UNIVERSIDAD DE GUANAJUATO

Momentos del grupo unitario

Tesis presentada como requisito parcial para obtener el título de:
Licenciado en Matemáticas

Gustavo Adolfo García Gutiérrez

Director de Tesis:
Dr. Carlos Vargas Obieta

Universidad de Guanajuato
Departamento de Matemáticas
Guanajuato, México
2019

Índice general

Introducción

En el artículo de Biane [3] se iniciaron a estudiar las relaciones entre la probabilidad no conmutativa y la teoría asintótica de representaciones. En ese trabajo se mostró que el comportamiento asintótico de los caracteres normalizados de representaciones de grupos simétricos pueden explicarse usando los cumulantes libres de una medida asociada la representación. Es decir, se utilizaron herramientas de probabilidad no conmutativa para entender el comportamiento asintótico de representaciones de grupos simétricos. También hay resultados en la otra dirección. En [6] Collins muestra como la teoría de representaciones del grupo simétrico puede usarse para calcular la distribución conjunta de las entradas de una matriz unitaria. Esto permite mejorar resultados de [15] sobre la independencia libre asintótica entre matrices deterministicas y matrices Haar unitarias.

Esta tesis trata de representaciones de grupos, principalmente del grupo simétrico S_n y el grupo unitario $U(d)$ y una de sus aplicaciones a la teoría de probabilidad no conmutativa. Como habíamos mencionado, la relación entre probabilidad no conmutativa y teoría de representaciones de grupos es simbiotica. En [3] se muestra que la probabilidad libre y la teoría de representaciones de grupos simétricos se encuentran relacionadas. Mas precisamente en virtud de la llamada transformada de Markov que le asocia una medida de probabilidad a un diagrama de Young. Biane muestra que operaciones de representaciones irreducibles de grupos simétricos grandes se comportan estadísticamente cercanas a operaciones entre variables aleatorias libres asociadas a los diagramas correspondientes. De esta forma Biane esclarece la aparición del diagrama del semicírculo en los trabajos previos de Kerov en [14] [10] al considerar cadenas de Markov valuadas en diagramas de Young con la medida de Plancherel como medida de transición.
Algunos años después Collins mostró que los cálculos combinatorios que muestran la independencia libre asintótica combinatoria de Voiculescu [15] puede mejorarse basándose en los trabajos previos de Biane [4] y Xu [18] y en el cálculo de la expansión de la función de Weingarten. La tesis se enfoca en esta segunda dirección, y se basa principalmente en el artículo de Collins y Sniady [5] . Uno de los objetivos principales es presentar todo el material de manera autocontenida, en la medida de lo posible, para que sea accesible tanto para los lectores interesados en matrices aleatorias y probabilidad no conmutativa como para los lectores interesados en teoría de representaciones.

Para cubrir el material requerido en teoría de representaciones en el capítulo 1 introducimos la definición de representación lineal un grupo, el concepto de representación irreducible y caracter. Además de presentar algunos resultados clásicos se prueba la existencia de una descomposición canónica de una representación. A esta la llamamos descomposición en componentes isotípicas y se da la fórmula para las proyecciones asociadas a esta. Para finalizar aterrizamos todos estos conceptos aplicándolos a la representación regular de un grupo.

Uno de los problemas que nos topamos al querer calcular los momentos del grupo unitario es que el álgebra del grupo unitario no tiene dimensión finita, una de las observaciones que hicieron Collins y Sniady en su artículo del 2006 es que los momentos de orden n de este solo dependen de la imagen del álgebra $\mathbb{C}[G]$ bajo un homomorfismo de álgebras (representación) dentro de un álgebra de dimensión finita.

Es por eso que en capítulo 2 se presentan resultados sobre la teoría de álgebras semisimples de dimensión finita y se explica como esto generaliza a la teoría de representaciones de grupos finitos. También se prueban dos resultados que serán fundamentales para entender la relación entre el grupo simétrico y el grupo unitario. Primero se presenta el teorema de Wedderburn que clasifica las álgebras semisimples de dimensión finita, lo que nos ayuda a entender sus representaciones. Además se prueba que la descomposición de Wedderburn de un álgebra de grupo coincide con la descomposición isotípica de la representación regular. Por último probamos el teorema del doble conmutador, un fenómeno de dualidad entre un álgebra y su conmutador, que nos permite entender las representaciones de un álgebra si conocemos las representaciones de su conmutador. Esto se usa mas adelante usaremos para mostrar una correspondencia entre representaciones del grupo unitario con representaciones del grupo simétrico: La dualidad de Schur-Weyl.

En el capítulo 3 se introduce la definición de espacio de probabilidad no conmutativo y algunos de los conceptos fundamentales sobre probabilidad no conmutativa como lo son momentos, cumulantes, distribución (álgebraica y analítica) de variables aleatorias no conmutativas y esperanzas condicionales. También se presentan algunos ejemplos para hacer énfasis entre las relaciones de la probabilidad no conmutativa y la teoría de representaciones de grupos. Además se da una prueba del teorema de Marchenko–Pastur basada en las pruebas de [12] y [11].

En el capítulo 4 se trabaja con la teoría desarrollada en los capítulos anteriores para calcular los momentos del grupo unitario. Empezamos por probar el resultado conocido como dualidad de Schur-Weyl para los grupos simétrico y unitario. Luego aplicamos este resultado para hacer el cálculo de los momentos del grupo unitario como en [5]. Por último se enuncia un resultado de asintoticidad libre entre matrices deterministas y Haar-unitarias cuya prueba depende del cálculo de los momentos del grupo unitario.

Capítulo 1

Representaciones de Grupos

Un método para estudiar la estructura de un grupo se basa en analizar las acciones de éste en otros conjuntos. Hay muchos teoremas de la teoría de grupos finitos que en sus enunciados no hablan de acciones pero la prueba se reduce a mostrar propiedades de cierta acción. Si un grupo G actúa en un espacio vectorial V nos interesa que la acción sea compatible con la estructura lineal de V, en concreto:

- $g(v+w) = gv + gw$
- $g(av) = a(gv)$,

para todos $g \in G$ $v, w \in V$ y a en el campo base. Estas dos propiedades nos dicen que el mapeo $\rho(g) : V \to V$ definido por $v \mapsto gv$ es una transformación lineal. Además por la propiedad de ser acción tenemos que $\rho(e) = Id_V$ y que $\rho(gh) = \rho(g)\rho(h)$, es decir, ρ es un homomorfismo entre G y el grupo $GL(V)$ de automorfismos lineales.

Definición 1.0.1. *Una **representación** compleja de un grupo G es un par (ρ, V) con V un $\mathbb{C}-$espacio vectorial y ρ un homomorfismo de grupos $\rho : G \to GL(V)$. La representación se dice **finita** si G es finito y V tiene dimensión finita. En este capítulo se presentarán algunos resultados fundamentales sobre la teoría de representaciones finitas.*

A continuación damos un ejemplo de una acción de grupo que aparece naturalmente cuando se estudia el espacio vectorial $\mathbb{C}^d$: permutar las coordenadas.

Ejemplo 1.0.1. *(**Matrices de permutación**). Consideremos S_n el grupo simétrico en n letras y el espacio vectorial $\mathbb{C}^n$. Para $\pi \in S_n$ y $(x_1, ..., x_n) \in \mathbb{C}^d$ definimos*

$$\rho(\pi)\,(v_1, ..., v_n) = (v_{\pi^{-1}(1)}, ..., v_{\pi^{-1}(n)}).$$

Esto define una representación de S_n además respecto a la base canónica la representación matricial de $\rho(\pi)$ es precisamente la matriz de permutación asociada a π.

En el siguiente ejemplo tenemos la acción mas simple de un grupo: la acción trivial.

Ejemplo 1.0.2. *(**Representación trivial**). Sean V un espacio vectorial y G un grupo. Entonces la representación trivial de G en V es el homomorfismo $\rho : G \to GL(V)$ dado por $\rho(g) = Id_V$.*

Por si solo el ejemplo anterior no es interesante pero mas adelante nos será de utilidad estudiar la componente trivial de una representación, de hecho en eso se basa el cálculo de Weingarten.

Proposición 1.0.1. *Sea $\rho : G \to GL(V)$ una representación finita y compleja. Entonces para cada $g \in G$ el endomorfismo $\rho(g)$ es diagonalizable y todos sus valores propios son raíces de la unidad.*

Demostración. Como G es finito todos sus elementos son de orden finito. Sea n el orden de g. Por definición tenemos que $g^n = 1$ y como ρ es un homomorfismo se sigue que $\rho(g)^n = Id_V$. Entonces el polinomio mínimo de $\rho(g)$ divide a $x^n - 1$, y como este último es producto de factores lineales distintos (sobre $\mathbb{C}$), tenemos que el polinomio mínimo de $\rho(g)$ también es producto de factores lineales distintos. Por lo tanto $\rho(g)$ es diagonalizable.
Como el polinomio mínimo de $\rho(g)$ divide a $x^n - 1$ todo valor propio de $\rho(g)$ también tiene que ser raíz del polinomio $x^n - 1$ y por lo tanto raíz $n-$ésima de la unidad. □

Definición 1.0.2. *Una **subrepresentación** W de (ρ, V) es un subespacio de V invariante bajo la acción de G, es decir, $\rho(g)w \in W$ para todos $g \in G$ y $w \in W$, de modo que el par está bien definido $(\rho_{|W}, W)$ y es una representación.*

Toda representación tiene al menos dos subrepresentaciones: V y 0. Si estas son sus únicas subrepresentaciones decimos que la representación es **simple** o **irreducible**.

Ejemplo 1.0.3. ***(Extensión lineal de una acción)*** *Supongamos que un grupo G actúa en un conjunto X y consideremos el espacio vectorial complejo generado por X:*

$$\mathbb{C}[X] = \left\{ \sum_{x \in X} a_x x : (a_x)_{x \in X} \subset \mathbb{C} \right\}.$$

Podemos extender la acción de G en X para obtener una representación definiendo:

$$\rho(g) \left(\sum_{x \in X} a_x x \right) = \sum_{x \in X} a_x g x.$$

En caso de que el conjunto sea finito podemos encontrar una subrepresentación con dimensión 1 pues en el espacio generado por el vector $\sum_{x \in X} x$ el grupo actúa trivialmente. Por lo que la representación $(\mathbb{C}[X], \rho)$ no es irreducible siempre que X sea un conjunto finito con al menos dos elementos.

Definición 1.0.3. *Un **homomorfismo** entre dos representaciones (ρ_1, V_1) y (ρ_2, V_2) del mismo grupo G es una transformación lineal $f : V_1 \to V_2$ que respeta la acción de G en cada espacio, es decir, el siguiente diagrama conmuta para cada $g \in G$:*

$$\begin{tikzcd} V_1 \arrow[r, "\rho_1(g)"] \arrow[d, "f"] & V_1 \arrow[d, "f"] \\ V_2 \arrow[r, "\rho_2(g)"] & V_2 \end{tikzcd}$$

Esta condición es equivalente a que para todos $v \in V_1$ y $g \in G$ se tenga que:

$$f(\rho_1(g)(v)) = \rho_2(g)(f(v)).$$

A un homomorfismo entre representaciones también le llamamos $G-$**homomorfismo**. El conjunto de todos los $G-$homomorfismos entre (ρ_1, V_1) y (ρ_2, V_2) lo denotamos por $Hom_G(V_1, V_2)$ y si $(\rho_1, V_1) = (\rho_2, V_2)$ escribimos $End_G(V_1)$.

Proposición 1.0.2. *El kernel y la imagen de un $G-$homomorfismo son subrepresentaciones.*

Proposición 1.0.3. *La suma y composición de $G-$homomorfismos es un $G-$homomorfismo siempre que este definida.*

Dos representaciones (ρ_1, V_1) y (ρ_2, V_2) del mismo grupo G se llaman **isomorfas** o **equivalentes** si existen $f : (\rho_1, V_1) \to (\rho_2, V_2)$ y $g : (\rho_2, V_2) \to (\rho_1, V_1)$ $G-$homomorfismos de modo que $g \circ f = Id_{V_1}$ y $f \circ g = Id_{V_2}$. En este caso decimos que f y g son $G-$**isomorfismos**. La teoría de representaciones no puede distinguir entre dos representaciones isomorfas ya que nos interesan estudiar propiedades invariantes bajo isomorfismo de representaciones. En ese sentido trataremos la representaciones isomorfas como iguales aunque desde el punto de vista de la teoría de conjuntos no lo sean.

Teorema 1.0.1. ***(Lema de Schur)**. Si (ρ_1, V_1) y (V_2, ρ_2) son representaciones finitas e irreducibles del mismo grupo G entonces todo $G-$homomorfismo no nulo $f : (\rho_1, V_1) \to (\rho_2, V_2)$ es $G-$isomorfismo. Además si $(\rho_1, V_1) = (\rho_2, V_2)$ y esta es una representación compleja entonces $f = aId$ para algún $a \in \mathbb{C}$.*

Demostración. Como $f \neq 0$ notamos que $ker(f)$ es una subrepresentación propia de V_1 y como esta representación es irreducible concluimos $ker(f) = 0$. Análogamente se tiene que $Im(f) = V_2$ ya que de lo contrario $Im(f)$ sería una subrepresentación propia y este espacio no puede ser cero pues $f \neq 0$. Por lo tanto f es un isomorfismo. Si $(\rho_1, V_1) = (\rho_2, V_2)$ entonces f es un operador lineal en un espacio vectorial de dimensión finita y por lo tanto tiene al menos un valor propio $a \in \mathbb{C}$. Por la proposición anterior $f - aId$ es un $G-$homomorfismo y como a es valor propio tenemos que $ker(f - aId)$ tiene un vector no nulo. Por lo tanto $ker(f - aId)$ es una subrepresentación no cero de una representación irreducible V_1 por lo tanto $ker(f - aId) = V_1$, es decir, $f = aId$. □

La segunda conclusión del lema de Schur no es valida si el campo no es algebraicamente cerrado. Este hecho hará que la teoría de representaciones finitas sobre $\mathbb{C}$ y sobre $\mathbb{R}$ sean muy distintas ya que muchos de los resultados de la teoría usan fuertemente este resultado.

Si (ρ_1, V_1) y (ρ_2, V_2) son dos representaciones del mismo grupo G podemos definir una representación $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ mediante la fórmula $\rho_1 \oplus \rho_2(g)(v_1 \oplus v_2) = \rho_1(g)(v_1) \oplus \rho_2(g)(v_2)$. Esta representación tiene como subrepresentaciones a (ρ_1, V_1) y (ρ_2, V_2). A esta representación la llamamos **suma directa** de (ρ_1, V_1) y (ρ_2, V_2) . También podemos realizar una construcción similar con el producto tensorial, es decir, definir una representación de G en $V_1 \otimes V_2$. Lo hacemos mediante la fórmula $\rho_1 \otimes \rho_2(g)(v_1 \otimes v_2) = \rho_1(g)(v_1) \otimes \rho_2(g)(v_2)$ a esta representación la llamamos **producto tensorial de Kronecker**.

Decimos que una representación es **semisimple** o **reducible** si se puede escribir como suma directa de representaciones irreducibles. En el siguiente ejemplo veremos que no todas la representaciones son reducibles.

Ejemplo 1.0.4. *En este ejemplos identificaremos $M_2(\mathbb{C})$ con $End(\mathbb{C}^2)$ mediante la base canónica. El grupo $\mathbb{Z}$ actúa en el espacio vectorial $\mathbb{C}^2$ de la siguiente manera:*

$$x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

Esto es una representación pues las matrices con esa forma son no singulares y si $x, y \in \mathbb{Z}$ entonces:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}.$$

Vamos a mostrar que el único subespacio invariante no trivial es el generado por e_1. Supongamos que existe W otra subrepresentación no trivial distinta al subespacio generado por e_1. Como W no es trivial tenemos que la dimensión de W no puede ser 0 ni 2. Por lo que W tiene dimensión 1. Sea $x \in W \leq \{0\}$ para cada $n \in \mathbb{Z}$ tenemos que $y = n\dot{x}$ actuando en x está en W y como este tiene dimensión 1 tenemos que y tiene que ser múltiplo de x. Por lo tanto x es un valor propio común de todas las matrices que definen la representación. Ahora mostraremos que este valor propio común no existe. Notamos que la matriz :

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

no es diagonalizable, pues es su propia forma canónica de Jordan. De lo anterior podemos concluir que esta representación no es reducible.
Un resultado de estructura importante conocido como el teorema de Maschke establece que toda representación finita se puede descomponer en suma directa de subrepresentaciones irreducibles. Para mostrar esto introduciremos un producto interno en el espacio vectorial subyacente.

Sean $\rho : G \to GL(V)$ una representación finita y $\langle , \rangle_0$ un producto interno en V. Para $v, w \in V$ definimos:

$$\langle v, w \rangle = \sum_{g \in G} \langle \rho(g)v, \rho(g)w \rangle_0.$$

Proposición 1.0.4. *El producto $\langle , \rangle : V \times V \to \mathbb{C}$ es un producto interno y además $\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$ para todos $v, w \in V$ y $g \in G$.*

Demostración. Tenemos que $\langle , \rangle$ es suma de formas sequilineales y hermitianas y por lo tanto es sesquilineal y hermitiana. Por otro lado para cualquier $v \in V$ tenemos que

$$\langle v, v \rangle = \sum_{g \in G} \langle \rho(g)v, \rho(g)v \rangle_0 \geq 0,$$

puesto que $\langle , \rangle$ es un producto interno. Debido a lo anterior esta forma es positiva. Además si para algún $v \in V$ se tiene que $\langle v, v \rangle = \sum_{g \in G} \langle \rho(g)v, \rho(g)v \rangle_0 = 0$, como cada sumando es no-negativo todos los sumandos deben de ser cero, en particular $\langle v, v \rangle_0 = \langle \rho(e)v, \rho(e)v \rangle_0 = 0$ y como $\langle , \rangle_0$ es un producto interno $v = 0$. Por lo tanto $\langle , \rangle$ es no degenerada. Lo anterior muestra que $\langle , \rangle$ es un producto interno.
Notamos que para $u, v, w \in V$ y $a \in \mathbb{C}$ se tiene que:

$$\begin{aligned} \langle \rho(h)v, \rho(h)w \rangle &= \sum_{g \in G} \langle \rho(g)\rho(h)v, \rho(g)\rho(h)w \rangle_0 && (1.1) \\ &= \sum_{g \in G} \langle \rho(gh)v, \rho(gh)w \rangle_0 && (1.2) \\ &= \sum_{g' \in G} \langle \rho(g')v, \rho(g')w \rangle_0 && (1.3) \\ &= \langle v, w \rangle. && (1.4) \end{aligned}$$

□

A todo producto interno que tenga la propiedad anterior lo llamaremos $G-$invariante o simplemente invariante si se entiende cual es el grupo subyacente. La proposición anterior muestra que una representación finita siempre puede ser dotada de un producto interno invariante. Los productos internos invariantes son casi únicos en el siguiente sentido.

Proposición 1.0.5. *Si $\rho : G \to GL(V)$ es una representación finita e irreducible entonces tiene un único producto interno $G-$invariante salvo por múltiplos escalares positivos.*

Proposición 1.0.6. *Sean $\rho : G \to GL(V)$ una representación y $\langle , \rangle$ un producto interno en V. Si $\langle , \rangle$ es $G-$invariante entonces $\rho(g)$ es un operador unitario para cada $g \in G$. Por otro lado si $\rho(g) \in U(V, \langle , \rangle)$ para toda $g \in G$ entonces $\langle , \rangle$ es un producto interno $G-$invariante.*

Demostración. Supongamos que $\langle , \rangle$ es un producto interno invariante. Tenemos que si $g \in G$ y $v, w \in V$ entonces :

$$\begin{aligned} \langle \rho(g)v, w\rangle &= \langle \rho(g^{-1})\rho(g)v, \rho(g^{-1})w\rangle &(1.5)\\ &= \langle \rho(g^{-1}g)v, \rho(g^{-1})w\rangle &(1.6)\\ &= \langle v, \rho(g)^{-1}w\rangle. &(1.7)\end{aligned}$$

Por lo tanto $\rho(g)^* = \rho(g)^{-1}$, es decir, $\rho(g)$ es un operador unitario.
Por otro lado si $\rho(g)$ es unitario entonces para $v, w \in G$ se tiene que:

$$\begin{aligned} \langle \rho(g)v, \rho(g)w\rangle &= \langle v, \rho(g)^*\rho(g)w\rangle &(1.8)\\ &= \langle v, \rho(g)^{-1}\rho(g)w\rangle &(1.9)\\ &= \langle v, w\rangle. &(1.10)\end{aligned}$$

Entonces, si $\rho(G) \subset U(V, \langle , \rangle)$ el producto interno $\langle , \rangle$ es $G-$invariante. □

Ejemplo 1.0.5. ***(Representación estándar).*** *En la representación de S_n en $\mathbb{C}^n$ definida por las matrices de permutación el producto interno usual de $\mathbb{C}^n$ es invariante ya que las matrices de permutación son unitarias respecto a este producto interno. Notamos también que esta representación no es irreducible (siempre que $n \geq 2$) ya que en el subespacio generado por $e_1 + ... + e_n$, el grupo S_n actúa trivialmente y por lo tanto es invariante. Notamos que el complemento ortogonal de este subespacio también debe de ser invariante siendo este:*

$$\left\{ \sum_{i=1}^{n} a_i e_i : \sum_{i=1}^{n} a_i = 0 \right\}.$$

Este último subespacio es irreducible y se le llama ***representación estándar*** *de S_n.*

En el siguiente resultado haremos se pone de manera general la idea de tomar el complemento bajo un producto interno invariante con el propósito de descomponer una representación.

Proposición 1.0.7. *Si V es un espacio vectorial de dimensión finita, $\rho : G \to GL(V)$ es una representación y $\langle , \rangle$ es un producto interno invariante entonces V es suma directa de representaciones irreducibles.*

Demostración. Basta mostrar que todo subespacio invariante tiene un complemento invariante. Sea $W \subset V$ un subespacio invariante. Sea $g \in G$. Como $\rho(g^{-1})W = W$ tenemos que $\rho(g^{-1})^* W^\perp = W^\perp$ por lo cual $\rho(g)W^\perp = W^\perp$. Por lo tanto $W^\perp$ es $G-$invariante y además $V = W \oplus W^\perp$ como subrepresentaciones. Podemos de esta forma descomponer a W o a $W^\perp$ si estas no son representaciones irreducibles. Este proceso no puede seguir de manera indefinida ya que V tiene dimensión finita por lo que obtenemos un descomposición de V en subrepresentaciones irreducibles eventualmente. □

1.1. Caracteres

Una función $f : G \to GL(V)$ se llama **función de clase** si $f(g) = f(h)$ siempre que g y h estén en la misma clase de conjugación. El conjunto de todas las funciones de clase forman un espacio vectorial el cual denotaremos por $C(G)$. En esta sección estudiaremos una clase de funciones de clase asociadas a representaciones del grupo.

Definición 1.1.1. *Dada una representación $\rho : G \to GL(V)$ definimos su* ***caracter*** *$\chi_\rho : G \to \mathbb{C}$ de la siguiente manera:*

$$\chi_\rho(g) = Tr(\rho(g)).$$

En este capítulo no solo será importante estudiar el caracter de una representación dada también se estudiarán todas las posibles funciones que son el caracter de una representación para un grupo fijo. Notamos que esta es una función de clase ya que si $g, h \in G$ entonces:

$$Tr(\rho(h^{-1}gh)) = Tr(\rho(h)^{-1}\rho(g)\rho(h)) = Tr(\rho(g)).$$

En la siguiente proposición vamos a mostrar algunas propiedades de los caracteres.

Proposición 1.1.1. *Si $\rho : G \to GL(V)$ y $\rho' : G \to GL(V')$ son representaciones y $g \in G$ entonces:*

1.- $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$.

2.- $\chi_{\rho\otimes\rho'} = \chi_\rho \chi_{\rho'}$.

3.- $\chi_\rho(e) = \dim(V)$.

4.- $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

5.- $|\chi_\rho(g)| \leq \dim(V)$ *con igualdad si y solo si* $\rho(g) = Id_V$.

Demostración. Sea $g \in G$ tenemos que:

$$\begin{aligned} \chi_{\rho\oplus\rho'}(g) &= Tr(\rho \oplus \rho'(g)) && (1.11)\\ &= Tr(\rho(g)) + Tr(\rho'(g)) && (1.12)\\ &= \chi_\rho + \chi_{\rho'}(g), && (1.13) \end{aligned}$$

lo cual muestra 1. Para 2 notamos que:

$$\begin{aligned} \chi_{\rho\otimes\rho'}(g) &= Tr(\rho \otimes \rho'(g) && (1.14)\\ &= Tr(\rho(g))Tr(\rho'(g)) && (1.15)\\ &= \chi_\rho(g)\chi_{\rho'}(g), && (1.16) \end{aligned}$$

de lo anterior tenemos 2. Recordamos que $\rho(e) = Id_V$ y que $Tr(Id_V) = \dim(V)$ de lo que se sigue 3. Como ρ es una representación finita tenemos que $\rho(g)$ es diagonalizable y sus valores propios son raíces de la unidad. Sean $\lambda_1, \ldots, \lambda_n$ sus valores propios. Como λ_i es raíz de la unidad tenemos que $\lambda_i^{-1} = \overline{\lambda_i}$ por lo cual:

$$\chi_\rho(g^{-1}) = Tr(\rho(g)^{-1}) = \sum_{i=1}^{n} \lambda_i^{-1},$$

de donde se siguen 4 y 5. □

Proposición 1.1.2. *Dos representaciones isomorfas tienen el mismo caracter.*

Demostración. Sean $\rho_1 : G \to GL(V_1)$ y $\rho_2 : G \to GL(V_2)$ representaciones y $f : V_1 \to V_2$ un $G-$isomorfismo. Tenemos que si $g \in G$ entonces $f \circ \rho_1(g) = \rho_2(g) \circ f$ por lo que $\rho_1(g) = f^{-1} \circ \rho_2(g) \circ f$. Esto muestra que $\rho_1(g)$ y $\rho_2(g)$ son transformaciones lineales conjugadas por lo cual tienen la misma traza. Por lo tanto $\chi_{\rho_1} = \chi_{\rho_2}$. □

También es cierto que dos representaciones con el mismo caracter son isomorfas esto lo demostraremos mas adelante. Para demostrarlo vamos a introducir un producto interno entre caracteres. Si G es un grupo finito y $f_1, f_2 \in C(G)$ definimos el producto interno de f_1 y f_2 de la siguiente manera:

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Proposición 1.1.3. ***(Primer relación de ortogonalidad)***
Los caracteres de las representaciones irreducibles son un conjunto ortonormal en $C(G)$.

Proposición 1.1.4. *La descomposición de una representación en irreducibles es única salvo isomorfismo de representaciones.*

Demostración. Tenemos que dos representaciones son isoformas si y solo si tienen el mismo caracter y como los caracteres irreducibles son una base ortonormal del subespacio generado por los caracteres en el espacio de funciones de clase se sigue el resultado. □

En el siguiente capítulo probaremos un resultado que nos dice que hay tantas clases de conjugación en G como representaciones finitas e irreducibles, de donde se sigue que los caracteres de las representaciones irreducibles forman una base ortonormal de $C(G)$.

1.2. La representación regular

La representación regular de un grupo G es la extensión lineal de la acción de multiplicación por la izquierda del grupo en si mismo, es decir, consideremos V_{reg} el espacio vectorial libre generado por los elementos $(e_g)_{g \in G}$ la representación regular está definida por $\rho_{reg}(g_0) : e_g \mapsto e_{g_0 g}$. Notamos que estos operadores actúan permutando elementos de la base y que si $g_0 \in G \setminus \{e\}$ tenemos que $\rho_{reg}(g_0)(e_g) \neq e_g$. Juntando los dos hechos anteriores tenemos que $Tr(\rho(g_0) = 0$.

Proposición 1.2.1. ***Carater de la representación regular.***
Si χ_{reg} denota el caracter de la representación regular tenemos que

$$\chi_{reg} = |G|\delta_{g,e}.$$

Proposición 1.2.2. *Si* $(\rho_1, V_1), ..., (\rho_n, V_n)$ *es una colección completa de representaciones finitas e irreducibles de* G *y* n_k *es la dimensión de* V_k *entonces:*

$V_{reg} = \oplus n_k V_k$ *como representaciones de grupos.*

Demostración. Si χ_k es el caracter de la representación V_k tenemos que la multiplicidad de V_k en una representación esta dada por el producto interno de los caracteres por lo que el número de veces que V_k aparece en la representación regular es:

$$\langle \chi_k, \chi_{reg} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_k(g) \overline{\chi_{reg}(g)} \tag{1.17}$$

$$= \sum_{g \in G} \chi_k(g) \overline{|G| \delta_{ge}} \tag{1.18}$$

$$= \chi_k(e) \tag{1.19}$$

$$= n_k. \tag{1.20}$$

□

De lo anterior como $\dim_{\mathbb{C}}(V_{reg}) = |G|$ tenemos que $\sum_i n_i^2 = |G|$.

Proposición 1.2.3. *Sean* $f : G \to \mathbb{C}$ *es una función de clase y* $\rho : G \to GL(V)$ *una representación. Entonces podemos obtener un* $G-$*endomorfismo de* V *promediando a* ρ *a través de* f*, es decir,* $\rho_f = \sum_{g \in G} f(g)\rho(g)$ *es un* $G-$*endomorfismo. Además si* ρ *es irreducible entonces* ρ_f *es un homotécia de radio* $\frac{|G|}{\dim V} \langle f, \overline{\chi_\rho} \rangle$

Demostración. Notamos que para cualquier $g_0 \in G$ se tiene que:

$$\rho_f \circ \rho(g_0) = \sum_{g \in G} f(g)\rho(g)\rho(g_0) \tag{1.21}$$

$$= \sum_{g \in G} f(g)\rho(gg_0) \tag{1.22}$$

$$= \sum_{h \in G} f(g_0 h g_0^{-1})\rho(g_0 h) \tag{1.23}$$

$$= \rho(g_0) \sum_{h \in G} f(h)\rho(h) \tag{1.24}$$

$$= \rho(g_0)\rho_f. \tag{1.25}$$

Por lo tanto ρ_f es un $G-$endomorfismo. Ahora si V es irreducible por el lema de Schur tenemos que $\rho(f)$ es una homotecia de radio $\frac{Tr(f)}{\dim V}$ y tenemos que

$$Tr(f) = \sum_{g \in G} f(g) Tr(\rho(g)) = |G| \langle f, \overline{\chi_\rho} \rangle.$$

También se puede probar que todos los $G-$endomorfismos se pueden escribir de esta manera, es decir, promediando la acción de grupo mediante pesos dados por una función de clase. □

1.3. La descomposición isotípica de una representación

Hay infinitas maneras de descomponer el plano $\mathbb{C}^2$ como suma directa de dos lineas por lo que para la representación trivial de cualquier grupo G en $\mathbb{C}^2$ la descomposición en componentes irreducibles no es única, las multiplicidades son únicas mas no los subespacios.

Teorema 1.3.1. *Sean G un grupo finito y $\rho : G \to GL(V)$ una representación compleja de grado finito. Consideremos una descomposición en componentes irreducibles $V = \oplus W_{i,j}$ de modo que $W_{i,j} \simeq W_{i,j'}$ como $G-$módulos y $W_{i,j} \not\cong W_{i',j'}$ si $i \neq i'$. Denotamos por χ_i al caracter de $W_{i,1}$ y por $V_i = \oplus_j W_{i,j}$. Entonces:*

1). La descomposición $V = \oplus V_i$ no depende de la descomposición inicial.

2). Si

$$p_i = \frac{\chi_i(e)}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \rho(g)$$

entonces p_i es la proyección de V en V_i asociada a esta descomposición.

Demostración. Empezaremos por probar el segundo punto de este teorema. Si restringimos a p_i a algún $W_{j,k}$ tenemos por la proposición anterior, (ya que los caracteres son funciones de clase), que p_i es una homotecia de radio $\frac{n_i}{n_j}\langle \chi_i, \chi_j \rangle$, es decir, 0 si $i \neq j$ y 1 si $i = j$. Por lo que p_i es la proyección de V con imagen V_i y kernel $\oplus_{j \neq i} V_j$. Como las proyecciones no dependen de la descomposición irreducible inicial tenemos que la descomposición no depende de la descomposición inicial. $\square$

A está descomposición se le conoce como descomposición en **componentes isotípicas** o solamente como descomposición **isotípica**.

Proposición 1.3.1. *Sean G un grupo finito y $\rho : G \to GL(V)$ una representación compleja finita con producto interno invariante. Entonces las componentes isotípicas son ortogonales con respecto a este producto interno.*

Demostración. En el teorema anterior observamos que la descomposición isotípica no depende de la descomposición irreducible con la que se construya. Si elegimos la descomposición irreducible construida inductivamente en la prueba del teorema de descomposición irreducible. Con esto tenemos una descomposición en componentes irreducibles ortogonales y sumando los espacios correspondientes obtenemos la descomposición isotípica con partes ortogonales. $\square$

Combinando esto con la teoría de Wedderburn es posible ver que para la representación regular del grupo simétrico la descomposición isotípica coincide con la descomposición de álgebras semisimples.

1.4. El grupo simétrico

En esta sección vamos a estudiar las representaciones irreducibles del grupo simétrico, para ello vamos a introducir objetos combinatorios que nos ayudaran a parametrizar las representaciones irreducibles de este grupo, las particiones aditivas de un entero y las tablas de Young.
Sea n un entero positivo. Una partición de n es una sucesión $\lambda = (\lambda_1, \ldots, \lambda_k)$ débilmente decreciente de enteros positivos tales que $\sum \lambda_i = n$ usamos la notación $\lambda \vdash n$ y decimos que λ parte a n. La clase de conjugación de una partición está determinada por su estructura cíclica.

Proposición 1.4.1. *Hay tantas clases de conjugación en S_n como particiones aditivas del entero n.*

Recordamos que toda representación $\sigma \in S_n$ se puede descomponer como producto de ciclos disjuntos $\sigma = \prod c_i$ con c_i un ciclo de tamaño λ_i. Como todos los enteros del 1 al n aparecen en exactamente un ciclo tenemos que $n = \sum \lambda_i$ por lo que podemos construir una partición con estas partes a esta le conocemos como tipo cíclico de la permutación. Además tenemos que dos permutaciones son conjugadas si y solo si tienen el mismo tipo cíclico.

1.4.1. Representaciones irreducibles del grupo simétrico

El objetivo de esta subsección es construir mediante herramientas combinatorias las representaciones irreducibles del grupo simétrico. En [7], Fulton expone herramientas combinatorias para después describir las representaciones irreducibles del grupo simétrico.
Podemos representar a cada partición $\lambda \dashv n$ de manera gráfica, con un diagrama poniendo λ_1 casillas, luego bajo estas λ_2 casillas y así sucesivamente. A esta representación se le conoce como **diagrama de Young** o **diagrama de Ferrer**. Notamos que hay una correspondencia entre diagramas y particiones por lo que nos referiremos por λ tanto al diagrama como a la partición.
El propósito de escribir una partición como casillas es de llenarlas con algo. Un **llenado** de un diagrama de Young λ es una forma de llenar las casillas del diagrama con números enteros positivos. Decimos que el llenado tiene **forma** λ y escribimos $s(T) = \lambda$. Si i es una casilla del llenado T denotaremos por $T(i)$ al número que está en la casilla i. A un llenado tal que todos los números de las casillas son distintos entre si y son los números $1, 2, \ldots, n$ le llamamos **numeración**. El grupo simétrico actúa en el conjunto de todas las numeraciones de forma λ, denotado por $Num(\lambda)$ mediante la fórmula:

$$\sigma T(i) = \sigma(i).$$

Para una numeración T definimos $R(T)$ como el subgrupo de S_n que estabiliza a las filas de la numeración y notamos que este grupo es isomorfo al producto cartesiano $\prod S_{\lambda_i}$. Análogamente hablaremos de $C(R)$, el subgrupo que estabiliza a las columnas de la numeración.
Un tabloide es la órbita de una numeración de un diagrama de Young T bajo el grupo $R(G)$ y lo denotamos como $\{T\}$. La acción de S_n en el conjunto de numeraciones de un diagrama de Young λ da lugar a una acción de S_n en el conjunto de tabloides de forma λ de la siguiente manera $\sigma\{T\} = \{\sigma T\}$. Llamamos M^λ a la representación compleja dada por la extensión lineal de esta acción. Encontraremos la subrepresentación irreducible buscada dentro de M^λ.
Definimos $v_T = \sum_{\sigma \in C(T)} sgn(\sigma)\{\sigma T\} \in M^\lambda$ y notamos que $\sigma v_T = v_{\sigma T}$.
Denotaremos por S^λ al espacio vectorial generado por los elementos v_T para T numeraciones del diagrama λ de la observación anterior se sigue que S^λ es una subrepresentación de M^λ.

Proposición 1.4.2. *Si $\lambda, \lambda' \dashv n$ entonces S^λ y $S^{\lambda'}$ son representaciones no isomorfas del grupo S_n.*

Proposición 1.4.3. *La colección $(S^\lambda)_{\lambda \dashv n}$ es una familia completa de representaciones irreducibles del grupo simétrico.*

En muchos textos a S^λ se le conoce como **módulo de Specht** y existe una fórmula combinatoria que permite calcular la dimensión de este conocida como la fórmula de longitud de gancho que solo depende de la estructura del diagrama λ.

Una **tabla** de forma λ es un llenado del diagrama que es estrictamente creciente, de izquierda a derecha, en las filas y débilmente creciente, de arriba hacia abajo, en las columnas. Una tabla se llamará estándar si es una enumeración.

Proposición 1.4.4. *Los vectores v_T con T una tabla estándar de forma λ conforman una base para el espacio vectorial S^λ.*

De la proposición anterior tenemos que la dimensión de S^λ es igual al número de tablas estándar de forma λ.

1.4.2. La estructura métrica del grupo simétrico

En este apartado estamos interesados en estudiar una distancia invariante en el grupo simétrico para ver esto con mayor profundidad se puede consultar en [4]. Dados un grupo G y un subconjunto generador de G estable bajo el anti-isomorfismo inversión de G construiremos una gráfica C. Los vértices de C son los elementos del grupo y habrá una arista entre g_1 y g_2 si $g_1 g_2^{-1} \in S$ esta gráfica es conocida como la **gráfica de Caley de** (G, S). Nosotros estamos interesados en estudiar la gráfica de Caley del grupo simétrico con aristas dadas por el conjunto de transposiciones.

Proposición 1.4.5. *Si $S \subset S_n$ es el subconjunto de transposiciones entonces este es invariante bajo la inversión y genera a S_n.*

Dada una gráfica finita podemos construir una distancia en el conjunto de vértices subyacente. Mas específicamente, definimos la distancia entre dos vértices como la mínima longitud de un camino que los une. Notamos que está distancia es invariante bajo la acción por multiplicación a la izquierda o derecha del grupo por lo que $d(g, h) = d(gh^{-1}, e)$ por lo que podemos codificar la estructura métrica de la gráfica conociendo únicamente $d(g, e)$ para todo $g \in G$, será conveniente definir la notación $|g| = d(g, e)$.

El siguiente lema será de utilidad para estudiar la distancia en la gráfica de Caley del grupo simétrico.

Proposición 1.4.6. *Sean $\sigma \in S_n$ una permutación y (a, b) una transposición, entonces:*

- *Si a y b pertenecen a ciclos disjuntos en σ entonces $|\sigma(a, b)| = |\sigma| - 1$.*
- *Si a y b pertenecen al mismo ciclo en σ entonces $|\sigma(a, b)| = |\sigma| + 1$.*

Los siguientes dos resultados se siguen del resultado anterior.

Proposición 1.4.7. *Para $\sigma \in S_n$ el mínimo número k tal que σ es producto de k transposiciones es $|\sigma|$.*

En la proposición anterior hemos convenido que el elemento identidad es producto de cero transposiciones.

Sea $\sigma \in S_n$ si escribimos su factorización $\sigma = C_1 \cdots C_k$ como producto de ciclos disjuntos, contando los puntos fijos de σ ($1-$ciclos) decimos que σ tiene k ciclos y escribimos $c(\sigma) = k$.

Proposición 1.4.8. *Para $\sigma \in S_n$ se tiene que $c(\sigma) + |\sigma| = n$.*

Demostración. Utilizaremos el método de inducción sobre el número de ciclos de σ. □

Capítulo 2

Álgebras

Este capítulo lo dedicaremos al estudio de álgebras semisimples de dimensión finita.

2.1. Álgebras semisimples y el teorema de Wedderburn

En esta sección hablaremos sobre álgebras semisimples, el teorema de Wedderburn y el teorema del doble centralizador, siendo este último el principal objetivo. Los dos principales trabajos en los que este capitulo se basa son [2] [9] .

Un **álgebra** A sobre un campo k es un anillo de dotado de una acción lineal de k. Si el anillo subyacente cuenta con unidad decimos que A es un álgebra con unidad. De aquí en adelante, aunque no se especifique, solo consideraremos álgebras con unidad de dimension finita sobre k.
Un módulo (izquierdo) sobre un álgebra A es a un álgebra como un espacio vectorial lo es a un campo, es decir, un grupo abeliano M junto con una acción lineal de A (por la izquierda), o lo que es lo mismo, que para todos $a, b \in A$ y $m, n \in N$ se cumpla que:

- $(a + b)m = am + bm$,
- $a(m + n) = am + an$,
- $(ab)m = a(bm)$,
- $1_A m = m$.

La primer parte de este capítulo damos algunos resultados y definiciones para módulos y álgebras similares a las que se conocen de álgebra lineal, exponiendo las similaridades de ambas teorías. También se dirá qué resultados no se generalizan cuando pasamos de estudiar espacios vectoriales al estudio de los módulos sobre un álgebra.

Si M es un $A-$módulo un **submódulo** de M es un subgrupo aditivo N estable bajo la acción de A en M. En otras palabras para cualquier par de elementos $a \in A$ y $n \in N$ se tiene que $an \in N$. Usamos la notación $N \leq M$.

Ejemplo 2.1.1. *Notamos que el álgebra A es un $A-$módulo. Consideremos $I \subset A$ un ideal del anillo subyacente de A. Notamos que I es un submódulo. Además todos los submódulos izquierdos de A son ideales izquierdos.*

Proposición 2.1.1. *La intersección de una familia no vacía de submódulos de un módulo es un submódulo.*

Si $X \subset M$ podemos considerar el submódulo:

$$\langle X \rangle = \bigcap \{N : N \leq M\}.$$

El cual definimos como el **módulo generado** por X. Notamos que $\langle X \rangle$ es el mínimo submódulo de M, con respecto a la inclusión, que contiene a X. Decimos que un módulo M es **finitamente generado** si existe un subconjunto finito $X \subset M$ tal que $\langle X \rangle = M$. En esta tesis estamos interesados únicamente en módulos finitamente generados.
Un $A-$módulo recibe la estructura de $k-$espacio vectorial heredada de A. Ya que para $\lambda \in k$ se tiene que $\lambda 1_A \in A$.
En la siguiente proposición encontramos una condición necesaria y suficiente para determinar si un $A-$módulo es finitamente generado usando la estructura de $k-$espacio vectorial subyacente.

Un $A-$módulo recibe la estructura de $k-$espacio vectorial heredada de A. Ya que para $\lambda \in k$ se tiene que $\lambda 1_A \in A$. En esta tesis estamos interesados únicamente en módulos finitamente generados.

Proposición 2.1.2. *Los $A-$módulos finitamente generados son aquellos que como $k-$espacios vectoriales tienen dimensión finita.*

Demostración. Sean M un $A-$módulo finitamente generado por $m_1, \ldots, m_n$ y $a_1, \ldots, a_k$ generadores de A sobre k. Claramente el conjunto $\{a_i m_j\}$ genera a M como $k-$espacio vectorial. Por otro lado si M es un $A-$módulo de dimensión finita sobre k claramente es finitamente generado sobre A. □

Un $A-$homomorfismo $f : M \to N$ es una transformación $k-$lineal que además conmuta con la acción de A, es decir,$f(am) = af(m)$ para cualesquiera $a \in A$ y $m \in M$. Si el homomorfismo f es una biyección entonces su su función inversa f^{-1} también es un $A-$homomorfismo y a estos dos homomorfismos los llamamos **isomorfismos**. El kernel de f es definido como:

$$ker(f) = \{m \in M : f(m) = 0\},$$

mientras que la imagen:

$$Im(f) = \{f(m) : m \in M\}.$$

Estos dos conjuntos tienen la estructura de $A-$submódulos de M y N respectivamente.

Si N es un A-submódulo de M notamos que es un subespacio vectorial por lo que podemos construir el espacio vectorial cociente

$$M/N = \{m + N : m \in M\},$$

el cual hereda la estructura de $A-$módulo con la acción de A dada por $a(m + N) = am + M$. Los resultados conocidos como teoremas de isomorfismo que son validos para estructuras como grupos, anillos o espacios vectoriales también aplican para módulos. Aquí solo presentaremos el mas importante: el primer teorema de isomorfismo.

Teorema 2.1.1. ***(Primer teorema de isomorfismo).***
Si $f : M \to N$ es un $A-$homomorfismo entonces la función $\tilde{f} : M/ker(f) \to Im(f)$ definida por $m + Ker(f) \mapsto f(m)$ es un $A-$isomorfismo.

El conjunto de todos lo $A-$homomorfismos entre M y N es un $k-$espacio vectorial con la suma y el producto puntuales, denotado por $Hom_A(M, N)$. Un espacio de homomorfismos que nos interesa estudiar es $Hom_A(M, M)$, es decir, cuando $M = N$. A este tipo de homomorfismos los llamamos **endomorfismos** y al espacio de todos ellos lo denotamos por $End_A(M)$.
Una de las razones por las que el estudio de $End_A(M)$ es interesante es que este tiene una estructura natural de $k-$álgebra con el producto dado por la composición de endomorfismos y el uno dado por el morfismo identidad (Id_M).

Todo $A-$módulo M tiene al memos dos submódulos M y $\{0\}$ el cual normalmente denotaremos como 0. Un módulo no nulo se llama **simple** si no tiene submódulos distintos a si mismo o 0. Dado que los módulos simples no tienen submódulos no triviales podemos deducir muchas cosas sobre ellos.

Teorema 2.1.2. ***(Lema de Schur).*** *Consideremos $f : S_1 \to S_2$ un $A-$homomorfismo entre dos módulos simples.*

1). Si $f \neq 0$ entonces es un isomorfismo.

2). Si S_1 y S_2 no son isomorfos entonces $f = 0$.

Demostración. Supongamos que $f \neq 0$ de esto se sigue que $Im(f) \neq 0$. Además $Im(f)$ es submódulo de S_2. Por la definición de módulo simple se tiene que $Im(f) = S_2$. Si $Ker(f) \neq 0$ entonces como $Ker(f)$ es un submódulo de S_1 tenemos que $Ker(f) = S_1$. Esto contradice el hecho de que $f \neq 0$. Por lo tanto $Ker(f) = 0$. Esto muestra que f es un $A-$isomorfismo, por lo que si S_1 y S_2 no son $A-$isomorfos entonces necesariamente $f = 0$.

Los módulos simples son los módulos mas pequeños, como no tienen submódulos propios no los podemos descomponer como suma directa de dos módulos. En general nos gustaría descomponer todo módulo como suma directa de módulos simples. Esto no siempre es posible (mas adelante trataremos este problema). Definiremos la clase de módulo que podemos descomponer como suma directa de módulos simples. □

Proposición 2.1.3. *Un módulo se dice* ***semisimple*** *si:*

(1) todo submódulo es un sumando directo,

(2) es suma directa de módulos simples o,

(3) es suma, no necesariamente directa, de submódulos simples.

Si un módulo cumple una de estas condiciones también se cumple las dos restantes bajo la hipótesis de dimensión finita.

Demostración. Probaremos que la condición (1) implica la condición (2). Esta prueba será por inducción sobre la dimensión del módulo.Como caso base tomamos los módulos de dimensión minimal que cumplen que todo submódulos es sumando directo, es decir los módulos simples, los cuales claramente cumplen la segunda condición. Dado un módulo M no simple hacemos la hipótesis de inducción de que todos los módulos con dimensión menor que la dimensión de M que satisfacen la condición (1) también cumplen la condición (2). Como M no es simple existe un $V \subset M$ un submódulo propio no trivial. Por la condición (1) tenemos que existe W tal que $M = V \oplus W$. Como todo submódulo de M es sumando directo de M tenemos que todo submódulo

de V es sumando directo de M y por los tanto es sumando directo de V, es decir, V hereda la propiedad (1). Análogamente W también cumple con la propiedad (1). Por la hipótesis inductiva tenemos que V y W son suma directa de módulos simples. Como $M = V \oplus W$ concluimos que M es suma directa de módulos simples. Lo cual concluye la prueba inductiva.
Claramente tenemos que la condición (2) implica (3).
Por último mostraremos que (3) implica (2). Sea M un módulo con la propiedad (3) vamos a mostrar que todos sus submódulos son sumandos directos. Sea V un submódulo de M, como complemento de V proponemos a W un submódulo de M con maximal con la propiedad de tener intersección vacía con V. Mostraremos que $M = V + W$. Supongamos que $V + W$ es un submódulo propio de M. Si todo submódulo simple de M esta contenido en $V + W$ entonces como M puede ser escrito como suma directa de módulos simples se tendría que $M \subset V + W$ por lo que $M = V + W$. Ahora vamos a mostrar que esto ocurre, procederemos por reducción al absurdo. Si algún submódulo simple de S de M no está contenido en $V + W$. Tenemos que $S \cap (V + W) = 0$ puesto que $S \cap (W + V)$ es un submódulo de S, S no es submódulo de $V + W$ y S es simple. De lo anterior tenemos que $V \cap S = 0$ y $W \cap S = 0$. Notamos que $(W + S) \cap V = V \cap W + S \cap W = 0$ lo cual contradice la elección de W como el submódulo de M maximal con intersección con V trivial. De lo anterior concluimos que todo submódulo simple de M está contenido en $V + W$ y por tanto $M = V + W$. Observamos que por elección de W tenemos que $M = V \oplus W$. Lo cual muestra que (3) implica (2). $\square$

Cabe mencionar que el módulo trivial es considerado semisimple y esto no contradice la proposición anterior ya que puede ser escrito como suma vacia de módulos simples. De la proposición anterior se tiene que los módulos simples son semisimples.

Del lema de Schur se sigue que la descomposición de un módulo semisimple en suma directa de módulos simples es única. En el sentido de las multiplicidades que los distintos módulos simples ocurren, no en el sentido que sean únicos como subespacios vectoriales. Justamente como ocurría en el caso de la descomposición en irreducibles de una representación de un grupo finito.

Proposición 2.1.4. *Los submódulos y cocientes de módulos semisimples son semisimples.*

Demostración. Sea M un $A-$módulo semisimple y $N \subset M$ un submódulo. Por la proposición anterior podemos escribir $M = \sum_{i=1}^{n} S_i$ con $S_1, \ldots, S_n$ módulos simples.
Primero mostraremos que el submódulo N es semisimple. Tenemos que:

$$N = N \cap M \tag{2.1}$$
$$= \sum_{i=1}^{n} S_i \cap N. \tag{2.2}$$

Además para cada i tenemos que $N \cap S_i$ es un submódulo del módulo simple S_i por lo cual $N \cap S_i = 0$ o $N \cap S_i = S_i$, quitando los índices tales que $N \cap S_i = 0$ podemos escribir $N = \sum_{i \in \alpha} S_i$ para algún $\alpha \subset [n]$. Por lo tanto N es suma de módulos simples y por lo tanto N es semisimple.
Ahora mostraremos que el cociente M/N es semisimple. Sea $\pi M \to M/N$ el homomorfismo cociente. Tenemos que:

$$\pi(M) = \pi\left(\sum_{i=1}^{n} S_i\right) = \sum_{i=1}^{n} \pi(S_i).$$

Por el lema de Schur tenemos que $\pi(S_i) = 0$ ó $\pi(S_i) \sim S_i$, por lo que si $\pi(S_i) \neq 0$ entonces

$\pi(S_i)$ es simple. Por lo tanto quitando los indices tales que $\pi(S_i) = 0$ tenemos que

$$M/N = \pi(S_i) = \sum_{i \in \beta} \pi(S_i),$$

para algún $\beta \subset [n]$. Por lo que M/N se puede escribir como suma de módulos simples, por la proposición anterior concluimos que es un módulo semisimple. □

Un resultado muy usado en álgebra lineal elemental es que todo espacio vectorial tiene una base. Notamos que el tomar una base del espacio es equivalente a construir un isomorfismo del espacio vectorial a una suma directa de copias de k. Por lo que del teorema se concluye que todo espacio vectorial es isomorfo a una suma directa de copias del campo. De donde podemos ver que todos los $k-$espacio vectoriales, no nulos, son $k-$módulos semisimples y los únicos simples son lo que tienen dimensión 1 (copias del campo).
Queremos generalizar esta propiedad de los campos para álgebras ya que si todos los módulos son semisimples para estudiar un módulo general basta descomponerlo en submódulos simples, entender los módulos simples y luego como interactuan estos dentro del módulo original. Un álgebra es **semisimple** si todos sus módulos finitamente generados lo son. Usar esta definición para mostrar que un álgebra es semisimple parece complicado. La siguiente proposición nos da una caracterización de las álgebras semisimples.

Proposición 2.1.5. *Un álgebra A es semisimple si y solo si el $A-$módulo A es semisimple como módulo.*

Demostración. Consideremos M el $A-$submódulo de A generado por $m_1, \ldots, m_n$. Definimos el $A-$homomorfismo $f : A^n \to M$ por $(a_1, \ldots, a_n) \mapsto a_1 m_1 + \cdots + a_n m_n$. Como M es generado por $m_1, \ldots, m_n$ tenemos que f es suprayectivo. Usando el primer teorema de los isomorfismos tenemos que $M \sim A^n/Ker(f)$ lo cual es un cociente de un módulo semisimple. Por lo tanto M es semisimple. Si A es semisimple entonces todos los $A-$módulos finitos son semisimples. Tenemos que el $A-$módulo A es finito pues es generado por 1_A. Por lo tanto A es un modulo semisimple. □

A *priori* el número de módulos simples de un álgebra de dimensión no es claro que sea finito. La siguiente proposición nos dará una cota para el caso semisimple.

Proposición 2.1.6. *Si A es semisimple entonces todos los $A-$módulos simples aparecen en la descomposición semisimple de A como módulo.*

Demostración. Escribimos $A = \oplus_{i=1}^n S_i$ la descomposición semisimple de A como módulo. Consideremos S un $A-$módulo simple y $s \in S$ un elemento no nulo. Consideremos el siguiente homomorfismo $f : A \to S$ definido por $a \mapsto as$. Denotamos por f_i la restricción de este homomorfismo a S_i. Como $s \neq 0$ tenemos que $f \neq 0$ por lo que al menos para algún i_0 el homomorfismo f_i no es nulo y por el lema de Schur tenemos que $S \sim S_{i_0}$. □

Por la proposición anterior tenemos que él número de módulos simples de un álgebra esta acotado por la dimensión como $k-$espacio vectorial de esta, por lo que es finito. Esta desigualdad es una cota óptima, ya que se tiene la igualdad si y solo si el álgebra es conmutativa.
Con la definición de álgebra semisimple hemos definido una clase de álgebra que tienen un comportamiento similar a los campos, que son las álgebras mas sencillas. Con las siguientes definiciones

generalizaremos dos propiedades más de los campos, la división y el hecho de que son simples y no solo semisimples como $k-$módulos.
Un **álgebra con división** es un álgebra donde todo elemento no-nulo tiene un inverso multiplicativo. Decimos que un álgebra es **simple** si es simple como anillo, es decir, si sus únicos ideales son A y cero.
Notamos que todo campo es un ejemplo de álgebra simple y álgebra con división. Hasta ahora las definiciones de un álgebra simple y semisimple no han sido relacionada, de hecho definimos álgebra semisimple antes de definir álgebra simple. Con el siguiente resultado relacionamos ambos conceptos.

Proposición 2.1.7. *Las álgebras simples son semisimples.*

Demostración. Sea A un álgebra simple, sea M la suma de todos los A-submódulos (izquierdos) simples. Tenemos que M es un submódulo izquierdo se A y por lo tanto un ideal izquierdo. Consideremos S un submódulo simple de A y $a_0 \in A \setminus 0$. Sea $\Phi : S \to A$ el homomorfismo definido por $s \mapsto sa_0$ por el lema de Schur tenemos que $Im\Phi = Sa$ es un submódulo simple o cero de A luego $Sa \subset M$. De lo anterior tenemos que $Ma \subset M$ y por lo tanto M es un submódulo derecho de A. Hemos probado que M es un ideal bilateral de A y por lo tanto $M = A$, es decir, A es suma de módulos simples. □

Proposición 2.1.8. *Toda álgebra con división es simple.*

Demostración. Sean A un álgebra con división y $I \subset A$ un ideal no nulo. Para cualquier $a \in I \setminus 0$ tenemos que existe $a^{-1} \in A$ por lo que $1_A = a^{-1}a \in I$. Lo cual muestra que $I = A$.
□

El problema de clasificar las álgebras reales con división fue resuelto por Frobenius en el siglo IX.

Teorema 2.1.3. ***(Teorema de Frobenius).*** *Sobre el campo de los números reales existen únicamente tres álgebras con división, a saber, los reales $\mathbb{R}$, los complejos $\mathbb{C}$ y los cuaternios $\mathbb{H}$.*

Un caso mas sencillo se presenta cuando el campo es algebraicamente cerrado.

Proposición 2.1.9. *Si k es un campo algebraicamente cerrado entonces la única $k-$álgebra con división de dimensión finita es k.*

Demostración. Consideremos D una $k-$álgebra con división. Notamos que D actúa en si mismo mediante multiplicación por la derecha por lo que un elemento $d \in D$ lo podemos pensar como un elemento de $End_k(D)$. Como k es algebraicamente cerrado d tiene al menos un valor propio $a \in k$. Por definición de valor propio el *kernel* de $d - a1_D$ es no vacío y por lo tanto no es invertible. Luego como D es una anillo con división tenemos que $d - a1_D = 0$, es decir, $d = a1_D$. Por lo tanto $D \sim k$ como álgebras. □

Si el campo k no es algebraicamente cerrado entonces este resultado no es cierto ya que si consideramos una extensión de campos $k \subset K$ de este modo tendremos que K es una $k-$álgebra con división. Por otro lado es conocido que todo campo no algebraicamente cerrado admite una extensión de dimensión finita. La dimensión finita en la prueba anterior también es una hipótesis fundamental ya que el campo de fracciones $k(x)$ es una $k-$álgebra con división pero no tiene dimensión finita. Un corolario del lema de Schur es el siguiente:

Proposición 2.1.10. *Si S es un $A-$módulo simple entonces $End_A(S)$ es un álgebra con división.*

Demostración. En el álgebra $End_A(S)$ la multiplicación esta dada por la composición de endomorfismos. Por el lema de Schur todo elemento no nulo es un isomorfismo, es decir, tiene un inverso multiplicativo. □

Combinando este resultado y el anterior tenemos que si el campo base es algebraicamente cerrado entonces $End_A(S) \sim k$. Este hecho simplifica la teoría de representaciones sobre campos algebraicamente cerrados.

De aquí en adelante nos dedicaremos a entender la estructura de las álgebras semisimples. Iniciaremos por entender cuales son todas las álgebras simples.

Proposición 2.1.11. *Las álgebras de matrices sobre un álgebra con división son simples.*

Demostración. Sean D un álgebra con división y $n \in \mathbb{N}$ un número natural. Basta mostrar que $M_n(D)$ es simple. Para $i, j \in [n]$ consideramos la matriz elemental $E_{ij} \in M_n(D)$, es decir, la matriz que consta de únicamente ceros salvo en la entrada ij cuyo valor es 1. Consideremos I un ideal no nulo del álgebra $M_n(D)$. Como I es no nulo existe $M \in I$ una matriz con alguna entrada distinta de cero digamos la entrada (i, j) la cual la denotamos por a. Notamos que $E_{ii}AE_{jj} = aE_{ij}$. Como a tiene un inverso multiplicativo tenemos que $E_{ij} \in I$. Notamos que para $k \in [n]$ se tiene que $E_{ki}E_{ij}E_{jk} = E_{kk}$. Por lo tanto $E_{kk} \in I$. Además $I_n = \ E_{11} + \cdots + E_{nn} \in I$. Por lo tanto $I = M_n(D)$. □

Del teorema que mostraremos mas adelante, se seguirá que estas son las únicas álgebras simples hasta isomorfismo.

Ahora que sabemos que las álgebras de matrices son álgebras simples estamos interesados en estudiar cuales son sus módulos simples. Resulta que solo existe uno y lo podemos describir a la perfección.

Proposición 2.1.12. *Para un álgebra con división D el único $M_n(D)-$módulo simple es D^n con la acción dada por multiplicación matriz por vector.*

Demostración. Esta prueba es muy similar a la anterior. Consideremos M un $M_n(D)-$submódulo de D^n no cero. Como M no es cero tenemos que existe un vector $v \in M$ con una entrada no nula digamos la entrada i en la cual esta el elemento a. Notamos que $a^{-1}E_{ii}v = e_i \in M$. Luego procedemos a usar matrices de permutación. Para cada $j \in [n]$ existe una matriz de permutación σ tal que $\sigma e_i = e_j \in M$. Por lo tanto $M = D^n$, es decir, D^n es simple. Por como multiplicamos una matriz por un vector columna tenemos que $nD^n \sim M_n(D)$ como $M_n(D)-$módulos. De la proposición 4 se sigue que el único $M_n(D)-$módulo simple es D^n. □

Un resultado fundamental de álgebra lineal es que $End(k^n) \sim M_n(k)$ como álgebras, ya que estamos interesados en estudiar transformaciones lineales pero es mucho mas sencillo hacer cálculos con matrices. Tendremos un resultado similar para módulos, solo tenemos que definir el análogo a k^n para el caso de un álgebra. Un módulo M semisimple es **isotípico** si en su descomposición semisimple todos los módulos simples son isomorfos, es decir, $M \sim nS$ para algún módulo simple S.

En el caso del campo considerado como álgebra sobre si mismo tendremos que k^n es isotípico además como el único módulo simple es el campo mismo tendremos que todo espacio vectorial es un módulo isotípico.

Proposición 2.1.13. *Si S es un $A-$módulo simple y n un número natural, entonces $End_A(nS) \sim M_n(End_A(S))$ como álgebras.*

Demostración. En esta demostración pensaremos a nS como vectores de tamaño n con entradas en S. Y la prueba será esencialmente la misma que para el caso de álgebra lineal. Para $M \in M_n(End_A(S))$ consideramos la función $\Phi(M) : nS \to nS$ definida para cada vector $v \in nS$ el vector $\Phi(M)(v)$ tendrá las siguientes entradas:

$$\Phi(M)(v)_j = \sum_{k=1}^{n} M_{jk} v_k$$

Mostraremos que $\Phi(M)$ en efecto es un $A-$endomorfimo. Sean $v, u \in nS$ y $a \in A$ notamos que:

$$\begin{aligned}
\Phi(M)(v+u)_i &= \sum_{j=1}^{n} M_{ij}((v+u)_j) \\
&= \sum_{j=1}^{n} M_{ij} v_k + \sum_{j=1}^{n} M_{ij} u_j \\
&= \Phi(M)(v)_i + \Phi(M)(v)_i
\end{aligned}$$

Por lo que $\Phi(M)$ es aditivo. Por otro lado se tiene que:

$$\begin{aligned}
\Phi(M)(av)_i &= \sum_{j=1}^{n} M_{ij}(av_j) \\
&= a \sum_{j=1}^{n} M_{ij} v_j \\
&= a\Phi(M)(v)_i
\end{aligned}$$

Por lo que $\Phi(M)$ es $A-$lineal. Con lo anterior tenemos que se puede definir una función $\Phi : M_n(End_A(S)) \to End_A(nS)$ mediante $M \mapsto \Phi(M)$ definido como arriba. Ahora mostraremos que Φ es un homomorfismo de álgebras. Sean $M, N \in M_n(End_A(S))$ y $c \in k$ se tiene que:

$$\begin{aligned}
\Phi(M+N)(v)_i &= \sum_{j=1}^{n} (M+N)_{ij}(v)_j \\
&= \sum_{j=1}^{n} M_{ij}(v)_j + \sum_{j=i}^{n} N_{ij}(v)_j \\
&= \Phi(M)(v)_i + \Phi(N)(v)_i
\end{aligned}$$

Por lo que Φ es una función aditiva. Por otro lado notamos que:

$$\begin{aligned}
\Phi(MN)(v)_i &= \sum_{j=1}^{n} (MN)_{ij}(v)_i \\
&= \sum_{j=1}^{n} \sum_{l=1}^{n} M_{il} N_{lj}(v)_j
\end{aligned}$$

Y además:

$$\begin{aligned}\Phi(M)\circ\Phi(N)(v)_i &= \Phi(M)(\Phi(N)(v))_i\\ &= \sum_{l=1}^{n} M_{il}(\Phi(N)v_l)\\ &= \sum_{l=1}^{n} M_{il}\sum_{j=1}^{n} N_{lj}(v_j)\\ &= \sum_{l=1}^{n}\sum_{j=1}^{n} M_{il}N_{lj}(v_j)\end{aligned}$$

Por lo tanto Φ es un homomorfismo de álgebras. Por lo anterior tenemos que el álgebra $M_n(End_A(S))$ es simple y por el lema de Schur se sigue que Φ es inyectivo. Para cada $f \in End_A(nS)$ definimos $F_{ij} = P_i f I_j$, con $P_i : nS \to S$ la proyección al $i-$ésimo factor y $I_j : S \to nS$ la inclusión al $i-$ésimo sumando. Con estas entradas podemos formar una matriz $F \in M_n(End_A(S))$. Por la definición de Φ se tiene que $\Phi(F) = f$. Lo cual muestra que Φ es una función suprayectiva. Por lo tanto Φ es un isomorfismo de álgebras por lo que $End_A(nS)$ y $M_n\left(End_A(S)\right)$ son isomorfas.

□

Proposición 2.1.14. *Si M es un módulo semisimple con descomposición en componentes irreducibles $M \sim \oplus n_i S_i$, entonces $End_A(M)$ se descompone como álgebras en $\oplus_i End_A(n_i S_i)$.*

Demostración. De el lema de Schur se sigue que si $i \neq j$ entonces $Hom_A(n_i S_i, n_j S_j) = 0$ por lo cual:

$$\begin{aligned}End_A(\oplus_i n_i S_i) &= Hom_A(\oplus_i n_i S_i, \oplus_i n_i S_i)\\ &= \bigoplus_{i,j} Hom_A(n_i S_i, n_j S_j)\\ &= \bigoplus_{i} Hom_A(n_i S_i, n_i S_i)\\ &= \bigoplus_{i} End_A(n_i S_i).\end{aligned}$$

□

Proposición 2.1.15. *Para toda álgebra A se cumple que $A^{op} \sim End_A(A)$.*

Demostración. Para $f \in End_A(A)$ denotamos por $\Phi(f) = f(1)$. Mostraremos que Φ es un isomorfismo entre estas dos álgebras.
Notamos que si $f, g \in End_A(A)$ y $a \in k$ entonces:

$$\Phi(af) = (af)(1) = af(1) = a\Phi(f)$$

$$\Phi(f+g) = (f+g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$

$$\Phi(fg) = f(g(1)) = f(g(1)1) = g(1)f(1) = \Phi(g)\cdot_{op}\Phi(f).$$

□

Proposición 2.1.16. *Para toda álgebra A y $n \geq 1$ se cumple que $M_n(A)^{op} \sim M_n(A^{op})$.*

Demostración. Si $A, B \in M_n(A)$ entonces:

$$(B \cdot_{op} A)_{ij}^t = (AB)_{ij}^t = \sum_k A_{ik} B_{kj}$$

Por otro lado:

$$(B^t A^t)_{ij} = \sum_k B_{kj} A_{ik} = \sum_k A_{ik} \cdot_{op} B_{kj}$$

De lo anterior y dado que $(\cdot)^t$ es $k-$lineal tenemos que $(\cdot)^t$ es un isomorfismo de álgebras entre $M_n(A)^{op}$ y $M_n(A^{op})$. □

Teorema 2.1.4. ***(de Wedderburn)*** *Las únicas álgebras semisimples son sumas directas de álgebras de matrices sobre álgebras con división.*

Demostración. Anteriormente se mostró que las álgebras de matrices sobre álgebras con división son simples por lo que su suma directa es semisimple. Ahora consideremos un álgebra semisimple A denotamos por $S_1, .., S_m$ una colección completa de $A-$módulos simples y por $n_1, \ldots, n_m$ sus multiplicidades en la descomposición semisimple de A como módulo. Notamos que:

$$\begin{aligned} A &\sim End_A(A)^{op} \\ &\sim End_A(\bigoplus_i n_i S_i)^{op} \\ &\sim \bigoplus_i End_A(n_i S_i)^{op} \\ &\sim \bigoplus_i M_{n_i}(End_A(S_i)^{op}). \end{aligned}$$

Ya habíamos probado antes que $End_A(S_i)$ es un álgebra con división por lo que $End_A(S_i)^{op}$ también lo es.

□

Un corolario del teorema de Wedderburn es que las únicas álgebras simples son álgebras de matrices sobre anillos con división. Por otro lado notemos que si el campo base es algebraicamente cerrado entonces toda álgebra de matrices es isomorfa al álgebra de endomorfismos de un espacio vectorial $End(V)$ para algún $k-$espacio vectorial V.

2.2. Conmutadores

Dado un anillo R y un subanillo S definimos el conmutador de S en R como el conjunto de elementos de R que conmutan con todos los elementos de S, es decir:

$$C_R(S) = \{r \in R : sr = sr, \ \ \forall s \in S\}.$$

Usualmente omiteremos el subíndice R cuando sea claro del contexto de que anillo hablamos. Notamos que el conmutador de R es el centro del anillo y que además el conmutador de un subanillo es un subanillo.
Consideremos $C_R(C_R(S))$ el doble conmutador de S notemos que este contiene a S. El objetivo de esta sección es introducir el teorema del doble conmutador.

Teorema 2.2.1. ***(del doble conmutador).*** *Consideremos un espacio vectorial V de dimensión finita sobre un campo algebraicamente cerrado k, A una subálgebra semisimple del álgebra de endomorfismos de V, $S_1, \ldots, S_m$ una colección completa de $A-$módulos simples y $U_i = Hom_A(S_i, V)$. Si B es el conmutador de A en $End_k(V)$ entonces B es un álgebra semisimple, $U_1, \ldots, U_m$ forman una colección completa de $B-$módulos simples y $V = \oplus_{i=1}^m S_i \otimes_k W_i$.*

Antes de probar este teorema trabajaremos con una versión cuando A es un álgebra simple, es decir cuando $A = End(V)$ y V es el único $A-$módulo simple de A.

Proposición 2.2.1. *Consideremos k un campo álgebraicamente cerrado, V un $k-$espacio vectorial, $A = End(V)$ su álgebra de endomorfismos, $\rho : A \to End(W)$ una representación de A y $B = C_{End(V)}(A)$ el conmutador de $End(V)$.*
Se tiene que B es un álgebra simple, $U = Hom_A(V, W)$ es el único $B-$modulo irreducible, el álgebra $A \otimes B$ es simple, W es el único $A \otimes B-$módulo simple, $S : V \otimes U \to W$ definido por $v \otimes u \mapsto u(v)$ es un $A \otimes B-$isomorfismo y este último diagonaliza a ρ en el sentido que $S^{-1}\rho(a)S = a \otimes Id_U$ para toda $a \in A$.

Demostración. Notamos que U admite la estructura de B modulo mediante la composición de funciones lineales, es decir, $bu = b \circ u$. Podemos definir una estructura de $A \otimes B-$modulo en $V \otimes U$ mediante $(a \otimes b)(v \otimes u) = av \otimes bu$.
Mostraremos que S es un $A-$homomorfismo. Si $a \in A$ y $v \otimes u \in V \otimes U$ entonces:

$$\begin{aligned} S(a(v \otimes u) &= S((av) \otimes u) \\ &= u(av) \\ &= au(v) \\ &= aS(v \otimes u), \end{aligned}$$

lo cual muestra que S es un $A-$homomorfismo. Ahora se mostrará que S es un $B-$homomorfismo. Si $b \in B$ y $v \otimes u \in V \otimes U$ entonces:

$$\begin{aligned} bS(v \otimes u) &= bu(v) \\ &= (b \circ u)(v) \\ &= S(v \otimes bu), \end{aligned}$$

lo cual muestra que S es un $B-$homomorfismo. Con esto y lo anterior tenemos que S es un $A \otimes B-$homomorfismo.
Al ser A el álgebra de los endomorfismo de V tenemos que A es un álgebra simple y por lo tanto semisimple. Como V es el único $A-$módulo simple tenemos que la descomposición de W en módulos simples es $W \sim nV$ para algún $n \in \mathbb{N}$. Tenemos que $U = Hom_A(V, W) \sim Hom_A(V, nV) = nHom_A(V, V) = nk$ por lo que $\dim U = n$. De lo anterior tenemos que $\dim W = n \dim V = \dim V \otimes U$ por lo tanto para mostrar que S es un isomorfismo basta probar que es suprayectiva.
Para mostrar que S es simple basta mostrar que el homomorfismo $s_0 : Hom_A(V, nV) \otimes V \to nV$ dado por $s_o(\otimes v) = f(v)$ es sobre. Sea $v \in V \setminus 0$ notamos que como $A-$módulo V está generado por v. Sea $f_i \in End(V, nV)$ la inclusión de V en la $i-$ésima coordenada. Claramente nV está generado por $f_1(v), \ldots, f_n(v)$ como $A-$módulo. Por lo tanto s_0 es sobre. Por la proposición 2.1.13 tenemos que:

$B = End_A(W) \sim M_n(k) \sim End(V)$ Lo cual muestra que B es un álgebra simple y de esto se sigue de tiene un único módulo simple hasta isomorfismo el cual debe de tener dimensión n y por lo tanto este módulo es U. Además tenemos que:

$$\begin{aligned} S^{-1}\rho(a)S(v\otimes u) &= S^{-1}\rho(a)u(v) \\ &= aS^{-1}u(v) \\ &= av\otimes u, \end{aligned}$$

por lo que S diagonaliza la acción de $A\otimes B$. □

Un resultado que se sigue de la demostración anterior es que si V, W son espacios vectoriales entonces $C(End(V)\otimes k) = k\otimes End(W)$ en el álgebra $End(V\otimes W)$.

Este último resultado es el teorema del doble conmutador para álgebras simples. Ahora vamos a extender el resultado anterior para el caso de álgebras semisimples, como ya lo habíamos enunciado anteriormente.

Demostración. Como A es una subálgebra de $End_k(V)$ actúa en V mediante la evaluación además:

$$B = C_{End_k(V)}(A) = \{f\in End_k(V) : fa = af\ ,\ \forall a\in A\} = End_A(V).$$

Análogamente se tiene que:

$$C_{End_k(V)}(B) = End_B(V).$$

Por otro lado como A es un álgebra semisimple entonces V es un módulo semisimple por lo que admite una descomposición en módulos simples $V = \oplus_{i=1}^m k_iS_i$. Usando la descomposición anterior podemos ver que:

$$B = End_A(V) = Hom_A\left(\bigoplus_{i=1}^m k_iS_i, \bigoplus_{i=1}^m k_iS_i\right) = \bigoplus_{i,j=i}^m Hom_A(k_iS_i, k_jS_j.)$$

Del lema de Schur se sigue que si $i\neq j$ entonces $Hom_A(k_iS_i, k_jS_j) = 0$ por lo que podemos reescribir lo anterior como:

$$B = \bigoplus_{i=1}^m Hom_A(k_iS_i, k_iS_i) = End_A(k_iS_i) \sim \bigoplus_{i=1}^m M_{k_i}(End_A(S_i)).$$

Notamos que todos los anteriores fueron isomorfismos de álgebras.
Por otro lado recodamos que $M_{k_i}(End_A(S_i))$ es un álgebra simple por lo cual B es un álgebra semisimple. Recordemos que $B = End_A(V)$ y que $W_i = Hom_A(U_i, V)$ notamos que si $f\in End_A(V)$ y $g\in Hom_A(U_i, V)$ entonces $f\circ g\in Hom_A(U_i, V) = W_i$. Como la composición de funciones lineales se distribuye en la suma y es asociativa se tiene que W_i es un $B-$módulo. Mostraremos que es un módulo simple.

Por otro lado por el teorema de Wedderburn tenemos que los $B-$módulos simples son precisamente $W_i = Hom_A(U_i, V)$. □

2.3. El álgebra de un grupo

Denotaremos por G a un grupo finito. En está sección usaremos la notación multiplicativa para G, es decir, la operación de G la escribiremos como producto y al elemento identidad de G lo denotaremos por e. Estudiaremos una forma de extender la multiplicación de G para obtener un álgebra. Consideremos el $\mathbb{C}-$espacio vectorial libre generado por los elementos de G, a este espacio lo podemos dotar de un producto extendiendo el producto en G de la siguiente manera:

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} a_g b_h gh.$$

Este producto no es mas que la extensión bilineal del producto de G y define un álgebra. Está estructura es conocida como el álgebra de grupo y es denotada por $\mathbb{C}[G]$.
Esta construcción es universal en el siguiente sentido.

Proposición 2.3.1. *Si A es un álgebra asociativa compleja y $f_0 : G \to U(A)$ es un homomorfismo de G al grupo de unidades de A entonces existe un único homomorfismo de álgebras $f : \mathbb{C}[G] \to A$ que extiende a f_0 , es decir si $i : G \to \mathbb{C}$ es la inclusión, se cumple que $f_0 = f \circ i$.*

Por otro lado si $f : \mathbb{C}[G] \to A$ es un homomorfismo de álgebras y $g \in G$ entonces g es una unidad del álgebra de grupo por lo cual $f(g)$ es una unidad de A. De lo anterior podemos restringir a f a un homomorfismo de grupos $f_0 : G \to U(A)$. De lo anterior notamos que hay una abyección natural entre los conjuntos $Hom(G, U(A))$ y $Hom(\mathbb{C}[G], A)$, donde el conjunto izquierdo se refiere a homomorfismos de grupos mientras que el derecho a homomorfismos de álgebras.

Otra forma de escribir el resultado anterior es que toda representación de $\rho : G \to Gl(V)$ puede obtenerse como la restricción de un homomorfimo de álgebras $f_\rho\mathbb{C}[G] \to End(V)$ y todo homomorfismo de álgebras $f\mathbb{C}[G] \to A$ puede restringirse a una representación $\rho_f : G \to End(A)$. Por lo que hay un diccionario entre representaciones de G y $\mathbb{C}[G]-$módulos. Bajo la correspondencia anterior la representación regular se corresponde con el módulo $\mathbb{C}[G]$. La idea de estudiarlos de esta manera es que usaremos los teoremas del doble conmutador y de Wedderburn para deducir propiedades acerca de la representación regular.
Un hipótesis indispensable en ambos teoremas es la semisimplicidad del álgebra lo cual probaremos en la siguiente proposición.

Teorema 2.3.1. *El álgebra $\mathbb{C}[G]$ es semisimple.*

Demostración. Basta mostrar que $\mathbb{C}[G]$ es un módulo semisimple. Consideremos $M \subset \mathbb{C}[G]$ un submódulo. En particular M es un subespacio vectorial de $\mathbb{C}[G]$ por lo cual existe V un subespacio complementario. Sea $\pi_0 : \mathbb{C}[G] \to \mathbb{C}[G]$ la proyección de $\mathbb{C}[G]$ es M. Definimos $\pi(v) = \frac{1}{|G|}\sum_{g\in G} g\pi_0(g^{-1}v)$ para $v \in \mathbb{C}[G]$. Vamos a probar que π es un $\mathbb{C}[G]-$homomorfismo. Sean $g_0 \in G$ y $v \in \mathbb{C}[G]$ notamos que:

$$\pi(g_0 v) = \frac{1}{|G|}\sum_{g\in G} g\pi_0(g^{-1}g_0 v).$$

Sea $h = g_0^{-1}g$ notamos que $h^{-1} = g^{-1}g_0$. Cambiando los indices tenemos que:

$$\frac{1}{|G|}\sum_{g\in G} g\pi_0(g^{-1}g_0 v) = \frac{1}{|G|}\sum_{h\in G} g_0 h\pi_0(h^{-1}v) = g_0\pi(v),$$

por lo cual π es un $G-$homomorfismo. Como $Im(\pi_0) = M$ y este es un $\mathbb{C}[G]-$submódulo tenemos que $Im(\pi) \subset M$. Como π_0 es una proyección en M. Tenemos para $m \in M$ y $g \in G$ que $g\pi_0(g^{-1}m) = m$ por lo cual $\pi(m) = m$. Lo anterior muestra que π es un una proyección de $\mathbb{C}[G]$ sobre M. Como π es un $G-$homomorfismo es tenemos que su kernel es un submódulo y además $\mathbb{C}[G] = M \oplus Ker(\pi)$. Esto muestra que $\mathbb{C}[G]$ es semisimple como $\mathbb{C}[G]-$módulo y por lo tanto como álgebra. □

La técnica de promediar una transformación lineal sobre el grupo para obtener un homomorfismo sobre $\mathbb{C}[G]$ es muy útil y no es la primera vez que la usamos. En el capitulo anterior hicimos algo similar para mostrar el teorema de descomposición isotípica.

Proposición 2.3.2. *Hay tantos $\mathbb{C}[G]-$módulos simples como clases de conjugación en G.*

Consideremos $S_1, \ldots, S_r$ una colección completa de $\mathbb{C}[G]-$módulos denotamos por n_i la multiplicidad de S_i en $\mathbb{C}[G]$ la cual no es nula ya que todo módulo simple aparece como submódulo en el álgebra. El teorema de Wedderburn establece que $\mathbb{C}[G] \sim \oplus_{i=1}^{r} M_{n_i}(\mathbb{C})$ como estas álgebras son isomorfas tenemos que sus centros son son isomorfos, es decir, $Z(\mathbb{C}[G]) \sim \oplus_{i=1}^{r} Z(M_{n_i}(\mathbb{C})$. Por otro lado sabemos que el centro del álgebra $M_n(\mathbb{C})$ son los múltiplos escalares de la matrices identidad por lo cual $\dim_{\mathbb{C}} Z(M_n(\mathbb{C})) = 1$. Por lo tanto $dim_{\mathbb{C}} Z(\mathbb{C}[G]) = r$. Ahora vamos a mostrar que:

$$Z(\mathbb{C}[G]) = \left\{ \sum_{g \in G} a_g g \ : \ a_g = a_{hgh^{-1}} \, g, h \in G \right\}.$$

Sea $C \subset G$ una clase se conjugación y $g_0 \in G$ un elemento. Se tiene que:

$$g_0^{-1} \sum_{g \in C} g g_0 = \sum_{g \in C} g_0^{-1} g g_0 = \sum_{g \in C} g.$$

Por lo tanto $\sum_{g \in C} g$ conmuta con todos los elementos del grupo y por lo tanto está en el centro de $\mathbb{C}[G]$. Notamos que el lado derecho de 2.3 está generado por todos los elementos de la forma $\sum_{g \in C} g$ variando C sobre todas las clases de conjugación de G. Sea $\sum_{g \in G} a_g g \in Z(\mathbb{C}[G])$ y $h_1, h_2 \in G$. Tenemos que $\sum_{g \in G} a_g g$ conmuta con todos los elementos de G por lo cual $h_1^{-1} \sum_{g \in G} a_g g h_1 = \sum_{g \in G} a_g g = \sum_{g \in G} a_{h_1 g h_1^{-1}} g$. Comparando el coeficiente de h_2 en ambos lados tenemos que $a_{h_2} = a_{h_1 h_2 h_1^{-1}}$ por lo tanto $\sum_{g \in G} a_g g \in \left\{ \sum_{g \in G} a_g g \ : \ a_g = a_{hgh^{-1}} \, g, h \in G \right\}$ lo cual muestra la igualdad 2.3. Notamos que bajo la correspondencia entre $\mathbb{C}[G]-$módulos y G-representaciones se correspondes módulos simples con representaciones irreducibles por lo que el resultado anterior se sigue que hay tantas representaciones irreducibles como clases de conjugación de G. También recordamos que los caracteres de las representaciones irreducibles son ortogonales en el espacio de funciones de clase como hay tantos caracteres irreducibles como la dimensión de espacio tenemos el siguiente resultado.

Proposición 2.3.3. *Los caracteres de representaciones irreducibles forman una base ortonormal del espacio de funciones de funciones de clase.*

La descomposición en componentes isotíticas de una representación es importante ya que es única y se puede escribir una fórmula para las proyecciones asociadas a la descomposición por otro lado la descomposición semisimple del álgebra de grupo es importante ya que nos permite probar resultados como el anterior. Un hecho que será fundamental adelante es que estas descomposiciones coinciden.

Proposición 2.3.4. *El álgebra $\mathbb{C}[G]$ tiene descomposición semisimple e isotípica $\oplus_{\lambda \in I} End(V_\lambda)$ de modo que $(V_\lambda)_\lambda \in I$ es una colección completa de representaciones irreducibles*

Demostración. Del teorema de Weddernburn se tiene que $\oplus_{\lambda \in I} End(V_\lambda)$ es la descomposición semisimple de $\mathbb{C}[G]$ como álgebra. Para mostrar que también es descomposición isotípica notamos que cada ideal $End(V_\lambda)$ tiene descomposición como $\mathbb{C}[G]-$módulo irreducible como $\dim(V_\lambda)V_\lambda$ por otro lado si $\lambda_1, \lambda_2 \vdash n$ son particiones distintas notamos que el álgebra $\mathbb{C}[G]$ actúa en $End(V_{\lambda_i})$ mediante la inclusión . Por lo que la descomposición isotípica coincide con la descomposición de álgebra semisimple. $\square$

Capítulo 3

Probabilidad Libre y Matrices Aleatorias

Muchas veces en la teoría clásica de la probabilidad no se trabaja directamente con las variables aleatorias sino con sus distribuciones. De forma aún más indirecta, pueden deducirse muchas propiedades de distribuciones (conjuntas) en función de sus momentos, como por ejemplo, la media y la (co-)varianza y la noción de independencia. La probabilidad algebraica (o no-conmutativa) hace énfasis y uso de esta aproximación a la probabilidad en términos de momentos.

En este capítulo se expondrán los fundamentos de la teoría de probabilidad no conmutativa, comenzando con el concepto básico de espacio de probabilidad no conmutativo $(\mathcal{A}, \tau)$. En la brevedad posible, introducimos la noción de independencia libre y su relevancia en la teoría de matrices aleatorias.

Además se introducen los espacios de probabilidad valuados en operadores, que corresponden a reemplazar el funcional lineal $\tau : \mathcal{A} \to \mathbb{C}$ (que se piensa como la esperanza), por una esperanza condicional $\mathbb{F} : \mathcal{A} \to \mathcal{B} \subset \mathcal{A}$. Para los propósitos de esta tesis, nos basta con adentrarnos en el caso en el que el álgebra $\mathcal{B}$ es de dimensión finita, generado por proyecciones ortogonales.

Entre otras cosas, considerar espacios de probabilidad en esta generalidad permite interpretar sumas convexas de medidas como convoluciones aditivas con respecto a una esperanza condicional, o equivalentemente, considerar variables aleatorias ortogonales como independientes. Entonces, descomposiciones en sumas directas de operadores (cruciales en la teoría de representaciones) son manifestaciones de una noción muy general de independencia algebraica (en el sentido de Ben Ghorbal y Schürmann [8]).

Por último se introducirán las matrices aleatorias y se bosquejarán demostraciones compactas y sencillas de algunos resultados clásicos y recientes en matrices aleatorias, como los teoremas de Wigner [16, 17], Marcěnko-Pastur [1] y Voiculescu [15], sobre el comportamiento espectral asintótico de matrices aleatorias Gaussianas y determinísticas. El caso de matrices unitarias aleatorias con distribución de Haar (que son la parte polar de las matrices de Ginibre Gaussianas) es mucho más difícil, pues no admite una aproximación combinatorica inmediata.

A diferencia del caso Gaussiano, donde las entradas (Gaussianas) son independientes entre sí y por lo tanto sus momentos y cumulantes son simples, la distribución conjunta de las entradas de una matriz unitaria aleatoria no es nada sencilla. El objetivo principal de la tesis es describir formulas para tales momentos mixtos, siguiendo los trabajos de Collins [6] Collins y Sniady [5]. Estas fórmulas permiten una demostración combinatórica de los resultados de independencia libre asintótica de Voiculescu para matrices unitarias aleatorias, que se bosqueja al final del último capítulo.

3.1. Definiciones y conceptos básicos

Definición 3.1.1. *Un espacio de probabilidad algebraico, o espacio de probabilidad no conmutativa (EPNC) es un par* $(\mathcal{A}, \tau)$ *donde* $\mathcal{A}$ *es una álgebra compleja y* $\tau : \mathcal{A} \to \mathbb{C}$ *un funcional lineal y unitario, es decir,* $\tau(1_{\mathcal{A}}) = 1$.

Típicamente $\mathcal{A}$ *estará dotada de una involución anti-lineal* $* : \mathcal{A} \to \mathcal{A}$ *y* τ *será positivo con respecto a esta involución (es decir,* $\tau(aa^*) \geq 0$ *para todo* $a \in \mathcal{A}$*) en este caso diremos que* $(\mathcal{A}, \tau, *)$ *es un* $*-$*espacio de probabilidad.*

En un $*-$espacio de probabilidad decimos que una variable a es **normal** si $aa^* = a^*a$, **auto adjunta** o **real** si $a^* = a$ ó **unitaria** si $aa^* = a^*a = 1$. Decimos que el funcional τ es positivo si $\tau(aa^*)$ es no negativo para cada $a \in \mathcal{A}$, fiel si $\tau(aa^*) = 0$ solo cuando $a = 0$ y tracial cuando $\tau(ab) = \tau(ba)$ para cualesquiera $a, b \in \mathcal{A}$. La nomenclatura fue heredada del estudio de álgebras de operadores sobre espacios de Hilbert en muchos de los ejemplos los espacios de probabilidad admiten una representación de este estilo.

Los ejemplos mas sencillos de espacios de probabilidad algebraicos son matrices complejas deterministicas $(M_n(\mathbb{C}), \tau)$ con su involución usual. Dado un producto interior $\langle , \rangle$ en $\mathbb{C}^n$ y un vector unitario $v \in \mathbb{C}^n$, el funcional $\tau := \tau_v$ definido como el vector estado $A \mapsto \langle Av, v\rangle$. En particular, si $(e_i)_{i\leq n}$ es la base ortonormal estándar de $\mathbb{C}^n$, el funcional τ_{e_i} es simplemente la i-ésima entrada en la diagonal $\tau_{e_i}(A) = (A_{ii})$.

Para una colección de funcionales $\tau_i : \mathcal{A} \to \mathbb{C}$ de tal forma que cada par $(\mathcal{A}, \tau_i)$ sea un EPNC, se tiene que cualquier suma convexa $\tau = \sum \lambda_i \tau_i$ el par $(\mathcal{A}, \tau)$ es un EPNC. Un caso notable, ampliamente estudiado es la traza normalizada $\tau = \frac{1}{n}\sum_{i\leq n} \tau_{e_i} = \frac{1}{n}\mathrm{Tr}$.

El segundo ejemplo fundamental se obtiene en el contexto de un espacio clásico de probabilidad $(\Omega, \mathcal{F}, \mathbb{P})$. Se puede considerar el álgebra de variables aleatorias complejas $\mathcal{F}$-medibles con soporte acotado $\mathcal{A}_{\mathcal{F}} = L^\infty(\Omega, \mathcal{F})$ y funcional dado por la esperanza usual $\tau = \mathbb{E} : X \mapsto \int_\Omega X \mathrm{d}\mathbb{P}$. La involución está dada por la conjugación puntual de una variable aleatoria compleja ($X^*(\omega) = \bar{X}(\omega)$, para todo $\omega \in \Omega$).

Recordemos que muchas medidas de probabilidad están determinadas por sus momentos. En el caso real $X = X^*$, los momentos son simplemente la sucesión $(\mathbb{E}(X^m))_{m\geq 1}$, en el caso complejo, los momentos son $(\mathbb{E}(Z^m \bar{Z}^n))_{m,n\geq 1}$.

El hecho de que dos (o más) variables aleatorias sean independientes es equivalente a que sus momentos mixtos se factoricen. Es decir, que para variables reales se tenga $\mathbb{E}(X^mY^n) = \mathbb{E}(X^m)\mathbb{E}(Y^n)$, para todo $m, n \geq 1$ y para variables complejas $\mathbb{E}(Z^{m_1}\bar{Z}^{m_2}W^{n_1}\bar{W}^{n_2}) = \mathbb{E}(Z^{m_1}\bar{Z}^{m_2})\mathbb{E}(W^{n_1}\bar{W}^{n_2})$, para todo $m_1, m_2, n_1, n_2 \geq 0$.

La nomenclatura se hereda de este último ejemplo: Nos referimos a los elementos del álgebra $\mathcal{A}$ como variables aleatorias no conmutativas o simplemente como variables aleatorias y para una variable aleatoria $a \in \mathcal{A}$ la sucesión $\tau(a), \tau(a^2), \ldots, \tau(a^n)\ldots$ es conocida como los momentos de a. Más generalmente, para una colección de variables aleatorias $\mathbf{a} = (a_1, \ldots, a_k) \in \mathcal{A}^k$, llamamos momento mixto a cualquier expresión de la forma $\tau(a_{i(1)}a_{i(2)}\ldots a_{i(m)})$, para $i : [m] \to [k]$.

Antes de continuar con más definiciones importantes, notemos que la variable aleatoria dada por la matriz (autoadjunta)

$$B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in (M_2(\mathbb{C}), \frac{1}{2}\mathrm{Tr})$$

y la variable aleatoria b resultante de lanzar una moneda justa con valores ± 1, es decir, una variable aleatoria con distribución Bernoulli simétrica $\mu_b = \frac{1}{2}(\delta_1 + \delta_{-1})$ tienen exactamente los mismos momentos. En efecto: B^2 es la matriz identidad I_2 y b^2 es la variable aleatoria constante

1 por lo que los momentos son simplemente $(\frac{1}{2}\mathrm{Tr}(B^n))_{n\geq 1} = (\frac{1}{2}\mathrm{Tr}(B), \frac{1}{2}\mathrm{Tr}(I_2), \frac{1}{2}\mathrm{Tr}(B), \dots)$ y $(\mathbb{E}(b^n))_{n\geq 1} = (\mathbb{E}(b), \mathbb{E}(\mathbf{1}), \mathbb{E}(b), \mathbb{E}(\mathbf{1}), \dots)$. Como además $\frac{1}{2}\mathrm{Tr}(I_2) = 1 = \mathbb{E}(\mathbf{1})$, y $\mathrm{Tr}(B) = 0 = \mathbb{E}(b)$ concluimos que todos los momentos coinciden.

Hay varias formas de recolectar toda la información acerca de los momentos de una variable o una k-tupla de variables aleatorias. La primera es puramente algebraica, basada en el álgebra $\mathbb{C}\langle X_1, X_2, \dots, X_k\rangle$ de polinomios en k-indeterminadas que no conmutan y producto dado por concatenación .

Definición 3.1.2. *La distribución algebraica de una variable aleatoria $a = (a_1, \dots, a_k)$ es el funcional lineal $\mu_{\mathbf{a}} : \mathbb{C}\langle X_1, X_2, \dots, X_k\rangle \to \mathbb{C}$ determinado por*

$$\mu_{\mathbf{a}}(X_{i(1)}X_{i(2)} \cdots X_{i(m)}) = \tau(a_{i(1)}a_{i(2)} \cdots a_{i(m)}).$$

Notamos que la definición de distribución no depende de todo el espacio donde esté la variable, siendo posible que dos variables en distintos espacios de probabilidad tengan la misma distribución.

Si estamos en un espacio con la estructura adicional de $*-$espacio de probabilidad podemos hablar de la $*-$distribución de una variable aleatoria a, es decir, de momentos mixtos de a y a^*; expresiones de la forma $\tau(a^{\varepsilon_1} \cdots a^{\varepsilon_n})$ de modo que $\varepsilon_i \in \{1, *\}$.. Definimos la $*-$ distribución de un vector aleatorio $(a_1, ..., a_n)$ como la distribución de $(a_1, a_1^*, \cdots, a_n, a_n^*)$.

En probabilidad clásica uno suele estar interesado al fin de cuentas en la medida de probabilidad asociada a una variable aleatoria y no directamente en ella misma o sus momentos, como es el caso de los teoremas límite. Por ejemplo, a la variable aleatoria Bernoulli b del ejemplo anterior le asociamos su medida de probabilidad $\mu_b = \frac{1}{2}(\delta_1 + \delta_{-1})$ y de esta podemos recuperar los momentos de la variable aleatoria.

En este caso, es importante que estamos hablando de una variable aleatoria real. Cuando la variable aleatoria a es compleja, no es posible deducir su medida de probabilidad asociada de los valores de $\tau(a^n)$. Sin embargo, sí es posible determinar μ_a si conocemos todos los momentos mixtos del par (a, a^*) y la variable es normal bajo condiciones muy generales, por ejemplo, si el soporte de a es compacto.

Para el caso general de una matriz normal A (es decir, $AA^* = A^*A$) en el espacio $(M_n(\mathbb{C}), \frac{1}{n}\mathrm{Tr})$, los momentos mixtos de (A, A^*) quedan completamente determinados por los valores del funcional $\frac{1}{n}Tr$ evaluados en las matrices $\{A^n A^{*m}\}$. Para el caso de matrices normales, sabemos que la condición $AA^* = A^*A$ es equivalente a la condición de que A y A^* son simultáneamente diagonalizables por una matriz unitaria: $A = U\Lambda U^*$, $A = U\Lambda^* U^*$, con Λ una matriz diagonal con los valores propios de A.

Observemos que, para todo $m \geq 1$ y todo $\varepsilon = (\varepsilon(1), \dots, \varepsilon(m)) \in \{1, *\}^m$ con $\varepsilon_1 = |i \in [m] : \{\varepsilon(i) = 1\}|$, $\varepsilon_* = |i \in [m] : \{\varepsilon(i) = *\}|$,

$$\frac{1}{n}\mathrm{Tr}(A^{\varepsilon(1)}A^{\varepsilon(2)} \cdots A^{\varepsilon(m)}) = \mathrm{Tr}(\Lambda^{\varepsilon(1)}\Lambda^{\varepsilon(2)} \cdots \Lambda^{\varepsilon(m)}) = \sum_{i\in[n]} \lambda_i^{\varepsilon_1}(\overline{\lambda_i})^{\varepsilon_*}.$$

Por tanto si A es normal, los momentos de (A, A^*) corresponden a los momentos de la medida compleja uniforme en los valores propios con multiplicidad $(\lambda_1(A), \lambda_2(A), \dots \lambda_n(A))$ de A. Es decir, los momentos de A quedan codificados en la medida uniforme con átomos en los valores propios: $\mu_A = \frac{1}{n}\sum_{i\in[n]} \delta_{\lambda_i(A)}$. A esta medida se le conoce como **medida espectral** de A.

Definición 3.1.3. *La distribución analítica de una variable aleatoria normal a es una medida compleja tal que:*

$$\tau(a^k(a^*)^l) = \int_{\mathbb{C}} z^k \bar{z}^l d\mu(z).$$

Notamos que no siempre existe dicha medida y de existir no necesariamente es única. En caso de que exista y tenga soporte compacto, está univocamente determinada por los $*$-momentos de a, ya que las medidas con soporte compacto lo están. En vista de lo expuesto anteriormente, en el espacio de probabilidad $(M_n(\mathbb{C}), \frac{1}{n}\mathrm{Tr})$, la medida μ_A asociada a toda matriz normal es simplemente su medida espectral.

En general no siempre es posible siempre asociar una medida de probabilidad a una tupla de variables aleatorias. En muchos casos, nos conformamos con entender la distribución algebraica de una colección de variables.

Las distribuciones algebraicas conjuntas son de gran utilidad. Por ejemplo, si comprendemos la distribución de (a_1, a_1^*, a_2, a_2^*), en particular entendemos la distribución de variables autoadjuntas como $a = a_1a_2a_2^*a_1^*$ o $b = (a_1 + a_1^*) + (a_2 + a_2^*)$. Existen actualmente trucos muy útiles que permiten calcular distribuciones analíticas en base a distribuciones conjuntas. Muchas se basan en relaciones entre distribuciones conjuntas y distribuciones con respecto a una esperanza condicional (como ejemplo notable hacemos referencia al artículo reciente de Belinschi Mai y Speicher [13]).

A continuación presentamos algunos ejemplos de distribuciones conjuntas.

1). Unidades Matriciales. Las "matrix units"son la familia de matrices $(E_{ij})_{i,j\in[n]}$ en el EPNC $(M_n(\mathbb{C}, \frac{1}{n}\mathrm{Tr})$ de modo que E_{ij} es la matriz que consta de únicamente ceros salvo en la entrada (i, j) donde tiene un 1. Estas matrices son una base ortonormal respecto al producto interno usual en $M_n(\mathbb{C})$. Notamos que $E_{ij}E_{kl} = \delta_{jk}E_{il}$ y que $E_{ij}^* = E_{ji}$ por lo que la distribución conjunta de estas matrices solo depende de los momentos individuales, los cuales son:

$$\tau(E_{ij}) = \frac{\delta_{ij}}{n}.$$

2). Consideremos ahora, para matrices deterministicas $A \in M_n(\mathbb{C}), B \in M_m(\mathbb{C})$, los encajes $\tilde{A} = (A \otimes I_m), \tilde{B} = (I_n \otimes B) \in M_n(\mathbb{C}) \otimes M_m(\mathbb{C}) \cong M_{mn}(\mathbb{C})$. Observemos que A en $(M_n(\mathbb{C}), \frac{1}{n}Tr)$ tiene la misma distribución que $\tilde{A}$ en $(M_{nm}(\mathbb{C}), \frac{1}{nm}Tr) \cong (M_m(\mathbb{C}) \otimes M_{mn}(\mathbb{C}), \frac{1}{n}Tr \otimes \frac{1}{m}Tr)$. Lo mismo ocurre con B y su encaje $\tilde{B}$

Así podemos considerar a $M_n(\mathbb{C}) \cong M_n(\mathbb{C}) \otimes I_m$ y a $M_m(\mathbb{C}) \cong I_n \otimes M_m(\mathbb{C})$ como subálgebras de $M_n(\mathbb{C}) \otimes M_m(\mathbb{C}) \cong M_{nm}(\mathbb{C})$. Notemos que dichas álgebras conmutan (debido a la propiedad del producto tensorial $(a \otimes b)(c \otimes d) = ac \otimes bd$), y además

$$\frac{1}{nm}\mathrm{Tr}(A \otimes B) = (\frac{1}{nm}\mathrm{Tr}(A \otimes I_m))(\frac{1}{nm}\mathrm{Tr}(I_n \otimes B)),$$

para todo $\tilde{A} = A \otimes I_m \in M_n(\mathbb{C}) \otimes I_m$ y para todo $\tilde{B} = I_n \otimes B$. En particular,

$$\frac{1}{nm}\mathrm{Tr}(\tilde{A}^{k_1}\tilde{B}^{k_2}) = \frac{1}{nm}\mathrm{Tr}(\tilde{A}^{k_1})\frac{1}{nm}\mathrm{Tr}(\tilde{B}^{k_2}).$$

Si uno reemplaza el símbolo $\frac{1}{nm}\mathrm{Tr}$ por $\mathbb{E}$, reconocemos la caracterización de independencia en términos de momentos.

3. En la presencia de proyecciones ortogonales $P_1, P_2, \ldots, P_k$, se puede calcular la distribución de $(P_1A_1P_1, P_2A_2P_2, \ldots, P_kA_kP_k)$ de manera muy sencilla (pues, por ortogonalidad, los momentos mixtos se anulan). Entonces la distribución conjunta queda completamente determinada por la colección de distribuciones individuales de cada $P_iA_iP_i$. En la siguiente sección veremos que son de hecho independientes, con respecto a una esperanza condicional muy general.

El siguiente ejemplo muestra la estrecha relación entre la teoría de probabilidad libre y no conmutativa con la teoría de representaciones de grupos (iniciada por Voiculescu implícitamente e impulsada por Biane, Xu, Collins y Sniady).

4. Sea G un grupo finito y $\rho : G \to M_n(\mathbb{C})$ una representación. Entonces la distribución conjunta de $(\rho(g), g \in G)$ está completamente determinada por los valores de $(\frac{1}{n}\mathrm{Tr}(\rho(g)))_{g\in G}$. Esto es solamente una normalizan del caracter de una representación, y como este determina la representación hasta isomorfismo, podemos decir que una representación está determinada por la distribución conjunta de $(\rho(g), g \in G)$.

Los bloques que construyen la teoría de representaciones son las representaciones irreducibles. El producto tensorial también es de crucial importancia en representaciones: Si $\rho_1 : G \to M_n(\mathbb{C})$ y $\rho_2 : H \to M_m(\mathbb{C})$ son representaciones irreducibles, entonces $\rho_1 \otimes \rho_2 : G \times H \to M_n(\mathbb{C}) \otimes M_m(\mathbb{C})$ es una representación irreducible de $G \times H$ y de hecho, toda representación irreducible de $G \times H$ es de esta forma.

4.1. Representación regular. Para algún orden de los elementos del grupo $g_1, g_2, \ldots, g_{|G|}$, la representación regular $\rho_{reg} : G \to M_{|G|}(\mathbb{C})$ se ve como la matriz de permutación asociada a la operación de multiplicar por g. Esto es, $(\rho_{reg}(g))_{i,j} = 1$ si $\rho(g_i) = g_j$ y cero en otro caso. Si pensamos a $M_{|G|}(\mathbb{C})$ con la traza normalizada, resulta que $\frac{1}{|G|}Tr(\rho(g)) = 0$, a menos que se trate del elemento neutro $g = e$, en cuyo caso el momento da 1.

Es decir, la representación regular induce una colección de variables aleatorias no-conmutativas (específicamente, una colección de matrices unitarias determinísticas) de tal forma que la traza normalizada anula a todo excepto a la identidad.

Este espacio de probabilidad no-conmutativo $(\langle \rho(g) : g \in G\rangle, \frac{1}{|G|}\mathrm{Tr} =: \tau_e)$, es central en la defunción de independencia libre.

Voiculescu hizo la observación fundamental de que, al considerar productos libres de grupos G y H (con identificación de unidades), el estado τ_e en el producto libre cumple que

$$\tau_e(g_1 h_1 g_2 h_2 \ldots) = 0$$

siempre que $\tau_{e_G}(g_i) = 0 = \tau_{e_H}(h_k)$. Observemos que estas hipótesis se cumplen siempre que $g_i \in G \setminus e_G$ y $h_i \in H \setminus e_H$. Entonces el producto alternado de elementos no triviales necesariamente es no-trivial (por las propiedades del producto libre de grupos) y funcional correspondiente se anula en dicho producto alternado.

De esta forma, se caracterizan productos libres de grupos y sus funcionales de manera similar a como se caracteriza la independencia de variables aleatorias en términos de productos tensoriales y la contemporización de los momentos mixtos.

Voiculescu se inspiró en esta propiedad de contemporización para acuñar su **independencia libre**, y posteriormente observó que las matrices aleatorias famosas (e.g. Ginibre, GUE, Wishart, Unitarias aleatorias) grandes se comportan, asintóticamente, como variables aleatorias libres (ver secciones 3 y 4).

Definición 3.1.4. *Sean $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k \subseteq \mathcal{A}$ subálgebras con unidad en un EPNC. Para todo $a \in \mathcal{A}$, sea $\dot{a} = a - \tau(a)$ Decimos que $\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_k$ son libres, si*

$$\tau(\dot{a}_1 \dot{a}_2 \ldots \dot{a}_m) = 0,$$

siempre que $a_i \in \mathcal{A}_{j(i)}$ sean tales que $j(1) \neq j(2) \neq j(3) \neq \cdots \neq j(m)$.

Para poder capturar ejemplos importantes en representaciones, extendemos nuestras consideraciones al caso de espacios de probabilidad valuados en operadores.

3.2. Espacios de Probabilidad valuados en operadores

Definición 3.2.1. *Un espacio de probabilidad valuado en operadores es una terna* $(\mathcal{A}, \mathcal{B}, \mathbb{F})$ *donde* $\mathcal{B} \subset \mathcal{A}$ *son álgebras asociativas y el mapa* $\mathcal{B}$*-lineal* $\mathbb{F} : \mathcal{A} \to \mathcal{B}$ *es una esperanza condicional. Es decir para cualesquiera* $a \in \mathcal{A}$, $b, b' \in \mathcal{B}$

$$\mathbb{F}(bab') = b\mathbb{F}(a)b' \quad \mathbb{F}(b) = b.$$

Típicamente, $\mathcal{A}$ *y* $\mathcal{B}$ *son álgebras con (la misma) unidad. En este contexto espacio de probablidad* $(\mathcal{A}, \tau)$ *se puede identificar con un EPVO con* $\mathcal{B} = 1_{\mathcal{A}}\mathbb{C}$.

Una esperanza condicional $\mathbb{F}_1 : \mathcal{A} \to \mathcal{B}_1$ es compatible con otra $\mathbb{F}_2 : \mathcal{A} \to \mathcal{B}_2$ si $\mathbb{F}_1 \circ \mathbb{F}_2 = \mathbb{F}_1$.

En el marco de una esperanza condicional $\mathbb{F} : \mathcal{A} \to \mathcal{B}$, la distribución conjunta de una colección de variables $(a_1, a_2, \ldots a_k) \in \mathcal{A}^k$ es la colección de momentos mixtos

$$(\mathbb{F}(a_{i(1)}b_1a_{i(2)}b_2a_{i(3)}b_3 \cdots b_{m-1}a_{i(m)}) : m \geq 1, i : [m] \to [k], b_1, \ldots b_{m-1} \in \mathcal{B})$$

(en el caso escalar $\mathcal{B} = \mathbb{C}$, o bien en en caso en el que $\mathcal{B}$ conmuta con $\mathcal{A}$, los escalares b_i's conmutan con el resto de las variables y por lo tanto se pueden omitir).

Recordemos que la noción de independencia estocástica es una propiedad universal, en el sentido de que se puede entender como una propiedad que guardan las álgebras generadas por las variables aleatorias independientes, y no solo las variables aleatorias entre sí. Con esto en mente introducimos las nociones de independencia estocástica no conmutativa.

Definición 3.2.2. *Sea* $(\mathcal{A}, \mathcal{B}, \mathbb{F})$ *un EPVO.*

1). Sean $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k \subseteq \mathcal{A}$ *subálgebras que contienen al álgebra con unidad* $\mathcal{B}$*. Decimos que son* **independientes (en el sentido clásico)** *si* $\mathcal{A}_i$ *conmuta con* $\mathcal{A}_j$ *para cualquier* $i \neq j$ *y además se tiene que para cualquier tupla* $(a_1, \ldots, a_k)$ *con* $a_i \in \mathcal{A}_i$ *la esperanza condicional se factoriza:*

$$\mathbb{F}(a_1a_2 \cdots a_k) = \mathbb{F}(a_1)\mathbb{F}(a_2) \cdots \mathbb{F}(a_k)$$

2). Para todo $a \in \mathcal{A}$, *sea* $\dot{a} = a - \mathbb{F}(a)$*. Sean* $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k \subseteq \mathcal{A}$ *subálgebras que contienen al álgebra con unidad* $\mathcal{B}$*. Decimos que son* **independientes en el sentido libre** *(o simplemente* **libres***) si para todo* $m \geq 1$

$$\mathbb{F}(\dot{a}_1\dot{a}_2 \cdots \dot{a}_m) = 0,$$

siempre que las variables provengan de álgebras alternantes (esto es, $a_i \in \mathcal{A}_{j(i)}$*, con* $j : [m] \to [k]$ *tal que* $j(1) \neq j(2) \neq j(3) \neq \cdots \neq j(k)$*).*

3). Sean $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_k \subseteq \mathcal{A}$ *subálgebras que contienen al álgebra* $\mathcal{B}$*. Las álgebras se dicen* **independientes en el sentido booleano***, si para todo* $m \geq 1$

$$\mathbb{F}(a_1a_2 \cdots a_m) = \mathbb{F}(a_1)\mathbb{F}(a_2) \cdots \mathbb{F}(a_m),$$

siempre que las variables provengan de álgebras alternantes.

Colecciones de variables aleatorias se dicen independientes si las álgebras (con o sin unidad, según sea el caso) generadas por los elementos de cada colección lo son.

A continuación presentamos algunos ejemplos básicos de EPVO's y variables aleatorias $\mathcal{B}$-independientes, que son de relevancia para esta tesis.

0). Para cualquier álgebra asociativa $\mathcal{A}$, se puede considerar el caso $\mathcal{B} = \mathcal{A}$, $\mathbb{F} = id$. Las nociones de independencia de la definición anterior se convierten en tautologías y cualesquiera colecciones de variables aleatorias son independientes. Aunque esta es una situación trivial, ésta garantiza, para cualesquiera colecciones de variables aleatorias, la existencia de una álgebra $\mathcal{B} \subseteq A$ para la cual las colecciones de variables aleatorias son independientes, en cualquiera de los tres sentidos mencionados. Suele ser de relevancia algorítmica encontrar el $\mathcal{B}$ más pequeño para el que se satisface dicha noción de independencia.

1). Ortogonalidad. Supongamos que en el marco de un EPNC $(\mathcal{A}, \tau)$, nuestra álgebra $\mathcal{A}$ está dotada de proyecciones ortogonales autoadjuntas $P_1, \ldots, P_k$, tales que $1_{\mathcal{A}} = P_1 + P_2 + \cdots + P_k$. Entonces existe una única esperanza condicional $\mathbb{F} : \mathcal{A} \to \mathcal{B} = \langle P_1, \ldots, P_k \rangle$ compatible con τ. Esta se encuentra dada por

$$\mathbb{F}(a) = \sum_i \frac{\tau(P_i a P_i)}{\tau(P_i)} P_i.$$

El i-ésimo componente de $\mathbb{F}$,

$$\mathbb{F}_i = \frac{\tau(P_i a P_i)}{\tau(P_i)} P_i$$

es una funcional lineal unitario en el espacio comprimido $(P_i \mathcal{A} P_i, \mathbb{F}_i)$, donde P_i es la unidad.

Se puede demostrar que operadores ortogonales (por ejemplo $P_i a_1 P_i, P_j a_2 P_j$ con $i \neq j$, o bien $P_i a P_i, P_j a P_j$) son independientes con respecto a $\mathbb{F}$. Nuevamente (como en el primer ejemplo), la independencia se observa en los tres sentidos. Cabe mencionar que, en el caso escalar, las nociones de independencia suelen ser casi mutuamente excluyentes, en el sentido de que si dos álgebras son independientes con respeto a dos nociones, necesariamente una de ellas es el álgebra $\langle 1_{\mathcal{A}} \rangle$.

En vista de lo anterior, la ortogonalidad debe entenderse como una noción básica de independencia estocástica valuada en operadores. Esto permite descomponer un operador diagonal a bloques $a = P_1 a P_1 + P_2 a P_2 + \cdots + P_k a P_k$ en sus piezas independientes/irreducibles. Dado que la descomposición en sumas directas (sub-módulos irreducibles) es fundamental en teoría de representaciones, encontramos alivio al saber que se puede acceder a las distintas piezas mediante una esperanza condicional. A nivel de medidas espectrales, las sumas directas corresponden a combinaciones convexas de medidas.

2). En el marco de un espacio de probabilidad clásico $(\Omega, \mathcal{F}, \mathbb{P})$ y su correspondiente EPNC $\mathcal{A}_{\mathcal{F}} = L^\infty(\Omega, \mathcal{F})$, consideremos una sub-$\sigma$-álgebra $\mathcal{H} \subset \mathcal{F}$. Entonces existe una única esperanza condicional $\mathbb{F} : \mathcal{A}_{\mathcal{F}} \to \mathcal{A}_{\mathcal{H}}$ compatible con la esperanza usual $\mathbb{E}$ (que se obtiene cuando $\mathcal{H}$ es la σ-álgebra trivial $\{\emptyset, \Omega\}$).

3.3. Matrices aleatorias

Antes de considerar matrices aleatorias grandes, pensemos como ejemplo básico a la matriz simétrica de 2 por 2 con tres variables Bernoullis independientes

$$a := \begin{pmatrix} b_1 & b_2 \\ b_2 & b_3 \end{pmatrix} \in (M_2(\mathbb{C}) \otimes \mathcal{A}, \frac{1}{2}\mathrm{Tr} \otimes \mathbb{E}).$$

Podemos hacer una realización algebraica de tres variables Bernoullis independientes en el EPNC $(M_8(\mathbb{C}), \frac{1}{8}\mathrm{Tr})$, considerando

$$B_1 = B \otimes I_2 \otimes I_2, \quad B_2 = I_2 \otimes B \otimes I_2, \quad B_3 = I_2 \otimes I_2 \otimes B, \quad B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Sustituyendo b_i por B_i obtenemos una matriz en $M_{16}(\mathbb{C})$. Observemos que si $UBU^* = \Lambda = \operatorname{diag}(1,-1)$, entonces la matriz $U \otimes U \otimes U$ diagonaliza simultáneamente a B_1, B_2 y B_3. Por lo tanto

$$\begin{pmatrix} U\otimes U\otimes U & 0 \\ 0 & U\otimes U\otimes U \end{pmatrix}\begin{pmatrix} B_1 & B_2 \\ B_2 & B_3 \end{pmatrix}\begin{pmatrix} U^*\otimes U^*\otimes U^* & 0 \\ 0 & U^*\otimes U^*\otimes U^* \end{pmatrix} \tag{3.1}$$

$$= \begin{pmatrix} \Lambda\otimes I_2\otimes I_2 & I_2\otimes\Lambda\otimes I_2 \\ I_2\otimes\Lambda\otimes I_2 & I_2\otimes I_2\otimes\Lambda \end{pmatrix} = \begin{pmatrix} \Lambda_1 & \Lambda_2 \\ \Lambda_2 & \Lambda_3 \end{pmatrix}, \tag{3.2}$$

donde $\Lambda_1 = \operatorname{diag}(1,1,1,1,-1,-1,-1,-1)$, $\Lambda_2 = \operatorname{diag}(1,1,-1,-1,1,1,-1,-1)$
$\Lambda_3 = \operatorname{diag}(1,-1,1,-1,1,-1,1,-1)$.

Si se conjuga con una matriz de permutación para cambiar de la base $(e_1, e_2, \dots, e_{15}, e_{16})$ a la base $(e_1, e_9, e_2, e_{10}, e_3, \dots, e_{15}, e_8, e_{16})$, se permutan columnas y filas obteniéndose la matriz diagonal a bloques de 2 por 2

$$\begin{pmatrix}
1 & 1 \\
1 & 1 \\
& & 1 & 1 \\
& & 1 & -1 \\
& & & & 1 & -1 \\
& & & & -1 & 1 \\
& & & & & & 1 & -1 \\
& & & & & & -1 & -1 \\
& & & & & & & & -1 & 1 \\
& & & & & & & & 1 & 1 \\
& & & & & & & & & & -1 & 1 \\
& & & & & & & & & & 1 & -1 \\
& & & & & & & & & & & & -1 & -1 \\
& & & & & & & & & & & & -1 & 1 \\
& & & & & & & & & & & & & & -1 & -1 \\
& & & & & & & & & & & & & & -1 & -1
\end{pmatrix}$$

Observemos que los bloques son exactamente todos los posibles valores (equiprobables) de la matriz aleatoria. Por lo tanto la medida espectral de la matriz grande es la combinación convexa de todas las medidas espectrales posibles. En este caso dicha medida espectral es $\mu = \frac{1}{8}(2\delta_0 + 2\delta_{\sqrt{2}} + 2\delta_{-\sqrt{2}} + \delta_2 + \delta_{-2})$.

Esto ocurre en general; los momentos de una matriz aleatoria normal con respecto $\frac{1}{N}\operatorname{Tr}\otimes\mathbb{E}$ son los momentos de la medida espectral promedio. El ejemplo anterior es meramente ilustrativo y la técnica de cambiar variables aleatorias por matrices determinísticas no ayuda mucho para casos más complicados, pues rápidamente los valores propios de matrices aleatorias más grandes dependen de manera no trivial (no polinomial) de las entradas de la matriz aleatoria. Entonces aunque estas tengan una distribución conjunta accesible la distribución de los valores propios es difícil de calcular y por lo tanto es difícil determinar la medida espectral promedio.

Una mejor idea, utilizada por E. Wigner en sus artículos pioneros, es calcular los momentos de estas medidas espectrales promedio. Si la matriz aleatoria en cuestión X en $(M_n(\mathbb{C})\otimes\mathcal{A}, \frac{1}{n}\operatorname{Tr}\otimes\mathbb{E})$ es normal, (como lo fue nuestra matriz de Bernoullis de arriba), entonces los momentos de la medida espectral promedio son exactamente los momentos de (X, X^*) con respecto a $\frac{1}{n}\operatorname{Tr}\otimes\mathbb{E}$. Por como se multiplican matrices y calculan trazas, dichos momentos se pueden calcular si la distribución conjunta es sencilla.

En el resto de esta sección, describiremos la distribución conjunta de matrices de Ginibre (caso Gaussiano) y matrices determinísticas.

Para cada N, la matriz de Ginibre $C_N = N^{-1/2}(z_{ij})_{i,j\in[N]}$ es simplemente una matriz de $N \times N$ con entradas independientes z_{ij}, cada una con distribución Gaussiana compleja. Notemos que esta matriz no es normal.

Dos modelos muy importantes en matrices aleatorias se pueden obtener a partir de matrices de Ginibre.

1. El ensamble unitario Gaussiano, (GUE) $X = (C_N + C_N^*)/\sqrt{2}$.

2. El ensamble de Wishart $W = CC^*$, o más generalmente, el de Marčenko-Pastur, $W(D) = C_N D C_N^*$, or $W(D, D_2) = D_2 C_N D C_N^* D_2^*$ (para matrices deterministicas $D = D^*$ y D_2).

Por lo tanto si describimos la distribución algebraica de $\langle C, C^*, D, D_2, D_2^* \rangle$ podremos describir los momentos de $X, W, W(D)$ y $W(D, D_2)$.

Necesitamos algunos preparativos para hacer estos cálculos.

3.3.1. Preliminares combinatorios: Cumulantes

Los cumulantes son polinomios en los momentos que nos permiten organizar información sobre distribuciones de una mejor manera. El primer cumlante es simplemente la media $K_1(X) = \mathbb{E}(X)$. El segundo cumulante (mixto) $K_2(X, Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)$ es la (co)varianza.

La covarianza se anula para variables aleatorias independientes. Los cumulantes son exactamente los polinomios de orden mayor que generalizan a la covarianza, y permiten caracterizar las distintas nociones de independencia de una manera uniforme.

Familias multiplicativas de funcionales

Una partición π (de conjuntos, no confundirse con particiones de enteros $\lambda \perp n$) es una relación de equivalencia en el conjunto $\{1, \ldots, n\}$. Las clases de equivalencia de π se llaman bloques. El conjunto de todas las particiones de $\{1, \ldots, n\}$ se denota por $\mathcal{P}(n)$ y $\mathcal{P} = \bigcup_{n\geq 1} \mathcal{P}(n)$.

Para cualquier familia de funcionales multilineales $f = (f_n)_{n\geq 1} : \mathcal{A}^n \to \mathbb{C}$, podemos definir una extensión multiplicativa de f a $(f_\pi)_{\pi\in\mathcal{P}}$ de la siguiente manera

- Para todo $n \geq 1$, $f_n = f_{1_n}$, donde $1_n = \{\{1, 2, \ldots, n\}\} \in \mathcal{P}(n)$ es la partición con un único bloque.
- Si $\pi = \{V_1, V_2, \ldots, V_k\}$ entonces $f_\pi : A^n \to \mathbb{C}$ se define como

$$f_\pi(a_1, \ldots, a_n) = \prod_{V\in\pi} f_V(a_1, \ldots, a_n),$$

  donde para cada bloque $V = \{i(1), i(2), \ldots i(k)\} \in \pi$, definimos

$$f_V(a_1, \ldots, a_n) = f_k(a_{i(1)}, a_{i(2)}, \ldots a_{i(k)})$$

Por ejemplo, si $\pi = \{\{1, 2, 4\}\{3, 6\}\{5, 7\}\}$, entonces

$$f_\pi(a_1, a_2, \ldots, a_7) = f_3(a_1, a_2, a_4) f_2(a_3, a_6) f_2(a_5, a_7).$$

Más generalmente, para una permutación $\sigma \in S(n)$ también es posible considerar la extensión multiplicativa $f_\alpha : \mathcal{A}^n \to \mathbb{C}$ de una familia de funcionales (f_n). Los bloques son simplemente los ciclos de la permutación, pero se toma en cuenta el orden en que los argumentos aparecen en el ciclo. Típicamente se pide que los funcionales sean cíclicamente invariantes (i.e. invariantes al permutar cíclicamente los argumentos) para que la definición no importe del orden en el que se escriban los elementos del ciclo. De lo contrario se especifica un primer elemento en cada ciclo). Por ejemplo, para la permutación $\sigma = (1, 4, 7, 5)(2, 6, 3)$ se tiene

$$f_\pi(a_1, a_2, \ldots, a_7) = f_4(a_1, a_4, a_7, a_5)f_3(a_2, a_6, a_3).$$

En el contexto de un EPNC, la principal familia de funcionales multilineales que considera esta dada por $\tau_n : (a_1, a_2, \ldots, a_n) = \tau(a_1 a_2 \cdots a_n)$. Cuando τ es tracial, τ_n es ciclicamente invariante.

Decimos que una partición $\pi \in \mathcal{P}(n)$ no se cruza si $a \sim_\pi c$, $b \sim_\pi d \Rightarrow a \sim_\pi b \sim_\pi c \sim_\pi d$, para todo $1 \leq a < b < c < d \leq n$. El conjunto de particiones que no se cruzan de $\{1, \ldots, n\}$ se denota por $\mathcal{NC}(n)$.

Un bloque $V \in \pi \in \mathcal{NC}(n)$ es un bloque intervalo si todos los elementos de V son números consecutivos. Toda partición $\pi \in \mathcal{NC}(n)$ debe tener forzosamente (al menos) un bloque intervalo, al remover este la partición sigue siendo una partición que no se cruza más pequeña. Aunque obvia, la anterior caracterización de $\mathcal{NC}(n)$ es importante para efectos de demostraciones inductivas, como la siguiente:

Proposición 3.3.1. *Consideremos las particiones por pares (también llamadas emparejamientos) $\pi \in \mathcal{P}_2(2m) \subset \mathcal{P}(2m)$. Pensemos a π como una permutación (observe que como los ciclos de π son binarios, no hay ambigüedad). Entonces la permutación $\pi\gamma$, donde γ es el ciclo completo $\gamma = (1, 2, 3, 4, \ldots, 2m)$ tiene a lo más $m+1$ ciclos, y esto ocurre si y solo si π es un emparejamiento que no se cruza.*

Para el caso base de inducción, $m = 1$ solo hay un posible emparejamiento $(1, 2)$, por lo que $(1, 2)\gamma = (1)(2)$, que tiene 2 ciclos. Para visualizar, es conveniente dibujar a $\pi\gamma$ alternadamente junto con $\pi \in \mathcal{P}(\{\bar{1}, \bar{2}, \ldots, \bar{m}\})$ en un 4m-ágono. De esta forma, $\pi\gamma$ se puede pensar como viajar en sentido horario a lo largo de los puentes indicados por π (ver dibujo con $m = 1, 2, 3$)

Supongamos que $\pi\gamma$ tiene al menos $m+1$ ciclos. Observese que, dado que se tienen $2m$ números, el hecho de que haya al menos $m + 1$ ciclos precisa que, por principio de las casillas, al menos uno de esos ciclos sea un singulete $(\bar{r})$. Pero entonces $r = \pi\gamma(r) = \pi(r + 1)$, por lo que π debe tener el emparejamiento consecutivo $(r, r + 1)$ y $\pi\gamma(r - 1) = \pi(r) = r + 1$, por lo que $\pi\gamma$ no solo tiene al singulete r sino que la arista dirigida $(r - 1, r + 1)$ es parte de un ciclo de π.

Observemos entonces que podemos remover el par $r, r + 1$ de π para obtener $\bar{\pi}$, y por otro lado remover r y e identificar los números $r - 1$ y $r + 1$ en γ para obtener $\bar{\gamma}$. Obtenemos así permutaciones de $2(m - 1)$ elementos, tales que que $\bar{\pi}\bar{\gamma}$ tiene exactamente un ciclo menos que $\pi\gamma$ (pues se eliminó el singulete y la parte $r - 1, r + 1$ se contrae del ciclo que contiene a $r - 1$ y $r + 1$) Por lo tanto, por hipótesis de inducción $\bar{\pi}\bar{\gamma}$ tiene a lo más m ciclos con igualdad si $\bar{\pi}$ no se cruza, y por lo tanto $\pi\gamma$ tiene a lo más $m + 1$ ciclos, con igualdad si π no se cruza.

A la partición asociada a $\pi\gamma$ se le llama el complemento de Kreweras de π.

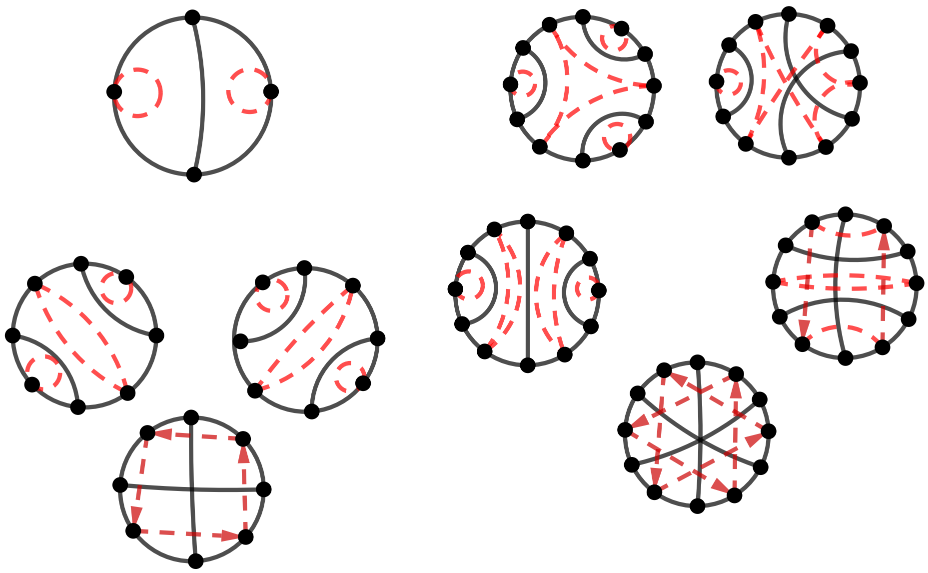


Figura 3.1: Emparejamientos (negro) y la permutación $\pi\gamma$ asociada (rojo)

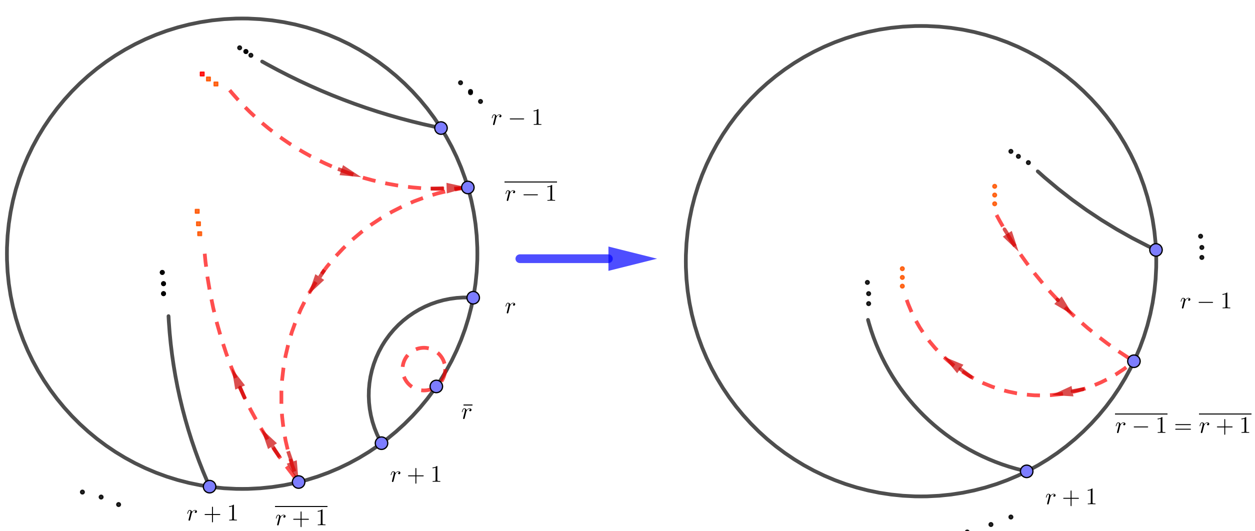


Figura 3.2: Paso de inducción

Cumulantes e independencia

Definición 3.3.1. *Sea $(\mathcal{A}, \tau)$ un EPNC. Definimos los cumulantes clásicos, libres y booleanos $(c_n)_{n\geq 1}$, $(\kappa_n)_{n\geq 1}$, $(r_n)_{n\geq 1}$ de manera inductiva con la formula cumulante momento:*

$$\begin{aligned} K_n(a_1, a_2, \ldots, a_n) &= \tau\left(a_1 \cdots a_n\right) - \sum_{\pi \neq 1_n \in \mathcal{P}(n)} \prod_{\substack{V \text{ block of } \pi \\ V=\left\{i_1,\ldots,i_s\right\}}} K_s\left(a_{i_1}, \ldots, a_{i_s}\right) \\ R_n(a_1, a_2, \ldots, a_n) &= \tau\left(a_1 \cdots a_n\right) - \sum_{\pi \neq 1_n \in \mathcal{NC}(n)} \prod_{\substack{V \text{ block of } \pi \\ V=\left\{i_1,\ldots,i_s\right\}}} R_s\left(a_{i_1}, \ldots, a_{i_s}\right) \\ B_n(a_1, a_2, \ldots, a_n) &= \tau\left(a_1 \cdots a_n\right) - \sum_{\pi \neq 1_n \in \mathcal{I}(n)} \prod_{\substack{V \text{ block of } \pi \\ V=\left\{i_1,\ldots,i_s\right\}}} B_s\left(a_{i_1}, \ldots, a_{i_s}\right). \end{aligned}$$

La importancia de los cumulantes radica en que caracterizan independencia de una forma muy útil.

Teorema 3.3.1. *Sea $(\mathcal{A}, \tau)$ un EPNC y sea $(a_n)_{n\geq 1}$ una colección de variables aleatorias en $\mathcal{A}$.*
i) $(a_n)_{n\geq 1}$ son independientes si y solo si, para todo $m \geq 1$ y $1 \leq i_1, \ldots, i_m$ los cumulantes se anulan

$$c_m\left(a_{i_1}, \ldots, a_{i_m}\right) = 0,$$

a menos de que todos los argumentos provengan de una misma álgebra $i_1 = \cdots = i_m$.
ii) $(a_n)_{n\geq 1}$ son libres si y solo si, para todo $m \geq 1$ y $1 \leq i_1, \ldots, i_m$ se tiene que

$$\kappa_m\left(a_{i_1}, \ldots, a_{i_m}\right) = 0,$$

a menos de que todos los argumentos provengan de una misma álgebra $i_1 = \cdots = i_m$.
iii) $(a_n)_{n\geq 1}$ son independientes en el sentido Booleano si y solo si, for all $m \geq 1$ and $1 \leq i_1, \ldots, i_m$ se tiene que

$$r_m\left(a_{i_1}, \ldots, a_{i_m}\right) = 0,$$

a menos de que todos los argumentos provengan de una misma álgebra $i_1 = \cdots = i_m$.

Momentos y cumulantes de variables Gaussianas

Los cumulantes organizan información sobre distribuciones de una mejor manera. Por ejemplo, el segundo cumulante es la varianza (que suele considerarse más a menudo que el segundo momento). Por ejemplo, si la varianza de una variable aleatoria es cero, entonces la variable aleatoria es constante.

Más generalmente los cumulantes de una variable aleatoria constante α están dados por $c_1(\alpha) = \alpha$ y $C_n(\alpha, \ldots, \alpha) = 0$, para todo $n \geq 2$.

Los cumulantes mixtos de variables aleatorias constantes con otras variables anulan (por lo tanto las variables aleatorias constantes son independientes de toda el álgebra $\mathcal{A}$, tanto en el sentido clásico como libre).

En general, se cumple que los cumulantes clásicos de una variable aleatoria Normal $X = X^* \sim \mathcal{N}(\mu, \sigma^2)$ están dados por $K_1(X) = \mu$, $K_2(X, X) = \sigma^2$ y $K_n(X, X, \ldots, X) = 0$ para $n \geq 3$.

Análogamente, una variable aleatoria autoadjunta $s = s^*$ tiene distribución semicircular si y solo si sus cumulantes están dados por $R_1(s) = \mu$, $R_2(s,s) = \sigma^2$ y $R_n(s, s \ldots, s) = 0$.

Si X, Y son variables aleatorias normales estándar independientes, la variable $Z = (X+iY)/\sqrt{2}$ tiene la distribución normal compleja estándar $\mathbb{C}\mathcal{N}(0,1)$. Es fácil ver que los cumulantes mixtos de $Z, \bar{Z}$ son todos cero, excepto los cumulantes $K_2(Z, \bar{Z}) = 1 = K_2(\bar{Z}, Z)$.

Una variable circular estándar se define como la variable $c = s_1 + is_2$, donde s_1, s_2 son variables semicirculares estándar libres.

Se puede mostrar fácilmente que c no es normal, y que los cumulantes libre mixtos de c, c^* son cero, excepto $R_2(c, c^*) = 1 = R_2(c^*, c)$. De la misma manera, si $c \in \mathcal{A}$ es una variable aleatoria circular, se puede mostrar que la variable autoadjunta $s = (c + c^*)/\sqrt{2}$ es semicircular.

Si $\langle c, c^* \rangle$ $\langle d \rangle$ son libres y c es circular estándar, podemos calcular momentos mixtos en (c, c^*, d) usando la formula cumulante-momento. Más precisamente tiene que para $k \geq 1$, $d_1, d_2, \ldots, d_k \in \langle d \rangle$ y $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k) \in \{1, *\}^k$, el momento mixto

$$\tau(c^{\varepsilon_1} d_1 c^{\varepsilon_2} d_2 \cdots c^{\varepsilon_k} d_k) = \sum_{\pi \in \mathcal{NC}_2(2k)} R_\pi(c^{\varepsilon_1}, d_1, c^{\varepsilon_2}, d_2, \cdots c^{\varepsilon_k}, d_k)$$

es cero si k es impar, o bien si $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$ no es balanceado en el sentido de que tenga a misma cantidad de 1's que de $*$'s.

Por las propiedades de las variables circulares, R_π se anula, a menos que $\pi \in \mathcal{NC}(4m)$ sea tal que la restricción σ de π a $\{1, 3, 5, \ldots, 4m-1\}$ sea un emparejamiento que no se cruza, que además conecta una c con una c^*. Se obtiene entonces

$$\tau(c^{\varepsilon_1} d c^{\varepsilon_2} d \cdots c^{\varepsilon_{2m}} d_{2m}) = \sum_{\pi \in \mathcal{NC}_2(2m)} \tau_{Kr(\sigma)}(d, d, \cdots, d).$$

Estos momentos aparecerán como los momentos límite de matrices de Ginibre y matrices determinísticas.

3.3.2. Momentos mixtos de matrices de Ginibre y matrices determinísticas

Ahora queremos calcular momentos mixtos de matrices de Ginibre y matrices deterministicas $C_N, C_N^* D_N D_N^*$ en el EPNC $(\mathcal{A}_N, \tau_N)$, con $\mathcal{A}_N := M_N(\mathbb{C}) \otimes \mathcal{A}$ y $\tau_N = \frac{1}{N}\mathrm{Tr} \otimes \mathbb{E}$. Por conveniencia omitimos el subíndice N de la notación.

Por tracialidad y linealidad τ_N, es suficiente calcular trazas esperadas de:

$$\tau_N(D^{(1)} C^{\varepsilon_1} D^{(2)} C^{\varepsilon_2} \ldots D^{(m)} C^{\varepsilon_m}) \tag{3.3}$$

con $D^{(k)} = (D^{(k)}_{i,j \in [N]}) \in \langle D_N, D_N^* \rangle$.

Entonces debemos calcular

$$\begin{aligned} & \tau_N(D^{(1)} C^{\varepsilon_1} D^{(2)} C^{\varepsilon_2} \ldots D^{(m)} C^{\varepsilon_m}) & (3.4) \\ = \quad & \frac{1}{N^{1+m/2}} \sum \mathbb{E}(D^{(1)}_{i_1 i_2} z^{\varepsilon_1}_{i_2 i_3} D^{(2)}_{i_3 i_4} z^{\varepsilon_2}_{i_4 i_5} \ldots D^{(m)}_{i_{2m-1} i_{2m}} z^{\varepsilon_m}_{i_{2m} i_1}) & (3.5) \end{aligned}$$

donde $\varepsilon = (\varepsilon_1, \ldots \varepsilon_m) \in \{1, *\}^m$, y (z_{ij}) son gaussianas complejas independientes, con $z^*_{ij} = \bar{z}_{ji}$ y $D^{(k)}_{ij}$ son constantes.

Debemos calcular

$$
\begin{aligned}
& \tau_N(D^{(1)}C^{\varepsilon_1}D^{(2)}C^{\varepsilon_2}\dots D^{(m)}C^{\varepsilon_m}) && (3.6)\\
= \; & \frac{1}{N^{1+m/2}} \sum_{i:[2m]\to[N]} \mathbb{E}(D^{(1)}_{i_1i_2} z^{\varepsilon_1}_{i_2i_3} D^{(2)}_{i_3i_4} z^{\varepsilon_2}_{i_4i_5}\dots D^{(m)}_{i_{2m-1}i_{2m}} z^{\varepsilon_m}_{i_{2m}i_1}) && (3.7)\\
= \; & \frac{1}{N^{1+m/2}} \sum_{i:[2m]\to[N]} \sum_{\pi\in\mathcal{P}(2m)} K_\pi(D^{(1)}_{i_1i_2}, z^{\varepsilon_1}_{i_2i_3}, D^{(2)}_{i_3i_4}, z^{\varepsilon_2}_{i_4i_5},\dots, D^{(m)}_{i_{2m-1}i_{2m}}, z^{\varepsilon_m}_{i_{2m}i_1}) && (3.8)\\
= \; & \frac{1}{N^{1+m/2}} \sum_{\pi\in\mathcal{P}(2m)} \sum_{i:[2m]\to[N]} K_\pi(D^{(1)}_{i_1i_2}, z^{\varepsilon_1}_{i_2i_3}, D^{(2)}_{i_3i_4}, z^{\varepsilon_2}_{i_4i_5},\dots, D^{(m)}_{i_{2m-1}i_{2m}}, z^{\varepsilon_m}_{i_{2m}i_1}) && (3.9)
\end{aligned}
$$

Entonces, para cada partición fija $\pi \in P(2m)$, calcularemos la última expresión

$$\sum_{i:[2m]\to[N]} K_\pi(D^{(1)}_{i_1i_2}, z^{\varepsilon_1}_{i_2i_3}, D^{(2)}_{i_3i_4}, z^{\varepsilon_2}_{i_4i_5},\dots, D^{(m)}_{i_{2m-1}i_{2m}}, z^{\varepsilon_m}_{i_{2m}i_1}).$$

Usando la formula cumulante-momento, observamos que K_π se anula para muchos casos. En particular, para valores impares de m o para momentos no balanceados en $\varepsilon \in \{1,*\}^m$. Los cumulantes clásicos de las Gaussianas complejas se anulan si la partición no empareja a las z_{ij}'s con sus adjuntas. Por último, los cumulantes no singuletes de las constantes se anulan, así que K_π se anula a menos de que $\pi \in \mathcal{P}(4m)$ sea una partición con solo singuletes en los impares, de tal forma que su restricción $\rho \in \mathcal{P}(\{2,4,6,\dots,4m\}) \cong \mathcal{P}(\{1,2,3,\dots,2m\})$ es un emparejamiento.

La evaluación de cumulantes de Gaussianas corresponde a una identificación de índices en la suma a calcular. Por ejemplo (ver figura), el emparejamiento de las variables $K_2(z_{i_{16}i_1}, \overline{z_{i_{11}i_{10}}})$ forza las identificaciones de índices $i_{16} = i_{11}$ y $i_1 = i_{10}$). Al considerar todos los emparejamientos, realizar las identificaciones de índices y sumar sobre todos los índices libres, se obtiene el producto de trazas

$$\sum_{i:[2m]\to[N]} K_\pi(z^{\varepsilon_1}_{i_1i_2} D^{(1)}_{i_2i_3} z^{\varepsilon_2}_{i_3i_4}\dots D^{(2m)}_{i_{2m-1}i_{2m}}) = \frac{1}{N^{m+1}} Tr_{\rho\gamma}(D^{(1)}, D^{(2)},\dots, D^{(2m)}).$$

Donde $\gamma = (1,2,3,\dots,2m)$ es el ciclo largo y el emparejamiento ρ se piensa como permutación.

Por ejemplo, los primeros momentos mixtos no nulos son los siguientes (ver figura).

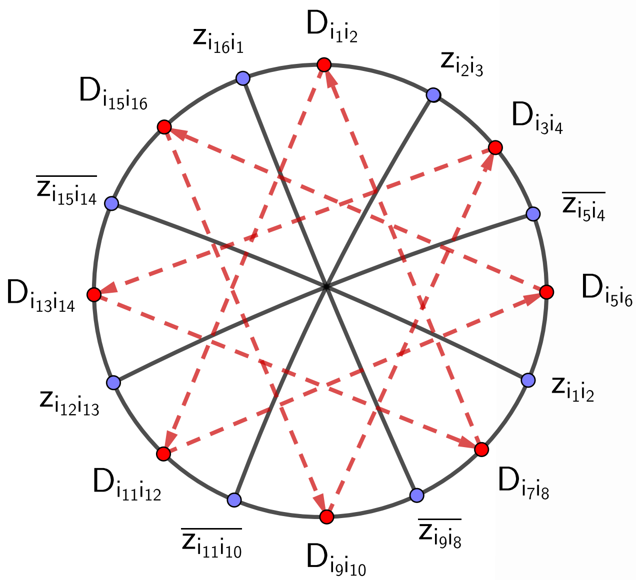
$$(\frac{1}{N}\mathrm{Tr}\otimes\mathbb{E})(C_N D^{(1)} C_N^* D^{(2)}) = \frac{1}{N^2}\mathrm{Tr}(D^{(1)})\mathrm{Tr}(D^{(2)}) = (\frac{1}{N}\mathrm{Tr}\otimes\mathbb{E})(C_N^* D^{(1)} C_N D^{(2)})$$

$$
\begin{aligned}
&(\frac{1}{N}\mathrm{Tr}\otimes\mathbb{E})(C_N D^{(1)} C_N^* D^{(2)} C_N^* D^{(3)} C_N D^{(4)}) = \\
&= \frac{1}{N^3}\mathrm{Tr}(D^{(1)})\mathrm{Tr}(D^{(3)})\mathrm{Tr}(D^{(4)}D^{(2)}) + \frac{1}{N^3}\mathrm{Tr}(D^{(4)}D^{(3)}D^{(2)}D^{(1)}),
\end{aligned}
$$

Donde el primer producto de trazas corresponde al emparejamiento que no se cruza $\rho_1 = \{\{1,2\}\{3,4\}\}$, mientras que el segundo producto de trazas corresponde al emparejamiento $\rho_2 = \{\{1,3\}\{2,4\}\}$.

Para el momento mixto

$$(\frac{1}{N}\mathrm{Tr}\otimes\mathbb{E})(C_N D^{(1)} C_N^* D^{(2)} C_N D^{(3)} C_N^* D^{(4)})$$



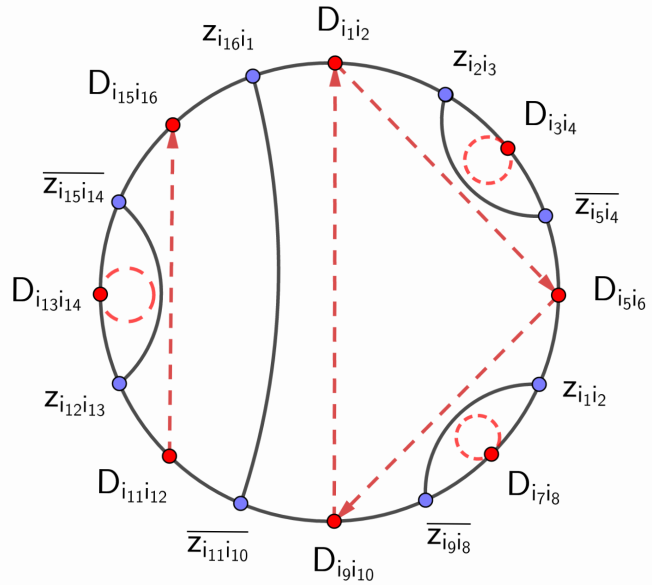


Figura 3.3: $\sum_i K_\pi$ para $\rho_1 = \{\{1,5\}\{2,6\}\{2,7\}\{4,8\}\}$ y $\rho_2 = \{\{1,2\}\{3,4\}\{5,8\}\{6,7\}\}$. $Tr_{\rho_1\gamma}(D^{(1)}, D^{(2)}, \ldots, D^{(2m)}) = Tr(D^{(1)}D^{(6)}D^{(3)}D^{(8)}D^{(5)}D^{(2)}D^{(7)}D^{(4)})$, mientras que $Tr_{\rho_2\gamma}(D^{(1)}, D^{(2)}, \ldots, D^{(2m)}) = Tr(D^{(1)}D^{(3)}D^{(5)})Tr(D^{(2)})Tr(D^{(4)})Tr(D^{(6)}D^{(8)})Tr(D^{(7)})$

se obtiene adicionalmente el producto de trazas $\frac{1}{N^3}\mathrm{Tr}(D^{(1)})\mathrm{Tr}(D^{(3)})\mathrm{Tr}(D^{(4)}D^{(2)})$ correspondiente al emparejamiento que no se cruza $\rho_3 = \{\{1,4\}\{2,3\}\}$.

En las hipótesis de Marčenko-Pastur, se asume que las matrices deterministicas son normales y tienen distribución espectral límite, o bien que los momentos mixtos $\frac{1}{N}\mathrm{Tr}(D^{(1)}D^{(2)}\cdots D^{(m)})$ convergen. Por lo tanto, cada traza que aparece en el producto $\mathrm{Tr}_{\gamma\rho}$ puede absorber un factor N^{-1}. Al hacer tender $N \to \infty$, solo los emparejamientos que no se cruzan contribuyen al momento mixto, pues estos producen el mayor número de trazas. Por lo tanto, obtenemos la siguiente fórmula:

Teorema 3.3.2. *Los momentos mixtos de una matriz de Ginibre, su adjunta y matrices deterministicas se calculan de la siguiente manera.*

$$(\frac{1}{N}\mathrm{Tr}\otimes\mathbb{E})(C_N^{\varepsilon_1}D^{(1)}\cdots C_N^{\varepsilon_{k-1}}D^{(k-1)}C_N^{\varepsilon_k}D^{(k)}) = 0,$$

si k es impar, o bien si en $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$ no hay la misma cantidad de 1's y $*$'s.

Para $k = 2m$ y ε balanceado. Se tiene que

$$\left(\frac{1}{N}\mathrm{Tr}\otimes\mathbb{E}\right)\left(C_N^{\varepsilon_1}D^{(1)}\cdots C_N^{\varepsilon_{2m-1}}D^{(2m-1)}C_N^{\varepsilon_{2m}}D^{(2m)}\right) = \frac{1}{N^{m+1}}\sum_{\pi\in\mathcal{P}_2(2m)}\mathrm{Tr}_{\gamma\pi}\left(D^{(1)}, D^{(2)}, \ldots, D^{(2m)}\right).$$

Además,

$$\lim_{N\to\infty}\frac{1}{N^{m+1}}\mathrm{Tr}_{\gamma\pi}\left(D^{(1)}, D^{(2)}, \ldots, D^{(2m)}\right) = 0,$$

a menos que π sea un emparejamiento que no se cruza.

Por tanto, los momentos asintóticos se calculan exactamente igual que los momentos mixtos de variables circulares y elementos provenientes de una álgebra libre.

Por lo tanto las matrices Determinísticas y las Matrices de Ginibre son asintóticamente libres y éstas últimas son asintóticamente circulares.

Para formular los resultados de Voiculescu de una manera más sucinta y más general, es conveniente introducir las nociones de convergencia en distribución no-conmutativa, así como algunas variables especiales.

Definición 3.3.2. *Para cada $N \geq 1$ sea $a^{(N)} = (a_1^{(N)}, a_2^{(N)}, \ldots, a_k^{(N)})$ una colección de variables aleatorias en EPNC's $(\mathcal{A}_N, \tau_N)$, y sea $a = (a_1, \ldots a_k)$ otra colección en otro EPNC $(\mathcal{A}, \tau)$.*

Decimos que $a^{(N)}$ converge en distribución (no conmutativa) a a si para todo $m \geq 1$ y para todo $i : [m] \to [k]$,

$$\lim_{N\to\infty} \tau_N(a_{i(1)}^{(N)} a_{i(2)}^{(N)} \cdots a_{i(m)}^{(N)}) = \tau(a_{i(1)} a_{i(2)} \cdots a_{i(m)})$$

Ya hemos descrito las distribuciones algebraicas de variables circulares, semicirculares, poisson libres (con parámetro $\lambda = 1$) y Poisson compuestas, en términos de cumulantes. Otra distribución importante es la de un operador Haar-unitario $u \in \mathcal{A}$. En términos de momentos, se caracteriza por ser normal (de hecho unitario, $u^* = u^{-1}$), con momentos dados por $\tau(u^k) = \delta_{0=k}$ para $k \in \mathbb{Z}$.

Recordemos que a partir de una matriz de Ginibre C_N se pueden construir matrices autoadjuntas de Wigner y de Wishart. Las matrices aleatorias unitarias de Haar se pueden obtener como las partes polares $U_N = (C_N)(C_N^* C_N)^{-1/2}$ de una matriz de Ginibre.

Los resultados de Voiculescu pueden resumirse en el siguiente enunciado.

Teorema 3.3.3. *Para cada $N \geq 1$, sean $C_1^{(N)}, C_2^{(N)}, \ldots, C_{k_1+k_2+k_3+k_4}^{(N)}$ matrices de Ginibre en el espacio de probabilidad $M_N(\mathbb{C}) \otimes \mathcal{A}_{\mathcal{F}}$. Se suprime el superíndice por conveniencia.*

Sean $X_i := (C_{k_1+i} + C_{k_1+i}^*)/\sqrt{2}$ para todo $i \leq k_2$, $W_i := (C_{k_1+k_2+i} C_{k_1+k_2+i}^*)$ para todo $i \leq k_3$

Sea $U_i := C_j(C_j^* C_j)^{-1/2}$ para $i \leq k_4$ y $j = i + k_1 + k_2 + k_3$. Entonces la colección de matrices aleatorias y determinísticas

$$\big(C_1, C_1^*, \ldots, C_{k_1}, C_{k_1}^*, X_1, X_2, \ldots, X_{k_2}, W_1, W_2, \ldots, W_{k_3}, U_1, U_1^*, \ldots, U_{k_4}, U_{k_4}^*, D\big)$$

converge en distribución a

$$(c_1, c_1^*, \ldots, c_{k_1}, c_{k_1}^*, x_1, x_2, \ldots, x_{k_2}, w_1, w_2, \ldots, w_{k_3}, u_1, u_1^*, \ldots, u_{k_4}, u_{k_4}^*, d)$$

, donde:

- *las álgebras $\langle c_1, c_1 * \rangle, \langle c_2, c_2 * \rangle, \ldots, \langle x_1 \rangle, \langle x_2 \rangle, \ldots, \langle w_1 \rangle, \langle w_2 \rangle, \ldots \langle u_1, u_1^* \rangle, \langle u_2, u_2^* \rangle, \langle u_{p_4}, u_{p_4}^* \rangle, \langle d \rangle$ son libres entre sí*

- *los elementos c_i son variables circulares estándar.*

- *los elementos s_i son variables semicirculares estándar.*

- *los elementos w_i son variables Poisson libre (con $\lambda = 1$).*

- *los elementos u_i son variables Haar-unitarias.*

- *los momentos de $d_i = d_i^*$ están dados por $\lim \frac{1}{N} \mathrm{Tr}(D_i^k) = \tau(d^k)$.*

Bosquejo de demostración.

En la sección anterior calculamos las trazas esperadas mixtas para el caso de una sola matriz de Ginibre y una matriz determinística. No es difícil extender este resultado al caso de varias matrices de Ginibre para obtener que la distribución conjunta de todas las matrices de Ginibre

$$(C_1, C_1^*, \ldots, C_{p_1}, C_{p_1}^*, C_{k_1+1}, C_{k_1+1}^* \ldots, C_{k_1+k_2+k_3+k_4}, C_{k_1+k_2+k_3+k_4}^*, D)$$

converge en distribución no conmutativa a

$$(c_1, c_1^*, \ldots, c_{p_1}, c_{p_1}^*, c_{k_1+1}, c_{k_1+1}^* \ldots, c_{k_1+k_2+k_3+k_4}, c_{k_1+k_2+k_3+k_4}^*, d),$$

donde las álgebras $\langle c_1, c_1* \rangle, \langle c_2, c_2* \rangle, \ldots, \langle c_{k_1+k_2+k_3+k_4}, c_{k_1+k_2+k_3+k_4}^* \rangle, \langle d \rangle$ son libres.

Como la independencia libre es una propiedad del álgebra, esta se hereda a las subálgebras generadas por matrices de Wigner y Wishart. Para el caso de matrices unitarias se necesitan consideraciones en álgebras W^*. Alternativamente, se describe la distribución conjunta de las entradas de matrices Unitarias, como procedemos en el capítulo 4.

3.3.3. Conjugación con matrices unitarias

Las matrices unitarias están detrás de la independencia libre asintótica. Las matrices de Ginibre son bi-unitariamente invariantes. Es decir, C tiene la misma distribución que UC_iV donde U y V son matrices unitarias (posiblemente aleatorias). En particular, se puede pensar que U y V son independientes y tienen la distribución uniforme en el grupo unitario.

Entonces, en el modelo de Marčenko-Pastur CDC^* se puede comprender estudiando la distribución del modelo $CUDU^*C^*$. Este último se puede explicar en términos de la distribución conjunta de las matrices (C, C^*, UDU^*). La independencia libre asintótica está relacionada con la operación de conjugar aleatoriamente una matriz.

Del Teorema de Voiculescu sabemos que si matrices determinísticas $\langle A_N, B_N \rangle$ convergen en distribución, entonces son asintóticamente libres de la parte polar de una matriz de Ginibre $\langle U_N, U_N^* \rangle$. Usando la definición directa de independencia libre de Voiculescu, se puede demostrar que $A_N, U_N B_N U_N^*$ son asintóticamente libres.

Además, $\frac{1}{N}\mathrm{Tr}((U_N B_N U_N^*)^k) = \frac{1}{N}\mathrm{Tr}(B_N^k)$. Por lo tanto $A_N, U_N B_N U_N^*$ para N grande son aproximaciones de operadores en relación libre. En particular, la distribución asintótica de $A_N + U_N B_N U_N^*$ depende únicamente de las distribuciones asintóticas de $\langle A_N \rangle$ y $\langle B_n \rangle$.

Si A_N y B_N convergen en distribución espectral a μ, ν, entonces la distribución asintótica $A_N + U_N B_N U_N^*$ se conoce como la convolución libre de μ y ν, y se le denota $\mu \boxplus \nu$.

Para todo grupo topológico localmente compacto G es posible construir una medida μ sobre la $\sigma-$álgebra de Borel de G con las siguientes propiedades:

- Los subconjunto compactos tienen medida finita.
- Es invariante bajo la traslación izquierda del grupo.

La tercer propiedad quiere decir que si $A \subset G$ es un conjunto medible y $g \in G$ entonces el conjunto $gA = \{ga : a \in A$ y A tienen la misma medida.A cualquier medida que cumpla estas dos propiedades la llamaremos **medida de Haar** . Las medidas de Haar buscan generalizar las propiedades del caso del grupo aditivo de los reales $(\mathbb{R}, +)$ dotado de la medida de Lebesgue.)Ejemplo con grupo finito (Consideremos el círculo unitario $S^1 \subset \mathbb{C}$ con la multiplicación de números complejos usual. Tenemos la longitud usual cumple con las propiedades anteriores y por lo tanto es una medida de Haar.

Teorema 3.3.4. *Para todo grupo topológico localmente compacto existe una única, salvo múltiplos, mediada de Haar.*

Si estamos trabajando con un grupo compacto notamos que $\mu(G)$ es finito y para algunos cálculos será útil considerar la medida de Haar tal que $\mu(G) = 1$. Notamos que un grupo finito lo podemos dotar de la topológia discreta y con esta sera un grupo topológico compacto. Si $A \subset G$ entonces $\mu(A) = \frac{|A|}{|G|}$. Por otro lado si $f : G \to \mathbb{C}$ es una función tenemos que es integrable y podemos calcular su integral de la siguiente manera:

$$\int_G f(g)d\mu(g) = \frac{1}{|G|} \sum_{g \in G} f(g).$$

Notamos que en los capítulos anteriores hemos trabajado ya con este tipo de expresiones, sobre todo en primer capítulo. Por lo que es de esperarse que la medida de Haar sea una herramienta fundamental en la teoría de representaciones de grupos mas complicados que los finitos.

El grupo unitario $U(d)$ se define como las matrices cuadradas de tamaño dxd que preservan el producto interno usual de $\mathbb{C}^d$, es decir, $U(d) = \{U \in M_d(\mathbb{C}) : UU^* = I_d\}$ este es un subgrupo del grupo general lineal. Identificando las matrices cuadradas $M_d(\mathbb{C})$ con $(\mathbb{C}^d)^d$ notamos que la función determinante es multilineal y por tanto continua luego $GL(d) = det^{-1}(\mathbb{C}^*)$. Esto muestra que $GL(d)$ es un abierto de un espacio euclidiano por lo que tiene una estructura de variedad diferenciable.
Consideremos la función $f : M_d(\mathbb{C}) \to Her(d)$ definida por $f(A) = AA^*$,notamos que esta es una función continua y que $f^{-1}(I_d) = U(d)$. Por lo que $U(d)$ es la preimagen de un punto bajo una función continua y por lo tanto es un cerrado. Por la regla de Leibniz se tiene que $d_Af(B) = AB^* + BA^*$ si $A \in U(d)$ entonces para mostrar que d_Af es sobre basta mostrar que la ecuación $AB^* + BA^* = C$ tiene solución para B proponemos $B = \frac{1}{2}CA$ como A es una matriz unitaria se tiene que:

$$AB^* + BA^* = \frac{1}{2}(A(CA)^* + CAA^*) = C.$$

Luego por el teorema del valor regular $U(d)$ es una subvariedad de dimension d^2, de hecho se puede identificar de forma natural $T_pU(d)$ con $\ker(d_pf)$. Por lo que el plano tangente en la identidad es:

$$T_{Id}U(d) = \{B \in M_d(\mathbb{C}) : B + B^* = 0\},$$

Es decir las matrices antihermitianas. Por $|\cdot|$ escribiremos la norma usual en $\mathbb{C}^d$ y por $\|\cdot\|$ a la norma del operador en $M_d(\mathbb{C})$ con respecto a $|\cdot|$, es decir,

$$\|A\| = \sup_{|v|=1} |Av|$$

Para una matriz $U \in U(d)$ tenemos que U preserva el producto interno por lo que $|Uv| = |v|$ para cada $v \in \mathbb{C}^d$ por lo que $\|U\| = 1$ por lo tanto $U(d)$ es un conjunto acotado. Como ya habíamos probado antes que este conjunto es cerrado tenemos que $U(d)$ es compacto.

Como grupo topo lógico localmente compacto el grupo unitario recibe una medida de Haar. Como este es compacto podemos normalizarla para obtener una medida de probabilidad. Con esta podemos construir matrices aleatorias sobre el grupo unitario invariantes bajo la acción por la izquierda y por conjugación de este. Estas matrices se conocen como Haar unitarias. La distribución analítica de las entradas una matriz de esta clase no está es sencilla.

Proposición 3.3.2. *Si $U \in U(d)$ es una matriz de Haar entonces $\frac{1}{d}\mathbb{E}Tr(U^n) = 0$ para todo $n \in \mathbb{Z} \setminus \{0\}$.*

Demostración. Tenemos que la medida de Haar es invariante bajo la acción izquierda del grupo unitario por lo cual $sU = (sI_d)U$ tiene la misma distribución que U para cada $s \in S^1$. Por lo que $\mathbb{E}Tr(U^n) = \mathbb{E}Tr((sU)^n) = s^n\mathbb{E}Tr(U^n)$ para todo $s \in S^1$. Por lo que $\mathbb{E}Tr(U^n) = 0$. $\square$

Notamos que para $n = 0$ se tiene que $U^0 = I_d$ por lo que $\mathbb{E}tr(U^0) = 1$. Debido a la proposición anterior en un espacio de probabilidad algebraico (A, τ) a un elemento $u \in A$ lo llamamos Haar unitario si cumple que $uu* = 1$ y $\tau(u^n) = 0$ para todo $n \in \mathbb{N}$.

Dedicaremos el siguiente capítulo al cálculo de los momentos conjuntos de las entradas de una matriz Haar unitaria.

Capítulo 4

Cálculo de los momentos del grupo unitario

Los momentos del grupo unitario son expresiones de la forma:

$$\mathbb{E}\left(U_{i_1j_1}\cdots U_{i_nj_n}\overline{U_{i'_1j'_1}\cdots U_{i'_nj'_n}}\right) = \int_{U\in U(d)} U_{i_1j_1}\cdots U_{i_nj_n}\overline{U_{i'_1j'_1}\cdots U_{i'_nj'_n}}dU.$$

Donde U es una matriz aleatoria en el grupo unitario con distribución de Haar. Estas expresiones aparecen en el cálculo de la distribución conjunta de las entradas de matrices Haar unitarias. Como hemos visto, las matrices unitarias aparecen de forma natural en la teoría de matrices aleatorias como la parte polar de una matriz de Ginibre. El principal objetivo de este capítulo es reducir esta integral sobre el grupo unitario a una suma sobre el grupo simétrico.
En este capítulo usaremos el teorema del doble conmutador, demostrado en el capítulo 2, para exponer una relación entre representaciones del grupo simétrico y representaciones del grupo unitario descubierta por Issai Schur a principios del siglo XVIII conocida como dualidad de Schur-Weyl. Con este teorema de dualidad y gracias a nuestro entendimiento de las representaciones del grupo simétrico podremos calcular el caracter de una representación conjunta de estos dos grupos el cual utilizaremos para calcular los momentos del grupo unitario basados en el trabajo de Collins y Sniady [5] este a su vez basado en [6] y [18].

Recordemos del primer capítulo que las representaciones irreducibles de grupo S_n están parametrizadas mediante particiones aditivas del entero n, por cada partición $\lambda \vdash n$ podemos construir una representación irreducible $\rho_\lambda : S_n \to End(V^\lambda)$. Además del capítulo 2 recordamos que la descomposición de Weddenburn del álgebra del grupo del grupo simétrico $\mathbb{C}[S_n]$ coincide con su descomposición isotípica de la representación regular y la primera está dada por $\mathbb{C}[S_n] \sim \bigoplus_{\lambda\vdash n} End(V_\lambda)$. Esté hecho será de utilidad para nosotros ya que la descomposición de Weddenburn es la que naturalmente aparece en el contexto del teorema del doble conmutador mientras que para la descomposición isotípica podemos escribir escribir las proyecciones en términos de los caracteres.
Por el teorema de descomposición isotípica tenemos que para $\lambda \vdash n$ la proyección de $\mathbb{C}[S_n]$ a $End(V_\lambda)$ esta dada por:

$$\frac{\chi_\lambda(e)}{n!}\sum_{\sigma\in S_n}\overline{\chi_\lambda(\sigma)}\rho_{reg}(\sigma).$$

Usando que los caracteres del grupo simétrico son enteros podemos notar que aplicar esta proyección a un elemento del álgebra de S_n es lo mismo que multiplicar por la izquierda a este elemento por

$$p_\lambda = \frac{\chi^\lambda(e)}{n!} \sum_{\sigma \in S_n} \chi_\lambda(\sigma).$$

Notamos que en el álgebra $\oplus_\lambda End(V^\lambda)$ las proyecciones a cada sumando se pueden escribir como la multilicación por la izquierda con los operadores Id_{V^λ}. Por lo tanto bajo el isomorfismo de álgebras $\mathbb{C}[S_n] \sim \oplus_{\lambda \vdash n} End(V_\lambda)$ el elemento $Id_{V^\lambda} \in \oplus_{\lambda \vdash n} End(V^\lambda)$ coincide con p_λ.
En este capitulo identificaremos el álgebra $\mathbb{C}[S_n]$ con funciones $S_n \to \mathbb{C}$ mediante la correspondencia $\sigma \leftrightarrow \delta_\sigma$. Mediante está identificación tenemos que

$$p_\lambda = \frac{\chi_\lambda(e)}{n!} \chi^\lambda.$$

Por el isomorfismo descrito anteriormente y las relaciones que cumplen los operadores $(Id_{V_\lambda})_{\lambda \dashv n}$ se tiene que $p_\lambda^2 = p_\lambda$, $p_\lambda p_\mu = 0$ siempre que $\mu, \lambda \dashv n$ son particiones distintas y que $\sum_{\lambda \dashv n} p_\lambda = 1_{\mathbb{C}[S_n]}$. Aquí es importante enfatizar que el producto $p_\lambda p_\mu$ que nos estamos refiriendo no es el producto puntual de funciones, es el producto de estos elementos en el álgebra de grupo. Además notamos que el centro de $\oplus_{\lambda \vdash n} End(V^\lambda)$ está generado por Id_{V^λ}. Por lo tanto los elementos p_λ generan en centro de $\mathbb{C}[S_n]$. Por lo anterior los elementos p_λ son conocidos como **proyectores centrales**.

Consideremos el espacio vectorial $(\mathbb{C}^d)^{\otimes n}$. En este espacio actúa el grupo simétrico S_n mediante $\rho_{S_n}^d : S_n \to End(\mathbb{C}^d)^{\otimes n}$, dado por la extensión lineal de:

$$\rho_{S_n}^d(\pi)(v_1 \otimes ... \otimes v_n) = v_{\pi^{-1}(1)} \otimes ... \otimes v_{\pi^{-1}(n)},$$

para $\pi \in S_n$ y $v_1 \otimes ... \otimes v_n \in (\mathbb{C}^d)^{\otimes n}$.
Por otro lado el grupo unitario $U(d)$ actúa en $\mathbb{C}^d$ mediante la inclusión $\rho : U(d) \subset End(\mathbb{C}^d)$. Podemos extender esta acción de forma diagonal, es decir, mediante el producto tensorial. Definimos $\rho_{U(d)}^n = \rho^{\otimes n}$. Esta representación actúa en tensores elementales de la siguiente manera:

$$\rho_{U(d)}^n(U)(v_1 \otimes \cdots \otimes v_n) = Uv_1 \otimes \cdots \otimes Uv_n,$$

es decir, $\rho_{U(d)}^n(U) = U^{\otimes n}$.
Podemos extender linealmente a $\rho_{S_n}^d$ a un homomorfismo de álgebras $\rho_{S_n}^d : \mathbb{C}[S_n] \to End(\mathbb{C}^d)^{\otimes n}$ usando la propiedad universal del álgebra de un grupo expuesta en el segundo capítulo. Estas dos acciones conmutan. En efecto, para $U \in U(d), \sigma \in S_n$ y $v_1 \otimes \cdots \otimes v_n \in (\mathbb{C}^d)^{\otimes n}$:

$$\begin{aligned}
\rho_{S_n}^d(\rho_{U(d)}^n(v_1 \otimes \cdots \otimes v_n)) &= \rho_{S_n}^d(Uv_1 \otimes \cdots \otimes Uv_n) \\
&= Uv_{\sigma^{-1}(1)} \otimes \cdots \otimes Uv_{\sigma^{-1}(n)} \\
&= \rho_{U(d)}^n(v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)} \\
&= \rho_{U(d)}^n(\rho_{S_n}^d(v_1 \otimes \cdots \otimes v_n)).
\end{aligned}$$

Esta última observación, aunque obvia, es fundamental para establecer la relación que buscamos entre representaciones de estos dos grupos.

Proposición 4.0.1. *El homomorfismo $\rho_{S_n}^d$ restringido a $\mathbb{C}_d[S_n] \sim \oplus_{\lambda \vdash n, l(\lambda) \leq d} End(V_\lambda)$ es inyectivo.*

Notamos que la imagen de un álgebra semisimple bajo un homomorfismo de álgebras es semisimple y que la imagen de un sumando directo simple es un simple o cero. Lo que vamos a hacer es restringir el homomorfismo a las partes simples del álgebra para reducir este problema a estudiar la representación del grupo simétrico en $(\mathbb{C}^d)^{\otimes n}$. Notamos que para álgebras simples, o lo que es lo mismo por el teorema de Wedderburn álgebras de matrices con entradas complejas, tenemos un comportamiento análogo al descrito por el lema de Schur. Si $\phi : M_n(\mathbb{C}) \to M_{n'}(\mathbb{C})$ es un homomorfismo de álgebras entonces es un isomorfismo (en este caso f no puede ser nulo ya que es requerido que $f(I_n) = I_{n'}$). De aquí notamos que para que pueda existir este homomorfismo es necesario que $n = n'$. Otro resultado interesante e ilustrativo es que el espacio de automorfismos del álgebra $M_n(\mathbb{C})$ coincide con el espacio de sus automorfismo internos, es decir, los que están dados por una conjugación. Notamos también que si $End(V^\lambda)$ aparece en la descomposición semisimple en la imagen de $\rho^d_{S_n}$ entonces podemos obtener una copia de V^λ en la representación $(\mathbb{C}^d)^{\otimes n}$. Por lo que basta entender que representaciones irreducibles ocurren en $(\mathbb{C}^d)^{\otimes n}$. Esto se puede revolver mediante la correspondencia de Robinson-Schensted (ver [7]). El resultado que se tiene es que si $l(\lambda) \leq d$ entonces V^λ aparece en $(\mathbb{C}^d)^{\otimes n}$ mientras que si $l(\lambda) > d$ entonces esta no aparece. También es posible dar una descripción combinatoria de las multiplicidades con las que aparece cada V^λ en $(\mathbb{C}^d)^{\otimes n}$.

Para $U \in U(d)$ usaremos la notación:

$$U^{-\otimes n} := (U^{-1})^{\otimes n} = (U^{\otimes n})^{-1}.$$

El grupo unitario actúa en $End(\mathbb{C}^d)^{\otimes n}$ mediante la conjugación:

$$U \cdot A = U^{\otimes n} A U^{-\otimes n}.$$

Los puntos fijos de esta acción, además de ser un subespacio, son una subálgebra. En efecto si $A, B \in End(\mathbb{C}^d)^{\otimes n}$ son puntos fijos tenemos que:

$$U^{\otimes n} AB U^{-\otimes n} = (U^{\otimes n} A U^{-\otimes n})(U^{\otimes n} B U^{-\otimes n}) = AB.$$

Analogamente notamos que cualquier combianción lineal de puntos fijos es un punto fijo y que la identidad es un punto fijo. A esta subálgebra la denotamos por $End_{U(d)}(\mathbb{C}^d)^{\otimes n}$.

Si $A \in End_{U(d)}(\mathbb{C}^d)^{\otimes n}$ notamos que para cada $U \in U(d)$ se cumple que $U^{\otimes n} A U^{\otimes -n} = A$ lo cual es equivalente a que $U^{\otimes n} A = A U^{\otimes n}$. De lo anterior tenemos que $End_{U(d)}(\mathbb{C}^d)^{\otimes n}$ es el conmutador de la imagen de $\rho^n_{U(d)}$. Además recordamos que los puntos fijos de una representación son la componente isotípica de la representación correspondiente a la representación trivial.

Proposición 4.0.2. *El conmutador de $\rho^d_{S_n}(\mathbb{C}_d[S_n])$ es $\rho^n_{U(d)}(\mathbb{C}[U(d)])$ y viceversa.*

Para mostrar esto serán necesarios tres resultados auxiliares.

Proposición 4.0.3. *Si V es un espacio vectorial complejo entonces $Sym_n(V)$ pensado como subespacio de $(\mathbb{C}^d)^{\otimes n}$ está generado por elementos de la forma $v \otimes \cdots \otimes v$ para $v \in V$.*

Notamos que si $\rho^n_{End(\mathbb{C}^d)} : End(\mathbb{C}^d) \to End(\mathbb{C}^d)^{\otimes n}$ es la extensión de $\rho^n_{U(d)}$ a $End(\mathbb{C}^d)$, es decir, $\rho^n_{End(\mathbb{C}^d)}(A) = A^{\otimes n}$ tenemos que:

$$\begin{aligned} Im(\rho^d_{S_n}) &= Sym_n(End(\mathbb{C}^d)^{\otimes n}) \\ &= \langle v \otimes \cdots \otimes v : v \in End(\mathbb{C}^d)^{\otimes n} \rangle \\ &= Im(\rho^n_{End(\mathbb{C}^d)}). \end{aligned}$$

Proposición 4.0.4. *Para toda matriz invertible $A \in GL(\mathbb{C}^d)$ la matriz $A^{\otimes n}$ se puede escribir como combinación lineal de matrices $U^{\otimes n}$ con $U \in U(d)$, en otras palabras, $Im(\rho^n_{GL(\mathbb{C}^d)}) = Im\left(\rho^n_{U(d)}\right)$.*

Demostración. En está demostración usaremos la siguiente notación para $A \in End(\mathbb{C}^d)$ y $n, k \in \mathbb{N}$:

$$A^{k\otimes n} := (A^k)^{\otimes n} = (A^{\otimes n})^k.$$

Sea $A \in GL(\mathbb{C}^d)$. Gracias al teorema de descomposición polar podemos factorizar $A = RU$ con R una matriz hermitiana y positiva y $U \in U(d)$ por lo cual se tiene que $A^{\otimes n} = R^{\otimes n}U^{\otimes n}$. Entonces basta mostrar que $R^{\otimes n} \in Im(\rho^n_{U(d)})$. Como la matriz R es simétrica podemos diagonalizarla unitariamente por lo que existen $V \in U(d)$ y D una matriz diagonal tal que $R = V^*DV$ por lo cual $R^{\otimes n} = V^{-\otimes n}D^{\otimes n}V^{\otimes n}$ lo cual reduce el problema a mostrar que $D^{\otimes n}$ está en la imagen de $\rho^n_{U(d)}$.
Sean $\omega = e^{2\pi i/d}$ y $\Omega = diag(\omega, \ldots, \omega^d)$. Notamos que el polinomio minimal de Ω es $x^d - 1$ por lo que las matrices $\Omega, \ldots, \Omega^d$ son linealmente independientes, además notamos que todas de ellas son diagonales por lo que son una base para el espacio de matrices diagonales $d \times d$. Por lo anterior podemos escribir a D como combinación lineal de $\Omega, \ldots, \Omega^d$, digamos $D = \sum_{k=1}^d c_k\Omega^k$ y como las matrices $\Omega, \ldots, \Omega^d$ conmutan tenemos que:

$$\begin{aligned}(e^D)^{\otimes n} &= e^{(D^{\otimes n})} \\ &= e^{\sum_i c_i(\Omega^i)^{\otimes n}} \\ &= \prod_i e^{c_i\Omega^{i\otimes n}}.\end{aligned}$$

Además notamos que las matrices Ω^i son unitarias, por lo que basta mostrar que $e^{cU^{\otimes n}}$ está en la imagen de $\rho^n_{U(d)}$.
Como el espacio vectorial $End(\mathbb{C}^d)^{\otimes n}$ tiene dimensión finita tenemos que existe $k \in \mathbb{N}$ tal que el espacio vectorial generado por $U^{\otimes n}, \ldots, U^{k\otimes n}$ coincide con el espacio vectorial generado por $(U^{s\otimes n})_{s\in\mathbb{N}}$ de aquí en adelante llamaremos V a dicho espacio. Como $(U^{s\otimes n})_{s\in\mathbb{N}} \subset Im(\rho^d_{S_n})$ tenemos que $V \subset Im(\rho^d_{S_n})$.
Sea $S_l = \sum_{j=1}^l cU^{j\otimes n}$ tenemos que $S_l \in V$ para todo $l \in \mathbb{N}$. Por lo tanto

$$e^{cU} = \lim_{l\to\infty} S_l \in V.$$

De lo anterior se muestra que $(e^D)^{\otimes n}$ está en la imagen de $\rho^d_{S_n}$, para cualquier matriz diagonal D concluimos la prueba notando que el mapeo exponencial $\exp : D_d(\mathbb{C}) \to D_d(\mathbb{C})$ (restringido a las matrices diagonales) es sobre.

$\square$

Como $GL(\mathbb{C}^d)$ es denso en $End(\mathbb{C}^d)$ podemos concluir 4.0.2 .
Las siguientes proposiciones son un caso particular de la restricción de escalares.

Proposición 4.0.5. *Todo $Im(\rho^d_{S_n})-$módulo admite a través de $\rho^d_{S_n}$ la estructura de $\mathbb{C}[S_n]-$módulo y bajo esta correspondencia se corresponden los $Im(\rho^d_{S_n})-$módulos irreducibles con $\mathbb{C}[S_n]-$módulos irreducibles.*

Proposición 4.0.6. *Si $\lambda \dashv n$ y $l(\lambda) \leq d$ entonces el S_n-módulo irreducible V^λ admite una estructura de $Im(\rho^d_{S_n})-$módulo irreducible y estos son todos los $Im(\rho^d_{S_n})-$módulos irreducibles.*

Demostración. Basta recordar que $Im(\rho^d_{S_n})$ $\square$

El fenómeno observado con las representaciones del grupo simétrico y las de $\Im(\rho^d_{S_n})$ no es exclusivo de este grupo. Se tiene un resultado análogo para el grupo unitario en la siguiente proposición.

Proposición 4.0.7. *Todo $Im(\rho^n_{U(d)})$-módulo irreducible admite la estructura de $U(d)-$módulo irreducible.*

Teorema 4.0.1. *Sea $W_\lambda = Hom_{S_n}(V_\lambda, (\mathbb{C}^d)^{\otimes n})$ para λ una partición del entero n con longitud menor o igual a d. Entonces W_λ es una representación irreducible de $U(d)$ y*

$$(\mathbb{C}^d)^{\otimes n} \sim \bigoplus_{\lambda \vdash n, l(\lambda) \leq d} W_\lambda \otimes V_\lambda.$$

Como representaciones de $S_n \times U(d)$, la representación $V_\lambda \otimes W_\lambda$ es $S_n \times U(d)-$irreducible y $V_{\lambda_1} \otimes W_{\lambda_1}$ es isomorfa a $V_{\lambda_2} \otimes W_{\lambda_2}$ solo cuando $\lambda_1 = \lambda_2$.

Demostración. Ya mostramos que el conmutador de $Im(\rho_{S_n})$ es $Im(\rho^n_{U(d)})$ por lo que podemos usar el teorema del doble conmutador para mostrar que existe esta descomposición como $Im(\rho^d_{S_n}) \otimes Im(\rho^n_{U(d)})-$módulos. Por las proposiciones anteriores podemos cambiar $Im(\rho^n_{U(d)})-$módulos irreducibles por $U(d)-$módulos irreducibles y $Im(\rho^d_{S_n})$-módulos irreducibles por módulos de Specht V^λ con λ una partición de n con longitud a lo mas d. $\square$

También del teorema del doble conmutador obtenemos el siguiente corolario.

Corolario 4.0.2. *La imagen de $\rho^d_{S_n}$ es $End_{U(d)}(\mathbb{C}^d)^{\otimes n}$.*

Proposición 4.0.8. *El producto interno $\langle A, B\rangle = Tr(AB^*)$ definido en $End(\mathbb{C}^d)^{\otimes n}$ es invariante bajo la acción de conjugación de $U(d)$.*

Demostración. Sean $A, B \in End((C^d)^{\otimes n}$ para cada operador unitario $U \in U(d)$ tenemos que:

$$\begin{aligned}
\langle U^{\otimes n} A U^{-\otimes n}, U^{\otimes n} B U^{-\otimes n}\rangle &= Tr((UAU^*)(UBU^*)^*) \\
&= Tr(UAB^*U^*) \\
&= Tr(AB^*) \\
&= \langle A, B\rangle.
\end{aligned}$$

$\square$

Para $A \in End(\mathbb{C}^d)^{\otimes n}$ definimos

$$\mathbb{E}(A) = \int_{U \in U(d)} U^{\otimes n} A U^{-\otimes n} dU.$$

Proposición 4.0.9. *La función $\mathbb{E}$ es la proyección ortogonal a $End_{U(d)}(\mathbb{C}^d)^{\otimes n}$ bajo el producto interno definido anteriormente.*

Demostración. Para $U_0 \in U(d)$ se tiene que por la invarianza de la medida de Haar:

$$\begin{aligned}
U_0^{\otimes n}\mathbb{E}(A)U_0^{-\otimes n} &= U_0^{\otimes n}\int_{U\in U(d)} U^{\otimes n}AU^{-\otimes n}dUU_0^{-\otimes n} \\
&= \int_{U\in U(d)} U_0^{\otimes n}U^{\otimes n}AU^{-\otimes n}U_0^{-\otimes n}dU \\
&= \int_{U\in U(d)} (U_0U)^{\otimes n}A(U_0U)^{-\otimes n}dU \\
&= \mathbb{E}(A).
\end{aligned}$$

Esto muestra que $Im(\mathbb{E}) \subset End_{U(d)}(\mathbb{C}^d)^{\otimes n}$ y que $\mathbb{E}^2 = \mathbb{E}$. Por lo tanto $\mathbb{E}$ es una proyección. Además si $A \in End_{U(d)}(\mathbb{C}^d)^{\otimes n}$ y $U \in U(d)$ es un operador unitario tenemos que $U^{\otimes n}AU^{-\otimes n} = A$ por lo que $\mathbb{E}(A) = A$. De donde concluimos que $End_{U(d)}(\mathbb{C}^d)^{\otimes n} \subset Im(\mathbb{E})$.

□

Proposición 4.0.10. *El mapa $\mathbb{E}$ es un $U(d)-$homomorfismo.*

Demostración. El resultado se sigue de que $\mathbb{E}$ es la proyección ortogonal a la componente isotípica trivial respecto a un producto interno $U(d)-$invariante. □

Gracias al teorema del doble conmutador tenemos el siguiente corolario.

Corolario 4.0.3. *La imagen de $\mathbb{E}$ coincide con la imagen de $\rho_{S_n}^d$.*

Proposición 4.0.11. *El homomorfismo $\mathbb{E}$ es una esperanza condicional de $End(\mathbb{C}^d)^{\otimes n}$ en la subálgebra $End_{U(d)}(\mathbb{C}^d)^{\otimes n}$.*

Demostración. Como la integral y la conjugación son $\mathbb{C}-$lineales tenemos que $\mathbb{E}$ es $\mathbb{C}-$lineal. Por otro lado notamos que $\mathbb{E}(B)$ y $U^{\otimes n}$ conmutan por lo que:

$$\begin{aligned}
\mathbb{E}(\mathbb{E}(A)B) &= \int_{U\in U(d)} U^{\otimes n}AU^{-\otimes n}\left(\mathbb{E}(B)\right)dU \\
&= \left(\int_{U\in U(d)} U^{\otimes n}AU^{-\otimes n}dU\right)E(B) \\
&= \mathbb{E}(A)\mathbb{E}(B).
\end{aligned}$$

Por otro lado como la traza es un invariante que distingue clases de conjugación se tiene que:

$$\begin{aligned}
Tr(\mathbb{E}(A)) &= Tr\left(\int_{U\in U(d)} U^{\otimes n}AU^{-\otimes n}dU\right) \\
&= \int_{U\in U(d)} Tr(U^{\otimes n}AU^{-\otimes n})dU \\
&= \int_{U\in U(d)} Tr(A)dU \\
&= Tr(A),
\end{aligned}$$

por lo que está esperanza condicional es compatible con la traza normalizada. □

Ahora definiremos otro homomorfismo estrechamente relacionado con el operador $\mathbb{E}$. Para $A \in End(\mathbb{C}^d)^{\otimes n}$ definimos

$$\Phi(A) = \sum_{\sigma \in S_n} Tr(A\rho^d_{S_n}(\sigma^{-1}))\sigma.$$

Notamos que $\Phi(A)$ es un elemento del álgebra de grupo $\mathbb{C}[S_n]$ y que Φ es lineal ya que la traza lo es. En la siguiente proposición se muestra que Φ es un $\mathbb{C}[S_n]$ bi-homomorfismo.

Proposición 4.0.12. *Para cualquiera $\sigma_0 \in S_n$ y $A \in End(\mathbb{C}^d)^{\otimes n}$ se tiene que:*

$$\Phi(A\rho^d_{S_n}(\sigma_0)) = \Phi(A)\sigma_0,$$

$$\Phi(\rho^d_{S_n}(\sigma_0)A) = \sigma_0\Phi(A).$$

Demostración. Se tiene que:

$$\begin{aligned}\Phi(A\rho^d_{S_n}(\sigma_0)) &= \sum_{\sigma \in S_n} Tr(A\rho^d_{S_n}(\sigma_0)\rho^d_{S_n}(\sigma^{-1}))\sigma \\ &= \sum_{\sigma \in S_n} Tr(A\rho^d_{S_n}(\sigma_0\sigma^{-1}))\sigma.\end{aligned}$$

Luego hacemos el cambio de variable $\tau = \sigma\sigma_0^{-1}$ por lo que $\tau^{-1} = \sigma_0\sigma^{-1}$ y $\sigma = \tau\sigma_0$ por lo que el último termino es lo mismo que :

$$\sum_{\tau \in S_n} Tr(A\rho^d_{S_n}(\tau^{-1}))\tau\sigma_0 = \Phi(A)\sigma_0.$$

Por otro lado tenemos que:

$$\begin{aligned}\Phi(\rho^d_{S_n}(\sigma_0)A) &= \sum_{\sigma \in S_n} Tr(\rho^d_{S_n}(\sigma_0)A\rho^d_{S_n}(\sigma^{-1}))\sigma \\ &= \sum_{\sigma \in S_n} Tr(A\rho^d_{S_n}(\sigma^{-1})\rho^d_{S_n}(\sigma_0))\sigma \\ &= \sum_{\sigma \in S_n} Tr(A\rho^d_{S_n}(\sigma^{-1}\sigma_0))\sigma.\end{aligned}$$

Haciendo el cambio de variable $\tau = \sigma_0^{-1}\sigma$ se tiene que $\tau^{-1} = \sigma^{-1}\sigma_0$ y que $\sigma = \sigma_0\tau$ por lo que el último termino se puede ver como:

$$\sum_{\tau \in S_n} Tr(A\rho^d_{S_n}(\tau^{-1})\sigma_0\tau = \sigma_0\Phi(A).$$

□

Este resultado lo podemos extender por linealidad a todos los elementos del álgebra $\mathbb{C}[S_n]$.

Corolario 4.0.4. *Para cualquier $f \in \mathbb{C}[S_n]$ tenemos que:*

$$\Phi(A\rho^d_{S_n}(f)) = \Phi(A)f,$$

$$\Phi(\rho^d_{S_n}(f)A) = f\Phi(A).$$

En la siguiente parte de este trabajo se estudiarán algunas de las relaciones que guardan el mapeo Φ y la esperanza condicional $\mathbb{E}$.

Proposición 4.0.13. *Para cualquier $A \in End(\mathbb{C}^d)^{\otimes n}$ se tiene que $\Phi(\mathbb{E}(A)) = \Phi(A)$.*

Demostración. Por definición tenemos que

$$\Phi(\mathbb{E}(A)) = \sum_{\sigma \in S_n} Tr\left(\int_{U \in U(d)} U^{\otimes n} A U^{-\otimes n} dU \rho^d_{S_n}(\sigma^{-1})\right)\sigma.$$

Como la integral conmuta con funciones lineales y Tr, $\rho^d_{S_n}$ son lineales, podemos escribir lo anterior como:

$$\sum_{\sigma \in S_n} \int_{U \in U(d)} Tr\left(U^{\otimes n} A U^{-\otimes n} \rho^d_{S_n}(\sigma^{-1})\right) dU \sigma.$$

Además se tiene que $U^{-\otimes n} = \rho^n_{U(d)}(U^{-1})$ por lo que este operador conmuta con $\rho^d_{S_n}(\sigma^{-1})$.

$$\Phi(\mathbb{E}(A)) = \sum_{\sigma \in S_n} \int_{U \in U(d)} Tr\left(U^{\otimes n} A \rho^d_{S_n}(\sigma^{-1}) U^{-\otimes n}\right) dU \sigma.$$

Además, la traza es un invariante en clases de conjugación, por lo que:

$$\Phi(\mathbb{E}(A)) = \sum_{\sigma \in S_n} \int_{U \in U(d)} Tr\left(A \rho^d_{S_n}(\sigma^{-1})\right) dU \sigma.$$

Como el volumen del grupo unitario respecto con la medida de Haar es 1 tenemos que:

$$\begin{aligned}\Phi(\mathbb{E}(A)) &= \sum_{\sigma \in S_n} Tr\left(A \rho^d_{S_n}(\sigma^{-1})\right)\sigma \\ &= \Phi(A).\end{aligned}$$

□

Proposición 4.0.14. *Para cualesquiera $A, B \in End(\mathbb{C}^d)^{\otimes n}$ se cumple que:*

$$\Phi(A\mathbb{E}(B))\Phi(Id) = \Phi(A)\Phi(B).$$

Demostración. Recordamos que $\mathbb{E}(B) \in End_{U(d)}(\mathbb{C}^d)^{\otimes n})$ y que esta álgebra es la imagen de $\rho^d_{S_n}$ por lo que $\mathbb{E}(B) = \rho^d_{S_n}(f)$ para algún $f \in \mathbb{C}[S_n]$ por lo que se tiene que:

$$\begin{aligned}\Phi(A\mathbb{E}(B))\Phi(Id) &= \Phi(A\rho^d_{S_n}(f))\Phi(Id) \\ &= \Phi(A) f \Phi(Id) \\ &= \Phi(A)\Phi(\rho^d_{S_n}(f) Id) \\ &= \Phi(A)\Phi(\mathbb{E}(B)) \\ &= \Phi(A)\Phi(B).\end{aligned}$$

□

Proposición 4.0.15. *Si pensamos al caracter de $\rho^d_{s_n}$ como elemento del álgebra de grupo este coincide con $\Phi(Id)$.*

Demostración. Como lo caracteres del grupo simétrico toman valores enteros tenemos que:

$$\begin{aligned}\Phi(Id) &= \sum_{\sigma\in S_n} Tr(Id\rho^d_{S_n}(\sigma^{-1}))\sigma \\ &= \sum_{\sigma\in S_n} \overline{Tr(\rho^d_{S_n}(\sigma))}\sigma \\ &= \sum_{\sigma\in S_n} Tr(\rho^d_{S_n}(\sigma))\sigma,\end{aligned}$$

por lo que a este ultimo elemento del álgebra del grupo S_n se corresponde con

$$\sum_{\sigma\in S_n} Tr(\rho^d_{S_n}(\sigma))\delta_\sigma,$$

y esto es el caracter de la representación $\rho^d_{S_n}$.

$\square$

Por la dualidad de Schur-Weyl tenemos que la $S_n \times U(d)$ representación $(\mathbb{C}^d)^{\otimes n}$ se descompone como

$$\bigoplus_{\lambda\dashv n, l(\lambda)\leq d} V^\lambda \otimes W^\lambda.$$

Por lo que el caracter de $\rho^d_{S_n}$ (pensando a la descomposición anterior únicamente como de $\mathbb{C}[S_n]-$módulos) se puede escribir como:

$$\begin{aligned}\chi_{\rho^d_{S_n}} &= \sum_{l(\lambda)\leq d} \dim(W_\lambda)\chi_\lambda \\ &= \sum_{l(\lambda)\leq d} \frac{n!\dim(W_\lambda)}{\chi_\lambda(e)} p_\lambda.\end{aligned}$$

De lo anterior notamos que $\Phi(Id) \in \mathbb{C}_d[S_n]$.

Proposición 4.0.16. *La imagen de* Φ *es* $\mathbb{C}_d[S_n]$.

Demostración. Notamos que $\bigoplus_{l(\lambda)\leq d} End(V_\lambda)$ es un ideal bilateral del álgebra $\bigoplus_{\lambda\dashv n} End(V_\lambda)$ por lo que $\mathbb{C}_d[S_n]$ es un ideal bilateral del álgebra de grupo $\mathbb{C}[S_n]$. De lo anterior tenemos que para todo $A \in End(\mathbb{C}^d)^{\otimes n}$ existe un elemento del álgebra de grupo $f \in \mathbb{C}[S_n]$ tal que $\rho^d_{S_n}(f) = \mathbb{E}(A)$. Por lo que:

$$\begin{aligned}\Phi(A) &= \Phi(\mathbb{E}(A)) \\ &= \Phi(\rho^d_{S_n}(f)Id) \\ &= f\Phi(Id),\end{aligned}$$

y por la propiedad de ideal tenemos que $\Phi(A) \in \mathbb{C}_d[S_n]$. $\square$

Ahora consideremos a $\mathbb{C}_d[S_n]$ como subálgebra. Para mostrar lo que queremos basta probar que $\Phi(Id)$ es invertible dentro de está subálgebra. Por lo que si $f \in \mathbb{C}_d[S_n]$ y g es la inversa de $\Phi(Id)$ en $\mathbb{C}_d[S_n]$ se tiene que:

$$\begin{aligned}\Phi(\rho^d_{S_n}(fg)) &= \Phi(\rho^d_{S_n}(fg)Id) \\ &= fg\Phi(Id) \\ &= f.\end{aligned}$$

Proposición 4.0.17. *En el álgebra $\mathbb{C}_d[S_n]$ tenemos que $\Phi(Id)$ en invertible, su inversa es conocida como la función de Weingarten y está dado por:*

$$Wg = \frac{1}{n!^2} \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} \frac{\chi_\lambda(e)^2}{\dim(W_\lambda)} \chi_\lambda.$$

Demostración. Recordamos que:

$$\Phi(Id) = \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} \dim(W_\lambda) \chi_\lambda.$$

Esto lo podemos escribir en términos de los proyectores centrales como:

$$\Phi(Id) = \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} \frac{n! \dim(W_\lambda)}{\chi_\lambda(e)} p_\lambda.$$

También podemos escribir a la función de Weingarten en termino de los proyectores centrales:

$$Wg = \frac{1}{n!} \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} \frac{\chi_\lambda(e)}{\dim(W_\lambda)} p_\lambda.$$

Recordamos que $\{p_\lambda\}_{\lambda \dashv n}$ son proyecciones ortogonales por lo que

$$\begin{aligned}
\Phi(Id)Wg &= \frac{1}{n!} \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} \frac{n! \dim(W_\lambda)\chi_\lambda(e)}{\dim(W_\lambda)\chi_\lambda(e)} p_\lambda p_\lambda \\
&= \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} p_\lambda^2 \\
&= \sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} p_\lambda.
\end{aligned}$$

Además tenemos que $\mathbb{C}[S_n]$ es isomorfo a $\bigoplus_{\lambda \dashv n} End(V_\lambda)$ y que bajo ese isomorfismo se corresponden las subálgebras $\mathbb{C}_d[S_n]$ con $\bigoplus_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} End(V_\lambda)$ y los elementos p_λ con Id_{V_λ}. Luego notamos que

$$\sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} Id_{V_\lambda} = Id_{\bigoplus_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} End(V_\lambda)}.$$

Usando el isomorfismo tenemos que:

$$\sum_{\substack{\lambda \dashv n \\ l(\lambda) \leq d}} p_\lambda = 1_{\mathbb{C}_d[S_n]}.$$

Por lo tanto la función de Weingarten es la inversa de $\Phi(Id)$ en la subálgebra $\mathbb{C}_d[S_n]$. $\square$

De lo anterior podemos concluir que dentro del álgebra $\mathbb{C}_d[S_n]$ se tiene que:

$$\begin{aligned}\Phi(A\mathbb{E}(B)) &= \Phi(A)\Phi(B)\Phi(Id)^{-1}\\ &= \Phi(A)\Phi(B)Wg.\end{aligned}$$

Proposición 4.0.18. *Si i, i', j y j' son $n-$tuplas de enteros positivos menores que d entonces:*

$$\int_{U\in U(d)} u_{i_1j_1}\cdots u_{i_nj_n}\overline{u_{i'_1j'_1}\cdots u_{i'_nj'_n}}dU = \sum_{\sigma,\tau\in S_n}\delta_{i_1i'_{\sigma(1)}}\cdots\delta_{i_ni'_{\sigma(n)}}\delta_{j_1j'_{\tau(1)}}\cdots\delta_{j_nj'_{\tau(n)}}Wg(\tau\sigma^{-1}).$$

Demostración. Denotaremos por $e_1, \cdots, e_d$ a la base canónica de $\mathbb{C}^d$ y por E_{ij} a la matriz elemental cuya única entrada no nula es 1.
Para cualesquiera matriz $U \in U(d)$ se tiene que:

$$\begin{aligned}(UE_{j_rj'_r}U^*)_{ij} &= \sum_{k,l} U_{il}(E_{j_rj_{r'}})_{lk}(U^*)_{kj}\\ &= U_{ij_r}\overline{U_{jj_{r'}}}.\end{aligned}$$

Usando esto tenemos que:

$$\begin{aligned}Tr(E_{i'_ri_r}UE_{j_rj'_r}U^*) &= \sum_{l}(E_{i'_ri_r}UE_{j_rj'_r}U^*)_{ll}\\ &= \sum_{l,k}(E_{i'_ri_r})_{lk}(UE_{j_rj'_r}U^*)_{kl}\\ &= (UE_{j_rj'_r}U^*)_{i_ri'_r}\\ &= U_{i_rj_r}\overline{U_{i'_rj_{r'}}},\end{aligned}$$

por lo que:

$$\begin{aligned}&Tr((E_{i'_1i_1}\otimes\cdots\otimes E_{i'_ni_n})(UE_{j_1j'_1}U^*\otimes\cdots\otimes UE_{j_nj'_n}U^*))\\ &= Tr(E_{i'_1i_1}UE_{j_1j'_1}U^*\otimes\cdots\otimes E_{i'_ni_n}UE_{j_nj'_n}U^*)\\ &= U_{i_1j_1}\cdots U_{i_nj_n}\overline{U_{i'_1j'_1}\cdots U_{i'_nj'_n}}.\end{aligned}$$

También notamos que:

$$UE_{j_1j'_1}U^*\otimes\cdots\otimes UE_{j_nj'_n}U^* = U^{\otimes n}(E_{j_1j'_1}\cdots\otimes E_{j_nj'_n})U^{-\otimes n},$$

y como la integral conmuta con funciones lineales se tiene que:

$$\begin{aligned}&\int_{U\in U(d)} U_{i_1j_1}\cdots U_{i_nj_n}\overline{U_{i'_1j'_1}\cdots U_{i'_nj'_n}}dU\\ &= \int_{U\in U(d)} Tr((E_{i'_1i_1}\otimes\cdots\otimes E_{i'_ni_n})(U^{\otimes n}E_{j_1j'_1}\cdots\otimes E_{j_nj'_n}U^{-\otimes n}))dU\\ &= Tr((E_{i'_1i_1}\otimes\cdots\otimes E_{i'_ni_n})\int_{U\in U(d)}(U^{\otimes n}E_{j_1j'_1}\cdots\otimes E_{j_nj'_n}U^{-\otimes n}))dU\\ &= \Phi((E_{i'_1i_1}\otimes\cdots\otimes E_{i'_ni_n})\mathbb{E}(E_{j_1j'_1}\cdots\otimes E_{j_nj'_n}))(e).\end{aligned}$$

Notamos que $E_{ij}e_k = \delta_{jk}e_i$. Por lo cual:

$$E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n}(e_{k_1} \otimes \cdots \otimes e_{k_n}) = (\delta_{k_1 i_1} \cdots \delta_{k_n i_n})(e_{i'_1} \otimes \cdots \otimes e_{i'_n}),$$

por lo que la expresión anterior se anula en todos los elementos de la base de $(\mathbb{C}^d)^{\otimes n}$ excepto en $e_{i_1} \otimes \cdots \otimes e_{i_n}$. Por lo que para toda $\sigma \in S_n$ se tiene que:

$$\begin{aligned}\Phi(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n}) &= \rho^d_{S_n}(\sigma)(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})(e_{i_1} \otimes \cdots \otimes e_{i_n}) \\ &= \rho^d_{S_n}(\sigma)(e_{i'_1} \otimes \cdots \otimes e_{i'_n}) \\ &= e_{i'_{\sigma^{-1}(1)}} \otimes \cdots \otimes e_{i'_{\sigma^{-1}(n)}},\end{aligned}$$

por lo tanto la traza de $\rho^d_{S_n}(\sigma)(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})$ es:

$$Tr(\rho^d_{S_n}(\sigma)(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})) = \delta_{i_1 i'_{\sigma^{-1}.(1)}} \cdots \delta_{i_1 i'_{\sigma^{-1}(n)}}$$

Para concluir evaluaremos la ecuación que relaciona Φ y $\mathbb{E}$ en las matrices $A = E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n}$ y $B = E_{j_1 j'_1} \otimes \cdots \otimes E_{j_n j'_n}$. Para obtener una igualdad de funciones las cuales evaluaremos en el elemento identidad del grupo simétrico. Tenemos que como elementos del álgebra $\mathbb{C}_d[S_n]$:

$$\begin{aligned}&\Phi(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})\Phi(E_{j_1 j'_1} \otimes \cdots \otimes E_{j_n j'_n})Wg \\ &= \sum_{\sigma,\tau,\mu \in S_n} \Phi(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})(\sigma)\Phi(E_{j_1 j'_1} \otimes \cdots \otimes E_{j_n j'_n})(\tau)Wg(\mu)(\sigma\tau\mu).\end{aligned}$$

Evaluando en la identidad tenemos que:

$$\begin{aligned}&[\Phi(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})\Phi(E_{j_1 j'_1} \otimes \cdots \otimes E_{j_n j'_n})Wg](e) \\ &= \sum_{\sigma,\tau \in S_n} \Phi(E_{i'_1 i_1} \otimes \cdots \otimes E_{i'_n i_n})(\sigma)\Phi(E_{j_1 j'_1} \otimes \cdots \otimes E_{j_n j'_n})(\tau)Wg(\tau^{-1}\sigma^{-1}) \\ &= \sum_{\sigma,\tau \in S_n} \delta_{i_1 i'_{\sigma(1)}} \cdots \delta_{i_n i'_{\sigma(n)}} \delta_{j_1 j'_{\tau(1)}} \cdots \delta_{j_n j'_{\tau(n)}} Wg(\tau\sigma^{-1}).\end{aligned}$$

□

Este resultado nos servirá para mostrar que las matrices Haar unitarias son asintóticamente libres de las matrices deterministas. Para ello necesitaremos una estimación asintótica de la función de Weingarten la cual puede ser encontrada en [6].

Proposición 4.0.19. *Se tiene que para $\sigma \in S_n$ la función de Weingarten es una expresión racional en d, además:*

$$Wg(\sigma) = Moeb(\sigma)d^{-n-|\sigma|} + O(d^{-n-|\sigma|-2}).$$

Usando la anterior se pueden probar resultados de independencia libre asintótica entre matrices deterministas y matrices de Haar.

Teorema 4.0.5. *Sean $(U_n^{(1)}, \ldots, U_n^{(p)})_{n\in\mathbb{N}}$ una familia de ensambles Haar unitarios independientes y $(D_n^{(1)}, \ldots, D_n^{(p)})_{n\in\mathbb{N}}$ ensambles deterministas de modo que $(D_n^{(1)}, \ldots, D_n^{(q)}) \to (d_1, \ldots, d_q)$ en $*-$distribución con respecto a la traza normalizada, entonces*

$$(U_n^{(1)}, \ldots, U_n^{(p)}, D_n^{(1)}, \ldots, D_n^{(q)}) \to (u_1, \ldots, u_p, d_1, \ldots, d_q)$$

en $*-$distribución donde $u_1, \ldots, u_p$ son elementos Haar unitarios y $u_1, \ldots, u_p, \{d_1, \ldots, d_q\}$ son libres.

Teorema 4.0.6. *Sean* $(A_n)_{n\in\mathbb{N}}$ *y* $(B_n)_{n\in\mathbb{N}}$ *son ensambles de matrices deterministas y* $(U_n)_{n\in\mathbb{N}}$*. Si existe un* $*-$*espacio de probabilidad* $(\mathcal{A},\tau)$ *y* $a,b\in\mathcal{A}$ *de modo que* $(A_n,B_n)\to(a,b)$ *en* $*-$*distribución con respecto a la traza normalizada. Entonces* $U_nA_nU_n^*$ *y* B_n *son asintoticamente libres.*

Bibliografía

[1] Distribution of eigenvalues for some sets of random matrices. *Mat. Sb. N.S. (en Ruso)*, 72:507–536, 1967.

[2] J.L. Alperin and R.B. Bell. *Groups and representations*. Graduate texts in mathematics. Springer, 1995.

[3] P. Biane. Representations of symmetric groups and free probability. *Advances in Mathematics*, 138(1):126 – 181, 1998.

[4] Philippe Biane. Some properties of crossings and partitions. *Discrete Mathematics*, 175(1):41 – 53, 1997.

[5] Benoît Collins and Piotr Śniady. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264(3):773–795, 06 2006.

[6] Benoît Collins. Moments and cumulants of polynomial random variables on unitarygroups, the itzykson-zuber integral, and free probability. *International Mathematics Research Notices*, 2003(17):953–982, 2003.

[7] W. Fulton. *Young Tableaux: With Applications to Representation Theory and Geometry*. London Mathematical Society St. Cambridge University Press, 1997.

[8] A. Ben Ghorbal and M. Schuermann. Non commutative notions of stochastic independence.

[9] R. Goodman and N.R. Wallach. *Representations and Invariants of the Classical Groups*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2000.

[10] S. Kerov. A differential model of growth of young diagrams. 1996.

[11] J.A. Mingo and R. Speicher. *Free Probability and Random Matrices*. Fields Institute Monographs. Springer New York, 2017.

[12] A. Nica and R. Speicher. *Lectures on the Combinatorics of Free Probability*. Number v. 13 in Lectures on the combinatorics of free probability. Cambridge University Press, 2006.

[13] Belinschi Serban T., Tobias M., and Speicher R. Analytic subordination theory of operator-valued free additive convolution and the solution of a general random matrix problem . *Journal für die reine und angewandte Mathematik (Crelles Journal)* ., 2017.

[14] S V. Kerov. Transition probabilities for continual young diagrams and markov moment problem. 27, 03 2000.

[15] Dan Voiculescu. Limit laws for random matrices and free products. *Inventiones mathematicae*, 104(1):201–220, Dec 1991.

[16] E. Wigner. Characteristic vectors of bordered matrices with infinite dimensions. *Ann. Math.*, 1955.

[17] E. Wigner. On the distribution of the roots of certain symmetric matrices. *Ann. Math.*, 1958.

[18] Feng Xu. A random matrix model from two dimensional yang-mills theory. *Communications in Mathematical Physics*, 190(2):287–307, Dec 1997.