado que $x \in K \subseteq V$. ▫

Proposición 1.13 *Sean $A, B \subseteq \mathbb{R}^I$ cerrados convexos tales que $A \cap B = \varnothing$. Si B es compacto entonces A y B están estrictamente separados.*

Demostración: Como $B \subseteq \mathbb{R}^I - A$ por Lema 1.12 existe $U \subseteq \mathbb{R}^I$ abierto, $0 \in U$ tal que $B + U \subseteq \mathbb{R}^I - A$. Sea $V \subseteq U$ abierto básico con $0 \in V$ que podemos suponer de la forma:

$$V = \prod_{i\in I} V_i$$

con $V_i = \mathbb{R}$ para todo $i \in I - I_0$ y $V_i = (-\epsilon, \epsilon)$ para todo $i \in I_0$, I_0 finito. Consideremos $\widetilde{V}$ definido por:

$$\widetilde{V} = \prod_{i\in I} \widetilde{V}_i$$

con $\widetilde{V}_i = \mathbb{R}$ para todo $i \in I - I_0$ y $\widetilde{V}_i = (-\frac{\epsilon}{2}, \frac{\epsilon}{2})$ para todo $i \in I_0$. Entonces, $(A + \widetilde{V}) \cap (B + \widetilde{V}) = \varnothing$ pues si existen $a \in A$, $b \in B$ y v_1, $v_2 \in \widetilde{V}$ tal que $a + v_1 = b + v_2$ entonces $a = b + v_2 - v_1$ y esto es absurdo dado que $v_2 - v_1 \in V$.

Además $A+\widetilde{V}$ y $B+\widetilde{V}$ son abiertos convexos. En efecto, son convexos pues si a_1+v_1, $a_2+v_2 \in A+\widetilde{V}$ y $t \in [0,1]$ entonces

$$t(a_1+v_1)+(1-t)(a_2+v_2) = (ta_1+(1-t)a_2)+(tv_1+(1-t)v_2).$$

Es claro que el primer término está en A y el segundo término está en $\widetilde{V}$. Para ver que son abiertos basta escribir:

$$A+\widetilde{V} = \bigcup_{a\in A}(a+\widetilde{V})$$

Luego, por Proposición 1.11, $A+\widetilde{V}$ y $B+\widetilde{V}$ están estrictamente separados y como $A \subseteq A+\widetilde{V}$ y $B \subseteq B+\widetilde{V}$ resulta que A y B están estrictamente separados, como queríamos. □

Como anticipamos al principio del capítulo, el objetivo es demostrar el Teorema de Krein-Milman que afirma que si K es un conjunto compacto y no vacío, entonces tiene puntos extremales y más aún el conjunto formado por todas las combinaciones convexas de puntos extremales es denso en K. Para poder enunciar (y demostrar) el teorema veamos algunas definiciones y resultados previos.

Definición 1.14 *Sea $A \subseteq \mathbb{R}^I$ subconjunto convexo, $a \in A$ es un **punto extremal** de A si $a = \theta x_1 + (1-\theta)x_2$ con $x_1, x_2 \in A$ y $0 \leq \theta \leq 1$ entonces $a = x_1$ o $a = x_2$. Notamos al conjunto de todos los puntos extremales de A como* $\mathrm{ext}(A)$.

Proposición 1.15 *Sea $A \subseteq \mathbb{R}^I$ subconjunto convexo, $a \in A$. Son equivalentes:*

(i) $a \in \mathrm{ext}(A)$.

(ii) Si x_1, $x_2 \in A$ tal que $a = \frac{1}{2}(x_1+x_2)$, entonces $x_1 = x_2 = a$.

(iii) $A - \{a\}$ es convexo.

Demostración: Es claro que si $a \in \mathrm{ext}(A)$ y tenemos que $a = \frac{1}{2}(x_1+x_2)$ con x_1, $x_2 \in A$, entonces $x_1 = x_2 = a$ (por definición de punto extremal). Recíprocamente, si vale *(ii)*, veamos que $a \in \mathrm{ext}(A)$. Supongamos $a = \theta x_1 + (1-\theta)x_2$ con $x_1, x_2 \in A$ y $0 \leq \theta \leq 1$. Observemos que si $\theta = 0, \frac{1}{2}, 1$ es claro que $a = x_1$ o $a = x_2$. Si $0 < \theta < \frac{1}{2}$, tomamos x_3 tal que $a = \frac{1}{2}(x_2+x_3)$, es decir

$$x_3 = 2\theta x_1 + (1-2\theta)x_2.$$

Dado que A es convexo, x_3 está en A entonces por *(ii)* $x_2 = x_3 = a$. Si $\frac{1}{2} < \theta < 1$ se procede de manera análoga. Esto muestra la equivalencia de las dos primeras afirmaciones.

Supongamos ahora que $a \in \text{ext}(A)$ y veamos que $A - \{a\}$ es convexo. Sean α, $\beta \in A - \{a\}$, dado que A es convexo es claro que $\theta\alpha + (1-\theta)\beta$ está en A para todo $0 \leq \theta \leq 1$, supongamos entonces que para algún θ se tiene que $\theta\alpha + (1-\theta)\beta = a$, como $a \in \text{ext}(A)$, se tiene que $a = \alpha$ o $a = \beta$, lo cual es un absurdo. Finalmente, supongamos que $A - \{a\}$ es convexo y veamos que $a \in \text{ext}(A)$. En efecto, si $a = \theta x_1 + (1-\theta)x_2$ con $x_1, x_2 \in A$, $0 \leq \theta \leq 1$ y $a \neq x_1$, $a \neq x_2$, entonces $\theta x_1 + (1-\theta)x_2 \in A - \{a\}$ para todo $0 \leq \theta \leq 1$, lo cual es absurdo y por lo tanto o bien $a = x_1$ o bien $a = x_2$ como queríamos. ▫

Definición 1.16 *Sea $A \subseteq \mathbb{R}^I$, la **cápsula convexa** de A, que notamos* $\text{co}(A)$*, es la intersección de todos los conjuntos convexos que contienen a A.*

Observación 1.17 *Dado que $\mathbb{R}^I$ es convexo,* $\text{co}(A)$ *está bien definida (es decir, hay algún elemento en esa intersección). Además, es fácil verificar que una intersección arbitraria de conjuntos convexos resulta convexa y por lo tanto* $\text{co}(A)$ *es convexo. De hecho, es el menor convexo que contiene a A.*

Finalmente, estamos ahora en condiciones de enunciar y demostrar el teorema principal de este capítulo.

Teorema 1.18 (Krein-Milman) *Si $K \subseteq \mathbb{R}^I$ compacto, convexo y no vacío, entonces* $\text{ext}(K) \neq \varnothing$ *y* $K = \overline{\text{co}(\text{ext}(K))}$.

Demostración: Consideremos $\mathfrak{U} = \{U \subsetneq K \mid U \text{ es convexo y abierto en } K\}$ con el orden parcial dado por la inclusión. Veamos que se puede aplicar el Lema de Zorn en $\mathfrak{U}$:

- $\mathfrak{U} \neq \varnothing$ pues $\varnothing \in \mathfrak{U}$.
- Sea $\mathfrak{U}_0$ una cadena en $\mathfrak{U}$, veamos que

$$U_0 := \bigcup_{U \in \mathfrak{U}_0} U$$

es cota superior de $\mathfrak{U}_0$. En efecto, U_0 es convexo (pues, dados x, $y \in U_0$, como $\mathfrak{U}_0$ es una cadena, existe $U \in \mathfrak{U}_0$ tal que x e y pertenecen a U, y, como U

es convexo, las combinaciones convexas de x e y están en U) y abierto en K (pues es unión de abiertos). Si

$$K = U_0 = \bigcup_{U \in \mathfrak{U}_0} U,$$

como K es compacto podemos extraer un subcubrimiento finito, es decir,

$$K = \bigcup_{i=1}^{n} U_i,$$

pero dado que $\mathfrak{U}_0$ es una cadena, $K = U_i$ para algún $i = 1 \dots n$, lo cual es absurdo pues $U_i \in \mathfrak{U}$. Luego $U_0 \in \mathfrak{U}$ y es claro que $U \leq U_0 \ \forall U \in \mathfrak{U}_0$.

Entonces, por el Lema de Zorn, existe $U \in \mathfrak{U}$ elemento maximal.

Observemos primero que si $U = \varnothing$, entonces K es un singleton y en este caso el resultado vale de manera trivial. Supongamos entonces $U \neq \varnothing$. Para cada $x \in K$ y $0 \leq \lambda < 1$ definimos $T_{x,\lambda} : K \to K$, $T_{x,\lambda}(y) := \lambda y + (1-\lambda)x$. Veamos que $T_{x,\lambda}^{-1}(U) = K \ \forall x \in U$, $0 \leq \lambda < 1$. En efecto, si $x \in U$, $T_{x,\lambda}(U) \subseteq U$ (pues U es convexo), es decir, $U \subseteq T_{x,\lambda}^{-1}(U)$. Veamos que la inclusión es estricta. Tomemos $y \in \overline{U}$, entonces, por la Proposición 1.5, $T_{x,\lambda}(y) \in [x, y) \subseteq U$ y por lo tanto, $\overline{U} \subseteq T_{x,\lambda}^{-1}(U)$. Por otro lado, $U \subsetneq \overline{U}$ pues si fueran iguales, entonces U sería abierto y cerrado en K, pero, como K es conexo (por ser convexo), se tiene que $U = \varnothing$ o $U = K$, lo cual es un absurdo. Luego, tenemos que $U \subsetneq \overline{U} \subseteq T_{x,\lambda}^{-1}(U)$. Veamos que $T_{x,\lambda}^{-1}(U)$ es convexo y abierto en K: es claro que es abierto en K pues U es abierto en K y $T_{x,\lambda}$ es continua. Para ver que es convexo tomemos y, $z \in T_{x,\lambda}^{-1}(U)$, entonces $T_{x,\lambda}(y)$, $T_{x,\lambda}(z) \in U$, y, como U es convexo, para todo $0 \leq t \leq 1$ se tiene que:

$$\begin{aligned} tT_{x,\lambda}(y) + (1-t)T_{x,\lambda}(z) &\in U, \\ t(\lambda y + (1-\lambda)x) + (1-t)(\lambda z + (1-\lambda)x) &\in U, \\ \lambda(ty + (1-t)z) + (1-\lambda)x &\in U, \\ T_{x,\lambda}(ty + (1-t)z) &\in U. \end{aligned}$$

En consecuencia, $ty + (1-t)z \in T_{x,\lambda}^{-1}(U)$. Luego, como $T_{x,\lambda}^{-1}(U)$ contiene estrictamente a U, por maximalidad de U, debe ser $T_{x,\lambda}^{-1}(U) = K$. Por lo tanto:

$$T_{x,\lambda}(K) \subseteq U \tag{1.1}$$

para todo $x \in U$, $0 \leq \lambda < 1$. Observemos los siguientes hechos:

- Si $V \subseteq K$ es convexo y abierto en K, entonces o bien $V \cup U = U$, o bien $V \cup U = K$ pues si $V \cup U \subsetneq K$, dado que $V \cup U$ es abierto en K (por ser unión de abiertos) y es convexo (ya que, si tomamos x, $y \in U \cup V$, es claro que si ambos están en U o en V, el segmento que los une también estará en U o en V respectivamente, y si $x \in U$ e $y \in V$, entonces, por (1.1), $T_{x,\lambda}(y) \in U$ para todo $0 \leq \lambda < 1$)), por maximalidad de U, debe ser $V \cup U = U$.

- $K - U$ es un singleton. En efecto, supongamos que existen $a, b \in K - U$, $a \neq b$, entonces, como K es Hausdorff, existen V_a, V_b abiertos en K, disjuntos, que podemos suponer convexos, tales que $a \in V_a$ y $b \in V_b$. Por la observación previa se tiene que, o bien $V_a \cup U = U$, o bien $V_a \cup U = K$, pero dado que $a \notin U$, la primer opción no puede ser y por lo tanto $V_a \cup U = K$, lo cual es un absurdo dado que $b \notin V_a$ y $b \notin U$. Entonces $K - U = \{a\}$, o equivalentemente $K - \{a\} = U$, dado que U es convexo se tiene que $a \in \text{ext}(K)$ por Proposición 1.15.

- Si $V \subseteq \mathbb{R}^I$ abierto convexo tal que $\text{ext}(K) \subseteq V$ entonces $K \subseteq V$. En efecto, llamemos $V' = V \cap K$ y veamos que $V' = K$. Si la inclusión fuera estricta, $V' \in \mathfrak{U}$ y podemos tomar $U \in \mathfrak{U}$ elemento maximal tal que $V' \subseteq U$. Pero $U = K - \{a\}$ con $a \in \text{ext}(K)$ y esto es un absurdo dado que $\text{ext}(K) \subseteq V$.

Finalmente, si $E = \overline{\text{co}(\text{ext}(K))}$, queremos ver que $E = K$. Es claro que $E \subseteq K$, supongamos que la inclusión es estricta y tomemos $x_0 \in K - E$, dado que E y $\{x_0\}$ son cerrados y convexos y $\{x_0\}$ es compacto, por la Proposición 1.13, existe $f : \mathbb{R}^I \to \mathbb{R}$ funcional lineal y continuo y $\alpha \in \mathbb{R}$ tal que $E \subseteq \{x \mid f(x) > \alpha\}$ y $x_0 \in \{x \mid f(x) < \alpha\}$, entonces si llamamos $V = \{x \mid f(x) > \alpha\}$, V es abierto convexo y $\text{ext}(K) \subseteq V$, luego, por lo observado previamente se tiene que $K \subseteq V$, lo cual es absurdo dado que $x_0 \in K$ pero $x_0 \notin V$. ▫

Capítulo 2

Estados puros

En este capítulo definiremos el concepto de estado puro, noción que resultará de suma importancia en los capítulos siguientes. Los resultados que veremos están basados mayormente en la exposición dada en [6, Chapter 4].

A lo largo de este capítulo G será un grupo abeliano cuya operación escribiremos con notación aditiva y $M \subseteq G$ será un subsemigrupo (es decir, un subconjunto cerrado para la suma con $0 \in M$).

Definamos la siguiente relación entre los elementos de G:

$$x \leq_M y \Leftrightarrow y - x \in M.$$

Observemos que $\leq_M$ es transitiva y reflexiva (pues $0 \in M$) y además cumple las siguientes propiedades: si $x \leq_M y$ entonces $x + z \leq_M y + z$ para todo $z \in G$ y $nx \leq_M ny$ para todo $n \in \mathbb{N}$. Con esta nueva notación, probar que un elemento x pertenece a M equivale a probar que $x \geq_M 0$. En general $\leq_M$ no es antisimétrica, aunque en algunos casos puede serlo, como observaremos a continuación.

Definición 2.1 *El* ***soporte*** *de M es el subgrupo* $\operatorname{supp}(M) := M \cap (-M)$.

Es fácil comprobar que $\leq_M$ resulta antisimétrica si y sólo si $\operatorname{supp}(M) = \{0\}$.

Antes de definir el concepto de *estado puro* necesitamos algunas definiciones previas:

Definición 2.2 *Decimos que un morfismo de grupos $\varphi : G \to \mathbb{R}$ es un* ***estado de (G,M)*** *si $\varphi|_M \geq 0$. Al conjunto de todos los estados de (G, M) lo notamos $S(G, M)$.*

Definición 2.3 *Un elemento $u \in M$ se llama* ***unidad de orden de (G,M)*** *si $G = M + \mathbb{Z}u$.*

Observación 2.4 *Veamos que $G = M + \mathbb{Z}u$ si y sólo si para todo $x \in G$ existe $n \in \mathbb{N}$ tal que $x \leq_M nu$. En efecto, si $G = M + \mathbb{Z}u$, dado $x \in G$, existen $m \in \mathbb{Z}$ e $y \in M$ tal que $-x = y + mu$, sea $k \in \mathbb{N}$ tal que $k - m \in \mathbb{N}$, entonces tenemos que:*

$$-x + (k-m)u = -x - mu + ku = y + ku \in M.$$

O sea, si tomamos $n = k - m$, tenemos que $x \leq_M nu$ como queríamos. Recíprocamente, dado $x \in G$, si existe $n \in \mathbb{N}$ tal que $-x \leq_M nu$, se tiene que $x = y - nu$ para algún $y \in M$.

Observación 2.5 *Supongamos que existe $u \in M$ unidad de orden de (G, M), y tomemos $\varphi \in S(G, M)$, no nulo, entonces $\varphi(u) > 0$. En efecto, es claro que $\varphi(u) \geq 0$ (pues $u \in M$). Supongamos que $\varphi(u) = 0$, entonces para cualquier $x \in G$ se tiene que $x = y + nu$, con $y \in M$, $n \in \mathbb{Z}$, luego:*

$$\varphi(x) = \varphi(y) + n\varphi(u) = \varphi(y) \geq 0.$$

Como debe valer la misma desigualdad para $-x \in G$ se tiene que $\varphi(x) = 0$, es decir $\varphi \equiv 0$, lo cual es absurdo.

Esta observación motiva la siguiente definición:

Definición 2.6 *Sea $u \in M$ unidad de orden de (G, M), dado φ estado de (G, M), decimos que φ es un* ***estado mónico de (G,M,u)*** *si $\varphi(u) = 1$. Al conjunto de todos los estados mónicos de (G, M, u) lo notamos $S(G, M, u)$.*

Observación 2.7 *Sea $u \in M$ unidad de orden de (G, M). En virtud de la Observación 2.5, dado φ estado no nulo de (G, M), se puede obtener fácilmente el estado mónico $\tilde{\varphi}$ de (G, M, u) dado por $\tilde{\varphi}(x) = \frac{\varphi(x)}{\varphi(u)}$.*

Observación 2.8 *Podemos pensar $S(G, M, u)$ como un subconjunto de $\mathbb{R}^G$ y tiene sentido hablar de puntos extremales de $S(G, M, u)$, dado que es fácil comprobar que $S(G, M, u)$ resulta convexo. En efecto, si φ_1, $\varphi_2 \in S(G, M, u)$, $0 \leq t \leq 1$ y llamamos $\varphi := t\varphi_1 + (1-t)\varphi_2$, es claro que $\varphi|_M \geq 0$ y $\varphi(u) = t\varphi_1(u) + (1-t)\varphi_2(u) = 1$.*

Definición 2.9 *Sea $u \in M$ unidad de orden de (G, M), dado φ estado mónico de (G, M, u), decimos que φ es un* ***estado puro*** *si es un punto extremal de $S(G, M, u)$.*

La primera cuestión que se plantea es si siempre existen estados puros, la respuesta es que sí, siempre que $M \subsetneq G$, dado que, como veremos en la Proposición 2.15, en este caso resulta $S(G, M, u) \neq \varnothing$, y como $S(G, M, u)$ es convexo y compacto (hecho que probaremos a continuación), estaremos en condiciones de aplicar el Teorema de Krein-Milman, que garantiza que el conjunto de puntos extremales de $S(G, M, u)$ es no vacío.

La demostración de la siguiente proposición es una adaptación de la dada en [10, Lemma 5.7.1, Lemma 5.7.2].

Proposición 2.10 *Sea u unidad de orden de (G, M), entonces $S(G, M, u)$ es un subconjunto compacto de $\mathbb{R}^G$.*

Demostración: Veamos primero que para cada $g \in G$ existe $I_g \subseteq \mathbb{R}$ intervalo cerrado y acotado tal que si

$$F := \prod_{g \in G} I_g,$$

entonces,

$$S(G, M, u) \subseteq F. \tag{2.1}$$

Fijado $g \in G$, sabemos que existen n_1, $n_2 \in \mathbb{N}$ tal que $n_1 u - g$, $n_2 u + g \in M$, llamemos $n_g = \max\{n_1, n_2\}$, entonces tenemos que $n_g u \pm g \in M$. Veamos que si $I_g := [-n_g, n_g]$ se cumple (2.1). En efecto, dada $\varphi \in S(G, M, u)$, como $n_g u \pm g \in M$, entonces $\varphi(n_g u \pm g) \geq 0$, usando que φ es morfismo y $\varphi(u) = 1$ tenemos que:

$$n_g \pm \varphi(g) \geq 0,$$

o equivalentemente,

$$-n_g \leq \varphi(g) \leq n_g.$$

Ahora, como F es compacto (por ser producto de compactos), para ver que $S(G, M, u)$ es compacto basta mostrar que $S(G, M, u)$ es cerrado en F. Tomemos $\varphi \in \overline{S(G, M, u)}$, entonces para todo $U \subseteq F$ entorno abierto de φ se tiene que $U \cap S(G, M, u) \neq \varnothing$. Veamos que φ es morfismo de grupos: Tomemos x, $y \in G$ y supongamos que $\varphi(x + y) \neq \varphi(x) + \varphi(y)$, entonces existen $U_x, U_y, U_{x+y} \subseteq \mathbb{R}$ entornos abiertos de

$\varphi(x)$, $\varphi(y)$, $\varphi(x+y)$ respectivamente tal que $(U_x + U_y) \cap U_{x+y} = \varnothing$, tomemos $U \subseteq \mathbb{R}^G$ el abierto definido por:

$$U = \prod_{g \in G} U_g$$

con U_g los definidos anteriormente si $g = x$, y ó $x + y$ y $U_g = \mathbb{R}$ en los demás casos, entonces $\tilde{U} = U \cap F$ es un entorno abierto en F de φ, pero $\tilde{U} \cap S(G, M, u) = \varnothing$ (ya que si $\psi \in \tilde{U}$, $\psi(x) + \psi(y) \neq \psi(x + y)$), lo cual es un absurdo. Por lo tanto $\varphi(x + y) = \varphi(x) + \varphi(y)$ para todo x, $y \in G$. De manera análoga se puede probar que $\varphi|_M \geq 0$ y que $\varphi(u) = 1$. Esto prueba que $\overline{S(G, M, u)} = S(G, M, u)$. ▫

A continuación vamos a ver algunos resultados que nos servirán, entre otras cosas, para concluir que existen estados puros siempre que $M \subsetneq G$. Adoptaremos la siguiente convención: dado un conjunto $A \subseteq \mathbb{R}$, no necesariamente no vacío ni acotado, escribiremos $\sup(A) = +\infty$, si A no está acotado superiormente y $\sup(A) = -\infty$, si $A = \varnothing$. Análogamente, escribiremos $\text{ínf}(A) = -\infty$, si A no está acotado inferiormente y $\text{ínf}(A) = +\infty$, si $A = \varnothing$.

Lema 2.11 *Sean M subsemigrupo, H subgrupo de G, $x \in G$ y f un estado de $(H, M \cap H)$. Definimos:*

$$p := \sup \left\{ \frac{f(y)}{m} \mid y \in H,\ m \in \mathbb{N},\ y \leq_M mx \right\},$$

$$r := \text{ínf} \left\{ \frac{f(z)}{n} \mid z \in H,\ n \in \mathbb{N},\ nx \leq_M z \right\}.$$

Entonces:

(i) $p \leq r$.

(ii) Si g es un estado de $(H + \mathbb{Z}x, M \cap (H + \mathbb{Z}x))$ que extiende a f, entonces $p \leq g(x) \leq r$.

(iii) Para todo $q \in \mathbb{R}$ tal que $p \leq q \leq r$, existe g estado de $(H + \mathbb{Z}x, M \cap (H + \mathbb{Z}x))$ que extiende a f con $g(x) = q$.

Demostración: (i) Para ver que $p \leq r$ basta ver que para todo y, $z \in H$, m, $n \in \mathbb{N}$ tal que $y \leq_M mx$ y $nx \leq_M z$ se tiene que:

$$\frac{f(y)}{m} \leq \frac{f(z)}{n}.$$

En efecto, como $ny \leq_M nmx \leq_M mz$ tenemos que $mz - ny \in M$, entonces $f(mz - ny) \geq 0$, usando que f es morfismo de grupos se tiene que $mf(z) - nf(y) \geq 0$ como queríamos.

(ii) Supongamos que g es un estado de $(H + \mathbb{Z}x, M \cap (H + \mathbb{Z}x))$ que extiende a f y veamos que

$$\frac{f(y)}{m} \leq g(x)$$

para todo $y \in H$, $m \in \mathbb{N}$ tal que $y \leq_M mx$. En efecto, si $mx - y \in M$ entonces $g(mx - y) \geq 0$, usando que g es morfismo de grupos y que $g(y) = f(y)$ tenemos que $mg(x) - f(y) \geq 0$ como queríamos. Por lo tanto, $p \leq g(x)$. De manera análoga se verifica la otra desigualdad.

(iii) Tomemos $p \leq q \leq r$. Veamos que para todo $w \in H$ y $k \in \mathbb{Z}$, si $w + kx \in M$ entonces $f(w) + kq \geq 0$:

- Si $k = 0$, $w \in M$ y $f(w) \geq 0$.
- Si $k > 0$ tenemos que $kx \geq_M -w$ con $-w \in H$ y $k \in \mathbb{N}$, entonces:

$$\frac{f(-w)}{k} \leq p \leq q.$$

- Si $k < 0$ tenemos que $w \geq_M -kx$ con $w \in H$ y $-k \in \mathbb{N}$, entonces:

$$\frac{f(w)}{-k} \geq r \geq q.$$

Definamos $g : H + \mathbb{Z}x \to \mathbb{R}$, $g(w + kx) := f(w) + kq$ para todo $w \in H$, $k \in \mathbb{Z}$. Por lo probado previamente g está bien definida (pues si $w + kx = 0$, $f(w) + kq = 0$) y $g|_{M \cap (H + \mathbb{Z}x)} \geq 0$ y es de fácil comprabación que g es morfismo de grupos y $g(x) = q$. □

Proposición 2.12 *Sean M subsemigrupo de G y H subgrupo de G con la propiedad de que para todo $x \in G$ existe $y \in H$ tal que $x \leq_M y$. Entonces todo estado de $(H, M \cap H)$ puede extenderse a un estado de (G, M).*

Demostración: Sea f un estado de $(H, M \cap H)$. Consideremos la familia

$$\mathfrak{A} = \{(L, g) \mid L \text{ subgrupo de } G \text{ con } H \subseteq L \text{ y } g \text{ estado de } (L, M \cap L) \text{ que extiende a } f\}.$$

Veamos que $\mathfrak{A}$ está en las hipótesis del Lema de Zorn:

- $\mathfrak{A} \neq \varnothing$ pues $(H, f) \in \mathfrak{A}$.
- Sea $\{L_i\}_{i\in I}$ cadena de elementos en $\mathfrak{A}$, entonces si tomamos:

$$L = \bigcup_{i\in I} L_i \text{ y } g : L \to \mathbb{R} \text{ definida por } g(x) := g_i(x) \text{ si } x \in L_i,$$

$(L, g) \in \mathfrak{A}$ y $(L_i, g_i) \leq (L, g)$ para todo $i \in I$.

Entonces existe $(L, g) \in \mathfrak{A}$ elemento maximal.
Vamos a ver que $L = G$. Supongamos que la inclusión es estricta y tomemos $x \in G - L$. Veamos que $-\infty < p \leq r < +\infty$, donde p y r son los definidos en el Lema 2.11 para el subgrupo L y el morfismo g. En efecto, por hipótesis existen u, $v \in H$ tales que $x \leq_M u$ y $-x \leq_M v$, luego $r \leq g(u)$ y $p \geq g(-v)$. Entonces, por *(iii)* del Lema 2.11 existe $\tilde{g}$ estado de $(L + \mathbb{Z}x, M \cap (L + \mathbb{Z}x))$ que extiende a g. En consecuencia $(L + \mathbb{Z}x, \tilde{g}) \in \mathfrak{A}$ y $(L + \mathbb{Z}x, \tilde{g}) > (L, g)$, lo cual contradice la maximalidad de (L, g). Entonces debe ser $L = G$. ▫

Corolario 2.13 *Sea $u \in M$ unidad de orden de (G, M), H subgrupo de G tal que $u \in H$, entonces todo estado mónico de $(H, M \cap H, u)$ se puede extender a un estado mónico de (G, M, u).*

Demostración: Dado que u es unidad de orden, para todo $x \in G$ existe $n \in \mathbb{N}$ tal que $x \leq_M nu$, luego como $nu \in H$ (pues $u \in H$), H satisface las hipótesis de la Proposición 2.12 y por lo tanto todo estado mónico de $(H, M \cap H, u)$ se puede extender a un estado de (G, M) que resultará un estado mónico de (G, M, u). ▫

Lema 2.14 *Sea $u \in M$ unidad de orden de (G, M) con $M \subsetneq G$ y sea $\eta : \mathbb{Z}u \to \mathbb{R}$ dada por $\eta(ku) = k$. Entonces η está bien definida y $\eta \in S(\mathbb{Z}u, M \cap \mathbb{Z}u, u)$.*

Demostración: Veamos primero que si $ku \in M$ para algún $k \in \mathbb{Z}$, entonces $k \in \mathbb{N}_0$. En efecto, supongamos que $k < 0$ y veamos que en este caso resulta $M = G$: sea $x \in G$ y $n \in \mathbb{N}$ tal que $-x \leq_M nu$, es decir $x + nu = m \in M$. Tomemos $l \in \mathbb{N}$ tal que $-kl \geq n$ entonces tenemos que:

$$x = m - nu - klu + klu = m + (-n - kl)u + klu.$$

Como cada término está en M, entonces $x \in M$.
Como consecuencia, se tiene que si existe $k \in \mathbb{Z}$ tal que $ku = 0$, entonces $k = 0$, lo cual prueba la buena definición de η. Además, como $M \cap \mathbb{Z}u = \mathbb{N}_0 u$, es claro que $\eta \in S(\mathbb{Z}u, M \cap \mathbb{Z}u, u)$. ▫

Proposición 2.15 *Sea $u \in M$ unidad de orden de (G, M), entonces $S(G, M, u) \neq \varnothing \Leftrightarrow M \subsetneq G$.*

Demostración: Supongamos primero que existe $\varphi \in S(G, M, u)$, como $\varphi(u) = 1$, $\varphi(-u) = -1 < 0$ y por lo tanto $-u \notin M$.
Para la otra implicación, tomamos $\eta \in S(\mathbb{Z}u, M \cap \mathbb{Z}u, u)$ como en el Lema 2.14. Por el Corolario 2.13, η se puede extender a un estado mónico de (G, M, u). ▫

Corolario 2.16 *Sea $u \in M$ unidad de orden de (G, M). Si $M \subsetneq G$ existe $\varphi \in S(G, M, u)$ estado puro.*

Demostración: En la Observación 2.8 vimos que $S(G, M, u)$ es convexo, en la Proposición 2.10 vimos que es compacto y en el Proposición 2.15 vimos que es no vacío, luego por el Teorema de Krein-Milman, el conjunto de puntos extremales de $S(G, M, u)$ es no vacío. ▫

El próximo objetivo será demostrar un resultado que da un criterio para determinar cuando un elemento del grupo es unidad de orden. Es uno de los resultado más importantes de este trabajo ya que, como se verá en el último capítulo, a partir de él se logra una sencilla demostración de los conocidos teoremas Schmüdgen Positivstellensatz y Putinar Positivstellensatz entre otros certificados de no negatividad.
Para demostrar este teorema necesitamos algunos resultados previos:

Proposición 2.17 *Sean $u \in M$ unidad de orden de (G, M), $x \in G$ y supongamos $M \subsetneq G$. Definimos:*

$$p := \sup \left\{ \frac{k}{m} \mid k \in \mathbb{Z},\ m \in \mathbb{N},\ ku \leq_M mx \right\},$$

$$r := \text{ínf} \left\{ \frac{l}{n} \mid l \in \mathbb{Z},\ n \in \mathbb{N},\ nx \leq_M lu \right\}.$$

Entonces:

(i) $p > -\infty$ *y* $r < +\infty$.

(ii) Si φ es un estado mónico de (G, M, u), entonces $p \leq \varphi(x) \leq r$.

(iii) Para todo $q \in \mathbb{R}$ tal que $p \leq q \leq r$, existe $\varphi : G \to \mathbb{R}$ estado mónico de (G, M, u) tal que $\varphi(x) = q$.

Demostración: (i) Como u es unidad de orden existen $k, l \in \mathbb{N}$ tales que $-x \leq_M ku$ y $x \leq_M lu$ y por lo tanto $p \geq -k > -\infty$ y $r \leq l < +\infty$.
(ii) Sea $\eta \in S(\mathbb{Z}u, M \cap \mathbb{Z}u, u)$ como en el Lema 2.14, luego

$$p = \sup \left\{ \frac{\eta(y)}{m} \mid y \in \mathbb{Z}u,\, m \in \mathbb{N},\, y \leq_M mx \right\},$$

$$r = \text{ínf} \left\{ \frac{\eta(z)}{n} \mid z \in \mathbb{Z}u,\, n \in \mathbb{N},\, nx \leq_M z \right\}.$$

Sea φ estado mónico de (G, M, u), como φ es morfismo de grupos, necesariamente extiende a η. El resultado se sigue de aplicar *(ii)* del Lema 2.11 a $H = \mathbb{Z}u$, $f = \eta$ y $g = \varphi|_{\mathbb{Z}u+\mathbb{Z}x}$.
(iii) Tomemos $p \leq q \leq r$. Nuevamente, sea $\eta \in S(\mathbb{Z}u, M \cap \mathbb{Z}u, u)$ como en el Lema 2.14. Por *(iii)* del Lema 2.11, existe $\tilde{\eta}$ estado de $(\mathbb{Z}u + \mathbb{Z}x, M \cap (\mathbb{Z}u + \mathbb{Z}x))$ que extiende a η con $\tilde{\eta}(x) = q$. Finalmente, por Corolario 2.13, $\tilde{\eta}$ se puede extender a un estado mónico φ de (G, M, u). ▫

Teorema 2.18 *Sea (G, M) tal que admite unidad de orden. Si $x \in G$ satisface que $\varphi(x) > 0$ para todo φ estado no nulo de (G, M), entonces existe $m \in \mathbb{N}$ tal que $mx \in M$; más aún, mx es unidad de orden de (G, M).*

Demostración: Observemos que si $M = G$ el resultado es cierto de manera trivial. Supongamos entonces $M \subsetneq G$. Sea $u \in M$ unidad de orden, veamos que existen $k \in \mathbb{Z}$, $m \in \mathbb{N}$ tales que $ku \leq_M mx$ y $\frac{k}{m} > 0$. Supongamos que esto no sucede y consideremos p y r los definidos en la Proposición 2.17, entonces tenemos que $p \leq 0$. Por otro lado, sean $l \in \mathbb{Z}$, $n \in \mathbb{N}$ tales que $nx \leq_M lu$, por la Proposición 2.15, existe $\phi \in S(G, M, u)$ y entonces se tiene que:

$$\phi(lu - nx) \geq 0.$$

Usando que ϕ es morfismo de grupos y que $\phi(u) = 1$:

$$l - n\phi(x) \geq 0.$$

En consecuencia,

$$\frac{l}{n} \geq \phi(x) > 0.$$

Por lo tanto, $r \geq 0$. Luego, por Proposición 2.17, como $p \leq 0 \leq r$, existe $\varphi : G \to \mathbb{R}$ estado mónico de (G, M, u) tal que $\varphi(x) = 0$, lo cual es un absurdo, y entonces

deben existir $k \in \mathbb{Z}$, $m \in \mathbb{N}$ tales que $ku \leq_M mx$ y $\frac{k}{m} > 0$. Como $m \in \mathbb{N}$ entonces $k \in \mathbb{N}$ y, como $ku \leq_M mx$, $mx - ku = y \in M$, luego, $mx = y + ku \in M$. Veamos que mx resulta unidad de orden. En efecto, dado $z \in G$, existe $n \in \mathbb{N}$ tal que $z \leq_M nu$, entonces se tiene que

$$z \leq_M nu \leq_M nku \leq_M nmx.$$

□

A continuación probaremos un lema que nos permitirá simplificar las hipótesis del teorema anterior, de modo que resulte más facil de usar en los capítulos siguientes.

Lema 2.19 *Sean $u \in M$ unidad de orden de (G, M) y $x \in G$. Entonces, son equivalentes:*

(i) $\varphi(x) > 0$ *para todo φ estado no nulo de (G, M).*

(ii) $\varphi(x) > 0$ *para todo φ estado puro de (G, M, u).*

Demostración: Es claro que *(i)* implica *(ii)*. Para la otra implicación, consideremos la función:

$$S(G, M, u) \to \mathbb{R}, \qquad \varphi \longmapsto \varphi(x). \tag{2.2}$$

Observemos que esta función es la restricción a $S(G, M, u)$ de la proyección $\pi_x : \mathbb{R}^G \to \mathbb{R}$ y por lo tanto es continua. Entonces, dado que, por la Proposición 2.10, $S(G, M, u)$ es un compacto, existe $\varphi_0 \in S(G, M, u)$ tal que $\varphi(x) \geq \varphi_0(x)$ para todo $\varphi \in S(G, M, u)$. Consideremos el conjunto de todos los estados mónicos donde se alcanza el mínimo, es decir, si llamamos $m := \varphi_0(x)$, consideramos:

$$A = \{\varphi \in S(G, M, u) \mid \varphi(x) = m\}.$$

Veamos que A verifica las hipótesis del Teorema de Krein-Milman:

- A es compacto: Observemos que A es cerrado en $S(G, M, u)$ pues es la preimágen de un punto por una función continua, entonces, como $S(G, M, u)$ es compacto y $A \subseteq S(G, M, u)$, tenemos que A es compacto (por ser cerrado en un compacto).

- A es convexo: Tomemos φ_1, $\varphi_2 \in A$ y $0 \leq t \leq 1$, entonces:

$$(t\varphi_1 + (1-t)\varphi_2)(x) = t\varphi_1(x) + (1-t)\varphi_2(x) = tm + (1-t)m = m.$$

- $A \neq \varnothing$ pues $\varphi_0 \in A$.

Entonces, existe $\tilde{\varphi}_0$ punto extremal de A. Veamos que $\tilde{\varphi}_0$ resulta estado puro de (G, M, u). En efecto, supongamos que:

$$\tilde{\varphi}_0 = \frac{1}{2}(\varphi_1 + \varphi_2) \tag{2.3}$$

con φ_1, $\varphi_2 \in S(G, M, u)$. Luego:

$$m = \tilde{\varphi}_0(x) = \frac{1}{2}(\varphi_1(x) + \varphi_2(x)) \geq \frac{1}{2}(m + m) = m.$$

Entonces deben ser todas igualdades y por lo tanto $(\varphi_1(x) + \varphi_2(x)) = 2m$. Dado que $\varphi_1(x)$ y $\varphi_2(x)$ son mayores o iguales a m, deben ser iguales a m y en consecuencia φ_1, $\varphi_2 \in A$ y como $\tilde{\varphi}_0$ es punto extremal de A, por (2.3), se tiene que $\varphi_1 = \varphi_2 = \tilde{\varphi}_0$ como queríamos. Para resumir, hasta ahora probamos que existe $\tilde{\varphi}_0$ estado puro de (G, M, u) que es mínimo de la función definida en (2.2). Para terminar, tomemos φ estado no nulo de (G, M) y veamos que $\varphi(x) > 0$. En efecto, por la Observación 2.5, $\varphi(u) > 0$ y por lo tanto $\tilde{\varphi} := \frac{\varphi}{\varphi(u)}$ es un estado mónico de (G, M, u), luego $\tilde{\varphi}(x) \geq \tilde{\varphi}_0(x) > 0$, entonces debe ser $\varphi(x) > 0$. ▫

Teorema 2.20 *Sea u unidad de orden de (G, M). Si $x \in G$ satisface que $\varphi(x) > 0$ para todo φ estado puro de (G, M, u), entonces existe $m \in \mathbb{N}$ tal que $mx \in M$; más aún, mx es unidad de orden de (G, M).*

Demostración: Por el Lema 2.19 se tiene que $\varphi(x) > 0$ para todo φ estado no nulo de (G, M) y entonces del Teorema 2.18 se concluye el resultado. ▫

Capítulo 3

Estados puros definidos sobre anillos

A lo largo de este capítulo, A será un anillo conmutativo. Veremos que si M es un subsemigrupo de A y 1 es unidad de orden de (A, M), entonces, bajo ciertas hipótesis, los estados puros de $(A, M, 1)$ resultan morfismo de anillos. Más específicamente, el capítulo consta de dos secciones, en cada una de las cuales se demostrará el resultado antes mencionado bajo distintas hipótesis para M. En la segunda sección veremos además que los morfismos de anillos resultan estados puros, hecho que si bien no ultilizaremos más adelante, es interesante en sí mismo. Como referencia general para los resultados que veremos se puede consultar [4].

Empecemos con algunas definiciones.

Definición 3.1 *Sea $P \subseteq A$ un subsemigrupo, P es **arquimediano** si para todo $a \in A$ existe $n \in \mathbb{N}$ tal que $n + a \in P$.*

Observación 3.2 *Sea $P \subseteq A$ un subsemigrupo tal que $1 \in P$, entonces P es arquimediano si y sólo si 1 es unidad de orden de (A, P). En efecto, si P es arquimediano, dado $a \in A$, existe $n \in \mathbb{N}$ tal que $n - a \in P$, es decir $a \leq_P n$. Por la Observación 2.4 esto prueba que 1 es unidad de orden de (A, P). Recíprocamente, si 1 es unidad de orden de (A, M), dado $a \in A$, existe $n \in \mathbb{N}$ tal que $-a \leq_M n$, es decir, $n + a \in M$.*

Definición 3.3 *Un subconjunto $S \subseteq A$ es un **subsemianillo** si:*

- $0, 1 \in S$,

- $S + S \subseteq S$,
- $SS \subseteq S$.

Observación 3.4 *Es de fácil comprabación que el conjunto $\sum A^2$ formado por sumas de cuadrados de elementos de A es un subsemianillo.*

Definición 3.5 *Sea $S \subseteq A$ un subsemianillo, un subconjunto $M \subseteq A$ es un **S-pseudomódulo** si:*

- $0 \in M$,
- $M + M \subseteq M$,
- $SM \subseteq M$.

*Si además $1 \in M$ se dice que M es un **S- módulo**.*

Definición 3.6 *Un **(pseudo-)módulo cuadrático** M es un $\sum A^2$-(pseudo-)módulo.*

Veamos ahora una observación que será de gran utilidad más adelante ya que, de una manera astuta, nos permite construir morfismos de grupos que resultan combinación convexa de otros morfismos de grupos.

Observación 3.7 *Sean $P \subseteq A$ un subsemigrupo y u unidad de orden de (A, P). Consideremos φ estado de (A, P) y para cada $a \in A$ tal que $\varphi(au) \neq 0$ definimos $\varphi_a : A \to \mathbb{R}$*

$$\varphi_a(b) := \frac{\varphi(ab)}{\varphi(au)}.$$

(i) Es claro que φ_a es morfismo de grupos y $\varphi_a(u) = 1$. Si además $\varphi_a|_P \geq 0$, φ_a es un estado mónico de (A, P, u). Esta última condición puede garantizarse por ejemplo si $aP \subseteq P$.

(ii) Tomemos ahora a_1, $a_2 \in A$ tal que $\varphi(a_i u) > 0$ para $i = 1, 2$; luego $\varphi((a_1 + a_2)u) > 0$. Entonces, para todo $b \in A$ se tiene que

$$\varphi((a_1 + a_2)u)\varphi_{a_1+a_2}(b) = \varphi((a_1 + a_2)b) =$$

$$= \varphi(a_1 b) + \varphi(a_2 b) = \varphi(a_1 u)\varphi_{a_1}(b) + \varphi(a_2 u)\varphi_{a_2}(b).$$

Por lo tanto,

$$\varphi((a_1 + a_2)u)\varphi_{a_1+a_2} = \varphi(a_1 u)\varphi_{a_1} + \varphi(a_2 u)\varphi_{a_2},$$

equivalentemente,

$$\varphi_{a_1+a_2} = \frac{\varphi(a_1 u)}{\varphi((a_1 + a_2)u)}\varphi_{a_1} + \frac{\varphi(a_2 u)}{\varphi((a_1 + a_2)u)}\varphi_{a_2}.$$

Entonces, dado que

$$\frac{\varphi(a_1 u)}{\varphi((a_1 + a_2)u)} + \frac{\varphi(a_2 u)}{\varphi((a_1 + a_2)u)} = 1,$$

se tiene que $\varphi_{a_1+a_2}$ es combinación convexa de φ_{a_1} y φ_{a_2}.

Consideramos $\mathrm{Hom}(A, \mathbb{R})$ el conjunto de morfismos de anillos de A en $\mathbb{R}$.

Notación 3.8 *Para cada $M \subseteq A$ notamos*

$$X(M) := \{\varphi \in \mathrm{Hom}(A, \mathbb{R}) \mid \varphi|_M \geq 0\}.$$

3.1. Módulos sobre semianillos arquimedianos

Consideremos $S \subseteq A$ un subsemianillo arquimediano y $M \subseteq A$ un S-módulo. En particular, como $1 \in M$, tenemos que $S \subseteq M$, luego M también es arquimediano y en consecuencia, por la Observación 3.2, 1 es unidad de orden de (A, M). Por lo tanto podemos considerar estados puros de $(A, M, 1)$.

El próximo objetivo será demostrar que, bajo estas hipótesis, los estados puros de $(A, M, 1)$ son morfismos de anillos. Como una primer aproximación tenemos el siguiente resultado.

Teorema 3.9 *Sean $S \subseteq A$ un subsemianillo arquimediano, $M \subseteq A$ un S-pseudomódulo y $u \in M$ unidad de orden de (A, M). Entonces todo estado puro φ de (A, M, u) cumple que*

$$\varphi(ab) = \varphi(au)\varphi(b) \text{ para todo } a, b \in A. \tag{3.1}$$

Demostración: Tomemos φ estado puro de (A, M, u). Si $n \in \mathbb{Z}$ y $b \in A$, entonces, como $\varphi(u) = 1$, se tiene que $\varphi(nu) = n$ y por lo tanto,

$$\varphi(nb) = n\varphi(b) = \varphi(nu)\varphi(b).$$

Como S es arquimediano, tenemos que $A = S + \mathbb{Z}$, luego, basta probar (3.1) para todo $a \in S$.

Fijemos $a \in S$ y analicemos dos casos:

- Si $\varphi(au) = 0$, queremos ver que $\varphi(ab) = 0$ para todo $b \in A$. En efecto, como u es unidad de orden de (A, M), se tiene que

  $$A = M + \mathbb{Z}u.$$

  Por lo tanto,

  $$aA = aM + \mathbb{Z}au.$$

  Luego, como $\varphi(au) = 0$, basta ver que $\varphi(am) = 0$ para todo $m \in M$.

  Tomemos $m \in M$, dado que $a \in S$ y M es un S-pseudomódulo, $am \in M$ y por lo tanto $\varphi(am) \geq 0$. Por otro lado, como u es unidad de orden de (A, M), existe $n \in \mathbb{N}$ tal que $nu - m \in M$ y en consecuencia $a(nu - m) \in M$. Luego,

  $$\varphi(a(nu - m)) \geq 0.$$

  Equivalentemente,

  $$\varphi(am) \leq \varphi(nau).$$

  Pero $\varphi(nau) = n\varphi(au) = 0$ y por lo tanto $\varphi(am) \leq 0$.

  Entonces, $\varphi(am) = 0$ como queríamos.

- Si $\varphi(au) \neq 0$, como $au \in M$, se tiene que $\varphi(au) > 0$. Utilizando *(i)* de la Observación 3.7, dado que $aM \subseteq M$, tenemos que φ_a es un estado mónico de (A, M, u).

  Por otro lado, dado que S es arquimediano, existe $n \in \mathbb{N}$ tal que $n - a \in S$, entonces $(n-a)M \subseteq M$ y tenemos que φ_{n-a} es un estado mónico de (A, M, u).

  Además, podemos suponer sin pérdida de generalidad que $\varphi(au) < n$ y en consecuencia

  $$\varphi\left((n - a)u\right) > 0.$$

Luego, por lo visto en *(ii)* de la Observación 3.7, podemos escribir

$$\varphi = \varphi_n = \varphi_{n-a+a} = \alpha\varphi_{n-a} + \beta\varphi_a,$$

con $\alpha + \beta = 1$ y $\alpha, \beta > 0$.

Luego, como φ es estado puro de (A, M, u), tenemos que $\varphi_{n-a} = \varphi_a = \varphi$. Entonces,

$$\varphi_a(b) = \varphi(b) \text{ para todo } b \in A,$$

y por lo tanto

$$\varphi(ab) = \varphi(au)\varphi(b) \text{ para todo } b \in A.$$

□

Corolario 3.10 *Sean S un subsemianillo arquimediano y $M \subseteq A$ un S-módulo, entonces todo estado puro de $(A, M, 1)$ está en $X(M)$.*

Demostración: Aplicar el Teorema 3.9 con $u = 1$. □

Veamos ahora el resultado que nos permitirá demostrar el Teorema de Pólya y otro certificado de no negatividad para el caso de poliedros compactos en la Sección 4.1.

Teorema 3.11 (Teorema de representación) *Sean S un subsemianillo arquimediano, $M \subseteq A$ un S-módulo y $a \in A$ tal que $\varphi(a) > 0$ para todo $\varphi \in X(M)$, entonces, existe $m \in \mathbb{N}$ tal que $ma \in M$.*

Demostración: Dado φ estado puro de $(A, M, 1)$, por el Corolario 3.10, φ está en $X(M)$ y por lo tanto, por hipótesis, $\varphi(a) > 0$. Luego, por el Teorema 2.20, existe $m \in \mathbb{N}$ tal que $ma \in M$. □

3.2. Módulos cuadráticos arquimedianos

En esta sección veremos que el Teorema 3.9 también vale cuando M es un módulo cuadrático. Si además M es arquimediano, por la Observación 3.2, tenemos que 1 es unidad de orden de (A, M) y podemos considerar estados puros de $(A, M, 1)$, en este caso tendremos un resultado análogo al Corolario 3.10.

Observemos que, en general, $\sum A^2$ no es arquimediano con lo cual tiene sentido estudiar este nuevo caso. En efecto, consideremos $A = \mathbb{R}[x]$ y $x \in \mathbb{R}[x]$, luego, es claro que no existe $n \in \mathbb{N}$ tal que $x + n \geq 0$ y por lo tanto $x + n$ no es suma de cuadrados.

Empecemos viendo algunos lemas técnicos.

Lema 3.12 *Sea $f(x) = \sqrt{1-x}$, entonces el polinomio de Taylor de orden n centrado en $x_0 = 0$ de f es*

$$t_n(x) = \sum_{k=0}^{n} \binom{\frac{1}{2}}{k} (-x)^k.$$

Además, la serie de Taylor tiene radio de convergencia $r = 1$.

Demostración: Veamos que para todo $k \in \mathbb{N}_0$,

$$\frac{f^{(k)}(0)}{k!} = (-1)^k \binom{\frac{1}{2}}{k}.$$

Inductivamente se puede ver que para todo $k \in \mathbb{N}_0$,

$$f^{(k)}(x) = \left(\prod_{i=0}^{k-1} \left(i - \frac{1}{2} \right) \right) (1-x)^{-\frac{2k-1}{2}}.$$

Por lo tanto,

$$\frac{f^{(k)}(0)}{k!} = \frac{\prod_{i=0}^{k-1} \left(i - \frac{1}{2} \right)}{k!} = \frac{(-1)^k \prod_{i=0}^{k-1} \left(\frac{1}{2} - i \right)}{k!} = (-1)^k \binom{\frac{1}{2}}{k}.$$

Para estudiar el radio de convergencia calculamos el límite para $k \to +\infty$ del cociente de D'Alambert:

$$\lim_{k \to +\infty} \frac{\left| (-1)^{k+1} \binom{\frac{1}{2}}{k+1} \right|}{\left| (-1)^k \binom{\frac{1}{2}}{k} \right|} =$$

$$= \lim_{k \to +\infty} \frac{\left| \left(\frac{1}{2} - k \right) \left(\frac{1}{2} - k + 1 \right) \cdots \left(\frac{1}{2} - 1 \right) \frac{1}{2} \right|}{(k+1)!} \frac{k!}{\left| \left(\frac{1}{2} - k + 1 \right) \left(\frac{1}{2} - k + 2 \right) \cdots \left(\frac{1}{2} - 1 \right) \frac{1}{2} \right|} =$$

$$= \lim_{k \to +\infty} \frac{k - \frac{1}{2}}{k+1} = 1,$$

Luego, la serie de Taylor tiene radio de convergencia $r = 1$. ▫

Lema 3.13 *Sea $f(x) = \sqrt{1-x}$ y t_n el polinomio de Taylor de orden n centrado en $x_0 = 0$ de f, entonces $p_n(x) := t_n(x)^2 - (1-x)$ tiene coeficientes no negativos en $\mathbb{Z}[\frac{1}{2}]$.*

Demostración: Escribamos

$$p_n(x) = t_n(x)^2 - (1-x) = \sum_{k=0}^{2n} a_k x^k,$$

$$t_n(x)^2 = \sum_{k=0}^{2n} b_k x^k.$$

Veamos que $a_k = 0$ para todo $0 \leq k \leq n$. En efecto,

$$a_0 = b_0 - 1 = 1 - 1 = 0,$$
$$a_1 = b_1 + 1 = \left(-\frac{1}{2} - \frac{1}{2}\right) + 1 = 0.$$

Para $2 \leq k \leq n$:

$$a_k = b_k = \sum_{i=0}^{k} \frac{f^{(i)}(0)}{i!}\frac{f^{(k-i)}(0)}{(k-i)!} = \frac{1}{k!}\sum_{i=0}^{k}\binom{k}{i} f^{(i)}(0) f^{(k-i)}(0) = \frac{1}{k!}(f^2)^{(k)}(0) = 0.$$

Para $n < k \leq 2n$ observemos primero que a_k es no negativo. En efecto,

$$a_k = \sum_{i=k-n}^{n} (-1)^k \binom{\frac{1}{2}}{i}\binom{\frac{1}{2}}{k-i}.$$

Luego, como el signo de $\binom{\frac{1}{2}}{j}$ es $(-1)^{j-1}$ para todo $j \in \mathbb{N}$, se tiene que $a_k \geq 0$. Para ver que $a_k \in \mathbb{Z}[\frac{1}{2}]$ basta ver que $\binom{\frac{1}{2}}{j} \in \mathbb{Z}[\frac{1}{2}]$ para todo $j \in \mathbb{N}$. Para $j = 0, 1$ es claro. Para $j \geq 2$, vemos primero que

$$\begin{aligned}
\frac{1}{j-1}\binom{2j-2}{j-2} &= \frac{1}{j-1}\left((2j-1)\binom{2j-2}{j-2} - (2j-2)\binom{2j-2}{j-2}\right) = \\
&= \frac{1}{j-1}\left(\frac{(2j-1)(2j-2)!(j-1)}{(j-2)!j!(j-1)} - (2j-2)\binom{2j-2}{j-2}\right) = \\
&= \frac{1}{j-1}\left(\frac{(2j-1)!(j-1)}{(j-1)!j!} - (2j-2)\binom{2j-2}{j-2}\right) = \\
&= \frac{1}{j-1}\left((j-1)\binom{2j-1}{j} - 2(j-1)\binom{2j-2}{j-2}\right) = \\
&= \binom{2j-1}{j} - 2\binom{2j-2}{j-2} \in \mathbb{Z}.
\end{aligned}$$

Luego

$$\begin{aligned}\binom{\frac{1}{2}}{j} &= \frac{\prod_{i=0}^{j-1}\left(\frac{1}{2}-i\right)}{j!} = \frac{\prod_{i=0}^{j-1}\left(\frac{1-2i}{2}\right)}{j!} = \frac{(-1)^{j-1}}{2^j j!}\prod_{i=1}^{j-1}(2i-1) = \\ &= \frac{(-1)^{j-1}}{2^j j!}\frac{(2j-3)!}{2\cdot 4\cdots(2j-4)} = \frac{(-1)^{j-1}}{2^j j!}\frac{(2j-3)!}{2^{j-2}(j-2)!} = \\ &= \frac{(-1)^{j-1}}{2^{2j-2}}\frac{(2j-3)!}{j!(j-2)!} = \frac{(-1)^{j-1}}{2^{2j-2}}\frac{(2j-3)!(2j-2)}{j!(j-2)!2(j-1)} = \\ &= \frac{(-1)^{j-1}}{2^{2j-1}}\frac{(2j-2)!}{j!(j-2)!(j-1)} = \frac{(-1)^{j-1}}{2^{2j-1}}\frac{1}{j-1}\binom{2j-2}{j-2},\end{aligned}$$

y por lo tanto tenemos que $\binom{\frac{1}{2}}{j} \in \mathbb{Z}[\frac{1}{2}]$ para todo $j \in \mathbb{N}$ como queríamos. ▫

A continuación veremos algunos resultados que necesitaremos más adelante.

Observación 3.14 *Sea $M \subseteq A$ pseudomódulo cuadrático. Si $\frac{1}{2} \in A$, se tiene que*

$$\frac{1}{2^k}M \subseteq M \text{ para todo } k \in \mathbb{N}.$$

Basta ver que $\frac{1}{2^k}$ es suma de cuadrados para todo $k \in \mathbb{N}$. En efecto, si k es par, es decir, $k = 2j$ para algún $j \in N$, entonces

$$\frac{1}{2^k} = \left(\frac{1}{2^j}\right)^2,$$

y si k es impar, es decir, $k = 2j-1$ para algún $j \in \mathbb{N}$, entonces

$$\frac{1}{2^k} = 2\frac{1}{2^{2j}} = \left(\frac{1}{2^j}\right)^2 + \left(\frac{1}{2^j}\right)^2.$$

El siguiente lema será útil para obtener a partir de un estado φ de (A, M, u) un nuevo estado φ_{1-a} de (A, M, u), siguiendo la Observación 3.7.

Lema 3.15 *Sean $M \subseteq A$ pseudomódulo cuadrático y u unidad de orden de (A, M). Si $\frac{1}{2} \in A$ y $a \in A$ cumple que $aM \subseteq M$ y $(1-2a)u \in M$, entonces para todo φ estado de (A, M) se tiene que $\varphi((1-a)M) \geq 0$.*

Demostración: Observemos que, dado que $aM \subseteq M$, por inducción se tiene que

$$a^k M \subseteq M \text{ para todo } k \in \mathbb{N}.$$

Veamos que $\frac{u}{2^k} - a^k u \in M$ para todo $k \in \mathbb{N}$. Por inducción en k:
Para $k = 1$, como $(1-2a)u \in M$, entonces, usando la Observación 3.14,

$$\frac{1}{2}(1-2a)u = \frac{u}{2} - au \in M.$$

Para el paso inductivo escribimos

$$\begin{aligned}\frac{u}{2^{k+1}} - a^{k+1}u &= \frac{1}{2}\left(\frac{u}{2^k} - a^k u + a^k u\right) - a^{k+1}u = \\ &= \frac{1}{2}\left(\frac{u}{2^k} - a^k u\right) + \frac{1}{2}a^k u - a^{k+1}u = \\ &= \frac{1}{2}\left(\frac{u}{2^k} - a^k u\right) + a^k\left(\frac{u}{2} - au\right).\end{aligned}$$

El primer término pertenece a M pues, por hipótesis inductiva, $\frac{u}{2^k} - a^k u \in M$ y por lo tanto $\frac{1}{2}\left(\frac{u}{2^k} - a^k u\right) \in M$. Para el segundo término, como, por el caso base, $\frac{u}{2} - au \in M$, entonces $a^k\left(\frac{u}{2} - au\right) \in a^k M \subseteq M$.
Sea φ estado de (A, M), observemos que si $\varphi \equiv 0$, el resultado es cierto de manera trivial. Supongamos entonces que φ es no nulo, entonces por la Observación 2.5, $\varphi(u) > 0$. Sin pérdida de generalidad podemos suponer que $\varphi(u) = 1$. De hecho, si $\varphi(u) \neq 1$ podemos tomar $\tilde{\varphi} := \frac{\varphi}{\varphi(u)}$, entonces $\tilde{\varphi}(u) = 1$ y $\tilde{\varphi}((1-a)m) \geq 0$ para todo $m \in M$ si y sólo si $\varphi((1-a)m) \geq 0$ para todo $m \in M$.
Dado que $\frac{u}{2^k} - a^k u \in M$ para todo $k \in \mathbb{N}$, se tiene que

$$\varphi\left(\frac{u}{2^k} - a^k u\right) \geq 0 \text{ para todo } k \in \mathbb{N}.$$

Equivalentemente,

$$\varphi(a^k u) \leq \varphi\left(\frac{u}{2^k}\right) \text{ para todo } k \in \mathbb{N}.$$

Pero, dado que φ es morfismo de grupos y $\varphi(u) = 1$, $\varphi\left(\frac{u}{2^k}\right) = \frac{1}{2^k}$ para todo $k \in \mathbb{N}$, y por lo tanto se tiene que

$$\varphi(a^k u) \leq \frac{1}{2^k} \text{ para todo } k \in \mathbb{N}. \tag{3.2}$$

Consideremos $f(x) = \sqrt{1-x}$, t_n el polinomio de Taylor de f de orden n centrado en $x_0 = 0$ y $p_n = t_n(x)^2 - (1-x)$. Por el Lema 3.13, p_n tiene coeficientes no negativos en $\mathbb{Z}[\frac{1}{2}]$. En consecuencia,

$$p_n(a)M \subseteq M. \tag{3.3}$$

En efecto, si escribimos

$$p_n(x) = \sum_{k=0}^{2n} a_k x^k,$$

y tomamos $m \in M$, tenemos que

$$p_n(a)m = \sum_{k=0}^{2n} a_k a^k m = \sum_{k=0}^{2n} a^k a_k m.$$

Luego, como $a_k \in \mathbb{Z}[\frac{1}{2}]$ y es no negativo, utilizando la Observación 3.14, es fácil ver que $a_k m \in M$, y por lo tanto, $a^k a_k m \in a^k M \subseteq M$.

Más aún, utilizando que φ es morfismo de grupos, tenemos que

$$\varphi(a_k m) = a_k \varphi(m) \text{ para todo } k = 0, \cdots, n \text{ y } m \in M. \tag{3.4}$$

Tomemos $m' \in M$ y veamos que $\varphi((1-a)m') \geq 0$. Como u es unidad de orden, existe $n_0 \in \mathbb{N}$ tal que $n_0 u - m' \in M$ y además, para todo $n \geq n_0$ también se tiene que $nu - m' \in M$, entonces, podemos tomar $r \in \mathbb{N}$ tal que $2^r u - m' \in M$. Luego, $\frac{1}{2^r}(2^r u - m') = u - \frac{m'}{2^r} \in \frac{1}{2^r} M \subseteq M$.

En consecuencia, por (3.3), $p_n(a)\left(u - \frac{m'}{2^r}\right) \in M$ y por lo tanto,

$$\varphi\left(p_n(a)\left(u - \frac{m'}{2^r}\right)\right) \geq 0,$$

equivalentemente,

$$\varphi\left(p_n(a)\frac{m'}{2^r}\right) \leq \varphi(p_n(a)u). \tag{3.5}$$

Además, usando (3.2) y (3.4),

$$\varphi(p_n(a)u) = \sum_{k=0}^{2n} \varphi(a_k a^k u) = \sum_{k=0}^{2n} a_k \varphi(a^k u) \leq \sum_{k=0}^{2n} a_k \frac{1}{2^k} = p_n\left(\frac{1}{2}\right). \tag{3.6}$$

Por otro lado, por el Lema 3.12, la serie de Taylor de f tiene radio de convergencia $r = 1$ y en particular

$$\lim_{n \longrightarrow +\infty} t_n\left(\frac{1}{2}\right) = f\left(\frac{1}{2}\right).$$

Luego, por definición de p_n,

$$\lim_{n \longrightarrow +\infty} p_n\left(\frac{1}{2}\right) = 0.$$

Entonces, dado $\epsilon > 0$ existe $n \in \mathbb{N}$ tal que

$$p_n\left(\frac{1}{2}\right) < \epsilon. \tag{3.7}$$

Por lo tanto, juntando (3.5), (3.6) y (3.7), tenemos que

$$\varphi\left(p_n(a)\frac{m'}{2^r}\right) < \epsilon.$$

Usando la definición de p_n, podemos escribir

$$\varphi\left(t_n(a)^2\frac{m'}{2^r}\right) - \varphi\left((1-a)\frac{m'}{2^r}\right) < \epsilon.$$

Equivalentemente,

$$\varphi\left((1-a)\frac{m'}{2^r}\right) > \varphi\left(t_n(a)^2\frac{m'}{2^r}\right) - \epsilon.$$

Como M es un pseudomódulo cuadrático, $t_n(a)^2\frac{m'}{2^r} \in M$ y por lo tanto, $\varphi\left(t_n(a)^2\frac{m'}{2^r}\right) \geq 0$, entonces,

$$\varphi\left((1-a)\frac{m'}{2^r}\right) > -\epsilon.$$

Haciendo $\epsilon \longrightarrow 0$, se tiene que

$$\varphi\left((1-a)\frac{m'}{2^r}\right) \geq 0.$$

Finalmente, $\varphi\left((1-a)\frac{m'}{2^r}\right) = \frac{\varphi((1-a)m')}{2^r}$, y por lo tanto $\varphi((1-a)m') \geq 0$. ▫

Veamos ahora un lema que nos permitirá simplificar algunas demostraciones más adelante.

Lema 3.16 *Sean $M \subseteq A$ un pseudomódulo cuadrático y u unidad de orden de (A, M). Consideremos*

$$A' := A \otimes_{\mathbb{Z}} \mathbb{Q},$$

$$M' := \{m \otimes q \mid m \in M \text{ y } q \in \mathbb{Q}_{\geq 0}\} \subseteq A' \text{ y}$$

$$u' := u \otimes 1.$$

Entonces,

(i) M' es un pseudomódulo cuadrático de A'.

(ii) u' *es unidad de orden de* (A', M').

(iii) Existe una correspondencia biunívoca entre los conjuntos $S(A, M, u)$ *y* $S(A', M', u')$ *que respeta estados puros.*

Demostración: (i) Es claro que $0 \in M'$. Tomemos $m_1 \otimes \frac{r_1}{n_1}$, $m_2 \otimes \frac{r_2}{n_2} \in M'$ con $r_1, r_2 \in \mathbb{N}_0$ y $n_1, n_2 \in \mathbb{N}$. Entonces

$$m_1 \otimes \frac{r_1}{n_1} + m_2 \otimes \frac{r_2}{n_2} = (r_1 n_2 m_1 + n_1 r_2 m_2) \otimes \frac{1}{n_1 n_2} \in M'.$$

Finalmente, si $a \otimes q \in A'$ y $m \otimes p \in M'$, entonces

$$(a \otimes q)^2 (m \otimes p) = a^2 m \otimes q^2 p \in M'.$$

Como M' es cerrado para la suma, podemos concluir que M' es pseudomódulo cuadrático.

(ii) Tomemos $a \otimes q \in A'$, sin pérdida de generalidad podemos suponer que $q > 0$. Como $u \in M$ es unidad de orden de (A, M), existe $n_1 \in \mathbb{N}$ tal que $n_1 u - a \in M$. Por otro lado, tomemos $n_2 \in \mathbb{N}$ tal que $n_2 - q \geq 0$. Entonces,

$$n_1 n_2 (u \otimes 1) - a \otimes q = n_1 u \otimes n_2 - a \otimes q = n_1 u \otimes (n_2 - q) + (n_1 u - a) \otimes q \in M'.$$

(iii) Definimos

$$S(A, M, u) \longrightarrow S(A', M', u'),\ \varphi \longmapsto \tilde{\varphi} \text{ definida por } \tilde{\varphi}(a \otimes q) := \varphi(a) q.$$

Es fácil comprobar que para todo $a, a' \in A$, $q, q' \in \mathbb{Q}$ y $n \in \mathbb{Z}$ se tiene que

$$\tilde{\varphi}((a + a') \otimes q) = \tilde{\varphi}(a \otimes q) + \tilde{\varphi}(a' \otimes q),$$

$$\tilde{\varphi}(a \otimes (q + q')) = \tilde{\varphi}(a \otimes q) + \tilde{\varphi}(a \otimes q') \text{ y}$$

$$\tilde{\varphi}(na \otimes q) = \tilde{\varphi}(a \otimes nq).$$

Luego, $\tilde{\varphi}$ está bien definida. Además, es claro que $\tilde{\varphi}$ es morfismo de grupos, $\tilde{\varphi}|_{M'} \geq 0$ y $\tilde{\varphi}(u') = 1$, luego la aplicación está bien definida.

Recíprocamente, definimos

$$S(A', M', u') \longrightarrow S(A, M, u),\ \psi \longmapsto \hat{\psi} \text{ definida por } \hat{\psi}(a) := \psi(a \otimes 1).$$

Es claro que $\hat{\psi}$ es morfismo de grupos, $\hat{\psi}|_M \geq 0$ y $\hat{\psi}(u) = 1$, luego la aplicación está bien definida.

Veamos que ambas aplicaciones son inversas; tomemos $\varphi \in S(A, M, u)$, entonces

$$\hat{\tilde{\varphi}}(a) = \tilde{\varphi}(a \otimes 1) = \varphi(a).$$

Recíprocamente, si tomamos $\psi \in S(A', M', u')$, entonces, como ψ es morfismo de grupos,

$$\tilde{\hat{\psi}}(a \otimes q) = \hat{\psi}(a)q = \psi(a \otimes 1)q = \psi(a \otimes q).$$

Finalmente, veamos que esta correspondencia respeta estados puros. Supongamos que φ es estado puro de (A, M, u) y veamos que $\tilde{\varphi}$ es estado puro de (A', M', u'). En efecto, si existen ψ_1, $\psi_2 \in S(A', M', u')$ tales que

$$\tilde{\varphi} = \frac{1}{2}\left(\psi_1 + \psi_2\right),$$

entonces,

$$\varphi = \frac{1}{2}\left(\hat{\psi}_1 + \hat{\psi}_2\right),$$

Luego, como φ es estado puro de (A, M, u) y $\hat{\psi}_1$, $\hat{\psi}_2 \in S(A, M, u)$, por *(ii)* de la Proposición 1.15, $\hat{\psi}_1 = \hat{\psi}_2 = \varphi$ y por lo tanto $\psi_1 = \psi_2 = \tilde{\varphi}$. De manera análoga se prueba que si ψ es estado puro de (A', M', u'), entonces $\hat{\psi}$ es estado puro de (A, M, u). □

Teorema 3.17 *Sean $M \subseteq A$ pseudomódulo cuadrático y $u \in M$ unidad de orden de (A, M). Entonces todo estado puro φ de (A, M, u) cumple que*

$$\varphi(ab) = \varphi(au)\varphi(b) \text{ para todo } a, b \in A. \tag{3.8}$$

Demostración: Consideremos

$$A' = A \otimes_{\mathbb{Z}} \mathbb{Q},$$

$$M' = \{m \otimes q \mid m \in M \text{ y } q \in \mathbb{Q}_{\geq 0}\} \subseteq A' \text{ y}$$

$$u' = u \otimes 1.$$

Entonces, como vimos en el Lema 3.16, $M' \subseteq A'$ es un pseudomódulo cuadrático, u' es unidad de orden y existe una correspondencia biunívoca entre los estados puros de (A, M, u) y los de (A', M', u'). Supongamos que tenemos probado (3.8) para los estados puros de (A', M', u') y tomemos φ estados puro de (A, M, u), entonces, según la correspondencia definida en el Lema 3.16, tenemos $\tilde{\varphi}$ estado puro de (A', M', u'); por lo tanto para todo $a, b \in A$ tenemos que

$$\tilde{\varphi}((a \otimes 1)(b \otimes 1)) = \tilde{\varphi}((a \otimes 1)(u \otimes 1))\tilde{\varphi}(b \otimes 1).$$

Luego, por definición de $\tilde{\varphi}$,

$$\varphi(ab) = \tilde{\varphi}(ab \otimes 1) = \tilde{\varphi}((a \otimes 1)(b \otimes 1)) =$$

$$= \tilde{\varphi}((a \otimes 1)(u \otimes 1))\tilde{\varphi}(b \otimes 1) = \tilde{\varphi}(au \otimes 1)\tilde{\varphi}(b \otimes 1) = \varphi(au)\varphi(b).$$

Entonces, basta probar (3.8) para los estados puros de (A', M', u'). Observemos que $\frac{1}{2} \in A'$, pues $\frac{1}{2} = 1 \otimes \frac{1}{2}$ y por lo tanto podemos suponer sin pérdida de generalidad que $\frac{1}{2} \in A$.

Como consecuencia, se tiene que $A = \sum A^2 - \sum A^2$, pues, para cada $a \in A$ podemos escribir

$$a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2.$$

Luego, basta probar (3.8) para todo $a \in \sum A^2$. Tomemos entonces φ estado puro de (A, M, u), $a \in \sum A^2$ y analicemos dos casos:

- Si $\varphi(au) = 0$, queremos ver que $\varphi(ab) = 0$ para todo $b \in A$. En efecto, como u es unidad de orden de (A, M), se tiene que

  $$A = M + \mathbb{Z}u.$$

  Por lo tanto,

  $$aA = aM + \mathbb{Z}au.$$

  Luego, como $\varphi(au) = 0$, basta ver que $\varphi(am) = 0$ para todo $m \in M$.

  Tomemos $m \in M$, dado que $a \in \sum A^2$ y M es un pseudomódulo cuadrático, $am \in M$ y por lo tanto $\varphi(am) \geq 0$. Por otro lado, como u es unidad de orden de (A, M), existe $n \in \mathbb{N}$ tal que $nu - m \in M$ y en consecuencia $a(nu - m) \in M$. Luego,

  $$\varphi(a(nu - m)) \geq 0.$$

  Equivalentemente,

  $$\varphi(am) \leq \varphi(nau).$$

  Pero $\varphi(nau) = n\varphi(au) = 0$ y por lo tanto $\varphi(am) \leq 0$.

  Entonces, $\varphi(am) = 0$ como queríamos.

- Si $\varphi(au) \neq 0$, como $au \in M$, se tiene que $\varphi(au) > 0$. Dado que u es unidad de orden de (A, M), existe $n \in \mathbb{N}$ tal que $nu - au \in M$, más aún, podemos suponer

sin pérdida de generalidad que $n = 2^m$ para algún $m \in \mathbb{N}$, en consecuencia, por la Observación 3.14,

$$\frac{1}{2^m}(2^m u - au) = u - \frac{1}{2^m}au = (1 - 2\frac{a}{2^{m+1}})u \in M.$$

Sea

$$a' := \frac{a}{2^{m+1}},$$

dado que $a \in \sum A^2$, tenemos que $aM \subseteq M$ y por lo tanto

$$a'M = \frac{a}{2^{m+1}}M \subseteq aM \subseteq M.$$

Además tenemos que

$$\varphi(a'u) = \varphi\left(\frac{au}{2^{m+1}}\right) = \frac{1}{2^{m+1}}\varphi(au) > 0.$$

Entonces, utilizando *(i)* de la Observación 3.7, tenemos que $\varphi_{a'}$ es estado mónico de (A, M, u).

Por otro lado, sin pérdida de generalidad, podemos suponer también que $\frac{1}{2^{m+1}}\varphi(au) < 1$ y entonces tenemos también que

$$\varphi((1 - a')u) = \varphi(u) - \varphi\left(\frac{au}{2^{m+1}}\right) = 1 - \frac{1}{2^{m+1}}\varphi(au) > 0.$$

Además, dado que $a'M \subseteq M$ y $(1 - 2a')u \in M$, podemos aplicar el Lema 3.15 tomando a' en lugar de a y por lo tanto $\varphi((1 - a')M) \geq 0$. Entonces $\varphi_{1-a'}$ también es estado mónico de (A, M, u).

Luego, siguiendo *(ii)* de la Observación 3.7, podemos escribir

$$\varphi = \varphi_1 = \varphi_{1-a'+a'} = \alpha\varphi_{1-a'} + \beta\varphi_{a'},$$

con $\alpha + \beta = 1$ y $\alpha, \beta > 0$ y como φ es estado puro de (A, M, u), tenemos que $\varphi_{1-a'} = \varphi_{a'} = \varphi$.

Entonces,

$$\varphi_{a'}(b) = \varphi(b) \text{ para todo } b \in A.$$

Es decir,

$$\varphi\left(\frac{a}{2^{m+1}}b\right) = \varphi\left(\frac{a}{2^{m+1}}u\right)\varphi(b) \text{ para todo } b \in A.$$

Finalmente, como φ es morfismo de grupos,

$$\varphi(ab) = \varphi(au)\varphi(b) \text{ para todo } A \in I.$$

□

Corolario 3.18 *Sea $M \subseteq A$ módulo cuadrático arquimediano, entonces todo estado puro de $(A, M, 1)$ está en $X(M)$.*

Demostración: Aplicar el Teorema 3.17 con $u = 1$. □

Veamos ahora el resultado que nos permitirá demostrar el Teorema de Reznick y los Schmüdgen y Putinar Positivstellensätze en la Sección 4.2.

Teorema 3.19 (Teorema de representación) *Sean $M \subseteq A$ módulo cuadrático arquimediano y $a \in A$ tal que $\varphi(a) > 0$ para todo $\varphi \in X(M)$, entonces, existe $m \in \mathbb{N}$ tal que $ma \in M$.*

Demostración: Dado φ estado puro de $(A, M, 1)$, por el Corolario 3.18, φ está en $X(M)$ y por lo tanto, por hipótesis, $\varphi(a) > 0$. Luego, por el Teorema 2.20, existe $m \in \mathbb{N}$ tal que $ma \in M$. □

Una pregunta que surge es si vale que todo morfismo de anillos es un estado puro. Si $\mathbb{R} \subseteq A$, la respuesta es sí. Los resultados que veremos a continuación nos servirán para probarlo.

Lema 3.20 *Sean $0 \leq \alpha, \beta \leq 1$, entonces*

$$(\alpha\beta)^{\frac{1}{2}} + ((1-\alpha)(1-\beta))^{\frac{1}{2}} \leq 1.$$

La igualdad vale solo cuando $\alpha = \beta$.

Demostración: Consideremos $K = [0,1] \times [0,1]$ y $f : K \to \mathbb{R}$ definida por

$$f(\alpha, \beta) = (\alpha\beta)^{\frac{1}{2}} + ((1-\alpha)(1-\beta))^{\frac{1}{2}},$$

Como K es compacto y f es continua, f alcanza máximo absoluto.

- En el interior de K:

  $$\nabla f(\alpha, \beta) = (0, 0)$$

  si y sólo si

  $$\begin{cases} (\alpha\beta)^{-\frac{1}{2}}\beta(1-\alpha) - ((1-\alpha)(1-\beta))^{\frac{1}{2}} = 0 \\ (\alpha\beta)^{-\frac{1}{2}}\alpha(1-\beta) - ((1-\alpha)(1-\beta))^{\frac{1}{2}} = 0 \end{cases}$$

  Restando las ecuaciones tenemos que

  $$(\alpha\beta)^{-\frac{1}{2}} \left(\beta(1-\alpha) - \alpha(1-\beta)\right) = 0.$$

  Por lo tanto, $\alpha = \beta$. Entonces, los puntos críticos de f en el interior de K son (α, α) con $0 < \alpha < 1$ y $f(\alpha, \alpha) = 1$ para todo $0 < \alpha < 1$.

- En el borde de K se puede ver fácilmente que el máximo de f se alcanza en $(0,0)$ y en $(1,1)$ y $f(0,0) = f(1,1) = 1$.

Luego, el máximo valor que alcanza f es 1 y se realiza sólo si $\alpha = \beta$. ▫

Lema 3.21 *Sea $M \subseteq A$ módulo cuadrático. Si $\mathbb{R} \subseteq A$, entonces para todo $\varphi \in S(A,M)$ se tiene que*

$$\varphi(\alpha x) = \alpha\varphi(x) \text{ para todo } \alpha \in \mathbb{R}, x \in A.$$

Demostración: Sea $\varphi \in S(A,M)$. Observemos que cada $x \in A$ tenemos que

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$$

y, como M es módulo cuadrático, $\sum A^2 \subseteq M$, luego basta probar que la igualdad vale para todo x en M.

Como φ es morfismo de grupos, es claro que $\varphi(qx) = q\varphi(x)$ para todo $q \in \mathbb{Q}$, $x \in M$.

Tomemos $\alpha_1, \alpha_2 \in \mathbb{R}$ tal que $\alpha_1 > \alpha_2$, entonces, para cada $x \in M$ tenemos que $(\alpha_1 - \alpha_2)x \in M$ pues $\alpha_1 - \alpha_2 = \sqrt{\alpha_1 - \alpha_2}^2$ es un cuadrado, y por lo tanto

$$\varphi(\alpha_1 x) - \varphi(\alpha_2 x) = \varphi((\alpha_1 - \alpha_2)x) \geq 0.$$

Entonces,

$$\varphi(\alpha_1 x) \geq \varphi(\alpha_2 x).$$

Finalmente, tomemos $\alpha \in \mathbb{R}$ y $x \in M$. Consideremos dos casos:

- Si $\varphi(x) = 0$, queremos ver que $\varphi(\alpha x) = 0$. En efecto, tomemos $q_1, q_2 \in \mathbb{Q}$ tal que $q_1 < \alpha < q_2$, entonces tenemos que

  $$\varphi(q_1 x) \leq \varphi(\alpha x) \leq \varphi(q_2 x).$$

  Luego, como $\varphi(q_i x) = q_i\varphi(x) = 0$ para $i = 1, 2$,

  $$\varphi(\alpha x) = 0.$$

- Si $\varphi(x) \neq 0$, entonces $\varphi(x) > 0$. Supongamos que $\varphi(\alpha x) \neq \alpha\varphi(x)$. Entonces, tenemos dos casos:

- Si $\varphi(\alpha x) > \alpha\varphi(x)$, tenemos que

$$\frac{\varphi(\alpha x)}{\varphi(x)} > \alpha.$$

Luego, existe $q \in \mathbb{Q}$ tal que

$$\frac{\varphi(\alpha x)}{\varphi(x)} > q > \alpha.$$

En particular,

$$\varphi(\alpha x) > q\varphi(x) = \varphi(qx).$$

Por otro lado, dado que $\alpha < q$, se tiene que

$$\varphi(\alpha x) \leq \varphi(qx),$$

lo cual es un absurdo.

- Si $\varphi(\alpha x) < \alpha\varphi(x)$ se procede de manera análoga.

Por lo tanto, $\varphi(\alpha x) = \alpha\varphi(x)$.

□

Lema 3.22 *Sean $M \subseteq A$ módulo cuadrático y $\varphi \in S(A, M)$. Supongamos $\mathbb{R} \subseteq A$, entonces,*

(i) $\varphi(x^2)^2 \leq \varphi(x)\varphi(x^3)$ *para todo* $x \in M$,

(ii) $\varphi(xy)^2 \leq \varphi(x^2)\varphi(y^2)$ *para todo* $x, y \in A$.

Demostración: (i) Tomemos $x \in M$, entonces, para cada $\alpha \in \mathbb{R}$ tenemos que, como M es un módulo cuadrático, $(x - \alpha)^2 x \in M$ y por lo tanto, usando el Lema 3.21,

$$0 \leq \varphi((x - \alpha)^2 x) = \varphi(x^3 - 2\alpha x^2 + \alpha^2 x) = \varphi(x^3) - 2\alpha\varphi(x^2) + \alpha^2\varphi(x).$$

En consecuencia, el discriminante de la cuadrática debe ser menor o igual a cero, es decir

$$4\varphi(x^2)^2 - 4\varphi(x)\varphi(x^3) \leq 0.$$

Equivalentemente,

$$\varphi(x^2)^2 \leq \varphi(x)\varphi(x^3).$$

(ii) Tomemos $\varphi \in S(A, M)$ y $x, y \in A$, entonces, para cada $\alpha \in \mathbb{R}$ tenemos que $(x - \alpha y)^2 \in M$ y por lo tanto

$$\varphi((x - \alpha y)^2) \geq 0.$$

El resultado se sigue repitiendo el argumento hecho en *(i)*. □

La demostración de la siguiente proposición esta basada en la dada en [3, Theorem 13].

Proposición 3.23 *Sea $M \subseteq A$ módulo cuadrático y supongamos $\mathbb{R} \subseteq A$. Si $\varphi \in S(A, M)$ verifica que*

$$\varphi(xy) = \varphi(x)\varphi(y) \text{ para todo } x, y \in M,$$

y existen φ_1, $\varphi_2 \in S(A, M)$ tales que $\varphi = \varphi_1 + \varphi_2$, entonces existen $c_1, c_2 \geq 0$ tales que $\varphi_i = c_i\varphi$ para $i = 1, 2$.

Demostración: Veamos que existe $c_1 \geq 0$ tal que $\varphi_1 = c_1\varphi$. Observemos que, como M es un módulo cuadrático y para cada $x \in A$ tenemos que

$$x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2,$$

basta probar que $\varphi_1 = c_1\varphi$ en M.
Tomemos $x \in M$ tal que $\varphi(x) = 0$, entonces

$$\varphi_1(x) = -\varphi_2(x),$$

pero, dado que $\varphi_i|_M \geq 0$ para $i = 1, 2$, se tiene que

$$\varphi_1(x) = \varphi_2(x) = 0.$$

Luego, basta probar que existe $c_1 \in \mathbb{R}$ tal que

$$\varphi_1(x) = c_1\varphi(x) \text{ para todo } x \in M \text{ tal que } \varphi(x) \neq 0.$$

Más aún, basta probar que

$$\varphi_1(x) = \varphi_1(y) \text{ para todo } x, y \in M \text{ tales que } \varphi(x) = \varphi(y) = 1. \tag{3.9}$$

En efecto, supongamos que tenemos probado (3.9) y tomemos $x, y \in M$ tales que $\varphi(x), \varphi(y) \neq 0$, es decir, $\varphi(x), \varphi(y) > 0$. Consideremos $\tilde{x} := \frac{x}{\varphi(x)}$ e $\tilde{y} := \frac{y}{\varphi(y)}$. Dado que M es un módulo cuadrático, tenemos que $\tilde{x}$, $\tilde{y} \in M$. Además, por el Lema 3.21

$$\varphi(\tilde{x}) = \varphi\left(\frac{x}{\varphi(x)}\right) = \frac{\varphi(x)}{\varphi(x)} = 1.$$

Análogamente, $\varphi(\tilde{y}) = 1$. Luego, por (3.9), se tiene que

$$\varphi_1(\tilde{x}) = \varphi_1(\tilde{y}).$$

Entonces, nuevamente, por el Lema 3.21,

$$\frac{\varphi_1(x)}{\varphi(x)} = \frac{\varphi_1(y)}{\varphi(y)}.$$

Es decir, $\frac{\varphi_1}{\varphi}$ es constante en $M \cap \{\varphi \neq 0\}$, como queríamos. Dado que $\varphi|_M \geq 0$ y $\varphi_1|_M \geq 0$, c_1 debe ser necesariamente mayor o igual a cero.

Veamos primero que para $x \in M$ tal que $\varphi(x) = 1$, ocurre que $\varphi_1(x) = \varphi_1(x^2)$.

Observemos que:

- Como $x \in M$, $\varphi_i(x) \geq 0$ para $i = 1, 2$. Además,

  $$1 = \varphi(x) = \varphi_1(x) + \varphi_2(x).$$

  Por lo tanto $0 \leq \varphi_1(x) \leq 1$.

- Si escribimos $x^3 = x^2 x$, dado que $x^2 \in \sum A^2$ y $x \in M$ tenemos que $x^3 \in M$ y por lo tanto $\varphi_i(x^3) \geq 0$ para $i = 1, 2$. Además, por hipótesis, se tiene que

  $$\varphi(x^3) = \varphi(x)^3 = 1.$$

  Entonces, con el mismo argumento del item anterior, se puede ver que $0 \leq \varphi_1(x^3) \leq 1$.

Por otro lado, por *(i)* del Lema 3.22, tenemos que

$$\varphi_i(x^2)^2 \leq \varphi_i(x)\varphi_i(x^3) \text{ para } i = 1, 2.$$

Equivalentemente, dado que $\varphi_i(x^2) \geq 0$ para $i = 1, 2$,

$$\varphi_i(x^2) \leq (\varphi_i(x)\varphi_i(x^3))^{\frac{1}{2}} \text{ para } i = 1, 2. \tag{3.10}$$

Además, como $x \in M$ y $\varphi(x) = 1$ se tiene que $\varphi(x^2) = \varphi(x)^2 = 1$.
Luego, tenemos que

$$1 = \varphi(x^2) = \varphi_1(x^2) + \varphi_2(x^2) \leq (\varphi_1(x)\varphi_1(x^3))^{\frac{1}{2}} + (\varphi_2(x)\varphi_2(x^3))^{\frac{1}{2}}.$$

Más aún, utilizando el Lema 3.20, con $\alpha = \varphi_1(x)$ y $\beta = \varphi_1(x^3)$, tenemos que

$$1 \leq (\varphi_1(x)\varphi_1(x^3))^{\frac{1}{2}} + (\varphi_2(x)\varphi_2(x^3))^{\frac{1}{2}} \leq 1.$$

Por lo tanto deben ser todas igualdades y en consecuencia $\varphi_1(x) = \varphi_1(x^3)$. Más aún, la desigualdad (3.10), debe ser una igualdad para $i = 1, 2$. En particular, para $i = 1$, se tiene que

$$\varphi_1(x^2) = (\varphi_1(x)\varphi_1(x^3))^{\frac{1}{2}} = \varphi_1(x).$$

Probemos ahora (3.9). Sean $x, y \in M$ tales que $\varphi(x) = \varphi(y) = 1$. Por lo probado arriba, tenemos que

$$\varphi_1(x^2) = \varphi_1(x) \text{ y } \varphi_1(y^2) = \varphi_1(y). \tag{3.11}$$

Por otro lado, tenemos que

$$\varphi((x-y)^2) = \varphi(x)^2 - 2\varphi(x)\varphi(y) + \varphi(y)^2 = 1 - 2 + 1 = 0.$$

Además, $(x-y)^2 \in M$ y en consecuencia, por lo probado al comienzo de la demostración, $\varphi_1((x-y)^2) = 0$.
Luego, utilizando *(ii)* de Lema 3.22, tenemos que

$$0 = \varphi_1(x^2)\varphi_1((x-y)^2) \geq \varphi_1(x(x-y))^2 \geq 0.$$

Entonces, deben ser todas igualdades y por lo tanto

$$\varphi_1(x(x-y)) = 0.$$

Equivalentemente,

$$\varphi_1(x^2) = \varphi_1(xy).$$

Análogamente,

$$\varphi_1(y^2) = \varphi_1(xy).$$

Finalemente, utilizando (3.11), tenemos que

$$\varphi_1(x) = \varphi_1(x^2) = \varphi_1(xy) = \varphi_1(y^2) = \varphi_1(y).$$

□

Corolario 3.24 *Sea $M \subseteq A$ módulo cuadrático arquimediano. Si $\mathbb{R} \subseteq A$, entonces todo $\varphi \in X(M)$ es estado puro de $(A, M, 1)$.*

Demostración: Tomemos $\varphi \in X(M)$ y supongamos que existen $\varphi_1, \varphi_2 \in S(A, M, 1)$ tales que

$$\varphi = \frac{1}{2}(\varphi_1 + \varphi_2).$$

Entonces, por la Proposición 3.23, existen $c_1, c_2 \geq 0$ tales que

$$\frac{1}{2}\varphi_i = c_i\varphi \text{ para } i = 1, 2.$$

En particular,

$$\frac{1}{2}\varphi_i(1) = c_i\varphi(1) \text{ para } i = 1, 2.$$

Luego, como $\varphi_1(1) = \varphi_2(1) = \varphi(1) = 1$,

$$\frac{1}{2} = c_1 = c_2.$$

En consecuencia,

$$\varphi_1 = \varphi_2 = \varphi.$$

Por la Proposición 1.15 esto prueba que φ es estado puro de $(A, M, 1)$. □

Capítulo 4

Certificados de no negatividad

Como anticipamos, como objetivo principal de esta tesis, en este capítulo veremos cómo a partir de la teoría de estados puros se consiguen nuevas demostraciones más conceptuales de varios resultados relacionados con certificados de no negatividad, incluyendo el Teoremas de Pólya y los Schmüdgen y Putinar Positivstellensätze, entre otros. Este nuevo enfoque proviene de [4] y utiliza varios resultados clásicos que se pueden encontrar por ejemplo en [10].

A partir de ahora consideraremos el anillo $A = \mathbb{R}[x_1, \cdots, x_n]$ de polinomios en n variables con coeficientes en $\mathbb{R}$, que por comodidad notaremos con $\mathbb{R}[x]$ si no presta a confusión.

Empecemos con un lema sencillo pero, como se verá más adelante, de gran importancia.

Lema 4.1

(i) La identidad es el único morfismo de anillos de $\mathbb{R}$ *en* $\mathbb{R}$.

(ii) La aplicación

$$\mathrm{Hom}(\mathbb{R}[x], \mathbb{R}) \longrightarrow \mathbb{R}^n,\ \varphi \longmapsto (\varphi(x_1), \cdots, \varphi(x_n))$$

es una biyección.

Demostración: (i) Consideremos $\varphi : \mathbb{R} \to \mathbb{R}$ morfismo de anillos. Es fácil comprobar que $\varphi|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}}$. Veamos que φ debe ser creciente; en efecto, tomemos $\alpha_1, \alpha_2 \in \mathbb{R}$ tal que $\alpha_1 > \alpha_2$, entonces

$$\varphi(\alpha_1) - \varphi(\alpha_2) = \varphi(\alpha_1 - \alpha_2) = \varphi(\sqrt{\alpha_1 - \alpha_2}^2) = \varphi(\sqrt{\alpha_1 - \alpha_2})^2 \geq 0.$$

Por lo tanto, $\varphi(\alpha_1) \geq \varphi(\alpha_2)$.
Finalmente, tomemos $\alpha \in \mathbb{R}$ y supongamos que $\varphi(\alpha) \neq \alpha$, entonces, tenemos dos casos:

- Si $\varphi(\alpha) > \alpha$, entonces existe $q \in \mathbb{Q}$ tal que

$$\varphi(\alpha) > q > \alpha. \tag{4.1}$$

  Dado que φ es creciente, tenemos que $\varphi(q) > \varphi(\alpha)$, pero $\varphi(q) = q$ y por lo tanto

$$q > \varphi(\alpha),$$

  lo cual contradice (4.1).

- Si $\varphi(\alpha) < \alpha$ se procede de manera análoga.

(ii) Veamos que la aplicación

$\mathbb{R}^n \longrightarrow \mathrm{Hom}(\mathbb{R}[x], \mathbb{R})$, $(a_1, \cdots, a_n) \longmapsto \varphi$ definido por $\varphi(x_i) = a_i$ para $i = 1, \cdots, n$

es la inversa. Consideremos $\varphi \in \mathrm{Hom}(\mathbb{R}[x], \mathbb{R})$. Por *(i)*, $\varphi|_{\mathbb{R}} = \mathrm{Id}_{\mathbb{R}}$ y por lo tanto φ queda determinado por $(\varphi(x_1), \cdots, \varphi(x_n))$; en efecto, tomemos $f \in \mathbb{R}[x]$, entonces,

$$f(x) = \sum_{\substack{e \in \mathbb{N}_0^n, \\ e_1 + \cdots + e_n \leq \mathrm{gr}(f)}} \alpha_e \prod_{i=1}^{n} x_i^{e_i}.$$

Luego,

$$\varphi(f) = \varphi\left(\sum_{\substack{e \in \mathbb{N}_0^n, \\ e_1 + \cdots + e_n \leq \mathrm{gr}(f)}} \alpha_e \prod_{i=1}^{n} x_i^{e_i} \right) =$$

$$= \sum_{\substack{e \in \mathbb{N}_0^n, \\ e_1 + \cdots + e_n \leq \mathrm{gr}(f)}} \alpha_e \prod_{i=1}^{n} \varphi(x_i)^{e_i} = f(\varphi(x_1), \cdots, \varphi(x_n)).$$

Ahora, es de fácil comprobación que ambas aplicaciones son inversas. □

A continuación introducimos el conjunto H_P que nos permitirá caracterizar a los conjuntos arquimedianos.

Definición 4.2 *Sea $P \subseteq \mathbb{R}[x]$ un subsemigrupo , definimos*

$$H_P := \{f \in \mathbb{R}[x] \mid \text{ existe } k \in \mathbb{Z} \text{ tal que } k \pm f \in P\}.$$

Observación 4.3 *Sea $P \subseteq \mathbb{R}[x]$ subsemigrupo tal que $1 \in P$ y tomemos $f \in H_P$, entonces existe $k \in \mathbb{Z}$ tal que $k \pm f \in P$. Dado que P es cerrado para la suma y $1 \in P$, podemos suponer sin pérdida de generalidad que $k > 0$; más aún, podemos suponer que k es mayor a cualquier constante positiva.*

Observación 4.4 *Sea $P \subseteq \mathbb{R}[x]$ subsemigrupo tal que $1 \in P$, entonces, P es arquimediano si y sólo si $H_P = \mathbb{R}[x]$. En efecto, es claro que si $H_P = \mathbb{R}[x]$, entonces P es arquimediano. Recíprocamente, si P es arquimediano y tomamos $f \in \mathbb{R}[x]$, entonces, existe $k_1, k_2 \in \mathbb{N}$ tales que $k_1 + f \in P$ y $k_2 - f \in P$. Luego, si $k = \max\{k_1, k_2\}$, $k \pm f \in P$.*

Notación 4.5 *Dado $S = \{g_1, \cdots, g_l\}$ un subconjunto finito de $\mathbb{R}[x]$, notamos*

$$K_S := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \text{ para } i = 1, \cdots, l\} \subseteq \mathbb{R}^n.$$

4.1. Teorema de Pólya y una aplicación del Teorema de Minkowski

Empecemos con algunas definiciones y resultados que necesitaremos.

Definición 4.6 *Sea $M \subseteq \mathbb{R}[x]$ un subconjunto, M es **preprimo** si*

- $M + M \subseteq M$,
- $MM \subseteq M$,
- $\mathbb{Q}_{\geq 0} \subseteq M$.

Observación 4.7 *Si M es preprimo, es un subsemianillo de $\mathbb{R}[x]$ y además es simultáneamente un M-módulo.*

Lema 4.8 *Sea $M \subseteq \mathbb{R}[x]$ preprimo, entonces $H_M \subseteq \mathbb{R}[x]$ es un subanillo.*

Demostración:

- $0 \in H_M$ pues $0 \pm 0 = 0 \in M$ y $1 \in H_M$ pues $1 \pm 0 = 1 \in M$.
- Dados $f_1, f_2 \in H_M$, existen $k_1, k_2 \in \mathbb{Z}$ tales que $k_i \pm f_i \in M$ para $i = 1, 2$, entonces
$$(k_1 + k_2) \pm (f_1 + f_2) = (k_1 \pm f_1) + (k_2 \pm f_2) \in M \text{ y}$$
$$k_1 k_2 \pm f_1 f_2 = \frac{1}{2}(k_1 \mp f_1)(k_2 - f_2) + \frac{1}{2}(k_1 \pm f_1)(k_2 + f_2) \in M.$$
- Finalmente, dado $f \in H_M$, existe $k \in \mathbb{Z}$ tal que $k \pm f \in M$, luego $-f \in H_M$.

□

Finalmente estamos en condiciones de demostrar el primer certificado de no negatividad de esta tesis. La demostración original de este resultado proviene de [11].

Teorema 4.9 (Teorema de Pólya) *Sean $f \in \mathbb{R}[x]$ homogéneo y*

$$K = \left\{ x \in \mathbb{R}^n \mid x_i \geq 0 \text{ para todo } i = 1, \cdots, n \text{ y } \sum_{i=1}^{n} x_i \neq 0 \right\}.$$

Si $f > 0$ en K, entonces existe $k \in \mathbb{N}$ tal que $\left(\sum_{i=1}^{n} x_i\right)^k f$ tiene coeficientes no negativos.

Demostración: Sean $M \subseteq \mathbb{R}[x]$ el preprimo generado por $\mathbb{R}_{\geq 0}$ y $x_1, \cdots, x_n$, es decir, el conjunto formado por todos los polinomios en $\mathbb{R}[x]$ con coeficientes no negativos e $I \subseteq \mathbb{R}[x]$ el ideal generado por $1 - \sum_{i=1}^{n} x_i$. Consideremos el preprimo $M_1 = M + I$. Tenemos que $x_i \in M_1$ y

$$1 - x_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} x_j + 1 - \sum_{j=1}^{n} x_j \in M_1$$

para todo $i = 1, \cdots, n$, entonces $x_i \in H_{M_1}$ para todo $i = 1, \cdots, n$. Además, como $\mathbb{R}_{\geq 0} \subseteq M_1$, entonces $\mathbb{R} \subseteq H_{M_1}$. Luego, usando el Lema 4.8, $H_{M_1} = \mathbb{R}[x]$ y por lo tanto, como vimos en la Observación 4.4, M_1 es arquimediano.

Consideremos ahora el conjunto

$$K_1 := \left\{ x \in \mathbb{R}^n \mid x_i \geq 0 \text{ para todo } i = 1, \cdots, n \text{ y } \sum_{i=1}^{n} x_i = 1 \right\} \subseteq \mathbb{R}^n.$$

Dado que $K_1 \subseteq K$, tenemos que $f > 0$ en K_1.
Veamos que, vía la aplicación definida en *(ii)* del Lema 4.1, $X(M_1)$ se corresponde con K_1. Tomemos $\varphi \in X(M_1)$, entonces, como $x_i \in M_1$ para todo $i = 1, \cdots, n$, $\varphi(x_i) \geq 0$ para todo $i = 1, \cdots, n$ y, como $\pm(1 - \sum_{i=1}^n x_i) \in M_1$, $\sum_{i=1}^n \varphi(x_i) = 1$. Recíprocamente, si $(a_1, \cdots, a_n) \in K_1$, veamos que $\varphi \in \mathrm{Hom}(\mathbb{R}[x], \mathbb{R})$ definido por $\varphi(x_i) = a_i$ para todo $i = 1, \cdots, n$ pertenece a $X(M_1)$. En efecto, como $a_i \geq 0$ para todo $i = 1, \cdots, n$, $\varphi|_M \geq 0$ y, como $\sum_{i=1}^n a_i = 1$, $\varphi|_I \equiv 0$. Entonces, $\varphi|_{M_1} \geq 0$.
Como consecuencia, si $\varphi \in X(M_1)$, $(\varphi(x_1), \cdots, \varphi(x_n)) \in K_1$ y como

$$\varphi(f) = f(\varphi(x_1), \cdots, \varphi(x_n)),$$

se tiene que $\varphi(f) > 0$.
Por el Teorema 3.11, existe $m \in \mathbb{N}$ tal que $mf \in M_1$; más aún, como M_1 es cerrado para la multiplicación y $\mathbb{Q}_{\geq 0} \subseteq M_1$, se tiene que $f \in M_1$, es decir,

$$f(x) = g(x) + h(x)\left(1 - \sum_{i=1}^n x_i\right) \tag{4.2}$$

con $g \in M$ y $h \in \mathbb{R}[x]$. Luego, sustituyendo x_i por $\frac{x_i}{\sum_{j=1}^n x_j}$ para todo $i = 1, \cdots, n$ en (4.2), el término $h(x)\,(1 - \sum_{i=1}^n x_i)$ se anula y si $d = \mathrm{gr}(f)$, como f es homogenéo, se tiene que

$$\frac{1}{\left(\sum_{j=1}^n x_j\right)^d} f(x_1, \cdots, x_n) = g\left(\frac{x_1}{\sum_{j=1}^n x_j}, \cdots, \frac{x_n}{\sum_{j=1}^n x_j}\right).$$

Dado que g tiene coeficientes no negativos, para concluir el resultado basta limpiar denominadores en g multiplicando la última igualdad por $\left(\sum_{j=1}^n x_j\right)^N$ para un $N \in \mathbb{N}$ suficientemente grande. ▫

Observación 4.10 *Vale la pena aclarar cual es el certificado que se obtiene en el Teorema 4.9. Observemos que si $f \in \mathbb{R}[x]$ verifica que $(\sum_{i=1}^n x_i)^k f$ tiene coeficientes no negativos para algún $k \in \mathbb{N}$, entonces, resulta evidente que f es no negativo en K.*

El siguiente certificado de no negatividad que probaremos en esta tesis es uno que aplica al caso de polinomios positivos sobre poliedros compactos. Utilizando la teoría de estados puros, este resultado se sigue fácilmente a partir del Teorema de Minkowski que probamos a continuación. Como referencia para este resultado se puede consultar [12, Theorem 5.4.5].

Teorema 4.11 (Teorema de Minkowski) *Sean $S = \{g_1, \cdots, g_l\} \subseteq \mathbb{R}[x]$ un subconjunto finito tal que g_i tiene grado 1 para todo $i = 1, \cdots, l$ y $f \in \mathbb{R}[x]$, también de grado 1. Si K_S es no vacío y $f \geq 0$ en K_S, entonces, $f \in \mathbb{R}_{\geq 0} + \mathbb{R}_{\geq 0}g_1 + \cdots + \mathbb{R}_{\geq 0}g_l$.*

Demostración: Podemos suponer sin pérdida de generalidad que $0 \in K_S$, pues si no tomamos $x_0 \in K_S$ y consideramos

$$\tilde{g}_i(x) := g_i(x + x_0) \text{ para } i = 1, \cdots, l,$$
$$\tilde{S} = \{\tilde{g}_1, \cdots, \tilde{g}_l\} \text{ y}$$
$$\tilde{f}(x) := f(x + x_0).$$

Es claro que $0 \in K_{\tilde{S}}$ y dado que $f \geq 0$ en K_S, $\tilde{f} \geq 0$ en $K_{\tilde{S}}$, luego si probamos que $\tilde{f} \in \mathbb{R}_{\geq 0} + \mathbb{R}_{\geq 0}\tilde{g}_1 + \cdots + \mathbb{R}_{\geq 0}\tilde{g}_l$, especializando en $x - x_0$, tenemos que $f \in \mathbb{R}_{\geq 0} + \mathbb{R}_{\geq 0}g_1 + \cdots + \mathbb{R}_{\geq 0}g_l$.
Escribamos

$$g_i = l_i + \alpha_i \text{ con } l_i \in \mathbb{R}[x] \text{ homogéneo y } \alpha_i \in \mathbb{R} \text{ para cada } i = 1, \cdots, l \text{ y}$$
$$f = l + \alpha \text{ con } l \in \mathbb{R}[x] \text{ homogéneo y } \alpha \in \mathbb{R}.$$

Luego, como $0 \in K_S$, tenemos que $\alpha_i \geq 0$ para todo $i = 1, \cdots, l$.
Consideremos para cada $i = 1, \cdots, l$, G_i la homogeinización de g_i, es decir

$$G_i(x_0, x_1, \cdots, x_n) = l_i(x_1, \cdots, x_n) + \alpha_i x_0,$$

y F la homogeinización de f, es decir

$$F(x_0, x_1, \cdots, x_n) = l(x_1, \cdots, x_n) + \alpha x_0.$$

Entonces, si $G_0(x_0, x_1, \cdots, x_n) := x_0$ y consideramos $S' = \{G_0, G_1, \cdots, G_l\} \subseteq \mathbb{R}[x_0, \cdots, x_n]$, tenemos que $F \geq 0$ en $K_{S'}$. En efecto, tomemos $(a_0, \cdots, a_n) \in K_{S'}$ y consideremos dos casos:

- Si $a_0 \neq 0$, entonces, $G_0(a_0, \cdots, a_n) = a_0 > 0$. Luego, como $G_i(a_0, \cdots, a_n) \geq 0$ para todo $i = 1, \cdots, l$, se tiene que

  $$g_i\left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) = \frac{1}{a_0}G_i(a_0, \cdots, a_n) \geq 0$$

  para todo $i = 1, \cdots, l$, es decir, $\left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) \in K_S$ y por lo tanto

  $$F(a_0, \cdots, a_n) = a_0 f\left(\frac{a_1}{a_0}, \cdots, \frac{a_n}{a_0}\right) \geq 0.$$

- Si $a_0 = 0$, entonces,

$$l_i(a_1, \cdots, a_n) = G_i(a_0, a_1, \cdots, a_n) \geq 0$$

para todo $i = 1, \cdots, l$ y como $\alpha_i \geq 0$ para todo $i = 1, \cdots, l$, se tiene que $g_i(a_1, \cdots, a_n) \geq 0$ para todo $i = 1, \cdots, l$, es decir, $(a_1, \cdots, a_n) \in K_S$ y por lo tanto

$$F(a_0, a_1, \cdots, a_n) = f(a_1, \cdots, a_n) \geq 0.$$

Ahora, como para $i = 1, \cdots, l$, $G_i \in \mathbb{R}[x_0, \cdots, x_n]$ es homogéneo de grado 1, se pueden identificar con un punto $p_i \in \mathbb{R}^{n+1}$, de igual manera $F \in \mathbb{R}[x_0, \cdots, x_n]$ se puede indentificar con un punto $p \in \mathbb{R}^{n+1}$. Consideremos

$$C = \left\{ \sum_{i=1}^{l} \beta_i p_i \mid \beta_i \in \mathbb{R}_{\geq 0} \text{ para todo } i = 1, \cdots, l \right\} \subseteq \mathbb{R}^{n+1}$$

y supongamos que p no pertenece a C, entonces, por la Proposición 1.13 tomando $A = C$ y $B = \{p\}$, existe $\rho : \mathbb{R}^{n+1} \to \mathbb{R}$ funcional lineal y continuo tal que $C \subseteq \{\rho > 0\}$ y $p \in \{\rho < 0\}$.

Por lo tanto, tenemos que

$$G_i(\rho(e_0), \cdots, \rho(e_n)) = \rho(p_i) > 0 \text{ para todo } i = 1, \cdots, l \text{ y}$$

$$F(\rho(e_0), \cdots, \rho(e_n)) = \rho(p) < 0,$$

lo cual es un absurdo. Luego $p \in C$, es decir, existen $\beta_i \in \mathbb{R}_{\geq 0}$ para $i = 1, \cdots, l$ tales que

$$p = \sum_{i=0}^{l} \beta_i p_i.$$

En consecuencia,

$$F = \sum_{i=0}^{l} \beta_i G_i.$$

Finalmente, si especializamos en $x_0 = 1$ tenemos que

$$f = \beta_0 + \sum_{i=1}^{l} \beta_i g_i.$$

□

Como aplicación del Teorema de Minkowski, obtenemos el siguiente certificado de no negatividad, que proviene originalmente de [7].

Notación 4.12 *Dado* $S = \{g_1, \cdots, g_l\} \subseteq \mathbb{R}[x]$ *notamos*

$$P_S := \left\{ \sum_{e \in \mathbb{N}_0^l} \beta_e \prod_{i=1}^{l} g_i^{e_i} \;\mid\; \beta_e \in \mathbb{R}_{\geq 0},\ \beta_e = 0 \text{ salvo para finitos } e \in \mathbb{N}_0^l \right\}.$$

Observación 4.13 *Se puede verificar fácilmente que* P_S *es preprimo y de hecho es el menor preprimo que contiene a* $\mathbb{R}_{\geq 0}$ *y* $g_1, \cdots, g_l$.

Teorema 4.14 *Sean* $S = \{g_1, \cdots, g_l\} \subseteq \mathbb{R}[x]$ *un subconjunto finito tal que* g_i *tiene grado* 1 *para todo* $i = 1, \cdots, l$ *y* $f \in \mathbb{R}[x]$. *Si* K_S *es un compacto no vacío y* $f > 0$ *en* K_S, *entonces* $f \in P_S$.

Demostración: Fijemos $i = 1, \cdots, n$, como K_S es compacto, existe $N \in \mathbb{N}$ tal que $N \pm x_i \geq 0$ en K_S, luego, por el Teorema 4.11,

$$N \pm x_i \in \mathbb{R}_{\geq 0} + \mathbb{R}_{\geq 0} g_1 + \cdots + \mathbb{R}_{\geq 0} g_l \subseteq P_S.$$

Por lo tanto $x_i \in H_{P_S}$. Además, como $\mathbb{R}_{\geq 0} \subseteq P_S$, $\mathbb{R} \subseteq H_{P_S}$, entonces, usando el Lema 4.8, $H_{P_S} = \mathbb{R}[x]$ y por lo tanto, P_S es arquimediano.
Veamos que, vía la aplicación definida en *(ii)* del Lema 4.1, $X(P_S)$ se corresponde con K_S. Tomemos $\varphi \in X(P_S)$, entonces para todo $i = 1, \cdots, l$

$$g_i(\varphi(x_1), \cdots, \varphi(x_n)) = \varphi(g_i) \geq 0.$$

Recíprocamente, si $(a_1, \cdots, a_n) \in K_S$, entonces $\varphi \in \mathrm{Hom}(\mathbb{R}[x], \mathbb{R})$ definido por $\varphi(x_i) := a_i$ para todo $i = 1, \cdots, n$ pertenece a $X(P_S)$. En efecto, basta observar que

$$\varphi(g_i) = g_i(a_1, \cdots, a_n) \geq 0,$$

luego, si $g \in P_S$ tenemos que

$$g = \sum_{e \in \mathbb{N}_0^l} \beta_e \prod_{i=1}^{l} g_i^{e_i} \text{ con } \beta_e \in \mathbb{R}_{\geq 0},\ \beta_e = 0 \text{ salvo para finitos } e \in \mathbb{N}_0^l$$

y por lo tanto

$$\varphi(g) = \sum_{e \in \mathbb{N}_0^l} \beta_e \prod_{i=1}^{l} \varphi(g_i)^{e_i} \geq 0.$$

Dado que $f > 0$ en K_S, concluimos que $\varphi(f) > 0$ para todo $\varphi \in X(P_S)$.
Finalmente, por el Teorema 3.11, existe $m \in \mathbb{N}$ tal que $mf \in P_S$ y, como P_S es preprimo, se tiene que $f \in P_S$. ▫

4.2. Teorema de Reznick y Schmüdgen y Putinar Positivstellensätze

Veamos para empezar algunas propiedades de H_M con M un módulo cuadrático, que necesitaremos más adelante.

Lema 4.15 *Sea $M \subseteq \mathbb{R}[x]$ módulo cuadrático, entonces, para todo $f \in \mathbb{R}[x]$ se tiene que $f \in H_M$ si y sólo si $f^2 \in H_M$.*

Demostración: Sea $f \in \mathbb{R}[x]$ y supongamos que $f \in H_M$, entonces, existe $k \in \mathbb{N}$ tal que $k \pm f \in M$. Veamos que $k^2 \pm f^2 \in M$, lo que prueba que $f^2 \in H_M$. En efecto, como M es módulo cuadrático, es claro que $k^2 + f^2 \in M$. Por otro lado, tenemos que

$$k^2 - f^2 = \frac{1}{2k}\left((k+f)^2(k-f) + (k-f)^2(k+f)\right) \in M.$$

Recíprocamente, supongamos que $f^2 \in H_M$, entonces, existe $k \in \mathbb{N}$ tal que $k \pm f^2 \in M$. Veamos que $k \pm f \in M$, lo que prueba que $f \in H_M$. En efecto,

$$k + f = \frac{1}{2}\left((k-1) + (k - f^2) + (f+1)^2\right) \in M,$$

$$k - f = \frac{1}{2}\left((k-1) + (k - f^2) + (f-1)^2\right) \in M.$$

□

Lema 4.16 *Sea $M \subseteq \mathbb{R}[x]$ módulo cuadrático, entonces $H_M \subseteq \mathbb{R}[x]$ es un subanillo.*

Demostración:

- $0 \in H_M$ pues $0 \pm 0 = 0 \in M$ y $1 \in H_M$ pues $1 \pm 0 = 1 \in M$.
- Dados $f_1, f_2 \in H_M$, existen $k_1, k_2 \in \mathbb{Z}$ tales que $k_i \pm f_i \in M$ para $i = 1, 2$, entonces
$$(k_1 + k_2) \pm (f_1 + f_2) = (k_1 \pm f_1) + (k_2 \pm f_2) \in M.$$
- Dado $f \in H_M$, existe $k \in \mathbb{Z}$ tal que $k \pm f \in M$, luego $-f \in H_M$.

- Finalmente, dados $f_1, f_2 \in H_M$, por lo probado anteriormente, $f_1 + f_2$ y $f_1 - f_2 \in H_M$, entonces, por el Lema 4.15, $(f_1 + f_2)^2$ y $(f_1 - f_2)^2 \in H_M$.

  Luego, si escribimos,

  $$(f_1 + f_2)^2 - (f_1 - f_2)^2 = 4f_1f_2,$$

  tenemos que $4f_1f_2 \in H_M$, es decir, existe $k \in \mathbb{Z}$ tal que $k \pm 4f_1f_2 \in M$ y podemos suponer $k = 4k'$, con $k' \in \mathbb{Z}$. Finalmente, como M es módulo cuadrático,

  $$\frac{1}{4}(k \pm 4f_1f_2) = k' \pm f_1f_2 \in M.$$

  Por lo tanto, $f_1f_2 \in H_M$.

□

Lema 4.17 *Sean $M \subseteq \mathbb{R}[x]$ módulo cuadrático y $f_1, \cdots, f_l \in \mathbb{R}[x]$. Entonces, $\sum_{i=1}^{l} f_i^2 \in H_M$ si y sólo si $f_i \in H_M$ para todo $i = 1, \cdots, l$.*

Demostración: Es claro que si $f_i \in H_M$ para todo $i = 1, \cdots, l$, entonces $\sum_{i=1}^{l} f_i^2 \in H_M$, pues, por el Lema 4.16, H_M es un subanillo. Supongamos que $\sum_{i=1}^{l} f_i^2 \in H_M$, entonces, existe $k \in \mathbb{N}$ tal que

$$k \pm \sum_{i=1}^{l} f_i^2 \in M.$$

Dado $i_0 = 1, \cdots, l$, es claro que $k + f_{i_0}^2 \in M$. Por otro lado, si escribimos

$$k - f_{i_0}^2 = k - \sum_{i=1}^{l} f_i^2 + \sum_{\substack{i=1 \\ i \neq i_0}}^{l} f_i^2.$$

Dado que $k - \sum_{i=1}^{l} f_i^2 \in M$ y $\sum_{\substack{i=1 \\ i \neq i_0}}^{l} f_i^2 \in M$, se tiene que $k - f_{i_0}^2 \in M$. Por lo tanto, $f_{i_0}^2 \in H_M$ y en consecuencia, por el Lema 4.15, $f_{i_0} \in H_M$. □

Lema 4.18 *Sea $M \subseteq \mathbb{R}[x]$ módulo cuadrático. Son equivalentes:*

(i) M es arquimediano.

(ii) Existe $k \in \mathbb{N}$ tal que

$$k - \sum_{i=1}^{n} x_i^2 \in M.$$

Demostración: Supongamos que M es arquimediano, entonces dado $\sum_{i=1}^{n} x_i^2 \in \mathbb{R}[x]$, existe $k \in \mathbb{N}$ tal que $k - \sum_{i=1}^{n} x_i^2 \in M$.

Recíprocamente, supongamos que existe $k \in \mathbb{N}$ tal que $k - \sum_{i=1}^{n} x_i^2 \in M$. Como M es un módulo cuadrático, también $k + \sum_{i=1}^{n} x_i^2 \in M$ y por lo tanto $\sum_{i=1}^{n} x_i^2 \in H_M$. Entonces, por el Lema 4.17, $x_i \in H_M$ para todo $i = 1, \cdots, n$.

Por otro lado, para todo $\alpha \in \mathbb{R}$ existe $m \in \mathbb{N}$ tal que $m \pm \alpha \geq 0$ y por lo tanto $m \pm \alpha \in M$. Entonces, $\alpha \in H_M$. Esto prueba que $\mathbb{R} \subseteq M$.

Finalmente, por el Lema 4.16, H_M es un subanillo y por lo tanto debe ser $H_M = A$, lo que prueba que M es arquimediano. ▫

Estamos en condiciones ahora de demostrar el siguiente certificado de no negatividad, que proviene originalmente de [14].

Teorema 4.19 (Teorema de Reznick) *Si $f \in \mathbb{R}[x]$ es homogéneo y $f > 0$ en $\mathbb{R}^n - \{0\}$, entonces existe $k \in \mathbb{N}$ tal que*

$$\left(\sum_{i=1}^{n} x_i^2\right)^k f \in \sum \mathbb{R}[x]^2.$$

Demostración: Observemos que f necesariamente debe tener grado par, pues, como f es homogéneo, tenemos que

$$f(\lambda x) = \lambda^d f(x)$$

para todo $\lambda \in \mathbb{R}$ y $x \in \mathbb{R}^n$, entonces, si d es impar, para $\lambda < 0$ y $x \neq 0$ se tiene un absurdo.

Sea $I \subseteq \mathbb{R}[x]$ el ideal generado por $1 - \sum_{i=1}^{n} x_i^2$. Consideramos el módulo cuadrático $M = \sum \mathbb{R}[x]^2 + I$. Como $1 - \sum_{i=1}^{n} x_i^2 \in M$, por el Lema 4.18, M es arquimediano.

Consideremos ahora la esfera

$$\mathbb{S}^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\}.$$

Veamos que, vía la aplicación definida en *(ii)* del Lema 4.1, $X(M)$ se corresponde con $\mathbb{S}^{n-1}$. Tomemos $\varphi \in X(M)$, entonces, como $\pm(1 - \sum_{i=1}^{n} x_i^2) \in M$, $\sum_{i=1}^{n} \varphi(x_i)^2 = 1$. Recíprocamente, si $(a_1, \cdots, a_n) \in \mathbb{S}^{n-1}$, veamos que $\varphi \in \mathrm{Hom}(\mathbb{R}[x], \mathbb{R})$ definido por $\varphi(x_i) = a_i$ para todo $i = 1, \cdots, n$ pertenece a $X(M)$. En efecto, basta observar que, como $\sum_{i=1}^{n} a_i^2 = 1$, entonces $\varphi|_I \equiv 0$.

Dado que $f > 0$ en $\mathbb{S}^{n-1}$, concluimos que $\varphi(f) > 0$ para todo $\varphi \in X(M)$.
Entonces, por el Teorema 3.19, existe $m \in \mathbb{N}$ tal que $mf \in M$. Como M es módulo cuadrático,

$$f = \left(\frac{1}{\sqrt{m}}\right)^2 mf \in M.$$

Es decir,

$$f(x) = \sum_{j=1}^{l} g_j(x)^2 + h(x)\left(1 - \sum_{i=1}^{n} x_i^2\right)$$

con $g_j, h \in \mathbb{R}[x]$. Luego, sustituyendo x_i por $\frac{x_i}{\|x\|}$ para todo $i = 1, \cdots, n$, el término $h(x)\left(1 - \sum_{i=1}^{n} x_i^2\right)$ se anula y si $d = \operatorname{gr}(f)$, como f es homogéneo, se tiene que

$$\frac{1}{\|x\|^d} f(x_1, \cdots, x_n) = \sum_{j=1}^{l} g_j\left(\frac{x_1}{\|x\|}, \cdots, \frac{x_n}{\|x\|}\right)^2. \tag{4.3}$$

Multiplicando por $\|x\|^{2N}$ para un $N \in \mathbb{N}$ suficientemente grande de manera de limpiar denominadores en g_j para todo $j = 1, \cdots, l$ en (4.3), se tiene que

$$\|x\|^{2k} f(x) = \sum_{j=1}^{l} \left(g_{j,1}(x) + g_{j,2}(x)\|x\|\right)^2 =$$

$$= \sum_{j=1}^{l} \left(g_{j,1}(x)^2 + g_{j,2}(x)^2\|x\|^2\right) + 2\left(\sum_{j=1}^{l} g_{j,1}(x)g_{j,2}(x)\right)\|x\|$$

donde $g_{j,1}, g_{j,2} \in \mathbb{R}[x]$ para todo $j = 1, \cdots, l$. Más aún, como la función $\|x\|$ no es una función racional, necesariamente tenemos que

$$\sum_{j=1}^{l} g_{j,1}(x)g_{j,2}(x) = 0$$

y por lo tanto

$$\|x\|^{2k} f(x) = \sum_{j=1}^{l} \left(g_{j,1}(x)^2 + g_{j,2}(x)^2\|x\|^2\right),$$

como queríamos demostrar. □

Observación 4.20 *Nuevamente, vale la pena aclarar cual es el certificado que se obtiene en el Teorema 4.19. Observemos que si $f \in \mathbb{R}[x]$ verifica que*

$$\left(\sum_{i=1}^{n} x_i^2\right)^k f \in \sum \mathbb{R}[x]^2$$

para algún $k \in \mathbb{N}$, entonces, resulta evidente que f es no negativo en $\mathbb{R}^n - \{0\}$.

Observación 4.21 *Notar que el Teorema de Reznick implica la respuesta afirmativa al Problema 17 de Hilbert en el caso de un polinomio homogéneo que resulta positivo en* $\mathbb{R}^n - \{0\}$.

Los últimos resultados que demostraremos en esta tesis son los Schmüdgen y Putinar Positivstellensätze. Para las demostraciones clásicas de estos resultados se puede consultar [15] y [13] respectivamente. Veamos primero algunas definiciones y resultados auxiliares.

Definición 4.22 *Un subsemianillo* $M \subseteq \mathbb{R}[x]$ *es un* ***preordering*** *si* $\sum \mathbb{R}[x]^2 \subseteq M$.

Definición 4.23 *Sea* $S = \{g_1, \cdots, g_l\}$ *un subconjunto finito de* $\mathbb{R}[x]$*, definimos el* ***preordering generado por S***

$$T_S := \left\{ \sum_{I \subseteq \{1,\cdots,l\}} p_I \prod_{i \in I} g_i \mid p_I \in \sum \mathbb{R}[x]^2 \right\}.$$

Observación 4.24 *Es fácil comprobar que* T_S *es un preodering y de hecho es el menor preodering que contiene a* S.

Recordemos la versión clásica del Positivstellensatz.

Teorema 4.25 (Positivstellensatz) *Sean* $S \subseteq \mathbb{R}[x]$ *subconjunto finito y* $f \in \mathbb{R}[x]$. *Entonces,*

(i) $f > 0$ *en* K_S *si y sólo si existen* $p, q \in T_S$ *tales que* $pf = 1 + q$.

(ii) $f \geq 0$ *en* K_S *si y sólo si existen* $n \in \mathbb{N}$, $p, q \in T_S$ *tales que* $pf = f^{2n} + q$.

(iii) $f = 0$ *en* K_S *si y sólo si existe* $n \in \mathbb{N}$ *tal que* $-f^{2n} \in T_S$.

(iv) $K_S = \varnothing$ *si y sólo si* $-1 \in T_S$.

Demostración: Ver [10, 2.2.1]. ▫

Lema 4.26 *Sea* $S \subseteq \mathbb{R}[x]$ *subconjunto finito. Entonces,* K_S *es compacto si y sólo si* T_S *es arquimediano.*

Demostración: Supongamos que K_S es compacto. En particular, K_S es acotado y por lo tanto, existe $k \in \mathbb{N}$ tal que

$$\sum_{i=1}^{n} x_i^2 < k \text{ para todo } x \in K_S.$$

Es decir,

$$k - \sum_{i=1}^{n} x_i^2 > 0 \text{ en } K_S.$$

Luego, por *(i)* del Teorema 4.25, existen $p, q \in T_S$ tales que

$$p\left(k - \sum_{i=1}^{n} x_i^2\right) = 1 + q.$$

Entonces,

$$p\left(k - \sum_{i=1}^{n} x_i^2\right)^2 = (1+q)\left(k - \sum_{i=1}^{n} x_i^2\right)$$

y por lo tanto,

$$(1+q)\left(k - \sum_{i=1}^{n} x_i^2\right) \in T_S. \tag{4.4}$$

Consideremos $S' = S \cup \{k - \sum_{i=1}^{n} x_i^2\}$, entonces, se tiene que $k - \sum_{i=1}^{n} x_i^2 \in T_{S'}$ y por lo tanto, por el Lema 4.18, $T_{S'}$ es arquimediano. Luego, existe $m \in \mathbb{N}$ tal que $m - q \in T_{S'}$, es decir

$$m - q = q_1 + q_2\left(k - \sum_{i=1}^{n} x_i^2\right) \text{ con } q_1, q_2 \in T_S.$$

Entonces,

$$\begin{aligned}(m-q)(1+q) &= \left(q_1 + q_2\left(k - \sum_{i=1}^{n} x_i^2\right)\right)(1+q) = \\ &= q_1(1+q) + q_2\left(k - \sum_{i=1}^{n} x_i^2\right)(1+q).\end{aligned}$$

Por lo tanto, usando (4.4),

$$(m-q)(1+q) \in T_S. \tag{4.5}$$

Luego, usando (4.4) y (4.5),

$$k\left((m-q)(1+q)+\left(\frac{m}{2}-q\right)^2\right)+(1+q)\left(k-\sum_{i=1}^{n}x_i^2\right)+q\sum_{i=1}^{n}x_i^2\in T_S.$$

Observemos que

$$(m-q)(1+q)+\left(\frac{m}{2}-q\right)^2=m+mq-q-q^2+\frac{m^2}{4}-mq+q^2=\frac{m^2}{4}+m-q.$$

Por lo tanto,

$$k\left((m-q)(1+q)+\left(\frac{m}{2}-q\right)^2\right)+(1+q)\left(k-\sum_{i=1}^{n}x_i^2\right)+q\sum_{i=1}^{n}x_i^2=$$

$$=k\left(\frac{m^2}{4}+m-q\right)+(1+q)\left(k-\sum_{i=1}^{n}x_i^2\right)+q\sum_{i=1}^{n}x_i^2=$$

$$=k\frac{m^2}{4}+km-kq+k-\sum_{i=1}^{n}x_i^2+kq-q\sum_{i=1}^{n}x_i^2+q\sum_{i=1}^{n}x_i^2=$$

$$=k\frac{m^2}{4}+km+k-\sum_{i=1}^{n}x_i^2=$$

$$=k\left(\frac{m}{2}+1\right)^2-\sum_{i=1}^{n}x_i^2.$$

Luego, se tiene que

$$k\left(\frac{m}{2}+1\right)^2-\sum_{i=1}^{n}x_i^2\in T_S.$$

Además podemos suponer sin pérdida de generalidad que m es par, luego, por el Lema 4.18, T_S es arquimediano.

Supongamos ahora que T_S es arquimediano, entonces, por el Lema 4.18, existe $k\in\mathbb{N}$ tal que

$$k-\sum_{i=1}^{n}x_i^2\in T_S.$$

Es decir, si $S=\{g_1,\cdots,g_l\}$,

$$k-\sum_{i=1}^{n}x_i^2=\sum_{I\subseteq\{1,\cdots,l\}}p_I\prod_{i\in I}g_i \text{ con } p_I\in\sum\mathbb{R}[x]^2.$$

Entonces, si $x \in K_S$,

$$k - \sum_{i=1}^{n} x_i^2 \geq 0.$$

Equivalentemente,

$$\sum_{i=1}^{n} x_i^2 \leq k.$$

Esto prueba que K_S es acotado. Es claro que K_S es cerrado y por lo tanto es compacto. □

Teorema 4.27 (Schmüdgen Positivstellensatz) *Sean $S \subseteq \mathbb{R}[x]$ subconjunto finito y $f \in \mathbb{R}[x]$. Si K_S es compacto y $f > 0$ en K_S, entonces $f \in T_S$.*

Demostración: Observemos que, como T_S es un preordering, en particular es un módulo cuadrático y como K_S es compacto, por Lema 4.26, T_S es arquimediano.
Veamos que, vía la aplicación definida en *(ii)* del Lema 4.1, $X(T_S)$ se corresponde con K_S. Supongamos que $S = \{g_1, \cdots, g_l\}$ y tomemos $\varphi \in X(T_S)$, entonces

$$g_i(\varphi(x_1), \cdots, \varphi(x_n)) = \varphi(g_i) \geq 0 \text{ para todo } i = 1, \cdots, l$$

pues $g_i \in T_S$ para todo $i = 1, \cdots, m$. Recíprocamente, si $(a_1, \cdots, a_n) \in K_S$, veamos que $\varphi \in \mathrm{Hom}(\mathbb{R}[x], \mathbb{R})$ definido por $\varphi(x_i) = a_i$ pertenece a $X(T_S)$. Sea $g \in T_S$, entonces

$$g = \sum_{I \subseteq \{1, \cdots, l\}} p_I \prod_{i \in I} g_i, \text{ con } p_I \in \sum \mathbb{R}[x]^2.$$

Luego, dado que $g_i(a_1, \cdots, a_n) \geq 0$ para todo $i = 1, \cdots, l$, se tiene que $g(a_1, \cdots, a_n) \geq 0$. Finalmente, basta observar que

$$\varphi(g) = g(a_1, \cdots, a_n).$$

Por lo tanto, $\varphi(g) \geq 0$.
Dado que $f > 0$ en K_S, concluimos que $\varphi(f) > 0$ para todo $\varphi \in X(T_S)$.
Entonces, por el Teorema 3.19, existe $m \in \mathbb{N}$ tal que $mf \in T_S$; como T_S es módulo cuadrático, se sigue que $f \in T_S$. □

Definición 4.28 *Sea $S = \{g_1, \cdots, g_l\}$ un subconjunto finito de $\mathbb{R}[x]$, definimos el* ***módulo cuadrático generado por S***

$$M_S := \left\{ p_0 + p_1 g_1 \cdots + p_l g_l \mid p_0, \cdots, p_l \in \sum \mathbb{R}[x]^2 \right\}.$$

Observación 4.29 *Es fácil comprobar que M_S es un módulo cuadrático y de hecho es el menor módulo cuadrático que contiene a S.*

Teorema 4.30 (Putinar Positivstellensatz) *Sean $S \subseteq \mathbb{R}[x]$ subconjunto finito y $f \in \mathbb{R}[x]$. Si existe $N \in \mathbb{N}$ tal que*

$$N - \sum_{i=1}^{n} x_i^2 \in M_S,$$

y $f > 0$ en K_S, entonces $f \in M_S$.

Demostración: Observemos que, como existe $N \in \mathbb{N}$ tal que $N - \sum_{i=1}^{n} x_i^2 \in M_S$, por el Lema 4.18, M_S es arquimediano.

De manera análoga a lo hecho en la demostración del Teorema 4.27, se puede ver que, vía la aplicación definida en *(ii)* del Lema 4.1, $X(M_S)$ se corresponde con K_S y por lo tanto, dado que $f > 0$ en K_S, se tiene que $\varphi(f) > 0$ para todo $\varphi \in X(M_S)$. Entonces, por el Teorema 3.19, existe $m \in \mathbb{N}$ tal que $mf \in M_S$; como M_S es módulo cuadrático, se sigue que $f \in M_S$. ▫

Bibliografía

[1] E. Artin, Uber die Zerlegung definiter Funktionen in Quadrate. *Abh. Math. Sem. Hamburg* 5, 85-99, 1927.

[2] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*. Results in Mathematics and Related Areas (3), 36. Springer-Verlag, Berlin, 1998.

[3] F. Bonsall, J. Lindenstrauss, R. Phelps, Extreme positive operators on algebras of functions. *Math. Scand*. 18, 161-182, 1966.

[4] S. Burgdorf, C. Scheiderer, M. Schweighofer, Pure States, Nonnegative Polynomial and Sums of Squares. *Comment. Math. Helv*. 87, 2012.

[5] John B. Conway, *A course in Functional Analysis*. Springer, 2nd edition, 1990.

[6] K. R. Goodearl, *Partially Ordered Abelian Groups with Interpolation*. Math. Surv. Monographs 20, AMS, Providence, RI, 1986.

[7] David Handelman, Representing polynomials by positive linear functions on compact convex polyhedra. *Pacific J. Math.* 132, no. 1, 35-62, 1988.

[8] J.-L. Krivine, Anneaux préordonnés. *J. Analyse Math.* 12, 307-326, 1964.

[9] J.-B. Lasserre, *Moments, positive polynomials and their applications*. Imperial College Press Optimization Series 1, Imperial College Press, London, 2010.

[10] M. Marshall, *Positive Polynomials and Sums of Squares*. Math. Surv. Monographs 146, AMS, Providence, RI, 2008.

[11] G. Polya, Über positive Darstellung von Polynomen. *Vierteljahresschrift der Naturforschenden Gesellschaft in Zurich* 73, 141-145, 1928.

[12] A. Prestel, Ch. Delzell, *Positive Polynomials: From Hilbert's 17th Problem to Real Algebra*. Monographs Math., Springer, 2001.

[13] M. Putinar, Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.* 42, no. 3, 969-984, 1993.

[14] B. Reznick, Uniform denominators in Hilbert's Seventeenth Problem. *Math. Z.* 220, 75-98, 1995.

[15] K. Schmüdgen, The K-moment problem for compact semi-algebraic sets. *Math. Ann.* 289, no. 2, 203-206 1991.

[16] G. Stengle, A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Math. Ann.* 207, 87-97, 1974.