UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Representaciones de grupos finitos y teoría de caracteres

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

P R E S E N T A :

Arturo López González

DIRECTOR DE TESIS:
Dra. Diana Avella Alaminos

Ciudad Universitaria, Cd. Mx., 2016

Representaciones de Grupos Finitos y Teoría de Caracteres

Arturo López González

22 de septiembre de 2016

Dedicado a mis padres

Índice general

Introducción

El estudio de las simetrías de un objeto geométrico, de partículas, moléculas, o sistemas (en general) lleva naturalmente a estudiar las realizaciones concretas de un grupo como un conjunto de matrices. El presente trabajo está basado principalmente en [13], en donde se hace la teoría de representaciones únicamente en términos del álgebra lineal (aunque al final termina en términos de la teoría de módulos) y la teoría de grupos finitos, de la cual, la herramienta que utilizaremos con más frecuencia y a lo largo de todo el trabajo, es el concepto de *acción* de un grupo G en un conjunto X con la propiedad de ser un espacio vectorial sobre algún campo. Así, teniendo una estructura adicional a la de G-conjunto, podemos hacer compatibles ambas estructuras algebraicas para dar origen al concepto de *acción lineal*, que como dijimos, es una forma hacer compatible la estructura de espacio vectorial dimensionalmente finito sobre un campo y la acción del grupo. Así, en lo que haremos estaremos usando *hibridaciones* de estructuras algebraicas.
Por otra parte, en [2] tenemos la visión moderna de la teoría de representaciones: los módulos finitamente generados sobre álgebras de grupo que se debe principalmente a E. Noether. Esta visión permite tratar de manera unificada problemas diversos, que van desde el estudio de formas cuadráticas hasta problemas de clasificación de sistemas de ecuaciones diferenciales, o los mencionados anteriormente.

Los grupos surgen en las matemáticas como conjuntos de simetrías de un objeto, por ejemplo S_n es el grupo de permutaciones de n letras o n símbolos, A_n es el grupo de permutaciones de n letras que preservan la paridad y $O(3)$ es el grupo de transformaciones rígidas (que fijan el origen) en el espacio euclideano, D_{2n} aparece como las simetrías de un polígono regular de n lados, etc, así, ya se ha respondido a una pregunta surgida desde la geometría ¿dado un objeto geométrico cuál es su grupo de simetrías? Pero la teoría de representaciones hace esta pregunta al revés: ¿Dado un grupo cualquiera, en qué objetos actúa? Para responderla habrá que clasificar tales objetos.
Una representación es una relación muy general que expresa similitudes entre objetos, es decir, una colección de objetos puede ser representada por otra colección de objetos, en nuestro caso, queremos ver a los grupos como conjuntos abstractos de matrices invertibles (o de operadores lineales).
Entonces, la idea básica de la teoría de representaciones de grupos finitos es poder visualizar a los grupos como operadores lineales en un espacio vectorial de dimensión finita. Y claro, si algo se va a ver o pensar como un grupo, en ese algo los elementos deben ser invertibles pues de lo contrario no tendríamos una buena identificación de ese algo con el grupo, así, se trabajará con isomorfismos de espacios vectoriales que se codifican (se ven) como matrices invertibles en el caso de dimensión

finita, por lo que la teoría de representaciones nos lleva a estudiar los morfismos de grupos abstractos a grupos de automorfismos de espacios vectoriales, y estos morfismos producen invariantes que son números cuyas propiedades aritméticas ayudan a obtener cierta información del grupo. Para todo lo que haremos consideraremos siempre espacios vectoriales de dimensión finita, y por lo tanto, una representación nos dará una manera de pensar a cada elemento de un grupo como una matriz invertible. Así, en el contexto de la teoría de representaciones los grupos son considerados como conjuntos abstractos de operadores lineales en un espacio vectorial de dimensión finita, que forman un álgebra, y si el grupo ya se ve dentro de un álgebra, es natural preguntarse cómo se puede extender el grupo a un álgebra, y esto nos llevará a la construcción del álgebra de grupo, que corresponde a esa forma de considerar al grupo como un subconjunto de un álgebra. La construcción del álgebra de grupo simplemente se hará considerando a los elementos del grupo como la base de un espacio vectorial.

El trabajo se divide en tres capítulos, el primero está dedicado a recordar conceptos y resultados básicos (que estaremos usando constantemente) de la teoría de grupos, la teoría de anillos, el álgebra lineal y la teoría de módulos, algunos son mencionados sin prueba ya que el trabajo requiere del conocimiento previo de los mismos.

El segundo capítulo abarca los fundamentos de la teoría de representaciones de grupos finitos, en la que pensaremos a los elementos de cualquier grupo finito G como matrices (u operadores lineales en un $\mathbb{F}$-espacio vectorial de dimensión finita V) mediante un morfismo de grupos y esa forma de ver a los elementos del grupo, nos llevará a definir una acción del grupo G en el espacio vectorial V correspondiente y ésta será compatible con la estructura de espacio vectorial. El grupo, más precisamente, sus elementos, serán la base de cierto espacio vectorial llamado el álgebra de grupo y será particularmente importante para lo que haremos, y en este espacio buscaremos una descomposición en subespacios que además de heredar la acción del grupo tendrán la propiedad de la irreducibilidad, así, bastará estudiar a estos subespacios para tener una visión completa de lo que sucede con espacios vectoriales en los que se tenga además una estructura adicional de G-conjunto. Estudiaremos en esta parte también los morfismos entre espacios vectoriales en los cuales actúe el grupo G y nos darán información acerca de la descomposición del álgebra de grupo como una suma directa de los subespacios mencionados anteriormente y con ayuda de ellos, clasificaremos a todos los espacios vectoriales (salvo isomorfismo) en los cuales exista además una acción del grupo compatible con la estructura de espacio vectorial.

Por último, el tercer capítulo consiste de los resultados fundamentales de la teoría de caracteres de grupos finitos que empezó a ser desarrollada en 1896 por Frobenius y algunos otros. La idea es asociar una función del grupo en los complejos (llamada un carácter del grupo) a un morfismo del grupo en el grupo general lineal de grado finito, asignando la traza de la matriz correspondiente al elemento del grupo bajo el morfismo, además esta asignación será constante en clases de conjugación del grupo y esa propiedad tendrá una conexión importante con el número de factores irreducibles en la descomposición del álgebra de grupo. Además los caracteres nos ayudarán a determinar cuándo dos representaciones son equivalentes y la irreducibilidad de representaciones también puede ser determinada por propiedades aritméticas de los caracteres.

Preliminares

Operaciones Binarias

Definición 0.1. *Sea $X \neq \emptyset$ un conjunto, una* ***operación binaria en*** *X es una función*

$$\begin{aligned} * : X \times X &\longrightarrow X \\ (x, y) &\longmapsto *(x, y) \ , \end{aligned}$$

donde $*(x, y)$ se denota como $x * y$. Se dice que la operación $*$ es una operación cerrada para indicar que cada vez que se opera una pareja de elementos $x, y \in X$ se obtiene un elemento $x * y$ de X (pero debe ser cerrada pues $*$ es una función con codominio X y así $x * y \in X$).
Diremos que una operación binaria $*$ es ***asociativa*** *si para todos $x, y, z \in X$ se tiene que $x*(y*z) = (x*y)*z$. Un elemento $e \in X$ es llamado* ***identidad izquierdo*** *con respecto a $*$ si para todo $x \in X$ se tiene que $e * x = x$. Análogamente, un elemento $e \in X$ es llamado* ***identidad derecho*** *con respecto a $*$ si para todo $x \in X$ se tiene que $x * e = x$. También, $e \in X$ es un* ***elemento identidad*** *de X con respecto a $*$ si para todo $x \in X$ se tiene que $e * x = e = x * e$, es decir, e es identidad izquierdo e identidad derecho con respecto a la operación $*$.*
Diremos que la operación binaria $*$ es ***conmutativa*** *si para todos $x, y \in X$ se tiene que $x*y = y*x$. Si $e \in X$ es un elemento identidad con respecto a $*$ si y $x \in X$, decimos que $y \in X$ es* ***un inverso de*** *x si $x * y = e = y * x$.*

Observación 0.2. Todas las **estructuras algebraicas** con las que trabajaremos dependen de la existencia de al menos una operación binaria asociativa en un conjunto no vacío, la asociatividad es la mínima condición que pediremos a una operación binaria para definir una estructura algebraica.

Observación 0.3. Si $X \neq \emptyset$ es un conjunto y $*$ es una operación binaria asociativa en X, es fácil ver que si existe un elemento identidad respecto a $*$ entonces es único, de igual forma, si algún elemento tiene un inverso respecto a $*$ entonces también es único.

Definición 0.4. *Sea $X \neq \emptyset$ un conjunto. Decimos que $(X, *)$ es un* ***semigrupo*** *si $*$ es una operación binaria asociativa en X, decimos que X es un* ***monoide*** *si $*$ es una operación binaria asociativa y existe un elemento identidad con respecto a $*$.*

No trabajaremos con estas estructuras, pero agregando una condición sobre la operación $*$ tendremos la estructura algebraica con menos propiedades con la que trabajaremos.

Grupos

Definición 0.5. *Sea $G \neq \emptyset$ un conjunto. Decimos que $(G, *)$ es un* ***grupo*** *si $*$ es una operación binaria asociativa en G, si existe un elemento identidad e_G en G con respecto a $*$ y si existe para cada elemento $g \in G$ un inverso de g con respecto a la operación $*$. Si la operación $*$ es conmutativa decimos que G es un* ***grupo abeliano****.*

Por la observación 0.3 en un grupo tanto el neutro como los inversos son únicos, al inverso de cada elemento $g \in G$ se le denota por g^{-1}. Si la operación $*$ es un producto y $x, y \in G$, es usual escribir $x * y = xy$, pero si es una suma, no se omite el signo de suma, además en este caso, el neutro del grupo se denota por 0 en lugar de e_G y los inversos en vez de x^{-1} se escriben como $-x$.
En un grupo son válidas las **leyes de cancelación**, es decir, si $xa = xb$ simplemente multiplicamos por x^{-1} a la izquierda en la igualdad y entonces $a = b$ (ley de cancelación izquierda). Análogamente se obtiene la ley de cancelación derecha.
El **orden de un grupo** G se define como el número de elementos que tiene y se denota por $|G|$. Un grupo es finito si tiene una cantidad finita de elementos, y es infinito en caso contrario.

Subgrupos y ejemplos de grupos

Definición 0.6. *Sea G un grupo. Un subconjunto $H \subseteq G$ es un* ***subgrupo*** *de G, denotado por $H \leq G$, si es por sí mismo un grupo con la restricción a H de la operación binaria en G. Si H está contenido propiamente en G decimos que es un* ***subgrupo propio*** *de G y se denota por $H < G$.*

Observación 0.7. $H \leq G$ si y sólo si $e_G \in H$, para todos $x, y \in H$ se tiene que $xy \in H$ y para todo $x \in H$ se tiene que $x^{-1} \in H$.

Todo grupo G tiene al menos dos subgrupos, $\{e_G\}$ y G llamados los **subgrupos triviales**. Todo subgrupo de un grupo finito G es finito, sin embargo, en un grupo infinito G siempre hay subgrupos de orden finito y de orden infinito, al menos los triviales. También todo subgrupo de un grupo abeliano es abeliano, pero grupos no abelianos siempre tienen subgrupos abelianos y no abelianos. La relación ser subgrupo de G, que denotamos por $\leq$, es un orden parcial en la familia de los subgrupos de G. La intersección de una familia arbitraria subgrupos es subgrupo, y la unión de dos subgrupos es subgrupo si y sólo si alguno de ellos está contenido en el otro.

Para todos $k \in \mathbb{Z}^+$, $x \in G$, x^k es el producto de x consigo mismo k veces y $x^{-k} = (x^{-1})^k$ es el producto de x^{-1} consigo mismo k veces, se define $x^0 = e_G$, así, de forma *recursiva o inductiva*, $x^{k+1} = x^k x$. Si el grupo es aditivo, entonces x^k se denota por kx, que es la suma de x consigo mismo k veces, de forma similar, $-kx$ es la suma de $-x$ consigo mismo k veces. En un grupo son válidas las **leyes de los exponentes**, es decir, para todos $x \in G$ y $m, n \in \mathbb{Z}$ tenemos que

$$x^m x^n = x^{m+n} \text{ y } x^{mn} = (x^m)^n.$$

Un elemento $x \in G$ es un **elemento de orden finito** si existe $m \in \mathbb{N}^+$ tal que $x^m = e_G$, al menor natural que cumpla lo anterior se le llama **el orden de** x. Un elemento $x \in G$ es de orden finito n si y sólo si $e_G, x, x^2, \ldots, x^{n-1}$ son todos distintos y $e_G = x^n$. Decimos que $x \in G$ es un **elemento de orden infinito** para todo $m \geq 1 \in \mathbb{N}$ se tiene que $x^m \neq e_G$, es decir, ninguna potencia con

exponente positivo de x se anula. En un grupo el único elemento de orden 1 es e_G. Si el único elemento de orden finito en un grupo es el neutro se dice que el grupo es **libre de torsión**. Si $x \in G$, entonces el conjunto

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} \subseteq G$$

es un subgrupo de G (por las leyes de los exponentes) llamado el **subgrupo cíclico generado por** x. Si G es un grupo, decimos que es un **grupo cíclico** si G es generado por un elemento, es decir, existe $g \in G$ tal que $G = \langle g \rangle$ y llamamos a g un **generador** de G. Una consecuencia más de las leyes de los exponentes es que todo grupo cíclico es abeliano. También todos los subgrupos de un grupo cíclico son cíclicos. Si $G = \langle x \rangle$ es cíclico infinito todas las potencias enteras de x son distintas y es un grupo abeliano libre de torsión. Si $g \in G$ tiene orden finito n el conjunto

$$\langle g \rangle = \{e_G, g, g^2, \ldots, g^{n-1}\}$$

es un subgrupo de orden finito n. Si $G = \langle x \rangle$ es cíclico finito de orden n debe tener un elemento generador de orden n, y el recíproco es cierto, si G es finito y existe un elemento de orden igual que $|G|$, entonces G es cíclico.
Todo elemento en un grupo finito tiene orden finito menor o igual que $|G|$ pues de lo contrario el subgrupo cíclico generado tendría más elementos que G. Generalizando la idea del subgrupo cíclico generado por un elemento tenemos lo siguiente.

Definición 0.8. *Sea G un grupo y $X \subseteq G$. El **subgrupo generado** por X es el conjunto*

$$\langle X \rangle = \bigcap_{H \leq G, X \subseteq H} H,$$

es decir, la intersección de todos los subgrupos de G que contienen a X.

Por ser intersección de subrupos, $\langle X \rangle$ es un subgrupo de G y es el menor subgrupo de G que contiene a X (por ser la intersección de los subgrupos que contienen a X, $\langle X \rangle$ está contenido en todos, es el menor en este sentido) y por lo tanto, si $X \leq G$ entonces $\langle X \rangle = X$. Si $X = \{x\}$, entonces escribimos $\langle x \rangle$ en lugar de $\langle X \rangle$, que es el cíclico generado por x, de forma similar, si $X = \{x_1, \ldots, x_n\}$ escribimos $\langle x_1, \ldots, x_n \rangle$ en lugar de $\langle X \rangle$. Otra forma equivalente de pensar a $\langle X \rangle$ es como el conjunto que consiste de e_G y de todas las **palabras** formadas por elementos de X y sus inversos, es decir,

$$\langle X \rangle = \{e_G,\ {x_1}^{\alpha_1} \cdots {x_r}^{\alpha_r} \mid r \in \mathbb{N}^+, x_i \in X, \alpha_i = \pm 1\ \forall\ i\}.$$

Ejemplo 0.9. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ y $(\mathbb{C}, +)$, donde $+$ es la suma usual, son grupos abelianos, además tenemos la cadena de subgrupos

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +).$$

Más aún, $(\mathbb{Z}, +)$ es el ejemplo canónico de un grupo cíclico infinito, tiene como únicos generadores a ± 1. Todos sus subgrupos deben ser cíclicos generados por una potencia de 1, es decir, por un elemento de la forma $n \cdot 1 = n$, por lo tanto son de la forma

$$H = n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\} = \langle n \rangle = \text{los múltiplos de } n.$$

También se puede probar que $(\mathbb{Q}, +)$ no es cíclico.

Ejemplo 0.10. $\mathbb{Z}^* := (\{\pm 1\}, \cdot)$, $\mathbb{Q}^* := (\mathbb{Q} - \{0\}, \cdot)$, $\mathbb{R}^* := (\mathbb{R} - \{0\}, \cdot)$ y $\mathbb{C}^* := (\mathbb{C} - \{0\}, \cdot)$, donde $\cdot$ es el producto usual, son grupos abelianos y tenemos las inclusiones

$$\mathbb{Z}^* \leq \mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*.$$

Tenemos otro ejemplo si restringimos el grupo $\mathbb{R}^* := (\mathbb{R} - \{0\}, \cdot)$ al conjunto de los números reales positivos $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$, es decir, $(\mathbb{R}_{>0}, \cdot)$ es un grupo llamado el **grupo multiplicativo los números reales positivos**.

Ejemplo 0.11. Para $n \geq 2$, el conjunto de los **enteros módulo** n

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

con la suma $[a] + [b] := [a + b]$ es el ejemplo canónico de un grupo cíclico finito de orden n y es generado canónicamente por $[1]$, tiene otros generadores que son las clases $[a]$ tales que $1 \leq a < n$ y $(a, n) = 1$.

Ejemplo 0.12. Para $n \geq 2$ sea ${\mathbb{Z}_n}^* := \{[a] \in \mathbb{Z}_n \mid 1 \leq a <$ y $(a, n) = 1\}$ el conjunto de los enteros no negativos menores que n y primos relativos con n. Entonces ${\mathbb{Z}_n}^*$ es un grupo con el producto (módulo n) definido como $[a][b] := [ab]$.

Ejemplo 0.13. El **círculo unitario**

$$\mathbb{S}^1 := \{z \in \mathbb{C}^* \mid |z| = 1\} \subset \mathbb{C}$$

con el producto usual de números complejos es un grupo abeliano.

Ejemplo 0.14. Para $n \geq 2$ el conjunto de las **raíces n-ésimas de la unidad**

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{\frac{2\pi i k}{n}} \mid 0 \leq k \leq n-1\} \subset \mathbb{S}^1 \subset \mathbb{C}^*$$

es un grupo abeliano con el producto usual de números complejos.

Ejemplo 0.15. Sea $X \neq \emptyset$ un conjunto, entonces el conjunto

$$S_X = \{f : X \longrightarrow X \mid f \text{ es biyectiva } \}$$

es un grupo con la composición de funciones como operación binaria ya que la composición es una operación cerrada pues la composición de funciones biyectivas es biyectiva, además la composición es asociativa, la función $id_X(x) = x$ para todo $x \in X$ es una función biyectiva y es el neutro para este grupo; por último cada función biyectiva f tiene una inversa f^{-1} que es su inverso respecto a la composición. El grupo S_X es llamado **el grupo simétrico de X o el grupo de permutaciones de X**. Si $X = \{1, 2, \ldots, n\} := n_{\leq}$, entonces escribiremos $S_X = S_n$ y decimos que S_n es el **grupo de permutaciones de n letras**. Si $|X| = n < \infty$, donde $|\ \ |$ denota al cardinal de X, entonces para $n \geq 3$ tenemos que S_X es no abeliano. Además S_n tiene un subgrupo dado por

$$A_n = \{\alpha \in S_n \mid \alpha \text{ es par } \}$$

llamado el **grupo alternante de n letras**.

Ejemplo 0.16. Producto directo. Si G y H son grupos, entonces podemos dar estructura de grupo al producto cartesiano $G \times H$ con la operación entrada a entrada. En general, podemos considerar un número finito de grupos $G_1, \ldots, G_k$ y tomando su producto cartesiano $G = \prod_{i=1}^{k} G_i$ definimos la operación

$$(a_1, \ldots, a_k)(b_1, \ldots, b_k) = (a_1 b_1, \ldots, a_k b_k).$$

y llamamos a G el **producto directo externo** de $G_1, \ldots, G_k$.

Ejemplo 0.17. El conjunto de matrices invertibles de $n \times n$ con entradas en $\mathbb{R}$

$$GL_n(\mathbb{R}) = \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) \mid det(A) \neq 0\}$$

es un grupo con el producto usual de matrices llamado el **grupo general lineal**. Este tiene un subgrupo llamado el **grupo especial lineal** dado por

$$SL_n(\mathbb{R}) = \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) \mid det(A) = 1\}.$$

En el ejemplo anterior puede sustituirse a los números reales por los números complejos $\mathbb{C}$.

Ejemplo 0.18. Para todo grupo G y cualquier subconjunto $X \subseteq G$, el conjunto

$$C_G(X) = \{g \in G \mid gx = xg \ \forall \ x \in X\},$$

es decir, de los elementos del grupo que conmutan con todos los elementos de X es un subgrupo de G llamado el **centralizador** de X en G.

Ejemplo 0.19. Para cualquier conjunto $X \neq \emptyset$, si $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ es la potencia de X y $\triangle$ es la diferencia simétrica de conjuntos, es decir, $A \triangle B := (A - B) \cup (B - A)$, entonces $(\mathcal{P}(X), \triangle)$ es un grupo abeliano pues $\triangle$ es cerrada, asociativa y conmutativa en $\mathcal{P}(X)$, el conjunto $\emptyset$ es el elemento neutro de este grupo y para cada $A \subseteq X$ su inverso respecto a $\triangle$ es él mismo.

Ejemplo 0.20. Grupo dihédrico. Consideremos un cuadrado en el plano euclideano con vértices

$$1 = (1, 1), 2 = (-1, 1), 3 = (-1, -1) \text{ y } 4 = (1, -1).$$

Podemos preguntarnos por sus simetrías, que no es más que un subconjunto del grupo de simetrías de 4 letras, pues una simetría del cuadrado mueve a lo más 4 letras, sus 4 vértices, y estas simetrías consisten de rotaciones respecto al origen (hay 4 de ellas) y reflexiones respecto a las diagonales y respecto a los ejes coordenados, éstas son también 4, más claramente éstas son:

1. $r_0 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{smallmatrix}\right) = (1) = 1$ es la rotación de cero grados.
2. $r_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{smallmatrix}\right) = (1234) = x$ es la rotación de 90 grados (multiplicar por i).
3. $r_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix}\right) = (13)(24) = x^2$ es la rotación de 180 grados.
4. $r_3 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{smallmatrix}\right) = (1432) = x^3$ es la rotación de 270 grados.
5. $m_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{smallmatrix}\right) = (12)(34) = y$ es la reflexión en el eje Y.
6. $m_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{smallmatrix}\right) = (14)(23) = x^2 y$ es la reflexión en el eje X.
7. $d_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{smallmatrix}\right) = (13) = xy$ es la reflexión respecto a la gráfica de la identidad negativa.

8. $d_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 1 \end{smallmatrix}\right) = (24) = x^3y$ es la reflexión respecto a gráfica de la identidad.

y forman un grupo llamado el **grupo dihédrico de orden** 8 y lo escribiremos como

$$D_8 = \langle x, y \mid x^4 = 1, y^2 = 1, xy = yx^{-1} \rangle.$$

Generalizando este ejemplo, para cualquier $n \geq 3$ podemos considerar el conjunto de simetrías de un polígono regular de n lados en el plano y éste forma un grupo llamado el grupo dihédrico de orden $2n$, dado por

$$D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, xy = yx^{-1} \rangle.$$

donde $x = r_{\frac{2\pi}{n}} = \begin{pmatrix} cos(\frac{2\pi}{n}) & -sen(\frac{2\pi}{n}) \\ sen(\frac{2\pi}{n}) & cos(\frac{2\pi}{n}) \end{pmatrix}$ es la rotación por el ángulo $\frac{2\pi}{n}$ y y es alguna reflexión que depende de la paridad de n, si n es par entonces D_{2n} contiene las $\frac{n}{2}$ reflexiones con respecto a las bisectrices de sus ángulos internos (sólo hay $\frac{n}{2}$ de éstas) y las $\frac{n}{2}$ reflexiones con respecto a las bisectrices de sus lados (también hay $\frac{n}{2}$ de éstas), si n es impar entonces D_{2n} contiene las n reflexiones con respecto a las bisectrices de sus ángulos internos (hay n de éstas).

Ejemplo 0.21. Cuaterniones. Consideremos el grupo de orden 8 dado por

$$Q = \{\pm 1, \pm i, \pm j, \pm k\},$$

cuyas reglas de multiplicación son

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$

Q es llamado el **grupo de cuaterniones**.

Clases laterales

Si $x \in G$ y $H \leq G$ entonces denotamos al conjunto $\{x\}H = \{xh \mid h \in H\}$ simplemente como xH y le llamamos a xH la **clase lateral izquierda** de x en H (se pueden considerar las clases laterales derechas Hx), el nombre de clase proviene del hecho de que ese conjunto consiste de la clase de equivalencia de x de la siguiente relación de equivalencia en G: $x, y \in G$ están relacionados (módulo H) si y sólo si $y^{-1}x \in H$, y el conjunto de clases de equivalencia de esta relación de equivalencia se conoce como el conjunto cociente de G por H y se denota por G/H.
Usamos clases laterales izquierdas pues todo lo que haremos en este trabajo será *por el lado izquierdo*.
Además existe una correspondencia biyectiva entre las clases laterales izquierdas y las clases laterales derechas de H en G mediante la función

$$\begin{array}{rcl} f : \{aH \mid a \in G\} & \longrightarrow & \{Ha \mid a \in G\} \\ xH & \longmapsto & (Hx)^{-1} = Hx^{-1} \end{array}$$

que está bien definida y es una biyección. Cualesquiera dos clases laterales son la misma o son ajenas pues generan una partición en G, entonces cada elemento $x \in G$ pertenece exactamente a una clase lateral, xH y también existe una correspondencia biyectiva entre H y xH dada por $h \longmapsto xh$.
El **índice** de H en G se denota por $[G : H]$ y se define como el número de clases laterales de H en G, si hay un número infinito de ellas entonces se le asigna al índice un número cardinal apropiado y se define el orden del grupo como el número cardinal $[G : \{e_G\}]$.

Si G es finito las clases laterales de H en G son un partición de G en $[G:H]$ conjuntos de cardinalidad igual a $|H|$ y entonces todo subgrupo tiene índice finito y está dado por $[G:H] = \frac{|G|}{|H|}$. Este último argumento es realmente la demostración del primer teorema importante de la teoría de grupos finitos:

Teorema 0.22. ***Teorema de Lagrange.***
Sea G un grupo finito y $H \leq G$. Entonces el orden de H es divisor del orden de G. ■

Así, si queremos encontrar los subgrupos de un grupo basta determinar qué posibles órdenes pueden tener, pues éstos deben ser divisores del orden del grupo.
Una consecuencia directa del Teorema de Lagrange es que los **grupos de orden primo son cíclicos** ya que si un grupo tiene orden primo, entonces cada elemento distinto del neutro tiene orden un divisor no trivial del orden del grupo, y ya que éste es primo, cada elemento tiene el orden igual al orden del grupo y por lo tanto un grupo de orden primo es cíclico generado por cada elemento distinto del neutro del grupo.
Cada vez que se tiene algún resultado es usual preguntarse si el *recíproco* es cierto, en este caso, nos hacemos la pregunta: ¿si G es un grupo finito y m es un divisor del orden de G, entonces existe $H \leq G$ de orden m? que es el recíproco del Teorema de Lagrange y se cumple para grupos cíclicos y para grupos abelianos en general. Un recíproco parcial es buscado y la búsqueda de la solución a este problema ayudó a desarrollar la teoría de grupos finitos, es decir, ¿para que divisores m del orden de G existe $H \leq G$ tal que el orden de H es m?.

Definición 0.23. *Sea G un grupo y $x, y \in G$. Decimos que y es **conjugado** de x si existe $g \in G$ tal que $y = gxg^{-1}$. Si $H \leq G$, decimos que H es un **subgrupo normal** de G, y lo denotaremos por $H \trianglelefteq G$, si H es **cerrado bajo conjugación**, es decir, si para todos $h \in H$ y $x \in G$ se tiene que $xhx^{-1} \in H$, o de forma equivalente, $xH = Hx$.*

Los subgrupos normales se escriben usualmente con la letra N. En un grupo existen al menos dos subgrupos normales, los triviales. Si un grupo no tiene subgrupos normales además de los triviales decimos que es un **grupo simple**. En un grupo abeliano todo subgrupo es normal.
Si $N \trianglelefteq G$, el cociente G/N tiene una buena definición de operación binaria heredada de la operación binaria en G dada por $(aN)(bN) = abN$ que otorga a G/N una estructura de grupo donde $N = e_{G/N}$ y el inverso de aN es $a^{-1}N$, llamamos a G/N el **grupo cociente o grupo factor** de G por N.
Si G es abeliano, entonces G/H es abeliano. También, si G es cíclico y $H \leq G$ entonces G/H es cíclico.

Ejemplo 0.24. El **grupo conmutador** de un grupo G es el subgrupo

$$G' = \langle\ [g,h]\ \mid g, h \in G\ \rangle,$$

donde $[g,h] = ghg^{-1}h^{-1}$ es llamado el **conmutador** de g y h. Además $G' \trianglelefteq G$.
Si $N \trianglelefteq G$, entonces

$$G' \leq N \text{ si y sólo si } G/N \text{ es abeliano.}$$

En particular G/G' es abeliano. De aquí tenemos que el conmutador de un grupo es el menor subgrupo normal con grupo cociente abeliano.

Morfismos de grupos.

Definición 0.25. *Sean G y $\tilde{G}$ grupos y $\varphi : G \longrightarrow \tilde{G}$ una función. Decimos que φ es un* ***morfismo de grupos*** *si para todos $x, y \in G$ se tiene que $\varphi(xy) = \varphi(x)\varphi(y)$. Si φ es un morfismo de grupos y es inyectivo decimos que es un* ***monomorfismo de grupos****, si es suprayectivo diremos que es un* ***epimorfismo de grupos****, si es biyectivo diremos que es un* ***isomorfismo de grupos*** *y se denotará por $G \cong \tilde{G}$.*

En otras palabras, una función es un morfismo de grupos si respeta las operaciones de ambos grupos, como consecuencia también respeta neutros e inversos, es decir, todo morfismo de grupos $\varphi : G \longrightarrow \tilde{G}$ asigna al neutro de G el neutro de $\tilde{G}$ y al inverso de cada elemento le asigna el inverso de la imagen del elemento. Para cualquier morfismo de grupos $\varphi : G \longrightarrow \tilde{G}$ tenemos asociados los conjuntos

$$Ker(\varphi) := \{g \in G \mid \varphi(g) = e_{\tilde{G}}\} \subseteq G \text{ y } Im(\varphi) := \{\varphi(g) \in \tilde{G} \mid g \in G\} \subseteq \tilde{G}$$

que son llamados **el núcleo** y **la imagen** de φ respectivamente y de hecho, es fácil ver que

$$Ker(\varphi) \trianglelefteq G \text{ y } Im(\varphi) \leq \tilde{G}.$$

En términos de los conjuntos anteriores podemos pensar las condiciones de inyectividad y suprayectividad para un morfismo de grupos $\varphi : G \longrightarrow \tilde{G}$ como sigue: φ es inyectivo si y sólo si $Ker(\varphi) = \{e_G\}$ y φ es suprayectivo si y sólo si $Im(\varphi) = \tilde{G}$.

Ejemplo 0.26. Sea G un grupo y $N \trianglelefteq G$. Entonces existe un epimorfismo de grupos

$$\begin{array}{rcl} \pi : G & \longrightarrow & G/N \\ g & \longmapsto & gN \end{array}$$

con $N = Ker(\pi)$, y es llamado el **epimorfismo canónico o la proyección natural**.
La existencia de π muestra que todo subgrupo normal es el núcleo de un epimorfismo de grupos y que todo grupo cociente es la imagen de un epimorfismo de grupos.

Teorema 0.27. ***Primer teorema de isomorfismo de grupos.***
Sean $G, \tilde{G}$ grupos y $\varphi : G \longrightarrow \tilde{G}$ un morfismo de grupos con $K = Ker(\varphi)$. Entonces existe un isomorfismo de grupos $G/K \cong Im(\varphi)$ dado por

$$\begin{array}{rcl} \widehat{\varphi} : G/K & \longrightarrow & Im(\varphi) \subset \tilde{G} \\ gK & \longmapsto & \varphi(g). \end{array}$$

El isomorfismo $\widehat{\varphi}$ es inducido por el morfismo φ y es canónico en el sentido de que es natural definir así la regla de correspondencia de $\widehat{\varphi}$. Además satisface que $\widehat{\varphi} \circ \pi = \varphi$.

Ejemplo 0.28. Para cualquier grupo G las funciones

$$\begin{array}{rcl} id_G : G & \longrightarrow & G \\ g & \longmapsto & g \end{array} \quad \text{y} \quad \begin{array}{rcl} \varphi_{e_G} : G & \longrightarrow & G \\ g & \longmapsto & e_G \end{array}$$

son morfismos de grupos llamados el **morfismo identidad** y el **morfismo trivial** respectivamente, y entonces inducen isomorfismos $G/\{e_G\} \cong G$ y $G/G \cong \{e_G\}$ respectivamente.

Observación 0.29. Si φ es un isomorfismo, su inversa $\varphi^{-1} : G' \longrightarrow G$ es también un morfismo de grupos. Luego, ya que la composición de funciones biyectivas es biyectiva y que fácilmente se ve que la composición de morfismos de grupos es un morfismo de grupos, entonces la composición de isomorfismos es un isomorfismo, esto junto con la existencia del morfismo identidad muestran que en la clase de todos los grupos tenemos la relación de equivalencia, $\cong$, *ser isomorfo*. Los isomorfismos son muy útiles pues nos permiten trabajar de manera más cómoda con identificaciones más sencillas de grupos dados.

Ejemplo 0.30. El grupo multiplicativo los números reales positivos $(\mathbb{R}_{>0}, \cdot)$ y el grupo aditivo de los números reales $(\mathbb{R}, +)$ son isomorfos vía *el logaritmo natural y la función exponencial*, es decir,

$$\begin{array}{rcl} log : \mathbb{R}_{>0} & \longrightarrow & \mathbb{R} \\ a & \longmapsto & log(a) \end{array} \quad \text{y} \quad \begin{array}{rcl} exp : \mathbb{R} & \longrightarrow & \mathbb{R}_{>0} \\ x & \longmapsto & e^x. \end{array}$$

Estas funciones en efecto son morfismos de grupos ya que

$$log(ab) = log(a) + log(b) \ \text{ y } \ e^{x+y} = e^x e^y.$$

Ejemplo 0.31. Sea S_n el grupo simétrico en n letras, $n \geq 2$, entonces la función

$$\begin{array}{rcl} sgn : S_n & \longrightarrow & \{\pm 1\} = \mathbb{Z}^* \subset \mathbb{C}^* \\ \alpha & \longmapsto & sgn(\alpha) \end{array}$$

es un epimorfismo de grupos llamado la **función signo**, y su núcleo es $Ker(sgn) = A_n$, el grupo alternante, así $A_n \trianglelefteq S_n$. Por lo tanto $S_n/A_n \cong \{\pm 1\}$.

Ejemplo 0.32. Para $n \geq 2$ sea $\mathbb{Z}_n$ el grupo aditivo de los enteros módulo n y $(\mathbb{Z}, +)$ el grupo aditivo de los enteros, entonces existe un epimorfismo de grupos

$$\begin{array}{rcl} \psi : (\mathbb{Z}, +) & \longrightarrow & \mathbb{Z}_n \\ a & \longmapsto & [a] \end{array}$$

donde $Ker(\psi) = n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\}$, es decir, los múltiplos de n y por el primer teorema de isomorfismo tenemos que $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Ejemplo 0.33. Cualesquiera dos grupos cíclicos finitos del mismo orden son isomorfos. Salvo isomorfismo, $\mathbb{Z}_n$, el grupo de los enteros módulo n, es el único grupo cíclico finito de orden n ya que si $G = \langle x \rangle$ un grupo cíclico finito de orden n entonces existe un isomorfismo de grupos

$$\begin{array}{rcl} \phi : \langle x \rangle & \longrightarrow & \mathbb{Z}_n \\ x^k & \longmapsto & [k] \end{array} \quad \text{con } \ 0 \leq k \leq n-1.$$

Así, *sólo existe un grupo cíclico finito de orden n,*. Entonces también tenemos un isomorfismo

$$\begin{array}{rcl} \psi : \mu_n & \longrightarrow & \mathbb{Z}_n \\ (e^{\frac{2\pi i}{n}})^k & \longmapsto & [k] \end{array} \quad \text{con } \ 0 \leq k \leq n-1.$$

entre el grupo de las raíces n-ésimas de la unidad y los enteros módulo n.

Ejemplo 0.34. Cualesquiera dos grupos cíclicos infinitos son isomorfos.
Nuestro ejemplo canónico de grupo cíclico infinito es el grupo aditivo de los enteros, si $G = \langle x \rangle$ es otro grupo cíclico infinito, entonces existe un isomorfismo de grupos

$$\begin{array}{rcl} \varphi : \langle x \rangle & \longrightarrow & \mathbb{Z} \\ x^k & \longmapsto & k. \end{array}$$

Entonces, salvo isomorfismo, *sólo existe un grupo cíclico infinito*,

Ejemplo 0.35. Existe un morfismo de grupos

$$\begin{array}{rcl} \varphi : (\mathbb{R}, +) & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & e^{ix} = cos(x) + isen(x) \end{array}$$

cuyo núcleo e imagen son

$$Ker(\varphi) = \{x \in \mathbb{R} \mid e^{ix} = 1\} = \{2\pi k \mid k \in \mathbb{Z}\} = \langle 2\pi \rangle \text{ y}$$
$$Im(\varphi) = \{z \in \mathbb{C}^* \mid |z| = 1\} = \mathbb{S}^1,$$

respectivamente, y entonces $\mathbb{R}/\langle 2\pi k \rangle \cong \mathbb{S}^1$.

Ejemplo 0.36. Conjuntos del mismo cardinal tienen grupos de permutaciones isomorfos. Sean $X, Y \neq \emptyset$ conjuntos tales que $|X| = |Y|$, donde $|\ |$ denota al cardinal de los conjuntos. Entonces existe un isomorfismo de grupos $S_X \cong S_Y$. Para ver esto, notemos que existe una función biyectiva

$$\begin{array}{rcl} f : X & \longrightarrow & Y \\ x & \longmapsto & f(x) \end{array}$$

ya que por hipótesis X y Y tienen el mismo cardinal, así tenemos la función

$$\begin{array}{rcl} \Phi : S_X & \longrightarrow & S_Y \\ \sigma & \longmapsto & f \circ \sigma \circ f^{-1} \end{array}$$

donde la función $f \circ \sigma \circ f^{-1}$ es una función biyectiva por ser composición de funciones biyectivas y por lo tanto $f \circ \sigma \circ f^{-1} \in S_Y$. Luego, la función Φ es inyectiva por que si $\Phi(\sigma_1) = \Phi(\sigma_2)$ entonces $f \circ \sigma_1 \circ f^{-1} = f \circ \sigma_2 \circ f^{-1}$ y componiendo por la derecha con f y por la izquierda con f^{-1} en esta igualdad tenemos que $\sigma_1 = \sigma_2$. Ahora, Φ es suprayectiva pues para cualquier $\tau \in S_Y$ tenemos que la función $f^{-1} \circ \tau \circ f \in S_X$ es tal que $\Phi\left(f^{-1} \circ \tau \circ f\right) = \tau$. Por lo tanto Φ es una función biyectiva y por último, Φ es un morfismo de grupos ya que si $\sigma_1, \sigma_2 \in S_X$ entonces

$$\Phi(\sigma_1\sigma_2) = f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1} = f \circ (\sigma_1 \circ (f^{-1} \circ f) \circ \sigma_2) \circ f^{-1} = (f \circ \sigma_1 \circ f^{-1}) \circ (f \circ \sigma_2 \circ f^{-1}) = \Phi(\sigma_1) \circ \Phi(\sigma_2).$$

Por lo tanto $\Phi : S_X \longrightarrow S_Y$ es un isomorfismo de grupos.

Ejemplo 0.37. La función determinante

$$\begin{array}{rcl} det : GL(n, \mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ A & \longmapsto & det(A) \end{array}$$

es un epimorfismo de grupos, pues el determinante es una función multiplicativa, luego

$$Ker(det) = SL(n, \mathbb{R}) \trianglelefteq GL(n, \mathbb{R}),$$

y por lo tanto $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^*$.

Ejemplo 0.38. Si $C_n = \langle x_n \rangle$, $C_m = \langle x_m \rangle$ y $C_{nm} = \langle x_{nm} \rangle$ son los grupos cíclicos de orden n, m y nm respectivamente y si $(n, m) = 1$, entonces existe un isomorfismo de grupos

$$\begin{array}{rcl} \sigma : C_{nm} & \longrightarrow & C_n \times C_m \\ x_{nm}{}^k & \longmapsto & (x_n{}^k, x_m{}^k) = (x_n, x_m)^k \end{array} \quad \text{donde } \ 0 \leq k \leq nm.$$

Ejemplo 0.39. . Sean $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, donde A se puede pensar como la reflexión en el eje X (la conjugación compleja) multiplicada por i y B es una rotación de 90 grados respecto al origen en el sentido de las manecillas del reloj. Entonces el subgrupo generado por A y B consiste de los elementos:

$$\begin{array}{c} A,\ B,\ A^2 = B^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = -I,\ A^3 = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right) = -A,\ A^4 = B^2 = I, \\ AB = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right),\ A^2B = -B = B^3 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \text{ y } A^3B = -AB = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right), \end{array}$$

y por sus relaciones entre generadores se puede escribir como

$$Q_8 = \langle A, B \mid A^4 = B^4 = I, B^{-1}AB = A^{-1} \rangle \subset GL_2(\mathbb{C}).$$

Entonces existe un monomorfismo de grupos

$$\begin{array}{rcl} \varphi : Q & \longrightarrow & GL_2(\mathbb{C}) \\ i^s j^t & \longmapsto & A^s B^t \end{array}$$

con $0 \leq s \leq 3$ y $0 \leq t \leq 1$, y por lo tanto

$$Q \cong Im(\varphi) = \langle A, B \rangle = Q_8.$$

el isomorfismo es

$$\begin{array}{c} 1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ i^2 = -1 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ i^3 = -i \mapsto \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} \\ j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ ij = k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ i^2j = -j \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ i^3j = -k \mapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}. \end{array}$$

Ejemplo 0.40. Consideremos las matrices $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ y $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, donde x es la rotación de 90 grados respecto al origen en el sentido contrario de las manecillas del reloj y y es la reflexión respecto al eje Y. Entonces el subgrupo de $GL_2(\mathbb{C})$ generado por A y B consiste de los elementos:

1. $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ es la rotación de 90 grados (multiplicar por i).
2. $B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ es la reflexión en el eje Y.
3. $A^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = -I$ es la rotación de 180 grados.
4. $A^3 = A^2A = -A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ es la rotación de 270 grados.
5. $A^4 = B^2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = I$ es la rotación de cero grados.
6. $AB = \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right)$ es la reflexión respecto a gráfica de la identidad negativa.
7. $A^2B = -B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ es la reflexión en el eje X.
8. $A^3B = -AB = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ es la reflexión respecto a la gráfica de la identidad.

Por lo que podemos escribir

$$\langle A, B \rangle = \langle A, B \mid A^4 = B^2 = 1, BAB = A^{-1} \rangle$$

y entonces existe un monomorfismo de grupos dado por

$$\begin{array}{rcl} \psi : D_8 & \longrightarrow & GL_2(\mathbb{C}) \\ x^i y^j & \longmapsto & A^i B^j \end{array}$$

con $0 \leq i \leq 3$ y $0 \leq j \leq 1$, y por lo tanto

$$D_8 \cong Im(\psi) = \langle A, B \mid A^4 = I, B^2 = I, AB = BA^{-1} \rangle.$$

Más claramente, el isomorfismo es

- $r_0 = (1) = 1 \longmapsto I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ es la rotación de cero grados.
- $r_1 = (1234) = x \longmapsto A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ es la rotación de 90 grados.
- $r_2 = (13)(24) = x^2 \longmapsto -I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ es la rotación de 180 grados.
- $r_3 = (1432) = x^3 \longmapsto A^3 = -A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ es la rotación de 270 grados.
- $m_1 = (12)(34) = y \longmapsto B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ es la reflexión en el eje Y.
- $d_1 = (13) = xy \longmapsto AB = \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right)$ es la reflexión respecto a la identidad negativa.
- $m_2 = (14)(23) = x^2 y \longmapsto A^2 B = -B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ es la reflexión respecto al eje X.
- $d_2 = (24) = x^3 y \longmapsto A^3 B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ es la reflexión respecto a gráfica de la identidad.

Sabemos que D_8 tiene un subgrupo dado por

$$\mathbf{V} = \{(1), (12)(34), (13)(24), (14)(23)\}$$

donde cada elemento no identidad tiene orden orden 2 pues son las reflexiones respecto a los ejes coordenados y el otro es la rotación de 180 grados y el producto de cualesquiera dos nos da el tercero, este grupo es llamado el **grupo de Klein**, y por el isomorfismo anterior, en matrices se ve como

$$\mathbf{V} = \left\{e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), a = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), c = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\right\}.$$

Teorema 0.41. ***CAYLEY.***
Sea G un grupo. Entonces G es isomorfo a un subgrupo de S_G. Más aún si $|G| = n < \infty$ entonces G es isomorfo a un subgrupo de S_n.

Demostración. Consideremos para cada $g \in G$ la función

$$\begin{array}{rcl} \tau_g : G & \longrightarrow & G \\ x & \longmapsto & gx. \end{array}$$

A τ_g se le llama la **traslación izquierda** por g y es inmediato (por la regla de correspondencia) que es una función biyectiva con inversa dada por

$$\begin{array}{rcl} \tau_{g^{-1}} : G & \longrightarrow & G \\ x & \longmapsto & g^{-1}x \end{array}$$

y por lo tanto $\tau_g \in S_G$, sin embargo, es claro que no es un morfismo de grupos. Ahora, para todos $g, h, x \in G$ tenemos que

$$\tau_{gh}(x) = (gh)x = g(hx) = \tau_g\left(\tau_h(x)\right) = \left(\tau_g \circ \tau_h\right)(x),$$

es decir, $\tau_{gh} = \tau_g \circ \tau_h$, y entonces la función

$$\begin{array}{rcl} \varphi : G & \longrightarrow & S_G \\ g & \longmapsto & \tau_g \end{array}$$

es un morfismo de grupos pues $\varphi(gh) = \tau_{gh} = \tau_g \circ \tau_h = \varphi(g) \circ \varphi(h)$. Además es inyectivo porque si $\varphi(g_1) = \varphi(g_2)$ entonces $\tau_{g_1} = \tau_{g_2}$ y por lo tanto $g_1 = g_2$ y por el primer teorema de isomorfismo

$$G \cong Im(\varphi) = \{\tau_g \mid g \in G\} := H \leq S_G.$$

Por otro lado, supongamos que $|G| = n < \infty$, entonces podemos escribir $G = \{e_G, g_2, g_3, \ldots, g_n\}$ y si $n_{\leq} = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$ (el conjunto de los números naturales entre 1 y n), entonces, por el ejemplo 0.36 la función

$$\begin{array}{rcl} f : n_{\leq} & \longrightarrow & G \\ i & \longmapsto & g_i \end{array}$$

es una biyección (f está enumerando a los elementos de G) que induce un isomorfismo de grupos

$$\begin{array}{rcl} \Phi : S_n & \longrightarrow & S_G \\ \sigma & \longmapsto & f \circ \sigma \circ f^{-1}. \end{array}$$

Por lo que $G \cong H \leq S_G \cong S_n$. ■

Observación 0.42. El teorema de Cayley tiene como consecuencia importante que por muy abstracto que sea un grupo, genéricamente es un grupo de permutaciones, entonces nos dice que basta estudiar los grupos simétricos para saber el comportamiento de los demás grupos. Aunque el resultado parezca sorprendente, no lo es tanto si observamos la tabla de multiplicación de cualquier grupo finito, en ella cada renglón nos da una permutación del grupo, pues en cada renglón aparecen todos los elementos del grupo sin repetirse, sucede lo mismo para las columnas, y en este sentido puede pensarse al grupo como un grupo de permutaciones.

Definición 0.43. *Sea G un grupo y $X \neq \emptyset$ un conjunto. Una **acción** de G en X es una función*

$$\begin{array}{rcl} \cdot : G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & \cdot\big((g, x)\big) := g \cdot x \end{array}$$

que satisface para todos $g, h \in G$ y $x \in X$ las siguientes propiedades:

i) $e_G \cdot x = x$.

ii) $(gh) \cdot x = g \cdot (h \cdot x)$.

*Si existe una acción de G en X decimos que X es un G**-conjunto**.*

Existe una conexión entre las acciones de un grupo G en un conjunto no vacío X y los morfismos de G en el grupo de permutaciones de X, estableceremos esa relación en los dos teoremas siguientes.

Teorema 0.44. *Sea G un grupo y $X \neq \emptyset$ un G-conjunto, entonces la acción de G en X induce un morfismo de grupos $\phi : G \longrightarrow S_X$.*

Demostración. Sea $\cdot$ la acción de G en X y consideremos la función

$$\begin{array}{rcl} \phi : G & \longrightarrow & S_X \\ g & \longmapsto & \phi(g) \end{array} \quad \text{donde} \quad \begin{array}{rcl} \phi(g) : X & \longrightarrow & X \\ x & \longmapsto & g \cdot x\ . \end{array}$$

Luego, $\phi(g)$ es biyectiva pues tiene inversa dada por

$$\begin{aligned} \phi(g^{-1}) : X &\longrightarrow X \\ x &\longmapsto g^{-1} \cdot x \ . \end{aligned}$$

En efecto, tenemos que

$$\begin{gathered} \left(\phi(g) \circ \phi(g^{-1})\right)(x) = g \cdot \left(g^{-1} \cdot x\right) = (gg^{-1}) \cdot x = x, \\ \text{y } \left(\phi(g^{-1}) \circ \phi(g)\right)(x) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = x, \end{gathered}$$

por lo tanto $\phi(g) \in S_X$. Ahora, para todos $g, h \in G$ y $x \in X$ tenemos que

$$\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = x = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x),$$

que significa que ϕ es un morfismo de grupos. ■

Teorema 0.45. *Sean G un grupo, $X \neq \emptyset$ un conjunto y $\phi : G \longrightarrow S_X$ un morfismo de grupos. Entonces ϕ induce una acción de G en X.*

Demostración. Sea $\phi : G \longrightarrow S_X$ morfismo de grupos y consideremos la función

$$\begin{aligned} \cdot : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x := \phi(g)(x) \end{aligned}$$

($g \cdot x := \phi(g)(x) \in X$ pues $\phi(g)(x) \in S_X$). Como ϕ es un morfismo de grupos entonces

i) $e_G \cdot x = \phi(e_G) \cdot x = id_X(x) = x$

ii) $g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x) = \phi(gh)(x) = (gh) \cdot x$,

que son los axiomas de una acción de G sobre X. ■

Resumiendo, los dos teoremas anteriores nos dicen que *una acción de un grupo G en un conjunto no vacío X es lo mismo que un morfismo de grupos de G en el grupo de simetrías de X.*
Diremos que una acción es **fiel** o que G **actúa fielmente** en X si el único elemento del grupo que fija a todos los del conjunto es el neutro, o de forma equivalente, si el morfismo inducido por la acción es inyectivo. Así, recordando que para todo grupo G, por el teorema de Cayley existe un morfismo de grupos $\varphi : G \longrightarrow S_G$, entonces este morfismo inyectivo induce una acción fiel de G en G, que de acuerdo con el teorema 0.45 está dada por $g \cdot x := \varphi(g)(x) = \tau_g(x) = gx$, que no es más que la traslación por g, es decir, el producto en G es una acción fiel. Y en términos del teorema 0.44, si la acción de G en G está dada por el producto en G (que es una acción fiel), entonces induce el morfismo de grupos inyectivo

$$\begin{aligned} \varphi : G &\longrightarrow S_G \\ g &\longmapsto \tau_g \end{aligned}$$

usado en la demostración del teorema de Cayley, este morfismo es llamado **la representación regular izquierda** de G. En general, un morfismo de grupos $\phi : G \longrightarrow S_X$ para algún conjunto no vacío X es llamado una **representación por permutaciones** de G.

Sea $X \neq \emptyset$ un G-conjunto, entonces para todo $x \in X$ naturalmente la acción de G en X le asigna un subconjunto de X y un subgrupo de G dados por

$$o(x) = \{y \in X \mid \exists\ g \in G \text{ tal que } gx = y\} \subseteq X \quad \text{y}$$
$$G_x = \{g \in G \mid gx = x\} \leq G$$

llamados la **órbita** de x y el **estabilizador** de x en G respectivamente.
Las órbitas son las clases de equivalencia de la relación de equivalecia en X dada por: $x \sim y$ si existe $g \in G$ tal que $gx = y$. Las órbitas también son por sí mismas G-conjuntos con la acción inducida de G. De hecho, un subconjunto $A \subseteq X$ es un G-conjunto con la acción inducida de G si y sólo si es una unión de órbitas. Luego, elementos en una misma órbita tienen estabilizadores conjugados, y en particular isomorfos, es decir, si $o(x) = o(y)$ entonces $G_y = gG_xg^{-1}$ donde g es tal que $gx = y$. Decimos que una acción es una **acción transitiva** o que X es un G**-conjunto transitivo** si existe $x \in X$ tal que $o(x) = X$, o de forma equivalente, la acción tiene una sola órbita, todo X, es decir, para todo $x \in X$ se tiene que $o(x) = X$. Ya que las órbitas son clases de equivalencia, un G-conjunto X tiene una única partición que consiste de G-conjuntos transitivos, su partición en órbitas (las órbitas son los únicos G-subconjuntos transitivos de X). Así, para describir a todos los G-conjuntos basta describir a todos los G-conjuntos transitivos.

Ejemplo 0.46. Todo grupo G actúa en sí mismo por conjugación, es decir, la función

$$\begin{array}{rcl} \cdot : G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g \cdot x := gxg^{-1}. \end{array}$$

es una acción, y en términos del teorema 0.44, la conjugación induce un morfismo de grupos

$$\begin{array}{rcl} \Gamma : G & \longrightarrow & S_G \\ g & \longmapsto & \gamma_g \end{array} \quad \text{donde} \quad \begin{array}{rcl} \gamma_g : G & \longrightarrow & G \\ x & \longmapsto & g \cdot x := gxg^{-1} \end{array}$$

donde para todo $g \in G$ la función $\gamma_g \in S_G$ no es más que la conjugación por g (es claro que es inyectiva, y por lo tanto suprayectiva pues su dominio y codominio tienen el mismo cardinal). Más aún, γ_g es un morfismo de grupos, y por lo tanto un automorfismo de G, los automorfismos γ_g son llamados **automorfismos internos** o **conjugaciones** de G, y el conjunto de ellos se denota por $Inn(G)$, cualquier otro automorfismo de G es llamado **automorfismo externo**, y se denotan por $Out(G)$. Entonces se tiene que

$$\begin{array}{rcl} \Gamma : G & \longrightarrow & Aut(G) \subset S_G \\ g & \longmapsto & \gamma_g \end{array}$$

es un morfismo de grupos pues $\gamma_{gh} = \gamma_g \circ \gamma_h$, y tiene como núcleo

$$\begin{array}{rcl} Ker(\Gamma) & = & \{g \in G \mid \gamma_g = \gamma_{e_G} = id_G\} = \{g \in G \mid gxg^{-1} = x\ \forall\ x \in G\} \\ & = & \{g \in G \mid gx = xg\ \forall\ x \in G\} = C_G(G), \end{array}$$

es decir, el conjunto de los elementos del grupo que conmutan con todos los elementos del grupo, escribiremos $Ker(\Gamma) := Z(G)$ y lo llamaremos el **centro** de G. Tenemos que $Z(G) \trianglelefteq G$ pues es el núcleo de un morfismo de grupos. Por último, por el primer teorema de isomorfismo se tiene que

$$G/Z(G) \cong Im(\Gamma) = Inn(G) \leq Aut(G) \leq S_G.$$

Más aún, $Im(\Gamma) = Inn(G) \trianglelefteq Aut(G)$ y además

$$Aut(G)/Inn(G) \cong Out(G).$$

Recíprocamente, si tenemos el morfismo

$$\begin{array}{rcl} \Gamma : G & \longrightarrow & S_G \\ g & \longmapsto & \gamma_g \end{array}$$

éste induce la acción de G en sí mismo que de acuerdo con el teorema 0.45 está dada por la conjugación, es decir, $g \cdot x := \gamma_g(x) = gxg^{-1}$.
Luego, la órbita de esta acción para cada $x \in G$ está dada por

$$o(x) = \{y \in G \mid y = gxg^{-1},\ g \in G\} \subseteq G$$

y es llamada la **clase de conjugación** de x en G y la denotaremos por x^G. También tenemos que

$$G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x) \leq G$$

es decir, estabilizador de x en este caso coincide con el centralizador de x en G.

Ejemplo 0.47. Conjuntos cocientes son G-conjuntos transitivos.
Si $H \leq G$ y G/H es el conjunto de clases laterales de H en G entonces la función

$$\begin{array}{rcl} \cdot : G \times G/H & \longrightarrow & G/H \\ (g, xH) & \longmapsto & g \cdot x := gxH. \end{array}$$

es una acción y es transitiva pues si $xH, yH \in G/H$ entonces tomando $g = yx^{-1}$ tenemos que $g(xH) = yx^{-1}(xH) = yH$. Y en términos del teorema 0.44, la acción induce un morfismo de grupos

$$\begin{array}{rcl} \varphi : G & \longrightarrow & S_{G/H} \\ g & \longmapsto & \tau_g \end{array} \quad \text{donde} \quad \begin{array}{rcl} \tau_g : G/H & \longrightarrow & G/H \\ xH & \longmapsto & g \cdot xH := gxH \end{array}$$

donde para todo $g \in G$ la función $\tau_g \in S_{G/H}$ no es más que la traslación izquerda por g en el cociente y por lo tanto es una acción fiel. Este ejemplo generaliza al Teorema de Cayley, que no es más que este resultado tomando $H = \{e_G\}$.

Vamos a clasificar ahora a todos los G conjuntos transitivos, vimos en el ejemplo anterior que conjuntos cocientes son G-conjuntos transitivos, vamos a ver que todo G-conjunto transitivo se puede ver como un cociente.
Si X y Y son G-conjuntos entonces una función $f : X \longrightarrow Y$ es llamada un **morfismo de G-conjuntos** si *respeta* la acción, o *conmuta* con la acción, es decir, para todos $g \in G$ y $x \in X$ se tiene que $f(gx) = gf(x)$. Si además f es biyectiva diremos que es un **isomorfismo de G-conjuntos**, diremos que X y Y son G-conjuntos isomorfos y se denota por $X \cong Y$.

Teorema 0.48. *Sea X un G-conjunto transitivo. Entonces tenemos un isomorfismo de G-conjuntos*

$$X \cong G/G_x \text{ para todo } x \in X.$$

Demostración. Para todo $x \in X$ definamos la función

$$\begin{array}{rcl} f : G/G_x & \longrightarrow & X \\ gG_x & \longmapsto & gx. \end{array}$$

La función f está bien definida pues si $gG_x = hG_x$ entonces $h^{-1}g \in G_x$ y por lo tanto $(h^{-1}g)x = x$ y así $gx = hx$. Revirtiendo este argumento se ve que f es inyectiva. Luego, si $y \in X$ existe $h \in G$ tal que $y = hx$, entonces tenemos que $f(hG_x) = y$ y por lo tanto f es suprayectiva. Luego, para todos $h \in G$, $gG_x \in G/G_x$ tenemos que

$$hf(gG_x) = h(gx) = (hg)x = f(hgG_x) = f(h(gG_x))$$

y por lo tanto f es un isomorfismo de G-conjuntos. ■

El teorema anterior no sólo clasifica a todos los G-conjuntos transitivos sino que tiene como consecuencia el siguiente importante teorema.

Teorema 0.49. ***Teorema Órbita-Estabilizador****. Sea X un G-conjunto. Entonces existe un isomorfismo de G-conjuntos $o(x) \cong G/G_x$ para todo $x \in X$. En particular si G es finito entonces*

$$|o(x)| = \frac{|G|}{|G_x|},$$

es decir, el número de elementos en la órbita de x es igual al índice del centralizador de x en G.

Demostración. Para todo $x \in X$ su órbita es un G-conjunto transitivo, y se sigue por lo tanto del teorema anterior. ■

Ahora, para finalizar con los resultados que usaremos de teoría de grupos recordemos el teorema Fundamental de los Grupos Abelianos Finitos, no haremos la prueba aquí, pero se puede encontrar en [20] donde se da una demostración aplicando los teoremas de Sylow.

Teorema 0.50. *Todo grupo abeliano finito G es producto directo de grupos cíclicos, es decir,*

$$G \cong C_{n_1} \times \cdots \times C_{n_m}.$$

donde $n_i | n_{i+1}$ y $C_{n_i} \cong \mathbb{Z}_{n_i} \cong \mathbb{Z}/n_i\mathbb{Z}$.

Demostración. Ver [27], capítulo 7. ■

Anillos

La estructura con la que se trabaja después de grupos es la de anillos, en ella tenemos una operación binaria más, y por lo tanto podría o no satisfacer las propiedades de conmutatividad, la existencia de un elemento identidad y la existencia de inversos, cada vez que agreguemos alguna propiedad a la operación binaria se obtiene una nueva estructura algebraica.

Definición 0.51. *Sea $R \neq \emptyset$ un conjunto. Decimos que R es un* ***anillo*** *si en R existen dos operaciones binarias, denotadas por $+$ y $*$ tales que $(R, +)$ es un grupo abeliano y $(R, *)$ es un semigrupo, es decir $*$ es asociativa, y además se satisfacen las* ***leyes distributivas***

$$a(b + c) = ab + ac \quad y \quad (a + b)c = ac + bc$$

para todos $a, b, c \in R$, es decir, ambas operaciones binarias son compatibles en R. Si $(R, *)$ es un monoide ($*$ es asociativa y existe un elemento identidad en G con respecto a la operación $*$) decimos que R es un ***anillo con uno*** *o que tiene elemento unidad, denotado por 1_R, cuando hablemos de anillos de ahora en adelante siempre supondremos que tiene elemento unidad. Si $*$ es conmutativa decimos que R es un* ***anillo conmutativo****.*

Un **dominio entero** es un anillo conmutativo con uno que satisface la siguiente propiedad:

$$\text{si } a \neq 0 \text{ y } b \neq 0 \in R \text{ entonces } ab \neq 0$$

o de forma equivalente, si el producto de dos elementos es cero entonces alguno de ellos debe ser cero. De hecho, un anillo es dominio entero si y sólo si se cumple la ley de la cancelación para el producto en R. Si $a \neq 0$ y $b \neq 0 \in R$ y $ab = 0$ decimos que a y b son **divisores de cero**, así, un dominio entero es un anillo conmutativo que no tiene divisores de cero.

Un elemento $a \in R$ es **unidad** si es invertible bajo el producto en R, es decir, existe $a^{-1} \in R$ tal que $aa^{-1} = a^{-1}a = 1_R$. El conjunto

$$\mathcal{U}(R) = \{u \in R \mid u \text{ es unidad } \} \subseteq R$$

es un grupo llamado el **grupo de unidades** del anillo R. Decimos que un anillo con uno es un **anillo con división** si $\mathcal{U}(R) = R^* := R - \{0\}$, es decir, todo elemento no cero es unidad. Un **campo** es un anillo con división conmutativo, es decir, un campo ya tiene practicamente todas las propiedades de grupo para la operación que se toma como el producto ($(R - \{0\}, \cdot)$ es un grupo), así, podemos decir, sólo en términos de grupos, que un campo es un conjunto con dos operaciones binarias con las que forma un grupo abeliano con cada una de ellas y estas operaciones son compatibles, que no es más que las leyes distributivas.
No existen elementos en un anillo que sean divisiores de cero y unidades al mismo tiempo, así, todo campo es un dominio entero.
Un resultado importante es que si un anillo finito tiene al menos dos elementos y no tiene divisores de cero entonces es un anillo con división, en particular, un dominio entero finito es un campo.

Definición 0.52. *Sea R un anillo con 1_R. La* ***característica*** *de R se define como*

$$char(R) := min\{m \in \mathbb{Z}^+ \mid m1_R = 0_R\},$$

es decir, es el mínimo número de veces que hay que sumar 1_R consigo mismo para obtener el 0_R. Si no existe tal m decimos que el anillo tiene característica cero. Ya que todo campo es un anillo, la característica de un campo es su característica como anillo.

Subanillos y ejemplos de anillos

Definición 0.53. *Sea R un anillo. Un subconjunto $S \subseteq R$ es un* ***subanillo*** *de R, denotado por $S \leq R$, si es por sí mismo un anillo con la restricción a S de las operaciones binarias en R. Si S está contenido propiamente en R decimos que es un* ***subanillo propio*** *de R y se denota por $S < R$. Un subanillo K de un campo $\mathbb{F}$ es un* ***subcampo*** *si tiene al uno de $\mathbb{F}$ y si es por sí mismo un campo con las operaciones de $\mathbb{F}$.*

Observación 0.54. $S \leq R$ si y sólo si S es un subgrupo aditivo de R y es cerrado bajo el producto.

Todo anillo R tiene al menos dos subanillos, $\{0_R\}$ y R. La relación ser subanillo de R, que denotamos por $\leq$, es un orden parcial en la familia de los subanillos de R. La intersección arbitraria de una familia de subanillos es un subanillo.

Definición 0.55. *Sea R un anillo e $I \subseteq R$. Decimos que I es un **ideal izquierdo** de R si I es subanillo de R y absorbe el producto por elementos de R del lado izquierdo, es decir, para todos $r \in R$, $x \in I$ se tiene que $rx \in I$, de forma similar, I es llamado **ideal derecho** de R si para todos $r \in R$, $x \in I$ tenemos que $xr \in I$. Llamamos a I un **ideal bilateral** si es un ideal tanto izquierdo como derecho, y simplemente diremos que es un ideal.*

Todo anillo R siempre tiene al menos dos ideales, $\{0_R\}$ y R, llamados los **ideales triviales** de R. En términos de ideales, una caracterización de los campos es que si R es un anillo conmutativo con uno, entonces R es un campo si y sólo si no tiene ideales propios además de los triviales.

Definición 0.56. *Sea R un anillo y $X \subseteq R$. El **subanillo generado por** X es el menor subanillo de R que contiene a X y el **ideal generado por** X es el menor ideal de R que contiene a X, y ya que la intersección de subanillos es subanillo entonces el subanillo (ideal) generado por X es la intersección de todos los subanillos (ideales) de R que contienen a X, usaremos la notación $\langle X \rangle$ para el ideal generado por X, es decir,*

$$\langle X \rangle = \cap I \text{ donde } X \subseteq I, I \text{ ideal de } R.$$

Lema 0.57. *Sea R un anillo y $X \subseteq R$ no vacío.*

1) *El subanillo generado por X es la suma o diferencia de todos los productos finitos de elementos de X.*
2) *El ideal generado por X es el conjunto*

$$RXR = \left\{ \sum_{i=1}^{n} r_i x_i s_i \mid r_i, s_i \in R, x_i \in X, n \geq 1 \right\}.$$

3) *Si R es conmutativo entonces el ideal generado por X es*

$$RX = \left\{ \sum_{i=1}^{n} r_i x_i \mid r_i \in R, x_i \in X, n \geq 1 \right\}.$$

En particular si $X = \{a\}$ entonces el ideal generado por X es

$$Ra = \{ra \mid r \in R\}$$

y es llamado el **ideal principal** generado por a, es decir, los múltiplos de a en R. Un dominio entero en el cual todo ideal es principal es llamado un **dominio de ideales principales** (DIP).

Si I es un ideal de un anillo R, entonces I es un subgrupo aditivo de R como grupo abeliano aditivo, entonces las clases laterales de I en R se escriben aditivamente como $a + I$ para todo $a \in R$, y forman el grupo abeliano aditivo R/I, entonces se le puede dar estructura de anillo a R/I de forma

natural con el producto inducido del producto del anillo, es decir, si $a+I, b+I \in R/I$ entonces $(a+I)(b+I) = ab+I$. Si R es conmutativo entonces R/I es conmutativo. Si R tiene 1_R entonces R/I tiene uno dado por $1_R + I$. El anillo R/I es llamado el **anillo cociente** del anillo R por el ideal I.

Ejemplo 0.58. Son anillos conmutativos con 1 sin divisores de cero los conjuntos

$$(\mathbb{Z}, +, \cdot),\ (\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot) \text{ y } (\mathbb{C}, +, \cdot)$$

donde $+$ y $\cdot$ son la suma y producto usuales, además tenemos la cadena de subanillos

$$(\mathbb{Z}, +, \cdot) \leq (\mathbb{Q}, +, \cdot) \leq (\mathbb{R}, +, \cdot) \leq (\mathbb{C}, +, \cdot).$$

Los grupos de unidades de estos anillos son

$$\mathcal{U}(\mathbb{Z}) = \mathbb{Z}^* := \{\pm 1\},\ \mathcal{U}(\mathbb{Q}) = \mathbb{Q}^* := \mathbb{Q} - \{0\},\ \mathcal{U}(\mathbb{R}) = \mathbb{R}^* := \mathbb{R} - \{0\} \text{ y } \mathcal{U}(\mathbb{C}) = \mathbb{C}^* := \mathbb{C} - \{0\}$$

y por lo tanto, $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ son campos y $\mathbb{Z}$ no lo es, aunque sí es dominio entero y $2\mathbb{Z}$ es un subanillo de $\mathbb{Z}$ que no tiene al 1, además $2\mathbb{Z}$ es un ideal de $\mathbb{Z}$, en general, para cualquier $m \geq 2$, $m\mathbb{Z}$ es un ideal de $\mathbb{Z}$ pues es el ideal principal generado por m.

Ejemplo 0.59. Para $n \geq 2$, el conjunto de los **enteros módulo** n

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

con la suma $[a] + [b] := [a+b]$ y producto (módulo n), $[a]\,[b] := [ab]$ es un anillo conmutativo con 1, de hecho es el anillo cociente $\mathbb{Z}/n\mathbb{Z}$, más aún, si n es compuesto tiene divisores de cero (las clases de los enteros que aparecen en la descomposición de n). Luego, el grupo de unidades de este anillo es el conjunto de los enteros no negativos menores que n y primos relativos con n, es decir,

$$\mathcal{U}(\mathbb{Z}_n) = {\mathbb{Z}_n}^* := \{[a] \in \mathbb{Z}_n \mid 1 \leq a < n \text{ y } (a, n) = 1\}.$$

Entonces $\mathbb{Z}_n$ es un campo si y sólo si n es un número primo.

Ejemplo 0.60. Anillos de funciones de un conjunto en un anillo.
Sea X un conjunto no vacío y R un anillo. Entonces el conjunto

$$R^X = \{f : X \longrightarrow R \mid f \text{ es función }\}$$

es un anillo con la suma puntual de funciones y el producto puntual de funciones, es decir

$$(f+g)(x) = f(x) + g(x) \quad \text{y} \quad (fg)(x) = f(x)g(x).$$

Luego, el anillo R^X tiene las siguientes propiedades.

i) Si R es un anillo con uno entonces R^X es un anillo con uno.

ii) R^X es conmutativo si y sólo si R es conmutativo.

iii) R^X tiene divisores de cero (no es dominio entero).

iv) Si $R = \mathbb{F}$ es un campo y $f \in \mathbb{F}^X$ es tal que $f(x) \neq 0$ para todo $x \in X$ entonces f es unidad en $\mathbb{F}^X$.

Ejemplo 0.61. Anillos de endomorfismos de grupos abelianos.
Sea A un grupo abeliano aditivo, entonces el conjunto

$$End(A) = \{f : A \longrightarrow A \mid f \text{ es morfismo } \}$$

con la suma puntual de funciones y la composición de funciones como producto es un anillo con uno, $id_A(a) = a$ para todo $a \in A$, llamado el **anillo de endomorfismos** de A, este anillo no es conmutativo ya que la composición de funciones en general no es conmutativa, luego

$$\mathcal{U}\left(End(A)\right) = Aut(A).$$

Ejemplo 0.62. Suma directa de anillos.
Si R y S son anillos, entonces podemos dar estructura de anillo al producto cartesiano $R \times S$ con las operaciones entrada a entrada. En general, podemos considerar un número finito de anillos $R_1, \ldots, R_k$ y tomando su producto cartesiano definimos las operaciones entrada a entrada para formar un anillo llamado la **suma directa de anillos** denotado por

$$R = \bigoplus_{i=1}^{k} R_i.$$

La suma directa de anillos es un anillo conmutativo si y sólo si todos los anillos son conmutativos y tiene uno si y sólo si todos tienen uno. No es un dominio entero. Sus unidades son los elementos $(a_1, a_2, \ldots, a_k)$ tales que $a_i \in R_i$ es unidad para todo i.

Ejemplo 0.63. Anillos de matrices con entradas en un anillo conmutativo.
Sea R un anillo conmutativo con uno, entonces el conjunto $\mathcal{M}_{n\times n}(R)$ de matrices de $n \times n$ con entradas en un anillo R es un anillo con uno con la suma y producto usual de matrices, además no es conmutativo y tiene divisores de cero (no es dominio entero), sus unidades son el grupo

$$GL_n(R) = \{A \in \mathcal{M}_{n\times n}(R) \mid det(A) \neq 0\}$$

llamado el **grupo general lineal de grado** n **sobre el anillo** R.
El anillo $\mathcal{M}_{n\times n}(\mathbb{R})$ tiene subanillos con uno, por ejemplo, el conjunto de matrices diagonales y los conjuntos de matrices triangulares superiores e inferiores. Pero tiene subanillos sin uno como por ejemplo los conjuntos de matrices estrictamente triangulares superiores e inferiores.

Ejemplo 0.64. Para todo anillo R y cualquier subconjunto $X \subseteq R$, el conjunto

$$Z(R) = \{s \in R \mid rs = sr \ \forall \ r \in R\},$$

es decir, de los elementos del anillo que conmutan con todos los elementos del anillo es un subanillo de R llamado el **centro** del anillo de R.

Ejemplo 0.65. Para cualquier conjunto $X \neq \emptyset$, si $\mathcal{P}(X) = \{A \mid A \subseteq X\}$ es la potencia de X y definimos la suma como $\triangle$, que es la diferencia simétrica de conjuntos y el producto como la intersección entonces $(\mathcal{P}(X), \triangle, \cap)$ es un anillo conmutativo con uno, todo el conjunto X.

Ejemplo 0.66. Anillos de polinomios sobre anillos conmutativos.
Sea R un anillo conmutativo con 1_R y consideremos el conjunto

$$R[x] = \{(a_0, a_1, a_2, \ldots) \mid a_i \in R \ \forall \ i \text{ donde } a_i \neq 0 \text{ sólo para un número finito de términos } a_i\},$$

es decir, el conjunto de todas las sucesiones infinitas con elementos de R con sólo un número finito de términos no nulos. Dos elementos en $R[x]$ son iguales (como sucesiones) si y sólo si todas sus correspondientes entradas son todas iguales entre sí. Entonces $R[x]$ es un anillo conmutativo con $1_{R[x]}$ con las operaciones de suma y producto dadas por

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots) \text{ y}$$
$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots), \text{ con } c_k = \sum_{i+j=k} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}.$$

Podemos *ver* al anillo R dentro de $R[x]$ considerando la función

$$\begin{array}{rcl} f : R & \longrightarrow & R[x] \\ a & \longmapsto & (a, 0, 0, \ldots). \end{array}$$

El uno de $R[x]$ es el elemento $(1_R, 0, 0, \ldots)$, y entonces se identifica con 1_R. Si $x := (0, 1_R, 0, \ldots)$, entonces $x^2 = (0, 0, 1_R, 0, \ldots)$, $x^3 = (0, 0, 0, 1_R, 0, \ldots)$, etc. Así, para cada $(a_0, a_1, a_2, \ldots) \in R[x]$ se tiene una expresión única

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_{m-1} x^m + a_m x^m.$$

El anillo $R[x]$ es llamado el **anillo de polinomios sobre R en la indeterminada x**. Se dice que R es el anillo de coeficientes de $R[x]$. Dos elementos en $R[x]$ son iguales si y sólo si coeficiente a coeficiente son iguales. Si n es el natural más grande tal que $a_n \neq 0$ decimos que es un **polinomio de grado n** y se denota al grado de un polinomio $p(x)$ por $deg(p(x))$ y a_n es llamado el **coeficiente principal** del polinomio. Un polinomio cuyo coeficiente principal es 1_R es llamado **polinomio mónico**. El **polinomio cero**, $p_0(x)$, es el polinomio cuyos coeficientes son todos cero y se define su grado como -1. También, si R es un dominio entero entonces $R[x]$ es un dominio entero y las unidades de $R[x]$ son las unidades de R.
Si $R = \mathbb{F}$ es un campo los elementos del campo vistos dentro del anillo de polinomios son unidades y son los polinomios de grado cero, además en el anillo de polinomios $\mathbb{F}[x]$ es válido el **algoritmo de la división**, es decir, para cualesquiera polinomios $f(x), g(x) \in \mathbb{F}[x]$ existen únicos $q(x), r(x) \in \mathbb{F}[x)$ tales que $g(x) = f(x)q(x) + r(x)$ con $deg(r(x)) < deg(g(x))$ o $r(x) = 0$. Una consecuencia del algoritmo de la división es que $\mathbb{F}[x]$ es un dominio de ideales principales, cada ideal es generado por un elemento de grado mínimo respecto a los otros elementos del ideal, y existe un único polinomio mónico que genera a cada ideal.

Morfismos de anillos

Definición 0.67. *Sean R y R' anillos y $\varphi : R \longrightarrow R'$ una función. Decimos que φ es un **morfismo de anillos** si es un morfismo de grupos aditivos y respeta el producto en los anillos, es decir, para todos $a, b \in R$ se tiene que*

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad y \quad \varphi(ab) = \varphi(a)\varphi(b).$$

Si ambos anillos tienen uno y un morfismo de anillos manda el uno en el uno decimos que es un ***morfismo unital****. Si φ es un morfismo de anillos y es inyectivo decimos que es un* ***monomorfismo de anillos****, si es suprayectivo diremos que es un* ***epimorfismo de anillos****, si es biyectivo diremos que es un* ***isomorfismo de anillos*** *y se denotará por $R \cong R'$. Un morfismo de un anillo en sí mismo es llamado un* ***endomorfismo****, un isomorfismo de un anillo en sí mismo es llamado un* ***automorfismo****.*

Para cualquier morfismo de anillos $\varphi : R \longrightarrow R'$ tenemos asociados los conjuntos

$$Ker(\varphi) := \{a \in R \mid \varphi(a) = 0_{R'}\} \subseteq R' \quad \text{y} \quad Im(\varphi) := \{\varphi(a) \in R' \mid a \in R\} \subseteq R'$$

que son llamados **el núcleo** y **la imagen** de φ respectivamente y de hecho, el núcleo es un ideal de R y la imagen un subanillo de R'. En términos de los conjuntos anteriores podemos pensar las condiciones de inyectividad y suprayectividad para un morfismo de anillos $\varphi : R \longrightarrow R'$ como sigue: φ es inyectivo si y sólo si $Ker(\varphi) = \{0_R\}$ y φ es suprayectivo si y sólo si $Im(\varphi) = R'$.

Observación 0.68. Si $\varphi : R \longrightarrow R'$ es un isomorfismo de anillos, su inversa $\varphi^{-1} : R' \longrightarrow R$ es también un morfismo de anillos. Luego, ya que la composición de funciones biyectivas es biyectiva y que fácilmente se ve que la composición de morfismos de anillos es un morfismo de anillos, entonces la composición de isomorfismos es un isomorfismo, esto junto con la existencia del morfismo identidad muestran que en la clase de todos los anillos tenemos la relación de equivalencia, $\cong$, *ser isomorfo*.

Ejemplo 0.69. Sea R un anillo e I un ideal de R. Entonces existe un epimorfismo de anillos

$$\begin{array}{rcl} \pi : R & \longrightarrow & R/I \\ a & \longmapsto & a + I \end{array}$$

con $I = Ker(\pi)$, y es llamado el **epimorfismo canónico o la proyección natural**.
La existencia de π muestra que todo ideal es el núcleo de un epimorfismo de anillos y que todo anillo cociente es la imagen de un epimorfismo de anillos.

Teorema 0.70. ***Primer teorema de isomorfismo de anillos.***
Sean R, R' anillos y $\varphi : R \longrightarrow R'$ un morfismo de anillos con $I = Ker(\varphi)$. Entonces existe un isomorfismo de anillos $R/I \cong Im(\varphi)$ dado por

$$\begin{array}{rcl} \widehat{\varphi} : R/I & \longrightarrow & Im(\varphi) \subseteq R' \\ a + I & \longmapsto & \varphi(a). \end{array}$$

Tenemos un teorema para anillos que juega el papel del Teorema de Cayley para grupos, éste nos decía todo grupo es isomorfo a un grupo de permutaciones, es decir, que a partir de los grupos simétricos obtenemos esencialmente todos los grupos finitos. En el teorema siguiente, para el caso de anillos el papel de los grupos simétricos es tomado por los anillos de endomorfismos de grupos abelianos.

Teorema 0.71. *Para todo anillo R existe un grupo abeliano A, tal que R es isomorfo a un subanillo de $End(A)$.*

Demostración. Sea R un anillo, y sea $A = (R, +)$ el grupo abeliano aditivo del anillo R, luego, para cada $a \in R$ definamos la función

$$\begin{array}{rcl} \lambda_a : R & \longrightarrow & R \\ r & \longmapsto & ar\ , \end{array}$$

entonces, por la distributividad en R tenemos que

$$\lambda_a(r+s) = a(r+s) = ar + as = \lambda_a(r) + \lambda_a(s),$$

es decir, $\lambda_a \in End(R)$, así podemos definir la función

$$\begin{array}{rcl} \Phi : R & \longrightarrow & End(R) \\ a & \longmapsto & \lambda_a \end{array} \quad \text{donde} \quad \begin{array}{rcl} \lambda_a : R & \longrightarrow & R \\ r & \longmapsto & ar\ , \end{array}$$

que es un morfismo de anillos ya que

$$\begin{array}{c} \lambda_{a+b}(r) = (a+b)r = ar + br = \lambda_a(r) + \lambda_b(r) = (\lambda_a + \lambda_b)(r) \ \text{ y} \\ \lambda_{ab}(r) = (ab)r = a(br) = \lambda_a(\lambda_b(r)) = (\lambda_a \circ \lambda_b)(r)\ , \end{array}$$

es decir,

$$\begin{array}{c} \Phi(a+b) = \lambda_{a+b} = \lambda_a + \lambda_b = \Phi(a) + \Phi(b) \ \text{ y} \\ \Phi(ab) = \lambda_{ab} = \lambda_a \circ \lambda_b = \Phi(a) \circ \Phi(b) \end{array}$$

y $\Phi(1_R)$ tiene como imagen la función

$$\begin{array}{rcl} \lambda_{1_R} : R & \longrightarrow & R \\ r & \longmapsto & 1_R r = r \end{array}$$

que es la identidad en R. Además Φ es inyectiva ya que si $\lambda_a = \lambda_b$ entonces $a = \lambda_a(1_R) = \lambda_b(1_R) = b$. Por último, la imagen de un morfismo de anillos es subanillo del codominio, así $Im(\Phi)$ es subanillo de $End(R)$ y por el primer teorema de isomorfismo de anillos tenemos que $R \cong Im(\Phi)$. ■

Álgebra lineal

Definición 0.72. *Sea $\mathbb{F}$ un campo. Un **espacio vectorial sobre** $\mathbb{F}$ (o un $\mathbb{F}$-espacio vectorial) es un grupo abeliano aditivo V equipado con un **producto por escalar**, que es una función*

$$\begin{array}{rcl} \cdot : \mathbb{F} \times V & \longrightarrow & V \\ (\lambda, v) & \longmapsto & \cdot\big((\lambda, v)\big) \end{array}$$

(donde escribiremos $\cdot\big((\lambda, v)\big)$ simplemente como λv) que satisface los siguientes axiomas para todos $v, u \in V$ y $\lambda, \mu \in \mathbb{F}$

1) $1v = v$.
2) $(\lambda\mu)v = \lambda(\mu v)$.
3) $\lambda(v+u) = \lambda v + \lambda u$.
4) $(\lambda+\mu)v = \lambda v + \mu v$.

*Los elementos de V son llamados **vectores** y los elementos de $\mathbb{F}$ son llamados **escalares**.*

Definición 0.73. *Sea $\mathbb{F}$ un campo y R un anillo. Decimos que R es una $\mathbb{F}$-**álgebra** si tiene estructura de espacio vectorial sobre $\mathbb{F}$ y satisface para todos $\lambda \in \mathbb{F}$ y $r, s \in R$ que*

$$\lambda(rs) = (\lambda r)s = r(\lambda s).$$

Podemos partir también de tener V un espacio vectorial sobre $\mathbb{F}$ y definir un producto en él que lo vuelva anillo y que cumpla la propiedad anterior para definir un álgebra.

Si $v_1, \ldots, v_n$, son vectores en un $\mathbb{F}$-espacio vectorial V, una **combinación lineal** de ellos es un vector $v \in V$ de la forma

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n \text{ para algunos } \lambda_1, \ldots, \lambda_n \in \mathbb{F}.$$

Decimos que $v_1, \ldots, v_n$ forman una lista **linealmente independiente** (abreviado l.i.) si en toda combinación lineal de ellos igualada a cero los escalares son cero, es decir, si $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ para algunos $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ entonces $\lambda_1 = \cdots = \lambda_n = 0$, decimos que es **linealmente dependiente** (abreviado l.d.) en caso contrario.

Definición 0.74. *Sea V un $\mathbb{F}$-espacio vectorial. Un subconjunto $W \subseteq V$ es un **subespacio** de V, denotado por $W \leq V$, si es por sí mismo un $\mathbb{F}$-espacio vectorial bajo la suma y producto por escalar heredados de V. Si W está contenido propiamente en V decimos que es un **subespacio propio** de V y se denota por $W < V$.*

Observación 0.75. $W \leq V$ si y sólo si $0_V \in W$ y para todos $w, u \in W$ y $\lambda \in \mathbb{F}$ se tiene que $w + u \in W$ y $\lambda w \in W$.

Todo espacio vectorial V tiene al menos dos subespacios, $\{0_V\}$ y V llamados los **subespacios triviales**. La relación ser subespacio de V, que denotamos por $\leq$, es un orden parcial en la familia de los subespacios de V. La intersección de una familia arbitraria de subespacios es un subespacio, y la unión de dos subespacios es un subespacio si y sólo si alguno de ellos está contenido en el otro.

Definición 0.76. *Sea V un $\mathbb{F}$-espacio vectorial y $\emptyset \neq S \subseteq V$. El **subespacio generado** por el subconjunto S es el conjunto*

$$\langle S \rangle = \bigcap_{W \leq V, S \subseteq W} W,$$

es decir, la intersección de todos los subespacios de V que contienen a S.

Por ser intersección de subespacios, $\langle S \rangle$ es un subespacio de V y es el menor subespacio de V que contiene a S (por ser la intersección de los subespacios que contienen a S, $\langle S \rangle$ está contenido en todos, es el menor en este sentido) y por lo tanto, si $S \leq V$ entonces $\langle S \rangle = S$. Si $S = \{s\}$, entonces escribimos $\langle s \rangle$ en lugar de $\langle S \rangle$, de forma similar, si $S = \{s_1, \ldots, s_n\}$ escribimos $\langle s_1, \ldots, s_n \rangle$ en lugar de $\langle S \rangle$. Otra forma equivalente de pensar a $\langle S \rangle$ es como el conjunto que consiste de todas las combinaciones lineales finitas de elementos de S, es decir,

$$\langle S \rangle = \{\lambda_1 s_1 + \cdots + \lambda_m s_m \mid m \in \mathbb{N}, s_i \in S, \alpha_i \in \mathbb{F} \ \forall \ i\}.$$

Decimos que $S = \{s_1, \ldots, s_n\}$ **genera** a V si $V = \langle s_1, \ldots, s_n \rangle$, es decir, todo vector en V es combinación lineal de $s_1, \ldots, s_n$. Un subconjunto $\beta = \{v_1, \ldots, v_n\} \subseteq V$ es una **base** de V si β es linealmente independiente y genera a V. Al número de elementos de una base β se le llama la **dimensión** de V, si es un número finito diremos que V tiene **dimensión finita** sobre $\mathbb{F}$ y se denotará por $dim_{\mathbb{F}}(V)$. Si β es una base de V entonces cada elemento $v \in V$ tiene una única expresión como combinación lineal de β, es decir, existen escalares únicos $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ tales que

$$v = \sum_{i=1}^{n} \lambda_i v_i.$$

Si R es una $\mathbb{F}$-álgebra y R como espacio vectorial sobre $\mathbb{F}$ tiene dimensión finita entonces diremos que R es un **álgebra de dimensión finita**.

Todo subespacio de un espacio de dimensión finita también tiene dimensión finita menor o igual que la dimensión del espacio, si se da la igualdad entonces son el mismo espacio, el total.

Dos resultados fundamentales sobre bases (en espacios de dimensión finita) son que todo conjunto generador finito se puede reducir a una base, y que todo conjunto linealmente independiente se puede extender a una base, es decir, si $\{v_1, \ldots, v_k\}$ es linealmente independiente entonces existen $v_{k+1}, \ldots, v_n \in V$ tales que $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ es una base de V.

También, un conjunto con más elementos que una base necesariamente es linealmente dependiente, un subconjunto de un espacio que contenga al cero no puede ser linealmente independiente. Todo subconjunto de un conjunto linealmente independiente es linealmente independiente.

Transformaciones lineales.

Definición 0.77. *Sean V y U espacios vectoriales sobre $\mathbb{F}$ y $T : V \longrightarrow U$ una función. Decimos que T es una **transformación lineal** (un morfismo de espacio vectoriales) si abre la suma y saca escalares, es decir, para todos $v, w \in V$ y $\lambda \in \mathbb{F}$ se tiene que*

$$T(v + w) = T(v) + T(w) \quad y \quad T(\lambda v) = \lambda T(v),$$

*o lo que es lo mismo, es un morfismo de grupos aditivos y respeta el producto por escalar. Si T es una transformación lineal y es inyectiva y suprayectiva diremos que es un **isomorfismo de espacios vectoriales** y se denotará por $V \cong U$. Una transformación lineal de un espacio vectorial en sí mismo es llamado un **operador lineal** en V o un **endomorfismo** de V.*

Toda transformación lineal $T : V \longrightarrow U$ tiene asociados dos subespacios, éstos son

$$Ker(T) := \{u \in V \mid T(v) = 0_U\} \leq V \quad y \quad Im(T) := \{T(v) \in U \mid v \in V\} \leq U$$

que son llamados **el núcleo** y **la imagen** de T respectivamente. En términos del núcleo y la imagen tenemos que para una transformación lineal $T : V \longrightarrow U$, T es inyectiva si y sólo si $Ker(T) = \{0_V\}$ y T es suprayectiva si y sólo si $Im(T) = U$. Una transformación lineal está completamente determinada por su efecto en la base pues abre sumas y saca escalares y cada vector es una combinación única de los elementos de la base.

Definición 0.78. *Sea V un $\mathbb{F}$-espacio vectorial y S_1, S_2 subconjuntos no vacíos de V, la suma de S_1 y S_2 es el conjunto $S_1 + S_2 := \{s_1 + s_2 \mid s_1 \in S_1, s_2 \in S_2\}$. De forma análoga se define la suma de un número finito de subconjuntos no vacíos de V.*

Observación 0.79. Si W_1, W_2 son subespacios de un espacio V entonces la suma $W_1 + W_2$ es un subespacio de V, en particular la suma de cualquier número finito de subespacios es un subespacio.

Definición 0.80. *Se dice que un $\mathbb{F}$-espacio vectorial V es la **suma directa** de subespacios W_1, W_2 si $V = W_1 + W_2$ y $W_1 \cap W_2 = \{0\}$. En general, V es la suma directa de un número finito de subespacios $W_1, \ldots, W_k$, denotada por $\bigoplus_{i=1}^{k} W_i$, si*

$$V = W_1 + \cdots + W_k \quad y \quad W_i \cap \sum_{i \neq j} W_j = \{0\} \text{ para } 1 \leq i \leq k.$$

Observación 0.81. $V = W_1 \oplus \cdots \oplus W_k$ es suma directa de subespacios si y sólo si para todo $v \in V$ existen únicos $w_i \in W_i$ tales que $v = w_1 + \cdots + w_k$.

Teorema 0.82. ***Teorema de la dimensión.***
Sean V y U espacios vectoriales sobre $\mathbb{F}$ con $dim_{\mathbb{F}}(V) < \infty$ y $T : V \longrightarrow U$ una transformación lineal, entonces $Ker(T)$ y $Im(T)$ son de dimensión finita y

$$dim_{\mathbb{F}}(V) = dim_{\mathbb{F}}(Ker(T)) + dim_{\mathbb{F}}(Im(T)).$$

Tenemos a continuación algunos ejemplos básicos del álgebra lineal.

Ejemplo 0.83. El espacio de vectores columna sobre un campo $\mathbb{F}$ son matrices $\begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_n \end{pmatrix}$ de $n \times 1$ con entradas en $\mathbb{F}$ y es identificado con

$$\mathbb{F}^n = \{(a_1, \ldots, a_n) \mid \ a_i \in \mathbb{F}\},$$

es decir, el producto cartesiano del campo consigo mismo n-veces con la suma y producto por escalar entrada a entrada. Una base para este espacio es $\mathcal{C} = \{e_1, ..., e_n\}$ donde $e_i = \begin{pmatrix} 0 \\ \vdots \\ i \\ \vdots \\ 0 \end{pmatrix}$ tiene el 1 en el lugar i y es llamada la **base canónica** de $\mathbb{F}^n$.

Ejemplo 0.84. El espacio de funciones de un conjunto en un campo. Sea X un conjunto no vacío y $\mathbb{F}$ un campo. Entonces el conjunto

$$\mathbb{F}^X = \{f : X \longrightarrow \mathbb{F} \mid f \text{ es función } \}$$

es un $\mathbb{F}$-espacio vectorial con las operaciones puntuales de suma y producto por escalar, es decir,

$$(f + g)(x) = f(x) + g(x) \quad \text{y} \quad (\lambda f)(x) = \lambda f(x), \ \lambda \in \mathbb{F}.$$

Con el producto puntual de funciones, $\mathbb{F}^X$ tiene estructura de anillo y por lo tanto de $\mathbb{F}$-álgebra. Si $|X| < \infty$ entonces $\mathbb{F}^X$ tiene dimensión igual a $|X|$.

Ejemplo 0.85. Espacio de polinomios con coeficientes en un campo.
El anillo $\mathbb{F}[x]$ (ejemplo 0.66) tiene estructura de $\mathbb{F}$-álgebra pues es un $\mathbb{F}$-espacio vectorial con la suma que le da su estructura de anillo y producto por escalar multiplicando a cada coeficiente. Este espacio no tiene dimensión finita, pero para todo $n \in \mathbb{N}$ el conjunto de los polinomios de grado menor o igual que n es un subespacio de $\mathbb{F}[x]$ de dimensión $n + 1$ denotado por $\mathbb{P}_n(\mathbb{F})$.

Ejemplo 0.86. Álgebra de matrices con entradas un campo.
Sea $\mathbb{F}$ un campo, entonces el anillo $\mathcal{M}_{m \times n}(\mathbb{F})$ (del ejemplo 0.63) de matrices de $m \times n$ con entradas en $\mathbb{F}$ es un $\mathbb{F}$-espacio vectorial con la suma (de su estructura de anillo) y producto por escalar entrada a entrada. La base canónica de $\mathcal{M}_{m \times n}(\mathbb{F})$ es el conjunto de matrices $\{E_{ij}\}_{ij}$ donde E_{ij} es la matriz que tiene todas sus entradas iguales a cero salvo la entrada ij, que es igual a 1, estas matrices son llamadas **matrices elementales**. Por lo tanto la dimensión de $\mathcal{M}_{m \times n}(\mathbb{F})$ es nm.

Si $n = m$ entonces escribimos $\mathcal{M}_n(\mathbb{F})$ en lugar de $\mathcal{M}_{m\times n}(\mathbb{F})$. El espacio $\mathcal{M}_n(\mathbb{F})$ tiene como ejemplos de subespacios al conjunto de matrices diagonales $\mathcal{D}_n(\mathbb{F})$ y a los conjuntos de matrices triangulares superiores $TU_n(\mathbb{F})$ e inferiores $TL_n(\mathbb{F})$ y de matrices estrictamente triangulares superiores $STU_n(\mathbb{F})$ e inferiores $STL_n(\mathbb{F})$. El subconjunto $GL_n(\mathbb{F}) = \{A \in \mathcal{M}_n(\mathbb{F}) \mid det(A) \neq 0\}$ forma un grupo con el producto usual de matrices y es conocido como el **grupo general lineal.**

Ejemplo 0.87. El espacio de transformaciones lineales entre dos $\mathbb{F}$-espacios vectoriales. Sean V y U espacios vectoriales sobre $\mathbb{F}$ de dimensiones finitas n y m con bases $\beta = \{v_1, \ldots, v_n\}$ y $\gamma = \{u_1, \ldots, u_m\}$ respectivamente. Entonces el conjunto

$$Hom_{\mathbb{F}}(V, U) := \{T : V \longrightarrow U \mid T \text{ es lineal }\},$$

es decir, todas las transformaciones lineales de V a U, es un $\mathbb{F}$-espacio vectorial con las operaciones puntuales de funciones, es decir,

$$(T + S)(v) := T(v) + S(v) \text{ y } (\lambda T)(v) = \lambda T(v), \text{ para todos } v \in V,\ \lambda \in \mathbb{F}.$$

Una base para este espacio está dada por las funciones $\Lambda = \{T_{ij}\}$ con $1 \leq i \leq m,\ 1 \leq j \leq n$ donde

$$T_{ij}(v_k) = \begin{cases} u_i & si \quad k = j \\ 0 & si \quad k \neq j \end{cases}$$

y por lo tanto su dimensión es nm.
El campo $\mathbb{F}$ es por sí mismo un $\mathbb{F}$-espacio vectorial de dimensión 1, así, el conjunto

$$Hom_{\mathbb{F}}(V, \mathbb{F}) := \{f : V \longrightarrow \mathbb{F} \mid f \text{ es lineal }\}$$

es llamado el **espacio dual** de V y se denota por V^*, un elemento en el espacio dual es llamado un **funcional lineal**. Si V tiene dimensión finita n y $\beta = \{v_1, \ldots, v_n\}$ es una base de V entonces la **base dual** de β, denotada por β^*, es una base para V^* y está dada por las funciones $\beta^* = \{\varphi_1, \ldots, \varphi_n\}$ donde

$$\varphi_i(v_j) = \begin{cases} 1 & si \quad i = j \\ 0 & si \quad i \neq j. \end{cases}$$

Ejemplo 0.88. Todo $\mathbb{F}$-espacio vectorial de dimensión finita n es isomorfo a $\mathbb{F}^n$.
Sea V cualquier $\mathbb{F}$-espacio vectorial de dimensión finita n con base $\beta = \{v_1, \ldots, v_n\}$. Entonces existe un isomorfismo de $\mathbb{F}$-espacios vectoriales

$$\begin{array}{rcl} \phi_\beta : V & \longrightarrow & \mathbb{F}^n \\ v = \sum_{i=1}^{n} \lambda_i v_i & \longmapsto & (\lambda_1, \ldots, \lambda_n) \end{array}$$

y escribiremos $\phi_\beta(v) = (\lambda_1, \ldots, \lambda_n)$ como $[v]_\beta$ y lo llamaremos el **vector de coordenadas** de v con respecto a la base β. Este isomorfismo depende de la elección de la base, si elegimos otra base, el vector de coordenadas se ve diferente.

Observación 0.89. Si $T : V \longrightarrow U$ es un isomorfismo de espacios vectoriales entonces su inversa $T^{-1} : U \longrightarrow V$ es también una transformación lineal. Ya que la composición de funciones biyectivas es biyectiva y que fácilmente se ve que la composición de transformaciones lineales es una transformación lineal, tenemos que la composición de isomorfismos es un isomorfismo, esto junto con la

existencia de la transformación lineal identidad ($id_V(v) = v$ para todo $v \in V$) en cualquier espacio V, muestra que en la clase de todos los $\mathbb{F}$-espacios vectoriales tenemos la relación de equivalencia, $\cong$, *ser isomorfo*. Las **clases de isomorfismo de espacios vectoriales de dimensión finita** están caracterizadas por la dimensión, es decir, dos espacios vectoriales sobre el mismo campo son isomorfos si y sólo si tienen la misma dimensión.

Teorema 0.90. *Sean V y U espacios vectoriales sobre $\mathbb{F}$ de dimensiones finitas n y m con bases $\beta = \{v_1, \ldots, v_n\}$ y $\gamma = \{u_1, \ldots, u_m\}$ respectivamente. Entonces existe un isomorfismo de $\mathbb{F}$-espacios vectoriales*

$$\begin{array}{rcl} \Phi : Hom_{\mathbb{F}}(V,U) & \longrightarrow & \mathcal{M}_{m\times n}(\mathbb{F}) \\ T & \longmapsto & [T]_{\beta}^{\gamma} \end{array}$$

*donde la j-ésima columna de $[T]_{\beta}^{\gamma}$ es $[T(v_j)]_{\gamma}$, el vector de coordenadas de $T(v_j)$ respecto a γ. La matriz $[T]_{\beta}^{\gamma}$ es la **matriz relativa** o la matriz que representa a la transformación lineal T en las bases β y γ.*

Observación 0.91. Si $\gamma = \beta$ escribimos $[T]_{\beta}^{\gamma}$ simplemente como $[T]_{\beta}$. Una de las propiedades fundamentales de este isomorfismo es que preserva la invertibilidad, es decir, la transformación $T : V \longrightarrow U$ es invertible si y sólo si $[T]_{\beta}^{\gamma}$ es invertible, más aún, $\left[T^{-1}\right]_{\gamma}^{\beta} = ([T]_{\beta}^{\gamma})^{-1}$

Teorema 0.92. *Sean V y U espacios vectoriales sobre $\mathbb{F}$ de dimensiones finitas n y m con bases $\beta = \{v_1, \ldots, v_n\}$ y $\gamma = \{u_1, \ldots, u_m\}$ respectivamente. Si $T, S : V \longrightarrow U \in Hom_{\mathbb{F}}(V,U)$ entonces*

$$[T+S]_{\beta}^{\gamma} = [T]_{\beta}^{\gamma} + [S]_{\beta}^{\gamma} \quad y \quad [\lambda T]_{\beta}^{\gamma} = \lambda\,[T]_{\beta}^{\gamma},$$

es decir, la matriz asociada a una suma de transformaciones lineales es la matriz resultante de la suma de las matrices asociadas a dichas transformaciones y la matriz asociada al producto de un escalar por una transformación es la matriz resultante de multiplicar el escalar por la matriz asociada a dicha transformación.

Análogo al teorema anterior, el comportamiento de matrices asociadas a una composición de funciones es:

Teorema 0.93. *Sean V, U y W espacios vectoriales sobre $\mathbb{F}$ de dimensiones finitas n, m y l con bases $\beta = \{v_1, \ldots, v_n\}, \gamma = \{u_1, \ldots, u_m\}$ y $\delta = \{w_1, \ldots, w_l\}$ respectivamente. Si $T \in Hom_{\mathbb{F}}(V,U)$ y $S \in Hom_{\mathbb{F}}(U,W)$ entonces $S \circ T \in Hom_{\mathbb{F}}(V,W)$ y*

$$[S \circ T]_{\beta}^{\delta} = [S]_{\gamma}^{\delta}\,[T]_{\beta}^{\gamma}$$

es decir, la matriz asociada a una composición de transformaciones lineales es la matriz resultante del producto de las matrices asociadas a dichas transformaciones.

Si V es un $\mathbb{F}$-espacio vectorial de dimensión finita n con base $\beta = \{v_1, \ldots, v_n\}$, entonces la matriz asociada a la transformación identidad en V es la identidad de tamaño n, es decir,

$$[I_V]_{\beta} = I_n.$$

Luego, otro resultado fundamental es que multiplicar a la izquierda un vector columna por la matriz asociada a una transformación lineal es una transformación lineal y *hace lo mismo* que T pues la representa, es decir,

$$[T]_{\beta}^{\gamma}\,[v]_{\beta} = [T(v)]_{\gamma} \text{ para todo } v \in V.$$

En las Matemáticas, para simplificar expresiones a algunas más sencillas se utiliza a menudo un *cambio de variable*, en el álgebra lineal, cambiar de variable se hace mediante una matriz:
Si V es un $\mathbb{F}$-espacio vectorial de dimensión finita n con bases $\beta = \{v_1, \ldots, v_n\}$ y $\beta' = \{v'_1, \ldots, v'_n\}$, entonces, si $Q = [I_V]_{\beta}^{\beta'}$ tenemos que

$$[v]_{\beta'} = [I_V]_{\beta}^{\beta'}\,[v]_{\beta} = Q\,[v]_{\beta}$$

La matriz Q es llamada **la matriz de cambio de coordenadas** que transforma las coordenadas de β en coordenadas de β'. Podemos preguntarnos por la relación entre las matrices asociadas a dos bases distintas del dominio y el codominio de una transformación lineal, es decir, si V es un $\mathbb{F}$-espacio vectorial de dimensión finita n con bases $\beta = \{v_1, \ldots, v_n\}$ y $\beta' = \{v'_1, \ldots, v'_n\}$, y U es un $\mathbb{F}$-espacio vectorial de dimensión finita m con bases $\gamma = \{u_1, \ldots, u_m\}$ y $\gamma' = \{u'_1, \ldots, u'_m\}$, entonces, si $Q = [I_V]_{\beta}^{\beta'}$ y $P = [I_U]_{\gamma}^{\gamma'}$ tenemos que

$$[T]_{\beta'}^{\gamma'} = [I_U]_{\gamma}^{\gamma'}\,[T]_{\beta}^{\gamma}\,[I_V]_{\beta'}^{\beta} = P\,[T]_{\beta}^{\gamma}\,Q^{-1}.$$

En particular, para un operador lineal $T : V \longrightarrow V$ se tiene que

$$[T]_{\beta'} = [I_V]_{\beta}^{\beta'}\,[T]_{\beta}\,[I_V]_{\beta'}^{\beta} = Q\,[T]_{\beta}^{\gamma}\,Q^{-1}$$

es decir, matrices que representan a un operador lineal en distintas bases son conjugadas, la matriz que las hace conjugadas es la matriz de cambio de coordenadas. Y también tenemos que

$$det\left([T]_{\beta}\right) = det\left([T]_{\beta'}\right)$$

pues el determinante es multiplicativo y son matrices conjugadas. Así, **el determinante de un operador lineal** T, denotado por $det(T)$, es el determinante de la matriz asociada a T en cualquier base de V y está bien definido pues es independiente de la elección de la base, de la misma forma, la **traza de un operador lineal** T, denotada por $tr(T)$, es la traza de la matriz (la suma de los elementos de la diagonal) asociada al operador en alguna base.

Teorema 0.94. *Si V es un $\mathbb{F}$-espacio vectorial de dimensión finita n y T un operador lineal en V, entonces T es invertible (es un isomorfismo) si y sólo si $det(T) \neq 0$.*

Sea V un $\mathbb{F}$-espacio vectorial de dimensión finita n y T un operador lineal en V, entonces hay una pregunta evidente: ¿existe una base β de V tal que $[T]_{\beta}$ es una matriz diagonal?, y si existe dicha base, ¿cómo puede encontrarse?. Para responder a esta pregunta se necesita el concepto de diagonalización de un operador lineal.

Definición 0.95. *Si V es un $\mathbb{F}$-espacio vectorial de dimensión finita n y T un operador lineal en V, decimos que T es **diagonalizable** si existe una base β de V tal que $[T]_{\beta}$ es una matriz diagonal. Una matriz cuadrada es diagonalizable si es similar (conjugada) a una matriz diagonal.*

Definición 0.96. *Si T es un operador lineal en un $\mathbb{F}$-espacio vectorial V de dimensión finita n, decimos que $0 \neq v \in V$ es un **vector propio** de T si existe $\lambda \in \mathbb{F}$ tal que $T(v) = \lambda v$. Al escalar λ se le llama **valor propio** asociado al vector propio v.*

Teorema 0.97. *Sea V un $\mathbb{F}$-espacio vectorial de dimensión finita n y T un operador lineal en V. Entonces T es diagonalizable en V si y sólo si existe una base $\beta = \{v_1, \ldots, v_n\}$ de V y escalares $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ (no necesariamente distintos) tales que $T(v_j) = \lambda v_j$, así*

$$[T]_\beta = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

Definición 0.98. *Sea V un $\mathbb{F}$-espacio vectorial de dimensión finita n con $\beta = \{v_1, \ldots, v_n\}$ cualquier base de V y sea T un operador lineal en V. Entonces, el **polinomio característico** de T es el polinomio en la indeterminada t dado por*

$$p(t) := det\left([T]_\beta - tI_n\right) .$$

Observación 0.99. El polinomio característico es de grado n y por lo tanto T tiene a lo más n valores propios distintos (se pueden repetir). El coeficiente principal del polinomio característico es $(-1)^n$. Entonces λ es valor propio de T si y sólo si λ es raíz del polinomio característico.

Teorema 0.100. *Si V es un $\mathbb{F}$-espacio vectorial de dimensión finita n y T es un operador diagonalizable en V, entonces su polinomio característico $p(t)$ se descompone como producto de n factores, todos de grado 1, es decir, existen escalares $\lambda_1, \ldots, \lambda_n$ (no necesariamente distintos) tales que*

$$p(t) = (-1)^n(t - \lambda_1)(t - \lambda_2)\cdots(t - \lambda_n)$$

Definición 0.101. *El **polinomio mínimo** $m(t)$, de un operador lineal T es el polinomio mónico de menor grado que anula a T, es decir, $m(T) = T_0$, donde T_0 es la transformación lineal cero.*

La propiedad fundamental del polinomio mínimo es que divide a cualquier otro polinomio que anule al operador T, en particular divide al polinomio característico (que se anula en T por el teorema de Cayley-Hamilton) y además el polinomio mínimo es único.

Teorema 0.102. *Si T es un operador en un $\mathbb{F}$-espacio vectorial V de dimensión finita n, entonces T es diagonalizable si y sólo si el polinomio mínimo $m(t)$ de T se descompone como producto de factores lineales, es decir,*

$$m(t) = (-1)^n(t - \lambda_1)(t - \lambda_2)\cdots(t - \lambda_k)$$

donde los escalares $\lambda_1, \ldots, \lambda_k$ son los distintos valores propios de T.

Observación 0.103. Dado un polinomio

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

mónico de grado n en $\mathbb{F}\,]x]$, la **matriz compañera** de $p(x)$ es la matriz

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

y además el polinomio característico de A es $p(x)$.

Definición 0.104. *Sean R y S dos álgebras sobre un campo $\mathbb{F}$. Un* ***morfismo de álgebras*** *es un morfismo de anillos de R en S que es además una transformación lineal. Un* ***isomorfismo de álgebras*** *es un isomorfismo de anillos que es también un isomorfismo de $\mathbb{F}$-espacios vectoriales.*

Para álgebras existe una versión del Teorema de Cayley en su versión para anillos, y éste en grupos significaba que todo grupo finito es genéricamente un subgrupo de permutaciones y eso se hacía con un monomorfismo del grupo en su grupo simétrico y éste inducía una acción en el grupo que era la traslación izquierda, donde además, el Teorema de Cayley era un caso particular de la acción de un grupo dado en un cociente de él por uno de sus subgrupos, por la traslación izquierda de clases izquierdas; tomando el subgrupo como el grupo trivial teníamos el Teorema de Cayley. La versión para anillos dice que todos los anillos son genéricamente subanillos de anillos de endomorfismos de grupos abelianos. La versión en álgebras es:

Teorema 0.105. *Sea R una $\mathbb{F}$-álgebra de dimensión finita. Entonces para algún $n \in \mathbb{N}$ el álgebra R es isomorfa a un subanillo de $\mathcal{M}_{n\times n}(\mathbb{F})$.*

Demostración. Consideremos la función

$$\begin{array}{rcl} \Lambda : R & \longrightarrow & End(R) \\ r & \longmapsto & \lambda_r \end{array} \quad \text{donde} \quad \begin{array}{rcl} \lambda_r : R & \longrightarrow & R \\ x & \longmapsto & rx \ . \end{array}$$

Entonces Λ es un morfismo de anillos pues para todos r, s y $x \in R$ tenemos que

$$\lambda_{r+s}(x) = (r+s)x = rx + sx = \lambda_r(x) + \lambda_s(x) = (\lambda_r + \lambda_s)(x) \quad \text{y}$$
$$\lambda_{rs}(x) = (rs)x = r(sx) = \lambda_r(\lambda_s(x)) = (\lambda_r \circ \lambda_s)(x) \ .$$

Además Λ es una transformación lineal pues ya vimos que abre suma y tenemos que si $a \in \mathbb{F}$

$$\lambda_{ar}(x) = (ar)x = a(rx) = a\lambda_r(x).$$

Por lo tanto, Λ es morfismo de álgebras, y por último, Λ es inyectivo ya que si $\lambda_r = \lambda_s$, entonces $r = \lambda_r(1_R) = \lambda_s(1_R) = s$. Por el primer teorema de isomorfismo de anillos,

$$R \cong Im(\Lambda) \leq End_{\mathbb{F}}(R) \cong \mathcal{M}_{n\times n}(\mathbb{F})$$

donde $n = dim_{\mathbb{F}}(R)$. ■

Módulos

La importancia de los Módulos en este trabajo se debe a que éstos son un concepto básico unificador en las Matemáticas ya que son la generalización de otro tipo de estructura algebraica: los espacios vectoriales y los grupos abelianos, más precisamente: los módulos son a anillos, como espacios vectoriales son a campos, es decir, los escalares ahora serán tomados en un anillo en lugar de un campo y al debilitar así las propiedades de los escalares se obtiene la teoría de módulos para explicar como ejemplos a la teoría de anillos y a la teoría de grupos abelianos finitos, también la teoría de Representaciones está en estos términos pues es el estudio de simetrías de espacios vectoriales.

Definición 0.106. *Sea R cualquier anillo con 1_R no necesariamente conmutativo. Un* ***R-módulo izquierdo*** *es una pareja $(M,\cdot)$, donde M es un grupo abeliano (aditivo) y $\cdot$ es un* ***producto por escalar****, que es una función*

$$\begin{array}{rcl} \cdot : R \times M & \longrightarrow & M \\ (r,m) & \longmapsto & \cdot\big((r,m)\big) \end{array}$$

(donde escribiremos $\cdot\big((r,m)\big)$ simplemente como rm) que satisface los siguientes axiomas para todos $a,b \in R$ y $m,n \in M$

$m_1)$ $1_R m = m$.

$m_2)$ $(ab)m = a(bm)$.

$m_3)$ $a(m+n) = am + an$.

$m_4)$ $(a+b)m = am + bm$.

Vamos a ver que una estructura de módulo sobre un anillo induce cierto morfismo de anillos del anillo en el anillo de endomorfismos del módulo (del grupo abeliano aditivo subyacente).

Teorema 0.107. *Sea M un R-módulo izquierdo. Entonces el producto por escalar $\cdot$ induce un morfismo de anillos $\lambda : R \longrightarrow End(M)$.*

Demostración. Consideremos la función

$$\begin{array}{rcl} \lambda : R & \longrightarrow & End(M) \\ r & \longmapsto & \lambda(r) \end{array} \quad \text{donde} \quad \begin{array}{rcl} \lambda(r) : M & \longrightarrow & M \\ m & \longmapsto & rm \ , \end{array}$$

que es un morfismo de anillos unital, es decir, manda el uno en el uno ya que

$$\begin{gathered} \lambda(r+s)(m) = (r+s)m = rm + sm = \lambda(r)(m) + \lambda(s)(m) \ \ , \\ \lambda(rs)(m) = (rs)m = r(sm) = \lambda(r)(\lambda(s)(m)) = (\lambda(r) \circ \lambda(s))(m) \text{ , y} \\ \lambda(1_R)(m) = 1_R m = m = id_M(m). \end{gathered}$$

■

El recíproco, como en el caso de grupos (Teorema de Cayley) es cierto:

Teorema 0.108. *Sea R un anillo con 1_R y M un grupo abeliano aditivo y supongamos que existe un morfismo de anillos $\lambda : R \longrightarrow End(M)$, entonces M es un R-módulo izquierdo.*

Demostración. Consideremos la función

$$\begin{array}{rcl} \cdot : R \times M & \longrightarrow & M \\ (r,m) & \longmapsto & \cdot\big((r,m)\big) = rm := \lambda(r)(m) \ . \end{array}$$

Entonces satisface para todos $r,s \in R$ y $m,n \in M$ que

$m_1)$ $1_R m := \lambda(1_R)(m) = id_M(m) = m$.

$m_2)$ $(rs)m := \lambda(rs)(m) = \big(\lambda(r) \circ \lambda(s)\big)(m) = \lambda(r)\big(\lambda(s)(m)\big) := r(sm)$.

$m_3)$ $r(m+n) := \lambda(r)(m+n) = \lambda(r)(m) + \lambda(r)(n) := rm + rn$.

$m_4)$ $(r+s)m := \lambda(r+s)(m) = \lambda(r)(m) + \lambda(s)(m) = (\lambda(r) + \lambda(s))(m) := rm + sm$.

Por lo tanto $\cdot$ es un producto por escalar y así M es un R-módulo izquierdo. ■

Entonces, un grupo abeliano aditivo equipado con un producto por escalar (un módulo sobre un anillo con uno) *es lo mismo* que un morfismo de anillos del anillo en el anillo de endomorfismos del grupo abeliano.
Notemos que los dos primeros axiomas nos dicen que si M es un R-módulo izquierdo entonces existe una *acción* del anillo R en el grupo abeliano M. Esto es análogo a las acciones en grupos como habíamos establecido en el teorema 0.71, y por ese teorema y el anterior tenemos que todo anillo es un módulo sobre sí mismo, que es un ejemplo clásico que se logra si definimos el producto por escalar por elementos del anillo como el producto en el anillo, y de hecho este ejemplo es el análogo a que todo campo es un espacio vectorial de dimensión 1 sobre sí mismo.

Definición 0.109. *Sea R un anillo con 1_R y M un grupo abeliano aditivo. Un morfismo de anillos $\lambda : R \longrightarrow End(M)$ es llamado una* ***representación del anillo*** *R.*

De la definición y los dos teoremas anteriores tenemos que las representaciones de anillos pueden traducirse al lenguaje de módulos, es decir, toda representación de un anillo induce una estructura de módulo sobre el anillo, y toda estructura de módulo sobre el anillo induce una representación del anillo. Más claramente:

Teorema 0.110. *Si R es un anillo con uno, existe una correspondencia biyectiva entre los R-módulos izquierdos y las representaciones de R en anillos de endomorfismos de grupos abelianos.*

Ejemplo 0.111. Para cualquier anillo R, el R-módulo más simple es él mismo definiendo un producto por escalar por elementos de R como el producto en R, y se denota por ${}_RR$, que es llamado la **representación regular del anillo** R.

Ejemplo 0.112. Si $\mathbb{F}$ es un campo, los $\mathbb{F}$-espacios vectoriales son $\mathbb{F}$-módulos pues satisfacen los mismos axiomas y en particular todo campo es un anillo.

Ejemplo 0.113. Todos los grupos abelianos son $\mathbb{Z}$-módulos por las leyes de los exponentes.

Definición 0.114. *Sea M un R-módulo. Un subconjunto $N \subseteq M$ es un* ***submódulo*** *de M, denotado por $N \leq M$, si es por sí mismo un R-módulo con la suma y producto por escalar heredados de M. Si N está contenido propiamente en M decimos que es un* ***submódulo propio*** *de M y se denota por $N < M$.*

Observación 0.115. $N \leq M$ si y sólo si N es un subgrupo abeliano aditivo de M y $rn \in N$ para todos $r \in R$ y $n \in N$.

Todo R-módulo M tiene al menos dos submódulos, $\{0\}$ y M llamados el **submódulo trivial** y el **submódulo impropio** respectivamente. Un R-módulo es **simple** o (**irreducible**) si sus únicos submódulos son él mismo y el trivial.
La relación de ser submódulo de M, que denotamos por $\leq$, es un orden parcial en la familia de los submódulos de M. La intersección de una familia arbitraria de submódulos es un submódulo.

Definición 0.116. *Sea M un R-módulo y $\emptyset \neq X \subseteq M$. El* ***submódulo generado por*** *X es el conjunto*

$$\langle X\rangle = \bigcap_{N\leq M, X\subseteq N} N,$$

es decir, la intersección de todos los submódulos de M que contienen a X.

Por ser la intersección de submódulos, $\langle X\rangle$ es un submódulo de M y es el menor submódulo de M que contiene a X (por ser la intersección de los submódulos que contienen a X, $\langle X\rangle$ está contenido en todos, es el menor en este sentido) y por lo tanto, si $N \leq M$ entonces $\langle N\rangle = N$. Si $X = \{x\}$, entonces escribimos $\langle x\rangle$ en lugar de $\langle X\rangle$, de forma similar, si $X = \{x_1, \ldots, x_k\}$ escribimos $\langle x_1, \ldots, x_k\rangle$ en lugar de $\langle X\rangle$. Si N es un R-submódulo de un R-módulo M, decimos que N es finitamente generado si puede ser generado por un subconjunto finito de M, es decir, $N = \langle x_1, \ldots, x_k\rangle$ con $\{x_1, \ldots, x_k\} \subseteq M$.
El **submódulo cíclico generado por** $m \in M$ es el conjunto

$$\langle m\rangle = Rm = \{y \in M \mid rm = y \text{ para algún } r \in R\}.$$

Si $X = \{x_i \mid i \in I\}$, una R-combinación lineal de elementos de X es un elemento de la forma $r_1x_1 + \cdots + r_lx_l = 0$ con $r_1, \ldots, r_l \in R$, es decir, una expresión de la forma $\sum_{i\in I} r_ix_i$ con $r_i \in R$ y sólo un número finito de $r_i \neq 0$. Un subconjunto $X = \{x_1, \ldots, x_k\} \subseteq M$ es llamado **R-linealmente dependiente** si existen elementos distintos $x_1, \ldots, x_l \in X$ y $r_1, \ldots, r_l \in R$ no todos nulos tales que

$$r_1x_1 + \cdots + r_lx_l = 0.$$

X es **R-linealmente independiente** si para cualesquiera elementos distintos $x_1, \ldots, x_l \in X$, tenemos que $x_1r_1 + \cdots + r_lx_l = 0$ con $r_1, \ldots, r_l \in R$, implica que $r_1 = \cdots = r_l = 0$.
Un R-módulo M es **finitamente generado** si es generado por un subconjunto finito de M, es decir,

$$M = \langle x_1, \ldots, x_k\rangle = \sum_{x_i\in X} Rx_i$$

con $\{x_1, \ldots, x_k\} \subseteq M$. Decimos que $x_1, \ldots, x_k$ son **generadores** de M.
Un subconjunto $B \subseteq M$ es una **base** de M si B es R-linealmente independiente y genera a M. Un R-módulo que tenga base es llamado **módulo libre.** Por ejemplo, el módulo trivial $\{0\}$ es libre, su base es el conjunto vacío. Todo $\mathbb{F}$-espacio vectorial de dimensión finita es un $\mathbb{F}$-módulo libre. De hecho, $B \subseteq M$ es una base de M si todo elemento de M se puede escribir de forma única como R-combinación lineal de elementos de B.

Definición 0.117. *Sean M y N R-módulos. Una función $f : M \longrightarrow N$ es un R-**morfismo** si para todos $m_1, m_2 \in M$ y $r \in R$ se tiene que*

$$f(m_1 + m_2) = f(m_1) + f(m_2) \quad y \quad f(rm_1) = rf(m_1)$$

*o lo que es lo mismo, es un morfismo de grupos aditivos y respeta el producto por escalar. Si f es un R-morfismo y es inyectivo y suprayectivo diremos que es un **isomorfismo de R-módulos** y se denotará por $M \cong N$. Un R-morfismo de un R-módulo en sí mismo es llamado un **endomorfismo** de R.*

Todo R-morfismo $f : M \longrightarrow N$ tiene asociados dos submódulos, estos son

$$Ker(f) := \{m \in M \mid f(m) = 0\} \leq M \quad y \quad Im(f) := \{f(m) \in N \mid m \in M\} \leq N$$

que son llamados **el núcleo** y **la imagen** de f respectivamente.
Sea M un R-módulo y $\{M_i\}_{i\in I}$ una familia de submódulos. Entonces su unión en general no es submódulo, pero el generado de la unión sí lo es y corresponde a la **suma de submódulos**, es decir,

$$\langle \bigcup_{i\in I} M_i \rangle = \sum_{i\in I} M_i.$$

Definición 0.118. *Sea M un R-módulo y $\{M_i\}_{i\in I}$ una familia de submódulos, entonces M es la* ***suma directa interna*** *de la familia $\{M_i\}_{i\in I}$, denotada por $M = \bigoplus_{i\in I} M_i$, si*

$$M = \sum_{i\in I} M_i \text{ y para cada } k \in I \text{ se tiene que } M_k \bigcap \sum_{i\neq k} M_i = \{0\}.$$

Observación 0.119. $M = \bigoplus_{i\in I} M_i$ si y sólo si para todo $m \in M$ existen únicos $m_i \in M_i, i \in I$ tales que $m = \sum_{i\in I} m_i$ con $m_i \neq 0$ para un número finito de índices i.

Un R-módulo M es **semisimple** si es suma directa de submódulos simples (irreducibles) o equivalentemente si todo R-submódulo N tiene complemento, es decir, existe un R-submódulo $\tilde{N}$ tal que $M = N \oplus \tilde{N}$. Por ejemplo, todo $\mathbb{F}$-espacio vectorial es un $\mathbb{F}$-módulo semisimple, cada subespacio tiene complemento y no es único en general porque su existencia depende de una base del subespacio dado.

Teorema 0.120. *Un R-módulo es libre si y sólo si es isomorfo a una suma directa de copias del R-módulo ${}_RR$.*

Observación 0.121. El centro de una $\mathbb{F}$-álgebra contiene una copia de $\mathbb{F}$.
Sea A una $\mathbb{F}$-álgebra con uno y sea $Z(A)$ el centro de A, entonces $Z(A)$ contiene una copia de $\mathbb{F}$, donde hacemos la identificación (la inclusión de $\mathbb{F}$ en A)

$$\begin{array}{rcl} i_{\mathbb{F}} : \mathbb{F} & \longrightarrow & A \\ \lambda & \longmapsto & \lambda \cdot 1_A \end{array}$$

que es un morfismo de anillos. Por lo tanto, si M es un A-módulo izquierdo (módulo sobre el álgebra A, denotado por ${}_AM$) entonces su producto por escalar

$$\begin{array}{rcl} * : A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & a * m = am \end{array}$$

define una estructura de $\mathbb{F}$-espacio vectorial en M (denotado por ${}_{\mathbb{F}}M$) con el producto por escalar

$$\begin{array}{rcl} \star : \mathbb{F} \times M & \longrightarrow & M \\ (\lambda, m) & \longmapsto & \lambda \star m := (\lambda \cdot 1_A) * m. \end{array}$$

Luego, si $\psi \in End_A(M) = \{f : M \longrightarrow M \mid f \text{ es un } A\text{-morfismo } \}$ (que es un A-módulo con las operaciones puntuales si el álgebra A es conmutativa) entonces $\lambda\psi(m) = \psi(\lambda m)$ para todos $\lambda \in \mathbb{F}, m \in M$, así, como $\mathbb{F}$-espacios vectoriales tenemos que

$$End_A(M) \leq End_{\mathbb{F}}(M) = \{T : M \longrightarrow M \mid T \text{ es un } \mathbb{F}\text{-morfismo } \} = \{T : M \longrightarrow M \mid T \text{ es lineal } \}.$$

Representaciones de Grupos

Los grupos aparecen naturalmente en la Matemáticas como conjuntos de *simetrías* de un objeto, por ejemplo $S_n, A_n, D_8, O(3)$. Luego, desde el punto de vista de la geometría, surge la pregunta, ¿dado un objeto geométrico X, cuál es su grupo de simetrías G?, la teoría de representaciones revierte esta pregunta a la siguiente: ¿Dado un grupo, en qué objetos X actúa? e intentaremos responder a esta pregunta clasificando tales X salvo isomorfismo.

Una representación es una relación muy general que expresa similitudes entre entre objetos, más claramente, una colección de objetos puede ser **representada** por otra colección de objetos.

La idea detrás de la teoría de representaciones de grupos finitos es **pensar a los grupos como endomorfismos (transformaciones lineales) de un espacio vectorial**. Por supuesto, si algo se va a *ver* como un grupo debemos tener en ese algo la propiedad de que cada elemento sea invertible, entonces la idea es trabajar con isomorfismos de espacios vectoriales, que en el caso de dimensión finita se pueden codificar mediante matrices invertibles.
Así, la teoría de representaciones es el estudio de los morfismos de grupos abstractos a grupos de automorfismos de espacios vectoriales, y cada uno de estos morfismos produce invariantes que son números cuyas propiedades aritméticas ayudan a probar teoremas acerca del grupo.
Estamos interesados en el caso en el que el espacio vectorial es de dimensión finita, y así, una representación nos da una forma de visualizar a cada elemento de un grupo como una matriz invertible (de tamaño igual a la dimensión del espacio) con entradas en el campo de escalares del espacio vectorial.

Representaciones de Grupos y $\mathbb{F}G$-Módulos

De aquí en adelante, a menos que se indique lo contrario, G denotará siempre un grupo finito, V denotará a un espacio vectorial de dimensión finita $n \in \mathbb{Z}^+$ sobre $\mathbb{F} = \mathbb{R}$ o $\mathbb{C}$ y $GL(V)$ denotará al grupo de los isomorfismos de V (con la composición). Bajo estas condiciones tenemos un isomorfismo de $\mathbb{F}$-espacios vectoriales $V \cong \mathbb{F}^n$ (donde $\mathbb{F}^n$ es el espacio de vectores columna con entradas en $\mathbb{F}$), dado por el vector de coordenadas respecto a alguna base de V, y también un isomorfismo de grupos $GL(V) \cong GL_n(\mathbb{F})$, donde $GL_n(\mathbb{F})$, denota al grupo de matrices invertibles de $n \times n$ con entradas en $\mathbb{F}$ (con el producto de matrices).
Vamos a dar ahora dos definiciones y veremos que realmente son equivalentes.

Definición 0.122. *Un morfismo de grupos $\rho : G \longrightarrow GL_n(\mathbb{F})$ es llamado* ***una representación de G sobre $\mathbb{F}$*** *y el* ***grado de la representación*** *es el entero n.*

Definición 0.123. *Sea V un espacio vectorial sobre $\mathbb{F}$ y sea G un grupo. Decimos que V es un $\mathbb{F}G$-**módulo** si existe una acción de G en V compatible con la estructura de espacio vectorial de V (también se usa el término **acción lineal**), es decir, hay definida una multiplicación gv que safistace los siguientes axiomas para cualesquiera $u, v \in V,\ g, h \in G$ y $\lambda \in \mathbb{F}$:*

1) $gv \in V$
2) $e_G v = v$
3) $(gh)v = g(hv)$
4) $g(\lambda v) = \lambda(gv)$
5) $g(v + u) = gv + gu$.

Tenemos ahora la conexión entre $\mathbb{F}G$-módulos y representaciones de G sobre $\mathbb{F}$.

Teorema 0.124. *Sea $\rho : G \longrightarrow GL_n(\mathbb{F})$ una representación de G sobre $\mathbb{F}$, entonces $V = \mathbb{F}^n$ tiene estructura de $\mathbb{F}G$-módulo.*

Demostración. La función

$$\begin{array}{rcl} \cdot : (G \times V) & \longrightarrow & V \\ (g, v) & \longmapsto & gv := \rho(g)v \end{array}$$

define una acción lineal de G en V ya que para todos $u, v \in V,\ g, h \in G$ y $\lambda \in \mathbb{F}$ tenemos que

1) $gv = \rho(g)v \in V$ pues el producto $\rho(g)v$ es una matriz de $n \times 1$.
2) $e_G v = \rho(e_G)v = I_n v = v$ pues ρ es un morfismo de grupos.
3) $(gh)v = \rho(gh)v = \rho(g)\rho(h)v = g(hv)$ pues ρ es un morfismo de grupos.
4) $g(\lambda v) = \rho(g)(\lambda v) = \lambda(\rho(g)v) = \lambda(gv)$ ya que el producto de matrices saca escalares.
5) $g(v + u) = \rho(g)(v + u) = \rho(g)v + \rho(g)u = gv + gu$ pues el producto de matrices distribuye a la suma de matrices.

Por lo tanto $\mathbb{F}^n$ es un $\mathbb{F}G$-módulo con esta multiplicación por elementos de G. ■

El recíproco de hecho es cierto, y completa la equivalencia (conexión) de la que hablábamos.

Teorema 0.125. *Sea V un $\mathbb{F}G$-módulo. Entonces existe una representación de G sobre $\mathbb{F}$.*

Demostración. Definimos para todo $g \in G$ la función

$$\begin{array}{rcl} \rho_g : V & \longrightarrow & V \\ v & \longmapsto & gv \end{array}$$

que es un endomorfismo de V (operador lineal) por las condiciones 1), 4) y 5) de la definición de $\mathbb{F}G$-módulo, es decir, ya que existe una acción lineal de G en V, para todos $u, v \in V,\ g \in G,\ \lambda \in \mathbb{F}$ tenemos que

- $\rho_g(v) = gv \in V$.
- $\rho_g(v+u) = g(v+u) = gv + gu = \rho_g(v) + \rho_g(u)$.
- $\rho_g(\lambda v) = g(\lambda v) = \lambda(gv) = \lambda\rho_g(v)$.

Luego, sea β una base de V y para cada $g \in G$ sea $[\rho_g]_\beta \in GL_n(\mathbb{F})$, que abreviaremos como $[g]_\beta$, la matriz asociada al operador ρ_g con respecto a la base β. Ahora, para todos $g, h \in G$ notemos que

$$\rho_{gh}(v) = (gh)v = g(hv) = \rho_g(hv) = (\rho_g \circ \rho_h)(v),$$

por lo que los operadores lineales ρ_{gh} y $\rho_g \circ \rho_h$ son iguales, y como la matriz asociada a una composición de transformaciones lineales es igual al producto de las matrices asociadas a cada transformación tenemos que

$$[gh]_\beta = [g]_\beta\,[h]_\beta,$$

y en particular se tiene que

$$[g]_\beta \left[g^{-1}\right]_\beta = [e_G]_\beta = I_n.$$

Por lo tanto, concluimos que para todo $g \in G$, la matriz $[g]_\beta$ es invertible con inversa $\left[g^{-1}\right]_\beta$ y así $\left[g^{-1}\right]_\beta = {[g]_\beta}^{-1}$. Y entonces la función

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [g]_\beta \end{array}$$

es una representación de G sobre $\mathbb{F}$ ya que es un morfismo de grupos pues tenemos que

$$\rho(gh) = [gh]_\beta = [g]_\beta\,[h]_\beta = \rho(g)\rho(h)$$

para todos $g, h \in G$. ■

Observación 0.126. Concluimos que toda representación $\rho : G \longrightarrow GL_n(\mathbb{F})$ de G sobre $\mathbb{F}$ induce una estructura de $\mathbb{F}G$-módulo en $\mathbb{F}^n$ (y por lo tanto en cualquier espacio vectorial de dimensión n) con la acción lineal $gv := \rho(g)v$. Y recíprocamente, si en un espacio vectorial V de dimensión n existe una acción lineal de un grupo G, entonces ésta induce una representación de G sobre $\mathbb{F}$, con la notación del teorema anterior

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [\rho_g]_\beta \end{array} \quad \text{donde} \quad \begin{array}{rcl} \rho_g : V & \longrightarrow & V \\ v & \longmapsto & gv\ , \end{array}$$

Con esto, también podemos pensar a una representación de grado n de un grupo G como una pareja consistente del espacio vectorial $\mathbb{F}^n$ y de un morfismo de grupos $\rho : G \longrightarrow GL_n(\mathbb{F})$.

Por lo tanto, los dos teoremas y la observación anteriores nos dicen que estudiar las representaciones de grupos es equivalente a estudiar las acciones lineales de grupos, es decir, nos garantizan que:

Teorema 0.127. *Sea G un grupo. Entonces existe una correspondencia biyectiva entre el conjunto de representaciones de G sobre $\mathbb{F}$ (morfismos de G en $GL_n(\mathbb{F})$) y el conjunto de acciones lineales de G en el espacio vectorial $\mathbb{F}^n$.*

Así, existen dos maneras de pensar a la teoría de representaciones, mediante las representaciones mismas, o mediante sus $\mathbb{F}G$-módulos inducidos correspondientes. De aquí en adelante usaremos indistintamente representaciones o $\mathbb{F}G$-módulos de acuerdo a cómo nos convenga.

Álgebra de Grupo y Módulos

Existe una visión más moderna para la teoría de representaciones de grupos finitos, ésta requiere otro concepto equivalente a una acción lineal: los módulos finitamente generados sobre álgebras de grupo, haremos en lo que sigue esa construcción y se omitirán algunas demostraciones ya que se trata de resultados clásicos sobre teoría de módulos.
En el contexto de la teoría de representaciones los grupos son considerados como conjuntos abstractos de operadores lineales en un espacio vectorial de dimensión finita, que forman un álgebra, en éste sentido nos falta *completar* el grupo a un álgebra, y el álgebra de grupo es esa manera de ver a un grupo dentro de un álgebra, y es importante ya que se comporta de tal forma que podemos obtener resultados acerca de $\mathbb{F}G$-módulos estudiándola, consideraremos después módulos sobre ésta. La construcción del álgebra de grupo se basa en considerar a los elementos de un grupo como la base de un espacio vectorial.

Definición 0.128. *Sea R un anillo con 1_R y G un grupo (puede ser infinito). El **anillo de grupo de G sobre** R es el conjunto*

$$R(G) = \left\{ \sum_{g\in G} a_g g \mid a_g \in R \right\}$$

donde sólo un número finito de $a_g \in R$ son distintos de 0_R. Así, el anillo de grupo son las R-combinaciones lineales finitas de elementos de G donde definimos la suma evidente y el producto extendiendo el producto en el grupo, es decir,

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g \quad y$$
$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g\in G}\sum_{h\in G} a_g b_h (gh) = \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g$$

y podemos reescribir el producto como $\displaystyle\sum_{g\in G}\left(\sum_{xy=g} a_x b_y\right) g = \sum_{g,h\in G} a_g b_h (gh)$.

Observación 0.129. El anillo de grupo tiene las siguientes propiedades:

(1) Tiene un elemento identidad, $1_{R(G)} = 1_R e_G$, que se identifica con el neutro del grupo.

(2) Podemos visualizar a cada elemento $g \in G$ en $R(G)$ como la combinación lineal $1_R g$, y denotaremos a esta combinación simplemente por g.

(3) $R(G)$ es conmutativo si y sólo G es abeliano y R es conmutativo.

(4) Si G tiene elementos de orden finito entonces $R(G)$ tiene divisores de cero (no es un dominio entero), por ejemplo, si tomamos en G un elemento g de orden m entonces

$$(1-g)\left(1+g+g^2+\cdots+g^{m-1}\right)=0.$$

Para lo que haremos estamos interesados en grupos G de orden finito, digamos n y $R=\mathbb{F}$ un campo. Bajo estas condiciones $R(G)=\mathbb{F}(G)$, además de su estructura de anillo con uno, tiene también estructura de espacio vectorial sobre $\mathbb{F}$ con el producto por escalar definido de la forma canónica, es decir,

$$a\sum_{g\in G}a_g g=\sum_{g\in G}(aa_g)g \quad \text{para todo} \quad a\in\mathbb{F},$$

y como espacio vectorial sobre $\mathbb{F}$ tiene como una base a los elementos del grupo G y por lo tanto dimensión $n=|G|$. Así, con este producto por escalar el anillo de grupo se conoce como el **álgebra de grupo** de G sobre $\mathbb{F}$, aunque debemos verificar la condición adicional

$$(av)u=a(vu)=v(au) \text{ para todos } a\in\mathbb{F} \text{ y } v,u\in\mathbb{F}(G).$$

y ésta se satisface ya que

$$(av)u=\left(a\sum_{g\in G}a_g g\right)\sum_{h\in G}b_h h=\sum_{g\in G}(aa_g)g\sum_{h\in G}b_h h=\sum_{g,h\in G}aa_g b_h(gh)=a\sum_{g,h\in G}a_g b_h(gh)=$$
$$a\left(\sum_{g\in G}a_g g\sum_{h\in G}b_h h\right)=a(vu)=\sum_{g,h\in G}aa_g b_h(gh)=\sum_{g,h\in G}a_g ab_h(gh)=\sum_{g\in G}a_g g\sum_{h\in G}(ab_h)h=v(au).$$

Observación 0.130. El álgebra de grupo de G sobre $\mathbb{F}$ es el $\mathbb{F}$-módulo libre con base G.

Regresando al contexto de representaciones tenemos la siguiente

Definición 0.131. *Sea G un grupo y sea $\rho: G\longrightarrow GL_n(\mathbb{F})$ una representación de G, entonces el **núcleo de la representación** ρ es el conjunto*

$$Ker(\rho)=\{g\in G \mid \rho(g)=I_n\}.$$

*Diremos que ρ es una **representación fiel** si $Ker(\rho)=\{e_G\}$, es decir, si ρ es monomorfismo.*

Observación 0.132. Para cualquier representación $\rho: G\longrightarrow GL_n(\mathbb{F})$ de G tenemos que $Ker(\rho)\trianglelefteq G$ pues ρ es morfismo de grupos.

Ejemplo 0.133. Si $\rho: G\longrightarrow GL_n(\mathbb{F})$ es una representación de G, y no es inyectiva (no es fiel), sea $Ker(\rho)=K$, entonces, por el primer teorema de isomorfismo de grupos tenemos un isomorfismo

$$\begin{array}{rcl}\widehat{\rho}: G/K & \longrightarrow & Im(\rho)\subset GL_n(\mathbb{F}) \\ gK & \longmapsto & \rho(g)\end{array}$$

que es una representación fiel del grupo cociente G/K, así, toda representación de un grupo que no sea fiel siempre induce una representación fiel en uno de sus grupos cocientes.

Ejemplo 0.134. El grupo cíclico de orden n, $\mathbb{Z}_n=\langle g\rangle$ tiene representaciones dadas por

$$\begin{array}{rcl} \theta_k : \mathbb{Z}_n & \longrightarrow & GL_1(\mathbb{C}) \cong \mathbb{C}^* \\ g & \longmapsto & \zeta^k \end{array}, \ 0 \leqslant k \leqslant n-1,$$

donde $\zeta = e^{\frac{2\pi i}{n}}$ es una raíz n-ésima primitiva de la unidad.

Ejemplo 0.135. Si S_n es el grupo simétrico en n letras entonces la función signo

$$\begin{array}{rcl} sgn : S_n & \longrightarrow & \{1, -1\} \subset \mathbb{C}^* \\ \alpha & \longmapsto & sgn(\alpha) \end{array}$$

es una representación de S_n de grado 1 que no es fiel pues $Ker(sgn) = A_n$, el grupo alternante en n letras (permutaciones pares).

Ejemplo 0.136. Todo espacio vectorial complejo V de dimensión n es identificado con $\mathbb{C}^n$ usando alguna base, así, V es naturalmente una representación de $GL_n(\mathbb{C})$ sobre $\mathbb{C}$ pues es un $\mathbb{C}GL_n(\mathbb{C})$-módulo con la acción lineal

$$\begin{array}{rcl} \cdot : GL_n(\mathbb{C}) \times V & \longrightarrow & V \\ (A, v) & \longmapsto & Av. \end{array}$$

Ejemplo 0.137. La representación trivial de G.
Para cualquier espacio vectorial V sobre $\mathbb{F}$ podemos considerar el morfismo trivial

$$\begin{array}{rcl} \tau : G & \longrightarrow & GL(V) \\ g & \longmapsto & Id_V. \end{array}$$

que es un morfismo de grupos y por lo tanto una representación de G sobre $\mathbb{F}$, cuya acción lineal inducida es $gv := \tau(g)(v) = Id_V(v) = v$ para todos $g \in G, v \in V$, luego, esta acción se extiende a una acción *trivial* de $\mathbb{F}(G)$ sobre V

$$\begin{array}{rcl} * : \mathbb{F}(G) \times V & \longrightarrow & V \\ \left(\sum_{g\in G} a_g g, v\right) & \longmapsto & \sum_{g\in G} a_g g * v := \sum_{g\in G} a_g v. \end{array}$$

En particular, podemos tomar $V = \mathbb{F}$ como un $\mathbb{F}$-espacio vectorial de dimensión 1 (cualquier espacio vectorial de dimensión 1 sobre $\mathbb{F}$ es isomorfo a $\mathbb{F}$), luego usando la acción trivial

$$\begin{array}{rcl} \cdot : G \times \mathbb{F} & \longrightarrow & \mathbb{F} \\ (g, a) & \longmapsto & ga := a, \end{array}$$

tenemos un $\mathbb{F}G$-módulo llamado **el $\mathbb{F}G$-módulo trivial de G**, y la representación inducida es

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL_1(\mathbb{F}) \cong \mathbb{F}^* \\ g & \longmapsto & 1 \end{array}$$

y es llamada **la representación trivial de G**.
La representación trivial de un grupo G es fiel si y sólo si $G = \{e_G\}$.

Ejemplo 0.138. Sea X un G-conjunto y $\mathbb{F}$ un campo. El espacio $\mathbb{F}^X$ de funciones de X en $\mathbb{F}$ es un $\mathbb{F}G$-módulo con la acción

$$\begin{array}{rcl} \cdot : G \times \mathbb{F}^X & \longrightarrow & \mathbb{F}^X \\ (g, \xi) & \longmapsto & g\xi \end{array} \quad \text{donde} \quad \begin{array}{rcl} g\xi : X & \longrightarrow & \mathbb{F} \\ x & \longmapsto & \xi(g^{-1}x). \end{array}$$

En efecto, para todos $g, h \in G$, $\xi, \nu \in \mathbb{F}^X$ y $\lambda \in \mathbb{F}$ tenemos que

1. $g\xi \in \mathbb{F}^X$ pues $g^{-1}x \in X$
2. $e_G\xi(x) = \xi(e_G x) = \xi(x)$
3. $(gh)\xi(x) = \xi((h^{-1}g^{-1})x) = \xi(h^{-1}\left(g^{-1}x\right)) = h\xi\left(g^{-1}x\right) = g(h\xi)(x)$
4. $g(\xi+\nu)(x) = (\xi+\nu)\left(g^{-1}x\right) = \xi(g^{-1}x) + \nu(g^{-1}x) = g\xi(x) + g\nu(x)$
5. $g(\lambda\xi)(x) = (\lambda\xi)(g^{-1}x) = \lambda(\xi)(g^{-1}x) = \lambda(g\xi)(x)$.

Ejemplo 0.139. Extensión lineal de una acción.
Sea G un grupo, $\mathbb{F} = \mathbb{C}$ y $X = \{x_1, \ldots, x_n\}$ un G-conjunto. Entonces la acción de G en X se extiende linealmente al $\mathbb{C}$-espacio vectorial

$$\langle X \rangle = \{c_1x_1 + \cdots + c_nx_n \mid c_i \in \mathbb{C}\},$$

(las combinaciones lineales de los elementos de X con coeficientes complejos) con la suma y producto por escalar evidentes. Así la extensión de la acción en este espacio es

$$\begin{array}{rcl} * : G \times \langle X \rangle & \longrightarrow & \langle X \rangle \\ \left(g\ , \sum_{i=1}^{n} c_i x_i\right) & \longmapsto & \sum_{i=1}^{n} c_i(gx_i). \end{array}$$

Una acción de este tipo induce un $\mathbb{C}G$-módulo llamado **módulo de permutaciones para** G. Las matrices correspondientes a los elementos del grupo bajo ésta representación consisten sólo de 1's y 0's con exactamente un 1 en cada renglón y columna, estas matrices son llamadas **matrices de permutación**. El módulo de permutaciones es un $\mathbb{F}G$-módulo fiel si la acción de G en X es fiel ya que en este caso, si $gx_i = x_i$ para toda $i \in \{1, \ldots, n\}$ entonces $g = e_G$.
El álgebra de grupo $\mathbb{F}(G)$, con su estructura de $\mathbb{F}$-espacio vectorial es un caso particular de éste ejemplo considerando $G = X$ y G actuando en sí mismo mediante el producto en G. Es decir, el álgebra de grupo no es más que un módulo de permutaciones de G (la extensión lineal del producto en G).

Ejemplo 0.140. Si S_n es el grupo simétrico en n letras entonces la función

$$\begin{array}{rcl} \rho : S_n & \longrightarrow & GL_n(\mathbb{C}) \\ \alpha & \longmapsto & A_\alpha = (a_{ij}) \end{array} \quad \text{donde} \quad a_{ij} = \delta_{i,\alpha(j)}$$

es una representación fiel de S_n de grado n, por ejemplo, si $\alpha = (235) \in S_5$, entonces

$$A_\alpha = \begin{pmatrix} 1&0&0&0&0 \\ 0&0&0&0&1 \\ 0&1&0&0&0 \\ 0&0&0&1&0 \\ 0&0&1&0&0 \end{pmatrix}$$

Notemos que estas matrices se obtienen de la matriz identidad I_n intercambiando sus columnas.

Ejemplo 0.141. Restricción. Sea V un $\mathbb{F}G$-módulo y $H \leqslant G$. Entonces V es un $\mathbb{F}H$-módulo si restringimos la acción de G sobre V al subgrupo H, es decir V es una representación de H sobre $\mathbb{F}$. Así, V visto como un $\mathbb{F}H$-módulo se conoce como **la restricción de** V **a** H y se denota por $V \downarrow H$.

Ejemplo 0.142. Pullback. Sean G_1, G_2 grupos, $f : G_1 \longrightarrow G_2$ un morfismo de grupos y $\rho : G_2 \longrightarrow GL(V)$ una representación de G_2 sobre $\mathbb{F}$. Entonces existe una representación de G_1 sobre $\mathbb{F}$ llamada **el pullback de ρ bajo f**, dada por la función

$$\begin{array}{rcl} f^*(\rho) : G_1 & \longrightarrow & GL(V) \\ g & \longmapsto & (\rho \circ f)(g). \end{array}$$

Ejemplo 0.143. El $\mathbb{F}G$-módulo de transformaciones lineales entre dos $\mathbb{F}G$-módulos.
Si U y V son $\mathbb{F}G$-módulos, entonces el espacio $Hom_{\mathbb{F}}(U, V)$ es un $\mathbb{F}G$-módulo con la función

$$\begin{array}{rcl} \cdot : G \times Hom_{\mathbb{F}}(U,V) & \longrightarrow & Hom_{\mathbb{F}}(U,V) \\ (g, \phi) & \longmapsto & g\phi \end{array} \quad \text{donde} \quad \begin{array}{rcl} g\phi : U & \longrightarrow & V \\ u & \longmapsto & g(\phi(g^{-1}u)) \end{array}$$

pues claramente es una acción porque $g\phi \in Hom_{\mathbb{F}}(U, V)$ y $e_G\phi = \phi$, y si $g_1, g_2 \in G$ tenemos que

$$(g_1g_2)\phi(u) := g_1g_2\phi((g_1g_2)^{-1}u) = g_1(g_2\phi(g_2^{-1}(g_1^{-1}u))) = g_1((g_2\phi)(g_1^{-1}u)) = (g_1(g_2\phi))(u)$$

y por lo tanto tenemos que $(g_1g_2)\phi = g_1(g_2\phi)$, luego, es lineal ya que si $\phi_1, \phi_2 \in Hom_{\mathbb{F}}(U, V)$ y $a \in \mathbb{F}$ entonces para todo $g \in G$ tenemos que

$$\begin{array}{rcl} g(\phi_1 + \phi_2)(u) & := & g\left((\phi_1 + \phi_2)(g^{-1}u)\right) = g\left(\phi_1(g^{-1}u) + \phi_2(g^{-1}u)\right) \\ & = & g\left(\phi_1(g^{-1}u)\right) + g\left(\phi_2(g^{-1}u)\right) = g\phi_1(u) + g\phi_2(u) \end{array}$$

$$\text{y} \quad g(a\phi_1)(u) := g\left((a\phi_1)(g^{-1}u)\right) = g\left(a\phi_1(g^{-1}u)\right) = a\left(g\phi_1((g^{-1}u))\right) = a(g\phi_1)(u).$$

Así, $Hom_{\mathbb{F}}(U, V)$ se vuelve un $\mathbb{F}G$-módulo. Luego, en el espacio dual $V^* = Hom_{\mathbb{F}}(V, \mathbb{F})$, donde $\mathbb{F}$ es visto como $\mathbb{F}G$-módulo sobre sí mismo (el $\mathbb{F}G$-módulo trivial) la acción es $(g\phi)(u) = \phi(g^{-1}u)$ pues G actúa trivialmente en $\mathbb{F}$.

Ejemplo 0.144. Morfismos definidos en el anillo de grupo.
Vamos a ver el anillo de grupo $\mathbb{F}(G)$ convierte ciertos morfismos de grupos (en particular, representaciones) en morfismos de anillos. Si R es una $\mathbb{F}$-álgebra y $f : G \longrightarrow R^*$ es un morfismo de grupos (R^* es el grupo de unidades de R), podemos definir una función

$$\begin{array}{rcl} \widehat{f} : \mathbb{F}(G) & \longrightarrow & R \\ \displaystyle\sum_{g\in G} a_g g & \longmapsto & \displaystyle\sum_{g\in G} a_g f(g) \end{array}$$

que es un morfismo de anillos pues

$$\begin{array}{rcl} \widehat{f}\Big(\displaystyle\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\Big) & = & \widehat{f}\Big(\displaystyle\sum_{g\in G}(a_g + b_g)g\Big) = \sum_{g\in G}(a_g + b_g)f(g) \\ & = & \displaystyle\sum_{g\in G} a_g f(g) + \sum_{g\in G} b_g f(g) = \widehat{f}\Big(\sum_{g\in G} a_g g\Big) + \widehat{f}\Big(\sum_{g\in G} b_g g\Big), \end{array}$$

y respeta el producto pues para todos $g, h \in G$

$$\widehat{f}(gh) = f(gh) = f(g)f(h) = \widehat{f}(g)\widehat{f}(h)$$

y usando la ley distributiva se obtiene el caso general.
Entonces, como un caso particular de esto, cualquier representación ρ de G de grado n puede ser extendida de forma única a un morfismo de $\mathbb{F}$-álgebras

$$\begin{array}{rcl} \widehat{\rho}:\mathbb{F}(G) & \longrightarrow & \mathcal{M}_{n\times n}(\mathbb{F}) \\ \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g \rho(g) \end{array}$$

pues $GL_n(\mathbb{F})$ es el grupo de unidades (vista como anillo) del álgebra $\mathcal{M}_{n\times n}(\mathbb{F})$.

Ejemplo 0.145. Extensión de morfismos de grupos.
Si G y H son grupos y $f : G \longrightarrow H$ es un morfismo de grupos, podemos extender f a un morfismo de anillos entre las álgebras de grupo de G y H, que es la función

$$\begin{array}{rcl} \widehat{f}:\mathbb{F}(G) & \longrightarrow & \mathbb{F}(H) \\ \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g f(g). \end{array}$$

En particular, si H es el grupo trivial entonces $\mathbb{F}(H) = \mathbb{F}$ y el morfismo de anillos mencionado anteriormente es la función

$$\begin{array}{rcl} \epsilon:\mathbb{F}(G) & \longrightarrow & \mathbb{F} \\ \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g \end{array}$$

que es llamada el **morfismo de aumento**, su núcleo

$$A\left(\mathbb{F}(G)\right) = \left\{ \sum_{g\in G} a_g g \in \mathbb{F}(G) \mid \sum_{g\in G} a_g = 0 \right\}$$

se conoce como **el ideal de aumento** de $\mathbb{F}(G)$. Claramente la función de aumento ϵ es una transformación lineal y es suprayectiva, y ya que $\mathbb{F}(G)$ como espacio vectorial tiene dimensión $|G| = n$, tenemos por el Teorema de la Dimensión que $dim_{\mathbb{F}}\left(A\left(\mathbb{F}(G)\right)\right) = n - 1$ como subespacio de $\mathbb{F}(G)$. Luego, el conjunto $\{g - e_G \mid e_G \neq g \in G\}$ es una base para el ideal de aumento pues es un conjunto linealmente independiente de $n - 1$ vectores en un espacio de dimensión $n - 1$.

Lo siguiente será construir un $\mathbb{F}G$-módulo a partir del álgebra de grupo, éste es un importante ejemplo para el desarrollo de la teoría de representaciones.

Ejemplo 0.146. Representación Regular de un Grupo.
Sea $\mathbb{F}$ un campo y G un grupo de orden finito n. La representación más básica de G es la inducida por el álgebra de grupo $\mathbb{F}(G)$ de G sobre $\mathbb{F}$ vista como $\mathbb{F}G$-módulo. Sabemos que $\mathbb{F}(G)$ es un espacio vectorial sobre $\mathbb{F}$, donde $dim_{\mathbb{F}}\big(\mathbb{F}(G)\big) = n = |G|$, y la función

$$\begin{array}{rcl} \diamond \ : \ G\times\mathbb{F}(G) & \longrightarrow & \mathbb{F}(G) \\ \left(x, \sum_{g\in G} a_g g\right) & \longmapsto & \sum_{g\in G} a_g (xg) \end{array}$$

es una acción lineal de G en $\mathbb{F}(G)$, más claramente, vemos que bajo $\diamond$ la acción G en $\mathbb{F}(G)$ está dada por el producto en $\mathbb{F}(G)$ si vemos a G dentro de $\mathbb{F}(G)$, es decir,

$$x \diamond v = x \diamond \left(\sum_{g\in G} a_g g \right) = \left(1_{\mathbb{F}(G)} x\right) \left(\sum_{g\in G} a_g g \right) = \sum_{g\in G} a_g (xg).$$

Con esta acción $\mathbb{F}(G)$ es un $\mathbb{F}G$-módulo llamado el $\mathbb{F}G$**-módulo regular**.
La representación de G de grado n inducida por la acción anterior es la función

$$\begin{array}{rcl}\rho_{reg} : G & \longrightarrow & GL\big(\mathbb{F}(G)\big) \\ x & \longmapsto & \rho_{reg}(x)\end{array} \quad \text{donde} \quad \begin{array}{rcl}\rho_{reg}(x) : \mathbb{F}(G) & \longrightarrow & \mathbb{F}(G) \\ \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g(xg)\ ,\end{array}$$

y es llamada la **representación regular de** G. Notemos que esto es el ejemplo 0.139 con el grupo actuando mediante el producto.

De hecho, generalizando, el álgebra de grupo actúa en cualquier $\mathbb{F}G$-módulo V, de modo más preciso:

Ejemplo 0.147. **$\mathbb{F}G$-módulos son $\mathbb{F}(G)$-módulos**.
El álgebra de grupo actúa en cualquier $\mathbb{F}G$-módulo V mediante la función

$$\begin{array}{rcl}\diamond : \mathbb{F}(G) \times V & \longrightarrow & V \\ \left(\sum_{g\in G} a_g g, v\right) & \longmapsto & \left(\sum_{g\in G} a_g g\right) \diamond v := \sum_{g\in G} a_g(g \cdot v)\end{array}$$

donde $\cdot$ denota la acción de G en V que lo hace un $\mathbb{F}G$-módulo.
Luego, con la acción $\diamond$ tenemos que V es un $\mathbb{F}(G)$-módulo pues G actúa linealmente en V y así para todos $r, s \in \mathbb{F}(G), v, u \in V$ se satisface que

1. $1_{\mathbb{F}(G)} v = e_G v = v$
2. $(rs)v = r(sv)$
3. $(r + s)v = rv + sv$
4. $r(v + u) = rv + ru$.

Luego, por el teorema 0.107, la *representación* de $\mathbb{F}(G)$ (vista como anillo) inducida por esta acción es un morfismo de anillos

$$\begin{array}{rcl}\lambda : \mathbb{F}(G) & \longrightarrow & End_{\mathbb{F}}(V) \cong \mathcal{M}_{n\times n}(\mathbb{F}) \\ \sum_{g\in G} a_g g & \longmapsto & \lambda\left(\sum_{g\in G} a_g g\right)\end{array} \quad \text{donde} \quad \begin{array}{rcl}\lambda\left(\sum_{g\in G} a_g g\right) : V & \longrightarrow & V \\ v & \longmapsto & \sum_{g\in G} a_g(gv).\end{array}$$

Observación 0.148. Los módulos izquierdos M sobre $\mathbb{F}(G)$ pueden considerarse también como espacios vectoriales sobre $\mathbb{F}$ (por la observación 0.121) con el producto por escalar si hacemos actuar $\lambda \in \mathbb{F}$ como $\lambda e_G \in \mathbb{F}(G)$, es decir, con la función

$$\begin{array}{rcl}\cdot : \mathbb{F} \times M & \longrightarrow & M \\ (\lambda, m) & \longmapsto & \lambda m := (\lambda e_G)m\ .\end{array}$$

En nuestro caso, G un grupo finito, tenemos la importante conexión entre estas estructuras:

Lema 0.149. *Sea $\mathbb{F}$ un campo y G un grupo finito, entonces un $\mathbb{F}(G)$-módulo es finitamente generado si y sólo si tiene dimensión finita como espacio vectorial sobre $\mathbb{F}$.*

Demostración. Si V es generado como $\mathbb{F}(G)$-módulo por $\{v_1, \ldots, v_t\}$, entonces V es generado como $\mathbb{F}$-espacio vectorial por el conjunto $\{gv_i \mid g \in G, 1 \leq i \leq t\}$ y ya que G es finito tenemos que $dim_{\mathbb{F}}(V) < \infty$. El converso es trivial por el inciso (2) de la observación 0.129. ■

De aquí vamos a obtener la conexión entre los módulos sobre el álgebra de grupo y la teoría de representaciones.

Teorema 0.150. *Sea $\mathbb{F}$ un campo y G un grupo finito. Entonces existe una correspondencia biyectiva entre $\mathbb{F}(G)$-módulos y acciones lineales de G en un espacio vectorial de dimensión finita sobre $\mathbb{F}$.*

Demostración. Si V es un $\mathbb{F}(G)$-módulo finitamente generado, por el lema anterior, $dim_{\mathbb{F}}(V)$ es finita y si el producto en V como $\mathbb{F}(G)$-módulo está dado por

$$\begin{array}{rcl} *:\mathbb{F}(G)\times V & \longrightarrow & V \\ \left(\sum_{g\in G} a_g g, v\right) & \longmapsto & \left(\sum_{g\in G} a_g g\right) * v\ , \end{array}$$

entonces restringiendo este producto a G, pues $g = 1_{\mathbb{F}}g \in \mathbb{F}(G)$ para todo $g \in G$, tenemos que la función

$$\begin{array}{rcl} *\,|_G\colon G\times V & \longrightarrow & V \\ (g,v) & \longmapsto & g*v = 1_{\mathbb{F}}g*v \end{array}$$

es una acción lineal de G en V por la propiedades de $*$.

Podemos demostrar esto usando de la misma forma la observación 0.121 y el lema anterior para ver a un $\mathbb{F}(G)$-módulo V finitamente generado como $\mathbb{F}$-espacio vectorial de dimensión finita, por el teorema 0.107 la estructura de $\mathbb{F}(G)$-módulo en V induce un morfismo de anillos $\varrho : \mathbb{F}(G) \longmapsto End_{\mathbb{F}}(V)$, y ya que los elementos de G son unidades (elementos invertibles) vistos dentro del anillo $\mathbb{F}(G)$, se tiene que $\varrho(g)$ es unidad (matriz invertible) en $End_{\mathbb{F}}(V)$ para todo $g \in G$, así la restricción de ϱ a G define un morfismo de grupos de G a $GL(V)$, es decir, una representación de G.

Recíprocamente, supongamos que V es un $\mathbb{F}$-espacio vectorial en el cual existe una acción lineal de un grupo G denotada como gv, entonces debemos equipar a V con una estructura de $\mathbb{F}(G)$-módulo, pero vimos en el ejemplo 0.147 que el álgebra de grupo actúa en cualquier $\mathbb{F}(G)$-módulo mediante la función

$$\begin{array}{rcl} \triangleright:\mathbb{F}(G)\times V & \longrightarrow & V \\ \left(\sum_{g\in G} a_g g\ ,\ v\right) & \longmapsto & \left(\sum_{g\in G} a_g g\right) \triangleright v := \sum_{g\in G} a_g(gv), \end{array}$$

y como G actúa linealmente en V entonces se satisfacen los axiomas de estructura de módulo sobre $\mathbb{F}(G)$, por lo tanto, V es un $\mathbb{F}(G)$-módulo.

Otra forma de demostrar lo anterior es la siguiente: Ya que V es un $\mathbb{F}G$-módulo existe una representación $\rho : G \longmapsto GL(V)$, que es por definición un morfismo de grupos, entonces, por el ejemplo 0.144 se extiende de forma única a un morfismo de anillos $\widehat{\rho} : \mathbb{F}(G) \longmapsto End_{\mathbb{F}}(V)$ tal que $\widehat{\rho}(g) = \rho(g)$ para todo $g \in G$, y este morfismo de anillos, por el teorema 0.108 induce una estructura de $\mathbb{F}(G)$-módulo en V. Así, en el lenguaje de representaciones de un grupo esto se traduce en que para cualquier representación ρ de G, $V = \mathbb{F}^n$ tiene estructura de $\mathbb{F}(G)$-módulo mediante

$$\begin{array}{rcl} \ominus:\mathbb{F}(G)\times V & \longrightarrow & V \\ \left(\sum_{g\in G} a_g g\ ,\ v\right) & \longmapsto & \left(\sum_{g\in G} a_g g\right) \ominus v := \sum_{g\in G} a_g(\rho(g)v)\ . \end{array}$$

■

Observación 0.151. Entonces, en términos de lo anterior, una representación de un grupo finito G sobre $\mathbb{F}$ induce un $\mathbb{F}(G)$-módulo V finitamente generado y todo $\mathbb{F}(G)$-módulo finitamente generado

V induce acción lineal de G en un espacio de dimensión finita V.
En otras palabras, es lo mismo pensar en representaciones lineales de G, en $\mathbb{F}G$-módulos o en $\mathbb{F}(G)$-módulos.

$\mathbb{F}G$-submódulos y morfismos de $\mathbb{F}G$-módulos

Definición 0.152. *Sea V un $\mathbb{F}G$-módulo (o equivalentemente, $\rho : G \longrightarrow GL(V)$ es una representación de G), un subconjunto U de V es llamado un $\mathbb{F}G$-**submódulo** de V si U es subespacio de V y $gu \in U$ para todos $g \in G$ y $u \in U$, es decir, U es cerrado bajo la acción de G. Así, un $\mathbb{F}G$-submódulo de V es un subespacio que también es un $\mathbb{F}G$-módulo (una **subrepresentación** de ρ es una representación σ asociada a un $\mathbb{F}G$-submódulo de V).*

Ejemplo 0.153. Si V es un $\mathbb{F}G$-módulo, entonces los espacios V y $\{0\}$ son dos $\mathbb{F}G$-submódulos, llamados los $\mathbb{F}G$**-submódulos triviales**.

Definición 0.154. *Sea V un $\mathbb{F}G$-módulo, decimos que V es un $\mathbb{F}G$-**módulo irreducible** si $V \neq \{0\}$ y sus únicos $\mathbb{F}G$-submódulos son V y $\{0\}$. Si V tiene un $\mathbb{F}G$-submódulo $W \neq \{0\}$ y $W \neq V$, entonces V es un $\mathbb{F}G$-**módulo reducible**. Equivalentemente, si $\rho : G \longrightarrow GL_n(\mathbb{F})$ es una representación de G, decimos que ρ es una **representación irreducible** si el correspondiente $\mathbb{F}G$-módulo $V = \mathbb{F}^n$ es irreducible, y es **reducible** si $\mathbb{F}^n$ es reducible.*

Observación 0.155. De forma equivalente, un $\mathbb{F}G$-módulo V es irreducible si es simple visto como $\mathbb{F}(G)$-módulo.

Ejemplo 0.156. Sumas directas.
Sea W un $\mathbb{F}G$-módulo y sean U y V $\mathbb{F}G$-submódulos de W y supongamos que $W = U \oplus V$ como espacios vectoriales, entonces podemos equipar a la suma directa $U \oplus V$ naturalmente con estructura de $\mathbb{F}G$-módulo componente a componente, es decir,

$$\begin{array}{rcl} \cdot : G \times (U \oplus V) & \longrightarrow & (U \oplus V) \\ (g, u+v) & \longmapsto & gu + gv. \end{array}$$

Si $\beta_1 = \{u_1, \ldots, u_k\}$ es una base de U y $\beta_2 = \{v_1, \ldots, v_l\}$ es una base de V sabemos que podemos unirlas y obtener una base de $W = U \oplus V$ y en esta base $\beta = \{u_1, \ldots, u_k, v_1, \ldots, v_l\}$ tenemos que para todo $g \in G$

$$[g]_\beta = \begin{pmatrix} [g]_{\beta_1} & 0 \\ 0 & [g]_{\beta_2} \end{pmatrix}$$

En general, si $W = U_1 \oplus \cdots \oplus U_s$ como espacios vectoriales y si $U_1, \cdots, U_s$ son $\mathbb{F}G$-submódulos de W, entonces, si β_i es una base de U_i para todo $1 \leq i \leq s$ tenemos que $\beta = \beta_1 \cup \cdots \cup \beta_s$ es una base de $W = U_1 \oplus \cdots \oplus U_s$ y así la representación de la suma directa (interna), para todo $g \in G$ cumple que

$$[g]_\beta = \begin{pmatrix} [g]_{\beta_1} & 0 & \cdots & 0 \\ 0 & [g]_{\beta_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & [g]_{\beta_s} \end{pmatrix}$$

Para el caso de la suma directa externa de $\mathbb{F}G$-módulos simplemente tomamos el producto cartesiano de los espacios en cuestión con las operaciones componente a componente y la acción del grupo es entrada a entrada como en la suma directa interna.

Definición 0.157. *V es una **representación indescomponible** de G si V es indescomponible como $\mathbb{F}G$-módulo, es decir, no es suma directa de otros $\mathbb{F}G$-módulos.*

Observación 0.158. Claramente todo $\mathbb{F}G$-módulo irreducible es indescomponible pero al revés no.

Definición 0.159. *Sean V y U dos $\mathbb{F}G$-módulos. Una transformación lineal $T : V \longrightarrow U$ es llamada un **morfismo de $\mathbb{F}G$-módulos** o un $\mathbb{F}G$-**morfismo** si respeta la acción del grupo (es un morfismo de G-conjuntos), es decir,*

$$T(gv) = gT(v) \quad \text{para todos } v \in V,\ g \in G.$$

*Un isomorfismo de espacios vectoriales que respete la acción es llamado un **isomorfismo de $\mathbb{F}G$-módulos**, en este caso escribiremos $V \cong U$ (que es un isomorfismo de espacios vectoriales y al mismo tiempo de G-conjuntos). Si los $\mathbb{F}G$-módulos no son isomorfos escribiremos $V \ncong U$. El conjunto de morfismos de $\mathbb{F}G$-módulos entre dos $\mathbb{F}G$-módulos se denotará $Hom_{\mathbb{F}G}(V, U)$.*

Notemos que por la biyección entre representaciones lineales de G (morfismos de G en $GL_n(\mathbb{F}) \cong GL(\mathbb{F}^n)$) y las acciones lineales de G en un espacio vectorial V sobre $\mathbb{F}$ de dimensión n, tenemos que si $\rho : G \longrightarrow GL(V)$ y $\tau : G \longrightarrow GL(U)$ son las representaciones asociadas a V y U, la definición anterior es equivalente a pedir que

$$(T \circ \rho(g))(v) = (\tau(g) \circ T)(v) \text{ para todos } v \in V,\ g \in G.$$

Diremos que $\rho : G \longrightarrow GL(V)$ y $\tau : G \longrightarrow GL(U)$ son **representaciones equivalentes o isomorfas** si hay un isomorfismo de $\mathbb{F}G$-módulos $T : V \longrightarrow U$ tal que $T \circ \rho(g) = \tau(g) \circ T$ para todo $g \in G$, que podemos reescribir como

$$T \circ \rho(g) \circ T^{-1} = \tau(g) \text{ para todo } g \in G$$

y entonces podemos traducir al lenguaje de matrices la equivalencia de representaciones diciendo que dos representaciones son equivalentes si son conjugadas por una matriz invertible. Por la equivalencia de acciones lineales y módulos sobre el álgebra de grupo también podemos pensar a un morfismo de $\mathbb{F}G$-módulos, como un morfismo de $\mathbb{F}(G)$-módulos ya que si $T : V \longrightarrow U$ es un morfismo de $\mathbb{F}G$-módulos, entonces tenemos que para todo $v \in V$ y $r = \sum_{g \in G} a_g g \in \mathbb{F}(G)$

$$T(rv) = T\left(\sum_{g \in G} a_g gv\right) = \sum_{g \in G} a_g T(gv) = \sum_{g \in G} a_g gT(v) = rT(v).$$

Observación 0.160. Dos representaciones equivalentes tienen el mismo grado pues existe un isomorfismo de espacios vectoriales sobre $\mathbb{F}$ entre los espacios V y U de la definición anterior.

Teorema 0.161. *Sean V y U dos $\mathbb{F}G$-módulos. Si $V \cong U$ vía un isomorfismo de $\mathbb{F}G$-módulos T, entonces $T^{-1} : U \longrightarrow V$ también es un $\mathbb{F}G$-isomorfismo, es decir, $U \cong V$ como $\mathbb{F}G$-módulos.*

Demostración. Si $u \in U$ y $g \in G$ se tiene que

$$T\big(g(T^{-1}(u))\big) = g\big(T(T^{-1}(u))\big) = gu = T\big(T^{-1}(gu)\big),$$

y usando que T es inyectivo tenemos que $g(T^{-1}(u)) = T^{-1}(gu)$ para todos $u \in U$ y $g \in G$. ■

Observación 0.162. Por la observación y el teorema anteriores, para dos $\mathbb{F}G$-módulos, ser isomorfos es una relación reflexiva y simétrica, y es fácil ver que es transitiva. Por lo tanto ser isomorfos es una relación de equivalencia en la clase de todos los $\mathbb{F}G$-módulos. Llamaremos a las clases de equivalencia de esta relación de equivalencia las **clases de isomorfismo de $\mathbb{F}G$-módulos.**

Un problema básico de la teoría de representaciones es clasificar todas las representaciones de un grupo G salvo isomorfismo (que para grupos de orden infinito suele ser bastante complicado). La siguiente proposición clasifica las representaciones de grado m de un grupo G.

Observación 0.163. Notemos que si $\rho \in Hom(G, GL_m(\mathbb{F})$ (ρ es una representación de G) y $T \in GL_m(\mathbb{F})$ entonces la conjugación de ρ por T nos da la función

$$\begin{array}{rcl} \rho_T : G & \longrightarrow & GL_m(\mathbb{F}) \\ g & \longmapsto & T \circ \rho(g) \circ T^{-1} \end{array}$$

que es un morfismo de grupos y por lo tanto una representación de G, y esto es lo que pedíamos para que dos representaciones fueran equivalentes. Así, el conjunto de clases de isomorfismo de representaciones de G de grado m tiene cardinal igual a $|GL_m(\mathbb{F})|$.

Ejemplo 0.164. Sean G un grupo y V, U dos $\mathbb{F}G$-módulos. Entonces cualquier morfismo de $\mathbb{F}G$-módulos $T : V \longrightarrow U$ naturalmente nos proporciona dos $\mathbb{F}G$-submódulos, éstos son los subespacios $Ker(T) \leq V$ y $Im(T) \leq U$ pues T es compatible con la acción, luego, si $g \in G$ y $v \in Ker(T)$ entonces

$$T(gv) = gT(v) = g0 = 0$$

y por lo tanto $gv \in Ker(T)$, por otro lado, si $g \in G$ y $u \in Im(T)$ entonces $u = T(w)$ para algún $w \in V$ y tenemos que

$$gu = gT(w) = T(gw) \in Im(T)$$

por lo que el núcleo y la imagen de cualquier $\mathbb{F}G$-morfismo son FG-submódulos.

Observación 0.165. Los isomorfismos de $\mathbb{F}G$-módulos hacen que los $\mathbb{F}G$-módulos en cuestión tengan las mismas propiedades estructurales, es decir, para V y U $\mathbb{F}G$-módulos isomorfos de dimensión finita tenemos que

1) $dim_{\mathbb{F}}(V) = dim_{\mathbb{F}}(U)$ ya que $\{v_1, \ldots, v_n\}$ es una base de V si y sólo si $\{T(v_1), \ldots, T(v_n)\}$ es una base de U.
2) V es irreducible si y sólo si U es irreducible ya que $X \subset V$ es un $\mathbb{F}G$-submódulo si y sólo si $T(X) \subset U$ es un $\mathbb{F}G$-submódulo.

Ejemplo 0.166. El doble dual. Sean V, U y W $\mathbb{F}G$-módulos. Si $V^* = Hom_{\mathbb{F}}(V, \mathbb{F})$, entonces existe un isomorfismo de $\mathbb{F}G$-módulos $V \cong V^{**}$.
Consideremos $T \in Hom_{\mathbb{F}G}(V, U)$, entonces T induce un $\mathbb{F}G$-morfismo

$$\begin{array}{rcl} T^* : U^* & \longrightarrow & V^* \\ \varphi & \longmapsto & \varphi \circ T. \end{array}$$

En efecto, para todos $g \in G$ y $v \in V$ tenemos que

$$\begin{array}{rcl} [gT^*(\varphi)](v) = [g(\varphi \circ T)](v) & = & g(\varphi \circ T)(g^{-1}v) \\ & = & \varphi\left(T(g^{-1}v)\right) \\ & = & \varphi\left(g^{-1}T(v)\right) \\ & = & g\left(\varphi\left(g^{-1}T(v)\right)\right) = (g\varphi \circ T)(v) = [T^*(g\varphi)](v). \end{array}$$

Notemos que si $T \in Hom_{\mathbb{F}G}(V,U)$ y $S \in Hom_{\mathbb{F}G}(U,W)$ entonces $(S \circ T)^* = T^* \circ S^*$.
Sabemos que en dimensión finita existe un isomorfismo de espacios vectoriales

$$\begin{array}{rcl} \Phi_V : V & \longrightarrow & V^{**} \\ v & \longmapsto & \varphi_v \end{array} \quad \text{donde} \quad \begin{array}{rcl} \varphi_v : V^* & \longrightarrow & \mathbb{F} \\ f & \longmapsto & f(v). \end{array}$$

Este isomorfismo en efecto es un $\mathbb{F}G$-morfismo pues para todos $g \in G$ y $v \in V$ tenemos que

$$\begin{array}{rcl} [g\Phi_V(v)](f) = [g\varphi_v](f) & = & g\left(\varphi_v(g^{-1}f)\right) \\ & = & (g^{-1}f)(v) \\ & = & g^{-1}(f(gv)) \\ & = & f(gv) = \varphi_{gv}(f) = [\Phi_V(gv)](f). \end{array}$$

Más aún, si $T \in Hom_{\mathbb{F}G}(V,U)$ entonces existe $T^{**} \in Hom_{\mathbb{F}G}(V^{**},U^{**})$ tal que $T^{**} \circ \Phi_V = \Phi_U \circ T$.
Evaluando en $v \in V$ y $l \in U^*$ tenemos que

$$\begin{array}{rcl} [T^{**} \circ \Phi_V](v) & = & T^{**}(\varphi_v) \\ & = & [\varphi_v \circ T^*](l) \\ & = & \varphi_v(l \circ T) \\ & = & l(T(v)) = \varphi_{T(v)}(l) = [\Phi_U \circ T](v). \end{array}$$

Ejemplo 0.167. El $\mathbb{F}G$-isomorfismo del álgebra de grupo con su dual.
Existe un isomorfismo de $\mathbb{F}G$-módulos $\mathbb{F}(G) \cong \mathbb{F}(G)^*$ mediante la función

$$\begin{array}{rcl} T : \mathbb{F}(G) & \longrightarrow & \mathbb{F}(G)^* \\ r = \sum_{g\in G} r_g g & \longmapsto & T(r) \end{array} \quad \text{donde} \quad \begin{array}{rcl} T(r) : \mathbb{F}(G) & \longrightarrow & \mathbb{F} \\ s = \sum_{g\in G} s_g g & \longmapsto & \sum_{g\in G} r_g s_g. \end{array}$$

Primero, si $r = \sum_{g\in G} r_g g$, $s = \sum_{g\in G} s_g g$, $t = \sum_{g\in G} t_g g \in \mathbb{F}(G)$ y $a \in \mathbb{F}$ entonces

$$T(r)(s+t) = T(r)\Big(\sum_{g\in G}(s_g+t_g)g\Big) = \sum_{g\in G} r_g(s_g+t_g) = \sum_{g\in G} r_g s_g + \sum_{g\in G} r_g t_g = T(r)(s) + T(r)(t) \text{ y}$$
$$T(r)(as) = T(r)\Big(\sum_{g\in G} as_g g\Big) = \sum_{g\in G} r_g(as_g) = \sum_{g\in G} a r_g s_g = a\sum_{g\in G} r_g s_g = aT(r)(s)$$

y por lo tanto $T(r) \in Hom_{\mathbb{F}}(\mathbb{F}(G),\mathbb{F}) = \mathbb{F}(G)^*$.
Ahora, para ver que T es inyectiva, si $0 \neq r = \sum_{g\in G} r_g g \in \mathbb{F}(G)$ entonces existe al menos un coeficiente $r_{\tilde{g}} \neq 0$, así, $T(r)(\tilde{g}) = r_{\tilde{g}}$ y por lo tanto $T(r)$ no es el funcional lineal cero, por lo que T es inyectiva, y entonces es un isomorfismo de $\mathbb{F}$-espacios vectoriales pues su dominio y codominio tienen la misma dimensión. Por último, T respeta la acción ya que para todo $g \in G$ tenemos que

$$[T(gr)](s) = T\Big(g\sum_{x\in G} r_x x\Big)(s) = T\Big(\sum_{x\in G} r_x(gx)\Big)\Big(\sum_{y\in G} s_y y\Big) = \sum_{y=gx\in G} r_x s_y$$

y por otro lado

$$[gT(r)](s) = g\,[T(r)](g^{-1}s) = T(r)\Big(\sum_{y\in G} s_y(g^{-1}y)\Big) = \sum_{x=g^{-1}y\in G} r_x s_y$$

y entonces $T(gr) = gT(r)$ pues $x = g^{-1}y$ si y sólo si $gx = y$.

Teorema 0.168. *Sea V un $\mathbb{F}G$-módulo con base β y como en la demostración del teorema 0.125 tomemos la representación*

$$\begin{array}{rcl}\rho : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [\rho_g]_\beta\end{array} \quad \textit{donde} \quad \begin{array}{rcl}\rho_g : V & \longrightarrow & V \\ v & \longmapsto & gv\ ,\end{array}$$

denotemos $[\rho_g]_\beta$ como $[g]_\beta$, entonces

i) Si γ es otra base de V tenemos que la representación

$$\begin{array}{rcl}\sigma : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [g]_\gamma\end{array}$$

es equivalente a la representación ρ.

ii) Si τ es una representación equivalente a ρ existe una base δ de V tal que

$$\begin{array}{rcl}\tau : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [g]_\delta\end{array}$$

Demostración. i) Consideremos $Q = [Id_V]_\beta^\gamma$ la matriz de cambio de coordenadas de β en γ, entonces tenemos que

$$[g]_\gamma = [Id_V]_\beta^\gamma\,[g]_\beta\,[Id_V]_\gamma^\beta = Q\,[g]_\beta\,Q^{-1},$$

es decir, $[g]_\gamma$ y $[g]_\beta$ son matrices conjugadas, y de aquí tenemos que

$$[g]_\gamma\,Q = Q\,[g]_\beta\ ,$$

que traducido a los operadores asociados a esas matrices con respecto a la base β no es otra cosa que la definición de representaciones equivalentes. Más claramente, sea T el operador lineal tal que $Q = [T]_\beta^\gamma$, entonces

$$[g]_\gamma\,[T]_\beta^\gamma = [T]_\beta^\gamma\,[g]_\beta \text{ y por lo tanto}$$

$$[\sigma(g)\circ T]_\beta^\gamma = [T\circ\rho(g)]_\beta^\gamma \text{ , o bien, } \sigma(g)\circ T = T\circ\rho(g),$$

es decir, ρ y σ son representaciones equivalentes.

ii) Supongamos que τ y ρ son representaciones equivalentes, entonces para alguna matriz invertible B, tenemos que

$$\tau(g) = B\rho(g)B^{-1} \text{ para todo } g\in G.$$

Ahora, sea δ la base de $\mathbb{F}^n$ tal que la matriz de cambio de base de β a δ es B, es decir, $B = [Id_V]_\beta^\delta$, entonces, para todo $g\in G$

$$\tau(g) = [Id_V]_\beta^\delta \, \rho(g) \, [Id_V]_\delta^\beta = [Id_V]_\beta^\delta \, [g]_\beta \, [Id_V]_\delta^\beta = [g]_\delta$$

■

Vamos a ver ahora que $\mathbb{F}G$-módulos isomorfos corresponden a representaciones equivalentes.

Lema 0.169. *Los $\mathbb{F}G$-módulos V y U son isomorfos si y sólo si existen bases β_V y β_U de V y U respectivamente tales que $[g]_{\beta_V} = [g]_{\beta_U}$ para todo $g \in G$.*

Demostración. Sea $T : V \longrightarrow U$ un $\mathbb{F}G$-isomorfismo y $\beta_V = \{v_1, \ldots, v_n\}$ una base de V, entonces $\beta_U = \{T(v_1), \ldots, T(v_n)\}$ es una base de U. Si $g \in G$ entonces $gT(v_i) = T(gv_i)$ para todo i, por lo que se sigue que $[g]_{\beta_V} = [g]_{\beta_U}$.
Conversamente, si $\beta_V = \{v_1, \ldots, v_n\}$ una base de V y $\beta_U = \{u_1, \ldots, u_n\}$ es una base de U tales que $[g]_{\beta_V} = [g]_{\beta_U}$ para todo $g \in G$. Consideremos la tranformación lineal invertible tal que

$$\begin{array}{rcl} T : V & \longrightarrow & U \\ v_i & \longmapsto & u_i \end{array} \quad \text{para todo } i.$$

Si $g \in G$, ya que $[g]_{\beta_V} = [g]_{\beta_U}$ se sigue que $T(gv_i) = gT(v_i)$, es decir, T es un $\mathbb{C}G$-isomorfismo. ■

Teorema 0.170. *Sea V un $\mathbb{F}G$-módulo con base β y U un $\mathbb{F}G$-módulo con base γ.*
Entonces $V \cong U$ si y sólo si

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [g]_\beta \end{array} \quad y \quad \begin{array}{rcl} \sigma : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [g]_\gamma \end{array}$$

son representaciones equivalentes, donde escribimos $[g]_\beta$ en lugar de $[\rho_g]_\beta$.

Demostración. Por el lema anterior si los $\mathbb{F}G$-módulos V y U son isomorfos entonces existen bases β_V y β_U de V y U respectivamente tales que $[g]_{\beta_V} = [g]_{\beta_U}$ para todo $g \in G$.
Definamos ahora una representación de G dada por la función

$$\begin{array}{rcl} \tau : G & \longrightarrow & GL_n(\mathbb{F}) \\ g & \longmapsto & [g]_{\beta_V} \end{array} .$$

Luego, por el teorema 0.168 *i)* tenemos que τ es equivalente a ρ y σ, y por lo tanto, ρ y σ son equivalentes.
Conversamente, supongamos que ρ y σ son equivalentes, entonces por el teorema 0.168 *ii)* existe una base δ de V tal que $\sigma(g) = [g]_\delta$ para todo $g \in G$, esto es, $[g]_\delta = [g]_\gamma$ para todo $g \in G$. Por lo tanto, V y U son isomorfos por el lema anterior. ■

Ejemplo 0.171. Representación cociente. Sea V un $\mathbb{F}G$-módulo y W un $\mathbb{F}G$-submódulo de V. Consideremos para cada $v \in V$ el conjunto $v + W = \{v + w \mid w \in W\}$.
Es fácil ver que

$$v + W = W \text{ si y sólo si } v \in W.$$

Luego, los conjuntos $v + W$ corresponden a las clases de equivalencia de la siguiente relación de equivalencia dada en términos de W: $v, u \in V$ son *comparables* (relativos a W), es decir, $v + W = u + W$ si y sólo si $v - u \in W$. Esto no es más que las clases laterales de W en V con sus estructuras de grupos abelianos aditivos. Entonces el conjunto

$$V/W = \{v + W \mid v \in V\}$$

es un $\mathbb{F}$-espacio vectorial con las operaciones

$$(v + W) + (u + W) = (v + u) + W \text{ y}$$
$$a(u + W) = (av) + W \text{ con } a \in \mathbb{F}.$$

Y usando lo anterior también es fácil ver que $dim_{\mathbb{F}}(V/W) = dim_{\mathbb{F}}(V) - dim_{\mathbb{F}}(W)$ simplemente eligiendo una base $\beta_W = \{w_1, \ldots, w_m\}$ de W, luego se completa a una base de V con vectores $\beta = \{v_{m+1}, \ldots, v_n\}$ y se toman las clases laterales cuyos representantes son los vectores con los que completamos, es decir, $\beta_{V/W} = \{v_{m+1} + W, \ldots, v_n + W\}$ es la base del espacio cociente. Más aún, V/W es una representación de G con la acción

$$\begin{array}{rcl} \cdot : G \times V/W & \longrightarrow & V/W \\ (g, v + W) & \longmapsto & gv + W. \end{array}$$

Ahora, si $V = W_1 \oplus W_2$, como $\mathbb{F}G$-módulos, es decir, para todo $v \in V$ tenemos que existen únicos $w_1 \in W_1, w_2 \in W_2$ tales que $v = w_1 + w_2$, entonces

$$v + W_1 = (w_1 + w_2) + W_1 = w_2 + w_1 + W_1 = w_2 + W_1$$

y así las representaciones V/W_1 y W_2 son equivalentes pues la función

$$\begin{array}{rcl} T : V/W_1 & \longrightarrow & W_2 \\ w_2 + W_1 & \longmapsto & w_2 \end{array}$$

es un isomorfismo de $\mathbb{F}G$-módulos.

Observación 0.172. En el lenguaje de matrices, si V es una representación reducible de G y W es una subrepresentación de V, entonces, eligiendo una base γ de W la podemos extender con un conjunto δ a una base β de V, es decir, $\beta = \gamma \cup \delta$ y entonces, por el ejempo 0.171 tenemos que la matriz asociada a la representación, para todo $g \in G$ tiene la forma

$$[\rho_V(g)]_\beta = \begin{pmatrix} [\rho_W(g)]_\gamma & (*) \\ 0 & \left[\rho_{V/W}(g)\right]_{\widehat{\delta}} \end{pmatrix}$$

donde $\rho_W(g)$ es el operador asociado a la representación de G en W, $(*)$ es una matriz arbitraria y $\rho_{V/W}(g)$ es el operador asociado a la representación de G en V/W cuya base es $\widehat{\delta}$ que es inducida por δ, es decir, las clases de los elementos de δ.
Si V es una representación descomponible de G, es decir, $V = W_1 \oplus W_2$ y W_1, W_2 son $\mathbb{F}G$-submódulos no triviales, entonces eligiendo bases γ_1 y γ_2 de W_1 y W_2 respectivamente, y uniendo estas bases tenemos una base de V, $\gamma = \gamma_1 \cup \gamma_2$, y entonces, por el ejemplo 0.171 tenemos que la matriz asociada a la representación, para todo $g \in G$ tiene la forma

$$[\rho_V(g)]_\beta = \begin{pmatrix} [\rho_{W_1}(g)]_{\gamma_1} & 0 \\ 0 & [\rho_{W_2}(g)]_{\gamma_2} \end{pmatrix}.$$

Teorema de Maschke y reducibilidad completa

Ahora tenemos el resultado más básico de la teoría de representaciones de grupos finitos. Fue descubierto por Heinrich Maschke en 1898. Como consecuencia tendremos que todo $\mathbb{F}G$-módulo es suma directa de $\mathbb{F}G$-submódulos irreducibles. Así, el estudio de la teoría de representaciones de grupos finitos se reduce al estudio de $\mathbb{F}G$-módulos irreducibles.

Teorema 0.173. ***MASCHKE.*** *Sea G un grupo finito y $\mathbb{F}$ un campo de $char(\mathbb{F}) = 0$ o tal que $char(\mathbb{F}) \nmid |G|$. Si V es un $\mathbb{F}G$-módulo de dimensión finita y $U \subset V$ es un $\mathbb{F}G$-submódulo, entonces U es sumando directo de V como $\mathbb{F}G$-módulos, es decir existe un $\mathbb{F}G$-submódulo $W \subset V$ tal que*

$$V = U \oplus W.$$

Demostración. Dado U un $\mathbb{F}G$-submódulo de un $\mathbb{F}G$-módulo V, tenemos que en particular U es un $\mathbb{F}$-subespacio vectorial de V por lo que existe un subespacio W_U tal que $V = U \oplus W_U$, por ejemplo, podemos elegir una base de U, completarla a una base de V y el generado por los vectores con los que completamos cumple lo anterior. Sin embargo, no necesariamente W_U es un $\mathbb{F}G$-submódulo de V y existen infinitas formas de elegir W_U, de acuerdo a cómo se elija una base de U y de cómo se extienda ésta a una base de V. Luego, consideremos la proyección de V en U, es decir, la función

$$\begin{array}{rccc} \pi_U & : & V & \longrightarrow & U \\ & & u+w & \longmapsto & u, \end{array}$$

y entonces $ker(\pi_U) = W_U$ y $Im(\pi_U) = U$. Vamos ahora a modificar esta proyección para obtener un morfismo de $\mathbb{F}G$-módulos de V en V que tenga imagen U, para esto definimos

$$\begin{array}{rccc} \vartheta_U : V & \longrightarrow & V \\ v & \longmapsto & \dfrac{1}{|G|}\displaystyle\sum_{g\in G} g\pi_U(g^{-1}v). \end{array}$$

Para que ϑ_U tenga sentido usamos la hipotésis sobre la característica de $\mathbb{F}$ y el hecho de que G es finito. Claramente ϑ_U es una transformación lineal de V en V y $Im(\vartheta_U) \subset U$. Veamos ahora que ϑ_U es un morfismo de $\mathbb{F}G$-módulos, entonces para todos $v \in V$ y $x \in G$ tenemos que

$$\vartheta_U(xv) = \frac{1}{|G|}\sum_{g\in G} g\pi_U(g^{-1}(xv)) = \frac{1}{|G|}\sum_{g\in G} g\pi_U((g^{-1}x)v)$$

pero g corre sobre todos los elementos de G, entonces sea $y = x^{-1}g$, así, y también varía sobre todos los elementos de G y podemos escribir entonces

$$\begin{array}{rcl} \vartheta_U(xv) & = & \dfrac{1}{|G|}\displaystyle\sum_{g\in G} xx^{-1}g\pi_U((g^{-1}x)v) \\ & = & \dfrac{1}{|G|}\ x\Big(\displaystyle\sum_{g\in G}(x^{-1}g)\pi_U((g^{-1}x)v)\Big) \\ & = & \dfrac{1}{|G|}\ x\Big(\displaystyle\sum_{y\in G} y\pi_U(y^{-1}v)\Big) \\ & = & x\Big(\dfrac{1}{|G|}\displaystyle\sum_{y\in G} y\pi_U(y^{-1}v)\Big) = x(\vartheta_U(v)). \end{array}$$

y por lo tanto ϑ_U es un morfismo de $\mathbb{F}G$-módulos.
Veamos ahora que $U \subset Im(\vartheta_U)$, primero notemos que para cualesquiera $u \in U$ y $g \in G$ se tiene que $gu \in U$ pues U es un $\mathbb{F}G$-submódulo de V y por lo tanto $\pi_U(gu) = gu$, así tenemos que

$$\vartheta_U(u) = \frac{1}{|G|}\sum_{g\in G} g\pi_U(g^{-1}u) = \frac{1}{|G|}\sum_{g\in G} g(g^{-1}u) = \frac{1}{|G|}\sum_{g\in G} u = u.$$

Esto significa que $Im(\vartheta_U) = U$. Ahora si $v \in V$, entonces $\vartheta_U(v) \in U$ y por lo anterior tenemos que $\vartheta_U(\vartheta_U(v)) = \vartheta_U(v)$, es decir, $\vartheta_U^2(v) = \vartheta_U(v)$ por lo que ϑ_U, es efectivamente una proyección. Luego, ya que $Im(\vartheta_U) = U$, entonces sea $W = ker(\vartheta_U)$, que es un $\mathbb{F}G$-submódulo de V, y $V = U \oplus W$ por ser ϑ_U una proyección. ■

Lo siguiente es una consecuencia importante del Teorema de Maschke, vamos a ver que todo $\mathbb{F}G$-módulo (representación de un grupo finito) es suma directa de $\mathbb{F}G$-submódulos irreducibles (subrepresentaciones irreducibles).

Definición 0.174. *Una representación $\rho : G \longrightarrow GL(V)$ (o equivalentemente, V, el $\mathbb{F}G$-módulo asociado) es llamada(o) **completamente reducible** si es suma directa de subrepresentaciones irreducibles, es decir, si existen $\mathbb{F}G$-submódulos irreducibles U_i tales que*

$$V = U_1 \oplus \cdots \oplus U_r.$$

Observación 0.175. En el lenguaje de módulos esta definición dice que un $\mathbb{F}G$-módulo V es completamente reducible si es semisimple visto como $\mathbb{F}(G)$-módulo (el módulo sobre el álgebra de grupo inducido por la acción).

Corolario 0.176. *Sea G un grupo. Entonces todo $\mathbb{F}G$-módulo no trivial es completamente reducible.*

Demostración. Sea V un $\mathbb{F}G$-módulo no trivial de dimensión finita, vamos a hacer inducción sobre $dim_{\mathbb{F}}(V) = n$. Si $dim_{\mathbb{F}}(V) = 1$ el resultado es cierto pues V siempre es irreducible ya que no hay $\mathbb{F}G$-submódulos no triviales. Si V es irreducible no hay nada que probar, entonces supongamos que V es reducible. Así V tiene un $\mathbb{F}G$-submódulo propio U, luego, por el Teorema de Maschke existe un $\mathbb{F}G$-submódulo W tal que $V = U \oplus W$. Ahora, ya que $dim_{\mathbb{F}}(U) < dim_{\mathbb{F}}(V)$ y $dim_{\mathbb{F}}(W) < dim_{\mathbb{F}}(V)$, por hipótesis de inducción U y W son completamente reducibles, es decir, tenemos una descomposición

$$U = U_1 \oplus \cdots \oplus U_r \quad \text{y} \quad W = W_1 \oplus \cdots \oplus W_s,$$

para algunos $r, s \in \mathbb{N}$, y entonces tenemos que

$$V = U_1 \oplus \cdots \oplus U_r \oplus W_1 \oplus \cdots \oplus W_s,$$

es decir, V es una suma directa de $\mathbb{F}G$-módulos irreducibles, por lo que V es completamente reducible.
■

Otra consecuencia útil del Teorema de Maschke es:

Proposición 0.177. *Sean V, W dos $\mathbb{C}G$-módulos y $\vartheta : V \longrightarrow W$ un morfismo de $\mathbb{C}G$-módulos. Entonces existe un $\mathbb{C}G$-submódulo U de V tal que*

$$V = Ker(\vartheta) \oplus U \text{ y } U \cong Im(\vartheta) \subset W.$$

Demostración. Sabemos que $Ker(\vartheta)$ es un $\mathbb{C}G$-submódulo, así, por el Teorema de Maschke existe un submódulo U de V tal que $V = Ker(\vartheta) \oplus U$, luego definamos la función

$$\begin{aligned} \overline{\vartheta} : U &\longrightarrow Im(\vartheta) \\ u &\longmapsto \vartheta(u). \end{aligned}$$

Claramente $\overline{\vartheta}$ es un morfismo de $\mathbb{C}(G)$-módulos pues ϑ es un morfismo de $\mathbb{C}(G)$-módulos. Más aún, es un isomorfismo ya que si $u \in Ker(\overline{\vartheta})$ entonces $u \in Ker(\vartheta) \cap U = \{0\}$ y por lo tanto $Ker(\overline{\vartheta}) = \{0\}$. Ahora, si $w \in Im(\vartheta)$ entonces $w = \vartheta(v)$ para algún $v \in V$, y por lo anterior, escribamos $v = k + u$ con $\in Ker(\vartheta),\ u \in U$. Entonces

$$w = \vartheta(v) = \vartheta(k+u) = \vartheta(k) + \vartheta(u) = \vartheta(u) = \overline{\vartheta}(u).$$

Por lo tanto $Im(\overline{\vartheta}) = Im(\vartheta)$ y así tenemos que $\overline{\vartheta} : U \longrightarrow Im(\vartheta)$ es un isomorfismo de $\mathbb{C}G$-módulos, es decir, $U \cong Im(\vartheta)$. ■

Observación 0.178. El corolario 0.176 nos dice que para entender $\mathbb{F}G$-módulos es suficiente estudiar todos los $\mathbb{F}G$-módulos irreducibles.

Entonces, en el lenguaje de módulos el Teorema de Maschke y el corolario 0.176 se enuncian como:

Teorema 0.179. *Si G es un grupo finito y $\mathbb{F}$ un campo tal que $char(\mathbb{F}) = 0$ o $char(\mathbb{F}) \nmid |G|$ entonces cualquier módulo sobre el álgebra de grupo $\mathbb{F}(G)$ es semisimple, y en particular, la representación regular $\mathbb{F}(G)$ es semisimple.*

Lema de Schur

Lo siguiente será un resultado concerniente a $\mathbb{F}G$-módulos irreducibles, llamado el Lema de Schur, éste es fundamental para la Teoría de Representaciones, y da una aplicación inmediata para determinar todas las representaciones irreducibles de grupos abelianos finitos. A partir de ahora consideraremos siempre $\mathbb{F} = \mathbb{C}$.

Lema 0.180. ***SCHUR.*** *Sean $\rho : G \longrightarrow GL(V)$ y $\tau : G \longrightarrow GL(U)$ dos representaciones irreducibles de un grupo G (es decir, V y U son $\mathbb{C}G$-módulos irreducibles).*

(1) *Si $T : V \longrightarrow U$ es un morfismo de $\mathbb{C}G$-módulos, entonces T es isomorfismo ($\rho \cong \tau$) o $T = T_0$, donde T_0 es la transformación lineal cero.*

(2) *Si $V = U$ y $T : V \longrightarrow V$ es un endomorfismo de $\mathbb{C}G$-módulos, entonces T es un múltiplo escalar de la identidad en V, es decir, $T = \lambda I_V$, para algún $\lambda \in \mathbb{C}$.*

Demostración. (1) Supongamos que $T(v) \neq 0$ para algún $v \in V$, por lo que $Im(T) \neq \{0\}$ y además $Im(T)$ es un $\mathbb{C}G$-sumódulo de U, pero U es irreducible, por lo que $Im(T) = U$ y como $ker(T) \neq V$ es un $\mathbb{C}G$-submódulo de V y V es irreducible entonces $Ker(T) = \{0\}$ y por lo tanto, T es invertible, así, T es un isomorfismo de $\mathbb{C}G$-módulos.
(2) Recordemos que $\lambda \in \mathbb{C}$ es valor propio de T si existe $0_V \neq v \in V$ tal que $T(v) = \lambda v$, es decir, si $(T - \lambda I_V)(v) = 0$ para algún $0_V \neq v \in V$, o de modo equivalente, si $T - \lambda I_V$ no es invertible.
Así, dada una base β de V, y si $n = dim_{\mathbb{C}}(V)$, entonces los valores propios de T son los escalares $\lambda \in \mathbb{C}$ que satisfacen la ecuación

$$det([T]_\beta - \lambda I_n) = 0$$

que no es más que el polinomio característico de T, un polinomio de grado n con coeficientes en $\mathbb{C}$, entonces por el Teorema Fundamental del Álgebra el polinomio característico de T tiene una raíz λ, es decir, un valor propio de T y entonces $Ker(T - \lambda I_V) \neq \{0\}$ por lo que $Ker(T - \lambda I_V)$ es un $\mathbb{C}G$-submódulo no cero de V, pero V es irreducible y entonces necesariamente se tiene que $Ker(T - \lambda I_V) = V$, esto significa que para todo $v \in V$ tenemos que $(T - \lambda I_V)(v) = 0$, es decir, $T(v) = \lambda I_V(v)$, por lo que $T = \lambda I_V$ como queríamos. ■

La segunda parte del Lema de Schur tiene el siguiente converso:

Teorema 0.181. *Sea V un $\mathbb{C}G$-módulo no cero y supongamos que todo $\mathbb{C}G$-morfismo $T : V \longrightarrow V$ es un múltiplo escalar de la identidad en V, es decir, $T = \lambda I_V$, entonces V es irreducible.*

Demostración. Supongamos que V es reducible, entonces existe un $\mathbb{C}G$-submodulo U propio de V. Luego, por el Teorema de Maschke U tiene un complemento W, es decir, un $\mathbb{C}G$-submódulo de V tal que $V = U \oplus W$. Entonces la proyeccion π_u es un morfismo de $\mathbb{C}G$-módulos que no es múltiplo escalar de la identidad, esto es una contradicción. Por lo tanto V es irreducible. ■

Luego la interpretación del Lema de Schur y su converso en términos de representaciones es:

Corolario 0.182. *Sea $\rho : G \longrightarrow GL_n(\mathbb{C})$ una representación de G. Entonces ρ es irreducible si y sólo si toda matriz A de $n \times n$ que satisface que*

$$A\rho(g) = \rho(g)A \quad \textit{para todo } g \in G$$

tiene la forma $A = \lambda I_n$ para algún $\lambda \in \mathbb{C}$.

Demostración. Recordemos que ρ induce una acción lineal en $\mathbb{C}^n$ dada por $gv = \rho(g)v$ para todos $v \in \mathbb{C}^n,\ g \in G$. Para cualquier $A \in M_n(\mathbb{C})$ consideremos la función

$$\begin{aligned} T_A : \mathbb{C}^n &\longrightarrow \mathbb{C}^n \\ v &\longmapsto Av\ , \end{aligned}$$

que es una transformación lineal en $\mathbb{C}^n$, y es un morfismo de $\mathbb{C}G$-módulos si y sólo si para todos $v \in \mathbb{C}^n,\ g \in G$ tenemos que $T_A(gv) = gT_A(v)$ si y sólo si $A(gv) = g(Av)$ si y sólo si $A\rho(g)v = \rho(g)Av$, es decir, si y sólo si $A\rho(g) = \rho(g)A$ para todo $g \in G$.
Por lo tanto, si ρ es irreducible y $A\rho(g) = \rho(g)A$ para todo $g \in G$, por lo anterior T_A es un morfismo de $\mathbb{C}G$-módulos, y por la segunda parte del Lema de Schur, A debe ser múltiplo escalar de I_n. Ahora, si toda matriz de $n \times n$ que satisface que $A\rho(g) = \rho(g)A$ para todo $g \in G$ tiene la forma $A = \lambda I_n$ para algún $\lambda \in \mathbb{C}$, por el converso del Lema de Schur tenemos que ρ es irreducible. ■

El Lema de Schur entonces establece que todo morfismo de $\mathbb{C}G$-módulos entre $\mathbb{C}G$-módulos irreducibles es siempre cero o un isomorfismo. También, los morfismos de $\mathbb{C}G$-módulos de un $\mathbb{C}G$-módulo irreducible en sí mismo son siempre múltiplos escalares de la identidad.

Representaciones de grupos abelianos finitos

Recordemos que el teorema 0.50 decía que todo grupo abeliano finito es producto directo de grupos cíclicos, y es el más importante sobre la estructura de grupos abelianos finitos, a partir de él, basta determinar las representaciones irreducibles de productos directos de grupos cíclicos para describir las representaciones irreducibles de todos los grupos abelianos finitos.
Primero tenemos una caracterización de las representaciones irreducibles de grupos abelianos.

Teorema 0.183. *Las representaciones irreducibles de un grupo abeliano son de grado* 1.

Demostración. Sea G un grupo abeliano y sea V un $\mathbb{C}G$-módulo irreducible.
Luego, para todo $x \in G$ la función

$$\begin{array}{rcl} T_x : V & \longrightarrow & V \\ v & \longmapsto & xv \end{array}$$

es un endomorfismo de V (operador lineal) pues la acción de G en V es lineal, más aún, ya que G es abeliano tenemos que $(gx)v = (xg)v$ para todo $g \in G$ y entonces

$$T_x(gv) = x(gv) = (xg)v = (gx)v = g(xv) = gT_x(v),$$

es decir, T_x es un morfismo de $\mathbb{C}G$-módulos, por el lema de Schur tenemos que la función T_x es un múltiplo escalar de la identidad, es decir $T_x = \lambda_x I_V$ para algún $\lambda_x \in \mathbb{C}$, por lo que

$$xv = T_x(v) = \lambda_x I_V(v) = \lambda_x v \text{ para todo } v \in V.$$

Por lo tanto si $W \subseteq V$ es un subespacio vectorial, entonces para todos $x \in G$ y $w \in W$ tenemos que

$$xw = T_x(w) = \lambda_x I_V(w) = \lambda_x w \in W,$$

por lo que todo subespacio vectorial W de V es cerrado bajo la acción de G y por lo tanto es un $\mathbb{C}G$-submódulo de V, pero como V es irreducible esto sólo es posible si $dim_{\mathbb{C}}(V) = 1$. ■

Teorema 0.184. *Sea G un grupo abeliano. Entonces existen tantas representaciones irreducibles de G sobre $\mathbb{C}$ de grado* 1 *como $|G|$.*

Demostración. Sea G un grupo abeliano tal que

$$G \cong C_{n_1} \times \cdots \times C_{n_m}$$

donde $|G| = n = n_1 \cdots n_m$, $n_i | n_{i+1}$ y $C_{n_i} \cong \mathbb{Z}/n_i\mathbb{Z} \cong \mathbb{Z}_{n_i}$. Sea ξ_i un generador de C_{n_i} y consideremos

$$g_i = (1, \ldots, \xi_i, \ldots 1)$$

con ξ_i en la i-ésima entrada, entonces

$$G = \langle g_1, \ldots, g_m \rangle \text{ con } {g_i}^{n_i} = e \text{ y } g_i g_j = g_j g_i \text{ para todos } i, j.$$

Ahora sea $\rho : G \longrightarrow GL_n(\mathbb{C})$ una representación de irreducible de G sobre $\mathbb{C}$. Entonces $n = 1$ por el teorema 0.183 y por lo tanto, para cada $1 \leqslant i \leqslant m$ existe $\zeta_i \in \mathbb{C}$ tal que

$$\rho(g_i) = (\zeta_i) \in M_{1\times 1}(\mathbb{C}).$$

Luego, ya que el orden de g_i es n_i tenemos que ${\zeta_i}^{n_i} = 1$, es decir, ζ_i es raíz n_i-ésima de la unidad. También, los valores $\zeta_1, \ldots, \zeta_m$ determinan a ρ ya que para todo $g \in G$ tenemos que $g = g_1^{i_1} \cdots g_m^{i_m}$ para algunos enteros $i_1, \ldots, i_m$, y entonces

$$\rho(g) = \rho(g_1^{i_1} \cdots g_m^{i_m}) = (\zeta_1^{i_1} \cdots \zeta_m^{i_m}).$$

Dada una representación de G que cumpla lo anterior para todos $i_1, \ldots, i_m$ se escribirá

$$\rho = \rho_{\zeta_1,\ldots,\zeta_m}.$$

A la inversa, dadas ζ_i ($1 \leqslant i \leqslant m$) cualesquiera raíces n_i-ésimas de la unidad, la función

$$\begin{array}{rcl} \rho \ : \ G & \longrightarrow & GL_1(\mathbb{C}) \cong \mathbb{C}^* \\ g_1^{i_1} \cdots g_m^{i_m} & \longmapsto & (\zeta_1^{i_1} \cdots \zeta_m^{i_m}) \end{array}$$

es una representación de G de grado 1 y por lo tanto existen $n = n_1 n_2 \cdots n_m$ de tales representaciones y dos a dos no son equivalentes por construcción. ■

Observación 0.185. El teorema 0.184 nos garantiza la existencia de tantas representaciones irreducibles de un grupo abeliano como su orden y de hecho el converso es cierto: si un grupo tiene tantas representaciones irreducibles como su orden, entonces debe ser abeliano, no daremos una demostración aquí, pueden consultarse los detalles en [1], Capítulo 8.

Álgebra de grupo y el espacio de $\mathbb{F}G$-morfismos.

Una consecuencia del Teorema de Maschke fue el corolario 0.176, así, tenemos que si G es un grupo finito entonces para el álgebra de grupo, vista como el $\mathbb{C}G$-módulo regular, existe una descomposición

$$\mathbb{C}(G) = U_1 \oplus \cdots \oplus U_r$$

en $\mathbb{C}G$-módulos irreducibles U_i, vamos a ver que todo $\mathbb{C}G$-módulo irreducible V es isomorfo a alguno de los sumandos U_i que aparecen en la descomposición de $\mathbb{C}(G)$. Y como consecuencia, existe sólo un número finito de $\mathbb{C}G$-módulos irreducibles no isomorfos. Luego, para encontrar todos los $\mathbb{C}G$-módulos irreducibles es suficiente descomponer a $\mathbb{C}(G)$ como suma directa de $\mathbb{C}G$-submódulos irreducibles.

Teorema 0.186. *Sea V un $\mathbb{C}G$-módulo y escribamos $V = U_1 \oplus \cdots \oplus U_s$, una suma directa de $\mathbb{C}G$-submódulos irreducibles U_i. Si $U \subset V$ es cualquier $\mathbb{C}G$-submódulo irreducible entonces $U \cong U_i$ para algún i, es decir, todo $\mathbb{C}(G)$-submódulo irreducible de G sobre $\mathbb{C}$ es isomorfo a un $\mathbb{C}(G)$-submódulo irreducible del álgebra de grupo $\mathbb{C}(G)$.*

Demostración. Para todo $u \in U \subset V$ tenemos que $u = u_1 + \cdots + u_s$ para vectores únicos $u_i \in U_i$. Consideremos ahora la proyección en la i-ésima componente de U, es decir, la función

$$\begin{array}{rcl} \pi_i : U & \longrightarrow & U_i \\ u & \longmapsto & u_i. \end{array}$$

Luego, podemos elegir i tal que $u_i \neq 0$ para alguna $u \in U$ y así $\pi_i \neq 0$, entonces, ya que U y U_i son irreducibles, y π_i claramente es un morfismo no cero de $\mathbb{C}G$-módulos entre ellos, por la primera parte del Lema de Schur tenemos que $U \cong U_i$. ■

Definición 0.187. *Si V es un $\mathbb{C}G$-módulo y U es un $\mathbb{C}G$-módulo irreducible entonces decimos que U es un* ***factor de composición*** *de V, si V tiene un $\mathbb{C}G$-submódulo isomorfo a U.*
Dos $\mathbb{C}G$-módulos V y W tienen un ***factor de composición común*** *si hay un $\mathbb{C}G$-módulo irreducible que es factor de composición de V y W.*

Podemos enunciar ahora el siguiente:

Teorema 0.188. *Todo $\mathbb{C}G$-módulo irreducible es factor de composición de $\mathbb{C}(G)$, es decir, si el álgebra de grupo, vista como el $\mathbb{C}G$-módulo regular, se escribe como*

$$\mathbb{C}(G) = U_1 \oplus \cdots \oplus U_r,$$

una suma directa de $\mathbb{C}G$-submódulos irreducibles U_i, entonces todo $\mathbb{C}G$-módulo irreducible W es isomorfo a alguno de los sumandos U_i.

Demostración. Sea W un $\mathbb{C}G$-módulo irreducible y tomemos un vector no nulo $w \in W$. Luego, notemos que el conjunto $\{rw \mid r \in \mathbb{C}(G)\}$ es un $\mathbb{C}G$-submódulo de W no nulo y ya que W es irreducible tenemos que

$$W = \{rw \mid r \in \mathbb{C}(G)\}.$$

Ahora, la función

$$\begin{array}{rcl} \vartheta : \mathbb{C}(G) & \longrightarrow & W \\ r & \longmapsto & rw \end{array}$$

tiene imagen W y claramente es una transformación lineal pues la acción de $\mathbb{C}(G)$ en W es lineal. Más aún, ϑ es un morfismo de $\mathbb{C}(G)$-módulos ya que para todos $r, s \in \mathbb{C}(G)$ tenemos que

$$\vartheta(rs) = (rs)w = r(sw) = r\vartheta(s)$$

y en particular, para los elementos de G vistos dentro del álgebra de grupo tenemos que

$$\vartheta(gr) = (gr)w = g(rw) = g\vartheta(r).$$

Ahora, por la proposición 0.177 tenemos que existe un $\mathbb{C}(G)$-submódulo U tal que

$$\mathbb{C}(G) = Ker(\vartheta) \oplus U \text{ con } U \cong Im(\vartheta) = W.$$

Ya que W es irreducible U debe ser irreducible y por el teorema 0.186 $U \cong U_i$ para algún i y así $W \cong U_i$. ■

Este teorema muestra que sólo existe un número finito de $\mathbb{C}G$-módulos irreducibles salvo isomorfismo, es decir,

Corolario 0.189. *Si G es un grupo finito, entonces existe sólo un número finito de $\mathbb{C}G$-módulos irreducibles no isomorfos.*

De acuerdo al teorema 0.188, para hallar todos los $\mathbb{C}G$-módulos irreducibles sólo necesitamos descomponer al $\mathbb{C}G$-módulo regular $\mathbb{C}(G)$ como suma directa de $\mathbb{C}G$-submódulos irreducibles.
Luego, recordando que tenemos la descomposición del $\mathbb{C}G$-módulo regular

$$\mathbb{C}(G) = U_1 \oplus \cdots \oplus U_r,$$

la siguiente pregunta es: ¿cuántos de estos U_i son isomorfos a un $\mathbb{C}G$-módulo irreducible dado V? la respuesta será que hay tantos como $dim_{\mathbb{C}}(V)$, para la prueba se requiere dar estructura de espacio vectorial al conjunto de $\mathbb{C}G$-morfismos entre dos $\mathbb{C}G$-módulos.

Teorema 0.190. *Sean V y U $\mathbb{C}G$-módulos, denotaremos $Hom_{\mathbb{C}G}(V,U)$ al conjunto de $\mathbb{C}G$-morfismos de V en U, entonces éste es un espacio vectorial sobre $\mathbb{C}$ con las operaciones puntuales de suma y producto por escalar, es decir,*

$$(T+S)(v) := T(v) + S(v),$$
$$(\lambda T)(v) := \lambda T(v).$$

Demostración. La prueba de que se satisfacen los axiomas de espacio vectorial es directa a partir de la forma en que están definidas las operaciones. ■

Como una consecuencia importante del Lema de Schur tenemos que si V es un $\mathbb{C}G$-módulo irreducible entonces

$$End_{\mathbb{C}G}(V) = \{\ \lambda I_V \mid \lambda \in \mathbb{C}\ \} \cong \mathbb{C},$$

es decir, $Hom_{\mathbb{C}G}(V,V) = End_{\mathbb{C}G}(V)$ es un anillo con división.
Además, en el espacio $Hom_{\mathbb{C}G}(V,U)$ tenemos lo siguiente:

Proposición 0.191. *Supongamos que V, U son $\mathbb{C}G$-módulos irreducibles, entonces*

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V,U)\big) = \begin{cases} 1 & si \quad V \cong U; \\ 0 & si \quad V \ncong U. \end{cases}$$

Demostración. Si $V \ncong U$ entonces por el Lema de Schur se tiene que $dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V,U)\big) = 0$. Ahora supongamos que $V \cong U$ y vía un $\mathbb{C}G$-isomorfismo $T : V \longrightarrow U$. Luego, para cualquier $\varphi \in Hom_{\mathbb{C}G}(V,U)$ no nulo tenemos que $T^{-1} \circ \varphi : V \longrightarrow V$ es un $\mathbb{C}G$-isomorfismo y por lo tanto, por el Lema de Schur se tiene que existe $\lambda \in \mathbb{C}$ tal que $T^{-1} \circ \varphi = \lambda I_V$, es decir, $\varphi = \lambda T$, así

$$Hom_{\mathbb{C}G}(V,U) = \{\lambda T \mid \lambda \in \mathbb{C}\},$$

que es un $\mathbb{C}$-espacio vectorial de dimensión 1. ■

Teorema 0.192. *Sean V y U dos $\mathbb{C}G$-módulos y supongamos que $Hom_{\mathbb{C}G}(V,U)$ es no trivial. Entonces V y U tienen un factor de composición común.*

Demostración. Sea $\varphi \in Hom_{\mathbb{C}G}(V,U)$ no nulo, entonces tenemos que $V \cong Ker(\varphi) \oplus W$ para algún $\mathbb{C}G$-submódulo no trivial W de V por el Teorema de Maschke. Sea X un $\mathbb{C}G$-submódulo irreducible de W. Ya que $\varphi(X) \neq \{0\}$, $\varphi|_X : X \longrightarrow \varphi(X)$ es un isomorfismo, es decir, $\varphi(X) \cong X$, así, X es factor de composición de V y de U. ■

Los siguientes resultados muestran cómo calcular en general la dimensión de $Hom_{\mathbb{C}G}(V,U)$.

Proposición 0.193. *Dados $\mathbb{C}G$-módulos V, W, V_i, W_j, con $i \in \{1,\dots,r\}$ y $j \in \{1,\dots,s\}$, entonces*

i) $dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V, W_1 \oplus \cdots \oplus W_s)\big) = \sum_{j=1}^{s} dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V,W_j)\big)$,

ii) $dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V_1 \oplus \cdots \oplus V_r, W)\big) = \sum_{i=1}^{r} dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V_i, W)\big)$, *y de ambas partes se sigue que*

iii) $dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V_1 \oplus \cdots \oplus V_r, W_1 \oplus \cdots \oplus W_s) = \sum_{i=1}^{r}\sum_{j=1}^{s} dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V_i, W_j)\big)$.

Demostración. La prueba se omite porque es algo técnica y se hace primero para dos factores y luego por inducción para s factores, para estos detalles ver [13] capítulo 11. ■

Si aplicamos *iii*) cuando V_i y W_j son irreducibles y por la Proposición 0.191 podemos encontrar en general $dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V, W)\big)$, en el siguiente corolario, tomamos nada más uno de los $\mathbb{C}G$-módulos irreducible.

Corolario 0.194. *Sea V un $\mathbb{C}G$-módulo con*

$$V = U_1 \oplus \cdots \oplus U_r,$$

donde cada U_i es un $\mathbb{C}G$-módulo irreducible y sea W cualquier $\mathbb{C}G$-módulo irreducible, entonces

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V, W)\big) = dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(W, V)\big) \text{ es el número de } U_i \text{ tal que } U_i \cong W.$$

Demostración. Se sigue de la proposición anterior que

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V, W) = \sum_{j=1}^{s} dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(U_j, W)\big), \text{ y}$$
$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(W, V)\big) = \sum_{i=1}^{r} dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(W, U_i)\big),$$

y de la proposición 0.191 tenemos que

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(U_i, W)\big) = dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(W, U_i)\big) = \begin{cases} 1 & si \quad U_i \cong W; \\ 0 & si \quad U_i \ncong W\ , \end{cases}$$

por lo que se tiene lo que deseabamos. ■

Vamos a aplicar esto al espacio de $\mathbb{C}G$-morfismos del $\mathbb{C}G$-módulo regular (álgebra de grupo) en cualquier otro $\mathbb{C}G$-módulo.

Teorema 0.195. *Sea V un $\mathbb{C}G$-módulo y $\mathbb{C}(G)$ el $\mathbb{C}G$-módulo regular. Entonces*

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}\big(\mathbb{C}(G), V\big)\big) = dim_{\mathbb{C}}V.$$

Demostración. Sean $d = dim_{\mathbb{C}}(V)$ y $\{v_1, \ldots, v_d\}$ una base de V, luego, para cada $i \in \{1, \ldots, d\}$ definamos la función

$$\begin{array}{rccl} \phi_i & : & \mathbb{C}(G) & \longrightarrow & V \\ & & \sum_{g\in G} a_g g & \longmapsto & \Big(\sum_{g\in G} a_g g\Big) v_i = \sum_{g\in G} a_g (g v_i). \end{array}$$

Luego, para todos $r \in \mathbb{C}(G)$ y $x \in G$ tenemos que

$$\begin{aligned}\phi_i(xr) &= \phi_i\Big(x\sum_{g\in G}a_g g\Big) = \phi_i\Big(\sum_{g\in G}a_g(xg)\Big)\\ &= \Big(\sum_{g\in G}a_g(xg)\Big)v_i = \sum_{g\in G}a_g((xg)v_i)\\ &= \sum_{g\in G}a_g x(gv_i) = x\Big(\sum_{g\in G}a_g(gv_i)\Big)\\ &= x\ \phi_i\Big(\sum_{g\in G}a_g g\Big) = x\phi_i(r),\end{aligned}$$

y por lo tanto $\phi_i \in Hom_{\mathbb{C}G}\big(\mathbb{C}(G), V\big)$. De hecho, para todo $r, s \in \mathbb{C}(G)$ tenemos que

$$\phi_i(rs) = (rs)v_i = r(sv_i) = r(\phi_i(s)).$$

Afirmamos ahora que $\{\phi_1, \ldots, \phi_d\}$ es una base de $Hom_{\mathbb{C}G}\big(\mathbb{C}(G), V\big)$.

Para cualquier $\psi \in Hom_{\mathbb{C}G}\big(\mathbb{C}(G), V\big)$ tenemos que $\psi(1_{\mathbb{C}(G)}) = \sum_{i=1}^{d}\mu_i v_i \in V$ para algunos $\mu_i \in \mathbb{C}$ y por lo tanto, para todo $r \in \mathbb{C}(G)$ tenemos que

$$\begin{aligned}\psi(r) &= \psi(r1_{\mathbb{C}(G)})\\ &= r\psi(1_{\mathbb{C}(G)})\\ &= r\big(\mu_1 v_1 + \cdots + \mu_d v_d\big)\\ &= \mu_1 r v_1 + \cdots + \mu_d r v_d\\ &= \mu_1\phi_1(r) + \cdots + \mu_d\phi_d(r)\\ &= \Big(\sum_{i=1}^{d}\mu_i\phi_i\Big)(r)\end{aligned}$$

es decir, $\psi = \sum_{i=1}^{d}\mu_i\phi_i$, por lo tanto, $\langle\phi_1, \ldots, \phi_d\rangle = Hom_{\mathbb{C}G}\big(\mathbb{C}(G), V\big)$.

Ahora supongamos que para algunos $\lambda_i \in \mathbb{C}$ se tiene que $\sum_{i=1}^{d}\lambda_i\phi_i = 0$, entonces, evaluando en $1_{\mathbb{C}(G)}$ tenemos que

$$\sum_{i=1}^{d}\lambda_i\phi_i(1_{\mathbb{C}(G)}) = \sum_{i=1}^{d}\lambda_i v_i = 0,$$

por lo que necesariamente $\lambda_i = 0$ para todo i pues los vectores v_i son una base de V, y esto significa que $\{\phi_1, \ldots, \phi_d\}$ es linealmente independiente, así concluimos que $\{\phi_1, \ldots, \phi_d\}$ es una base de $Hom_{\mathbb{C}G}\big(\mathbb{C}(G), V\big)$, por lo tanto, $dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(\mathbb{C}(G), V)\big) = d$. ■

Tenemos ahora el resultado principal de esta sección, que nos dirá cuántas veces aparece cada $\mathbb{C}G$-módulo irreducible en la descomposición de $\mathbb{C}(G)$.

Teorema 0.196. *Consideremos el $\mathbb{C}G$-módulo regular $\mathbb{C}(G)$ y supongamos que*

$$\mathbb{C}(G) = U_1 \oplus \cdots \oplus U_r,$$

donde cada U_i es un $\mathbb{C}G$-submódulo irreducible. Si V es cualquier $\mathbb{C}G$-módulo irreducible, entonces el número de $\mathbb{C}G$-módulos U_i tal que $U_i \cong V$ es igual a $dim_{\mathbb{C}}(V)$.

Demostración. Por el teorema 0.195 tenemos que

$$dim_{\mathbb{C}}(V) = dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(\mathbb{C}(G), V)\big),$$

y por el corolario 0.194 éste es igual al número de $\mathbb{C}G$-módulos U_i tal que $U_i \cong V$. ■

Este teorema dice que todo $\mathbb{C}G$-módulo irreducible es factor de composición del álgebra de grupo $\mathbb{C}(G)$ y aparece tantas veces como su dimensión.

Una consecuencia de lo anterior involucra a las dimensiones de todos los $\mathbb{C}G$-módulos irreducibles.

Definición 0.197. *Sean $V_1, \ldots, V_k$ $\mathbb{C}G$-módulos irreducibles. Decimos que $V_1, \ldots, V_k$ forman un* ***conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos*** *si dos a dos no son isomorfos y si todo $\mathbb{C}G$-módulo irreducible V es isomorfo a algún V_i.*

Observación 0.198. El corolario 0.189 establecía que para cualquier grupo finito G existe sólo un número finito de $\mathbb{C}G$-módulos irreducibles no isomorfos, por lo que para todo grupo finito G siempre existe un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos.

Teorema 0.199. *Sean $V_1, \ldots, V_k$ un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos, entonces*

$$\sum_{i=1}^{k} \big(dim_{\mathbb{C}}(V_i)\big)^2 = |G|.$$

Demostración. Sea $\mathbb{C}(G) = U_1 \oplus \cdots \oplus U_r$, una suma directa de $\mathbb{C}G$-submódulos irreducibles. Para $i \in \{1, \ldots, k\}$ denotemos $d_i = dim_{\mathbb{C}}(V_i)$, luego, por el teorema 0.195 para cada i, el número de $\mathbb{C}G$-módulos U_j tales que $U_j \cong V_i$ es igual a d_i y por lo tanto

$$|G| = dim_{\mathbb{C}}\big(\mathbb{C}(G)\big) = \sum_{j=1}^{r} dim_{\mathbb{C}}(U_j) = \sum_{i=1}^{k} d_i(dim_{\mathbb{C}}(V_i)) = \sum_{i=1}^{k} d_i^2.$$

■

Teoría de Caracteres

Seguiremos considerando G un grupo finito y representaciones de G sobre $\mathbb{C}$ ($\mathbb{C}G$-módulos de dimensión finita), también llamadas por algunos autores **representaciones ordinarias** de G.
Recordemos que la traza de una matriz cuadrada $A = (a_{ij})$ de tamaño n con entradas en $\mathbb{C}$ es el escalar resultante de la suma de los elementos de la diagonal, es decir, la función

$$\begin{aligned} tr : M_n(\mathbb{C}) &\longrightarrow \mathbb{C} \\ A &\longmapsto \sum_{i=1}^{n} a_{ii} \ . \end{aligned}$$

Tenemos las siguientes propiedades acerca de la traza.

Proposición 0.200. *Sean A, B y T matrices de $n \times n$, con T invertible, entonces*

1. *$tr(A+B) = tr(A) + tr(B)$,*
2. *$tr(AB) = tr(BA)$,*
3. *$tr(TAT^{-1}) = tr(A)$, es decir, matrices conjugadas tienen la misma traza.*

Demostración. Sean $A = (a_{ij})$ y $B = (b_{ij})$, entonces

1. $tr(A+B) = \sum_{i=1}^{n}(a_{ii} + b_{ii}) = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} b_{ii} = tr(A) + tr(B)$.
2. $tr(AB) = \sum_{i=1}^{n} a_{ij} \sum_{j=1}^{n} b_{ji} = \sum_{j=1}^{n} b_{ji} \sum_{i=1}^{n} a_{ij} = tr(BA)$
3. Sea $B = TAT^{-1}$, entonces tenemos que

$$\begin{aligned} tr(B) &= tr\left(TAT^{-1}\right) \\ &= tr\left((TA)T^{-1}\right) \\ &= tr\left(T^{-1}(TA)\right) \\ &= trA. \end{aligned}$$

■

Notemos que por el contrario, la función traza no es multiplicativa como lo es el determinante.

Caracteres de grupos finitos

Definición 0.201. *Sea $\rho : G \longrightarrow GL_n(\mathbb{C})$ una representación de G sobre $\mathbb{C}$, como $\rho(g)$ es una matriz, considerando su traza podemos definir la función*

$$\begin{array}{rcl} \chi_\rho : G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & tr\left(\rho(g)\right) \end{array}$$

que llamaremos ***el carácter de la representación*** *ρ. Si ρ es de grado n diremos que χ_ρ es un* ***carácter de grado n****. Los caracteres de grado 1 son llamados* ***caracteres lineales***

De forma equivalente, para la representación $\rho : G \longrightarrow GL_n(\mathbb{C})$, consideremos el $\mathbb{C}G$-módulo correspondiente $V = \mathbb{C}^n$ y β la base canónica de $\mathbb{C}^n$, por el teorema 0.125 tenemos que $[g]_\beta = \rho(g)$. Entonces el **carácter de** V es la función

$$\begin{array}{rcl} \chi_V : G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & tr([g]_\beta) \end{array}$$

Observación 0.202. El carácter de V no depende de la base β ya que si γ es otra base de V entonces $[g]_\gamma = T\,[g]_\beta\,T^{-1}$ donde T es la matriz de cambio de coordenadas de β a γ, por el teorema 0.168 y por la proposición 0.200 inciso 3) tenemos que

$$tr\,[g]_\gamma = tr\,[g]_\beta\,.$$

La palabra *carácter* surge de que para una representación ρ, su carácter χ_ρ la caracteriza en el sentido de que si hay otra representación con el mismo carácter entonces deben ser equivalentes, como veremos más adelante.

Definición 0.203. *Decimos que χ es* ***un carácter*** *de G si χ es el carácter de algún $\mathbb{C}G$-módulo, le llamaremos a χ* ***un carácter irreducible*** *de G si es el carácter de algún $\mathbb{C}G$-módulo irreducible, o bien, χ es* ***un carácter reducible*** *de G si es el carácter de algún $\mathbb{C}G$-módulo reducible.*

Ejemplo 0.204. El carácter trivial (o principal) de G es el carácter del $\mathbb{C}G$-módulo trivial y es un carácter lineal de G. Así, dado un grupo G conocemos siempre al menos un carácter irreducible de G, el carácter trivial. Hallar todos los caracteres irreducibles de un grupo generalmente es complicado.

Ejemplo 0.205. Caracteres lineales corresponden a morfismos.
Todo carácter lineal de un grupo G es un morfismo de grupos $G \longrightarrow \mathbb{C}^*$, de hecho, éstos son los únicos caracteres de G que son morfismos de grupos.
Más claramente, si χ_V es un carácter lineal de G (el carácter de una representación ρ de dimensión 1), entonces para todo $g \in G$

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL_1(\mathbb{C}) \cong \mathbb{C}^* \\ g & \longmapsto & \lambda_g \end{array}$$

y así $gv = \lambda_g v$ para todo $v \in V$ y $\chi_V(g) := tr\left(\rho(g)\right) = \lambda_g$. Como

$$(gg')v = g(g')v = g(\lambda_{g'}v) = \lambda_g\lambda_{g'}v$$

entonces $\lambda_{gg'} = \lambda_g \lambda_{g'}$, es decir, $\chi_V(gg') = \chi_V(g)\chi_V(g')$ que significa que χ_V es un morfismo de grupos de G en $\mathbb{C}^*$.
Recíprocamente, todo morfismo de grupos $\phi : G \longrightarrow \mathbb{C}^* \cong GL_1(\mathbb{C})$ es una representación de grado 1 por definición, así tiene asociado un carácter lineal que podemos tomar $\chi_V = \phi$. Entonces existe una correspondecia biyectiva entre caracteres lineales de G y morfismos de grupos de G en $\mathbb{C}^*$.

Ahora vamos a ver que el carácter es invariante en clases de isomorfismo de $\mathbb{C}G$-módulos, es decir,

Proposición 0.206. *Sean V y U $\mathbb{C}G$-módulos. Si $V \cong U$ entonces tienen el mismo carácter.*

Demostración. Supongamos que V y U son $\mathbb{C}G$-módulos isomorfos, entonces, por el lema 0.169 existen bases β_V y β_U de V y U respectivamente tales que

$$[g]_{\beta_V} = [g]_{\beta_U} \text{ para todo } g \in G.$$

Y por lo tanto $tr\,[g]_{\beta_V} = tr\,[g]_{\beta_U}$ para todo $g \in G$, es decir, V y U tiene el mismo carácter. ■

La versión para representaciones de este teorema dice que dos representaciones equivalentes tienen el mismo carácter.
Veremos ahora cómo se comportan los caracteres al evaluarlos en elementos de una misma clase de conjugación.

Proposición 0.207. *Los valores de los caracteres son constantes en clases de conjugación de G.*

Demostración. Supongamos que x y y son conjugados en G, entonces $y = gxg^{-1}$ para algún $g \in G$. Luego, si V es un $\mathbb{C}G$-módulo y β es una base de V entonces

$$[y]_\beta = \left[gxg^{-1}\right]_\beta = [g]_\beta\,[x]_\beta\,[g]_\beta^{-1}$$

y por la proposición 0.200 inciso 3) tenemos que $tr\,[y]_\beta = tr\,[x]_\beta$, es decir, si χ es el carácter de V entonces $\chi(y) = \chi(x)$. ■

Seguimos con algunos resultados sobre los valores de caracteres, pero primero necesitamos el siguiente lema, que habla sobre la diagonalizabilidad de los operadores dados por una representación.

Lema 0.208. *Sea G un grupo finito y V un $\mathbb{C}G$-módulo. Entonces para todo $g \in G$, el operador $\rho(g)$ es diagonalizable, es decir, existe una base β de V tal que la matriz $[g]_\beta$ es diagonal. Si g tiene orden m entonces las entradas en la diagonal de $[g]_\beta$ son raíces m-ésimas de la unidad.*

Demostración. Consideremos $H = \langle g \rangle$ el subgrupo cíclico de orden m generado por g, luego $\rho_H := \rho|_H$ es una representación de H, es decir, con la restricción de ρ a H tenemos que V es un $\mathbb{C}H$-módulo, luego, por el Teorema de Maschke V tiene una descomposición en $\mathbb{C}H$-submódulos irreducibles $V = U_1 \oplus \cdots \oplus U_r$ y como H es abeliano, por el teorema 0.183 estos irreducibles tienen dimensión 1, es decir, $U_i = \langle u_i \rangle$, para algún $u_i \in V$, por lo tanto $r = dim_{\mathbb{C}}(V)$.
Ahora, si $\rho_i : H \longrightarrow GL(U_i) \cong GL_1(\mathbb{C}) \cong \mathbb{C}^*$ es la representación correspondiente a cada U_i entonces

$$\rho_i(g)^m = \rho_i(g^m) = \rho_i(e) = 1_{\mathbb{C}}$$

y esto quiere decir que $\rho_i(g)$ es raíz m-ésima de la unidad, digamos $\rho_i(g) = \omega^{\alpha_i}$ con $\omega = e^{\frac{2\pi i}{m}}$ una raíz m-ésima primitiva de la unidad, por lo tanto, para todo i existen enteros α_i tales que

$$gu_i = \rho_i(g)u_i = \omega^{\alpha_i}u_i$$

por lo que, para la base $\beta = \{u_1, \ldots, u_r\}$ de V, la matriz asociada a $\rho(g)$ es suma directa de las matrices asociadas a cada $\rho_i(g)$, así

$$[\rho(g)]_\beta = \begin{pmatrix} [\rho_1(g)]_\beta & 0 & \cdots & 0 \\ 0 & [\rho_2(g)]_\beta & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & [\rho_r(g)]_\beta \end{pmatrix} = \begin{pmatrix} \omega^{\alpha_1} & 0 & \cdots & 0 \\ 0 & \omega^{\alpha_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{\alpha_r} \end{pmatrix}$$

que es una matriz diagonal y por lo tanto $\rho(g)$ es diagonalizable. Aquí los valores propios de $\rho(g)$ son precisamente raíces m-ésimas de la unidad (potencias de ω).

Otra forma de demostrarlo es notando que si $g \in G$ es de orden m entonces $g^m = e$, por lo que $\rho(g)^m = \rho(g^m) = I_V$, entonces $\rho(g)$ es cero del polinomio $x^m - 1$, que se descompone en distintos factores lineales en $\mathbb{C}[x]$, sus ceros son raíces m-ésimas de la unidad y así, el polinomio mínimo del operador $\rho(g)$ también se descompone en distintos factores lineales en $\mathbb{C}[x]$ y esto sucede si y sólo si $\rho(g)$ es diagonalizable. ■

Como consecuencia del lema anterior tenemos lo siguiente.

Teorema 0.209. *Sea V un $\mathbb{C}G$-módulo, χ su carácter y $g \in G$ un elemento de orden m, entonces*

(i) $\chi(e) = dim_{\mathbb{C}}(V)$.

(ii) $\chi(g)$ *es una suma (con multiplicidad) de raíces m-ésimas de la unidad (los valores propios del operador $\rho(g)$). Más aún, $\chi(g)$ es una suma de $\chi(e) = n = dim_{\mathbb{C}}(V)$ raíces m-ésimas de la unidad.*

(iii) $\chi(g^{-1}) = \overline{\chi(g)}$.

(iv) $\chi(g) \in \mathbb{R}$ *si g es conjugado de g^{-1}.*

Demostración. Sea $n = dim_{\mathbb{C}}(V)$ y β una base de V, entonces
(i) Tenemos que $[e]_\beta = I_n$, por lo tanto $\chi(e) = tr\,[e]_\beta = tr(I_n) = n$.
(ii) Por el lema 0.208, existe una base β de V tal que

$$[g]_\beta = \begin{pmatrix} \omega_1 & 0 & \cdots & 0 \\ 0 & \omega_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_n \end{pmatrix}$$

donde cada ω_i es una raíz m-ésima de la unidad, así,

$$\chi(g) = \omega_1 + \cdots + \omega_n.$$

(iii) Notemos que el operador $\rho(g^{-1})$ tiene, con respecto a la base β del inciso anterior, la matriz asociada

$$\left[g^{-1}\right]_\beta = \begin{pmatrix} \omega_1^{-1} & 0 & \cdots & 0 \\ 0 & \omega_2^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_n^{-1} \end{pmatrix}$$

es decir, sus valores propios son los inversos de los valores propios de $\rho(g)$ y como éstos son complejos de norma 1, el inverso coincide con el conjugado, es decir, ${\omega_i}^{-1} = \overline{\omega_i}$ y por lo tanto

$$\chi(g^{-1}) = \sum_{i=1}^{n} \overline{\omega_i} = \overline{\sum_{i} \omega_i} = \overline{\chi(g)}$$

(iv) Si g es conjugado de g^{-1} entonces $\chi(g) = \chi(g^{-1})$ por la proposición 0.207, así, $\chi(g) = \overline{\chi(g)}$ y entonces $\chi(g) \in \mathbb{R}$.

■

Seguimos con un resultado que nos va a permitir conocer el núcleo de una representación si conocemos su carácter.

Teorema 0.210. *Sea $\rho : G \longrightarrow GL_n(\mathbb{C})$ una representación de G, y χ el carácter de ρ, entonces*

i) Para $g \in G$, $|\chi(g)| = \chi(e)$ si y sólo si $\rho(g) = \lambda I_n$ para algún $\lambda \in \mathbb{C}$.

ii) $Ker(\rho) = \{g \in G \mid \chi(g) = \chi(e) = n\}$

Demostración. $i)$ Sea $g \in G$ de orden m y supongamos que $\rho(g) = \lambda I_n$ con $\lambda \in \mathbb{C}$, y así $\chi(g) = n\lambda$. Además λ es una raíz m-ésima de la unidad, y por lo tanto $|\chi(g)| = n = \chi(e)$.
Supongamos que $|\chi(g)| = \chi(e)$. Ahora, por el lema 0.208 existe una base β de $\mathbb{C}^n$ tal que

$$[g]_\beta = \begin{pmatrix} \omega_1 & 0 & \cdots & 0 \\ 0 & \omega_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_n \end{pmatrix}$$

donde cada ω_i es una raíz m-ésima de la unidad, y entonces $|\chi(g)| = |\omega_1 + \cdots + \omega_n| = \chi(e) = n$.
Recordemos que para cualesquiera números complejos $z_1, \ldots, z_n$, es válida la desigualdad del triángulo, es decir,

$$|z_1 + \ldots + z_n| \leq |z_1| + \cdots + |z_n|$$

que es una igualdad si y sólo si los argumentos de $z_1, \ldots, z_n$ son todos iguales.
Ya que $|\omega_i| = 1$ para todo i, de la igualdad anterior y de la desigualdad del triángulo deducimos que $\omega_i = \omega_j$ para todo i, j. Por lo tanto

$$[g]_\beta = \begin{pmatrix} \omega_1 & 0 & \cdots & 0 \\ 0 & \omega_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_1 \end{pmatrix} = \omega_1 I_n.$$

Por lo que para todas las bases γ de $\mathbb{C}^n$ tenemos que $[g]_\gamma = \omega_1 I_n$ y así $\rho(g) = \omega_1 I_n$ para alguna raíz m-ésima de la unidad.
$ii)$ Si $g \in Ker(\rho)$ entonces $\rho(g) = I_n$ por lo que $\chi(g) = n = \chi(e)$.
Ahora supongamos que $\chi(g) = n = \chi(e)$, entonces por $i)$ tenemos que $\rho(g) = \lambda I_n$ algún $\lambda \in \mathbb{C}$. Esto implica que $\chi(g) = tr\rho(g) = \lambda n = \lambda\chi(e)$ por lo que necesariamente $\lambda = 1$ y por lo tanto $\rho(g) = I_n$, es decir, $g \in Ker(\rho)$. ■

En términos del teorema anterior vamos a definir el núcleo de un carácter de la siguiente manera.

Definición 0.211. *Si χ es un carácter de un grupo G, entonces el **núcleo** de χ es el conjunto*

$$Ker(\chi) = \{g \in G \mid \chi(g) = \chi(e)\}.$$

*Por el teorema 0.210, si ρ es una representación de G con carácter χ, entonces $Ker(\rho) = Ker(\chi)$ por lo que $Ker(\chi) \trianglelefteq G$. Diremos que χ es **fiel** si $Ker(\chi) = \{e_G\}$, es decir, si ρ es fiel.*

Proposición 0.212. *Sea $\chi : G \longrightarrow \mathbb{C}^*$ un carácter de G. Entonces la función*

$$\begin{array}{rcl} \overline{\chi} : G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & \overline{\chi(g)} \end{array}$$

es un carácter de G. Más aún, si χ es irreducible entonces $\overline{\chi}$ también es irreducible.

Demostración. Sea χ el carácter de una representación $\rho : G \longrightarrow GL_n(\mathbb{C})$, entonces, para $g \in G$ se tiene que $\chi(g) = tr(\rho(g))$, luego, si $A = (a_{ij}) \in M_{n\times n}(\mathbb{C})$, definamos su matriz conjugada claramente como $\overline{A} = (\overline{a_{ij}})$. Ahora notemos que si $A = (a_{ij}), B = (b_{ij}) \in M_{n\times n}(\mathbb{C})$ entonces $\overline{AB} = \overline{A}\ \overline{B}$, pues la entrada ij de $\overline{A}\ \overline{B}$ es $\sum_{k=1}^{n} \overline{a_{ik}}\overline{b_{kj}}$ que es el complejo conjugado de $\sum_{k=1}^{n} a_{ik}b_{kj}$, la entrada ij de AB. Y por lo tanto la función

$$\begin{array}{rcl} \overline{\rho} : G & \longrightarrow & GL_n(\mathbb{C}) \\ g & \longrightarrow & \overline{\rho}(g) := \overline{\rho(g)} \end{array}$$

es una representación de G. Y ya que

$$tr(\overline{\rho}(g)) := tr(\overline{\rho(g)}) = \overline{tr(\rho(g))} = \overline{\chi(g)}$$

el carácter de la representación $\overline{\rho}$ es $\overline{\chi}$. Luego, si ρ es reducible entonces $\overline{\rho}$ es reducible por la observación 0.172. Por lo tanto χ es irreducible si sólo si $\overline{\chi}$ es irreducible. ■

Definición 0.213. *Dado un carácter $\chi : G \longrightarrow \mathbb{C}^*$, el **carácter conjugado** de χ es la función*

$$\begin{array}{rcl} \overline{\chi} : G & \longrightarrow & \mathbb{C}^* \\ g & \longmapsto & \overline{\chi(g)} \end{array}$$

de la proposición anterior, es decir, los valores del carácter conjugado son los complejos conjugados de los valores de χ.

Ejemplo 0.214. El carácter regular de un grupo finito G de orden n es el carácter asociado a la representación regular de G estudiada en el ejemplo 0.146, ésta es el álgebra de grupo $\mathbb{C}(G)$ como espacio vectorial sobre $\mathbb{C}$, es decir tenemos que la función

$$\begin{array}{rcl} \diamond\ :\ G \times \mathbb{C}(G) & \longrightarrow & \mathbb{C}(G) \\ \left(x, \sum_{g\in G} a_g g\right) & \longmapsto & \sum_{g\in G} a_g(xg) \end{array}$$

es una acción lineal con la cual $\mathbb{C}(G)$ es un $\mathbb{C}G$-módulo y la representación de G de grado n inducida por la acción anterior es la función

$$\begin{array}{rcl} \rho_{reg} : G & \longrightarrow & GL\big(\mathbb{C}(G)\big) \\ x & \longmapsto & \rho_{reg}(x) \end{array} \quad \text{donde} \quad \begin{array}{rcl} \rho_{reg}(x) : \mathbb{C}(G) & \longrightarrow & \mathbb{C}(G) \\ \sum_{g\in G} a_g g & \longmapsto & \sum_{g\in G} a_g(xg)\ . \end{array}$$

Denotaremos al carácter regular de un grupo finito G como χ_{reg}.

Lema 0.215. *Para cualesquiera $\mathbb{C}G$-módulos U y V el valor del carácter de su suma directa es igual la suma de los valores de los carácteres de U y V, es decir,*

$$\chi_{U\oplus V} = \chi_U + \chi_V$$

Demostración. Sea $\beta = \{u_1, \ldots, u_n, v_1, \ldots, v_m\}$ una base de $U \oplus V$, con, $\beta_U = \{u_1, \ldots, u_n\}$ una base de $U \oplus 0$, y $\beta_V = \{v_1, \ldots, v_m\}$ una base de $0 \oplus V$, entonces

$$[g]_\beta = \begin{pmatrix} [g]_{\beta_U} & 0 \\ 0 & [g]_{\beta_V} \end{pmatrix}$$

así tenemos que para todo $g \in G$

$$\chi_{U\oplus V}(g) = tr([g]_\beta) = tr([g]_{\beta_U}) + tr([g]_{\beta_V}) = \chi_U(g) + \chi_V(g).$$

■

Vamos a ver ahora que a partir de los caracteres irreducibles de un grupo G se puede determinar el carácter del álgebra de grupo de G sobre $\mathbb{C}$. Necesitamos antes el siguiente

Lema 0.216. *Sea V un $\mathbb{C}G$-módulo y supongamos que*

$$V = U_1 \oplus \cdots \oplus U_r,$$

es una suma directa de $\mathbb{C}G$-módulos irreducibles U_i. Entonces el carácter de V es la suma de los caracteres de $\mathbb{C}G$-módulos $U_1, \ldots, U_r$.

Demostración. Es inmediata por el ejemplo 0.156 y la definición de carácter. ■

Teorema 0.217. *Sean $V_1, \ldots, V_k$ un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos. Para cada $1 \leqslant i \leqslant k$ sea χ_i el carácter de V_i y $d_i = dim_{\mathbb{C}}(V_i) = \chi_i(e_G)$, entonces*

$$\chi_{reg} = d_1\chi_1 + \cdots + d_k\chi_k$$

Demostración. Por el teorema 0.196 tenemos que

$$\mathbb{C}G \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

donde cada V_i aparece sumado consigo mismo tantas veces como su dimensión d_i, luego el resultado se sigue por el lema 0.216. ■

Ahora vamos a describir los valores del carácter regular, tenemos el siguiente

Teorema 0.218. *Si χ_{reg} es el carácter regular de un grupo finito G entonces*

$$\chi_{reg}(e_G) = |G| \quad y$$
$$\chi_{reg}(g) = 0 \text{ si } g \neq e_G.$$

Demostración. Sean $g_1, \ldots, g_n$ los elementos de G y sea β la base $\{g_1, \ldots, g_n\}$ de $\mathbb{C}(G)$, por el teorema 0.209 inciso i) tenemos que $\chi_{reg}(e_G) = dim_{\mathbb{C}}(\mathbb{C}(G)) = |G|$.
Ahora, si $e_G \neq g \in G$ entonces para todo $1 \leqslant i \leqslant n$ tenemos que $gg_i = g_j$ para algún j y $j \neq i$. Entonces la i-ésima columna de la matriz $[g]_\beta$ tiene ceros en todos lados salvo en el lugar del renglón j, en particular la entrada ii de $[g]_\beta$ es cero para todo i. Por lo tanto $\chi_{reg}(g) = tr\,[g]_\beta = 0$. ■

Producto interno de caracteres

Notemos que los caracteres de un grupo finito G son ciertas funciones $\chi : G \longrightarrow \mathbb{C}$. El conjunto

$$\mathbb{C}^G = \{\phi : G \longrightarrow \mathbb{C} \mid \phi \text{ es función } \}$$

(todas las funciones de G a $\mathbb{C}$) está equipado con una estructura de $\mathbb{C}$-espacio vectorial con las operaciones puntuales, es decir, si $\phi, \psi : G \longrightarrow \mathbb{C}$ son funciones y $\lambda \in \mathbb{C}$ entonces la suma y el producto por escalar son:

$$\begin{array}{rcl} \phi+\psi : G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \phi(g)+\psi(g) \end{array} \quad \text{y} \quad \begin{array}{rcl} \lambda\phi : G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \lambda\phi(g). \end{array}$$

Luego, en este espacio de funciones también podemos definir el producto puntual de funciones

$$\begin{array}{rcl} \phi\psi : G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \phi(g)\psi(g) \end{array}$$

y con este producto $\mathbb{C}^G$ es un anillo conmutativo con 1, y tiene divisores de cero. Las unidades de este anillo son las funciones que no se anulan nunca, es decir

$$\mathcal{U}(\mathbb{C}^G) = \{\phi : G \longrightarrow \mathbb{C} \mid \phi(g) \neq 0 \ \forall \ g \in G\}$$

Este producto puntual de funciones vuelve a $\mathbb{C}^G$ un $\mathbb{C}$-álgebra.

Observación 0.219. Notemos que la suma, el producto, y el producto por escalar no necesariamente son caracteres cuando las funciones involucradas en las operaciones son caracteres pero después veremos cuándo lo son.

Luego, podemos definir un producto interno definido positivo el espacio vectorial $\mathbb{C}^G$ de la siguiente manera.

Definición 0.220. *Si $\phi, \psi : G \longrightarrow \mathbb{C}$ son funciones entonces existe en $\mathbb{C}^G$ un* ***producto interno***

$$\begin{array}{rcl} \langle\ ,\ \rangle : \mathbb{C}^G \times \mathbb{C}^G & \longrightarrow & \mathbb{C} \\ (\phi, \psi) & \longmapsto & \langle \phi, \psi \rangle := \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \phi(g)\overline{\psi(g)}. \end{array}$$

Claramente esta definición satisface los axiomas de un producto interno, es decir, para todos $\phi, \phi_1, \phi_2, \psi, \psi_1, \psi_2 \in \mathbb{C}^G$ y $\lambda \in \mathbb{C}$ tenemos que

(a) $\langle \phi, \phi \rangle \geq 0$ y $\langle \phi, \phi \rangle = 0$ si y sólo si $\phi = 0$.

(b) $\langle \phi, \psi \rangle = \overline{\langle \psi, \phi \rangle}$.

(c) $\langle \lambda\phi, \psi \rangle = \lambda \langle \phi, \psi \rangle$

(d) $\langle \phi_1 + \phi_2, \psi \rangle = \langle \phi_1, \psi \rangle + \langle \phi_2, \psi \rangle$.

Las siguientes propiedades son consecuencia de las primeras

(e) $\langle \phi, \lambda\psi \rangle = \overline{\lambda} \langle \phi, \psi \rangle$

(f) $\langle \phi, \psi_1 + \psi_2 \rangle = \langle \phi, \psi_1 \ \rangle + \langle \phi, \psi_2 \rangle$.

Observación 0.221. Notemos que si ${x_1}^G, \ldots, {x_l}^G$ son las distintas clases de conjugación de G y denotamos ${x_i}^G = C_i$ para todo i, entonces, por el Teorema Órbita-Estabilizador tenemos que el producto interno se puede escribir como

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)} = \frac{1}{|G|} \sum_{i=1}^{l} \#C_i \ \phi(x_i)\overline{\psi(x_i)} = \sum_{i=1}^{l} \frac{\phi(x_i)\overline{\psi(x_i)}}{|C_G(x_i)|}.$$

En lo que sigue vamos a desarrollar el resultado más importante sobre el producto interno: los caracteres irreducibles de un grupo finito G forman un conjunto ortonormal del espacio $\mathbb{C}^G$. La demostración es algo técnica y requiere de varios resultados previos que se desarrollarán bajo la siguiente hipótesis temporal: escribir como suma directa de dos $\mathbb{C}G$-submódulos a $\mathbb{C}(G)$ donde los sumandos no tiene factores de composición comunes.

Hipótesis 0.222. Sea $\mathbb{C}(G) = U_1 \oplus U_2$, donde U_1 y U_2 son $\mathbb{C}(G)$-submódulos que no tienen factores de composición comunes. Escribamos $1_{\mathbb{C}G} = e_1 + e_2$, donde $e_1 \in U_1$ y $e_2 \in U_2$.

Proposición 0.223. *Para todos $u_1 \in U_1$ y $u_2 \in U_2$ tenemos que*

$$e_1 u_1 = u_1, \ e_1 u_2 = 0$$
$$e_2 u_1 = 0, \ e_2 u_2 = u_2.$$

Demostración. Si $u_1 \in U_1$ entonces la función

$$\begin{aligned} f : U_2 &\longrightarrow U_1 \\ u_2 &\longmapsto u_2 u_1 \end{aligned}$$

es un morfismo de $\mathbb{C}G$-módulos, pero por hipótesis U_1 y U_2 no tienen factores de composición comunes, así, por el teorema 0.192 todo morfismo de $\mathbb{C}G$-módulos de U_2 y U_1 es cero, por lo tanto $u_2 u_1 = 0$ para todos $u_1 \in U_1$, $u_2 \in U_2$. Análogamente, tenemos que $u_1 u_2 = 0$ para todos $u_1 \in U_1$, $u_2 \in U_2$. En particular $e_2 u_1 = e_1 u_2 = 0$. Luego,

$$u_1 = 1_{\mathbb{C}(G)} u_1 = (e_1 + e_2)u_1 = (e_1 u_1 + e_2)u_1 = e_1 u_1, \text{ y}$$
$$u_2 = 1_{\mathbb{C}(G)} u_2 = (e_1 + e_2)u_2 = (e_1 u_2 + e_2)u_2 = e_2 u_2.$$

■

Observación 0.224. En particular si en la proposición anterior $u_1 = e_1$ y $u_2 = e_2$ entonces

$${e_1}^2 = e_1, \ {e_2}^2 = e_2 \text{ y } e_1 e_2 = e_2 e_1 = 0$$

Proposición 0.225. *Sea χ_1 el carácter del $\mathbb{C}G$-módulo U_1 de la hipótesis 0.222. Entonces*

$$e_1 = \frac{1}{|G|} \sum_{g \in G} \chi_1(g^{-1}) g.$$

Demostración. Sean χ y χ_2 los caracteres de $\mathbb{C}(G)$ y W_2 respectivamente, y ya que $e_1 \in \mathbb{C}(G)$, entonces para algunos $\lambda_g \in \mathbb{C}$ tenemos que

$$e_1 = \sum_{g \in G} \lambda_g g.$$

Vamos a calcular los coeficientes λ_g en términos del carácter χ_1. Sea $x \in G$, entonces la función

$$\begin{aligned} T : \mathbb{C}(G) &\longrightarrow \mathbb{C}(G) \\ w &\longmapsto x^{-1} e_1 w \end{aligned}$$

es un endomorfismo de $\mathbb{C}(G)$. Vamos a calcular la traza de T de dos formas (la traza de un operador es la traza de cualquier matriz asociada al operador en alguna base).
Primero, para $u_1 \in U_1,\ u_2 \in U_2$, por la proposición 0.223 tenemos que

$$T(u_1) = x^{-1}e_1u_1 = x^{-1}u_1 \ \text{ y } \ T(u_2) = x^{-1}e_1u_2 = 0.$$

Por lo tanto,

$$\begin{array}{rcl} T|_{U_1} : U_1 & \longrightarrow & \mathbb{C}(G) \\ u_1 & \longmapsto & x^{-1}u_1 \end{array} \quad \text{y} \quad \begin{array}{rcl} T|_{U_1} : U_2 & \longrightarrow & \mathbb{C}(G) \\ u_2 & \longmapsto & 0\ , \end{array}$$

y así, $T|_{U_1} := T_1$ y $T|_{U_2} := T_2$ son endomorfismos de U_1 y U_2 respectivamente, luego, ya que χ_1 es el carácter de U_1 entonces $tr(T_1) = \chi_1(x^{-1})$ y $tr(T_2) = 0$, por lo tanto el valor de $\chi(x^{-1}e_1)$ es

$$\chi(x^{-1}e_1) = tr(T) = tr(T_1) + tr(T_2) = \chi_1(x^{-1}) + \chi_2(0) = \chi_1(x^{-1}).$$

Luego, por el teorema 0.218, el endomorfismo

$$\begin{array}{rcl} S_{x,g} : \mathbb{C}(G) & \longrightarrow & \mathbb{C}(G) \\ w & \longmapsto & x^{-1}gw \end{array}$$

tiene traza cero si $g \neq x$ y tiene traza $|G|$ si $g = x$, por lo tanto, ya que

$$T(w) = x^{-1}\sum_{g\in G}\lambda_g gw = \sum_{g\in G}\lambda_g x^{-1}gw$$

tenemos que

$$tr(T) = \sum_{g\in G}\lambda_g tr(S_{x,g}) = \lambda_x tr(S_{x,x}) = \lambda_x|G|.$$

Así $tr(T) = \lambda_x|G|$. Igualando las dos expresiones para la traza, tenemos que para todo $x \in G$

$$\lambda_x = \frac{\chi_1(x^{-1})}{|G|}.$$

Por lo tanto

$$e_1 = \sum_{g\in G}\frac{\chi_1(g^{-1})}{|G|}g = \frac{1}{|G|}\sum_{g\in G}\chi_1(g^{-1})g.$$

■

Corolario 0.226. *Sea χ_1 el carácter de U_1 en la hipótesis 0.222. Entonces*

$$\langle \chi_1, \chi_1 \rangle = \chi_1(e_G).$$

Demostración. Por la definición de producto en $\mathbb{C}(G)$ y por la proposición 0.225 tenemos que

$${e_1}^2 = \left(\frac{1}{|G|}\sum_{g\in G}\chi_1(g^{-1})g\right)\left(\frac{1}{|G|}\sum_{g^{-1}\in G}\chi_1(g)g^{-1}\right),$$

y en esta expresión, el coeficiente de e_G es

$$\frac{1}{|G|^2}\sum_{g\in G}\chi_1(g^{-1})\chi_1(g) = \frac{1}{|G|}\langle \chi_1, \chi_1 \rangle.$$

Por otro lado, de la proposición 0.225, el coeficiente de e_G en e_1 es $\dfrac{\chi_1(e_G)}{|G|}$, y por la observación 0.224 teníamos que ${e_1}^2 = e_1$, entonces $\langle \chi_1, \chi_1 \rangle = \chi_1(e_G)$. ■

Podemos ahora enunciar y demostrar nuestro resultado principal:

Teorema 0.227. *Si V y U son $\mathbb{C}G$-módulos irreducibles no isomorfos con caracteres χ y ψ respectivamente, entonces*

$$\langle \chi, \chi \rangle = 1, \quad y$$
$$\langle \chi, \psi \rangle = 0$$

Demostración. Recordemos que por el teorema 0.196

$$\mathbb{C}(G) = U_1 \oplus \cdots \oplus U_r,$$

donde cada U_i es un $\mathbb{C}G$-submódulo irreducible y el número de $\mathbb{C}G$-módulos U_i tal que $U_i \cong V$ es igual a $dim_{\mathbb{C}}(V)$. Si $m = dim_{\mathbb{C}}(V)$, definamos

$$W = U_1 \oplus \cdots \oplus U_m,$$

donde $U_i \cong V$ para todo $1 \leqslant i \leqslant m$ y sea X la suma del resto de los U_i que no son isomorfos a V. Entonces

$$\mathbb{C}(G) = W \oplus X.$$

Así, todo factor de composición de W es isomorfo a V y ningún factor de composición de X es isomorfo a V, en particular W y X no tienen factores de composición comunes.
Luego, el carácter de W es $m\chi$ ya que W es suma directa de m $\mathbb{C}G$-submódulos, cada uno con carácter χ, Aplicando el corolario anterior a $m\chi$ tenemos que

$$\langle m\chi, m\chi \rangle = m\chi(e_G).$$

Ya que $\chi(e_G) = dim_{\mathbb{C}}(V) = m$, entonces $\langle \chi, \chi \rangle = 1$.
Ahora, sea Y la suma de los $\mathbb{C}G$-submódulos U_i donde cada U_i es isomorfo a V o es isomorfo a U y Z la suma de los $\mathbb{C}G$-submódulos U_i restantes, es decir, donde cada U_i no es isomorfo a V y no es isomorfo a U. Entonces

$$\mathbb{C}(G) = Y \oplus Z.$$

y Y y Z no tienen factores de composición comunes. Luego, el carácter de Y es $m\chi + n\psi$, donde $n = dim_{\mathbb{C}}(U)$. Por el corolario anterior tenemos que

$$\begin{aligned}(m\chi + n\psi)(e_G) &= m\chi(e_G) + n\psi(e_G) \\ &= \langle m\chi + n\psi, m\chi + n\psi \rangle \\ &= m^2\langle \chi, \chi \rangle + n^2\langle \psi, \psi \rangle + mn\left(\langle \chi, \psi \rangle + \langle \psi, \chi \rangle\right).\end{aligned}$$

Ahora, habíamos visto antes que $\langle \chi, \chi \rangle = 1$, de manera análoga, $\langle \psi, \psi \rangle = 1$, y también $\chi(e_G) = m$ y $\psi(e_G) = n$. Por lo tanto

$$\langle \chi, \psi \rangle + \langle \psi, \chi \rangle = 0.$$

Por último, notemos que

$$\langle \chi, \psi \rangle = \frac{1}{|G|}\sum_{g \in G} \chi(g)\overline{\psi(g)} = \frac{1}{|G|}\sum_{g \in G} \chi(g)\psi(g^{-1}).$$

Pero el conjunto $\{g^{-1} \mid g \in G\} = G$, por lo que

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})\psi(g) = \frac{1}{|G|} \sum_{g \in G} \psi(g)\chi(g^{-1}) = \langle \psi, \chi \rangle.$$

Por lo tanto, $\langle \chi, \psi \rangle = 0$. ■

Como consecuencia del teorema anterior, tenemos que

Teorema 0.228. *Si G es un grupo finito y $V_1, \ldots, V_k$ es un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos con caracteres $\chi_1, \ldots, \chi_r$, entonces para cada i, j*

$$\delta_{ij} = \langle \chi_i, \chi_j \rangle$$

Observación 0.229. El teorema anterior implica que los caracteres irreducibles $\chi_1, \ldots, \chi_r$ son todos distintos.

Teorema 0.230. *Sean $\chi_1, \ldots, \chi_k$ los distintos caracteres irreducibles de G. Entonces cualquier carácter ψ de G se puede escribir como*

$$\psi = d_1\chi_1 + \cdots + d_k\chi_k$$

para algunos enteros no negativos $d_1, \ldots, d_k$. Más aún,

$$\langle \psi, \chi_i \rangle = d_i \text{ para todo } i, \quad y \quad \langle \psi, \ \psi \rangle = \sum_{i=1}^{k} {d_i}^2.$$

Demostración. Para G un grupo finito, vimos en el teorema 0.176 que todo $\mathbb{C}G$-módulo V es completamente reducible, es decir, es suma directa de $\mathbb{C}G$-submódulos irreducibles, luego, si $V_1, \ldots, V_k$ es un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos con caracteres $\chi_1, \ldots, \chi_k$ entonces cada sumando es isomorfo a algún V_i y existen enteros no negativos $d_1, \ldots, d_k$ tales que

$$V \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

donde para cada i, hay d_i factores V_i. Por lo tanto, el carácter χ de V está dado por

$$\psi = d_1\chi_1 + \cdots + d_k\chi_k.$$

Luego, notemos que para todo $1 \leqslant i \leqslant k$, por el teorema 0.228 tenemos que

$$\langle \psi, \chi_i \rangle = \langle \chi_i, \psi \rangle = d_i, \text{ y}$$
$$\langle \psi, \psi \rangle = {d_1}^2 + \cdots + {d_k}^2.$$

■

Definición 0.231. *Sea ψ cualquier carácter de G y χ un carácter irreducible de G. Decimos que χ es un **constituyente** de ψ si $\langle \psi, \chi \rangle \neq 0$. Entonces, los **constituyentes** de ψ son los caracteres irreducibles de G para los cuales el entero d_i en la expresión $\psi = d_1\chi_1 + \cdots + d_r\chi_k$ es distinto de cero* 0 .

Otra consecuencia importante del teorema 0.228 es un resultado que permitirá determinar cuándo un $\mathbb{C}G$-módulo es irreducible o no.

Teorema 0.232. *Sea V un $\mathbb{C}G$-módulo con carácter χ. Entonces*

V *es irreducible si y sólo si* $\langle \chi, \chi \rangle = 1$

Demostración. Si V es irreducible, entonces, por el teorema 0.227, tenemos que $\langle \chi, \chi \rangle = 1$.
Supongamos ahora que $\langle \chi, \chi \rangle = 1$. Sabemos que $\psi = d_1\chi_1 + \cdots + d_r\chi_k$ para algunos enteros no negativos $d_1, \ldots, d_i$, y por el teorema anterior

$$1 = \langle \chi, \chi \rangle = \sum_{i=1}^{k} {d_i}^2,$$

por lo que uno de los d_i debe ser igual a 1 y los otros iguales a cero, así, $V \cong V_i$ y por lo tanto V es irreducible. ■

Podemos ahora demostrar otro hecho importante: todo $\mathbb{C}G$-módulo está determinado por su carácter. Este resultado es importante porque significa que podemos responder preguntas acerca de $\mathbb{C}G$-módulos usando teoría de caracteres.

Teorema 0.233. *Sean* V *y* U *dos* $\mathbb{C}G$*-módulos con caracteres* χ *y* ψ *respectivamente. Entonces*

$$V \cong U \text{ si y sólo si } \chi = \psi$$

Demostración. En la proposición 0.206 vimos que si $V \cong U$ entonces $\chi = \psi$.
Ahora supongamos que $\chi = \psi$. Sea $V_1, \ldots, V_k$ un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos con caracteres $\chi_1, \ldots, \chi_k$, igual que en la demostración del teorema 0.230, existen enteros no negativos c_i, d_i, con $1 \leqslant i \leqslant k$ tales que

$$V \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

con c_i factores V_i para cada i, y

$$U \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

con d_i factores V_i para cada i, luego, por el teorema 0.230 tenemos que

$$c_i = \langle \chi, \chi_i \rangle = d_i \text{ y } \langle \psi, \chi_i \rangle = d_i \text{ para todo } i.$$

Ya que $\chi = \psi$ entonces $c_i = d_i$ para todo i, por lo tanto $V \cong U$. ■

Teorema 0.234. *Los caracteres irreducibles de un grupo* G*, como elementos de* $\mathbb{C}^G$*, son linealmente independientes sobre* $\mathbb{C}$*.*

Demostración. Sean $\chi_1, \ldots, \chi_k$ los distintos caracteres irreducibles de G y supongamos que

$$\sum_{j=1}^{k} \lambda_j \chi_j = f_0,\ \lambda_j \in \mathbb{C},$$

donde f_0 es la función cero, es decir, $g \mapsto 0$ para todo $g \in G$, entonces, usando el producto interno tenemos que por el teorema 0.228, para todo i

$$0 = \langle f_0, \chi_i \rangle = \langle \sum_{j=1}^{k} \lambda_j \chi_j, \chi_i \rangle = \sum_{j=1}^{k} \lambda_j \langle \chi_j, \chi_i \rangle = \lambda_i,$$

por lo tanto, $\chi_1, \ldots, \chi_r$ son linealmente independientes en $\mathbb{C}^G$. ■

Teorema 0.235. *Sean* V *y* U *dos* $\mathbb{C}G$*-módulos con caracteres* χ *y* ψ *respectivamente. Entonces*

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V,U)\big) = \langle \chi, \psi \rangle$$

Demostración. Una vez más, igual que en la demostración del teorema 0.230, existen enteros no negativos c_i, d_i, con $1 \leqslant i \leqslant k$ tales que tales que

$$V \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

con c_i factores V_i para cada i, y

$$U \cong (V_1 \oplus \cdots \oplus V_1) \oplus (V_2 \oplus \cdots \oplus V_2) \oplus \cdots \oplus (V_k \oplus \cdots \oplus V_k)$$

con d_i factores V_i para cada i.
Por el teorema 0.191, para todos i, j tenemos que

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V_i,V_j)\big) = \delta_{ij} \ .$$

Así, usando la proposición 0.193 inciso *iii*) tenemos que

$$dim_{\mathbb{C}}\big(Hom_{\mathbb{C}G}(V,U)\big) = \sum_{i=1}^{k} c_i d_i \ .$$

Por otro lado tenemos que $\chi = \sum_{i=1}^{k} c_i \chi_i$ y $\psi = \sum_{i=1}^{k} d_i \chi_i$, entonces

$$\langle \chi, \psi \rangle = \sum_{i=1}^{k} c_i d_i.$$

Por lo tanto, tenemos lo que queríamos. ■

Así, para distinguir caracteres de $\mathbb{C}G$-módulos, basta distinguir a los $\mathbb{C}G$-módulos mismos. De lo anterior, aunque cada carácter determine un $\mathbb{C}G$-módulo salvo isomorfismo, no existe una forma genérica de construir un módulo a partir de su correspondiente carácter. Así, algo de información es perdida estudiando caracteres en vez de módulos. Sin embargo, los caracteres llegan a ser un medio eficaz de traducir información acerca la teoría ordinaria de representaciones para G, en información acerca de G mismo, por esta razón tenemos interés en estudiar $\mathbb{C}G$-módulos y sus caracteres.

Funciones de clase y el número de caracteres irreducibles

El objetivo de esta parte será establecer que el número de caracteres irreducibles de un grupo finito G es igual al número de clases de conjugación, es decir, vamos a ver la conexión fundamental entre el número de $\mathbb{C}G$-módulos irreducibles y clases de conjuación de G.

Definición 0.236. *Una **función de clase** en G es una función $f : G \longrightarrow \mathbb{C}$ cuyo valor dentro de cualquier clase de conjugación es siempre constante. Denotaremos*

$$\mathbb{C}^G(C) = \{ f : G \longrightarrow \mathbb{C} \mid f \text{ es función de clase } \}.$$

Teorema 0.237. *El conjunto $\mathbb{C}^G(C)$ es un subespacio vectorial de $\mathbb{C}^G$ y además*

$$dim_{\mathbb{C}}\Big(\mathbb{C}^G(C)\Big) = r$$

donde r es el número de clases de conjugación de G.

Demostración. Veremos que una base de este espacio es el conjunto de las funciones que tienen valor 1 precisamente en una clase de conjugación y 0 en todas las demás clases, es decir,

$$\psi_i(g) = \begin{cases} 1 & si \quad g \in {x_i}^G \\ 0 & si \quad g \notin {x_i}^G. \end{cases}$$

Claramente son linealmente independientes porque si $f_0 = \sum_{i=1}^{r} \mu_i \psi_i$ para algunos $\mu_i \in \mathbb{C}$, y si $h \in G$ con $h \in {x_t}^G$, entonces $0 = \sum_{i=1}^{r} \mu_i \psi_i(h) = \mu_t$. Por lo tanto, $\mu_i = 0$ para todo i. Estas funciones generan a las funciones de clase porque si $f \in \mathbb{C}^G(C)$ entonces $f = \sum_{i=1}^{r} f(x_i)\psi_i$. ■

Notemos que para cada función de clase ψ_i tenemos que

$$\begin{aligned} \langle \psi_i, \psi_i \rangle &= \frac{1}{|G|} \sum_{g \in G} \psi_i(g)\overline{\psi_i(g)} \\ &= \frac{1}{|G|} \sum_{h \in {x_i}^G} \psi_i(h)\overline{\psi_i(h)} \\ &= \frac{1}{|G|} \sum_{h \in {x_i}^G} 1 \\ &= \frac{\#{x_i}^G}{|G|} \\ &= \frac{1}{|C_G(x_i)|}. \end{aligned}$$

Y también $\langle \psi_i, \psi_j \rangle = 0$ para $i \neq j$. Esto significa que es una base ortogonal que no es ortonormal, sin embargo sí podemos ortogonalizarla y la base es $\{\sqrt{|C_G(x_i)|}\psi_i\}_i$.

Observación 0.238. Por la proposición 0.207 los caracteres de un grupo finito G (los caracteres de $\mathbb{C}G$-módulos) son funciones de clase.

Observación 0.239. Toda función de clase $f : G \longrightarrow \mathbb{C}$ se puede ver como un elemento dentro del álgebra de grupo si hacemos la identificación

$$f \longleftrightarrow \sum_{g \in G} f(g)g.$$

Entonces la asignación para las funciones ψ_i, para todo i es

$$\psi_i \longleftrightarrow \sum_{g \in G} \psi_i(g)g = \sum_{g \in {x_i}^G} g \in \mathbb{C}(G).$$

Esta asignación aparecerá naturalmente después.

Ahora consideremos los elementos del álgebra de grupo que conmutan con todo elemento del álgebra de grupo, es decir, el conjunto

$$Z(\mathbb{C}(G)) = \{z \in \mathbb{C}(G) \mid zy = yz \ \forall \ y \in \mathbb{C}(G)\}$$

que llamaremos el **centro del álgebra de grupo**. Claramente el centro del álgebra de grupo es un subespacio del álgebra de grupo y el centro de cualquier anillo es subanillo, por lo tanto es una subálgebra. La siguiente proposición es una consecuencia más del Lema de Schur.

Proposición 0.240. *Sea V un $\mathbb{C}G$-módulo irreducible y sea $z \in Z(\mathbb{C}(G))$.*
Entonces existe $\mu \in \mathbb{C}$ tal que

$$zv = \mu v \quad \textit{para todo } v \in V.$$

Demostración. Para todos $r \in \mathbb{C}(G)$ y $v \in V$ tenemos que $(zr)v = (rz)v$, por lo tanto, la función

$$\begin{array}{rccc} T : V & \longrightarrow & V \\ v & \longmapsto & zv \end{array}$$

es un morfismo de $\mathbb{C}G$-módulos ya que

$$gT(v) = g(zv) = (gz)v = (zg)v = z(gv) = T(gv),$$

entonces, por el Lema de Schur tenemos que existe $\mu \in \mathbb{C}$ tal que $T = \mu I_V$. ■

Teorema 0.241. *El número de caracteres irreducibles de G (número de $\mathbb{C}G$-módulos irreducibles o equivalentemente, representaciones irreducibles de G) es igual al número de clases de conjugación de G.*

Demostración. Sean $\chi_1, \ldots, \chi_k$ los caracteres irreducibles de G y sea r el número de clases de conjugación de G. Por el teorema 0.234 $\chi_1, \ldots, \chi_k$ son linealmente independientes en $\mathbb{C}^G(C)$ y por el teorema 0.237 $dim_{\mathbb{C}}\left(\mathbb{C}^G(C)\right) = r$, así, $k \leqslant r$.
Vamos a dar ahora una base para $Z\big(\mathbb{C}(G)\big)$ en términos de las clases de conjugación de G, de aquí tendremos la relación fundamental entre el centro del álgebra de grupo y las clases de conjugación del grupo. Sea ${x_i}^G := C_i$ la i-ésima clase de conjugación de G, con $i \in \{1, \ldots, r\}$ y definimos

$$\overline{C}_i = \sum_{g \in C_i} g \ \in \mathbb{C}(G).$$

Es decir, cada $\overline{C}_i$ consiste de la suma de todos los elementos del grupo pertenecientes a la i-ésima clase de conjugación de G (no debe confundirse esta notación con la conjugación compleja). Los elementos $\overline{C}_1, \ldots, \overline{C}_r$ son llamados las **sumas de clase**. Notemos que las sumas de clase son las asignaciones en el álgebra de grupo para cada función ψ_i de la base de las funciones de clase como habíamos dicho antes, es decir,

$$\psi_i \longleftrightarrow \sum_{g \in G} \psi_i(g) g = \sum_{g \in {x_i}^G} g = \overline{C}_i \in \mathbb{C}(G).$$

Vamos a ver ahora que la base del centro del álgebra de grupo es $\{\overline{C}_1, \ldots, \overline{C}_r\}$.
Primero necesitamos ver que en efecto, las sumas de clase son elementos de $Z\big(\mathbb{C}(G)\big)$. Consideremos x_i el i-ésimo representante de las clases de conjugación y si $\#C_i = t_i$ para todo i entonces la i-ésima clase es de la forma

$$C_i = \{g_1 x_i g_1^{-1}, \ldots, g_{t_i} x_i g_{t_i}^{-1}\},$$

es decir, consiste de los t_i distintos conjugados de x_i en G, por lo que cada suma de clase se puede escribir como

$$\overline{C}_i = \sum_{j=1}^{t_i} g_j x_i g_j^{-1}.$$

Luego, para todo $h \in G$ tenemos que $1h \in \mathbb{C}\big(G\big)$ por lo que

$$h\overline{C}_i h^{-1} = \sum_{j=1}^{t_i} h g_j x_i g_j^{-1} h^{-1} = \sum_{j=1}^{t_i} (hg_j) x_i (hg_j)^{-1}$$

y aquí, para cada i, $(hg_j)x_i(hg_j)^{-1} \in C_i$ y como la suma corre de 1 hasta t_i tenemos que

$$h\overline{C}_i h^{-1} = \sum_{j=1}^{t_i} (hg_j) x_i (hg_j)^{-1} = \overline{C}_i$$

y por lo tanto tenemos que

$$h\overline{C}_i = \overline{C}_i h,$$

es decir, toda suma de clase conmuta con todo elemento del grupo y por lo tanto con todo elemento $\sum_{h\in G} \lambda_h h \in \mathbb{C}(G)$ ya que por definición

$$\Big(\sum_{h\in G} \lambda_h h\Big)\, \overline{C}_i = \sum_{h\in G} \lambda_h (h\overline{C}_i) = \sum_{h\in G} \lambda_h (\overline{C}_i h) = \overline{C}_i \Big(\sum_{h\in G} \lambda_h h\Big),$$

es decir $\overline{C}_i \in Z\big(\mathbb{C}(G)\big)$. Luego, $\{\overline{C}_1, \ldots, \overline{C}_r\}$ es linealmente independiente porque si

$$0 = \sum_{i=1}^{r} \mu_i \overline{C}_r = \sum_{i=1}^{r} \mu_i \Big(\sum_{y\in C_i} y\Big) = \sum_{i=1}^{r} \sum_{y\in C_i} \mu_i y,\ \mu_i \in \mathbb{C},$$

entonces $\mu_i = 0$ para todo i pues las clases $C_1, \ldots, C_r$ son disjuntas por pares. Sólo falta ver que $\langle \overline{C}_1, \ldots, \overline{C}_r \rangle = Z\big(\mathbb{C}(G)\big)$, para esto consideremos $w = \sum_{g\in G} \lambda_g g \in Z\big(\mathbb{C}(G)\big)$ y $h \in G$, entonces $hw = wh$ por lo que $hwh^{-1} = w$, es decir

$$h\Big(\sum_{g\in G} \lambda_g g\Big) h^{-1} = \sum_{g\in G} \lambda_g \left(hgh^{-1}\right) = \sum_{hgh^{-1}\in G} \lambda_g \left(hgh^{-1}\right) = \sum_{g\in G} \lambda_{h^{-1}gh} g = \sum_{g\in G} \lambda_g g.$$

Esto significa que para todo $h \in G$ el coeficiente λ_g de g es el mismo que el coeficiente $\lambda_{h^{-1}gh}$ de $h^{-1}gh$, es decir, la función

$$\begin{array}{rcl} coef : G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \lambda_g \end{array}$$

es constante en cada clase de conjugación, y por lo tanto es una función de clase de G, de aquí se sigue que $w = \sum_{g\in G} \lambda_g g = \sum_{i=1}^{r} \lambda_i \overline{C_i}$, donde $\lambda_i = \lambda_{g_i}$ es el coeficiente de algún $g_i \in C_i$. Por lo tanto

$$dim_{\mathbb{C}}\big(Z(\mathbb{C}(G))\big) = r.$$

Ahora consideremos al álgebra de grupo como el $\mathbb{C}G$-módulo regular y sea $V_1, \ldots, V_k$ un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos. Por el teorema 0.176 sabemos que

$$\mathbb{C}(G) \cong W_1 \oplus \cdots \oplus W_k$$

donde para cada i, W_i es isomorfo a una suma directa de copias de V_i. Luego, ya que $\mathbb{C}(G)$ tiene elemento identidad $1_{\mathbb{C}(G)}$, existen $s_i \in W_i$ tales que

$$1_{\mathbb{C}(G)} = s_1 + \cdots + s_k.$$

Por último, para $z \in Z(\mathbb{C}(G))$, por la proposición 0.240, para cada i existen $\mu_i \in \mathbb{C}$ tal que para todo $v \in V_i$

$$zv = \mu_i v$$

Por lo tanto $zw = \mu_i w$ que para todo $w \in W_i$, y en particular

$$zs_i = \mu_i s_i \text{ que para todo } 1 \leqslant i \leqslant k.$$

Entonces

$$z = z1_{\mathbb{C}(G)} = z(s_1 + \cdots + s_k) = zs_1 + \cdots + zs_k = \mu_1 s_1 + \cdots + \mu_k s_k.$$

Esto muestra que

$$Z(\mathbb{C}(G)) \subset \langle s_1, \ldots, s_k \rangle,$$

pero habíamos visto que la dimensión de $Z(\mathbb{C}(G))$ es r, por lo tanto, $r \leqslant k$, y así, $k = r$. ■

Corolario 0.242. *Los caracteres irreducibles $\{\chi_1, \ldots, \chi_r\}$ de G forman una base ortonormal para el espacio de funciones de clase en G.*

Demostración. Por el teorema 0.234, los caracteres irreducibles de G son linealmente independientes en $\mathbb{C}^G(C)$, pero su número es igual al número de clases de conjugación de G por el teorema 0.241, que es igual a la dimensión de $\mathbb{C}^G(C)$ por lo que los caracteres irreducibles forman una base de $\mathbb{C}^G(C)$. Más aún, $\{\chi_1, \ldots, \chi_r\}$ es un conjunto ortonormal por el teorema 0.228. ■

Observación 0.243. Por álgebra lineal, podemos escribir

$$\varphi = \sum_{i=1}^{r} \lambda_i \chi_i, \text{ con } \lambda_i = \langle \varphi, \chi_i \rangle$$

ya que $\varphi = \sum_{j=1}^{r} \lambda_j \chi_j$ para algunos $\lambda_j \in \mathbb{C}$, y entonces para todo i

$$\langle \varphi, \chi_i \rangle = \Big\langle \sum_{j=1}^{r} \lambda_j \chi_j, \chi_i \Big\rangle = \sum_{j=1}^{r} \lambda_j \langle \chi_j, \chi_i \rangle = \sum_{j=1}^{r} \lambda_j \delta_{ji} = \lambda_i.$$

A una $\mathbb{Z}$-combinación lineal de los caracteres irreducibles $\chi_1, \ldots, \chi_r$ de G le llamaremos un **carácter virtual**.

Corolario 0.244. *Si $\alpha = \sum_{i=1}^{r} a_i \chi_i$ y $\beta = \sum_{i=1}^{r} b_j \chi_j$ son caracteres virtuales de G, entonces*

$$\langle \alpha, \beta \rangle = \sum_{i=1}^{r} a_i b_i$$

Demostración. Tenemos que

$$\langle \alpha, \beta \rangle = \Big\langle \sum_{i=1}^{r} a_i \chi_i, \sum_{i=1}^{r} b_j \chi_j \Big\rangle = \sum_{i=1}^{r} \sum_{j=1}^{r} a_i b_j \langle \chi_i, \chi_j \rangle = \sum_{i=1}^{r} \sum_{j=1}^{r} a_i b_j \delta_{ij} = \sum_{i=1}^{r} a_i b_i.$$

■

Corolario 0.245. *Si α es un carácter de G y $n \in \{1,2,3\}$, entonces*

$$\langle \alpha, \alpha \rangle = n \text{ si y sólo si } \alpha \text{ es una suma de } n \text{ caracteres irreducibles.}$$

Demostración. Dado que α es un carácter de G, descomponiendo el módulo asociado en módulos irreducibles tenemos que $\alpha = \sum_{i=1}^{r} a_i \chi_i$ con a_i enteros no negativos. Entonces, por el corolario anterior tenemos que $\langle \alpha, \alpha \rangle = \sum_{i=1}^{r} {a_i}^2$. Luego, si $\langle \alpha, \alpha \rangle = n$ entonces tenemos que $a_j = 1$ para exactamente n números $1 \leqslant j \leqslant r$ y $a_i = 0$ para los otros i, y entonces α es una suma de n caracteres irreducibles. Por el corolario anterior el recíproco es trivial. ■

Corolario 0.246. *Si α es un carácter virtual de G, entonces cada χ_j aparece con coeficiente $\langle \alpha, \chi_j \rangle$ en la única expresión de α como una $\mathbb{Z}$-combinación lineal de los caracteres irreducibles de G.*

Demostración. Si $\alpha = \sum_{i=1}^{r} a_i \chi_i$ con a_i enteros no negativos, entonces $\langle \alpha, \chi_j \rangle = a_j$ por el corolario 0.244. ■

Tabla de caracteres

Habíamos concluído que cualquier carácter de un grupo G es una $\mathbb{Z}$-combinación lineal de los r caracteres irreducibles $\chi_1, \ldots, \chi_r$ de G, donde r es el número de clases de conjugación de G.
Ya que cada carácter es especificado por su valor en cada clase de conjugación de G, se sigue que los caracteres de G están completamente determinados por un arreglo de $r \times r$ dando los valores de los r caracteres irreducibles en las r clases de conjugación de G.

Definición 0.247. *Sean $\chi_1, \ldots, \chi_r$ los caracteres irreducibles de G, donde r es el número de clases de conjugación de G y $x_1, \ldots, x_r$ son los representantes de las clases de conjugación.*
*La **tabla de caracteres** de G es la matriz Υ de $r \times r$ cuya entrada ij es $\chi_i(x_j)$, $i, j \in \{1, \ldots, r\}$. Es decir, los renglones están indexados por los caracteres irreducibles y las columnas por las clases de conjugación (o por los representantes).*

Por convención, $x_1 = e_G$, así que la primera columna de la tabla de caracteres consiste de los grados d_i de G (las dimensiones de un conjunto completo de $\mathbb{C}G$-módulos irreducibles no isomorfos), y χ_1 es el carácter trivial, denotaremos además $|{x_i}^G| = k_i = [G : C_G(x_i)]$ al tamaño de la clase de conjugación de x_i (por el Teorema Órbita-Estabilizador) para cada i. Entonces Υ se escribe como:

	1	k_2	k_3	$\cdots$	k_r
	e_G	x_2	x_3	$\cdots$	x_r
χ_1	e_G	1	1	$\cdots$	1
χ_2	d_2	$\chi_2(x_2)$	$\chi_2(x_3)$	$\cdots$	$\chi_2(x_r)$
χ_3	d_3	$\chi_3(x_2)$	$\chi_3(x_3)$	$\cdots$	$\chi_3(x_r)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_r	d_r	$\chi_r(x_2)$	$\chi_r(x_3)$	$\cdots$	$\chi_r(x_r)$

Observación 0.248. La tabla de caracteres de G está bien definida, salvo reordenamientos de renglones o columnas. Además es una matriz invertible. Más claramente, sea Ω la matriz cuya entrada ij es

$$\Omega_{ij} = \frac{k_i\overline{\chi_j}(x_i)}{|G|} = \frac{1}{|G|} = \sum_{y\in C_t}\overline{\chi_j(g_t)},$$

entonces

$$\begin{aligned}(\Upsilon\Omega)ij &= \frac{1}{|G|}\sum_{t=1}^{r}\chi_i(x_t)k_t\overline{\chi_j}(x_t)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j}(g)\\ &= \langle\chi_i,\chi_j\rangle\\ &= \delta_{ij}\end{aligned}$$

ya que $k_t\overline{\chi_j}(x_t) = \sum_{y\in C_t}\overline{\chi_j(y)}$ y así tenemos que $\Upsilon\Omega = I$.

Lo siguiente será establecer algunas propiedades fundamentales de los caracteres.

Teorema 0.249. ***Relaciones de ortogonalidad****. Sean $\chi_1,\ldots,\chi_r$ los caracteres irreducibles de G y sean $x_1,\ldots,x_r$ los representantes de las clases conjugación de G con $k_1,\ldots,k_r$ sus respectivos tamaños, entonces para todos $t,s\in\{1,\ldots,r\}$ tenemos que*

i) Los renglones de la tabla de caracteres (como vectores renglón en $\mathbb{C}^r$) son ortogonales, más aún,

$$\delta_{ij} = \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = \frac{1}{|G|}\sum_{t=1}^{r}k_t\chi_i(x_t)\overline{\chi_j(x_t)} = \sum_{t=1}^{r}\frac{1}{|C_G(x_t)|}\chi_i(x_t)\overline{\chi_j(x_t)} = \langle\chi_i,\chi_j\rangle.$$

ii) Las columnas de la tabla de caracteres son ortogonales, más aún,

$$\sum_{t=1}^{r}\chi_t(x_i)\overline{\chi_t(x_j)} = \frac{|G|}{k_i}\delta_{ij} = |C_G(x_i)|\delta_{ij}.$$

Demostración. *i*) Si $V_1,\ldots,V_r$ es un conjunto completo de $\mathbb{C}G$- módulos irreducibles no isomorfos entonces tienen caracteres $\chi_1,\ldots,\chi_r$ por el teorema 0.233, y por el teorema 0.235

$$\langle\chi_i,\chi_j\rangle = dim_{\mathbb{C}}\left(Hom_{\mathbb{C}G}(V_i,V_j)\right),$$

pero ya que los V_i son irreducibles no isomorfos, la dimensión de $Hom_{\mathbb{C}G}(V_i,V_j)$ es cero si $i\neq j$ y es 1 si $i=j$ por el teorema 0.228.
ii) Para $1\leq j\leq r$ sea ψ_j la función de clase que satisface

$$\psi_j(x_i) = \delta_{ij} \text{ con } 1\leq i\leq r.$$

Por el corolario 0.242 tenemos que $\psi_j = \sum_{t=1}^{k}\lambda_t\chi_t$ para algunos $\lambda_1,\ldots,\lambda_t\in\mathbb{C}$, y por *i*)

$$\lambda_t = \langle\psi_j,\chi_t\rangle = \frac{1}{|G|}\sum_{g\in G}\psi_j(g)\overline{\chi_t}(g).$$

Ahora, $\psi_j(g) = 1$ si g es conjugado de x_j y 0 en otro caso. También hay $\frac{|G|}{|C_G(x_j)|}$ elementos conjugados a x_j (los elementos en su órbita) y por lo que

$$\lambda_t = \frac{1}{|G|} \sum_{g \in {x_j}^G} \psi_j(g)\overline{\chi_t(g)} = \frac{\overline{\chi_t(x_j)}}{|C_G(x_j)|}.$$

Por lo tanto

$$\delta_{ij} = \psi_j(x_i) = \sum_{t=1}^{r} \lambda_t \chi_t(x_i) = \sum_{t=1}^{r} \frac{\chi_t(x_i)\overline{\chi_t(x_j)}}{|C_G(x_j)|}.$$

■

Proposición 0.250. *Si α es un carácter lineal de G y χ carácter irreducible de G, entonces $\alpha\chi$ es un carácter irreducible de G.*

Demostración. Sea $\rho : G \longrightarrow GL_n(\mathbb{C})$ una representación de G con carácter χ y definamos la función

$$\begin{array}{rcl} \alpha\rho : G & \longrightarrow & GL_n(\mathbb{C}) \\ g & \longmapsto & \alpha(g)\rho(g). \end{array}$$

Entonces $(\alpha\rho)(g)$ es la matriz $\rho(g)$ multiplicada por el escalar $\alpha(g)$, y ya que α y ρ son morfismos de grupos, entonces $\alpha\rho$ es morfismo de grupos pues

$$(\alpha\rho)(gh) = \alpha(gh)\rho(gh) = \alpha(g)\alpha(h)\rho(g)\rho(h) = \alpha(g)\rho(g)\alpha(h)\rho(h) = \alpha\rho(g)\alpha\rho(h)$$

para todos $g, h \in G$. Luego, la matriz $(\alpha\rho)(g) = \alpha(g)\rho(g)$ tiene traza igual a $\alpha(g)tr\left(\rho(g)\right) = \alpha(g)\chi(g)$, entonces $\alpha\rho$ es una representación de G con carácter $\alpha\chi$.
Ya que α es lineal, de la proposición 0.209 inciso $ii)$ tenemos que $\alpha(g)$ es una raíz de la unidad para todo $g \in G$, y en particular que $1 = |\alpha(g)| = \alpha(g)\overline{\alpha(g)}$ para todo $g \in G$. Por lo tanto

$$\begin{array}{rcl} \langle \alpha\chi, \alpha\chi \rangle & = & \frac{1}{|G|} \sum_{g \in G} \alpha(g)\chi(g)\overline{\alpha(g)\chi(g)} \\ & = & \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)}\alpha(g)\overline{\alpha(g)} \\ & = & \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \langle \chi, \chi \rangle = 1. \end{array}$$

■

Llegaremos a ver que las relaciones de ortogonalidad harán posible construir la tabla de caracteres siempre y cuando sepamos algo acerca del grupo G en cuestión.
Podríamos plantearnos la pregunta conversa, ¿qué información acerca del grupo G puede ser obtenida a partir de su tabla de caracteres?
Para responder a esta pregunta primero necesitamos cierta información acerca de la conexión que existe entre la teoría de representaciones de un grupo y sus grupos cocientes.

Levantamiento de caracteres

En esta sección vamos a hallar los caracteres de un grupo cociente, que son más fáciles de describir que los de G mismo, para esto, si $N \trianglelefteq G$ entonces usaremos los caracteres de G/N para hallar ciertos caracteres de G.

Teorema 0.251. *Sea $N \trianglelefteq G$ y $\widehat{\chi} : G/N \longrightarrow \mathbb{C}$ un carácter de G/N, entonces la función*

$$\begin{array}{rcl} \chi : G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \widehat{\chi}(gN) \end{array}$$

es un carácter de G, además χ y $\widehat{\chi}$ tienen el mismo grado.

Demostración. Sea $\widehat{\rho} : G/N \longrightarrow GL_n(\mathbb{C})$ una representación de G/N con carácter $\widehat{\chi}$. Luego, la función $\rho : G \longrightarrow GL_n(\mathbb{C})$ dada por la composición $g \mapsto gN \mapsto \widehat{\rho}(gN)$ (es decir, $\rho = \widehat{\rho} \circ \pi$) es un morfismo de grupos por ser composición de morfismos de grupos y por lo tanto ρ es una representación de G y el carácter χ de ρ satisface que

$$\chi(g) = tr(\rho(g)) = tr(\widehat{\rho}(gN)) = \widehat{\chi}(gN).$$

para todo $g \in G$. Más aún, $\chi(e) = \widehat{\chi}(N)$ y por lo tanto χ y $\widehat{\chi}$ tienen el mismo grado. ■

Definición 0.252. *Al carácter χ en el teorema 0.251 se le llama el **levantamiento** de $\widehat{\chi}$ a G.*

Observación 0.253. El levantamiento es caso particular de pullback.

Denotemos al conjunto de caracteres de un grupo G por $Ch(G)$.

Teorema 0.254. *Si $N \trianglelefteq G$ entonces la siguiente función es una biyección*

$$\begin{array}{rcl} \Lambda : \{\widehat{\chi} \in Ch(G/N)\} & \longrightarrow & \{\chi \in Ch(G) \mid N \leq Ker(\chi)\} \\ \widehat{\chi} & \longmapsto & \chi = \widehat{\chi} \circ \pi. \end{array}$$

es decir, Λ es asignar a los caracteres de G/N sus levantamientos a G. Bajo esta biyección caracteres irreducibles de G/N corresponden a caracteres irreducibles de G cuyo núcleo contiene a N.

Demostración. Si $\widehat{\chi}$ es un carácter de G/N y χ es el levantamiento de $\widehat{\chi}$ a G, entonces $\widehat{\chi}(N) = \chi(e_G)$. También, si $k \in N$ entonces

$$\chi(k) = \widehat{\chi}(kN) = \widehat{\chi}(N) = \chi(e_G),$$

y por lo tanto $N \leqslant Ker(\chi)$.
Ahora sea χ un carácter de G con $N \leqslant Ker(\chi)$ y sea $\rho : G \longmapsto GL_n(\mathbb{C})$ una representación de G con carácter χ. Si $g_1, g_2 \in G$ y $g_1N = g_2N$ entonces $g_2^{-1}g_1 \in N$, y así tenemos que $\rho(g_2^{-1}g_1) = I_n$, y por lo tanto que $\rho(g_2)^{-1}\rho(g_1) = I_n$, es decir, $\rho(g_1) = \rho(g_2)$. Entonces podemos definir la función

$$\begin{array}{rcl} \widehat{\rho} : G/N & \longrightarrow & GL_n(\mathbb{C}) \\ gN & \longmapsto & \rho(g). \end{array}$$

Luego, para todos $g, h \in G$ tenemos que

$$\widehat{\rho}\,((gN)(hN)) = \widehat{\rho}(ghN) = \rho(gh) = \rho(g)\rho(h) = \widehat{\rho}(gN)\widehat{\rho}(hN)$$

y por lo tanto $\widehat{\rho}$ es una representación de G/N. Ahora, si $\widehat{\chi}$ es el carácter asociado a $\widehat{\rho}$ entonces para $g \in G$

$$\widehat{\chi}(gN) = \chi(g).$$

Por lo tanto χ es el levantamiento de $\widehat{\chi}$ a G.
Así, hemos visto que la función que manda a cada carácter de G/N a su levantamiento a G es una biyección entre el conjunto de caracteres de G/N y el conjunto de los caracteres de G que contienen a N en su núcleo. Por último veremos que caracteres irreducibles corresponden a caracteres irreducibles. Para ver esto, sea U un subespacio de $\mathbb{C}^n$ y notemos que

$$gu = \rho(g)u \in U \text{ para todo } u \in U \text{ si y sólo si } (gN)u = \widehat{\rho}(gN)u \in U \text{ para todo } u \in U.$$

Por lo tanto U es un $\mathbb{C}G$-submódulo de $\mathbb{C}^n$ si y sólo si U es un $\mathbb{C}(G/N)$-submódulo de $\mathbb{C}^n$.
La representación ρ es por lo tanto irreducible si y sólo si la representación $\widehat{\rho}$ es irreducible.
Por lo que si $\widehat{\chi}$ es un carácter del $\mathbb{C}(G/N)$-módulo U, entonces el carácter del $\mathbb{C}G$-módulo U es $\chi = \widehat{\chi} \circ \pi$ donde $\pi : G \longrightarrow G/N$ es la proyección canónica, y entonces χ es irreducible si y sólo si $\widehat{\chi}$ es irreducible. ■

Podemos obtener información acerca de los subgrupos normales de G considerando los núcleos $K_{\chi_i} := K_i$ de los carácteres irreducibles χ_i de G.

Proposición 0.255. *Los subgrupos normales de G son precisamente intersecciones de núcleos de carácteres irreducibles de G, es decir, si $N \lhd G$ entonces*

$$N = \bigcap_{i=1}^{k} K_i \text{ para algunos } i.$$

Demostración. La prueba se omite porque no usaremos este resultado, pero lo encunciamos porque es una caracterización de los subgrupos normales de un grupo en términos de los caracteres ireducibles del grupo. De hecho, parecido a la caracterización de un subgrupo normal como unión de clases de conjugación. Ver [13], capítulo 17. ■

Recordemos que el conmutador de un grupo G es el subgrupo

$$G' = \langle\ [g,h] \mid g,h \in G\ \rangle \text{ donde } [g,h] = ghg^{-1}h^{-1} \text{ para cada } g,h \in G.$$

Vamos a probar que los caracteres lineales de G son precisamente los levantamientos de los caracteres irreducibles de G/G'. Necesitamos la siguiente

Proposición 0.256. *Si χ es un carácter lineal de G entonces $G' \leq Ker(\chi)$.*

Demostración. Sea χ un carácter lineal de G, ya que en este caso $\chi : G \longrightarrow \mathbb{C}^*$ es un morfismo de grupos por el ejemplo 0.205, tenemos que su valor en todo conmutador de elementos $g,h \in G$ es

$$\chi(ghg^{-1}h^{-1}) = \chi(g)\chi(h)\chi(g^{-1})\chi(h^{-1}) = \chi(g)\chi(h)\chi(g)^{-1}\chi(h)^{-1} = 1$$

y por lo tanto $G' \leq Ker(\chi)$. ■

Teorema 0.257. *Los caracteres lineales de G son los levantamientos a G de los caracteres irreducibles de G/G' En particular, el número de distintos caracteres lineales de G es igual a $|G/G'|$, y por lo tanto un divisor de $|G|$.*

Demostración. Sea $s = |G/G'|$. Ya que G/G' es abeliano (ejemplo 0.24), entonces todas sus representaciones irreducibles son de grado 1 y hay tantas como su orden, como vimos en el teorema 0.184, así G/G' tiene exactamente s caracteres irreducibles (necesariamente lineales), digamos $\widehat{\chi}_1, \ldots, \widehat{\chi}_s$ y sus levantamientos a G, $\chi_1, \ldots, \chi_s$ también son caracteres lineales y por el teorema 0.254 son precisamente los caracteres lineales de G cuyos núcleos contienen al conmutador G' y por la proposición 0.256, los caracteres $\chi_1, \ldots, \chi_s$ son todos los caracteres lineales de G. ■

Además de ser importantes los caracteres lineales de un grupo G por ser caracteres irreducibles, son importantes porque a partir de ellos se pueden construir nuevos caracteres irreducibles del grupo, como se vió en el teorema 0.250. Esto sugiere que podríamos multiplicar dos caracteres y el producto puede ser de nuevo un carácter, en lo que sigue veremos las condiciones necesarias para que suceda eso, veremos que depende del producto tensorial de $\mathbb{C}G$-módulos.

Producto tensorial y producto de caracteres

La idea de esta parte es ver bajo qué condiciones el producto de dos caracteres es un nuevo carácter, y para eso se construye a partir de dos $\mathbb{C}G$-módulos un nuevo $\mathbb{C}G$-módulo llamado el producto tensorial cuyo carácter es el producto de los dos caracteres asociados a los $\mathbb{C}G$-módulos iniciales. Si esto tiene sentido, un caso importante sería tomar el producto de un carácter consigo mismo tantas veces como lo deseemos y obtener nuevos caracteres.

Recordemos que si U y V son $\mathbb{C}$-espacios vectoriales de dimensiones m y n respectivamente entonces el producto tensorial de U y V es el $\mathbb{C}$-espacio vectorial $U \otimes V$ de dimensión mn con base $\{u_i \otimes v_j\}_{ij}$ donde $\{u_1, \ldots, u_m\}$ es una base de U y $\{v_1, \ldots, v_n\}$ es una base de V y así los elementos en el producto tensorial son expresiones de la forma $\sum_{ij} a_{ij}(u_i \otimes v_j)$, con $a_{ij} \in \mathbb{C}$.

Si $u = \sum_{i=1}^{m} \lambda_i u_i \in U$ y $v = \sum_{j=1}^{m} \mu_j v_j \in V$ entonces definimos $u \otimes v \in U \otimes V$ como

$$u \otimes v = \sum_{i=1}^{n} \lambda_i u_i \otimes \sum_{j=1}^{m} \mu_j v_j = \sum_{i,j}^{n,m} \lambda_i \mu_j \, (u_i \otimes v_j),$$

donde $\sum_{i,j}^{n,m}$ significa la doble suma $\sum_{i=1}^{n}\sum_{j=1}^{m}$.
También se sabe que la construcción del producto tensorial no depende de las bases de los espacios en cuestión.

Definición 0.258. *Si U y V son $\mathbb{C}G$-módulos con bases como arriba, entonces definimos una acción de G en la base de $U \otimes V$ como sigue:*

$$\begin{aligned} \odot : G \times (U \otimes V) &\longrightarrow U \otimes V \\ (g, u_i \otimes v_j) &\longmapsto gu_i \otimes gv_j \end{aligned}$$

Antes de dar una acción del grupo en el producto tensorial necesitamos estudiar algunas propiedades del producto tensorial.

Proposición 0.259. *Para todos $u \in U, v \in V, a \in \mathbb{C}, x_{1'}, \ldots, x_{k'} \in U, y_{1'}, \ldots, y_{l'} \in V$ tenemos que*

(a) $u \otimes (av) = (au) \otimes v = a(u \otimes v)$

(b) $\left(\sum_{i'=1}^{k'} x_{i'}\right) \otimes \left(\sum_{j'=1}^{l'} y_{j'}\right) = \sum_{i',j'}^{k',l'} x_{i'} \otimes y_{j'}$

Demostración. (a) Sean $u = \sum_{i=1}^{m} \lambda_i u_i \in U$ y $v = \sum_{j=1}^{m} \mu_j v_j \in V$ entonces

$$\begin{aligned}
u \otimes (av) &= \left(\sum_{i=1}^{m} \lambda_i u_i\right) \otimes \left(\sum_{j=1}^{n} a\mu_j v_j\right) = \sum_{i,j}^{m,n} a\lambda_i\mu_j (u_i \otimes v_j), \\
(au) \otimes v &= \left(\sum_{i=1}^{m} a\lambda_i u_i\right) \otimes \left(\sum_{j=1}^{n} \mu_j v_j\right) = \sum_{i,j}^{m,n} a\lambda_i\mu_j (u_i \otimes v_j), \\
a(u \otimes v) &= a\left(\sum_{i,j}^{m,n} \lambda_i\mu_j (u_i \otimes v_j)\right) = \sum_{i,j}^{m,n} a\lambda_i\mu_j (u_i \otimes v_j).
\end{aligned}$$

(b) Para todos $i' \in \{1, \ldots k'\}$, $j' \in \{1, \ldots l'\}$, sean $x_{i'} = \sum_{i=1}^{m} a_{ix_{i'}} u_i$ y $y_{j'} = \sum_{j=1}^{n} b_{jy_{j'}} v_j$, entonces

$$\begin{aligned}
\left(\sum_{i'=1}^{k'} x_{i'}\right) \otimes \left(\sum_{j'=1}^{l'} y_{j'}\right) &= \left(\sum_{i'=1}^{k'} \left(\sum_{i=1}^{m} a_{ix_{i'}} u_i\right)\right) \otimes \left(\sum_{j'=1}^{l'} \left(\sum_{j=1}^{n} b_{jy_{j'}} v_j\right)\right) \\
&= \left(\sum_{i=1}^{m} \left(\sum_{i'=1}^{k'} a_{ix_{i'}}\right) u_i\right) \otimes \left(\sum_{j=1}^{n} \left(\sum_{j'=1}^{l'} b_{jy_{j'}}\right) v_j\right) \\
&= \sum_{i,j}^{m,n} \left(\left(\sum_{i'=1}^{k'} a_{ix_{i'}}\right)\left(\sum_{j'=1}^{l'} b_{jy_{j'}}\right)\right)(u_i \otimes v_j) \\
&= \sum_{i,j}^{m,n} \left(\sum_{i',j'}^{k',l'} a_{ix_{i'}} b_{jy_{j'}}\right)(u_i \otimes v_j) \\
&= \sum_{i',j'}^{k',l'} \left(\sum_{i,j}^{m,n} a_{ix_{i'}} b_{jy_{j'}} (u_i \otimes v_j)\right) \\
&= \sum_{i',j'}^{k',l'} \left(\left(\sum_{i=1}^{m} a_{ix_{i'}} u_i\right) \otimes \left(\sum_{j=1}^{n} b_{jy_{j'}} v_j\right)\right) \\
&= \sum_{i',j'}^{k',l'} x_{i'} \otimes y_{j'}.
\end{aligned}$$

■

Veamos ahora que si U y V son $\mathbb{F}G$-módulos entonces el producto tensorial puede ser equipado con estructura de $\mathbb{F}G$-módulo. Para garantizar esto, primero, extendemos la acción $\odot$ al producto tensorial como

$$g \sum_{i,j}^{n,m} \lambda_{ij} (u_i \otimes v_j) := \sum_{i,j}^{n,m} \lambda_{ij} (gu_i \otimes gv_j).$$

Teorema 0.260. *Para todos $u \in U,\ v \in V,\ g \in G$ se tiene que*

$$g(u \otimes v) = gu \otimes gv$$

Demostración. $u = \sum_{i=1}^{m} \lambda_i u_i \in U$ y $v = \sum_{j=1}^{n} \mu_j v_j \in V$, entonces por definición y ambas partes de la proposición 0.259 tenemos que

$$\begin{aligned} g(u \otimes v) &= g\left(\sum_{i=1}^{m} \lambda_i u_i \otimes \sum_{j=1}^{n} \mu_j v_j\right) \\ &= g\left(\sum_{i,j}^{m,n} \lambda_i \mu_j (u_i \otimes v_j)\right) \\ &= \sum_{i,j}^{m,n} \lambda_i \mu_j \, (gu_i \otimes gv_j) \\ &= \left(\sum_{i=1}^{m} \lambda_i g u_i\right) \otimes \left(\sum_{j=1}^{n} \mu_j g v_j\right) \\ &= g\left(\sum_{i=1}^{m} \lambda_i u_i\right) \otimes g\left(\sum_{j=1}^{n} \mu_j v_j\right) \\ &= gu \otimes gv. \end{aligned}$$

■

Teorema 0.261. *Si U y V son $\mathbb{F}G$-módulos entonces $U \otimes V$ es $\mathbb{F}G$-módulo con la acción*

$$\begin{aligned} \odot : G \times (U \otimes_{\mathbb{F}} V) &\longrightarrow U \otimes_{\mathbb{F}} V \\ (g, u_i \otimes v_j) &\longmapsto gu_i \otimes gv_j \end{aligned}$$

que habíamos definido antes y extendida linealmente.

Demostración. Verifiquemos que se cumplen las condiciones de $\mathbb{F}G$-módulo. Notemos que para cualesquiera $i \in \{1, \dots m\}$, $j \in \{1, \dots n\}$, $u \in U,\ v \in V,\ g, h \in G,\ a \in \mathbb{F}$ tenemos que

(1) $g\left(\sum_{ij} a_{ij}(u_i \otimes v_j)\right) = \sum_{ij} a_{ij}(gu_i \otimes gv_j) \in U \otimes V$,

(2) $e_G\left(\sum_{ij} a_{ij}(u_i \otimes v_j)\right) = \sum_{ij} a_{ij}(e_G u_i \otimes e_G v_j) = \sum_{ij} a_{ij}(u_i \otimes v_j)$,

(3) Por el teorema 0.260 tenemos que

$$\begin{aligned} (gh)\left(\sum_{ij} a_{ij}(u_i \otimes v_j)\right) &= \sum_{ij} a_{ij}\left((gh)u_i \otimes (gh)v_j\right) \\ &= \sum_{ij} a_{ij}\left(g(hu_i) \otimes g(hv_j)\right) \\ &= \sum_{ij} a_{ij}\left(g(hu_i \otimes hv_j)\right) \\ &= \sum_{ij} a_{ij}\left(g(h(u_i \otimes v_j)\right) \\ &= g \sum_{ij} a_{ij}\left(h(u_i \otimes v_j)\right) \\ &= g\left(h\left(\sum_{ij} a_{ij}(u_i \otimes v_j)\right)\right) \end{aligned}$$

(4) $g\Big(a\sum_{ij}a_{ij}(u_i\otimes v_j)\Big)=g\Big(\sum_{ij}aa_{ij}(u_i\otimes v_j)\Big)=\sum_{ij}aa_{ij}(gu_i\otimes gv_j)=a\Big(g\sum_{ij}a_{ij}(u_i\otimes v_j)\Big)$

(5) y por último

$$\begin{aligned} g\Big(\sum_{ij}a_{ij}(u_i\otimes v_j)+\sum_{ij}b_{ij}(u_i\otimes v_j)\Big) &= g\Big(\sum_{ij}(a_{ij}+b_{ij})(u_i\otimes v_j)\Big)\\ &= \sum_{ij}(a_{ij}+b_{ij})(gu_i\otimes gv_j)\\ &= \sum_{ij}a_{ij}(gu_i\otimes gv_j)+\sum_{ij}b_{ij}(gu_i\otimes gv_j)\\ &= g\Big(\sum_{ij}a_{ij}(u_i\otimes v_j)\Big)+g\Big(\sum_{ij}b_{ij}(u_i\otimes v_j)\Big). \end{aligned}$$

Por lo tanto $U\otimes V$ es un $\mathbb{F}G$-módulo. ■

Proposición 0.262. *Sean V y U $\mathbb{C}G$-módulos. Si $U^*=Hom_{\mathbb{C}}(U,\mathbb{C})$, entonces existe un isomorfismo de $\mathbb{C}G$-módulos*

$$U^*\otimes V\cong Hom_{\mathbb{C}}(U,V)$$

Demostración. Sean $\beta=\{u_1,\dots,u_n\}$ y $\gamma=\{v_1,\dots,v_m\}$ bases de U y V respectivamente y y sea $\beta^*=\{\varphi_1,\dots,\varphi_n\}$ la base dual de β. Consideremos la función

$$\begin{array}{rcl}\Gamma: U^*\otimes V & \longrightarrow & Hom_{\mathbb{C}}(U,V)\\ \phi\otimes v & \longmapsto & \Gamma(\phi\otimes v)\end{array} \quad \text{donde} \quad \begin{array}{rcl}\Gamma(\phi\otimes v): U & \longrightarrow & V\\ u & \longmapsto & \phi(u)v.\end{array}$$

Luego, si $\phi\in U^*$ entonces ϕ es la transformación cero o ϕ es suprayectiva pues su codominio es un campo. Entonces, si $\Gamma(\phi\otimes v)$ es la función cero tenemos que

$$0=\Gamma(\phi\otimes v)(u)=\phi(u)v \text{ para todo } u\in U,$$

y entonces $\phi=f_0$, el funcional cero o $v=0$. Así, los elementos en $Ker(\Gamma)$ son los elementos $f_0\otimes w$ y $\psi\otimes 0$. Usando esto para los vectores de la base $\{\varphi_i\otimes v_k\}_{ik}$ tenemos que para algún $u_j\in\beta$

$$\Gamma(\varphi_i\otimes v_k)(u_j)=\varphi_i(u_j)v_k=\delta_{ij}v_k$$

y entonces $\Gamma(\varphi_i\otimes v_k)(u_i)=\varphi_i(u_i)v_k=v_k$ y si $i\neq j$ entonces $\Gamma(\varphi_i\otimes v_k)(u_j)=\varphi_i(u_j)v_k=0$, luego, se puede ver que $\{\Gamma(\varphi_i\otimes v_k)\}_{i,k}$ genera a $Hom_{\mathbb{C}}(U,V)$. Más aún, Γ tiene inversa dada por la función

$$\begin{array}{rcl}\Theta: Hom_{\mathbb{C}}(U,V) & \longrightarrow & U^*\otimes V\\ T & \longmapsto & \sum_{i=1}^{n}\varphi_i\otimes T(u_i)\end{array}$$

que es lineal por las propiedades del producto tensorial y la definición de suma de transformaciones lineales, y entonces para todo $u=\sum_{i=1}^{n}a_iu_i\in U$ tenemos que

$$\begin{aligned}(\Gamma\circ\Theta)(T)(u)=\Gamma\left(\Theta(T)\right)(u) &= \Gamma\left(\sum_{i=1}^{n}\varphi_i\otimes T(u_i)\right)(u)\\ &= \sum_{i=1}^{n}\Gamma\left(\varphi_i\otimes T(u_i)\right)(u)\\ &= \sum_{i=1}^{n}\varphi_i(u)T(u_i)=\sum_{i=1}^{n}a_iT(u_i)=T\left(\sum_{i=1}^{n}a_iu_i\right)=T(u)\end{aligned}$$

y por lo tanto $\Gamma \circ \Theta = I_{Hom_{\mathbb{C}}(U,V)}$. Por otro lado, para todo $\phi \otimes v \in U^* \otimes V$ se tiene que

$$(\Theta \circ \Gamma)(\phi \otimes v) = \Theta\left(\Gamma(\phi \otimes v)\right) = \sum_{i=1}^{n} \varphi_i \otimes \left(\Gamma(\phi \otimes v)(u_i)\right) = \sum_{i=1}^{n} \varphi_i \otimes (\phi(u_i)v) = \sum_{i=1}^{n} \phi(u_i)\varphi_i \otimes v = \phi \otimes v,$$

por lo tanto $\Theta \circ \Gamma = I_{U^* \otimes V}$ y así Γ es un isomorfismo de espacios vectoriales (además $U^* \otimes V$ y $Hom_{\mathbb{C}}(U,V)$ son espacios de la misma dimensión desde el inicio, así bastaba exihibir una transformación lineal inyectiva, suprayectiva o biyectiva).
Luego, Γ es un morfismo de $\mathbb{C}G$-módulos pues para todo $g \in G$ tenemos que

$$\begin{aligned}
\left[g\left(\Gamma(\phi \otimes v)\right)\right](u) &= g\left(\phi(g^{-1}u)v\right) \\
&= \phi(g^{-1}u)gv \\
&= (g\phi)(u)gv \\
&= \Gamma(g\phi \otimes gv)(u) \\
&= \left[\Gamma\left(g(\phi \otimes v)\right)\right](u).
\end{aligned}$$

También se puede ver que Θ es un morfismo de $\mathbb{C}G$-módulos. Por lo tanto $U^* \otimes V \cong Hom_{\mathbb{C}}(U,V)$.
■

Lo que sigue es calcular el carácter de $U \otimes V$.

Teorema 0.263. *Sean U, V $\mathbb{C}G$-módulos con caracteres χ_U y χ_V respectivamente, entonces el carácter de su producto tensorial es el producto de los dos caracteres, es decir,*

$$\chi_{U \otimes V} = \chi_U \chi_V.$$

Demostración. Sea $g \in G$. Consideremos $\rho_U : G \longmapsto GL(U)$ la representación asociada a U. Por la proposición 0.208, la transformación $\rho_U(g)$ es diagonalizable. Sea $C_U = \{u_1, \ldots, u_m\}$ una base de U formada por vectores propios de $\rho_U(g)$ con valores propios asociados $\lambda_1, \ldots, \lambda_m$, de la misma forma, sea $C_V = \{v_1, \ldots, v_n\}$ una base de V formada por vectores propios de $\rho_V(g)$ (la transformación dada por la acción de g en V) cuyos valores propios son $\mu_1, \ldots, \mu_n$, entonces

$$\begin{aligned}
\chi_U(g) := tr(\rho_U(g)) = tr\left[g\right]_{C_U} = \lambda_1 + \lambda_2 + \cdots + \lambda_m \text{ y} \\
\chi_V(g) := tr(\rho_V(g)) = tr\left[g\right]_{C_V} = \mu_1 + \mu_2 + \cdots + \mu_n.
\end{aligned}$$

Ahora, sea $\{u_i \otimes v_j\}_{ij}$ una base de $U \otimes V$, por el teorema 0.261 tenemos la acción

$$\begin{aligned}
\odot : G \times (U \otimes_{\mathbb{F}} V) &\longrightarrow U \otimes_{\mathbb{F}} V \\
(g, u_i \otimes v_j) &\longmapsto g \odot (u_i \otimes v_j) := gu_i \otimes gv_j,
\end{aligned}$$

entonces, ya que las bases constan de valores propios para todo i, j tenemos que

$$g(u_i \otimes v_j) = gu_i \otimes gv_j = \lambda_i u_i \otimes \mu_j v_j = \lambda_i \mu_j (u_i \otimes v_j).$$

Entonces la base $\{u_i \otimes v_j\}_{ij}$ es una base de vectores propios de la transformación $\rho_{U \otimes V}(g)$ definida por la acción de g en $U \otimes V$, y los valores propios asociados son $\{\lambda_i \mu_j\}_{ij}$, por lo tanto

$$\chi_{U \otimes V}(g) = \sum_{ij} \lambda_i \mu_j = \left(\sum_i \lambda_i\right)\left(\sum_j \mu_j\right) = \chi_U(g)\chi_V(g).$$

■

Proposición 0.264. *Sea U un $\mathbb{C}G$-módulo con carácter χ_U, entonces $\chi_{U^*} = \overline{\chi_U}$*

Demostración. Sea $g \in G$ y así como anteriormente en el teorema 0.263, sea $\{u_1, \ldots, u_m\}$ una base de U formada por vectores propios de $\rho_U(g)$ (la transformación dada por la acción de g en U), con valores propios asociados $\lambda_1, \ldots, \lambda_m$.
Sea $\{\varphi_1, \ldots, \varphi_m\}$ la base dual de $\{u_1, \ldots, u_m\}$, es decir, la base de U^* con la propiedad de que para cada i, $\varphi_i : U \longrightarrow \mathbb{C}$ se define, para cada j como:

$$\varphi_i(u_j) = \delta_{ij} = \begin{cases} 1 & si \quad i = j; \\ 0 & si \quad i \neq j. \end{cases}$$

Fijando algún j, tenemos que $gu_j = \lambda_j u_j$ así que $g^{-1}u_j = {\lambda_j}^{-1} u_j$ (los valores propios son distintos de cero pues $\rho_U(g)$ es invertible).
Luego, por el lema 0.208 observamos que λ_j es una raíz de la unidad por lo que ${\lambda_j}^{-1} = \overline{\lambda_j}$. Y para cualesquiera i, j tenemos por el ejemplo 0.143 que la acción de g en la base del dual está dada por

$$g\varphi_i(u_j) := \varphi_i(g^{-1}u_j) = \varphi_i(\overline{\lambda_j}u_j) = \overline{\lambda_j}\delta_{ij}$$

y por lo tanto $g\varphi_i = \overline{\lambda_j}\varphi_i$ para cada i, por lo que la base $\{\varphi_1, \ldots, \varphi_m\}$ consiste de valores propios de la transformación $\rho_{U^*}(g)$ dada por la acción de g en U^*, con respectivos valores propios $\overline{\lambda_1}, \ldots, \overline{\lambda_m}$, y por lo tanto

$$\chi_{U^*}(g) = \overline{\lambda_1} + \cdots + \overline{\lambda_m} = \overline{\lambda_1 + \cdots + \lambda_m} = \overline{\chi_U(g)}.$$

■

Corolario 0.265. *Sean U y V dos $\mathbb{C}G$-módulos con caracteres χ_U y χ_V respectivamente, entonces*

$$\chi_{Hom_{\mathbb{C}}(U,V)} = \overline{\chi_U}\chi_V.$$

Demostración. Por la proposición 0.262 $Hom_{\mathbb{C}}(U, V) \cong U^* \otimes V$ y el resultado se sigue del teorema 0.263 y la proposición 0.264. ■

Corolario 0.266. *Los caracteres virtuales de un grupo G forman un anillo.*

Demostración. Se sigue del teorema 0.263 que el producto de dos caracteres es un carácter, y para la parte de la suma del lema 0.216. ■

Teorema 0.267. ***Producto tensorial y caracteres de un producto directo.***
Sean G y H grupos con caracteres irreducibles $\chi_1, ..., \chi_r$ y $\psi_1, ..., \psi_s$ respectivamente.
Entonces $G \times H$ tiene rs caracteres irreducibles, a saber $\{\chi_i\psi_j\}_{i,j}$.

Demostración. Dados $(x, y),\ (x', y') \in G \times H$, tenemos que éstos son conjugados si y sólo si existe $(g, h) \in G \times H$ tal que $(g, h)(x, y)(g^{-1}, h^{-1}) = (x', y')$, es decir, se tiene que

$$(g, h)(x, y)(g^{-1}, h^{-1}) = (gx, hy)(g^{-1}, h^{-1}) = (gxg^{-1}, hyh^{-1}) = (x', y')$$

por lo tanto $(x, y),\ (x', y') \in G \times H$ son conjugados si y sólo si x' es conjugado de x en G y y' es conjugado de y en H. Luego, el número de clases de conjugación es igual al número de caracteres irreducibles por el teorema 0.241, luego tenemos que G y H tienen r y s clases de conjugación respectivamente, entonces concluimos que $G \times H$ tiene rs clases de conjugación, donde cada una de ellas es el producto directo de una clase de G y una clase de H, y por el mismo teorema usado

anteriormente tenemos que $G \times H$ tiene rs caracteres irreducibles.
Luego, para hallar estos rs caracteres irreducibles consideremos $S_1, \ldots, S_r$ y $T_1, \ldots, T_s$ los distintos $\mathbb{C}G$-módulos y $\mathbb{C}H$-módulos irreducibles inducidos por las representaciones irreducibles de G y H respectivamente. Para cada $1 \leq i \leq r$, $1 \leq j \leq s$ vamos a dar a $S_i \otimes T_j$ una estructura de $\mathbb{C}(G \times H)$-módulo. Para cada i sea $C_{S_i} = \{u_{i_1}, \ldots, u_{i_{f_i}}\}$ una base de S_i formada por vectores propios de $\rho_i(g)$ (esta transformación es diagonalizable) con valores propios asociados $\lambda_{i_1}, \ldots, \lambda_{i_{f_i}}$ (χ_i es el carácter de ρ_i), de la misma forma, para cada j sea $C_{T_j} = \{v_{j_1}, \ldots, v_{j_{t_j}}\}$ una base de T_j formada por vectores propios de $\rho_j(h)$ (esta transformación es diagonalizable y ψ_j es el carácter de ρ_j) con valores propios asociados $\mu_{j_1}, \ldots, \mu_{j_{t_j}}$, donde $dim_{\mathbb{C}}(S_i) = f_i$ y $dim_{\mathbb{C}}(T_j) = t_j$ entonces, por la parte (ii) de la proposición 0.209 tenemos que

$$\begin{aligned}\chi_i(g) &:= tr(\rho_i(g)) = tr\,[g]_{C_{S_i}} = \lambda_{i_1} + \lambda_{i_2} + \cdots + \lambda_{i_{f_i}} \text{ y} \\ \psi_j(h) &:= tr(\rho_j(h)) = tr\,[h]_{C_{T_j}} = \mu_{j_1} + \mu_{j_2} + \cdots + \mu_{j_{t_j}}.\end{aligned}$$

Sea $\{s_{i'} \otimes t_{j'}\}_{i'j'}$ una base de $S_i \otimes T_j$, entonces definimos la acción en la base como

$$\begin{aligned} * : (G \times H) \times (S_i \otimes T_j) &\longrightarrow S_i \otimes T_j \\ ((g,h),(s_{i'} \otimes t_{j'})) &\longmapsto (g,h) * (s_{i'} \otimes t_{j'}) = g s_{i'} \otimes h t_{j'} \end{aligned}$$

y la extendemos de manera lineal a $S_i \otimes T_j$. Luego, ya que las bases constan de valores propios para todo i, j tenemos que

$$(g,h)\left(s_{i'} \otimes t_{j'}\right) = g s_{i'} \otimes h t_{j'} = \lambda_{i'} s_{i'} \otimes \mu_{j'} t_{j'} = \lambda_{i'}\mu_{j'}(s_{i'} \otimes t_{j'}),$$

pero esto quiere decir que la base $\{s_{i'} \otimes t_{j'}\}_{i'j'}$ es una base de vectores propios de la transformación inducida por la acción de (g,h) en $S_i \otimes_{\mathbb{F}} T_j$ con valores propios $\{\lambda_{i'}\mu_{j'}\}_{i'j'}$ y por lo tanto

$$\chi_{S_i \otimes T_j}((g,h)) = \sum_{i'j'} \lambda_{i'}\mu_{j'} = \left(\sum_{i'} \lambda_{i'}\right)\left(\sum_{j'} \mu_{j'}\right) = \chi_i(g)\psi_j(h).$$

Reescribiremos para toda i, j, $\chi_{S_i \otimes T_j} := \chi_i \times \psi_j = \nu_{ij}$ para el carácter de $S_i \otimes T_j$.
Notemos que los ν_{ij} son distintos y que podemos recuperar los caracteres χ_i y ψ_j a partir de ν_{ij} restringiendo adecuadamente. Ahora calcularemos el producto interno para ver que los ν_{ij} son irreducibles. Entonces para i, j, i', j' se tiene que

$$\begin{aligned} \langle \nu_{ij}\ ,\ \nu_{i'j'} \rangle &= \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \nu_{ij}(g,h)\ \overline{\nu_{i'j'}(g,h)} \\ &= \frac{1}{|G||H|} \sum_{g \in G} \sum_{h \in H} \chi_i(g)\psi_j(h)\overline{\chi_{i'}(g)\psi_{j'}(h)} \\ &= \left(\frac{1}{|G|}\sum_{g \in G} \chi_i(g)\ \overline{\chi_{i'}(g)}\right)\ \left(\frac{1}{|H|}\sum_{h \in H} \psi_j(h)\ \overline{\psi_{j'}(h)}\right) \\ &= \langle \chi_i\ ,\ \chi_{i'} \rangle \langle \psi_j\ ,\ \psi_{j'} \rangle \\ &= \delta_{ii'}\delta_{jj'} \end{aligned}$$

por la ortogonalidad de renglones. En particular tenemos que $\langle \nu_{ij}\ ,\ \nu_{ij} \rangle = 1$ para cada i y j por lo que ν_{ij} es un carácter irreducible y $\nu_{ij} \neq \nu_{i'j'}$ para $(i,j) \neq (i',j')$ ya que en este caso ν_{ij} y $\nu_{i'j'}$ son ortogonales. Por lo tanto, los ν_{ij} son los rs caracteres irreducibles de $G \times H$, es decir, el conjunto de los caracteres irreducibles de $G \times H$ es $\{\chi_i \times \psi_j\}_{ij}$. ■

Ejemplo 0.268. Caracteres irreducibles del grupo de Klein.
Sea G el grupo de Klein, es decir $G = \mathbf{V} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \langle a, b\rangle$, donde $a = (12)(34)$ y $b = (13)(24)$ tienen orden 2 y por el ejemplo 0.205, sus 4 caracteres irreducibles corresponden todos los posibles morfismos de grupos de V en $\mathbb{C}^*$, y ya que los generadores tienen orden 2, sus imágenes bajo estos morfismos de grupos tienen orden menor o igual que 2, entonces, estas posibles imágenes de los generadores pueden ser sólo 1 y -1 y las combinaciones que tengan, que corresponden a los pares ordenados

$$(1,1),\ (1,-1),\ (-1,1) \text{ y } (-1,-1),$$

es decir, las representaciones irreducibles de V corresponden a los morfismos

$$\begin{array}{rcl|rcl|rcl|rcl} \chi_1 : V & \longrightarrow & \mathbb{C}^*, & \chi_2 : V & \longrightarrow & \mathbb{C}^*, & \chi_3 : V & \longrightarrow & \mathbb{C}^*, & \chi_4 : V & \longrightarrow & \mathbb{C}^* \\ a & \longmapsto & 1 & a & \longmapsto & 1 & a & \longmapsto & -1 & a & \longmapsto & -1 \\ b & \longmapsto & 1 & b & \longmapsto & -1 & b & \longmapsto & 1 & b & \longmapsto & -1 \end{array}$$

y por lo tanto la tabla de caracteres de V es

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Aquí, la segunda y tercera columna corresponden a los pares ordenados dados anteriormente y la cuarta columna es determinada las dos columnas previas, correspondiéndose con el hecho de que el cuarto elemento (o cualquiera distinto del neutro) es el producto de los otros dos elementos no identidad en el grupo de Klein.

Sabemos que sólo existen dos grupos no abelianos de orden 8 salvo isomorfismo, los grupos D_8 y Q, los detalles de éste resultado se pueden consultar en [20]. Los siguientes ejemplos describen algunas de sus representaciones.

Ejemplo 0.269. Caracteres del grupo de cuaterniones Consideremos el grupo de los cuaterniones unitarios

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Notemos que $Z(Q) = \{\pm 1\}$, de hecho, el subgrupo conmutador de Q en este caso coincide con el centro, y tenemos que

$$Q/\{\pm 1\} = \big\{\{\pm 1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}\big\} \cong \mathbf{V},$$

donde $\mathbf{V}$ es el grupo de Klein que es abeliano (de hecho todo grupo cociente de un grupo con su conmutador es abeliano). Así, por el teorema 0.184, $V \cong Q/\{\pm 1\}$ tiene 4 representaciones ρ_i $(1 \leqslant i \leqslant 4)$ de grado 1, necesariamente irreducibles, y si $\pi : Q \longrightarrow Q/\{\pm 1\}$ es la proyección canónica se tiene que $\rho_i \circ \pi = \psi_i$ son 4 representaciones de grado 1 de Q pues ψ_i es el pullback de ρ_i bajo π para toda i.
Luego, recordemos que por el ejemplo 0.39 existe un monomorfismo de grupos

$$\begin{array}{rcl} \tau : Q & \longrightarrow & GL_2(\mathbb{C}) \\ i^r j^s & \longmapsto & A^r B^s \end{array}$$

donde $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ y $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ y $0 \leq r \leqslant 3$, $0 \leq s \leqslant 1$, por lo tanto

$$Q \cong Im(\tau) = \langle A, B \rangle = Q_8.$$

Así, τ es una representación fiel de Q_8 de grado 2 sobre $\mathbb{C}$, la correspondencia completa es:

$$\begin{array}{rcl} \tau(\pm 1) & = & \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \quad \tau(\pm i) = \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix} \\ \tau(\pm j) & = & \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}, \quad \tau(\pm k) = \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}. \end{array}$$

Ahora, si χ_τ es el carácter de la representación τ, entonces sus valores están dados por

$$\begin{array}{c} \chi_\tau(1) = 2, \ \ \chi_\tau(-1) = -2, \ \ \chi_\tau(i) = 0, \ \ \chi_\tau(-i) = 0, \\ \chi_\tau(j) = 0, \ \ \chi_\tau(-j) = 0, \ \ \chi_\tau(k) = 0, \ \ \chi_\tau(-k) = 0. \end{array}$$

Luego, los caracteres irreducibles de Q son tantos como las clases de conjugación de Q, que son

$$\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}.$$

Vimos en el ejemplo anterior que la tabla de caracteres del grupo de Klein es:

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Por lo anterior tenemos que $\chi_i = \psi_i$ para toda i, y entonces, la tabla de caracteres de Q es

${x_i}^Q$	1	1	2	2	2
x_i	1	-1	i	j	k
ψ_1	1	1	1	1	1
ψ_2	1	1	1	-1	-1
ψ_3	1	1	-1	1	-1
ψ_4	1	1	-1	-1	1
χ_τ	2	-2	0	0	0

Ejemplo 0.270. Caracteres del grupo dihédrico de orden 8. Sea $\mathbb{F} = \mathbb{C}$ y consideremos el grupo dihédrico de orden 8

$$D_8 = \langle x, y \mid x^4 = 1, y^2 = 1, xy = yx^{-1} \rangle.$$

Por el ejemplo 0.40 teníamos un monomorfismo

$$\begin{array}{rcl} \phi : D_8 & \longrightarrow & GL_2(\mathbb{C}) \\ x^i y^j & \longmapsto & A^i B^j, \end{array}$$

es decir, ϕ es una representación fiel de grado 2 de G, la correspondencia es

1. $r_0 = (1) = 1 \longmapsto I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ es la rotación de cero grados.
2. $r_1 = (1234) = x \longmapsto A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ es la rotación de 90 grados.
3. $r_2 = (13)(24) = x^2 \longmapsto -I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ es la rotación de 180 grados.
4. $r_3 = (1432) = x^3 \mapsto A^3 = -A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ es la rotación de 270 grados.
5. $m_1 = (12)(34) = y \mapsto B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ es la reflexión en el eje Y.
6. $d_1 = (13) = xy \mapsto AB = \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right)$ es la reflexión respecto a la identidad negativa.
7. $m_2 = (14)(23) = x^2 y \mapsto A^2 B = -B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ es la reflexión respecto al eje X.
8. $d_2 = (24) = x^3 y \longmapsto A^3 B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ es la reflexión respecto a gráfica de la identidad.

Si χ_ϕ es el carácter de D_8 de grado 2 asociado a la representación ϕ entonces sus valores son

$$\chi_\phi(e) = 2, \ \ \chi_\phi(x) = 0, \ \ \chi_\phi(x^2) = -2, \ \ \chi_\phi(x^3) = 0,$$
$$\chi_\phi(y) = 0, \ \ \chi_\phi(xy) = 0, \ \ \chi_\phi(x^2 y) = 0, \ \ \chi_\phi(x^3 y) = 0.$$

Luego, ϕ es una representación irreducible para ya que no existen subespacios de dimensión 1 porque la rotación A no manda una líneal en $\mathbb{R}^2$ en sí misma, entonces ya conocemos un carácter irreducible de D_8 de grado 2 dado por la representación ϕ. Vamos a encontrar el resto de los caracteres irreducibles de D_8, sabemos que debemos hallar 4 pues existen 5 clases de conjugación de D_8 que son:

$$\{1\}, \{x^2\}, \{x, x^3\}, \{y, x^2 y\}, \{xy, x^3 y\},$$

pues podemos ver a D_8 dentro de S_4 con la correspondecia

$$\{(1)\}, \{(13)(24)\}, \{(1234), (1432)\}, \{(13), (24)\}, \{(14)(23), (12)(34)\}.$$

Para hallar estos caracteres vamos a hacer los pullbacks de los caracteres de un cociente de D_8 (estos pullbacks no son más que los levantamientos de los caracteres del grupo $D_8/{D_8}'$). Más claramente consideremos el subgrupo $H = \{e, x^2\}$, un cálculo que no haremos aquí muestra que el sugrupo conmutador ${D_8}'$ de D_8 es precisamente el sugrupo H, por lo que existen tantos caracteres lineales lineales de D_8 como $|D_8/{D_8}'|$ por el teorema 0.257, es decir, 4 (el número que nos falta).
Entonces, $D_8/{D_8}' = \{{D_8}', x{D_8}', y{D_8}', xy{D_8}'\}$ es un grupo abeliano de orden 4 por lo que tiene 4 representaciones de grado 1, $\chi_i : D_8/{D_8}' \longrightarrow \mathbb{C}^*$ y si $\pi_i : D_8 \longrightarrow D_8/{D_8}'$ es la proyección canónica, entonces la composición $\chi_i \circ \pi = \psi_i$ es una representación de grado 1 de D_8. Luego, estas representaciones están dadas por las representaciones del grupo de Klein pues $D_8/{D_8}' \cong V$, estas estaban dadas por

$$\begin{array}{rcl} \chi_1 : D_8/{D_8}' & \longrightarrow & \mathbb{C}^*, \\ a & \longmapsto & 1 \\ b & \longmapsto & 1 \end{array} \qquad \begin{array}{rcl} \chi_2 : D_8/{D_8}' & \longrightarrow & \mathbb{C}^*, \\ a & \longmapsto & 1 \\ b & \longmapsto & -1 \end{array}$$

$$\begin{array}{rcl} \chi_3 : D_8/{D_8}' & \longrightarrow & \mathbb{C}^*, \\ a & \longmapsto & -1 \\ b & \longmapsto & 1 \end{array} \qquad \begin{array}{rcl} \chi_4 : D_8/{D_8}' & \longrightarrow & \mathbb{C}^* \\ a & \longmapsto & -1 \\ b & \longmapsto & -1 \end{array}$$

Así, la tabla de caracteres de D_8 es

${x_i}^{D_8}$	1	1	2	2	2
x_i	1	x^2	x	y	xy
ψ_1	1	1	1	1	1
ψ_2	1	1	1	-1	-1
ψ_3	1	1	-1	1	-1
ψ_4	1	1	-1	-1	1
χ_ϕ	2	-2	0	0	0

En general, para el grupo dihédrico de orden $2n$, es decir, el grupo de simetrías de un polígono regular de n lados en el plano complejo

$$G = D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, xy = yx^{-1} \rangle$$

entonces existe una representación de ρ de D_{2n} sobre $\mathbb{C}$ dada por

$$\rho(x) = A = \begin{pmatrix} cos\left(\frac{2\pi}{n}\right) & -sen\left(\frac{2\pi}{n}\right) \\ sen\left(\frac{2\pi}{n}\right) & cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \quad \rho(y) = B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

donde A es una rotación de $\frac{2\pi}{n}$ radianes alrededor del origen en el sentido contrario de la manecillas del reloj y B una reflexión respecto al eje Y. Esta representación ρ es fiel y es irreducible para $n \geqslant 3$ porque no existen subespacios de dimensión 1 ya que la rotación A no manda una líneal en $\mathbb{R}^2$ en sí misma.

Observación 0.271. Si la tabla de caracteres de un grupo nos da información importante acerca del grupo, de los dos ejemplos anteriores podemos responder inmediatamente a la siguiente pregunta fundamental:

¿Si dos grupos tienen la misma tabla de caracteres entonces necesariamente son isomorfos?

La respuesta es que no, pues Q y D_8 tienen la misma tabla de caracteres y es bien sabido que no son isomorfos.

Dualidad de Pontryagin

Ejemplo 0.272. Representaciones de grupos cíclicos.
Sea $G = \mathbb{Z}_n \cong \langle g \rangle$ el grupo cíclico de orden n, por el teorema 0.184 tiene exactamente n representaciones de grado 1 y son todas. Consideremos

$$\begin{array}{rcl} \rho : \mathbb{Z}_n & \longrightarrow & GL_1(\mathbb{C}) \cong \mathbb{C}^* \\ g & \longmapsto & z \end{array}$$

para algún $z \in \mathbb{C}^*$ cualquier representación de grado 1 de $\mathbb{Z}_n$, entonces, ya que ρ es morfismo de grupos tenemos que

$$\rho(g^m) = \rho(g)^m = z^m \text{ para todo } g^m \in \mathbb{Z}_n,$$

es decir, ρ está completamente determinada por su valor en el generador g. Esto de hecho es consecuencia de que cualquier morfismo de grupos que tenga como dominio un grupo cíclico está completamente determinado por la imagen de un generador. Luego, como g es generador de $\mathbb{Z}_n$ tenemos que $g^n = 1_G \equiv [1]$ y por lo tanto

$$\rho(g^n) = \rho(g)^n = z^n = 1_{\mathbb{C}}$$

y esto sólo sucede si y sólo si z es una raíz n-ésima de la unidad, por lo que hay n posibles imágenes para z, que son las n distintas raíces n-ésimas de la unidad. Así, concluimos que cada raíz n-ésima de la unidad nos da una representación de grado 1 de $\mathbb{Z}_n$, y hay n de éstas, cómo habíamos dicho, cada una de ellas se determina enviando al generador a las diferentes raíces n-ésimas de la unidad. Más claramente, si $\mu_n = \langle \zeta \rangle \subset S^1$ es el grupo de las raíces n-ésimas de la unidad bajo el producto en $\mathbb{C}$, con $\zeta = e^{\frac{2\pi i}{n}}$ una raíz n-ésima primitiva de la unidad, toda raíz n-ésima es potencia de ζ y éste es un grupo cíclico de orden n y por tanto isomorfo a $\mathbb{Z}_n$. Por lo que tenemos que todas las representaciones de $\mathbb{Z}_n$ están dadas por

$$\begin{array}{rcl} \theta_k : \mathbb{Z}_n & \longrightarrow & GL_1(\mathbb{C}) \cong \mathbb{C}^* \\ g & \longmapsto & \zeta^k \end{array} \quad , \ 0 \leqslant k \leqslant n-1,$$

que son precisamente las representaciones del ejemplo 0.134.
Luego, los caracteres asociados a estas n representaciones θ_k están dados por

$$\begin{array}{rcl} \chi_{\theta_k} : \mathbb{Z}_n & \longrightarrow & \mathbb{C}^* \\ g^m & \longmapsto & tr(\theta_k(g^m)) = tr(\zeta^{km}) = \zeta^{km} \end{array}$$

con $0 \leq m \leq n-1$ y $0 \leq k \leq n-1$, y por lo tanto $\chi_{\theta_k} = \theta_k$, cosa que sucede siempre para caracteres lineales, pues son morfismos de grupos por el ejemplo 0.205 Así, existen n caracteres lineales distintos para $\mathbb{Z}_n$ y para todo k, χ_{θ_k} está bien definido pues si $g^r = g^s$, con r y s enteros, entonces $[r] \equiv [s]$ mód n y por lo tanto $\zeta^{kr} = \zeta^{ks}$.

Luego, para la representación regular $\mathbb{C}(\mathbb{Z}_n)$ tenemos un isomorfismo

$$\mathbb{C}(\mathbb{Z}_n) \cong \theta_0 \oplus \theta_1 \oplus \cdots \oplus \theta_{n-1}$$

pues en la base $\{e, g, g^2, \ldots, g^{n-1}\}$ de $\mathbb{C}(\mathbb{Z}_n)$ tenemos que

$$\sigma(g) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

que no es más que la matriz compañera del polinomio $x^n - 1$, por lo tanto

$$m_{\sigma(g)}(x) = c_{\sigma(g)}(x) = x^n - 1.$$

Ya que $\mathbb{C}$ es algebraicamente cerrado, el polinomio $x^n - 1$ se descompone en n distintos factores lineales en $\mathbb{C}$, es decir,

$$x^n - 1 = \prod_{k=0}^{n-1} (x - \zeta^k),$$

por lo tanto, $\sigma(g)$ es diagonalizable y los elementos de la diagonal (valores propios) son $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, luego, cada espacio propio asociado a un valor propio es un $\mathbb{C}(\mathbb{Z}_n)$-submódulo y por lo tanto se sigue el resultado.

Definición 0.273. *Sea G un grupo abeliano finito, llamamos al conjunto de morfismos $\phi : G \longrightarrow S^1$ con el producto puntual de funciones* ***el grupo dual*** *o* ***el grupo caracteres*** *de G. Denotaremos al grupo dual de G como $\widehat{G}$.*

Observación 0.274. El carácter trivial de G es el neutro del grupo dual, y el inverso de cada carácter es el carácter conjugado. Además $\widehat{G}$ es abeliano pues el producto en $\mathbb{C}^*$ es conmutativo.

El siguiente teorema se conoce como Dualidad de Pontryagin, que es cierto para cualquier grupo abeliano (ver [6]), pero únicamente haremos la prueba para grupos cíclicos.

Teorema 0.275. *El grupo dual de un grupo cíclico de orden n es también cíclico de orden n bajo el producto de carácteres, es decir,*

$$G \cong \widehat{G}.$$

Demostración. Sin perdida de generalidad sea $G = \mathbb{Z}_n$. Vamos a ver que $\widehat{G}$ es cíclico, para esto debemos encontrar un generador, que proponemos canónicamente como el carácter

$$\begin{array}{rcl} \chi : \mathbb{Z}_n & \longrightarrow & \mu_n \subset \mathbb{S}^1 \subset \mathbb{C}^* \\ g & \longmapsto & \zeta = e^{\frac{2\pi i}{n}}. \end{array}$$

es decir, $\chi(g^m) \longmapsto e^{\frac{2\pi i}{n} m}$ para todo entero m. Luego, sean $\{\chi_0, \ldots, \chi_{n-1}\}$ los caracteres irreducibles de G dados en el ejemplo 0.272, así, $\chi = \chi_1$, y en general para $\psi \in \{\chi_0, \ldots, \chi_{n-1}\}$ se tiene que $\psi(g) = e^{\frac{2\pi i}{n} j}$ para algún $0 \leq j \leq n-1$, por lo tanto $\psi(g) = \chi(g)^j = e^{\frac{2\pi i}{n} j} = \zeta^j$, entonces

$$\psi(g^m) = \psi(g)^m = (\zeta^j)^m = \zeta^{mj} = \chi(g)^{mj} = \chi(g^m)^j$$

que muestra que $\psi = \chi^j$. Por lo tanto χ genera a $\widehat{G}$.
Entonces el conjunto de los caracteres irreducibles de G, $\{\chi_1, \ldots, \chi_n\}$ es un grupo cíclico bajo el producto de caracteres, su generador es χ_1 ya que $\chi_j = {\chi_1}^j$ para todo $0 \leq j \leq n-1$. Si cambiamos el generador, el isomorfismo cambiará.
En resumen, para cada $0 \leq k \leq n-1$ sea V_k el $\mathbb{C}\mathbb{Z}_n$-módulo inducido de grado 1 por la representación θ_k, es decir, $V_k \cong \mathbb{C}$ y sea g actuando en V_k por multiplicación por ζ^k, y ya que G es cíclico, esta definición (acción) determina completamente una estructura de $\mathbb{C}G$-módulo en V_k. Cada V_k es un $\mathbb{C}G$-módulo irreducible pues es de dimensión 1.

Luego, si χ_k es el carácter de V_k entonces su valor en el generador es $\chi_k(g) = \zeta^k$, por lo que $\chi_k(g^m) = \zeta^{mk}$ para todo $0 \leq m \leq n-1$.

Y entonces la tabla de caracteres de G es

	1	1	1	$\cdots$	1
	1	g	g^2	$\cdots$	g^{n-1}
χ_0	1	1	1	$\cdots$	1
χ_1	1	ζ	ζ^2	$\cdots$	ζ^{n-1}
χ_2	1	ζ^2	ζ^4	$\cdots$	ζ^{n-2}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_{n-1}	1	ζ^{n-1}	ζ^{n-2}	$\cdots$	ζ

■

Ejemplo 0.276. Para ilustrar el teorema anterior hagamos la tabla de caracteres *del* grupo cíclico de orden 4 (recordemos que sólo hay uno salvo isomorfismo). Sea σ su generador, de hecho podemos identificar a σ con i porque i es raíz cuarta primitiva de la unidad, entonces tenemos que $\sigma^4 = 1$, por lo que para cualquier carácter χ de G tenemos que $\chi(\sigma^4) = \chi(\sigma)^4 = 1$ y así el valor de χ en σ sólo tiene 4 posibilidades, a saber, $\{1, i, -1, -i\} = \langle\sigma\rangle$, que son precisamente las raíces cuartas de la unidad, y ya sabemos que χ está completamente determinado por su valor en σ, entonces la tabla de caracteres del grupo cíclico de orden 4 es

	1	1	1	1
	1	σ	σ^2	σ^3
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

luego el conjunto $\{1_G, \chi_2, \chi_3, \chi_4\}$ es un grupo cíclico bajo el producto de caracteres, su generador es χ_1 ya que $\chi_k = {\chi_1}^k$ para todo $0 \leq k \leq 3$.

El **doble dual** de un grupo G es el grupo dual de $\widehat{G}$ y se denota por $\widehat{\widehat{G}}$, y ya que $G \cong \widehat{G}$ tenemos que $G \cong \widehat{\widehat{G}}$. Sin embargo no hay una manera natural de dar el isomorfismo entre G y $\widehat{G}$, pero sí la hay para G y $\widehat{\widehat{G}}$, ésta consiste de la función evaluación.

Teorema 0.277. *Si G es un grupo cíclico finito entonces existe un isomorfismo natural*

$$G \cong \widehat{\widehat{G}}$$

Demostración. Consideremos la función evaluación en g para todo $g \in G$:

$$\begin{array}{rcl} \Phi : G & \longrightarrow & \widehat{\widehat{G}} \\ g & \longmapsto & \phi_g \end{array} \quad \text{donde} \quad \begin{array}{rcl} \phi_g : \widehat{G} & \longrightarrow & \mathbb{S}^1 \\ \chi & \longmapsto & \chi(g) \end{array} \quad \text{y} \quad \begin{array}{rcl} \chi : G & \longrightarrow & \mathbb{S}^1 \\ g & \longmapsto & \chi(g). \end{array}$$

Entonces ϕ_g es un carácter de $\widehat{G}$. Por lo tanto, el grupo doble dual de un grupo cíclico de orden n es isomorfo al grupo. ■

Observación 0.278. El isomorfismo entre el grupo doble dual un grupo de cíclico de orden n y el grupo es conocido como **Dualidad de Pontryagin**, que es un resultado más general donde podemos cambiar la hipótesis de que G sea cíclico por la de ser abeliano finito. El isomorfismo en la Dualidad

de Pontryagin es natural porque no depende de elección, como lo hace el isomorfismo entre el grupo y su dual, que si depende de a qué raíz n-ésima de la unidad mandemos al generador.

Un grupo abeliano finito es isomorfo a su grupo dual, aunque no en un camino natural, pero naturalmente isomorfo a su doble dual, y eso hace que podamos pensar a cualquier grupo abeliano finito como su doble dual.

Bibliografía

[1] Adkins W.A., Weintraub S.H., *Algebra: An Approach via Module Theory*, Springer-Verlag, Nueva York, 1992.

[2] Alperin J.L., Bell R.B., *Groups and Representations*, Springer-Verlag, Nueva York, 1995.

[3] Anderson F.W., Fuller K.R., *Rings and Categories of Modules*, Springer-Verlag, Nueva York, 1992.

[4] Beachy J. A., *Introductory Lectures on Rings and Modules*, Cambridge University Press, United Kingdom First Edition, 1999.

[5] Butler R.C., *A quick introduction to finite representations*, http://www.math.utah.edu/ rbutler/ Representations/Representations.pdf.

[6] Conrad K., *Characters of finite abelian groups*, http://www.math.uconn.edu / kconrad/blurbs /grouptheory/charthy.pdf.

[7] Etingof P., Golberg O., Hensel S., Liu T, Schwendner A., Vaintrob D., Yudovina E., *Introduction to representation theory*, January 10, 2011, http://math.mit.edu/ etingof/replect.pdf.

[8] Evseev A., *Character theory of finite groups: Concise lecture notes, lectures 1–24*, January–March 2009, http://web.mat.bham.ac.uk/ A.Evseev/pdf/characters1.pdf.

[9] Fraleigh. J.B, *A First Course in Abstract Algebra*, Pearson Education, U.S.A, Seventh Edition, 1975.

[10] Friedberg S. H, , *Álgebra Lineal*, Publicaciones Cultura, S.A. Primera edición, México, 1992

[11] Fulton W., Harris J., *Representation Theory: A First Course*, Springer-Verlag, New York.

[12] Hill M.A., *Irreducible representations of* $GL_2(\mathbb{F}_q)$, http://math.harvard.edu /archive/126 fall 98/papers /mahill.pdf.

[13] James G., Liebeck M., *Representations and Characters of Groups*, Cambridge University Press, United Kingdom, Second Edition, 2001.

[14] Lent C.T., *Representation theory*, 2005, https://math.berkeley. edu/ teleman/math/RepThry.pdf.

[15] Martin S., *Representation theory*, 2009, https://www.dpmms.cam.ac.uk /study/II /RepresentationTheory /2010-2011/Representation Theory.pdf.

[16] Mohammed A.B., *Character tables of general linear group and some of its subgroups*, School of mathematical sciences, University of KwaZulu-Natal, Pietermaritzburg, South Africa, November 2008, https://www.researchgate.net /publication/277053785 Character tables of the general linear group and some of its subgroups.

[17] Panyushev D.I., *Lectures on representations of finite groups and invariant theory*, Independent university of Moscow, http://www.mccme.ru/ panyush/lecturesRT.pdf.

[18] Reeder M., *Notes on representations of finite groups*, November 2014, https://www2.bc.edu / reederma/RepThy.pdf.

[19] Rotman, J.J., *Advanced Modern Algebra*, Pearson Education, New Jersey, 2002.

[20] Sahai V., Bist V., *Algebra*, Alpha Science International Ltd., India, 2008.

[21] Sahai V., Bist V., *Linear Algebra*, Alpha Science International Ltd., India, 2002.

[22] Souvignier B., *Groups and representations*, January 2010, http://www.math.ru.nl/ souvi/rep 10/syllabus.pdf.

[23] Stentrom B., *Rings of Quotients*, Springer-Verlag, Nueva York, 1975.

[24] Vargas C., *Relaciones entre probabilidad libre y representaciones de grupos*, división de ciencias naturales y exactas, departamento de matemáticas, Universidad de Guanajuato, Junio 2009, http://www.cimat.mx/ pabreu/TesisCarlosVargas.pdf.

[25] Weintraub S.H., *Representation Theory of Finite Groups: Algebra and Arithmetic*, American Mathematical Society, U.S.A., 2003.

[26] Yafaev A., *Group algebras*, http://www.ucl.ac.uk/ ucahaya/GroupAlgebras.pdf.

[27] Zaldívar F., *Introducción a la Teoría de Grupos*, Sociedad Matemática Mexicana-Instituto de Matemáticas-UNAM-Universidad Autónoma Metropolitana-Reverté Ediciones, México D.F.,1a Reimpresión, 2009.