Acciones de grupo y aplicaciones en la teoría de Galois y Teoría de representaciones

Leonel Enrique Contreras Quirós

UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ciencias y Humanidades

Acciones de grupo y aplicaciones en la teoría de Galois y Teoría de representaciones

Trabajo de graduación en modalidad de Tesis presentado por
Leonel Enrique Contreras Quirós
para optar al grado académico de Licenciado en Matemática Aplicada

Guatemala,

2024

UNIVERSIDAD DEL VALLE DE GUATEMALA
Facultad de Ciencias y Humanidades

Acciones de grupo y aplicaciones en la teoría de Galois y Teoría de representaciones

Trabajo de graduación en modalidad de Tesis presentado por
Leonel Enrique Contreras Quirós
para optar al grado académico de Licenciado en Matemática Aplicada

Guatemala,

2024

Vo.Bo.:

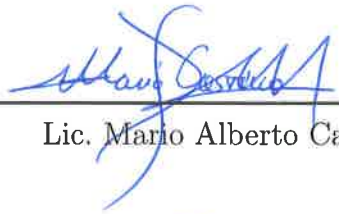
(f) 

Lic. Monica Lucía Cabria Zambrano

Tribunal Examinador:

(f) 

Lic. Monica Lucía Cabria Zambrano

(f) 

Lic. Mario Alberto Castillo

(f) 

Lic. Juan Fernando Valdés Cruz

Fecha de aprobación: Guatemala, 21 de junio 2024.

Prefacio y agradecimientos

En el presente trabajo de tesis, se aborda un tema fascinante en la teoría de grupos como lo son las acciones de grupo. La teoría de grupos aparece como una disciplina distinta en toda la matemática moderna e impregna los más variados ámbitos como principio ordenador y clasificador. Éstas son un concepto fundamental en las matemáticas ya que son la manera en que los matemáticos modernos utilizan la teoría de grupos. Por ejemplo, un geómetra está interesado en la acción de los grupos de traslaciones, reflexiones y rotaciones en el espacio, en la teoría de representaciones de grupos de grupos nos interesa la acción de un grupo sobre un espacio vectorial para estudiar la simetría en un espacio lineal, en la teoría de grafos nos interesa la acción de un grupo sobre un grafo.

En esta tesis estaremos interesados en la acción de un grupo sobre un conjunto, para la reformulación de varios teoremas aprendidos en el curso de álgebra moderna. De igual manera, para mostrar la relevancia de las acciones de grupo mostraremos cómo se utilizan las acciones de grupo en la teoría de Galois. Asimismo, veremos cómo las acciones de grupos sobre espacios vectoriales nos introducen al mundo de la teoría de representaciones de grupos; el cual es un tema activo e importante de investigación debido a su vinculación con el famoso programa de Langlands, el cual ha sido una pieza clave para la prueba del último teorema de Fermat, ya que Andrew Wiles utiliza una conjetura que es parte de dicho programa para probar el último teorema de Fermat, y ha conjeturado muchas conexiones interesantes en diversas ramas de la matemática.

A mi familia y profesores.

Índice

Lista de figuras

Resumen

Este trabajo se enfoca en las acciones de grupo como una nueva metodología para impartir la teoría elemental de grupos en la UVG. Se introduce el concepto de acción de grupo sobre un conjunto, los conceptos de órbitas y estabilizadores y se demuestra el principio fundamental de conteo; el cual nos provee una relación entre el orden del grupo que realiza la acción, la cardinalidad de la órbita de un elemento del conjunto en el que sea actúa y el orden del estabilizador del mismo.

Se prueba el teorema de Lagrange considerando la acción por multiplicación izquierda de un grupo finito sobre el conjunto de todas las clases laterales izquierdas de un subgrupo dado. Asimismo, consideramos la acción por conjugación de un grupo sobre sí mismo y cómo esta acción, junto con el principio fundamental de conteo, nos permite derivar la ecuación de clases, la cual nos indica que el orden del grupo que realiza la acción es igual al orden del centro del grupo más los órdenes de ciertas clases conjugadas.

Por otro lado, se prueban los primeros dos Teoremas de Sylow. El primer teorema de Sylow nos permite garantizar la existencia de subgrupos de ciertos tamaños, en otras palabras, es un seudo-converso del teorema de Lagrange. Para la prueba del primer teorema de Sylow, consideramos la acción por multiplicación izquierda de un grupo G sobre el conjunto de todos los subconjuntos de una cardinalidad específica. Mientras que el segundo teorema de Sylow nos indica que cualquier p-subgrupo, denotado por Q, es subgrupo de un conjugado de un p-subgrupo de Sylow, denotado por P. Para esta prueba consideramos la acción de Q por multiplicación izquierda en el conjunto de todas las clases laterales izquierdas de P. Como último resultado de la teoría elemental de grupos, probamos el teorema de Burnside. Dicho teorema nos permite contar la cantidad de órbitas que se producen al tener una acción de un grupo en un conjunto. Ya que las órbitas de la acción particionan el conjunto X, nos permite hallar la cardinalidad del conjunto cociente X/G.

Finalmente, para justificar dicho cambio de metodología en la impartición del curso de teoría de grupos, mostramos mediante dos ejemplos cómo las acciones de grupos son un tema recurrente en la matemática. Primero, mostramos que las acciones de grupo aparecen en la teoría de Galois ya que el grupo de Galois de un polinomio actúa sobre las raíces del mismo. Esta acción la utilizaremos para probar el conocido teorema que nos indica que si un número complejo es raíz de un polinomio sobre los reales, entonces su conjugado complejo también lo es. El segundo ejemplo proviene de la teoría de representaciones de grupos finitos. Para ello, consideramos la acción de un grupo finito sobre un espacio vectorial unitario finito dimensional; esto nos permite concebir los elementos del grupo como operadores del espacio y desarrollar así parte de la teoría de representaciones de grupos.

CAPÍTULO 1

Introducción: Historia de la teoría de Grupos, teoría de Galois y teoría de representaciones de grupos

Primeramente, debemos notar que la historia de los temas pertinentes a esta tesis, la teoría de grupos, teoría de Galois y representaciones de grupo, no son tres sucesos aislados en la historia. Mas bien, son un solo hilo temporal en el cual avances en una rama conduce eventualmente a avances en las otras dos. Nuestra historia empieza en los textos babilónicos alrededor del año 1770 antes de Cristo, en los cuales se encuentran los primeros registros de intentos para resolver ecuaciones cuadráticas. Por ejemplo, en el museo británico, se encuentra la tableta de arcilla con número de inventario BM 34568 en la cual se propone el problema de encontrar un rectángulo cuya longitud y altura sumadas sean 14 unidades y cuya área sea 18 unidades (Bewersdorff, 2021). Se conjetura que los argumentos que empleaban para la solución de dichos problemas eran argumentos geométricos.

Posteriormente, el matemático indio Brahmagupta (598-668), en su texto Brāhmasphutasiddhánta, lo cual se traduce a perfeccionando la técnica de Brahma, emplea técnicas algebraicas para la solución de ecuaciones cuadráticas. Sin embargo, sus cálculos aritméticos y algebraicos eran sucintos y sin prueba (Bewersdorff, 2021). Luego el matemático y astrónomo iraquí Muhammad ibn Mūsā al-Khwārizmī, escribe un compendio sobre la completación y balanceo como métodos para resolver polinomios. El término álgebra que utilizamos hoy para denotar esta bella rama de la matemática se debe a una mala traducción al latín de su trabajo Algoritmi de numero Indorum, lo cual se traduciría a Al-Khwārizmī sobre los números indios (Bewersdorff, 2021). Al-Khwārizmī describe las reglas de aumento y balanceo para resolver problemas de herencias, comercio, cálculos geométricos y la construcción de canales; de igual manera, sus argumentos son geométricos, pero utiliza técnicas algebraicas para transformar una ecuación polinómica a una de las seis categorías de ecuaciones que desarrolla a lo largo de su texto.

Para los primeros registros de la solución de polinomios cúbicos debemos remontarnos aproximadamente a los años 1048-1131, donde el matemático persa Omar Khayyam en su texto Maqāla fi l-jabr wa l-muqābala, cuya traducción es: Sobre cómo tratar el álgebra de aumento y el equilibrio, calcula, a partir de construcciones geométricas, soluciones numéricas a ecuaciones cúbicas (Bewersdorff, 2021). Al igual que sus predecesores, únicamente considera coeficientes positivos y en su texto desarrolla técnicas para encontrar soluciones a un total de 25 casos particulares de ecuaciones cúbicas. Después de siglos sin un progreso fundamental en el álgebra, en el siglo XVI, Scipione del Ferro, quien fue catedrático en la universidad de Bologna, es el primero en poder resolver ecuaciones cúbicas del tipo $x^3 + px = q$ (Bewersdorff, 2021). Ferro comparte el método de solución a su alumno Antonio Fior. Al mismo tiempo, Niccolò Tartaglia también se encontraba estudiando las ecuaciones

cúbicas; él crea un procedimiento mediante el cual se producen ecuaciones especiales que permiten encontrar fácilmente soluciones para ecuaciones del tipo $x^3 + px^2 = q$ (Bewersdorff, 2021). Dichas técnicas se mantenían secretas ya que, en esa época, se realizaban duelos matemáticos en los cuales cada rival proponía 30 ejercicios a resolver al otro. El ganador era la persona que lograba resolver la mayor cantidad de ejercicios en un plazo determinado.

Al principio de 1535, Fior y Tartaglia tienen uno de los mencionados duelos, en los cuales resulta vencedor Tartaglia. Posterior a su victoria, es contactado por el físico y matemático Gerolamo Cardano, quien quería publicar el descubrimiento de Tartaglia en un texto sobre álgebra en el cual estaba trabajando (Bewersdorff, 2021). El texto en el cual Caradano estaba trabajando era su revolucionario Ars Magna; el cual es el primer texto en el que se consideran soluciones negativas a ecuaciones polinómicas -las cuales Cardano denota como debitum, i.e., deuda- y la primera vez en la historia en la que se consideran soluciones complejas -las cuales Cardano denota como soluciones ficta, i.e., falsas- (Bewersdorff, 2021). Cardano propone reglas tentativas para realizar cálculos con dichos números. Sin embargo, tomaría siglos para que los matemáticos aceptaran y axiomatizaran los números complejos.

A pesar de lo innovador que resulta el texto de Cardano, vemos que los matemáticos de su época siguen limitados por un pensamiento geométrico. Cardano menciona en el prefacio de su libro que las ecuaciones lineales se asocian con una recta, las cuadráticas con una superficie y las cúbicas con un volumen; sería absurdo tratar de extrapolar ya que la naturaleza no lo permite (Bewersdorff, 2021). Sin embargo, su estudiante Ludovico Ferrari logra transformar ecuaciones de la forma tipo $x^4 + px^2 + qx + r = 0$, al añadir dos términos en las potencias de x y x^2 de manera que se obtiene un cuadrado perfecto en ambos lados de la ecuación; permitiendo así encontrar soluciones a dicho tipo de ecuación (Bewersdorff, 2021). Una limitación al método de Ferrari es que se puede utilizar únicamente en los casos donde no ocurre el término x^3.

Dados los resultados previos, los matemáticos querían extender los métodos para resolver polinomios de grado 5 en adelante. En 1615 es publicado póstumamente el tratado De aequatoinnum recognitione et emendatione Tractatus duo, lo cual se traduce a Tratado 2do. sobre la revisión y enmienda de la ecuación, cuya autoría se debe a François Viète. En sendo trabajo, Viéte se interesa en el estudio de ciertas transformaciones a polinomios que no cambian las raíces de este. Él encuentra una manera de construir polinomios que poseen tales números $x_1, ..., x_n$ como soluciones (Bewersdorff, 2021). Consecutivamente, en 1637 René Descartes publica La Géométrie. En este texto, Descartes propone una construcción para obtener un polinomio con $x_1, ..., x_n$ soluciones dadas:el polinomio $(x - x_1)...(x - x_n)$. Asimismo, Descartes investiga cuándo un polinomio admite una factorización en términos lineales y determina que una ecuación polinómica de grado

En 1761 Euler presenta una prueba al Famoso teorema de Fermat sobre congruencias. Dicho método es el mismo que posteriormente utiliza Langrange para probar el teorema que lleva su nombre; el cual indica que el orden de todo subgrupo de un grupo finito divide el orden del grupo (der Waerden, 2013). Esto nos provee unos de los primeros indicios de lo que posteriormente se formalizaría en la teoría de grupos. Luego, entre 1770 y 1771, en su artículo Réflexions sur la résolution algébrique des équations, Lagrange hace un estudio sistemático de varios de los métodos conocidos para la resolución de polinomios cúbicos y cuárticos, éstos incluían métodos propuestos por Viète, Descartes, Euler y Bezout (Kleiner, 1986). En dicho trabajo, Lagrange estudia los polinomios simétricos elementales y se propone encontrar una solución algebraica a la quíntica. La característica que comparten todos estos métodos es la reducción a ecuaciones auxiliares, llamadas resolventes, las cuales tienen un grado menor que la ecuación dada. Dicho trabajo es una piedra angular para la teoría de grupos ya que es la primera vez que se asocian los conceptos de las soluciones de una ecuación polinómica y las permutaciones de las raíces. Lagrange especulaba que dichas conexiones forman "los verdaderos principios para la solución de ecuaciones" (Kleiner, 1986). En 1799 Ruffini empieza a publicar su trabajo sobre la imposibilidad de encontrar una solución por radicales a polinomios de quinto grado (Bewersdorff, 2021). La prueba completa de dicha imposibilidad sería dada por Niels Henrick Abel, en honor a quién se nombró el premio Abel, y tendría que esperar

hasta 1826 (Bewersdorff, 2021).

Posteriormente, en 1801 Gauss publica su Famoso Disquisitiones Arithmeticae; algunos autores consideran este texto como el inicio del estudio de los grupos abelianos finitos (Kleiner, 1986). Gauss se enfoca en los siguientes cuatro ejemplos de grupo: el grupo aditivo de los enteros modulo m, el grupo multiplicativo de los enteros módulo m, i.e., los primos relativos de m bajo el producto, el grupo de las clases de equivalencia de las formas binarias cuadráticas y el grupo de la n-ésima raíz de la unidad. Gauss establece muchas propiedades de dichos grupos sin utilizar la terminología de la teoría de grupos y considera cada uno de los grupos mencionados como casos aislados, sin una teoría que los unifique como distintas manifestaciones de un mismo concepto. El siguiente personaje relevante para el desarrollo de la teoría de grupos es Evariste Galois. El trabajo de Galois fue escrito alrededor de 1830 y publicado después de su muerte en 1846 por Liouville (Kleiner, 1986). Galois estaba interesado en los principios generales en la solución de polinomios. Él mismo distinguía la diferencia entre la teoría de Galois, la cual indica una correspondencia entre grupos y campos, y su aplicación a la solución de ecuaciones. Indicando que los primeros eran los principios generales mientras que los segundos solo eran aplicaciones de dichos principios. Galois reconoce que las propiedades importantes de una ecuación algebraica se ven reflejadas en el "grupo de la ecuación" el cual está asociado de manera única con dicho polinomio; para describir estas propiedades, crea el concepto de subgrupo normal. Galois aprovecha el concepto de subgrupo normal notando que la existencia de un resolvente es equivalente a la existencia de un subgrupo normal de índice primo. Galois procede a demostrar la existencia de dicho grupo de la ecuación y a investigar cómo cambia dicho grupo bajo las extensiones de campo al agregar elementos a un campo dado.

En 1844 Cauchy da el primer desarrollo sistemático de la teoría de permutaciones y define el concepto de un grupo generado por ciertos elementos (Kleiner, 1986). Cauchy aporta mucha de la notación actual utilizada, por ejemplo, la notación cíclica para permutaciones. Asimismo, introduce conceptos nuevos y relevantes para la teoría de grupos, como el de centralizador de un elemento el conjunto de elementos del grupo que conmutan con un elemento particular. De igual manera, Cauchy aporta muchos resultados concretos al desarrollo de la teoría como el famoso "teorema de Cauchy" que indica que, si un primo p divide el orden del grupo, entonces el grupo tiene un elemento de orden p. En 1870, Camille Jordan publica su Traité des substitutions et des équations álgebriques, en el cual unifica los resultados previos dados por Cauchy, Galois y otros. Dicho tratado es un estudio de todas las aplicaciones de la teoría de grupos de permutación en las diversas ramas de las matemáticas de su época. Jordan recopila ejemplos del uso de grupos de permutaciones en la geometría algebraica, la teoría de números y la teoría de funciones. En dicho tratado, Jordan introduce el concepto de grupo soluble, serie de composición y prueba una parte del teorema de Jordan-Hölder. El toerema indica que los índices en dos series de composición son los mismos. En este mismo año, Kronecker desarrolla los axiomas para grupos abelianos finitos y prueba una parte del teorema fundamental de los grupos abelianos finitos, este teorema indica que grupo abeliano finito es el producto directo de grupos cíclicos cuyos órdenes son potencias de primos (der Waerden, 2013). La unicidad de los factores fué probada hasta 1879 por Frobenius y Stickelberger (der Waerden, 2013).

En 1871, Felix Klein y Sophus Lie publican un artículo conjunto sobre los grupos de transformaciones lineales. Dichos grupos son grupos continuos unidimensionales, lo que hoy conocemos por grupos de Lie (der Waerden, 2013). Sophus Lie utiliza esta teoría para el estudio de ecuaciones diferenciales y pretende formular una "Teoría de Galois para ecuaciones diferenciales" (Kleiner, 1986). El trabajo de Frobenius y Lie marca un cambio de grupos de permutación a grupos de transformación, cambiando así el interés de grupos finitos a grupos infinitos. Klein señaló que en la teoría de Galois se trata de un número finito de elementos discretos, mientras que en su obra se trata de un número infinito de elementos de una variedad continua (Kleiner, 1986). Un año después, en 1872 Feliz Klein propone su famoso programa de Erlangen, el cual pretendía clasificar la geometría como el estudio de invariantes bajo varios grupos de transformaciones. Algunos de éstos son el grupo proyectivo, el grupo de movimientos rígidos, el grupo de similaridades. Éstos son los primeros pasos en la dirección de la teoría que propondrían ulteriormente E. Picard y E. Vessiot. Como el propio Klein destacaría, la teoría de grupos aparece como una disciplina distinta en toda la matemática moderna. Impregna

los más variados ámbitos como principio ordenador y clasificador](Kleiner, 1986). En su trabajo de las décadas de 1870 y 1880, Klein utilizó matrices para realizar grupos específicos, lo cual podría sugerir un inicio en el estudio de la teoría de representaciones de grupos. Sin embargo, no existía indicio alguno del desarrollo de una teoría (Lam, 1998).

En el mismo año 1872 el matemático noruego Sylow presenta los famosos teoremas de Sylow que nos permiten entender la estructura de los grupos finitos (der Waerden, 2013). Dichas pruebas son publicadas en su quinto volumen de Mathematische Annalen (Lam, 1998).

La historia de la teoría de representaciones de grupos inicia en1896. Frobenius escribe una carta a R. Dedekind en la cual el describe sus conceptos nuevos para realizar la factorización de cierto polinomio homogéneo asociado a un grupo finito, llamado el "determinante del grupo" (Lam, 1998). Al final de dicho año, Frobenius había sentado ya las bases de la teoría de carácteres para grupos finitos (Lam, 1998). Tendríamos que esperar hasta 1879 para que apareciera la primera definición de un carácter abeliano; esta definición sería dada por Richard Dedekind como un homomorfismo de un grupo abeliano G al grupo multiplicativo de los complejos $\mathbb{C}^*$ (Lam, 1998).

En 1897, Burnside publica su clásico e influyente texto Theory of Groups of Finite Order, en el cual presenta la teoría de manera abstracta sin incluir aplicaciones (Etingof, 2011). A los pocos meses, Burnside lee los artículos de Frobenius respecto a la teoría de caracteres y deriva todos los resultados de Frobenius sobre la teoría de carácteres y el determinante de un grupo utilizando métodos de la teoría de grupos de Lie y álgebras de Lie. (Etingof, 2011). Esto incita a una competencia entre Burnside y Frobenius para determinar la solubilidad de los grupos $p^\alpha q^\beta$ (Etingof, 2011). La prueba del caso general sería dada por el mismo Burnside en 1904.

A lo largo de esta breve introducción histórica, podemos apreciar que la estructura de grupo y las acciones de grupo han permeado y motivado, la investigación y progreso de esta bella disciplina que nos apasiona. Dicha estructura matemática nos provee una herramienta tan poderosa y ubicua que el matemático Henri Poincaré destacaría que todas las matemáticas son un cuento sobre grupos y Émile Picard escribió en una carta a Sophus Lie que Paris se estaba convirtiendo en un centro para el estudio de la teoría de grupos (Etingof, 2011). Por ende, motivados por las palabras de Poincaré y Frobenius, indicando que la teoría de grupos es un principio ordenador y clasificador, esta tesis investiga la omnipresencia y aplicaciones prácticas de la teoría de grupos, destacando su papel crucial en diversas disciplinas matemáticas y la aplicación de las acciones de grupo en las mismas.

CAPÍTULO 2

Objetivos

2.1. Objetivo general

Presentar la teoría elemental de grupos mediante el uso de acciones de grupo y mostrar que diversas ideas aparentemente distintas, son manifestaciones de este concepto. Presentar dos ejemplos del uso de las acciones de grupo en distintas ramas de las matemáticas, como lo son la Teoría de Galois y la teoría de representaciones de grupos finitos.

2.2. Objetivos específicos

1. Definir la acción de un grupo en un conjunto y los conceptos de órbita de un elemento del conjunto y estabilizador de este. Probar el principio fundamental de conteo, el cual nos relaciona el tamaño de las órbitas con el tamaño de los estabilizadores y el orden del grupo que realiza la acción. A partir de estos conceptos probar los siguientes teoremas como casos particulares de acciones de grupo:

   - Teorema de Lagrange
   - Ecuación de clases
   - Primer y segundo teorema de Sylow
   - Teorema de Cauchy
   - Teorema de Burnside

2. Probar que el grupo de Galois de un polinomio actúa sobre las raíces del mismo y probar, mediante la acción del grupo de Galois sobre las raíces de un polinomio, el conocido resultado que indica que, si un número complejo es raíz de un polinomio sobre los reales, entonces su conjugado complejo también es una raíz de dicho polinomio.

3. Introducir el concepto de representación de un grupo y su relación con la acción de un grupo sobre un espacio vectorial. Probar el teorema de Maschke, el cual nos indica que toda representación finito dimensional compleja de un grupo G es la suma de representaciones irreducibles.

CAPÍTULO 3

Justificación

Esta tesis pretende dar un esquema de cómo caracterizar los teoremas fundamentales de la teoría de grupos mediante acciones de grupo para posteriormente poder enseñar la teoría de grupos a estudiantes universitarios a través de este concepto tan importante. De igual manera, se pretende mostrar cómo el concepto de acción de grupo permite al estudiante introducirse en la teoría de Galois y la teoría de representaciones de grupos finitos.

CAPÍTULO 4

Acciones de grupo

4.1. ¿Qué es una acción de grupo?

Consideremos un cuadrado con sus esquinas numeradas de la manera siguiente:

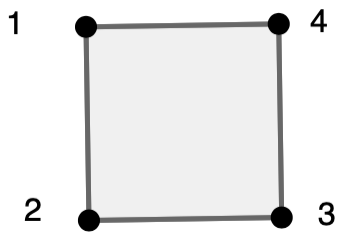
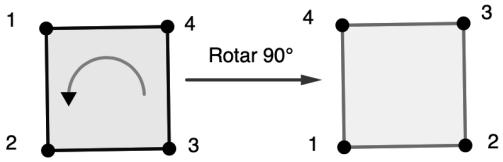
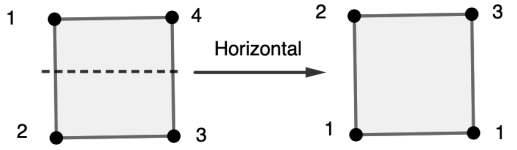


Figura 4.1: Cuadrado con sus esquinas enumeradas

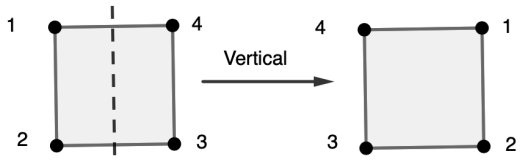
A este cuadrado le podemos aplicar una serie de transformaciones. Podemos realizar una rotación de 90° en contra de las agujas del reloj, lo podemos rotar respecto a su eje horizontal, así como lo podemos rotar respecto a su eje vertical o respecto a una de sus diagonales. Por último, podemos aplicarle la transformación nula o identidad, la cual deja el cuadrado con todas sus esquinas en la misma posición. A continuación, describimos algunas de dichas transformaciones.



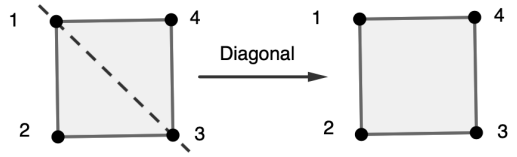
(a) Rotación del cuadrado en 90°



(b) Rotación del cuadrado respecto a la horizontal



(c) Rotación del cuadrado respecto a la vertical.



(d) Rotación del cuadrado respecto a una de sus diagonales

Figura 4.2: Distintas transformaciones del cuadrado

Ahora bien, al cuadrado podemos aplicarle dichas transformaciones de manera sucesiva. Por ejemplo, podemos primero rotarlo 90° en contra de las agujas del reloj y posteriormente rotarlo respecto a su horizontal. Sin embargo, esto es equivalente a rotarlo respecto a la diagonal que pasa por las esquinas enumeradas por 1 y 3. Es decir, podemos aplicar dos transformaciones sucesivamente u operar primero dichas transformaciones y después aplicarle dicho producto al cuadrado.

Es decir, este conjunto de transformaciones sobre el cuadrado satisface las siguientes dos propiedades:

1. Existe una transformación nula que deja al cuadrado invariante
2. Dadas dos transformaciones, podemos aplicarlas sucesivamente, lo cual significa aplicar la primera transformación y al resultado, aplicarle la segunda transformación.

En la siguiente sección formalizaremos en el concepto de acción de un grupo sobre un conjunto. En este caso, es la acción del grupo de transformaciones sobre las esquinas del cuadrado sobre el conjunto de dichas esquinas.

4.2. Axiomas de una acción de grupo

De la manera más general posible, una acción de un grupo sobre un conjunto es un homorfismo del grupo hacia el conjunto de todos los mapeos que preservan la estructura del conjunto en el que se actúa. Es decir, una acción de G en X es un homomorfismo del grupo G a $End(X)$. Dependiendo de qué estructura tenga el conjunto X, varía la estructura de $End(X)$.

Por ejemplo, si el grupo G actúa sobre un conjunto finito, $End(X)$ es simplemente el conjunto de permutaciones de X, ya que al ser X conjunto, no tiene ninguna estructura adicional y lo único que se debe preservar es la cardinalidad del mismo. Por otro lado, si el grupo G actúa sobre un espacio vectorial $V, Hom(V, V)$ es el espacio de operadores. Aquí los morfismos entre espacios vectoriales son las transformaciones lineales. Si G actúa sobre un espacio topológico, la acción de grupo sería un homorfismo de G hacia el conjunto de todos los homeomorfismos del espacio topológico.

En esta sección, formalizamos el concepto de axión de grupo como una terna (G, X, $*$), donde G es un grupo, X un conjunto y $* : G \times X \to X$ es una operación a la cual se le imponen dos axiomas. Introducimos dos ejemplos, la acción del grupo dihedral de orden 8 sobre las esquinas de un cuadrado y la acción del grupo dihedral de orden 6 sobre el hexágono.

Definición 4.2.1. *Para definir la acción de un grupo sobre un conjunto, requerimos de tres objetos:*

1. *Un grupo* $(G, \cdot)$,
2. *Un conjunto* X,
3. *Una operación* $* : G \times X \to X$.

A la operación se le imponen dos axiomas:

- ***Identidad:*** $\forall x \in X, e * x = x$,
- ***Asociatividad:*** $\forall g, h \in G, \forall x \in X, g * (h * x) = (g \cdot h) * x$.

La primera restricción de la acción del grupo indica que la acción del elemento identidad deja invariante a todos los elementos del conjunto. Mientras que la segunda restricción, nos propone que podemos aplicarle al elemento del conjunto, primero la acción de h y después la acción de g o equivalentemente, primero realizar el producto en el grupo y después aplicarle la acción de este producto al elemento del conjunto.

Ejemplo 4.2.1. *Ya que hemos dado los axiomas que debe satisface una acción de un grupo sobre un conjunto, formalizamos el ejemplo visto en la sección previa del cuadrado 4.1. Si consideramos el grupo dihedral de grado 8* $D_8 \coloneqq \langle a, b \mid a^4 = b^2 = e, ba = a^3b \rangle$*; el cual está generado por los elementos a y b. Es decir, todo elemento de* D_8 *es un producto de potencias de a y b. Tomemos la acción de dicho grupo sobre las esquinas de un cuadrado.*

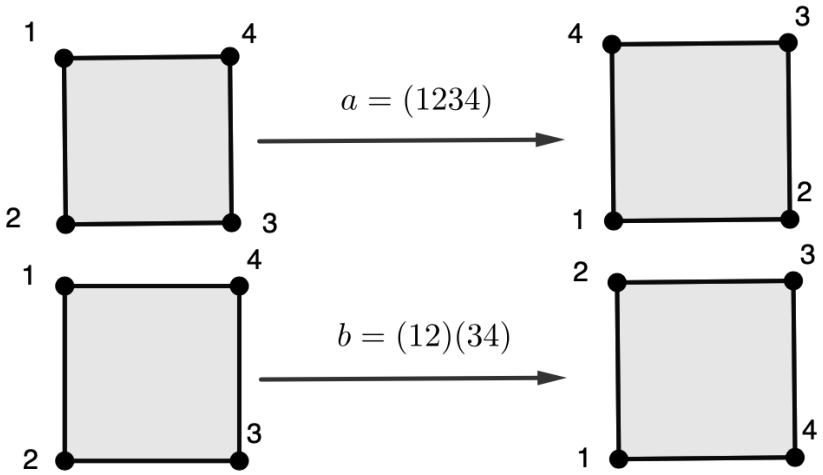


Figura 4.3: Acción de los generadores de D8 en un cuadrado

Nótese que la acción de a sobre las esquinas de cuadrado es equivalente a rotar el cuadrado 90 grados en sentido antihorario. Por otro lado, la acción de b sobre las esquinas del cuadrado es

equivalente a reflejarlo sobre el eje horizontal del cuadrado. Además, hemos utilizado la notación de ciclos para las permutaciones, lo que se describe en el anexo 10.1.

A partir de estas dos acciones, podemos determinar la acción de cualquier elemento de D_8 sobre el cuadrado. Ahora bien, si queremos saber cuál es el resultado de la acción de a^2b sobre el cuadrado tenemos:

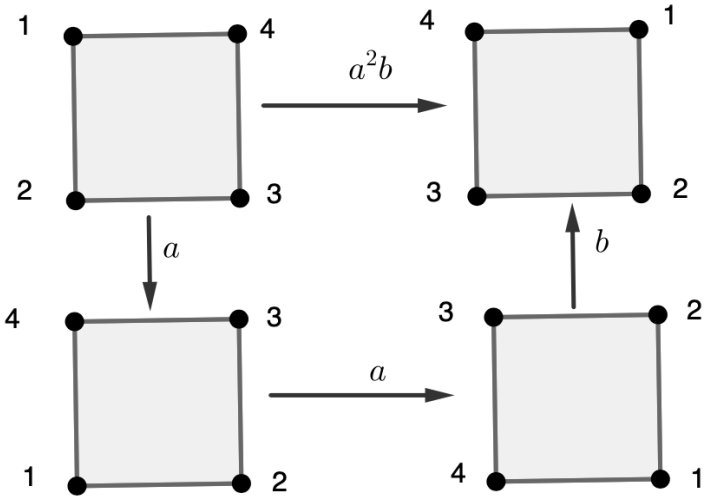


Figura 4.4: Acción de a^2b sobre las esquinas de un cuadrado

Ejemplo 4.2.2. *Ahora consideraremos la acción del grupo Dihedral de grado 6 sobre las esquinas de un hexágono. Dicho grupo está compuesto por:* $D_6 := \{e, a, a^2, a^3, a^4, a^5, b, b'\}$. *Donde la acción de a es rotar el hexágono $60°$ en sentido antihorario, b es rotar el hexágono sobre su eje vertical y por último, b' corresponde a rotar el hexágono sobre su eje horizontal. Es decir:*

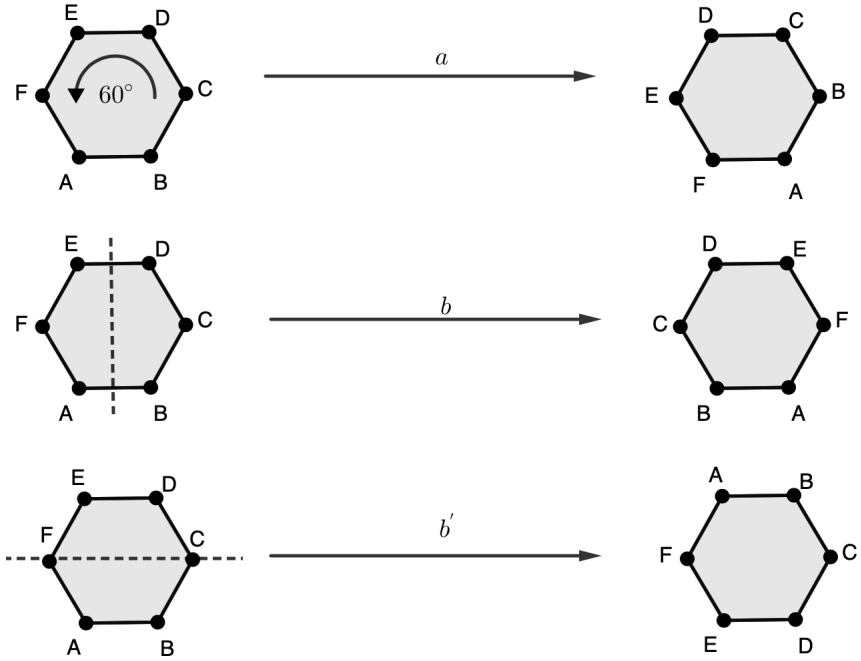


Figura 4.5: Acción de los generadores de D_6 sobre un hexágono

4.3. La acción de un grupo induce permutaciones del conjunto

Los ejemplos 4.2.1 y 4.2.2, nos permiten intuir que la acción de cada elemento es una permutación de las esquinas del n-ágono. En esta breve sección, formalizamos esta intuición en el siguiente lema.

Lema 4.3.1. *Sea G grupo actuando en el conjunto X. A cada $g \in G$ defina*

$$\tau_g : X \to X \ni \tau_G(x) = g * x.$$

Entonces,

$$\tau_g \in Perm(X).$$

Demostración. Primero, debemos probar la inyectividad. Considere

$$\tau_g(x) = \tau_g(y), \text{ entonces } g * x = g * y \text{ entonces } x = (g^{-1} \cdot g) * x = (g^{-1} \cdot g) * y = y$$

Ahora bien, para probar la sobreyectividad, sea

$$x \in X, \text{ entonces existe } g^{-1} * x \in G \text{ tal que } \tau_g(g^{-1} * x) = (g \cdot g^{-1}) * x = x$$

□

4.4. Estabilizadores y órbitas

A cada acción de un grupo sobre un conjunto, le corresponden dos conceptos útiles para el estudio de la acción, el estabilizador y la órbita de un elemento del conjunto. El primero es un subgrupo del grupo que realiza la acción, mediante las acciones de grupo y sus estabilizadores tenemos un mecanismo para producir subgrupos del grupo G. Haga al grupo actuar sobre un conjunto y halle los estabilizadores de los elementos.

Por otro lado, las órbitas son subconjuntos del conjunto X y particionan a X. Dichas particiones nos permiten desarollar técnicas de conteo e introducir relaciones de equivalencia en el conjunto en el que sea actúa.

4.4.1. Estabilizador

El estabilizador de x, es el conjunto de todos los elementos de G cuya acción deja fijo a x. Dicho subconjunto de G posee una cualidad especial; es un subgrupo de G.

Definición 4.4.1. *A cada elemento $x \in X$, le corresponde su estabilizador, el cual es el conjunto de todos los elementos del grupo G cuya acción sobre x lo deja invariante. Es decir,*

$$Stab_G(x) \coloneqq \{g \in G \mid g * x = x\}.$$

Teorema 4.4.1. *Para $\alpha \in X, Stab_G(\alpha) \leq G$*

Demostración. Primero, probamos la cerradura respecto al producto. Si

$$x, y \in Stab_G(x), \text{ entonces } (x \cdot y) * \alpha = x * (y * \alpha) = x * \alpha = \alpha.$$

Ahora, debemos probar la cerradura respecto a los inversos. Si

$$x \in Stab_G(\alpha), \text{ entonces } x^{-1} * \alpha = (x^{-1} \cdot x)\alpha = \alpha.$$

□

4.4.2. Órbitas

La órbita de un elemento es el conjunto de todas las imágenes de α bajo la acción del grupo. Es decir, es el conjunto de todos los elementos que resultan de la acción de cada $g \in G$ sobre el elemento α en cuestión.

Definición 4.4.2. *A cada elemento $\alpha \in X$, le asignamos el conjunto:*

$$O_X(\alpha) \coloneqq \{\beta \in X \mid \exists g \in G, g * \alpha = \beta\}.$$

La propiedad característica de las órbitas de un conjunto X es que las órbitas de los elementos del conjunto particionan al conjunto X. Por ende, dado el teorema fundamental del conjunto cociente, la acción de grupo nos induce una relación de equivalencia en el conjunto (Gorodentsev, 2017).

Teorema 4.4.2. *Las órbitas de los elementos de X particionan X*

Demostración. Primero, debemos probar que las órbitas son exhaustivas. Para ello, debemos notar que

$$\forall \alpha, e * \alpha = \alpha.$$

Entonces,

$$\alpha \in O_X(\alpha).$$

Concluyendo así que,

$$X = \bigcup_{\alpha \in X} O_X(\alpha).$$

Por otro lado, si

$$\gamma \in O_X(\alpha) \cap O_X(\beta) \text{ entonces existen } g, h \in G \ni \gamma = g * \alpha \text{ y } \gamma = h * \beta.$$

Entonces, existe

$$g^{-1}h \in G \text{ tal que } \alpha = g^{-1} * \gamma = g^{-1}h * \beta.$$

Por ende, si

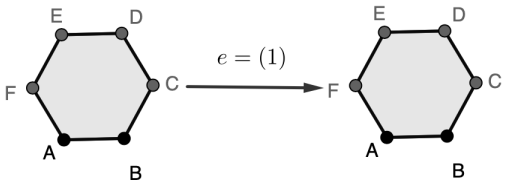
$\rho \in O_X(\alpha)$ entonces existe $x \in G, \rho = x\alpha$ entonces existe $xg^{-1}h \in G$ tal que $\rho = xg^{-1}h\beta$ entonces $\rho \in O_X(\beta)$.

De manera análoga,

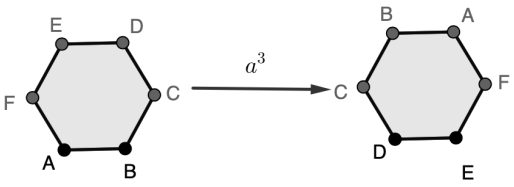
$$O_X(\beta) \subseteq O_X(\alpha).$$

□

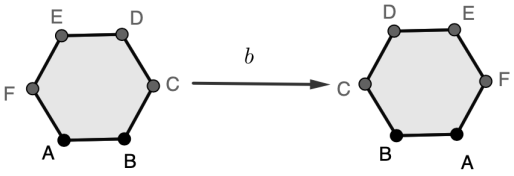
Ejemplo 4.4.1. *Consideremos el subgrupo $G = \{e, a^3, b, b'\}$ de D_6 y lo hacemos actuar por multiplicación izquierda en las esquinas del hexágono, como en 4.2.2. Tenemos lo siguiente:*



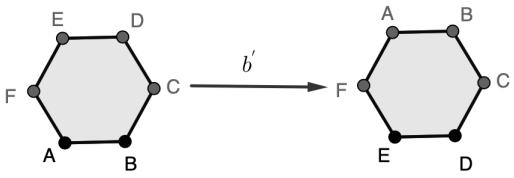
(a) El vértice C llega a la posición de la esquina F. Entonces, F está en la órbita de C.



(b) La identidad fija a C bajo su acción.



(c) El vértice C queda invariante bajo dicha acción.



(d) El vértice C pasa al vértice F y vice versa.

Figura 4.6: Acción del gupo G sobre el hexágono

Concluimos así que la órbita del vértice bajo la acción de G sobre las esquinas del hexágono es:

$$O_X(C) = \{C, F\}.$$

.

Por otro lado, vemos que el estabilizador es

$$Stab_G(C) = \{e, b^{'}\}.$$

.

En el siguiente ejemplo, estudiamos la acción de S_3 sobre el conjunto de subgrupos de S_3. Para una breve introducción sobre los grupos de permutaciones S_n véase 10.1 en los anexos.

Ejemplo 4.4.2. *Consideraremos la acción por multiplicación izquierda del grupo S_3 en el conjunto de subgrupos de S_3. En particular, determinaremos el estabilizador y la órbita del subgrupo alternante $A_3 \leq S_3$. Es decir, la imagen de $g * A_3$ donde $g \in S_3$, es la clase lateral izquierda de A_3 en S_3. Entonces tenemos:*

$$e \cdot A_3 = \{e, (123), (132)\} = (123) \cdot A_3 = (132) \cdot A_3.$$

Esto se debe a que

$$(123)(123) = (132) \ y \ (132)e = (132).$$

Por otro lado, tenemos que

$$(12) \cdot A_3 = \{(12), (23), (13)\} = (23) \cdot A_3 = (13) \cdot A_3.$$

En este ejemplo, podemos notar que la órbita del subgrupo alternate es el conjunto compuesto de las siguientes dos clases laterales izquierdas:

$$O_X = \{A_3, (12) \cdot A_3\}.$$

La cual es una partición del grupo cociente S_3/A_3 (véase el anexo 10.3).

Por otra parte, el estabilizador de A_3 bajo esta acción es:

$$Stab_{S_3}(A_3) = \{e, (123), (132)\}.$$

el cual claramente es subgrupo de S_3.

Ejemplo 4.4.3. *Calcularemos la órbita y el estabilizador del subgrupo $H = \{e, a, a^2, a^3\} = \langle a \rangle$ bajo la acción de D_8. Tenemos:*

$$e * H = \{e, a, a^2, a^3\} = a * H = a^2 * H = a^3 * H.$$

Mientras que la acción de los elementos b,ab, a^2b, a^3b de D_8 sobre H producen la siguiente clase lateral:

$$b * H = \{b, a^3b, a^2b, ab\} = ab * H = a^2b * H = a^3b = H.$$

Nótese que bajo esta acción, la órbita de H es

$$O_X(H) = \{H, bH\}.$$

Es decir, el conjunto compuesto por las dos clases laterales izquierdas eH, bH. Mientras que el estabilizador de H es

$$Stab_{D_8}(H) = \{e, a, a^2, a^3\} = H.$$

CAPÍTULO 5

Acciones en la teoría elemental de grupos

5.1. Digrafo de Cayley

Hasta el momento hemos visto los axiomas que debe satisfacer una acción de un grupo actuando sobre un conjunto. Hemos visto que a cada elemento del grupo actuando sobre un conjunto le corresponde su estabilizador, el cual es un subgrupo del grupo que realiza acción. Asimismo, a cada elemento del conjunto en el que sea actúa le corresponde su órbita, es decir el conjunto de imágenes del elemento bajo la acción del grupo. Vimos que dichas órbitas particionan al conjunto sobre el cual se realiza la acción.

En esta sección introducimos el concepto de digrafo de Cayley, el cual nos permite representar de manera visual la acción de un grupo finitamente generado sobre un conjunto finito. Así como, usando la tabla de Cayley de un grupo podemos determinar información del grupo, podemos usar digrafos de Cayley para determinar información de la acción. Este capítulo también nos servirá para introducir ejemplos que posteriormente analizaremos mediante nuestros teoremas y acciones de grupo.

Definición 5.1.1. *Definimos un* ***digrafo*** *como una pareja* (V, A)*, donde:*

- V *es un conjunto no vacío de vértices.*
- $A \subseteq V \times V$ *donde cada par ordenado* (u, v) *representa un segmento dirigido del vértice* u *al vértice* v*. Nótese que* $(u, v) \neq (v, u)$ *lo cual nos indica que dichos segmentos son, en efecto, dirigidos.*

En el caso particular de un ***digrafo de Cayley*** *tenemos:*

- *Los elementos del conjunto como vértices del grafo.*
- *Asignamos un estilo distinto de arco a cada elemento del conjunto generador* $G = \langle g_1, g_2, ..., g_n \rangle$*.*
- *Trazamos un segmento dirigido de estilo diferente para cada* g_i *desde el elemento del conjunto* α *hacia el elemento* β*, si* $g_i * \alpha = \beta$*. Obteniendo así el conjunto* A *de aristas de la definición.*

Como primera convención, no trazamos bucles del punto a sí mismo. Por otro lado, si existe una flecha del mismo g-estilo de α hacia β y vice versa, eliminamos ambas flechas y colocamos una flecha doble uniendo ambos vértices.

Ejemplo 5.1.1. *Consideremos un digrafo $G = (V, E)$, donde:*

1. *$V = \{1, 2, 3, 4\}$ es el conjunto de vértices.*
2. *$E = \{(1, 2), (2, 3), (3, 4), (4, 1), (1, 3)\}$ es el conjunto de aristas dirigidas.*

El digrafo anterior tiene la siguiente representación gráfica:

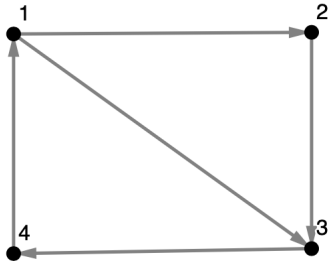


Figura 5.1: Digrafo G=(V, E, ϕ)

Ejemplo 5.1.2. *Siguiendo el ejemplo 4.2.1 tenemos que el grupo D_8 está generado por los elementos a y b. Entonces, al saber como actúan estos dos elementos sobre las esquinas de un cuadrado podemos determinar la acción de cualquier elemento de D_8 ya que este va a ser un producto de potencias de a y b.*

Si quisiéramos determinar cuál es la imagen de 3 bajo la acción de a^3b por multiplicación derecha, vemos que al aplicarle la acción de a tres veces a la esquina numerada con 3 llegamos a la esquina enumerada con 2. De allí, la aplicación de b a esta esquina nos traslada al número 1. Por ende, $3 * a^3b = 1$.

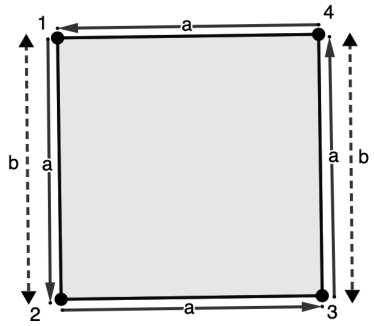


Figura 5.2: Digrafo de la acción de D_8 sobre el cuadrado

En el siguiente ejemplo, abusando del lenguaje, decimos que un **grupo actúa sobre sí mismo**. A lo largo de esta tesis, utilizaremos esta expresión para referirnos al hecho que el grupo G actúa sobre el conjunto de elementos de G, sin considerar su estructura de grupo.

Ejemplo 5.1.3. *En esta acción tenemos que D_8 actúa sobre sí mismo por multiplicación izquierda. Por ejemplo la acción de b sobre a^3 por multiplicación izquierda produciría:*

$$ba^3 = a^9b = ab$$

recordando el hecho que $ba = a^3b$ *según la definción en* 4.2.1

Posterior al cálculo de la acción de los generadores sobre D_8*, obtenemos el siguiente digrafo:*

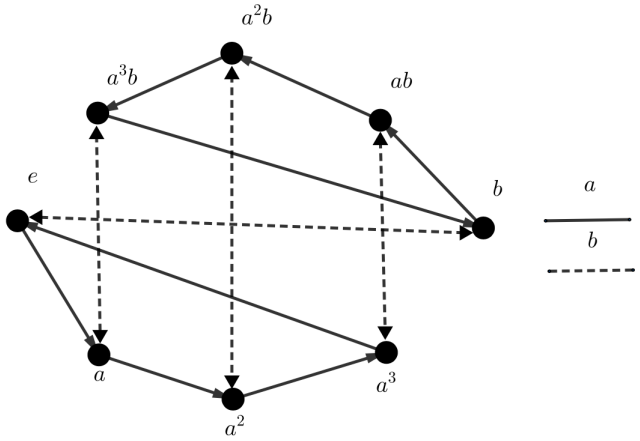


Figura 5.3: D_8 actuando en D_8 por multiplicación izquierda.

En este digrafo, dados dos vértices se puede encontrar una trayectoria, no única, entre ellos. Por ende, esta acción tiene una sola órbita.

Por ejemplo, si quisiéramos encontrar un elemento del grupo cuya acción en a^2 *nos produzca* ab*; viendo el digrafo podemos apreciar que* $ba * a^2 = ab$*. De igual manera,* $a^3b * a^2 = ab$*. Esto se lee del digrafo de Cayley en las siguientes trayectorias:*

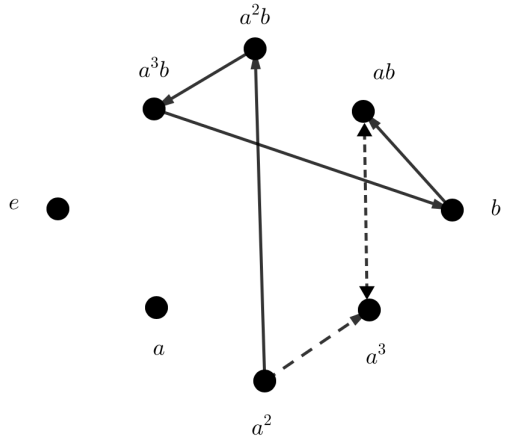


Figura 5.4: Distintos elementos de D_8 producen la misma imagen bajo la acción

Previo al siguiente ejemplo, introducimos la definición de la acción de un grupo sobre sí mismo por conjugación y la aplicamos al caso particular del grupo D_8 actuando en sí mismo por conjugación.

Definición 5.1.2. *Sean* $g, x \in G$ *grupo, definimos la acción por conjugación de* g *en* x *como*

$$g * x = gxg^{-1}.$$

Ejemplo 5.1.4. *A partir de esta acción tenemos el siguiente digrafo de Cayley.*

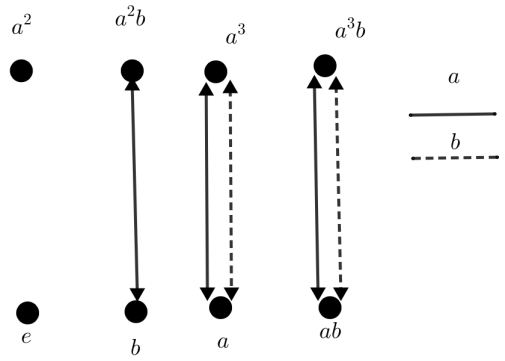


Figura 5.5: D_8 actuando sobre sí mismo por conjugación

Podemos apreciar la existencia de vértices aislados. Esto quiere indicar que la órbita de dicho elemento es el conjunto unitario que lo contiene. Por ejemplo, la órbita de a^2 *es*

$$O_{D_8}(a^2) = \{a^2\}.$$

.

Esto nos indica que la acción de cualquier elemento del grupo en a^2 *nos da como imagen* a^2 *mismo.*

En este caso, vemos que las órbitas de esta acción son:

1. $O_{D_8}(e) = \{e\}$,
2. $O_{D_8}(a) = \{a, a^3\}$,
3. $O_{D_8}(a^2) = \{a^2\}$,
4. $O_{D_8}(b) = \{b, a^2b\}$,
5. $O_{D_8}(ab) = \{ab, a^3, b\}$.

Las cuales son disjuntas a pares y exhaustivas, es decir, particionan D_8*, tal y como vimos en 4.4.2.*

5.2. El principio fundamental de Conteo

El principio fundamental de conteo es un teorema que nos brinda una relación entre la cardinalidad de la órbita de un elemento, su estabilizador y el orden del grupo que realiza la acción.

Esta relación será nos dará herramientas para probar resultados fundamentales de la teoría de grupos. Esto nos da una perspectiva distinta del curso de teoría de grupos ya que, tradicionalmente uno parte de introducir relaciones de equivalencia y utilizar las particiones que estas inducen para desarollar ciertas técnicas de conteo.

Sin embargo, en esta perspectiva, al introducir una acción de un grupo sobre un conjunto, uno parte de la partición mediante orbitas del conjunto en el que se actúa 4.4.2 y esto induce una relación de equivalencia en el conjunto sobre el que se actúa. Es decir, tenemos dos caras de la misma moneda.

Posteriormente implementamos el principio fundamental de conteo para obtener las técnicas de conteo deseadas. En esta sección probamos una única vez este teorema general y especificamos su contenido a la acción que nos sea útil.

Teorema 5.2.1. *Sea G un grupo actuando sobre un conjunto X. Sea $\alpha \in X$. Entonces,*

$$| O_X(\alpha) | = | G : Stab_G(\alpha) |$$

Demostración. Debemos hallar una biyección entre la óbita de α y las clases laterales en G de $Stab_G(\alpha)$. Considere la función

$$\phi : G/Stab_G(\alpha) \to O_X(\alpha), \text{ tal que } \phi(g \cdot Stab_G(\alpha)) = g * \alpha.$$

.

Primero, al ser un mapeo de clases laterales, debemos probar que dicha función está bien definida. Sin pérdida de generalidad, utilizaremos clases laterales izquierdas.

Si

$$g_1 \cdot Stab_G(\alpha) = g_2 \cdot Stab_G(\alpha), \text{ entonces } g_2^{-1} g_1 \in Stab_G(\alpha).$$

Se sigue que:

$$g_2^{-1} g_1 \alpha = \alpha, \text{ entonces } g_1 \alpha = g_2 \alpha.$$

Por ende:

$$\phi(g_1 \cdot Stab_G(\alpha)) = \phi(g_2 \cdot Stab_G(\alpha)).$$

Ahora bien, debemos probar que es una biyección. Empezaremos con la inyectividad:

Si

$$\phi(g_1 \cdot Stab_G(\alpha)) = \phi(g_2 \cdot Stab_G(\alpha)), \text{ entonces } g_1 \alpha = g_2 \alpha, \text{ entonces } g_2^{-1} g_1 \alpha = \alpha.$$

Concluyendo así que:

$$g_2^{-1} g_1 \in Stab_G(\alpha), \text{ entonces } g_1 \cdot Stab_G(\alpha) = g_2 \cdot Stab_G(\alpha).$$

Para mostrar la sobreyectividad tenemos que,

$$\beta \in O_X(\alpha), \text{ entonces existe } g \in G \text{ tal que } g\alpha = \beta.$$

Por ende, existe

$$g \cdot Stab_G(\alpha) \in G/Stab_G(\alpha) \text{ tal que}$$
$$\phi(g \cdot Stab_G(\alpha)) = \beta.$$

□

Ejemplo 5.2.1. *Retomando el ejemplo de la acción de D_8 en D_8 por conjugación 5.1.4, vemos a partir del su digrafo de Cayley 5.5 que*

$$O_{D_8}(a) = \{a, a^3\}.$$

De manera exhaustiva obtenemos que el estabilizador de a bajo la acción es

$$Stab_{D_8}(a) = \{e, a, a^2, a^3\}.$$

Entonces el cociente de D_8 módulo $Stab_{D_8}(a)$ es el conjunto compuesto por las siguientes clases laterales:

$$D_8/Stab_{D_8}(a) = \{Stab_{D_8}(a), b \cdot Stab_{D_8}(a)\}.$$

La prueba del principio fundamental nos indica que cualquier elemento de $Stab_{D_8}(a)$ *al actuar en a por conjugación produce a. Por ejemplo,*

$$a^3 * a = (a^3)a(a^3)^{-1} = a^3aa = a^5 = a.$$

Por otro lado, cualquier elemento de $b \cdot Stab_{D_8}(a) = \{b, ab, a^2b, a^3b\}$ *al actuar en a por conjugación produce* a^3*. Por ejemplo,*

$$ab * a = (ab)a(ab)^{-1} = (ab)a(ab) = a^7b^2 = a^3.$$

El teorema nos indica que hay tantas imágenes de un elemento bajo la acción como hay clases laterales del estabilizador del elemento en el grupo G. Es decir, existe una biyección entre la órbita de un elemento y el conjunto cociente del grupo módulo el estabilizador del elemento.

Además, en la prueba de dicho teorema, mostramos que todos los elementos de una clase lateral de $Stab_G(\alpha)$ tienen la misma imagen al actuar sobre α.

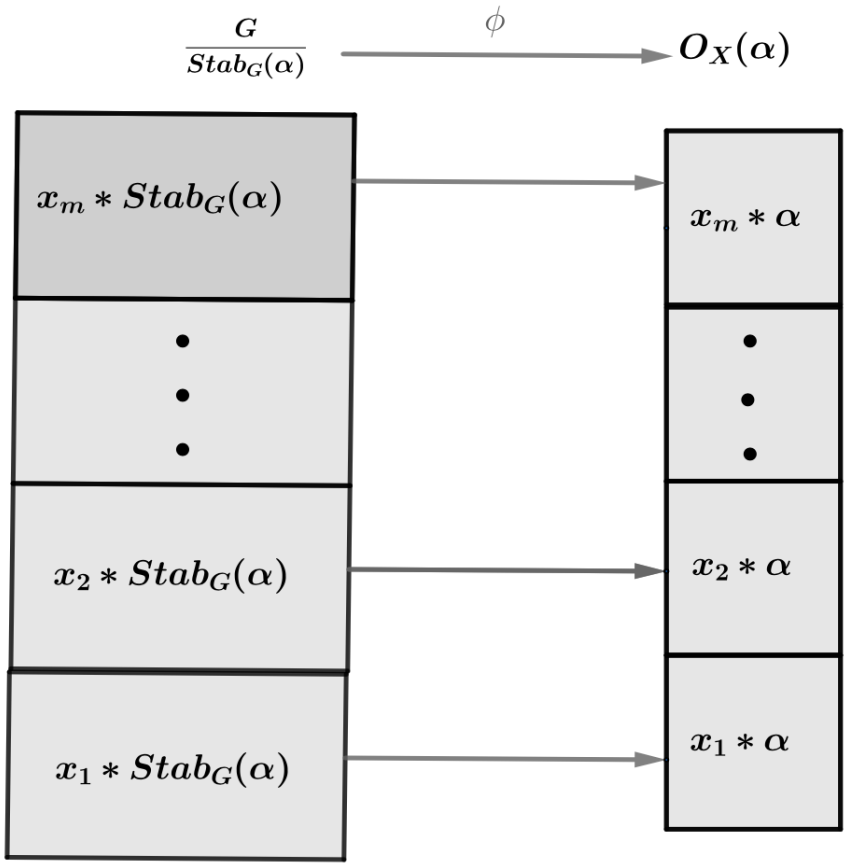


Figura 5.6: Elementos de clases laterales del estabilizador producen la misma imágen. (Shariari, 2017)

5.3. El Teorema de Lagrange

El método tradicional para probar el teorema de Lagrange es introduciendo la congruencia módulo algún subgrupo H y utilizar el grupo cociente para desarrollar técnicas de conteo. Sin embargo, utilizando las acciones de grupo, veremos que este teorema es un caso particular del principio fundamental de conteo, el cual ya probamos de manera general.

Definición 5.3.1. *Para probar el teorema de Lagrange, consideramos la siguiente acción. Sea G un grupo finito y $H \leq G$. Sea $X = \{x \cdot H \mid x \in G\}$, el conjunto de todas las clases laterales izquierdas de H. Definimos la acción de G en X por*

$$g * xH = gxH$$

Dicha acción la denominaremos por ***acción por traslación****.*

Primero, debemos probar que 5.3.1 es, en efecto, una acción de G en H.

Lema 5.3.1. *La acción de G en X por $g * xH = gxH$ es, en efecto, una acción.*

Demostración. Debemos probar que dicha acción satisface los axiomas 4.2.

1. $e \in G, gH \in G/H$ entonces $e * gH = e \cdot gH = gH, \forall gH$.
2. Sean $h_1, h_2 \in G, gH \in G/H$ entonces

$$h_1 * (h_2 * gH) = h_1 * (h_2 \cdot gH) = h_1 \cdot (h_2 \cdot gH) = (h_1 \cdot h_2) \cdot gH = (h_1 \cdot h_2) * gH$$

□

Ya que comprobamos que la acción traslación es una acción de grupo, nos preguntamos: ¿Cuáles son las órbitas de esta acción?, ¿Cuáles son los estabilizadores de la acción?

Definición 5.3.2. *Decimos que una acción es* ***transitiva*** *si tiene una sola órbita. Es decir, para cada elemento, su órbita es todo el conjunto.*

Ejemplo 5.3.1. *Como vimos en el ejemplo 5.1.3 la acción grupo D_8 actuando sobre sí mismo por multiplicación izquierda es transitiva ya que la órbita de cada elemento es el grupo mismo.*

Por otro lado, el ejemplo 5.1.4 nos muestra que la acción de D_8 sobre sí mismo por conjugación no es transitiva. Esto debido a que existe más de una órbita

La acción 5.3.1 es transitiva. Cuando una acción es transitiva, podemos ir de cualquier elemento del conjunto a otro cualquiera mediante la acción de grupo. Esto se debe a que si

$$xH, yH \in G/H \text{ entonces existe } yx^{-1} \in G \text{ tal que } yx^{-1} * xH = yH$$

.

Nótese que el subgrupo H es una clase lateral derecha de G, $H = eH$ (ver 10.3). Entonces, si consideramos la órbita y el estabilizador de H tenemos:

$$g \in Stab_G(H) \text{ si y sólo si } gH = H \text{ si y sólo si } g \in H$$

.

Concluyendo así que

$$H = Stab_G(H)$$

Teorema 5.3.1. ***Lagrange*** *Si G es un grupo finito y $\emptyset \neq H \leq G$, entonces el orden de H divide al orden de G.*

Demostración. El principio fundamental de conteo 5.2.1 y la transitividad de la acción nos indica que

$$| O_G(H) | = | G : H | \text{ , entonces } | G | = | O_G(H) | \cdot | H | = | G : H | \cdot | H |$$

□

El teorema de Lagrange es un caso particular del principio fundamental de conteo.

Ejemplo 5.3.2. *Consideremos la acción regular, i.e., por multiplicación izquierda, de D_8 en el conjunto de todos los subgrupos de D_8. En particular, consideremos el subgrupo $H = \langle a \rangle = \{e, a, a^2, a^3\}$.*

Como se mostró en 4.4.3 la órbita de H en D_8 bajo esta acción es $O_{D_8}(H) = \{H, b \cdot H\}$. Entonces,

$$8 = | D_8 | = | O_{D_8}(H) | \cdot | H | = 2 \cdot 4$$

En el siguiente ejemplo, estudiamos un caso particular de los grupos de permutaciones S_n, por lo cual referimos al lector al anexo 10.1. Asimismo, consideramos las clases laterales izquierdas del subgrupo alternante A_3 de S_3 para ejemplificar el teorema de Lagrange, por lo tanto, referimos al lector al anexo 10.3.

Ejemplo 5.3.3. *Consideremos la acción de S_3 por multiplicación izquierda en el conjunto de todos los subgrupos de S_3. Si nos enfocamos en dicha acción sobre el subgrupo alternante como en el ejemplo 4.4.2, tenemos los siguiente:*

$$S_3/A_3 = \{A_3, (12) \cdot A_3\} \text{ entonces } | O_{S_3}(A_3) | = | S_3 : A_3 | = 2.$$

Por el teorema de Lagrange, tenemos que:

$$6 = | S_3 | = | O_{S_3}(A_3) | \cdot | A_3 | = 2 \cdot 3.$$

5.4. La acción por conjugación y la ecuación de clases

En esta sección introducimos la acción de un grupo en sí mismo por conjugación, probamos que en efecto esto define una acción y analizamos las órbitas y estabilizadores de la misma. En esta acción, damos los nombres especiales de centralizador de un elemento y clase conjugada a los estabilizadores y órbitas de los elementos, respectivamente.

Para mostrar el uso del principio fundamental de conteo 5.2.1 en la acción por conjugación, probamos la ecuación de clase, la cual nos muestra que el orden del grupo es igual a la suma del orden del centro del grupo más la suma de los órdenes de las clases conjugadas de representantes canónicos que no pertenecen al centro del grupo. Por último, ejemplificamos la ecuación de clase en el caso particular de D_8 actuando sobre sí mismo por conjugación.

Definición 5.4.1. *Consideremos un elemento $x \in G$ y para cada $g \in G$, los elementos de la forma*

$$y = gxg^{-1},$$

son los ***conjugados*** *de x. Llamaremos a esta operación de tomar los conjugados de un elemento, la acción por* ***conjugación*** *de G en G.*

Primero, debemos probar que, en efecto, esta es una acción del grupo G en el conjunto G. Para ello debemos probar que se satisfacen los axiomas 4.2.

Lema 5.4.1. *La acción de un grupo sobre sí mismo, definida por conjugación es, en efecto, una acción.*

Demostración. Si $g \in G$ entonces

$$e * g = e \cdot g \cdot e^{-1} = ege = g.$$

Si $g_1, g_2, x \in G$ entonces

$$g_1 * (g_2 * x) = g_1 * (g_2 x g_2^{-1}) = (g_1 g_2) x (g_2^{-1} g_1^{-1}) = (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2) * x.$$

□

Ya que hemos verificado que esta es una acción de grupo, de nuevo nos preguntamos: ¿Cuáles son las órbitas y estabilizadores de esta acción?

En esta acción, llamamos a la órbita de un elemento su **clase conjugada**.

Definición 5.4.2. *La órbita de un elemento, denominada **clase conjugada**, se define como el conjunto*

$$O_G(x) \coloneqq \{gxg^{-1} \mid g \in G\}.$$

Y se denota por $cl_G(x)$.

Por otro lado, al estabilizador de un elemento bajo esta acción le llamamos el **centralizador** de dicho elemento, el cual ya sabemos por 4.4.1 que es un subgrupo del grupo que realiza la acción.

Definición 5.4.3. *El estabilizador se denota por*

$$Stab_G(x) \coloneqq \{g \in G \mid gxg^{-1} = x\} = C_G(x)$$

5.4.1. El principio fundamental de conteo aplicado a la conjugación

Sabemos que el principio fundamental de conteo nos provee una relación entre el tamaño de las órbitas y la cantidad de clases laterales del estabilizador. Por ende, aplicándolo a esta acción particular obtenemos:

Teorema 5.4.1. *Sea G grupo y x elemento de G. Entonces, la cardinalidad de la clase conjugada de x es igual a la cardinalidad del conjunto cociente G módulo centro en G de x. Lo cual se denota por:*

$$\mid cl_G(x) \mid = \mid G : C_G(x) \mid$$

.

Demostración. El teorema es una aplicación de 5.2.1. □

En particular, si el grupo G es finito, tenemos que la cardinalidad de cada clase conjugada de G divide el orden de G.

5.4.2. La ecuación de clase

La ecuación de clase nos indica que el orden del grupo es igual a la suma del orden del centro del grupo más la suma de los órdenes de las clases conjugadas de representantes canónicos que no pertenecen al centro del grupo (ver anexo 10.3).Antes de probar la ecuación de clase, necesitamos algunas definiciones.

Definición 5.4.4. *Decimos que un elemento x pertenece al* ***centro*** *del grupo G, denotado por $Z(G)$, si este elemento conmuta con todos los elementos de G. Es decir $x \in Z(G)$ si y sólo si $gx = gx, \forall g \in G$.*

Necesitaremos las siguientes equivalencias de pertenencia al centro del grupo para probar la ecuación de clase.

Lema 5.4.2. *Los siguientes enunciados son equivalentes:*

1. $x \in Z(G)$,
2. $C_G(x) = G$,
3. $\mid cl_G(x) \mid = 1$.

Demostración. Probaremos una cadena de implicaciones.

(1)→ (2) Primero, suponga $x \in Z(G)$. Sabemos que el estabilizador es subgrupo del grupo G. Por ende, $C_G(x) \subseteq G$. Por otro lado, si

$$g \in G \text{ entonces } gx = xg \text{ ergo } gxg^{-1} = x \text{ entonces } g \in C_G(x)$$

.

(2)→ (3) Nótese que, al ser $C_G(x) = G$, para cualquier g,

$$gxg^{-1} = x \text{ entonces } cl_G(x) = \{x\} \text{ entonces } \mid cl_G(x) \mid = 1$$

(3)→ (1) Nótese que $exe^{-1} = x \in cl_G(x)$ entonces al ser $\mid cl_G(x) \mid = 1$, tenemos que

$$cl_G(x) = \{x\}$$

Si $g \in G$ se sigue que

$$gxg^{-1} = x \text{ entonces } gx = xg, \forall g \in G \text{ concluyendo así que } x \in Z(G).$$

□

Con este resultado, estamos listos para mostrar cómo la ecuación de clase se sigue del principio fundamental de conteo.

Teorema 5.4.2. *Sean $x_1, ..., x_n$ representantes canónicos de distintas clases conjugadas de G que tienen más de un elemento. Entonces*

$$\mid G \mid = \mid Z(G) \mid + \sum_{i=1}^{n} \mid cl_G(x_i) \mid = \mid Z(G) \mid + \sum_{i=1}^{n} \mid G : C_G(x_i) \mid .$$

Demostración. Al considerar la acción de G en G mediante conjugación, vemos que las clases conjugadas, i.e., las órbitas, particionan G. Por otro lado, vemos que existen algunas órbitas de tamaño 1, que son precisamente las órbitas de elementos en el centro de G por la caracterización del lema anterior 5.4.2.

Entonces, si sumamos las cardinalidades de dichas clases obtenemos la cardinalidad del centro de G. Por ende,

$$\mid G \mid = \mid Z(G) \mid + \sum_{i=1}^{n} \mid cl_G(x_i) \mid .$$

.

Por el principio fundamental de conteo, para los representantes canónicos $x_1, ..., x_n$ de distintas clases conjugadas de G que tienen más de un elemento, tenemos que $\mid cl_G(x_i) \mid = \mid G : C_G(x_i) \mid$; al sustituir en la ecuación anterior:

$$\mid G \mid = \mid Z(G) \mid + \sum_{i=1}^{n} \mid G : C_G(x_i) \mid .$$

□

Ejemplo 5.4.1. *Si hacemos que D_8 actúe en sí mismo por conjugación, obtenemos el digrafo de Cayley 5.1.3. A partir de este digrafo podemos extraer las clases conjugadas de los elementos, es decir, las órbitas de los elementos. Estas son:*

1. $cl_{D_8}(e) = \{e\}$,
2. $cl_{D_8}(a) = \{a, a^3\}$,
3. $cl_{D_8}(a^2) = \{a^2\}$,
4. $cl_{D_8}(b) = \{b, a^2b\}$,
5. $cl_{D_8}(ab) = \{ab, a^3b\}$.

Podemos apreciar que los elementos de $Z(D_8)$, el centro del grupo D_8 son precisamente los elementos cuya clase conjugada consiste de un solo elemento. Entonces, $Z(D_8) = \{e, a^2\}$. Por ende, la ecuación de clase nos indica que

$$8 = \mid D_8 \mid = \mid Z(D_8) \mid + \mid cl_{D_8}(a) \mid + \mid cl_{D_8}(b) \mid + \mid cl_{D_8}(ab) \mid = 2 + 2 + 2 + 2.$$

5.5. Los teoremas de Sylow

Una de las técnicas tradicionales para probar los teoremas de Sylow es introduciendo el concepto de clase lateral doble y la relación de equivalencia de clase lateral doble en G. Mediante nuestro concepto de acción de grupo, hacemos actuar al grupo en cuestión sobre ciertos conjuntos particulares para obtener los primeros dos teoremas de Sylow y el teorema de Cauchy.

El primer teorema de Sylow nos permite garantizar la existencia de subgrupos de ciertos tamaños, en otras palabras, es un seudo-converso del teorema de Lagrange. El segundo teorema de Sylow nos indica que cualquier p-subgrupo es subgrupo de un conjugado de un p-subgrupo de Sylow. Por último, el teorema de Cauchy nos garantiza la existencia de un elemento de un orden específico; garantizando así, la existencia de un subgrupo de un orden particular.

Necesitamos las siguientes definiciones.

Definición 5.5.1. *Un **p-subgrupo** es un subgrupo cuyo orden es igual a p, número primo.*

Definición 5.5.2. *Un **p-subgrupo de Sylow** es un subgrupo cuyo orden es la mayor potencia del primo p que divide al orden del grupo, la notación empleada para decir que un número entero a divide a otro b es: $a \mid b$.*

Denotamos el conjunto de todos los p-subgrupos de Sylow por $Syl_p(G)$.

Previo al teorema de Sylow, necesitaremos este resultado de combinatoria. Para la prueba del teorema de Sylow nos será útil el converso, el cual nos da una condición suficiente para que $\binom{n}{p^a}$ no sea divisible entre un primo p.

Proposición: Sea p primo y m entero positivo. Suponga $n = p^a m$, donde p a es un entero no negativo. Entonces $\binom{n}{p^a} \equiv m$, mod p. En particular, si m no es divisible entre p, tampoco lo es $\binom{n}{p^a}$ (Silverman, 2022)

5.5.1. Primer teorema de Sylow (Existencia)

Para la prueba del primer teorema de Sylow, consideramos la acción por multiplicación izquierda de un grupo G sobre el conjunto de todos los subconjuntos de una cardinalidad específica.

Teorema 5.5.1. ***Sylow.*** *Si G es un grupo finito y p es un primo, entonces G tiene un p-subgrupo de Sylow.*

Demostración. Suponga $\mid G \mid = p^a \cdot m$. Para esta prueba, consideramos la acción de G en el conjunto $X = \{Y \subseteq G \ni \mid Y \mid = p^a\}$. Es decir, consideramos la acción por multiplicación izquierda del grupo sobre el conjunto de todos los subconjuntos de G cuyo orden es p^a.

Nótese que la cardinalidad del conjunto X es precisamente $\binom{n}{p^a}$. Por la propiedad previa al teorema,

$$\mid X \mid = \binom{n}{p^a} \equiv \text{m mod p.}$$

.

Se sigue que, $p \not\mid \mid X \mid$.

Ahora bien, Sabemos que las órbitas de dicha acción particionan al conjunto X, entonces debe existir alguna órbita cuya cardinalidad no es divisible entre p; ya que en caso contrario, p dividiría el orden del conjunto X.

Sea Y un conjunto que pertenece a dicha órbita cuyo orden no es divisible entre p. El principio fundamental de conteo indica que

$$\mid O_X(Y) \mid = \frac{\mid G \mid}{\mid Stab_G(Y) \mid}.$$

Entonces al saber que p no divide el orden de la órbita, debe ocurrir que p^a divida el orden $\mid Stab_G(Y) \mid$, i.e.,

$$p^a \leq \mid Stab_G(Y) \mid .$$

Por otro lado, vemos que si $y \in Y$, para cualquier

$$g \in Stab_G(Y), gy \in Y \rightarrow \mid Stab_G(Y) \mid = \mid Stab_G(Y)y \mid \leq \mid Y \mid = p^a.$$

Por lo tanto, $Stab_G(Y)$ satisface $\mid Stab_G(Y) \mid = p^a$ y es el p-subgrupo de Sylow deseado. □

5.5.2. Teorema de Cauchy

Como un resultado inmediato del primera teoerma de Sylow, tenemos el teorema de Cauchy. Este teorema nos garantiza la existencia de un elemento de un orden específico, y por ende, la existencia de un subgrupo de un orden específico. Es importante notar que este resultado se sigue de la implementación de la acción del grupo por multiplicación izquierda sobre el conjunto de todos los subconjuntos de un orden dado del grupo.

Teorema 5.5.2. ***Cauchy.*** *Sea $(G, \cdot)$ un grupo finito y p un número primo. Suponga p divide el orden de G, entonces existe un elemento $g \in G$ cuyo orden es p.*

Demostración. Por el primer teorema de Sylow existe un subgrupo $S \in Syl_p(G)$. Sea $x \neq 0 \in S$ entonces por el teorema de Lagrange 5.3.1, el orden de x dividide el orden de S. Es decir, es una potencia no nula de p. Entonces

$$o(x) = p^b \text{ con } b \neq 0.$$

Considere

$$g = x^{p^b - 1} \in G \text{ entonces } g^p = (x^{p^b-1})^p = x^{p^b} = e$$

. □

5.5.3. Segundo teorema de Sylow

Para esta prueba consideramos la acción de un p-subgrupo Q de G por multiplicación izquierda en el conjunto de todas las clases laterales izquierdas de P, dónde P es un p-sungrupo de Sylow de G.

Teorema 5.5.3. *Sea G un grupo finito, p un número primo y sea P un p-subgrupo de Sylow de G. Asuma $Q \leq G$ es un p-grupo. Entonces existe*

$$x \in G \text{ tal que } Q \leq xPx^{-1}.$$

Demostración. Suponga P y Q satisfacen la hipótesis. Para esta prueba consideramos la acción de Q por multiplicación izquierda en el conjunto de todas las clases laterales izquierdas de P. Es decir, $X = \{gP \mid g \in G\}$ y la acción de $q \in Q$, se denota por:

$$q * gP = qgP.$$

Al ser P un p-subgrupo de Sylow tenemos que

$$p \nmid | X | \text{ y } | X | = | G : P | .$$

Por otro lado, por el principio fundamental de conteo, el tamaño de las órbitas de dicha acción dividen el orden del grupo Q. Es decir, son potencias de p.

Si no existiera una órbita de tamaño uno, tendríamos que p dividiría el tamaño de cada órbita. Por ende, la cardinalidad del conjunto X, el cual es la suma del tamaño de las órbitas, sería divisible entre p.

Esto contradice el hecho que

$$p \nmid | X | = | G : P | .$$

La existencia de dicha órbita de tamaño uno quiere decir que una clase lateral izquierda de P es fijada bajo la acción de Q, entonces

$$O_X(gP) = \{gP\}.$$

Si $q \in Q$ su acción deja a gP invariante. Es decir,

$$q * gP = qgP = gP \text{ entonces } qgPg^{-1} = gPg^{-1}, \text{ por ende, } q \in gPg^{-1}.$$

Concluimos así que $Q \leq gPg^{-1}$. □

Ejemplo 5.5.1. *Hallaremos los 2-subgrupos de Sylow de S_3. El primer teorema de Sylow nos indica que debemos considerar la acción por multiplicación izquierda del grupo S_3 en el conjunto de todos los subconjuntos de cardinalidad 2. Por ende, primero debemos hallar todos los subconjuntos de tamaño 2 de S_3.*

Dicho conjunto contiene $\binom{6}{2} = 15$ elementos, ya que estamos escogiendo conjuntos de dos elementos y $| S_3 | = 3! = 6$. Por ende, dicho conjunto es:

$$\begin{aligned} X = \{&\{e,(12)\},\{e,(23)\},\{e,(13)\},\{e,(123)\},\{e,(132)\},\\ &\{(12),(23)\},\{(12),(13)\},\{(12),(123)\},\{(12),(132)\},\\ &\{(23),(13)\},\{(23),(123)\},\{(23),(132)\},\{(13),(123)\},\{(13),(132)\},\\ &\{(123),(132)\}\} \end{aligned}$$

Posteriormente, debemos hallar órbitas de elementos en X cuyo orden no sea divisible entre 2. Entonces, al calcular algunas de las órbitas de los conjuntos en X tenemos:

1. $O_X(\{(12),(23)\}) = \{\{(12),(23)\},\{e,(123)\},\{(123),(132)\},\{e,(132)\},\{(13),(12)\},\{(23),(13)\}\}$
2. $O_X(\{e,(12)\}) = \{\{(e,(12)\},\{(13),(123)\},\{(23),(132)\}\}$
3. $O_X(\{e,(23)\}) = \{\{(e,(23)\},\{(12),(123)\},\{(13),(132)\}\}$
4. $O_X(\{e,(13)\}) = \{\{(e,(13)\},\{(12),(132)\},\{(23),(123)\}\}$

Las órbitas que satisfacen la condición que 2 no divide el orden de dicha órbita son:

1. $O_X(\{e,(12)\})$
2. $O_X(\{e,(23)\})$
3. $O_X(\{e,(13)\})$

El siguiente paso es hallar los estabilizadores de dichos elementos de X. Es decir, hallar los estabilizadores de {e, (12)}, {e, (23)} y {e, (13)}. Después de un poco de cálculos vemos que:

1. $Stab_{S_3}(\{e,(12)\}) = \{(e,(12)\}$
2. $Stab_{S_3}(\{e,(23)\}) = \{(e,(23)\}$

3. $Stab_{S_3}(\{e,(13)\}) = \{(e,(13)\}$

Dichos estabilizadores son todos los 2-subgrupos de Sylow de S_3.

Ejemplo 5.5.2. *Para hallar un elemento de orden 2 en S_3, según el teorema de Cauchy, debemos seleccionar un elemento no nulo algún 2-subgrupo de Sylow de S_3. En este caso tenemos, a partir de 5.5.1, que los elementos de orden 2 son:*

1. $(12)(12) = e \to o((12)) = 2$
2. $(23)(23) = e \to o((23)) = 2$
3. $(13)(13) = e \to o((13)) = 2$

5.6. El teorema de Burnside

El siguiente teorema nos permite contar la cantidad de órbitas que se producen al tener una acción de un grupo en un conjunto. Es decir, ya que las órbitas de la acción partcionan el conjunto X; queremos hallar la cardinalidad del conjunto cociente X/G.

Para la prueba de dicho teorema, utilizaremos el concepto de la fibra de un mapeo, esto nos es útil al momento de comparar cardinalidades de conjuntos. Un mapeo $f : X \to Y$ descompone el conjunto X en la unión disjunta de subconjuntos no vacíos $f^{-1}(y)$ indexado por los elementos $y \in Im(f)$. En otras palabras, particionamos X en las preimágenes de los elementos $y \in Im(f)$.

Denotamos esto por $X = \bigsqcup_{y \in Im(f)} f^{-1}(y)$, dónde esto representa una unión disjunta. El hecho que $f^{-1}(y_1) \cap f^{-1}(y_2) = \emptyset$ se sigue de la definición de un mapeo. Ya que de lo contrario, habría un elemento con dos imágenes.

Teorema 5.6.1. ***Burnside.*** *Sea G un grupo finito actuando en un conjunto X. Para cada elemento $g \in G$, sea $X^g = \{x \in X \mid g * x = x\}$, el conjunto de los elementos de X fijados por la acción de g. Entonces, n el número de órbitas es igual a:*

$$n = \frac{1}{\mid G \mid} \sum_{g \in G} \mid X^g \mid .$$

Demostración. Consideremos $F = \{(g,x) \mid g * x = x\} \subseteq G \times X$. Ahora bien, utilizando las proyecciones $\pi_X : F \to X$ tal que $\pi(g,x) = x$ y $\pi_G : F \to X \ni \pi(g,x) = g$ obtenemos, mediante la partición descrita anteriormente obtenemos

$$\bigsqcup_{x \in X} Stab(x) = F = \bigsqcup_{g \in G} X^g$$

.

A partir de la igualdad $\bigsqcup_{x \in X} Stab(x) = F$ obtenemos que la cardinalidad de F es igual al producto de la cardinalidad de G por la cardinalidad del conjunto cociente de X en sus órbitas:

$$\mid F \mid = \mid G \mid \cdot \mid X/G \mid$$

.

Esto se debe a que todos los elementos α de una misma órbita tienen la misma cardinalidad

$$\frac{\mid G \mid}{\mid O_X(\alpha) \mid}$$

Entonces, al sumar por cada elemento de la órbita obtenemos la cardinalidad de G. Ahora, sumamos la cardinalidad de G $\mid X/G \mid$ veces.

Por otro lado, a partir de $F = \bigsqcup_{g \in G} X^g$ obtenemos que

$$\mid F \mid = \sum_{g \in G} \mid X^g \mid$$

.

Entonces,

$$\mid G \mid \cdot \mid X/G \mid = \sum_{g \in G} \mid X^g \mid$$

. Entonces, al despejar

$$\mid X/G \mid = \frac{1}{\mid G \mid} \sum_{g \in G} \mid X^g \mid .$$

□

En los ejemplos, aprendemos una manera más intuitiva para implementar el resultado dado por el teorema. Creamos una tabla donde, en cada fila, colocamos los elementos del grupo y en las columnas listamos los elementos del conjunto. Ahora, en la (i,j)-ésima entrada de la tabla utilizamos la siguiente regla de asignación:

$$(i,j) = \begin{cases} 1 & g_i * \alpha_j = \alpha_j \\ 0 & \text{cualquier otro caso} \end{cases}$$

Es decir, colocamos un 1 si el i-ésimo elemento del grupo fija al j-ésimo elemento del conjunto; colocamos 0 en cualquier otro caso. Posteriormente, para hallar n el número de órbitas, sumamos la cantidad de números 1 por fila y luego se suman dichos resultado. Por último, dividimos lo anteriormente calculado entre el órden del grupo.

Ejemplo 5.6.1. *Determinaremos la cantidad de Órbitas de la acción de D_8 en D_8 por multiplicación izquierda.*

Como vimos en el ejemplo 5.1.2, dicha acción es transitiva, i.e., tiene una única órbita. A partir de nuestro algoritmo tenemos la siguiente tabla:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	1	1	1	1	1	1	1	1
a	0	0	0	0	0	0	0	0
a^2	0	0	0	0	0	0	0	0
a^3	0	0	0	0	0	0	0	0
b	0	0	0	0	0	0	0	0
ab	0	0	0	0	0	0	0	0
a^2b	0	0	0	0	0	0	0	0
a^3b	0	0	0	0	0	0	0	0

Según nuestro algoritmo calculamos:

1. $\mid X^e \mid = 8$
2. $\mid X^a \mid = 0$

3. $| X^{a^2} | = 0$

4. $| X^{a^3} | = 0$

5. $| X^{b} | = 0$

6. $| X^{ab} | = 0$

7. $| X^{a^2b} | = 0$

8. $| X^{a^3b} | = 0$

Ahora, sumamos las cardinalidades calculadas y dicho resultado lo dividimos entre el orden de D_8*. Entonces,*

$$n = \frac{8+0+0+0+0+0+0+0}{8} = 1.$$

Vemos que 5.1.2 *concuerda con nuestro cálculo utilizando el teorema de Burnside.*

Ejemplo 5.6.2. *Consideramos la acción de* D_8 *en el conjunto de todos los subgrupos de* D_8 *por conjugación. A partir de un poco de cálculos, obtenemos que el digrafo de Cayley de dicha acción es el siguiente:*

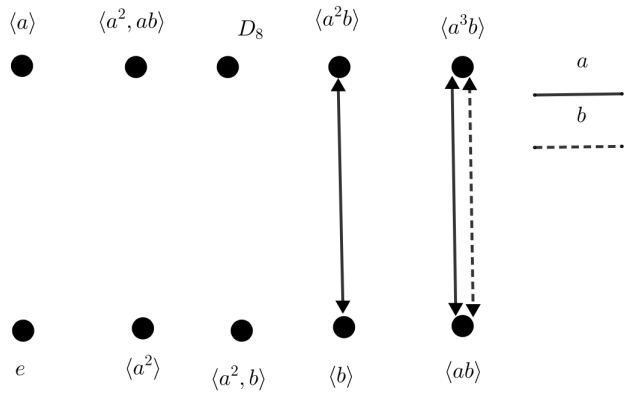


Figura 5.7: Digrafo de Cayley de la acción por conjugación de D_8 en sus subgrupos

A partir de esto, observamos que las órbitas son 8. Siguiendo nuestro algoritmo para el teorema de Burnside tenemos la siguiente tabla:

	e	$\langle a \rangle$	$\langle a^2 \rangle$	$\langle a^2, ab \rangle$	$\langle a^2, b \rangle$	$\langle b \rangle$	$\langle a^2b \rangle$	$\langle ab \rangle$	$\langle a^3b \rangle$	D_8
e	1	1	1	1	1	1	1	1	1	1
a	1	1	1	1	1	0	0	0	0	1
a^2	1	1	1	1	1	1	1	1	1	1
a^3	1	1	1	1	1	0	0	0	0	1
b	1	1	1	1	1	1	1	0	0	1
ab	1	1	1	1	1	0	0	1	1	1
a^2b	1	1	1	1	1	1	1	0	0	1
a^3b	1	1	1	1	1	0	0	1	1	1

Ahora, calculamos las cardinalidades de X^g *para cada elemento del grupo:*

1. $| X^{e} | = 10$

2. $| X^a | = 6$

3. $| X^{a^2} | = 10$

4. $| X^{a^3} | = 6$

5. $| X^b | = 8$

6. $| X^{ab} | = 8$

7. $| X^{a^2 b} | = 8$

8. $| X^{a^3} b | = 8$

Por último, sumamos las cardinalidades y dividimos entre el orden de D_8*. Entonces,*

$$n = \frac{10 + 6 + 10 + 6 + 8 + 8 + 8 + 8}{8} = 8.$$

CAPÍTULO 6

Aplicaciones de las acciones de grupo

Hasta el momento hemos introducido los axiomas de una acción de grupo y revisitado varios de los teoremas del curso de teoría de grupos desde esta perspectiva. En la metodología tradicional, uno emppieza a partir de relaciones de equivalencia en un conjunto e implementa la partición inducido por dicha relación sobre el conjunto para desarrollar técnicas de conteo. Sin embargo, en esta metodología de acciones de grupo, uno va en dirección contraria. Es decir, uno parte de la partición generada por las órbitas de la acción del grupo y a partir de estas desarrolla técnicas de conteo.

En esta sección mostramos la relevancia y vigencia del concepto de acción de grupo al mostrar su aplicación en la teoría de Galois, mediante la acción del grupo de Galois sobre las raíces de un polinomio. De igual manera, mostramos la aplicación de de dicho concepto en la teoría de representaciones de grupos finitos y probamos el teorema de Maschke, el cual nos indica que toda representación finito dimensional compleja de un grupo G es la suma de representaciones irreducibles.

6.1. Teoría de Galois

6.1.1. F-isomorfismos

En esta sección mostramos que dado un polinomio, con coeficientes en un campo dado, cuyo grado sea mayor a cero, podemos hallar una extensión de campo donde dicho polinomio tiene una raíz. Asimismo, introducimos el concepto de F-isomorfismo, los cuales nos permiten caracterizar elementos de una extensión de campo $F \subseteq E$ que tienen el mismo polinomio mínimo sobre F. Por último, probamos teoremas que serán las herramientas necesarias para probar que la acción del grupo de Galois sobre las raíces de un polinomio es, bajo ciertas condiciones, transitiva, i.e., tiene una sola órbita.

Ahora utilizaremos una técnica conocida de factorizar módulo un ideal generado por un polinomio irreducible para contruir un campo en el cual el polinomio irreducible tiene una raíz y el cual contiene una copia isomorfa del campo subyacente. Este teorema nos será útil para probar la existencia de los campos de descomposición.

Teorema 6.1.1. *Sea F un campo, y sea $f(x) \in F[x] \ni deg(f) > 0$. Entonces existe un campo E que satisface:*

1. *E tiene un subcampo isomorfo a F*
2. *f tiene una raíz en E*

Demostración. Nótese que al ser F campo, $F[x]$ es un dominio de factorización única (véase el anexo 10.4). Entonces cualquier polinomio se puede escribir de manera única, salvo asociados, como el producto de polinomios irreducibles. Por ende, podemos asumir directamente que f es irreducible, ya que en caso contrario haríamos la misma construcción con uno de dichos factores irreducibles.

Al ser $F[x]$ un dominio Euclideano, ver anexo 10.4, $\langle f(x)\rangle$ es un ideal maximal de $F[x]$ entonces $F[x]/\langle f(x)\rangle$ es un campo.

Consideremos el mapeo $\alpha \in F \mapsto \alpha + \langle f(x)\rangle$. Dicho mapeo claramente es un homomorfismo. Únicamente debemos mostrar que es inyectivo. Suponga $\alpha + \langle f(x)\rangle = \langle f(x)\rangle$ entonces $f(x) \mid \alpha$ pero α es una unidad y tiene grado menor que f, entonces $\alpha = 0$. Por ende, $F[x]/\langle f\rangle$ contiene una copia isomorfa de F.

Nótese que podemos extender el isomorfismo anterior a polinomios. Entonces, la imagen isomorfa de

$$f(x) = a_0 + ... + a_n x^n, \text{ a saber, } f^*(x) = (a_0 + \langle f\rangle) + ... + (a_n + \langle f\rangle)x^n$$

la identificamos con f.

Considere

$\alpha = x + \langle f(x)\rangle$ entonces $f(\alpha) = f^*(\alpha) = (a_0 + \langle f\rangle) + ... + (a_n + \langle f\rangle)(x + \langle f\rangle)^n = (a_0 + ... + a_n x^n) + \langle f(x)\rangle = \langle f(x)\rangle$.

Concluyendo así que f tiene una raíz en $F[x]/\langle f\rangle$ □

Ejemplo 6.1.1. *Consideremos el campo $\mathbb{Q}$ de los racionales y el polinomio $p(x) = x^2 + 1 \in \mathbb{Q}[x]$, el cual claramente es irreducible en dicho campo. Considerando el ideal generado por dicho polinomio $I = \langle x^2 + 1\rangle$ tenemos que*

$$\mathbb{Q}[x]/\langle x^2 + 1\rangle$$

es un campo.

Ahora bien, los elementos de dicho campo son clases laterales de la forma

$$f(x) + \langle x^2 + 1\rangle = f(x) + I, \text{ donde, } f(x) \in \mathbb{Q}[x]$$

Al ser $\mathbb{Q}[x]$ un dominio Euclideano, utilizando el algoritmo de la división, tenemos que existen polinomios

$$q(x), r(x) \in \mathbb{Q}[x] \text{ tales que } f(x) = q(x) \cdot (x^2 + 1) + r(x)$$

y $r(x)$ satisface que

$$r(x) = 0 \text{ o } deg(r) < deg(x^2 + 1) = 2.$$

Por lo tanto,

$$r(x) = a_0 + a_1 x, \ a_i \in \mathbb{Q},$$

entonces tenemos que

$$f(x) + I = r(x) + I = a_0 + I + a_1(x + I) = a_0 + a_1 x + I$$

El siguiente teorema nos permitirá probar la unicidad de los campos de descomposición.

Teorema 6.1.2. *Sean $F_1 \subseteq E_1$ y $F_2 \subseteq E_2$ campos, asuma $\theta : F_1 \to F_2$ es un isomorfismo. Sean $f_1(x) \in F_1[x], f_2(x) \in F_2[x]$ irreducibles tales que $\theta(f_1) = f_2$. Asuma $f_1(\alpha) = 0$ y $f_2(\beta) = 0$ para $\alpha \in E_1$ y $\beta \in E_2$. Entonces existe un único isomorfismo $\phi : F_1[\alpha] \to F_2[\beta]$ tal que:*

1. *$\phi\big|_{F_1} = \theta$, i.e., la restricción de ϕ a F_1 es igual a θ,*
2. *$\phi(\alpha) = \beta$.*

Demostración. Considere

$$\phi : F_1[x] \to F_2[x] \text{ tal que } \phi(g(\alpha)) = \theta(g)(\beta).$$

Primeramente, debemos notar que al ser $f(x)$ irreducible y tener a α como una raíz,

$$mín_{F_1}(\alpha)\big|f_1(x)$$

pero, al ser $f_1(x)$ irreducible, $f_1(x)$ es un múltiplo unitario de $mín_{F_1}(\alpha)$, i.e., un múltiplo constante de $mín_{F_1}(\alpha)$. Por ende, si

$$mín_{F_1}(\alpha) \mid g(x) \text{ entonces } f_1(x) \mid g(x)$$

Considere $g(x) = x \in F_1[x]$, entonces

$$\phi(\alpha) = \phi(g(\alpha)) = \theta(g)(\beta) = \beta$$

Concluyendo así que $\phi(\alpha) = \beta$.

Suponga

$$g(\alpha) = h(\alpha) \text{ entonces } (g-h)(\alpha) = 0 \text{ entonces } min_{F_1}(\alpha) \mid (g-h)(x)$$

Ergo,

$$f_1(x) \mid (g-h)(x) \text{ entonces existe } k(x) \in F_1[x] \text{ tal que } (g-h)(x) = f_1(x)k(x)$$

Entonces,

$$\phi((g-h)(\alpha)) = \theta(g-h)(\beta) = \theta(f_1)(\phi(\alpha)) \cdot \theta(k)(\phi(\alpha)) = f_2(\beta)\theta(k)(\beta) = 0$$

Por ende,

$$\phi(g(\alpha)) = \theta(g)(\beta) = \theta(h)(\beta) = \phi(h(\alpha)).$$

Concluyendo así que la función está bien definida.

Ahora probaremos que el mapeo es suprayectivo. Sea $g(\beta) \in F_2[x]$, entonces

$$g(\beta) = b_0 + b_1 \cdot \beta + ... + b_n \cdot \beta^n$$

entonces, para cada

$$b_i \in F_2, i = 1, .., n, \text{ existe } a_i \in F_1 \text{ tal que } \theta(a_i) = b_i$$

entonces existe

$$a_0 + ... + a_n\alpha^n \in F_1[\alpha] \text{ tal que } \phi(a_0 + ... + a_n\alpha^n) = \theta(a_0) + ... + \theta(a_n)\beta^n = \theta(g)(\beta)$$

Para probar la inyectividad, suponga

$$g(\alpha) \in F_1[x] \text{ tal que } \phi(g(\alpha)) = \theta(g)(\beta) = 0$$

Entonces,

$$min_{F_2}(\beta) \mid \theta(g)(\beta)$$

Por ende, al ser $f_1(x)$ irreducible, $f_2(x) = \theta(f_1(x))$ debe serlo también; por ende, $f_2(x)$ es un múltiplo unitario de $mín_{F_2}(\beta)$. Entonces existe

$k_2(x) \in F_2[x]$ tal que $\theta(g(x)) = f_2(x) \cdot k_2(x)$ entonces existe $k_1(x) \in F_1[x]$ tal que $\theta(k_1(x)) = k_2(x)$

Concluyendo así que

$$g(x) = f_1(x) \cdot k_1(x) \text{ entonces } g(\alpha) = f_1(\alpha) \cdot k_1(\alpha) = 0.$$

Por ende, el kernel de este mapeo es $\{0\}$

Por último, concluimos que el mapeo es un homomorfismo ya que,

$$\phi(g(\alpha)h(\alpha)) = \phi(gh(\alpha)) = \theta(gh)(\beta) = \theta(g)(\beta)\theta(h)(\beta) = \phi(g(\alpha))\phi(h(\alpha))$$

.

Ahora probaremos que $\phi \mid_{F_1} = \theta$. Sea $a \in F_1$ entonces $\phi(a) = \theta(a)$.

Por último, probamos la unicidad del mapeo propuesto. Suponga

$$\lambda : F_1[\alpha] \to F_2[\beta]$$

es otro mapeo que satisface las condiciones del teorema. Entonces

$$\lambda(g(\alpha)) = \lambda(g)(\lambda(\alpha)) = \theta(g)(\beta) = \phi(g(\alpha))$$

Ya que

$$\lambda \mid_{F_1} = \theta \text{ y } \lambda(\alpha) = \beta.$$

□

Ahora bien, si consideramos el caso particular en el que los campos satisfacen $F_1 = F_2 = F$, los polinomios son tales que $f_1 = f_2 = f$, y el mapeo $\theta = 1_F$ obtenemos el siguiente resultado como corolario. El siguiente resultado nos muestra que dos raíces del mismo polinomio irreducible, a saber α, β, nos da extensiones $F[\alpha], F[\beta]$ isomorfas que fijan el campo subyacente y las raíces desempeñan el mismo rol es sus respectivos campos.

Teorema 6.1.3. *Sean F, E_1, E_2 campos tales que $F \subseteq E_1$ y $F \subseteq E_2$. Sea $f(x) \in F[x]$ irreducible en F. Asuma $f(\alpha) = 0$ y $f(\beta) = 0$ para elementos $\alpha \in E_1, \beta \in E_2$. Entonces, existe un único isomorfismo $\phi : F[\alpha] \to F[\beta]$ tal que:*

1. *$\phi(\alpha) = \beta$*
2. *ϕ deja invariante a F, i.e., $\phi \mid_F = 1_F$*

Demostración. Se sigue de las observaciones anteriores. □

Definición 6.1.1. *Si $F \subseteq E_1$ y $F \subseteq E_2$ y $\phi : E_1 \to E_2$ es un isomorfismo que deja fijo al campo F, decimos que ϕ es un F-isomorfismo.*

Los F-isomorfismos nos permiten caracterizan elementos de un extensión de campo $F \subseteq E$ que tienen el mismo polinomio mínimo sobre F. El siguiente teorema nos será útil para mostrar que la acción del grupo de Galois es transitivia bajo ciertas condiciones.

Teorema 6.1.4. *Sean $F \subseteq E$ campos y $\alpha, \beta \in E$ elementos algebraicos sobre F. Entonces, los siguientes enunciados son equivalentes:*

- *$mín_F(\alpha) = mín_F(\beta)$*
- *$\exists \phi : F[\alpha] \to F[\beta]$ F-isomorfismo tal que $\phi(\alpha) = \beta$*

Demostración. La primera implicación se sigue directamente del teorema 6.1.3.

Para el converso, supongamos

$$f = mín_F(\alpha) \text{ y } g = mín_F(\beta)$$

Entonces,

$$\phi(0) = \phi(f(\alpha)) = \phi(f)(\phi(\alpha)) = f(\beta) = 0 \text{ entonces } g(x) \mid f(x)$$

Por ende, existe

$$u \in F[x]^* \text{ tal que } f(x) = ug(x)$$

Entonces, al ser $f(x)$ y $g(x)$ mónicos, $u = 1$. □

6.1.2. Campos de descomposición, el Grupo de Galois y la acción del Grupo de Galois sobre las raíces de un polinomio

En esta sección mostramos la existencia y unicidad de un campo de descomposición para cualquier polinomio sobre un campo F. Posteriormente, mostramos que si E es el campo de descomposición de algún polinomio sobre un campo F, entonces cualquier F-isomorfismo puede ser extendido a un automorfismo de E. Este resultado nos permitirá probar que el grupo de Galois Gal(E/F) actúa de manera transitiva sobre las raíces del polinomio dado.

Por otro lado, estudiamos el conjunto de todos los F-isomorfismos de una extensión $F \subseteq E$. Probaremos que dicho conjunto es un subgrupo del grupo de automorfismos de E y haremos actuar dicho subgrupo sobre las raíces de un polinomio. Por último, ejemplificamos la utilidad de las acciones de grupo en la teoría de Galois, al calcular el grupo de Galois $Gal(\mathbb{C}/\mathbb{R})$ y probar el conocido resultado que indica que, si un número complejo es una raíz de un polinomio con coeficientes en los reales, entonces su conjugado complejo también lo es.

Definición 6.1.2. *Sea F campo y $f(x) \in F[x]$, decimos que f se* ***descompone*** *en $F[x]$ si existen $c, \alpha_1, ..., \alpha_n \in F$ tal que $f(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$.*

Definición 6.1.3. *Si $F \subseteq E$ es una extensión de campo y $f(x) \in F[x]$, E es un campo de descomposición de f sobre F si f se descompone en $E[x]$ y f no se descompone en ningún campo $F \subseteq K \subseteq E$.*

Intuitivamente, un campo de descomposición es el campo más pequeño en el cual podemos descomponer un polinomio. El siguiente teorema nos permite mostrar la existencia de los campos de descomposición.

Teorema 6.1.5. *Sea F campo y $f(x) \in F[x]$. Entonces existe un campo de descomposición para f sobre F.*

Demostración. La prueba se hace por inducción sobre del grado de f. Para el caso base, consideramos deg(f)=1. En este caso, f es un polinomio lineal, el cual ya está descompuesto en $F[x]$.

Ahora, para la hipótesis inductiva, suponemos que deg(f)=n>1 y que el teorema está probado para cualquier polinomio de grado menor a n.

Ahora bien, por el teorema 6.1.1, sabemos que existe un campo K que contiene una copia isomorfa a F y en el cual f tiene un raíz, a saber, $\alpha \in K$ entonces existe

$$g(x) \in K[x] \text{ tal que } f(x) = (x - \alpha)g(x) \text{ y } \deg(g) < \deg(f)$$

Por la hipótesis inductiva, existe un campo de descomposición L de g sobre K.

Puesto que $F \subseteq K \subseteq L$ y f se descompone en L. Considere E como la intersección de todos los subcampos de L que contienen una copia isomorfa de F y en los cuales f se descompone; E es el campo de descomposición de f sobre F deseado. □

Vale la pena resaltar la importancia del paso intermedio para hallar el campo K, el cual nos permite mostrar que el conjunto de subcampos de L que contienen a F y en los cuales f se descompone es no vacío. Por ende, podemos asegurar que la intersección de dicho conjunto es el campo deseado.

Por lo tanto, el siguiente teorema, es una propiedad sencilla que nos permitirá inmediatamente probar la unicidad del campo de descomposición.

Lema 6.1.1. *Sea F campo y $f \in F[x]$. Suponga E es un campo de descomposición para f sobre F y K es otro campo tal que $F \subseteq K \subseteq E$. Entonces E es un campo de descomposición para f sobre K.*

Demostración. Por hipótesis, al ser $F \subseteq K$, $f \in K[x]$ entonces E es un campo de descomposición de f sobre K. Si existiera otro campo de descomposición L de f sobre K, por definición, $L \subseteq E$ y $E \subseteq L$. □

Teorema 6.1.6. *Sean F_1, F_2 campos y $\theta : F_1[x] \to F_2[x]$ un isomorfismo. Sean $f_1 \in F_1[x]$, $f_2 \in F_2[x]$ y $\theta(f_1) = f_2$. Si E_1 un campo de descomposición para f_1 sobre F_1 y E_2 un campo de descomposición para f_2 sobre F_2. Entonces existe un isomorfismo $\phi : E_1 \to E_2$ tal que la restricción de ϕ a F_1 es igual a θ, i.e., $\phi \mid_{F_1} = \theta$.*

Demostración. La prueba se hace sobre el grado de la extensión $\mid E_1 : F_1 \mid$. Para el caso base, consideramos $\mid E_1 : F_1 \mid = 1 \to E_1 = F_1$ entonces f_1 se descompone en F_1 entonces $f_2 = \theta(f_1)$ se descompone en F_2 entonces $E_2 = F_2$ y podemos considerar el mapeo deseado ϕ como el isomorfismo θ dado por la hipótesis.

Para la hipótesis inductiva, suponga $\mid E_1 : F_1 \mid = n > 1$ y el teorema ha sido probado para toda extensión de grado menor a n.

Puesto que $\mid E_1 : F_1 \mid = n > 1$ sabemos que $E_1 \neq F_1$. Entonces f_1 no se descompone en F_1 y, por ende, f_1 tiene un factor irreducible $g_1(x) \in F_1[x]$. Sin embargo, $g_1(x)$ sí se descompone en E_1 entonces existe una raíz de g_1, a saber $\alpha \in E_1$.

De manera análoga, al ser $f_2 = \theta(f_1)$ entonces existe $g_2 = \theta(g_1)$ un factor irreducible de f_2 en $F_2[x]$. Al ser E_2 un campo de descomposición de f_2 sobre F_2, existe una raíz de g_2, a saber $\beta \in E_2$.

La idea ahora es utilizar el teorema 6.1.2 para garantizar la existencia de un isomorfismo entre $F_1[\alpha]$ y $F_2[\beta]$ para, mediante la hipótesis inductiva, extenderlo a un isomorfismo entre E_1 y E_2.

Nótese que α, β son algebraicos entonces $F_1[\alpha], F_2[\beta]$ son campos y $f_1 \in F_1[\alpha]$ mientras que $f_2 \in F_2[\beta]$. Además,

$$\mid F_1[\alpha] : F_1 \mid = \deg(mín_{F_1}(\alpha)) = deg(g_1) > 1.$$

Entonces, por el teorema 6.1.2 existe un único isomorfismo

$$\lambda : F_1[\alpha] \to F_2[\beta] \text{ tal que } \lambda \mid_{F_1} = \theta \text{ y } \lambda(\alpha) = \beta.$$

Entonces

$$\lambda(f_1) = \theta(f_1) = f_2.$$

Por la propiedad 6.1.1, E_1 es un campo de descomposición de f_1 sobre F_1 y E_2 es un campo de descomposición de f_2 sobre F_2 respectivamente.

Resumiendo los resultados hasta ahora, tenemos que $\lambda : F_1[\alpha] \to F_2[\beta]$ es un isomorfismo tal que $\lambda \mid_{F_1} = \theta$. E_1 es un campo de descomposición de f_1 sobre F_1 y E_2 es un campo de descomposición de f_2 sobre F_2 . Además

$$\mid E_1 : F_1[\alpha] \mid < \mid E_1 : F_1 \mid \text{ , ya que } F_1 \subseteq F_1[\alpha] \subseteq E_1.$$

Por lo tanto, por la hipótesis inductiva, existe

$$\phi : E_1 \to E_2$$

isomorfismo tal que

$$\phi \mid_{F_1[\alpha]} = \lambda \to \phi \mid_{F_1} = \lambda \mid_{F_1} = \theta.$$

□

Como corolario tenemos la unicidad del campo de descomposición.

Lema 6.1.2. *Sea F campo, $f(x) \in F[x]$. Si E_1, E_2 son campos de descomposición de f sobre F, entonces $E_1 \simeq_F E_2$.*

Demostración. En el teorema anterior considere $F_1 = F_2 = F$, $f_1 = f_2 = f$ y $\theta = 1_F$. □

El siguiente teorema nos indica que si E es el campo de descomposición de algún polinomio, entonces cualquier F-isomorfismo puede ser extendido a un automorfismo de E. Este teorema nos será útil para mostrar que el grupo de Galois Gal(E/F) -el cual definiremos posteriormente- actúa de manera transitiva sobre las raíces del polonomio dado.

Teorema 6.1.7. *Sea F campo y E campo de descomposición de algún polinomio f sobre F. Suponga L_1 y L_2 son subcampos de E que contienen a F. Además, $\theta : L_1 \to L_2$ es un F-isomorfismo. Entonces existe un F-isomorfismo ϕ de E sobre E tal que $\phi \mid_{L_1} = \theta$.*

Demostración. Nótese que, al ser

$$F \subseteq L_1 \text{ tenemos que } f \in L_1.$$

Además, θ es un F-isomorfismo, entonces

$$\theta(f) = f \in L_2.$$

Por ende, la propiedad 6.1.1 nos indica que E es un campo de descomposición de f sobre L_1 y sobre L_2. Entonces el Teorema 6.1.6 nos permite extender θ a un automorfismo ϕ de E tal que

$$\phi \mid_{L_1} = \theta \text{ entonces } \phi \mid_F = \theta \mid_F = 1_F$$

□

Toda la teoría que hemos desarrollado nos permite llegar a este momento el cual es de interés para esta tesis. Enfocaremos nuestro estudio en la colección de todos los F-automorfismos de una extensión $F \subseteq E$. Veremos que dicho conjunto es un subgrupo del grupo de automorfismos del campo E (ver anexo 10.2) y actúa sobre las raíces de un polinomio. Esto con la finalidad de determinar fácilmente el grupo de Galois. Como ejemplo, probaremos un resultado que indica que si un número complejo es una raíz de un polinomio con coeficientes en los reales, entonces su conjugado complejo también lo es.

Definición 6.1.4. *Al subconjunto del grupo de automorfismo de E definido por*

$$Gal(E/F) = \{\sigma \in Aut(E) \mid \sigma \text{ es un } F\text{-isomorfismo de } E\},$$

lo llamamos el ***Grupo de Galois*** *de E sobre F.*

Probaremos ahora que dicho conjunto es, en efecto, un subgrupo de Aut(E).

Teorema 6.1.8. $Gal(E/F) \leq Aut(E)$.

Demostración. Sean

$$\sigma, \tau \in Gal(E/F)$$

Claramente, $\sigma \circ \tau$ es un automorfismo de E.

Únicamente debemos probar que la composición deja invariante a F. Sea

$$x \in F \text{ entonces } (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma(x) = x$$

Por ende, el conjunto es cerrado bajo el producto

Por otro lado, sea

$$\sigma \in Gal(E/F),$$

entonces σ^{-1} es un automorfismo de E.

De igual manera, debemos probar que el inverso fija F. Sea $x \in F$ entonces al ser σ un F-isomorfismo,

$$\sigma(x) = x \to \sigma^{-1}(x) = \sigma^{-1}(\sigma(x)) = x.$$

□

Como pudimos observar en la primera parte de esta tesis, podemos apreciar las propiedades de un grupo cuando éstos actúan sobre un conjunto. Por ende, deseamos mostrar que si $f(x) \neq 0 \in F[x]$, entonces $Gal(E/F)$ actúa sobre las raíces en E de f.

Teorema 6.1.9. *Sean $F \subseteq E$ campos y $f \in F[x]$. Sea $\Omega = \{\alpha \in E \mid f(\alpha) = 0\}$, el conjunto de las raíces de f en E. Entonces Gal(E/F) actúa sobre Ω.*

Demostración. Primero debemos probar que los elementos de $Gal(E/F)$ permutan las raíces de f en E. Sea $\sigma \in Gal(E/F)$ y sea $\alpha \in \Omega$, entonces

$$\sigma(f(\alpha)) = \sigma(f)(\sigma(\alpha)) = \sigma(0) = 0 \text{ entonces } \sigma(\alpha) \in \Omega.$$

Es decir, aplicar un elemento de Gal(E/F) a una raíz de f nos produce una raíz de f.

Ahora debemos probar que esta operación satisface los dos axiomas de la acción de grupo 4.2. Primero, notamos que

$$e * \alpha = \alpha,$$

para todo elemento de Ω.

Por otro lado, si $\sigma, \tau \in Gal(E/F)$ y $\alpha \in \Omega$ entonces

$$\sigma * (\tau * \alpha) = \sigma * (\tau(\alpha)) = \sigma(\tau(\alpha)) = (\sigma \circ \tau) * \alpha.$$

□

Lema 6.1.3. *Si $F \subseteq E$ son campos, $f \in F[x]$, $\Omega = \{\alpha \in E \mid f(\alpha) = 0\}$, es el conjunto de las raíces de f en E y E es el campo de descomposición de algún polinomio f sobre F el cual es irreducible, entonces Gal(E/F) actúa transitivamente sobre las raíces de f en E.*

Demostración. Suponga E es el campo de descomposición de f irreducible sobre F. Sean α, β raíces de f en E. Entonces,

$$mín_F(\alpha) \big| f \text{ y } mín_F(\beta) \big| f.$$

Entonces existen u, v unidades tales que

$$f = u \cdot mín_F(\alpha) = v \cdot mín_F(\beta) \text{ entonces } mín_F(\alpha) = u^{-1}v \cdot mín_F(\beta).$$

Al ser ambos polinomios mínimos mónicos, se cumple que $u^{-1}v = 1$ entonces, por la proposición 6.1.4, existe un F-isomorfismo

$$\theta : F[\alpha] \to F[\beta] \text{tal que } \theta(\alpha) = \beta.$$

Entonces, por el teorema 6.1.7, podemos extender el mapeo θ a un mapeo

$$\sigma : E \to E$$

que es un F-isomorfismo tal que

$$\sigma \mid_{F[\alpha]} = \theta.$$

Obtenemos que $\sigma(\alpha) = \theta(\alpha) = \beta$. Es decir, cualquier raíz de f en E está en la órbita de α. □

Ejemplo 6.1.2. *Aplicaremos las acciones de grupo en la teoría de Galois mediante el cálculo de Gal(ℂ/ℝ) aprovechándonos de la acción de dicho conjunto sobre las raíces $\{i, -i\}$ del polinomio $x^2 + 1 \in \mathbb{R}[x]$. Esto con el fin de probar el siguiente teorema:*

Teorema 6.1.10. *Sea $f(x) \in \mathbb{R}[x]$, entonces si $a + bi \in \mathbb{C}$ es una raíz de $f(x)$, su conjugado $a - bi$ también lo es.*

Demostración. Nótese que $\mathbb{R} \subseteq \mathbb{C}$ es una extensión de campo y tiene como base el conjunto $\{1, i\}$. Además el polinomio mínimo sobre $\mathbb{R}$ para $\{i, -i\}$ es $x^2 + 1$. Entonces, utilizando el teorema 6.1.4 existen $\mathbb{R}$-isomorfismos que mapean i a sí mismo y otro que mapea $i \mapsto -i$. Es decir:

1. $\sigma_1(i) = i$
2. $\sigma_2(i) = -i$

Donde σ_1 fija a los complejos $\mathbb{C}$. Es decir, es el mapeo identidad, $\sigma_1 = e$. Además, σ_2 mapea un número compejo a su conjugado complejo. Ambos mapeos fijan a los reales $\mathbb{R}$, i.e., son $\mathbb{R}$ isomorfismos.

Entonces, tenemos que $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{e = \sigma_1, \sigma_2\} \approx \mathbb{Z}/2\mathbb{Z}$. Por el teorema 6.1.9, ya que el grupo de Galois actúa sobre las raíces de un polinomio, si $a + bi$ es raíz de un polinomio en $\mathbb{R}$, entonces $\sigma_2(a + bi) = a - bi$ también lo es. □

6.2. Teoría de Representaciones de grupos finitos

6.2.1. Una representación produce una acción de grupo

Ahora estudiaremos la acción de un grupo finito sobre un espacio vectorial finito dimensional sobre los complejos. Asumimos que el campo subyacente son los números complejos para garantizar la existencia de autovalores y autovectores.

Definición 6.2.1. *Una **representación** de un grupo G a un espacio vectorial V es un homomorfismo, $\sigma : g \mapsto T_g$, de G hacia el subgrupo $GL(V) \subseteq L(V)$ de operadores invertibles (ver anexo 10.5). Si dicha representación es inyectiva, decimos que es **fiel**.*

Definición 6.2.2. *Por otro lado, la **dimensión** de la representación se define como la dimensión del espacio vectorial, en el caso de esta tesis, siempre sobre los complejos $\mathbb{C}$.*

Una representación σ de G en V convierte al espacio vectorial en un G-espacio, (G,V,σ). En dicho G-espacio, existe una acción de G en V mediante los mapeos lineales asignados por σ.

Teorema 6.2.1. *Si V es un G-espacio, G actúa sobre V mediante las transformaciones lineales asignadas por σ.*

Demostración. Debemos probar que se satisfacen los dos axiomas de la acción de grupo 4.2. Primero, consideramos

$$e \in G, v \in V \text{ entonces } \sigma(e) * v = T_e v = Iv = v.$$

Por ende, la acción de la identidad deja invariante a todos los vectores.

Ahora, consideramos

$$g_1, g_2 \in G, v \in V \text{ entonces}$$

$$\sigma(g_1) * (\sigma(g_2) * v) = \sigma(g_1) * T_{g_2} v = T_{g_1} T_{g_2} v = T_{g_1 \cdot g_2} v = \sigma(g_1 \cdot g_2) * v.$$

□

Por otro lado, debemos notar que los operadores T_g son necesariamente invertibles ya que si

$$g \in G \text{ entonces } g^{-1} \in G \text{ entonces existen } T_g \text{ y } T_{g^{-1}}.$$

Además,

$$T_e = T_{g \cdot g^{-1}} = T_g T_{g^{-1}} \text{ entonces } T_{g^{-1}} = (T_g)^{-}1,$$

ya que al estar en un espacio vectorial finito dimensional, es suficiente ser inverso por la derecha para ser inverso. Por ende, todo $T_g \in GL(V)$.

Definición 6.2.3. *Si σ es una representación de G en V, entonces un **G-subespacio** de V es un subespacio $W \leq V$ que es invariante bajo la acción de G, es decir,*

$$\forall g \in G, \forall w \in W, \boldsymbol{g}w \in W.$$

*También decimos que dicho subespacio es **G-invariante***

La restricción de un operador $\sigma(g) = \boldsymbol{g}$ a W es llamada una subrepresentación de σ.

6.2.2. La representación dual

Para un notación más concisa, denotaremos por $\mathbf{g}= \sigma(g) = T_g$.

Definición 6.2.4. *Si σ es una representación de G en V, obtenemos una representación σ^* de G en el dual V^* definida por $\sigma^*(g) = (\sigma(g^{-1}))^* = T^*_{g^{-1}}$. Es decir, el dual del inverso de la acción de G en V. Donde el mapeo dual satisface:*

$$\forall v \in V, \forall w^* \in V^*, T \in L(V), (Tv, w^*) = (v, T^* w^*).$$

Teorema 6.2.2. *G actúa sobre V^* mediante σ^*.*

Demostración. Primero probaremos que la identidad del grupo deja invariante a todos los vectores, es decir $\sigma^*(e) = 1_{V^*}$

Sea

$$e \in G, v \in V, w^* \in V^* \text{ entonces } (v, (T_{e^{-1}})^* w^*) = (T_{e^{-1}} v, w^*) = (T_e v, w^*) = (v, w^*), \forall w^* \in V^*$$

Por lo tanto,

$$(T_{e^{-1}})^* = 1_{V^*}$$

.

Ahora debemos probar que $\sigma^*(g_1 g_2) = \sigma^*(g_1)\sigma^*(g_2)$. Sean $g_1, g_2 \in G, v \in V, w^* \in W^*$ entonces

$$(v, \sigma^*(g_1 g_2) w^*) = (v, (T_{(g_1 g_2)^{-1}})^* w^*) = ((T_{(g_1 g_2)^{-1}})v, w^*) = (T_{g_2^{-1}} T_{g_1^{-1}} v, w^*) =$$
$$(T_{g_1^{-1}} v, T^*_{g_2^{-1}} w^*) = (v, T^*_{g_1^{-1}} T^*_{g_2^{-1}} w^*) = (v, \sigma^*(g_1)\sigma^*(g_2) w^*)$$

□

Al asumir que trabajamos en un espacio vectorial complejo, podemos asumir también que dicho espacio tiene un producto interno (ver anexo 10.5) -lo cual siempre se puede hacer, ya que al designar una base como ortonormal, podemos definir un producto interno en el espacio (Katznelson, 2008)-. Denotaremos dicho G-espacio como H.

Definición 6.2.5. *Una representación σ de G en un espacio complejo con un producto interno, es decir, un espacio Hermitiano H, es* ***unitaria*** *si $\sigma(g)$ es un operador unitario para todo $g \in G$, i.e., $(\sigma(g))^* \sigma(g) = I$, pero al trabajar en un espacio finito dimensional, esto equivale a*

$$(\sigma(g))^* = (\sigma(g))^{-1}.$$

Teorema 6.2.3. *Si la representación σ de G sobre H es unitaria, entonces $\sigma^* = \sigma$*

Demostración. Sea $g \in G$ entonces,

$$\sigma^*(g) = (T_{g-1})^* = (T_{g^-1})^{-1} = T_g = \sigma(g).$$

□

6.2.3. Promediando

Sea H un espacio complejo finito dimensional con producto interno (ver anexo 10.5), y sea G un subgrupo finito de $Gl(H)$. Definimos el operador:

Definición 6.2.6. $Q=\frac{1}{|G|}\sum_{g\in G} g^*g$.

Lema 6.2.1. *El operador Q es auto-adjunto y positivo.*

Demostración. Primero, probaremos que Q es autoadjunto. Entonces,

$$\langle Qv,v\rangle = \left\langle \tfrac{1}{|G|}\textstyle\sum_{g\in G} g^*gv, v\right\rangle = \tfrac{1}{|G|}\left\langle \textstyle\sum_{g\in G} gv, \sum_{g\in G} gv\right\rangle = \left\langle v, \tfrac{1}{|G|}\textstyle\sum_{g\in G} g^*gv\right\rangle = \langle v, Q^*v\rangle$$

Ahora, probaremos que es positivo definido.

$$\langle Qv,v\rangle = \left\langle \frac{1}{\mid G\mid}\sum_{g\in G} g^*gv, v\right\rangle = \frac{1}{\mid G\mid}\left\langle \sum_{g\in G} gv, \sum_{g\in G} gv\right\rangle = \frac{1}{\mid G\mid}\sum_{g\in G}\|gv\| \geq 0;$$

donde la igualdad se da si y sólo si,

$$\forall g\in G, \|gv\| = 0.$$

En particular,

$$e * v = 0 \text{ entonces } v = 0.$$

□

El operador Q definido en 6.2.6 lo utilizaremos para introducir el siguiente producto interno.

Definición 6.2.7. *Definimos el siguiente producto interno en H,*

$$\langle v,u\rangle_Q = \langle Qv,u\rangle = \frac{1}{\mid G\mid}\sum_{g\in G}\langle gv,gu\rangle.$$

Lema 6.2.2. *El producto interno 6.2.7 es, en efecto, un producto interno.*

Demostración. Debemos probar que dicho producto interno satisface los axiomas 10.5.4:

No negatividad:

$$\langle v,v\rangle_Q = \frac{1}{\|G\|}\sum_{g\in G}\langle gv,gv\rangle = \frac{1}{\mid G\mid}\sum_{g\in G}\|gv\|^2 \geq 0.$$

Además,

$$\langle v,v\rangle_Q = 0 \text{ si y sólo si } \forall g\in G, \frac{1}{\mid G\mid}\sum_{g\in G}\|gv\|^2 = 0 \text{ entonces } \|ev\| = \|v\|^2 = 0 \text{ entonces } v = 0.$$

Hermitiano:

$$\langle u,v\rangle_Q = \frac{1}{\mid G\mid}\sum_{g\in G}\langle g^*gu,v\rangle = \frac{1}{\mid G\mid}\sum_{g\in G}\langle u,g^*gv\rangle = \frac{1}{\mid G\mid}\sum_{g\in G}\overline{\langle g^*gv,u\rangle} = \overline{\langle v,u\rangle_Q}.$$

Lineal en la primera entrada:

Sean $\alpha, \beta \in \mathbb{C}, x, y, v \in H$ entonces

$$\langle \alpha x+\beta y, v\rangle_Q = \frac{1}{\mid G \mid}\sum_{g\in G}\langle g(\alpha x+\beta y), gv\rangle = \frac{1}{\mid G \mid}\left[\alpha\sum_{g\in G}\langle gx, gv\rangle + \beta\sum_{g\in G}\langle gy, gv\rangle\right] = \alpha\langle x, v\rangle_Q+\beta\langle y, v\rangle_Q.$$

□

Nótese que el ser Hermitiano y lineal en la primera entrada implica que el producto interno es sesquilineal, ya que

$$\langle u, \lambda v\rangle = \overline{\langle \lambda v, u\rangle} = \overline{\lambda}\langle u, v\rangle$$

Por ende, es suficiente satisfacer esas dos propiedades para ser un producto interno en un espacio vectorial sobre los complejos.

Con el producto interno 6.2.7, introducimos la norma inducida:

Definición 6.2.8. *Definimos la siguiente norma,*

$$\|v\|_Q^2 = \frac{1}{\mid G \mid}\sum_{g\in G}\langle gv, gv\rangle = \frac{1}{\mid G \mid}\sum_{g\in G}\|gv\|^2.$$

Lema 6.2.3. *La norma definida anteriormente es, en efecto, una norma.*

Demostración. Debemos probar que 6.2.8 satisface los axiomas 10.5.5:

Positividad: Nótese que

$$\forall g \in G, g * 0 = 0.$$

Entonces,

$$\forall g \in G, \|g0\|^2 = 0 \text{ entonces } \|0\|_Q^2 = 0.$$

Por otro lado, si

$$v \neq 0 \text{ entonces } e * v = v \neq 0 \text{ se sigue que } \|v\|^2 > 0 \text{ ergo } \|v\|_Q^2 > 0.$$

Homogeneidad: Sea $\alpha \in \mathbb{C}, v \in H$ entonces,

$$\|\alpha v\|_Q^2 = \frac{1}{\mid G \mid}\sum_{g\in G}\alpha\overline{\alpha}\langle gv, gv\rangle = \frac{\mid \alpha \mid^2}{\mid G \mid}\sum_{g\in G}\|gv\|^2 =\mid \alpha \mid^2 \|v\|_Q^2.$$

Desigualdad triangular:

$$\|u+v\|_Q^2 = \frac{1}{\mid G \mid}\sum_{g\in G}\|g(u+v)\|^2 \leq \frac{1}{\mid G \mid}\left[\sum_{g\in G}(\|gu\|^2+\|gv\|^2)\right].$$

Por otro lado,

$$\frac{1}{\mid G \mid}\left[\sum_{g\in G}(\|gu\|^2+\|gv\|^2)\right] = \frac{1}{\mid G \mid}\sum_{g\in G}\|gu\|^2 + \frac{1}{\mid G \mid}\sum_{g\in G}\|gv\|^2 = \|u\|_Q^2 + \|v\|_Q^2.$$

Uniendo ambos resultados,

$$\|u+v\|_Q^2 \leq \|u\|_Q^2 + \|v\|_Q^2.$$

□

Ahora, queremos mostrar que, si G es una representación de un grupo, el subgrupo $\sigma(G)$ es un subgrupo del grupo unitario $U(H)$ correspodiente al producto interno $\langle \cdot, \cdot \rangle_Q$ -ver anexo 10.5-.

Lema 6.2.4. *Si $\sigma : G \to GL(H)$ es una representación de grupo, entonces $G^* = \sigma(G)$ es un subgrupo del grupo unitario $U(H)$.*

Demostración. Como se puede ver en el anexo 10.5, un operador es unitario si y sólo si es una isometría. Por ende, debemos probar que

$$\forall h \in G^*, \forall v \in H, \|hv\|_Q = \|v\|_Q$$

Entonces, sea

$$h \in G^*, v \in H, \|hv\|_Q = \frac{1}{\mid G^* \mid} \sum_{g \in G^*} \langle ghv, ghv \rangle =$$

$$\frac{1}{\mid G^* \mid} \sum_{x \in G^*} \langle xv, xv \rangle = \|v\|_Q$$

Entonces, $G^* \leq U(H)$. □

Definición 6.2.9. *Decimos que un subespacio $W \leq H$ es **G-reducible** si es G-invariante y su complemento también lo es, i.e., $H = W \oplus Y$, donde ambos W, Y son G-invariantes.*

Definición 6.2.10. *Una representación (G, H, σ) es **irreducible** si no existe ningún subespacio G-invariante de H que sea no trivial. En caso contrario, decimos que es **reducile**.*

Ejemplo 6.2.1. *Si consideramos el grupo cíclico $C_3 = \{e, a, a^2\}$ y definimos:*

$$\sigma : C_3 \to GL(\mathbb{C}^3)$$

tal que

$$\sigma(a^i) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^i$$

A partir de esto, tenemos que la representación σ tiene la siguiente asignación:

$$\sigma(e) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\sigma(a) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\sigma(a^2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Por otro lado, consideremos el subespacio $W = \langle [1, 1, 1]^t \rangle$. Al aplicarle la acción de cada elemento del grupo a un vector $[\alpha, \alpha, \alpha] \in W$:

1.

$$\sigma(e)[\alpha, \alpha, \alpha] = [\alpha, \alpha, \alpha]$$

2.
$$\sigma(a)[\alpha,\alpha,\alpha] = [\alpha,\alpha,\alpha]$$

3.
$$\sigma(a^2)[\alpha,\alpha,\alpha] = [\alpha,\alpha,\alpha]$$

Concluyendo así que W es G-invariante. Por ende, (G, H, σ) es una representación reducible.

Ahora probaremos el teorema de Maschke, nuestro resultado principal. Este teorema nos indica que dada una representación de dimension finita de un grupo G, todo subespacio G-invariante, $W \leq H$ es G-reducible.

Teorema 6.2.4. *Sea $\sigma : G \to GL(H)$ es una representación de G en un espacio vectorial complejo finito dimensional. Si existe un subespacio G-invariante, entonces (G, H, σ) es G-reducible.*

Demostración. Sea $W \leq H$ un subespacio G-invariante. Si dotamos al espacio vectorial H con el producto interno $\langle \cdot, \cdot \rangle_Q$, tenemos el subespacio siguiente:

$$W^{\perp} = \{y \in H \mid \forall x \in W, \langle x, y\rangle_Q = 0\}.$$

Nótese que por el lema 6.2.4, toda transformación g es unitaria, i.e., $g^* = g^{-1}$. Entonces. Sean $g \in G, x \in W, y \in W^{\perp}$ entonces

$$\langle x, gy\rangle_Q = \frac{1}{\mid G \mid} \sum_{h\in G} \langle hx, hgy\rangle = \frac{1}{\mid G \mid} \sum_{h\in G} \langle g^{-1}h^{-1}hx, y\rangle =$$

$$\frac{1}{\mid G \mid} \sum_{g\in G} \langle g^{-1}x, y\rangle = \langle x, y\rangle_Q = 0.$$

Por ende, $W^{\perp}$ es G-invariante. □

Ahora ilustramos la descomposición garantizada por el teorema de Maschke siguiendo el ejemplo 6.2.1

Ejemplo 6.2.2. *Siguiendo con el ejemplo 6.2.1. Considere $\sigma : C_3 \to GL(\mathbb{C}^3)$ y $W = \langle [1,1,1]^t \rangle \leq \mathbb{C}^3$. Sabemos que $\mathbb{C}^3$ está dotado del producto interno usual:*

$$\langle u, v\rangle = \sum_{i=1}^{3} u_i \overline{v_i}.$$

Podemos dotar dicho espacio con el producto interno dado por 6.2.7, el cual en este ejemplo se describe como:

$$\langle u, v\rangle_Q = \frac{1}{\mid G \mid} \sum_{g\in G} g u_i \overline{g v_i}.$$

Ahora veremos qué efecto tiene la acción de cada elemento de la representación sobre un vector cualquiera de $\mathbb{C}^3$:

$$\sigma(e)[x_1,x_2,x_3]^t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} [x_1,x_2,x_3]^t = [x_1,x_2,x_3]^t.$$

$$\sigma(a)[x_1,x_2,x_3]^t = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} [x_1,x_2,x_3]^t = [x_3,x_1,x_2]^t.$$

$$\sigma(a^2)[x_1,x_2,x_3]^t = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} [x_1,x_2,x_3]^t = [x_2,x_3,x_1]^t.$$

Por ende, el producto interno inducido se decribe como:

$$\langle u,v\rangle_Q = \frac{1}{|\,C_3\,|}[(u_1\overline{v_1}+u_2\overline{v_2}+u_3\overline{v_3})+(u_3\overline{v_3}+u_1\overline{v_1}+u_2\overline{v_2})+(u_2\overline{v_2}+u_3\overline{v_3}+u_1\overline{v_1})] = u_1\overline{v_1}+u_2\overline{v_2}+u_3\overline{v_3}.$$

Considere $w \neq 0 \in W$ entonces $w = [\lambda,\lambda,\lambda]$. Se sigue que

$$\langle x,w\rangle_Q = x_1\overline{\lambda}+x_2\overline{\lambda}+x_2\overline{\lambda} = \overline{\lambda}[x_1+x_2+x_3].$$

Tenemos que dicho producto es cero cuando

$$x_1+x_2+x_3 = 0.$$

Por ende,

$$W^{\perp} = \{x \mid \forall w \in W, \langle x,w\rangle_Q = 0\} = \{[x_1,x_2,x_3]^t \mid x_1+x_2+x_3 = 0\}.$$

Sabemos que $W = \langle [1,1,1]^t\rangle$ y podemos completar la base de W a una base de $\mathbb{C}^3$, a saber:

$$\left\{[1,1,1]^t,[1,0,0]^t,[0,0,1]^t\right\}.$$

Por último, aplicaremos el proceso de Gram-Schmidt, respecto al producto interno $\langle\cdot,\cdot\rangle_Q$, para obtener una base ortonormal de $\mathbb{C}^3$. Primero. normalizamos el primer vector de nuestra base, obteniendo así:

$$u_1 = \frac{[1,1,1]^t}{\|[1,1,1]^t\|_Q} = \left[\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right]^t.$$

Ahora, quitamos de $[1,0,0]^t$, el segundo vector de nuestra base, su proyección sobre u_1 y lo normalizamos usando la norma 6.2.8. Obteniendo así:

$$u_2 = \left[\frac{\sqrt{2}}{\sqrt{3}},\frac{-1}{\sqrt{6}},\frac{-1}{\sqrt{6}}\right]^t.$$

Por último, quitamos del vector $[0,0,1]^t$ su proyección sobre u_2 y u_1 y normalizamos. Resultando en el vector:

$$u_3 = \left[0,\frac{-\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right]^t.$$

Ya que tenemos la base ortonormal, respecto al producto interno 6.2.7,

$$\{u_1,u_2,u_3\}$$

podemos descomponer el espacio vectorial de la siguiente manera, tal como lo indica el teorema de Maschke 6.2.4:

$$\mathbb{C}^3 = W \oplus W^{\perp} = \left\langle \left[\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right]^t \right\rangle \oplus \left\langle \left[\frac{\sqrt{2}}{\sqrt{3}},\frac{-1}{\sqrt{6}},\frac{-1}{\sqrt{6}}\right]^t, \left[0,\frac{-\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right]^t \right\rangle.$$

CAPÍTULO 7

Conclusiones

1. Las acciones de grupo nos permiten reformular el curso de teoría de grupos dado en la UVG. En esta perspectiva partimos de las particiones generadas por las órbitas de los elementos del conjunto en el que se actúa, a diferencia del método tradicional en el cual se van introduciendo relaciones de equivalencia para así obtener dichas particiones.

2. Es posible realizar una prueba del teorema de Lagrange, la ecuación de clases, los primeros dos teoremas de Sylow, el teorema de Cauchy y el teorema de Burnside mediante una acción particular.

3. Las acciones de grupo nos permiten introducirnos en temas más avanzados de matemáticas como lo son la teoría de Galois, al aprovechar la acción del grupo de Galois sobre las raíces de un polinomio, y la teoría de representaciones de grupos finitos, ya que la existencia de una representación es equivalente a la acción del grupo sobre un espacio vectorial mediante los operadores inducidos por la representación.

4. Las acciones de grupo nos permiten introducirnos en temas de investigación actual como lo es el programa de Langlands. Mediante las representaciones de grupo, uno puede empezar a inmiscuirse en este tema de investigación. Sin embargo, es posible ver instancias de este concepto en la topología, geometría y diversas otras ramas de la matemática mostrándonos así la ubicuidad y largo alcance de dicho concepto.

CAPÍTULO 8

Recomendaciones

1. Se recomienda planificar una introducción a la teoría elemental de grupos mediante las acciones de grupo para el curso impartido en la UVG. Esto con la finalidad de comparar y contrastar la metodología actual y la propuesta en esta tesis para determinar si es factible realizar dicha transición.

2. Se recomienda estudiar la acciones de grupos abelianos finitos sobre espacios vectoriales finito dimensionales, lo cual permite probar resultados conocidos, como el teorema fundamental de los grupos abelianos o el famoso teorema de Burnside para grupos no simples, los cuales se mencionan sin prueba en el curso elemental dado en la UVG, pero cuya prueba y comprensión se realiza mediante acciones de grupo. Es decir, al extender la teoría a este concepto, tenemos herramientas para probar resultados que en la metodología tradicional son muy complicados o inalcanzables.

3. Se sugiere impartir un seminario sobre Teoría de Galois o Representaciones de grupos finitos para motivar a los estudiantes a aprender acciones y dar continuidad, en caso de implementarse la recomendación anterior, al curso de teoría de grupos mediante acciones de los mismos.

4. Por último, se aconseja estudiar instancias de acciones de grupos en otras ramas de la matemática. Por ejemplo, en la topología en el estudio de colímites, la geometría en el programa de Erlangen, la teoría de nudos, entre otros temas selectos.

CAPÍTULO 9

Bibliografía

Referencias

Bewersdorff, J. (2021). *Galois theory for beginners: A historical perspective*. Providence, Rhode Island: American Mathematical Society.

der Waerden, V. (2013). *A history of algebra*. New York: Springer Science Business Media.

Etingof, P. (2011). *Introduction to representation theory*. Providence, Rhode Island: American Mathematical Society.

Gorodentsev, A. L. (2017). *Algebra i*. New York: Springer International Pu.

Judson, T. W. (2022). *Abstract algebra: Theory and applications*. Texas: Stephen F. Austin State University.

Katznelson, Y. (2008). *A (terse) introduction to linear algebra*. Providence, Rhode Island: American Mathematical Society.

Kleiner, I. (1986). The evolution of group theory: A brief survey. *Mathematics Magazine*(4), 195-215.

Lam, T. (1998). Representations of groups: A hundred years, part i. *Notices of the AMS*(1), 361-372.

Shariari, S. (2017). *Algebra in action: A course in groups, rings and fields*. Providence, Rhode Island: American Mathematical Society.

Silverman, J. H. (2022). *Abstract algebra*. Providence, Rhode Island: American Mathematical Society.

Taylor, M. E. (2020). *Linear algebra*. Providence, Rhode Island: American Mathematical Society.

CAPÍTULO 10

Anexos

10.1. Grupos de permutaciones

En esta sección exploraremos cómo, dado un conjunto finito de n elementos, denotado por $[n]$, podemos inducir un producto en el conjunto de todas las biyecciones de $[n]$ sobre sí mismo. Al introducir dicho producto, el cual es la composición de funciones, obtenemos la estructura de grupo. Dichos grupos son conocidos como el grupo de permutaciones de n letras, denotado por S_n.

Esto nos permite, de cierta manera, entender cómo funcionan todos los grupos finitos ya que, por el teorema de Cayley, todo grupo finito es isomorfo a un subgrupo de un grupo de permutaciones S_n. (Judson, 2022)

Definición 10.1.1. *Dado un conjunto [n] finito de n elementos, una* ***permutación*** *de dicho conjunto es una función*

$$\sigma : [n] \mapsto [n] \ni \sigma \text{ es una biyección}$$

Ahora bien, si consideramos el conjunto de todas las permutaciones de un conjunto finito, podemos introducir la operación de composición en dicho conjunto. Resulta ser que la composición de permutaciones en S_n es un producto bien definido en el conjunto y así inducimos la estructura de grupo a $(S_n, \circ)$(Judson, 2022).

Definición 10.1.2. *Si* $[n] = \{1, .., n\}$ *es un conjunto finito de n elementos, el conjunto de permutaciones* $S_n = \{\sigma : [n] \to [n] \mid$ *tal que es biyectiva*$\}$ *es el* ***grupo simétrico de n letras o el grupo simétrico de orden n****.*

Ejemplo 10.1.1. *Considerando el grupo simétrico de orden 3,* S_3*. Tenemos que uno de sus elementos es la permutación:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Donde la permutación descrita nos indica que:

- $\sigma(1) = 3$
- $\sigma(2) = 1$
- $\sigma(3) = 2$

Al ser S_n un grupo, podemos calcular el producto de elementos de S_n.

Ejemplo 10.1.2. *Sea $\tau \in S_3$ tal que:*

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Podemos hallar el producto $\sigma \circ \tau$, el cual resulta de aplicar σ a τ. Para calcular la imagen de 1 bajo $\sigma \circ \tau$ tenemos que:

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 3$$

Siguiendo con este procedimiento:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Asimismo, podemos calcular potencias de elementos de S_n, lo cual equivale a componer un elemento con sí mismo n-veces. Siguiendo con el ejemplo 10.1.1para hallar la imagen de 1 bajo σ^2 tenemos que:

$$\sigma^2(1) = \sigma(\sigma(1))$$

A partir de los ejemplos 10.1.1, $\sigma(1) = 3$. Entonces:

$$\sigma^2(1) = \sigma(3) = 2$$

Continuando con este razonamiento, llegamos a la conclusión que:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Definición 10.1.3. *Una permutación es un **ciclo** de longitud k si existen*

$$a_1, ..., a_k \in X \ni \sigma(a_i) = a_j, 1 \leq i < j < k \ y \ \sigma(a_k) = a_1$$

Además, la permutación σ deja invariante al resto de elementos $x \in X$. Denotamos esto por

$$(a_1 a_2 \cdots a_k)$$

Ejemplo 10.1.3. *Ahora, daremos la notación en ciclos de las permutaciones de los ejemplos 10.1.1 y 10.1.2. Primeramente, descomponemos σ en ciclos:*

$$\sigma = (132) = (213) = (321)$$

Por otro lado, ya que τ deja invariante a 1, tenemos que:

$$\tau = (23) = (32)$$

Por último, calculamos $\sigma \circ \tau$. Vemos que dicho producto deja invariante a 2, entonces:

$$\sigma \circ \tau = (13) = (31)$$

Los ciclos son los bloques con los que podemos construir todas las permutaciones ya que toda permutación se puede escribir como el producto de ciclos disjuntos a pares. (Judson, 2022) De particular de interés son las transposiciones:

Definición 10.1.4. *Una **transposición** es un ciclo de longitud 2.*

Ejemplo 10.1.4. *En el ejemplo 10.1.3 podemos apreciar que tanto τ como $\sigma \circ \tau$ son transposiciones.*

Podemos apreciar que todo ciclo se puede escribir como el producto de transposiciones ya que:

$$(a_1 a_2 \cdots a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_2)$$(Judson, 2022)

A partir de los dos resultados previos, concluimos que toda permutación se puede escribir como un producto de transposiciones. (Judson, 2022)

Ejemplo 10.1.5. *La descomposición en transposiciones de σ en 10.1.1 es:*

$$\sigma = (12)(13)$$

Definición 10.1.5. *Decimos que una permutación es **par** si, al descomponer su ciclo en transposiciones, la cantidad de éstas es par; decimos que es **impar** en el otro caso.*

Resulta que una permutación puede ser par o impar pero no ambas. Entonces, el conjunto de permutaciones de n letras, S_n, está particionado por el conjunto de permutaciones pares, el cual es subgrupo de S_n, y el conjunto de permutaciones impares. Más aún, ambos conjuntos dividen a S_n perfectamente a la mitad, es decir, ambos tienen cardinalidad $\frac{n!}{2}$.(Judson, 2022)

Definición 10.1.6. *El conjunto de permutaciones pares es denominado el **subgrupo alternante de orden n,** A_n*

Ejemplo 10.1.6. *Sea S_3 el grupo simétrico de orden 3.*

Subgrupo Alternante (Permutaciones Pares) :

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$

Conjunto de Permutaciones Impares :

$$S_3 \setminus A_3 = \{(1\ 2), (1\ 3), (2\ 3)\}$$

Los cuales particionan a S_3 y ambos tienen la misma cardinalidad $\mid A_3 \mid = \mid S_3 \setminus A_3 \mid = \frac{3!}{2} = 3$

10.2. Grupos de automorfismos

En este anexo estudiaremos el conjunto de todos los homomorfismos de un grupo sobre sí mismo y lo dotaremos de un producto, la composición de dichos mapeos, lo cual nos permitirá formar el grupo de automorfismos de un grupo dado.

Los homomorfismos son los mapeos entre grupos que respetan la estructura de grupo. Formalmente tenemos:

Definición 10.2.1. *Dados dos grupos $(G_1, \cdot_{G_1})$ y $(G_2, \cdot_{G_2})$, un mapeo $\phi : G_1 \to G_2$ que satisface*

$$\forall x, y \in G_1, \phi(x \cdot_{G_1} y) = \phi(x) \cdot_{G_2} \phi(y)$$

*es denominado un **homomorfismo de grupos**.*

Definición 10.2.2. *En el caso particular que el homomorfismo ϕ es un mapeo inyectivo, decimos que ϕ es un **monomorfismo**. Si ϕ es sobreyectivo decimos que el mapeo es un **epimorfismo**. Por último, si ϕ es una biyección, decimos que es un **isomorfismo**.*

De particular interés para nosotros es el caso cuando tenemos un isomorfismo de un grupo G sobre sí mismo.

Definición 10.2.3. *Dado un grupo $(G, \cdot)$, si $\phi : G \to G$ es un isomorfismo de grupos, decimos que ϕ es un* ***automorfismo****.*

Definición 10.2.4. *Dado un grupo $(G, \cdot)$, consideramos el conjunto*

$$Aut(G) = \{\phi : G \to G \mid \phi \text{ es un automorfismo de } G\}$$

Dicho conjunto es denominado el conjunto de automorfismos de G

Puesto que cada elemento de Aut(G) son automorfismos, sabemos que si

$$\phi, \lambda \in Aut(G) \text{ entonces } \phi \circ \lambda \text{ y } \phi^{-1} \text{ son mapeos biyectivos}$$

Resulta ser que ambos mapeos, $\phi \circ \lambda$ y ϕ^{-1}, también preservan la estrucura de grupo. Es decir,

$$\phi, \lambda \in Aut(G) \text{ entonces } \phi \circ \lambda \text{ y } \phi^{-1} \in Aut(G) \text{(Judson, 2022)}.$$

Por ende, al dotar Aut(G) con la composición de funciones tenemos que, $(Aut(G), \circ)$ es un grupo (Judson, 2022).

10.3. Clases laterales y Grupos cociente

Ahora introducimos los conceptos de clases laterales y conjuntos cociente. Asimismo, destacamos ciertos subgrupos especiales, llamados subgrupos normales los cuales nos permiten inducir de un producto al conjunto cociente, permitiéndonos así introducir los grupos cociente.

Definición 10.3.1. *Sea G grupo y H subgrupo de G. Definimos la* ***clase lateral izquierda*** *de H con* ***representante*** *$g \in G$ como el conjunto*

$$gH = \{g \cdot h \mid h \in H\}$$

.

De manera análoga, se definen las ***clases laterales derechas****.*

Debido a que existen distintos representantes para una misma clase lateral, al escoger un representante particular, decimos que es un ***representante canónico*** *de la clase lateral de H en G. Sin pérdida de generalidad, a lo largo de esta tesis se trabajará con clases laterales izquierdas.*

Ejemplo 10.3.1. *Consideremos el siguiente subgrupo de S_3:*

$$N = \{(1), (123), (132)\}$$

Se puede verificar que las clases laterales izquierdas de dicho subgrupo son:

$$(1)N = (123)N = (132)N = N$$

Por otro lado:

$$(12)N = (13)N = (23)N = \{(12), (13), (23)\}$$

Concluyendo así que dicho subgrupo tiene dos clases laterales izquierdas.

Podemos caracterizar cuando dos clases laterales son iguales mediante sus representantes. Tenemos que

$$g_1H = g_2H \text{ si y sólo si } \exists h \in H, g_1 = g_2 \cdot h \text{ si y sólo si}$$
$$\exists h \in H, g_2^{-1}g_1 = h \text{ si y sólo si } g_2^{-1}g_1 \in H.$$

Las clases laterales nos permiten particionar el grupo subyacente (Judson, 2022).

Definición 10.3.2. *Llamamos a la cantidad de clases laterales izquierdas de un subgrupo H el* ***índice*** *del subgrupo, lo cual denotamos como*

$$| G : H |$$

Resulta ser que existen tantas clases laterales izquierdas de un subgrupo H en G como clases laterales derechas de H en G (Judson, 2022). Es decir, existe una biyección entre el cociente G módulo H y el conjunto de clases laterales derechas de H en G.

Sin embargo, existen algunos subgrupos especiales que nos permiten introducir un producto bien definido en el conjunto cociente del grupo G módulo subgrupo H.

Definición 10.3.3. *Un subgrupo H de G es un subgrupo* ***normal*** *si toda clase lateral izquierda del elemento $g \in G$ coincide con la clase lateral derecha del mismo representante. Es decir,*

$$\forall g \in G, gH = Hg,$$

donde g es el mismo representante en ambos lados de la igualdad.

Denotamos que H es un subgrupo normal de G como $H \trianglelefteq G$

La propiedad de ser subgrupo normal no es algo atribuible a todos los subgrupos.

Ejemplo 10.3.2. *Si consideramos el subgrupo $H = \{1, (12)\} \leq S_3$, vemos que*

$$(23)H = \{(23), (132)\} \neq \{(23), (123)\} = H(23)$$

Por ende, H no es normal en S_3. Sin embargo, si consideramos $Q = \{1, (123), (132)\}$ es un subgrupo normal en S_3, ya que tiene índice 2 y es un resultado conocido que todo subgrupo de índice 2 es normal (Judson, 2022).

La primer caracterización sencilla de subgrupo normal es mediante el índice de dicho subgrupo. El subgrupo H de G es normal en G si y sólo si tiene índice de orden 2, i.e., $\mid G : H \mid = 2$. Esto debido a que para cualquier elemento no nulo $g \in G$, la clase lateral derecha e izquierda de dicho representante debe contener al elemento mismo:

$$g \cdot e \in gH \text{ y } e \cdot g \in Hg$$

Entonces, al haber únicamente dos clases laterales derechas e izquierdas de H en G, $gH = Hg$.

Ejemplo 10.3.3. *A partir de la caracterización anterior y debido a que el orden del subgrupo alternante es $\frac{n}{2}$, todo subgrupo alternante es normal en su respectivo grupo de permutaciones. Es decir, $A_n \trianglelefteq S_n$ para todo n.*

De igual manera, podemos caracterizar los subgrupos normales mediante la siguiente igualdad. :

$$H \trianglelefteq G \text{ si y sólo si } \forall g \in G, gHg^{-1} = H$$

Sin embargo, podemos relajar dicha igualdad a la siguiente inclusión:

$$H \trianglelefteq G \text{ si y sólo si } \forall g \in G, gHg^{-1} \subseteq H \text{(Judson, 2022)}$$

El propósito de introducir los subgrupos normales es poder introducir en el conjunto cociente G módulo subgrupo normal H un producto bien definido y dotarlo de la estructura de grupo.

Definición 10.3.4. *Si $H \trianglelefteq G$, introducimos en G/H el producto de clases laterales, el cual se realiza mediante la multiplicación de representantes. Es decir:*

$$g_1H, g_2H \in G/H \text{ entonces } (g_1H) * (g_2H) = (g_1 \cdot g_2)H$$

Vemos que dicho producto está bien definido si y sólo sí el subgrupo H es normal. Esto debido a que:

$$\text{Si } H \trianglelefteq G \text{ entonces } g_1H * g_2H = g_1(Hg_2)H = (g_1 \cdot g_2)HH = (g_1 \cdot g_2)H$$

Por otro lado, si la operación está bien definida:

Sea $ghg^{-1} \in gHg^{-1} \rightarrow ghg^{-1}H = ghH \cdot g^{-1}H = gH \cdot g^{-1}H = (gg^{-1})H = H \rightarrow ghg^{-1} \in H \rightarrow gHg^{-1} \subseteq H$

Entonces por la caracterización anterior 10.3, $H \trianglelefteq G$.

Ejemplo 10.3.4. *Considerando el subgrupo $N = \{(1), (123), (132)\} \trianglelefteq S_3$, del ejemplo 10.3.1. Tenemos que el conjunto cociente S_3/N tiene la siguiente tabla de Cayley:*

	N	$(12)N$
N	N	$(12)N$
$(12)N$	$(12)N$	N

Tabla 10.1: Tabla de Cayley del grupo cociente S_3/N

La quintaesencia de los grupos cocientes es dejar de pensar en términos de elementos. ¿Qué pasa si multipico la permutación (123) con la permutación (12)? Y pensar en términos de clases de elementos: ¿Qué pasa si multiplico un elemento de la clase $(123)N = N$ con uno de la clase $(12)N$?

10.4. Anillos y campos

En este anexo es un amalgama de ciertos elementos de la teoría de anillos y campos, los cuales son necesarios para nuestro desarrollo de la teoría de Galois en 6.1.1. Iniciamos con la siguiente definición.

Definición 10.4.1. *Un **anillo** es una tripleta $(R, +, \cdot)$, donde R es un conjunto, $(R, +)$ es un grupo abeliano y $(R, \cdot)$ es un producto que satisface los siguientes axiomas:*

1. ***asociatividad*** $\forall r, s, t \in R, r \cdot (s \cdot t) = (r \cdot s) \cdot t$
2. ***Distributividades*** $\forall r, s, t \in R$,
   - $r \cdot (s + t) = r \cdot s + r \cdot t$
   - $(r + s) \cdot t = r \cdot t + s \cdot t$

En esta tesis consideraremos únicamente anillos con identidad. Asimismo, tenemos tipos de anillos más especializados, es decir, anillos que satisfacen axiomas adicionales. Entre estos tenemos:

Definición 10.4.2. *Un **dominio entero** es un anillo conmutativo sin **divisores de cero**. Esto quiere decir que, si $a \cdot b = 0$ entonces, $a = 0$ o $b = 0$.*

Definición 10.4.3. *Un **campo** es un anillo $(R, +, \cdot)$ donde $(R \setminus \{0\}, \cdot)$ es un grupo abeliano.*

Ejemplo 10.4.1. *Si R es un anillo, entonces podemos considerar el conjunto $R[x] = \{a_0 + a_1x + ... + a_nx^n \mid a_i \in R, n \geq 0\}$, de los polinomios en x con coeficientes en $\mathbb{R}$. Dicho conjunto lo podemos dotar de una suma y producto de polinomios habituales. Entonces, $(R[x], +, \cdot)$ es un anillo.*

De particular interés para esta tesis será el caso cuando el anillo subyacente sea un campo y generemos el anillo de polinomios sobre el campo.

Definición 10.4.4. *Los morfismos entre anillos son los **homomorfismos de anillos**.*

A cada homomorfismo le corresponde su kernel, dicho conjunto lo definimos de la siguiente manera:

Definición 10.4.5. *Sea $\phi : (R_1, +_{R_1}, \cdot_{R_1}) \to (R_2, +_{R_2}, \cdot_{R_2})$ un homomorfismo de anillo, el **kernel de** ϕ es el conjunto*

$$ker_\phi = \{r \in R_1 \mid \phi(r) = 0_{R_2}\}$$

Definición 10.4.6. *Un **ideal** I de un anillo R es un subanillo de R que atrapa productos. Es decir,*

$$\forall r \in R, \forall i \in I, r \cdot i \in I \text{ y } i \cdot r \in I$$

En esta tesis consideramos únicamente ideales por ambos lados.

Los ideales son a los anillos, lo que los subgrupos normales son a los grupos. El objetivo es introducir en el anillo cociente R/I un producto bien definido. Resulta ser que R/I es un anillo si y sólo si I es un ideal. Por otro lado, dado un homomorfismo de anillos, su kernel es un ideal (Judson, 2022).

Por otro lado, tenemos los teoremas de homomorfismos. Para esta tesis, es relevante el siguiente enunciado, conocido como el teorema de correspondencias:

Teorema 10.4.1. *Sea $\phi : R \to S$ un homomorfismo de anillos y sea $K = ker(\phi)$. Sean:*

$$I = \{\text{ideales de } R \text{ que contienen a } K\} \text{ y } J = \{\text{ideales de } \phi(R)\}$$

Entonces, el mapeo ϕ se extiende a un mapeo $\phi : I \to J$ el cual es una biyección de I a J.(Judson, 2022)

Este teorema nos indica que si X es un ideal de $\phi(R)$, entonces, su preimagen bajo el mapeo ϕ, $\phi(X)^{-1}$ es un ideal de R que contiene al kernel de ϕ.

Ahora, introduciremos una serie de definiciones las cuales son necesarias para entender una cadena de implicaciones que nos será útil.

Definición 10.4.7. *Un **dominio de ideal principal (DIP)** es un dominio entero en el cual todo ideal es **principal**. Esto quiere decir que, dado un ideal I, existe un elemento $a \in R$ tal que I es generado por a, esto se denota por $I = \langle a \rangle$.*

Definición 10.4.8. *Un **dominio Euclideano (DE)** es un dominio entero $(R, +, \cdot)$ dotado de una **función Euclideana***

$$d : R \setminus \{0\} \to \mathbb{Z}^{\geq 0}$$

que satisface:

1. $\forall a, b \in R \setminus 0, d(a) \leq d(ab)$
2. *Si $a, b \neq 0 \in R$ entonces existen $q, r \in R$ tales que: $a = qb + r$ y $r = 0$ o $d(r) < d(b)$.*

Definición 10.4.9. *Un elemento $a \in R \setminus \{0\}$ es una **unidad** si existe $b \in R$ tal que $a \cdot b = 1$. El conjunto de unidades de un anillo se denota por R^**

Definición 10.4.10. *Un elemento $a \in R$ es **irreducible** si cumple que si $a = bc$ entonces, b es una unidad o c es una unidad.*

Definición 10.4.11. *Dos elementos $a, b \in R$son **asociados** si existe una unidad $u \in R^*$ tal que $a = u \cdot b$.*

Definición 10.4.12. *Un **dominio de factorización única (DFU)** es un dominio entero D que satisface las siquientes condiciones:*

- *Si $a \neq 0 \in D$ es no unidad, entonces*

$$a = p_1 \cdots p_n$$

donde n es un entero positivo y cada p_i es irreducible

- *Si*

$$a = p_1 \cdots p_n = q_1 \cdots q_m \tag{10.1}$$

entonces $n{=}m$ y cada p_i es asociado de $q_i, 1 \leq i \leq n$.

Otro resultado importante para esta tesis es la siguiente cadena de implicaciones: Sea R un dominio Euclideano entonces, R es un dominio de ideal principal, lo cual implica también que R es un dominio de factorización única (Judson, 2022). Lo cual se puede representar esquemáticamente por:

$$\text{DE} \Rightarrow DIP \Rightarrow DFU$$

Como mencionamos en el ejemplo 10.4.1, los anillos de polinomios juegan un rol importante en la teoría de Galois. Particularmente, nos interesa el anillo de polinomios sobre un campo. Es decir $F[x] = \{a_0 + a_1x + ... + a_nx^n \mid a_i \in F, n \geq 0\}$, donde F es campo. En este caso tenemos que, si F es campo, entonces $F[x]$ es un dominio Euclideano, donde su función Euclideana es el **grado** del polinomio, el cual denotamos por deg(f(x))(Judson, 2022).

Entonces, al ser $F[x]$ un dominio Euclideano este es a su vez, un dominio de ideal principal y un dominio de factorización única.(Judson, 2022)

Ahora introduciremos ciertas definiciones necesarias para el estudio de las extensiones de campo. Queremos llegar al enunciado que muestra la la existencia y unicidad del polinomio mínimo de un elemento algebraico. Asimismo, enunciaremos el resultado que una extensión de campo es un espacio vectorial sobre el campo subyacente; este resultado nos permite introducir herramientas del álgebra lineal a nuestro estudio. De igual manera, introducimos el concepto de grado de una extensión, el cual es la jerga utilizada en la teoría de campos para referirnos a la dimensión del espacio vectorial mencionado anteriormente. Por último, enunciamos la propiedad multiplicativa de los grados de una extensión.

Definición 10.4.13. *Dados dos campos E, F tales que $F \subseteq E$ decimos que E es una **extensión de campo** de F.*

Definición 10.4.14. *Definimos $F[\alpha] = \{g(\alpha) \mid g(x) \in F[x]\}$, donde $F[x]$ es el anillo de polinomios con coeficientes sobre el campo F, y $F(\alpha)$ como el menor subcampo de E que contiene a $F[\alpha]$.*

Como primer resutlado, tenemos que $F[\alpha]$ es un dominio entero y que $F(\alpha)$ es el campo de cocientes de $F[\alpha]$. (Silverman, 2022)

Definición 10.4.15. *Si $F \subseteq E$, decimos que E es una **extensión simple** de F si $F(\alpha) = E$ para algún $\alpha \in E$. Asimismo, decimos que dicho α es un elemento **primitivo** de E.*

Definición 10.4.16. *Si existe un polinomio no nulo $f \in F[x]$ tal que α es una raíz del mismo, decimos que α es **algebraico sobre F**; en caso contrario decimos que es **trascendental sobre F**.*

Definición 10.4.17. *Por último, una extensión E de F en la cual todos sus elementos son algebraicos es denominada una **extensión algebraica**.*

Definición 10.4.18. *Decimos que un polinomio es **mónico** si su coeficiente principal es 1.*

Definición 10.4.19. *Decimos que un polinomio $f(x)$ es **irreducible** si satisface que, si $f(x) = g(x)h(x)$ entonces $g(x)$ es una unidad o $h(x)$ es una unidad.*

El siguiente resultado nos garantiza la existencia de un polinomio mónico e irreducible para cualquier elemento algebraico de E sobre F que tiene como raíz a dicho elemento.

Teorema 10.4.2. *Sean $F \subseteq F$ y $\alpha \in E$ un elemento algebraico. Entonces existe un único $f \in F[x]$ que satisface:*

1. *f es mónico e irreducible,*
2. *$f(\alpha) = 0$.*

*A dicho polinomio garantizado por el teorema le denominamos el **polinomio mínimo** del elemento y lo denotamos por $mín_F(\alpha)$. (Shariari, 2017)*

Para poder hablar del grado de una extensión, debemos introducir el siguiente teorema.

Teorema 10.4.3. *Sea R un anillo conmutativo con identidad y F campo tales que $F \subseteq R$ y $1_f = 1_R$. Entonces R es un espacio vectorial sobre F. (Silverman, 2022)*

El siguiente teorema nos permite caracterizar los elementos algebraicos y determinar cuándo $F[\alpha] = F(\alpha)$.

Teorema 10.4.4. *Sea L/F una extensión de campo, y sea $\alpha \in L$. Entonces, $F[\alpha] = F(\alpha)$ si y sólo si α es algebraico sobre F. (Silverman, 2022)*

Ahora, enunciamos la propiedad multiplicativa de los grados de las extensiones de campo.

Teorema 10.4.5. *Sean $F \subseteq K \subseteq E$ campos tales que $\mid E : K \mid < \infty$ y $\mid K : F \mid < \infty$. Entonces, $\mid E : F \mid = \mid E : K \mid \cdot \mid K : F \mid$. (Silverman, 2022)*

10.5. Álgebra Lineal

10.5.1. Operadores y el Grupo general lineal

En este anexo, veremos el isomorfismo que existe entre los operadores de un espacio vectorial n-dimensional con el conjunto de matrices de $n \times n, \mathbb{M}(n \times n, \mathbb{F})$. Veremos la existencia de un subespacio especial de dicho conjunto llamado el grupo general lineal de tamaño n sobre el campo subyacente.

Por otro lado, introduciremos el concepto de producto interno y los axiomas que debe satisfacer. De igual manera, veremos que un producto interno induce una norma en el espacio vectorial y enunciaremos los axiomas que debe satisfacer una norma.

Definición 10.5.1. *Dado un espacio vectorial $(V, \mathbb{F}, +, \cdot)$, un mapeo $T : V \to V$ que satisface:*

$$\forall u, v \in V, \forall \alpha, \beta \in \mathbb{F}, T(\alpha \cdot x + \beta \cdot y) = \alpha \cdot T(x) + \beta \cdot T(y)$$

*es un **operador**. El conjunto de todos los operadores es denominado por $L(V)$.*

Como primer resultado, tenemos que $L(V)$ es un espacio vectorial sobre el campo $\mathbb{F}$, con la suma definida por:

$$T, S \in L(V), x \in V \text{ entonces } (T + S)(x) = T(x) + S(x)$$

Y el producto por un escalar:

$$\alpha \in \mathbb{F}, T \in L(V), x \in V \text{ entonces } (\alpha \cdot T)(x) = \alpha \cdot T(x) \text{(Taylor, 2020)}$$

Definición 10.5.2. *En particular, si T es un operador es biyectivo, decimos que es un **isomorfismo**. El conjunto de todos los isomorfismos de un espacio vectorial V sobre sí mismo, es denominado el **Grupo general lineal de V**, denotado por $Gl(V)$ por sus cifras en inglés (general linear group).*

Definición 10.5.3. *Sea $W \subseteq V$ no vacío. Decimos que W es un **subespacio** de V si W es un espacio vectorial sobre el campo subyacente con las operaciones inducidas por V. Lo cual es denotado por $W \leq V$*

Resulta ser que $GL(V)$ es un subespacio de $L(V)$. Entonces, en particular, $GL(V)$ es un grupo con la suma de operadores (Taylor, 2020).

Cuando trabajamos en un espacio vectorial n-dimensional, como es el caso a lo largo de esta tesis, existe un isomorfismo entre el espacio de operadores $L(V)$ y el espacio de matrices de $n \times n, \mathbb{M}(n \times n, \mathbb{F})$. Al ser $GL(V) \leq L(V)$, tenemos que $GL(V)$ es isomorfo al subespacio de todas las matrices invertibles, i.e., al subespacio de todas las matrices con determinante no nulo . Por otro lado, tenemos los operadores unitarios, los cuales satisfacen, en el caso finito dimensional, que su adjunta sea el inverso del operador, i.e., si $T \in L(V)$, entonces

$$T^* = T^{-1} \text{ (Taylor, 2020).}$$

10.5.2. Espacios con producto interno y norma

Dado un espacio vectorial $(V, \mathbb{C}, +, \cdot)$ podemos dotarlo de un producto interno, el cual nos permite, a su vez, dotarlo de una norma.

Definición 10.5.4. *Un **producto interno** en un espacio vectorial sobre los complejos es una función $\langle ., . \rangle : V \times V \to \mathbb{C}$ que satisface los siguientes axiomas:*

1. $\forall \alpha, \beta \in \mathbb{C}, \forall x, y, z \in V, \langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle$,
2. $\forall x, y \in V, \langle x, y \rangle = \overline{\langle y, x \rangle}$,
3. $\forall x \in V, \langle x, x \rangle \geq 0$ *tal que* $\langle x, x \rangle = 0$ *si y sólo si* $x = 0$.

Dado un producto interno, podemos inducir una norma en el espacio.

Definición 10.5.5. *Definimos una **norma** en un espacio vectorial con producto interno sobre los complejos como:*

$$\forall x \in V, \|x\| = \sqrt{\langle x, v \rangle}.$$

La cual satisface los siguientes axiomas:

1. *Si* $x \neq 0 \in V$ *entonces* $\|x\| > 0$,
2. $\forall \alpha \in \mathbb{C}, \forall x \in V, \|\alpha x\| = \mid \alpha \mid \|x\|$,
3. $\forall x, y \in V, \|x + y\| \leq \|x\| + \|y\|$.

Definición 10.5.6. *En un espacio de producto interno, decimos que un operador $T \in L(V)$ es una **isometría** si*

$$\forall v \in V, \ \|Tv\| = \|v\|.$$

Entonces, en un espacio de producto interno, podemos caracterizar los operadores unitarios como isometrías (Taylor, 2020).

Definición 10.5.7. *Dado un subespacio lineal $W \leq V$, decimos que el **complemento ortogonal** es el conjunto*

$$W^{\perp} := \{y \in V \mid \forall w \in W, \langle w, y \rangle = 0\}.$$

La siguiente descomposición es un resultado importante que nos servirá para la prueba del Teorema de Maschke. Dado un subespacio $W \leq V$, podemos descomponer el espacio vectorial V como el siguiente producto directo:

$$V = W \oplus W^{\perp}.\text{(Taylor, 2020)}$$