UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

TESIS:

TEORÍA DE REPRESENTACIONES DE GRUPOS FINITOS Y ALGUNAS APLICACIONES A LA PROBABILIDAD

POR:

MERCEDES ELISA PÉREZ FERNÁNDEZ

PARA OPTAR AL GRADO DE:

LICENCIADA EN MATEMÁTICA

Ciudad Universitaria, noviembre de 2018

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

TESIS:

TEORÍA DE REPRESENTACIONES DE GRUPOS FINITOS Y ALGUNAS APLICACIONES A LA PROBABILIDAD

POR:

MERCEDES ELISA PÉREZ FERNÁNDEZ

PARA OPTAR AL GRADO DE:

LICENCIADA EN MATEMÁTICA

ASESOR:

PhD. RIQUELMI SALVADOR CARDONA FUENTES

Ciudad Universitaria, noviembre de 2018

AUTORIDADES

RECTOR:

MSc. ROGER ARMANDO ARIAS ALVARADO

SECRETARIO GENERAL:

LIC. CRISTOBAL HERNÁN RÍOS BENÍTEZ

FISCAL GENERAL:

LIC. RAFAEL HUMBERTO PEÑA MARÍN

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

DECANO:

LIC. MAURICIO HERNÁN LOVO CÓRDOVA

SECRETARIA:

LIC. DAMARIS MELANY HERRERA TURCIOS

ESCUELA DE MATEMÁTICA

DIRECTOR:

PhD. JOSÉ NERYS FUNES TORRES

SECRETARIA:

MsC. ALBA IDALIA CÓRDOVA CUÉLLAR

Ciudad Universitaria, noviembre de 2018

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA
ESCUELA DE MATEMÁTICA

PhD. RIQUELMI SALVADOR CARDONA FUENTES

ASESOR

Ciudad Universitaria, noviembre de 2018

Agradecimientos

La culminación de este trabajo de investigación marca el fin de este camino.

Producto no solo de mi esfuerzo,

sino también de muchas voces que se unieron en medio del ruido de la vida.

A todas ellas gracias por susurrarme al corazón cuando las dificultades me bloqueaban, así como por acompañarme en los momentos de dicha.

Primeramente a Dios por sostener mi mano en medio de los momentos de tribulación.

A mi asesor, PhD. Riquelmi Salvador Cardona Fuente, por guiarme y ayudarme a pulir mis esfuerzos, por haber tenido la paciencia de guiar con sus palabras firmes mis inconsistencias, agradezco enormemente su valiosa dirección y apoyo para seguir este camino y llegar a la conclusión del mismo.

También al Lic. Américo Mejía López, docente y motivación en este proceso de prueba y error para llegar a este logro.

De igual manera Al MSc. Rene Palacios que incentivó y motivo mi curiosidad para abordar este tema.

Agradezco, a mi compañero y afecto en la vida, Jonathan de Jesús Árevalo Duran por caminar a mi lado durante este viaje.

Y sin olvidar lo importante que son mi madre Karla Patricia Fernández de Pérez, mi padre Francisco Antonio Pérez y mi tía Mercedes Galdámez, por sus consejos, paciencia e incondicional apoyo durante toda mi carrera, gracias por todo lo que en palabras no puedo expresar pero que en silencio saben.

Ad referendam gratiam sencera.

Resumen

El presente trabajo de graduación contiene el desarrollo teórico de las Representaciones de Grupos Finitos sobre los números complejos utilizando conocimientos de Álgebra Lineal y teoría básica de grupos. Asimismo, presenta algunas de las aplicaciones de este tópico a la Probabilidad. En general este trabajo incluye: definiciones básicas y ejemplos de representaciones de grupos finitos, la Teoría de Caracteres, el Álgebra de Grupo y Análisis de Fourier, *pq*-Teorema de Burnside y el Teorema de la Dimensión, finalizando con algunas aplicaciones a la Teoría de Probabilidad a través de los Paseos Aleatorios.

En el primer capítulo se expone la teoría básica de representaciones de grupos finitos (definiciones, ejemplos y algunos resultados) sobre el cuerpo de los complejos, en el segundo capítulo se desarrolla la teoría básica de caracteres como: el carácter de una representación, las relaciones de ortogonalidad, la descomposición de la representación regular de un grupo finito, el lema de Schur y sus aplicaciones, entre otros. Además, se hace un breve estudio del Análisis de Fourier sobre Grupos Finitos en el tercer capítulo, que permite ver a las representaciones de grupos a través de la transformada de Fourier utilizando la Teoría de Caracteres.

Finalmente, en este trabajo se presentan dos tipos de aplicaciones en dos capítulos diferentes, la primera de esta aplicaciones es teórica, se desarrolla en el cuarto capítulo y consiste en la demostración del *pq*-Teorema de Burnside, para la cuál fue necesario hacer un breve repaso de Teoría de Números y Teoría básica de Galois. La otra aplicación que se desarrolla en el último capítulo, consiste en aplicar los conceptos fundamentales de la Teoría de Representaciones a la Probabilidad, específicamente al Barajado de Cartas utilizando los Paseos Aleatorios. Cabe mencionar que si el lector no desea ver la aplicación teórica puede, sin ningún problema, omitir el capítulo 4 y leer directamente el capítulo 5, ya que para abordar las probabilidades sobre grupos, basta con tener conocimiento de la transformada de Fourier y el producto convolución.

Atentamente

Elisa Fernández

Palabras clave:

Representaciones de Grupos

Teoría de Caracteres

Análisis de Fourier sobre grupos finitos

Barajado de Cartas

Índice general

Índice de Figuras

Índice de Tablas

Introducción

La Teoría de Representaciones de Grupos es un elemento importante en la matemática ya que actualmente, es un a´rea que posee gran cantidad de aplicaciones, en diversas ciencias ya sea exactas, e inexactas, por ejemplo en matemática y música; asimismo pueden encontrarse aplicaciones en Geometría Algebraica, Teoría del Número, Teoría de Grafos, Antropología Algebraica, Estadística y Probabilidad. Por otro lado, el estudio de los grupos especialmente los de orden finito aparece en diversas áreas de las ciencias como en Física particularmente en Mecánica Cuántica y en la Química en donde es muy útil para estudiar moléculas.

Históricamente el mayor triunfo de la Teoría de Representaciones fue el pq-Teorema de Burnside, que establece que un grupo no abeliano de orden $p^a q^b$ con p y q primos, no puede ser simple[(1)], o lo que es lo mismo, que cada grupo finito de orden $p^a q^b$ es soluble[(2)], en este trabajo se pretende demostrar este teorema, para lo cual tendremos que hacer una breve revisión de Teoría del Número; se estudiará además un resultado de Frobenius que usualmente es conocido como *El Teorema de la Dimensión*, el cual establece que el grado de cada representación irreducible de un grupo G divide al orden del grupo. Este resultado fue muy útil para determinar la tabla de caracteres de un grupo G cualquiera y con el tiempo, los caracteres resultaron ser extremadamente ricos y se convirtieron en una de las herramientas fundamentales de esta teoría, además Burnside se auxilió de ellos también para demostrar su teorema.

Se darán a conocer algunas aplicaciones de la Teoría de Representaciones a la Probabilidad, debido a su amplio campo de trabajo y las aplicaciones que tiene esta en diversas áreas, para ello se definirán los conceptos fundamentales que permitan poder abordar las Probabilidades sobre Grupos Finitos: probabilidad sobre grupos, norma y otros tópicos necesarios como el análisis de Fourier desde el punto de vista de la teoría de representaciones; además como otra de las aplicaciones se hará un pequeño abordaje de la teoría desarrollada por Diaconnis, que en su tiempo, fue necesaria para el estudio de problemas relativos al barajado de cartas. El desarrollo de la teoría básica y ambas aplicaciones mostraran, a lo largo de este trabajo, el vínculo entre la Probabilidad y la Teoría de Representaciones de Grupos Finitos.

La intención del trabajo que se plantea en este proyecto de graduación, será presentar

[(1)] Debemos recordar que un grupo es simple si no contiene subgrupos normales no triviales.

[(2)] Un grupo G se dice que es soluble si existe una cadena de subgrupos de G que satisfacen $\{e\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_k = G$, y en la que todos sus factores H_{i+1}/H_i, $i = 0, 1, 2, \ldots, k-1$, son abelianos.

el desarrollo teórico de este tópico, para lo cuál se incluirán ejercicios y demostraciones detalladas lo mejor posible de los teoremas y corolarios asociados al tema, de esta forma se pretende dar cumplimiento al objetivo especifico de este trabajo, el cual es exponer los ingredientes esenciales de la Teoría de Representaciones de Grupos Finitos sobre los números complejos utilizando conocimientos de Álgebra Lineal y teoría básica de grupos, para luego poder aplicarlos al Barajado de Cartas en Teoría de Probabilidad.

Metodología

1. **TIPO DE INVESTIGACIÓN**

   La investigación se realizó a través del *método bibliográfico*[3], por medio de un proceso sistemático y secuencial de recolección, selección, clasificación, evaluación y análisis de contenido del material existente sobre Representaciones de Grupos Finitos, cuyo estudio de teoremas, hipótesis, ejemplos, resultados, entre otros, estuviesen desarrollados por medio del Álgebra Lineal.

2. **PLAN PARA LA RECOLECCIÓN DE LA INFORMACIÓN**

   - Detección de información: Se consultaron diferentes fuentes como libros, artículos, tesis y revistas de divulgación matemática, todas principalmente en inglés.
   - Revisión de la información: De la información detectada en medios bibliográficos, se indagó la información pertinente al estudio de las representaciones, de la teoría de caracteres, el análisis de Fourier y las probabilidades sobre grupos vistas desde el álgebra lineal.
   - Selección de información: Se identificó la información pertinente al propósito de la investigación, priorizando la información relevante al estudio.
   - Extracción de información: De la información consultada, se extrajo la que abonó a la comprensión y demostración de los teoremas, lemas, proposiciones y ejemplos expuestos en el tema investigado.
   - Análisis de información: Se concretó y adecuó la información recabada, adecuándola según las necesidades de cada tópico estableciendo parámetros de organización y presentación de la información, tomando en cuenta las directrices de la investigación.

3. **ANÁLISIS**

   La información recabada se analizó en función del constructo teórico de la investigación, agrupándola en temas y subtemas para formar la base teórica del estudio.

[3] La investigación bibliográfica se caracteriza por la utilización de documentos; recolecta, selecciona, analiza y presenta resultados coherentes; porque utiliza los procedimientos lógicos y mentales de toda investigación; análisis, síntesis, deducción, inducción.

Antecedentes

Preliminares históricos: Los inicios de la Teoría de Representaciones

Las raíces históricas de la Teoría de Grupos son la Teoría del Número, y la teoría de ecuaciones algebraicas y geométricas. El desarrollo de las fuentes antes mencionadas empieza con Leonhard Euler, y es continuada por la obra de Gauss en la Aritmética Modular, y en los grupos aditivos y multiplicativos relacionados con los campos cuadráticos. Lagrange, Ruffini y Abel en la búsqueda de soluciones que fueran generales para las ecuaciones polinómicas de alto grado, fueron además pioneros en obtener resultados acerca de los grupos de permutaciones. Evariste Galois acuñó el término "grupo" y creó lo que ahora se conoce como la famosa teoría de Galois. En el área de la geometría, los grupos primero tuvieron relevancia en la geometría proyectiva y, algún tiempo después, en la geometría no euclidiana. El matemático alemán Félix Klein inauguró en 1872 su Programa de Erlangen proclamando que la Teoría de Grupos pasaba a ser el principio organizador o los puntos focales de estudio de la geometría. En este contexto el noruego Ludwig Sylow publicó la primera prueba de sus ahora famosos teoremas.

De los primeros tratados sobre grupos fue el de Jordan en su *Traité des Substitutions et des Équations Algébriques* (1870) y *Substitutionentheorie und Ihre Anwendungen auf die Algebra* (1882) de Netto. Ambos libros fueron sobre la teoría de permutaciones de grupos, sinónimo en aquel entonces de la Teoría de Grupos.

El primer artículo científico sobre teoría de representaciones de grupos finitos fue publicado por Ferdinand Georg Frobenius (1849-1917) teniendo como origen la correspondencia entre el mismo Frobenius y Richard Dedekind, en este sentido Dedekind propuso a Frobenius el problema de factorizar ciertos polinomios homogéneos provenientes de un determinante (llamado "Determinante de Grupo") asociado con un grupo finito G. En el caso en el que G es abeliano, Dedekind pudo factorizar el determinante de grupo en factores lineales usando los caracteres de G (que no son más que los homomorfismos de G dentro de un grupo con números complejos no nulos). Fue la genialidad de Frobenius la que permitió la invención de una *Teoría General de Caracteres* para grupos finitos arbitrarios y la uso para dar una solución completa al problema del determinante de grupo de Dedekind. El subsiguiente trabajo de Frobenius le permitió formular en 1897 la definición moderna de una representación de un grupo como un homomorfismo $\varphi\colon G \to GL_n(\mathbb{C})$ (una definición matricial). Además

de la invención de la *Teoría de Caracteres*, Frobenius hizo muchos otros aportes a la Teoría de Representación de Grupos Finitos, entre ellos tenemos:

- Fue capaz de introducir formalmente la noción de representaciones de grupo y relacionarlos con su determinante.

- Introdujo la "composición" de Caracteres (ahora llamada producto tensorial) y desarrolló la relación entre los caracteres de un grupo y los de sus subgrupos.

- Los cálculos de Frobenius para los caracteres de algunos grupos específicos, tuvieron un gran impacto en la teoría de representaciones y años después este trabajo se convirtió en un área de estudio sorprendentemente rica de la teoría de representación de grupos finitos de Lie.

- Incluso antes de su trabajo en la teoría de caracteres Frobenius tuvo interés en los grupos finitos solubles, publicando dos artículos en este sentido enfocados a la existencia y estructura de sus subgrupos. Posteriormente su interés se enfocó en su nueva teoría de caracteres de grupo.

- Con su estudiante Issai Schur, Frobenius introdujo la noción de índice (o indicador) de un carácter irreducible. Los índices de Frobenius-Schur contienen información importante del grupo G que va más allá de la tabla de caracteres de G.

La aparición del primer tratado en inglés sobre teoría de grupos finitos, fue gracias a William Burnside (1852-1927), esto después de la aparición de varios artículos de él mismo titulados "Notas Sobre la Teoría de Grupos de Orden Finito" y otros más. Posteriormente se hizo una segunda edición del libro con nuevo material en relación a la Teoría de Representaciones de Grupos.

Burnside tenía conocimientos sobre la teoría de grupos discontinuos debido a los trabajos de Klein y Poincaré, después de esto él se alejó de las matemáticas aplicadas y enfocó sus investigaciones en la teoría de grupos de orden finito. El y seguido de cerca por los trabajos de Hölder en grupos de orden específico, publicó sus propios resultados sobre la naturaleza del orden de grupos simples finitos. Los trabajos previos de Frobenius aparentemente despertaron su interés en los grupos solubles finitos.

En cuanto al trabajo de Burnside en la Teoría de Representaciones de Grupos, podemos decir que después de leer los artículos de Frobenius vio la importancia de la nueva teoría en su propia investigación de grupos finitos y lo primero que intento hacer fue entender los resultados de Frobenius a su propia manera, para después acercase a los trabajos de Sophus Lie en relación a la trasformación de grupos finitos (él era versado en los grupos y álgebras de

Lie, a diferencia de Frobenius). En este sentido analizando la estructura del Álgebra de Lie logro derivar los principales resultados de Frobenius tanto en la teoría de caracteres como con el determinante de grupo. Burnside nunca alegó que había descubierto algo nuevo, siempre le dio el reconocimiento a Frobenius, sólo aclarando que la forma de probar los teoremas fue por un camino distinto al seguido por este. En una siguiente etapa de su trabajo Burnside enfocó sus investigaciones a la naturaleza de las representaciones irreducibles y sus aplicaciones.

En general podemos decir entonces que Frobenius y Burnside, trabajando independientemente, exploraron esta nueva área y además sus aplicaciones a la Teoría de Grupos Finitos. A este trabajo contribuyeron también lssai Schur 1875-1941) y algunos años después Richard Bauer (1901-1977) entre otros.

Si recapitulamos, ya ha pasado más de un siglo desde que Dedekind le planteo el problema a Frobenius sobre factorizar un determinante asociado con un cierto grupo finito. La solución de este problema abstracto planteado a Frobenious permitió la invención de la Teoría de Caracteres y subsecuentemente la Teoría de Representación de Grupos Finitos. Actualmente estas teorías proveen herramientas básicas en varias ramas del Álgebra y su generalización a la topología. Estas teorías han sido aplicadas ampliamente en muchas áreas teóricas y aplicadas de la Física y la Química, como la Espectroscopia, Cristalografía, Mecánica Cuántica, teoría de orbitales, etc. Toda esta gran diversidad de aplicaciones son posibles gracias al trabajo puramente teórico de personajes como Dedekind, Frobenius y el mismo Burnside y de ahí la importancia de su estudio desde el punto de vista de las matemáticas puras así como de las matemáticas aplicadas.

Relación con otras áreas de la matemática

Las representaciones de los grupos son importantes porque permiten que muchos de los problemas de la Teoría de Grupos se reduzcan a problemas de Álgebra Lineal, haciéndolos más fáciles de entender. Es también importante en Física, ya que por ejemplo, describen cómo el grupo de simetría de un sistema físico afecta a las soluciones de las ecuaciones que describen ese sistema; y en el campo de la química, como por ejemplo la simetría molecular, el espacio se agrupa y los grupos puntuales de simetría describen simetrías moleculares y simetrías cristalinas.[10]

El término representación de un grupo también se utiliza en un sentido más general para referirse a cualquier *"Descripción"* de un grupo como un grupo de transformaciones de un objeto matemático. Más formalmente, una *"representación"* es un homomorfismo del grupo para el grupo de automorfismos de un objeto. Si el objeto es un espacio vectorial, por ejemplo, se tiene una representación lineal. Algunos autores utilizan la realización de la idea general y reservan el término representación para el caso especial de las representaciones lineales.

Ramas de la Teoría de Representaciones de Grupos Finitos

La Teoría de la Representaciones de Grupos se divide en subteorías dependiendo del tipo de grupo representado. Estas a pesar de que son muy diferentes en sus detalles, poseen algunas similitudes en las definiciones y conceptos básicos; entre estas tenemos:

- Grupos compactos o grupos localmente compactos.
- Grupos de Lie.
- Grupos algebraicos lineales.
- Grupos topológicos no compactos.
- Grupos finitos.

En este trabajo sólo se estudiaran estos últimos.

Física

Entre las aplicaciones en el campo de la Física destacan el análisis de la simetría de la función de onda de Schrödinger, la explicación de la degeneración *"complementaria"* en un campo de Coulomb, y ciertas cuestiones relacionadas con la teoría del estado sólido.[6]

Algunos ejemplos de grupos que se utilizan en Física

1. Grupo de desplazamientos (traslaciones) en el espacio tridimensional, cuyos elementos son las transformaciones de traslación del origen de coordenadas en un vector arbitrario $\mathbf{a}$, es decir: $r' = r + a$.
2. Grupo de rotaciones $O^+(3)$, cuyos elementos son las transformaciones de rotación del espacio tridimensional o matrices ortogonales correspondientes con el determinante igual a la unidad.
3. Los grupos de simetría de las moléculas (o grupos puntuales) están compuestos por ciertas transformaciones ortogonales del espacio tridimensional.
4. Los grupos de simetría de los cristales (o grupos especiales) están compuestos por un número finito de transformaciones ortogonales, de desplazamientos (traslaciones) discretos y de los productos de estas transformaciones. Rigurosamente hablando, tal simetría es inherente sólo a un cristal infinito o bien a un modelo de cristal con las denominadas *condiciones de contorno cíclicas*.
5. Grupo de Lorentz L^+ está formado por las transformaciones que describen el paso de un sistema de referencia a otro que se encuentra en movimiento rectilíneo uniforme respecto al primero. El requisito de la invariancia de las ecuaciones de movimiento respecto al grupo de Lorentz es una consecuencia de los postulados de la teoría de relatividad.

La lista mencionada apenas cubre, por supuesto, todos los ejemplos de los grupos que tienen aplicación en física, sin embargo, el interés de esta área se concentra precisamente en estos. Por otro lado la teoría de grupos proporciona la posibilidad de clasificar los estados de un sistema físico a partir de sus propiedades de simetría, sin tener que resolver las propias ecuaciones de movimiento, y es precisamente en esto donde reside la importancia de estos métodos, ya que la obtención de al menos una solución aproximada a estas ecuaciones requiere a menudo de cálculos muy laboriosos, pero haciendo uso de los métodos proporcionados por la teoría de grupos se puede determinar las propiedades de simetría de las soluciones exactas de las ecuaciones de movimiento, obteniendo así información bastante importante sobre el sistema físico examinado.

Química

La simetría molecular, y su articulación matemática a través de la Teoría de Grupos, desempeña un papel fundamental en la descripción y predicción de las propiedades de las moléculas. La Espectroscopía concretamente se combina de forma muy eficaz con la simetría molecular para especificar las reglas de selección e interpretar los espectros moleculares.[10]

Por otro lado en Cristalografía, el espacio se agrupa y los grupos puntuales de simetría describen simetrías moleculares y simetrías cristalinas. Estas simetrías son subyacentes al comportamiento físico y químico de estos sistemas, y la teoría de grupos permite simplificar el análisis en mecánica cuántica de estas propiedades. Por ejemplo, se usa para mostrar que las transiciones ópticas entre ciertos niveles cuánticos no pueden ocurrir simplemente debido a la simetría de los estados implicados.[9]

No sólo hay grupos útiles para evaluar las implicaciones de las simetrías en moléculas, sino que sorprendentemente también pronostican que las moléculas a veces pueden cambiar la simetría. El efecto Jahn-Teller es una distorsión de una molécula de alta simetría cuando adopta un estado particular de baja simetría a partir de un conjunto de estados base posibles, que se relacionan el uno con el otro por las operaciones de simetría de la molécula. Del mismo modo, la teoría de grupos ayuda a pronosticar los cambios a propiedades físicas que ocurren cuando un material sufre un cambio de estado. Por otro lado los grupos de simetría mencionados, como por ejemplo los grupos de Mathieu, se usan en teoría de códigos, que se aplica en la corrección de errores en los datos transmitidos, y a los reproductores de CDs.

Probabilidad

Particularmente una de las aplicaciones más importantes de la Teoría de Representaciones de Grupos es en Probabilidad y la Estadística. Esta aplicación se hace vía el estudio de las probabilidades sobre grupos, las cuales a su vez son fundamentales para obtener algunos resultados en otros campos.

Otra aplicación importante, son los paseos aleatorios, que no es más que realizar una formalización matemática de la trayectoria que resulta de hacer sucesivos pasos aleatorios. Por ejemplo, la ruta trazada por una molécula mientras viaja por un líquido o un gas, el camino que sigue un animal en su búsqueda de comida, el precio de una acción fluctuante y la situación financiera de un jugador pueden tratarse como un paseo aleatorio. El término

paseo aleatorio fue introducido por Karl Pearson en 1905. Los resultados de los análisis de los paseos aleatorios, han sido aplicados a muchos campos como la computación, la física, la química, la ecología, la biología, la psicología o la economía. En particular en este último campo la teoría del paseo aleatorio de Burton G. Malkiel en su obra *A Random Walk Down Wall Street* (cuya traducción en español es *Un Paseo Aleatorio Por Wall Street*) se fundamenta en la hipótesis de los mercados eficientes, desarrollado en tres formas o hipótesis. En física, el modelo ha servido, por ejemplo, para modelar el camino seguido por una molécula que viaja a través de un líquido o un gas (movimiento browniano). En ecología, se emplea para modelar los movimientos de un animal de pastoreo, entre otros. A menudo, los paseos aleatorios se suponen que son cadenas de Márkov o procesos de Márkov, pero otros paseos más complicados también son de interés. Algunos paseos aleatorios están en grafos, otros en la recta, en el plano, o en dimensiones mayores, mientras algunos paseos aleatorios están en grupos.

Entre otras aplicaciones de los paseos aleatorios tenemos:

1. En genética de poblaciones, el paseo aleatorio describe las propiedades estadísticas de la deriva genética.

2. En física, los paseso aleatorios son utilizados como modelos simplificados del movimiento *browniano* y difusión tales como el movimiento aleatorio de las moléculas en líquidos y gases. Véase, por ejemplo, la agregación limitada por difusión. Además, los paseos aleatorios y algunos de los paseos que interactúan consigo mismos juegan un papel en la teoría cuántica de campos.

3. En biología matemática, los paseos aleatorios son utilizados para describir los movimientos individuales de los animales, para apoyar empíricamente los procesos de biodifusión, y en ocasiones para desarrollar la dinámica de poblaciones.

4. En otros campos de las matemáticas, el paseo aleatorio se utiliza para calcular las soluciones de la ecuación de Laplace, para estimar la media armónica, y para varias construcciones en el análisis y la combinatoria.

5. En informática, los paseos aleatorios son utilizados para estimar el tamaño de la Web. En la World Wide Web conference-2006, Bar-Yossef Et Al. publicó sus descubrimientos y algoritmos para lo mismo.

6. En el procesamiento de imágenes, los paseos aleatorios son utilizados para determinar las etiquetas (es decir, "objeto.º "fondo") para asociarlas con cada píxel. Este algoritmo se suele denominar como algoritmo de segmentación del paseo aleatorio.

Es un hecho que el estudio de los paseos aleatorios es muy importante y es por ello que a través del tiempo se le ha dedicado particular interés a su estudió y desarrollo, y una forma muy viable de hacerlo es por medio de las representaciones de grupos.

Objetivos

Objetivo General

1. Desarrollar la Teoría de Representaciones de Grupos Finitos y establecer las bases matemáticas para su aplicación en la Probabilidad.

Objetivos Específicos

1. Desarrollar la Teoría de Caracteres y las relaciones de ortogonalidad.

2. Dar a conocer el vínculo entre la Probabilidad y la Teoría de Representaciones de Grupos Finitos.

3. Aplicar la Teoría de Representaciones de Grupos Finitos al estudio de los barajados de cartas.

4. Crear una brecha para que la Teoría de Representaciones de Grupos Finitos sirva como herramienta de estudio en las otras carreras de la Escuela de Matemática de la Universidad de El Salvador.

Definiciones básicas y notación

Sean V y W espacios vectoriales, para los cuales se tienen las siguientes definiciones

- $M_{mn}(\mathbb{C}) = \{m \times n$ matrices con entradas en $\mathbb{C}\}$.
- $M_n(\mathbb{C}) = M_{nn}(\mathbb{C})$.
- $\mathrm{Hom}(V, W) = \{A\colon V \longrightarrow W \mid A$ es un mapeo lineal$\}$.
- $\mathrm{End}(V) = \mathrm{Hom}(V, V)$ (el endomorfismo de anillos de V).
- $GL(V) = \{A \in \mathrm{End}(V) \mid A$ es invertible$\}$ (se conoce como el grupo general lineal de V).
- $GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid A$ es invertible$\}$.
- La matriz identidad/transformación lineal está denotada por Id, o Id_n si se desea hacer énfasis en la dimensión n.
- $\mathbb{Z}$ es el anillo de los números enteros.
- $\mathbb{N}$ es el conjunto de los números enteros no negativos (también conocidos como números naturales).
- $\mathbb{Q}$ es el campo de los números racionales.
- $\mathbb{R}$ es el campo de los números reales.
- $\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$ es el anillo de los enteros módulo n.
- S_n es el grupo de permutaciones de $\{1, \ldots, n\}$, es decir, el *grupo simétrico*.

Capítulo 1

Representaciones de Grupos

Se observará en este capítulo, que el objetivo de las representaciones de grupos es estudiar a los grupos por medio de sus acciones sobre los espacios vectoriales, ya que, a través de sus acciones sobre estos podemos obtener información más detallada acerca de ellos, de esta forma, el estudio de sus matrices de representación conducirá naturalmente al análisis de Fourier y al estudio de las funciones de valores complejos en un grupo.

1.1. Definiciones básicas

Se debe recordar que una *acción* de un grupo G sobre un conjunto A es por definición un homomorfismo $\varphi\colon G \to S_A$, donde S_A es el grupo simétrico sobre A.

Definición 1.1.1. Representación.

Una representación de un grupo G es un homomorfismo $\varphi\colon G \to GL(V)$ para algún espacio vectorial V (de dimensión finita). La dimensión de V es llamada el *grado de* φ. Usualmente escribimos φ_g para $\varphi(g)$ y $\varphi_g(v)$, o simplemente $\varphi_g v$, para la actuación de φ_g sobre $v \in V$.

Observación 1.1.2. *Se asumirá de aquí en adelante que todas las representaciones son no nulas, ya que las representaciones de grado cero formalmente no están contempladas en la definición.*

Uno de los ejemplos clásicos es el siguiente homomorfismo:

Ejemplo 1.1.3. ***La Representación Trivial***

La representación trivial de un grupo G es el homomorfismo $\varphi\colon G \to \mathbb{C}^*$ cuya regla de asignación esta dada por $\varphi(g) = 1\ \forall g \in G$.

Desarrollo. Comprobemos que efectivamente se trata de un homomorfismo $\varphi(g)\varphi(h) = (1)(1) = 1\varphi(gh)\ \forall g, h \in G$. □

Observación 1.1.4. *La Representación Trivial puede asociarse con los complejos sin el cero* $(\mathbb{C}^*)$*, ya que por definición se hace el mapeo hacia un grupo general lineal para un espacio* V *definido como* $GL(V) = \{A \in (V) \mid A \text{ es invertible}\}$*, quiere decir que todos los elementos que pertenezcan a* $GL(V)$ *deberán ser invertibles y de grado* 1.

A continuación otros ejemplos de representaciones, que de la misma forma que el anterior tienen grado 1.

Ejemplo 1.1.5. Sea $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^*$ con regla de asignación $\varphi([m]) = (-1)^m$, entonces φ es una representación.

Desarrollo. Se probará que es un homomorfismo; sean $[m]$ y $[n]$ dos elementos de $\mathbb{Z}/2\mathbb{Z}$

$$\begin{aligned}\varphi([m]+[n]) &= \varphi([m+n])\\ &= (-1)^{m+n}\\ &= (-1)^m(-1)^n\\ &= \varphi([m])\varphi([n])\end{aligned}$$

□

Ejemplo 1.1.6. Sea $\varphi\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{C}^*$ cuya definición esta dada por $\varphi([m]) = i^m$, es una representación.

Desarrollo. Se probará que es un homomorfismo, para ello se tomaran dos elementos tales que $[m]$ y $[n] \in \mathbb{Z}/4\mathbb{Z}$, entonces

$$\begin{aligned}\varphi([m]+[n]) &= \varphi([m+n])\\ &= i^{m+n}\\ &= i^m i^n\\ &= \varphi([m])\varphi([n])\end{aligned}$$

□

Ejemplo 1.1.7. Dada $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ cuya regla de asignación es $\varphi([m]) = e^{\frac{2\pi i m}{n}}$, es una representación.

Desarrollo. Se probará que es un homomorfismo, para ello se tomaran dos elementos de $\mathbb{Z}/n\mathbb{Z}$, sean $[m]$ y $[p]$, entonces

$$\begin{aligned}\varphi([m]+[p]) &= \varphi([m+p])\\ &= e^{\frac{2\pi i(m+p)}{n}}\\ &= e^{\frac{2\pi i m}{n}} e^{\frac{2\pi i p}{n}}\\ &= \varphi([m])\varphi([p])\end{aligned}$$

□

Sea $\varphi\colon G \to GL(V)$ una representación de grado n, a una base B del espacio V puede asociarsele el isomorfismo de espacios vectoriales $T\colon V \to \mathbb{C}^n$, es decir, se puede proporcionar un isomorfismo entre la base y un espacio vectorial solo tomando las coordenadas, de esa forma se pude definir una representación $\psi\colon G \to GL_n(\mathbb{C})$ haciendo $\psi_g = T\varphi_g T^{-1}$ para $g \in G$. Para garantizar que se trata de una representación debe comprobarse que es un homomorfismo, entonces se tiene

$$\begin{aligned}
\psi_{gm} &= T\varphi_{gm}T^{-1} \\
&= T\varphi_g\varphi_m T^{-1} \\
&= T\varphi_g \left(T^{-1}T\right)\varphi_m T^{-1} \\
&= (T\varphi_g T^{-1})(T\varphi_m T^{-1}) \\
&= \psi_g\psi_m
\end{aligned}$$

Si B' es otra base, se tendría otro isomorfismo $S\colon V \to \mathbb{C}^n$ y por tanto, una representación $\psi'\colon G \to GL_n(\mathbb{C})$ dada por $\psi'_g = S\varphi_g S^{-1}$ para $g \in G\ \forall g \in G$. Como cabría suponer las representaciones ψ y ψ' estarán relacionadas de la siguiente manera

$$\psi'_g = ST^{-1}\psi_g TS^{-1} = (ST^{-1})\psi_g(ST^{-1})^{-1}$$

Podría pensarse que las representaciones φ, ψ y ψ' son todas la misma representación, y esta inquietud es la que da la noción de equivalencia planteada en la Definición 1.1.8 y nótese que esta idea está asociada al cambio de base.

Definición 1.1.8. Equivalencia.

Dos representaciones $\varphi\colon G \to GL(V)$ y $\psi\colon G \to GL(W)$ son *equivalentes* si existe un isomorfismo $T\colon V \to W$ tal que $\psi_g = T\varphi_g T^{-1}\ \forall g \in G$, es decir, $\psi_g T = T\varphi_g\ \forall g \in G$. En este caso, se escribirá $\varphi \sim \psi$. A partir de lo anterior puede formarse el siguiente diagrama que conmuta

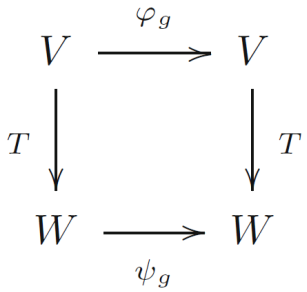

Figura 1.1: Equivalencia de Representaciones

Lo que significa que cualquiera de las dos formas de ver el diagrama (pasar de la parte superior izquierda a la esquina inferior derecha) dará la misma respuesta.

Ejemplo 1.1.9. Se define $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to GL_2(\mathbb{C})$ por medio de

$$\varphi_{[m]} = \begin{bmatrix} \cos\left(\dfrac{2\pi m}{n}\right) & -\sin\left(\dfrac{2\pi m}{n}\right) \\ \\ \sin\left(\dfrac{2\pi m}{n}\right) & \cos\left(\dfrac{2\pi m}{n}\right) \end{bmatrix}$$

que es la matriz de rotación de $\dfrac{2\pi m}{n}$ grados y se define a $\psi\colon \mathbb{Z}/n\mathbb{Z} \to GL_2(\mathbb{C})$ por

$$\psi_{[m]} = \begin{bmatrix} e^{\frac{2\pi m i}{n}} & 0 \\ \\ 0 & e^{-\frac{2\pi m i}{n}} \end{bmatrix}$$

Entonces $\varphi \sim \psi$

Desarrollo. Nótese que φ y ψ, no son más que las representaciones matriciales de las transformaciones lineales.

Sea la matriz $T = \begin{bmatrix} i & -i \\ 1 & 1 \end{bmatrix}$ y se utilizará la matriz inversa para una matriz de 2×2: $A^{-1} = \dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, entonces la matriz inversa de T es: $T^{-1} = \dfrac{1}{2i}\begin{bmatrix} 1 & i \\ -1 & i \end{bmatrix}$.

Mediante un cálculo directo, se comprobará que $T^{-1}\varphi_{[m]}T = \psi_{[m]}$, para demostrar que efectivamente $\varphi \sim \psi$.

$$T^{-1}\varphi_{[m]}T = \tfrac{1}{2i}\begin{bmatrix} 1 & i \\ -1 & i \end{bmatrix} \begin{bmatrix} \cos\left(\dfrac{2\pi m}{n}\right) & -\sin\left(\dfrac{2\pi m}{n}\right) \\ \\ \sin\left(\dfrac{2\pi m}{n}\right) & \cos\left(\dfrac{2\pi m}{n}\right) \end{bmatrix} \begin{bmatrix} i & -i \\ 1 & 1 \end{bmatrix}$$

Se hace primero el producto $T^{-1}\varphi_{[m]}$, para ello se define $\alpha = \dfrac{2\pi m}{n}$

$$T^{-1}\varphi_{[m]} = \begin{bmatrix} 1 & i \\ -1 & i \end{bmatrix} \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} = \begin{bmatrix} \cos(\alpha) + i\sin(\alpha) & -\sin(\alpha) + i\cos(\alpha) \\ \\ -\cos(\alpha) + i\sin(\alpha) & \sin(\alpha) + i\cos(\alpha) \end{bmatrix}$$

Recuérdese que

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)$$
$$e^{-i\theta} = \cos(\theta) - i\sin(\theta)$$

por lo que, se hacen los siguientes cálculos

$$\begin{array}{rcl|rcl} -\sin(\alpha)+i\cos(\alpha) &=& i\cos(\alpha)+i^2\sin(\alpha) & \sin(\alpha)+i\cos(\alpha) &=& i\left[\cos(\alpha)+\frac{1}{i}\sin(\alpha)\right] \\ &=& i[\cos(\alpha)+i\sin(\alpha)] & &=& i[\cos(\alpha)-i\sin(\alpha)] \\ &=& ie^{i\alpha} & &=& ie^{-i\alpha} \end{array}$$

Operando adecuadamente se tiene que $T^{-1}\varphi_{[m]} = \begin{bmatrix} e^{i\alpha} & ie^{i\alpha} \\ -e^{-i\alpha} & ie^{-i\alpha} \end{bmatrix}$

Sustituyendo la matriz anterior y cambiando el valor de α se tiene que

$$T^{-1}\varphi_{[m]}T = \frac{1}{2i}\begin{bmatrix} e^{\frac{2\pi mi}{n}} & ie^{\frac{2\pi mi}{n}} \\ -e^{-\frac{2\pi mi}{n}} & ie^{-\frac{2\pi mi}{n}} \end{bmatrix}\begin{bmatrix} i & -i \\ 1 & 1 \end{bmatrix}$$

Sea $T^{-1}\varphi_{[m]} = M$ y se lleva a cabo el producto de MT

$$MT = \begin{bmatrix} e^{i\alpha} & ie^{i\alpha} \\ -e^{-i\alpha} & ie^{-i\alpha} \end{bmatrix}\begin{bmatrix} i & -i \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} ie^{i\alpha}+ie^{i\alpha} & -ie^{i\alpha}+ie^{-i\alpha} \\ -ie^{-i\alpha}+ie^{-i\alpha} & ie^{-i\alpha}+ie^{-i\alpha} \end{bmatrix} = \begin{bmatrix} 2ie^{i\alpha} & 0 \\ 0 & 2ie^{-i\alpha} \end{bmatrix}$$

Se reemplaza el resultado anterior, se retoman los valores originales y se tiene:

$$T^{-1}\varphi_{[m]}T = \frac{1}{2i}\begin{bmatrix} 2ie^{\frac{2\pi mi}{n}} & 0 \\ 0 & 2ie^{-\frac{2\pi mi}{n}} \end{bmatrix} = \begin{bmatrix} e^{\frac{2\pi mi}{n}} & 0 \\ 0 & e^{-\frac{2\pi mi}{n}} \end{bmatrix} = \psi_{[m]}$$

□

Un grupo puede tener solo una representación o más de una, depende del grupo con el que se trabaje.

Existen representaciones que se tornan importantes por el uso que se les da en diversas áreas y por el grupo mismo, una de estas es la del Grupo Simétrico S_n, que se utiliza en la Teoría de Galois, la Teoría de Representaciones de los Grupos de Lie, entre otras. De hecho el Teorema de Cayley establece que cada grupo G es isomorfo a un subgrupo del Grupo Simétrico. Por la importancia de este grupo es que la siguiente representación es muy valiosa en este tópico.

Ejemplo 1.1.10. ***La Representación Estándar de*** S_n

Se define a $\varphi\colon S_n \to GL_n(\mathbb{C})$ sobre la base estándar $\varphi_\sigma(e_i) = e_{\sigma(i)}$. Se obtiene la matriz para φ_σ permutando las filas de la matriz identidad correspondiente a σ.

Así por ejemplo si $n = 3$ se tienen los elementos generadores (1 2) y (1 2 3), y puede calcularse sus respectivas representaciones.

Desarrollo. Para (1 2)

$$(12) = \begin{matrix} x_1 & x_2 & x_3 \end{matrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{entonces} \quad \begin{matrix} x_1' = 0x_1 + 1x_2 + 0x_3 \Longrightarrow [0\ 1\ 0] \\ x_2' = 1x_1 + 0x_2 + 0x_3 \Longrightarrow [1\ 0\ 0] \\ x_3' = 0x_1 + 0x_2 + 1x_3 \Longrightarrow [0\ 0\ 1] \end{matrix} \Longrightarrow \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Para (1 2 3)

$$(123) = \begin{matrix} x_1 & x_2 & x_3 \end{matrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{entonces} \quad \begin{matrix} x_1' = 0x_1 + 1x_2 + 0x_3 \Longrightarrow [0\ 1\ 0] \\ x_2' = 0x_1 + 0x_2 + 1x_3 \Longrightarrow [0\ 0\ 1] \\ x_3' = 1x_1 + 0x_2 + 0x_3 \Longrightarrow [1\ 0\ 0] \end{matrix} \Longrightarrow \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

De aquí que las matrices de representación para los elementos (1 2) y (1 2 3) están dadas por

$$\varphi_{(1\ 2)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad , \quad \varphi_{(1\ 2\ 3)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

□

Observación 1.1.11. *Se debe recordar que* $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$ *y por definición* $\varphi_\sigma(e_1 + e_2 + \ldots + e_{n-1} + e_n) = e_{\sigma(1)} + e_{\sigma(2)} + \ldots + e_{\sigma(n-1)} + e_{\sigma(n)}$*, es decir, al aplicar* $\sigma(i) = j$ *(donde* i *no es necesariamente igual a* j*), con* $i, j = 1, 2, \ldots, n$ *generamos a los elementos* $1, 2, 3, \ldots, n$ *(no necesariamente en ese orden). Si se observa de forma vectorial, se tiene que por cada elemento* i *que se obtenga de aplicar* σ*, su representación matricial tendrá la forma* $[\ldots 0\ 0\ \ldots\ 1\ 0 \ldots]$*, es entonces evidente que lo que se esta generando es la base canónica* e_i *y como la adición es conmutativa quedaría como*

$$e_{\sigma(1)} + e_{\sigma(2)} + \ldots + e_{\sigma(n-1)} + e_{\sigma(n)} = e_1 + e_2 + \ldots + e_{n-1} + e_n.$$

Nótese que en el Ejemplo 1.1.10 lo que se tiene es que

$$\begin{aligned} \varphi_\sigma(e_1 + e_2 + \ldots + e_{n-1} + e_n) &= e_{\sigma(1)} + e_{\sigma(2)} + \ldots + e_{\sigma(n-1)} + e_{\sigma(n)} \\ &= e_1 + e_2 + \ldots + e_{n-1} + e_n \end{aligned}$$

y la igualdad se cumple ya que σ *es una permutación y la adición es conmutativa. Por tanto,* $\mathbb{C}(e_1 + e_2 + \ldots + e_{n-1} + e_n)$ *es invariante para toda* φ_σ *con* $\sigma \in S_n$*.*

Esta observación permite establecer la siguiente definición.

Definición 1.1.12. Subespacios G-invariantes.

Sea $\varphi\colon G \to GL(V)$ una representación. Un subespacio $W \leq V$ es *G-invariante* si, $\forall g \in G$ y $w \in W$, se obtiene que $\varphi_g w \in W$.

Ejemplo 1.1.13. Para la representación ψ del *Ejemplo 1.1.9* los subespacios $\mathbb{C}e_1$ y $\mathbb{C}e_2$ se afirma que son ambos $\mathbb{Z}/n\mathbb{Z}$-invariantes y $\mathbb{C}^2 = \mathbb{C}e_1 \oplus \mathbb{C}e_2$.

Desarrollo. Se probará entonces que $\mathbb{C}e_1$ y $\mathbb{C}e_2$ son ambos subespacios $\mathbb{Z}/n\mathbb{Z}$-invariantes de $\mathbb{Z}/n\mathbb{Z}$, para ello, deben considerarse algunos presaberes, para hacer más fácil la comprensión de dicha demostración.

1. En el espacio vectorial complejo $\mathbb{C}^2$ todo vector (x, y) es combinación lineal de los vectores $(1, 0)$ y $(0, 1)$, ya que $(x, y) = x(1, 0) + y(0, 1)$ con $x, y \in \mathbb{C}$, de aquí que $\{(1, 0), (0, 1)\}$ es base.

2. Para un cuerpo $\mathbb{K}$ y V un espacio vectorial de $\mathbb{K}$ se tiene que $V \leq W$ (un subespacio) si:

   - para cualquier $w, w' \in W \Longrightarrow w + w' \in W$
   - para cada $w \in W$ y cada $\lambda \in \mathbb{K} \Longrightarrow \lambda w \in W$

3. En general en el espacio vectorial $\mathbb{K}^n$ los n vectores

   $$\{e_1 = (1, 0, \ldots, 0, 0); e_2 = (0, 1, \ldots, 0, 0); \ldots; e_i = (0, \ldots, 1, \ldots, 0); \ldots; e_n = (0, 0, \ldots, 0, 1)\}$$

   forman la base estándar de $\mathbb{K}^n$ en donde cada e_i son linealmente independiente (Li) y son una base que genera a $\mathbb{K}^n$.

Entonces, se tiene que $\psi\colon Z/nZ \to GL_2(\mathbb{C})$

$$\psi_{[m]} = \begin{bmatrix} e^{\frac{2\pi mi}{n}} & 0 \\ \\ 0 & e^{-\frac{2\pi mi}{n}} \end{bmatrix}$$

Para que, $\mathbb{C}e_1$ y $\mathbb{C}e_2$ sean $\mathbb{Z}/n\mathbb{Z}$-invariantes debería de pasar que si $W \leq \mathbb{C}$ se debe demostrar que $\forall g \in \mathbb{Z}/n\mathbb{Z}$ con $\psi_g(w) \in W$.

Ahora las veces de W las hacen

$$\mathbb{C}e_1 = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; ; a \in \mathbb{C} \right\} \quad \text{y} \quad \mathbb{C}e_2 = \left\{ \begin{pmatrix} 0 \\ b \end{pmatrix} = b \begin{pmatrix} 0 \\ 1 \end{pmatrix} \; ; b \in \mathbb{C} \right\}$$

y se busca que $\mathbb{C}e_1, \mathbb{C}e_2 \leq \mathbb{C}$, se toma $v \in \mathbb{C}e_1$ y $w \in \mathbb{C}e_2$.

Para $\mathbb{C}e_1 \leq \mathbb{C}$

$$\psi_{[m]}(v) = \begin{pmatrix} e^{\frac{2\pi mi}{n}} & 0 \\ \\ 0 & e^{-\frac{2\pi mi}{n}} \end{pmatrix} \begin{pmatrix} a \\ \\ 0 \end{pmatrix} = \begin{pmatrix} ae^{\frac{2\pi mi}{n}} \\ \\ 0 \end{pmatrix} = ae^{\frac{2\pi mi}{n}} \begin{pmatrix} 1 \\ \\ 0 \end{pmatrix} = x \begin{pmatrix} 1 \\ \\ 0 \end{pmatrix}$$

con $x = ae^{\frac{2\pi mi}{n}}$ y $x \in \mathbb{C} \Longrightarrow \psi_{[m]}(v) \in \mathbb{C}e_1$; por lo tanto $\mathbb{C}e_1$ es $\mathbb{Z}/n\mathbb{Z}$-Invariante

Para $\mathbb{C}e_2 \leq \mathbb{C}$

$$\psi_{[m]}(w) = \begin{pmatrix} e^{\frac{2\pi mi}{n}} & 0 \\ 0 & e^{-\frac{2\pi mi}{n}} \end{pmatrix} \begin{pmatrix} 0 \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ be^{-\frac{2\pi mi}{n}} \end{pmatrix} = be^{-\frac{2\pi mi}{n}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = y \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

con $y = be^{-\frac{2\pi mi}{n}}$ e $y \in \mathbb{C} \Longrightarrow \psi_{[m]}(w) \in \mathbb{C}e_2$; por lo tanto, $\mathbb{C}e_2$ es $\mathbb{Z}/n\mathbb{Z}$-Invariante

Además, $\mathbb{C}e_1 \cap \mathbb{C}e_2 = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, es decir, el único vector que comparten es el vector nulo. Ahora faltará corroborar que $\mathbb{C}^2 = \mathbb{C}e_1 \oplus \mathbb{C}e_2$ la suma directa se sabe que sus elementos pertenecen a $\mathbb{C} \times \mathbb{C}$.

Así que, si se toma $x \in \mathbb{C}^2 \Rightarrow x = \begin{pmatrix} a \\ b \end{pmatrix}$ con $a, b \in \mathbb{C}$.

También se puede reescribir como $x = \begin{pmatrix} a \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

y nótese que $a\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}e_1$ así como $b\begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}e_2$; de esta forma se cumplirá afirmado anteriormente. □

Definición 1.1.14. Suma directa de representaciones.

Supóngase que las representaciones $\varphi^{(1)} \colon Gó \to GL(V_1)$ y $\varphi^{(2)} \colon G \to GL(V_2)$ están dadas. Entonces su *suma directa* (externa) esta dada por $\varphi^{(1)} \oplus \varphi^{(2)} \colon G \to GL(V_1 \oplus V_2)$ definida por

$$(\varphi^{(1)} \oplus \varphi^{(2)})_g(v_1, v_2) = (\varphi_g^{(1)}(v_1), \varphi_g^{(2)}(v_2)).$$

Para ver las sumas directas en términos de matrices, se supondrá que $\varphi^{(1)} \colon G \to GL_m(\mathbb{C})$ y $\varphi^{(2)} \colon G \to GL_n(\mathbb{C})$ son representaciones. Entonces

$$\varphi^{(1)} \oplus \varphi^{(2)} \colon G \to GL_{m+n}(\mathbb{C})$$

será una matriz cuadrada, es decir, por las definiciones matriciales de $\varphi^{(1)}$ y $\varphi^{(2)}$ el conjunto de llegada para la suma directa serán matrices cuadradas de $(m+n) \times (m+n)$ ya que

$$(\varphi^{(1)} \oplus \varphi^{(2)})_g = \underbrace{\begin{bmatrix} [\varphi_g^{(1)}]_{m\times m} & 0_{m\times n} \\ 0_{n\times m} & [\varphi_g^{(2)}]_{n\times n} \end{bmatrix}}_{m+n} \Big\} m+n$$

Nótese que en la matriz anterior los espacios ocupados por 0 son matrices también de dimensión $m \times n$ y $n \times m$ respectivamente, la idea es contemplar a la suma directa como una matriz compuesta por submatrices de las representaciones y matrices nulas.

Ejemplo 1.1.15. Se definen las representaciones $\varphi^{(1)} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ por $\varphi_{[m]}^{(1)} = e^{2\pi im/n}$, y $\varphi^{(2)} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ por $\varphi_{[m]}^{(2)} = e^{-2\pi im/n}$.

Desarrollo. De acuerdo a la definición de suma directa se tiene que

$$(\varphi^{(1)} \oplus \varphi^{(2)})_{[m]} = \begin{bmatrix} e^{\frac{2\pi i m}{n}} & 0 \\ 0 & e^{\frac{-2\pi i m}{n}} \end{bmatrix}.$$

Notemos que en este ejemplo se ha aplicado directamente la definición de suma directa. □

Observación 1.1.16. *Si $n > 1$, entonces la representación*

$$\begin{aligned} \rho\colon G &\to GL_n(\mathbb{C}) \\ g &\mapsto \rho_g = I;\ \forall g \in G \end{aligned}$$

(donde I es la matriz identidad de $n \times n$) no es equivalente a la representación trivial, porque se sabe que la representación trivial esta dada por

$$\begin{aligned} \varphi\colon G &\to \mathbb{C}^* \\ g &\mapsto \varphi(g) = 1;\ \forall g \in G \end{aligned}$$

Mas bien, la matriz identidad termina siendo equivalente a la suma directa de n copias de la representación trivial. Porque es posible observar a cada elemento de la diagonal como una matriz de 1×1 y por la definición de suma directa.

$$\rho = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}_{n\times n} = \begin{bmatrix} [1]_{1\times 1} & 0 & \cdots & 0 & 0 \\ 0 & [1]_{1\times 1} & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & [1]_{1\times 1} & 0 \\ 0 & 0 & \cdots & 0 & [1]_{1\times 1} \end{bmatrix}_{n\times n} = \underbrace{1_g \oplus 1_g \oplus \cdots \oplus 1_g}_{n \text{ veces}}$$

Ya que las representaciones son un tipo especial de homomorfismos, si un grupo G es generado por un conjunto X, entonces una representación φ de G se determina por los valores que toma en X; pero debe tenerse en cuenta que, no cualquier asignación de matrices a los generadores dará una representación válida, porque la asignación debe preservar todas las relaciones que cumplen los generadores.

A continuación se muestra un ejemplo de como se construye la suma directa de representaciones.

Ejemplo 1.1.17. Sea $\rho\colon S_3 \to GL_2(\mathbb{C})$ especificada sobre los generadores (1 2) y (1 2 3) por

$$\rho_{(1\ 2)} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}, \rho_{(1\ 2\ 3)} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

Desarrollo. Es importante asegurar que, se trata de una representación, para ello se debe corroborar que ρ sea un homomorfismo. Además, No se conoce la regla de asignación, pero se conoce las imágenes de los generadores, entonces solo faltaría comprobar que cumplen con las mismas reglas de S_3.

Se comprobará que $s^2 = I$ sabiendo que $s = \rho_{(1\ 2)}$

$$\begin{aligned}\left(\rho_{(1\ 2)}\right)^2 &= \left(\rho_{(1\ 2)}\right)\left(\rho_{(1\ 2)}\right)\\ &= \left(\begin{bmatrix}-1 & -1\\ 0 & 1\end{bmatrix}\right)\left(\begin{bmatrix}-1 & -1\\ 0 & 1\end{bmatrix}\right)\\ &= \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\\ &= I\end{aligned}$$

Ahora se probará para $r^3 = I$ si $r = \rho_{(1\ 2\ 3)}$

$$\begin{aligned}\left(\rho_{(1\ 2\ 3)}\right)^3 &= \left(\rho_{(1\ 2\ 3)}\right)\left(\rho_{(1\ 2\ 3)}\right)\left(\rho_{(1\ 2\ 3)}\right)\\ &= \left(\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\right)\left(\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\right)\left(\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\right)\\ &= \left(\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}\right)\left(\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\right)\\ &= \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\\ &= I\end{aligned}$$

Por último, se verifica que $sr = r^{-1}s$

$$\begin{aligned}\left(\rho_{(1\ 2)}\right)\left(\rho_{(1\ 2\ 3)}\right) &= \left(\rho_{(1\ 2\ 3)}\right)^{-1}\left(\rho_{(1\ 2)}\right)\\ \left(\begin{bmatrix}-1 & -1\\ 0 & 1\end{bmatrix}\right)\left(\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\right) &= \left(\begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\right)^{-1}\left(\begin{bmatrix}-1 & -1\\ 0 & 1\end{bmatrix}\right)\\ \left(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right) &= \left(\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}\right)\left(\begin{bmatrix}-1 & -1\\ 0 & 1\end{bmatrix}\right)\\ \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} &= \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\end{aligned}$$

Como la representación de los elementos conserva las propiedades de los generadores de S_3, se podrá concluir que es un homomorfismo y, por tanto, una representación.

Después de haber verificado que ρ es una representación, se tómese a $\psi\colon S_3 \to \mathbb{C}^*$ definida por $\psi_\sigma = 1$. Véase que $\psi_\sigma = 1 \approx [1]_{1\times 1}$ y por definición de suma directa

$$(\rho \oplus \psi)_{(1\ 2)} = \begin{bmatrix}\rho_{(1\ 2)} & 0_{2\times 1}\\ 0_{1\times 2} & \psi_{(1\ 2)}\end{bmatrix} = \begin{bmatrix}\begin{bmatrix}-1 & -1\\ 0 & 1\end{bmatrix} & 0\\ 0 & 0 & [1]\end{bmatrix} = \begin{bmatrix}-1 & -1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{bmatrix}$$

Se podrá desarrollar el mismo procedimiento para el otro elemento

$$(\rho \oplus \psi)_{(1\ 2\ 3)} = \begin{bmatrix} \rho_{(1\ 2\ 3)} & 0_{2\times 1} \\ 0_{1\times 2} & \psi_{(1\ 2\ 3)} \end{bmatrix} \quad \begin{bmatrix} \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 \end{matrix} & [1] \end{bmatrix} = \begin{bmatrix} -1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Finalmente, se podrá observar que los elementos quedan escritos de la siguiente forma

$$(\rho \oplus \psi)_{(12)} = \begin{bmatrix} -1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, (\rho \oplus \psi)_{(1\ 2\ 3)} = \begin{bmatrix} -1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

□

Se mostrará más adelante que $\rho \oplus \psi$ es equivalente a la representación de S_3 considerada en el Ejemplo 1.1.10, esto se demostrara más adelante.

Sea $\varphi\colon G \to GL(V)$ una representación, si $W \leq V$ es un subespacio G-invariante, podremos restringir φ para obtener una representación $\varphi|_W : G \to GL(W)$ definiendo $(\varphi|_W)_g(\omega) = \varphi_g(\omega)$ para $\omega \in W$. Precisamente porque W es G-Invariante, se tiene $\varphi_g(\omega) \in W$. A veces decimos que $\varphi|_W$ es una *subrepresentación* de φ. Si $V_1, V_2 \leq V$ son G-invariantes y $V = V_1 \oplus V_2$, entonces se verifica que φ es equivalente a la suma directa (externa) $\varphi|_{V_1} \oplus \varphi|_{V_2}$. Para ello veáse esto en términos de matrices.

Sea $\varphi^{(i)} = \varphi|_{V_i}$ y se escogen las bases B_1 y B_2 para V_1 y V_2, respectivamente. Entonces se deduce de la definición de una suma directa que $B = B_1 \cup B_2$ es una base para V. Como V_i es G-invariante, se tiene que $\varphi_g(B_i) \subseteq V_i = \mathbb{C}B_i$ el subespacio generado por B_i) por definición de subespacio invariante. Así se obtiene la matriz

$$[\varphi_g]_B = \begin{bmatrix} [\varphi^{(1)}]_{B_1} & 0 \\ 0 & [\varphi^{(2)}]_{B_2} \end{bmatrix}$$

Que no es más que la matriz de cambio de base B y también que $\varphi \sim \varphi^{(1)} \oplus \varphi^{(2)}$, es decir, un isomorfismo.

A menudo se tiene algún tipo de factorización única en primos, o irreducibles, y en este caso aplica algo similar para la teoría de representación. En este contexto la noción de "irreducible" esta inspirada en la idea de un grupo simple.

Definición 1.1.18. Representación Irreducible.

Una representación no nula $\varphi\colon G \to GL(V)$ de un grupo G se dice que es *irreducible* si y sólo si los únicos subespacios G-invariantes de V son $\{0\}$ y V.

En la Definición 1.1.18 se podrá notar que no tiene subespacios propios que sean G-Invariantes.

Ejemplo 1.1.19. Cualquier representación de grado uno de $\varphi\colon G \to \mathbb{C}^*$ es irreducible, ya que $\mathbb{C}$ no tiene subespacios distintos de cero.

La Tabla 1.1 muestra algunas analogías entre los conceptos que se han visto hasta ahora con los de la Teoría de Grupos y Álgebra Lineal.

Tabla 1.1: Analogías entre grupos, espacios vectoriales, y representaciones

Grupos	Espacio Vectorial	Representación
Subgrupo	Subespacio	Subespacio G-invariante
Grupo Simple	Subespacio Unidimensional	Representación irreducible
Producto directo	Suma directa	Suma directa
Isomorfismo	Isomorfismo	Equivalencia

Si $G = \{1\}$ es el grupo trivial y $\varphi\colon G \to GL(V)$ es una representación, entonces necesariamente $\varphi_1 = I$. Entonces, para producir una representación del grupo trivial, basta con escoger un espacio vectorial. Para el grupo trivial, un subespacio G-invariante no es más que un subespacio. Una representación del grupo trivial es irreducible si y sólo si tiene grado uno. Así la columna central de la **Tabla 1.1** es un caso especial de la tercera columna.

Ejemplo 1.1.20. Las representaciones φ y del Ejemplo 1.1.9 no son irreducibles.

Ya que por ejemplo, $\mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix}$ y $\mathbb{C}\begin{bmatrix} -i \\ 1 \end{bmatrix}$ son subespacios $\mathbb{Z}/n\mathbb{Z}$-invariantes para φ, mientras que los ejes coordenados $\mathbb{C}_{e_1}$ y $\mathbb{C}_{e_2}$ son subespacios invariantes para ψ.

Desarrollo. Véase que φ tiene la siguiente definición

$$\begin{aligned} \varphi\colon \mathbb{Z}/n\mathbb{Z} &\to GL_2(\mathbb{C}) \\ [m] \mapsto \varphi_{[m]} &= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}; \text{ donde } \alpha = \tfrac{2\pi m}{n} \end{aligned}$$

Así como

$$\mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix} = \left\{ a\begin{pmatrix} i \\ 1 \end{pmatrix} = \begin{pmatrix} ai \\ a \end{pmatrix} \; ; \, a \in \mathbb{C} \right\} \text{ y } \mathbb{C}\begin{bmatrix} -i \\ 1 \end{bmatrix} = \left\{ a\begin{pmatrix} -i \\ 1 \end{pmatrix} = \begin{pmatrix} -ai \\ a \end{pmatrix} \; ; \, a \in \mathbb{C} \right\}$$

Hay que probar que son subespacios invariantes, es decir, que si $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to GL_2(\mathbb{C})$ y $\mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix} \leq \mathbb{C}$ es $\mathbb{Z}/n\mathbb{Z}$-Invariante $\forall g \in \mathbb{Z}/n\mathbb{Z}$, entonces $\varphi_g[w] \in \varphi$.

Para ello sea $[m]$ y $u \in \mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix}$ entonces

$$\begin{aligned}
\varphi_{[m]}(u) &= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} ai \\ a \end{bmatrix} \\
&= \begin{bmatrix} ai\cos\alpha - a\sin\alpha \\ ai\sin\alpha + a\cos\alpha \end{bmatrix} \\
&= a\begin{bmatrix} i\cos\alpha - \sin\alpha \\ i\sin\alpha + \cos\alpha \end{bmatrix} \\
&= a\begin{bmatrix} i\cos\alpha + i^2\sin\alpha \\ \cos\alpha + i\sin\alpha \end{bmatrix} \\
&= a\begin{bmatrix} i(\cos\alpha + i\sin\alpha) \\ (\cos\alpha + i\sin\alpha) \end{bmatrix} \\
&= a(\cos\alpha + i\sin\alpha)\begin{bmatrix} i \\ 1 \end{bmatrix} \in \mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix}\text{; ya que } a(\cos\alpha + i\sin\alpha) \in \mathbb{C}
\end{aligned}$$

Ahora para el mismo elemento $[m]$ y $v \in \mathbb{C}\begin{bmatrix} -i \\ 1 \end{bmatrix}$ se tiene

$$\begin{aligned}
\varphi_{[m]}(v) &= \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} -ai \\ a \end{bmatrix} \\
&= \begin{bmatrix} -ai\cos\alpha - a\sin\alpha \\ -ai\sin\alpha + a\cos\alpha \end{bmatrix} \\
&= a\begin{bmatrix} -i\cos\alpha + i^2\sin\alpha \\ \cos\alpha - i\sin\alpha \end{bmatrix} \\
&= a\begin{bmatrix} -i(\cos\alpha - i\sin\alpha) \\ (\cos\alpha - i\sin\alpha) \end{bmatrix} \\
&= a(\cos\alpha - i\sin\alpha)\begin{bmatrix} -i \\ 1 \end{bmatrix} \in \mathbb{C}\begin{bmatrix} -i \\ 1 \end{bmatrix}\text{; ya que } a(\cos\alpha + i\sin\alpha) \in \mathbb{C}
\end{aligned}$$

Por tanto, $\mathbb{C}\begin{bmatrix} i \\ 1 \end{bmatrix}$ y $\mathbb{C}\begin{bmatrix} -i \\ 1 \end{bmatrix}$ ambos son $\mathbb{Z}/n\mathbb{Z}$-Invariantes para φ.

Por otro lado, ψ se define como

$$\begin{aligned}
\psi\colon \mathbb{Z}/n\mathbb{Z} &\to GL_2(\mathbb{C}) \\
[m] &\mapsto \psi_{[m]} = \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix}\text{; donde } \alpha = \tfrac{2\pi m}{n}
\end{aligned}$$

Así como los ejes coordenados

$$\mathbb{C}_{e_1} = \left\{ a\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix} \ ;\ a \in \mathbb{C} \right\} \text{ y } \mathbb{C}_{e_2} = \left\{ a\begin{pmatrix} 0 \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ a \end{pmatrix} \ ;\ a \in \mathbb{C} \right\}$$

entonces se podrá comprobar que los ejes coordenados son subespacios invariantes para ψ.

Sea $\psi_{[m]}$ y $u \in \mathbb{C}_{e_1}$ entonces

$$\begin{aligned}\varphi_{[m]}(u) &= \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} a \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} ae^{i\alpha} \\ 0 \end{bmatrix} \\ &= ae^{i\alpha} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{; ya que } ae^{i\alpha} \in \mathbb{C}, \text{ por tanto } \psi_{[m]}(u) \in \mathbb{C}_{e_1}\end{aligned}$$

Ahora para $\psi_{[m]}$ se toma $v \in \mathbb{C}_{e_2}$ entonces

$$\begin{aligned}\varphi_{[m]}(v) &= \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} 0 \\ a \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ ae^{-i\alpha} \end{bmatrix} \\ &= ae^{-i\alpha} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{; ya que } ae^{-i\alpha} \in \mathbb{C}, \text{ por tanto } \psi_{[m]}(v) \in \mathbb{C}_{e_2}\end{aligned}$$

Con lo expuesto anteriormente, se puede aegurar, que los ejes coordenados son subespacios $\mathbb{Z}n/\mathbb{Z}$-Invariantes; en conclusión tanto como φ y ψ no son irreducibles, ya que poseen más subespacios invariantes distintos a él mismo y a $\{0\}$. □

Después de las representaciones unidimensionales, la siguiente clase para analizar consta de las representaciones bidimensionales.

Ejemplo 1.1.21. La representación $\rho\colon S_3 \to GL_2(\mathbb{C})$ del Ejemplo 1.1.17 es irreducible.

Desarrollo. Por contradicción decimos que la representación ρ no es irreducible, es decir, tiene más subespacios invariantes además del $\{0\}$ y el mismo espacio, por otro lado $GL_2(\mathbb{C}) = GL(\mathbb{C}^2)$ (por la definición de grupo general lineal), entonces la $\dim\mathbb{C}^2 = 2$ por ello cualquier subespacio propio W no nulo que sea S_3-invariante será unidimensional. ¿Cómo seria este vector?

Sea v un vector no nulo de W y $W = \mathbb{C}v$ (un escalar por un vector) y sea $\sigma \in S_3$, entonces $\rho_\sigma(v) = \lambda v$, en donde $v \in \mathbb{C}v$ y este tiene dimensión 1, para algún $\lambda \in \mathbb{C}$, ya que por la S_3-invarianza de W se tiene que $\rho_\sigma(v) \in W = \mathbb{C}v$. De ello se deduce que, v debe ser un vector propio para todos los ρ_σ con $\sigma \in S_3$, ya que un vector propio cumple con $f(u) = \lambda u$; $\lambda \in \mathbb{C}$.

Lo que se ha encontrado es que hay un vector propio para todas ρ_σ con $\sigma \in S_3$, es decir, un vector común; tomemos dos elementos de S_3, tales como $\rho_{(1\ 2)}$ y $\rho_{(1\ 2\ 3)}$ y veamos si en efecto ambos poseen dicho vector en común.

Encontremos sus valores propios, haciendo uso de $|A - \lambda I| = 0$, donde A será la matriz asociada a cada elemento, I la matriz identidad y λ los valores propios a encontrar.

$$\begin{aligned}
|A - \lambda I| &= 0 \\
|\rho(1\ 2) - \lambda I| &= 0 \\
\left|\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right| &= 0 \\
\left|\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right| &= 0 \\
\left|\begin{pmatrix} -1-\lambda & -1 \\ 0 & 1-\lambda \end{pmatrix}\right| &= 0 \\
(1-\lambda)(-1-\lambda) &= 0 \\
\Leftrightarrow (1-\lambda) = 0 \text{ o } (-1-\lambda) &= 0 \\
\text{por tanto } \lambda = 1 \text{ o } \lambda &= -1
\end{aligned}$$

Ahora se deberá encontrar uno de lo vectores propios asociado a uno de los valores propios encontrados ($\lambda_1 = -1$ o $\lambda_2 = 1$), es decir, se deberá encontrar $\rho_{(1\ 2)}(v) = \lambda v$.

Para $\lambda_1 = -1$ se tiene:

$$\begin{aligned}
\rho_{(1\ 2)}(v) &= \lambda_1 v \\
\begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} &= -1 \begin{bmatrix} a \\ b \end{bmatrix} \\
\begin{bmatrix} -a-b \\ b \end{bmatrix} &= \begin{bmatrix} -a \\ -b \end{bmatrix} \text{ de aquí que } -a-b = -a \text{ y } b = -b \\
&\Longrightarrow b = 0 \text{ y } a = a
\end{aligned}$$

por lo tanto, el vector queda como $V_{\lambda_1} = \begin{bmatrix} a \\ 0 \end{bmatrix} = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \mathbb{C}e_1$

Para $\lambda_2 = 1$ se tiene:

$$\begin{aligned}
\rho_{(1\ 2)}(v) &= \lambda_2 v \\
\begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} &= 1 \begin{bmatrix} a \\ b \end{bmatrix} \\
\begin{bmatrix} -a-b \\ b \end{bmatrix} &= \begin{bmatrix} a \\ b \end{bmatrix} \text{ de aquí que } -a-b = a \text{ y } b = b \\
&\Longrightarrow b = -2a \text{ y } a = -\frac{b}{2}
\end{aligned}$$

por lo tanto, el vector queda como $V_{\lambda_2} = \begin{bmatrix} -\frac{b}{2} \\ b \end{bmatrix} = -\frac{1}{2} b \begin{bmatrix} -1 \\ 2 \end{bmatrix} = \mathbb{C} \begin{bmatrix} -1 \\ 2 \end{bmatrix}$

Una vez encontrados estos vectores propios por lo asumido anteriormente deberían ser vectores comunes a $\rho_{(1\ 2\ 3)}$, pero con un cálculo rápido queda demostrado que no es así, pues debería cumplirse que $\rho_{(1\ 2\ 3)}(v) = \lambda_1 v$ y que $\rho_{(1\ 2\ 3)}(v) = \lambda_2 v$, donde $v \in \{V_{\lambda_1}, V_{\lambda_2}\}$.

Para $v = V_{\lambda_1}$ se encontrara que e_1 no es un vector propio:

$$\rho_{(1\ 2\ 3)}(e_1) = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \end{bmatrix} = -1 \begin{bmatrix} 1 \\ -1 \end{bmatrix} \notin \mathbb{C}e_1$$

Así como para $v = V_{\lambda_2}$ tampoco lo es $w = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$ pues:

$$\rho_{(1\ 2\ 3)}(w) = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -1 \\ 2 \end{bmatrix} = \begin{bmatrix} -1 \\ -1 \end{bmatrix} \notin \mathbb{C} \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

Con este contra ejemplo se ha demostrado que $\rho_{(1\ 2)}$ y $\rho_{(1\ 2\ 3)}$ no tienen vectores propios en común, es decir que, si esto pasa entonces no puede existir dicho W. Y esto es una contradicción que parte de haber asumido que la representación no era irreducible y que poseía mas subespacios invariantes, además de los triviales. □

La idea que subyace en este ejemplo, se resume en la siguiente proposición.

Proposición 1.1.22. *Si $\varphi\colon G \to GL(V)$ es una representación de grado 2, es decir, $\dim V = 2$, entonces φ es irreducible si y solo si no existe un vector propio común v para toda φ_g con $g \in G$.*

Demostración. "$\Longrightarrow$"

φ es irreducible si no existe un vector propio común v para toda φ_g con $g \in G$.

Se abordara esta prueba por contradicción, supóngase que las representaciones φ_g poseen un vector propio $v \in V$ en común. Entonces $v \neq 0$ y por tanto $W = \mathbb{C}v$ es un subespacio unidimensional de V, además como es una representación de grado 2 entonces $W \neq V$. Para $g \in G$ se tiene que $\varphi_g(v) = \lambda v$ para algún $\lambda \in \mathbb{C}$, pues se ha asumido que v es un vector propio para toda φ_g con $g \in G$.

Entonces si hacemos $\varphi_g(W) = \varphi_g(\mathbb{C}v) = \mathbb{C}\varphi_g(v) = \lambda\mathbb{C}v \in W$, es decir, hemos encontrado que W es un subespacio G-invariante por tanto la representación no es irreducible y esto es una contradicción, pues se sabía que si era irreducible; esta contradicción proviene de haber supuesto que poseían un vector propio en común.

"$\Longleftarrow$"

Si no existe un vector propio común v para toda φ_g con $g \in G$ entonces φ es irreducible.

Supóngase por contradicción que φ_g no es irreducible, por ello posee más subespacios G-invariantes además del $\{0\}$ y el mismo espacio. Sea W un subespacio G-invariante tal que $W \neq \{0\}$ y $W \neq V$, como la representación es de grado 2 entonces W es unidimensional, por tanto existe un vector no nulo $v \in V$ tal que $W = \mathbb{C}v$, de tal forma que para $g \in G$ se tiene $\varphi_g(v) \in W$ pues $v \in W$ y este es un subespacio G-invariante. Entonces se tiene que $\varphi_g(v) = \lambda v$ para algún $\lambda \in \mathbb{C}$, quiere decir que se ha encontrado un vector propio que es común para toda φ_g con $g \in G$, pero esto es una contradicción pues se sabía que no habían vectores propios en común.

□

Se debe tener en cuenta que este insumo, utilizando vectores propios, sólo funciona para representaciones de grado 2 y grado 3 (este último caso requiere finitud de G).

Ejemplo 1.1.23. Sea r la rotación por $\pi/2$ y s la reflexión sobre el eje x. Estas permutaciones generan el grupo diedro D_8. Sea la representación $\varphi\colon D_8 \to GL_2(\mathbb{C})$ definido por

$$\underbrace{\varphi(r^k) = \begin{bmatrix} i^k & 0 \\ 0 & (-i)^k \end{bmatrix}}_{\text{Una rotación}} \qquad \underbrace{\varphi(sr^k) = \begin{bmatrix} 0 & (-i)^k \\ i^k & 0 \end{bmatrix}}_{\text{Una reflexión por una rotación}}$$

Entonces se podrá aplicar la Proposición 1.1.22 anterior para comprobar que φ es una representación irreducible.

Desarrollo. Se deberá encontrar los valores propios de las representaciones para determinar si no existe un vector propio en común.

Nótese que i al igual que $-i$ tienen orden 4 y podemos tomar en particular los siguientes elementos $\varphi(r)$ y $\varphi(sr)$. Realizando un calculo similar al del Ejercicio 1.1.21 para $\varphi(r)$ se obtendrá que sus valores propios son $\lambda = i$ y $\lambda = -i$, con sus correspondientes vectores propios $\mathbb{C}e_1$ y $\mathbb{C}e_2$.

Pero estos no son comunes a $\varphi(sr)$, pues un cálculo rápido revela que $\varphi(sr)Ce_1 = \varphi(sr)\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\i\end{bmatrix}$ y $\varphi(sr)Ce_1 = \varphi(sr)\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$. Como la representación es de grado 2 y no tiene vectores propios en común, se puede afirmar por la Proposición 1.1.22 que φ es una representación Irreducible. □

Una de las metas es mostrar que cada representación es equivalente a una suma directa de representaciones irreducibles, para lo cual se definirá cierta terminología para este propósito.

Definición 1.1.24. Completamente Reducible.

Sea G un grupo y una representación $\varphi\colon G \to GL(V)$, definimos una representación *completamente reducible* si $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ donde los V_i son subespacios $G-$invariantes y $\varphi|_{V_i}$ es irreducible para todo $i = 1, \ldots, n$.

Observación 1.1.25. *Cada V_i es irreducible pero restringido a la acción de φ.*

De forma equivalente φ es completamente reducible si $\varphi \sim \varphi^{(1)} \oplus \varphi^{(2)} \oplus \cdots \oplus \varphi^{(n)}$ donde los $\varphi^{(i)}$ son las representaciones irreducibles.

Definición 1.1.26. Representación Separable[(1)].

Una representación no nula φ de un grupo G es *separable* si $V = V_1 \oplus V_2$ con V_1 y V_2 subespacios $G-$invariantes no nulos. De lo contrario V es llamado *no-separable*. En Teoría de Representaciones de Grupos la Reducibilidad completa es análoga a la propiedad de diagonalizar una matriz en Álgebra Lineal.

El objetivo es mostrar que toda representación de un grupo finito es completamente reducible. Para ello se mostrará que toda representación es **irreducible** o **separable**, y luego se procederá por inducción sobre el grado. Pero, en primer lugar, se tiene que mostrar que estas nociones sólo dependen de la clase de equivalencia de una representación.

Lema 1.1.27. *Sea $\varphi\colon G \to GL(V)$ equivalente a una representación separable. Entonces φ es separable.*

Demostración. Sea $\psi\colon G \to GL(W)$ una representación separable con $\psi \sim \varphi$ (equivalentes) y $T\colon V \to W$ un isomorfismo de espacios vectoriales con $\varphi_g = T^{-1}\psi_g T$. Supóngase que W_1 y W_2 son subespacios invariantes distintos de cero de W tal que $W = W_1 \oplus W_2$. Ya que T es una equivalencia se tiene que el siguiente diagrama conmuta.

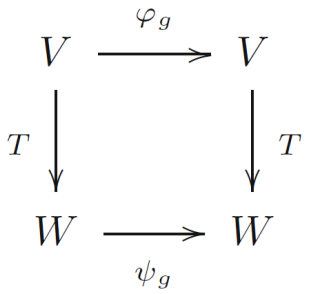

Figura 1.2: Representaciones equivalentes

Es decir, $T\varphi_g = \psi_g T$ para todo $g \in G$. Sean V_1 y V_2 dos subespacios definidos como sigue $V_1 = T^{-1}(W_1)$ y $V_2 = T^{-1}(W_2)$.

No debe perderse de vista que se quiere demostrar que φ es separable, con este objetivo se probará que $V = V_1 \oplus V_2$. Para abordar esto, se demostrará su equivalencia utilizando la definición de suma directa.

(1)El termino en inglés es *Decomposable*, que en un preliminar intento de traducción al español puede entenderse como "descomponible" pero dicho termino, no existe en nuestro idioma (no es una palabra válida para la RAE) a pesar de que en muchos textos traducidos al español lo encontremos de esa manera; por ello y dada la naturaleza de este tipo de representación, en este texto reconoceremos a las representaciones que sean "*Decomposables*" como representaciones *Separables* y como *no-separables* a las representaciones que sean "*Indecomposables*".

Véase que para un v cualquiera se tiene

$$\begin{aligned} v \in V_1 \cap V_2 &\Rightarrow T(v) \in T(V_1 \cap V_2) \\ &\Rightarrow Tv \in T(T^{-1}(W_1) \cap T^{-1}(W_2)); \text{ reemplazando } V_1 \text{ y } V_2 \\ &\Rightarrow Tv \in T(T^{-1}(W_1)) \cap T(T^{-1}(W_2)); \text{ esto es cierto porque } T \text{ es biyectiva} \\ &\Rightarrow Tv \in W_1 \cap W_2 \end{aligned}$$

Además, $W_1 \cap W_2 = \{0\}$, ahora si $Tv \in W_1 \cap W_2 \Rightarrow Tv = 0$; como T es un isomorfismo, sabemos que es inyectiva, esto implica que $v = 0$[(2)] entonces esto implica que la intersección es el espacio cero.

Por otro lado, para un elemento cualquiera $v \in V$, dado que $Tv \in W_1 \oplus W_2$ este puede escribirse como $Tv = w_1 + w_2$, donde $w_1 \in W_1$ y un $w_2 \in W_2$. De aquí se tiene que

$$\begin{aligned} Tv &= w_1 + w_2 \\ T^{-1}(Tv) &= T^{-1}(w_1 + w_2) \\ \left(T^{-1}T\right) v &= T^{-1}(w_1) + T^{-1}(w_2) \\ v &= T^{-1}w_1 + T^{-1}w_2 \text{ ; nótese que } T^{-1}w_1 \in V_1 \text{ así como } T^{-1}w_2 \in V_2 \\ \Rightarrow v &= \left(T^{-1}w_1 + T^{-1}w_2\right) \in V_1 + V_2, \text{ por tanto, } v \in V_1 \oplus V_2 \end{aligned}$$

Por lo desarrollado anteriormente se puede concluir que se puede reescribir al espacio de partida de φ como una suma directa, es decir, $V = V_1 \oplus V_2$. Ahora solo falta mostrar que V_1, V_2 son subespacios G-invariantes de V.

Si $v \in V_i$ con $i \in \{1, 2\}$ y $\varphi \sim \psi$ entonces para un elemento g se tiene:

$$T\varphi_g v = \psi_g T v$$

Pero se sabía que $Tv \in W_i$ y que este es un subespacio G-invariante, por ello $\psi_g Tv \in W_i$ con $i = 1, 2$. Y se puede reescribir como:

$$\begin{aligned} T\varphi_g v &\in W_i \\ T^{-1}\left(T\varphi_g v\right) &\in T^{-1}\left(W_i\right) \\ \varphi_g v &\in T^{-1}\left(W_i\right) \text{ ; por definición se sabe que } T^{-1}(W_i) = V_i \\ \Rightarrow \varphi_g v &\in V_i; \text{ para } i \in \{1, 2\} \end{aligned}$$

Entonces V_1 y V_2 son ambos G-invariantes, por lo tanto, φ también es separable, pues el espacio V puede ser escrito como suma directa de subespacios invariantes.

En conclusión si una representación es equivalente a una representación separable, esta también será separable. □

A continuación, se presentan resultados análogos para otros tipos de representaciones.

[(2)] Recordemos que una de las propiedades de las transformaciones lineales es que el cero del espacio de partida, es mapeado al cero del espacio de llegada.

Lema 1.1.28. *Sea $\varphi\colon G \to GL(V)$ equivalente a una representación irreducible. Entonces φ es irreducible.*

Demostración. Sea $\psi\colon G \to GL(V)$ una representación irreducible con $\psi \sim \varphi$ (equivalentes) y $T\colon W \to V$ un isomorfismo de espacios vectoriales, con $\varphi_g = T\psi_g T^{-1}$.

Se quiere demostrar que φ solo posee a $\{0\}$ y V como únicos subespacios G-invariantes.

Por contradicción, se puede afirmar que la representación φ no es irreducible, es decir, existen más subespacios invariantes además del $\{0\}$ y el mismo espacio V. Supongamos que V_1 es dicho subespacio invariante distinto de cero ($V_1 \leq V$), además, como T es una equivalencia se sabe que $T\varphi_g = \psi_g T\ \forall g \in G$. Sea $W_1 = T^{-1}(V_1)$, en el Lema 1.1.27 se comprobó que la imagen inversa también era un subespacio G-invariante, por lo tanto W_1 también será invariante.

Si $V_1 = T(W_1)$ de tal forma que se va de subespacios invariantes a subespacios invariantes, a V_1 no le queda más ser el espacio trivial o todo el espacio, ya que ψ es irreducible y el isomorfismo T es biunívoco, así para cada elemento de V existirá uno en W o se corresponderá con el espacio trivial, por ello se puede afirmar que V también es irreducible.

En conclusión, si una representación es equivalente a una representación irreducible entonces esta también será irreducible. □

Lema 1.1.29. *Sea $\varphi\colon G \to GL(V)$ equivalente a una representación completamente reducible. Entonces φ es completamente reducible.*

Demostración. Sea $\psi\colon G \to GL(W)$ una representación completamente reducible con $\psi \sim \varphi$ (equivalentes) y $T\colon V \to W$ un isomorfismo de espacios vectoriales con $\varphi_g = T^{-1}\psi_g T$. Supóngase para W que los siguientes subespacios no nulos W_1, W_2, $\cdots$, W_n, todos ellos G-invariantes tales que $W = W_1 \oplus W_2 \oplus \cdots \oplus W_n$. Como T es una equivalencia se sabe que $T\varphi_g = \psi_g T$ para todo $g \in G$, se definen los subespacios $V_i = T^{-1}(W_i)$ para $i = 1, \ldots, n$ en cada caso.

Se quiere demostrar que φ es completamente reducible, con este objetivo se probará que $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$. Para abordar esto, se demostrará su equivalencia a través de la definición de suma directa.

Véase que para un u cualquiera y para $i = 1, \ldots, n$ se tiene

$$
\begin{aligned}
u \in V_1 \cap V_2 \cap \cdots \cap V_n &\Rightarrow Tu \in T\left(\bigcap_{i=1}^{n} V_i\right) \\
&\Rightarrow Tu \in T\left(\bigcap_{i=1}^{n} T^{-1}(W_i)\right); \text{ reemplazando a cada } V_i \\
&\Rightarrow Tu \in \bigcap_{i=1}^{n} T\left(T^{-1}(W_i)\right); \text{ esto es cierto por que } T \text{ es biyectiva} \\
&\Rightarrow Tu \in \bigcap_{i=1}^{n} W_i
\end{aligned}
$$

Agregado a ello se sabe que $\bigcap_{i=1}^{n} W_i = \{0\}$, así que $Tu = 0$ entonces por la inyectividad del isomorfismo T, implica que $u = 0$ por tanto la intersección es el subespacio cero.

Por otro lado, para un elemento cualquiera $u \in V$ se tiene que $Tu \in \bigoplus_{i=1}^{n} W_i$, por ello Tu puede escribirse como $Tu = w_1 + w_2 + \ldots + w_n = \sum_{i=1}^{n} w_i$ con $w_i \in W_i$ para cada i.

De aquí se tiene que

$$\begin{aligned} Tu &= \sum_{i=1}^{n} w_i \\ T^{-1}(Tu) &= T^{-1}\left(\sum_{i=1}^{n} w_i\right) \\ \left(T^{-1}T\right)u &= \sum_{i=1}^{n} T^{-1}(w_i) \\ u &= \sum_{i=1}^{n} \left(T^{-1}w_i\right) \end{aligned}$$

Nótese que $\forall i\ T^{-1}w_i \in V_i$; entonces se puede escribir $T^{-1}w_i = v_i$, para todo i con $v_i \in V_i$.

$$\Rightarrow u = (v_1 + v_2 + \ldots + v_n) \in \sum_{i=1}^{n} V_i \text{; por tanto } u \in \bigoplus_{i=1}^{n} V_i = V_1 \oplus \cdots \oplus V_n$$

Por lo desarrollado anteriormente se concluye que se puede reescribir al espacio de partida de φ como una suma directa, es decir, $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$. Ahora solo falta mostrar que cada V_i con $i = 1,\ \ldots,\ n$, es un subespacio G-invariante de V.

Si $u \in V_i$ con $i = 1,\ \ldots,\ n$ y $\varphi \sim \psi$ entonces para un elemento de G se tiene:

$$TT\varphi_g u = \psi_g Tu$$

Pero ya se sabe que $Tu \in W_i$, y cada uno de estos es un subespacio G-invariante, por ello $\psi_g Tu \in W_i$ para algún i. Y puede reescribirse como:

$$\begin{aligned} T\varphi_g u &\in W_i \\ T^{-1}\left(T\varphi_g u\right) &\in T^{-1}\left(W_i\right) \\ \varphi_g u &\in T^{-1}\left(W_i\right) \text{; por definición } T^{-1}(W_i) = V_i \\ \Rightarrow \varphi_g u &\in V_i \text{; para algún } i \in \{1,\ \ldots,\ n\} \end{aligned}$$

De aquí que se puede concluir que cada V_i es G-invariante, por lo tanto φ también es completamente irreducible, pues el espacio V puede ser escrito como suma directa de subespacios invariantes y cada representación restringida a los subespacios es irreducible.

En conclusión si una representación es equivalente a una representación completamente reducible, esta también será completamente reducible.

□

1.2. El Teorema de Maschke y la Completa Reducibilidad

Con el fin de poder efectuar sumas directas de separaciones de representaciones, se aprovecharán las herramientas proporcionadas por el producto interno y la descomposición ortogonal.

Definición 1.2.1. Representación Unitaria.

Sea V un espacio con producto interno. Una representación $\varphi\colon G \to GL(V)$ se dice que es unitaria si φ_g es unitaria $\forall g \in G$, es decir,

$$\langle \varphi_g(v), \varphi_g(w) \rangle = \langle v, w \rangle$$

para todo $v, w \in W$. En otras palabras, debe observarse a φ como un mapeo de $\varphi\colon G \to U(V)$ [(3)].

Se identifica a $GL_1(\mathbb{C})$ con $\mathbb{C}^*$, véase que un número complejo z es unitario (visto como una matriz) si y solo si $\overline{z} = z^{-1}$, esto es $z\overline{z} = 1$. Pero esto dice exactamente que $|z| = 1$, entonces $U_1(\mathbb{C})$ es exactamente el círculo unitario $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ en $\mathbb{C}$. Por lo tanto una representación unitaria unidimensional es un homomorfismo $\varphi\colon G \to \mathbb{T}$.

Ejemplo 1.2.2. Se define a $\varphi\colon \mathbb{R} \to \mathbb{T}$ por $\varphi(t) = e^{2\pi i t}$. Entonces φ es una representación unitaria del grupo aditivo de $\mathbb{R}$.

Desarrollo. Sean s y $t \in \mathbb{R}$, aplicando la definición se tiene

$$\begin{aligned} \varphi(t+s) &= e^{2\pi i(t+s)} \\ &= e^{2\pi i t} e^{2\pi i s} \\ &= \varphi(t)\varphi(s) \end{aligned}$$

Luego de que se ha probado que es un homomorfismo, debe verse que es unitaria, ya que, por definición su conjunto de llegada es el circulo unitario $\mathbb{T}$ □

Un hecho crucial, el cual hace a una representación unitaria tan útil, es que cada una es separable o es irreducible como lo muestra la siguiente proposición.

Proposición 1.2.3. *Sea $\varphi\colon G \to GL(V)$ una representación unitaria de un grupo, entonces φ es irreducible o separable.*

[(3)] El operador lineal $U \in GL(V)$ se dice que es unitario si $\langle Uv, Uw \rangle = \langle v, w \rangle$ para todo $v, w \in V$, en donde estos operadores unitarios son invertibles. Por otro lado $U(V)$ es el conjunto de mapeos unitarios, que a su vez es un subgrupo de $GL(V)$.

Demostración. Supóngase que φ no es irreducible. Entonces hay un W subespacio propio no nulo G-invariante de U. Sea $W^{\perp}$ su complemento ortogonal, entonces también es distinto de cero y se sabe que $V = W \oplus W^{\perp}$.

Por lo tanto, para demostrar que es separable si $v \in W^{\perp}$ y $w \in W$, se sabe que $\langle v, w \rangle = 0$, por ser ortogonales, entonces

$$\begin{aligned}
\langle \varphi_g(v), w \rangle &= \langle \varphi_{g^{-1}}\varphi_g(v), \varphi_{g^{-1}}(w) \rangle \text{; ya que } \varphi_{g^{-1}} \text{ es unitaria, por Definición 1.2.1} \\
&= \langle v, \varphi_{g^{-1}}(w) \rangle \text{; nótese que } \varphi_{g^{-1}} \circ \varphi_g = \varphi_1 = I \\
&= \langle v, w' \rangle \text{; como } \varphi_{g^{-1}}(w) \in W \text{ por ser invariante} \\
&= 0 \text{; ya que } \langle v, w' \rangle = 0
\end{aligned}$$

Se concluye que φ es separable ya que puede ser escrita como suma directa de espacios irreducibles. □

Resulta que para los grupos finitos toda representación es equivalente a una representación unitaria. Esto no es cierto para los grupos infinitos por supuesto.

Proposición 1.2.4. *Cada representación de un grupo finito G es equivalente a una representación unitaria.*

Demostración. Sea $\varphi\colon G \to GL(V)$ una representación donde $\dim V = n$. Se escoge una base B para V, y sea $T\colon V \to \mathbb{C}^n$ el isomorfismo que toma coordenadas con respecto a B. Entonces se establece $\rho_g = T\varphi_g T^{-1}$, para $g \in G$, dicha asignación tiene sentido porque estamos trabajando con elementos invertibles, y produce una representación $\rho\colon G \to GL_n(\mathbb{C})$ equivalente a φ. Sea $\langle \cdot, \cdot \rangle$ el producto interno estándar en $\mathbb{C}^n$, se define un nuevo producto interno $(\cdot, \cdot)$ en $\mathbb{C}^n$ utilizando el crucial "truco de la suma"[(4)], que será utilizado con frecuencia en todo el texto. Sean $v, w \in G$, se define

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

Esta suma sobre G, por supuesto, requiere que G sea finito. El procedimiento que describe la definición puede ser visto como un proceso de "suavizado".

[(4)] En término en inglés es "Averaging trick", que puede ser traducido como "truco del promedio", sin embargo, por la forma en la que se comporta en este trabajo consideramos más adecuado llamarlo como "truco de la suma".

Se verá que esto es un producto interno. En primer lugar, se comprueba que:

$$\begin{aligned}(c_1v_1 + c_2v_2, w) &= \sum_{g\in G}\langle \rho_g(c_1v_1 + c_2v_2), \rho_g w\rangle;\ \rho \text{ es una transformación lineal.}\\ &= \sum_{g\in G}\langle \rho_g(c_1v_1) + \rho_g(c_2v_2), \rho_g w\rangle\\ &= \sum_{g\in G}[c_1\langle \rho_g v_1, \rho_g w\rangle + c_2\langle \rho_g v_2, \rho_g w\rangle]\end{aligned}$$

; se sabe que $\langle (a_1U_1) + (a_2U_2), w\rangle = a_1\langle U_1, w\rangle + a_2\langle U_2, w\rangle$ entonces

$$\begin{aligned}&= c_1\sum_{g\in G}\langle \rho_g v_1, \rho_g w\rangle + c_2\sum_{g\in G}\langle \rho_g v_2, \rho_g w\rangle\\ &= c_1(v_1, w) + c_2(v_2, w).\end{aligned}$$

Luego se verifica:

$$\begin{aligned}(w, v) &= \sum_{g\in G}\langle \rho_g w, \rho_g v\rangle\\ &= \sum_{g\in G}\overline{\langle \rho_g v, \rho_g w\rangle};\ \text{porque se sabe que } \langle x, y\rangle = \overline{\langle y, x\rangle}\\ &= \overline{\sum_{g\in G}\langle \rho_g v, \rho_g w\rangle}\\ &= \overline{(v, w)}.\end{aligned}$$

Finalmente, se observa que

$$(v, v) = \sum_{g\in G}\langle \rho_g v, \rho_g v\rangle \geq 0;\ \text{porque cada término } \langle \rho_g v, \rho_g v\rangle \geq 0.$$

Si $(v, v) = 0$, $0 = \sum_{g\in G}\langle \rho_g v, \rho_g v\rangle$, lo que implica $\langle \rho_g v, \rho_g v\rangle = 0$ para todo $g \in G$ ya que se esta añadiendo números no negativos. Por lo tanto, $0 = \langle \rho_1 v, \rho_1 v\rangle = \langle v, v\rangle$, y entonces $v = 0$. Ahora hemos establecido que $(\cdot, \cdot)$ es un producto interno.

Para verificar que la representación es unitaria con respecto a este producto interno, se calcula

$$(\rho_h v, \rho_h w) = \sum_{g\in G}\langle \rho_g\rho_h v, \rho_g\rho_h v\rangle = \sum_{g\in G}\langle \rho_{gh} v, \rho_{gh} w\rangle;\ \text{por que } \rho \text{ es un homomorfismo.}$$

Se define $x = gh$, para alicar un cambio de variables. Como g se extiende sobre todo G, x se extiende sobre todos los términos de G ya que si $k \in G$, entonces cuando $g = kh^{-1}$, $x = k$. Por lo tanto $(\rho_h v, \rho_h w) = \sum_{x\in G}\langle \rho_x v, \rho_x w\rangle = (v, w)$. Lo que completa la prueba. □

Así se obtiene el siguiente corolario, que asegura que cada representación no-separable de un grupo finito es irreducible.

Corolario 1.2.5. *Sea $\varphi\colon G \to GL(V)$ una representación no nula de un grupo finito. Entonces φ es irreducible o separable.*

Demostración. Por la Proposición 1.2.4, φ es equivalente a la representación unitaria ρ. La Proposición 1.2.3 entonces implica que ρ es irreducible o separable. Los Lemas 1.1.27 y 1.1.28 entonces sostienen que φ es irreducible o ya sea separable, como era deseado. □

El siguiente ejemplo muestra que el Corolario 1.2.5 falla en grupos infinitos y, por lo tanto, la Proposición 1.2.4 también debe fallar en los grupos infinitos, ya que si se observa la contrapositiva del corolario se tiene: "Si φ es una representación reducible y no separable, entonces es una representación no nula de un grupo infinito"

Ejemplo 1.2.6. A continuación, se proporciona un ejemplo de una representación no-separable de $\mathbb{Z}$, que no es irreducible. Se define $\varphi\colon \mathbb{Z} \to GL_2(\mathbb{C})$ por

$$\varphi(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Desarrollo. Se verifica que φ es un homomorfismo, tomando dos elementos n, $m \in \mathbb{Z}$:

$$\begin{aligned} \varphi(n+m) &= \begin{bmatrix} 1 & n+m \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \\ &= \varphi(n)\varphi(m) \end{aligned}$$

El vector $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ es un vector propio de $\varphi(n)$ ya que

$$\begin{aligned} \varphi_n(e_1) &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \ \forall n \in \mathbb{Z} \end{aligned}$$

Además se comprueba que $\mathbb{C}e_1$ es un subespacio $\mathbb{Z}$-invariante, tomando $u = \begin{bmatrix} a \\ 0 \end{bmatrix} \in \mathbb{C}e_1$

$$\begin{aligned} \varphi_n(u) &= \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} a \\ 0 \end{bmatrix} \\ &= u \in \mathbb{C}e_1 \ \forall n \in \mathbb{Z} \end{aligned}$$

Esto demuestra que φ no es irreducible.

Por otro lado para corroborar que no es diagonalizable debe determinarse que no es posible reducirla a una matriz diagonal, por el proceso de diagonalización se busca:

$$\begin{vmatrix} 1- & n \\ 0 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 \text{; entonces tiene un valor propio } \lambda = 1$$

Se buscan los vectores propios utilizando la ecuación característica $(A - I)x = 0$:

$$\begin{aligned} \left(\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ \left(\begin{bmatrix} 0 & n \\ 0 & 0 \end{bmatrix} \right) \begin{bmatrix} x \\ y \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} ny \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \end{aligned}$$

De donde se obtiene que $x = 0$ y $y = 0$, al ser el vector cero, se puede decir que no es posible diagonalizar esta matriz.

De ello se deduce que φ es no-separable, ya que si fuera separable sería posible poder escribirla como suma directa de las representaciones unidimensionales y se sabe por la Definición 1.1.14 que su representación es una matriz diagonal.

□

Observación 1.2.7. *Es importante notar que cualquier representación irreducible es no-separable, ya que por definición una representación es irreducible si no tiene subespacios invariantes y es no-separable si no puede ser escrita como la suma directa de subespacios invariantes, en resumen, una representación irreducible es no-separable, porque de lo contrario podría descomponerse en una suma directa de irreducibles.*

Sin embargo, lo contrario no se cumple, es decir, que una representación que sea no-separable sea irreducible, el Ejemplo 1.2.6 es un contra ejemplo a dicha afirmación.

El siguiente teorema es el resultado principal de este capítulo. Esta prueba es bastante análoga a la prueba de la existencia de una descomposición en factores primos de un entero o de una factorización de polinomios por medio de irreducibles.

Teorema 1.2.8. ***(Maschke)***.

Cada representación de un grupo finito es completamente reducible.

Demostración. Sea $\varphi\colon G \to GL(V)$ la representación de un grupo finito G. La prueba procede por inducción sobre el grado de φ, esto es, $\dim V$. Si $\dim V = 1$, entonces φ es irreducible ya que V no tiene subespacios propios diferentes de cero.

Supóngase que la afirmación es cierta para dimV $\leq$ n, se deberá verificar que para $\varphi\colon G \to GL(V)$ una representación con dim$V = n+1$ también se cumple que sea completamente reducible.

Si φ es irreducible, entonces se ha terminado la demostración, ya que, la representación ya esta escrita como la suma directa de representaciones irreducibles (ella misma).

De lo contrario, φ es separable por el Corolario 1.2.5, lo que permite poder escribir al espacio como la suma directa de al menos dos subespacios G-invariantes, sean V_1, $V_2 \neq 0$ esos subespacios tales que $V = V_1 \oplus V_2$. Además, se tiene que dimV$_1$, dimV$_2$ $<$ dimV, *asíporinducción*$\varphi|_{V_1}$ y $\varphi|_{V_2}$ son completamente reducibles. Por lo tanto, se puede reescribir a los subesapcios como $V_1 = U_1 \oplus \cdots \oplus U_s$ y $V_2 = W_1 \oplus \cdots \oplus W_r$ donde los U_i, W_i son G-invariantes y las subrepresentaciones $\varphi|_{U_i}$, $\varphi|_{W_j}$ son irreducibles para todo $1 \leq i \leq s$, $1 \leq j \leq r$.

Entonces $V = U_1 \oplus \cdots \oplus U_s \oplus W_1 \oplus \cdots \oplus W_r$ y φ es completamente irreducible, por que ha podido ser escrito como suma directa de representaciones irreducibles. □

Observación 1.2.9. *Si se escoge φ como la representación de la cual habla el teorema, se puede verificar que cuando φ es una matriz de representación unitaria, entonces φ es equivalente a una suma directa de representaciones unitarias irreducibles a través de una equivalencia implementada por una matriz unitaria T (Proposición 1.2.4). En resumen podemos decir que las representaciones unitarias están compuestas por matrices unitarias.*

En conclusión, si $\varphi\colon G \to GL_n(\mathbb{C})$ es cualquier representación de un grupo finito, entonces

$$\varphi \sim \begin{bmatrix} \varphi^{(1)} & 0 & \cdots & 0 \\ 0 & \varphi^{(2)} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varphi^{(m)} \end{bmatrix}$$

donde $\varphi^{(i)}$ es irreducible para cada i[5]. Ahora queda por determinar cuando una descomposición en irreducibles es única, a esta interrogante se le dará respuesta en el siguiente capítulo.

[5] Esto es análogo al teorema espectral que indica que todas las matrices autoadjuntas son diagonalizables.

Capítulo 2

Teoría de Caracteres y Relaciones de Ortogonalidad

En este capítulo se estudiará la Teoría de Caracteres, que por decirlo de alguna manera es el corazón de la Teoría de Representaciones de Grupos, la idea principal es poder codificar una representación $\varphi\colon G \to GL_n(\mathbb{C})$ de G en una función con valores complejos $\chi_\varphi\colon G \to \mathbb{C}$. En otras palabras, se reemplaza una función de un espacio n-dimensional por otra función de un espacio uno-dimensional.

Se establecerán las relaciones de ortogonalidad de Schur, las cuales a grandes rasgos muestran que las entradas de las representaciones unitarias irreducibles, de un grupo finito G forman una base ortogonal para el espacio de funciones complejas en G.

2.1. Morfismos de Representaciones

Un principio de la matemática moderna es que los mapeos entre los objetos matemáticos tienen la misma importancia que los propios objetos. Teniendo esta idea en mente, se define la noción de "morfismo" entre representaciones. Sea $\varphi\colon G \to GL(V)$ una representación, puede pensarse en los elementos de G como escalares por medio de $g \cdot v = \varphi_g v$ para $v \in V$, es decir, se tiene a los elementos del grupo que actúan sobre v por medio de una función (el morfismo); de aquí que un morfismo entre $\varphi\colon G \to GL(V)$ y $\rho\colon G \to GL(W)$ debe ser una transformación lineal $T\colon V \to W$ tal que $Tgv = gTv$ para todo $g \in G$ y $v \in V$. Formalmente, esto significa $T\varphi_g v = \rho_g T v$ para todo $v \in V$, es decir, $T\varphi_g = \rho_g T$ para todo $g \in G$.

Definición 2.1.1. Morfismo.

Sean $\varphi\colon G \to GL(V)$ y $\rho\colon G \to GL(W)$ dos representaciones. Un *morfismo* entre φ y ρ es por definición un mapeo lineal $T\colon V \to W$ tal que $T\varphi_g = \rho_g T$, para todo $g \in G$. En otras palabras el siguiente diagrama muestra que conmuta para todo $g \in G$.

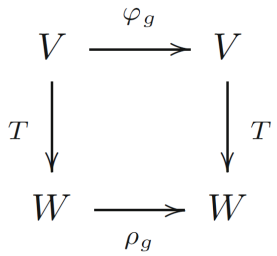

Figura 2.1: Morfismo de Representaciones

El conjunto de todos morfismos de φ a ρ, esta denotado por $\mathrm{Hom}_G(\varphi, \rho)$. Observése que $\mathrm{Hom}_G(\varphi, \rho) \subseteq \mathrm{Hom}(V, W)$, nótese que los $\mathrm{Hom}_G(\varphi, \rho)$ son un caso particular de los $\mathrm{Hom}(V, W)$, ya que en el primer conjunto están solo los homomorfismos que representan a G y en el otro conjunto se encuentran a todos los operadores lineales que existen entre V y W.

Observación 2.1.2. *Si $T \in \mathrm{Hom}_G(\varphi, \rho)$ es invertible, entonces $\varphi \backsim \rho$ y T es una equivalencia (o isomorfismo).*

Observación 2.1.3. *Observése que $T\colon V \to V$ pertenece a $\mathrm{Hom}_G(\varphi, \varphi)$ si y solo si $T\varphi_g = \varphi_g T$ para todo $g \in G$, esto es, T conmuta (o centraliza) con $\varphi(G)$. En particular, la función identidad $I\colon V \to V$ es siempre un elemento de $\mathrm{Hom}_G(\varphi, \varphi)$.*

En álgebra, para los homomorfismos el núcleo (centro) y la imagen de un morfismo de representaciones suelen ser subrepresentaciones.

Proposición 2.1.4. *Sea $T\colon V \to W$ que pertenece a $\mathrm{Hom}_G(\varphi, \rho)$, entonces $\ker T$ es un subespacio G-invariante de V y $T(V) = \mathrm{Im}\, T$ es un subespacio G-invariante de W.*

Demostración. Se sabe que $\ker T \leq V$, entonces para probar que es un subespacio invariante se toman $v \in \ker T$ y $g \in G$ y se quiere que $\varphi_g v \in \ker T$.

Se sabe que $T\varphi_g v = \rho_g T v$ por definición de morfismo y como $v \in \ker T$ entonces $Tv = 0$ de aquí que

$$\begin{aligned} &\rho_g T v = 0 \\ \Rightarrow\ &T\varphi_g v = 0; \text{ por el morfismo} \\ \Rightarrow\ &\varphi_g v = 0; \text{ por lo tanto } \varphi_g v \in \ker T \end{aligned}$$

como se han obtenido los resultados deseados, se concluye que $\ker T$ es G-invariante.

Por otro lado se sabe que $\mathrm{Im}\, T \leq W$ entonces para probar que es un subespacio invariante se toma $w \in \mathrm{Im}\, T$, entonces este w tiene la forma $w = Tv$ con $v \in V$, si ahora se aplica ρ_g a w se quiere probar que $\rho_g w \in \mathrm{Im}\ T$.

Ahora, se tiene que $\rho_g w = \rho_g T v$ (solo sustituyendo el valor de w) y por el morfismo se tiene $\rho_g T v = T\varphi_g v$ y como $\varphi_g v \in V$ es evidente que $T\varphi_g v \in \mathrm{Im}\, T$. Por lo tanto hemos encontrado que $\mathrm{Im}\, T$ es G-invariante también. □

El conjunto de morfismos de φ a ρ tiene la estructura adicional de un espacio vectorial, como se muestra en la siguiente proposición.

Proposición 2.1.5. *Sean* $\varphi\colon G \to GL(V)$ *y* $\rho\colon G \to GL(W)$ *representaciones. Entonces* $\mathrm{Hom}_G(\varphi, \rho)$ *es un subespacio de* $\mathrm{Hom}(V, W)$.

Demostración. Para probar que un conjunto es un subespacio recuérdese que se puede utilizar la caracterización que establece que dados $w, w' \in W$ y $\lambda, \lambda' \in \mathbb{K} \Longrightarrow \lambda w + \lambda' w' \in W$

Se toma $T_1, T_2 \in \mathrm{Hom}_G(\varphi, \rho)$ y $c_1, c_2 \in \mathbb{C}$ y se quiere probar que $(c_1T_1 + c_2T_2)\varphi_g = \rho_g(c_1T_1 + c_2T_2)$ para que $(c_1T_1 + c_2T_2)$ pertenezca a $\mathrm{Hom}_G(\varphi, \rho)$.

Entonces

$$\begin{aligned}(c_1T_1 + c_2T_2)\varphi_g &= c_1T_1\varphi_g + c_2T_2\varphi_g \text{ ; ya que } T_1, T_2 \in Hom_G(\varphi, \rho)\\ &= c_1\rho_gT_1 + c_2\rho_gT_2 \text{ ; ya que } T_i\varphi_g = \rho_gT_i \text{ con } i = 1, 2\\ &= \rho_g(c_1T_1 + c_2T_2); \text{ ya que } \rho_g \text{ es un operador lineal.}\end{aligned}$$

De aquí que $(c_1T_1 + c_2T_2) \in \mathrm{Hom}_G(\varphi, \rho)$ como se quería, por tanto es un subespacio. □

Es importante observar que a grandes rasgos en toda la teoría de representaciones los morfismos entre representaciones irreducibles son muy limitados. Aquí es cuando debe notarse que se esta trabajando sobre el campo de los números complejos y no en el campo de los números reales. Es decir, se utiliza el hecho de que cada operador lineal sobre un espacio vectorial complejo de dimensión finita tiene un valor propio y esto es una consecuencia del hecho que cada polinomio sobre $\mathbb{C}$ posee una raíz; en particular el polinomio característico del operador tiene una raíz.

Lema 2.1.6. ***(Lema de Schur)***.

Sean φ, ρ *representaciones irreducibles de* G, *y* $T \in \mathrm{Hom}_G(\varphi, \rho)$. *Entonces* T *es invertible o* $T = 0$. *En consecuencia:*

(a) Si $\varphi \nsim \rho$, *entonces* $\mathrm{Hom}_G(\varphi, \rho) = \{0\}$;

(b) Si $\varphi = \rho$, *entonces* $T = \lambda I$ *con* $\lambda \in \mathbb{C}$ *(esto quiere decir que* T *es la multiplicación por un escalar).*

Demostración. Sea $\varphi\colon G \to GL(V)$, $\rho\colon G \to GL(W)$, y sea $T\colon V \to W$ que pertenece a $\mathrm{Hom}_G(\varphi, \rho)$.

Si $T = 0$ la demostración habrá terminado, ya que, dadas las premisas basta con que una de las dos condiciones se cumpla.

Entonces se asume que $T \neq 0$. La Proposición 2.1.4 implica que el ker de T es G-invariante y por lo tanto el $\ker T = V$ o el $\ker T = 0$. Véase que si el $\ker T = V$ entonces $\forall v \in V$ se tiene que $T(v) = 0 \Longrightarrow T = 0$ y se había asumido que $T \neq 0$, por tanto $\ker T = 0$ y se afirma que T es inyectiva.

Por otro lado, por la Proposición 2.1.4 se tiene que $\operatorname{Im} T$ es G-invariante y por tanto $\operatorname{Im} T = W$ o $\operatorname{Im} T = 0$, pero si $\operatorname{Im} T = 0 \implies T\colon V \to W$ entonces para $u \in V$ se tiene $T(u) = 0$, si $w = T(u)$ entonces esto seria cierto $\forall w \in W$; esto pasa cuando $T = 0$ y se ha asumido que $T \neq 0$, de aquí que $\operatorname{Im} T = W$ y como la imagen del homomorfismo es todo el espacio de llegada entonces T es sobreyectiva.

En conclusión como T es inyectiva y sobreyectiva, entonces es biyectiva y por tanto es invertible, que era lo que se deseaba probar.

Ahora se probará la consecuencia del Lema de Schur

(a) Se demostrará por la contrapositiva, que dice que: Si $\operatorname{Hom}_G(\varphi, \rho) \neq 0$ entonces $\varphi \sim \rho$. Nótese que si $\operatorname{Hom}_G(\varphi, \rho) \neq 0$ entonces existe $T \neq 0 \in \operatorname{Hom}_G$ y sería invertible ya que por la primera parte del Lema todos los homomorfismos no nulos son invertibles, y se cumpliría que $\rho_g T = T\varphi_g \ \forall g \in G$, es decir, $\varphi \sim \rho$

(b) Sea λ un valor propio de T (nótese que se trabaja sobre $\mathbb{C}$ y no sobre $\mathbb{R}$). Entonces $\lambda I - T$ no es invertible ya que por definición de valor propio se tiene que $\det(\lambda I - T) = 0$ y si $\det = 0$ entonces la matriz no es invertible.

Ahora como $I \in \operatorname{Hom}_G(\varphi, \varphi)$, la prueba de la Proposición 2.1.5 dice que $\lambda I - T$ pertenece a $\operatorname{Hom}_g(\varphi, \varphi)$. Nótese que según la primera parte de este lema, todos los elementos no nulos de $\operatorname{Hom}_g(\varphi, \varphi)$ son invertibles y ya se estableció que $\lambda I - T$ no es invertible, entonces no le queda más que $\lambda I - T = 0$ y si se despeja a T se tiene que $T = \lambda I$.

□

Observación 2.1.7. *Se deduce del Lema de Schur que*

1. *Todos los homomorfismos no nulos son invertibles y si no son invertibles obligatoriamente son nulos.*

2. *El ítem (a) dice que si* $\operatorname{Hom}_G(\varphi, \rho) = \{0\}$ *entonces* $T = \{0\}$ *y las representaciones no son equivalentes.*

3. *Del ítem (b) se observa que si* φ *y* ρ *son representaciones irreducibles equivalentes entonces* $\dim \operatorname{Hom}_G(\varphi, \rho) = 1$*, ya que si se toma* $S\colon \varphi \to \rho$ *y* $T\colon \varphi \to \rho$*, si* $S^{-1}\colon \rho \to \varphi$ *y se calcula la composición* $S^{-1}T\colon \varphi \to \varphi$ *entonces* $S^{-1}T \in \operatorname{Hom}(\varphi, \varphi)$ *entonces*

$$\begin{aligned} S^{-1}T &= \lambda I \\ T &= S\lambda I \\ &= \lambda S I \\ &= \lambda S \end{aligned}$$

Por lo tanto si φ *y* ρ *son representaciones irreducibles equivalentes entonces habría un solo homomorfismo (una sola matriz) que los relacione, exceptuando los múltiplos que estarían dados por todos los posibles valores de* λ *de acuerdo a lo expuesto en el literal (b).*

Después de los resultados anteriores, se puede describir las representaciones irreducibles de un grupo abeliano.

Corolario 2.1.8. *Sea G un grupo abeliano. Entonces cualquier representación irreducible de G tendrá grado uno.*

Demostración. Sea $\varphi\colon G \to GL(V)$ una representación irreducible. Se fija por el momento $h \in G$, haciendo $T = \varphi_h$ se obtiene para todo $g \in G$ que

$$\begin{aligned} T\varphi_g &= \varphi_h\varphi_g \text{ ; sustituyendo a } T \\ &= \varphi_{hg} \text{ ; por propiedades del homomorfismo } \varphi \\ &= \varphi_{gh} \text{ ; como } G \text{ es conmutativo } hg = gh \\ &= \varphi_g\varphi_h \text{ ; por propiedades del homomorfismo } \varphi \\ &= \varphi_g T \text{ ; sustituyendo a } \varphi_h \end{aligned}$$

Observése que T cumple con la Definición 2.1.1 entonces $T \in \mathrm{Hom}_G(\varphi, \varphi)$, nótese que al hablar de T o de φ_h, se habla de la misma representación, por ello puede tratarse como una matriz sin ningún problema. Consecuentemente, el lema de Schur implica que $T = \varphi_h = \lambda_h I$ para algún escalar $\lambda_h \in \mathbb{C}$ [(1)].

Sea $\mathbb{C}v$, se probará que es G-invariante, para ello sea v un vector no nulo y $k \in \mathbb{C}$, lo que se busca es comprobar que $\varphi_h(kv) \in \mathbb{C}v$ entonces

$$\begin{aligned} \varphi_h(kv) &= (\lambda_h I)kv \text{ ; sustituyendo a } \varphi_h \\ &= (\lambda_h k)v \text{ ; nótese que } (\lambda_h k) \in \mathbb{C} \text{ e } I \text{ es la matriz identidad.} \end{aligned}$$

Entonces $(\lambda_h k)v \in \mathbb{C}v$, y como h se tomo arbitrario se puede afirmar sin pérdida de generalidad que $\mathbb{C}v$ es un subespacio G-invariante. Por otro lado recuérdese que los únicos subespacios G-invariantes son $\{0\}$ y todo el espacio V, como $\mathbb{C}v$ es G-invariante entonces se concluye que $V = \mathbb{C}v$ por la irreducibilidad de la representación, además $\dim \mathbb{C}v = 1$ entonces al ser arbitrario se puede concluir que, cualquier representación irreducible de G de un grupo abeliano, tendrá grado 1. □

A continuación se muestran algunas de las aplicaciones de este resultado en el álgebra lineal.

Corolario 2.1.9. *Sea G un grupo abeliano finito y $\varphi\colon G \to GL_n(\mathbb{C})$ una representación. Entonces existe una matriz invertible T tal que $T^{-1}\varphi_g T$ es diagonal para toda $g \in G$ (con T independiente de g).*

Demostración. Por el Teorema de Maschke (Teorema 1.2.8) se tiene que φ es completamente reducible, por la Definición 1.1.24 esto quiere decir que $\varphi \sim \varphi^{(1)} \oplus \cdots \oplus \varphi^{(m)}$ donde las $\varphi^{(i)}$, con $i = 1, \ldots, m$ son irreducibles. Como G es abeliano, debido al Corolario 2.1.8 el

[(1)] El subíndice indica la dependencia sobre h

grado de cada $\varphi^{(i)}$ es 1 (y por lo tanto $n = m$).

En consecuencia, $\varphi_g^{(i)} \in \mathbb{C}^* \ \forall \ g \in G$ ya que son irreducibles y de grado uno. Ahora como $\varphi \sim \bigoplus_{i=1}^{n} \varphi^{(i)}$ entonces existe T tal que $T\colon \mathbb{C}^n \to \mathbb{C}^n$ que permite la equivalencia antes descrita, haciendo uso de la Definición 1.1.14 se tiene

$$T^{-1}\varphi_g T = \begin{bmatrix} \varphi_g^{(1)} & 0 & \cdots & 0 \\ 0 & \varphi_g^{(2)} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \varphi_g^{(n)} \end{bmatrix}$$

que es una matriz diagonal para todo $g \in G$. □

El siguiente corolario obtenido a partir de las aplicaciones directas del Corolario 2.1.8 presenta un requisito para la diagonalización de matrices de orden finito.

Corolario 2.1.10. *Sea $A \in GL_m(\mathbb{C})$ una matriz de orden finito, si $A^n = I$, entonces los valores propios de A son las raíces n-ésimas de la unidad. Además A es diagonalizable*[2].

Demostración. Supóngase que $A^n = I$ y se define una representación $\varphi\colon \mathbb{Z}/n\mathbb{Z}$[3] $\to GL_m(\mathbb{C})$ por medio de $\varphi([k]) = A^k$. Se verificará que esta función está bien definida y es una representación.

$$\begin{aligned} \text{Si } [k] &= [p] \\ \text{entonces } k &= p + nq \text{ con } q \in \mathbb{Z} \\ \text{así } \varphi([k]) &= A^{p+nq} \\ A^k &= A^p A^{nq} \\ A^k &= A^p \left(A^n\right)^q \\ A^k &= A^p \left(I\right)^q \\ A^k &= A^p \\ \text{que no es más que } \varphi([k]) &= \varphi([p]) \end{aligned}$$

por lo tanto está bien definida, se comprbabrá que es homomorfismo.

$$\begin{aligned} \text{Sea } \varphi([k+p]) &= A^{k+p} \\ &= A^k A^p \\ &= \varphi([k])\varphi([p]) \end{aligned}$$

[2] Que una matriz sea *diagonalizable* quiere decir que existe una base de vectores propios, cuya transformación resultante es una matriz diagonal.

[3] $\mathbb{Z}/n\mathbb{Z}$ es abeliano

Por lo tanto existe $T \in GL_n(\mathbb{C})$ tal que $T^{-1}AT$ es diagonal por el Corolario 2.1.9, este afirma también que es diagonalizable. Supóngase

$$T^{-1}AT = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_m \end{bmatrix} = D$$

Entonces

$$\begin{aligned} D^n &= (T^{-1}AT)^n \\ &= T^{-1}A^nT \\ &= T^{-1}IT = I \end{aligned}$$

Para lo cual se tiene

$$\begin{bmatrix} \lambda_1^n & 0 & \cdots & 0 \\ 0 & \lambda_2^n & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_m^n \end{bmatrix} = D^n = I$$

y por lo tanto $\lambda_i^n = 1$ para todo i. Esto establece que los valores propios de A son raíces n-ésimas de la unidad. □

2.2. Relaciones de Ortogonalidad

Desde este punto en adelante, el grupo G siempre se asumirá finito. Sea $\varphi\colon G \to GL_n(\mathbb{C})$ una representación. Entonces $\varphi_g = (\varphi_{ij}(g))$ donde $\varphi_{ij}(g) \in \mathbb{C}$ para $1 \leq i, j \leq n$. Así, hay n^2 funciones (pues es una matriz de $n \times n = n^2$) $\varphi_{ij}\colon G \to \mathbb{C}$ asociadas al grado n de representación φ. ¿Qué se puede decir de las funciones φ_{ij} cuando φ es irreducible y unitaria? Resulta que las funciones de este tipo forman una base ortogonal para $\mathbb{C}^G$.

Definición 2.2.1. Álgebra de grupo.

Sea G un grupo, se define

$$L(G) = \mathbb{C}^G = \{f \mid f\colon G \to \mathbb{C}\}.$$

entonces $L(G)$ es un espacio vectorial con producto interno, con operaciones de adición y multiplicación escalar dadas por

$$\begin{aligned} (f_1 + f_2)(g) &= f_1(g) + f_2(g) \\ (cf)(g) &= c \cdot f(g) \end{aligned}$$

y cuyo producto interno está definido por

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

A $L(G)$ se le llamará *álgebra de grupo* de G.

Se probará que $L(G)$ es un producto interno con las operaciones ya antes definidas.

Desarrollo. Sean f_1, f_2 que pertenecen a $L(G)$ y c_1, $c_2 \in \mathbb{C}$ entonces

$$\begin{aligned}
\langle c_1 f_1 + c_2 f_2, f_3 \rangle &= \frac{1}{|G|} \sum_{g \in G} (c_1 f_1 + c_2 f_2)(g)\overline{f_3(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} [(c_1 f_1)(g) + (c_2 f_2)(g)]\,\overline{f_3(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} [c_1 \cdot f_1(g) + c_2 \cdot f_2(g)]\,\overline{f_3(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \left[c_1 \cdot f_1(g)\overline{f_3(g)} + c_2 \cdot f_2(g)\overline{f_3(g)}\right] \\
&= c_1 \cdot \left[\frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_3(g)}\right] + c_2 \cdot \left[\frac{1}{|G|} \sum_{g \in G} f_2(g)\overline{f_3(g)}\right] \\
&= c_1 \cdot \langle f_1(g), f_3(g) \rangle + c_2 \cdot \langle f_2(g), f_3(g) \rangle
\end{aligned}$$

Luego se verifica que

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

Por ultimo se tiene que

$$\begin{aligned}\langle f_1, f_1\rangle &= \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_1(g)}\\ &= \frac{1}{|G|}\sum_{g\in G} |f_1(g)|^2\\ &\geq 0;\text{ será 0 cuando } f_1(g)=0\end{aligned}$$

□

Otro resultado importante para este espacio vectorial es que la dimensión del espacio coincide con el orden del grupo, es decir, $\dim L(G) = |G|$

Desarrollo. Para probarlo tómese $G = \{g_1, \cdots, g_n\}$ tal que $|G| = n$ y se definen las siguientes funciones $f_i = \delta_{\{g_i\}}$ tales que

$$\delta_{\{g_i\}}(g) = \begin{cases} 0 & \text{si } g \neq g_1 \\ 1 & \text{si } g = g_i \end{cases}$$

Debe encontrarse una base para $L(G)$, para ello sea el conjunto formado por las funciones $\{f_1, \cdots, f_n\}$, si se determinará que este conjunto genera el espacio (ya que tienen la misma dimensión que G), podría concluirse lo deseado. Si $f_1, \cdots, f_n$ fuera una base, entonces se debería probar que si $f \in L(G)$ en donde $f\colon G \longrightarrow \mathbb{C}$ y cuya definición esta dada por $z_i = f(g_i) \in \mathbb{C}$, entonces $f = \sum_{i=1}^{n} z_i f_i$ (una función escrita como combinación lineal de elementos de la base) se prueba que estas funciones son exactamente la misma, ya que para todo $g_j \in G$

$$\begin{aligned}\sum_{i=1}^{n} z_i f_i(g_j) &= z_j f_j(g_j);\text{ ya que } f_i(g_j) = 0 \text{ si } i \neq j\\ &= z_j.1\\ &= z_j\\ &= f(g_j)\end{aligned}$$

Efectivamente $f = \sum_{i=1}^{n} z_i f_i$ se cumple, es decir toda f se puede escribir como combinación lineal de las f_i, ahora solo falta probar que son linealmente independientes, puede usarse el producto interno y averiguar si es ortogonal, ya que por ende seria linealmente independiente. Entonces se calcula

$$\begin{aligned}\langle f_i, f_j\rangle &= \frac{1}{|G|}\sum_{g\in G} f_i(g)\overline{f_j(g)}\\ &= 0;\text{ cuando } i \neq j \text{ ya que } f_i(g) \neq 0 \text{ y } f_j(g) = 0\end{aligned}$$

Como es un conjunto linealmente independiente y es base para $L(G)$ se afirma que la dimensión del espacio se corresponde con el orden del grupo. □

Uno de los objetivos de este capítulo es probar el siguiente resultado importante debido a I. Schur. Recuérdese que $U_n(\mathbb{C})$ es un grupo de matrices unitarias de $n \times n$.

(Resultado importante: Relaciones de ortogonalidad de Schur).

Supóngase que $\varphi\colon G \to U_n(\mathbb{C})$[4] y $\rho\colon G \to U_m(\mathbb{C})$ son representaciones unitarias irreducibles no equivalentes. Entonces:

1. $\langle \varphi_{ij}, \rho_{kl} \rangle = 0$;
2. $\langle \varphi_{ij}, \varphi_{kl} \rangle = \begin{cases} 1/n & \text{si } i = k \text{ y } j = l \\ 0 & \text{de lo contrario.} \end{cases}$

La prueba de este teorema requiere de algunas proposiciones que se irán mencionando, hasta que se tengan los prerrequisitos necesarios para afrontar su demostración. Primero se comenzará utilizando nuevamente el "truco de la suma" en la siguiente propisición.

Proposición 2.2.2. *Sean $\varphi\colon G \to GL(V)$ y $\rho\colon G \to GL(W)$ representaciones y supóngase que $T\colon V \to W$ es una transformación lineal. Entonces:*

(a) $T^\sharp = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \rho_{g^{-1}} T \varphi_g \in \mathrm{Hom}_G(\varphi, \rho)$;

(b) Si $T \in \mathrm{Hom}_G(\varphi, \rho)$, entonces $T^\sharp = T$;

(c) El mapeo $P\colon \mathrm{Hom}(V, W) \to \mathrm{Hom}_G(\varphi, \rho)$ definido por $P(T) = T^\sharp$ es una transformación lineal.

Demostración. Se verifica (a) por medio un cálculo directo.

$$T^\sharp \varphi_h = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_g \varphi_h = \frac{1}{|G|} \sum_{g \in G} \rho_{g^{-1}} T \varphi_{gh} \tag{2.1}$$

Se aplica un cambio de variable $x = gh$, considerando que la multiplicación por la derecha de h es una permutación de G [5], ya que g varía con G también lo hace x. Notemos que:

$$\begin{aligned} x &= gh \\ g^{-1}x &= h \\ g^{-1} &= hx^{-1} \end{aligned}$$

[4] Recuérdese que este es el grupo de las matrices unitarias de $n \times n$.

[5] Cualquier producto de este elemento por otro siempre dará un elemento del grupo.

con lo anterior se llega a la conclusión de que el lado derecho de (2.1)

$$\begin{aligned}\frac{1}{|G|}\sum_{x\in G}\rho_{hx^{-1}}T\varphi_x &= \frac{1}{|G|}\sum_{x\in G}\rho_h\rho_{x^{-1}}T\varphi_x\\ &= \rho_h\frac{1}{|G|}\sum_{x\in G}\rho_{x^{-1}}T\varphi_x\\ &= \rho_h T^\sharp\end{aligned}$$

Esto demuestra que $T^\sharp \in \mathrm{Hom}_G(\varphi,\rho)$. Para probar (b), nótese que si $T \in \mathrm{Hom}_G(\varphi,\rho)$, entonces

$$\begin{aligned}T^\sharp &= \frac{1}{|G|}\sum_{g\in G}\rho_{g^{-1}}T\varphi_g\text{; ya que } T\varphi_g = \rho_g T\\ &= \frac{1}{|G|}\sum_{g\in G}\rho_{g^{-1}}\rho_g T\text{; nótese que } \rho_{g^{-1}}\rho_g = \rho_{g^{-1}g} = \rho_e = I_n\\ &= \frac{1}{|G|}\sum_{g\in G}T\text{; observése que la sumatoria es igual a la cantidad de elementos de } G\\ &= \frac{1}{|G|}|G|T\text{; se simplifica y se obtiene}\\ &= T.\end{aligned}$$

Finalmente para (c) se establece la linealidad[(6)] comprobando que

$$\begin{aligned}P(c_1T_1+c_2T_2) &= (c_1T_1+c_2T_2)^\sharp\\ &= \frac{1}{|G|}\sum_{g\in G}\rho_{g^{-1}}(c_1T_1+c_2T_2)\varphi_g\\ &= c_1\frac{1}{|G|}\sum_{g\in G}\rho_{g^{-1}}T_1\varphi_g + c_2\frac{1}{|G|}\sum_{g\in G}\rho_{g^{-1}}T_2\varphi_g\\ &= c_1T_1^\sharp + c_2T_2^\sharp\\ &= c_1P(T_1)+c_2P(T_2).\end{aligned}$$

Si $T \in \mathrm{Hom}_G(\varphi,\rho)$, entonces (b) implica que $T = T^\sharp = P(T)$ y por tanto P es sobreyectiva. □

La siguiente proposición es una variante al lema de Schur y es la forma en la que comúnmente será usado. Esta variante se basa en la observación trivial que si I_n es la matriz

[(6)] Para probar la linealidad recuérdese $f(\alpha x+\beta y) = \alpha f(x)+\beta f(y)$, para α y β escalares.

identidad $n \times n$ y $\lambda \in \mathbb{C}$, entonces

$$\begin{aligned}\operatorname{Tr}(\lambda I_n) &= \sum_{i=1}^{n} \lambda \\ &= \lambda \sum_{i=1}^{n} 1 \\ &= \lambda n\end{aligned}$$

Proposición 2.2.3. *Sean $\varphi\colon G \to GL(V)$, $\rho\colon G \to GL(W)$ representaciones irreducibles de G y sea $T\colon V \to W$ un mapeo lineal. Entonces:*

(a) Si $\varphi \nsim \rho$, entonces $T^{\#} = \{0\}$;

(b) Si $\varphi = \rho$, entonces $T^{\#} = \dfrac{\operatorname{Tr}(T)}{\operatorname{grad}\varphi} I$.

Demostración. Supóngase primero que $\varphi \nsim \rho$. Entonces $\operatorname{Hom}_G(\varphi, \rho) = 0$ por el literal a) del Lema de Schur, asimismo $T^{\sharp} = 0$, ya que $T^{\sharp} \in \operatorname{Hom}_G(\varphi, \rho)$.

Luego se supone a $\varphi = \rho$, por el literal b) del lema de Schur, $T^{\sharp} = \lambda I$ para $\lambda \in \mathbb{C}$ y el objetivo será resolver para este.

Como $T^{\sharp}\colon V \to V$, se tiene

$$\begin{aligned}\operatorname{Tr}(T^{\sharp}) &= \operatorname{Tr}(\lambda I) \\ &= \lambda \operatorname{Tr}(I) \\ &= \lambda \dim V \\ &= \lambda \operatorname{grad}\varphi \\ \Longrightarrow \frac{\operatorname{Tr}(T^{\sharp})}{\operatorname{grad}\varphi} &= \lambda\end{aligned}$$

De lo calculado anteriormente se tiene que $T^{\sharp} = \lambda I = \frac{\operatorname{Tr}(T^{\sharp})}{\operatorname{grad}\varphi} I$.

Por otro lado, también se puede calcular la traza directamente de la definición de $T^{\sharp}$, usando $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$, con lo que se obtiene

$$\begin{aligned}
\operatorname{Tr}(T^\sharp) &= \frac{1}{|G|}\sum_{g\in G}\operatorname{Tr}(\varphi_{g^{-1}}T\varphi_g)\\
&= \frac{1}{|G|}\sum_{g\in G}\operatorname{Tr}(\varphi_{g^{-1}}\varphi_g T)\\
&= \frac{1}{|G|}\sum_{g\in G}\operatorname{Tr}(\varphi_{g^{-1}g}T)\\
&= \frac{1}{|G|}\sum_{g\in G}\operatorname{Tr}(T)\\
&= \frac{|G|}{|G|}\operatorname{Tr}(T)\\
&= \operatorname{Tr}(T)
\end{aligned}$$

y por tanto $T^\sharp = \dfrac{\operatorname{Tr}(T)}{\operatorname{grad}\varphi} I$, como se requería. □

Si $\varphi\colon G \to GL_n(\mathbb{C})$ y $\rho\colon G \to GL_m(\mathbb{C})$ son representaciones, entonces $\operatorname{Hom}(V,W) = M_{mn}(\mathbb{C})$ y $\operatorname{Hom}_G(\varphi,\rho)$ es un subespacio de $M_{mn}(\mathbb{C})$. Por lo tanto el mapeo P de la Proposición 2.2.2 puede ser visto como una transformación lineal $P\colon M_{mn}(\mathbb{C}) \to M_{mn}(\mathbb{C})$. Entonces sería natural calcular la matriz de P con respecto a la base estándar para $M_{mn}(\mathbb{C})$.

Resulta que cuando φ y ρ son representaciones unitarias, la matriz de P tiene una forma especial. Recuérdese que la base estándar para $M_{mn}(\mathbb{C})$ consiste en las matrices $E_{11}, E_{12}, \cdots, E_{mn}$ donde E_{ij} es una matriz de $m \times n$ con 1 en la posición ij y 0 en las demás. Entonces se tiene $(a_{ij}) = \sum_{ij} a_{ij}E_{ij}$.

El siguiente lema es un cálculo directo con la fórmula para la multiplicación de matrices.

Lema 2.2.4. *Sean $A \in M_{rm}(\mathbb{C})$, $B \in M_{ns}(\mathbb{C})$, y $E_{ki} \in M_{mn}(\mathbb{C})$. Entonces la fórmula $(AE_{ki}B)_{\ell j} = a_{\ell k}b_{ij}$ es cierta si $A = (a_{ij})$ y $B = (b_{ij})$.*

Demostración. Si se multiplican las 3 matrices A, B y $C = E_{ki}$ se tendría $ACB = (a_{\ell x})(c_{xy})(b_{yj})$, en donde c_{xy} tiene un 1 en la posición ki, observése que cualquier producto entre los elementos de A o de B por C serán 0, excepto cuando se multiplique por la posición ki. De aquí que cada elemento de la matriz ACB tendrá la forma:

$$\begin{aligned}
(ACB)_{\ell j} &= \sum_{x,y} a_{\ell x}c_{xy}b_{yj}\\
(AE_{ki}B)_{\ell j} &= \sum_{x,y} a_{\ell x}(E_{ki})_{xy}b_{yj}
\end{aligned}$$

Y como $c_{ki} = 1$ entonces todos los términos en esta suma son 0, excepto cuando $x = k$, $y = i$, así solo se tendría:

$$\begin{aligned}(AE_{ki}B)_{\ell j} &= a_{\ell k}E_{ki}b_{ij}\\ &= a_{\ell k}(1)b_{ij}\\ &= a_{\ell k}b_{ij}\end{aligned}$$

□

Ejemplo 2.2.5. Este ejemplo ilustra el Lema 2.2.4:

Desarrollo.

$$\begin{aligned}(a_{ij})E_{ki}(b_{ij}) &= \begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}\\ &= \begin{bmatrix}0 & a_{11}\\ 0 & a_{12}\end{bmatrix}\begin{bmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{bmatrix}\\ &= \begin{bmatrix}a_{11}b_{21} & a_{11}b_{22}\\ a_{21}b_{21} & a_{21}b_{22}\end{bmatrix}.\end{aligned}$$

Lo que también podría haberse encontrado haciendo

$$\begin{aligned}(AE_{12}B)_{11} &= a_{11}b_{21}\\ (AE_{12}B)_{12} &= a_{11}b_{22}\\ (AE_{12}B)_{21} &= a_{21}b_{21}\\ (AE_{12}B)_{22} &= a_{21}b_{22}\end{aligned}$$

□

Los resultados expuestos anteriormente, permiten calcular la matriz P con respecto a la base estándar. Se establece el resultado en la forma en la que se utilizará.

Lema 2.2.6. *Sean $\varphi\colon G \to U_n(\mathbb{C})$ y $\rho\colon G \to U_m(\mathbb{C})$ representaciones unitarias. Sea $A = E_{ki} \in M_{mn}(\mathbb{C})$. Entonces $(A)^{\sharp}_{\ell j} = \langle \varphi_{ij}, \rho_{k\ell}\rangle$.*

Demostración. Ya que ρ es unitario, se cumple que $\rho_{g^{-1}} = \rho_g^{-1} = \rho_g^{*}$[(7)], debido a que ρ es una representación y si se quiere encontrar el inverso de un elemento, se debe buscar su matriz inversa.[(8)][12], así si ρ es la representación y el elemento g está representado por ρ_g entonces g^{-1} está representado por $\rho_{g^{-1}} = \rho_g^{-1}$.

[(7)] Con respecto al producto interno estándar sobre $\mathbb{C}^n$ la transformación lineal asociada a la matriz $A \in GL_n(\mathbb{C})$ es unitaria si y solo si $A^{-1} = A^*$, es decir, el conjugado de A es $\overline{A} = (\overline{a_{ij}})$. El conjugado de la transpuesta de la adjunta de A es la matriz $A^* = A^T$

[(8)] Recuérdese que esta representado como: $g \mapsto \rho_g$ y $g^{-1} \mapsto \rho_{g^{-1}}$

Como cada $\rho_{\ell k}(g^{-1})$ es una raíz n-ésima de la unidad y su inverso coincide con el complejo conjugado, en consecuencia $\rho_{\ell k}(g^{-1}) = \overline{\rho_{k\ell}(g)}$. Teniendo esto en cuenta, se calcula

$$\begin{aligned}(A)^{\sharp}_{\ell j} &= \frac{1}{|G|}\sum_{g\in G}(\rho_{g^{-1}}E_{ki}\varphi_g)_{\ell j}\\ &= \frac{1}{|G|}\sum_{g\in G}\rho_{\ell k}(g^{-1})\varphi_{ij}(g) \text{ por el Lema 2.2.4}\\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\rho_{\ell k}(g)}\varphi_{ij}(g); \text{ ya que } \rho_{\ell k}(g^{-1}) = \overline{\rho_{\ell k}(g)} \text{ y por la Definición 2.2.1de} T^{\sharp}\\ &= \langle \varphi_{ij}, \rho_{k\ell}\rangle\end{aligned}$$

como se quería. □

Observación 2.2.7. *Sea $P\colon M_{mn}(\mathbb{C}) \to M_{mn}(\mathbb{C})$ la transformación lineal dada por $P(T) = T^{\sharp}$ y sea B la matriz de P con respecto a la base estándar para $M_{mn}(\mathbb{C})$. Entonces B es una matriz $mn \times mn$ cuyas filas y columnas son indexados por pares ℓj, ki, donde $1 \leq j$, $k \leq m$ y $1 \leq j$, $i \leq n$. El contenido del Lema 2.2.6 es que las entradas ℓj,ki de B es el producto interno $\langle \varphi_{ij},\ \rho_{k\ell}\rangle = T^{\sharp}$.*

Con los resultados antes propuestos se puede demostrar el teorema de las relaciones de Ortogonalidad de Schur.

Teorema 2.2.8. ***Relaciones de ortogonalidad de Schur.***
Supóngase que $\varphi\colon G \to U_n(\mathbb{C})$ y $\rho\colon G \to U_m(\mathbb{C})$ son representaciones unitarias irreducibles no equivalentes. Entonces:

1. $\langle \varphi_{ij}, \rho_{k\ell}\rangle = 0$;
2. $\langle \varphi_{ij}, \varphi_{k\ell}\rangle = \begin{cases} \frac{1}{n} & \text{si } i = k \text{ y } j = \ell \\ 0 & \text{de lo contrario.}\end{cases}$

Demostración. Se demostrará cada numeral

1. Sea $A = E_{ki} \in M_{mn}\mathbb{C}$, entonces por el Lema 2.2.6

$$\begin{aligned}(A)^{\sharp}_{\ell j} &= \langle \varphi_{ij}, \varphi_{k\ell}\rangle; \text{ ya que } \rho \nsim \varphi\\ &= 0; \text{ por la Proposición 2.2.3}\end{aligned}$$

Por tanto $\langle \varphi_{ij}, \rho_{k\ell}\rangle = 0$.

2. Aplicando la Proposición 2.2.3 y el Lema 2.2.6 considerando $\varphi = \rho$, sea $A = E_{ki} \in M_n(\mathbb{C})$. Entonces

$$\begin{aligned} A^\sharp &= \frac{\operatorname{Tr}(A)}{\operatorname{grad}\varphi} I; \text{ por la Proposición 2.2.3} \\ &= \frac{\operatorname{Tr}(E_{ki})}{n} I; \text{ por definición de } A \end{aligned}$$

El Lema 2.2.6 nos dice que $(A)^\sharp_{\ell j} = \langle \varphi_{ij}, \varphi_{k\ell} \rangle$.

- Supóngase que $j \neq \ell$, entonces dado que $I_{\ell j} = 0$ (ya que tiene valor cuando $\ell = j$, es decir, cuando se toma un elemento de la diagonal), se deduce que $(A)^\sharp_{\ell j} = \langle \varphi_{ij}, \varphi_{k\ell} \rangle = 0$.

- Luego supóngase que $i \neq k$, entonces E_{ki} sólo tendría ceros en la diagonal (recuérdese que la matriz E_{ki} posee un único 1 en la posición ki) y así $\operatorname{Tr}(E_{ki}) = 0$. Así tendríamos nuevamente $(A)^\sharp_{\ell j} = \langle \varphi_{ij}, \varphi_{k\ell} \rangle = 0$.

- Finalmente, para los casos en donde $\ell = j$ e $i = k$, se sabe que E_{ki} tiene un único 1 que dadas las circunstancias estaría en la diagonal y el resto de las entradas serían 0. Por lo tanto $\operatorname{Tr}(E_{ki}) = 1$ y así $(A)^\sharp_{\ell j} = \frac{\operatorname{Tr}(E_{ki})}{n} I = \frac{1}{n}$ y a su vez se deduce que $\langle \varphi_{ij}, \varphi_{k\ell} \rangle = \frac{1}{n}$.

Con lo anterior se demuestra el teorema. □

Una simple renormalización establece:

Corolario 2.2.9. *Sea φ una representación unitaria irreducible de G de grado d. Entonces las d^2 funciones $\{\sqrt{d}\varphi_{ij} \mid 1 \leqslant i, j \leqslant d\}$ forman un conjunto ortonormal.*

Demostración. Hay que probar que el producto interno $\langle \sqrt{d}\varphi_{ij}, \sqrt{d}\varphi_{ij} \rangle = 1$, para que sean normales, entonces

$$\begin{aligned} \langle \sqrt{d}\varphi_{ij}, \sqrt{d}\varphi_{ij} \rangle &= \sqrt{d}\langle \varphi_{ij}, \sqrt{d}\varphi_{ij} \rangle; \text{ utilizando la linealidad conjugada por la derecha} \\ &= \left(\sqrt{d}\right)\left(\sqrt{d}\right)\langle \varphi_{ij}, \varphi_{ij} \rangle \\ &= \left(\sqrt{d}\right)^2 \langle \varphi_{ij}, \varphi_{ij} \rangle \\ &= d\langle \varphi_{ij}, \varphi_{ij} \rangle; \text{ por Teorema 2.2.8} \\ &= d\left(\frac{1}{d}\right) \\ &= 1 \end{aligned}$$

Como los elementos se han tomado arbitrarios y la ortogonalidad se sigue del teorema anterior, se concluye que es un conjunto ortonormal. □

Un resultado importante del Teorema 2.2.8 podría ser que hay que hay un número finito de clases de equivalencia de representaciones irreducibles de G, ya que por el Teorema de Maschke se sabe que si φ es una representación unitaria entonces puede particionarse en representaciones irreducibles unitarias y cada una de ellas pertenecerán a distintas clases de equivalencia, además se sabe que $\dim L(G) = |G|$, es decir, ningún conjunto de vectores linealmente independiente de $L(G)$ podrá tener más de $|G|$ elementos. Por otro lado las Relaciones de Ortogonalidad de Schur dicen que las entradas de representaciones unitarias no equivalentes de G forman un conjunto ortogonal de vectores no nulos en $L(G)$, con esto se tendría que la cantidad de clases de equivalencia sería a lo sumo $|G|$. De la discusión anterior se puede deducir que G tiene como máximo $|G|$ clases de equivalencia de representaciones irreducibles. Ahora si se toma a $\varphi^{(1)}, \cdots, \varphi^{(s)}$ como representantes de cada una de las clases tomadas anteriormente y si se forma un conjunto completo de representantes de las clases de representaciones irreducibles de G y se define como $d_i = \operatorname{grad} \varphi^{(i)}$, entonces por las Relaciones de Ortogonalidad de Schur y el Corolario 2.2.9 cada una de las d^2 funciones de cada una de las representaciones irreducibles d_k^2 representadas por $\sqrt{d_k}\varphi_{ij}^{(k)}$ serán ortonormales entre si.

Entonces el conjunto de las $d_1^2 + d_2^2 + \cdots + d_s^2$ funciones representadas como $\{\sqrt{d_k}\varphi_{ij}^{(k)} \mid 1 \leq k \leq s, 1 \leq i, j \leq d_k\}$, si se toman dos representaciones por el numeral 1 del Teorema de Schur, formarían un conjunto ortonormal de vectores en $L(G)$ entre si y por lo tanto $s \leq d_1^2 + \cdots + d_s^2 \leq |G|$, ya que hay por lo menos un representante en cada clase, se tiene s representantes y por tanto el grado de una de las representaciones estará entre $1 \leq k \leq s$ porque $d_i \geq 1$ para todo i, además nótese que no pueden ser más que la dimensión del espacio por lo que se ha discutido, de aquí que las cotas sean s y $|G|$.

Esta discusión se resume en la siguiente proposición.

Proposición 2.2.10. *Sea G un grupo finito. Sean $\varphi^{(1)}, \ldots, \varphi^{(s)}$ un conjunto completo de representantes de las clases de equivalencia de las representaciones irreducibles de G y el conjunto $d_i = \operatorname{grad} \varphi^{(i)}$. Entonces las funciones*

$$\{\sqrt{d_k}\varphi_{ij}^{(k)} \mid 1 \leqslant k \leqslant s, 1 \leqslant i, j \leqslant d_k\}$$

forman un conjunto ortonormal en $L(G)$ y por lo tanto $s \leqslant d_1^2 + \cdots + d_s^2 \leqslant |G|$.

Más adelante, se verá que la segunda desigualdad en la proposición es, de hecho, una igualdad; la primera es sólo una igualdad para los grupos abelianos.

2.3. Caracteres y Funciones de Clase

En este capítulo se probará la unicidad de la descomposición de una representación en representaciones irreducibles. El ingrediente clave es asociar a cada representación φ una función $\chi_\varphi \colon G \to \mathbb{C}$ que codifica toda la representación.

Definición 2.3.1. Carácter.

Sea $\varphi\colon G \to GL(V)$ una representación. El carácter $\chi_\varphi\colon G \to \mathbb{C}$ de φ se define estableciendo $\chi_\varphi(g) = \mathrm{Tr}(\varphi_g)$. El carácter de una representación irreducible es llamado un *carácter irreducible*.

Entonces si $\varphi\colon G \to GL_n(\mathbb{C})$ es una representación dada por $\varphi_g = (\varphi_{ij}(g))$, entonces

$$\chi_\varphi(g) = \sum_{i=1}^{n} \varphi_{ii}(g).$$

En general para calcular el carácter de una representación, debe escogerse una base y por tanto cuando se hable de caracteres se asumirá sin pérdida de generalidad que se refieren también a la matrices de representación. Véanse a continuación algunas generalidades de los caracteres.

Observación 2.3.2. *Si $\varphi\colon G \to \mathbb{C}^*$ es una representación de grado 1, entonces $\chi_\varphi = \varphi$. A partir de ahora, no se distinguirá entre una representación de grado 1 y su carácter.*

La primero que debe saberse del carácter es el grado de la representación.

Proposición 2.3.3. *Sea φ una representación de G. Entonces $\chi_\varphi(1) = \operatorname{grad}\varphi$.*

Demostración. En efecto, supóngase que $\varphi\colon G \to GL(V)$ es una representación. Entonces calculando la traza del elemento identidad

$$\begin{aligned}\chi_\varphi(1) &= \mathrm{Tr}(\varphi_1)\\ &= \mathrm{Tr}(I)\\ &= \dim V\\ &= \operatorname{grad}\varphi\end{aligned}$$

□

Una propiedad de los caracteres que es clave es que dependen únicamente de las clases de equivalencia de la representación.

Proposición 2.3.4. *Si φ y ρ son representaciones equivalentes, entonces $\chi_\varphi = \chi_\rho$.*

Demostración. Dado que la traza se calcula mediante la selección de una base, se puede asumir que $\varphi, \rho\colon G \to GL_n(\mathbb{C})$. Entonces, como las representaciones son equivalentes, existe una matriz invertible $T \in GL_n(\mathbb{C})$ tal que $\varphi_g = T\rho_g T^{-1}$, para todo $g \in G$. Recuérdese que $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, entonces

$$\begin{aligned}\chi_\varphi(g) &= \mathrm{Tr}(\varphi_g)\\ &= \mathrm{Tr}(T\rho_g T^{-1})\\ &= \mathrm{Tr}(T^{-1}T\rho_g);\ \text{usando } \mathrm{Tr}(AB) = \mathrm{Tr}(BA) \text{ donde } A = T\rho_g \text{ y } B = T^{-1}\\ &= \mathrm{Tr}(\rho_g)\\ &= \chi_\rho(g)\end{aligned}$$

como se quería. □

Esencialmente la misma prueba permite otra propiedad crucial de los caracteres que son constantes sobre las clases conjugadas.

Proposición 2.3.5. *Sea φ una representación de G. Entonces, para todo $g, h \in G$, se cumple la igualdad $\chi_\varphi(g) = \chi_\varphi(hgh^{-1})$.*

Demostración. En efecto, se calcula

$$\begin{aligned}
\chi_\varphi(hgh^{-1}) &= \mathrm{Tr}(\varphi_{hgh^{-1}}); \text{ por el homomorfismo} \\
&= \mathrm{Tr}(\varphi_h\varphi_g\varphi_h^{-1}); \text{ por propiedad de la traza, haciendo } A = \varphi_h\varphi_g \text{ y } B = \varphi_h^{-1} \\
&= \mathrm{Tr}(\varphi_h^{-1}\varphi_h\varphi_g) \\
&= \mathrm{Tr}(\varphi_{h^{-1}}\varphi_h\varphi_g) \\
&= \mathrm{Tr}(\varphi_{h^{-1}h}\varphi_g) \\
&= \mathrm{Tr}(\varphi_g) \\
&= \chi_\varphi(g)
\end{aligned}$$

□

Las funciones que son constantes en las clases conjugadas juegan un papel importante en la TRG (Teoría de Representación de Grupos) y, por tanto, merecen un nombre propio.

Definición 2.3.6. Función de clase.

Una función $f\colon G \to \mathbb{C}$ es llamada una *función de clase* si $f(g) = f(hgh^{-1})$ para todo $g, h \in G$, o de forma equivalente si f es constante sobre las clases conjugadas de G. El espacio de las funciones de clase es denotado por $Z(L(G))$.

En particular, los caracteres son funciones de clases, la notación $Z(L(G))$ sugiere que las funciones de clases deberían ser el centro de algún anillo y de hecho esto será el caso. Si $f\colon G \to \mathbb{C}$ es una función de clase y C es la clase de conjugación, $f(C)$ denotará el valor constante que f toma sobre C.

Proposición 2.3.7. *$Z(L(G))$ es un subespacio de $L(G)$.*

Demostración. Sean f_1, f_2 funciones de clase sobre G y sea c_1, $c_2 \in \mathbb{C}$. Entonces utilizando la Definición 2.3.6 y la caracterización para los subespacios, se tiene:

$$\begin{aligned}
(c_1f_1 + c_2f_2)(hgh^{-1}) &= c_1f_1(hgh^{-1}) + c_2f_2(hgh^{-1}); \ f_1 \text{ y } f_2 \text{ son funciones de clase} \\
&= c_1f_1(g) + c_2f_2(g) \\
&= (c_1f_1 + c_2f_2)(g)
\end{aligned}$$

lo que muestra que $c_1f_1 + c_2f_2$ es una función de clase, por tanto es un subespacio. □

A continuación, se calculará la dimensión de $Z(L(G))$, para ello, sea $Cl(G)$ el conjunto de clases conjugadas de G. Para $C \in Cl(G)$, se define la función $\delta_C\colon G \to \mathbb{C}$ (función característica) con regla de asignación:

$$\delta_C(g) = \begin{cases} 1, & \text{si } g \in C \\ 0, & \text{si } g \notin C \end{cases}$$

Proposición 2.3.8. *El conjunto* $B = \{\delta_C \mid C \in Cl(G)\}$ *es una base para* $Z(L(G))$. *En consecuencia,* $\dim Z(L(G)) = |Cl(G)|$.

Demostración. Nótese que cada δ_C por definición es constante en las clases conjugadas y por lo tanto es una función de clase. Se comenzará por mostrar que B genera a $Z(L(G))$.

Si $f \in Z(L(G))$, se verificará que $f = \sum_{C \in Cl(G)} f(C)\delta_C$, para ello, sea C' la clase conjugada de g entonces

$$\begin{aligned}\sum_{C \in Cl(G)} f(C)\delta_C(g) &= f(C')\delta_{C'}(g);\ \text{se evalúa en } g \text{ porque es de interés } C' \\ &= f(C')1;\ \text{como } g \in C' \Rightarrow \delta_{C'}(g) = 1 \\ &= f(g);\ ;\ \text{por definición } f(C') = f(g)\end{aligned}$$

entonces $f = \sum_{C \in Cl(G)} f(C)\delta_C$, por lo tanto δ_C genera a las funciones de clase.

Para establecer la independencia lineal, se verificará que B es un conjunto ortogonal de vectores distintos de cero, ya que la ortogonalidad implica independencia lineal. Sean C, $C' \in Cl(G)$, entonces

$$\langle \delta_C, \delta_{C'} \rangle = \frac{1}{|G|} \sum_{g \in G} \delta_C(g)\overline{\delta_{C'}(g)}$$

Observése que se obtendrán dos tipos de resultados que dependerán de la pertenencia de g a las clases C o C' por la definición de la función característica. Por ello, obtendremos un resultado diferente de cero, solo cuando las clases sean iguales y así

$$\sum_{g \in G} \delta_C(g)\overline{\delta_{C'}(g)} = \sum_{g \in C} 1 = |C|$$

reescribiendo se tiene

$$\langle \delta_C, \delta_{C'} \rangle = \begin{cases} |C|/|G|, & C = C'; \text{ si pertenece a ambos, entonces son iguales} \\ 0, & ;\ \text{si } C \neq C'; \text{ entonces } g \in C' \text{ y } g \notin C \text{ o viceversa} \end{cases}$$

Esto completa la demostración de que B es una base.

Ahora para calcular la dimensión, observése que por los cálculos anteriores se tiene tantas clases conjugadas como elementos de la base, es decir, $|B| = |Cl(G)|$, por otro lado como B es una base entonces $\dim(Z(L(G))) = |B| = |Cl(G)|$ □

El siguiente teorema es uno de los resultados fundamentales en Teoría de Representaciones de Grupos. Este muestra que los caracteres irreducibles forman un conjunto ortonormal de funciones de clase. Este resultado se utilizará para establecer la unicidad de la descomposición de una representación en componentesirreducibles y calcular exactamente el número de clases de equivalencia de representaciones irreducibles.

Teorema 2.3.9. ***(Primeras relaciones de Ortogonalidad).***

Sean φ, ρ representaciones irreducibles de G. Entonces

$$\langle \chi_\varphi, \chi_\rho \rangle = \begin{cases} 1, & si\ \varphi \sim \rho \\ 0, & si\ \varphi \nsim \rho \end{cases}$$

Por tanto los caracteres irreducibles de G forman un conjunto ortonormal de funciones de clases.

Demostración. Por la Proposición 1.2.4, supóngase sin pérdida de generalidad que dados φ_1 y ρ_1 dos representaciones irreducibles, existen φ y ρ representaciones unitarias tales que $\varphi_1 \sim \varphi$ y $\rho_1 \sim \rho$, tales que $\varphi\colon G \to U_n(\mathbb{C})$ y $\rho\colon G \to U_m(\mathbb{C})$. Por la Proposición 2.3.4 se tiene que $\chi_{\varphi_1} = \chi_\varphi$ y $\chi_{\rho_1} = \chi_\rho$. De aquí que se puede calcular

$$\begin{aligned}
\langle \chi_\varphi, \chi_\rho \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g) \overline{\chi_\rho(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^{n} \varphi_{ii}(g) \right) \left(\sum_{j=1}^{m} \overline{\rho_{jj}}(g) \right) \text{; por Definición 2.3.1 para } \varphi \text{ y } \rho \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \left(\varphi_{ii}(g) \sum_{j=1}^{m} \overline{\rho_{jj}}(g) \right) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^{n} \sum_{j=1}^{m} \varphi_{ii}(g) \overline{\rho_{jj}}(g) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{m} \left(\frac{1}{|G|} \sum_{g \in G} \varphi_{ii}(g) \overline{\rho_{jj}(g)} \right) \text{; nótese que es la definición de producto interno} \\
&= \sum_{i=1}^{n} \sum_{j=1}^{m} \langle \varphi_{ii}(g), \rho_{jj}(g) \rangle
\end{aligned}$$

Las relaciones de ortogonalidad de Schur (Teorema 2.2.8) verifican que $\langle \varphi_{ii}(g), \rho_{jj}(g) \rangle = 0$ [(9)] si $\varphi \nsim \rho$ y por lo tanto $\langle \chi_\varphi, \chi_\rho \rangle = 0$.

Si $\varphi \sim \rho$ en este caso, las relaciones de ortogonalidad de Schur establecen que:

$$\langle \varphi_{ii}, \varphi_{jj} \rangle = \begin{cases} 1/n, & i = j \\ 0, & i \neq j \end{cases}$$

[(9)] De hecho es válido para cualquier índice.

y por tanto de

$$\begin{aligned}\langle \chi_\varphi, \chi_\rho \rangle &= \langle \chi_\varphi, \chi_\varphi \rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}\langle \varphi_{ii}, \varphi_{jj}\rangle \text{ solo es de interés los } \langle \varphi_{ii}, \varphi_{jj}\rangle \neq 0, \text{ es decir, los de índices iguales} \\ &= \sum_{i=1}^{n}\langle \varphi_{ii}, \varphi_{ii}\rangle \\ &= \sum_{i=1}^{n}\frac{1}{n} \\ &= 1\end{aligned}$$

como se requería. □

Corolario 2.3.10. *Hay a lo sumo $|Cl(G)|$ clases de equivalencia de representaciones irreducibles de G.*

Demostración. Nótese que el teorema recién demostrado (Teorema 2.3.9) implica que las representaciones irreducibles no equivalentes tienen caracteres diferentes y, más aún, los caracteres irreducibles forman un conjunto ortonormal en $Z(L(G))$. Como $\dim Z(L(G)) = |Cl(G)|$ (por la Propiedad 2.3.8) y los conjuntos ortonormales son linealmente independientes, entonces a lo sumo puede tener el tamaño de la base, es decir, $|Cl(G)|$ elementos. □

Definición 2.3.11. Multiplicidad.

Si V es un espacio vectorial, φ es una representación y $m > 0$, entonces se establece

$$mV = V \oplus \overbrace{\cdots}^{\times m} \oplus V \text{ y } m\varphi = \varphi \oplus \overbrace{\cdots}^{\times m} \oplus \varphi$$

Ahora si $\rho \sim m_1\varphi^{(1)} \oplus m_2\varphi^{(2)} \oplus \cdots \oplus m_s\varphi^{(s)}$, entonces m_i es llamada la multiplicidad de $\varphi^{(i)}$ en ρ. Si $m_i > 0$, entonces se dice que $\varphi^{(i)}$ es un componente irreducible de ρ.

Sea $\varphi^{(1)}, \cdots, \varphi^{(s)}$ un conjunto completo de representaciones unitarias irreducibles de G, salvo equivalencia. Nuevamente se establece $d_i = \operatorname{grad}\varphi^{(i)}$.

En este momento no puede afirmarse que la multiplicidad está bien definida, ya que todavía no se ha establecido la unicidad de la descomposición de una representación en irreducibles, ya que se ha visto que una representación puede ser equivalente a la suma directa de representaciones irreducibles, pero no se ha dicho hasta este momento si está representación es única. Para demostrar que está bien definido, se encontró una forma de calcular la multiplicidad directamente del carácter de ρ. Dado que el carácter sólo depende de la clase de equivalencia, se deduce que la multiplicidad de $\varphi^{(i)}$ será la misma sin importar como se descomponga, ya que $\rho \sim \bigoplus m_i\varphi^{(i)}$ entonces por la Proposición 2.3.4 $\chi_\rho = \chi_{\bigoplus m_i\varphi^{(i)}}$.

Observación 2.3.12. *Si* $\rho \sim m_1\varphi^{(1)} \oplus m_2\varphi^{(2)} \oplus \cdots m_s\varphi^{(s)}$, *entonces*

$$\operatorname{grad}\rho = m_1d_1 + m_2d_2 + \cdots m_sd_s$$

donde se ha conservado la notación anterior.

Lema 2.3.13. *Sea* $\varphi = \rho \oplus \psi$ *con* ρ *y* ψ *irreducibles. Entonces* $\chi_\varphi = \chi_\rho + \chi_\psi$.

Demostración. Supóngase que $\rho\colon G \to GL_n(\mathbb{C})$ y $\psi\colon G \to GL_m(\mathbb{C})$. Entonces $\varphi\colon G \to GL_{n+m}(\mathbb{C})$ tiene la forma:

$$\varphi_g = \begin{bmatrix} \rho_g & 0 \\ 0 & \psi_g \end{bmatrix}.$$

Como la traza es la suma de los elementos diagonales, se deduce que

$$\begin{aligned} \chi_\varphi(g) &= \operatorname{Tr}(\varphi_g); \text{ ya que } \varphi = \rho \oplus \psi \\ &= \operatorname{Tr}(\rho_g) + \operatorname{Tr}(\psi_g) \text{ esto se debe a que son matrices cuadradas} \\ &= \chi_\rho(g) + \chi_\psi(g). \end{aligned}$$

De donde se concluye que $\chi_\varphi = \chi_\rho + \chi_\psi$. □

El lema anterior implica que cada carácter es una combinación lineal entera de caracteres irreducibles. Puede utilizarse la ortonormalidad de los caracteres irreducibles para extraer los coeficientes.

Teorema 2.3.14. *Sea* $\varphi^{(1)}, \cdots, \varphi^{(s)}$ *un conjunto completo de representantes de las clases de equivalencia de las representaciones irreducibles de* G *y sea*

$$\rho \sim m_1\varphi^{(1)} \oplus m_2\varphi^{(2)} \oplus \cdots \oplus m_s\varphi^{(s)}$$

Entonces $m_i = \langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle$ *y la descomposición de* ρ *en componentes irreducibles es única y la representación de* ρ *está determinada, salvo equivalencias, por su carácter.*

Demostración. Se sabe que $\rho \sim m_1\varphi^{(1)} \oplus m_2\varphi^{(2)} \oplus \cdots \oplus m_s\varphi^{(s)}$ (una descomposición cualquiera), si se aplica el Lema 2.3.13 se tiene que $\chi_\rho = m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}$. Se sustituye lo anterior en $\langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle$ y se utilizan las Primeras Relaciones de Ortogonalidad, a fin de encontrar m_i, que como se verá solo depende del carácter de ρ (ni siquiera depende de los componentes, ni de la descomposición) y de sus representantes. Entonces se tiene que:

$$\langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle = \langle m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}, \chi_{\varphi^{(i)}} \rangle$$

Utilizando la linealidad por la izquierda del producto interno:

$$\begin{aligned} \langle m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}, \chi_{\varphi^{(i)}} \rangle &= m_1\langle \chi_{\varphi^{(1)}}, \chi_{\varphi^{(i)}} \rangle + \cdots + m_s\langle \chi_{\varphi^{(s)}}, \chi_{\varphi^{(i)}} \rangle \\ &= m_i \end{aligned}$$

Este calculo resulta de considerar que $\langle \chi_{\varphi^{(j)}}, \chi_{\varphi^{(i)}} \rangle$ es igual a 0 o 1, por las primeras Relaciones de Ortogonalidad, entonces cuando cuando $i = j$ el producto interno dará 1, así se tiene que $\langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle = m_i$.

Para probar que la descomposición de ρ en componentes irreducibles es única, se utiliza otra descomposición para la representación, sea $\rho \sim n_1\varphi^{(1)} \oplus n_2\varphi^{(2)} \oplus \cdots \oplus n_s\varphi^{(s)}$ con lo cual $\chi_\rho = n_1\chi_{\varphi^{(1)}} + \cdots + n_s\chi_{\varphi^{(s)}}$, a través de un calculo similar al mostrado se llega a la conclusión de que $\langle \chi_\rho, \chi_{\varphi^{(i)}} \rangle = n_i$, entonces $m_i = n_i$, por lo tanto es única, con lo cual ρ esta determinada salvo equivalencia por su carácter, porque se basa solo en el carácter de la representación. □

El Teorema 2.3.14 ofrece un criterio práctico para comprobar si una representación es irreducible.

Corolario 2.3.15. *Una representación ρ es irreducible si y solo si $\langle \chi_\rho, \chi_\rho \rangle = 1$*

Demostración. "$\Longrightarrow$"La implicación directa se cumple ya que si ρ es irreducible entonces por el Teorema 2.3.9 se cumple que $\langle \chi_\rho, \chi_\rho \rangle = 1$.

"$\Longleftarrow$"

Para la otra implicación supóngase que $\rho \sim m_1\varphi^{(1)} \oplus m_2\varphi^{(2)} \oplus \cdots \oplus m_s\varphi^{(s)}$ y por tanto $\chi_\rho = m_1\chi_{\varphi^{(1)}} + \cdots + m_s\chi_{\varphi^{(s)}}$.

Usando la ortonormalidad de los caracteres irreducibles se obtiene

$$\begin{aligned}
\langle \chi_\rho, \chi_\rho \rangle &= \langle \sum_{i=1}^{s} m_i\chi_{\varphi^{(i)}}, \sum_{i=1}^{s} m_i\chi_{\varphi^{(i)}} \rangle \\
&= \sum_{j=1}^{s} m_j \langle \chi_{\varphi^{(j)}}, \sum_{i=1}^{s} m_i\chi_{\varphi^{(i)}} \rangle \text{; utilizando la linealidad por la izquierda} \\
&= \sum_{j=1}^{s}\sum_{i=1}^{s} m_j\overline{m_i}\langle \chi_{\varphi^{(j)}}, \chi_{\varphi^{(i)}} \rangle \text{; utilizando la linealidad conjugada por la derecha}
\end{aligned}$$

es de interés cuando $i = j$ ya que el producto interno dará 1 por el Teorema 2.3.9, entonces

$$\begin{aligned}
\langle \chi_\rho, \chi_\rho \rangle &= \sum_{i=1}^{s} m_i\overline{m_i}\langle \chi_{\varphi^{(i)}}, \chi_{\varphi^{(i)}} \rangle \\
&= m_1^2 + \cdots + m_s^2
\end{aligned}$$

Ahora, como los m_i son números enteros no negativos, se observa que $\langle \chi_\rho, \chi_\rho \rangle = 1$ e implica que

$$\sum_{i=1}^{s} m_i^2 \leq 1 \Rightarrow \forall i \text{ se cumple que } m_i^2 \leq 1 \Rightarrow m_1 = 0, 1 \Rightarrow \exists j \text{ tal que } m_j = 1 \Rightarrow \sum_{i=1, i\neq j}^{s} m_i^2 = 0$$

de aquí que $m_j = 1$ y $m_i = 0$ para $i \neq j$. Con esto se probó que $\rho \sim 1.\varphi^{(j)}$, es decir, una representación irreducible y por el Lema 1.1.28, también ρ será irreducible.

□

Se utilizará el corolario anterior para demostrar que la representación del Ejemplo 1.1.17 es irreducible.

Ejemplo 2.3.16. Sea ρ la representación de S_3 del Ejemplo 1.1.17, entonces ρ es irreducible.

Desarrollo. Ya que Id, (12) y (123) forman un conjunto completo de las representantes de las clases de conjugación de S_3, ya estos poseen la misma estructura de ciclo, es decir los que tienen longitud 1, longitud 2 y longitud 3. Observése que podemos utilizar el Corolario 2.3.15 para calcular el producto interno $\langle \chi_\rho, \chi_\rho \rangle$ de los valores del carácter de estos elementos.

$$\rho(Id) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad ; \quad \rho(1\ 2) = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \quad ; \quad \rho(1\ 2\ 3) = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

Ahora $\chi_\rho(Id) = 2$, $\chi_\rho((12)) = 0$ y $\chi_\rho((123)) = -1$.[(10)] Por otro lado $\dfrac{1}{|G|} = \dfrac{1}{|S_3|} = \dfrac{1}{6}$, ya que el grupo es S_3 y el orden del grupo es $3! = 6$. Por último debe calcularse el producto interno:

$$\begin{aligned}
\langle \chi_\rho, \chi_\rho \rangle &= \frac{1}{|S_3|} \sum_{g \in S_3} \chi_\rho(g)\overline{\chi_\rho(g)} \\
&= \frac{1}{6} \sum_{g \in S_3} \chi_\rho^2(g); \text{ ya que } \chi_\rho(g) = \overline{\chi_\rho(g)} \\
&= \frac{1}{6} \left[\chi_\rho^2(Id) + \chi_\rho^2(12) + \chi_\rho^2(13) + \chi_\rho^2(23) + \chi_\rho^2(123) + \chi_\rho^2(132)\right] \\
&= \frac{1}{6} \left[\chi_\rho^2(Id) + 3\chi_\rho^2(12) + 2\chi_\rho^2(123)\right]; \text{ ya que } \chi_\rho^2(12) = \chi_\rho^2(13) = \chi_\rho^2(23) \text{ y } \chi_\rho^2(123) = \chi_\rho^2(132) \\
&= \frac{1}{6} \left(2^2 + 3 \cdot 0^2 + 2 \cdot (-1)^2\right) \\
&= \frac{1}{6}(6) \\
&= 1.
\end{aligned}$$

Como ρ es una representación de S_3 hay tres transposiciones y dos 3-ciclos, además de la identidad, por ello queda de la forma expresada. Como el producto interno $\langle \chi_\rho, \chi_\rho \rangle = 1$, entonces ρ es irreducible por el Corolario 2.3.15. □

Se tratará de encontrar todos los caracteres irreducibles de S_3 y descomponer la representación estándar (véase el Ejemplo 1.1.10) en irreducibles en el siguiente ejemplo.

[(10)] Recuérdese que para calcular el carácter debe de calcularse la traza de la matriz de representación.

Ejemplo 2.3.17. Buscar los caracteres de S_3

Desarrollo. Sabemos que S_3 admite el carácter trivial $\chi_1 \colon S_3 \to \mathbb{C}^*$ dada por $\chi_1(\sigma) = 1$ para todo $\sigma \in S_3$ (recuérdese que se identificó una representación de grado uno con su carácter). También se tiene el carácter χ_3 de la representación irreducible del Ejemplo 1.1.17, que se calculó en el ejemplo anterior.

Como S_3 tiene tres clases de conjugación, por el Corolario 2.3.10 se puede esperar que existan tres representaciones irreducibles no equivalentes de S_3, porque serán a lo sumo la cantidad de clases conjugadas.

De acuerdo a la Proposición 2.2.10, se sabe que si d es el grado de la representación que falta (porque ya se calcularon χ_1 y χ_3), entonces se utiliza la Proposición 2.2.10 para saber el grado de la representación, entonces se tiene $1^2+d^2+2^2 \leq 6$, de aquí que el único valor posible para d es $d = 1$, para que la suma de los cuadrados de los grados de las representaciones sea menor o igual a 6. Entonces para definir una segunda representación de grado uno (porque ya se tiene a la identidad que también era de grado uno) se tiene:

$$\chi_2(\sigma) = \begin{cases} 1, & \sigma \text{ es par} \\ -1, & \sigma \text{ es impar} \end{cases}$$

Con la información obtenida en el Ejemplo 2.3.16 y lo obtenido anteriormente se ha encontrado que es una descomposición de la representación estándar en irreducibles y se ha encontrado que un conjunto completo de representantes de las clases de equivalencia, puede formar una tabla que codifique esta información a la que se conocerá como *tabla de carácter*. En la tabla las filas corresponderán a los caracteres irreducibles, mientras que las columnas corresponderán con los representantes de clases conjugadas.

En la Tabla 2.1 se resumirá la información obtenida en los ejemplos antes mencionados.

Tabla 2.1: Tabla de carácter de S_3

	Id	(1 2)	(1 2 3)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

La representación estándar de S_3 del Ejemplo 1.1.10 está dada por las matrices

$$\varphi_{(12)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \varphi_{(123)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Por lo tanto se puede representar los valores del carácter en la Tabla 2.2, alternativamente se puede usar el Teorema 2.3.14 para obtener los resultados mostrados en dicha tabla.

$$\langle \chi_\varphi, \chi_1 \rangle = \frac{1}{6}(3 + 3 \cdot 1 + 2 \cdot 0) = 1$$
$$\langle \chi_\varphi, \chi_2 \rangle = \frac{1}{6}(3 + 3 \cdot (-1) + 2 \cdot 0) = 0$$
$$\langle \chi_\varphi, \chi_3 \rangle = \frac{1}{6}(6 + 3 \cdot 0 + 2 \cdot 0) = 1$$

Tabla 2.2: Tabla de carácter de χ_φ

	Id	(1 2)	(1 2 3)
χ_φ	3	1	0

Nótese que la Tabla 2.2 muestra que $\chi_\varphi = \chi_1 + \chi_3$ y por lo tanto $\varphi \sim \chi_1 \oplus \rho$, como se había mencionado en el Ejemplo 1.1.17. □

Se estudiará la tabla de caracteres en detalle más adelante, en particular, vamos a demostrar que las columnas son siempre por pares ortogonales, como es el caso en la Tabla 2.1.

2.4. La Representación Regular

El teorema de Cayley afirma que G es isomorfo a un subgrupo de S_n donde $n = |G|$. La representación estándar del Ejemplo 1.1.10 proporciona una representación $\varphi\colon S_n \to GL_n(\mathbb{C})$; a la restricción de esta representación a G, visto como un subgrupo de S_n, se le llamará *representación regular de* G, aunque se construirá formalmente de una manera diferente.

Sea X un conjunto finito, se construye el espacio vectorial con base X, utilizando sumas formales de elementos en X, haciendo

$$\mathbb{C}X = \left\{ \sum_{x \in X} c_x x \mid c_x \in \mathbb{C} \right\}.$$

En donde c_x son complejos que dependen de x, así $\mathbb{C}X$ consta de todas las combinaciones lineales de elementos de X.

Dos elementos $\sum_{x \in X} a_x x$ y $\sum_{x \in X} b_x x$ se dice que son iguales si y sólo si $a_x = b_x$ para todo $x \in X$.

La adición está definida por

$$\sum_{x\in X} a_x x + \sum_{x\in X} b_x x = \sum_{x\in X} (a_x + b_x)x$$

La multiplicación escalar se define de manera similar

$$\sum_{x\in X} k a_x x = k \sum_{x\in X} a_x x$$

Se identifica a $x \in X$ con la combinación lineal $1 \cdot x$ en donde X es una base para $\mathbb{C}X$, como ya se ha dicho. El producto interno puede ser definido sobre $\mathbb{C}X$ de la siguiente forma:

$$\left\langle \sum_{x\in X} a_x x, \sum_{x\in X} b_x x \right\rangle = \sum_{x\in X} a_x \overline{b_x}$$

Definición 2.4.1. Representación regular.

Sea G un grupo finito. La *representación regular* de G es el homomorfismo: $L\colon G \to GL(\mathbb{C}G)$ definido por

$$L_g \sum_{h\in G} c_h h = \sum_{h\in G} c_h gh = \sum_{x\in G} c_{g^{-1}x} x,$$

Para $g \in G$ (donde la ultima igualdad proviene del cambio de variables de $x = gh \Rightarrow h = g^{-1}x$). Con lo que ha hecho se esta probando que esta bien definido, es decir, se esta trabajando con el grupo general lineal y esas son transformaciones lineales adentro, al final lo que se consigue es el conocimiento para trabajar un elemento de este tipo y hacia donde se mapea.

La L aquí significa "izquierda", es decir operar por la izquierda. Observése que sobre un elemento base $h \in G$, L opera como $L_g h = gh$, es decir, L_g actúa sobre la base a través de la multiplicación por la izquierda del elemento g. La definición anterior proporciona una fórmula para un operador lineal que actúa sobre una combinación lineal de vectores base, dada la acción sobre la base. De ello se deduce que L_g es un mapeo lineal para todo $g \in G$. La representación regular nunca es irreducible cuando G no es trivial, pero tiene la característica que contiene todas las representaciones irreducibles de G como componentes. Primero se demostrará que es una representación.

Proposición 2.4.2. *La representación regular es una representación unitaria de G.*

Demostración. Ya hemos señalado que el mapeo L_g es lineal para $g \in G$. Además si g_1, $g_2 \in G$ y $h \in G$ es un elementos base de $\mathbb{C}G$, entonces

$$\begin{aligned} L_{g_1} L_{g_2} h &= L_{g_1 g_2 h} \\ &= g_1 g_2 h \\ &= L_{g_1 g_2} h \end{aligned}$$

de modo que L es un homomorfismo. Si se demuestra que L_g es unitario, entonces L será una representación unitaria.

Ahora por la Definición 2.4.1 y haciendo $x = gh$ se tiene

$$\begin{aligned}\left\langle L_g \sum_{h\in G} c_h h, L_g \sum_{h\in G} k_h h \right\rangle &= \left\langle \sum_{h\in G} c_h gh, \sum_{h\in G} k_h gh \right\rangle \\ &= \left\langle \sum_{x\in G} c_{g^{-1}x} x, \sum_{x\in G} k_{g^{-1}x} x \right\rangle \\ &= \sum_{x\in G} c_{g^{-1}x}\overline{k_{g^{-1}x}}; \text{ definición de producto interno sobre } \mathbb{C}X\end{aligned}$$

Para continuar recuérdese que se hizo el cambio de variables $x = gh$ en donde $h = g^{-1}x$, de esa forma se tiene

$$\begin{aligned}\sum_{x\in G} c_{g^{-1}x}\overline{k_{g^{-1}x}} &= \sum_{h\in G} c_h \overline{k_h} \\ &= \left\langle \sum_{h\in G} c_h h, \sum_{y\in G} k_h h \right\rangle ; \text{ por definición de producto interno}\end{aligned}$$

Como $\left\langle L_g \sum_{h\in G} c_h h, L_g \sum_{h\in G} k_h h \right\rangle = \left\langle \sum_{h\in G} c_h h, \sum_{h\in G} k_h h \right\rangle$, se establece que L_g es unitario.

□

Para calcular el carácter de L, se usa la siguiente proposición que tiene una forma particularmente simple.

Proposición 2.4.3. *El carácter de la representación regular L esta dado por*

$$\chi_L(g) = \begin{cases} |G|, & si\ g = 1 \\ 0, & si\ g \neq 1 \end{cases}$$

Demostración. Sea $G = \{g_1, \cdots, g_n\}$ donde $n = |G|$ y sea $L_g g_j = g g_j$. Así si $[L_g]$ es la matriz de L_g con respecto a la base G con este orden, intentemos ver como se comportan estos elementos a partir de la información que se tiene:

Dado $G = \{g_1, \cdots, g_n\}$

Se tiene $L_g g_j = g g_j$ y estos se comportan como:

$L_g g_1 = g g_1$; hagamos $g g_1 = g_i$ entonces $g_i = 0g_1 + 0g_2 + \ldots + 1g_i + 0g_{i+1} + \ldots$

$L_g g_2 = g g_2$; hagamos $g g_2 = g_p$ entonces $g_p = 0g_2 + \ldots + 1g_p + 0g_{p+1} + \ldots$

$\vdots$

$L_g g_k = g g_k = g_m = 0g_1 + 0g_2 + \ldots + 1g_m + 0g_{m+1} + \ldots$

$\vdots$

De esa forma se va formando la matriz, no se sabe en que orden, solo que en una de sus posiciones hay un 1 y cero en las demás. Esta información puede resumirse de la siguiente manera:

$$\begin{aligned}[L_g]_{ij} &= \begin{cases} 1, & g_i = gg_j \\ 0, & \text{en otro caso} \end{cases} \\ &= \begin{cases} 1, & g = g_i g_j^{-1} \\ 0, & \text{en otro caso} \end{cases}\end{aligned}$$

En particular,

$$\begin{aligned}[L_g]_{ii} &= \begin{cases} 1, & g = g_i g_i^{-1} \\ 0, & \text{en otro caso} \end{cases} \\ &= \begin{cases} 1, & g = 1 \\ 0, & \text{en otro caso} \end{cases}\end{aligned}$$

de lo que se concluye

$$\chi_L(g) = \operatorname{Tr}(L_g) = \begin{cases} |G|, & g = 1 \\ 0, & g \neq 1 \end{cases}$$

En donde se tiene la suma de los elementos de la diagonal y en la cual hay tantos elementos como tenga el grupo. □

Ahora se descompondrá a la representación regular L en componentes irreducibles, se fijará a $\{\varphi^{(1)}, \cdots, \varphi^{(s)}\}$ como un conjunto completo de representaciones irreducibles unitarias no equivalentes de un grupo finito G en donde $d_i = \operatorname{grad} \varphi^{(i)}$. Se escribirá por conveniencia $\chi_i = \chi_{\varphi^{(i)}}$ para $i \in \{1, \cdots, s\}$.

Teorema 2.4.4. *Sea L la representación regular de G. Entonces se cumple siguiente la descomposición*

$$L \sim d_1\varphi^{(1)} \oplus d_2\varphi^{(2)} \oplus \cdots \oplus d_s\varphi^{(s)}$$

Demostración. Sea $\{\varphi^{(1)}, \varphi^{(2)}, \cdots, \varphi^{(s)}\}$ un conjunto completo de representaciones unitarias irreducibles no equivalentes. Se calculará la descomposición usando $\chi_L(g) = 0$ para $g \neq 1$ y $\chi_L(1) = |G|$, por definición de producto interno sobre $\mathbb{C}X$ se tiene

$$\begin{aligned}\langle \chi_L, \chi_{\varphi^{(i)}} \rangle &= \langle \chi_L, \chi_i \rangle; \text{ con } i \in \{1, \ldots, s\} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_L(g) \overline{\chi_i(g)}\end{aligned}$$

Nótese que los sumandos anteriores serán 0 para cualquier valor de g, excepto para cuando $g = 1$ en donde $\chi_L(1) = |G|$, entonces se tiene

$$\begin{aligned}
\langle \chi_L, \chi_i \rangle &= \frac{1}{|G|}|G|\overline{\chi_i(1)} \\
&= \overline{\chi_i(1)} \\
&= \overline{\chi_i(1)} \\
&= \chi_{\varphi^{(i)}}(1); \text{ ya que } \overline{\chi_i(1)} = \chi_i(1) \text{ y } \chi_i = \chi_{\varphi^{(i)}} \\
&= \overline{\operatorname{grad} \varphi^{(i)}} \\
&= \operatorname{grad} \varphi^{(i)}; \text{ por la Propiedad 2.3.3} \\
&= d_i
\end{aligned}$$

Ahora por el Teorema 2.3.14 se tiene: $L \sim m_1\varphi^{(1)} \oplus m_2\varphi^{(2)} \oplus \cdots \oplus m_s\varphi^{(s)}$, en donde

$$\begin{aligned}
m_i &= \left\langle \chi_L, \chi_{\varphi(i)} \right\rangle \\
&= \langle \chi_L, \chi_i \rangle \\
&= d_i
\end{aligned}$$

En conclusión $L \sim d_1\varphi^{(1)} \oplus d_2\varphi^{(2)} \oplus \cdots \oplus d_s\varphi^{(s)}$ □

Con este teorema a la mano, se puede seguir con la idea principal de este capítulo, que es encontrar una forma de codificar una representación de un grupo en una función con valores complejos.

Corolario 2.4.5. *La fórmula* $|G| = d_1^2 + d_2^2 + \cdots + d_s^2$ *se cumple.*

Demostración. Por el teorema anterior se tiene $L \sim d_1\varphi^{(1)} \oplus d_2\varphi^{(2)} \oplus \cdots \oplus d_s\varphi^{(s)}$ entonces por el Lema 2.3.13 $\chi_L = d_1\chi_1 + d_2\chi_2 + \ldots + d_s\chi_s$, donde $\chi_i = \chi_{\varphi^{(i)}}$. Así al evaluar χ_L en 1, puede verse que se cumple que

$$\begin{aligned}
\chi_L(1) &= d_1\chi_1(1) + d_2\chi_2(1) + \ldots + d_s\chi_s(1) \\
&= d_1(d_1) + d_2(d_2) + \cdots + d_s(d_s) \\
&= d_1^2 + d_2^2 + \cdots + d_s^2
\end{aligned}$$

Por otro lado se verifico en la Propiedad 2.4.3 que $\chi_L(1) = |G|$, entonces $|G| = d_1^2 + d_2^2 + \cdots + d_s^2$, completando la demostración. □

Con este resultado se puede inferir que la matriz de coeficientes de una representación irreducible unitaria forma una base ortogonal para el espacio de todas las funciones de G.

Teorema 2.4.6. *El conjunto* $B = \{\sqrt{d_k}\varphi_{ij}^{(k)} \mid 1 \leq k \leq s, 1 \leq i, j \leq d_k\}$ *es una base ortonormal para* $L(G)$*, conservando la notación anterior.*

Demostración. Se sabe que B es un conjunto ortonormal para $L(G)$ por la Proposición 2.2.10, ademas aplicando las relaciones de ortogonalidad de Schur (Teorema 2.2.8) se tiene

$$\begin{aligned}\left\langle \sqrt{d_k}\varphi_{ij}^k, \sqrt{d_k}\varphi_{ij}^k \right\rangle &= \sqrt{d_k}\left\langle \varphi_{ij}^k, \sqrt{d_k}\varphi_{ij}^k \right\rangle \\ &= \left(\sqrt{d_k}\right)^2 \left\langle \varphi_{ij}^k, \varphi_{ij}^k \right\rangle \\ &= d_k \frac{1}{d_k} \\ &= 1\end{aligned}$$

Para $|B| \leq d_1^2 + \cdots + d_s^2 \leq |G|$, así $|B| = |G| = \dim L(G)$, por lo tanto B es una base. □

El siguiente teorema muestra que $\chi_1, \cdots, \chi_s$ es una base ortonormal para el espacio de las funciones de clase $Z(L(G))$.

Teorema 2.4.7. *El conjunto $\chi_1, \cdots, \chi_s$ es una base ortonormal para $Z(L(G))$.*

Demostración. Para probar el teorema se conservara la notación anterior. Las primeras relaciones de ortogonalidad (Teorema 2.3.9) afirman que los caracteres irreducibles forman un conjunto ortonormal de funciones de clase. Por lo tanto se debe mostrar que $\chi_1, \cdots, \chi_s$ generan todo $Z(L(G))$.

Sea $f \in Z(L(G))$, por el teorema anterior se puede escribir a f como una combinación lineal de elementos de la base

$$f = \sum_{i,j,k} c_{ij}^{(k)} \varphi_{ij}^{(k)}$$

para algunos $c_{ij}^{(k)} \in \mathbb{C}$ donde $1 \leq k \leq s$ y $1 \leq i, j \leq d_k$. Como f es una función de clase ($f(x) = f\left(g^{-1}xg\right)$), para cualquier $x \in G$, véase que

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G} f(g^{-1}xg) &= \frac{1}{|G|}\sum_{g\in G} f(x); \text{ ya que } f \text{ es función de clase} \\ &= \frac{|G|}{|G|} f(x) \\ &= f(x)\end{aligned}$$

Luego se tiene que

$$\begin{aligned}
f(x) &= \frac{1}{|G|}\sum_{g\in G} f(g^{-1}xg) \\
&= \frac{1}{|G|}\sum_{g\in G}\left(\sum_{i,j,k} c_{ij}^{(k)}\varphi_{ij}^{(k)}\right)(g^{-1}xg); \text{ reemplazando f} \\
&= \sum_{i,j,k} c_{ij}^{(k)}\frac{1}{|G|}\sum_{g\in G}\varphi_{ij}^{(k)}(g^{-1}xg); \text{ debido al homomorfismo} \\
&= \sum_{i,j,k} c_{ij}^{(k)}\left[\frac{1}{|G|}\sum_{g\in G}\varphi_{g^{-1}}^{(k)}\varphi_{x}^{(k)}\varphi_{g}^{(k)}\right]_{ij} \\
&= \sum_{i,j,k} c_{ij}^{(k)}[(\varphi_x^{(k)})^{\sharp}]_{ij}; \text{ por la Proposición 2.2.2} \\
&= \sum_{i,j,k} c_{ij}^{(k)}\left[\frac{\mathrm{Tr}(\varphi_x^{(k)})}{\operatorname{grad}\varphi^{(k)}}I\right]_{ij}; \text{ por la Proposición 2.2.3}
\end{aligned}$$

además se tiene que $\mathrm{Tr}(\varphi_x^{(k)}) = \chi_k$ y $\operatorname{grad}\varphi^{(k)} = d_k$ entonces

$$= \sum_{i,k} c_{ii}^{(k)}\frac{1}{d_k}\chi_k(x)$$

Nótese que en la ultima igualdad se colocan solo aquellos elementos que contribuyen a la suma, que son precisamente los elementos de la diagonal. Esto establece que está generado por $\chi_1, \cdots, \chi_s$, completando así la prueba de que los caracteres irreducibles forman una base ortonormal para $Z(L(G))$. □

Corolario 2.4.8. *El número de clases de equivalencia de las representaciones irreducibles de G es el número de clases de conjugación de G.*

Demostración. Sea s el número de clases de equivalencia de las representaciones irreducibles de G, el teorema anterior implica que $s = \dim Z(L(G))$, ya que las funciones de clase forman una base y por la Proposición 2.3.8 $\dim Z(L(G)) = |Cl(G)|$, en donde, $|Cl(G)|$ es el número de clases de conjugación, así $s = |Cl(G)|$ por lo tanto se cumple el corolario. □

Corolario 2.4.9. *Un grupo finito G es abeliano si y solo si este tiene $|G|$ clases de equivalencia de las representaciones irreducibles.*

Demostración. En un grupo abeliano se cumple que para un elemento arbitrario $x \in G$ y para todo $g \in G$ se tiene que $gx = xg$, de aquí que $x = gxg^{-1}$, esto quiere decir que cada elemento del grupo pertenece a una clase de conjugación distinta, con lo cual podemos concluir que $|G| = |Cl(G)|$.

Por otro lado si $|G| = |Cl(G)|$ quiere decir que para un elemento arbitrario $x \in G$ su clase conjugada es un conjunto unipuntual, entonces se cumple que para todo $g \in G$ $x = gxg^{-1}$ de aquí que $gx = xg$ para cualesquiera elementos del grupo, por lo tanto es abeliano.

□

Ejemplo 2.4.10. *Representaciones irreducibles de* $\mathbb{Z}/n\mathbb{Z}$

Sea $\omega_n = e^{2\pi i/n}$, entonces sus representaciones irreducibles están definidas por $\chi_k \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ con regla de asignación $\chi_k([m]) = \omega_n^{km}$ para $0 \leq k \leq n-1$.

Desarrollo. Primero nótese que $\mathbb{Z}/n\mathbb{Z}$ es cíclico por tanto es abeliano, además $|\mathbb{Z}/n\mathbb{Z}| = n$.

Los χ_k son irreducibles porque la representación w_n es de grado 1, entonces el carácter coincide con el grado de la representación por la Proposición 2.3.3 y cada ω_n^{km} es diferente.

Entonces $\chi_0, \cdots, \chi_{n-1}$ son las distintas representaciones irreducibles de $\mathbb{Z}/n\mathbb{Z}$. □

La representación de la información teórica acerca de un grupo finito puede resumirse en una matriz conocida como *tabla de caracteres*.

Definición 2.4.11. Tabla de Caracteres.

Sea G un grupo finito con caracteres irreducibles $\chi_1, \cdots, \chi_s$ y clases de conjugación $C_1, \cdots, C_s$. *La tabla de caracteres* de G es la matriz X de dimensiones $s \times s$ con $X_{ij} = \chi_i(C_j)$. En otras palabras, las filas de X son indexadas por los caracteres de G, las columnas por las clases de conjugación de G y la ij-entrada es el valor del i-ésimo carácter sobre la j-ésima clase de conjugación.[(11)]

La tabla de caracteres de S_3 se registra en la Tabla 2.1, mientras que la de $\mathbb{Z}/4\mathbb{Z}$ (Tabla 2.3) se puede encontrar de la siguiente forma:

Desarrollo. Por el Ejemplo 2.4.10 se sabe que

$$\begin{aligned} \chi_k([m]) &= w_n^{km} \\ &= e^{\frac{\pi i k m}{2}} \end{aligned}$$

Por otro lado, recuérdese que $\mathbb{Z}/4\mathbb{Z}$ es isomorfo a $\mathbb{Z}_4$ entonces las clases son $[m] \in \{0, 1, 2, 3\}$. Por lo tanto se realizan los siguientes cálculos

		[0]	[1]	[2]	[3]	
Si $k=1$	$\Rightarrow e^{\frac{\pi i m}{2}}$	$\chi_1([0]) = 1$	$\chi_1([1]) = i$	$\chi_1([2]) = -1$	$\chi_1([3]) = -i$	χ_1
Si $k=2$	$\Rightarrow e^{\pi i m}$	$\chi_2([0]) = 1$	$\chi_2([1]) = -1$	$\chi_2([2]) = 1$	$\chi_2([3]) = -1$	χ_2
Si $k=3$	$\Rightarrow e^{\frac{3\pi i m}{2}}$	$\chi_3([0]) = 1$	$\chi_3([1]) = -i$	$\chi_3([2]) = -1$	$\chi_3([3]) = i$	χ_3
Si $k=4$	$\Rightarrow e^{2\pi i m}$	$\chi_4([0]) = 1$	$\chi_4([1]) = 1$	$\chi_4([2]) = 1$	$\chi_4([3]) = 1$	χ_4

Con los datos anteriores se forma la tabla de caracteres correspondientes

[(11)] Los índices en las filas de X quedan determinados por los caracteres de G

Tabla 2.3: Tabla de carácter de $\mathbb{Z}/4\mathbb{Z}$

	[0]	[1]	[2]	[3]
χ_1	1	i	-1	-i
χ_2	1	-1	1	-1
χ_3	1	-i	-1	i
χ_4	1	1	1	1

□

Observése que en ambos ejemplos las columnas son ortogonales con respecto al producto interno estándar. Se demostrará que este es siempre el caso. Si g, $h \in G$, entonces el producto interno de las columnas correspondientes a sus clases de conjugación esta dada por la expresión.

$$\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(h)}.$$

Claramente ese sigue siendo un producto interno aun cuando no se este dividiendo por $|G|$, cuando el grupo es finito.

Por otro lado, recuérdese que si C es una clase de conjugación, entonces

$$\delta_C(g) = \begin{cases} 1, & g \in C \\ 0, & \text{en otro caso} \end{cases}$$

Los δ_C con $C \in Cl(G)$ forman una base para $Z(L(G))$, así como los caracteres irreducibles, por lo tanto resulta natural expresar los δ_C en términos de los caracteres irreducibles, dando lugar así a la ortogonalidad de las columnas de la tabla de caracteres.

Teorema 2.4.12. ***(Segundas Relaciones de Ortogonalidad)***.

Sean C, C' clases de conjugación de G y sean $g \in C$ y $h \in C'$. Entonces el producto interno de las columnas correspondientes a sus clases de conjugación está dado por

$$\sum_{i=1}^{S} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} \frac{|G|}{|C|}, & si\ C = C' \\ 0, & si\ C \neq C' \end{cases}$$

Consecuentemente, las columnas de la tabla de caracteres son ortogonales y por lo tanto la tabla de caracteres es invertible.

Observación 2.4.13. *Los caracteres representan la base ortonormal y los δ son funciones de clase.*

Demostración. El espacio con el que se esta trabajando es finito, posee producto interno y tiene una base ortonormal, entonces cualquier elemento del espacio puede escribirse $\delta_{C'} = \sum_{i=1}^{s} \langle \delta_{C'}, \chi_i \rangle \chi_i$, con lo cual puede calcularse

$$\begin{aligned}
\delta_{C'}(g) &= \sum_{i=1}^{s} \langle \delta_{C'}, \chi_i \rangle \chi_i(g) \\
&= \sum_{i=1}^{s} \frac{1}{|G|} \sum_{x \in G} \delta_{C'}(x) \overline{\chi_i(x)} \chi_i(g); \text{ si } x \in C' \Rightarrow \delta_{C'}(x) = 1 \\
&= \frac{1}{|G|} \sum_{i=1}^{s} \sum_{x \in C'} \overline{\chi_i(x)} \chi_i(g); \text{ se toman solo con los elementos de la clase} \\
&= \frac{1}{|G|} \sum_{i=1}^{s} \chi_i(g) \sum_{x \in C'} \overline{\chi_i(x)}
\end{aligned}$$

pero el carácter es constante sobre las clases conjugadas, entonces se estaría sumando $|C'|$ un valor de la clase (por hipótesis se sabe que $h \in C'$), obteniendo $\sum_{x \in C'} \overline{\chi_i(x)} = |C'| \overline{\chi_i(h)}$, así

$$\delta_{C'}(g) = \frac{|C'|}{|G|} \sum_{i=1}^{s} \chi_i(g) \overline{\chi_i(h)}$$

Ahora si $g \in C'$ entonces $\delta_{C'}(g) = 1$ y

$$\begin{aligned}
1 &= \frac{|C'|}{|G|} \sum_{i=1}^{s} \chi_i(g) \overline{\chi_i(h)} \\
\frac{|G|}{|C'|} &= \sum_{i=1}^{s} \chi_i(g) \overline{\chi_i(h)}
\end{aligned}$$

o en caso contrario $\delta_{C'}(g) = 0$ y $\sum_{i=1}^{s} \chi_i(g) \overline{\chi_i(h)} = 0$.

Resumiendo este resultado se tiene

$$\sum_{i=1}^{s} \chi_i(g) \overline{\chi_i(h)} = \begin{cases} |G|/|C|, & C = C' \\ 0, & C \neq C' \end{cases}$$

como se quería.

Se deduce que las columnas de la tabla de caracteres forman un conjunto ortogonal de vectores distintos de cero, ya que al calcular $\langle \chi_i(g), \chi_j(h) \rangle$ se obtiene que es igual a 0, porque la clase para los elementos g y h son distintas por hipótesis, esto implica que sean linealmente

independientes. Este resultado produce la invertibilidad de la tabla de caracteres, por que al ser linealmente independientes las columnas, si se aplicará el proceso de Gauus-Jordan se llegaría a la identidad. □

Observación 2.4.14. *La tabla de caracteres es de hecho la transpuesta de la matriz de cambio de base, es decir, de la base* $\{\chi_1, \cdots, \chi_s\}$ *a la base* $\{\delta_C \mid C \in Cl(G)\}$ *para* $Z(L(G))$.

2.5. Representación de Grupos Abelianos

En esta sección, se calcularán los caracteres de un grupo abeliano. El ejemplo 2.4.10 proporciona los caracteres del grupo $\mathbb{Z}/n\mathbb{Z}$. Como cualquier grupo abeliano finito es un producto directo de grupos cíclicos, todo lo que se necesita saber es cómo calcular los caracteres de un producto directo de grupos abelianos.

Proposición 2.5.1. *Sean* G_1, G_2 *grupos abelianos y supóngase que* $\chi_1, \cdots, \chi_n$ *y* $\varphi_1, \cdots, \varphi_n$ *son las representaciones irreducibles de* G_1, G_2, *respectivamente. En particular,* $m = |G_1|$ *y* $n = |G_2|$. *Entonces las funciones* $\alpha_{ij} \colon G_1 \times G_2 \to \mathbb{C}^*$ *con* $1 \leq i \leq m$, $1 \leq j \leq n$ *definidas como*

$$\alpha_{ij}(g_1, g_2) = \chi_i(g_1)\varphi_j(g_2)$$

forman un conjunto completo de representaciones irreducibles de $G_1 \times G_2$.

Demostración. En primer lugar se debe comprobar que los α_{ij} son representaciones.

$$\begin{aligned}
\alpha_{ij}(g_1, g_2)\alpha_{ij}(g_1', g_2') &= \chi_i(g_1)\varphi_j(g_2)\chi_i(g_1')\varphi_j(g_2') \\
&= \chi_i(g_1)\chi_i(g_1')\varphi_j(g_2)\varphi_j(g_2'); \text{ el producto es conmutativo en los complejos} \\
&= \chi_i(g_1g_1')\varphi_j(g_2g_2') \\
&= \alpha_{ij}(g_1g_1', g_2g_2') \\
&= \alpha_{ij}((g_1, g_2)(g_1', g_2'))
\end{aligned}$$

Ahora debe verificarse que todas las representaciones son distintas, es decir, si $\alpha_{ij} = \alpha_{k\ell}$ implica que $i = k$ y $j = \ell$. Entonces para todo $g \in G_1$ se tiene que

$$\begin{aligned}
\chi_i(g) &= \chi_i(g).1 \\
&= \chi_i(g)\varphi_j(e_{G_2}) \\
&= \alpha_{ij}(g, e_{G_2}) \\
&= \alpha_{k\ell}(g, e_{G_2}) \\
&= \chi_k(g)\varphi_\ell.1 \\
&= \chi_k(g)(1) \\
&= \chi_k(g)
\end{aligned}$$

Por lo tanto $i = k$, porque se esta probando que dado un g arbitrario en G_1 se cumple que $\chi_i(g) = \chi_k(g)$, es decir coinciden cuando los indices son iguales, de aquí que dos representaciones irreducibles sean diferentes de lo contrario. La demostración para $j = \ell$ es análoga. Ahora hace falta probar la irreducibilidad, por ello se utilizará el resultado obtenido en el Corolario 2.3.15 para demostrar que $\langle \chi_{\alpha_{ij}}, \chi_{\alpha_{ij}} \rangle = 1$.

$$\begin{aligned}
\langle \chi_{\alpha_{ij}}, \chi_{\alpha_{ij}} \rangle &= \langle \alpha_{ij}, \alpha_{ij} \rangle \\
&= \frac{1}{|G_1 \times G_2|} \sum_{\substack{g_1 \in G_1, \\ g_2 \in G_2}} \alpha_{ij}(g_1, g_2)\overline{\alpha_{ij}(g_1, g_2)} \\
&= \frac{1}{mn} \sum_{\substack{g_1 \in G_1, \\ g_2 \in G_2}} \chi_i(g_1)\varphi_j(g_2)\overline{\chi_i(g_1)\varphi_j(g_2)} \\
&= \frac{1}{mn} \sum_{\substack{g_1 \in G_1, \\ g_2 \in G_2}} \chi_i(g_1)\overline{\chi_i(g_1)}\varphi_j(g_2)\overline{\varphi_j(g_2)} \\
&= \left(\frac{1}{m} \sum_{g_1 \in G_1} \chi_i(g_1)\overline{\chi_i(g_1)} \right) \left(\frac{1}{n} \sum_{g_2 \in G_2} \varphi_j(g_2)\overline{\varphi_j(g_2)} \right) \\
&= \langle \chi_i, \chi_i \rangle \langle \varphi_j, \varphi_j \rangle \\
&= (1)(1); \text{ por el Corolario 2.3.15 para } \chi_i \text{ y } \varphi_j \text{ irreducibles} \\
&= 1
\end{aligned}$$

Por otro lado como $G_1 \times G_2$ tiene $|G_1 \times G_2| = |G_1||G_2| = mn$ distintas representaciones irreducibles, se deduce que el α_{ij} con $1 \leq i \leq m$, $1 \leq j \leq n$ son todas ellas. □

Ejemplo 2.5.2. Calcular la tabla de caracteres del 4-grupo de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ utilizando la Proposición 2.5.1.

Se encuentra primero la tabla de caracteres para $\mathbb{Z}/2\mathbb{Z}$

$$\begin{aligned}
\mathbb{Z}/2\mathbb{Z} \approx Z_2 &\Longrightarrow w_n = e^{\frac{2\pi i}{n}} \Rightarrow w_n = e^{\pi i}; \text{ ya que } n = 2 \Rightarrow w_n = -1 \\
&\Longrightarrow \chi_k([m]) = w_n^{km} = (-1)^{km}
\end{aligned}$$

			[0]	[1]	
Si	$k = 1$	$\Rightarrow (-1)^m$	$\chi_1([0]) = 1$	$\chi_1([1]) = -1$	χ_1
Si	$k = 2$	$\Rightarrow (-1)^{2m}$	$\chi_2([0]) = 1$	$\chi_2([1]) = 1$	χ_2

La tabla de caracteres de $\mathbb{Z}/2\mathbb{Z}$ podemos observarla en la Tabla 2.4, ahora se calculará la tabla de caracteres de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, que quedará representada como en la Tabla 2.5.

Tabla 2.4: Tabla de carácter de $\mathbb{Z}/2\mathbb{Z}$

	[0]	[1]
χ_1	1	-1
χ_2	1	1

Se calculan los elementos $\alpha_{ij}(g_1, g_2) = \rho_i(g_1)\varphi_j(g_2)$ con $g_i = [j]$ con $1 \leq i, j \leq 2$, nótese que $\rho_i = \chi_i$ y $\varphi_j = \chi_j$ para i y j antes definidas, por ejemplo, si $i = 1$ y $j = 2$ entonces $\rho_1([m])\varphi_2([n]) = \chi_1([m])\chi_2([m])$ con $[m], [n] \in \mathbb{Z}/2\mathbb{Z}$

$$\begin{array}{llll|llll}
\alpha_{11}([0],[0]) & = \rho_1([0])\varphi_1([0]) & = (1)(1) & = 1 & \alpha_{12}([0],[0]) & = \rho_1([0])\varphi_2([0]) & = (1)(1) & = 1 \\
\alpha_{11}([0],[1]) & = \rho_1([0])\varphi_1([1]) & = (1)(-1) & = -1 & \alpha_{12}([0],[1]) & = \rho_1([0])\varphi_2([1]) & = (1)(1) & = 1 \\
\alpha_{11}([1],[0]) & = \rho_1([1])\varphi_1([0]) & = (-1)(1) & = -1 & \alpha_{12}([1],[0]) & = \rho_1([1])\varphi_2([0]) & = (-1)(1) & = -1 \\
\alpha_{11}([1],[1]) & = \rho_1([1])\varphi_1([1]) & = (-1)(-1) & = 1 & \alpha_{12}([1],[1]) & = \rho_1([1])\varphi_2([1]) & = (-1)(1) & = -1 \\
\hline
\alpha_{21}([0],[0]) & = \rho_2([0])\varphi_1([0]) & = (1)(1) & = 1 & \alpha_{22}([0],[0]) & = \rho_2([0])\varphi_2([0]) & = (1)(1) & = 1 \\
\alpha_{21}([0],[1]) & = \rho_2([0])\varphi_1([1]) & = (1)(-1) & = -1 & \alpha_{22}([0],[1]) & = \rho_2([0])\varphi_2([1]) & = (1)(1) & = 1 \\
\alpha_{21}([1],[0]) & = \rho_2([1])\varphi_1([0]) & = (1)(1) & = 1 & \alpha_{22}([1],[0]) & = \rho_2([1])\varphi_2([0]) & = (1)(1) & = 1 \\
\alpha_{21}([1],[1]) & = \rho_2([1])\varphi_1([1]) & = (1)(-1) & = -1 & \alpha_{22}([1],[1]) & = \rho_2([1])\varphi_2([1]) & = (1)(1) & = 1
\end{array}$$

Una vez calculados cada uno de los elementos, los resumimos tal y como sigue:

Tabla 2.5: Tabla de carácter de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

	([0],[0])	([0],[1])	([1],[0])	([1],[1])
α_{11}	1	-1	-1	1
α_{12}	1	1	-1	-1
α_{21}	1	-1	1	-1
α_{22}	1	1	1	1

Capítulo 3

Análisis de Fourier en grupos finitos

En este capítulo se introducirá una estructura algebraica para $L(G)$ procedente del producto convolución, en donde la transformada de Fourier permitirá analizar esta estructura en términos de algunos anillos conocidos. El análisis de Fourier tiene diversas aplicaciones en la matemática y aun cuando hay libros enteros dedicados al análisis de Fourier en grupos finitos, este capítulo se limitará a presentar una aplicación para el cálculo de los valores propios de la matriz de adyacencia del Grafo de Cayley de un grupo abeliano.

3.1. Funciones periódicas sobre Grupos cíclicos

Se definen a las funciones periódicas en los enteros.

Definición 3.1.1. (Función periódica).

Una función $f\colon \mathbb{Z} \to \mathbb{C}$ es periódica con período n, si $f(x) = f(x+n)$ para todo $x \in \mathbb{Z}$ [(1)].

Debe tenerse en cuenta que si n es el período de f, entonces también lo es cualquier múltiplo de n. En general las funciones periódicas con periodo n están en biyección con los elementos de $L(\mathbb{Z}/n\mathbb{Z})$, es decir, con las funciones $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$. Para ver esto, se tiene que en cada función periódica $F\colon \mathbb{Z} \longrightarrow \mathbb{C}$ tal que $F(i+nk) = z_i$ para toda $i \in \{1, 2, \cdots, n\}$, se le asocia una función $f\colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}$ tal que $f([i]) = z_i$ para toda $i \in \{1, 2, \cdots, n\}$, de hecho, la definición de una función periódica dice que f es constante en las clases de residuos módulo n.

Por otro lado, los caracteres irreducibles forman una base para $L(\mathbb{Z}/n\mathbb{Z})$ por el Teorema 2.4.7 y por el Ejemplo 2.4.10.

Entonces si $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ es una función, se tiene que

$$f = \langle f, \chi_0\rangle\chi_0 + \cdots + \langle f, \chi_{n-1}\rangle\chi_{n-1} \tag{3.1}$$

$$= \sum_{i=0}^{n-1} \langle f, \chi_i\rangle\chi_i \tag{3.2}$$

[(1)] Esta es otra forma de referirse a las funciones de clase del grupo cociente.

donde $\chi_k([m]) = e^{2\pi ikm/n}$. Se verá que la transformada de Fourier codifica esta información como una función.

Definición 3.1.2. (Transformada de Fourier).

Sea $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, se define la transformada de Fourier $\widehat{f}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ de f por

$$\begin{aligned}\widehat{f}([m]) &= n\langle f, \chi_m\rangle \\ &= n\left(\frac{1}{n}\sum_{k=0}^{n-1} f([k])\overline{\chi_k([m])}\right); \text{ definición de producto interno} \\ &= \sum_{k=0}^{n-1} f([k])e^{-2\pi imk/n}; \text{ ya que } \overline{\chi_k([m])} = e^{-2\pi ikm/n}\end{aligned}$$

Nótese que la transformada de Fourier $T\colon L(\mathbb{Z}/n\mathbb{Z}) \to L(\mathbb{Z}/n\mathbb{Z})$ es lineal, ya que

$$\begin{aligned}T(c_1f + c_2g)([m]) &= n\left\langle c_1f + c_2g, \chi_m\right\rangle \\ &= nc_1\left\langle c_1f, \chi_m\right\rangle + nc_2\left\langle c_2g, \chi_m\right\rangle \\ &= c_1T(f) + c_2T(g)\end{aligned}$$

Esto se debe a la linealidad del producto interno en la primera componente. Entonces se puede reescribir la ecuación (3.2) como una proposición de la siguiente manera:

Proposición 3.1.3. ***(Inversión de Fourier)*** .

La transformada de Fourier es invertible. Más precisamente, $f = \dfrac{1}{n}\displaystyle\sum_{k=0}^{n-1} \widehat{f}([k])\chi_k$

Demostración. De acuerdo a la definición dada en la ecuación (3.2) se puede reescribir a la función como sigue:

$$\begin{aligned}f &= \sum_{k=0}^{n-1}\left\langle f, \chi_k\right\rangle \chi_k \\ &= \frac{1}{n}\sum_{k=0}^{n-1} n\left\langle f, \chi_k\right\rangle \chi_k \\ &= \frac{1}{n}\sum_{k=0}^{n-1} \widehat{f}([k])\chi_k; \text{ por la definición de transformada de Fourier}\end{aligned}$$

Con lo que se ha probado la igualdad de la proposición, ahora recuérdese que una función es invertible si es biyectiva, luego para comprobar la inyectividad se tomarán las funciones

$\widehat{f}$ y $\widehat{g}$, así si $\widehat{f} = \widehat{g}$ se tendría que $f = g$. De aquí que

$$\begin{aligned} f &= \frac{1}{n}\sum_{k=0}^{n-1} \widehat{f}([k])\chi_k \\ &= \frac{1}{n}\sum_{k=0}^{n-1} \widehat{g}([k])\chi_k; \text{ por hipótesis} \\ &= g; \text{ de acuerdo a lo que ya se ha demostrado} \end{aligned}$$

Por lo tanto es inyectiva, falta demostrar la sobreyectividad para que sea invertible. Para ello sea $f([k]) = z_k$ tal que f es la transformada de una función, se define a la función g como sigue

$$g = \frac{1}{n}\sum_{k=0}^{n-1} f([k])\chi_k$$

Ahora

$$\begin{aligned} \widehat{g}([m]) &= n\,\langle g, \chi_m\rangle \\ &= n\left\langle \frac{1}{n}\sum_{k=0}^{n-1} f([k])\chi_k, \chi_m \right\rangle \\ &= n\frac{1}{n}\left\langle \sum_{k=0}^{n-1} f([k])\chi_k, \chi_m \right\rangle \\ &= \sum_{k=0}^{n-1} f([k])\,\langle \chi_k, \chi_m\rangle \text{ ; ya que cada } f([k]) \text{ es un valor escalar} \\ &= f([k]) \end{aligned}$$

La última igualdad se cumple ya que los caracteres irreducibles forman una base para $L(\mathbb{Z}/n\mathbb{Z})$, entonces al ser linealmente independientes el producto interno será 0 a menos que se trate del mismo carácter, entonces la transformada de Fourier es biyectiva y por lo tanto invertible. □

La transformada de Fourier en los grupos cíclicos se utiliza en procesamiento de imágenes y señales. La idea es que los valores de $\widehat{f}$ corresponden a las longitudes de onda asociadas a la función de onda f. Se ajusta a cero todos los valores suficientemente pequeños de $\widehat{f}$, comprimiendo de ese modo la onda. Para recuperar la onda original o acercarse lo suficientemente a ella, se aplica la inversión de Fourier.

3.2. El Producto de Convolución

En esta sección se introduce el producto de convolución en $L(G)$, lo cual le dará sentido a la terminología definida en el álgebra de grupo para $L(G)$.

Definición 3.2.1. (Convolución).

Sea G un grupo finito y $a,\ b \in L(G)$. Entonces la convolución de $a * b$: $G \to \mathbb{C}$ esta definida por

$$a * b(x) = \sum_{y \in G} a(xy^{-1})b(y) \tag{3.3}$$

Observése como funciona la definición de convolución, se tiene que para cada elemento $g \in G$, se ha asociado la función delta δ_g. Es natural tratar de asignar una operación de multiplicación $(*)$ a $L(G)$ de manera que $\delta_g * \delta_h = \delta_{gh}$ [(2)], se corroborará que en efecto la convolución tiene esta propiedad en la siguiente proposición.

Proposición 3.2.2. *Para $g,\ h \in G, \delta_g * \delta_h = \delta_{gh}$.*

Demostración.

$$\delta_g \delta_h(x) = \sum_{y \in G} \delta_g(xy^{-1})\delta_h(y)$$

En donde los únicos términos no nulos se obtienen cuando $h = y$ y $g = xy^{-1} = xh^{-1}$, entonces

$$\begin{aligned} \delta_g * \delta_h(x) &= \begin{cases} 1 & ;\text{ si } x = gh \\ 0 & ;\text{ caso contrario} \end{cases} \\ &= \delta_{gh}(x) \end{aligned}$$

□

Una de las metas será mostrar que la convolución de $L(G)$ da la estructura de un anillo. Ahora si $a,\ b \in L(G)$, entonces

$$a = \sum_{g \in G} a(g)\delta_g \text{ y } b = \sum_{h \in G} b(h)\delta_h$$

Se corrobora que efectivamente esta definición devuelve a la función a

$$\begin{aligned} a(x) &= \sum_{g \in G} a(g)\delta_g(x) \\ &= \begin{cases} a(x) & ;\text{ si } g = x \\ 0, & ;\text{ caso contrario} \end{cases} \end{aligned}$$

[(2)] Recuérdese que $\delta_h(y) = 1$ si $h = y$ y $\delta_h(y) = 0$ si $h \neq y$

Pasaría exactamente lo mismo para b. Ahora si $L(G)$ fuera un anillo, entonces la ley distributiva obligaría a que

$$\begin{aligned} a * b &= \left(\sum_{g\in G} a(g)\delta_g\right) * \left(\sum_{h\in G} b(h)\delta_h\right) \\ &= \sum_{g,h\in G} (a(g)\delta_g) * (b(h)\delta_h) \\ &= \sum_{g,h\in G} a(g)b(h)\,(\delta_g * \delta_h) \\ &= \sum_{g,h\in G} a(g)b(h)\delta_{gh} \end{aligned}$$

Si se aplica el cambio de variables $y = h$ y $x = gh$ en donde $g = xy^{-1}$ se obtiene lo siguiente

$$\begin{aligned} a * b &= \sum_{h\in G}\left(\sum_{g\in G} a(g)b(h)\delta_{gh}\right) \\ &= \sum_{y\in G}\left(\sum_{xy^{-1}\in G} a(xy^{-1})b(y)\delta_{xy^{-1}y}\right) \\ &= \sum_{y\in G}\left(\sum_{xy^{-1}\in G} a(xy^{-1})b(y)\delta_{x}\right) \end{aligned}$$

la primera sumatoria varia sobre y y la otra sobre xy^{-1}, con la primera se controlan a todo los y, de esta manera, sin pérdida de generalidad puede reescribir como sigue.

$$\begin{aligned} &= \sum_{y\in G}\left(\sum_{x\in G} a(g)b(y)\delta_{x}\right) \\ &= \sum_{x\in G}\left(\sum_{y\in G} a(xy^{-1})b(y)\right)\delta_x \end{aligned}$$

que es equivalente a la fórmula (3.3).

Teorema 3.2.3. *El conjunto $L(G)$ es un anillo con la adición tomada punto a punto y la convolución como multiplicación. Por otra parte, δ_1 es la identidad multiplicativa.*

Demostración. La adición está dada en la Definición 2.2.1, ahora se verificará que δ_1 es la identidad para la operación $*$ de la convolución, sea $f \in L(G)$

$$\begin{aligned} f * \delta_1(x) &= \sum_{y\in G} f(xy^{-1})\delta_1(y^{-1}) \\ &= f(x\cdot 1)\cdot 1; \text{ ya que } \delta_1(y^{-1}) = 0 \text{ excepto cuando } y^{-1} = 1 \\ &= f(x) \end{aligned}$$

De manera similar se comprueba que $\delta_1 * f(x) = f(x)$

$$\begin{aligned}\delta_1 * f(x) &= \sum_{y\in G} \delta_1(xy^{-1})f(y)\\ &= 1\cdot f(x)1; \text{ ya que } xy^{-1} = 1 \text{ entonces } x = y\end{aligned}$$

Esto demuestra que δ_1 es la identidad multiplicativa.

Para comprobar la asociatividad, sea f, h, $w \in L(G)$. Entonces

$$[(f * h) * w](x) = \sum_{y\in G}[f * h](xy^{-1})w(y) \tag{3.4}$$

$$= \sum_{y\in G}\sum_{z\in G} f(xy^{-1}z^{-1})h(z)w(y) \tag{3.5}$$

Se hace un cambio de variables para continuar, sea $u = zy$ (y así $y^{-1}z^{-1} = u^{-1}, z = uy^{-1}$). Así el lado derecho de (3.5) se convierte en

$$\begin{aligned}\sum_{y\in G}\sum_{u\in G} f(xu^{-1})h(uy^{-1})w(y) &= \sum_{u\in G}\sum_{y\in G} f(xu^{-1})h(uy^{-1})w(y)\\ &= \sum_{u\in G} f(xu^{-1})\sum_{y\in G} h(uy^{-1})w(y)\\ &= \sum_{u\in G} f(xu^{-1})[h * w](u)\\ &= [f * (h * w)](x)\end{aligned}$$

Ahora se comprobará la distributividad, para ello sean f, h, $w \in L(G)$, entonces debe cumplirse que

$$\begin{aligned}[(f + h) * w](x) &= \sum_{y\in G}[f + h](xy^{-1})w(y)\\ &= \sum_{y\in G}\left[f(xy^{-1}) + h(xy^{-1})\right]w(y)\\ &= \sum_{y\in G}\left[f(xy^{-1})w(y) + h(xy^{-1})w(y)\right]\\ &= \sum_{y\in G} f(xy^{-1})w(y) + \sum_{y\in G} h(xy^{-1})w(y)\\ &= f * w(x) + h * w(x)\end{aligned}$$

y también que

$$\begin{aligned} w * (f+h)(x) &= \sum_{y\in G} w(xy^{-1})[f+h](y) \\ &= \sum_{y\in G} w(xy^{-1})\,[f(y)+h(y)] \\ &= \sum_{y\in G} \left[w(xy^{-1})f(y) + w(xy^{-1})h(y)\right] \\ &= \sum_{y\in G} w(xy^{-1})f(y) + \sum_{y\in G} w(xy^{-1})h(y) \\ &= w * f(x) + w * h(x) \end{aligned}$$

Lo que completa la prueba. □

Ahora es momento de justificar la notación $Z(L(G))$ para el espacio de las funciones de clase en G. Recuérdese que el centro $Z(R)$ de un anillo R consta de todos los elementos $a \in R$ tal que $ab = ba$ para todos $b \in R$. Por ejemplo, se puede demostrar que las matrices escalares forman el centro de $M_n(\mathbb{C})$.

Proposición 3.2.4. *Las funciones de clase forman el centro de $L(G)$. Es decir, $f\colon G \to \mathbb{C}$ es una función de clase si y sólo si $a * f = f * a$ para todo $a \in L(G)$.*

Demostración. "$\Longrightarrow$"

Supóngase que f es una función de clase y sea $a \in L(G)$. entonces

$$a * f(x) = \sum_{y\in G} a(xy^{-1})f(y); \text{ como } f \text{ es función de clase, entonces} \tag{3.6}$$

$$= \sum_{y\in G} a(xy^{-1})f(xyx^{-1}) \tag{3.7}$$

Si se hace $z = xy^{-1}$ se tendría que $yx^{-1} = z^{-1}$ y el lado derecho de (3.7) se reescribiría como

$$\begin{aligned} \sum_{z\in G} a(z)f(xz^{-1}) &= \sum_{z\in G} f(xz^{-1})a(z); \text{ ya que el producto de complejos es conmutativo.} \\ &= f * a(x) \end{aligned}$$

Y por lo tanto $a * f = f * a$ (está en el centro).

"$\Longleftarrow$"

Sea f un elemento del centro de $L(G)$, se demostrará primero la siguiente conjetura.

$f(gh) = f(hg)$ para todo g, $h \in G$.

Demostración. (de la conjetura).

Observése que se puede reescribir a $f(gh)$ ocupando la función característica

$$\begin{aligned} f(gh) &= \sum_{y\in G} f(gy^{-1})\delta_{h^{-1}}(y); \text{ los elementos de la sumatoria serán distintos de cero cuando } h = y^{-1} \\ &= f * \delta_{h^{-1}}(g); \text{ utilizando la definición de la convolución} \\ &= \delta_{h^{-1}} * f(g); \text{ como } f \text{ pertenece al centro puede conmutar} \\ &= \sum_{y\in G} \delta_{h^{-1}}(gy^{-1})f(y); \text{ reescribiendo utilizando la definición} \\ &= f(hg); \text{ como } \delta_{h^{-1}}(gy^{-1}) = 1 \text{ si } h^{-1} = gy^{-1} \Rightarrow y = gh \end{aligned}$$

Fin de la conjetura. □

Para completar la demostración, se observa que por el resultado de la conjetura $f(ghg^{-1}) = f(hg^{-1}g) = f(h)$, con lo que se establece que f es una función de clase. □

Como consecuencia de este resultado, la notación $Z(L(G))$ para el conjunto de funciones de clase no es ambigua.

3.3. Análisis de Fourier en Grupos Abelianos Finitos

En esta sección, se considerará el caso de grupos abelianos como una situación mucho más simple, y esto es frecuentemente suficiente para las aplicaciones en procesamiento de señales y en la teoría del número. En esta última, los grupos de interés habitualmente son $\mathbb{Z}/n\mathbb{Z}$ y $\mathbb{Z}/n\mathbb{Z}^*$.

Sea G un grupo abeliano finito, entonces las funciones de clase de G son las mismas del álgebra de grupo, es decir, $L(G) = Z(L(G))$, por consiguiente, $L(G)$ es un anillo conmutativo (se intentará identificar, salvo isomorfismo, con un anillo conocido). La clave para analizar la estructura de anillo de $L(G)$ es la transformada de Fourier.

Definición 3.3.1. (Grupo Dual)

Sea G un grupo abeliano finito y sea $\widehat{G}$ el conjunto de todos los caracteres irreducibles $\chi\colon G \longrightarrow \mathbb{C}^*$. A $\widehat{G}$ se le conoce como el grupo dual de G.

Proposición 3.3.2. *Sea G un grupo abeliano finito. Se define el producto de $\widehat{G}$ a través de la multiplicación punto a punto, es decir, $(\chi \cdot \theta)(g) = \chi(g)\,\theta(g)$. Entonces $\widehat{G}$ es un grupo abeliano de orden $|G|$ con respecto a esta operación binaria.*

Demostración. Se probará que es cerrado bajo la operación definida. Para ello primero obsérvese que dados $\chi, \theta \in \widehat{G}$, se cumple que

$$\begin{aligned}\chi \cdot \theta\,(g_1 g_2) &= \chi\,(g_1 g_2)\,\theta\,(g_1 g_2)\\ &= \chi\,(g_1)\,\chi\,(g_2)\,\theta\,(g_1)\,\theta\,(g_2)\\ &= \chi\,(g_1)\,\theta\,(g_1)\,\chi\,(g_2)\,\theta\,(g_2)\,;\text{ ya que } \mathbb{C}^* \text{ es conmutativo}\\ &= (\chi \cdot \theta)\,(g_1) \cdot (\chi \cdot \theta)\,(g_2)\end{aligned}$$

De esta manera $\widehat{G}$ es cerrada bajo el producto punto a punto. Se comprobará si este producto es asociativo, para ello sean χ, θ y $\varphi \in \widehat{G}$

$$\begin{aligned}\chi \cdot [\theta \cdot \varphi](g) &= \chi(g) \cdot (\theta \cdot \varphi)(g);\text{ aplicando la definición}\\ &= \chi(g)\theta(g)\varphi(g)\\ &= (\chi \cdot \theta)(g)\varphi(g);\text{ asociando convenientemente}\\ &= [\chi \cdot \theta].\varphi(g)\end{aligned}$$

Por lo tanto se dice que es asociativo. Se probará la conmutatividad, sean χ, $\theta \in \widehat{G}$

$$\begin{aligned}\chi \cdot \theta(g) &= \chi(g)\theta(g);\text{ aplicando la definición}\\ &= \theta(g)\chi(g);\text{ recuérdese que } \mathbb{C}^* \text{ es conmutativo}\\ &= \theta \cdot \chi(g)\end{aligned}$$

La identidad es el carácter trivial $\chi_1(g) = 1$ para todo $g \in G$. La inversa viene dada por

$$\begin{aligned}\chi^{-1}(g) &= \chi(g^{-1});\text{ por propiedades de los homomorfismos } {}^{(3)}\\ &= \overline{\chi(g)}\end{aligned}$$

(ya que χ es unitaria[(4)]), además χ^{-1} es un carácter, porque los caracteres pueden ser definidos como un elemento de $L(G)$ hacia $\mathbb{C}$ y estos son homomorfismos, por lo tanto el inverso es el homomorfismo que me lleva a los inversos para el cual la composición es la vía de operación, además el carácter es la traza de una matriz de representación, por lo tanto, el carácter inverso sera la traza de la inversa de esa representación. Por ende se tiene que $\chi \cdot \chi^{-1} = \chi_1$. Así $\widehat{G}$ es un grupo abeliano. Ya se sabía que el número de caracteres irreducibles de G es $|G|$ (una conclusión del Corolario 2.4.9). Lo cual completa la demostración. □

Ejemplo 3.3.3. Sea $G = \mathbb{Z}/n\mathbb{Z}$. Entonces $\widehat{G} = \{\chi_0, \ldots, \chi_{n-1}\}$ con

$$\chi_k\,([m]) = e^{2\pi i k m/n}$$

Entonces la asignación $[k] \mapsto \chi_k$ es un isomorfismo de grupo $G \longrightarrow \widehat{G}$.

[(4)] Lema 2.2.6

Desarrollo. Se verifica que existe el isomorfismo

$$\begin{aligned}\varphi\colon G &\longrightarrow \widehat{G}\\ [k] &\mapsto \chi_k\end{aligned}$$

Se debe probar que es homomorfismo, para ello, sean $[k]$, $[m]$ y $[p] \in \mathbb{Z}/n\mathbb{Z}$ entonces

$$\begin{aligned}\varphi([k+p])([m]) &= \chi_{k+p}([m]);\text{ para todo } [m] \in \mathbb{Z}/n\mathbb{Z}\\ &= e^{2\pi i(k+p)m/n}\\ &= e^{2\pi i(k)m/n}e^{2\pi i(p)m/n}\\ &= \chi_k([m])\chi_p([m])\\ &= \chi_k \cdot \chi_p([m])\\ &= \varphi([k]) \cdot \varphi([p])([m])\end{aligned}$$

Por lo tanto es homomorfismo. Además, debe comprobarse que es inyectiva, para ello sean $[k]$, $[p]$ y $[m] \in \mathbb{Z}/n\mathbb{Z}$ entonces

$$\begin{aligned}\varphi([k]) &= \varphi([p])([m])\text{ entonces para todo } [m] \in \mathbb{Z}/n\mathbb{Z}\\ \chi_k([m]) &= \chi_p([m])\\ e^{2\pi i(k)m/n} &= e^{2\pi i(p)m/n};\text{ pero esto es cierto cuando}\\ e^{2\pi i(k-p)m/n} &= 1;\text{ con } (k-p)m/n \in \mathbb{Z} \Longrightarrow n \mid (k-p) \Longrightarrow k \equiv p(\quad(\text{mód })n)\\ \Longleftrightarrow [k] &= [p]\end{aligned}$$

Por tanto es inyectiva, para continuar con la sobreyección observése que $\widehat{\mathbb{Z}/n\mathbb{Z}}$ tiene orden n, al igual que $\mathbb{Z}/n\mathbb{Z}$ y como se tiene una función inyectiva que va de un grupo finito a otro con el mismo orden, entonces también es sobreyectiva. Por tanto al ser un homomorfismo biyectivo se puedes concluir que es un isomorfismo. □

Observación 3.3.4. *Nótese que la asignación $[k] \mapsto \chi_k$ permite deducir que a cada clase le corresponderá un solo carácter.*

El ejemplo mostrado, presenta una situación en la que siempre se tiene que $G \cong \widehat{G}$, esto se deduce del ejemplo, de los resultados de la **Sección 2.5** y el hecho de que cada grupo finito abeliano es un producto directo de grupos cíclicos.

Ahora se introducirá un isomorfismo de espacio vectorial $L(G) \longrightarrow L(\widehat{G})$ llamado *Transformada de Fourier*. Para hacer un homomorfismo de anillos, se tendrá que usar un producto diferente en $L(\widehat{G})$ que viene siendo la convolución.

Definición 3.3.5. (**Transformada de Fourier**)[(5)].

[(5)] Esta es la definición de la Transformada de Fourier de un Espacio Vectorial.

Sea $f * G \longrightarrow \mathbb{C}$ una función compleja evaluada en un grupo abeliano finito G. Entonces la *Transformada de Fourier* $\widehat{f} * \widehat{G} \longrightarrow \mathbb{C}$ está definida por

$$\widehat{f}(\chi) = |G|\langle f, \chi\rangle = \sum_{g\in G} f(g)\overline{\chi(g)}$$

Los números complejos $|G|\langle f, \chi\rangle$ son a menudo llamados *coeficientes de Fourier* de f.

En la **Sección 3.1**, se definió la transformada de Fourier en una forma distinta para grupos cíclicos. Sin embargo, es equivalente bajo el isomorfismo entre $\widehat{G}$ y G considerado en el ejemplo 3.3.3.

Ejemplo 3.3.6. Si $\chi, \theta \in \widehat{G}$, entonces $\widehat{\chi} = |G|\delta_\chi$.

Desarrollo. Aplicando la definición de transformada de Fourier a χ se tiene

$$\begin{aligned}\widehat{\chi} &= |G|\langle \chi, \theta\rangle; \text{ aplicando el Teorema 2.3.9 a } \chi \text{ y } \theta \text{ se tiene}\\ &= |G| \begin{cases} 1 & ; \text{si } \chi \sim \theta \\ 0 & ; \text{caso contrario} \end{cases}\end{aligned}$$

Como χ, $\theta \in \widehat{G}$, se sabe que a este conjunto pertenecen todas las representaciones irreducibles, por lo que si hay dos que son equivalentes implica que son iguales, de aquí que

$$\begin{aligned}\widehat{\chi} &= |G| \begin{cases} 1 & ; \text{si } \chi = \theta \\ 0 & ; \text{caso contrario} \end{cases}\\ &= |G|\delta_\chi\end{aligned}$$

□

Teorema 3.3.7. ***(Inversión de Fourier).***

Si $f \in L(G)$, entonces

$$f = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi$$

Demostración. Como los caracteres forman una base ortonormal para G, se puede escribir a f como sigue y realizar un calculo sencillo:

$$\begin{aligned} f &= \sum_{\chi\in\widehat{G}} \langle f, \chi\rangle\chi\\ &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}} |G|\langle f, \chi\rangle\chi\\ &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi\end{aligned}$$

tal y como se requiere. □

Observación 3.3.8. *Nótese que la Proposición 3.1.3 es un caso particular del teorema anterior.*

A continuación se observa que la Transformada de Fourier es un mapeo lineal.

Proposición 3.3.9. *El mapeo $T\colon L(G) \longrightarrow L(\widehat{G})$ dado por $Tf = \widehat{f}$ es una transformación lineal invertible.*

Demostración. Sea $|G| = n$, f_1 y $f_2 \in L(G)$, se sabe por definición que $T(c_1f_1 + c_2f_2) = \widehat{c_1f_1 + c_2f_2}$. Se probará que es una transformación lineal

$$\begin{aligned}
T(c_1f_1 + c_2f_2)(\chi) &= (\widehat{c_1f_1 + c_2f_2})(\chi); \text{ aplicando la definición} \\
&= |G|\langle c_1f_1 + c_2f_2, \chi\rangle; \text{ por la transformada de Fourier} \\
&= n(c_1\langle f_1, \chi\rangle + c_2\langle f_2, \chi\rangle); \text{ por linealidad por la izquierda} \\
&= c_1n\langle f_1, \chi\rangle + c_2n\langle f_2, \chi\rangle \\
&= c_1\widehat{f}_1(\chi) + c_2\widehat{f}_2(\chi) \\
&= c_1T(f_1) + c_2T(f_2)
\end{aligned}$$

y así se establece que T es lineal, ahora se debe probar que también es inyectiva ya que si

$$\begin{aligned}
T(f_1) &= T(f_2) \\
\text{para } \chi \in \widehat{G} \text{ se tiene } \widehat{f}_1(\chi) &= \widehat{f}_2(\chi) \\
\frac{1}{n}\widehat{f}_1(\chi) &= \frac{1}{n}\widehat{f}_2(\chi) \\
\frac{1}{n}\widehat{f}_1(\chi)\chi &= \frac{1}{n}\widehat{f}_2(\chi)\chi
\end{aligned}$$

al tomar χ arbitrario, se observa que la igualdad se mantiene, sin perdida de generalidad se puede sumar todos los elementos de $\widehat{G}$ de la siguiente forma

$$\begin{aligned}
\frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{f}_1(\chi_i)\chi &= \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{f}_2(\chi_i)\chi; \text{ aplicando el Teorema 3.3.7 se tiene} \\
f_1 &= f_2
\end{aligned}$$

Lo que implica que T es una función lineal inyectiva, por otro lado como es un mapeo lineal inyectivo, la dimensión de la imagen es la dimensión del dominio (debido a que por cada elemento hay una función), es decir, $\dim L(G) = n = \dim L(\widehat{G})$, de aquí que T es sobreyectiva, con lo cual decimos que es biyectiva y por lo tanto invertible. □

Sea A un grupo abeliano. Existen dos caminos para hacer a $L(A)$ un anillo, uno es a través de la convolución; el otro es usar la multiplicación punto a punto: $(f\cdot g)(x) = f(x)g(x)$. Observése que δ_1 es la identidad para la convolución y el mapeo constante a 1 es la identidad para el producto punto a punto. El siguiente teorema demuestra que la transformada de Fourier da el isomorfismo entre estas dos estructuras de anillo, esto es, envía la convolución a la multiplicación punto a punto.

Teorema 3.3.10. *La Transformada de Fourier satisface*

$$\widehat{a * b} = \widehat{a} \cdot \widehat{b}$$

En consecuencia, el mapeo lineal $T\colon L(G) \longrightarrow L(\widehat{G})$ *dado por* $Tf = \widehat{f}$ *provee un isomorfismo de anillos entre* $(L(G), +, *)$ *y* $(L(\widehat{G}), +, \cdot)$.

Demostración. Por lo desarrollado en la proposición anterior, se sabe que T es un isomorfismo de espacios vectoriales con la suma, entonces para demostrar que es un isomorfismo de anillos bastaría con demostrar que también cumple para el producto $T(a * b) = Ta \cdot Tb$, es decir, $\widehat{a * b} = \widehat{a} \cdot \widehat{b}$. Sea $n = |G|$ entonces

$$\begin{aligned}
\widehat{a * b}(\chi) &= n\langle a * b, \chi\rangle \\
&= n \cdot \frac{1}{n} \sum_{x \in G} (a * b)(x)\overline{\chi(x)}; \text{ por la definición de la transformada de Fourier para } (a * b)(x) \\
&= \sum_{x \in G} \sum_{y \in G} a(xy^{-1})b(y)\overline{\chi(x)}; \text{ aplicando la definición de la convolución} \\
&= \sum_{y \in G} b(y) \sum_{x \in G} a(xy^{-1})\overline{\chi(x)}
\end{aligned}$$

Hacemos un cambio de variables $z = xy^{-1}$, con lo cual $(x = zy)$. Entonces se obtiene

$$\begin{aligned}
\widehat{a * b}(\chi) &= \sum_{y \in G} b(y) \sum_{z \in G} a(z)\overline{\chi(zy)} \\
&= \sum_{y \in G} b(y) \sum_{z \in G} a(z)\overline{\chi(z)\chi(y)} \\
&= \sum_{y \in G} b(y)\overline{\chi(y)} \sum_{z \in G} a(z)\overline{\chi(z)}
\end{aligned}$$

Multiplicamos por "1"

$$\begin{aligned}
\sum_{y \in G} b(y)\overline{\chi(y)} \sum_{z \in G} a(z)\overline{\chi(z)} &= n.\frac{1}{n} \sum_{z \in G} a(z)\overline{\chi(z)} n.\frac{1}{n} \sum_{y \in G} b(y)\overline{\chi(y)} \\
&= n\langle a, \chi\rangle n\langle b, \chi\rangle \\
&= \widehat{a}(\chi)\widehat{b}(\chi) \\
&= \widehat{a} \cdot \widehat{b}(\chi)
\end{aligned}$$

y así $\widehat{a * b} = \widehat{a} \cdot \widehat{b}$, como era requerido. □

Funciones Periódicas en $\mathbb{Z}$

A continuación, se hace un resumen de lo que se ha podido demostrar para el caso clásico de funciones periódicas en $\mathbb{Z}$, en donde $\mathbb{Z}/n\mathbb{Z}$ lo identificamos con $\widehat{\mathbb{Z}/n\mathbb{Z}}$ a través del isomorfismo $[k] \mapsto \chi_k$.

Sean $f,\ g * \mathbb{Z} \longrightarrow \mathbb{C}$ funciones periódicas con periodo n y sea $m \in \mathbb{Z}$, entonces por la biyección que existe entre las funciones periódicas y los elementos de $L(\mathbb{Z}/n\mathbb{Z})$ (vista al principio de este capitulo), se sabe que se puede trabajar con las funciones enteras modulo n en vez de las funciones periódicas y así en vez de tomar la clase de equivalencia $[k]$ se trabaja con el entero k modulo n, siempre y cuando se tenga un número finito de k. Por lo anterior se puede definir la convolución, la transformada de Fourier y la inversa de Fourier como sigue:

La convolución: $f * g(m) = \sum_{k=0}^{n-1} f(m-k)g(k).$

La transformada de Fourier[(6)]: $\widehat{f}(m) = \sum_{k=0}^{n-1} f(k)e^{-2\pi imk/n}.$

La inversión de Fourier: $f(m) = \frac{1}{n}\sum_{k=0}^{n-1} \widehat{f}\,(k)\, e^{2\pi imk/n}.$

La fórmula de multiplicación dice que $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$. En la práctica para calcular $\widehat{f * g}$ es más fácil calcular $\widehat{a} \cdot \widehat{b}$ y luego aplicar la inversión de Fourier para obtener $f * g$.

3.4. Una aplicación a la teoría de grafos

Un *grafo* Γ consiste en un conjunto V de *vértices* y en un conjunto E de pares no ordenados de elementos de V, llamados *bordes* o *aristas*. Sólo se consideraran grafos finitos en esta sección.

A menudo, los grafos se ilustran gráficamente representando cada vértice como un punto y dibujando un segmento de línea entre dos vértices para que formar un borde.

Definición 3.4.1. (**Matriz adyacente**).

Sea Γ un grafo con con un conjunto de vértices $V = \{v_1, \ldots, v_n\}$ y un conjunto de aristas B. Entonces la matriz adyacente $A = (a_{ij})$ esta dada por $a_{ij} = \begin{cases} 1 & ; \text{si } \{v_i, v_j\} \in B \\ 0 & ; \text{caso contrario} \end{cases}$

Ejemplo 3.4.2. Si Γ tiene un conjunto de vértices $V = \{1, 2, 3, 4\}$ y un conjunto de aristas $B = \{\{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$, entonces el grafo queda como sigue

[(6)] Puede verificarse la Definición 3.1.2

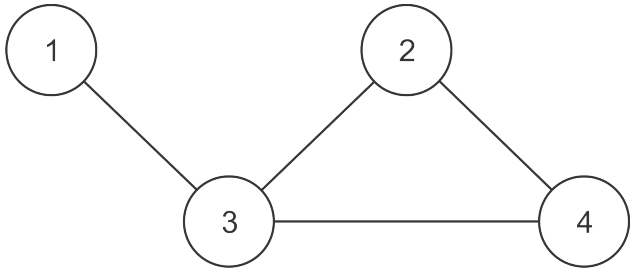

Figura 3.1: Un ejemplo de grafo

Y la matriz adyacente es $A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

Desarrollo. Para obtener los componentes de la matriz de adyacencia calculamos cada a_{ij} utilizando la definición

$$\begin{array}{ll} \{1,1\} \notin B \Longrightarrow a_{11} = 0 & \{2,1\} \notin B \Longrightarrow a_{21} = 0 \\ \{1,2\} \notin B \Longrightarrow a_{12} = 0 & \{2,2\} \notin B \Longrightarrow a_{22} = 0 \\ \{1,3\} \in B \Longrightarrow a_{13} = 1 & \{2,3\} \in B \Longrightarrow a_{23} = 1 \\ \{1,4\} \notin B \Longrightarrow a_{14} = 0 & \{2,4\} \in B \Longrightarrow a_{24} = 1 \end{array}$$

$$\begin{array}{ll} \{3,1\} \in B \Longrightarrow a_{31} = 1 & \{4,1\} \notin B \Longrightarrow a_{41} = 0 \\ \{3,2\} \in B \Longrightarrow a_{32} = 1 & \{4,2\} \in B \Longrightarrow a_{42} = 1 \\ \{3,3\} \notin B \Longrightarrow a_{33} = 0 & \{4,3\} \in B \Longrightarrow a_{43} = 1 \\ \{3,4\} \in B \Longrightarrow a_{34} = 1 & \{4,4\} \notin B \Longrightarrow a_{44} = 0 \end{array}$$

□

Nótese que la matriz adyacente es simétrica y por ende diagonalizable con valores propios reales por *el teorema espectral de matrices*. El conjunto de valores propios de A se le llama *espectro* del grafo; este no depende del orden de los vértices. Se puede obtener información importante a partir de los valores propios, como la cantidad de árboles recubridores. Además A_{ij}^n es el número de caminos de longitud n desde vi hasta v_j, ya que, por ejemplo, al realizar el producto $A_{ij} \times A_{ij}$, se tendrá que $A_{ij} = \sum_{k=1}^{n} a_{ik}a_{kj}$ será diferente de cero cuando en la posición a_{ik} y en la posición a_{kj} haya un 1, esto indica que existe un camino que une a ambos vértices, luego al realizar esto $\underbrace{A_{ij} \times \cdots \times A_{ij}}_{n-veces}$, se sabe que se obtendrá el número de caminos entre un vértice y otro. Para una matriz diagonalizable, conocer los valores propios da mucha información acerca de las potencias de las matrices. Existe un área completa de teoría de grafos, llamada *teoría de grafos espectrales*, dedicada a estudiar grafos a través de

sus valores propios. La matriz de adyacencia también está estrechamente relacionada con el estudio de caminos aleatorios en los grafos.

Una fuente natural de grafos, conocidos como grafos de Cayley, proviene de la teoría de grupos. La Teoría de Representaciones proporciona un medio para analizar los valores propios de los grafos de Cayley, al menos para los grupos abelianos.

Definición 3.4.3. (**Grafo de Cayley**).

Sea G un grupo finito, cuando se habla de un *subconjunto simétrico* de G, se quiere decir que $S \subseteq G$ de manera que:

- $1 \notin S$;
- $s \in S$ implica $s^{-1} \in S$.

Si S es un subconjunto simétrico de G, entonces el grafo de *Cayley* de G con respecto a S es el grafo con un conjunto de vértices G y con una arista $\{g, h\}$ conectando a g y h si $gh^{-1} \in S$, o de forma equivalente $hg^{-1} \in S$.

Observación 3.4.4. *En esta definición S puede estar vacío, en cuyo caso el grafo de Cayley no tiene bordes.*

Ejemplo 3.4.5. El grafo de *Cayley* esta conectado (cualquiera dos vértices puede estar conectado por un camino) si y solo si S genera a G.

Desarrollo. "$\Longrightarrow$" *El grafo de Cayley esta conectado entonces S genera a G.*

Tomemos $g \in G$ arbitrario, se sabe que $S \neq \varnothing$, además si $s \in S$ por definición $s^{-1} \in S$ entonces g esta conectado con 1 porque existe un camino por conectividad en el grafo, por lo tanto existe la sucesión siguiente gh_1^{-1}, $h_1^{-1}h_2$, ..., $h_k \in S$, es decir,

$$g \bullet\overset{gh_1^{-1}}{---}\bullet\overset{h_1}{---}\bullet\overset{h_1^{-1}h_2}{---}\bullet\overset{h_2}{---}\bullet\overset{\cdots}{---}\bullet\overset{h_{k-1}}{---}\bullet\overset{h_{k-1}^{-1}h_k}{---}\bullet\overset{h_k}{---}\bullet\overset{h_k}{---}\bullet 1$$

por lo tanto $g = gh_1^{-1} \cdots h_k \in \langle S \rangle$ y todos los $h_{i-1}h_i$ están en S, de esta forma el producto de todos estos elementos estaría en $\langle S \rangle$ y como este elemento fue tomado arbitrariamente, significa que S genera a G.

"$\Longleftarrow$" *Si S genera a G entonces el grafo de Cayley esta conectado.*

Si S genera a G, por definición se sabe que $S^{-1} = \{s^{-1} |\ s \in S\} \subseteq S$ entonces $\langle S \rangle = \{s_1 \cdots s_n |\ n \in \mathbb{N},\ s_1, \cdots, s_n \in S\}$ y lo que se quiere demostrar es que esta conectado, es decir, hay un vértice si un elemento s multiplicado por su inverso pertenece a S. Véase que existe un camino entre g y 1. Sea $g \in \langle S \rangle$ tal que $g = s_1 s_2 \cdots s_n$ y

$$g \bullet\overset{s_1}{---}\bullet\overset{s_1^{-1}g}{---}\bullet\overset{s_2}{---}\bullet\overset{(s_1s_{21})^{-1}g}{---}\bullet\overset{\cdots}{---}\bullet\overset{(s_1s_{21}\cdots s_n)^{-1}g}{---}\bullet\overset{s_n}{---}\bullet 1$$

Por lo tanto existe un camino que lleva de g a 1 y como este elemento fue tomado arbitrariamente, significa que cualesquiera dos elementos están conectados por al menos un camino. □

Ejemplo 3.4.6. Sea $G = \mathbb{Z}/4\mathbb{Z}$ y $S = \{\pm[1]\}$. Se encontrará el grafo de Cayley y su matriz de adyacencia.

Desarrollo. Para encontrar el grafo se hace uso de la definición, se tiene $S = \{\pm[1]\}$ y $\mathbb{Z}/4\mathbb{Z} = \{[0],[1],[2],[3]\}$, entonces

$$\begin{array}{llll} \{[0],[0]\} \Longrightarrow [0]+[0] = [0] & \notin S & \{[1],[0]\} \Longrightarrow [1]+[0] = [1] & \in S \\ \{[0],[1]\} \Longrightarrow [0]+[3] = -[1] & \in S & \{[1],[1]\} \Longrightarrow [1]+[3] = [0] & \notin S \\ \{[0],[2]\} \Longrightarrow [0]+[2] = [2] & \notin S & \{[1],[2]\} \Longrightarrow [1]+[2] = -[1] & \in S \\ \{[0],[3]\} \Longrightarrow [0]+[1] = [1] & \in S & \{[1],[3]\} \Longrightarrow [1]+[1] = [2] & \notin S \end{array}$$

$$\begin{array}{llll} \{[2],[0]\} \Longrightarrow [2]+[0] = [2] & \notin S & \{[3],[0]\} \Longrightarrow [3]+[0] = -[1] & \in S \\ \{[2],[1]\} \Longrightarrow [2]+[3] = [1] & \in S & \{[3],[1]\} \Longrightarrow [3]+[3] = [2] & \notin S \\ \{[2],[2]\} \Longrightarrow [2]+[2] = [0] & \notin S & \{[3],[2]\} \Longrightarrow [3]+[2] = [1] & \in S \\ \{[2],[3]\} \Longrightarrow [2]+[1] = -[1] & \in S & \{[3],[3]\} \Longrightarrow [3]+[1] = [0] & \notin S \end{array}$$

Entonces el grafo de Cayley de G respecto a S se dibuja en la figura 3.2.

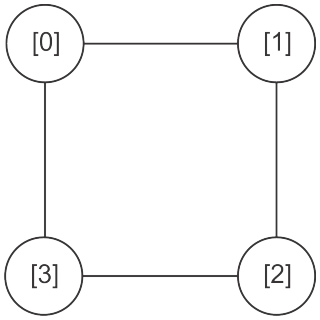

Figura 3.2: El grafo de Cayley de $\mathbb{Z}/4\mathbb{Z}$ con respecto a $\{\pm[1]\}$

Ahora para calcular la matriz adyacente de este grafo de Cayley se tiene un conjunto de vértices $V = \{[0],[1],[2],[3]\} = \{v_1, v_2, v_3, v_4\}$ y un conjunto de aristas

$$\begin{aligned} B &= \{\{[0],[1]\},\{[0],[3]\},\{[1],[2]\},\{[2],[3]\}\} \\ &= \{\{v_1, v_2\},\{v_1, v_4\},\{v_2, v_3\},\{v_3, v_4\}\} \end{aligned}$$

Así calculamos

$$\begin{array}{ll} \{[0],[0]\} \notin B \Longrightarrow a_{11} = 0 & \{[1],[0]\} \in B \Longrightarrow a_{21} = 1 \\ \{[0],[1]\} \in B \Longrightarrow a_{12} = 1 & \{[1],[1]\} \notin B \Longrightarrow a_{22} = 0 \\ \{[0],[2]\} \notin B \Longrightarrow a_{13} = 0 & \{[1],[2]\} \in B \Longrightarrow a_{23} = 1 \\ \{[0],[3]\} \in B \Longrightarrow a_{14} = 1 & \{[1],[3]\} \notin B \Longrightarrow a_{24} = 0 \end{array}$$

$$\{[2],[0]\} \notin B \Longrightarrow a_{31} = 0 \qquad \{[3],[0]\} \in B \Longrightarrow a_{41} = 1$$
$$\{[2],[1]\} \in B \Longrightarrow a_{32} = 1 \qquad \{[3],[1]\} \notin B \Longrightarrow a_{42} = 0$$
$$\{[2],[2]\} \notin B \Longrightarrow a_{33} = 0 \qquad \{[3],[2]\} \in B \Longrightarrow a_{43} = 1$$
$$\{[2],[3]\} \in B \Longrightarrow a_{34} = 1 \qquad \{[3],[3]\} \notin B \Longrightarrow a_{44} = 0$$

y la matriz de adyacencia queda como:

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

□

Ejemplo 3.4.7. En este ejemplo se toma a $G = \mathbb{Z}/6\mathbb{Z}$ y $S = \{\pm[1], \pm[2]\}$ y se encontrará el grafo de Cayley (figura 3.3) y la matriz de adyacencia.

Desarrollo. Para encontrar el grafo se hará uso de la definición, se tiene $S = \{\pm[1], \pm[2]\}$ y $\mathbb{Z}/6\mathbb{Z} = \{[0],[1],[2],[3],[4],[5]\}$, entonces

$$\begin{array}{llll} \{[0],[0]\} \Longrightarrow [0]+[0] = [0] \notin S & & \{[1],[0]\} \Longrightarrow [1]+[0] = [1] \in S \\ \{[0],[1]\} \Longrightarrow [0]+[5] = -[1] \in S & & \{[1],[1]\} \Longrightarrow [1]+[5] = [0] \notin S \\ \{[0],[2]\} \Longrightarrow [0]+[4] = -[2] \in S & & \{[1],[2]\} \Longrightarrow [1]+[4] = -[1] \in S \\ \{[0],[3]\} \Longrightarrow [0]+[3] = [3] \notin S & & \{[1],[3]\} \Longrightarrow [1]+[3] = -[2] \in S \\ \{[0],[4]\} \Longrightarrow [0]+[2] = [2] \in S & & \{[1],[4]\} \Longrightarrow [1]+[2] = [3] \notin S \\ \{[0],[5]\} \Longrightarrow [0]+[1] = [1] \in S & & \{[1],[5]\} \Longrightarrow [1]+[1] = [2] \in S \end{array}$$

$$\begin{array}{llll} \{[2],[0]\} \Longrightarrow [2]+[0] = [2] \in S & & \{[3],[0]\} \Longrightarrow [3]+[0] = [3] \notin S \\ \{[2],[1]\} \Longrightarrow [2]+[5] = [1] \in S & & \{[3],[1]\} \Longrightarrow [3]+[5] = [2] \in S \\ \{[2],[2]\} \Longrightarrow [2]+[4] = [0] \notin S & & \{[3],[2]\} \Longrightarrow [3]+[4] = [1] \in S \\ \{[2],[3]\} \Longrightarrow [2]+[3] = -[1] \in S & & \{[3],[3]\} \Longrightarrow [3]+[3] = [0] \notin S \\ \{[2],[4]\} \Longrightarrow [2]+[2] = -[2] \in S & & \{[3],[4]\} \Longrightarrow [3]+[2] = -[1] \in S \\ \{[2],[5]\} \Longrightarrow [2]+[1] = [3] \notin S & & \{[3],[5]\} \Longrightarrow [3]+[1] = -[2] \in S \end{array}$$

$$\begin{array}{llll} \{[4],[0]\} \Longrightarrow [4]+[0] = -[2] \in S & & \{[5],[0]\} \Longrightarrow [5]+[0] = -[1] \in S \\ \{[4],[1]\} \Longrightarrow [4]+[5] = [3] \notin S & & \{[5],[1]\} \Longrightarrow [5]+[5] = -[2] \in S \\ \{[4],[2]\} \Longrightarrow [4]+[4] = [2] \in S & & \{[5],[2]\} \Longrightarrow [5]+[4] = [3] \notin S \\ \{[4],[3]\} \Longrightarrow [4]+[3] = [1] \in S & & \{[5],[3]\} \Longrightarrow [5]+[3] = [2] \notin S \\ \{[4],[4]\} \Longrightarrow [4]+[2] = [0] \notin S & & \{[5],[4]\} \Longrightarrow [5]+[2] = [1] \in S \\ \{[4],[5]\} \Longrightarrow [4]+[1] = -[1] \in S & & \{[5],[5]\} \Longrightarrow [5]+[1] = [0] \notin S \end{array}$$

Entonces el grafo de Cayley de G respecto a S se dibuja en la figura 3.3.

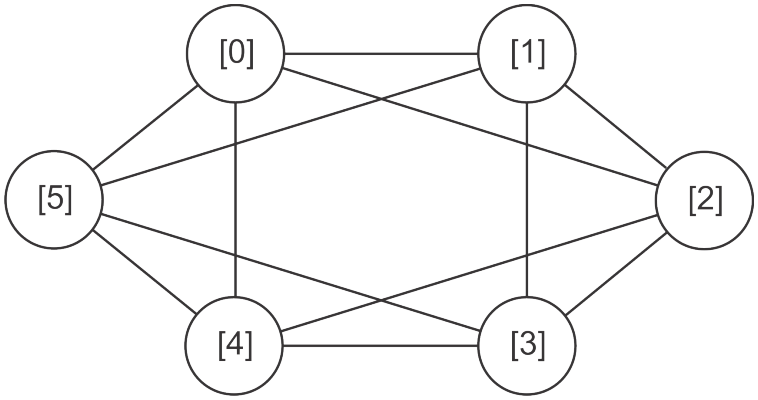

Figura 3.3: El grafo de Cayley de $\mathbb{Z}/6\mathbb{Z}$ con respecto a $\{\pm[1], \pm[2]\}$

Ahora para calcular la matriz adyacente de esté se tiene un conjunto de vértices $V = \{[0],[1],[2],[3],[4],[5]\} = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ y un conjunto de aristas

$$B = \left\{ \begin{array}{l} \{[0],[1]\}, \{[0],[2]\}, \{[0],[4]\}, \{[0],[5]\}, \{[1],[2]\}, \{[1],[3]\}, \\ \{[1],[5]\}, \{[2],[3]\}, \{[2],[4]\}, \{[3],[4]\}, \{[3],[5]\}, \{[4],[5]\} \end{array} \right\}$$

$$B = \left\{ \begin{array}{l} \{v_1, v_2\}, \{v_1, v_3\}, \{v_1, v_5\}, \{v_1, v_6\}, \{v_2, v_3\}, \{v_2, v_4\}, \\ \{v_2, v_6\}, \{v_3, v_4\}, \{v_3, v_5\}, \{v_4, v_5\}, \{v_4, v_6\}, \{v_5, v_6\} \end{array} \right\}$$

Así se calcula

$$\begin{array}{ll} \{[0],[0]\} \notin B \Longrightarrow a_{11} = 0 & \{[1],[0]\} \in B \Longrightarrow a_{21} = 1 \\ \{[0],[1]\} \in B \Longrightarrow a_{12} = 1 & \{[1],[1]\} \notin B \Longrightarrow a_{22} = 0 \\ \{[0],[2]\} \in B \Longrightarrow a_{13} = 1 & \{[1],[2]\} \in B \Longrightarrow a_{23} = 1 \\ \{[0],[3]\} \notin B \Longrightarrow a_{14} = 0 & \{[1],[3]\} \in B \Longrightarrow a_{24} = 1 \\ \{[0],[4]\} \in B \Longrightarrow a_{15} = 1 & \{[1],[4]\} \notin B \Longrightarrow a_{25} = 0 \\ \{[0],[5]\} \in B \Longrightarrow a_{16} = 1 & \{[1],[5]\} \in B \Longrightarrow a_{26} = 1 \end{array}$$

$$\begin{array}{ll} \{[2],[0]\} \in B \Longrightarrow a_{31} = 1 & \{[3],[0]\} \notin B \Longrightarrow a_{41} = 0 \\ \{[2],[1]\} \in B \Longrightarrow a_{32} = 1 & \{[3],[1]\} \in B \Longrightarrow a_{42} = 1 \\ \{[2],[2]\} \notin B \Longrightarrow a_{33} = 0 & \{[3],[2]\} \in B \Longrightarrow a_{43} = 1 \\ \{[2],[3]\} \in B \Longrightarrow a_{34} = 1 & \{[3],[3]\} \notin B \Longrightarrow a_{44} = 0 \\ \{[2],[4]\} \in B \Longrightarrow a_{35} = 1 & \{[3],[4]\} \in B \Longrightarrow a_{45} = 1 \\ \{[2],[5]\} \notin B \Longrightarrow a_{36} = 0 & \{[3],[5]\} \in B \Longrightarrow a_{46} = 1 \end{array}$$

$$\begin{aligned}
\{[4],[0]\} \in B &\Longrightarrow a_{51} = 1 & \{[5],[0]\} \in B &\Longrightarrow a_{61} = 1\\
\{[4],[1]\} \notin B &\Longrightarrow a_{52} = 0 & \{[5],[1]\} \in B &\Longrightarrow a_{62} = 1\\
\{[4],[2]\} \in B &\Longrightarrow a_{53} = 1 & \{[5],[2]\} \notin B &\Longrightarrow a_{63} = 0\\
\{[4],[3]\} \in B &\Longrightarrow a_{54} = 1 & \{[5],[3]\} \in B &\Longrightarrow a_{64} = 1\\
\{[4],[4]\} \notin B &\Longrightarrow a_{55} = 0 & \{[5],[4]\} \in B &\Longrightarrow a_{65} = 1\\
\{[4],[5]\} \in B &\Longrightarrow a_{56} = 1 & \{[5],[5]\} \notin B &\Longrightarrow a_{66} = 0
\end{aligned}$$

y la matriz de adyacencia queda como:

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

□

Las grafos que se han considerado son grafos de Cayley de grupos cíclicos. Este tipo de grafos tiene un nombre especial.

Definición 3.4.8. (**Grafo Circulante**)

Un grafo de Cayley $\mathbb{Z}/n\mathbb{Z}$ es llamado *grafo circulante* (en n vértices).

La matriz adyacente de un grafo circulante es un ejemplo de un tipo especial de matriz conocida como matriz circulante.

Definición 3.4.9. (**Matriz Circulante**).

Una matriz circulante $n \times n$ es una matriz de la forma

$$A = \begin{bmatrix}
a_0 & a_1 & \cdots & a_{n-2} & a_{n-1}\\
a_{n-1} & a_0 & a_1 & \cdots & a_{n-2}\\
\vdots & a_{n-1} & a_0 & \ddots & \vdots\\
a_2 & \vdots & \ddots & \ddots & a_1\\
a_1 & a_2 & \cdots & a_{n-1} & a_0
\end{bmatrix} \tag{3.8}$$

En donde se puede observar que cada columna se obtiene de la anterior al hacer un desplazamiento cíclico hacia abajo. La matriz esta completamente definida por un vector v que en este caso es la primera columna, las demás columnas de la matriz son permutaciones cíclicas de la primera. Por otro lado, la última fila es el vector v pero en orden inverso y las demás filas son también permutaciones cíclicas de esta fila. De forma equivalente, puede decirse que si existe una función $f\colon \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}$ tal que $A_{ij} = f([j]-[i])$, en (3.8), se tiene que $a_i = f([i])$ para $0 \leq i \leq n-1$. Así por ejemplo si se quisiera encontrar $A_{n-1,1}$ se haría:

$$\begin{aligned}
A_{n-1,1} &= f([1]-[n-1])\\
&= f([1-(n-1)])\\
&= f([2-n])\\
&= f([2])\\
&= a_2
\end{aligned}$$

Si S es un subconjunto simétrico de $\mathbb{Z}/n\mathbb{Z}$, entonces la matriz circulante correspondiente a las funciones características δ_S de S es la matriz adyacente de la gráfica de Cayley de $\mathbb{Z}/n\mathbb{Z}$ con respecto a S.

El objetivo es describir los valores propios de la gráfica de Cayley de un grupo abeliano. Pero primero se necesita un lema acerca del álgebra de grupo de $L(G)$.

Lema 3.4.10. *Sea G un grupo abeliano y $a \in L(G)$. Se define el operador convolución $A * L(G) \longrightarrow L(G)$ por $A(b) = a * b$. Entonces A es lineal y χ es un vector propio de A con valor propio $\widehat{a}(\chi)$ para todo $\chi \in \widehat{G}$. Consecuentemente, A es un operador diagonalizable.*

Demostración. Usando la distributividad de la convolución sobre la suma, se verifica que A es lineal. Sea $a \in L(G)$, se aplica la definición del operador convolución y se tiene que

$$\begin{aligned}
A(vb + wc) &= a * (vb + wc) \\
&= a * (vb) + a * (wc); \text{ por el Teorema 3.2.3} \\
&= \sum_{x \in G} \left(v \sum_{y \in G} a(xy^{-1}) b(y) + w \sum_{y \in G} a(xy^{-1}) c(y) \right) \delta_\chi \\
&= \sum_{x \in G} \left(v \sum_{y \in G} a(xy^{-1}) b(y) \right) \delta_x + \sum_{x \in G} \left(w \sum_{y \in G} a(xy^{-1}) c(y) \right) \delta_\chi \\
&= v\,(a * b) + w\,(a * c) \\
&= vA(b) + wA(c)
\end{aligned}$$

Sea $n = |G|$ y supóngase que $\chi \in \widehat{G}$. Observése que

$$\begin{aligned}
\widehat{a * \chi} &= \widehat{a} \cdot \widehat{\chi}; \text{ por el Teorema 3.3.10} \\
&= \widehat{a} \cdot n\delta_\chi; \text{ por el ejemplo 3.3.6}
\end{aligned}$$

Si se aplica $(\widehat{a} \cdot n\delta_\chi)(\theta)$ para $\theta \in \widehat{G}$, en dónde $\delta_\chi(\theta) = 1$ si $\chi = \theta$, entonces se tiene que

$$\begin{aligned}
(\widehat{a} \cdot n\delta_x)(\theta) &= \widehat{a}()n\delta_\chi(); \text{ aplicando la Proposición 3.3.2} \\
&= \begin{cases} \widehat{a}(\theta)n & ; \text{si } \chi = \theta \\ 0 & ; \text{caso contrario} \end{cases}
\end{aligned}$$

Así $\widehat{a} \cdot n\delta_\chi = (\widehat{a}(\chi)n)\,\delta_\chi$. Dados los resultados obtenidos anteriormente se sabe que $\widehat{a * \chi} = \widehat{a}(\chi)n\delta_\chi$, ahora aplicando la transformada inversa de Fourier a esta igualdad se obtiene que

$$\begin{aligned}
a * \chi &= \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{a * \chi}(\chi_1)\chi_1 \\
&= \frac{1}{n} \sum_{\chi \in \widehat{G}} (\widehat{a}(\chi)n\delta_\chi(\chi_1))\,\chi_1 \\
&= \begin{cases} \widehat{a}(\chi)\chi_1 & ; \text{si } \chi_1 = \chi \\ 0 & ; \text{caso contrario} \end{cases} \\
&= \widehat{a}(\chi)\chi
\end{aligned}$$

En otras palabras, $A\chi = \widehat{a}(\chi)\chi$ y así χ es un vector propio de A con valor propio $\widehat{a}(\chi)$.

Los elementos de $\widehat{G}$ forman una base ortonormal de vectores propios para A por el Teorema 2.4.7 y como $\dim L(G) = \dim G = \dim \widehat{G}$ entonces al tener un conjunto de vectores propios $\{\chi_1, \cdots, \chi_n\}$ se tiene

$$\left.\begin{array}{lll} A\chi_1 & = \widehat{a}(\chi_1)\chi_1 & = \widehat{a}(\chi_1)\chi_1 + 0\chi_2 + \ldots + 0\chi_n \\ A\chi_2 & = \widehat{a}(\chi_2)\chi_2 & = 0\chi_1 + \widehat{a}(\chi_2)\chi_2 + \ldots + 0\chi_n \\ & \vdots & \vdots \\ A\chi_n & = \widehat{a}(\chi_n)\chi_n & = 0\chi_1 + 0\chi_2 + \ldots + \widehat{a}(\chi_n)\chi_n \end{array}\right\} \implies \begin{pmatrix} \widehat{a}(\chi_1) & 0 & \cdots & 0 & 0 \\ 0 & \widehat{a}(\chi_2) & 0 & \cdots & 0 \\ \vdots & 0 & \widehat{a}(\chi_3) & \ddots & \vdots \\ 0 & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \widehat{a}(\chi_n) \end{pmatrix}$$

con lo que se deduce que A es diagonalizable. □

El lema anterior es el ingrediente clave para calcular los valores propios de la matriz adyacente del grafo de Cayley de un grupo abeliano. Lo único que resta es corroborar que la matriz de adyacente es la matriz de un operador de convolución.

Teorema 3.4.11. *Sea $G = \{g_1, \ldots, g_n\}$ un grupo abeliano y $S \subseteq G$ un conjunto simétrico. Sea $\chi_1, \ldots, \chi_n$ los caracteres irreducibles de G y A la matriz adyacente del grafo de Cayley de G con respecto a S (usando este orden para los elementos de G). Entonces*

1. *Los valores propios de la matriz adyacente A son números reales*

$$\lambda_i = \sum_{s \in S} \chi_i(s)$$

2. *La base ortonormal correspondiente a los vectores propios viene dada por $\{v_i, \ldots, v_n\}$ donde*

$$v_i = \frac{1}{\sqrt{|G|}} \left(\chi_i(g_1), \ldots, \chi_i(g_n)\right)^T$$

Demostración. Sea $G = \{g_1, \ldots g_n\}$ y $\delta_S = \sum_{s \in S} \delta_s$ la función característica (o indicador) de S, así

$$\delta_S(x) = \begin{cases} 1 & ; \text{si } x \in S \\ 0 & \text{caso contrario} \end{cases}$$

Sea $F \colon L(G) \to L(G)$ el operador convolución

$$F(b) = \delta_S * b$$

El Lema 3.4.10 implica que los caracteres irreducibles χ_i son vectores propios de F y que su correspondiente valor propio es

$\widehat{\delta_S}(\chi_i) = n\langle \delta_S, \chi_i\rangle$; se aplica la definición y $|G| = n$

$$
\begin{aligned}
&= \sum_{x\in G} \delta_S(x)\overline{\chi_i(x)}; \text{ se sabe que } \delta_S(x) = 1 \text{ si } s \in S \text{ tal que } s = x \text{ y } x \in S \\
&= \sum_{s\in S} \overline{\chi_i(s)}; \text{ como una representación de grado 1 es unitaria entonces} \\
&= \sum_{s\in S} \chi_i(s^{-1}); \text{ ya que } S \text{ es simétrico} \\
&= \sum_{s\in S} \chi_i(s) \\
&\text{sea } \lambda_i = \sum_{s\in S} \chi_i(s)
\end{aligned}
$$

En donde los últimos resultados se han obtenido del siguiente hecho

$$
\begin{aligned}
\sum_{s\in S} \chi_i(s^{-1}) &= \sum_{s\in S^{-1}} \chi_i(s) \\
&= \sum_{s\in S} \chi_i(s)
\end{aligned}
$$

con lo que se puede concluir que $S = S^{-1}$, ya que por definición $S^{-1} = \{s^{-1} |\ s \in S\}$.

Ahora, si $B = \{\delta_{g_1}, \ldots \delta_{g_n}\}$ es una base para $L(G)$, entonces la matriz $[F]_B$ de F respecto a esta base tiene valores propios $\lambda_1, \ldots, \lambda_n$ y vectores propios $v_1, \ldots, v_n$. Los v_i son ortonormales ya que los χ_i son ortonormales; como el orden del grupo es $|G| = n$ entonces el tamaño del vector será el orden del grupo, por ello para normalizarlo habrá que multiplicar por el factor de escala $1/\sqrt{|G|}$, además esto viene del hecho que los δ_{g_i} son ortonormales respecto al producto interno $(f_1, f_2) = |G|\langle f_1, f_2\rangle$. Por lo tanto, queda por demostrar que $A = [F]_B$.

Para esto sea $\delta_{g_j} \in B$ y se calcula

$$
\begin{aligned}
F(\delta_{g_j}) &= \delta_S * \delta_{g_j} \\
&= \sum_{s\in S} \delta_s * \delta_{g_j} \\
&= \sum_{s\in S} \delta_{sg_j}; \text{ Por la proposición 3.2.2}
\end{aligned}
$$

Recuérdese que $([F]_B)_{ij}$ es el coeficiente de δ_{g_j} en $F(\delta_{g_j})$, de aquí se concluye que

$$\begin{aligned}([F]_B)_{ij} &= \begin{cases} 1 & g_i = sg_j \text{ ; para algún } s \in S \\ 0 & \text{ ; caso contrario} \end{cases} \\ &= \begin{cases} 1 & g_i g_j^{-1} \in S \text{; si } g_i = sg_j \Longrightarrow s = g_i g_j^{-1} \\ 0 & \text{ ; caso contrario} \end{cases} \\ &= \begin{cases} 1 & \{g_i, g_j\} \quad \text{; por la Definición 3.4.3 existe un camino entre } g_i \text{ y } g_j \\ 0 & \text{ ; caso contrario} \end{cases} \\ &= A_{ij}\end{aligned}$$

en esta última linea se concuerda con la definición 3.4.1, osea la matriz de adyacencia con respecto a S como se requiere.

Finalmente, para verificar que λ_i es real, se observa que si $s \in S$, entonces $s = s^{-1}$ y así $\chi_i(s) = \chi_i(s^{-1}) = \overline{\chi_i(s)}$ es real, o $s \neq s^{-1} \in S$ lo que sería una contradicción porque S es simétrico y $\chi(s) + \chi(s^{-1}) = \chi(s) + \overline{\chi(s)}$ y se sabe que la suma de un complejo con su conjugado es un real. □

Especializado para el caso de matrices circulantes, se obtiene:

Corolario 3.4.12. *Sea A una matriz circulante de grado n, la cual es la matriz adyacente de la gráfica de Cayley para $\mathbb{Z}/n\mathbb{Z}$ con respecto al conjunto simétrico S. Entonces los valores propios de A son*

$$\lambda_k = \sum_{[m]\in S} e^{2\pi ikm/n}$$

donde $k = 0, \ldots, n-1$ y su correspondiente base de vectores ortonormales viene dada por $v_0, \ldots, v_{n-1}$, donde

$$v_k = \frac{1}{\sqrt{n}} \left(1, e^{4\pi ik/n}, \ldots, e^{2\pi ik(n-1)/n}\right)^T$$

Demostración. Utilizando el teorema 3.4.11 sea $G = \mathbb{Z}/n\mathbb{Z}$ y $\widehat{G} = \{\chi_0, \ldots, \chi_n\}$ donde $\chi_k([m]) = e^{2\pi ikm/n}$ para $k \in \{0, \ldots, n-1\}$ y $[m] \in S$, entonces

$$\begin{aligned}\lambda_k &= \sum_{s\in S} \chi_k(s) \\ &= \sum_{[m]\in S} e^{2\pi ikm/n}\end{aligned}$$

La base de vectores ortonormales $v_0, \ldots, v_{n-1}$, en donde cada vector tiene la forma

$$\begin{aligned}v_k &= \frac{1}{\sqrt{|G|}} \left(\chi_k([0]), \chi_k([1]), \chi_k([2]), \ldots \chi_k([n-1])\right)^T \\ &= \frac{1}{\sqrt{n}} \left(e^{2\pi ik(0)/n}, e^{2\pi ik(1)/n}, e^{2\pi ik(2)/n}, \ldots, e^{2\pi ik(n-1)/n}\right)^T \\ &= \frac{1}{\sqrt{n}} \left(1, e^{2\pi ik/n}, e^{4\pi ik/n}, \ldots, e^{2(n-1)\pi ik/n}\right)^T\end{aligned}$$

□

Ejemplo 3.4.13. Sea A la matriz adyacente del grafo circulante del ejemplo 3.4.7. Se encontrarán los valores propios.

Desarrollo. Se tiene que $G = \mathbb{Z}/6\mathbb{Z}$ y $\widehat{G} = \{\chi_0, \ldots, \chi_5\}$ donde $\chi_k([m]) = e^{2\pi ikm/6} = e^{\pi ikm/3}$ para $k \in \{0, \ldots, 5\}$ y $[m] \in S \Longrightarrow S = \{\pm[1], \pm[2]\}$. Los valores propios de A son $\lambda_0, \ldots, \lambda_5$ donde

$$\begin{aligned}
\lambda_k &= \sum_{[m]\in S} \chi_k(s) \\
&= e^{\pi ik/3} + e^{-\pi ik/3} + e^{2\pi ik/3} + e^{-2\pi ik/3} \\
&= \left(e^{\pi ik/3} + e^{-\pi ik/3}\right) + \left(e^{2\pi ik/3} + e^{-2\pi ik/3}\right); \text{ recordando que } e^{i\theta} + e^{-i\theta} = 2\cos\theta \\
&= 2\cos\frac{\pi k}{3} + 2\cos\frac{2\pi k}{3}
\end{aligned}$$

□

Observación 3.4.14. *Este enfoque puede ser generalizado a grupos no abelianos proporcionado por el conjunto simétrico S y cerrado bajo la conjugación.*

3.5. Análisis de Fourier en Grupos no Abelianos

Para un grupo no abeliano G, se tiene que $L(G) \neq Z(L(G))$ y por ende $L(G)$ es un anillo no conmutativo. Por lo tanto, no puede encontrarse una transformada de Fourier que transforme la convolución en una multiplicación punto a punto (ya que una multiplicación punto a punto es conmutativa). En su lugar, se tratará de remplazar la multiplicación punto a punto por una multiplicación matricial. Para lograr esto, se manejará el caso abeliano de una forma distinta, observése además que el Teorema 3.3.10 puede ser reinterpretado de la siguiente manera.

Teorema 3.5.1. *Sea G un grupo abeliano finito de orden n. Entonces $L(G) \cong \mathbb{C}^n$.*

Demostración. Supóngase que los caracteres irreducibles del grupo abeliano finito G son $\chi_1, \ldots, \chi_n$ y que $|G| = n$. Entonces para cada función $f\colon G \longrightarrow \mathbb{C}$, se puede asociar su vector de coeficientes de Fourier. Es decir, definimos $T\colon L(G) \longrightarrow \mathbb{C}^n$ por

$$\begin{aligned}
Tf &= (n\langle f, \chi_1\rangle, n\langle f, \chi_2\rangle, \ldots, n\langle f, \chi_n\rangle) \\
&= (\widehat{f}(\chi_1), \widehat{f}(\chi_2), \ldots, \widehat{f}(\chi_n))
\end{aligned}$$

Se demostrará que Tf es un isomorfismo.

Se debe comprobar que T es inyectivo, para ello sean Tf_1 y Tf_2, entonces si

$$\begin{aligned} Tf_1 &= Tf_2 \\ (\widehat{f}_1(\chi_1), \widehat{f}_1(\chi_2), \ldots, \widehat{f}_1(\chi_n)) &= (\widehat{f}_2(\chi_1), \widehat{f}_2(\chi_2), \ldots, \widehat{f}_2(\chi_n)) \\ &\iff \widehat{f}_1(\chi_i) = \widehat{f}_2(\chi_i) \\ &\implies \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{f}_1(\chi)\chi = \frac{1}{n}\sum_{\chi\in\widehat{G}} \widehat{f}_2(\chi)\chi \\ &\implies f_1 = f_2; \text{ aplicando la inversión de Fourier (Teorema 3.3.7)} \end{aligned}$$

Se comprobar también que es lineal (en esencia esto es una reformulación de la Proposición 3.3.9)

$$\begin{aligned} T(c_1f_1 + c_2f_2) &= (n\langle c_1f_1 + c_2f_2, \chi_1\rangle, \ldots, n\langle c_1f_1 + c_2f_2, \chi_n\rangle) \\ &= (n[c_1\langle f_1, \chi_1\rangle + c_2\langle f_2, \chi_1\rangle], \ldots, n[c_1\langle f_1, \chi_n\rangle + c_2\langle f_2, \chi_n\rangle]) \\ &= (n[c_1\langle f_1, \chi_1\rangle], \ldots, n[c_1\langle f_1, \chi_n\rangle]) + (n[c_2\langle f_2, \chi_1\rangle], \ldots, n[c_2\langle f_2, \chi_n\rangle]) \\ &= c_1(n\langle f_1, \chi_1\rangle, \ldots, n\langle f_1, \chi_n\rangle) + c_2(n\langle f_2, \chi_1\rangle, \ldots, n\langle f_2, \chi_n\rangle) \\ &= c_1Tf_1 + c_2Tf_2 \end{aligned}$$

con lo cual es lineal. Lo que implica que T es una función lineal inyectiva, entonces la dimensión de la imagen es la dimensión del dominio (por cada elemento hay una función), es decir, $\dim L(G) = n = \dim \mathbb{C}^n$, de aquí que T es sobreyectiva, con lo cual se afirma que es biyectiva.

Ahora $\mathbb{C}^n = \mathbb{C} \times \cdots \times \mathbb{C}$ tiene una estructura de un producto directo de anillos donde la multiplicación es tomada coordenada a coordenada:

$$(a_1, \ldots, b_n)\,(b_1, \ldots, b_n) = (a_1b_1, \ldots, a_nb_n) \tag{3.9}$$

Veamos por último que T es un homomorfismo de anillos

$$\begin{aligned} T\,(a * b) &= (\widehat{a * b}\,(\chi_1)\,, \ldots, \widehat{a * b}\,(\chi_n)); \text{ por definición de } T \\ &= (\widehat{a}\chi_1 \cdot \widehat{b}\chi_1, \ldots, \widehat{a} \cdot \chi_n\widehat{b}\chi_n); \text{ por el Teorema 3.3.10} \\ &= (\widehat{a}(\chi_1), \ldots, \widehat{a}(\chi_n))(\widehat{b}(\chi_1), \ldots, \widehat{b}(\chi_n)); \text{ por la ecuación (3.9)} \\ &= TaTb; \text{ nuevamente por la definición de } T \end{aligned}$$

Por lo tanto es un isomorfismo de espacios vectoriales. □

Se puede suponer que esto refleja el hecho que todas las representaciones irreducibles de un grupo abeliano tienen grado uno y que, para grupos no abelianos, se debe remplazar $\mathbb{C}$ por anillos de matrices sobre $\mathbb{C}$, y esto es justo lo que sucede. Sin mas preámbulos se corrobora lo anterior de la siguiente manera, sea G un grupo finito de orden n con un conjunto completo $\varphi^{(1)}, \ldots, \varphi^{(s)}$ de representantes unitarios de las clases de equivalencia de representaciones

irreducibles de G. Como es usual, se define $d_k = \operatorname{grad}\varphi^{(k)}$, además, los coeficientes de la matriz son funciones $\varphi_{ij}^{(k)} \colon G \longrightarrow \mathbb{C}$ dadas por $\varphi_g^{(k)} = (\varphi_{ij}^{(k)}(g))$. El teorema 2.4.6 dice que las funciones $\sqrt{d_k}\varphi_{ij}^{(k)}$ forman una base ortonormal para $L(G)$.

Definición 3.5.2. (**Transformada de Fourier**).

Se define

$$\begin{aligned} T \colon L(g) &\longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C}) \\ f &\mapsto (\widehat{f}(\varphi^{(1)}), \ldots, \widehat{f}(\varphi^{(s)})) \end{aligned}$$

donde

$$\widehat{f}(\varphi^{(k)})_{ij} = n\left\langle f, \varphi_{ij}^{(k)} \right\rangle \tag{3.10}$$

$$= \sum_{g\in G} f(g)\overline{\varphi_{ij}^{(k)}(g)} \tag{3.11}$$

Sea Tf la *Transformada de Fourier* de f, observése que $M_{d_i}(\mathbb{C})$ es una matriz cuadrada de orden d_i elementos con entradas en los complejos. Por otro lado, (3.11) puede ser escrita de forma más concisa de la siguiente manera $\widehat{f}(\varphi^{(k)}) = \sum_{g\in G} f(g)\overline{\varphi_g^{(k)}}$, la cual tiene la forma mas comúnmente usada.

Se inicia el estudio del análisis de Fourier para grupos no abelianos con el teorema de inversión de Fourier.

Teorema 3.5.3. *(**Inversión de Fourier**).*

Sea $f \colon G \longrightarrow \mathbb{C}$ una función de valores complejos en G. Entonces

$$f = \frac{1}{n}\sum_{i,j,k} d_k \widehat{f}(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)}$$

donde $n = |G|$.

Demostración. Se calcula utilizando una propiedad de la ortonormalidad de $\sqrt{d_k}\varphi_{ij}^{(k)}$ (Teorema 2.4.6), ya que se puede escribir f como combinación lineal de estos elementos

$$\begin{aligned} f &= \sum_{i,j,k} \langle f, \sqrt{d_k}\varphi_{ij}^{(k)}\rangle \sqrt{d_k}\varphi_{ij}^{(k)} \\ &= \frac{n}{n}\sum_{i,j,k} \langle f, \varphi_{ij}^{(k)}\rangle (\sqrt{d_k})^2 \varphi_{ij}^{(k)} \\ &= \frac{1}{n}\sum_{i,j,k} d_k \left(n\langle f, \varphi_{ij}^{(k)}\rangle \right) \varphi_{ij}^{(k)}; \text{ utilizando la definición 3.5.2 para } n\langle f, \varphi_{ij}^{(k)}\rangle \text{ se tiene} \\ &= \frac{1}{n}\sum_{i,j,k} d_k \widehat{f}(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)} \end{aligned}$$

como se requería. □

Se demostrará que T es un isomorfismo de espacios vectoriales.

Proposición 3.5.4. *El mapeo* $T\colon L(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$ *es un isomorfismo de espacios vectoriales.*

Demostración. Para mostrar que T es lineal es suficiente con probar que

$$\left(\widehat{c_1 f_1 + c_2 f_2}\right)(\varphi^{(k)}) = c_1 \widehat{f}_1(\varphi^{(k)}) + c_2 \widehat{f}_2(\varphi^{(k)})$$

para $1 \leq k \leq s$.

$$\begin{aligned}\left(\widehat{c_1 f_1 + c_2 f_2}\right)(\varphi^{(k)}) &= \sum_{g\in G} (c_1 f_1 + c_2 f_2)(g)\overline{\varphi_g^{(k)}} \\ &= c_1 \sum_{g\in G} f_1(g)\overline{\varphi_g^{(k)}} + c_2 \sum_{g\in G} f_2(g)\overline{\varphi_g^{(k)}} \\ &= c_1 \widehat{f}_1(\varphi^{(k)}) + c_2 \widehat{f}_2(\varphi^{(k)})\end{aligned}$$

El teorema de inversión de Fourier implica que T es inyectiva, ya que

$$\begin{aligned} Tf_1 &= Tf_2 \\ (\widehat{f}_1(\varphi^{(1)}), \widehat{f}_1(\varphi^{(2)}), \ldots, \widehat{f}_1(\varphi^{(n)})) &= (\widehat{f}_2(\varphi^{(1)}), \widehat{f}_2(\varphi^{(2)}), \ldots, \widehat{f}_2(\varphi^{(n)})) \\ \text{donde } \widehat{f}_1(\varphi^{(k)})_{ij} &= \widehat{f}_2(\varphi^{(k)})_{ij} \\ \implies \frac{\delta_k}{n}\widehat{f}_1(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)} &= \frac{\delta_k}{n}\widehat{f}_2(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)} \\ \implies \frac{1}{n}\sum_{i,j,k} d_k \widehat{f}_1(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)} &= \frac{1}{n}\sum_{i,j,k} d_k \widehat{f}_2(\varphi^{(k)})_{ij}\varphi_{ij}^{(k)} \\ \implies f_1 = f_2&; \text{ aplicando la inversión de Fourier (Teorema 3.5.3)}\end{aligned}$$

Recuérdese que la dimensión $\dim L(G) = |G|$ entonces

$$\begin{aligned}\dim L(G) &= |G| \\ &= d_1^2 + \ldots + d_s^2; \text{ por el Corolario 2.4.5} \\ &= \dim M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})\end{aligned}$$

y se deduce que T es un isomorfismo. □

Todo el trabajo, hecho hasta ahora ha sido con el motivo de demostrar que que la transformada de Fourier es un isomorfismo de anillos. Esto lleva a un caso especial del teorema más general de Wedderburn, que usualmente es tomado como el punto de partida para el estudio de la teoría de representaciones de grupos finitos.

Teorema 3.5.5. *(**Wedderburn**).*

La transformada de Fourier

$$T\colon L(G) \longrightarrow M_{d_1}(\mathbb{C}) \times \cdots \times M_{d_s}(\mathbb{C})$$

Es un isomorfismo de anillos.

Demostración. La proposición anterior afirma que T es un isomorfismo de espacios vectoriales. Por lo tanto, para demostrar que es un isomorfismo de anillo es suficiente verificar que $T(a) = Ta$. A su vez, por la definición de multiplicación en el producto directo, para hacer esto es suficiente establecer que $\widehat{a * b}(\varphi^{(k)}) = \widehat{a}(\varphi^{(k)}) \cdot \widehat{b}(\varphi^{(k)})$ para $1 \leq k \leq s$. El calculo es similar el caso abeliano:

$$\begin{aligned}
\widehat{a * b}(\varphi^{(k)}) &= \sum_{x\in G} (a * b)(x)\overline{\varphi_x^{(k)}}; \text{ se aplica la definición de transformada de Fourier} \\
&= \sum_{x\in G} \overline{\varphi_x^{(k)}} \sum_{y\in G} a\left(xy^{-1}\right) b(y); \text{ por la Definición 3.2.1} \\
&= \sum_{x\in G}\sum_{y\in G} \overline{\varphi_x^{(k)}} a\left(xy^{-1}\right) b(y) \\
&= \sum_{y\in G} b(y) \sum_{x\in G} a\left(xy^{-1}\right) \overline{\varphi_x^{(k)}}
\end{aligned}$$

Haciendo $z = xy^{-1}$ (y así $x = zy$) se tiene

$$\begin{aligned}
\widehat{a * b}(\varphi^{(k)}) &= \sum_{y\in G} b(y) \sum_{z\in G} a(z)\overline{\varphi_{zy}^{(k)}} \\
&= \sum_{y\in G} b(y) \sum_{z\in G} a(z)\overline{\varphi_z^{(k)}\varphi_y^{(k)}}; \text{ ya que } \varphi \text{ es homomorfismo} \\
&= \sum_{y\in G} b(y)\overline{\varphi_y^{(k)}} \sum_{z\in G} a(z)\overline{\varphi_z^{(k)}}; \text{ debido a que } \overline{\varphi_y^{(k)}} \text{ es una constante} \\
&= \sum_{z\in G} a(z)\overline{\varphi_z^{(k)}} \sum_{y\in G} b(y)\overline{\varphi_y^{(k)}} \\
&= \widehat{a}(\varphi^{(k)}) \cdot \widehat{b}(\varphi^{(k)})
\end{aligned}$$

Esto concluye la demostración de que T es un isomorfismo de anillo. □

Para grupos no abelianos, es todavía cierto que calcular $Ta \cdot Tb$ e invertir T, puede ser algunas veces mas rápido que calcular directamente $a * b$.

Observación 3.5.6. *Nótese que*

$$\widehat{\delta}_g(\varphi^{(k)}) = \sum_{x\in G} \delta_g(x)\overline{\varphi_x^{(k)}} = \overline{\varphi_g^{(k)}};\ si\ g = x$$

El conjugado de una representación irreducible es irreducible, ya que si dos representaciones son conjugadas tienen el mismo carácter y por el Corolario 2.3.15 se tiene que la conjugada también cumple con $\langle \overline{\chi_\rho}, \overline{\chi_\rho} \rangle = 1$, entonces se tiene que $T\delta_g$ es un vector cuyas entradas consisten en las imágenes de g bajo todas las representaciones irreducibles de G, en algún orden.

Capítulo 4

Teorema de Burnside

En este capítulo, se muestra una de las mayores aplicaciones de la Teoría de Representaciones de Grupos: El **pq-teorema de Burnside**. Este teorema establece que no hay grupos no-abelianos de orden $p^a q^b$ que sean simples. Recuérdese que un grupo es *simple* si no contiene subgrupos propios normales no-triviales. Para demostrar el teorema de Burnside se hará una breve incursión en la teoría de números, además, se probará un resultado de Frobenius que a veces es conocido como teorema de la dimensión, el cual dice que el grado de cada una de las representaciones irreducibles de un grupo G divide el orden de G. Este hecho resulta ser muy útil para determinar la tabla de caracteres de un grupo.

4.1. Un repaso de Teoría de Números

Un número complejo es llamado un *número algebraico* si este es la raíz de un polinomio con coeficientes enteros. Los números que no son algebraicos son llamados *trascendentales*. Por ejemplo $\frac{1}{2}$ es algebraico, siendo una raíz del polinomio $2z - 1$, y también lo es $\sqrt{2}$, ya que es una raíz de $z^2 - 2$. Se sabe que el conjunto $\overline{\mathbb{Q}}$ (definido como la cerradura de $\mathbb{Q}$[(1)]) es un campo de números algebraicos y que es contable (sólo hay una cantidad numerable de polinomios sobre $\mathbb{Z}$ y cada uno tiene sólo raíces finitas). Por otro lado, se sabe que $\mathbb{C}$ es no numerable, nótese que la mayoría de los números no son algebraicos, sin embargo, es extremadamente difícil demostrar que un número dado es trascendental, por ejemplo e y π son trascendentales, pero esto no es tan trivial de probar. Aunque la teoría de números se refiere a los números en general, esta se enfoca principalmente en enteros y para los propósitos de esta investigación es de interés un tipo especial de números algebraicos llamados *números enteros algebraicos*.

Definición 4.1.1. Entero algebraico.

Un número complejo α se dice que es un entero algebraico si es raíz de un polinomio mónico[(2)] con coeficientes enteros.

[(1)] Este es un conjunto que contiene todos los enteros algebraicos.

[(2)] Un polinomio mónico se caracteriza por que el coeficiente del término de mayor grado es igual a 1.

Es decir, α es un entero algebraico si hay un polinomio

$$p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$$

con $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ y $p(\alpha) = 0$

El hecho de que el coeficiente líder de p es 1 es crucial para la definición. Cada entero $m \in \mathbb{Z}$ es un entero algebraico, ya que es la raíz del polinomio $z - m$. Observése que si α es un entero algebraico, entonces también lo es -α porque si $p(z)$, $P(-z)$ y $-P(-z)$ son polinomios mónicos con coeficientes enteros tales que

$$\begin{array}{ll|ll|ll} P(z) & = z-\alpha & P(-z) & = -z-\alpha & -P(-z) & = z+\alpha \\ P(\alpha) & = \alpha-\alpha & P(-\alpha) & = -(-\alpha)-\alpha & -P(-\alpha) & = -\alpha+\alpha \\ P(\alpha) & = 0 & P(-\alpha) & = 0 & -P(-\alpha) & = 0 \end{array}$$

Por lo tanto, α y -α son raíces de estos polinomios. De hecho, se verá más adelante que los enteros algebraicos forman un subanillo de $\mathbb{C}$.

Ejemplo 4.1.2. Raíces n-ésimas

Si m es un entero, entonces $z^n - m$ es un polinomio mónico con coeficientes enteros, en donde cualquier raíz n-ésima de m es un entero algebraico.

Para encontrar las raíces del polinomio mónico $z^n - m$ se iguala a cero, $z^n - m = 0$ de aquí que $z = \sqrt[n]{m}$, así, por ejemplo $\sqrt{2}$ es un entero algebraico para el polinomio $z^2 - 2$.

De hecho, cualquier raíz n-ésima de la unidad es un entero algebraico, es decir, cualquier complejo de la forma $z = e^{\frac{2\pi ik}{n}}$ con $k \in \mathbb{Z}$ es un entero algebraico porque es raíz del polinomio $z^n - 1$ con $n \geq 2$.

Ejemplo 4.1.3. Valores propios de matrices enteras

Si $A = (a_{ij})$ con el $a_{ij} \in \mathbb{C}$ una matriz $n \times n$ entera, entonces los valores propios de A son enteros algebraicos.

Recuérdese que para obtener los valores propios de una matriz se utiliza el polinomio característico $P_A(z) = \det(zI - A)$, el cual es mónico con coeficientes enteros. De esta manera, al igualarlo a 0 se encuentran los valores propios de A y cada uno de estos al ser raíces del polinomio $P_A(z)$ se convierten en enteros algebraicos.

Un número racional $\frac{m}{n}$ es una raíz del polinomio entero no mónico $nz - m$. Podría suponerse que un número racional no debe ser un entero algebraico, a menos que de hecho sea un número entero, que es justo lo que se demuestra en la siguiente proposición.

Proposición 4.1.4. *Un número racional es un número entero algebraico si y sólo si es un número entero.*

Demostración. "$\Longrightarrow$"

Sea $r = \frac{m}{n}$ con $m, n \in \mathbb{C}$, $n > 0$ y $\text{MCD}(m, n) = 1$. Supóngase que r es una raíz del polinomio con coeficientes enteros $z^k + a_{k-1}z^{k-1} + \cdots + a_0$. Entonces

$$\begin{aligned} z^k + a_{k-1}z^{k-1} + \cdots + a_0 &= 0 \\ \left(\frac{m}{n}\right)^k + a_{k-1}\left(\frac{m}{n}\right)^{k-1} + \cdots + a_0 &= 0 \\ \frac{m^k}{n^k} + \frac{a_{k-1}m^{k-1}}{n^{k-1}} + \cdots + a_0 &= 0 \\ n^k\left(\frac{m^k}{n^k}\right) + n^k\left(\frac{a_{k-1}m^{k-1}}{n^{k-1}}\right) + \cdots + n^k(a_0) &= n^k(0) \end{aligned}$$

$m^k + a_{k-1}m^{k-1}n + \cdots + a_1mn^{k-1} + a_0n^k = 0$; ahora se multiplica por -1 y se despeja m^k

$-n(a_{k-1}m^{k-1} + \cdots + a_1mn^{k-1} + a_0n^{k-1}) = m^k$

De aquí que $n|m^k$ y por hipótesis se sabe que $\text{MCD}(m, n) = 1$, entonces a n no le queda más que ser ± 1. Por lo tanto $r = \pm m \in \mathbb{Z}$ como se quería.

"$\Longleftarrow$"

Sea $\alpha \in \mathbb{Z}$ tal que $\frac{\alpha}{1} \in \mathbb{Q}$, sea el polinomio mónico $P(x) = x - \alpha$, entonces α es raíz de este polinomio y por tanto es un entero algebraico. □

Como estrategia general para mostrar que un entero d divide un entero n, se demostrará que $\dfrac{n}{d}$ es un entero algebraico. La proposición anterior implica que para que sea entero entonces $d|n$. Se mostrará que los enteros algebraicos forman un subanillo $\mathbb{A}$ de $\mathbb{C}$. Para ello, se necesita la siguiente caracterización de enteros algebraicos.

Lema 4.1.5. *Un elemento $y \in \mathbb{C}$ es un entero algebraico si y sólo si existen $y_1, \cdots, y_t \in \mathbb{C}$, no todos cero, de tal manera que*

$$yy_i = \sum_{j=1}^{t} a_{ij}y_j$$

con el $a_{ij} \in \mathbb{C}$ para todo $1 \leq i \leq t$ (es decir, yy_i es una combinación lineal entera de y_i para todo i).

Demostración. "$\Longrightarrow$"

Supóngase que y es un entero algebraico, es decir, sea y una raíz de

$$\begin{aligned} p(z) &= z^n y + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \cdots + a_0 \\ 0 &= y^n + a_{n-1}y^{n-1} + a_{n-2}y^{n-2} + \cdots + a_0y^0 \ (*) \end{aligned}$$

Se toma $y_i = y^{i-1}$ para $1 \leq i \leq n$, luego, para $1 \leq i \leq n-1$, se tiene

$$yy_i = yy^{i-1} = y^i = y_{i+1} \ (**)$$

de esta manera $y^i = y_{i+1}$ con $i \leq i \leq n-1$, en donde estos elementos van a formar una base, ya que y^n es una combinación lineal de todos los anteriores, como se muestra a continuación:

$$\begin{aligned} yy_n &= y_{n+1} = y^n; \text{ despejando a } y^n \text{ de la ecuación } (*) \text{ se tiene} \\ yy_n &= -a_{n-1}y^{n-1} - a_{n-2}y^{n-2} - \cdots - a_0y^0; \text{ se utiliza el resultado dado en } (**) \\ yy_n &= -a_{n-1}y_n - a_{n-2}y_{n-1} - \cdots - a_0y_1; \text{ con } y_1 = y^{1-1} = y^0 = 1 \end{aligned}$$

sea $a_i = a_{ij}$ entonces

$$yy_n = \sum_{j=1}^{n-1} -a_{ij}y^j$$

Por lo tanto yy_i es una combinación lineal entera de y_i para todo i. "$\Longleftarrow$"

Ahora sean $y_1, \cdots, y_t \in \mathbb{C}$ no todos ceros, $A = (a_{ij})$ y

$$y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{bmatrix} \in \mathbb{C}^t$$

Entonces

$$\begin{aligned} AY &= \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ a_{21} & a_{21} & \cdots & a_{2t} \\ \vdots & & \ddots & \vdots \\ a_{t1} & a_{t2} & \cdots & a_{tt} \end{bmatrix}_{t\times t} \quad \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{bmatrix}_{t\times 1} \\ &= [AY]_{t\times 1} \end{aligned}$$

De donde $a_{i1}y_1 + a_{i2}y_2 + \cdots + a_{it}y_t = \sum_{j=1}^{t} a_{ij}y_j$ entonces $[AY]_i$ es la i-ésima componente de AY, de esta manera

$$\begin{aligned} [AY]_i &= \sum_{j=1}^{t} a_{ij}y_j \\ &= yy_i \\ &= y\,[Y]_i \end{aligned}$$

Con lo anterior se tiene que $AY = yY$, como $Y \neq 0$ por hipótesis, se deduce que y es un valor propio de la matriz entera $A_{t\times t}$ y por lo tanto es un entero algebraico por el Ejemplo 4.1.3. □

Corolario 4.1.6. *El conjunto $\mathbb{A}$ de enteros algebraicos es un subanillo de $\mathbb{C}$. En particular, la suma y el producto de enteros algebraicos es algebraico.*

Demostración. Al principio de este capitulo se observó que si $\alpha \in \mathbb{A}$ entonces también $-\alpha \in \mathbb{A}$, es decir, $\mathbb{A}$ es cerrado bajo inversos aditivos. Sean y, $y' \in \mathbb{A}$ y se toman $y_1, y_2, \cdots, y_t \in \mathbb{C}$ no todos nulos y a $y'_1, \cdots, y'_s \in \mathbb{C}$ no todos nulos, de tal forma que haciendo uso del Lema 4.1.5 se tiene

$$yy_i = \sum_{j=1}^{t} a_{ij}y_j \quad , \quad y'y'_k = \sum_{j=1}^{s} b_{kj}y'_j$$

En donde cada yy_i es una combinación lineal entera elementos de la forma y_i y cada $y'y'_k$ es una combinación lineal entera de elementos de la forma y'_k. Entonces se probará que es subanillo (Para que $\mathbb{A}$ sea subanillo de $\mathbb{C}$ debe cumplirse que $a - b \in \mathbb{A} \forall a, b \in \mathbb{A}$, además $ab \in \mathbb{A} \forall a, b \in \mathbb{A}$ y por último $1 \in \mathbb{A}$)

$$\begin{aligned}(y + y')y_iy'_k &= yy_iy'_k + y'y_iy'_k \\ &= yy_iy'_k + y'y'_ky_i; \text{ ahora sustituimos a } yy_i \text{ y a } y'y'_k \\ &= \sum_{j=1}^{t} a_{ij}y_jy'_k + \sum_{j=1}^{s} b_{kj}y'_jy_i\end{aligned}$$

en donde se tiene la suma de combinaciones lineales enteras de los elementos y_i y y'_k como la suma, sin embargo, las combinaciones lineales siguen siendo una combinación lineal, por lo tanto, se tiene una combinación lineal de elementos de la forma $y_iy'_k$, estableciendo que $y + y' \in \mathbb{A}$ por el Lema 4.1.5. De forma similar,

$$\begin{aligned}yy'y_iy'_k &= yy_iy'y'_k \\ &= \left(\sum_{j=1}^{t} a_{ij}y_j\right)\left(\sum_{j=1}^{s} b_{kj}y'_j\right); \text{ por distributividad} \\ &= \sum_{j=1}^{t}\sum_{j=1}^{s} a_{ij}b_{kj}y_jy'_j\end{aligned}$$

con lo que se obtiene es una combinación lineal entera de elementos de la forma $y_jy'_k$ y así $yy' \in \mathbb{A}$, por lo tanto A es un subanillo de $\mathbb{C}$ y la suma y el producto de enteros algebraicos será algebraico. □

Se necesita que el conjugado complejo de un entero algebraico sea una entero algebraico. En efecto, si $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$ es un polinomio con coeficientes enteros y α es una raíz de $p(z)$, entonces

$$\begin{aligned}p(\overline{\alpha}) &= \overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \cdots + \overline{a_0} \\ &= \overline{\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0} \\ &= \overline{p(\alpha)} \\ &= 0\end{aligned}$$

4.2. El Teorema de La Dimensión

La relevancia de los enteros algebraicos de la TGR se hace evidente considerando la siguiente consecuencia del Corolario 4.1.6.

Corolario 4.2.1. *Sea χ un carácter de un grupo finito G. Entonces $\chi(g)$ es un entero algebraico para toda $g \in G$.*

Demostración. Sea $\varphi\colon G \to GL_m(\mathbb{C})$ una representación con carácter χ y sea n el orden de G. Entonces $g^n = 1$, cambiándolo por su representación se tiene $\varphi_g^n = I$. El corolario 2.1.10 implica que φ_g es diagonalizable y posee $\lambda_1, \cdots, \lambda_m$ valores propios, que son las raíces n-ésimas de la unidad. En particular, los valores propios de φ_g son enteros algebraicos debido al Ejemplo 4.1.3, por otro lado utilizando la definición de carácter se tiene que

$$\begin{aligned}\chi(g) &= Tr(\varphi_g)\\ &= \lambda_1 + \cdots + \lambda_m\end{aligned}$$

el Corolario 4.1.6 afirma que la suma de enteros algebraicos es un entero algebraico, ya que el conjunto de todos ellos forman un subanillo de $\mathbb{C}$, por todo lo anterior se concluye que $\chi(g)$ es un entero algebraico. □

Observación 4.2.2. *Observése que la demostración del corolario anterior muestra que $\chi(g)$ es una suma de m raíces n-ésimas de la unidad.*

Observación 4.2.3. *El corolario anterior implica que $\overline{\chi(g)}$ es entero algebraico también, ya que los conjugados también son raíces.*

El próximo objetivo es demostrar que el grado de una representación irreducible divide el orden del grupo. Para ello se necesitan algunos enteros algebraicos extras.

Teorema 4.2.4. *Sea φ una representación irreducible de un grupo finito G de grado d. Sea $g \in G$ y sea h el tamaño de la clase de conjugación de g. Entonces $h\chi_\varphi(g)/d$ es un entero algebraico.*

Demostración. Sean $C_1, \cdots, C_s$ las clases de conjugación de G. Sean: $= h_i$: $= |C_i|$ y χ_i el valor de χ_φ en la clase C_i. Se quiere mostrar que $\dfrac{h_i\chi_i}{d}$ es un entero algebraico para cada i. Con este fin se considera el siguiente operador

$$T_i = \sum_{x \in C_i} \varphi_x$$

que no es más que la suma de las representaciones de G para los g en cada clase, es decir, es un operador que actuá sobre toda la clase y cada una de ellas.

Antes de proseguir con la demostración, deben probarse algunos resultados que serán útiles para construir la prueba.

Afirmación 1: $T_i = \frac{h_i}{d}\chi_i \cdot I$.

Demostración. Primero se mustra que $\varphi_g T_i \varphi_{g^{-1}} = T_i$ para todo $g \in G$.

$$\begin{aligned}
\varphi_g T_i \varphi_{g^{-1}} &= \varphi_g \left(\sum_{x \in C_i} \varphi_x \right) \varphi_{g^{-1}} \\
&= \sum_{x \in C_i} \varphi_g \varphi_x \varphi_{g^{-1}}; \text{ como } \varphi \text{ es un homomorfismo entonces} \\
&= \sum_{x \in C_i} \varphi_{gxg^{-1}}; \text{ haciendo } y = gxg^{-1} \text{ se tiene} \\
&= \sum_{y \in C_i} \varphi_y \\
&= T_i
\end{aligned}$$

esto es válido ya que C_i es cerrado bajo la conjugación[(3)] y la conjugación por g es una permutación.

De acuerdo al resultado anterior se tiene que

$$\begin{aligned}
\varphi_g T_i \varphi_{g^{-1}} &= T_i \\
\varphi_g T_i \varphi_{g^{-1}} \varphi_g &= T_i \varphi_g \\
\varphi_g T_i &= T_i \varphi_g \Longrightarrow T_i \in \mathrm{Hom}_G(\varphi, \varphi)
\end{aligned}$$

por lo tanto, se tiene un morfismo de si mismo en si mismo además se sabe que ϕ es irreducible y es igual a si mismo, entonces utilizando el literal (b) del lema de Schur se tiene que $T_i = \lambda I$ para algún $\lambda \in \mathbb{C}$.

Ya que I es el operador identidad en un espacio vectorial d-dimensional, se tiene que $\mathrm{Tr}(\lambda I) = d\lambda$ y que

$$\begin{aligned}
\mathrm{Tr}(\lambda I) &= \mathrm{Tr}(T_i) \\
&= \mathrm{Tr}\left(\sum_{x \in C_i} \varphi_x \right) \\
&= \sum_{x \in C_i} \mathrm{Tr}(\varphi_x); \text{ por la propiedad de la traza } \mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B) \\
&= \sum_{x \in C_i} \chi_\varphi(x); \text{ por definición de carácter} \\
&= \sum_{x \in C_i} \chi_i; \text{ como el carácter es constante en toda la clase conjugada (Propiedad 2.3.5)} \\
&= |C_i| \chi_i \\
&= h_i \chi_i
\end{aligned}$$

[(3)] Como son clases invariantes bajo conjugación, cada una de estas conjugaciones definen una biyección que es un automorfismo en las clases conjugadas.

Entonces

$$\begin{aligned} d\lambda &= \mathrm{Tr}(\lambda I) \\ d\lambda &= h_i\chi_i \\ \lambda &= \frac{h_i\chi_i}{d} \end{aligned}$$

Con lo anterior podemos ver que

$$\begin{aligned} T_i &= \lambda I \text{; sustituyendo el valor de } \lambda \\ &= \frac{h_i\chi_i}{d} I \end{aligned}$$

estableciendo la *Afirmación 1.* □

Ahora se necesita ver que los T_i se "comportan" como enteros algebraicos que satisfacen una fórmula similar a la del Lema 4.1.5 y es precisamente lo que dice la segunda afirmación.

Afirmación 2: $T_iT_j = \sum_{k=1}^{s} a_{ijk}T_k$ para algún $a_{ijk} \in \mathbb{Z}$.

Demostración.

$$\begin{aligned} T_iT_j &= \sum_{x\in C_i} \varphi_x \cdot \sum_{y\in C_j} \varphi_y \\ &= \sum_{\substack{x\in C_i \\ y\in C_j}} \varphi_x\varphi_y \\ &= \sum_{\substack{x\in C_i \\ y\in C_j}} \varphi_{xy} \end{aligned}$$

Nótese que $\sum_{\substack{x\in C_i \\ y\in C_j}} \varphi_{xy}$ suma todas las veces en donde g aparece, por lo tanto sea a_{ij} [(4)] el número de formas distintas de escribir g como producto de xy , es decir, $g = xy$ con $x \in C_i$ y $y \in C_j$.

Ahora supóngase que se cumple que a_{ijg} sólo depende de la clase de conjugación de g, entonces sea a_{ijk} el valor de a_{ijg} con $g \in C_k$. Como se tienen s clases de conjugación distintas,

[(4)] Nótese que el i y el j de la notación a_{ij} están referidos a la clase C_i y C_j

se suman por cada clase lo siguiente:

$$\begin{aligned}\sum_{g\in G} a_{ijg}\varphi_g &= \sum_{k=1}^{s}\sum_{g\in C_k} a_{ijg}\varphi_g \\ &= \sum_{k=1}^{s} a_{ijk}\sum_{g\in C_k}\varphi_g \\ &= \sum_{k=1}^{s} a_{ijg}T_k\end{aligned}$$

probando con esto la *Afirmación 2.* □

Para la Afirmación 2, se supuso que a_{ijg} solo dependía de la clase de conjugación, la siguiente afirmación demuestra que efectivamente así es.

Afirmación 3: a_{ijg} sólo depende de la clase de conjugación de g.

Demostración. Sea

$$X_g = \{(x, y) \in C_i \times C_j \mid xy = g\};$$

la cantidad de elementos pares ordenados que se forman cuando $g = xy$, entonces $a_{ijg} = |X_g|$. Lo que se quiere probar es que coinciden las cardinalidades cuando se toma el conjugado, es decir, si g' es el conjugado de g, se mostrara que $|X_g| = |X_{g'}|$. Supóngase que $g' = kgk^{-1}$, se define una función

$$\begin{aligned}\psi\colon X_g &\to X_{g'} \\ (x, y) &\mapsto (kxk^{-1}, kyk^{-1})\end{aligned}$$

y se quiere demostrar que existe una correspondencia uno a uno entre X_g y $X_{g'}$; nótese que $kxk^{-1} \in C_i$, $kyk^{-1} \in C_j$ ya que es un conjugado de x y de y. Se probará que esta bien definida, es decir, si la imagen de los elementos pertenece al dominio; además se sabe que es una función ya que por definición la imagen de un elemento es única.

Entonces tomando $kxk^{-1} \in C_i$ y $kyk^{-1} \in C_j$ se tiene

$$\begin{aligned}kxk^{-1}kyk^{-1} &= kxyk^{-1} \\ &= kgk^{-1} \\ &= g'\end{aligned}$$

por lo tanto el producto de los elementos del par ordenado (kxk^{-1}, kyk^{-1}) es igual a g', con lo que se corrobora que $\psi(x, y) \in X'_g$.

Ahora observése que ψ tiene inversa, sea τ esa función tal que

$$\begin{aligned}\tau\colon X_{g'} &\to X_g \\ (x', y') &\mapsto (k^{-1}x'k, k^{-1}y'k)\end{aligned}$$

La prueba de que τ es una función, es similar a la abordada para ψ. Ahora para que sea inversa debe cumplirse que $\psi \circ \tau = 1$ y que $\tau \circ \psi = 1$, para ello se toma (x, y) y se comprueba la primera condición

$$\begin{aligned}\psi \circ \tau(x, y) &= \psi(\tau(x, y)) \\ &= \psi(k^{-1}xk, k^{-1}yk) \\ &= (kk^{-1}xkk^{-1}, kk^{-1}ykk^{-1}) \\ &= (x, y)\end{aligned}$$

Ahora véase la segunda condición

$$\begin{aligned}\tau \circ \psi(x, y) &= \tau(\psi(x, y)) \\ &= \psi(kxk^{-1}, kyk^{-1}) \\ &= (k^{-1}kxk^{-1}k, k^{-1}kyk^{-1}k) \\ &= (x, y)\end{aligned}$$

Como ψ tiene inversa, entonces es una biyección y por lo tanto se cumple que $|X_g| = |X_{g'}|$, con lo que se establece la *Afirmación 3.* □

Se completa la prueba del teorema, sustituyendo la fórmula para el T_i de la *Afirmación 1* en la fórmula de la *Afirmación 2* y se tiene

$$\begin{aligned}T_iT_j &= \sum_{k=1}^{s} a_{ijg}T_k \\ (\frac{h_i}{d}\chi_i)T_j &= \sum_{k=1}^{s} a_{ijg}T_k; \text{ con } \frac{h_i}{d}\chi_i = \frac{h_i}{d}\chi_{\varphi(g)} \\ \frac{h_i}{d}\chi_{\varphi(g)}T_j &= \sum_{k=1}^{s} a_{ijg}T_k\end{aligned}$$

por lo tanto $\frac{h_i}{d}\chi_{\varphi(g)}$ es un entero algebraico por lo visto en el Lema 4.1.5 ya que es una combinación lineal de los T_j. □

Teorema 4.2.5. ***(Teorema de la Dimensión)***

Sea φ una representación irreducible de G de grado d. Entonces d divide a $|G|$.

Demostración. Utilizando las primeras relaciones de ortogonalidad (Teorema 2.3.9) y la definición de producto interno se tiene

$$\begin{aligned}1 &= \langle \chi_\varphi, \chi_\varphi \rangle \\ &= \frac{1}{|G|}\sum_{g \in G} \chi_\varphi(g)\overline{\chi_\varphi(g)}\end{aligned}$$

Se despeja y se tiene

$$1 = \frac{1}{|G|}\sum_{g\in G}\chi_\varphi(g)\overline{\chi_\varphi(g)} \tag{4.1}$$

$$|G| = \sum_{g\in G}\chi_\varphi(g)\overline{\chi_\varphi(g)}\text{; se divide por } d \text{ y obtiene} \tag{4.2}$$

$$\frac{|G|}{d} = \sum_{g\in G}\frac{\chi_\varphi(g)}{d}\overline{\chi_\varphi(g)} \tag{4.3}$$

Sean $C_1, \cdots, C_s$ las clases conjugada de G, sea χ_i el valor de χ_φ en C_i y sea $h_i = |C_i|$. Entonces en la ecuación (4.3) se tiene

$$\frac{|G|}{d} = \sum_{i=1}^{s}\sum_{g\in C_i}\frac{\chi_g(g)}{d}\overline{\chi_\varphi(g)}\text{; ya que el carácter es una función de clase} \tag{4.4}$$

$$= \sum_{i=1}^{s}\sum_{g\in C_i}\left(\frac{1}{d}\chi_i\right)\overline{\chi_i}\text{; porque el carácter es constante en cada clase} \tag{4.5}$$

$$= \sum_{i=1}^{s}\left(\frac{h_i}{d}\chi_i\right)\overline{\chi_i}\text{; se suma tantas veces como elementos hay en cada la clase} \tag{4.6}$$

Pero $\dfrac{h_i\chi_i}{d}$ es un entero algebraico por el teorema anterior (4.2.4), mientras que $\overline{\chi_i}$ es un entero algebraico por el Corolario 4.2.1 y la suma de enteros algebraicos es también un entero algebraico, así como el producto de enteros algebraicos es también algebraico (cierre de enteros algebraicos bajo la conjugación compleja). Como los enteros algebraicos forman un anillo, por cerradura se deduce en (4.6) que $\dfrac{h_i}{d}\chi_i\overline{\chi_i}$ son enteros algebraicos para todo i, así $|G|/d$ es un entero algebraico y por lo tanto un entero por la Proposición 4.1.4, con lo que se concluye que d divide $|G|$. □

Observación 4.2.6. *El Teorema de la Dimensión primero fue demostrado por Frobenius. Más tarde fue mejorado por Schur, que mostró que el grado d de una representación irreducible de G divide a $[G\colon Z(G)]$ el índice de $Z(G)$ en G o lo que es lo mismo al número de elementos del conjunto cociente $G/Z(G)$.*

Los siguientes corolarios son resultados estándar de teoría de grupos que, generalmente, son demostrados utilizando propiedades sobre los p-grupos y los teoremas de Sylow, sin embargo, en este documento se utilizará el teorema anterior para demostrarlos, sin necesidad de trabajar con la ecuación de clase, utilizando unicamente la información de las representaciones irreducibles.

Corolario 4.2.7. *Sea p un número primo y sea G un grupo de orden p^2. Entonces G es abeliano.*

Demostración. Sean $d_1, \cdots, d_s$ los grados de las representaciones irreducibles de G. Como el grado de una representación trivial divide al orden del grupo $d_i | p^2$ entonces d_i puede ser 1, p o p^2. Se sabe que la representación trivial tiene grado 1 y es irreducible, además que $p^2 = |G|$ entonces

$$|G| = d_1^2 + \cdots + d_s^2$$

Entonces si alguno de los d_i fuera igual a p^2 se tendría que

$$d_1^2 + \cdots + d_s^2 \geq 1 + (p^2)^2$$

por lo tanto la suma sería al menos $1 + p^4$, lo cual supera a p^2. Ahora si algún $d_i = p$ se tendría que

$$d_1^2 + \cdots + d_s^2 \geq 1 + (p)^2$$

entonces la suma sería al menos $1 + p^2$, lo cual también supera al orden del grupo. Por lo tanto no queda más que $d_i = 1$ para todo i, es decir, todas las clases serían de grado 1 y esto implica que s (el número de clases conjugadas) coincidirá con el orden del grupo $s = |G|$ y por el Corolario 2.4.9 al tener $|G|$ clases de conjugación se concluye que G es abeliano. □

Recuérdese que el *subgrupo commutador* G' de un grupo G es el subgrupo generado por todos los elementos de la forma $g^{-1}h^{-1}gh$ con $g, h \in G$. El commutador es un subgrupo normal y posee las propiedades de que G/G' es abeliano y si N es cualquier subgrupo normal con G/N abeliano, entonces $G' \subseteq N$.

Lema 4.2.8. *Sea G un grupo finito entonces número de las representaciones de grado uno de G divide a $|G|$. Más precisamente, si G' es el subgrupo commutador de G, entonces hay una biyección entre las representaciones de grado uno de G y las representaciones irreducibles del grupo abeliano G/G'. Por lo tanto G tiene $|G/G'| = [G : G']$ representaciones de grado uno.*[(5)]

Demostración. Sea α el conjunto de las representaciones de grado 1 de G y sea β el conjunto de las representaciones irreducibles del grupo abeliano G/G'. Para probar este lema se necesita establecer una biyección entre α y β con lo cual se tendría que $|G/G'| = [G : G']$

Sea θ la biyección buscada, para definirla se hará uso de la proyección canónica π con regla de asignación

$$\begin{aligned} \pi : G &\to G/G' \\ g &\mapsto gG' \end{aligned}$$

además, sea $\rho : G \to \mathbb{C}^*$ una representación de grado uno y sea ψ una representación irreducible, entonces la biyección buscada estaría dada por

$$\begin{aligned} \theta : \beta &\to \alpha \\ \psi &\mapsto \psi \circ \pi = \rho \end{aligned}$$

[(5)] Hay tantas representaciones como el índice de $[G : G']$

en donde $\psi \circ \pi \colon G \to \mathbb{C}^*$ es una representación de grado uno.

Se demostrará que cada representación de grado uno de G se obtiene de esta manera. Se debe comprobar que θ es una función sobreyectiva, es decir, se toma $\rho \in \alpha$ y se probará que existe $\psi \in \beta$ tal que $\theta(\psi) = \rho$.

Como ρ es una representación de grado uno, por el Primer Teorema Fundamental de Isomorfía se sabe que $G/\ker\rho \cong Img(G) \leq \mathbb{C}^*$ entonces $G/\ker\rho$ es abeliano. Por otro lado, se sabe que $\ker\rho \trianglelefteq G$ y $G/\ker\rho$ es abeliano, entonces $G' \subseteq \ker\rho$, es más $G' \leq \ker\rho$.

Ahora se define ψ como

$$\begin{aligned} \psi \colon G/G' &\to \mathbb{C}^* \\ gG' &\mapsto \rho(g) \end{aligned}$$

Se probará que esta bien definida, para ello tomamos gG' y $hG' \in G/G'$ entonces

$$\begin{aligned} gG' = hG' &\iff h^{-1} \in G' \subseteq \ker\rho \\ &\implies \rho(h^{-1}g) = 1 \\ &\implies \rho(h)^{-1}\rho(g) = 1 \\ &\implies \rho(g) = \rho(h) \\ &\implies \psi(gG') = \psi(hG') \end{aligned}$$

Con lo que se concluye que esta bien definida. Ahora se probará que es una representación, para ello se toman gG' y $hG' \in G/G'$ entonces

$$\begin{aligned} \psi(gG'hG') &= \psi((gh)G'); \text{ ya que son clases de equivalencia} \\ &= \rho(gh) \\ &= \rho(g)\rho(h); \text{ ya que } \rho \text{ es un homomorfismo} \\ &= \psi(gG')\psi(hG') \end{aligned}$$

de aquí que ψ es una representación de grado uno y por lo tanto irreducible; todo lo anterior implica que $\psi \in \beta$, con lo que se prueba que θ es una función sobreyectiva.

Ahora se calcula $\theta(\psi)$, se sabe que por definición $\theta(\psi) = \psi \circ \pi$, se debe probar que $\psi \circ \pi = \rho$, por ello se toma $g \in G$ entonces

$$\begin{aligned} \psi \circ \pi(g) &= \psi(\pi(g)) \\ &= \psi(gG') \\ &= \rho(g) \end{aligned}$$

Además, es necesario verificar que θ es inyectiva, se toma ψ, $\gamma\colon G/G' \to \mathbb{C}^*$ entonces

$$\begin{aligned} \theta(\psi) &= \theta(\gamma) \\ \psi \circ \pi &= \gamma \circ \pi; \text{ en donde ambos pertenecen a } \alpha \\ \implies \forall\ g \in G \text{ se tiene que} & \\ \psi \circ \pi(g) &= \gamma \circ \pi(g) \\ \psi(\pi(g)) &= \gamma(\pi(g)) \\ \psi(gG') &= \gamma(gG') \\ \implies \forall\ gG' \in G/G' \text{ se cumple que} & \\ \psi &= \gamma \end{aligned}$$

Por último nótese que como ρ es una representación de grado 1 para cada ψ irreducible con G/G' abeliano, de aquí que se tienen $|G/G'|$ representaciones irreducibles, con lo que se completa la prueba. □

Corolario 4.2.9. *Sean p, q números primos con $p < q$ y $q \not\equiv 1 \pmod{p}$. Entonces cualquier grupo G de orden pq es abeliano.*

Demostración. Sean $d_1, \cdots, d_s$ los grados de las representaciones irreducibles de G. Se sabe que la representación trivial tiene grado 1 y es irreducible, además que $p < q$, $pq = |G|$ y d_i divide a $|G|$, entonces

$$|G| = d_1^2 + \cdots + d_s^2$$

Por lo tanto los d_i solo pueden tomar los valores de 1, p, pq y q, para que dividan al orden del grupo. Observése que pq no puede ser, ya que

$$d_1^2 + \cdots + d_s^2 \geq 1 + (pq)^2$$

quiere decir que se tendría al menos $1 + p^2q^2$ y esto es mayor que pq, por otro lado observése que q tampoco puede ser porque se tendría

$$d_1^2 + \cdots + d_s^2 \geq 1 + (q)^2$$

se sabe que $p < q$ entonces $pq < q^2$ con lo que sería también mayor que pq. Por lo tanto se deduce que d_i solo puede tomar los valores de 1 y p para todo i. Sea n el número de representaciones de grado p de G, como se tiene $[G\colon G'] = m$ representaciones de grado 1 de G. Entonces $pq = m + np^2$, ahora como el número de representaciones de grado 1 divide a $|G|$ por el lema anterior, $m \geq 1$ (porque se cuenta al menos con la representación trivial), entonces se tiene que

$$\begin{aligned} pq &= m + np^2 \\ pq - np^2 &= m \\ p(q - np) = m &\implies p|m \text{ con } q - np \in \mathbb{Z} \end{aligned}$$

Como $m|pq$ debe suceder que $m = 1$, $m = q$, $m = p$ o $m = pq$; pero $m|p$ entonces $m \neq 1$, q, por lo tanto puede solo puede ser p o pq.

Si $m = p$, entonces

$$\begin{aligned} pq &= p + np^2; \text{ se divide por } p \\ q &= 1 + np \\ q - 1 &= np \\ \implies p|(q-1) &\implies q \equiv 1 \pmod{p} \end{aligned}$$

Lo que supondría una contradicción a la suposición. Por lo tanto, $m = pq$ y así todas las representaciones irreducibles de G tienen grado uno y por el Corolario 2.4.9 se tienen pq clases de conjugación y estas coinciden con el orden del grupo, por lo tanto G es abeliano. □

4.3. El Teorema de Burnside

Sea G un grupo de orden n y supóngase que $\varphi\colon G \to GL_d(\mathbb{C})$ es una representación. Entonces $\chi_\varphi(g)$ es la suma de d n-ésimas raíces de la unidad, como se vió en la Observación 4.2.3. Está explica la relevancia del siguiente lema.

Lema 4.3.1. *Sean $\lambda_1, \cdots, \lambda_d$ las raíces n-ésimas de la unidad. Entonces $|\lambda_1 + \cdots + \lambda_d| \leq d$ y la igualdad se cumple si y sólo si $\lambda_1 = \lambda_2 = \cdots = \lambda_d$.*

Demostración. Se sabe que en los complejos se cumple la desigualdad triangular $|\lambda_1 + \lambda_2| \leq |\lambda_1| + |\lambda_2| = 2$, ya que $|\lambda_1| = 1$ y $|\lambda_2| = 1$, en donde, la igualdad se cumple si y solo si $\lambda_1 = \lambda_2$ ya que sus módulos son iguales por ser raíces n-ésimas de la unidad y el argumento de uno de ellos es múltiplo escalar del otro (este será el caso base).

Por inducción asumimos que se cumple para $|\lambda_1 + \cdots + \lambda_k| \leq k$ en donde, la igualdad es cierta si y solo si $\lambda_1 = \cdots = \lambda_k$ ya que sus módulos son iguales por ser raíces n-ésimas de la unidad y sus argumentos son múltiplos escalares de alguno de ellos; ahora se quiere saber si se cumple para $|\lambda_1 + \cdots + \lambda_{k+1}| \leq k + 1$ en donde, la igualdad se cumplirá si y solo si $\lambda_1 = \cdots = \lambda_{k+1}$; entonces se tiene:

$$\begin{aligned} |\lambda_1 + \cdots + \lambda_k + \lambda_{k+1}| &\leq |\lambda_1 + \cdots + \lambda_k| + |\lambda_{k+1}|; \text{ por el caso base} \\ &\leq k + |\lambda_{k+1}|; \text{ por hipótesis inductiva} \\ &\leq k + 1 \end{aligned}$$

Por lo tanto, se observa que se cumple que $|\lambda_1 + \cdots + \lambda_d| \leq |\lambda_1| + \cdots + |\lambda_d|$, como son raíces n-ésimas de la unidad entonces $|\lambda_1| = \cdots = |\lambda_d| = 1$ en donde, la igualdad se cumple si y solo si $\lambda_1 = \cdots = \lambda_k$ ya que sus módulos son iguales y sus argumentos son múltiplos escalares de alguno de ellos. Con lo que se completa la demostración. □

Sea $\omega_n = e^{2\pi i/n}$, se denota por $\mathbb{Q}[\omega_n]$ el subcampo más pequeño de $\mathbb{C}$ que contiene a ω_n. Este es el subcampo F más pequeño de $\mathbb{C}$ en donde $z^n - 1 = (z - \alpha_1)\cdots(z - \alpha_n)$ para algún $\alpha_1, \cdots, \alpha_n \in F$, es decir, este F es el campo de escisión[6] de $z^n - 1$.

Los campos de la forma $\mathbb{Q}[\omega_n]$ son llamados *campos ciclotómicos*[7]. Por otro lado sea ϕ la función ϕ *de Euler*; así $\phi(n)$ es el número de enteros positivos menores que n que son primos relativos con él. El siguiente resultado es usual de la teoría de anillos y campos [13].

Lema 4.3.2. *El campo $\mathbb{Q}[\omega_n]$ tiene dimensión $\phi(n)$ como un $\mathbb{Q}$-espacio vectorial.*

Lo único que debemos observar es que la dimensión es finita, lo cual se sabe porque ω_n es un entero algebraico sobre $\mathbb{Q}$ si y solo si la extensión simple $\mathbb{Q}(\omega_n)/\mathbb{Q}$ es finita. Por otro lado, se define $\Gamma = \mathrm{Gal}(\mathbb{Q}[\omega_n]\colon \mathbb{Q})$ como el grupo de Galois [8] de $\mathbb{Q}[\omega_n]$ sobre $\mathbb{Q}$. Esto quiere decir que Γ es el conjunto de todos los automorfismos de campo $\sigma\colon \mathbb{Q}[\omega_n] \to \mathbb{Q}[\omega_n]$ tal que $\sigma(r) = r$ para todo $r \in \mathbb{Q}$ y σ finito.

Un hecho crucial es que si $p(z)$ es un polinomio con coeficientes racionales, entonces Γ permuta las raíces de p en $\mathbb{Q}[\omega_n]$, es decir, sus raíces se mapean a otras raíces. Las raíces primitivas de la unidad forman un grupo cíclico que tiene orden $\phi(n)$ y el grupo de Galois esta en correspondencia con este, al igual que el de las raíces con $\mathbb{Z}/n\mathbb{Z}^*$.

Lema 4.3.3. *Sea $p(z)$ un polinomio con coeficientes racionales y supongamos que $\alpha \in \mathbb{Q}[\omega_n]$ es una raíz de p. Entonces $\sigma(\alpha)$ es también una raíz de p para todo $\sigma \in \Gamma$.*

Demostración. Supóngase que $p(z) = a_k z^k + a_{k-1}z^{k-1} + \cdots + a_0$ con $a_i \in \mathbb{Q}$. Como σ es un homomorfismo de anillos que fija a los elementos ($\sigma(a_i) = a_i\ \forall i$), entonces

$$\begin{aligned}
p(\sigma(\alpha)) &= a_k\sigma(\alpha)^k + a_{k-1}\sigma(\alpha)^{k-1} + \cdots + a_0\sigma(\alpha)^0; \text{ como } \sigma \text{ es homomorfismo entonces}\\
&= a_k\sigma(\alpha^k) + a_{k-1}\sigma(\alpha^{k-1}) + \cdots + a_0\sigma(\alpha^0)\\
&= \sigma(a_k)\sigma(\alpha^k) + \sigma(a_{k-1})\sigma(\alpha^{k-1}) + \cdots + \sigma(a_0)\sigma(\alpha^0)\\
&= \sigma(a_k\alpha^k) + \sigma(a_{k-1}\alpha^{k-1}) + \cdots + \sigma(a_0\alpha^0)\\
&= \sigma(a_k\alpha^k + a_{k-1}\alpha^{k-1} + \cdots + a_0)\\
&= \sigma(p(\alpha)); \text{ ya que } \alpha \text{ es raíz de } p(z)\\
&= \sigma(0); \text{ como } \sigma \in \Gamma\\
&= 0
\end{aligned}$$

Entonces $\sigma(\alpha)$ es también una raíz de p para todo $\sigma \in \Gamma$ con α que se ha tomo arbitrario, entonces se cumple para todas las raíces de P. □

[6] Es el campo más pequeño donde el polinomio se factoriza completamente en los racionales.

[7] Un campo ciclotómico es el campo de escisión del polinomio $x^n - 1$, además es una extensión de Galois del cuerpo de los racionales y el grado de esta extensión es $[\mathbb{Q}[\omega_n]\colon \mathbb{Q}]$.

[8] Sea F una extensión del cuerpo K, el *grupo de Galois* de F sobre K se define como el grupo de automorfismos de F que dejan fijo al cuerpo K, es decir, $\mathrm{Gal}(F/K) = \{\phi \in \mathrm{Aut}(F) |\ \ \phi(a) = a\ \forall\ a \in K\}$.

Corolario 4.3.4. *Sea α una raíz n-ésima de la unidad. Entonces $\sigma(\alpha)$ también es una raíz n-ésima de la unidad para todo $\sigma \in \Gamma$.*

Demostración. Basta notar que $p(z)$ es un polinomio con coeficientes racionales; ahora como $\alpha \in \mathbb{Q}[\omega_n]$, aplicando el lema anterior al polinomio $p(z) = z^n - 1$ que tiene coeficientes racionales se tiene:

$$\begin{aligned} p(z) &= z^n - 1 \\ p(\sigma(\alpha)) &= (\sigma(\alpha))^n - 1 \\ 0 &= \sigma(\alpha)^n - 1 \\ \sigma(\alpha)^n &= 1 \end{aligned}$$

En donde $\sigma(\alpha)$ es una raíz n-ésima de la unidad y como α se tomo arbitrario entonces es una raíz n-ésima la unidad para todo $\sigma \in \Gamma$. □

Este hecho no va a ser utilizado; para los fines de este trabajo lo importante es que Γ es finito.

Corolario 4.3.5. *Sea $\alpha \in \mathbb{Q}[\omega_n]$ un entero algebraico y supóngase que $\sigma \in \Gamma$. Entonces $\sigma(\alpha)$ es un entero algebraico.*

Demostración. Sea α un entero algebraico que pertenece al campo de escisión $\mathbb{Q}(\omega_n)$, tal que es una raíz del polinomio mónico p con coeficientes enteros, y se toma un automorfismo $\sigma \in \Gamma$ arbitrario, por el Lema 4.3.3 $\sigma(\alpha)$ también es raíz de p, por lo tanto es un entero algebraico. □

Una consecuencia del Teorema Fundamental de la Teoría de Galois[(9)] cuyo resultado necesitamos es el siguiente:

Teorema 4.3.6. *Sea $\alpha \in \mathbb{Q}[\omega_n]$, entonces $\sigma(\alpha) = \alpha$ para todo $\sigma \in \Gamma$ si y solo si $\alpha \in \mathbb{Q}$*

El siguiente corolario es una variación del "truco de la suma".

Corolario 4.3.7. *Sea $\alpha \in \mathbb{Q}[\omega_n]$, entonces $\prod_{\sigma\in\Gamma} \sigma(\alpha) \in \mathbb{Q}$.*

Demostración. Sea $\tau \in \Gamma$, entonces se tiene

$$\begin{aligned} \tau\left(\prod_{\sigma\in\Gamma} \sigma(\alpha)\right) &= \prod_{\sigma\in\Gamma} \tau\sigma(\alpha); \text{ haciendo } \rho = \tau \circ \sigma \text{ con } \tau, \sigma \in \Gamma \\ &= \prod_{\rho\in\Gamma} \rho(\alpha); \text{ ya que } \tau \circ \sigma \in \Gamma \end{aligned}$$

[(9)] En su forma más básica el teorema dice que dada una extensión de cuerpos E/F que sea finita y Galois, existe una correspondencia uno a uno entre sus cuerpos intermedios (cuerpos K que satisfacen $F \subseteq K \subseteq E$; también llamados subextensiones de E/F) y los subgrupos de su grupo de Galois.

con lo cual se obtiene que $\tau\left(\prod_{\sigma\in\Gamma}\sigma(\alpha)\right)=\prod_{\rho\in\Gamma}\rho(\alpha)$ (τ fija al producto de los $\rho(\alpha)$) y aplicando el Teorema 4.3.6 se tiene que $\prod_{\sigma\in\Gamma}\sigma(\alpha)\in\mathbb{Q}$. □

El siguiente teorema es crucial para demostrar el teorema de Burnside.

Teorema 4.3.8. *Sea G un grupo de orden n y sea C una clase conjugada de G. Supóngase que $\varphi\colon G\to GL_d(\mathbb{C})$ es una representación irreducible y se asumirá que $h=|C|$ es primo relativo con con d, entonces:*

1. *Existe $\lambda\in\mathbb{C}^*$ tal que $\varphi_g=\lambda I$ para todo $g\in C$; o*
2. *$\chi_\varphi(g)=0$ para todo $g\in C$*

Demostración. Se probará cada literal

1. Sea $\chi=\chi_\varphi$ una representación irreducible, primero nótese que si $\varphi_g=\lambda I$ para algún $g\in C$ y $=kgk^{-1}$ entonces

$$\begin{aligned}\varphi_x&=\varphi_k\varphi_g\varphi_{k^{-1}}\\&=\varphi_k\lambda I\varphi_{k^{-1}}\\&=\lambda\varphi_k\varphi_{k^{-1}}\\&=\lambda\varphi_1\\&=\lambda I;\text{ para todo } x\in C\end{aligned}$$

   Además χ es una función de clase y el carácter es constante en las clases conjugadas, con lo que se puede decir que si se cumple para un elemento se cumplirá para todos; de la misma manera si se anula en cualquier elemento de C, se anula en todos los elementos de la clase. Por lo tanto, será suficiente mostrar que si $\varphi_g\neq\lambda I$ para algún $g\in C$, entonces $\chi_\varphi(g)=0$.

2. Por el Teorema 4.2.4 se sabe que $h\chi(g)/d$ es un entero algebraico; también se sabe que $\chi(g)$ es una entero algebraico por el Corolario 4.2.1. Por hipótesis $\text{MCD}(d,h)=1$ y por el Teorema de Bezout se pueden encontrar enteros k, j tales que $kh+jd=1$ de manera que:

$$\begin{aligned}kh+jd&=1\\k\frac{h}{d}+j&=\frac{1}{d};\text{ por el Corolario 4.1.6}\\k\left(\frac{h}{d}\chi(g)\right)+j\chi(g)&=\frac{\chi(g)}{d};\text{ por lo tanto este es un entero algebraico}\end{aligned}$$

Sea $\alpha = \dfrac{\chi(g)}{d}$, esto muestra que una combinación lineal de al menos dos enteros algebraicos sigue siendo un entero algebraico. Por Corolario 2.1.10, como $\varphi\colon G \to GL_d(\mathbb{C})$ es una representación irreducible entonces φ_g es diagonalizable y sus valores propios $\lambda_1, \cdots, \lambda_d$ son raíces n-ésimas de la unidad. Como φ_g es diagonalizable pero no una matriz escalar, por hipótesis $\varphi \neq \lambda I$ sus valores propios no son todos iguales. Aplicando el Lema 4.3.1 a $\chi(g) = \lambda_1 + \cdots + \lambda_d$ resulta

$$\begin{aligned} |\lambda_1 + \cdots + \lambda_d| &= |\chi(g)| \\ |\chi(g)| &< d \\ \frac{|\chi(g)|}{d} &< 1 \\ |\frac{\chi(g)}{d}| &< 1 \\ |\alpha| &< 1 \end{aligned}$$

Con lo que se puede concluir que $\alpha \in \mathbb{Q}[\omega_n]$ ya que α es la suma de todas las raíces n-ésimas de la unidad, por tanto es una suma de algebraicos y $\mathbb{Q}[\omega_n]$ es algebraicamente cerrado bajo la suma. Sea $\sigma \in \Gamma$, el Lema 4.3.3 implica que $\sigma(\alpha)$ es un entero algebraico. El Corolario 4.3.4 dice que si σ es raíz n-ésima de la unidad $\sigma(\alpha)$ también lo es, es decir que si $\chi(g)$ es entero algebraico también lo es $\sigma(\chi(g))$ y se cumple

$$\begin{aligned} \sigma(\chi(g)) &= \sigma(\lambda_1 + \cdots + \lambda_d);\ \sigma \text{ es un homomorfismo} \\ &= \sigma(\lambda_1) + \cdots + \sigma(\lambda_d) \end{aligned}$$

con lo que se tiene una suma de d raíces n-ésimas de la unidad y como σ permuta las raíces, entonces todas son diferentes. Ahora, como $\sigma \in \Gamma$ y $\sigma(\alpha) = \alpha$ (Teorema 4.3.6), otro procedimiento similar al anterior nos conduce a una aplicación del Lema 4.3.1 y se tiene

$$\begin{aligned} |\sigma(\chi(g))| &< d \\ \frac{|\sigma(\chi(g))|}{d} &< 1 \\ |\frac{\sigma(\chi(g))}{d}| &< 1 \\ |\frac{\chi(g)}{d}| &< 1 \\ |\alpha| &< 1 \\ |\sigma(\alpha)| &< 1 \end{aligned}$$

Y como $\sigma \in \Gamma$ es arbitrario, se obtiene que $q = \prod_{\sigma\in\Gamma} \sigma(\alpha)$ es un entero algebraico con

$$\begin{aligned} |q| &= |(\prod_{\sigma\in\Gamma} \sigma(\alpha))| \\ &= \prod_{\sigma\in\Gamma} |\sigma(\alpha)| \\ &< 1 \end{aligned}$$

Nótese que se tiene un producto finito de enteros algebraicos, por lo tanto q es un entero algebraico, además, el Corolario 4.3.7 garantiza que $q \in \mathbb{Q}$ y por la Proposición 4.1.4 $q \in \mathbb{Z}$. Como $|q| < 1$, se puede concluir que $q = 0$ y por lo tanto $\sigma(\alpha) = 0$ para algún $\sigma \in \Gamma$ porque se encuentra en algún campo y no hay divisores de cero. Debido a que σ es un automorfismo, esto implica que $\alpha = 0$. Finalmente se concluye que $\chi(g) = 0$.

□

Antes de demostrar el teorema de Burnside, que es el objetivo principal en este capítulo, se necesita el siguiente resultado.

Lema 4.3.9. *Sea G un grupo no abeliano finito. Supóngase que hay una clase de conjugación $C \neq \{1\}$ de G tal que $|C| = p^t$ con p primo y $t \geq 0$. Entonces G no es simple.*

Demostración. Por contradicción, supóngase que G es simple y sean $\varphi^{(1)}, \cdots, \varphi^{(s)}$ un conjunto completo de representantes de clases de equivalencia de representaciones irreducibles de G. Sean $\chi_1, \cdots, \chi_s$ sus respectivos caracteres, $d_1, \cdots, d_s$ sus grados respectivos y se tomará a $\varphi^{(1)}$ como la representación trivial.

Como G es simple, el núcleo $\ker \varphi^{(k)} = \{1\}$ para $k > 1$ (porque si $\ker \varphi^{(k)} = G$ esto implicaría que $\varphi^{(k)}$ es la representación trivial y se ha asumiendo que G es simple), entonces si $\varphi^{(k)} \colon G \longrightarrow GL_n(\mathbb{C})$ se tiene que $\ker \varphi = \{g \in G |\ \varphi(g) = I_n\} \trianglelefteq G$, y al ser un subgrupo normal entonces $\ker \varphi = \{1, G\}$, ahora si φ fuera la representación trivial, esta mapea todos los elementos g a la identidad, entonces el núcleo sería todo G; pero si no es trivial quiere decir que existe un g que no se enviá a la identidad, entonces el núcleo de φ no podría ser todo G, por lo tanto el núcleo de φ tiene que ser igual a la identidad en G, por lo tanto las demás representaciones tienen que tener núcleo trivial porque son homomorfismos normales y simples.

Como en el centro solo se tiene a la identidad, $\varphi^{(k)}$ es inyectiva para $k > 1$, como G no es abeliano y $\mathbb{C}^*$ es abeliano, las representaciones deben tener un grado mayor que 1, ya que si no fuera así al tener una función inyectiva con una imagen abeliana pasaría que

$$\begin{aligned} \varphi(ab) &= \varphi(a)\varphi(b) \\ &= \varphi(b)\varphi(a); \text{ ya que } \varphi(a) \text{ y } \varphi(b) \in \mathbb{C}^* \\ &= \varphi(ba) \end{aligned}$$

como φ es inyectiva entonces $ab = ba$, lo que implicaría que G es conmutativo y esto contradice la hipótesis; por ello se deduce que $d_k > 1$ para $k > 1$. Como G es simple el centro puede ser $Z(G) = \{1, G\}$, pero G no puede ser porque el centro es normal al grupo y si fuera G entonces sería abeliano, por ello $Z(G) = \{1\}$, lo que implica que $t > 0$ ya que $|C| = p^0 = 1$ es la clase conjugada de la identidad.

Sea $g \in C$, $k > 1$ y sea Z_k el conjunto de todos los elementos $x \in G$ tal que $\varphi_x^{(k)}$ es una matriz escalar, que en este caso sera una matriz diagonalizable. Sea $H = \{\lambda I_{d_k} \mid \lambda \in \mathbb{C}^*\}$ estas matrices escalares; como $\lambda I_{dk} A = \lambda A I_{d_k} = A\lambda I_{d_k}$, entonces está contenida en el centro, ahora haría falta probar que es un subgrupo. Sea $I_{d_k} \in H \neq \varnothing$ y λI_{d_k}, $\beta I_{d_k} \in H$ entonces

$$\lambda I_{d_k}(\beta I_{d_k})^{-1} = \lambda I_{d_k}\left(\frac{1}{\beta}\right) I_{d_k} = \frac{\varphi}{\beta} I_{d_k} \in H$$

en el proceso anterior $\beta \neq 0$ por lo tanto H es un subgrupo normal de $GL_{d_k}(\mathbb{C})$.

Nótese que Z_k así como esta definido es la imagen inversa de H bajo $\varphi^{(k)}$, ya que es el conjunto de elementos tales que la imagen es una matriz diagonal, como H es normal se concluye que Z_k es un subgrupo normal de G. Nuevamente como G es simple entonces $Z_k = \{1, G\}$, pero $d_k > 1$, entonces si $Z_k = G$ se tendría que todos los elementos de G están siendo mapeados a matrices escalares esto implica que $\varphi_x^k = \lambda I_{dk}$ y esto es equivalente a decir que mapea a λ, entonces esta representación sería de grado 1, pero ya se vió que solo la representación trivial tenía grado 1 y que el grado tiene que ser mayor que 1, por lo tanto $Z_k = \{1\}$.

Supóngase por el momento que $p \nmid d_k$ (primos relativos) ya que el orden de la clase debe ser primo relativo con d_k que es el grado de la representación, porque le máximo común solo puede ser 1 o p; p no puede ser porque estamos asumiendo que son primos relativos, entonces existe un λ tal que $\varphi_g^k = \lambda I_{dk}$ para todo $g \in C$, pero si fuera así este pertenecería a Z_k, el cual ya sabíamos que tiene tamaño uno y la clase C tiene tamaño p^t con $t > 0$, entonces tiene tamaño mayor que 1; así lo que se prueba es que ningún elemento de la clase mapea a un escalar, por lo tanto, no se cumple el literal 1 del Teorema 4.3.8, por lo que debe cumplirse el literal 2, con lo que se tendría que $\chi_k(g) = 0$ para todo g..

Ahora sea L la representación regular de G, por el Teorema 2.4.4 se tiene que $L \sim d_1\varphi^{(1)} \oplus \cdots \oplus d_s\varphi^{(s)}$, como $g \neq 1$, la proposición 2.4.3 y el Lema 2.3.13 conduce a

$\chi_L(g) = d_1\chi_1(g) + \cdots + d_s\chi_s(g)$; como $\chi_1(g) = 1$ y $d_1 = 1$ se tiene

$$0 = 1 + \sum_{k=2}^{s} d_k\chi_k(g); \text{ si } p \nmid d_k \Longrightarrow \chi_k(g) = 0 \text{ para todo } g, \text{ por tanto se sumará donde } p|d_k$$

$$0 = 1 + \sum_{p|d_k} d_k\chi_k(g); \text{ por el Corolario 4.2.1 } \chi_k(g) \text{ es algebraico para todo } g$$

$$0 = 1 + p\sum_{p|d_k} a_k\chi_k(g); \text{ con } d_k = pa_k$$

$$0 = 1 + pz; \text{ con } z = \sum_{p|d_k} a_k\chi_k(g)$$

En donde pz es también un algebraico por que es el producto de algebraicos, esto lleva a obtener que $z = -\frac{1}{p}$ es un entero algebraico por la Proposición 4.1.4, pero esto es una contradicción porque se esta afirmando que $-\frac{1}{p}$ es el negativo del inverso de un primo, lo cual no es un entero. Por lo tanto G es no simple. □

Teorema 4.3.10. ***(Burnside)***

Sea G un grupo de orden $p^a q^b$ con p, q primos. Entonces G no es simple a menos que sea cíclico de orden primo.

Demostración. Por el Teorema de Cauchy, un grupo abeliano es simple si y sólo si es cíclico de orden primo. Si G fuera abeliano la única forma que fuera simple es que fuera cíclico de orden primo, por tanto puede suponerse que G no es abeliano. Dado que los grupos de orden primo tienen centros no triviales [13] (si G no es igual a 1 y es un p-grupo finito su centro no es trivial). Si los grupos de orden primo tienen centros no triviales, al tomar un grupo G no abeliano con a o b igual a cero, significaría que el grupo tiene un subgrupo normal y por lo tanto no seria simple.

Ahora supóngase que $a, b \geq 1$, por los Teoremas de Sylow [13], G tiene un subgrupo H de orden q^b. Sea $1 \neq g \in Z(H)$ porque ya se sabe que tiene un centro no trivial y los q-grupos tienen orden mayor que 1, sea $N_G(g) = \{x \in G \mid xg = gx\}$ el normalizador de g en G. Como $H \leq G$ tal que $|H| = q^b$ y $g \in Z(H)$, entonces $H \subseteq N_G(g)$ debido a que $g \in Z(H)$ entonces para todo $x \in H$ sucede que $gx = xg$. De esta manera

$$\begin{aligned} p^a &= \frac{p^a q^b}{q^b} \\ &= \frac{|G|}{|H|} \\ &= [G\colon H]; \text{ entonces por propiedad de los índices si } k \leq H \leq G [G\colon k] = [G\colon H][H\colon K] \\ &= [G\colon N_G(g)][N_G(g)\colon H]; \text{ ya que } H \subseteq N_G(g) \end{aligned}$$

y entonces $[G\colon N_G(g)] = p^t$ porque es un divisor de p^a para algún $t \geq 0$ y $t \leq a$. Pero $[G\colon N_G(g)]$ es el tamaño de la clase conjugada de g. El lema anterior implica que existe un elemento que no es la identidad por que así se ha definido, tal que el orden de la clase es p^t con $t > 0$ por lo tanto G no es simple. □

Capítulo 5

Probabilidad y Paseos Aleatorios sobre Grupos

Una de las aplicaciones de la Teoría de Representaciones de Grupos es en la Probabilidad y la Estadística. En un famoso artículo [16], Bayer y Diaconis dieron estimaciones muy precisas sobre la cantidad de "riffles" [(1)] que se necesitan para aleatorizar una baraja de n cartas. Bayer y Diaconis concluyeron con base en sus resultados que, para un mazo de 52 cartas, siete *riffle*s son suficientes, sin embargo, cualquier reordenamiento está demasiado lejos de ser aleatorio, mientras que la ganancia neta en aleatoriedad para hacer más de siete barajados, no es suficiente para garantizar los barajados adicionales.

Bayer y Diaconis basaron su trabajo en un modelo de *riffles* de n cartas como un paseo aleatorio en el Grupo Simétrico S_n. Las propiedades del álgebra $L(S_n)$ juegan un papel importante en su análisis. También, se han analizado otros métodos de intercambio de cartas utilizando la teoría de representaciones del grupo simétrico S_n [14], pero no se retomarán en este trabajo; en este capítulo se presenta la teoría básica de probabilidad sobre grupos y se describen algunos ejemplos de barajado de cartas, como aplicaciones de la Teoría de Representaciones en la Probabilidad.

5.1. Probabilidades sobre Grupos

Sea G sea un grupo finito y supóngase que X es una *variable aleatoria* con valores en G. Formalmente, esto significa que X es una función $X\colon \Omega \longrightarrow G$, donde Ω es algún espacio de probabilidad. La distribución de la variable aleatoria X es la función $P\colon G \longrightarrow [0,1]$ definida

[(1)] El término utilizado en inglés es "riffle shuffle", que no es más que cortar el paquete de cartas en dos grupos, tomar con cada mano cada uno de estos, colocarlos uno frente al otro por el lado corto y luego barajar (intercalar) las cartas de forma rápida dejando caer cartas de cada una de las manos (de preferencia una a una para una mejor mezcla) en esa misma posición; a este movimiento se le llama también "Barajado a la americana" o "Cola de Milano". Esta acción puede verse como un reordenamiento de las cartas en alguna posición diferente de la original.

por

$$P(g) = \text{Prob}[X = g]$$

Para todos los propósitos prácticos, todo lo que se necesita saber sobre la variable aleatoria X es que está codificada en su distribución y, por lo tanto, ni siquiera se necesita saber qué es Ω. Observése que P satisface

$$\sum_{g \in G} P(g) = 1 \tag{5.1}$$

Por el contrario, cualquier función $P\colon G \longrightarrow [0,1]$ que satisfaga (5.1) será la distribución de alguna variable aleatoria con G-valores. Entonces, en este trabajo, se utilizará exclusivamente distribuciones de probabilidad en lugar de variables aleatorias.

Definición 5.1.1. (Distribución de probabilidad). Una *distribución de probabilidad*, o simplemente una *probabilidad*, sobre un grupo finito G es una función $P\colon G \longrightarrow [0,1]$ en donde (5.1) se mantiene. Sea un evento A tal que $A \subseteq G$, entonces la probabilidad de ese evento esta dado por

$$P(A) = \sum_{g \in A} P(g)$$

El *soporte* de la probabilidad P es el conjunto $\text{supp}(P) = \{g \in G \mid P(g) \neq 0\}$, es decir, este es el conjunto para el cuál tiene sentido hablar de probabilidad.

Intuitivamente, si P es una probabilidad sobre G, entonces si aleatoriamente se elege un elemento X de G de acuerdo a P, entonces la probabilidad de que $X = g$ esta dada por $P(g)$. De manera más general, si $A \subseteq G$, entonces $P(A)$ es la probabilidad de que un elemento X de G que es elegido al azar de acuerdo con P, pertenezca a A. Por ejemplo, si tiramos una moneda el grupo a considerar puede ser $G = \mathbb{Z}/2\mathbb{Z}$ y $P([0]) = 1/2$, $P([1]) = 1/2$, entonces P es una probabilidad sobre G para la cual $[0]$ y $[1]$ son igualmente probables; lo descrito anteriormente se puede generalizar a cualquier grupo en la siguiente definición.

Definición 5.1.2. (Distribución uniforme) Sea G sea un grupo finito, entonces la *distribución uniforme* U sobre G viene dada por

$$U(g) = \frac{1}{|G|}$$

para toda $g \in G$

Normalmente se piensa que la distribución uniforme es imparcial. Por lo general, cuando alguien informalmente habla de elegir un elemento al azar, significa elegir un elemento de acuerdo con la distribución uniforme, es decir, que sea equiprobable. Por otro lado, se observa que para cualquier $g \in G$, la función

$$\delta_g = \begin{cases} 1, & \text{si } x = g; \\ 0, & \text{caso contrario ;} \end{cases}$$

es una distribución de probabilidad para la cual g tiene probabilidad 1 de ser elegido, y todos los demás elementos no tienen probabilidad de ser elegidos en absoluto o mejor dicho tienen probabilidad 0 de ser elegidos; nótese que es una distribución de probabilidad ya que la suma de las probabilidades es siempre 1.

Observése que una probabilidad P se puede ver como un elemento de $L(G)$ ya que $P\colon G \to [0,1]$ y $[0,1] \subseteq \mathbb{C}$. Un hecho conveniente es que la convolución de probabilidades es nuevamente una probabilidad; podemos notar que la convolución tiene una interpretación probabilística muy natural. Se comprobará lo anterior, para ello sean P y Q probabilidades sobre G. Supóngase que se elige X al azar de acuerdo con P y se elige al azar Y de acuerdo con Q. Se calcula la probabilidad $XY = g$. Si $Y = h$, entonces para que ocurra $XY = g$, se debe tener $X = gh^{-1}$. La probabilidad de que estos dos eventos ocurran simultáneamente es $P(gh^{-1})Q(h)$ (por independencia). Sumando todas las elecciones posibles de h se tiene que

$$\text{Prob}[XY = g] = \sum_{h \in G} P(gh^{-1})Q(h) = P * Q(g)$$

Por lo tanto, $P * Q$ es la distribución de la variable aleatoria XY siempre que X e Y sean variables aleatorias independientes con distribuciones P y Q respectivamente. La siguiente proposición verifica formalmente que $P * Q$ es una distribución de probabilidad.

Antes de ver la siguiente propiedad para el soporte de la convolución, se define el producto entre elementos de conjuntos de la siguiente manera: "Sean A y $B \subseteq G$ entonces $A \cdot B = \{xy \mid x \in A \wedge y \in B\}$".

Proposición 5.1.3. *Sean P y Q probabilidades sobre G, entonces $P * Q$ es una probabilidad sobre G con soporte* $\text{supp}(P * Q) = \text{supp}(P) \cdot \text{supp}(Q)$.

Demostración. Como P y Q son probabilidades entonces su rango es el intervalo $[0,1]$, de esta forma se puede construir las siguientes desigualdades

$$\begin{aligned} 0 &\leq \sum_{h \in G} P(gh^{-1})Q(h); \text{ pero } P(gh^{-1}) \leq 1 \text{ y } Q(h) \leq 1 \text{ entonces} \\ &\leq \sum_{h \in G} Q(h) \\ &= 1 \end{aligned}$$

y entonces $P * Q(g) \in [0,1]$. Luego, se calcula

$$\sum_{g\in G} P * Q(g) = \sum_{g\in G}\sum_{h\in G} P(gh^{-1})Q(h) \tag{5.2}$$
$$= \sum_{h\in G} Q(h)\sum_{g\in G} P(gh^{-1}) \tag{5.3}$$
$$= \sum_{h\in G} Q(h) \tag{5.4}$$
$$= 1 \tag{5.5}$$

donde (5.4) resulta de tomar h fijo y g barre con todos los elementos entonces gh^{-1} corre a través de cada elemento de G exactamente una vez. Se sigue que $P * Q$ es una distribución de probabilidad sobre G.

Ahora observése que pasa con el soporte de la convolución, para ello se utilizará la doble inclusión para probarlo.

"*Si* $g \in \text{supp}(P * Q)$ *entonces* $g \in \text{supp}(P)\cdot\text{supp}(Q)$"

Se sabe por definición que $\text{supp}(P * Q) = \{g \in G \mid P * Q(g) \neq 0\}$ sea $g \in \text{supp}(P * Q)$ observése que $P * Q(g) \neq 0$ si y solo si existe $h \in G$ tal que $P(gh^{-1}) \neq 0$ y $Q(h) \neq 0$; si se hace $x = gh^{-1}$ y $y = h$, entonces $P(x) \neq 0$ y $Q(y) \neq 0$ y por lo tanto $x \in \text{supp}(P)$ e $y \in \text{supp}(Q)$ con $xy = g$, entonces $g \in \text{supp}(P)\cdot\text{supp}(Q)$.

Por otro lado

"*Si* $t \in \text{supp}(P)\cdot\text{supp}(Q)$ *entonces* $t \in \text{supp}(P * Q)$"

$$\begin{aligned}\text{supp}(P)\cdot\text{supp}(Q) &= \{xy \in G \mid x \in \text{supp}(P) \wedge y \in \text{supp}(Q)\}\\ &= \{xy \in G \mid P(x) \neq 0 \text{ y } Q(y) \neq 0\}\end{aligned}$$

sea $t \in \text{supp}(P)\cdot\text{supp}(Q)$ tal que $t = xy$, en donde $x = ty^{-1}$

$$\begin{aligned}P * Q(t) &= \sum_{h\in G} P(th^{-1})Q(h)\\ &= \sum_{h\in\{G-\{y\}\}} P(th^{-1})Q(h) + P(ty^{-1})Q(y)\\ &= \sum_{h\in\{G-\{y\}\}} P(th^{-1})Q(h) + P(x)Q(y)\\ &> 0\end{aligned}$$

Entonces $P * Q(t) \neq 0$ por lo tanto $t \in \text{supp}(P * Q)$.

Se concluye que $\text{supp}(P * Q) = \text{supp}(P)\cdot\text{supp}(Q)$, como se requería. □

En orden de determinar si una distribución es uniforme o que tan lejos esta de serlo, se necesita definir alguna noción de distancia entre probabilidades. Para ello se presenta la L^1-norma sobre $L(G)$.

Definición 5.1.4. **(L^1-norma)** La L^1 sobre $L(G)$*norma* esta definida por

$$\|f\|_1 = \sum_{g\in G} |f(g)|$$

para $f\colon G \longrightarrow \mathbb{C}$.

Por ejemplo, si P es una probabilidad sobre G, entonces $\|P\|_1 = 1$ ya que por definición se sabe que $\sum_{g\in G} P(g) = 1$ y como el rango son los reales en el intervalo $[0, 1]$ entonces $|g| = g$.

Véase algunas de las propiedades que posee la L^1-norma.

Definición 5.1.5. Sean a, $b \in L(G)$, entonces:

1. $\|a\|_1 = 0$ si y solo si $a = 0$;
2. $\|ca\|_1 = |c| \cdot \|a\|_1$ para $c \in \mathbb{C}$;
3. $\|a + b\|_1 \leq \|a\|_1 + \|b\|_1$ (la desigualdad triangular)
4. $\|a * b\|_1 \leq \|a\|_1 \cdot \|b\|_1$

Demostración. Se probará cada uno de los numerales; se observa que del numeral 1 al 3 lo único que se esta probando es que es una norma, el literal 4 es una propiedad extra para la L^1-norma.

- $\|a\|_1 = 0$ si y solo si $a = 0$;

$$\begin{aligned}\|a\|_1 &= \sum_{g\in G} |a(g)| \\ &= 0; \text{ si y solo si } |a(g)| = 0 \Longleftrightarrow a \text{ es la función nula, para todo } g \in G\end{aligned}$$

- $\|ca\|_1 = |c| \cdot \|a\|_1$ para $c \in \mathbb{C}$;

$$\begin{aligned}\|ca\|_1 &= \sum_{g\in G} |ca(g)| \\ &= \sum_{g\in G} |c||a(g)| \\ &= |c| \sum_{g\in G} |a(g)| \\ &= |c| \, \|ca\|_1 \text{ ; para } c \in \mathbb{C}\end{aligned}$$

- $\|a+b\|_1 \leq \|a\|_1 + \|b\|_1$ (la desigualdad triangular)

$$\begin{aligned}
\|a+b\|_1 &= \sum_{g\in G} |(a+b)(g)| \\
&= \sum_{g\in G} |a(g)+b(g)| \\
&\leq \sum_{g\in G} |a(g)| + |b(g)|; \text{ por la desigualdad triangular} \\
&\leq \sum_{g\in G} |a(g)| + \sum_{g\in G} |b(g)| \\
&\leq \|a\|_1 + \|b\|_1
\end{aligned}$$

- $\|a*b\|_1 \leq \|a\|_1 \cdot \|b\|_1$

$$\begin{aligned}
\|a*b\|_1 &= \sum_{g\in G} |a*b(g)| \\
&= \sum_{g\in G} \left| \sum_{h\in G} a(gh^{-1})b(h) \right| \\
&\leq \sum_{g\in G} \sum_{h\in G} |a(gh^{-1})b(h)|; \text{ generalización de la desigualdad triangular (Lema 4.3.1)} \\
&\leq \sum_{g\in G} \sum_{h\in G} \left|a(gh^{-1})\right| |b(h)| \\
&= \sum_{h\in G} |b(h)| \sum_{g\in G} \left|a(gh^{-1})\right| \\
&= \|a\|_1 \cdot \|b\|_1
\end{aligned}$$

  donde la ultima igualdad se cumple para h fijo y g variable, de esta manera gh^{-1} barre con todos los elementos sobre G.

□

Los probabilistas usan una variación de la L^1-norma para definir la distancia entre las probabilidades, como la que se muestra a continuación.

Definición 5.1.6. Variación Total
La *variación total* entre dos probabilidades P y Q sobre un grupo G esta definida por

$$\|P-Q\|_{TV} = \sup_{A\subseteq G} |P(A)-Q(A)| \tag{5.6}$$
$$= \max_{A\subseteq G} |P(A)-Q(A)| \tag{5.7}$$

Se observa que el *máximo* coincide con el *supremo*, ya que el conjunto es finito y por lo tanto se tiene un número finito de subconjuntos ($2^{|G|}$ de hecho), de tal forma que siempre se podrá encontrar un subconjunto más grande en donde se dará la variación total.

Esta definición permite determinar si dos probabilidades están cerca con respecto a la distancia de variación total, es decir, si difieren poco en cada subconjunto de G. La distancia de variación total está estrechamente relacionada con la L^1-norma y para establecer esta relación, se necesita el siguiente lema que describe el conjunto A donde se alcanza el máximo en (5.7).

Lema 5.1.7. *Sean P y Q probabilidades sobre Q, además sean*

$$B = \{g \in G \mid P(g) \geq Q(g)\}$$
$$C = \{g \in G \mid Q(g) \geq P(g)\}$$

Entonces $\|P - Q\|_{TV} = P(B) - Q(B) = Q(C) - P(C)$

Demostración. Se verá por casos, si $P = Q$, no hay nada que probar ya que $\|P - Q\|_{TV} = P(B) - Q(B) = Q(C) - P(C) = 0$.

Entonces podemos suponer que $P \neq Q$; entonces debe existir un elemento $w \in G$ tal que $P(w) > Q(w)$; ya que si $P(h) \leq Q(h)$ para todo $h \in G$ se tendría que $Q - P$ no es negativo sobre G y

$$\begin{aligned}\sum_{h\in G}(Q(h) - P(h)) &= \sum_{h\in G} Q(h) - \sum_{h\in G} P(h)\\ &= 1 - 1\\ &= 0 \iff Q(h) - P(h) = 0; \text{ para todo } h\end{aligned}$$

por tanto $P = Q$ y se sabe con esto que $w \in B$ y que pertenece a $B - C$ (no es vacío).

Entonces para todo $g \in B$ se cumple que $P(g) \geq Q(g)$ con lo que $P(g) - Q(g) \geq 0$ y se sabe que

$$\begin{aligned}\|P - Q\|_{TV} &\geq |P(B) - Q(B)|\\ &= P(B) - Q(B); \text{ ya que es positivo}\end{aligned}$$

Se sabe por definición que existe $A \subseteq G$ tal que es máximo, es decir,

$$\|P - Q\|_{TV} = |P(A) - Q(A)| \tag{5.8}$$

ya que G es finito; sea $A^c = G - A$ el complemento de A. Entonces

$$\begin{aligned}|P(A^c) - Q(A^c)| &= |1 - P(A) - (1 - Q(A))|\,; \text{ por propiedades de la probabilidad}\\ &= |1 - P(A) - 1 + Q(A)|\\ &= |Q(A) - P(A)|\\ &= |-[P(A) - Q(A)]|\,; \text{ por propiedades del valor absoluto se tiene que}\\ &= |P(A) - Q(A)|\,; \text{ por (5.8)}\\ &= \|P - Q\|_{TV}\end{aligned}$$

con lo que se observa que el complemento también cumple. Ahora, se reemplazará A por su complemento, debido a que este tiene dos opciones: $w \in A$ o $w \in A^c$; se asume sin pérdida de generalidad que $w \in A$[(2)], entonces $|P(A) - Q(A)| = P(A) - Q(A)$ y se observa que debe ser así.

Se asume por contradicción que $|P(A) - Q(A)| = Q(A) - P(A)$, entonces se tendría que

$$\begin{aligned} Q(A - \{w\}) - P(A - \{w\}) &= Q(A) - Q(w) - [P(A) - P(w)]\,; \text{ con } P(w) - Q(w) \geq 0 \\ &= Q(A) - P(A) + P(w) - Q(w); \text{ con } P(w) - Q(w) \geq 0 \\ &> Q(A) - P(A) \\ &= \|P - Q\|_{TV} \end{aligned}$$

lo cual es una contradicción, ya que se ha encontrado una distancia mayor y esto implicaría que el máximo no era $\|P - Q\|_{TV}$. Similarmente, si existe otro elemento $h \in A$ que cumpla con $Q(h) > P(h)$, entonces con un argumento similar al mostrado se encuentra que $P(A - \{h\}) - Q(A - \{h\}) > P(A) - Q(A)$, lo que se tiene de nuevo a una contradicción que viene de asumir que esta en el subconjunto A, pero que no esta en B; entonces para todo $h \in A$ debe cumplirse $Q(h) < P(h)$ por lo tanto $A \subseteq B$ y $B = A \cup (B - A)$, se tendría que

$$P(A) - Q(A) + P(B - A) - Q(B - A) = P(B) - Q(B); \text{ pero } P(B - A) - Q(B - A) \geq 0$$

y como a $P(A) - Q(A)$ se le esta sumando algo mayor o igual que cero, entonces $P(B) - Q(B) \geq P(A) - Q(A)$ para cualquier subconjunto $A \subseteq B$ y por tanto esta sería la distancia máxima, obteniendo que $\|P - Q\|_{TV} = P(B) - Q(B)$.

Un argumento dual, en donde se intercambia el orden de las desigualdades, muestra que $\|P - Q\|_{TV} = Q(C) - P(C)$, con lo que se concluye que $\|P - Q\|_{TV} = P(B) - Q(B) = Q(C) - P(C)$. □

Proposición 5.1.8. *La igualdad*

$$\|P - Q\|_{TV} = \frac{1}{2}\|P - Q\|_1$$

se cumple para todas las probabilidades P, Q sobre el grupo finito G.

Demostración. Sean B, C como en el lema anterior, entonces se cumple que

$$\begin{aligned} \|P - Q\|_{TV} &= Q(C) - P(C) \\ \|P - Q\|_{TV} &= P(B) - Q(B) \end{aligned}$$

Ahora si se multiplica cada igualdad por $\frac{1}{2}$, se tiene

$$\begin{aligned} \frac{1}{2}\|P - Q\|_{TV} &= \frac{1}{2}(P(B) - Q(B)) \\ \frac{1}{2}\|P - Q\|_{TV} &= \frac{1}{2}(Q(C) - P(C)) \end{aligned}$$

(2) Ya que se ha visto que el complemento cumple lo mismo, por lo tanto puede ser reemplazado a conveniencia, cuando sea necesario.

luego se suman ambos resultados y se obtiene

$$\begin{aligned}
\|P-Q\|_{TV} &= \frac{1}{2}(P(B)-Q(B))+\frac{1}{2}(Q(C)-P(C)) \\
&= \frac{1}{2}[P(B)-Q(B)+Q(C)-P(C)] \\
&= \frac{1}{2}\left[\sum_{\{g|P(g)\geq Q(g)\}}(P(g)-Q(g))+\sum_{\{g|Q(g)\geq P(g)\}}(Q(g)-P(g))\right] \\
&= \frac{1}{2}\left[\sum_{\{g|P(g)\geq Q(g)\}}(P(g)-Q(g))+\sum_{\{g|Q(g)\geq P(g)\}}(Q(g)-P(g))+0\right] \\
&= \frac{1}{2}\left[\sum_{\{g|P(g)\geq Q(g)\}}|P(g)-Q(g)|+\sum_{\{g|Q(g)\geq P(g)\}}|P(g)-Q(g)|+\sum_{\{g|P(g)=Q(g)\}}|P(g)-Q(g)|\right] \\
&= \frac{1}{2}\left[\sum_{g\in G}|P(g)-Q(g)|\right] \\
&= \frac{1}{2}\sum_{g\in G}|P(g)-Q(g)| \\
&= \frac{1}{2}\|P-Q\|_1 \text{ ; por la definición de la } L^1\text{-norma}
\end{aligned}$$

como se quería. □

En consecuencia la Variación Total posee todas las propiedades habituales de una distancia, por lo tanto, tiene sentido hablar de limites, en donde el limite de P_n es igual a P, cuando $n \longrightarrow \infty$.

5.2. Paseos Aleatorios sobre Grupos Finitos

En esta sección se presentan algunos resultados importantes de los paseos aleatorios para ser utilizados en los ejemplos de la siguiente sección.

¿Qué es un *paseo aleatorio*? para hacerse una idea de lo que se verá en esta sección imagínese un turista que sale de un hotel en una ciudad que no conoce y que decide recorrerla sin un destino particular, entonces la ciudad se modela a través de un grafo, donde los vértices representan intersecciones y las aristas representan calles, así cada vez que el turista llega a una intersección, elige al azar una calle y continúa su camino. La pregunta natural es ¿cuál es la probabilidad de que el turista regrese al hotel después de n pasos?, ¿cuál es la distribución de probabilidad sobre las intersecciones que describe dónde se encuentra el turista después

de n pasos? Las definiciones que se verán en esta sección dan respuesta a estas interrogantes.

Existen varios procesos que están modelados por paseos aleatorios, por ejemplo, los vértices de un grafo pueden representar configuraciones de algunos objetos, como el orden de una baraja de cartas, en donde los bordes representarían como una configuración puede transformarse en otra después de un solo paso (por ejemplo, cómo puede cambiar la baraja después de un *riffle*). El paseo aleatorio modela cómo se pasa aleatoriamente de una configuración a la siguiente y es precisamente esta noción la que se necesita para la siguiente sección. Por último se considera que si Γ es el grafo de Cayley de un grupo G, entonces un paseo aleatorio en Γ también se conoce como paseo aleatorio sobre G.

Si P es una probabilidad sobre un grupo G, se define la k-ésima convolución de P como la potencia P^{*k}, en lugar de P^k para evitar confusiones con el producto punto a punto de las funciones.

Definición 5.2.1. (Paseo Aleatorio)

Sea P una probabilidad sobre un grupo finito G. Entonces un paseo aleatorio sobre G inducido[(3)] por P es la sucesión de distribuciones de probabilidad $(P^{*k})_{k=0}^{\infty}$.

Se puede pensar en los paseos aleatorios de la siguiente forma: se comienza en la identidad y se elige un elemento X_1 de G de acuerdo a P y se mueve a X_1. Luego se elige un elemento X_2 de acuerdo a P y se mueve a X_2X_1, etc. Formalmente hablando, se considera una sucesión de variables aleatorias X_1, $X_2, \cdots$ independientes e idénticamente distribuidas, con una distribución común P.

Sea Y_0 una variable aleatoria con distribución δ_1, es decir, $Y_0 = 1$ con probabilidad 1. Sean $Y_k = X_kY_{k-1}$ para $k > 1$. La variable aleatoria Y_k devuelve la posición de un caminante en el k-ésimo paso del paseo aleatorio, así se obtiene que Y_k es una variable aleatoria con distribución P^{*k}. Entonces el paseo aleatorio se puede identificar con la sucesión de variables aleatorias Y_0, Y_1, $\cdots$ o la sucesión de distribuciones de probabilidad δ_1, P, P^{*2}, $\cdots$.

Ejemplo 5.2.2. (Paseo aleatorio simple)

Sean G un grupo, S un subconjunto simétrico y Γ el grafo de Cayley de G con respecto a S. Entonces, el *paseo aleatorio simple* sobre Γ es el paseo aleatorio sobre G dirigido por la probabilidad $\frac{1}{|S|} \cdot \delta_S$.

Ya que si el caminante se encuentra en el vértice g del grafo de Cayley, se sabe que se tiene tantas salidas como elementos tenga S y la probabilidad de tomar una de estas salidas, al ser uniforme la distribución de probabilidad, es $\dfrac{1}{|S|}$. Así, si se toma un elemento de G y este está en S, entonces tiene probabilidad $\dfrac{1}{|S|} \cdot d_S$ ya que es uno de los elementos que permite el movimiento en el grafo.

(3) El término utilizado en inglés es "driven by" que en español sería "dirigido por", sin embargo, al traducirlo así, parece que la probabilidad es determinista, por ello se utilizó la expresión "inducido por" para solventar esta dificultad.

Un paseo aleatorio simple puede verse de la siguiente manera: el caminante comienza con la identidad de G, ahora supóngase que en el k-ésimo paso del paseo, el caminante está en el vértice $g \in G$. Entonces un elemento $s \in S$ es elegido al azar (con todos los elementos de S igualmente probables ya que se trata de una distribución uniforme) y el caminante se mueve al vértice sg, entonces por construcción, los vértices adyacentes en Γ hacia el vértice g son precisamente los elementos de la forma sg con $s \in S$.

El siguiente tipo de paseo aleatorio es la *urna de Ehrenfest*, que es un paseo aleatorio sobre $(Z/2\mathbb{Z})^n$. Para ver más ejemplos, puede consultarse [15].

Ejemplo 5.2.3. (La urna de Ehrenfest)

Se tienen dos urnas A y B que contienen un total de n bolas entre ellas. Al principio todas las bolas están en la urna A, en cada paso en el tiempo, una de las n bolas se elige al azar (todas las bolas son igualmente probables) y se mueve a la otra urna. Se codifica el espacio de configuración a través de elementos de $(\mathbb{Z}/2\mathbb{Z})^n$ de la siguiente manera: si $v = (c_1, \cdots, c_n) \in (\mathbb{Z}/2\mathbb{Z})^n$, entonces esta configuración permite conocer en cuál de las dos urnas se encuentra una determinada bolita, es decir, si $c_i = [0]$ esto corresponde a tener la bola i en la urna A y $c_i = [1]$ a tener la bola i en la urna B, obteniendo un total de n cambios.

Entonces, la configuración inicial es el vector canónico $([0], \cdots, [0])$ (la identidad), luego sea e_i el vector con $[1]$ en la i-ésima coordenada y $[0]$ en todas las demás, entonces a partir de la configuración correspondiente a v se puede cambiar la urna que contiene la bola i y me lleva a la configuración $e_i + v$. Este proceso estocástico de cambiar las bolas entre las urnas corresponde a un paseo aleatorio sobre $(\mathbb{Z}/2\mathbb{Z})^n$ inducido por la probabilidad

$$\begin{aligned} P &= \frac{1}{n}(\delta_{e_1} + \cdots + \delta_{e_n}) \\ &= \frac{1}{n}\delta_S; \text{ con } S = \{e_1, \ldots, e_n\} \end{aligned}$$

en donde $\delta_{e_i} = 1$ si tiene un 1 en la i-ésima posición.

De esta forma una urna de Ehrenfest se considera un paseo aleatorio simple en el grafo de Cayley de $(\mathbb{Z}/2\mathbb{Z})^n$ con respecto al conjunto simétrico $\{e_1, \cdots, e_n\}$.

Una paseo aleatorio sobre un grupo G se puede ver como una forma de generar aleatoriamente un elemento de G. Usualmente, se quiere que todos los elementos de G sean igualmente probables, es decir, en términos de las distancias entre probabilidades, encontrar un $k \in \mathbb{N}$ tal que $\left\|P^{*k} - U\right\|_{TV}$ sea muy pequeña, pero que no sea demasiado grande, de tal forma que P^{*k} convergiera a U, para que todos los elementos estuviesen uniformemente distribuidos, sin embargo, la convergencia de P^{*k}esto esta fuera de los alcances de este trabajo.

En la siguiente sección, se verán algunos ejemplos adicionales provenientes de barajar cartas y se terminará esta sección citando (sin demostración) el teorema de convergencia para paseos aleatorios en grupos finitos, pero para ello se necesita definir primero cuando un paseo aleatorio es ergódico.

Definición 5.2.4. (Paseo aleatorio Ergódico)

Se dice que un paseo aleatorio sobre un grupo G inducido por una probabilidad P es *ergódico* si existe un número entero $N > 0$ tal que $P^{*N}(g) > 0$ para todo $g \in G$, es decir, $\text{supp}(P^{*N}) = G$.

Proposición 5.2.5. *Sea P una probabilidad sobre un grupo finito G y supóngase que:*

1. $P(1) > 0$
2. $\text{supp}(P)$ *genera el grupo* G

Entonces el paseo aleatorio dirigido por P es ergódico.

Demostración. Sea $S = \text{supp}(P)$, como $P(1) > 0$ entonces $1 \in S$ y nótese que $S^k \subseteq S^{k+1}$ para todo $k \geq 0$.

Además por (2) se sabe que

$$\langle S \rangle = G$$

entonces por definición

$$\langle S \rangle = \left\{ s_1 \cdots s_k \mid s_i \in S \cup S^{-1} \ \forall i \in \{1, \cdots, k\} \right\}$$

como el grupo es finito sea $|G| = n$ y como S lo genera, entonces para todo s que pertenece a S implica que $s \in G$ y que

$$\begin{aligned} s^n &= 1 \\ s \cdot s^{n-1} &= 1; \text{ entonces} \\ s^{-1} = s^{n-1} \in S^{n-1} &\Longrightarrow S \cup S^{-1} \subseteq S \cup S^{n-1} \subseteq S^{n-1} \end{aligned}$$

Con esto se garantiza que se tiene a todos los elementos en S^{n-1} y se quiere demostrar que se puede encontrar un producto finito y que permita generar a todo $\langle S \rangle$, entonces se toma $x \in G$ esto significa que para este elemento $\exists\ k_x$ tal que $x = s_1 \cdots s_{k_x} \in S^{n-1}$ y para todo $i \in \{1, \cdots, k_x\}$ se cumple que $s_i \in S^{n-1}$ por lo tanto $x \in (S^{n-1})^{k_x}$; como hay una cantidad finita se toma el máximo de estos k_x, por ello sea $N = \text{máx}\{k_x | x \in G\}$ entonces $G \subseteq (S^{n-1})^N$; la inclusión $\langle S \rangle \subseteq G$ es trivial, por tanto, existe $N > 0$ tal que $S^N = G$.

Ahora por la Proposición 5.1.3, se tiene que

$$\begin{aligned} \text{supp}(P^{*N}) &= \underbrace{\text{supp}(P) \cdot \ldots \cdot \text{supp}(P)}_{N} \\ &= \underbrace{S \cdot \ldots \cdot S}_{N} \\ &= S^N \\ &= G \end{aligned}$$

por lo tanto el soporte de P^{*N} es G, entonces $P^{*N}(g) > 0$ para todo $g \in G$, con lo que se comprueba la ergodicidad del paseo aleatorio. □

Un resultado importante es el teorema de convergencia para paseos aleatorios en grupos finitos, cuya demostración esta más allá de los propósitos de este trabajo, por eso solo lo mencionaremos.

Teorema 5.2.6. *Sea $(P^{*k})_{k=0}^{\infty}$ un paseo aleatorio ergódico sobre un grupo finito G dirigido por la probabilidad P. Entonces la sucesión (P^{*k}) converge hacia la distribución U.*

Este teorema significa intuitivamente que un paseo aleatorio ergódico sobre un grupo finito G puede usarse para generar elementos aleatoriamente de G.

5.3. Barajado de cartas

En esta sección se hace una breve introducción de la matemática detrás del barajado de cartas visto como un paseo aleatorio sobre el grupo simétrico.

Supóngase que tenemos un mazo de n cartas, la acción de barajar las cartas significa reordenarlas de alguna manera y esto corresponde a la permutación que realiza un elemento del grupo simétrico S_n. Se considera al grupo simétrico actuando sobre las posiciones de las cartas y no de los nombres de ellas.

Por ejemplo, la permutación (3 2 1) corresponde a colocar la carta de arriba en la tercera posición. Este mueve la segunda carta al principio y la tercera a la segunda posición. Las demás cartas se dejan solas. Esto conduce al primer ejemplo de un método de barajar cartas como una paseo aleatorio.

Ejemplo 5.3.1. ("Top-to-random" o "Carta aleatoria")

El "Top-to-random" consiste en tomar la carta de arriba del mazo y colocarla en alguna de las n posiciones de este de forma aleatoria (con todas las posiciones igualmente probables), en donde, colocar la carta superior en la posición superior corresponde a la identidad, por su puesto. Para $i \geq 2$, colocar la carta superior en la i-ésima posición desplaza las posiciones anteriores hasta uno y por lo tanto corresponde al ciclo $(i\ i-1\ \cdots 1)$. De esta forma el *Top-to-random* puede ser modelado como un paseo aleatorio simple sobre S_n inducido por la probabilidad

$$P = \frac{1}{n}\delta_{I_d} + \sum_{i=2}^{n} \frac{1}{n}\delta_{(i\ i-1\ \cdots 1)}$$

en donde, $\frac{1}{n}\delta_{I_d}$ es la probabilidad que la carta de arriba no se haya movido de su posición (cuando $i = 1$), considerando que posee n posibilidades para moverse con todas las cartas igualmente probables y $\frac{1}{n}\delta_{(i\ i-1\ \cdots 1)}$ es la probabilidad de que la primera carta se haya movido a la k-ésima posición en el mazo.

Además, se sabe que las permutaciones (2 1) (cuando $i = 1$) y $(n\ n-1\ \cdots 1)$ (cuando $i = n$) generan a S_n y que $P(Id) = \frac{1}{n} > 0$, por lo tanto, por la Proposición 5.2.5 este paseo

es ergódico, esto significa que después de suficientes *Top-to-random*, el mazo eventualmente estará mezclado, porque la distribución es uniforme y eventualmente se generan todas las posibilidades, así uno de los lugares en donde se encuentre la primera carta será totalmente aleatorio.

El siguiente método de barajado que se considera es el de las transposiciones aleatorias, en donde, Diaconis y Shahshahani fueron los primeros en obtener los tiempos de convergencia para este método, utilizando la teoría de representaciones del grupo simétrico [14]. El modelo funciona de la siguiente manera.

Ejemplo 5.3.2. ("Transposiciones aleatorias")

El *crupier*[(4)] elige al azar con cada una de sus manos una carta de un mazo (puede suceder que ambas manos elijan la misma carta). Luego intercambia las dos cartas (si eligió la misma carta con cada mano, entonces no hace nada, es decir, no la movió). Dadas dos posiciones $i \neq j$, existen dos formas en que el crupier puede elegir este par (ya sea que la mano izquierda elija a i y la mano derecha tome a j, o viceversa) y entonces la probabilidad de realizar la transposición $(i\ j)$ es 2! por la probabilidad de escoger cada una de las cartas $\left(\frac{1}{n}\right)$, es decir, $\frac{2}{n^2}$ ya que ser tomada por una mano o por la otra son eventos independientes.

La probabilidad que el croupier escoja la posición i con ambas manos es de $\frac{1}{n^2}$. Sin embargo, la permutación resultante de las posiciones es la identidad para todo i, por lo que se realiza la permutación de la identidad con probabilidad $\frac{1}{n}$ porque se tiene una para cada i y se tiene n i's con probabilidad $1/n^2$.

Por lo tanto, el barajado de transposiciones aleatorias, es el paseo aleatorio sobre S_n inducido por la probabilidad Q definida como:

$$Q(\sigma) = \begin{cases} \frac{1}{n}, & \text{si } \sigma = Id; \\ \frac{2}{n^2}, & \text{si } \sigma \text{ es una transposición;} \\ 0, & \text{caso contrario ;} \end{cases}$$

Como las transposiciones de dos elementos generan a S_n y $Q(Id) = \frac{1}{n} > 0$, la Proposición 5.2.5 implica que es un paseo aleatorio ergódico y de nuevo este barajado aleatorizará el mazo.

[(4)] El "dealer" o el repartidor.

5.3.1. Barajados por "Riffles"

Nadie realmente baraja un mazo intercambiando una carta al azar o de dos en dos. La reproducción aleatoria más comúnmente utilizada en la práctica son los *riffles*, también conocida como "Cola de Milano"[(5)] o "Barajado a la americana".

En este tipo de barajado, el distribuidor corta el paquete en algún lugar cerca del centro y luego coloca la mitad superior del paquete en su mano derecha y la mitad inferior en su mano izquierda, a continuación, mezcla las cartas de cada paquete, intercalando los dos paquetes. En una mezcla perfecta, el crupier soltaría una carta de cada paquete en alternancia, pero en realidad varias cartas del mismo paquete a menudo se dejan caer a la vez. Un modelo matemático de barajar barajas fue propuesto por Gilbert y Shannon, de forma independiente también fue propuesto por Reeds y se conoce como barajado de "*Gilbert-Shannon-Reeds*".

Se verá como funciona este modelo; supóngase que el mazo tiene n cartas y se lanza una moneda n veces, sea k el número de caras que se han obtenido en los lanzamientos, entonces el *crupier* toma k cartas de la parte superior del mazo y las coloca en la mano derecha y las $n-k$ cartas que quedaron en la parte de abajo las colocá en la mano izquierda.

En lenguaje técnico, esto significa que la posición del corte es asumida por una variable aleatoria binomial en donde la probabilidad de éxito y fracaso es de $\frac{1}{2}$. Entonces, si X es la variable aleatoria que cuenta el número de cartas en la mitad superior de la baraja después del corte, se tiene:

$$\begin{aligned}\text{Prob}[X=k] &= \binom{n}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{n-k}\\ &= \binom{n}{k}\frac{1}{2^k 2^{n-k}}\\ &= \binom{n}{k}\frac{1}{2^n}\end{aligned}$$

Nótese que mientras más cerca este k de $\frac{n}{2}$, es más probable que suceda que $X=k$; este comportamiento puede observarse en el Triángulo de Pascal que contiene todos los coeficientes binomiales y la probabilidad está dada por los coeficientes que se obtienen en la $n+1$-ésima fila por $\frac{1}{2^n}$ y estos coeficientes puede observarse que son mayores en el centro de la fila. Así, este modelo refleja el hecho de que se tiende a cortar el mazo cerca del medio.

Luego de dividir la baraja, el *crupier* deja caer las cartas de la mano izquierda y de la derecha hasta que ambas manos estén vacías, en donde, la probabilidad de dejar caer una carta de una mano dada, es proporcional al número de cartas en esa mano. Por ejemplo, si hay a cartas en la mano derecha y b cartas en la mano izquierda en un momento dado, entonces la probabilidad de dejar caer una carta de la mano derecha es $\frac{a}{(a+b)}$ y la probabilidad

[(5)] El término en inglés es "Dovetail shuffle".

de dejar una carta desde la mano izquierda es $\frac{b}{(a+b)}$. Nótese que este modelo permite la posibilidad que todas las cartas se caigan de la mano izquierda primero, en cuyo caso el ordenamiento de la baraja permanece como estaba antes. Además, si se consideran los caso triviales cuando $k = 0$ o $k = n$ (los casos triviales), realmente no se corta el mazo y el resultado es que las cartas permanecen en su orden original. Se podría argumentar que esto no sucede en la realidad, pero en cualquier caso, la probabilidad de que esto ocurra es aún muy pequeña $\left(\frac{n}{2^n}\right)$ en este modelo.

En este trabajo se describirá la baraja de *Gilbert-Shannon-Reeds* como un paseo aleatorio sobre S_n. La clave para comprender el orden aleatorio es la noción de una secuencia ascendente, que se define a continuación.

Definición 5.3.3. (Secuencias ascendentes).

Una *secuencia ascendente* en una permutación σ de $\{1, \cdots, n\}$, es una subsecuencia consecutiva de las secuencias de las imágenes $\sigma(1), \sigma(2), \cdots, \sigma(n)$ que es creciente y maximal en tamaño.

Para comprender mejor esta definición observése el siguiente ejemplo.

Ejemplo 5.3.4. Sea $\sigma = (1\ 2\ 3)(7\ 4\ 8)(5\ 6) \in S_8$, entonces la secuencia de imágenes es

$$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1, \sigma(4) = 8, \sigma(5) = 6, \sigma(6) = 5, \sigma(7) = 4, \sigma(8) = 7$$

en donde se puede ver las siguientes secuencias ascendentes de σ: $2, 3,$; $1, 8$; 6; 5; y $4, 7$. De esta manera σ tiene cinco secuencias ascendentes y maximales en tamaños porque son las subsecuencias más grandes que pueden tomarse y que a su vez sean crecientes.

Supóngase ahora que realizamos un *riffle* donde la mitad superior de la baraja tiene k cartas. Luego las cartas en las posiciones $1, \cdots, k$ están intercaladas con las cartas en las posiciones $k+1, \cdots, n$, en donde el orden relativo de las cartas se conserva. Por lo tanto, σ que es la permutación resultante de las posiciones cuando aumenta en $1, \cdots, k$ y en $k+1, \cdots, n$, entonces se tiene exactamente dos secuencias ascendentes: $\sigma(1), \cdots, \sigma(k)$ y $\sigma(k+1), \cdots, \sigma(n)$ (excepto en el caso de que la mitad inferior de la baraja se caiga en su totalidad antes de que se caigan las cartas de la mitad superior, en cuyo caso se obtiene la permutación identidad, que tiene una secuencia ascendente) ya que el orden relativo de las cartas se conserva.

Se expone a continuación un ejemplo para explicar mejor lo anteriormente dicho.

Ejemplo 5.3.5. Supóngase que el mazo tiene diez cartas en el siguiente orden (de arriba a abajo) -$A, 2, 3, 4, 5, 6, 7, 8, 9, 10$- y se realiza un *riffle* con con la siguiente distribución:

$$\underbrace{A, 2, 3, 4}_{\text{superior}} \text{ y } \underbrace{5, 6, 7, 8, 9, 10}_{\text{inferior}}$$

Además, se asume que la secuencia de caídas es:

$$\overset{T}{4},\overset{B}{10},\overset{B}{9},\overset{T}{3},\overset{B}{8},\overset{T}{2},\overset{T}{A},\overset{B}{7},\overset{B}{6},\overset{B}{5}$$

donde T significa "arriba" para referirse al paquete superior y B para "abajo" para el paquete inferior[(6)].

De esta manera en el mazo ahora barajado, el orden de las cartas será (de nuevo, de arriba a abajo)

Cartas:	5,	6,	7,	A,	2,	8,	3,	9,	10,	4
Posiciones:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10

Que corresponde a la permutación σ de las posiciones.

Nótese que la carta A inicialmente estaba en la primera posición, después del barajado se encuentra en la cuarta posición, lo mismo sucede para 2 estaba en la segunda posición y ahora se encuentra en la quinta posición y así sucesivamente con las demás cartas. Entonces las imágenes son

Cartas:	A,	2,	3,	4,	5,	6,	7,	8,	9,	10
Posiciones:	4,	5,	7,	10,	1,	2,	3,	6,	8,	9

En donde, las secuencias ascendentes de σ son $4, 5, 7, 10$ y $1, 2, 3, 6, 8, 9$.

De lo anterior se observa que si P es la distribución de probabilidad en S_n que corresponde a una combinación aleatoria de *Gilbert-Shannon-Reeds*, entonces se tiene que $P(\sigma) = 0$, a menos que σ tenga como máximo dos secuencias ascendentes, ya que si solo tiene una, significa que no se ha hecho ningún movimiento a la baraja o que se ha dejado caer la mitad superior primero y luego la otra mitad, además se ha visto hasta ahorita que al ejecutar un *riffle* se puede tener una sola secuencia ascendente o exactamente dos, entonces nunca se podrá dar cero secuencias o más de dos. Solo queda calcular la probabilidad de que se obtenga una permutación σ con dos secuencias ascendentes, así como la probabilidad de obtener la identidad.

Sea k el número de cartas en la mitad superior de la baraja después del corte, nótese que hay n posiciones para colocar estas k cartas y una vez que se eligen estas posiciones, se puede conocer el orden de las cartas, ya que al tener $\underbrace{\_\ \_\ \ldots\ \_}_{n}$ posiciones donde depositar k cartas, una vez elegidas estas posiciones las $n-k$ cartas restantes quedan automáticamente posicionadas en el mazo. Por lo tanto, dado el valor de k se pueden obtener $\binom{n}{k}$ permutaciones.

[(6)] Esta simbología se debe a que en inglés "Top" significa arriba y "Bottom" significa abajo.

Véase que cada una de las permutaciones anteriores son igualmente probables. Supóngase que se fijamos una permutación σ, ¿cuál es su probabilidad? Debe recordarse el modelo con el que se esta trabajando: se define el evento T como las caídas de las cartas que pertenecen al paquete superior, entonces su probabilidad es $\dfrac{a}{(a+b)}$ y definamos el evento B como las caídas de las cartas que pertenecen al paquete inferior, con probabilidad $\dfrac{b}{(a+b)}$ donde a es el número de cartas en el paquete superior y b es el número de cartas en el paquete inferior, de tal forma que a y b pueden variar desde el momento que se realice la primera caída. Entonces, cuando se realiza un corte de k cartas en el paquete superior y $n-k$ cartas en el paquete inferior, la probabilidad de que la secuencia de caídas comience con T es $\dfrac{k}{n}$ y la probabilidad de que la secuencia comience con una B es $\dfrac{(n-k)}{n}$ para la primera.

Observése que el denominador para la probabilidad de la segunda caída se reducirá en 1 y pasará a ser $n-1$ independientemente de si la primera caída es una T o una B y el numerador para el elegido en la primera posición se reducirá en 1 y será $k-1$ o $n-k-1$, dependiendo de si la carta cae del paquete superior o inferior, respectivamente. Esto se repite para cada posición subsiguiente, por lo que los números $n, n-1, n-2, \cdots, 1$ aparecerán en los denominadores lo cual da la idea de que la probabilidad contiene a $n!$ en el denominador y los números $k, k-1, \cdots, 1$ y $n-k, n-k-1, \cdots, 1$ aparecerán en alguno de los numeradores, por lo que $k!$ y $(n-k)!$ aparecerán en el numerador cuando caiga la primera carta del mazo superior y cuando caiga la primera carta del mazo inferior.

Dado que la probabilidad de cualquier secuencia de caídas (por independencia) es el producto de estas probabilidades individuales, en todos los casos la probabilidad buscada es $\dfrac{k!(n-k)!}{n!}$, independientemente de si la secuencia de caídas comienza con el paquete superior o el inferior, con lo que se puede concluir que todas las permutaciones son igualmente probables, porque se ha tomado una permutación arbitraria.

Para hacer esto más concreto, se analizará el siguiente ejemplo.

Ejemplo 5.3.6. Supóngase que hay cinco cartas y que $k=2$. Además dadas dos secuencias de caídas cualquiera, la probabilidad para todos los casos es la misma.

Desarrollo. De acuerdo a lo que se ha discutido en el modelo la probabilidad es

$$\begin{aligned}\frac{k!(n-k)!}{n!} &= \frac{2!(5-2)!}{5!}\\ &= \frac{2!3!}{5!}\\ &= \frac{1}{10}\end{aligned}$$

Ahora se consideran dos secuencias de caídas cualquiera, sabiendo que inicialmente la probabilidad de que una carta este en el paquete superior es de $\frac{2}{5}$ y que este en el paquete inferior es $\frac{3}{5}$:

1. Sea T, B, T, B, B la primera secuencia de caídas.

   De acuerdo al modelo, se tiene que:

   $$\begin{matrix} \text{T}, & \text{B}, & \text{T}, & \text{B}, & \text{B} \\ \frac{2}{5}, & \frac{3}{4}, & \frac{1}{3}, & \frac{2}{2}, & \frac{1}{1} \end{matrix}$$

   por independencia se multiplican las probabilidades y se tiene que

   $$\left(\frac{2}{5}\right)\left(\frac{3}{4}\right)\left(\frac{1}{3}\right)(1)(1) = \frac{1}{10}$$

2. Como un segundo ejemplo, véase la secuencia B, T, B, T, B

   De acuerdo al modelo, se tiene que:

   $$\begin{matrix} \text{B}, & \text{T}, & \text{B}, & \text{T}, & \text{B} \\ \frac{3}{5}, & \frac{2}{4}, & \frac{2}{3}, & \frac{1}{2}, & \frac{1}{1} \end{matrix}$$

   en donde su probabilidad sería:

   $$\left(\frac{3}{5}\right)\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{1}{2}\right)(1) = \frac{1}{10}$$

Como vemos en el ejemplo dadas dos secuencias de caídas distintas se obtiene el mismo resultado. □

En resumen, la probabilidad de obtener una permutación σ, la cual se obtiene cuando la posición del corte es k, es

$$\frac{k!(n-k)!}{n!} = \frac{1}{\binom{n}{k}} \tag{5.9}$$

Exactamente una de estas permutaciones será la identidad. Las demás tendrán dos sucesiones ascendentes: una de longitud k, seguida por una de longitud $n-k$. La probabilidad de tener k cartas en la mitad superior es $\binom{n}{k} \cdot \frac{1}{2^n}$, se sigue que si $1 \leq k \leq n-1$ y si σ es una

permutación con dos sucesiones ascendientes $\sigma(1), \cdots, \sigma(k)$ y $\sigma(k+1), \cdots, \sigma(n)$, entonces la probabilidad de obtener σ en un solo *riffle* es:

$$\binom{n}{k} \cdot \frac{1}{2^n} \cdot \frac{1}{\binom{n}{k}} = \frac{1}{2^n}$$

Por otro lado, para cualquier k entre 1 y $n-1$, la probabilidad de obtener la permutación identidad es también $\frac{1}{2^n}$, porque simbolizaría que se dejan caer todas las cartas del mazo inferior primero y luego las del mazo superior, con cada carta equiprobable y este calculo es el mismo que se ha realizado anteriormente.

Ahora, si se deja que k varíe de 0 a n, la probabilidad de no barajar el mazo, es decir, cuando se dejan caer las cartas del paquete inferior primero y luego las del paquete superior (ya que así caerían en el mismo orden), para cada k se tiene

$$\begin{array}{cccccc} k=0, & k=1, & \cdots, & k=n-1, & k=n \\ \frac{1}{2^n}, & \frac{1}{2^n}, & \cdots, & \frac{1}{2^n}, & \frac{1}{2^n} \end{array}$$

Sumando las probabilidades por cada uno de los casos, se concluye que la probabilidad de obtener la permutación de la identidad es $\frac{(n+1)}{2^n}$.

Por lo tanto, se tiene el siguiente modelo del barajado de *Gilbert-Shannon-Reeds* como un paseo aleatorio sobre S_n.

Proposición 5.3.7. *El barajado de Gilbert-Shannon-Reeds corresponde a un paseo aleatorio sobre S_n inducido por la distribución de probabilidad P definida por*

$$P(\sigma) = \begin{cases} \frac{(n+1)}{2^n}, & \text{si } \sigma = I; \\ \frac{1}{2^n}, & \text{si } \sigma \text{ tiene exactamente dos sucesiones ascendentes}; \\ 0, & \text{caso contrario}\ ; \end{cases}$$

Observése que la permutación $\sigma = (1\ 2)$ corresponde a la acción de cortar el mazo en la carta superior y soltar todas las cartas excepto una de la mitad inferior primero, en donde las imágenes son $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$, $\sigma(4) = 4$, $\cdots$, $\sigma(n) = n$, entonces las secuencias de imágenes son (2) y $(1\ 3\ \cdots\ n)$. Por otro lado, la permutación $\sigma' = (1\ 2\ \cdots\ n)$ que corresponde a la acción de cortar el mazo en la última carta y dejar caer primero la mitad superior completa, tiene como imágenes a $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 5$,

$\cdots$, $\sigma(n) = 1$, en donde, las secuencias de imágenes son $(2\ 3\ \cdots\ n)$ y (1). Con lo anterior se puede concluir que las permutaciones $(1\ 2)$ y $(1\ 2\ \cdots\ n)$ tienen exactamente dos secuencias de caídas.

De lo anterior se puede concluir que $(1\ 2)$ y $(1\ 2\ \cdots\ n)$ generan al grupo, además se encontró que $P(Id) > 0$, por lo tanto por la Proposición 5.2.5 el paseo aleatorio asociado con el modelo de *Gilbert-Shannon-Reeds* es ergódico, lo que permite a afirmar que ¡la repetición aleatoria de *rifles* aleatorizará el mazo!

Conclusiones

Con este trabajo se concluye que:

1. El desarrollo de la Teoría de Caracteres y las relaciones de ortogonalidad, fueron elementos que ayudaron a comprender el Análisis de Fourier en grupos Finitos, debido a los alcances que tiene el Producto Convolución en el estudio de la Probabilidad y los Paseos Aleatorios sobre grupos finitos.

2. El vínculo entre la Probabilidad y la Teoría de Representaciones de Grupos Finitos se establece cuando se demuestra que una función de probabilidad P pertenece al Álgebra de Grupo $L(G)$, lo cuál permitió establecer una interpretación estadística bastante natural para la convolución de probabilidades.

3. Aplicar la Teoría de Representaciones de Grupos Finitos al estudio de los barajados de cartas, permitió modelar la probabilidad que una carta se encuentre en una posición aleatoria en el mazo, esto se hizo por medio de varios modelos como el *Top-to-random*, las Transposiciones Aleatorias y el modelo de *Gilbert-Shannon-Reeds*, siendo este último un modelo más cercano a la realidad en el juego de cartas.

Por último se espera que este trabajo sirva como herramienta en el estudio de la Teoría de Representaciones de Grupos Finitos y que pueda motivar a otras personas en la facultad Ciencias Naturales y Matemática de la Universidad de El Salvador, a continuar con la investigación de las aplicaciones de este tópico en otras áreas de la ciencia.

Bibliografía

[1] Steinberg B., *Representation Theory of Finite Groups, an Introductory Aproach*, 1st Edition. Springer Universitext. Canada. 2012.

[2] Burrow M., *Representation Theory of Finite Groups*, 1st Edition. Academic Press, New York. 1965.

[3] Lam T. Y., *Representations of Finite Groups: A Hundred Years*, Part I. American Mathematical Society (AMS). United States. 1998.

[4] Lam T. Y., *Representations of Finite Groups: A Hundred Years*, Part II. American Mathematical Society (AMS). United States. 1998.

[5] Curstis C. W, *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer History of Mathematics*, (Book 15). American Mathematical Society, London Mathematical Society. United States. 2000.

[6] Pietrásheñ M. I., Trífonov Ie. D., *Teoría de grupos. Aplicación a la Mecánica Cuántica.*, 3ra Edición. Editorial URSS, Moscú, 2000.

[7] F. Albert Cotton, *Chemical Applications of Group Theory.*, 3rd Edition. A Wiley-Intersciencie Publication, New York. 1990.

[8] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras.*, Wiley Classics Library. John Wiley Sons Inc., New York, 1988 (Reprint of the 1962 original, A Wiley-Interscience Publication.)

[9] Vidal Guzmán R. M., *Anillo de representación de los grupos de Lie*, (tesis). Universidad Nacional del Callao, Facultad de Ciencias Naturales y Matemática. Lima, Perú. 2010.

[10] Facultad de Química, UNAM, *Teoría de Grupos Aplicada a la simetría molecular*, [en línea]. Dirección URL: <http://www3.uah.es/edejesus/resumenes/DECI/tema$_1$.*pdf*¿.[*Consulta* : 19*diciembre*2017].

[11] Ernesto de Jesús Alcañiz, Universidad de Alcalá, *Teoría de Grupos Aplicada a la simetría*, [en línea]. Dirección URL:<http://www.uah.es/edejesus/resumenes/DECI/tema_1.pdf>. [Consulta: 20 diciembre 2017].

[12] CharlesW. Curtis, *Linear algebra. Undergraduate Texts inMathematics.*, 4ta Edición. Springer-Verlag. An introductory approach, NewYork, 1993.

[13] John B. Fraleigh., *A first course in abstract algebra.*, 7th edition. Addison-Wesley Publishing Co., Mass.-London-Don Mills, Ont., 2002.

[14] Persi Diaconis and Mehrdad Shahshahani., *Generating a random permutation with random transpositions.*, Zeitschrift fÜr Wahrscheinlichkeitstheorie und Verwandte Gebiete, 57(2):159179, 1981.

[15] Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli., *Harmonic analysis on finite groups. Representation theory, Gelfand pairs and Markov chains.*, volume 108 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2008.

[16] Dave Bayer and Persi Diaconis., *Trailing the dovetail shuffle to its lair. The Annals of Applied Probability*, 2(2):294313, 1992.