Universidad de Cantabria

Facultad
de
Ciencias

Una prueba meramente algebraica del Lema de Sauer-Shelah-Perles

(A purely algebraic proof of the Sauer-Shelah-Perles Lemma)

Trabajo de Fin de Grado
para acceder al

Grado en Matemáticas

Autor: David Gutiérrez Cambra
Director: Luis Miguel Pardo Vasallo
Julio - 2023

Abstract. The objective of this memory is to give a purely algebraic proof of the Sauer-Shelah-Perles Lemma (inspired by the elegant proof in [**FrPa,1983**]), based only in duality in the $\mathbb{Q}-$algebra $\mathbb{Q}[V_n]$ of polynomial functions defined on the zero-dimensional algebraic variety of subsets of the set $[n] := \{1, 2, \ldots, n\}$. In fact, two different proofs of this lemma will be given. Furthermore, we prove how several other classical results from Combinatorics are particular examples of a Trace (Inversion) Formula in finite $\mathbb{Q}-$algebras. For instance, one of this results is the general form of the Inclusion-Exclusion Principle (both with direct and reverse order associated to subsets inclusion). This approach also allows us to show a basis of the space of null $t-$designs, which differs from the one described in Theorem 4 of [**DeFr,1982**]. All results are still true if we replace $\mathbb{Q}[V_n]$ by $K[V_n]$, where K is a perfect field of characteristic different from 2. This memory has then the underlying purpose of connecting two fields of mathematical knowledge that are not usually connected, at least not in this form.

Key words. Sauer-Shelah-Perles Lemma, Combinatorics, Duality in artinian $K-$algebras, Trace (Inversion) Formula, Exclusion-Inclusion Principle.

Resumen. El objetivo de esta memoria es dar una demostración puramente algebraica del Lema de Sauer-Shelah-Perles (inspirada en la elegante demostración que aparece en [**FrPa,1983**]), basada únicamente en técnicas de dualidad en la $\mathbb{Q}-$álgebra $\mathbb{Q}[V_n]$ de funciones polinomiales definidas en la variedad algebraica cero-dimensional de subconjuntos del conjunto $[n] := \{1, 2, \ldots, n\}$. De hecho, se darán dos demostraciones distintas de este lema. Además, demostramos cómo algunos otros resultados clásicos de la combinatoria son ejemplos particulares de una Fórmula (de Inversión) de la Traza en $\mathbb{Q}-$álgebras finitas. Por ejemplo, uno de estos resultados es la forma general del Principio de Inclusión-exclusión (considerando tanto el orden usual como el orden reverso asociado a la inclusión de subconjuntos). Este enfoque también nos permite presentar una base del espacio de null $t-$designs, que difiere de la proporcionada en el Teorema 4 de [**DeFr,1982**]. Todos los resultados siguen siendo ciertos si reemplazamos $\mathbb{Q}[V_n]$ por $K[V_n]$, donde K es un cuerpo perfecto de característica distinta de 2. Así, esta memoria tiene el propósito subyacente de conectar dos campos del conocimiento matemático que no suelen estarlo, al menos no de la forma aquí presentada.

Palabras clave. Lema de Sauer-Shelah-Perles, Combinatoria, Dualidad en $K-$álgebras artinianas, Fórmula (de Inversión) de la Traza, Principio de Inclusión-exclusión.

Índice

CAPíTULO 0

Introducción y Resumen de Contenidos de la Memoria

Índice

0.1. Introducción

El presente Trabajo de Fin de Grado pretende completar, hasta hacer auto-contenida, revisar y exponer los resultados esenciales que se exponen en el trabajo [**Pa,2023**]. En palabras de su autor, [**Pa,2023**] es una "stravaganza" y un "divertimento", concebido como una composición musical para divertirse, cuya excentricidad reside en proponer una demostración del Lema de Sauer-Shelah-Perles desde una postura puramente algebraica. En palabras de M.F. Atiyah, *la Dualidad en matemáticas no es un teorema, sino un "principio"*. Este trabajo pretende, siguiendo esta filosofía, mostrar una serie de resultados clásicos de "Extreme Combinatorics" como casos particulares de propiedades relacionadas con la dualidad en algunas $K-$álgebras artinianas. No se pretende así concluir nuevos resultados, sino adaptar (proporcionando nuevas pruebas) algunos resultados clásicos al marco de la dualidad. Este trabajo está inspirado y motivado por la prueba del Lema de Sauer-Shelah-Perles dada en [**FrPa,1983**]. De hecho, podríamos resumir este trabajo como sigue: *Así como otros resultados de Combinatoria, la prueba del Lema de Sauer-Shelah-Perles dada por Frankl-Pach puede re-escribirse como un resultado de dualidad en el contexto de las $K-$álgebras finitas.* No se pretende simplificar las pruebas existentes sino explorar cómo este tipo de enunciados puede ser reconsiderado en un contexto abstracto en términos de dualidad y traza en $K-$álgebras cero-dimensionales. Pretendemos que el presente trabajo sea lo más autocontenido posible, proporcionando descripciones detalladas de cada argumento presentado.

El Lema de Sauer-Shelah-Perles es un resultado clásico de combinatoria, que enunciaremos más adelante (cuando la terminología necesaria haya sido introducida). Inicialmente fue demostrado, simultáneamente e independientemente, por N. Sauer (en [**Sa,1972**], quien se lo atribuye a M. Perles) y por S. Shelah en [**Sh,1972**]. El resultado fue retomado por V. Vapnik y A. Chervonenkis en [**VaCh,1971**]. Aunque Vapnik y Chervonenkis rehacen la prueba, la relevancia de su contribución es que usan ese Lema de Sauer-Shelah-Perles en relación con la noción hoy conocida como dimensión de Vapnik-Chervonenkis. Esta noción es esencial para fundamentar el Aprendizaje Computacional moderno. La dimensión de Vapnik-Chervonenkis determina el tamaño suficiente de una muestra para que se puedan realizar algoritmos de aprendizaje a clases de funciones características de subconjuntos de un conjunto fijado. Se considera esa relación como el Fundamento del Aprendizaje Computacional moderno. Posteriormente, autores como Pollard, Nataranjan o Smale, entre otros muchos, tratarán de generalizar la idea de Vapnik-Chervonenkis a otras clases de funciones y muestras. Pero este trabajo de Fin de Grado no pretende entrar en esa conexión ni en esas generalizaciones. El lector puede consultar el Trabajo de Fin de Grado [**Za,2022**].

La prueba original de Sauer y Shelah era un argumento puramente inductivo (una descripción detallada puede verse en el TFG [**Za,2022**]). También era de este estilo la prueba de Vapnik y Chervonenkis. Por la relevancia de sus implicaciones, muchos autores se han volcado históricamente en revisar dicho Lema y en dar una prueba alternativa que ayude a entender mejor el

significado y el impacto de los sencillos argumentos usados originalmente. Obviamente, se persigue comprender mejor las generalizaciones potenciales que caractericen el Aprendizaje; pero este asunto, como ya hemos dicho, se escapa de los objetivos de este TFG. Entre los autores que han explorado las pruebas originales y las alternativas de este Lema técnico podemos citar a D. Haussler en [**Ha,1995**], L. Hu, R. Wu, T. Li y L. Wang en [**HWLW,2017**], P. Frankl en [**Fr,1983**], T. Gowers (course notes) o G. Kalai en su blog sobre "Extreme Combinatorics". Entre las variaciones y exploraciones más recientes podemos citar [**BCDMY,2022**] y las referencias allí expuestas. El Trabajo [**Pa,2023**] en el que se basa este TFG se une a esa tendencia con una aproximación distinta basada en elementos de traza, dualidad y una variación que denominaremos dimensión VC en términos de rango, que introduciremos más adelante.

El trabajo que centra el nuestro se enmarca en lo que T. Tao denomina en [**Ta,2014**] "'The Polynomial Method". Simplificando, el "Polynomial Method" consiste en explorar la interacción entre resultados relativos a polinomios, ecuaciones y $K-$álgebras en resultados de combinatoria. El lector interesado en otros resultados del estilo puede acudir al survey de T. Tao ya citado o a alguno de los resultados expuestos en [**PaSe, 2022**]. Tampoco es propósito de este trabajo explorar el contexto del "Polynomial method" sino, simplemente, exponer un ejemplo más.

Los conceptos de dualidad y traza a considerar en este texto pueden ser introducidos de la siguiente forma: Sea K un cuerpo perfecto (i.e. toda extensión finita es separable) de característica distinta de 2 y A una $K-$álgebra artiniana. Los elementos de A tienen definida una Traza y una Norma (véase la Definición 9), definida a través del $K-$endomorfismo que definen en A. Esto permite establecer una forma bilineal simétrica

$$\begin{array}{rccc} \mathrm{Tr}_A: & A\times A & \longrightarrow & K \\ & (x,y) & \longmapsto & Tr(xy), \end{array}$$

donde $Tr(xy)$ es la traza de $xy \in A$. Nos centraremos en el caso en el que $A = K[W]$ es el anillo de funciones polinomiales con valores en K sobre una variedad algebraica $K-$racional cero-dimensional W (i.e. $W \subseteq K^n$ es un conjunto finito de puntos). En este caso, la traza sobre $K[W]$ es una forma simétrica bilineal no degenerada determinada por los puntos de W (véase el Capítulo 2 para más detalles). La traza aquí considerada es la clásica noción algebraica y difiere de la terminología usada en [**Fr,1983**].

Como W es un conjunto algebraico cero-dimensional, tenemos que $K[W] = K^W$ (i.e. toda función de W en K es polinomial) y, adicionalmente, por el clásico Teorema Chino de los Restos (ver Teorema A.2.1), tenemos que

$$\dim_K(K[W]) = \deg(W) = \sharp(W),$$

donde $\deg(W)$ es el grado de W (véase [**He,1983**], por ejemplo). En particular, toda base $\mathscr{B}$ de $K[W]$ puede indexarse en W: Si $\mathscr{B} \subseteq K[W]$ es una base de $K[W]$ como $K-$espacio vectorial, los elementos de $\mathscr{B}$ pueden describirse de la siguiente forma:

$$\mathscr{B} := \{v_x \ : \ x \in W\}.$$

Una base dual de $\mathscr{B}$ respecto de la traza es cualquier base $\mathscr{B}^* := \{w_y \ : \ y \in W\}$ tal que

$$\mathrm{Tr}_{K[W]}(v_x, w_y) = \delta_{x,y},$$

donde $\delta_{x,y}$ es la delta de Kronecker con índices en W. Probamos en el presente texto que si W es una variedad algebraica $K-$racional cero-dimensional, toda base $\mathscr{B}$ de $K[W]$ admite una base dual respecto de su traza (una prueba elemental de este hecho se da en la Proposición 2.2.4).

Dada una base $\mathscr{B} := \{v_x \ : \ x \in W\}$ de $K[W]$ y una función polinomial $f \in K[W]$, definimos la transformada dual de f respecto de la base $\mathscr{B}$ como la función polinomial $f^*_{\mathscr{B}} \in K[W]$ dada por la siguiente identidad:

$$f^*_{\mathscr{B}}(x) := \mathrm{Tr}_{K[W]}(f, v_x) \in K, \ \forall x \in W.$$

Observamos que la transformada dual es simplemente la función (polinomial) que describe los coeficientes de f respecto de una base dual de $\mathscr{B}$. Lo anterior queda descrito por la Fórmula

(de Inversión) de la Traza (2.3.2) : Dada una base $\mathscr{B}$ y una base $\mathscr{B}^* := \{v_y^* \ : \ y \in W\}$, dual de $\mathscr{B}$ (respecto de la traza), se satisface la siguiente igualdad:

$$f = \sum_{x \in W} f^*_{\mathscr{B}}(x) v_x^*, \tag{0.1.1}$$

Concluimos que, para cada $z \in W$ se tiene la *Fórmula (de Inversión) de la Traza*:

$$f(z) = \sum_{x \in W} f^*_{\mathscr{B}}(x) v_x^*(z) = \sum_{x \in W} \mathrm{Tr}_{K[W]}(f, v_x) v_x^*(z). \tag{0.1.2}$$

Denominamos a la anterior identidad Fórmula de Inversión de la Traza porque, en algunas de nuestras aplicaciones de la misma, se comporta como la Fórmula de Inversión de Möbius. Esta fórmula se sigue inmediatamente de la existencia de base dual respecto de la traza y, posteriormente a su introducción en este trabajo, estudiamos cómo se relaciona con la Combinatoria.

Dado $[n] := \{1, \ldots, n\}$ un conjunto finito de n elementos, definimos $2^{[n]}$ como el conjunto de todos sus subconjuntos, y definimos la siguiente variedad algebraica $\mathbb{Q}-$racional cero-dimensional:

$$V_n := \{(x_1, \ldots, x_n) \in \mathbb{Q}^n \ : \ x_i^2 - x_i = 0, \ 1 \leq i \leq n\}.$$

Ahora, consideramos la $\mathbb{Q}-$álgebra $\mathbb{Q}[V_n]$ de funciones polinomiales definida en V_n con valores en $\mathbb{Q}$. Hemos elegido $\mathbb{Q}$ por simplicidad, pero, en realidad, todos nuestros resultados se cumplen para $K[V_n]$ donde K es un cuerpo perfecto de característica distinta de 2. Consideramos además el ideal

$$I(V_n) := \{f \in \mathbb{Q}[X_1, \ldots, X_n] \ : \ f(V_n) = 0\} = (X_1^2 - X_1, \ldots, X_n^2 - X_n),$$

obteniendo la identificación clásica $\mathbb{Q}[V_n] = \mathbb{Q}[X_1, \ldots, X_n]/I(V_n)$. Como V_n es finito tenemos de manera evidente que $\mathbb{Q}[V_n] = \mathbb{Q}^{V_n}$.

Se observa de manera inmediata que existe una biyección entre V_n y $2^{[n]}$ y, por ende, denotaremos de manera indistinta los puntos $Y \in V_n$ y los subconjuntos $Y \subseteq [n]$. Teniendo en cuenta nuestra hipótesis, concluimos que la traza $\mathrm{Tr}_n := \mathrm{Tr}_{\mathbb{Q}[V_n]}$ es una forma bilineal simétrica no degenerada definida sobre $\mathbb{Q}[V_n] \times \mathbb{Q}[V_n]$.

En el presente trabajo, estudiamos algunas bases de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial:

- *La base monomial*, definida como sigue: Para cada subconjunto $S \in 2^{[n]}$ consideramos el monomio
$$P_S(X_1, \ldots, X_n) := \prod_{i \in S} X_i \in \mathbb{Q}[X_1, \ldots, X_n],$$
donde $\mathbb{Q}[X_1, \ldots, X_n]$ es el anillo de polinomios en n variables con coeficientes en $\mathbb{Q}$. Este monomio define una función polinomial $p_S : V_n \longrightarrow \mathbb{Q}$, dada por $p_S := P_S + I(V_n)$. Se tiene que la siguiente es una base de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial:
$$\mathscr{B}_1 := \{p_S \ : \ S \subseteq [n]\} \subseteq \mathbb{Q}[V_n].$$
- *La base anti-monomial,* definida como sigue: Para cada subconjunto $S \in 2^{[n]}$ consideramos el polinomio multivariado
$$Q_S := \prod_{i \in [n] \setminus S} (1 - X_i) \in \mathbb{Q}[X_1, \ldots, X_n],$$
donde $[n] \setminus S$ es el complementario de S en $[n]$. Cada uno de estos polinomios define una función polinomial $q_S : V_n \longrightarrow \mathbb{Q}$ que, como antes, se define como $q_S := Q_S + I(V_n) \in \mathbb{Q}[V_n]$. La siguiente es pues otra base de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial:
$$\mathscr{B}_2 := \{q_S \ : \ S \subseteq [n]\} \subseteq \mathbb{Q}[V_n].$$

Las bases duales $\mathscr{B}_1^* := \{p_S^* \ : \ S \subseteq [n]\}$ y $\mathscr{B}_2^* := \{q_S^* \ : \ S \subseteq [n]\}$, respectivamente de $\mathscr{B}_1$ y $\mathscr{B}_2$, se estudian en las Proposiciones 3.4.1 y 3.5.1, aplicando el método de cálculo de una base dual descrito en la Sección 2.4. Una vez establecidas estas bases, estamos en posición de probar algunos resultados clásicos de Combinatoria, que serán simplemente aplicaciones concretas de la Fórmula (de Inversión) de la Traza (0.1.2) anterior.

i) En el Corolario 3.4.2 probamos que la Fórmula (de Inversión) de la Traza descrita en (0.1.2) aplicada a la base $\mathscr{B}_1$ y a su base dual $\mathscr{B}_1^*$ es, esencialmente, el Principio general de Inclusión-exclusión (de orden reverso). Es decir, la Identidad (0.1.2) se puede interpretar como el siguiente resultado: Para cada $Y \subseteq [n]$ y para cada $f \in \mathbb{Q}[V_n]$, se tiene:

$$f(Y) := \sum_{Y \subseteq S} (-1)^{\sharp(S \setminus Y)} f^*_{\mathscr{B}_1}(S) = \sum_{Y \subseteq S} (-1)^{\sharp(S \setminus Y)} \left(\sum_{S \subseteq T} f(T) \right)$$

ii) En el Corolario 3.5.2 probamos que la Fórmula (de Inversión) de la Traza (0.1.2) aplicada a la base $\mathscr{B}_2$ y a su base dual $\mathscr{B}_2^*$ es, esencialmente el Principio general de Inclusión-exclusión. Es decir, la Identidad (0.1.2) se puede intepretar como el siguiente resultado: Para cada $Y \subseteq [n]$ y para cada $f \in \mathbb{Q}[V_n]$, se tiene:

$$f(Y) := \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} \left(\sum_{T \subseteq S} f(T) \right).$$

iii) Por otro lado, en la Proposición 3.6.1 probamos que la siguiente es una base del $\mathbb{Q}-$espacio vectorial formado por los "null $t-$designs" [1] asociados a $[n]$ (como aparecen definidos en [**FrPa,1983**]):

$$P_t^* := \{p_F^* \ : \ F \subseteq [n], \sharp(F) > t\}.$$

Observamos que éste es un subconjunto de la base dual $\mathscr{B}_1^*$ de la base monomial $\mathscr{B}_1$. Además, la base anteriormente proporcionada difiere de la citada en [**FrPa,1983**], descrita en el Teorema 4 de [**DeFr,1982**].

Tras estas consideraciones, estudiamos lo que clásicamente se conoce como la dimensión VC (de Vapnik y Chervonenkis): Dada $Y \subseteq [n]$, denotamos a la clase de sus subconjuntos como $2^Y := \{S \subseteq [n] : S \subseteq Y\}$ (que es una subvariedad de $2^{[n]}$). Ahora, dada $\mathscr{F} \subseteq V_n$ y dado $Y \subseteq [n]$ podemos definir la siguiente aplicación:

$$\begin{array}{rccc} \rho_Y : & 2^{[n]} & \longrightarrow & 2^Y \\ & T & \longmapsto & T \cap Y. \end{array}$$

Decimos que $\mathscr{F}$ fragmenta (shatters) Y si $\rho_Y(\mathscr{F}) = 2^Y$. Se define, finalmente, la dimensión de Vapnik-Chervonenkis de $\mathscr{F}$ como:

$$VCD(\mathscr{F}) := \max\{\#(Y) : \rho_Y(\mathscr{F}) = 2^Y\}.$$

Con esta noción introducida, estamos en condiciones de enunciar el ya nombrado Lema de Sauer-Shelah-Perles, en la versión que probaremos en el trabajo:

LEMA 0.1.1 (**Lema de Sauer-Shelah-Perles**). *Con las notaciones precedentes, dada una subvariedad $\mathscr{F} \subseteq V_n$, se tiene la siguiente cota para el cardinal de $\mathscr{F}$:*

$$\#(\mathscr{F}) \leq \sum_{i=0}^{VCD(\mathscr{F})} \binom{n}{i},$$

donde $VCD(\mathscr{F})$ es la dimensión VC de $\mathscr{F}$.

Para encaminarnos hacia la prueba de este resultado, volvemos a la base $\mathscr{B}_2$. Las funciones polinomiales de dicha base son especialmente interesantes en nuestro contexto. Antes de nada, consideraremos una forma más simple de la cota superior proporcionada por el Lema de Sauer-Shelah-Perles. Dado $\mathscr{F} \subseteq 2^{[n]}$, consideramos los siguientes subconjuntos de funciones polinomiales:

$$Q_{\mathscr{F}} := \{q_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[V_n]. \tag{0.1.3}$$

Podemos considerar en V_n la distancia de Hamming $d_H : V_n \times V_n \longrightarrow \mathbb{R}$, y tomar en este contexto las bolas cerradas de centro $\mathbf{0} \in V_n$ definidas por dicha distancia:

$$W_d := \overline{B}_H(\mathbf{0}, d) := \{Y \in V_n \ : \ d_H(Y, \mathbf{0}) \leq d\}.$$

[1] Hemos preferido mantener el término en inglés de "null $t-$design" en lugar de su traducción literal al español porque nos parece menos descriptiva y menos elegante. Pedimos disculpas por ello al lector.

Se tiene la siguiente cadena ascendente de bolas cerradas (que son subvariedades algebraicas finitas) de V_n:

$$W_0 \subsetneq W_1 \subsetneq W_2 \subsetneq \cdots \subsetneq W_n = V_n.$$

$Q_{\mathscr{F}}$ es una familia de funciones linealmente independientes, de cardinal igual al cardinal de $\mathscr{F}$. Dado $i \in \{0, \ldots, n\}$, podemos definir el conjunto de las restricciones a W_i de las funciones polinomiales en $Q_{\mathscr{F}}$:

$$Q_{\mathscr{F},i} := \{q_F\big|_{W_i} \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[W_i].$$

Notamos que $Q_{\mathscr{F},n} = Q_{\mathscr{F}}$. Para cada $i \in [n]$, consideramos también el $\mathbb{Q}-$espacio vectorial $\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle$ generado por $Q_{\mathscr{F},i}$ en $\mathbb{Q}[W_i]$.
Como $W_i \subseteq W_{i+1}$ tenemos un epimorfismo de $\mathbb{Q}-$algebras, $i_r^* : \mathbb{Q}[W_{i+1}] \longrightarrow \mathbb{Q}[W_i]$, definido simplemente como la restricción a W_i de las funciones polinomiales en $\mathbb{Q}[W_{i+1}]$. Por ende, la siguiente es una sucesión creciente de dimensiones:

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle\right) \leq \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},i+1}\rangle\right).$$

Por lo tanto, tiene sentido introducir la siguiente noción:

Definición 1 (**Dimensión del Rango de VC**). *Con las notaciones precedentes, definimos la Dimensión del Rango de VC de $\mathscr{F}$ como el mínimo r tal que $Q_{\mathscr{F},r}$ es una familia $\mathbb{Q}-$linealmente independiente de funciones polinomiales en $\mathbb{Q}[W_r]$. Es decir, el mínimo r tal que*

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},n}\rangle\right) = \sharp(\mathscr{F}).$$

Lo denotamos por $RVCD(\mathscr{F})$.

El término "rango" se utiliza porque $RVCD$ está relacionado con el rango de algunas matrices dependientes de las funciones polinomiales de $Q_{\mathscr{F}}$. En el Lema 5.2.1 mostramos que se da la siguiente igualdad:

$$RVCD(\mathscr{F}) := \min\{r \in \{0, \ldots, n\} \ : \ \operatorname{rank}(M_{\mathscr{F},r}) = \sharp(\mathscr{F})\},$$

donde $M_{\mathscr{F},r} \in \mathscr{M}_{N\times\delta(r)}(\mathbb{Q})$, $N = \sharp(\mathscr{F})$ y $\delta(r) = \sharp(W_r)$, es una matriz construida a partir de los elementos de la familia $Q_{\mathscr{F}}$ evaluados en los puntos $S \in W_r$ (véase el Capítulo 5 para una descripción más precisa de esto último).
Como $\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle$ es un subespacio vectorial de $\mathbb{Q}[W_i]$, el siguiente Corolario se sigue directamente de las definiciones previas:

Corolario 0.1.2. *Si $r = RVCD(\mathscr{F})$, se tiene que $\sharp(\mathscr{F}) = \sharp(Q_{\mathscr{F},n}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right)$. Por tanto, se tiene que*

$$\sharp(\mathscr{F}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) \leq \dim_{\mathbb{Q}}\left(\mathbb{Q}[W_r]\right) = \sharp\left(W_r\right) = \sum_{i=0}^{RVCD(\mathscr{F})} \binom{n}{i}.$$

Consideramos el siguiente ideal principal como herramienta de trabajo en lo que prosigue:

$$\mathfrak{q}_Y := (q_Y) := \{fq_Y \ : \ f \in \mathbb{Q}[V_n]\} \subseteq \mathbb{Q}[V_n],$$

es decir, el ideal principal generado por $q_Y \in \mathscr{B}_2$ en $\mathbb{Q}[V_n]$, donde $Y \subseteq [n]$. Este ideal $\mathfrak{q}_Y$ es isomorfo (como $\mathbb{Q}-$espacio vectorial) a la $\mathbb{Q}-$álgebra $\mathbb{Q}[2^Y]$ formada por todas las funciones polinomiales definidas en el conjunto $2^Y \subseteq V_n$ formado por todos los subconjuntos de Y (véase el Lema 4.2.1). Por ende, todo lo que queda por probar para llegar al Lema de Sauer-Shelah-Perles es la desigualdad $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$. Esta última desigualdad se concluye en el Corolario 5.2.3 usando un argumento que involucra algunos aspectos desarrollados en resultados precedentes.

Por último, en la Sección 5.3 damos "otra" prueba del Lema de Sauer-Shelah-Perles. La diferencia con la prueba propuesta en la Sección 5.2 anterior es que, en ella, solo se usarán técnicas de dualidad aplicadas al ideal $\mathfrak{q}_Y$. La prueba es algo más compleja que la dada en la Sección anterior, pero tiene importancia porque exhibe cómo la línea general de este trabajo entiende a un plano de abstracción superior lo que, inconscientemente, subyace a las ideas expuestas en [**FrPa,1983**].

Recordamos las bases $\mathscr{B}_1$ y $\mathscr{B}_2$ y sus bases duales $\mathscr{B}_1^*$ y $\mathscr{B}_2^*$. Introducimos ahora dos "transformadas duales" (que son, de hecho, automorfismos de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial de dimensión finita):

- La transformada dual basada en la base monomial $\mathscr{B}_1$:

$$\begin{array}{rccc} \mathscr{D}_1: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & (f)^*_{\mathscr{B}_1}, \end{array} \tag{0.1.4}$$

  donde, para cada $S \subseteq [n]$ se tiene:

$$\mathscr{D}_1(f)(S) := \mathrm{Tr}_n(f, p_S),$$

  y p_S es el elemento de $\mathscr{B}_1$ determinado por $S \subseteq [n]$.
- Otra transformada dual basada en $\mathscr{B}_2^*$, que llamamos *transformada dual de Frankl-Pach:*

$$\begin{array}{rccc} \mathscr{D}_2: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longrightarrow & (f)^*_{\mathscr{B}_2^*}, \end{array} \tag{0.1.5}$$

  donde, para cada $S \subseteq [n]$ se tiene:

$$\mathscr{D}_2(f)(S) := \mathrm{Tr}_n(f, q_S^*),$$

  y q_S^* es el elemento de la base dual $\mathscr{B}_2^*$ determinado por $S \subseteq [n]$.

Denominamos a $\mathscr{D}_2$ la *transformada dual de Frankl-Pach* por estar ésta implícita en la prueba principal de [**FrPa,1983**]. De hecho, la idea esencial en la prueba del Lema de Sauer-Shelah-Perles dada en [**FrPa,1983**] se puede reescribir en nuestro lenguaje de la siguiente manera:

PROPOSICIÓN 0.1.3. *Con las notaciones precedentes, $\mathscr{D}_2$ es la inversa de $\mathscr{D}_1$: Es decir, para cada $f \in \mathbb{Q}[V_n]$ se tiene que*

$$f = \mathscr{D}_1\left(\mathscr{D}_2\left(f\right)\right) = \mathscr{D}_2\left(\mathscr{D}_1\left(f\right)\right).$$

Además, para cada $Y \subseteq [n]$, las restricciones al ideal $\mathfrak{q}_Y$ de $\mathscr{D}_1$ y $\mathscr{D}_2$ son también automorfismos de $\mathbb{Q}-$espacios vectoriales sobre $\mathfrak{q}_Y$, uno inverso del otro.

Este último enunciado se prueba en la Proposición 5.3.2 de la Sección 5.3. A partir de esta última proposición, en el Corolario 5.3.3, concluimos que $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ usando únicamente técnicas de dualidad y la Proposición 0.1.3. Y, por tanto, el Lema de Sauer-Shelah-Perles queda, de nuevo, probado.

El presente trabajo se estructura de la siguiente forma: El Capítulo 1 se dedica a introducir los anillos y módulos de Artin, así como algunos resultados fundamentales relevantes. El Capítulo 2 se dedica a las nociones básicas y a algunos resultados clásicos sobre dualidad y traza en $K-$álgebras finitas. El Capítulo 3 se dedica a establecer los resultados y conceptos principales relacionados con la variedad algebraica V_n. En las Secciones 3.4 y 3.5 probamos dos formas del Principio de Inclusión-exclusión, que son consecuencia directa de la Fórmula (de Inversión) de la Traza. En el Capítulo 4 estudiamos el ideal principal $\mathfrak{q}_Y$, los ideales $\mathfrak{q}_{\mathscr{F}}$, y algunas propiedades de éstos. Por último, en el Capítulo 5 comenzamos introduciendo la noción de Dimensión del Rango de VC, para luego probar el Lema de Sauer-Shelah-Perles (véase el Corolario 5.2.3). Finalmente, en la Sección 5.3 se introducen las pruebas de la Proposición 0.1.3 y del Corolario 5.3.3, haciendo patente la inspiración de este trabajo en [**FrPa,1983**].

Insistimos en el objetivo principal de este trabajo: Conectar dos áreas del conocimiento matemático habitualmente inconexas (y que, cuando han sido conectadas, no ha sido de la manera aquí presentada).

0.1.1. Apéndices Finales. El trabajo presentado se finaliza con el Apéndice A. Dicho Apéndice está dedicado a completar ciertos contenidos básicos de Álgebra Conmutativa que pueden ayudar a la lectura del trabajo: se proporciona una introducción al concepto de $R-$álgebra, así como al concepto de radical de Jacobson (y algunas propiedades), y al de producto tensorial de $R-$módulos, así como el enunciado del fundamental Teorema Chino de los Restos.

0.1.2. Sobre el estilo y la ortografía usados en este TFG. En algún caso precedente se ha discutido el estilo y la ortografía de las memorias presentadas como Trabajo de Fin de Grado en Matemáticas. En evitación de intervenciones innecesarias, queremos clarificar algunos aspectos relativos al estilo elegido en este texto. Se ha elegido el formato de libro (book) de la American Mathematical Society (AMS). Aunque el idioma utilizado es el español, hemos tratado de seguir lo más fielmente posible las recomendaciones del Libro de Estilo de esta asociación [2] , juntamente con las reglas de estilo recomendadas por D. E. Knuth y co-autores para la Mathematical Association of America (MAA) [3].
Específicamente, hemos tratado de seguir atentamente las siguientes dos reglas:

- *"Numbered theorems, lemmas, etc. are proper nouns and, thus, are capitalized: Theorem 2.3, Lemma 3.1, Figure 4.5"* (p. 79 del AMS Style Guide).
- *"Rule 19. Capitalize names like Theorem 1, Lemma 2, Algorithm 3, Method 4"* (en D. E. Knuth et al.).

[2] M. Letourneau, J. Wright Sharp, AMS Style Guide, Journals, October 2017, AMS, Providence, 2017
[3] D. E. Knuth, T. Larrabee, P. M. Roberts, Mathematical Writing, MAA, 1989

CAPíTULO 1

Unas palabras sobre anillos y módulos de Artin

Índice

1.1. Introducción

El matemático austríaco Emil Artin se incorpora a la Universidad de Götingen en 1921. Allí coincidirá con D. Hilbert y colaborará con E. Noether y H. Hasse, hasta su marcha, en 1923, a la Universidad de Hamburgo y su exilio en Princeton, por causa del nazismo, en 1937. Mientras se encuentra en Göttingen, colabora en el seminario de E. Noether. Noether introdujo en dicho seminario la condición de cadena numerable descendente para ideales en anillos, como noción dual de sus propias ideas sobre la condición de cadena ascendente numerable (el testimonio proviene del texto histórico [**VdW, 1985**], cuyo autor fue testigo privilegiado de aquél tiempo).

En 1927, ya en Hamburgo, Artin generaliza el Teorema de Wedderburn de 1908 sobre números hipercomplejos (es decir, una teoría de álgebras sobre cuerpos arbitrarios). La generalización de Artin en [**Ar,1927**] reposa sobre esa condición de cadena descendente numerable de Noether (de nuevo, según testimonio de [**VdW, 1985**]). Nuestro objetivo es hablar de $K-$álgebras de Artin y, por extensión, de *anillos y módulos de Artin*, que será el objeto de este capítulo.

La estructura de este capítulo es así la siguiente: se dan en la Sección 1.2 las definiciones de anillo y módulo artiniano o de Artin, así como algunos resultados fundamentales. En la Sección 1.3, daremos una demostración del Teorema de Jordan-Hölder, introduciendo la terminología adecuada previamente. Tras ello, en la Sección 1.4 probaremos el Teorema de Akizuki junto con algunos resultados sobre la estructura de los anillos de Artin relevantes para nuestro desarrollo. Por último, en la Sección 1.5, daremos una demostración de las Proposiciones 1.5.1 y 1.5.2, que se usarán en el capítulo siguiente.

1.2. Algunas propiedades de los anillos y módulos artinianos

Comenzamos recordando que siempre se asumirá el Axioma de Elección Dependiente en la posterior discusión:

Definición 2 (**Axioma de Elección Dependiente**). *Sea X un conjunto no vacío y $R \subseteq X \times X$ una relación. Supongamos que R satisface la siguiente propiedad:*

$$\forall a \in X, \exists b \in X : aRb.$$

Entonces, existe una sucesión $\{x_n : n \in \mathbb{N}\} \subseteq X$ de tal modo que $x_n R x_{n+1}, \forall n \in \mathbb{N}$.

Ahora, suponiendo el anterior axioma damos la siguiente equivalencia, que nos lleva a la Definición de Anillo de Artin.

Proposición 1.2.1 (**Anillos de Artin**). *Bajo el Axioma de Elección Dependiente, sea R un anillo. Las dos propiedades siguientes son equivalentes:*

i) Toda cadena descendente numerable de ideales se estabiliza. Es decir, dada una cadena descendente numerable de ideales de R:

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \ldots,$$

existe $m \in \mathbb{N}$ tal que $\mathfrak{a}_n = \mathfrak{a}_m$, $\forall n \geq m$.

ii) Todo conjunto no vacío de ideales de R posee elemento minimal.

Los anillos que satisfacen cualquiera de estas dos propiedades equivalentes se llaman anillos de Artin o artinianos.

DEMOSTRACIÓN. Basta con tomar como relación entre ideales de R la relación "que invierte el contenido", i.e. dos ideales $\mathfrak{a}, \mathfrak{b} \subseteq R$ están relacionados si y solo si $\mathfrak{a} \supsetneq \mathfrak{b}$. Ahora, probemos la equivalencia:

- *ii)* $\Rightarrow$ *i)*: Sea $\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \ldots$ una cadena descendente numerable de ideales de R. Consideramos $\mathcal{A} := \{\mathfrak{a}_j\}_{j\in\mathbb{N}}$ el conjunto formado por todos los ideales de la cadena precedente. Por *ii)*, existe un elemento minimal $\mathfrak{a}_k$ de $\mathcal{A}$, y se sigue inmediatamente que, entonces, $\mathfrak{a}_j = \mathfrak{a}_k$ para cada $j \geq k$.
- *i)* $\Rightarrow$ *ii)*: Supongamos que toda cadena descendente numerable de ideales de R se estabiliza. Sea Σ una familia no vacía de ideales, y supongamos que no tiene elemento minimal. Entonces, podríamos construir iterativamente una cadena descendente numerable de ideales que no se estabiliza, y por ende, se llegaría a contradicción con *i)*.

□

Del mismo modo, podemos hablar de $R-$módulos de Artin:

PROPOSICIÓN 1.2.2 (**Módulo de Artin**). *Bajo el Axioma de Elección Dependiente, sea R un anillo y M un $R-$módulo. Las dos propiedades siguientes son equivalentes:*

i) Toda cadena descendente numerable de submódulos de M se estabiliza. Es decir, dada una cadena descendente numerable de submódulos de M:

$$M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \ldots,$$

existe $m \in \mathbb{N}$ tal que $M_n = M_m$, $\forall n \geq m$.

ii) Todo conjunto no vacío de submódulos de M posee elemento minimal.

Los $R-$módulos que satisfacen cualquiera de estas dos propiedades equivalentes se llaman $R-$módulos de Artin o artinianos.

DEMOSTRACIÓN. Es análoga a la precedente, pero trabajando con submódulos en lugar de con ideales. □

OBSERVACIÓN 1.2.3. Como los submódulos de un anillo R son sus ideales, un anillo R es un anillo de Artin si y solamente si es de Artin como $R-$módulo.

Damos ahora algunas propiedades elementales de los módulos y anillos de Artin:

PROPOSICIÓN 1.2.4. *Con la terminología precedente, los submódulos y los cocientes de $R-$módulos artinianos son artinianos (y, por ende, también los cocientes de anillos de Artin son anillos de Artin).*

DEMOSTRACIÓN. Es obvio que una cadena descendente numerable de submódulos de un submódulo N de un $R-$submódulo M forma una cadena descendente numerable de submódulos de M, con lo que si M es artiniano, todo submódulo suyo es también artiniano. Para los cocientes, baste con recordar la biyección entre los submódulos de un cociente M/N y los submódulos de M que contienen a N. Así, las cadenas de submódulos numerables descendentes del cociente M/N se trasladan a cadenas de M y, usando la condición de cadena descendente numerable de M, concluimos que la cadena en M/N se estabiliza. □

PROPOSICIÓN 1.2.5. *Dada una sucesión exacta corta de $R-$módulos:*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0,$$

entonces, M es artiniano (resp. noetheriano) si y solamente si M' y M'' son artinianos (resp. noetherianos).

DEMOSTRACIÓN. Lo probamos para el caso artiniano, siendo la prueba análoga para anillos noetherianos. En primer lugar, si M es artiniano también lo son M' y M'', ya que M' es isomorfo a un submódulo de M y M'', a un cociente de M. Recíprocamente, si M' y M'' son artinianos, tendremos que probar que también lo es M. Consideramos una cadena descendente numerable de submódulos de M,

$$M_0 \supseteq M_1 \supseteq \cdots \supseteq M_m \supseteq \cdots .$$

Ahora, tomamos las siguientes transformaciones sobre la cadena precedente, que definen las aplicaciones g y f:

$$g(M_0) \supseteq g(M_1) \supseteq \cdots \supseteq g(M_m) \supseteq \cdots ,$$
$$f^{-1}(M_0) \supseteq f^{-1}(M_1) \supseteq \cdots \supseteq f^{-1}(M_m) \supseteq \cdots .$$

Como M' y M'' son artinianos, estas dos cadenas se estabilizan. Tomando el máximo de los índices donde estas cadenas se estabilizan podemos concluir que existe $n \in \mathbb{N}$ tal que, para todo $m \geq n$, se tiene

$$g(M_m) = g(M_n) \quad \text{y} \quad f^{-1}(M_m) = f^{-1}(M_n).$$

Para concluir la prueba, basta probar que si se tienen las igualdades anteriores, $M_m = M_n$ para cada $m \geq n$. Como $M_m \subseteq M_n$, basta ver la otra inclusión. Si $x \in M_n$ entonces $g(x) \in g(M_n) = g(M_m)$, luego existe $y \in M_m$ tal que $g(x) = g(y)$. Por tanto, $g(x-y) = 0$, y se tiene que $x - y \in \ker(g) = \mathrm{Im}(f)$. Por tanto, existe $z \in M'$ tal que $f(z) = x - y$. Por otro lado, como $M_m \subseteq M_n$, $x - y \in M_n$. Por tanto, $z \in f^{-1}(M_n)$. Como $f^{-1}(M_n) = f^{-1}(M_m)$, entonces $z \in f^{-1}(M_m)$. Entonces, $f(z) = x - y \in M_m$. Es decir, existe $u \in M_m$ tal que $x - y = u$. Como $u \in M_m$ e $y \in M_m$, entonces $x = y + u \in M_m$, y la prueba está terminada. □

PROPOSICIÓN 1.2.6. *Dado R un anillo artiniano, todo $R-$módulo finitamente generado es un $R-$módulo artiniano.*

DEMOSTRACIÓN. Vamos a proceder por inducción en el número de generadores: Sabemos que si R es artiniano, también lo son sus cocientes $R/\mathfrak{a}$, para cualquier ideal $\mathfrak{a} \subseteq R$. Dado M un $R-$módulo generado por un solo elemento, se tiene que M es isomorfo (como $R-$módulo) a $R/\mathfrak{a}$, donde $\mathfrak{a}$ es un ideal de R, y como $R/\mathfrak{a}$ es $R-$módulo artiniano, entonces también lo será M. Esto prueba el caso de $R-$módulos principales (base inductiva). Ahora si M es un $R-$módulo generado por un conjunto de elementos finito $\{a_1, \ldots, a_n\}$, consideramos el submódulo N de M generado por $\{a_1, \ldots, a_{n-1}\}$ y la sucesión exacta corta:

$$0 \longrightarrow N \xrightarrow{\ i\ } M \xrightarrow{\ \pi\ } M/N \longrightarrow 0,$$

donde i es la inclusión y π es la proyección canónica. Observemos que M/N es el $R-$módulo generado por la clase $\{a_n + N\}$. Ahora, por hipótesis inductiva, N es artiniano y M/N es artiniano (ver la base inductiva). Aplicando la proposición precedente, concluiremos que M es artiniano. □

1.3. El Teorema de Jordan-Hölder: longitud y condiciones de cadena

En esta sección, introduciremos el concepto de longitud de una serie de composición de un $R-$módulo. Asimismo probaremos el Teorema de Jordan-Hölder. El resultado es parcialmente debido a Jordan en sus trabajos [**Jo,1869**] y [**Jo,1870**] y a O. Hölder (cf. [**Ho,1889**]). Será O. Schreier quien, entre otras muchas contribuciones, le dé su forma actual en [**Sc,1928**].

DEFINICIÓN 3 (**Series de Composición (o de Jordan-Hölder)**). *Se introducen las siguientes nociones:*

i) Un $R-$módulo M se dice simple si no posee más submódulos que $0 := R\langle 0\rangle$ y M.

ii) Una cadena finita estricta de submódulos de M es una familia finita de submódulos que satisface:

$$(0) \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n.$$

Abreviaremos la expresión "cadena finita estricta" mediante SFC.

iii) Dados dos cadenas finitas estrictas de submódulos de M:

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_r = M, \tag{1.3.1}$$

$$0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_{s-1} \subsetneq N_s = M, \tag{1.3.2}$$

decimos que la cadena finita estricta descrita en (1.3.1) es refinable a la cadena finita estricta descrita en (1.3.2) si $s \geq r$ y existe una aplicación inyectiva

$$\sigma : [r] = \{1, \ldots, r\} \longrightarrow [s] = \{1, \ldots s\},$$

tal que

$$M_i = N_{\sigma(i)}, \ \forall i \in [r].$$

Es decir, si los submódulos que aparecen en la cadena descrita en (1.3.1) son algunos de los submódulos que aparecen en la cadena descrita en (1.3.2).

iv) Una serie de composición (o de Jordan-Hölder) en un $R-$módulo M es una cadena estricta finita de submódulos:

$$(0) \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M,$$

tal que los cocientes M_{i+1}/M_i son $R-$módulos simples para cada $i \in \{0, \ldots, n-1\}$ (con $M_0 := (0)$). Diremos que esta serie de composición es de longitud n.

PROPOSICIÓN 1.3.1. *Si un $R-$módulo M es artiniano y noetheriano, entonces posee una serie de composición.*

DEMOSTRACIÓN. La idea de la prueba es usar el Axioma de Elección Dependiente, junto con las propiedades que definen a los módulos artinianos y noetherianos. Para cada submódulo N de M consideremos el conjunto

$$\mathscr{S}(N) := \{M' \subseteq N : M' \text{ es submódulo de } N \text{ y } M' \neq N,\ M' \neq (0)\}.$$

Comenzando con M, si $\mathscr{S}(M) = \emptyset$, entonces, tenemos una serie de composición $(0) \subsetneq M$. Si $\mathscr{S}(M) \neq \emptyset$, posee elemento maximal $M_1 \in \mathscr{S}(M)$ (por ser M noetheriano). Entonces, M/M_1 ha de ser un módulo simple (ya que, en otro caso, M_1 no sería maximal en $\mathscr{S}(M)$). Consideraríamos así la cadena

$$(0) \subsetneq M_1 \subsetneq M.$$

Procediendo inductivamente, dada una cadena descendente numerable de longitud n,

$$(0) \subsetneq M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M,$$

con M_i/M_{i+1} simple, para $1 \leq i \leq n-1$, si $\mathscr{S}(M_n) \neq \emptyset$, existirá M_{n+1} elemento maximal de $\mathscr{S}(M_n)$ y una cadena de contenidos estrictos de longitud $n+1$:

$$(0) \subsetneq M_{n+1} \subsetneq M_n \subsetneq M_{n-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M.$$

Si para cada $m \in \mathbb{N}$, $\mathscr{S}(M_m)$ fuera no vacío, tendríamos una cadena descendente de submódulos de M que no se estabilizaría, contradiciendo que M es artiniano. Por ende, ha de existir $m \in \mathbb{N}$ tal que $\mathscr{S}(M_m) = \emptyset$. Esto significará que M_m es un $R-$módulo simple y tendremos una serie de composición:

$$(0) \subsetneq M_m \subsetneq M_{m-1} \subsetneq \cdots \subsetneq M_1 \subsetneq M.$$

□

DEFINICIÓN 4 (**Longitud**). *Sea M un $R-$módulo. Llamaremos longitud de M como $R-$módulo al mínimo de las longitudes de sus series de composición, si posee alguna. En otro caso, diremos que M es de longitud infinita. Denotaremos por $\ell_R(M)$ la longitud de M como $R-$módulo.*

TEOREMA 1.3.2 (**Teorema de Jordan-Hölder (para módulos)**). *Si M es un $R-$módulo de longitud finita (i.e. que posee al menos una serie de composición), entonces:*

i) Todas las series de composición de M tienen la misma longitud (y, por tanto, son de longitud igual a $\ell_R(M)$).
ii) Toda cadena finita estricta tiene longitud menor que $\ell_R(M)$.
iii) Toda cadena finita estricta de submódulos de M puede refinarse hasta obtener una serie de composición de M.

En particular, un $R-$módulo es de longitud finita si y solamente si es artiniano y noetheriano a la vez.

DEMOSTRACIÓN. En primer lugar, observemos que si M es un $R-$módulo de longitud finita, todos sus submódulos son también de longitud finita y si $N \subsetneq M$ es un submódulo propio de M, entonces $\ell_R(N) < \ell_R(M)$: Es claro que si tenemos una serie composición de M de longitud mínima:

$$(0) \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M,$$

entonces tenemos una cadena de submódulos de N:

$$(0) \subseteq M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \subseteq M_{n-1} \cap N \subseteq M_n \cap N = N.$$

Ahora, en esta cadena, dado $i \in \{1, \ldots, n\}$, tenemos dos posibilidades: o bien $M_i \cap N = M_{i+1} \cap N$, o bien $(M_{i+1} \cap N)/(M_i \cap N) = M_{i+1}/M_i$ porque M_{i+1}/M_i es simple. Eliminando los casos en los que $M_i \cap N = M_{i+1} \cap N$, nos quedará una serie de composición de N de longitud menor o igual que n. Es decir, una serie de composición

$$(0) \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_{r-1} \subsetneq N_r = N.$$

Si, eventualmente, $r = n$, tendríamos $N_i = M_i \cap N$ para cada $i \in \{1, \ldots, n\}$, y una cadena de contenidos estrictos

$$(0) \subsetneq M_1 \cap N \subsetneq M_2 \cap N \subsetneq \cdots \subsetneq M_{n-1} \cap N \subsetneq M_n \cap N = N.$$

Ahora, como M_{i+1}/M_i es simple y $(M_{i+1} \cap N)/(M_i \cap N)$ es un submódulo propio, entonces tendremos

$$M_{i+1}/M_i = (M_{i+1} \cap N)/(M_i \cap N).$$

Tomando $i = 0$, concluiremos que

$$M_1 = M_1/(0) = (M_1 \cap N)/((0) \cap N) = (M_1 \cap N).$$

Procediendo inductivamente, probaríamos que $M_i \cap N = M_i$ y, llegando al caso $i = n$, concluiríamos que $M_n \cap N = M_n = M$, lo que contradice la hipótesis $N \subsetneq M$.
Sea ahora $\ell := \ell_R(M)$ la longitud de una serie de composición de longitud mínima de M, y sea dada

$$(0) \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M,$$

cualquier otra serie de composición de M. Entonces, tendremos que $n \geq \ell$ porque ℓ es mínimo y, de otro lado, por la primera parte de la prueba,

$$0 = \ell_R(0) < \ell_R(M_1) < \cdots < \ell_R(M_{n-1}) < \ell_R(M_n) = \ell_R(M) = \ell.$$

Por tanto, necesariamente, $n \leq \ell$ y tendremos que cualesquiera dos series de composición de M tienen la misma longitud, lo que prueba la afirmación i).

De otro lado, dada una cadena finita cualquiera de submódulos de M,

$$N_r \subsetneq N_{r-1} \subsetneq \cdots \subsetneq N_1 \subsetneq N_0 = M,$$

ha de satisfacer $r \leq \ell_R(M)$, por el mismo argumento antes indicado, lo que prueba la afirmación ii).

Para la afirmación iii), comencemos considerando el siguiente conjunto:
(1.3.3)

$$\mathscr{C} := \{r \in \mathbb{N} \ : \text{ existe una SFC de longitud } r, \text{ no refinable a una serie de composición}\}.$$

Por la afirmación ii) precedente, sabemos que toda cadena finita estricta tiene longitud acotada por $\ell_R(M)$. De otro lado, toda cadena finita estricta posee, por definición, al menos dos términos (0 y M). Por tanto, $\mathscr{C} \subseteq [\ell_R(M)] = \{1, 2, \ldots, \ell_R(M)\}$. Ahora bien, $\ell_R(M) \notin \mathscr{C}$. Para probarlo, consideremos una cadena finita estricta

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = 0, \tag{1.3.4}$$

con $r = \ell_R(M)$. Entonces ha de ser una serie de composición de M, porque si no lo fuera, ha de existir i tal que el $R-$módulo cociente M_i/M_{i+1} no es un $R-$módulo simple. Entonces, existirá $M_i' \subsetneq M_i$ un submódulo propio de M_i tal que tenemos

$$(0) = M_{i+1}/M_{i+1} \subsetneq M_i'/M_{i+1} \subsetneq M_i/M_{i+1}.$$

Tendríamos así una cadena finita estricta de submódulos de M de longitud $r + 1 > \ell_R(M)$:

$$M = M_0 \supsetneq M_1 \supsetneq \cdots M_i \supsetneq M_i' \supsetneq M_{i+1} \supsetneq \cdots \supsetneq M_r,$$

lo que contradice *ii)*. Por tanto, $\mathscr{C} \subseteq [\ell_R(M) - 1]$.
Supongamos que $\mathscr{C} \neq \emptyset$ es un conjunto no vacío y sea $r := \max(\mathscr{C}) < \ell_R(M)$ su máximo. Consideremos una cadena finita estricta de longitud r que no es refinable a una serie de composición:

$$M = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0, \tag{1.3.5}$$

Por *i)*, esta cadena no puede ser serie de composición por no tener longitud $\ell_R(M)$. Por tanto, y con el mismo argumento antes expuesto, existirá $i \in [r]$ tal que el $R-$módulo cociente N_i/N_{i+1} no es un $R-$módulo simple. De nuevo, por los mismos argumentos anteriores, tendremos una cadena de longitud $r+1$ que refine a la cadena descrita en (1.3.5):

$$M = N_0 \supsetneq N_1 \supsetneq \cdots N_i \supsetneq N_i' \supsetneq N_{i+1} \supsetneq \cdots \supsetneq N_r. \tag{1.3.6}$$

Pero $r+1 \notin \mathscr{C}$, porque $r = \max(\mathscr{C})$, luego esta nueva cadena finita estricta puede ser refinada a una serie de composición de M. Pero si la cadena descrita en (1.3.6) se puede refinar a una serie de composición de M, entonces su subcadena descrita en (1.3.5) también se puede refinar a una serie de composición de M, con lo que $r = \max(\mathscr{C}) \notin \mathscr{C}$. Por tanto, necesariamente, $\mathscr{C} = \emptyset$ y toda cadena finita estricta de submódulos de M puede ser refinada hasta obtener una serie de composición de M.

Para concluir con la última afirmación del Teorema, procedemos como sigue: Ya hemos visto, en la Proposición 1.3.1, que si un $R-$módulo es artiniano y noetheriano a la vez, entonces posee una serie de composición, y por ende, su longitud es finita. De otro lado, si su longitud es finita, toda cadena ascendente o descendente no puede extenderse indefinidamente porque, entonces, tendríamos cadenas finitas estrictas de cualquier longitud, contradiciendo *ii)*. Por tanto, ha de verificar las condiciones de cadena ascendente numerable ascendente y descendente para submódulos, y por tanto, ser simultáneamente artiniano y noetheriano. □

COROLARIO 1.3.3. *Sea K un cuerpo y V un $K-$módulo (o, equivalentemente, $K-$espacio vectorial). Las siguientes afirmaciones son equivalentes:*

i) V es un $K-$espacio vectorial de dimensión finita.
ii) V es un $K-$módulo de longitud finita.
iii) V es un $K-$módulo noetheriano.
iv) V es un $K-$módulo de Artin.

Además, en ese caso, se tiene que:

$$\ell_K(V) = \dim_K(V).$$

DEMOSTRACIÓN. Estudiamos cada implicación de manera independiente:

- *i)* $\Rightarrow$ *ii)*: Si V es de dimensión finita, con $\dim_K(V) = n \in \mathbb{N}$, tomemos una base $\{v_1, \ldots, v_n\} \subseteq V$. Entonces, se tiene la siguiente serie de composición:

  $$\langle 0 \rangle \subsetneq K\langle v_1 \rangle \subsetneq K\langle v_1, v_2 \rangle \subsetneq \cdots \subsetneq K\langle v_1, v_2, \ldots, v_n \rangle = V.$$

  Y, por tanto, la longitud de V como $K-$espacio vectorial es finita, e igual a n por el Teorema de Jordan-Hölder.
- Las implicaciones *ii)* $\Rightarrow$ *iii)* y *ii)* $\Rightarrow$ *iv)* son inmediatas por el Teorema de Jordan-Hölder.
- *iii)* $\Rightarrow$ *i)*: Si *i)* es falso, existe una sucesión infinita $(x_n)_{n\in\mathbb{N}}$ de elementos linealmente independientes de V. Sea U_n el $K-$espacio vectorial generado por $x_1, \ldots, x_n$. Entonces, la cadena ascendente numerable $U_1 \subsetneq U_2 \subsetneq \cdots \subsetneq U_n \subsetneq \ldots$ no se estabiliza, y se tiene que *iii)* es falso, concluyendo por contrarrecíproco.
- *iv)* $\Rightarrow$ *i)*: La prueba de esta implicación es análoga a la anterior, sustituyendo el subespacio U_n por V_n, donde V_n es el subespacio generado por la sucesión infinita de elementos $\{x_k\}_{k=n+1}^{\infty}$.

□

1.4. Algunos resultados sobre la estructura de los anillos de Artin: El Teorema de Akizuki

PROPOSICIÓN 1.4.1. *En un anillo de Artin R,*

$$Spec(R) = MaxSpec(R),$$

es decir, todo ideal primo es maximal.

DEMOSTRACIÓN. Basta probar la inclusión $Spec(R) \subseteq MaxSpec(R)$. Sea $\mathfrak{p}$ un ideal primo. Entonces, el anillo cociente $R/\mathfrak{p}$ es un dominio de integridad. Sea $x \in R$ tal que $x + \mathfrak{p} \neq 0 + \mathfrak{p}$ en $R/\mathfrak{p}$. Veamos que $x + \mathfrak{p} \in (R/\mathfrak{p})^*$: Consideremos la siguiente cadena descendente de ideales de $R/\mathfrak{p}$,

$$(x + \mathfrak{p}) \supseteq (x^2 + \mathfrak{p}) \supseteq \cdots \supseteq (x^n + \mathfrak{p}) \supseteq \ldots.$$

Como $R/\mathfrak{p}$ es artiniano, la cadena anterior se estabiliza, i.e., existe $m \in \mathbb{N}$ tal que

$$(x^m + \mathfrak{p}) = (x^{m+1} + \mathfrak{p}).$$

Por tanto, podemos deducir que existe $y + \mathfrak{p} \in R/\mathfrak{p}$ tal que

$$yx^{m+1} + \mathfrak{p} = x^m + \mathfrak{p}.$$

Como $x + \mathfrak{p} \neq 0 + \mathfrak{p}$, deducimos de lo anterior, teniendo en cuenta que $R/\mathfrak{p}$ es dominio de integridad, que

$$yx + \mathfrak{p} = 1 + \mathfrak{p}.$$

Por ende, deducimos que $x + \mathfrak{p}$ es unidad en $R/\mathfrak{p}$, como se quería. De esto último deducimos directamente que $R/\mathfrak{p}$ es cuerpo, es decir, $\mathfrak{p}$ es un ideal maximal. □

Inmediatamente del anterior resultado, deducimos, por ejemplo, que el radical de Jacobson y el nilradical de un anillo de Artin coinciden.

PROPOSICIÓN 1.4.2. *Si R es un anillo de Artin,*

i) El espectro maximal $MaxSpec(R)$ es finito.
ii) El nilradical de R (i.e., $\sqrt{(0)}$) es nilpotente.
iii) El ideal (0) es un producto finito de ideales maximales. Es decir, existen ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ y enteros positivos $n_1, \ldots, n_s \in \mathbb{N}$ tales que

$$(0) = \mathfrak{m}_1^{n_1} \ldots \mathfrak{m}_s^{n_s}.$$

DEMOSTRACIÓN. Para probar $i)$, tomemos el conjunto de todas las intersecciones finitas de ideales maximales de R, i.e.,

$$\mathcal{A} := \{\mathfrak{a} \subseteq R \ : \ \exists r \in \mathbb{N},\ r \geq 1, \exists \mathfrak{m}_1, \ldots, \mathfrak{m}_r \in MaxSpec(R), \mathfrak{a} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r\}.$$

Por ser R un anillo de Artin, el anterior conjunto no vacío de ideales (recordemos que la no vacuidad del espectro maximal se deduce del Lema de Zorn) tiene elemento minimal. Sea dicho elemento minimal $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \in \mathcal{A}$. Entonces, para cada ideal maximal $\mathfrak{m}$, se tiene que

$$\mathfrak{m} \cap (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n,$$

es decir, que cualquier ideal maximal de R contiene a la intersección $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. Se deduce de esto último fácilmente que $\mathfrak{m}_j \subseteq \mathfrak{m}$ para algún $j \in \{1, \ldots, n\}$. Por lo tanto, concluimos que, como $\mathfrak{m}_j$ es maximal, $\mathfrak{m} = \mathfrak{m}_j$, y se tiene $i)$.

Por otra parte, consideremos la siguiente cadena descendente numerable de ideales:

$$\sqrt{(0)} \supseteq \sqrt{(0)}^2 \supseteq \cdots \supseteq \sqrt{(0)}^k \supseteq \ldots.$$

Como R es anillo artiniano la anterior cadena se estabiliza, i.e. existe $m \in \mathbb{N}$ tal que $\mathfrak{a} := \sqrt{(0)}^m = \sqrt{(0)}^n$ para cada $n \geq m$. Ahora, supongamos que $\mathfrak{a} \neq (0)$, y consideremos el conjunto Σ formado por todos los ideales $\mathfrak{b}$ tales que $\mathfrak{a}\mathfrak{b} \neq (0)$. Entonces, como $\Sigma \neq \emptyset$ ($\mathfrak{a} \in \Sigma$), Σ tiene un elemento minimal $\mathfrak{c}$. Como $\mathfrak{c}\mathfrak{a} \neq (0)$, se tiene que existe $x \in \mathfrak{c}$ tal que $x\mathfrak{a} := \{xa : a \in \mathfrak{a}\} \neq (0)$, con lo que deducimos que $(x) \in \Sigma$. Por tanto, como $(x) \subseteq \mathfrak{c}$, se tiene, por minimalidad, que $\mathfrak{c} = (x)$. Se observa que el ideal $(x)\mathfrak{a}$ pertenece a Σ, ya que $(x)\mathfrak{a}\mathfrak{a} = (x)\mathfrak{a}^2 = (x)\mathfrak{a} \neq (0)$. Además, $(x)\mathfrak{a} \subseteq (x)$, y por tanto, por minimalidad, $(x)\mathfrak{a} = (x)$. Concluimos así que $x = xy$ para algún $y \in \mathfrak{a}$, lo que implica que $x = xy^k$ para todo $k \in \mathbb{N}$. Pero, por definición de $\mathfrak{a}$, $y \in \sqrt{(0)}$. Por ende, y debe ser un elemento nilpotente, lo que implica que existe $p \in \mathbb{N}$ tal que

$x = xy^p = 0$. Pero esto contradice cómo se ha elegido x: Por tanto, por reducción al absurdo, concluimos que $\mathfrak{a} = (0)$, probando *ii)*.

En cuanto a *iii)*, como $\{\mathfrak{m}_1, \dots, \mathfrak{m}_r\} = MaxSpec(R) = Spec(R)$ es finito, por el Teorema Chino de los Restos (véase Teorema A.2.1) concluimos que

$$\sqrt{(0)} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \mathfrak{m}_1 \dots \mathfrak{m}_r.$$

Ahora, por *ii)*, como el nilradical es nilpotente, se tiene que, para algún $n \in \mathbb{N}$,

$$(0) = \sqrt{(0)}^n = \mathfrak{m}_1^n \dots \mathfrak{m}_r^n.$$

Basta pues tomar las menores potencias de cada ideal maximal que satisfacen la propiedad anterior para concluir el resultado. □

PROPOSICIÓN 1.4.3. *Sea R un anillo en el que el ideal (0) es un producto finito de ideales maximales, no necesariamente distintos. Entonces, son equivalentes:*

i) R es un anillo noetheriano.
ii) R es un anillo artiniano.

DEMOSTRACIÓN. Primeramente, observemos que el anillo R es noetheriano (respectivamente artiniano) si y solamente si es noetheriano (respectivamente artiniano) como $R-$módulo. Por tanto, se trata de probar la siguiente equivalencia:

Con la misma hipótesis sobre el ideal (0), son equivalentes:
- *I)* R es un $R-$módulos noetheriano,
- *II)* R es un $R-$módulo artiniano.

Seguidamente, introduzcamos algunas notaciones a partir de la hipótesis. Existen ideales maximales $\mathfrak{m}_1, \dots, \mathfrak{m}_r \in MaxSpec(R)$, no necesesariamente distintos, tales que

$$(0) = \mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_r.$$

Definamos los ideales de R dados por la siguiente identidad:

- $\mathfrak{n}_0 = R$, $\mathfrak{n}_1 = \mathfrak{m}_1$,
- Para $i \geq 2$ sea

$$\mathfrak{n}_i := \mathfrak{m}_i \mathfrak{n}_{i-1} = \mathfrak{m}_1 \cdots \mathfrak{m}_i.$$

Nótese que $\mathfrak{n}_r = (0)$. Además, se satisfacen las siguientes equivalencias:

- R es un $R-$módulo noetheriano (respectivamente artiniano)
- Los ideales $\mathfrak{n}_0, \dots, \mathfrak{n}_r$ son $R-$módulos noetherianos (respectivamente artinianos).

Probemos el caso artiniano porque, de manera análoga, se tendrá el caso noetheriano. Obviamente si $\mathfrak{n}_0, \dots, \mathfrak{n}_r$ son $R-$módulos artinianos, como $\mathfrak{n}_0 = R$ ya tenemos que R es un $R-$módulo artiniano. Recíprocamente, si R es un $R-$módulo artiniano, por la Proposición 1.2.4, también son artinianos sus ideales (i.e. submódulos) y se tiene que $\mathfrak{n}_0, \dots, \mathfrak{n}_r$ son todos artinianos.

Por tanto, la equivalencia entre *I)* y *II)* queda reducida a probar, bajo nuestra hipótesis sobre el ideal (0), la equivalencia entre las siguientes dos afirmaciones:

- *A)* Los ideales $\mathfrak{n}_0, \dots, \mathfrak{n}_r$ son todos $R-$módulos noetherianos.
- *B)* Los ideales $\mathfrak{n}_0, \dots, \mathfrak{n}_r$ son todos $R-$módulos artinianos.

Consideremos ahora la familia de sucesiones exactas cortas de $R-$módulos siguiente:

$$0 \longrightarrow \mathfrak{n}_i \xrightarrow{\lambda_{i-1}} \mathfrak{n}_{i-1} \xrightarrow{\pi_{i-1}} \mathfrak{n}_{i-1}/\mathfrak{n}_i \longrightarrow 0,$$

donde λ_{i-1} y π_{i-1} son, respectivamente, las inclusiones y proyecciones respectivas. Ahora observamos que se verifica la equivalencia entre las siguientes afirmaciones:

- $\mathfrak{n}_0, \dots, \mathfrak{n}_r$ son todos $R-$módulos noetherianos (respectivamente artinianos).
- Los $R-$módulos $\mathfrak{n}_0/\mathfrak{n}_1, \mathfrak{n}_1/\mathfrak{n}_2, \dots, \mathfrak{n}_{r-1}/\mathfrak{n}_r$ son $R-$módulos noetherianos (respectivamente artinianos).

De nuevo, hagamos solamente el caso artiniano. Por la Proposición 1.2.5, si todos los ideales $\mathfrak{n}_0, \ldots, \mathfrak{n}_r$ son artinianos, las sucesiones exactas cortas introducidas en (1.4) nos garantizan que todos los $R-$módulos de la lista $\mathfrak{n}_0/\mathfrak{n}_1, \mathfrak{n}_1/\mathfrak{n}_2, \ldots, \mathfrak{n}_{r-1}/\mathfrak{n}_r$ son artinianos.
Para el recíproco, procedamos inductivamente. Supongamos que todos los elementos de la lista $\mathfrak{n}_0/\mathfrak{n}_1, \mathfrak{n}_1/\mathfrak{n}_2, \ldots, \mathfrak{n}_{r-1}/\mathfrak{n}_r$ son artinianos. Como $\mathfrak{n}_r = (0)$ y tenemos la siguiente sucesión exacta corta:

$$0 \longrightarrow (0) = \mathfrak{n}_r \xrightarrow{\lambda_{r-1}} \mathfrak{n}_{r-1} \xrightarrow{\pi_{r-1}} \mathfrak{n}_{r-1}/\mathfrak{n}_r \longrightarrow 0.$$

De lo anterior, concluimos que $\mathfrak{n}_r = (0)$ y $\mathfrak{n}_{r-1} \cong \mathfrak{n}_{r-1}/\mathfrak{n}_r$ son $R-$módulos artinianos.
Supongamos, inductivamente, que hemos probado que son $R-$módulos artinianos los ideales $\mathfrak{n}_r, \mathfrak{n}_{r-1}, \ldots, \mathfrak{n}_i$ y tomemos, como hipótesis, que $\mathfrak{n}_{i-1}/\mathfrak{n}_i$ es un $R-$módulo artiniano. Tomemos la sucesión exacta corta en el lugar $i-1$ descrita en la Ecuación (1.4):

$$0 \longrightarrow \mathfrak{n}_i \xrightarrow{\lambda_{i-1}} \mathfrak{n}_{i-1} \xrightarrow{\pi_{i-1}} \mathfrak{n}_{i-1}/\mathfrak{n}_i \longrightarrow 0,$$

Como $\mathfrak{n}_i$ y $\mathfrak{n}_{i-1}/\mathfrak{n}_i$ son $R-$módulos artinianos, también lo será $\mathfrak{n}_{i-1}$ por aplicación de la Proposición 1.2.5 precedente.

Con esta última equivalencia, la prueba de la equivalencia expuesta en el enunciado queda reducida a probar la equivalencia entre las dos afirmaciones siguientes:

- 1) Los $R-$módulos $\mathfrak{n}_0/\mathfrak{n}_1, \mathfrak{n}_1/\mathfrak{n}_2, \ldots, \mathfrak{n}_{r-1}/\mathfrak{n}_r$ son $R-$módulos noetherianos.
- 2) Los $R-$módulos $\mathfrak{n}_0/\mathfrak{n}_1, \mathfrak{n}_1/\mathfrak{n}_2, \ldots, \mathfrak{n}_{r-1}/\mathfrak{n}_r$ son $R-$módulos artinianos.

Para probar con la equivalencia entre 1) y 2) procedamos del modo siguiente:
Sea $\kappa(\mathfrak{m}_i) := R/\mathfrak{m}_i$ el cuerpo residual de R con respecto al ideal maximal $\mathfrak{m}_i$. Ahora consideremos el $R-$módulo cociente

$$\mathfrak{n}_{i-1}/\mathfrak{n}_i := \mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1}.$$

Este $R-$módulo cociente tiene una estructura natural de $\kappa(\mathfrak{m}_i)-$espacio vectorial dado por la operación externa siguiente:

$$\begin{array}{rccc} \cdot_\kappa : & R/\mathfrak{m}_i \times \mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1} & \longrightarrow & \mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1} \\ & (x+\mathfrak{m}_i, n+\mathfrak{m}_i\mathfrak{n}_{i-1}) & \longmapsto & xn+\mathfrak{m}_i\mathfrak{n}_{i-1}. \end{array}$$

Además, es un ejercicio de fácil verificación observar que los submódulos de $\mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1}$ como $R-$módulo y los subespacios de $\mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1}$ como $\kappa(\mathfrak{m}_i)-$espacio vectorial son los mismos. Por tanto, para cada i se tiene la equivalencia siguiente

- Los submódulos de $\mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1}$ como $R-$módulo verifican la condición de cadena numerable descendente como $R-$módulo.
- Los subespacios de $\mathfrak{n}_{i-1}/\mathfrak{m}_i\mathfrak{n}_{i-1}$ como $\kappa(\mathfrak{m}_i)-$espacio vectorial verifican la condición de cadena numerable descendente como $\kappa(\mathfrak{m}_i)-$espacio vectorial.

Y una equivalencia análoga se da para el caso noetheriano. En conclusión, la equivalencia entre 1) y 2) queda reducida, en nuestro caso, a las equivalencias siguientes:

- $\mathscr{A}$) Para cada $i \in \{1, \ldots, r\}$, el $\kappa(\mathfrak{m}_i)-$espacio vectorial $\mathfrak{n}_{i-1}/\mathfrak{n}_i$ es noetheriano.
- $\mathscr{B}$) Para cada $i \in \{1, \ldots, r\}$, el $\kappa(\mathfrak{m}_i)-$espacio vectorial $\mathfrak{n}_{i-1}/\mathfrak{n}_i$ es artiniano.

Pero, en el caso de espacios vectorial (i.e. módulos sobre un cuerpo) esta equivalencia se da, bajo nuestras hipótesis, como consecuencia del Corolario 1.3.3 precedente.
Por tanto, $\mathscr{A}) \iff \mathscr{B})$, lo que implica 1) $\iff$ 2) y, a su vez, esta última implica la equivalencia $A) \iff B)$. Estas equivalencias implican la equivalencia entre $I)$ y $II)$ y, finalmente, la equivalencia entre las afirmaciones $i)$ y $ii)$ del enunciado. □

TEOREMA 1.4.4 (**Teorema de Akizuki**). *Un anillo R es artiniano si y solamente si se verifican las dos propiedades siguientes:*

i) R es noetheriano.
ii) Todo ideal primo en R es maximal.

DEMOSTRACIÓN. Aunque las partes más dificultosas ya han sido estudiadas, probemos cada implicación separadamente:

- $\Longrightarrow$: Supongamos que R es un anillo de Artin. Por la afirmación *iii)* de la Proposición 1.4.2, el ideal (0) es un producto finito de ideales maximales de R. Por la Proposición 1.4.3 precedente, si R es artiniano, entonces es neotheriano. Además, por la Proposición 1.4.1, $Spec(R) = MaxSpec(R)$.
- $\Longleftarrow$: Por el Teorema de Lasker-Noether para anillos noetherianos (véase [**Pa,2022**], [**AtMc,1969**]), como R es un anillo noetheriano, el ideal (0) posee una descomposición primaria irredundante:

$$(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r,$$

donde cada ideal $\mathfrak{q}_i$ es un ideal $\mathfrak{m}_i-$primario. Además, como $Spec(R) = MaxSpec(R)$, todos los ideales primos asociados a esta descomposición primaria irredundante son maximales en R. Es decir, $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\} \subseteq MaxSpec(R)$. Además, como R es noetheriano, para cada $i \in \{1, \ldots, r\}$ existe un entero positivo $n_i \in \mathbb{N}$ tal que $\mathfrak{m}_i^{n_i} \subseteq \mathfrak{q}_i$ (véase la Proposición 7.14 del Capítulo 7 de [**AtMc,1969**]). Por tanto, tenemos

$$(0) \subseteq \mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_r^{n_r} \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r = (0).$$

Es decir, tenemos que

$$(0) = \mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_r^{n_r}. \tag{1.4.1}$$

Ahora observemos que los ideales maximales $\mathfrak{m}_i$ son dos a dos distintos (porque nuestra descomposición primaria es irredundante). Pero, además, dados $i \neq j$ se tiene que

$$\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j} = R. \tag{1.4.2}$$

Para probarlo, observemos que si $\mathfrak{m} \in MaxSpec(R)$ es un ideal maximal que contiene a la suma $\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}$, se tendrá

$$\mathfrak{m}_i^{n_i} \subseteq \mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j} \subseteq \mathfrak{m},$$

y

$$\mathfrak{m}_j^{n_j} \subseteq \mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j} \subseteq \mathfrak{m}.$$

Tomando radicales en estas inclusiones, obtenemos:

$$\mathfrak{m}_i = \sqrt{\mathfrak{m}_i^{n_i}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m},$$

y

$$\mathfrak{m}_j = \sqrt{\mathfrak{m}_j^{n_j}} \subseteq \sqrt{\mathfrak{m}} = \mathfrak{m},$$

por las propiedades obvias del radical de un ideal. Como tanto $\mathfrak{m}_i$ como $\mathfrak{m}_j$ son ambos ideales maximales concluiríamos que $\mathfrak{m}_i = \mathfrak{m} = \mathfrak{m}_j$, contradiciendo el hecho de que $\mathfrak{m}_i \neq \mathfrak{m}_j$. En particular, no existe ningún ideal maximal de R que contenga a la suma $\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}$. Como en anillos noetherianos, asumiendo el Axioma de Elección Dependiente, todo ideal propio debe estar contenido en algún ideal maximal, concluimos que la suma de ideales $\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}$ debe ser todo el anillo R y concluye la prueba de la Igualdad (1.4.2).
Finalmente, el Teorema Chino de los Restos (cf. Teorema A.2.1) nos dice que si la familia de ideales $\{\mathfrak{m}_1^{n_1}, \ldots, \mathfrak{m}_r^{n_r}\}$ son dos a dos co-maximales, entonces la intersección de todos ellos es igual a su producto, es decir, se tiene:

$$\mathfrak{m}_1^{n_1} \cap \cdots \cap \mathfrak{m}_r^{n_r} = \mathfrak{m}_1^{n_1} \cdot \cdots \cdot \mathfrak{m}_r^{n_r}.$$

Por la Igualdad (1.4.1) concluimos que

$$(0) = \mathfrak{m}_1^{n_1} \cdot \cdots \cdot \mathfrak{m}_r^{n_r}.$$

En particular, R es un anillo noetheriano en el que el ideal (0) es un producto finito de ideales maximales de R. Ahora podemos aplicar la Proposición 1.4.3 y concluir que, necesariamente, R ha de ser un anillo de Artin.

□

1.5. $K-$álgebras de Artin

En esta sección consideraremos K un cuerpo, $\mathbb{K}$ su clausura algebraica. Sea ahora $K[X_1,\ldots,X_n]$ el anillo de polinomios en n variables con coeficientes en K. Fijamos los siguiente conceptos:

DEFINICIÓN 5 (**Variedad algebraica $K-$definible**). *Una variedad algebraica $K-$definible es un subconjunto $W \subseteq \mathbb{K}^n$ tal que existe una familia de polinomios $f_1,\ldots,f_s \in K[X_1,\ldots,X_n]$ tales que*

$$W := V_{\mathbb{A}}(f_1,\ldots,f_s) := \{x \in \mathbb{K}^n \ : \ f_1(x) = \cdots = f_s(x) = 0\}.$$

DEFINICIÓN 6 (**Variedad cero-dimensional. Grado de una variedad cero-dimensional**). *Una variedad algebraica $K-$definible W se dice cero-dimensional si W es un conjunto finito. El cardinal de una variedad algebraica W se denomina grado de W, y lo denotaremos por* $\deg(W) = \sharp(W)$.

DEFINICIÓN 7 (**Puntos $K-$racionales. Variedad algebraica $K-$racional**). *Dada una variedad algebraica $K-$definible W, definimos los puntos $K-$racionales de W como el conjunto*

$$W_K := W \cap K^n.$$

Además, si $W_K = W$, decimos que W es una variedad algebraica $K-$racional.

Asociamos, biyectivamente, a cada variedad algebraica $K-$definible W su ideal (radical) en $K[X_1,\ldots,X_n]$ dado por la siguiente expresión:

$$I_K(W) := \{f \in K[X_1,\ldots,X_n] \ : \ f(x) = 0, \ \forall x \in W\}. \tag{1.5.1}$$

Cuando no haya confusión sobre el cuerpo K que se está considerando, simplemente escribiremos $I(W)$.

DEFINICIÓN 8 (**Función polinomial $K-$definible**). *Una función polinomial $K-$definible sobre una variedad algebraica $K-$definible W es una aplicación $v : W \longrightarrow K$ tal que existe un polinomio $f \in K[X_1,\ldots,X_n]$ que satisface*

$$v(x) = f(x_1,\ldots,x_n), \ \forall x = (x_1,\ldots,x_n) \in W.$$

Denotamos por $K[W]$ al anillo de todas las funciones polinomiales $K-$definibles sobre W (con las operaciones de suma y producto de aplicaciones).

Notamos además que, dada una variedad algebraica $K-$definible W, $K[W]$ cumple

$$K[W] \cong {}^{K[X_1,\ldots,X_n]}\!\diagup_{I_K(W)}. \tag{1.5.2}$$

Comenzamos observando la siguiente proposición:

PROPOSICIÓN 1.5.1. *Con las notaciones y terminología precedentes, son equivalentes para una variedad $V \subseteq \mathbb{A}^n(\mathbb{K})$:*

i) V es una variedad algebraica cero-dimensional (i.e. un conjunto finito de puntos).
ii) $\mathbb{K}[V]$ es un $\mathbb{K}-$espacio vectorial de dimensión finita.
iii) $\mathbb{K}[V]$ es un $\mathbb{K}-$módulo de longitud finita.
iv) $\mathbb{K}[V]$ es un $\mathbb{K}-$módulo noetheriano en el cual $Spec(\mathbb{K}[V]) = MaxSpec(\mathbb{K}[V])$.
v) $\mathbb{K}[V]$ es un $\mathbb{K}-$módulo artiniano.

Además, en este caso, la dimensión de $\mathbb{K}[V]$ es igual al cardinal de V, i.e.

$$\dim_{\mathbb{K}}(\mathbb{K}[V]) = \sharp(V) = \deg(V),$$

DEMOSTRACIÓN. Las equivalencias *ii)* $\iff$ *iii)* $\iff$ *iv)* $\iff$ *v)* se siguen del Corolario 1.3.3. Probemos *i)* $\Longrightarrow$ *v)*: El Nullstellensatz de Hilbert nos garantiza que existe una biyección entre los puntos de V y los ideales maximales de $\mathbb{K}[V]$. Por tanto, si V es finito, entonces $MaxSpec(\mathbb{K}[V])$ es también un conjunto finito. Además, el anillo $\mathbb{K}[V]$ es un anillo de Jacobson (véase la Proposición A.3.3 de la Sección A.3 del Apéndice), y por tanto el ideal cero satisface

$$(0) = \sqrt{(0)} = {}^{J}\sqrt{(0)} = \bigcap_{\mathfrak{m} \in MaxSpec(\mathbb{K}[V])} \mathfrak{m}.$$

Pero, por el Nullstellensatz de Hilbert tenemos que

$$MaxSpec(\mathbb{K}[V]) = \{\overline{\mathfrak{m}}_\zeta \ : \ \zeta \in V\},$$

donde $\overline{\mathfrak{m}}_\zeta = \{v \in \mathbb{K}[V] \ : \ v(\zeta) = 0\}$ es el ideal maximal de $\mathbb{K}[V]$ asociado al punto $\zeta \in V$. Luego, tenemos

$$(0) = \bigcap_{\zeta \in V} \overline{\mathfrak{m}}_\zeta.$$

Por la Proposición 1.4.3, como $\mathbb{K}[V]$ es un anillo noetheriano, entonces $\mathbb{K}[V]$ es un anillo artiniano y tenemos que la propiedad $v)$ se sigue de todas las anteriores.

Para concluir, probemos $iv) \Longrightarrow i)$: Como $\mathbb{K}[V]$ es noetheriano y $Spec(\mathbb{K}[V]) = MaxSpec(\mathbb{K}[V])$, deducimos (por el Teorema de Akizuki) que es artiniano y $MaxSpec(\mathbb{K}[V])$ es un conjunto finito. Por el Nullstellensatz de Hilbert, existe una biyección entre los puntos de V y los ideales maximales de $\mathbb{K}[V]$, por lo que V es un conjunto finito.

La igualdad entre las dimensiones y los puntos se satisface gracias al Teorema Chino de los Restos (véase Teorema A.2.1). Ya hemos visto que, bajo nuestras hipótesis, se tiene:

$$(0) = \bigcap_{\zeta \in V} \overline{\mathfrak{m}}_\zeta.$$

Por el Teorema Chino de los Restos, tendremos el isomorfismo de anillos siguiente:

$$\begin{array}{rccc} \Phi: & \mathbb{K}[V] = \mathbb{K}[V]/\cap_{\zeta\in V}\overline{\mathfrak{m}}_\zeta & \longrightarrow & \prod_{\zeta\in V}\mathbb{K}[V]/\overline{\mathfrak{m}}_\zeta \\ & v & \longmapsto & (v+\overline{\mathfrak{m}}_\zeta \ : \ \zeta\in V). \end{array}$$

Ahora recordemos que, para cada $\zeta \in V$, se tiene el siguiente isomorfismo de anillos y de $\mathbb{K}-$álgebras:

$$\begin{array}{rccc} \varphi_\zeta: & \mathbb{K}[V]/\overline{\mathfrak{m}}_\zeta & \longrightarrow & \mathbb{K} \\ & v+\overline{\mathfrak{m}}_\zeta & \longmapsto & v(\zeta). \end{array}$$

Por tanto, tenemos inducido el siguiente isomorfismo de anillos y de $\mathbb{K}-$espacios vectoriales, donde $V = \{\zeta_1, \ldots, \zeta_D\}$, siendo $\zeta_i \neq \zeta_j$ para cada $i \neq j$:

$$\begin{array}{rccc} \overline{\Phi}: & \mathbb{K}[V] = \mathbb{K}[V]/\cap_{\zeta\in V}\overline{\mathfrak{m}}_\zeta & \longrightarrow & \prod_{\zeta\in V}\mathbb{K}[V]/\overline{\mathfrak{m}}_\zeta \cong \mathbb{K}^D \\ & v & \longmapsto & (v(\zeta_1), \ldots, v(\zeta_D)), \end{array}$$

lo que implica la igualdad entre $\dim_{\mathbb{K}}(\mathbb{K}[V])$ y $\sharp(V) = \deg(V)$. □

PROPOSICIÓN 1.5.2. *Con las notaciones y terminología precedentes, son equivalentes para una variedad $V \subseteq \mathbb{A}^n(\mathbb{K})$ tal que $V = V \cap K^n$:*

i) V es una variedad algebraica cero-dimensional (i.e. un conjunto finito de puntos) formada por puntos $K-$racionales.
ii) $K[V]$ es un $K-$espacio vectorial de dimensión finita.
iii) $K[V]$ es un $K-$módulo de longitud finita.
iv) $K[V]$ es un $K-$módulo noetheriano en el cual $Spec(\mathbb{K}[V]) = MaxSpec(\mathbb{K}[V])$.
v) $K[V]$ es un $K-$módulo artiniano.
vi) $\mathbb{K}[V]$ es un $\mathbb{K}-$módulo artiniano.

Además, en cualquiera de estos casos se tiene la igualdad siguiente:

$$\dim_K(K[V]) = \sharp(V) = \deg(V).$$

En particular, si se tiene cualquiera de estos casos, se tiene $K[V] = K^V$.

DEMOSTRACIÓN. Las equivalencias $ii) \iff iii) \iff iv) \iff v)$ se siguen del Corolario 1.3.3. La equivalencia entre $i)$ y $vi)$ se sigue del mero hecho de ser V cero-dimensional.
Veamos la implicación $i) \Longrightarrow ii)$: Como V es un conjunto finito, tenemos que $K[V]$ es un subespacio vectorial del K-espacio vectorial K^V, que es un $K-$espacio vectorial de dimensión finita igual a $\sharp(V)$. Por tanto, se tiene que $K[V]$ es un $K-$espacio vectorial de dimensión finita.
Para la implicación $ii) \Longrightarrow i)$, consideremos que $K[V]$ es un $K-$espacio vectorial de dimensión finita. Consideremos, fijada $i \in \{1, \ldots, n\}$, el elemento $x_i := X_i + I_K(V)$, y las potencias siguientes:

$$\{1, x_i, x_i^2, \ldots, x_i^n, \ldots\} = \{x_i^m \ : \ m \in \mathbb{N}\}.$$

Como $K[V]$ es un $K-$espacio vectorial de dimensión finita, ha de existir un entero positivo $d_i \in \mathbb{N}$ tal que $x_i^{d_i}$ es linealmente dependiente sobre K de los elementos $\{1, x_i, \ldots, x_{d_i-1}\}$. En particular, tendremos un polinomio $f_i \in K[T]$ de la forma

$$f_i(T) := T^{d_i} + a_{d_i-1}^{(i)} T^{d_i-1} + \cdots + a_1^{(i)} T + a_0^{(i)} \in K[T],$$

tal que $f_i(X_i) \in I_K(V)$ con $a_j^{(i)} \in K$ para cada $j \in \{0, \ldots, d_i - 1\}$. Por tanto, como $V = V_{\mathbb{A}}(I_K(V))$, tendremos la siguiente inclusión

$$V \subseteq W := \{(z_1, \ldots, z_n) \in \mathbb{K}^n \ : \ f_i(z_i) = 0, \ 1 \leq i \leq n\}.$$

Ahora bien, como $f_i \neq 0$ es un polinomio univariado de grado d_i, para cada i, el conjunto $\{z_i \in \mathbb{K} \ : \ f_i(z_i) = 0\} \subseteq \mathbb{K}$ es un conjunto de, a lo sumo, d_i elementos de $\mathbb{K}$. Por tanto, se verifica que el conjunto W es un conjunto finito. De hecho

$$W \subseteq \prod_{i=1}^{n} \{z_i \in \mathbb{K} \ : \ f_i(z_i) = 0\}.$$

Y, por tanto, $\sharp(W) \leq \prod_{i=1}^{n} d_i$. En particular, $V \subseteq W$ debe ser también un conjunto finito.
Para concluir el enunciado, observemos que si V es una variedad de puntos $K-$racionales, y si $\zeta = (z_1, \ldots, z_n) \in V$, podemos considerar el ideal de $K[V]$ siguiente:

$$\mathfrak{n}_\zeta := (\overline{X_1 - z_1}, \ldots, \overline{X_n - z_n}) \subseteq K[V],$$

donde $\overline{X_i - z_i} = (X_i - z_i) + I_K(V)$. Es sencillo verificar que se tiene

$$\mathfrak{n}_\zeta = \{g \in K[V] \ : \ g(\zeta) = g(z_1, \ldots, z_n) = 0\},$$

que no es otra cosa que la contracción a $K[V]$ del ideal maximal $\overline{\mathfrak{m}}_\zeta$ de $\mathbb{K}[V]$ discutido en la demostración de la Proposición precedente. Es decir, dada la inclusión $K[V] \subseteq \mathbb{K}[V]$ se tiene que $(\overline{\mathfrak{m}}_\zeta)^c = \mathfrak{n}_\zeta$. Razonando como en la Proposición anterior, como $\zeta \in K^n$, se tiene que

$$K[V]/\mathfrak{n}_\zeta \cong K,$$

y concluimos que $\mathfrak{n}_\zeta$ es un ideal maximal.

De otro lado, como $(0) = \cap_{\zeta \in V} \overline{\mathfrak{m}}_\zeta$ es un igualdad cierta en $\mathbb{K}[V]$, entonces, su contracción seguirá siendo cierta en $K[V]$. Es decir, se tendrá que

$$(0) = \bigcap_{\zeta \in V} \mathfrak{n}_\zeta,$$

es una igualdad de ideales en $K[V]$. Finalmente, por el Teorema Chino de los Restos, el isomorfismo Φ restringido a $K[V]$ seguirá siendo un isomorfismo entre los anillos siguientes:

$$\Phi : K[V] \longrightarrow \prod_{\zeta \in V} K[V]/\mathfrak{n}_\zeta.$$

Uniendo estas construcciones como en la demostración de la Proposición precedente, dado que V es finito y está hecho de puntos K-racionales, podemos suponer $V = \{\zeta_1, \ldots, \zeta_D\} \subseteq K^n$ y tenemos un isomorfismo de $K-$espacios vectoriales:

$$\begin{array}{rccc} \widetilde{\Phi} : & K[V] & \longrightarrow & \prod_{i=1}^{D} K[V]/\mathfrak{n}_\zeta = K^D \\ & v & \longrightarrow & (v(\zeta_1), \ldots, v(\zeta_D)). \end{array}$$

Este isomorfismo es un isomorfismo de $K-$espacios vectoriales y, por tanto,

$$\dim_K(K[V]) = D = \sharp(V).$$

Más aún, como $K[V]$ es un subespacio del espacio vectorial de dimensión finita K^V, se tendrá $K[V] = K^V$. □

CAPíTULO 2

Traza y Dualidad en $K-$álgebras Artinianas de variedades algebraicas $K-$racionales

Índice

2.1. Introducción

A lo largo de este capítulo, K denotará a un cuerpo perfecto de característica distinta de 2 y $\mathbb{K}$ a su clausura algebraica. En este segundo capítulo, nos ocuparemos de exhibir notaciones básicas y a probar, de manera auto-contenida, las propiedades elementales de la traza sobre $K-$álgebras de Artin, que serán usadas en el resto de la memoria. Así, para una variedad algebraica afín $K-$definible $V \subseteq \mathbb{A}^n(\mathbb{K}) = \mathbb{K}^n$, denotaremos mediante $K[V]$ al anillo de funciones polinomiales $K-$definibles sobre V. Por la Proposición 1.5.2, se sigue que $K[V]$ es una $K-$álgebra de Artin (o, equivalentemente, un $K-$espacio vectorial finitamente generado) si y solamente si V es una variedad algebraica cero-dimensional $K-$racional.

Por el interés de las aplicaciones que escribiremos en esta memoria, nos restringiremos así al caso en el que $V \subseteq \mathbb{A}^n(\mathbb{K})$ es una variedad algebraica cero-dimensional formado por puntos $K-$racionales (i.e. $V \subseteq \mathbb{A}^n(K) = K^n$). En este caso, como ya se ha mencionado, V es obviamente $K-$definible y $K[V]$ es un $K-$espacio vectorial de dimensión igual a $\deg(V) = \#(V)$ (cardinal de V). Por ello, cada base $\mathscr{B}$ de $K[V]$ como $K-$espacio vectorial puede indexarse a partir de los puntos de V (es decir, siempre podemos escribir $\mathscr{B} = \{v_x : x \in V\}$, independientemente del modo en que elijamos los sub-índices). La idea que subyace es el Teorema Chino de los Restos combinado con el Nullstellensatz, como ya se ha visto en el capítulo precedente.

Nuestro objetivo es estudiar algunas propiedades elementales de la traza canónica. Para ello, y bajo las notaciones precedentes, para cada elemento $v \in K[V]$ consideramos el endomorfismo de $K[V]$ dado por la homotecia de multiplicación por $v \in K[V]$:

$$\begin{array}{rccc} \eta_v : & K[V] & \longrightarrow & K[V] \\ & w & \longmapsto & v \cdot w. \end{array}$$

Al ser un endomorfismo de un $K-$espacio vectorial de dimensión finita, la traza canónica resulta ser

$$\mathrm{Tr}(v) := \mathrm{Tr}\,(\eta_v) := \sum_{x \in V} v(x).$$

Usando la traza canónica como elemento base, podemos definir la forma bilineal simétrica (conocida también como traza canónica) dada mediante la forma siguiente:

$$\begin{array}{rccc} \mathrm{Tr}_V : & K[V] \times K[V] & \longrightarrow & K \\ & (v, w) & \longmapsto & \mathrm{Tr}(v, w) = \mathrm{Tr}(vw), \end{array}$$

donde $v \cdot w \in K[V]$ es el producto en la $K-$álgebra $K[V]$ de los elementos $v, w \in K[V]$. La traza Tr_V será una forma bilineal simétrica no degenerada, lo que nos permitirá usar el lenguaje de dualidad con respecto de la traza.

Así, dada una base $\mathscr{B} = \{v_x : x \in V\}$ de $K[V]$ como $K-$espacio vectorial, una base $\mathscr{B}' = \{w_x : x \in V\}$ se denominará base dual de $\mathscr{B}$ con respecto a la traza si se verifica:

$$\mathrm{Tr}_V(v_x, w_y) = \delta_{x,y},$$

donde $\delta_{x,y}$ es la delta de Kronecker asociada a los puntos de V. El primer resultado elemental que probamos en esta memoria es la Proposición 2.2.4 que afirma que, bajo las restricciones antes descritas, para cada base $\mathscr{B}$ de $K[V]$ como $K-$espacio vectorial existe, al menos, una base dual $\mathscr{B}^*$ de $K[V]$.

Una de las propiedades, y usos, habituales de la traza en $K-$álgebras finitamente generadas es la propiedad de inversión. Aquí hemos optado por la siguiente presentación de esta idea clásica. Bajo nuestras restricciones, dada $f \in K[V]$ y dada una base $\mathscr{B}$ de $K[V]$ definiremos la transformada de f con respecto a $\mathscr{B}$ y la traza como la función polinomial $f^*_{\mathscr{B}} \in K[V]$ dada por la siguiente identidad:

$$f^*_{\mathscr{B}}(x) := \mathrm{Tr}_V(f, v_x), \forall x \in V, \mathscr{B} = \{v_x : x \in V\}.$$

Esta transformada dual simplemente significa la expresión de los coeficientes de f con respecto a una base dual de $\mathscr{B}$ (ver Proposición 2.3.1). Una forma alternativa de presentar esta misma ideal es mediante la *Fórmula (de Inversión) de la Traza*:

Proposición 2.1.1. *Dada $f \in K[V]$ y una base $\mathscr{B}$ de $K[V]$, para cada $z \in V$ se tiene:*

$$f(z) := \sum_{x \in V} f^*_{\mathscr{B}}(x) v^*_x(z),$$

donde $\mathscr{B}^* = \{v^*_x : x \in V\}$ es una base dual de $\mathscr{B}$.

Veremos cómo, en ciertas aplicaciones, esta sencilla fórmula se convierte en una Fórmula de Inversión al estilo de la Fórmula de Inversión de Möbius.

La Sección 2.4, sección final del capítulo, se dedica a escribir un sencillo procedimiento, que se aplicará más tarde, para realizar la tarea siguiente:

Proposición 2.1.2. *Sean dadas $W_1, \ldots, W_m$ variedades algebraicas cero-dimensionales formadas por puntos $K-$racionales, $W_i \subseteq \mathbb{A}^{n_i}(K)$. Sea $V = W_1 \times \cdots \times W_m \subseteq \mathbb{A}^n(K)$, $n = n_1 + \cdots + n_m$. Se tiene que V es una variedad algebraica cero-dimensional formada por puntos $K-$racionales y $K[V] \cong K[W_1] \otimes_K \cdots \otimes_K K[W_m]$. Entonces, dadas bases como $K-$espacio vectorial $\{\mathscr{B}_i \subseteq K[W_i] : 1 \leq i \leq m\}$ y bases duales en $K[W_i]$, $\{\mathscr{B}^*_i \subseteq K[W_i] : 1 \leq i \leq m\}$, podemos escribir bases $\mathscr{B} = \mathscr{B}_1 \otimes \cdots \otimes \mathscr{B}_m$ y $\mathscr{B}^* = \mathscr{B}^*_1 \otimes \cdots \otimes \mathscr{B}^*_m$ de tal modo que $\mathscr{B}$ y $\mathscr{B}^*$ sean duales con respecto a Tr_V.*

Mostrar explícitamente esta construcción es lo que se hace en la Sección 2.4 y será de utilidad más adelante.

2.2. Terminología básica y propiedades generales

Sea K un cuerpo perfecto de característica distinta de 2, $\mathbb{K}$ su clausura algebraica y A una $K-$algebra Artiniana. Una $K-$álgebra Artiniana (también llamada $K-$algebra cero-dimensional o finita, dependiendo del contexto) se puede caracterizar como una $K-$álgebra que es un $K-$espacio vectorial de dimensión finita (como se ha estudiado en el capítulo precedente). Para todo elemento $a \in A$, podemos considerar el endomorfismo de A como $K-$espacio vectorial, η_a, definido como la multiplicación por a:

$$\begin{array}{rccc} \eta_a : & A & \longrightarrow & A \\ & x & \longmapsto & ax. \end{array}$$

Definición 9 (**Traza y norma**). *Con estas notaciones, para cada $a \in A$, definimos los siguientes conceptos:*

i) Llamaremos traza de a a la traza del endomorfismo η_a:

$$\mathrm{Tr}(a) := Traza(\eta_a) \in K.$$

ii) Llamaremos norma de a al determinante del endomorfismo η_a:

$$\mathrm{Norm}(a) := \det(\eta_a).$$

Definimos ahora la traza bilineal simétrica de la K-álgebra A de la siguiente manera:

$$\begin{array}{rccc} \mathrm{Tr}_{A}: & A\times A & \longrightarrow & K \\ & (a,b) & \longmapsto & \mathrm{Tr}(a,b)=\mathrm{Tr}(ab). \end{array}$$

Estamos ahora en condiciones de definir el siguiente concepto:

DEFINICIÓN 10 (**Base dual**). *Con las notaciones anteriores, sea $\mathscr{B} := \{v_i \,:\, i\in I\}$ una base de A como K-espacio vectorial, donde $\sharp(I) = \dim_K(A)$. Sea $\mathscr{B}^* := \{w_j \,:\, j\in I\}$ otra base de A como K-espacio vectorial, indexada sobre el mismo conjunto I. Decimos que $\mathscr{B}^*$ es una base dual de $\mathscr{B}$ respecto de Tr_{A} si se da la siguiente igualdad:*

$$\mathrm{Tr}_{A}(v_i, w_j) := \delta_{i,j},\ \ \forall i,j\in I,$$

donde $\delta_{i,j}$ es la delta de Kronecker con índices en I.

Por otro lado, en el capítulo anterior, se probó que el hecho de que W fuera una variedad algebraica afín cero-dimensional $K-$definible, era equivalente a que el anillo $\mathbb{K}[W]$ fuera una $\mathbb{K}-$álgebra de Artin (ver la Proposición 1.5.1). En dicha Proposición 1.5.1, se probó implícitamente el siguiente resultado:

TEOREMA 2.2.1. *Si W es una variedad algebraica $K-$definible cero-dimensional, el siguiente es un isomorfismo de $\mathbb{K}-$álgebras:*

$$\begin{array}{rccc} \overline{\Phi}: & \mathbb{K}[W] & \longrightarrow & \mathbb{K}^{\sharp(W)} \\ & v & \longmapsto & (v(x)\,:\, x\in W), \end{array} \tag{2.2.1}$$

donde $(v(x)\,:\, x\in W)\in \mathbb{K}^{\sharp(W)}$ es el vector fila cuyas coordenadas son los valores de la función polinomial $v\in\mathbb{K}[W]$ en los puntos $x\in W$.

También se estudió, en la Proposición 1.5.2, que eran equivalentes que W fuera una variedad algebraica $K-$racional y que $K[W]$ fuera un $K-$espacio vectorial de dimensión finita (i.e. una $K-$álgebra de Artin), con lo que podemos particularizar la discusión inicial para este caso concreto. El siguiente Corolario también se demostró implícitamente en la Proposición 1.5.2.

COROLARIO 2.2.2. *Con las notaciones precedentes, si W es una variedad algebraica $K-$racional cero-dimensional, el Teorema Chino de los restos implica que*

$$\begin{array}{rccc} \widetilde{\Phi}: & K[W] & \longrightarrow & K^{\sharp(W)} \\ & v & \longmapsto & (v(x)\,:\, x\in W), \end{array} \tag{2.2.2}$$

es un isomorfismo de anillos y un isomorfismo de K-espacios vectoriales, donde $(v(x)\,:\, x\in W)\in K^{\sharp(W)}$ es el vector fila cuyas coordenadas son los valores de la función polinomial $v\in K[W]$ en los puntos $x\in W$.

A partir de este punto, nos restringimos solamente al caso en el que W es una variedad algebraica $K-$racional cero-dimensional. De todo lo anterior, deducimos que

$$\dim_K(K[W]) = \dim_{\mathbb{K}}(\mathbb{K}[W]) = \deg(W) = \sharp(W).$$

Luego, toda base $\mathscr{B}$ de $K[W]$ (como $K-$espacio vectorial) puede indexarse en W (sin importar cómo los elementos de la base $\mathscr{B}$ están relacionados con los puntos de W). Es decir, si $\mathscr{B}\subseteq K[W]$ es una base de $K[W]$ como $K-$espacio vectorial, podremos describir los elementos de $\mathscr{B}$ de la siguiente manera:

$$\mathscr{B} := \{v_x \,:\, x\in W\}.$$

Además, el isomorfismo previamente construido es la clave para probar el siguiente resultado clásico:

COROLARIO 2.2.3. *Sea $W\subseteq K^n$ una variedad algebraica K-racional cero-dimensional. Entonces, para cada $v\in K[W]$, el endomorfismo η_v es diagonalizable sobre K. Además, la forma canónica de Jordan de η_v sobre K es la matriz diagonal $Diag(v(x)\,:\, x\in W)\in \mathscr{M}_{\sharp(W)}(K)$ y la traza y el determinante de η_v satisfacen:*

$$\mathrm{Tr}(\eta_v) = \sum_{x\in W} v(x)\in K,\ \ \det(\eta_v) = \prod_{x\in W} v(x)\in K.$$

DEMOSTRACIÓN. En primer lugar, supongamos que $W = \{x_1, \ldots, x_D\}$. Tras esto, observemos que, si $\widetilde{\Phi}$ es el isomorfismo descrito en el Corolario 2.2.2, $\widetilde{\Phi} \circ \eta_v \circ \widetilde{\Phi}^{-1} : K^{\#W} \to K^{\#W}$ se puede expresar en forma matricial, tomando en $K^{\#W} = K^D$ la base "canónica" $\{e_1, \ldots, e_D\}$, de la siguiente forma:

$$\begin{pmatrix} v(x_1) & 0 & \ldots & 0 \\ 0 & v(x_2) & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & v(x_n) \end{pmatrix}.$$

Lo anterior se sigue de la forma que toma $\widetilde{\Phi} \circ \eta_v \circ \widetilde{\Phi}^{-1}$: Dado $(a_1, \ldots, a_D) \in K^{\#W}$, sea $w \in K[W]$ tal que $\widetilde{\Phi}^{-1}(a_1, \ldots, a_D) = w$. Ahora, teniendo en cuenta las definiciones de las aplicaciones,

$$\left(\widetilde{\Phi} \circ \eta_v \circ \widetilde{\Phi}^{-1}\right)(a_1, \ldots, a_D) = \left(\widetilde{\Phi} \circ \eta_v\right)(w) =$$

$$= (v(x_i) \cdot w(x_i) : 1 \leq i \leq D) = (v(x_i) \cdot a_i : 1 \leq i \leq D) \in K^D.$$

Por último, se tiene claramente que, para cada $i \in \{1, \ldots, D\}$,

$$\left(\widetilde{\Phi} \circ \eta_v \circ \widetilde{\Phi}^{-1}\right)(e_i) = v(x_i) \cdot e_i.$$

Ahora, sabemos que, por ser $\widetilde{\Phi}$ isomorfismo, $\{\widetilde{\Phi}^{-1}(e_i) : 1 \leq i \leq D\}$ es una base de $K[W]$. Concluimos que, considerando la anterior base en $K[W]$, $Diag(v(x) : x \in W)$ es la forma canónica de Jordan de $\eta_v : K[W] \to K[W]$, concluyendo la prueba. □

Denotamos por $\mathrm{Tr}_W := \mathrm{Tr}_{K[W]}$ a la forma bilineal simétrica sobre $K[W]$ asociada a la función traza descrita en la Ecuación (2.2). Tal y como ya hemos descrito, dadas dos bases $\mathscr{B} := \{v_x : x \in W\}$ y $\mathscr{B}^* := \{w_x : x \in W\}$ de $K[W]$ como $K-$espacio vectorial, con índices en W, decimos que $\mathscr{B}$ y $\mathscr{B}^*$ son bases duales respecto de la traza si y solo si

$$\mathrm{Tr}_W(v_x, w_y) = \delta_{x,y}, \ \forall x, y \in W,$$

donde $\delta_{x,y}$ es de nuevo la Delta de Kronecker con índices en W.

PROPOSICIÓN 2.2.4. *Sea $W \subseteq K^n$ una variedad algebraica $K-$racional cero-dimensional. Entonces, $\mathrm{Tr}_W : K[W] \times K[W] \longrightarrow K$ es una forma bilineal simétrica no degenerada. Además, para cada base $\mathscr{B}$ de $K[W]$ como $K-$espacio vectorial, existe una base dual $\mathscr{B}^*$ de $\mathscr{B}$ respecto de Tr_W.*

DEMOSTRACIÓN. En primer lugar, probamos la existencia de una base dual $\mathscr{B}^*$ para todo base $\mathscr{B}$ de $K[W]$. Gracias al isomorfismo $\widetilde{\Phi}$ descrito en la Identidad (2.2.2), sabemos que una lista de funciones polinomiales $\mathscr{B} := \{v_1, \ldots, v_D\} \subseteq K[W]$ es base si y solo si la siguiente matriz es regular:

$$vdM(\mathscr{B}) := \begin{pmatrix} v_1(x_1) & \cdots & v_1(x_D) \\ \vdots & \ddots & \vdots \\ v_D(x_1) & \cdots & v_D(x_D) \end{pmatrix},$$

donde $W = \{x_1, \ldots, x_D\}$ y $D = \sharp(W) = \deg(W)$. Para cada i, $1 \leq i \leq D$, sea e_k el $k-$ésimo vector de la base "canónica" de K^D. Sea $\omega_i := (\omega_{i,1}, \ldots, \omega_{i,D}) \in K^D$ la única solución del siguiente sistema de ecuaciones lineal:

$$vdM(\mathscr{B}) \begin{pmatrix} \omega_{i,1} \\ \vdots \\ \omega_{i,D} \end{pmatrix} = e_i^T,$$

donde e_i^T es la matriz transpuesta del vector e_i (i.e. su presentación en columna). Entonces, usando el isomorfismo $\widetilde{\Phi}$ de la Identidad (2.2.2) existe $w_i \in K[W]$ tal que:

$$\widetilde{\Phi}(w_i) = (w_i(x_1), \ldots, w_i(x_D)) = (\omega_{i,1}, \cdots, \omega_{i,D}) = \omega_i.$$

La familia $\mathscr{B}^* := \{w_1, \ldots, w_D\}$ es la base "dual" de $\mathscr{B}$, ya que

$$\mathrm{Tr}_W(v_i, w_j) = \sum_{k=1}^{D} v_i(x_k)w_j(x_k) = (v_i(x_1), \ldots, v_i(x_d)) \begin{pmatrix} w_j(x_1) \\ \vdots \\ w_j(x_D) \end{pmatrix} = \delta_{i,j}.$$

Obviamente, el hecho de que $\mathscr{B}^*$ es una base dual de $\mathscr{B}$ con respecto de Tr_W implica que Tr_W es una forma bilineal simétrica no degenerada:
Sea $v := \sum_{i=1}^{D} \lambda_i v_i \in K[W] \setminus \{0\}$, entonces existe $j \in \{1, \ldots, D\}$ tal que $\lambda_j \neq 0$ y, por tanto,

$$\mathrm{Tr}_W(v, w_j) = \sum_{i=1}^{D} \lambda_i \mathrm{Tr}_W(v_i, w_j) = \lambda_j \neq 0,$$

lo que significa que Tr_W es una forma no degenerada y bilineal. □

2.3. La Fórmula (de Inversión) de la Traza

Con las mismas notaciones que en la Sección precedente, nos restringimos al estudio de $K[W]$, donde, de nuevo, $W \subseteq K^n$ es una variedad algebraica K-racional cero-dimensional (i.e. se da la Proposición 2.2.4). En esta sección estableceremos la Fórmula (de Inversión) de la Traza, que de hecho, es el elemento motivador de este trabajo. Esta fórmula es una consecuencia casi inmediata de la existencia de base dual ya vista, pero aún así la probamos con detalle, para fijar las notaciones a usar:

Definición 11 (**Transformada dual de una función respecto de Tr_W y de una base dada**). *Dada una base $\mathscr{B} := \{v_x \ : \ x \in W\}$ de $K[W]$, y una función polinomial $f \in K[W]$, podemos definir la transformada dual de f respecto de la base $\mathscr{B}$ y de Tr_W como la función polinomial $f^*_{\mathscr{B}} \in K[W]$ dada por la siguiente identidad:*

$$f^*_{\mathscr{B}} : \begin{array}{ccc} W & \longrightarrow & K \\ x & \longmapsto & \mathrm{Tr}_W(f, v_x). \end{array} \tag{2.3.1}$$

Proposición 2.3.1. *Con las notaciones precedentes, sea $\mathscr{B}^* := \{v^*_x \ : \ x \in W\}$ una base dual de $\mathscr{B}$ con respecto a Tr_W y sea $f \in K[W]$. Entonces, los coeficientes de f como combinación lineal de los elementos de $\mathscr{B}^*$ son exactamente los valores de la transformada dual de f en los puntos de W. Es decir, se tiene que*

$$f := \sum_{x \in W} \lambda_x v^*_x = \sum_{x \in W} f^*_{\mathscr{B}}(x) v^*_x,$$

con $\lambda_x = f^*_{\mathscr{B}}(x) = \mathrm{Tr}_W(f, v_x)$.

Demostración. Supongamos que tenemos

$$f := \sum_{x \in W} \lambda_x v^*_x,$$

con $\lambda_x \in K$. Entonces, como Tr_W es bilineal y $\mathscr{B}^*$ es una base dual de $\mathscr{B}$ respecto de Tr_W, tenemos que:

$$\mathrm{Tr}_W(f, v_y) = \sum_{x \in W} \lambda_x \mathrm{Tr}_W(v^*_x, v_y) = \sum_{x \in W} \lambda_x \delta_{x,y} = \lambda_y,$$

como afirma el resultado. □

Introducimos ahora, basándonos en la Proposición anterior, una Fórmula (de Inversión) de la Traza, objetivo final de esta sección, que nos permitirá evaluar la función polinomial $f \in K[W]$ de la siguiente manera:

Fórmula (de Inversión) de la Traza: Con las hipótesis precedentes, para cada $f \in K[W]$ y para cada $z \in W$ tenemos

$$f(z) = \sum_{x \in W} f^*_{\mathscr{B}}(x) v^*_x(z) = \sum_{x \in W} \mathrm{Tr}_W(f, v_x) v^*_x(z). \tag{2.3.2}$$

2.4. Construcción de bases duales en el caso de variedades obtenidas como producto cartesiano

Ya hemos probado, en la Proposición 2.2.4, que toda base $\mathscr{B}$ de $K[W]$ tiene una base dual. Ahora, trataremos de presentar una forma explícita de construir una base dual en el caso de variedades algebraicas cero-dimensionales obtenidas como producto cartesiano. Nos restringimos, de nuevo, al caso de variedades algebraicas K-racionales cero-dimensionales.

Sea $\{W_i \subseteq K^{n_i} : 1 \leq i \leq m\}$ una familia de variedades algebraicas $K-$racionales cero-dimensionales. Ahora, consideramos la variedad algebraica $K-$racional cero-dimensional dado por el producto cartesiano $W := \prod_{i=1}^{n} W_i \subseteq K^n$, donde $n := \sum_{i=1}^{m} n_i$. Observamos que, en lo que respecta al grado de W, se tiene que

$$\deg(W) = \sharp(W) = \prod_{i=1}^{m} \deg(W_i).$$

Ahora, consideramos la $K-$álgebra $K[W]$ de las funciones polinomiales sobre W. Esta $K-$álgebra viene dada por el producto tensorial de las $K-$álgebras $K[W_1], \ldots, K[W_m]$ (véase el Teorema A.4.4 de la Sección A.4 del Apéndice):

$$K[W] := K[W_1] \otimes_K \cdots \otimes_K K[W_m].$$

Como la dimensión de $K[W]$ como $K-$espacio vectorial es igual al grado de W, se tiene que

$$\dim_K(K[W]) = \prod_{i=1}^{n} \dim_K(K[W_i]) = \deg(W).$$

Dada una lista de funciones polinomiales $\varphi_1 \in K[W_1], \ldots, \varphi_m \in K[W_m]$, denotamos el producto tensorial de estas aplicaciones por

$$\otimes_{i=1}^{m} \varphi_i := \varphi_1 \otimes \cdots \otimes \varphi_m \in K[W].$$

El lector puede interpretar la función polinomial $\otimes_{i=1}^{m} \varphi_i$ de la siguiente forma:

$$\begin{array}{rccc} \otimes_{i=1}^{m}\varphi_i : & W = \prod_{j=1}^{m} W_i & \longrightarrow & K \\ & (\zeta_1, \ldots, \zeta_m) & \longmapsto & \prod_{j=1}^{m} \varphi_j(\zeta_j). \end{array} \tag{2.4.1}$$

De hecho, algunas autores prefieren la notación $\prod_{i=1}^{m} \varphi_i := \otimes_{i=1}^{m} \varphi_i$. En este trabajo, usaremos una u otra dependiendo del contexto.

Sea $(D) := (D_1, \ldots, D_m) \in \mathbb{N}^m$ una lista de números enteros no negativos. Para cada lista de naturales $(k) := (k_1, \ldots, k_m) \in \mathbb{N}^m$, escribimos $(k) \preceq (D)$ si y solo si $1 \leq k_i \leq D_i$ para cada i, $1 \leq i \leq m$. Dada $(k) := (k_1, \ldots, k_m) \preceq (D)$ y $(r) := (r_1, \ldots, r_m) \preceq (D)$, denotamos por $\delta_{(k),(r)}$ a la delta de Kronecker de valores (k) y (r), i.e.

$$\delta_{(k),(r)} := \begin{cases} 1, & \text{si y solo si } k_i = r_i, \text{ para cada } i,\ 1 \leq i \leq m \\ 0, & \text{en otro caso.} \end{cases}$$

Consideremos una familia de bases de cada $K[W_i]$ como K-espacio vectorial. Además, supongamos que estas bases están dadas por

$$\mathscr{B}_i := \{\varphi_1^{(i)}, \ldots, \varphi_{D_i}^{(i)}\},\ 1 \leq i \leq m,$$

donde $D_i := \deg(W_i)$. Como el producto tensorial "conmuta" con la suma directa (ver Proposición A.4.3 de la Sección A.4 del Apéndice) concluimos que la siguiente es una base de $K[W]$ como $K-$espacio vectorial:

$$\mathscr{B} := \{\Phi_{(k)} := \otimes_{i=1}^{m} \varphi_{k_i}^{(i)} \ : \ (k) = (k_1, \ldots, k_m) \preceq (D)\}. \tag{2.4.2}$$

El siguiente resultado muestra cómo construir una base dual de $\mathscr{B}$ respecto de Tr_W.

Proposición 2.4.1. *Con las notaciones e hipótesis precedentes, para cada i, $1 \leq i \leq m$, consideramos $\mathscr{B}_i^* \subseteq K[W_i]$ una base dual de $\mathscr{B}_i$ respecto de la traza Tr_{W_i} en $K[W_i]$. Asumamos que los elementos de $\mathscr{B}_i^*$ toman la forma siguiente:*

$$\mathscr{B}_i^* := \{\psi_1^{(i)}, \ldots, \psi_{D_i}^{(i)}\}.$$

Entonces, la siguiente es una base dual de $\mathscr{B}$ respecto de la traza Tr_{W} en $K[W]$:

$$\mathscr{B}^* := \{\Psi_{(r)} := \otimes_{i=1}^{(m)} \psi_{r_i}^{(i)} \ : \ (r) := (r_1, \ldots, r_m) \preceq (D)\}.$$

En particular, para cada $(k), (r) \preceq (D)$, se tiene el siguiente resultado:

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \delta_{(k),(r)}. \tag{2.4.3}$$

Demostración. El hecho de que W sea un producto cartesiano es crucial para nuestra prueba. Procedemos por inducción sobre m. El caso $m = 1$ es inmediato; por ende, asumamos que $m \geq 2$.
Tomemos $\Phi_{(k)} \in \mathscr{B}$ y $\Psi_{(r)} \in \mathscr{B}^*$ tales que $(k), (r) \preceq (D)$. Atendiendo a la definición de la función traza $\mathrm{Tr}_{W} : K[W] \times K[W] \longrightarrow K$ (y al Corolario 2.2.3), se tiene que

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \mathrm{Tr}(\Phi_{(k)} \cdot \Psi_{(r)}) = \sum_{\zeta \in W} \left(\Phi_{(k)}\Psi_{(r)}\right)(\zeta) = \sum_{\zeta \in W} \left(\Phi_{(k)}(\zeta)\right)\left(\Psi_{(r)}(\zeta)\right).$$

Adicionalmente, atendiendo a la definición de los elementos de $\mathscr{B}$ y $\mathscr{B}^*$, tendremos que

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta \in W} \left(\otimes_{i=1}^{m} \varphi_{k_i}^{(i)}\right)(\zeta) \left(\otimes_{i=1}^{m} \psi_{r_i}^{(i)}\right)(\zeta).$$

Como $W = \prod_{i=1}^{m} W_i$, de la Identidad (2.4.1) se tiene que

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta_1 \in W_1} \cdots \sum_{\zeta_m \in W_m} \left(\prod_{i=1}^{m} \varphi_{k_i}^{(i)}(\zeta_i)\right)\left(\prod_{i=1}^{m} \psi_{r_i}^{(i)}(\zeta_i)\right).$$

Como K es un cuerpo conmutativo, podemos reescribir la última identidad como

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta_1 \in W_1} \cdots \sum_{\zeta_m \in W_m} \prod_{i=1}^{m} \left(\varphi_{k_i}^{(i)}(\zeta_i)\psi_{r_i}^{(i)}(\zeta_i)\right).$$

Además, tenemos que

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \sum_{\zeta_1 \in W_1} \varphi_{k_1}^{(1)}(\zeta_1)\psi_{r_1}^{(1)}(\zeta_1) \left(\sum_{\zeta_2 \in W_2} \cdots \sum_{\zeta_m \in W_m} \prod_{i=2}^{m} \left(\varphi_{k_i}^{(i)}(\zeta_i)\psi_{r_i}^{(i)}(\zeta_i)\right)\right).$$

Denotemos por R_{m-1} a la siguiente suma

$$R_{m-1} := \left(\sum_{\zeta_2 \in W_2} \cdots \sum_{\zeta_m \in W_m} \prod_{i=2}^{m} \left(\varphi_{k_i}^{(i)}(\zeta_i)\psi_{r_i}^{(i)}(\zeta_i)\right)\right).$$

Sea $W' := \prod_{i=2}^{m} W_i$ la variedad algebraica cero-dimensional que "olvida" W_1. Sea $\mathrm{Tr}_{W'} : K[W'] \times K[W'] \longrightarrow K$ la traza de W', que es también un producto cartesiano. Fijamos las siguientes notaciones:

- $(D') := (D_2, \ldots, D_m)$.
- $(k') := (k_2, \ldots, k_m)$.
- $(r') := (r_2, \ldots, r_m)$.

Por la hipótesis, es claro que $(k') \preceq (D')$ y $(r') \preceq (D')$. Siguiendo lo anterior, denotemos por

$$\Phi_{(k')} := \otimes_{i=2}^{m} \varphi_{k_i}^{(i)} \in K[W'], \ \ \Psi_{(r')} := \otimes_{i=2}^{m} \varphi_{r_i}^{(i)} \in K[W'].$$

Ahora, aplicando la hipótesis inductiva, lo siguiente se cumple:

$$R_{m-1} := \mathrm{Tr}_{W'}(\Phi_{(k')}, \Psi_{(r')}) = \delta_{(k'),(r')},$$

donde $\delta_{(k'),(r')}$ es la delta de Kronecker, como anteriormente. Por lo tanto, hemos probado:

$$\mathrm{Tr}_{W}(\Phi_{(k)}, \Psi_{(r)}) = \left(\sum_{\zeta_1 \in W_1} \varphi_{k_1}^{(1)}(\zeta_1)\psi_{r_1}^{(1)}(\zeta_1)\right) R_{m-1} = Tr_{W_1}\left(\varphi_{k_1}^{(1)}, \psi_{r_1}^{(1)}\right)\delta_{(k'),(r')},$$

donde $Tr_{W_1} : K[W_1] \longrightarrow K$ es la traza de $K[W_1]$. Como $\mathscr{B}_1^*$ es la base dual de $\mathscr{B}_1$ en $K[W_1]$ respecto de Tr_{W_1}, concluimos que

$$\mathrm{Tr}_{W}(\Phi_{(k_1,\ldots,k_m)}, \Psi_{(r_1,\ldots,r_m)}) = \delta_{k_1,r_1}\delta_{(k'),(r')} = \delta_{(k),(r)},$$

donde δ_{k_1,r_1} es la función delta de Kronecker, y hemos probado la Identidad (2.4.3).
Concluimos de manera inmediata que $\mathscr{B}^*$ es una base y que es una base dual de $\mathscr{B}$ respecto de la forma bilineal no degenerada Tr_W. □

CAPíTULO 3

La variedad algebraica $\mathbb{Q}$-racional $2^{[n]}$: base, traza, dualidad y aplicaciones inmediatas en Combinatoria

Índice

3.1. Introducción

Este capítulo está dedicado a trasladar los resultados principales estudiados en el capítulo precedente a algunos resultados clásicos de Combinatoria. Básicamente, el propósito consiste en probar cómo algunos resultados clásicos de Combinatoria no son sino versiones particulares de la Fórmula (de Inversión) de la Traza, dependiendo de las bases del $K-$espacio vectorial V elegidas. Haremos la discusión para $K = \mathbb{Q}$, aunque todos los resultados son válidos si K es un cuerpo perfecto de característica distinta de 2.

Nuestro propósito trata de analizar algunas propiedades del conjunto $2^{[n]}$ formado por todos los subconjuntos del conjunto $[n] = \{1, \ldots, n\}$. Para comenzar, vemos $2^{[n]}$ como la variedad algebraica cero-dimensional formada por puntos $\mathbb{Q}-$racionales

$$V_n := \{(x_1, \ldots, x_n) \in \mathbb{Q}^n \ : \ x_i^2 - x_i = 0, \ 1 \leq i \leq n\}.$$

La identificación entre V_n y $2^{[n]}$ es la obvia y escribiremos libremente $Y \in V_n$ para $Y \subseteq [n]$. Denotaremos por $\mathrm{Tr}_n = Tr_{V_n}$ a la forma bilineal definida sobre $\mathbb{Q}[V_n]$ que satisface las propiedades descritas en el Capítulo precedente. Comenzamos trabajando con tres bases de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial (en las Secciones 3.3, 3.4 y 3.5).

En la Sección 3.3 consideramos las funciones características asociadas a puntos de V_n. Esto es, dado $S \in V_n = 2^{[n]}$ definimos

$$\begin{array}{rccc} \chi_{\{S\}} : & V_n = 2^{[n]} & \longrightarrow & \mathbb{Q} \\ & T & \longmapsto & \begin{cases} 1, & \text{si } S = T \\ 0, & \text{en otro caso.} \end{cases} \end{array}$$

Se observa que estas funciones polinomiales constituyen una base auto-dual con respecto a la traza, que denotaremos por $\mathscr{B}_0 := \{\chi_{\{S\}} : S \subseteq [n]\}$. La usaremos como base auxiliar cuando convenga.

En la Sección 3.4, consideraremos la base monomial de $\mathbb{Q}[V_n]$. De hecho, esa base monomial está determinada por los subconjuntos de $[n]$. Es decir, consideramos para cada $S \subseteq [n]$ la

función monomial siguiente:

$$p_S := \left(\prod_{i\in S} X_i\right) + I(V_n) \in \mathbb{Q}[V_n].$$

Definimos la base $\mathscr{B}_1 := \{p_S : S \subseteq [n]\}$ y construimos una base dual $\mathscr{B}_1^*$ siguiendo el procedimiento descrito en la Sección 2.4.

Analizamos alguna que otra propiedad que será de utilidad en Capítulos subsiguientes. Es destacable observar que el Principio general de Inclusión-exclusión (en orden reverso) no es sino una reformulación de la Fórmula (de Inversión) de la Traza aplicada a la base $\mathscr{B}_1$:

PROPOSICIÓN 1. Dada $f \in V_n = 2^{[n]} \to \mathbb{Q}$ cualquier función ($f \in \mathbb{Q}[V_n]$ por ser V_n finito), se tiene que, para cada $Y \subseteq [n]$ (i.e. $Y \in V_n$),

$$f(Y) := \sum_{Y\subseteq S} p_S^*(Y) f^*_{\mathscr{B}_1}(S) = \sum_{Y\subseteq S} (-1)^{\sharp(S\setminus Y)} f^*_{\mathscr{B}_1}(S) = \sum_{Y\subseteq S} (-1)^{\sharp(S\setminus Y)} \left(\sum_{S\subseteq T} f(T)\right).$$

En la Sección 3.5 nos ocupamos de otra base de $\mathbb{Q}[V_n]$ inspirada en [**FrPa,1983**]. La denominaremos anti-monomial porque es dada como una cierta transformación de la base monomial antes descrita, tomando complementarios. Es decir, para cada $S \subseteq [n]$, definimos

$$q_S := \left(\prod_{i\in[n]\setminus S} (1 - X_i)\right) + I(V_n) \in \mathbb{Q}[V_n].$$

Introducimos así la base $\mathscr{B}_2 := \{q_S : S \subseteq [n]\}$ de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial. Hallamos una base dual $\mathscr{B}_2^*$ y probamos algunas de sus propiedades de uso ulterior en esta memoria.

De nuevo, destacamos otro resultado clásico de Combinatoria que no es sino una mera reescritura de la Fórmula (de Inversión) de la Traza en $\mathbb{Q}[V_n]$ usando la base anti-monomial $\mathscr{B}_2$ precedente. Nos referimos al Principio general de Inclusión-exclusión:

PROPOSICIÓN 2. Dada $f \in V_n = 2^{[n]} \to \mathbb{Q}$ cualquier función ($f \in \mathbb{Q}[V_n]$ por ser V_n finito), se tiene que, para cada $Y \subseteq [n]$ (i.e. $Y \in V_n$),

$$f(Y) := \sum_{S\subseteq Y} q_S^*(Y) f^*_{\mathscr{B}_2}(S) = \sum_{S\subseteq Y} (-1)^{\sharp(Y\setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S\subseteq Y} (-1)^{\sharp(Y\setminus S)} \left(\sum_{T\subseteq S} f(T)\right).$$

La Sección 3.6 se dedica a mostrar bases del subespacio vectorial de los null $t-$designs, que difieren de las exhibidas en [**FrPa,1983**] y antecedentes. De nuevo, se trata de usar traza y dualidad aunque, en este caso, para estudiar conceptos combinatorios un poco más sofisticados.

Los null $t-$designs son definidos en [**FrPa,1983**] del modo siguiente: Una función $f : 2^{[n]} \to \mathbb{Q}$ se denomina un null $t-$design si para todo $A \subseteq [n]$, $\#(A) \leq t$, se verifica

$$\sum_{A\subseteq Y} f(Y) = 0.$$

Dado que V_n es finito, toda función $f : 2^{[n]} \to \mathbb{Q}$ es una función polinomial $\mathbb{Q}-$definible. Entonces, $f \in \mathbb{Q}[V_n]$ es un null $t-$design si y solamente si $f^*_{\mathscr{B}_1}$ es idénticamente cero sobre todos los conjuntos de cardinal acotado por t. Pero, por la Fórmula (de Inversión) de la Traza eso es equivalente a que sus coeficientes en la base dual $\mathscr{B}_1^*$ sean nulos para los elementos $\{p_A^* : A \subseteq [n], \#(A) \leq t\}$, donde $\mathscr{B}_1$ es la base monomial de $\mathbb{Q}[V_n]$ y $\mathscr{B}_1^*$ es su base dual. Por tanto, una base de los null $t-$designs es dada por

$$\{p_A^* : A \subseteq [n], \#(A) > t\},$$

hecho que se prueba en la Proposición 3.6.1 que cierra la Sección 3.6.

3.2. La variedad algebraica $\mathbb{Q}-$racional de los subconjuntos de un conjunto finito

Sea $[n] = \{1, \ldots, n\}$ un conjunto de cardinal n. Denotamos por $2^{[n]}$ a la clase de todos los subconjuntos de $[n]$, y por $\mathbb{F}_2[[n]]$ a la $\mathbb{F}_2-$álgebra formada por todas las funciones características (tambien llamadas indicadores) $\chi_{_Y}$ determinadas por los subconjuntos $Y \in 2^{[n]}$. Consideramos la siguiente variedad algebraica $\mathbb{Q}-$racional cero-dimensional de grado $\deg(V_n) = 2^n$ (véase [**Pa,1995**] para otros usos de esta variedad algebraica):

$$V_n := \{(x_1, \ldots, x_n) \in \mathbb{Q}^n \ : \ x_i^2 - x_i = 0, \ 1 \leq i \leq n\} = \{0,1\}^n \subseteq \mathbb{Q}^n.$$

Se observa que los conjuntos $2^{[n]}$, $\mathbb{F}_2[[n]]$ y V_n están biyectados: Identificamos $Y \subseteq [n]$ con el grafo $Gr(\chi_{_Y}) \subseteq \{0,1\}^n$ de su función característica, visto como un punto en V_n. Para ayudar al lector, denotaremos por el mismo símbolo al subconjunto $Y \subseteq [n]$ y al punto $Y := (y_1, \ldots, y_n) \in V_n$, donde

$$y_i := \begin{cases} 1, & \text{si } i \in Y \\ 0, & \text{en otro caso.} \end{cases}$$

Podemos así ver una familia finita de subconjuntos $\mathscr{F} \subseteq 2^{[n]}$ como una subvariedad algebraica $\mathbb{Q}-$racional cero-dimensional de V_n.

Denotemos por $\mathrm{Tr}_{_n} := \mathrm{Tr}_{_{V_n}} : \mathbb{Q}[V_n] \times \mathbb{Q}[V_n] \longrightarrow \mathbb{Q}$ a la forma bilineal simétrica no degenerada definida por la traza sobre $\mathbb{Q}[V_n] \times \mathbb{Q}[V_n]$, como ya hemos visto en el Capítulo precedente. Por la Proposición 2.2.4, sabemos que toda base $\mathscr{B}$ de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial tiene una base dual $\mathscr{B}^*$ respecto de $\mathrm{Tr}_{_n}$ y, además, la Fórmula (de Inversión) de la Traza (2.3.2) se satisface en $\mathbb{Q}[V_n]$. Finalmente, es claro que $V_n := \{0,1\}^n$ es el producto cartesiano de n variedades algebraicas $\mathbb{Q}-$racionales cero-dimensionales. Con todas estas afirmaciones, podemos deducir el siguiente corolario, que resume las principales propiedades que hemos probado anteriormente:

COROLARIO 3.2.1. *Sea $\mathscr{B} := \{v_Y \ : \ Y \in 2^{[n]}\}$ una base de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial. Entonces, se tienen las siguientes propiedades:*

i) Existe una base dual $\mathscr{B}^* := \{v_Y^* \ : \ Y \in 2^{[n]}\}$ de $\mathscr{B}$ en $\mathbb{Q}[V_n]$ respecto de $\mathrm{Tr}_{_n}$.

ii) La Fórmula (de Inversión) de la Traza se satisface para la transformada dual. Es decir, para cada $f \in \mathbb{Q}[V_n]$ se satisface la siguiente igualdad en $\mathbb{Q}[V_n]$:

$$f = \sum_{Y \in 2^{[n]}} f^*_{\mathscr{B}}(Y) v_Y^*.$$

iii) El método de construcción de bases duales descrito en la Sección 2.4 es aplicable a bases de $\mathbb{Q}[V_n]$.

Tras este Corolario, procedemos a aplicar estas técnicas a varios ejemplos de bases de $\mathbb{Q}[V_n]$ que se usarán más adelante.

3.3. Un ejemplo de base auto-dual: Funciones características sobre átomos en $2^{[n]}$

Para todo $S \subseteq [n]$, consideramos la función característica (a veces llamada indicador) del átomo $\{S\} \in 2^{V_n}$, i.e. la siguiente función:

$$\begin{array}{rccc} \chi_{\{S\}} : & V_n = 2^{[n]} & \longrightarrow & \mathbb{Q} \\ & T & \longmapsto & \begin{cases} 1, & \text{si } S = T \\ 0, & \text{en otro caso.} \end{cases} \end{array} \tag{3.3.1}$$

Es de procedencia remarcar que $\chi_{\{S\}} \in \mathbb{Q}[V_n]$ es distinta de la función característica $\chi_{_S} \in \mathbb{F}_2[[n]]$.

PROPOSICIÓN 3.3.1 (**Bases auto-duales de átomos**). *Con las notaciones precedentes, la función polinomial $\chi_{\{S\}}$ es idempotente en $\mathbb{Q}[V_n]$ (i.e. $(\chi_{\{S\}})^2 - \chi_{\{S\}} = 0$ en $\mathbb{Q}[V_n]$). Además,*

i) El conjunto de las funciones características de átomos en V_n define una base $\mathscr{B}_0$ de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial, donde:

$$\mathscr{B}_0 := \{\chi_{\{S\}} \ : \ S \in V_n = 2^{[n]}\}.$$

ii) La base $\mathscr{B}_0$ es auto-dual (i.e. $\mathscr{B}_0$ es base dual de sí misma). Es decir, si Tr_n es la traza de $\mathbb{Q}[V_n]$, para cada $S,T \in V_n$ tenemos que

$$\mathrm{Tr}_n(\chi_{\{S\}}, \chi_{\{T\}}) = \delta_{S,T},$$

donde, como en secciones precedentes, $\delta_{S,T}$ es la delta de Kronecker.

DEMOSTRACIÓN. Observamos que $\mathscr{B}_0$ genera $\mathbb{Q}[V_n]$ ya que para toda función $f \in \mathbb{Q}[V_n]$ se tiene que

$$f := \sum_{S\subseteq[n]} f(S)\chi_{\{S\}}.$$

Como $\sharp(\mathscr{B}_0) = 2^n = \dim_{\mathbb{Q}}(\mathbb{Q}[V_n])$, se tiene que $\mathscr{B}_0$ debe ser una base de dicho $\mathbb{Q}-$espacio vectorial. Esto prueba *i)*.

Por el Corolario 2.2.3 sabemos que:

$$\mathrm{Tr}_n(\chi_{\{S\}}, \chi_{\{T\}}) := \sum_{Y\in V_n} \chi_{\{S\}}(Y)\chi_{\{T\}}(Y),$$

y, por la definición de las funciones $\chi_{\{S\}}$ y $\chi_{\{T\}}$ anteriores, concluimos inmediatamente que

$$\mathrm{Tr}_n(\chi_{\{S\}}, \chi_{\{T\}}) = \delta_{S,T},$$

lo que concluye la prueba de *ii)*. □

3.4. El ejemplo de la base monomial: Base dual, Fórmula (de Inversión) de la Traza y el Principio general de Inclusión-exclusión (de orden reverso)

Para todo subconjunto $S \in 2^{[n]}$ consideramos el monomio

$$P_S(X_1,\ldots,X_n) := \prod_{i\in S} X_i = \prod_{i=1}^{n} X_i^{\mu_i} \in \mathbb{Q}[X_1,\ldots,X_n], \tag{3.4.1}$$

donde el elemento $S \in V_n$ tiene coordenadas $S = (\mu_1,\ldots,\mu_n) \in \{0,1\}^n$. Este monomio define una función polinomial en V_n que denotamos por $p_S := P_S + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n]$. La siguiente proposición resume las principales propiedades que satisfacen estas funciones polinomiales:

PROPOSICIÓN 3.4.1. *Con las notaciones precedentes, se tienen las siguientes propiedades:*

i) La función polinomial $p_S : V_n \longrightarrow \mathbb{Q}$ satisface para cada $Y \subseteq [n]$:

$$p_S(Y) = \begin{cases} 1, & \text{si } S \subseteq Y \\ 0, & \text{en otro caso.} \end{cases} \tag{3.4.2}$$

En particular, toda función polinomial p_S es idempotente en $\mathbb{Q}[V_n]$.

ii) El conjunto $\mathscr{B}_1 := \{p_S \ : \ S \in V_n = 2^{[n]}\}$ formado por todas las funciones monomiales es una base de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial.

iii) El conjunto $\mathscr{B}_1^* := \{p_S^* \ : \ S \in V_n = 2^{[n]}\}$ es una base dual de $\mathscr{B}_1$ respecto de Tr_n, donde

$$p_S^* := \left(\prod_{i\in S}(2X_i - 1)\prod_{j\in[n]\setminus S}(1 - X_j)\right) + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n].$$

iv) Las funciones polinomiales en la base dual anterior satisfacen:

$$p_S^*(Y) = \begin{cases} (-1)^{\sharp(S\setminus Y)} & \text{si } Y \subseteq S \\ 0, & \text{en otro caso.} \end{cases} \tag{3.4.3}$$

DEMOSTRACIÓN. La afirmación *i)* se prueba por mera verificación. Por otra parte, la afirmación *ii)* se sigue del hecho de que $\{X_1^2 - X_1,\ldots,X_n^2 - X_n\}$ es una base de Gröebner del ideal $I_K(V_n)$ respecto de numerosos órdenes monomiales (como "degree+lexicographic", véase [**Co,1992**] para una explicación sobre esta terminología, si fuera necesario). Para probar *iii)*, observemos que $\mathscr{B}_1$ es la base del producto tensorial $\mathbb{Q}[V_n] = \mathbb{Q}[W_1]\otimes_{\mathbb{Q}}\cdots\otimes_{\mathbb{Q}}\mathbb{Q}[W_n]$, construida a través del método descrito en la Identidad (2.4.2), donde $W_i = \{0,1\}$ y la base de $\mathbb{Q}[W_i]$ elegida es $\mathscr{B}_{1,i} := \{1 + I_{\mathbb{Q}}(W_i), X_i + I_{\mathbb{Q}}(W_i)\}$ (téngase en cuenta el isomorfismo descrito en (1.5.2), y

que $X_i - 1 \notin I_{\mathbb{Q}}(W_i)$). Sea Tr_{W_i} la traza asociada a la variedad algebraica W_i. Verificamos que una base dual de $\mathscr{B}_{1,i}$ respecto de Tr_{W_i} viene dada por

$$\mathscr{B}^*_{1,i} := \{(1 - X_i) + I_{\mathbb{Q}}(W_i), (2X_i - 1) + I_{\mathbb{Q}}(W_i)\}.$$

Para ello, observamos evidentemente que es base, usando argumentos ya citados, y que, usando el Corolario 2.2.3, se tiene que

$$\mathrm{Tr}_{W_i}((1 - X_i) + I_{\mathbb{Q}}(W_i), 1 + I_{\mathbb{Q}}(W_i)) = \mathrm{Tr}(\eta_{(1-X_i)+I_{\mathbb{Q}}(W_i)}) = (1 - 1) + (1 - 0) = 1,$$

$$\mathrm{Tr}_{W_i}((1 - X_i) + I_{\mathbb{Q}}(W_i), X_i + I_{\mathbb{Q}}(W_i)) = \mathrm{Tr}(\eta_{(X_i-X_i^2)+I_{\mathbb{Q}}(W_i)}) = (1 - 1^2) + (0 - 0^2) = 0,$$

$$\mathrm{Tr}_{W_i}((2X_i - 1) + I_{\mathbb{Q}}(W_i), 1 + I_{\mathbb{Q}}(W_i)) = \mathrm{Tr}(\eta_{(2X_i-1)+I_{\mathbb{Q}}(W_i)}) = (2 \cdot 1 - 1) + (2 \cdot 0 - 1) = 0,$$

$$\mathrm{Tr}_{W_i}((2X_i - 1) + I_{\mathbb{Q}}(W_i), X_i + I_{\mathbb{Q}}(W_i)) = \mathrm{Tr}(\eta_{(2X_i^2-X_i)+I_{\mathbb{Q}}(W_i)}) = (2 \cdot 1^2 - 1) + (2 \cdot 0^2 - 0) = 1.$$

Con lo anterior, aplicamos el método descrito en la Proposición 2.4.1 de la Sección 2.4, concluyendo que la siguiente es una base dual de $\mathscr{B}_1$ respecto de Tr_n:

$$\mathscr{B}^*_1 := \left\{ \left(\prod_{i \in S} (2X_i - 1) \prod_{j \in [n] \setminus S} (1 - X_j) \right) + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n] \ : \ S \in 2^{[n]} \right\}.$$

Por último, *iv)* es inmediata a partir de la definición de p^*_S. □

La Fórmula (de Inversión) de la Traza para esta base $\mathscr{B}_1$ es un "principio" habitual en combinatoria: El Principio de Inclusión-Exclusión (de orden reverso).

COROLARIO 3.4.2 (**Dualidad, base monomial y Principio de Inclusión-exclusión (de orden reverso)**). *Con las notaciones precedentes, sea $f \in \mathbb{Q}[V_n]$ una función polinomial definida en $2^{[n]}$. Se tienen las siguientes propiedades:*

i) Para cada $S \subseteq [n]$, la siguiente igualdad se satisface:

$$\mathrm{Tr}_n(f, p_S) = \sum_{S \subseteq T} f(T).$$

En particular, si $f^*_{\mathscr{B}_1} \in \mathbb{Q}[V_n]$ es la transformada dual de f respecto de la base $\mathscr{B}_1$ y de Tr_n, se tiene que:

$$f^*_{\mathscr{B}_1}(S) = \sum_{S \subseteq T} f(T).$$

ii) Se tiene que:

$$f := \sum_{S \subseteq [n]} f^*_{\mathscr{B}_1}(S) p^*_S.$$

iii) **Principio general de Inclusión-exclusión (de orden reverso):** *Para cada $Y \subseteq [n]$ tenemos que*

$$f(Y) := \sum_{Y \subseteq S} (-1)^{\sharp(S \setminus Y)} f^*_{\mathscr{B}_1}(S) = \sum_{Y \subseteq S} (-1)^{\sharp(S \setminus Y)} \left(\sum_{S \subseteq T} f(T) \right).$$

iv) Para cada $T \subseteq [n]$ se tiene

$$\chi_{\{T\}} := \sum_{T \subseteq S} (-1)^{\sharp(S \setminus T)} p_S. \tag{3.4.4}$$

DEMOSTRACIÓN. La mayoría de afirmaciones son inmediatas a partir de las definiciones y resultados anteriores. De todas formas, damos algunas indicaciones de la prueba para explicar cómo se aplican dichos resultados precedentes. Por el Corolario 2.2.3, sabemos que:

$$\mathrm{Tr}_n(f, p_S) := \sum_{Y \in V_n} f(Y) p_S(Y).$$

Por la Identidad (3.4.2) de la Proposición 3.4.1 sabemos que $p_S(Y) = 1$ si y solo si $S \subseteq Y$, siendo cero en otro caso. Por lo tanto, concluimos que

$$f^*_{\mathscr{B}_1}(S) := \mathrm{Tr}_n(f, p_S) := \sum_{S \subseteq Y} f(Y).$$

La afirmación *ii*) se sigue directamente de la Fórmula (de Inversión) de la Traza (2.3.2) anteriormente descrita. Por otra parte, *iii*) es simplemente *ii*) usando la presentación estándar del Principio de Inclusión-Exclusión y la forma de evaluar la función polinomial p_S^* descrita en la Identidad (3.4.3).

Por último, notamos que *iv*) es también otra forma de la Fórmula (de Inversión) de la Traza, pero cambiando los roles de las bases $\mathscr{B}_1$ y $\mathscr{B}_1^*$: Sabemos que existe una combinación lineal tal que:

$$\chi_{\{T\}} := \sum_{S\subseteq[n]} \lambda_{S,T} p_S,$$

donde $\lambda_{S,T} \in \mathbb{Q}$. Ahora, como $\mathscr{B}_1^*$ es una base dual de $\mathscr{B}_1$ respecto de la traza, tenemos que:

$$\lambda_{S,T} := \mathrm{Tr}_n(\chi_{\{T\}}, p_S^*) = \sum_{W\subseteq[n]} \chi_{\{T\}}(W) p_S^*(W) = p_S^*(T).$$

Por último, de acuerdo con (3.4.3), concluimos la Identidad (3.4.4):

$$\lambda_{S,T} = p_S^*(T) = \begin{cases} (-1)^{\sharp(S\setminus T)} & \text{si } T \subseteq S \\ 0, & \text{en otro caso.} \end{cases}$$

Esto concluye la prueba de la afirmación *iv*). □

3.5. El ejemplo de la base anti-monomial: Base dual, Fórmula (de Inversión) de la Traza y la forma general del Principio de Inclusión-Exclusión

Consideremos ahora la siguiente aplicación definida sobre la variedad algebraica V_n:

$$\begin{array}{rccc} \Psi: & V_n & \longrightarrow & V_n \\ & (x_1,\ldots,x_n) & \longmapsto & (1-x_1,\ldots,1-x_n). \end{array} \tag{3.5.1}$$

Esta aplicación es un isomorfismo birregular (i.e. su inversa también es una función polinomial) cuya inversa es él mismo, i.e., $\Psi^{-1}(y_1,\ldots,y_n) = (1-y_1,\ldots,1-y_n) = \Psi(y_1,\ldots,y_n)$. Además, para cada $S \in V_n$, $\Psi(S)$ es el complementario de S en $[n]$ (i.e. $\Psi(S) = [n]\setminus S$). Este isomorfismo birregular induce el siguiente isomorfismo de $\mathbb{Q}-$álgebras, mediante la composición:

$$\begin{array}{rccc} \psi := \Psi_*: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & f\circ\Psi. \end{array} \tag{3.5.2}$$

Ahora, para cada $S \in V_n$ introducimos las siguientes funciones polinomiales $q_S \in \mathbb{Q}[V_n]$:

$$q_S := \left(\prod_{i\in[n]\setminus S} (1-X_i)\right) + I(V_n) \in \mathbb{Q}[V_n]. \tag{3.5.3}$$

Con las notaciones precedentes, se tiene que la siguiente Identidad se satisface para cada $S \subseteq [n]$:

$$\psi(p_S) = q_{[n]\setminus S}.$$

En particular, como $\mathscr{B}_1$ era una base (la base monomial), la clase $\mathscr{B}_2 := \{q_S : S \in V_n\}$ también una base de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial (por ser ψ un isomorfismo de $\mathbb{Q}-$álgebras). El siguiente resultado resume algunas de las propiedades que satisfacen los elementos de la base $\mathscr{B}_2$:

Proposición 3.5.1. *Con las notaciones precedentes, se tiene que:*

i) La función polinomial $q_S : V_n \longrightarrow \mathbb{Q}$ satisface para cada $Y \subseteq [n]$:

$$q_S(Y) = \begin{cases} 1, & \text{si } Y \subseteq S \\ 0, & \text{en otro caso.} \end{cases} \tag{3.5.4}$$

En particular, para cada $S \subseteq [n]$, la función polinomial q_S es un elemento idempotente de $\mathbb{Q}[V_n]$.

ii) Para cada $S \subseteq [n]$, $q_S(Y) := p_{([n]\setminus S)}(\mathbf{1} - Y)$, donde $\mathbf{1} = (1,\ldots,1) \in V_n$ está asociado a $[n]$ como elemento de V_n y $[n]\setminus S$ es el complementario de S en $[n]$.

iii) El conjunto $\mathscr{B}_2 := \{q_S : S \in V_n = 2^{[n]}\}$ es una base de $\mathbb{Q}[V_n]$ como $\mathbb{Q}-$espacio vectorial.

iv) El conjunto $\mathscr{B}_2^* = \{q_S^* \ : \ S \subseteq [n]\}$ *es una base dual de* $\mathscr{B}_2$ *respecto de* Tr_n*, donde*

$$q_S^* := \left(\prod_{i \in S} X_i \prod_{j \in [n] \setminus S} (1 - 2X_j) \right) + I_{\mathbb{Q}}(V_n) \in \mathbb{Q}[V_n].$$

v) La función polinomial en esta base dual satisface

$$q_S^*(Y) = \begin{cases} (-1)^{\sharp(Y \setminus S)}, & \text{si } S \subseteq Y \\ 0, & \text{en otro caso.} \end{cases} \tag{3.5.5}$$

Demostración. La afirmación $i)$ es obvia usando la definición de q_S. Pasamos ahora a detallar la prueba de $v)$: Sea $Y \subseteq [n]$ y denotemos por Y al punto $Y := (y_1, \ldots, y_n) \in V_n$, donde $y_i = 1$ si y solo si $i \in Y$. Consideremos las funciones polinomiales de la familia $\mathscr{B}_2 := \{q_S^* \ : \ S \subseteq [n]\}$. Si $S \subseteq Y$, se tiene la siguiente igualdad:

$$q_S^*(Y) = \prod_{i \in S} y_i \prod_{j \in Y \setminus S} (1 - 2y_j) \prod_{k \in [n] \setminus Y} (1 - 2y_k).$$

De esto último, tenemos que:

- Si $i \in S \subseteq Y$, entonces $y_i = 1$ y, por lo tanto, $\prod_{i \in S} y_i = 1$.
- Si $j \in Y \setminus S$, entonces $y_j = 1$ y, por lo tanto, $\prod_{j \in Y \setminus S} (1 - 2y_j) = (-1)^{\sharp(Y \setminus S)}$.
- Si $k \in [n] \setminus Y$, entonces $y_k = 0$ y, por lo tanto, $\prod_{k \in X \setminus Y} (1 - 2y_k) = 1$.

Por lo tanto, concluimos que si $S \subseteq Y$ tenemos que $q_S^*(Y) = (-1)^{\sharp(Y \setminus S)}$.
Por otro lado, si $S \not\subseteq Y$, entonces existe $i \in S \setminus Y$ y, por tanto, $\prod_{i \in S} y_i = 0$, lo que implica que $q_S^*(Y) = 0$. Esto concluye la prueba del apartado $v)$.

Con las notaciones precedentes ($Y := (y_1, \ldots, y_n) \in V_n$, tal que $y_i = 1$ si y solo si $i \in Y$), observamos que:

$$q_S(Y) = \prod_{i \in [n] \setminus S} (1 - y_i) \in \mathbb{Q}.$$

Por la definición de los polinomios P_T (ver Identidad (3.4.1)) concluimos que

$$q_S(Y) = p_{[n] \setminus S}(1 - y_1, \ldots, 1 - y_n) = p_{[n] \setminus S}(\mathbf{1} - Y),$$

y $ii)$ queda probado.

Por otra parte, ya hemos comprobado que la siguiente aplicación es un isomorfismo de $\mathbb{Q}-$álgebras:

$$\begin{array}{rccc} \psi : & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & f(\mathbf{1} - Y). \end{array}$$

Con lo anterior, observamos que la afirmación $ii)$ implica que $\mathscr{B}_2 := \psi(\mathscr{B}_1)$ y, por tanto, $\mathscr{B}_2$ es una base de $\mathbb{Q}[V_n]$ visto como $\mathbb{Q}-$espacio vectorial, concluyendo por ende la prueba de $iii)$.

Tras esto, tomando $W_i := \{0, 1\}$, nos percatamos de que $V_n := \prod_{i=1}^n W_i = \{0, 1\}^n$ es una variedad algebraica $\mathbb{Q}-$racional obtenida como un producto cartesiano. Sea Tr_{W_i} la traza asociada a la variedad algebraica W_i. Existe una base de $\mathbb{Q}[W_i]$, de construcción inmediata dada por

$$\mathscr{B}_{2,i} := \{\overline{1}, \overline{1 - X_i}\},$$

donde $\overline{1} := 1 + I(W_i)$ y $\overline{1 - X_i} := (1 - X_i) + I(W_i)$ son respectivamente las funciones polinomiales en $\mathbb{Q}[W_i]$ definidas por 1 y $(1 - X_i)$. Comprobamos que la siguiente es una base dual de $\mathscr{B}_{2,i}$:

$$\mathscr{B}_{2,i}^* := \{\overline{X_i}, \overline{1 - 2X_i}\} \subseteq \mathbb{Q}[W_i].$$

Para ello, observamos que se tienen las siguientes igualdades:

$$\mathrm{Tr}_{W_i}(\overline{X_i}, \overline{X_i}) = 1, \mathrm{Tr}_{W_i}(\overline{X_i}, \overline{1 - X_i}) = 0,$$

$$\mathrm{Tr}_{W_i}(\overline{X_i}, \overline{1 - 2X_i}) = 0, \ \mathrm{Tr}_{W_i}(\overline{1 - X_i}, \overline{1 - 2X_i}) = 1.$$

Ahora, por la Proposición 2.4.1, concluimos que la siguiente es una base dual de $\mathscr{B}_2$:

$$\{\psi_1 \otimes \cdots \otimes \psi_n \ : \ \psi_i \in \mathscr{B}_{2,i}^*\}.$$

Esta última base es simplemente el conjunto $\mathscr{B}_2^* = \{q_S^* \,:\, S \subseteq [n]\}$ ya descrito (siendo la prueba de este hecho una mera comprobación). Esto concluye la prueba de *iv*). □

Observamos también que la Fórmula (de Inversión) de la Traza aplicada a la base $\mathscr{B}_2$ es, en esencia, la forma general del Principio de Inclusión-Exclusión.

COROLARIO 3.5.2 (**Dualidad, la base anti-monomial y el Principio de Inclusión-Exclusión en su forma general**). *Con las notaciones precedentes, sea $f \in \mathbb{Q}[V_n]$ una función polinomial definida sobre $2^{[n]}$. Entonces, se tiene que:*

i) Para cada $S \subseteq [n]$, la transformada dual $f^*_{\mathscr{B}_2}$ de f respecto de la base $\mathscr{B}_2$ y de Tr_n, satisface:

$$f^*_{\mathscr{B}_2}(S) = \mathrm{Tr}_n(f, q_S) = \sum_{T \subseteq S} f(T).$$

ii) Se tiene que:

$$f := \sum_{S \subseteq [n]} f^*_{\mathscr{B}_2}(S) q^*_S.$$

iii) **Forma general del Principio de Inclusión-Exclusión:**

$$f(Y) := \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} \left(\sum_{T \subseteq S} f(T) \right).$$

iv) Para cada $T \subseteq [n]$, se tiene que

$$\chi_{\{T\}} := \sum_{S \subseteq T} (-1)^{\sharp(T \setminus S)} q_S. \tag{3.5.6}$$

DEMOSTRACIÓN. La afirmación *i*) se sigue directamente de la Proposición precedente. Por otro lado, *ii*) no es más que la ya bien conocida Fórmula (de Inversión) de la Traza (2.3.2). Tras esto, notamos que *iii*) se sigue de aplicar *ii*) a cualquier subconjunto $Y \subseteq [n]$: Se tiene que

$$f(Y) := \sum_{S \subseteq [n]} f^*_{\mathscr{B}_2}(S) q^*_S(Y).$$

Ahora, de acuerdo con la Identidad (3.5.5) de la Proposición anterior, sabemos que $q^*_S(Y) = 0$ si $S \not\subseteq Y$ y que $q^*_S(Y) = (-1)^{\sharp(Y \setminus S)}$ si $S \subseteq Y$. Por tanto, usando la afirmación *i*) concluimos:

$$f(Y) := \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} f^*_{\mathscr{B}_2}(S) = \sum_{S \subseteq Y} (-1)^{\sharp(Y \setminus S)} \left(\sum_{T \subseteq S} f(T) \right),$$

que es la forma usual de Principio de Inclusión-Exclusión.

El apartado *iv*) es también la Fórmula (de Inversión) de la Traza, pero cambiando los roles de $\mathscr{B}_2$ y $\mathscr{B}_2^*$: Ya sabemos que existe una combinación lineal tal que

$$\chi_{\{T\}} := \sum_{S \subseteq [n]} \lambda_{S,T} q_S,$$

donde $\lambda_{S,T} \in \mathbb{Q}$. Como $\mathscr{B}_2^*$ es una base dual de $\mathscr{B}_2$ respecto de la traza, concluimos, usando la Fórmula (de Inversión) de la Traza, que

$$\lambda_{S,T} := \mathrm{Tr}_n(\chi_{\{T\}}, q^*_S) = \sum_{W \subseteq [n]} \chi_{\{T\}}(W) q^*_S(W) = q^*_S(T).$$

Atendiendo a la Identidad (3.5.5), concluimos (3.5.6):

$$\lambda_{S,T} := \begin{cases} (-1)^{\sharp(T \setminus S)}, & \text{si } S \subseteq T \\ 0, & \text{en otro caso.} \end{cases}$$

□

3.6. El ejemplo del subespacio vectorial de los "null $t-$designs": Otra base explícita

En esta sección, mostramos el papel de la base $\mathscr{B}_1$ en $\mathbb{Q}[V_n]$ que está relacionado con los llamados *null $t-$designs*. Definimos con precisión este último concepto:

DEFINICIÓN 12 (**Null $t-$design**). *Con las mismas notaciones que en las secciones anteriores, una función $f : 2^{[n]} \longrightarrow \mathbb{Q}$ se denomina null $t-$design si para cada $A \subseteq [n]$, tal que $\sharp(A) \leq t$, se satisface la siguiente igualdad:*

$$\sum_{A \subseteq Y} f(Y) = 0.$$

Recordamos ahora el concepto de distancia de Hamming:

DEFINICIÓN 13 (**Distancia de Hamming en V_n**). *La distancia de Hamming sobre V_n es una métrica, que denotamos por $d_H : V_n \times V_n \to \mathbb{R}$, definida de la siguiente manera: Dados $X = (x_1, \ldots, x_n), Y = (y_1, \ldots, y_n) \in V_n = \{0,1\}^n$, definimos*

$$d_H(X,Y) = \#\{i \in [n] : x_i \neq y_i\}.$$

Es decir, la distancia de Hamming de X e Y no es más que el número de posiciones en las que esas dos $n-$tuplas difieren.

Consideramos ahora $W_t := \overline{B}_H(\mathbf{0}, t) \subseteq V_n$ la bola cerrada de centro $\mathbf{0}$ y de radio t respecto a la distancia de Hamming en V_n, i.e.,

$$\overline{B}_H(\mathbf{0}, t) := \{X \in V_n : d_H(\mathbf{0}, X) \leq t\} = \{X \in V_n : \#(X) \leq t\} \subseteq V_n.$$

Entonces, tenemos el siguiente resultado:

PROPOSICIÓN 3.6.1. *Con las notaciones precedentes, las siguientes propiedades se cumplen para toda función $f : 2^{[n]} \longrightarrow \mathbb{Q}$:*

i) Una función $f \in \mathbb{Q}[V_n]$ es un null $t-$design si y solo si se cumple:

$$\mathrm{Tr}_n(f, p_A) = 0, \ \forall A \in W_t.$$

ii) Una función $f : 2^{[n]} \longrightarrow \mathbb{Q}$ es un null $t-$design si y solo si f pertenece al $\mathbb{Q}-$espacio vectorial generado por la siguiente familia de funciones polinomiales linealmente independientes:

$$P_t^* := \{p_F^* \ : \ F \subseteq [n], F \notin W_t\} = \{p_F^* \ : \ F \subseteq [n], \#(F) > t\}.$$

DEMOSTRACIÓN. Por la afirmación $i)$ del Corolario 3.4.2, sabemos que para cada $A \in W_t$ se tiene que

$$\mathrm{Tr}_n(f, p_A) = \sum_{A \subseteq Y} f(Y) = 0.$$

Por lo tanto, $i)$ es una tautología.
En cuanto a $ii)$, observamos que $\mathscr{B}_1^*$ es una base de $\mathbb{Q}[V_n]$ (se recuerda que la definición de $\mathscr{B}_1^*$ ya se ha dado en la Proposición 3.4.1). Por ende, toda función $f \in \mathbb{Q}[V_n]$ puede expresarse de la siguiente manera:

$$f := \sum_{F \subseteq [n]} \mu_F^* p_F^*,$$

donde $\mu_F^* \in \mathbb{Q}$. Supongamos que f es un null $t-$design: entonces, como $\mathscr{B}_1^*$ es la base dual de $\mathscr{B}_1$ respecto de Tr_n, tendremos, usando la Fórmula (de Inversión) de la Traza, que

$$\mu_A^* := \mathrm{Tr}_n(f, p_A) = 0, \ \forall A \in W_t.$$

Por lo tanto, concluimos de manera inmediata que la clase de los null $t-$designs en $\mathbb{Q}[V_n]$ está contenida en el $\mathbb{Q}-$espacio vectorial generado por P_t^*.

Ahora, probemos el resultado recíproco: Como $\mathscr{B}_1^*$ es una base dual de $\mathscr{B}_1$, tenemos que

$$\mathrm{Tr}_n(p_F^*, p_A) = 0, \ \ \forall A \neq F.$$

En particular, si $F \notin W_t$ y $A \in W_t$, tenemos obviamente que $A \neq F$ y, por tanto, dado $p_F^* \in P_t^*$ se tiene:

$$\mathrm{Tr}_n(p_F^*, p_A) = 0, \ \ \forall A \in W_t,$$

lo que prueba, por $i)$, que p_F^* es un null $t-$designs para cada $F \subseteq [n]$, $F \notin W_t$. Concluimos que P_t^* es un conjunto finito de null $t-$designs. Ahora, si tomo f perteneciente al $\mathbb{Q}-$espacio vectorial generado por P_t^*, f podrá ser expresado como combinación lineal de null $t-$designs, i.e., podremos expresar f como sigue:

$$f = \sum_{F \in V_n \setminus W_t} \lambda_{f,F} p_F^*,$$

donde $\lambda_{f,F} \in \mathbb{Q}$. Sea ahora $A \subseteq [n]$ tal que $\#(A) \leq t$. Entonces,

$$\sum_{A \subseteq Y} f(Y) = \sum_{A \subseteq Y} \left(\sum_{F \in V_n \setminus W_t} \lambda_{f,F} p_F^*(Y) \right) = \sum_{F \in V_n \setminus W_t} \lambda_{f,F} \left(\sum_{A \subseteq Y} p_F^*(Y) \right) = 0,$$

por ser cada elemento de P_t^* un null $t-$designs. Por tanto, concluimos finalmente que f es un null $t-$design. □

Notamos que la base para el $\mathbb{Q}-$espacio vectorial de los null $t-$designs descrita anteriormente difiere de la base que se puede encontrar citada en [**FrPa,1983**], descrita en el Teorema 4 de [**DeFr,1982**].

CAPíTULO 4

Los ideales principales $\mathfrak{q}_Y$ y los conjuntos cerrados hacia abajo

Índice

4.1. Introducción

En este capítulo, comenzamos a tratar la dimensión VC (de Vapnik y Chervonenkis), cantidad crucial para medir el tamaño requerido (teóricamente) de las muestras para tener control de error en los algoritmos de aprendizaje aplicados a clasificadores. Los clasificadores sobre $[n]$ son las funciones características χ_S asociadas a subconjuntos $S \subseteq [n]$. Por tanto, una familia de hipótesis $\mathscr{F}$ se puede identificar con una subvariedad $\mathscr{F} \subseteq V_n = 2^{[n]}$. Del mismo modo, dada $Y \subseteq [n]$, la clase de sus subconjuntos $2^Y := \{S \subseteq [n] : S \subseteq Y\}$ es también una subvariedad algebraica de $V_n = 2^{[n]}$. Ahora, dada $\mathscr{F} \subseteq V_n$ y dado $Y \subseteq [n]$ podemos definir la siguiente aplicación:

$$\begin{array}{rccc} \rho_Y : & 2^{[n]} & \longrightarrow & 2^Y \\ & T & \longmapsto & T \cap Y. \end{array}$$

Decimos que $\mathscr{F}$ fragmenta (shatters) Y si $\rho_Y(\mathscr{F}) = 2^Y$. Se define, finalmente, la dimensión de Vapnik-Chervonenkis de $\mathscr{F}$ como:

$$VCD(\mathscr{F}) := \max\{\#(Y) : \rho_Y(\mathscr{F}) = 2^Y\}.$$

La idea de fragmentación se relaciona bien con los elementos de la base $\mathscr{B}_2$ introducida en el Capítulo precedente. Para ello, dado $\mathscr{F} \subseteq V_n$, definamos

$$Q_{\mathscr{F}} := \{q_F : F \in \mathscr{F}\},$$

donde $\mathscr{B}_2 = \{q_S : S \subseteq [n]\}$ es la base anti-monomial. Definamos, también, los ideales $\mathfrak{q}_Y := (q_Y)$ generado por q_Y y $\mathfrak{q}_{\mathscr{F}} := (q_F : F \in \mathscr{F})$ generado por los elementos de $Q_{\mathscr{F}}$. Definamos también el subespacio vectorial generado por los elementos de $Q_{\mathscr{F}}$, $W_{\mathscr{F}} := \mathbb{Q}\langle q_F : F \in \mathscr{F}\rangle$. Además, dados $Y \subseteq [n]$, $\mathscr{F} \subseteq V_n$, definamos

$$Q_{\mathscr{F},Y} = \{q_F q_Y : F \in \mathscr{F}\} \subseteq \mathfrak{q}_Y.$$

Nuestro primer resultado (Proposición 4.2.2) prueba que la dimensión de Vapnik-Chervonenkis está caracterizada por la siguiente identidad:

$$VCD(\mathscr{F}) = \max\{\sharp(Y) \ : \ Q_{\mathscr{F},Y} \text{ es una base de } \mathfrak{q}_Y \text{ como } \mathbb{Q}-\text{espacio vectorial}\}.$$

De hecho, el ideal $\mathfrak{q}_Y$ es isomorfo, como $\mathbb{Q}-$espacio vectorial, a la $\mathbb{Q}-$álgebra $\mathbb{Q}[2^Y]$ y esa es la clave de esta primera relación.

Una herramienta usada en [**Ha,1995**] y sus referencias, es la condición de "closedness downward" (que, amablemente, traducimos por "cerrado hacia abajo") en su análisis de la técnica del "Shifting". En esta Sección 4.3 vamos a caracterizar la condición de ser cerrado hacia abajo para subvariedades $\mathscr{F} \subseteq V_n$ a través de los ideales $\mathfrak{q}_{\mathscr{F}}$ generados por los elementos de la base anti-monomial $\mathscr{B}_2$ indexados por $\mathscr{F}$.

Una subvariedad $\mathscr{F} \subseteq V_n$ se dice cerrada hacia abajo si dado $F \in \mathscr{F}$ y dado $Y \subseteq F$, entonces $Y \in \mathscr{F}$. Es decir, si es cerrada "hacia abajo" con respecto a la inclusión. Dado $\mathscr{F} \subseteq V_n$, podemos definir su clausura hacia abajo como "el conjunto de todos los subconjuntos de conjuntos en $\mathscr{F}$". Esto es, denotando por $\overline{\mathscr{F}}^d$ a la clausura hacia abajo de $\mathscr{F}$, definimos

$$\overline{\mathscr{F}}^d := \{Y \in 2^{[n]} \ : \ \exists F \in \mathscr{F}, \ Y \subseteq F\}.$$

Analizamos varias propiedades de esta construcción pero, posiblemente, merece la pena destacar la Proposición 4.3.4 que se resume en la siguiente:

PROPOSICIÓN 4.1.1. *Dados $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ dos familias de subconjuntos de $[n]$, son equivalentes:*

i) Los ideales $\mathfrak{q}_{\mathscr{F}}$ y $\mathfrak{q}_{\mathscr{G}}$ coinciden (i.e. $\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{\mathscr{G}}$).

ii) $\overline{\mathscr{F}}^d = \overline{\mathscr{G}}^d$.

En particular, existe una biyección entre los subconjuntos de $2^{[n]}$ cerrados hacia abajo y los ideales de la forma $\mathfrak{q}_{\mathscr{F}}$.

Dado que los ideales monomiales son un clásico de la literatura de la Teoría de la Eliminación moderna, vale la pena pensar en esos ideales generados por monomios en nuestro contexto. Un ideal monomial es un ideal de la forma siguiente:

$$\mathfrak{p}_{\mathscr{F}} := (p_S \ : \ S \in \mathscr{F}) \subseteq \mathbb{Q}[V_n],$$

donde $\mathscr{F} \subseteq V_n$ y la base monomial $\mathscr{B}_1 = \{p_S : S \subseteq [n]\}$ es la descrita en la sección precedente. Una subvariedad $\mathscr{F} \subseteq V_n$ se dice cerrada hacia arriba si satisface

$$\forall F \in \mathscr{F}, \ \forall Y \in V_n, \ F \subseteq Y \implies Y \in \mathscr{F}.$$

Esto nos permite también hablar de la clausura hacia arriba (upward closure) definiéndola mediante:

$$\overline{\mathscr{F}}^u := \{Y \in V_n \ : \ \exists F \in \mathscr{F}, \ F \subseteq Y\}.$$

Y, de forma dual al caso de los cerrados hacia abajo, probamos la Proposición 4.4.1 que, sucintamente, afirma:

PROPOSICIÓN 4.1.2. *Dados $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ dos familias de subconjuntos de $[n]$, son equivalentes:*

i) Los ideales monomiales que determinan son iguales (i.e. $\mathfrak{p}_{\mathscr{F}} = \mathfrak{p}_{\mathscr{G}}$).

ii) $\overline{\mathscr{F}}^u = \overline{\mathscr{G}}^u$.

En particular, existe una biyección entre los subconjuntos de $2^{[n]}$ cerrados hacia arriba y los ideales monomiales de $\mathbb{Q}[V_n]$.

4.2. Los ideales principales $\mathfrak{q}_Y$

Usando las mismas notaciones que en secciones precedentes, dado $Y \subseteq [n]$, podemos considerar la clase $2^Y \subseteq V_n$ de los subconjuntos de Y vista como una subvariedad algebraica cero-dimensional de V_n:

$$2^Y := \{S \in V_n \ : \ S \subseteq Y\} = \{(x_1, \ldots, x_n) \in V_n \ : \ x_j = 0, \ \forall j \notin Y\},$$

donde, como en las secciones anteriores, identificamos los subconjuntos $S \subseteq [n]$ y los puntos $S \in V_n$. Algunos autores prefieren denominar a la clase 2^Y como la *caja $\sharp(Y)-$dimensional determinada por Y*. Denotamos por $I(2^Y) \subseteq \mathbb{Q}[V_n]$ al ideal formado por las funciones polinomiales en $\mathbb{Q}[V_n]$ que se anulan en 2^Y. Observamos que se tiene el siguiente isomorfismo:

$$\mathbb{Q}[V_n]/_{I(2^Y)} \cong \mathbb{Q}[2^Y] := \{f : 2^Y \longrightarrow \mathbb{Q} \ : \ f \text{ es una función}\}.$$

El anterior isomorfismo se sigue, evidentemente, de que la aplicación canónica siguiente es un epimorfismo de anillos, de núcleo $I(2^Y)$:

$$\begin{array}{rccc} p: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[2^Y] \\ & f & \longmapsto & f\big|_{2^Y}. \end{array}$$

Anteriormente, también hemos identificado la clase 2^Y y la clase de las funciones características de los subconjuntos en 2^Y:

$$2^Y \cong \mathbb{F}_2[Y] := \{\chi_S \ : \ S \subseteq Y\}.$$

Ahora, dado $Y \subseteq [n]$, podemos considerar la aplicación restricción siguiente:

$$\begin{array}{rccc} \rho_Y: & 2^{[n]} & \longrightarrow & 2^Y \\ & T & \longmapsto & T \cap Y. \end{array}$$

Dado $\mathscr{F} \subseteq 2^{[n]}$, denotamos por $\mathscr{F}\big|_Y$ a la familia de restricciones $\rho_Y(\mathscr{F})$, i.e., a la clase formada por la restricción a Y de cada función binaria de $\mathscr{F}$.

DEFINICIÓN 14 ([VaCh,1971]). *Con las notaciones precedentes, dado $Y \subseteq [n]$ y $\mathscr{F} \subseteq V_n$, decimos que $\mathscr{F}$ fragmenta (shatters) Y si y solo si la siguiente igualdad se satisface:*

$$\rho_Y(\mathscr{F}) = \mathbb{F}_2[Y] = 2^Y.$$

Definimos la dimensión de Vapnik-Chervonenkis de $\mathscr{F}$ (y la denotamos por $VCD(\mathscr{F})$) como el máximo cardinal de cualquier subconjunto Y tal que $\mathscr{F}$ fragmenta Y, es decir,

$$VCD(\mathscr{F}) = \max\{\#(Y) : Y \subseteq [n],\ \mathscr{F} \text{ fragmenta } Y\}.$$

Tras fijar la terminología anterior, introducimos el siguiente ideal principal en $\mathbb{Q}[V_n]$:

$$\mathfrak{q}_Y := (q_Y) := \{fq_Y \ : \ f \in \mathbb{Q}[V_n]\}, \tag{4.2.1}$$

donde q_Y es la función polinomial introducida en la Sección 3.5.

LEMA 4.2.1. *Para cada $f \in \mathbb{Q}[V_n]$, lo siguiente se cumple para cualesquiera $S, Y \subseteq [n]$:*

$$(fq_Y)(S) = \begin{cases} f(S), & \text{si } S \subseteq Y \\ 0, & \text{en otro caso.} \end{cases} \qquad (fp_Y)(S) = \begin{cases} f(S), & \text{si } Y \subseteq S \\ 0, & \text{en otro caso.} \end{cases} \tag{4.2.2}$$

En particular, podemos identificar fq_Y con la restricción de f a 2^Y (i.e. $f\big|_{2^Y} \in \mathbb{Q}[2^Y]$), y tenemos:

$$\mathfrak{q}_Y = \{f \in \mathbb{Q}[V_n] \ : \ f(T) = 0, \forall T \not\subseteq Y\} = I(\mathscr{O}_Y),$$

donde $\mathscr{O}_Y := V_n \setminus 2^Y = \{S \in V_n \ : \ q_Y(S) = 0\}$ es el conjunto (denominado abierto distinguido por algunos autores) de todos los subconjuntos de $[n]$ que no están contenidos en Y. Además, tenemos una descomposición como suma directa de subespacios vectoriales de $\mathbb{Q}[V_n]$ dada por

$$\mathbb{Q}[V_n] \cong \mathfrak{q}_Y \oplus I(2^Y), \tag{4.2.3}$$

la cual resulta en un isomorfismo de $\mathbb{Q}-$espacios vectoriales entre $\mathbb{Q}[2^Y]$ y $\mathfrak{q}_Y$.

DEMOSTRACIÓN. Las identidades en (4.2.2) se siguen de manera inmediata de las definiciones ya introducidas. Estas identidades implican, en particular, que $\mathfrak{q}_Y \subseteq I(\mathscr{O}_Y)$. Recíprocamente, dado $f \in I(\mathscr{O}_Y) \subseteq \mathbb{Q}[V_n]$, consideremos la función polinomial $g := fq_Y$. Como f se anula fuera de 2^Y, las Identidades (4.2.2) implican que $g(S) = f(S)$ para cada $S \in V_n$ y, por tanto, $f = fq_Y \in \mathfrak{q}_Y$. Por último, para probar el isomorfismo de la Ecuación (4.2.3), basta observar que para cada $f \in \mathbb{Q}[V_n]$, se tiene que $f - fq_Y \in I_{\mathbb{Q}}(2^Y)$ y que $\mathfrak{q}_Y \cap I_{\mathbb{Q}}(2^Y) = (0)$. El isomorfismo de $\mathbb{Q}-$espacios vectoriales entre $\mathbb{Q}[2^Y]$ y $\mathfrak{q}_Y$ se sigue directamente del Segundo Teorema de Isomorfía. □

Para cada $\mathscr{F} \subseteq V_n$, introducimos la siguiente clase de funciones:

$$Q_{\mathscr{F}} := \{q_F \ : \ F \in \mathscr{F}\}. \tag{4.2.4}$$

Como $Q_{\mathscr{F}} \subseteq \mathscr{B}_2$ (que es una base de $\mathbb{Q}[V_n]$; se recuerda que se definió esta base en la Proposición 3.5.1), la familia $Q_{\mathscr{F}}$ es una familia de funciones linealmente independientes y su cardinalidad es igual a la cardinalidad de $\mathscr{F}$ (i.e. $\sharp(Q_{\mathscr{F}}) = \sharp(\mathscr{F})$). Con las mismas notaciones, introducimos también

$$\mathscr{F}^{(\max)} := \{F \in \mathscr{F} \ : \ F \text{ es maximal en } \mathscr{F} \text{ respecto de } \subseteq\} \subseteq \mathscr{F}. \tag{4.2.5}$$

Finalmente, para cada subconjunto $\mathscr{F} \subseteq V_n$ introducimos las siguientes notaciones:

- El ideal $\mathfrak{q}_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ generado por $Q_{\mathscr{F}}$:

$$\mathfrak{q}_{\mathscr{F}} := (q_F \ : \ F \in \mathscr{F}). \tag{4.2.6}$$

- El espacio vectorial $W_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ generado por $Q_{\mathscr{F}}$:

$$W_{\mathscr{F}} := \mathbb{Q}\langle q_F \ : \ F \in \mathscr{F}\rangle. \tag{4.2.7}$$

Se tiene de manera obvia que $\mathfrak{q}_Y$ es el ideal $\mathfrak{q}_{\{Y\}}$, que $W_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{F}}$ y que la dimensión de $W_{\mathscr{F}}$ como $\mathbb{Q}-$espacio vectorial es $\sharp(\mathscr{F})$ ya que los elementos de $Q_{\mathscr{F}}$ son linealmente independientes sobre $\mathbb{Q}$. Probamos ahora la siguiente proposición que resume algunas otras propiedades fundamentales del ideal principal $\mathfrak{q}_Y$:

PROPOSICIÓN 4.2.2. *Con las notaciones precedentes, se tiene:*

i) Para cada $Z, Y \subseteq [n]$, la siguiente propiedad se satisface en $\mathbb{Q}[V_n]$:

$$q_Z q_Y = q_{Z\cap Y}.$$

ii) Además, para cada $Z, Y \subseteq [n]$ los siguientes son enunciados equivalentes:
   (a) $Z \subseteq Y$.
   (b) q_Y divide a q_Z en $\mathbb{Q}[V_n]$.
   (c) $\mathfrak{q}_Z \subseteq \mathfrak{q}_Y$.

iii) El isomorfismo entre $\mathbb{Q}[2^Y]$ y $\mathfrak{q}_Y$ es un isomorfismo de $\mathbb{Q}[V_n]-$módulos.

iv) Las siguientes son bases de $\mathfrak{q}_Y$ como $\mathbb{Q}-$espacio vectorial:

$$\mathscr{B}_{0,2^Y} := \{\chi_{\{T\}} \ : \ T \subseteq Y\}, \ \ \mathscr{B}_{2,2^Y} := \{q_T \ : \ T \subseteq Y\}.$$

v) El ideal $I(2^Y)$ es el anulador en $\mathbb{Q}[V_n]$ del ideal $\mathfrak{q}_Y$:

$$I(2^Y) := Ann_{\mathbb{Q}[V_n]}(\mathfrak{q}_Y) := \{f \in \mathbb{Q}[V_n] \ : \ fq_Y = 0\},$$

y $\{q_T^* \ : \ T \not\subseteq Y\} \subseteq I(2^Y)$.

vi) Dado $\mathscr{F} \subseteq 2^{[n]}$ y un subconjunto $Y \subseteq [n]$, denotemos por $Q_{\mathscr{F},Y}$ a la clase de las funciones polinomiales definida como sigue:

$$Q_{\mathscr{F},Y} := \{q_F q_Y \ : \ F \in \mathscr{F}\} \subseteq \mathfrak{q}_Y.$$

Entonces, $\mathscr{F}$ fragmenta Y si y solo si $Q_{\mathscr{F},Y}$ es una base de $\mathfrak{q}_Y$ como $\mathbb{Q}-$espacio vectorial. En particular, $\mathscr{F}$ fragmenta Y si y solo si

$$2^{\sharp(Y)} \leq \sharp\left(Q_{\mathscr{F},Y}\right).$$

En particular, la dimensión de Vapnik-Chervonenkis se puede caracterizar como sigue:

$$VCD(\mathscr{F}) = \max\{\sharp(Y) \ : \ 2^{\sharp(Y)} \leq \sharp\left(Q_{\mathscr{F},Y}\right)\} =$$

$$= \max\{\sharp(Y) \ : \ Q_{\mathscr{F},Y} \text{ es una base de } \mathfrak{q}_Y \text{ como } \mathbb{Q}-\text{espacio vectorial}\}.$$

DEMOSTRACIÓN. Probamos cada afirmación por separado:

- *i):* Se sigue de manera inmediata de la Identidad (3.5.4).
- *ii):* La equivalencia entre (b) y (c) es evidente atendiendo a la definición de $\mathfrak{q}_Y$ y $\mathfrak{q}_Z$. La afirmación $i)$ nos permite probar de manera inmediata que $(a) \implies (c)$, ya que $Z \cap Y = Z$ si $Z \subseteq Y$. Por último, para la implicación $(b) \implies (a)$, supongamos que $q_Z = fq_Y$ para algún $f \in \mathbb{Q}[V_n]$. Si $Z \not\subseteq Y$, entonces tendremos que:

$$1 = q_Z(Z) = f(Z)q_Y(Z) = f(Z) \cdot 0 = 0,$$

  lo cual es imposible.
- *iii):* La proyección canónica ya introducida $p : \mathbb{Q}[V_n] \to \mathbb{Q}[2^Y]$ induce el siguiente isomorfismo:

$$\begin{array}{rccc} \varphi : & \mathfrak{q}_Y & \longrightarrow & \mathbb{Q}[2^Y] \\ & f & \longmapsto & f\big|_{2^Y}. \end{array}$$

  Obviamente, el anterior es un $\mathbb{Q}[V_n]-$isomorfismo.
- *iv):* En primer lugar, notamos que 2^Y puede identificarse con V_m, donde $m = \sharp(Y)$. Se concluye ahora de manera directa usando las Proposiciones 3.3.1 y 3.5.1.
- *v):* Dada una función $f \in \mathbb{Q}[V_n]$, si f se anula en todos los puntos de $S \in 2^Y$, entonces, se tiene que

$$fq_Y(S) = 0, \ \forall S \in 2^Y.$$

  Adicionalmente, sabemos que

$$fq_Y(T) = 0, \ \forall T \notin 2^Y.$$

Por lo tanto, si $f \in I_{\mathbb{Q}}(2^Y)$, entonces $fq_Y \in \mathbb{Q}[V_n]$ es la función polinomial nula y, por ende, $f \in Ann_{\mathbb{Q}[V_n]}(q_Y)$. Recíprocamente, si $f \in Ann_{\mathbb{Q}[V_n]}(2^Y)$, entonces

$$0 = fq_Y(S) = f(S),\ \forall S \subseteq Y,$$

y, por tanto, $f \in I(2^Y)$.
La segunda afirmación de este apartado es obvia por la Identidad (3.5.5).

- *vi):* Observamos que $\mathscr{F}$ fragmenta Y si y solo si se satisface la siguiente igualdad conjuntista:

$$Q_{\mathscr{F},Y} = \{q_{F\cap Y} \ : \ F \in \mathscr{F}\} = \{q_S \ : \ S \subseteq Y\}.$$

Por lo tanto, la implicación $\Longrightarrow$ es obvia. La otra implicación se sigue de que la dimensión de $\mathfrak{q}_Y$ como $\mathbb{Q}-$espacio vectorial es igual a la dimensión $\mathbb{Q}[2^Y]$ y esta dimensión es $2^{\sharp(Y)}$. Por ende, si $Q_{\mathscr{F},Y}$ es una base de $\mathfrak{q}_Y$ como $\mathbb{Q}-$espacio vectorial, concluimos que $\sharp(Q_{\mathscr{F},Y}) = 2^{\sharp(Y)}$. Como $Q_{\mathscr{F},Y}$ es siempre un subconjunto de $\{q_S \ : \ S \subseteq Y\}$, si ambos conjuntos finitos tienen el mismo cardinal ambos deben ser iguales y, por tanto, $\mathscr{F}$ fragmenta Y. La última afirmación de *vi)* se sigue de los anteriores argumentos.

El último enunciado se sigue inmediatamente de *vi)*. □

4.3. Subvariedades algebraicas de V_n cerradas hacia abajo que están en biyección con ideales de la forma $\mathfrak{q}_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$

Esta sección explica el papel de los ideales $\mathfrak{q}_{\mathscr{F}}$ introducidos anteriormente en términos de sistemas de generadores cerrados hacia abajo.

Definición 15 (**Cerrado hacia abajo**). *Con las notaciones precedentes, sea $\mathscr{F} \subseteq V_n$. Decimos que $\mathscr{F}$ es una subvariedad cerrada hacia abajo si dados $F \in \mathscr{F}$ e $Y \in V_n$, si $Y \subseteq F$, entonces $Y \in \mathscr{F}$.*

Seguimos las mismas notaciones que en la sección anterior.

Lema 4.3.1. *Sea $\mathscr{F} \subseteq V_n$. Entonces, tenemos que*

$$\mathfrak{q}_{\mathscr{F}} = (q_{Y_1}, \ldots, q_{Y_r}) := \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r},$$

donde

$$\mathscr{F}^{(\max)} = \{Y_1, \ldots, Y_r\},$$

y $\mathscr{F}^{(\max)} \subseteq \mathscr{F}$ es el conjunto definido en la Identidad (4.2.5).

Demostración. La inclusión $\supseteq$ es obvia ya que $q_{Y_i} \in Q_{\mathscr{F}}$ para cada $i \in \{1, \ldots, r\}$. Por otra parte, dado $F \in \mathscr{F}$, debe existir un elemento maximal Y_i tal que $F \subseteq Y_i$. Por el apartado *i)* de la Proposición 4.2.2, tenemos que $q_F = q_F q_{Y_i} \in \mathfrak{q}_{Y_i}$ y la inclusión $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r}$ queda probada.

□

Podemos introducir el concepto de clausura hacia abajo de un subconjunto $\mathscr{F} \subseteq 2^{[n]}$ como sigue:

Definición 16 (**Clausura hacia abajo**). *Dado $\mathscr{F} \subseteq 2^{[n]}$ definimos la clausura hacia abajo de $\mathscr{F}$ de la siguiente manera:*

$$\overline{\mathscr{F}}^d := \{Y \in 2^{[n]} \ : \ \exists F \in \mathscr{F},\ Y \subseteq F\}.$$

El siguiente resultado resume las principales propiedades de los subconjuntos de V_n que son cerrados hacia abajo:

Proposición 4.3.2. *Sea $\mathscr{F} \subseteq V_n$ una subvariedad algebraica de V_n. Las siguientes propiedades son equivalentes:*

i) $\mathscr{F}$ es una subvariedad cerrada hacia abajo.
ii) $\mathscr{F}$ es unión finita de cajas, i.e., existen $Z_1, \ldots, Z_s \in V_n$ tales que

$$\mathscr{F} = \bigcup_{j=1}^{s} 2^{Z_j}.$$

iii) $\mathscr{F}$ *es la unión finita de las cajas determinadas por sus elementos maximales, i.e.*

$$\mathscr{F} = \bigcup_{j=1}^{r} 2^{Y_j},$$

donde $\mathscr{F}^{(\max)} = \{Y_1, \ldots, Y_r\}$.

iv) El subespacio vectorial $W_{\mathscr{F}}$ *asociado a* $\mathscr{F}$ *es un ideal en* $\mathbb{Q}[V_n]$.

v) La siguiente igualdad se satisface:

$$W_{\mathscr{F}} = \mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r} = (q_{Y_1}, \ldots, q_{Y_r}),$$

donde $\mathscr{F}^{(\max)} = \{Y_1, \ldots, Y_r\}$.

vi) Para cada $i \in [n]$ *y para cada* $F \in \mathscr{F}$, $(1 - X_i)q_F \in W_{\mathscr{F}}$.

vii) Para cada $i \in [n]$ *y para cada* $f \in W_{\mathscr{F}}$, $(1 - X_i)f \in W_{\mathscr{F}}$.

En particular, si $\mathscr{F}$ *es una subvariedad cerrada hacia abajo se tiene*

$$VCD(\mathscr{F}) = \max\{\sharp(F) \ : \ F \in \mathscr{F}\} = \max\{\sharp(Y) \ : \ Y \in \mathscr{F}^{(\max)}\},$$

y

$$\mathscr{F} \subseteq \overline{B}_H(\mathbf{0}, VCD(\mathscr{F})),$$

donde $\overline{B}_H(\mathbf{0}, r) \subseteq V_n$ *es la bola cerrada de centro* $\mathbf{0} = \emptyset \in V_n$ *y radio* r *respecto de la distancia de Hamming. En particular, si* $\mathscr{F}$ *es cerrado hacia abajo se satisface la cota del Lema de Sauer-Shelah-Perles, es decir, se satisface*

$$\#(\mathscr{F}) \leq \#\left(\overline{B}_H(\mathbf{0}, VCD(\mathscr{F}))\right) = \sum_{i=0}^{VCD(\mathscr{F})} \binom{n}{i}.$$

Demostración. La equivalencia de las afirmaciones *i)*, *ii)* y *iii)* es inmediata. Estudiamos las demás equivalencias en detalle:

- *i)* $\Longrightarrow$ *iv)*: Supongamos que $\mathscr{F}$ es una subvariedad cerrada hacia abajo. Consideremos ahora $f \in W_{\mathscr{F}}$ y $g \in \mathbb{Q}[V_n]$. Como $Q_{\mathscr{F}}$ es una base de $W_{\mathscr{F}}$ como subespacio vectorial de $\mathbb{Q}[V_n]$, existen $\{\lambda_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}$ tales que
$$f = \sum_{F \in \mathscr{F}} \lambda_F q_F \in W_{\mathscr{F}}.$$
Por otra parte, $\mathscr{B}_2 := \{q_Y \ : \ Y \subseteq [n]\}$ es una base de $\mathbb{Q}[V_n]$ como espacio vectorial. Entonces, existen $\{\mu_Y \ : \ Y \in V_n\} \subseteq \mathbb{Q}$ tales que
$$g = \sum_{Y \in V_n} \mu_Y q_Y.$$
Entonces, por la afirmación *i)* de la Proposición 4.2.2 concluimos que
$$gf = \sum_{F \in \mathscr{F}, Y \in V_n} \lambda_F \mu_Y q_F q_Y = \sum_{F \in \mathscr{F}, Y \in V_n} \lambda_F \mu_Y q_{F \cap Y}.$$
Como $\mathscr{F}$ es una subvariedad cerrada hacia abajo, para cada $F \in \mathscr{F}$ y para cada $Y \in V_n$, $F \cap Y \in \mathscr{F}$ y, por tanto, $q_{F \cap Y} \in Q_{\mathscr{F}} \subseteq W_{\mathscr{F}}$. Por tanto, concluimos que $gf \in W_{\mathscr{F}}$ y, por tanto, $W_{\mathscr{F}}$ debe ser un ideal en $\mathbb{Q}[V_n]$.
- *iv)* $\Longleftrightarrow$ *v)*: : Por el Lema 4.3.1, ya sabemos que
$$\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{Y_1} + \cdots + \mathfrak{q}_{Y_r} = (q_{Y_1}, \ldots, q_{Y_r}).$$
Por tanto, como $W_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{F}}$ y $\{q_{Y_1}, \ldots, q_{Y_r}\} \subseteq Q_{\mathscr{F}} \subseteq W_{\mathscr{F}}$, si $W_{\mathscr{F}}$ es un ideal, entonces debe ser igual a $\mathfrak{q}_{\mathscr{F}}$. El recíproco es inmediato.
- *v)* $\Longrightarrow$ *vi)*: Suponiendo que $W_{\mathscr{F}}$ es un ideal, como $1 - X_i \in \mathbb{Q}[V_n]$ y $q_F \in W_{\mathscr{F}}$ para cada $F \in \mathscr{F}$, deducimos que $(1 - X_i)q_F \in W_{\mathscr{F}}$ y se sigue *vi)*.
- *vi)* $\Longrightarrow$ *i)*: De nuevo por la afirmación *i)* de la Proposición 4.2.2, concluimos que
$$(1 - X_i)q_F = q_{F \setminus \{i\}}.$$
Además, observamos que para cada $Z \subseteq [n]$, $q_Z \in W_{\mathscr{F}}$ si y solo si $Z \in \mathscr{F}$. Detallamos esto último: Si $q_Z \in W_{\mathscr{F}}$, existen $\{\lambda_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}$ tales que
$$q_Z = \sum_{F \in \mathscr{F}} \lambda_F q_F.$$

Por lo tanto, si $Z \notin \mathscr{F}$, tendríamos una combinación lineal no trivial de elementos de la base $\mathscr{B}_2$ igual a 0:

$$1q_Z + \sum_{F \in \mathscr{F}} (-\lambda_F) q_F = 0.$$

Y esto último no es posible. Por lo tanto, la afirmación *vi)* significa que para cada $F \in \mathscr{F}$ y para cada $i \in [n]$, $F \setminus \{i\} \in \mathscr{F}$. Obviamente, esto significa que dados $F \in \mathscr{F}$ e $Y \subseteq F$, se tiene que $Y \in \mathscr{F}$, y por tanto, concluimos que $\mathscr{F}$ es una subvariedad cerrada hacia abajo.

- *vi)* $\iff$ *vii)*: Si $f \in W_{\mathscr{F}}$, entonces existen $\{\lambda_F \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}$ tales que

$$f = \sum_{F \in \mathscr{F}} \lambda_F q_F.$$

Por lo tanto,

$$(1 - X_i) f = \sum_{F \in \mathscr{F}} \lambda_F (1 - X_i) q_F,$$

y por *vi)*, concluimos que $(1 - X_i) f \in W_{\mathscr{F}}$. El recíproco es trivial.

En cuanto al último resultado, si $\mathscr{F}$ es una subvariedad cerrada hacia abajo, la dimensión de Vapnik-Chervonenkis de $\mathscr{F}$ está determinada por el cardinal de la caja maximal 2^Y contenida en $\mathscr{F}$ y la igualdad a probar se obtiene. De los enunciados *ii)* y *iii)*, se tiene claramente que si $\mathscr{F}$ es una subvariedad cerrada hacia abajo, todos sus elementos $F \in \mathscr{F}$ pertenecen a alguna caja 2^{Y_i} y por tanto, $\sharp(F) \leq \sharp(Y_i) \leq VCD(\mathscr{F})$. Por ende, concluimos que $\mathscr{F} \subseteq \overline{B}_H(\mathbf{0}, VCD(\mathscr{F}))$, como se quería. □

Mientras que el subespacio vectorial $W_{\mathscr{F}}$ está determinado (y determina) la clase $\mathscr{F}$ (porque $Q_{\mathscr{F}} \subseteq \mathscr{B}_2$ es una familia de funciones linealmente independientes), el ideal $\mathfrak{q}_{\mathscr{F}}$ está determinado (y determina) la clase $\mathscr{F}^{(\max)}$ de elementos maximales en $\mathscr{F} \subseteq 2^{[n]}$. Además, el ideal $\mathfrak{q}_{\mathscr{F}}$ está determinado (y determina) la clausura hacia abajo $\overline{\mathscr{F}}^d$. Esto se explica en los siguientes resultados:

LEMA 4.3.3. *Sean $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ dos subvariedades algebraicas de V_n. Entonces, $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$ si y solo si para cada $F \in \mathscr{F}$ existe $G \in \mathscr{G}$ tal que $F \subseteq G$.*

DEMOSTRACIÓN. Supongamos que se cumple la siguiente propiedad:

$$\forall F \in \mathscr{F}, \ \exists G \in \mathscr{G}, \ F \subseteq G.$$

Entonces, para cada $q_F \in Q_{\mathscr{F}}$ existe $G \in \mathscr{G}$ tal que $F \subseteq G$. De acuerdo con la afirmación *ii)* de la Proposición 4.2.2, tenemos que $q_G \mid q_F$ en $\mathbb{Q}[V_n]$. Por lo tanto, se tiene que $Q_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$, y por tanto, $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$, como se quería.

Para probar el recíproco, supongamos que $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$ y tomemos $F \in \mathscr{F}$. Entonces, $q_F \in \mathfrak{q}_G$ y, por tanto, existen $\{f_G \ : \ G \in \mathscr{G}\} \subseteq \mathbb{Q}[V_n]$ tales que

$$q_F = \sum_{G \in \mathscr{G}} f_G q_G.$$

Como $\mathscr{B}_2$ es una base de $\mathbb{Q}[V_n]$ como espacio vectorial, para cada $G \in \mathscr{G}$ existen $\{\lambda_{Y,G} : Y \in V_n\} \subseteq \mathbb{Q}$ tales que

$$f_G := \sum_{Y \in V_n} \lambda_{Y,G} q_Y.$$

Por lo tanto, concluimos:

$$q_F = \sum_{G \in \mathscr{G}, Y \in V_n} \lambda_{Y,G} q_Y q_G = \sum_{G \in \mathscr{G}, Y \in V_n} \lambda_{Y,G} q_{Y \cap G}.$$

Si $F \not\subseteq G$ para cada $G \in \mathscr{G}$ tendríamos una combinación lineal no trivial de elementos de $\mathscr{B}_2$ igual a cero:

$$q_F + \sum_{G \in \mathscr{G}, Y \in V_n} (-\lambda_{Y,G}) q_{Y \cap G} = 0,$$

y lo anterior no es posible. Por tanto, debe existir algún $Y \in V_n$ y algún $G \in \mathscr{G}$ tales que $F = Y \cap G$. Por lo tanto, $F \subseteq G$ y el Lema queda probado. □

PROPOSICIÓN 4.3.4. *Sean $\mathscr{F},\mathscr{G} \subseteq 2^{[n]}$ dos subvariedades algebraicas de V_n. Entonces, las siguientes propiedades son equivalentes:*

i) $\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{\mathscr{G}}$.
ii) $\mathscr{F}^{(\max)} = \mathscr{G}^{(\max)}$.
iii) $\overline{\mathscr{F}}^{d} = \overline{\mathscr{G}}^{d}$.

En particular, la aplicación $\mathscr{F} \longmapsto \mathfrak{q}_{\mathscr{F}}$ es una biyección entre los subconjuntos de $2^{[n]}$ que están cerrados hacia abajos y los ideales de la forma $\mathfrak{q}_{\mathscr{F}}$.

DEMOSTRACIÓN. En primer lugar, la implicación $ii) \Longrightarrow i)$ se sigue directamente del Lema 4.3.1 anterior. Para probar la implicación $i) \Longrightarrow ii)$, supongamos que $\mathfrak{q}_{\mathscr{F}} = \mathfrak{q}_{\mathscr{G}}$ y tomemos $F \in \mathscr{F}^{(\max)}$. Por el Lema 4.3.3, como $\mathfrak{q}_{\mathscr{F}} \subseteq \mathfrak{q}_{\mathscr{G}}$, debe existir $G \in \mathscr{G}$ tal que $F \subseteq G$. Existirá también $G' \in \mathscr{G}^{(\max)}$ tal que $G \subseteq G'$. De nuevo, como se tiene también que $\mathfrak{q}_{\mathscr{G}} \subseteq \mathfrak{q}_{\mathscr{F}}$, debe existir $F' \in \mathscr{F}$ tal que $G' \subseteq F'$ y, entonces, $F \subseteq G \subseteq G' \subseteq F'$. Como $F \in \mathscr{F}^{(\max)}$ es maximal en $\mathscr{F}$, se tiene que $F = G = G' = F'$. En particular, $F = G' \in \mathscr{G}^{(\max)}$, obteniendo $\mathscr{F}^{(\max)} \subseteq \mathscr{G}^{(\max)}$. Intercambiando $\mathscr{G}^{(\max)}$ y $\mathscr{F}^{(\max)}$, concluimos la igualdad entre ambos conjuntos, y, por tanto, $ii)$ se sigue de $i)$. La equivalencia entre $ii)$ y $iii)$ es evidente ya que dos conjuntos $\mathscr{F},\mathscr{G} \subseteq 2^{[n]}$ tienen la misma clausura hacia abajo si y solo si sus elementos maximales son los mismos. □

Por último, el siguiente resultado explica la diferencia entre el ideal $\mathfrak{q}_{\mathscr{F}}$ y el subespacio vectorial $W_{\mathscr{F}}$.

COROLARIO 4.3.5. *Dado $\mathscr{F} \subseteq 2^{[n]}$, se satisface la siguiente igualdad:*

$$\dim_{\mathbb{Q}} \left(\mathfrak{q}_{\mathscr{F}}/W_{\mathscr{F}}\right) = \sharp\left(\overline{\mathscr{F}}^{d}\right) - \sharp\left(W_{\mathscr{F}}\right),$$

donde $\dim_{\mathbb{Q}}$ *significa la dimensión como $\mathbb{Q}-$espacio vectorial y $\mathfrak{q}_{\mathscr{F}}/W_{\mathscr{F}}$ denota al cociente como $\mathbb{Q}-$espacios vectoriales.*

DEMOSTRACIÓN. La prueba de este corolario es inmediata comparando la base $Q_{\overline{\mathscr{F}}^{d}}$ de $\mathfrak{q}_{\mathscr{F}}$ y la base $Q_{\mathscr{F}}$ de $W_{\mathscr{F}}$. □

4.4. Ideales monomiales en $\mathbb{Q}[V_n]$ y subvariedades algebraicas de V_n cerradas hacia arriba

Los ideales monomiales son un tema usual de investigación en métodos simbólicos utilizados en Geometría Algebraica Computacional (véase, por ejemplo, [Te,2004], [MiSt,2005]). Un ideal monomial en $\mathbb{Q}[V_n]$ es un ideal generado por un conjunto de algunos monomios de esta $\mathbb{Q}-$álgebra. Es decir, dado $\mathscr{F} \subseteq V_n$, el ideal monomial generado por los monomios asociados a $\mathscr{F}$ es el ideal:

$$\mathfrak{p}_{\mathscr{F}} := (p_F \ : \ F \in \mathscr{F}) \subseteq \mathbb{Q}[V_n].$$

Sea $\psi : \mathbb{Q}[V_n] \longrightarrow \mathbb{Q}[V_n]$ el isomorfismo de $\mathbb{Q}-$álgebras introducido en la Identidad (3.5.2). Se puede comprobar de manera sencilla que el anterior isomorfismo de $\mathbb{Q}-$álgebras satisface la siguiente identidad para todo $\mathscr{F} \subseteq V_n$:

$$\psi(\mathfrak{p}_{\mathscr{F}}) = \mathfrak{q}_{C(\mathscr{F})}, \tag{4.4.1}$$

donde $C(\mathscr{F}) := \{[n] \setminus S \in V_n \ : \ S \in \mathscr{F}\} \subseteq V_n$ es la clase formada por los complementarios de los conjuntos en $\mathscr{F}$. Esto motiva la idea de considerar subvariedades algebraicas de V_n que sean cerradas hacia arriba.

DEFINICIÓN 17 (**Cerrado hacia arriba**). *Con las notaciones precedentes, un subconjunto $\mathscr{F} \subseteq V_n$ es una subvariedad cerrada hacia arriba si se satisface la siguiente propiedad:*

$$\forall F \in \mathscr{F},\ \forall Y \in V_n,\ F \subseteq Y \implies Y \in \mathscr{F}.$$

Observamos que para cada $\mathscr{F} \subseteq V_n$, $\mathscr{F}$ es una subvariedad cerrada hacia arriba si y solo si $C(\mathscr{F})$ es una subvariedad cerrada hacia abajo. De manera similar a como hicimos en la sección anterior, podemos considerar la clausura hacia arriba de un subconjunto $\mathscr{F} \subseteq V_n$:

DEFINICIÓN 18 (**Clausura hacia arriba**). *Dado $\mathscr{F} \subseteq V_n$ definimos la clausura hacia arriba de $\mathscr{F}$ de la siguiente manera:*

$$\overline{\mathscr{F}}^{u} := \{Y \in V_n \ : \ \exists F \in \mathscr{F},\ F \subseteq Y\}. \tag{4.4.2}$$

Notemos que, en el caso de los átomos de la forma $\mathscr{F} := \{F\}$, la clausura hacia arriba toma la siguiente forma:

$$\overline{\{F\}}^u := \{Y \in V_n \ : \ F \subseteq Y\}.$$

De la misma forma, podemos considerar la clase $\mathscr{F}^{(\min)}$ de los subconjuntos minimales de un subconjunto $\mathscr{F} \subseteq V_n$ respecto de $\subseteq$. Se tiene que $\mathscr{F}$ es una subvariedad cerrada hacia arriba si y solo si se satisface la siguiente igualdad:

$$\overline{\mathscr{F}}^u = \bigcup_{F \in \mathscr{F}^{(\min)}} \overline{\{F\}}^u.$$

De hecho, observamos que se tiene la siguiente relación entre las clausuras hacia arriba y hacia abajo de cada $\mathscr{F} \subseteq V_n$:

$$\overline{\mathscr{F}}^u := C\left(\overline{C\left(\mathscr{F}\right)}^d\right).$$

Teniendo en cuenta las anteriores identidades, concluimos a partir de la Proposición 4.3.4 la siguiente relación entre ideales monomiales en $\mathbb{Q}[V_n]$ y subconjuntos cerrados hacia arriba en $2^{[n]}$:

PROPOSICIÓN 4.4.1. *Con las notaciones precedentes, sean $\mathscr{F}, \mathscr{G} \subseteq 2^{[n]}$ dos clases de subconjuntos de $[n]$. Entonces, los siguientes enunciados son equivalentes:*

i) Los ideales monomiales que generan son iguales, i.e. $\mathfrak{p}_{\mathscr{F}} = \mathfrak{p}_{\mathscr{G}}$.
ii) Ambos conjuntos tienen los mismo elementos minimales, i.e. $\mathscr{F}^{(\min)} = \mathscr{G}^{(\min)}$.
iii) Las clausuras hacia arriba de ambos conjuntos coinciden, i.e. $\overline{\mathscr{F}}^u = \overline{\mathscr{G}}^u$.

En particular, la aplicación $\mathscr{F} \longmapsto \mathfrak{p}_{\mathscr{F}}$ es una biyección entre los subconjuntos cerrados hacia arriba de $2^{[n]}$ y los ideales monomiales de $\mathbb{Q}[V_n]$.

Si bien esta sección no es utilizada para nuestra prueba del Lema de Sauer-Shelah-Perles, creemos que tiene importancia en la comprensión de la conexión entre ideales generados por elementos y las bases $\mathscr{B}_1$ y $\mathscr{B}_2$. Remarcamos que, aún sin perder de vista la importancia de la relación de los ideales monomiales y los ideales del tipo $\mathfrak{p}_{\mathscr{F}}$, solo usaremos en este trabajo aquello que concierna a los ideales $\mathfrak{q}_{\mathscr{F}}$ y a su relación con la combinatoria.

CAPíTULO 5

Dos nuevas demostraciones del Lema de Sauer-Shelah-Perles

Índice

5.1. Introducción

En este Capítulo culminaremos el Trabajo Fin de Grado escribiendo dos nuevas demostraciones del Lema de Sauer-Shelah-Perles. Concretando, probaremos el resultado siguiente:

LEMA 5.1.1 (**Lema de Sauer-Shelah-Perles**). *Con las notaciones introducidas en los capítulos precedentes, dado $\mathscr{F} \subseteq 2^{[n]}$, se tiene la siguiente desigualdad:*

$$\#(\mathscr{F}) \leq \sum_{i=0}^{VCD(\mathscr{F})} \binom{n}{i},$$

donde $VCD(\mathscr{F})$ denota la dimensión de Vapnik-Chervonenkis de $\mathscr{F}$.

Como ya se ha indicado, este es un resultado clásico de Combinatoria "extrema" que concita recurrentemente su interés por nuevas pruebas, en especial para la extensión a conjuntos de funciones no dicotómicas (i.e. cuyos valores no están en $\{0,1\}$). Muchos son los nombres que podemos citar, aunque no aportan mucho más a esta discusión. La mayoría de las pruebas conocidas son demostraciones por inducción y, cuando se tratan de generalizar, acaban en nociones incompletas como sucede con Natarajan o Pollard. Citemos, por ejemplo, el intento más reciente [**BCDMY,2022**] y sus referencias. Lo que sigue es sólo una contribución modesta más, inspirada en el trabajo de [**FrPa,1983**], pero dándole un contexto algebraico, y haciendo uso de la Fórmula (de Inversión) de la Traza, y de los resultados expuestos en Capítulos precedentes.

Comenzamos introduciendo una variante de la dimensión de Vapnik-Chervonenkis introducida en el Capítulo precedente. La denominaremos "dimensión, basada en el rango, de Vapnik-Chervonenkis" (abreviada mediante $RVCD$) porque utiliza el rango de una matriz asociada a las familias $Q_{\mathscr{F}}$ introducidas anteriormente. Esencialmente, dada $\mathscr{F} \subseteq V_n$ y dada la cadena ascendente de bolas de Hamming en V_n

$$W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq W_r \subsetneq \cdots \subsetneq V_n,$$

donde $W_i = \overline{B}_H(\mathbf{0}, r)$, consideramos las familias

$$Q_{\mathscr{F},r} := \{q_F\big|_{W_r} \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[W_r],$$

y los subespacios vectoriales $\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle \subseteq \mathbb{Q}[W_r]$ que generan. Se define RVCD de $\mathscr{F}$ como el valor mínimo r tal que

$$\dim_{\mathbb{Q}}(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle) = \dim_{\mathbb{Q}}(\mathbb{Q}\langle Q_{\mathscr{F},n}\rangle) = \dim_{\mathbb{Q}}(\mathbb{Q}\langle Q_{\mathscr{F}}\rangle) = \#(\mathscr{F}),$$

dado que las funciones polinomiales en $Q_{\mathscr{F}}$ son linealmente independientes. Así, si $r = RVCD(\mathscr{F})$, se tiene:

$$\#(\mathscr{F}) = \dim_{\mathbb{Q}}(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle) \leq \dim_{\mathbb{Q}}(\mathbb{Q}[W_r]).$$

Como $\dim_{\mathbb{Q}}(\mathbb{Q}[W_r]) = \#(W_r) = \sum_{i=0}^{r}\binom{n}{i}$, tenemos la determinación obvia del cardinal de $\mathscr{F}$ mediante

$$\#(\mathscr{F}) \leq \sum_{i=0}^{RVCD(\mathscr{F})}\binom{n}{i},$$

que es un preludio del Lema de Sauer-Shelah-Perles. La única diferencia es que, en esta desigualdad, el Lema de Sauer-Shelah-Perles hace aparecer $VCD(\mathscr{F})$ en lugar de $RVCD(\mathscr{F})$. Por tanto, todo lo que resta es probar la desigualdad

$$RVCD(\mathscr{F}) \leq VCD(\mathscr{F}).$$

Esto se hace mediante dos demostraciones distintas. En la Sección 5.2 se hace probando el Corolario 5.2.3 que usa la relación entre las funciones polinomiales atómicas $\chi_{\{Y\}}$ y las anti-monomiales q_Y.

En la Sección 5.3 se pretende ser más "purista" usando esencialmente las propiedades de dualidad ya descritas. Se definen dos transformadas duales:

$$\begin{array}{rccc} \mathscr{D}_1 := (\cdot)^*_{\mathscr{B}_1}: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & (f)^*_{\mathscr{B}_1}, \end{array}$$

$$\begin{array}{rccc} \mathscr{D}_2 := (\cdot)^*_{\mathscr{B}_2^*}: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & (f)^*_{\mathscr{B}_2^*}, \end{array}$$

usando, respectivamente, las bases $\mathscr{B}_1$ (monomial) y $\mathscr{B}_2^*$ (dual de la anti-monomial). Se prueba entonces el siguiente resultado:

PROPOSICIÓN 5.1.2. *Con las notaciones precedentes, $\mathscr{D}_2$ es la inversa de $\mathscr{D}_1$: Es decir, para cada $f \in \mathbb{Q}[V_n]$ se tiene que*

$$f = \mathscr{D}_1\left(\mathscr{D}_2\left(f\right)\right) = \mathscr{D}_2\left(\mathscr{D}_1\left(f\right)\right).$$

Además, para cada $Y \subseteq [n]$, las restricciones al ideal $\mathfrak{q}_Y$ de $\mathscr{D}_1$ y $\mathscr{D}_2$ son también automorfismos de $\mathbb{Q}-$espacios vectoriales sobre $\mathfrak{q}_Y$, uno inverso del otro.

Con este sencillo resultado, cuya prueba reposa en la Fórmula (de Inversión) de la Traza, resulta sencillo concluir que $RVCD(\mathscr{F}) \leq VCD(\mathscr{F})$ (como se hace en el Corolario 5.3.3) y, por tanto, cerrar una segunda prueba del Lema de Sauer-Shelah-Perles.

5.2. El ideal principal $\mathfrak{q}_Y$ y el Lema de Sauer-Shelah-Perles: La dimensión del Rango de Vapnik-Chervonenkis

Consideramos la siguiente cadena ascendente de bolas en V_n respecto de la distancia de Hamming:

$$W_0 \subsetneq W_1 \subsetneq \cdots \subsetneq W_r \subsetneq \cdots \subsetneq V_n,$$

donde $W_i := \overline{B}_H(\mathbf{0}, i) \subseteq V_n$ es la bola cerrada de centro $\mathbf{0} \in V_n$ y radio i respecto de la distancia de Hamming. Tomemos la clase $Q_{\mathscr{F}} \subseteq \mathbb{Q}[V_n]$ definida en la Identidad (4.2.4).
Dado $r \in \{0, \ldots, n\}$, podemos definir el siguiente subconjunto de funciones polinomiales:

$$Q_{\mathscr{F},r} := \{q_F\big|_{W_r} \ : \ F \in \mathscr{F}\} \subseteq \mathbb{Q}[W_r]. \tag{5.2.1}$$

Notamos que $Q_{\mathscr{F},n} = Q_{\mathscr{F}}$. Observamos también que toda inclusión $i_r : W_r \hookrightarrow W_{r+1}$ induce un epimorfismo natural de $\mathbb{Q}-$algebras:

$$\begin{array}{rccc} i_r^*: & \mathbb{Q}[W_{r+1}] & \longrightarrow & \mathbb{Q}[W_r] \\ & f & \longmapsto & f\big|_{W_r}. \end{array}$$

Por ende, la siguiente es una sucesión creciente de dimensiones:

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle\right) \leq \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},i+1}\rangle\right).$$

Por lo tanto, tiene sentido introducir la siguiente noción:

DEFINICIÓN 19 (**Dimensión del Rango de VC**). *Con las notaciones precedentes, definimos la Dimensión del Rango de VC de $\mathscr{F}$ como el mínimo r tal que $Q_{\mathscr{F},r}$ es una familia $\mathbb{Q}-$linealmente independiente de funciones polinomiales en $\mathbb{Q}[W_r]$. Es decir, el valor r mínimo tal que*

$$\dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},n}\rangle\right),$$

donde $\mathbb{Q}\langle Q_{\mathscr{F},i}\rangle$ es el subespacio vectorial generado por $Q_{\mathscr{F},i}$ en $\mathbb{Q}[W_i]$. Denotamos por $RVCD(\mathscr{F})$ a la Dimensión del Rango de VC de $\mathscr{F}$.

El término rango se utiliza debido a que $RVCD$ está relacionado con el rango de algunas matrices: Tomemos $N := \sharp(\mathscr{F}) \in \mathbb{N}$, y para cada entero no negativo $d \in \mathbb{N}$ definimos $\delta(d) := \deg(W_d) = \sharp(W_d)$. Ahora, consideremos $M_{\mathscr{F},d} \in \mathscr{M}_{N\times\delta(d)}(\mathbb{Q})$ la matriz cuyas filas $\rho_{F,d}$, para cada $F \in \mathscr{F}$, vienen dadas por la siguiente relación:

$$\rho_{F,d} := (q_F(S) \ : \ S \in W_d) \in \mathbb{Q}^{\delta(d)}.$$

Por lo tanto, la matriz se puede describir como:

$$M_{\mathscr{F},d} := (\rho_{F,d})_{F\in\mathscr{F}} \in \mathscr{M}_{N\times\delta(d)}(\mathbb{Q}).$$

El rango de esas matrices define claramente una función monótona creciente: Para cada d, se tiene que:

$$\operatorname{rank}(M_{\mathscr{F},d}) \leq \operatorname{rank}(M_{\mathscr{F},d+1}).$$

El siguiente lema muestra la relación entre el $RVCD$ y los rangos de esas matrices:

LEMA 5.2.1. *Con las notaciones precedentes, se tiene que*

i) $\operatorname{rank}(M_{\mathscr{F},n}) = \sharp(\mathscr{F})$.

ii) Se tiene que

$$\operatorname{rank}(M_{\mathscr{F},r}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right).$$

En particular, tenemos que

$$RVCD(\mathscr{F}) := \min\{r \in \{0,\dots,n\} \ : \ \operatorname{rank}(M_{\mathscr{F},r}) = \sharp(\mathscr{F})\}.$$

DEMOSTRACIÓN. La afirmación $i)$ es inmediata ($W_n = V_n$) y $ii)$ es una consecuencia casi inmediata del Teorema Chino de los Restos aplicado a $\mathbb{Q}[W_r]$ (véase la Identidad (2.2.2)): Tenemos un isomorfismo entre los elementos de $\mathbb{Q}[W_r]$ y los vectores formados por sus valores en los puntos de W_r:

$$q_F \longleftrightarrow \rho_{F,r} := (q_F(S) \ : \ S \in W_r) \in \mathbb{Q}^{\delta(r)}.$$

Por ende, la familia de elementos $Q_{\mathscr{F},r}$ es linealmente independiente en $\mathbb{Q}[W_r]$ si y solo si los siguientes son vectores linealmente independientes en $\mathbb{Q}^{\delta(r)}$:

$$\{\rho_{F,r} \ : \ F \in \mathscr{F}\}.$$

Esto es, simplemente, el enunciado $ii)$. La última igualdad es una consecuencia inmediata de $ii)$ y de la definición de $RVCD$. □

Estamos ahora en condiciones de probar el siguiente corolario:

COROLARIO 5.2.2. *Si $r = RVCD(\mathscr{F})$, entonces se tiene que $\sharp(\mathscr{F}) = \sharp(Q_{\mathscr{F},n}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right)$. Y, por tanto,*

$$\sharp(\mathscr{F}) = \dim_{\mathbb{Q}}\left(\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle\right) \leq \dim_{\mathbb{Q}}\left(\mathbb{Q}[W_r]\right) = \sharp\left(W_r\right) = \sum_{i=0}^{RVCD(\mathscr{F})} \binom{n}{i}.$$

DEMOSTRACIÓN. Es inmediato por las definiciones. Como $\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle$ es un subespacio vectorial de $\mathbb{Q}[W_r]$ y como la dimensión de $\mathbb{Q}\langle Q_{\mathscr{F},r}\rangle$ es igual al cardinal de $\mathscr{F}$, se tiene de manera obvia la desigualdad del enunciado. La última igualdad es evidente, ya que el cardinal de $\#(W_r)$ representa el número de subconjuntos de $[n]$ de cardinal menor o igual que r. □

Para concluir ahora la forma estándar del Lema de Sauer-Shelah-Perles, solo necesitamos probar que $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ para cada $\mathscr{F} \subseteq \mathbb{Q}[V_n]$. Este último paso se desarrolla en el siguiente corolario, que incluye la forma clásica del Lema de Sauer-Shelah-Perles:

COROLARIO 5.2.3. *Con estas notaciones, $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$ y, por tanto, la siguiente desigualdad se satisface:*

$$\sharp(\mathscr{F}) \leq \sum_{i=0}^{VCD(\mathscr{F})} \binom{n}{i}. \tag{5.2.2}$$

DEMOSTRACIÓN. Asumamos que $r = RVCD(\mathscr{F})$. Como $RVCD$ es un mínimo, tenemos que:

- La familia $Q_{\mathscr{F},r}$ es una familia $\mathbb{Q}-$linealmente independiente de elementos en $\mathbb{Q}[V_n]$.
- La familia $Q_{\mathscr{F},r-1}$ es una familia $\mathbb{Q}-$linealmente dependiente de elementos en $\mathbb{Q}[V_n]$.

Por lo tanto, existen $\underline{\lambda} := (\lambda_F \ : \ F \in \mathscr{F}) \in \mathbb{Q}^{\sharp(\mathscr{F})} \setminus \{\underline{0}\}$ tales que si consideramos $Q := \sum_{F\in\mathscr{F}} \lambda_F q_F \in \mathbb{Q}[V_n]$, las siguientes dos propiedades se satisfacen:

$$Q\big|_{W_r} \in \mathbb{Q}[W_r] \setminus \{0\}. \tag{5.2.3}$$

$$Q\big|_{W_{r-1}} \equiv 0. \tag{5.2.4}$$

Por lo tanto, debe existir algún $Y \in W_r \setminus W_{r-1}$ tal que $Q(Y) \neq 0$ y Q se anule en todos los subconjuntos propios de Y. Teniendo en cuenta lo anterior, consideremos $Qq_Y \in \mathfrak{q}_Y$. Se observa que la siguiente igualdad se satisface:

$$Q(Y)\chi_{\{Y\}} = Qq_Y,$$

donde $Q(Y) \in \mathbb{Q} \setminus \{0\}$ es un número racional no negativo. Vemos esta última igualdad en detalle:

- Si $T \subseteq [n]$ es tal que $T \not\subseteq Y$, entonces $q_Y(T) = 0$ y $Qq_Y(T) = 0$.
- Por otro lado, si $S \subsetneq Y$, entonces $Q(S) = 0$ y, por tanto, se tiene también que $Qq_Y(S) = 0$.
- Finalmente, $Qq_Y(Y) = Q(Y) = Q(Y)\chi_{\{Y\}}(Y)$, concluyendo que las dos funciones polinomiales que estábamos estudiando son iguales.

Por lo anterior, y usando la afirmación $i)$ de la Proposición 4.2.2 tenemos que:

$$Q(Y)\chi_{\{Y\}} = Qq_Y := \sum_{F\in\mathscr{F}} \lambda_F q_F q_Y = \sum_{F\in\mathscr{F}} \lambda_F q_{F\cap Y} = \sum_{S\subseteq Y} \left(\sum_{\substack{F\in\mathscr{F} \\ F\cap Y = S}} \lambda_F \right) q_S.$$

Por otro lado, de la Identidad (3.5.6) sabemos que:

$$\chi_{\{Y\}} := \sum_{S\subseteq Y} (-1)^{\sharp(Y\setminus S)} q_S.$$

Por lo tanto, como $\{q_S \ : \ S \subseteq Y\}$ es una familia linealmente independiente de funciones polinomiales, concluimos que para cada $S \subseteq Y$:

$$0 \neq Q(Y) \cdot (-1)^{\sharp(Y\setminus S)} = \left(\sum_{\substack{F\in\mathscr{F} \\ F\cap Y = S}} \lambda_F \right),$$

y por tanto, $\mathscr{F}$ fragmenta Y, con $\sharp(Y) = r$ (porque para cada $S \subseteq Y$, existe $F \in \mathscr{F}$ tal que $F \cap Y = S$, debido a que el sumatorio de escalares anterior es no nulo). Esto implica, por la definición de VCD, que $VCD(\mathscr{F}) \geq r$ como se pretendía. La desigualdad se sigue de manera directa de la dada en el Corolario 5.2.2. □

5.3. La transformada dual de Frankl-Pach

En esta sección, desarrollamos una prueba, distinta de la dada en la sección precedente, del Lema de Sauer-Shelah-Perles. Si bien esta prueba que se va a proporcionar es más compleja que la anterior, la incluimos en este trabajo por estar fuertemente inspirada en la ya nombrada prueba del Lema de Sauer-Shelah-Perles dada en [**FrPa,1983**].

Con todas las notaciones ya introducidas en secciones anteriores, consideramos las siguientes "transformadas duales":

- En primer lugar, consideramos la transformada dual inducida por la base $\mathscr{B}_1$:

$$\begin{array}{rccc} \mathscr{D}_1 := (\cdot)^*_{\mathscr{B}_1}: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & (f)^*_{\mathscr{B}_1}. \end{array}$$

- En segundo lugar, consideramos la transformada dual inducida por la base dual $\mathscr{B}_2^*$:

$$\begin{array}{rccc} \mathscr{D}_2 := (\cdot)^*_{\mathscr{B}_2^*}: & \mathbb{Q}[V_n] & \longrightarrow & \mathbb{Q}[V_n] \\ & f & \longmapsto & (f)^*_{\mathscr{B}_2^*}. \end{array}$$

Diremos que $\mathscr{D}_2$ es la Transformada Dual de Frankl-Pach. Esta terminología se ha elegido teniendo en cuenta que dicha transformada dual es el objeto que explica la contribución principal del trabajo [**FrPa,1983**].

LEMA 5.3.1. *Con las notaciones precedentes, para cada subconjunto $Y \subseteq [n]$, se tiene lo siguiente:*

i) Para cada $f \in \mathfrak{q}_Y$, $\mathscr{D}_1(f) \in \mathfrak{q}_Y$.
ii) Para cada $f \in \mathfrak{q}_Y$, $\mathscr{D}_2(f) \in \mathfrak{q}_Y$. Además, para cada $f \in \mathfrak{q}_Y$ se tiene la siguiente igualdad:

$$f = \sum_{W \subseteq Y} \mathscr{D}_2(f)(W) q_W, \quad \forall f \in \mathfrak{q}_Y. \tag{5.3.1}$$

DEMOSTRACIÓN. Probamos cada enunciado por separado:

- *i):* Por el apartado *i)* del Corolario 3.4.2, dados $f \in \mathfrak{q}_Y$ y $S \not\subseteq Y$, tenemos que:

$$\mathscr{D}_1(f)(S) = \sum_{S \subseteq T} f(T). \tag{5.3.2}$$

Notemos que, como $S \not\subseteq Y$, entonces $T \not\subseteq Y$, para cada $T \supseteq S$. Como $f \in \mathfrak{q}_Y$, concluimos que $f(T) = 0$, para cada $T \supseteq S$ y la ecuación (5.3.2) implica $\mathscr{D}_1(f)(S) = 0$ para cada $S \not\subseteq Y$. Por lo tanto, por el Lema 4.2.1 concluimos que $\mathscr{D}_1(f) \in \mathfrak{q}_Y$ y se tiene el resultado.

- *ii):* Finalmente, debido a *iv)* de la Proposición 4.2.2 sabemos que $\mathscr{B}_{2,Y} := \{q_W : W \subseteq Y\}$ es una base de $\mathfrak{q}_Y$ como $\mathbb{Q}-$espacio vectorial. Por ende, para cada $f \in \mathfrak{q}_Y$ tenemos que:

$$f = \sum_{W \subseteq Y} \mu_W q_W,$$

para algún $\mu_W \in \mathbb{Q}$. Entonces, si $S \subseteq [n]$ es tal que $S \not\subseteq Y$ tenemos que:

$$\mathscr{D}_2(f)(S) := \mathrm{Tr}_n(f, q_S^*) = \sum_{W \subseteq Y} \mu_W \mathrm{Tr}_n(q_W, q_S^*) = 0,$$

porque $\mathscr{B}_2^*$ es una base dual de $\mathscr{B}_2$. Por lo tanto, por el Lema 4.2.1 concluimos que $\mathscr{D}_2(f) \in \mathfrak{q}_Y$. Adicionalmente, para cada $W \subseteq Y$, concluimos también que

$$\mu_W := \mathrm{Tr}_n(f, q_W^*) = \mathscr{D}_2(f)(W),$$

lo que implica la Identidad (5.3.1).

□

PROPOSICIÓN 5.3.2. *Con las notaciones precedentes, $\mathscr{D}_2$ es la inversa de $\mathscr{D}_1$: Es decir, para cada $f \in \mathbb{Q}[V_n]$ se tiene que*

$$f = \mathscr{D}_1(\mathscr{D}_2(f)) = \mathscr{D}_2(\mathscr{D}_1(f)) = \sum_{S \subseteq [n]} f^*_{\mathscr{B}_1}(S) p_S^* = \sum_{S \subseteq [n]} f^*_{\mathscr{B}_2}(S) q_S^*.$$

Además, para cada $Y \subseteq [n]$, las restricciones al ideal $\mathfrak{q}_Y$ de $\mathscr{D}_1$ y $\mathscr{D}_2$ son también automorfismos de $\mathbb{Q}-$espacios vectoriales sobre $\mathfrak{q}_Y$, uno inverso del otro.

DEMOSTRACIÓN. Por el apartado *i)* del Corolario 3.4.2 y para cada $W \subseteq [n]$, lo siguiente se satisface:

$$\mathscr{D}_1(\mathscr{D}_2(f))(W) = \mathrm{Tr}_n(\mathscr{D}_2(f), p_W) = \sum_{W \subseteq S} \mathscr{D}_2(f)(S).$$

Como $q_S(W) = 1$ si $W \subseteq S$ (véase la afirmación i) de la Proposición 3.5.1) concluimos que:

$$\mathscr{D}_1\left(\mathscr{D}_2\left(f\right)\right)(W) = \sum_{S \subseteq Y} \mathscr{D}_2(f)(S) q_S(W).$$

Se sigue, por la Fórmula (de Inversión) de la Traza, lo siguiente:

$$\mathscr{D}_1\left(\mathscr{D}_2\left(f\right)\right)(W) = f(W).$$

Por lo tanto, $\mathscr{D}_2 \circ \mathscr{D}_1(f) = f$ para cada $f \in \mathbb{Q}[V_n]$. Como los anteriores son $\mathbb{Q}-$automorfismos lineales, también tenemos $\mathscr{D}_1 \circ \mathscr{D}_2(f) = f$ para cada $f \in \mathbb{Q}[V_n]$ y se tiene el resultado. Las dos últimas igualdades son simplemente la Fórmula (de Inversión) de la Traza aplicada respectivamente a $\mathscr{B}_1$ y $\mathscr{B}_2$. La última frase de la Proposición se sigue de manera inmediata del Lema 5.3.1. □

Nuestro último resultado es una prueba alternativa de la desigualdad $VCD(\mathscr{F}) \geq RVCD(\mathscr{F})$. Vamos a aplicar la Proposición anterior (inspirada en [**FrPa,1983**]) para dar otra prueba del Lema de Sauer-Shelah-Perles. Notamos que, en la siguiente prueba, solo se usarán técnicas de dualidad en su forma más pura. Seguimos las notaciones de la Sección 5.2 precedente.

Corolario 5.3.3. *Con las notaciones precedentes, dado $Y \subseteq [n]$ tal que $r = \sharp(Y) = RVCD(\mathscr{F})$, entonces $\mathscr{F}$ fragmenta Y y $VCD(\mathscr{F}) \geq r$.*

Demostración. Como ya se ha visto, si $r = \sharp(Y) = RVCD(\mathscr{F})$, existe una lista de coeficientes racionales $\underline{\lambda} = (\lambda_F : F \in \mathscr{F}) \in \mathbb{Q}^{\#(\mathscr{F})} \setminus \{0\}$ tal que la siguiente función polinomial

$$Q := Q_{\underline{\lambda}} := \sum_{F \in \mathscr{F}} \lambda_F q_F \in \mathbb{Q}[V_n] \setminus \{0\},$$

es no nula en $\mathbb{Q}[V_n]$ con $Q(Y) \neq 0$, anulándose además en todo subconjunto propio $S \subsetneq Y$.

Tras esto, consideremos $S \subseteq Y$ y observemos que para cada $W \subseteq [n]$, tenemos que $\mathscr{D}_2(q_S)(W) = \mathrm{Tr}_n(q_S, q_W^*) = \delta_{S,W}$. En otras palabras,

$$\mathscr{D}_2(q_S) = \chi_{\{S\}}, \quad \forall S \subseteq Y.$$

Consideremos $G := \mathscr{D}_2(Qq_Y) \in \mathfrak{q}_Y$ y denotemos por $f := \mathscr{D}_1(G) = Qq_Y \in \mathfrak{q}_Y$.
Aplicando iii) del Corolario 3.4.2, podemos concluir fácilmente que para cada $S \subseteq [n]$, se tiene:

$$G(S) := \sum_{S \subseteq T \subseteq [n]} (-1)^{\sharp(T \setminus S)} \mathscr{D}_1(G)(T).$$

Como $\mathscr{D}_1(G) = \mathscr{D}_1(\mathscr{D}_2(f)) = f = Qq_Y$, concluimos que, como Q se anula en todos los subconjuntos propios de Y,

$$G(S) := \sum_{S \subseteq T \subseteq Y} (-1)^{\sharp(T \setminus S)} f(T) = (-1)^{\sharp(Y \setminus S)} f(Y) = (-1)^{\sharp(Y \setminus S)} Q(Y) \neq 0.$$

Por otra parte, como en el Corolario 5.2.3, tenemos que

$$G = \mathscr{D}_2(f) = \mathscr{D}_2(Qq_Y) = \mathscr{D}_2\left(\sum_{F \in \mathscr{F}} \lambda_F q_F q_Y\right) = \mathscr{D}_2\left(\sum_{F \in \mathscr{F}} \lambda_F q_{F \cap Y}\right).$$

Como $\mathscr{D}_2$ es lineal tenemos que

$$G := \sum_{S \subseteq Y} \left(\sum_{\substack{F \in \mathscr{F} \\ F \cap Y = S}} \lambda_F\right) \mathscr{D}_2(q_S) = \sum_{S \subseteq Y} \left(\sum_{\substack{F \in \mathscr{F} \\ F \cap Y = S}} \lambda_F\right) \chi_{\{S\}}.$$

Por lo tanto, para cada $S \subseteq Y$,

$$\mathscr{D}_2(f)(S) = \left(\sum_{\substack{F \in \mathscr{F} \\ F \cap Y = S}} \lambda_F\right) = G(S) = (-1)^{\sharp(Y \setminus S)} Q(Y) \neq 0,$$

y, en consecuencia, Y está fragmentado por $\mathscr{F}$ (porque para cada $S \subseteq Y$, existe $F \in \mathscr{F}$ tal que $F \cap Y = S$, debido a que el sumatorio de escalares anterior es no nulo). Por lo tanto, $VCD(\mathscr{F}) \geq \sharp(Y)$ y el resultado se sigue. □

La prueba anterior difiere de la expuesta en la Sección 5.2 en que se omite el tratamiento de $f := Qq_Y$. En vez de eso, solo usaremos la Proposición 5.3.2 y técnicas de dualidad. Si bien la prueba de la Sección 5.2 puede ser más simple que la proporcionada justo anteriormente, la dada es esta sección sigue la línea argumental subyacente (ímplicita pero no explícita) en [**FrPa,1983**], y por eso creemos en la importancia de incluirla.

APÉNDICE A

Resultados de álgebra conmutativa implícitos en los Capítulos 1 y 2

Índice

A.1. El concepto de $R-$álgebra

Dado R un anillo, recordamos la Definición de $R-$álgebra:

DEFINICIÓN 20 (**$R-$álgebra**). *Dados R y A anillos, si $f : R \to A$ es un morfismo de anillos, decimos que A es una $R-$álgebra.*

Podemos dotar a toda $R-$álgebra de una estructura de $R-$módulo de manera natural:

PROPOSICIÓN A.1.1. *Dados R, B anillos, sea $f : R \to B$ un morfismo de anillos (o, equivalentemente, una estructura de $R-$álgebra sobre B). Podemos definir sobre B una estructura de R-módulo sobre B mediante:*

$$\begin{array}{rccc} \star_f : & R \times B & \to & B \\ & (x, b) & \mapsto & x \star_f b := f(x) \cdot_B b, \end{array}$$

donde $\cdot_B$ es el producto de B como anillo.

Damos algo más de terminología:

DEFINICIÓN 21. *Con las notaciones precedentes,*

- *Una $R-$álgebra se dice finitamente generada si es isomorfa a un cociente de algún anillo de polinomios $R[X_1, \ldots, X_n]$ por alguno de sus ideales.*
- *Una $R-$álgebra se dice finita si es un $R-$módulo finitamente generado (haciendo referencia a la estructura de $R-$módulo ya introducida).*

A.2. El Teorema Chino de los Restos

Enunciamos el conocido Teorema Chino de los Restos. Una prueba de este resultado troncal puede encontrarse en [**Pa,2022**]:

TEOREMA A.2.1 (**Teorema Chino de los Restos**). *Sea $\{\mathfrak{a}_i : 1 \leq i \leq n\}$ un conjunto finito de ideales de un anillo R. Supongamos que son dos a dos co-maximales (i.e. $\mathfrak{a}_i + \mathfrak{a}_j = R$, $\forall i \neq j$) y consideremos el morfismo de anillos:*

$$\begin{array}{rccc} \Phi : & R & \longrightarrow & \prod_{i=1}^n (R/\mathfrak{a}_i) \\ & a & \longmapsto & (a + \mathfrak{a}_1, a + \mathfrak{a}_2, \ldots, a + \mathfrak{a}_n). \end{array}$$

Se tiene:

i) Φ es un epimorfismo de anillos.
ii) El núcleo verifica:

$$\ker(\Phi) = \bigcap_{i=1}^n \mathfrak{a}_i = \prod_{i=1}^n \mathfrak{a}_i.$$

iii) Φ induce un isomorfismo de anillos:

$$\begin{array}{rccc} \Phi: & R/\left(\bigcap_{i=1}^n \mathfrak{a}_i\right) & \longrightarrow & \prod_{i=1}^n (R/\mathfrak{a}_i) \\ & x+\left(\bigcap_{i=1}^n \mathfrak{a}_i\right) & \longmapsto & (x+\mathfrak{a}_1, x+\mathfrak{a}_2, \ldots, x+\mathfrak{a}_n). \end{array}$$

A.3. El radical de Jacobson

La siguiente noción fue introducida por N. Jacobson en [**Ja,1945**] y, a partir de [**Kr,1951**], pasó a conocerse como el radical de Jacobson.

DEFINICIÓN 22 (**Radical de Jacobson**). *Sea $\mathfrak{a}$ un ideal de un anillo R. Llamaremos radical de Jacobson de $\mathfrak{a}$ a la intersección de todos los ideales maximales de R que contienen a $\mathfrak{a}$. Es decir,*

$$\sqrt[J]{\mathfrak{a}} := \bigcap \{\mathfrak{m} \in MaxSpec(R) \ : \ \mathfrak{m} \supseteq \mathfrak{a}\}.$$

Se denomina radical de Jacobson del anillo R al radical de Jacobson del ideal (0).

OBSERVACIÓN A.3.1. Se tiene la siguiente inclusión obvia:

$$\sqrt{\mathfrak{a}} = \bigcap \{\mathfrak{p} \in Spec(R) \ : \ \mathfrak{p} \supseteq \mathfrak{a}\} \subseteq \sqrt[J]{\mathfrak{a}}.$$

La igualdad no siempre se verifica.

La siguiente es una de las propiedades al uso:

PROPOSICIÓN A.3.2. *Sea $\mathfrak{N}_R = \sqrt[J]{(0)}$ el radical de Jacobson de un anillo R. Se tiene:*

$$x \in \mathfrak{N}_R \Longleftrightarrow 1 - xy \in R^\times, \ \forall y \in R.$$

DEMOSTRACIÓN. Véase [**AtMc,1969**],[**Pa,2022**]. □

DEFINICIÓN 23 (**Anillo de Jacobson**). *Un anillo R se dice anillo de Jacobson si para cada ideal propio $\mathfrak{a}$ se verifica la siguiente igualdad:*

$$\sqrt{\mathfrak{a}} = \sqrt[J]{\mathfrak{a}}.$$

PROPOSICIÓN A.3.3. *Sea K un cuerpo algebraicamente cerrado y $V \subseteq \mathbb{A}^n(K)$ una variedad algebraica. Entonces, $K[V]$ es un anillo de Jacobson. En particular, bajo estas hipótesis, $K[X_1, \ldots, X_n]$ es un anillo de Jacobson.*

DEMOSTRACIÓN. Probemos el resultado para $K[X_1, \ldots, X_n]$ y el resultado general se sigue de manera obvia. Es claro que $\sqrt{\mathfrak{a}} \subseteq \sqrt[J]{\mathfrak{a}}$ porque esta propiedad se sigue para cualquier anillo. Se trata de probar el otro contenido. Para ello, consideremos $f \in K[X_1, \ldots, X_n]$ tal que $f \notin \sqrt{\mathfrak{a}}$. Sea $V = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}) \subseteq \mathbb{A}^n(K)$, la variedad algebraica asociada. Por el Teorema de Rabinowitsch, $f \notin I(V)$. En particular, existe un punto $\zeta \in V$ que no está en la hipersuperficie $V_{\mathbb{A}}(f)$ (o, equivalentemente, existe un punto $\zeta \in V(\mathfrak{a})$ tal que $f(\zeta) \neq 0$). Por tanto, $f \notin \mathfrak{m}_\zeta \in MaxSpec(K[X_1, \ldots, X_n])$, donde $\mathfrak{m}_\zeta$ es el ideal maximal en $K[X_1, \ldots, X_n]$ asociado al punto ζ. Como $\zeta \in V(\mathfrak{a})$, entonces $\mathfrak{m}_\zeta \supseteq \mathfrak{a}$ y habremos concluido que existe un ideal maximal que contiene a $\mathfrak{a}$ y no contiene a f. por tanto, $f \notin \sqrt[J]{\mathfrak{a}}$ y hemos probado el segundo contenido buscado. □

A.4. El producto tensorial de $R-$módulos

En esta sección, dado R un anillo, desarrollamos el concepto de producto tensorial de $R-$módulos. Nos basamos principalmente en [**Pa,2022**].

Recordamos la definición de función multilineal: Dada $M_1, M_2, \ldots, M_p, N$ una lista finita de $R-$módulos, una aplicación $f : M_1 \times M_2 \times \cdots \times M_p \to N$ se dice multilineal si es lineal en cada coordenada. El objetivo de introducir el concepto de producto tensorial de una lista finita de $R-$módulos $M_1, M_2, \ldots, M_p$ es el introducir un $R-$módulo T, solamente dependiente de $M_1, M_2, \ldots, M_p$, tal que para cada $R-$módulo N, las funciones multilineales entre $M_1, M_2, \ldots, M_p$ y N se puedan ver como morfismos de $R-$módulos entre T y N. Es dicho $R-$módulo T lo que llamaremos producto tensorial de $M_1, M_2, \ldots, M_p$. Denotaremos a dicho producto tensorial por $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p$ y se caracteriza justamente por ser isomorfo

como $R-$módulo al $R-$módulo que forman las funciones multilineales (en [Pa,2022] se detalla la manera de dotar a dicho conjunto de estructura de $R-$módulo), i.e.,

$$Hom_R(M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p, N) \cong \text{Multi} - \text{lin}(M_1, M_2, \ldots, M_p).$$

Pasamos a definir ahora, como tal, el producto tensorial de $R-$módulos mediante una Propiedad Universal.

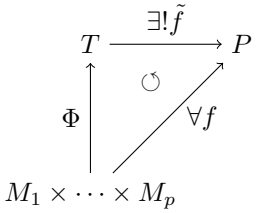
TEOREMA A.4.1 (**Producto tensorial de $R-$módulos**). *Sean $M_1, M_2, \ldots, M_p$ dos R-módulos. Entonces, existe un par (T, Φ) formado por un R-módulo T y una aplicación multilineal*

$$\Phi : M_1 \times \cdots \times M_p \to T,$$

tal que se verifica la siguiente propiedad:
Para todo otro R-módulo P y para toda aplicación multilineal

$$f : M_1 \times \cdots \times M_p \to P,$$

existe un único morfismo de R-módulos $\tilde{f} \in Hom_R(T, P)$ tal que el siguiente diagrama es conmutativo:



Además, existe un único (salvo isomorfismo) par (T, Φ) que satisface esta propiedad y que llamaremos producto tensorial de los R-módulos M y N. Denotaremos a ese único R-módulo mediante $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p$ y a la aplicación bilineal Φ la denotaremos mediante:

$$\begin{array}{rccc} \otimes^{(p)} : & M_1 \times \cdots \times M_p & \to & M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p \\ & (x_1, \ldots, x_p) & \mapsto & x_1 \otimes \cdots \otimes x_p, \end{array}$$

y su imagen será un sistema generador de $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p$. Llamaremos al par $(M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p, \otimes^{(p)})$ producto tensorial de los $R-$módulos $M_1, \ldots, M_p$. Usualmente, simplicaremos escribiendo simplemente $M_1 \otimes_R M_2 \otimes_R \cdots \otimes_R M_p$, dando por sobre-entendida la aplicación multilineal.

DEMOSTRACIÓN. Véase [Pa,2022]. □

Por lo visto en la Sección A.1 precedente, podemos particularizar toda la discusión anterior para el caso de $R-$álgebras, ya que podemos dotarlas de manera natural de una estructura de $R-$módulo.

Dados sistemas generadores de una lista finita de $R-$módulos, podemos construir, aprovechando la multi-linealidad de $\otimes^{(p)}$, un sistema generador del producto tensorial de los mismos:

PROPOSICIÓN A.4.2. *Sean dados $M_1, \ldots, M_p$ una familia de $R-$módulos. Supongamos que para cada i, $1 \leq i \leq p$, tenemos un subconjunto $\mathcal{F}_i \subseteq M_i$, que es sistema generador de M_i como $R-$módulo. Entonces, el siguiente conjunto es un sistema generador del producto tensorial $M_1 \otimes_R \cdots \otimes_R M_p$:*

$$\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_p := \{e_1 \otimes \cdots \otimes e_p : e_i \in \mathcal{F}_i, 1 \leq i \leq p\}.$$

DEMOSTRACIÓN. Véase [Pa,2022]. □

Enunciamos algunas propiedades útiles del producto tensorial:

PROPOSICIÓN A.4.3. *Dado R un anillo, se tienen las siguientes propiedades:*

i) Dados M, N dos $R-$módulos,

$$M \otimes_R N \cong N \otimes_R M.$$

ii) Dado M un $R-$módulo,

$$R \otimes_R M \cong M.$$

iii) Dada una familia $\{M_i : i \in I\}$ de $R-$módulos y dado N un $R-$módulo, se tiene:

$$\left(\bigoplus_{i\in I} M_i\right) \otimes_R N \cong \bigoplus_{i\in I}(M_i \otimes_R N).$$

En particular, si M y N son $R-$módulos libres, también es $R-$módulo libre $M \otimes_R N$ y, en el caso de $R-$módulos libres de rango finito, tendremos:

$$\operatorname{rank}(M \otimes_R N) = \operatorname{rank}(M) \cdot \operatorname{rank}(N).$$

DEMOSTRACIÓN. Véase [Pa,2022]. □

Planteamos una última construcción: Dados R, T dos anillos y M un $R-$módulo, podemos definir una estructura de $T-$módulo en $T \otimes_R M$ del modo siguiente:

$$\begin{array}{rccc} \cdot_T : & T \times (T \otimes_R M) & \longrightarrow & T \otimes_R M \\ & \left(\lambda, \sum_{i\in I} x_i \otimes m_i\right) & \longmapsto & \sum_{i\in I}(\lambda x_i) \otimes m_i, \end{array}$$

para cada conjunto finito I, con $x_i \in T$, $m_i \in M$.

Además, teniendo en cuenta lo anterior, si M es finitamente generado, entonces $T \otimes_R M$ es un $T-$módulo finitamente generado. De hecho, si $\{m_i : i \in J\}$ es un sistema generador de M como $R-$módulo, entonces el siguiente conjunto

$$\{1_T \otimes m_i : i \in J\},$$

es un sistema generador de $T \otimes_R M$ como $T-$módulo. Se dice que $T \otimes_R M$ es el módulo obtenido de M mediante *extensión de escalares.*

Enunciamos un teorema que describe las funciones polinomiales sobre el producto cartesiano de variedades algebraicas:

TEOREMA A.4.4. *Sea K un cuerpo y $\mathbb{K}$ su clausura algebraica. Sean $V \subseteq \mathbb{A}^n(\mathbb{K})$, $W \subseteq \mathbb{A}^n(\mathbb{K})$ dos subvariedades algebraicas respectivamente de los espacios afines $\mathbb{A}^n(\mathbb{K})$ y $\mathbb{A}^m(\mathbb{K})$. Entonces, el siguiente es un isomorfismo de $K-$álgebras:*

$$K[V] \otimes_K K[W] \cong K[V \times W],$$

donde $K[V]$, $K[W]$ y $K[V \times W]$ son, respectivamente, las $K-$álgebras de aplicaciones polinomiales $K-$definibles de V, W y $V \times W$ en K.

DEMOSTRACIÓN. Véase [Pa,2022]. □

Bibliografía

[Ar,1927] E. Artin, *Zur Theorie der hyperkomplexen Zahlen.* Abhandlugngen math. seminar Hamburg 5 (1927), 251-260.

[AtMc,1969] M.F. Atiyah, I.G. MacDonald,*"Introduction to Commutative Algebra"*. Addison-Wesley, 1969.

[BCDMY,2022] N. Brukhim, D. Carmon, I. Dinur, S. Moran, A. Yehudayoff, *A characterization of Multiclass Learnability.* (2022) ArXiv 2203.01550.

[Co,1992] D. A. Cox, J. Little, D. O'Shea, *"Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra"*. Springer Verlag, 1992.

[DeFr,1982] M. Deza, P. Frankl, *On the vector space of 0-configurations* Combinatorica **2** (1982), 341-345.

[Fr,1983] P. Frankl, *On the Trace of Finite Sets.* J. of Combinatorial Theory, Series A, **34** (1983), 41-45.

[FrPa,1983] P. Frankl, J. Pach, *On the number of sets in a null t-design.* European J. Combinatorics **4** (1983), 21-23.

[Ha,1995] D. Haussler, *Sphere packing numbers for subsets of the Boolean n-cube with bounded Vapnik-Chervonenkis dimension.* J. Comb. Theory, Ser. A **69** (1995), 217-232.

[He,1983] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields.* Theoret. Comput. Sci. **24** (1983), 239-277.

[Ho,1889] O. Hölder, *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen.* Math. Ann. **34** (1889), 26-56.

[HWLW,2017] L. Hu, R. Wu, T. Li, L. Wang, *Quadratic Upper Bound for Recursive Teaching Dimension of Finite VC Classes.* Proceedings of Machine Learning Research vol **65** (2017), 1–10.

[Ja,1945] N. Jacobson, *The radical and semi-simplicity for arbitrary rings.* Amer. Journal of Math. **67** (1945), 300-320.

[Jo,1869] C. Jordan, "*Théorème sur les équations algébriques*". C.R. Acad. Sci. Paris **68** (1869), 257-258.

[Jo,1870] C. Jordan, "*Traité des substitutions et des équations algébriques*". Gauthier-Villars, Paris, 1870.

[Kr,1951] W. Krull, *Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie.* Mathematische Zeitschrift, **54** (1951), 354-387.

[MiSt,2005] E. Miller, B. Sturmfels, *"Combinatorial Commutative Algebra"*, Graduate Texts in Mathematics, vol. **227**, New York: Springer-Verlag, 2005.

[Na,1989] B.K. Natarajan, *On Learning sets and functions.* Machine Learning. **4** (1989), 67–97.

[Pa,1995] L. M. Pardo, *How lower and upper complexity bounds meet in elimination theory.* In "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes" , G. Cohen, M. Giusti & T. Mora, eds., Lecture Notes in Computer Science **948** , Springer Verlag, 1995, 33-69.

[Pa,2022] L.M. Pardo, *"Notas para un Curso Básico de Álgebra Conmutativa"*. Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria. Curso 2022/23.

[Pa,2023] L.M. Pardo, *Exploring implications of Trace (Inversion) Formula an Artin algebras in extreme Combinatorics.* To appear in Applicable Algebra in Engineering, Communications and Computing, 2023.

[PaSe, 2022] L.M. Pardo, D. Sebastián, *A promenade through correct test sequences I: Degree of constructible sets, Bézout's Inequality and density.* J. of Complexity **68** (2022), 101588.

[Sa,1972] N. Sauer, *On the density of families of sets.* J. of Combinatorial Theory, Series A, **13** (1972), 145–147.

[Sc,1928] O. Schreier, *Ueber den Jordan-Hölderschen Satz.* Abh. Math. Sem. Univ. Hamburg **6** (1928), 300-302.

[Sh,1972] S. Shelah, *A combinatorial problem; stability and order for models and theories in infinitary languages.* Pacific J. of Mathematics **41** (1972) 247–261.

[Ta,2014] T. Tao, *Algebraic Combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory.* EMS Surveys Math. Sci. **1** (2014), 1-46.

[Te,2004] B. Teissier, *Monomial Ideals, Binomial Ideals, Polynomial Ideals.* In "Trends in Commutative Algebra", MSRI Publications **21**, 2004, 211- 246.

[VaCh,1971] V. N. Vapnik, A. Ya. Chervonenkis, *On the uniform Convergence of relative Frequencies of rvents to their probabilities.* Theory Probab. Appl. **16** (1971), 264–280.

[VdW, 1985] B.L. van der Waerden, "*The History of Algebra*". Springer, 1985.

[Za,2022] U. Zabaleta Gañán, *"Redes Neuronales con Función de Activación Racional: Función de Crecimiento y Erzeugungsgrad"*. Trabajo Fin de Grado en Matemáticas, Facultad de Ciencias, Universidad de Cantabria, 2022. Repositorio UCrea.