Curso de Álgebra Moderna

Ángel Zaldivar

July 6, 2020

Contenido

Introducción

esta seccion

Capítulo 1

Teoría de grupos

1.1 Acciones de grupo

En un grupo G su operación binaria es una función definida en $G \times G \longrightarrow G$ que asigna a cada par (σ, τ) de elementos de G el único elemento $\sigma\tau \in G$. Generalizando lo anterior, si G es un grupo y Y es un conjunto no vacío, una acción de G en Y es una función

$$* : G \times Y \longrightarrow G$$

Como G es un grupo, es natural pedir que esta acción satisfaga las propiedades siguientes:

1. Si e es el neutro de G, entonces para todo $x \in Y$ se tiene $e * x)x$.

2. Si $\sigma\tau \in G$ y $x \in Y$, entonces $(\sigma\tau) * x) = \sigma * (\tau * x)$.

Ejemplo Si Y es cualquier conjunto no vacío, sea $* : G \times Y \longrightarrow G$ dada por $\sigma * x = x$ es una acción de grupo y decimos que G actúa trivialmente en Y

Ejemplo Si Y es cualquier conjunto no vacío, consideremos $G = S_Y$ el grupo de permutaciones de Y.Sea $* : G \times Y \longrightarrow G$ dada por $\sigma * x = \sigma(x)$ (esto es, la función σ calculada en x) entonces G actúa sobre Y permutando sus elementos.

Ejemplo Sea G cualquier grupo y se $H \subseteq G$ un subgrupo de G. Entonces H actúa sobre G mediante el producto de G, es decir, $* : H \times G \longrightarrow G$ dada por $h * \sigma = h\sigma$ (traslación izquierda). En el caso particular en el que consideramos $H = G$ se tiene que el grupo actúa sobre sí mismo.

Ejemplo Si V es un k-espacio vectorial entonces

$$* : k \times V \longrightarrow V$$

es una acción

Ejemplo Si M es un grupo abeliano y R es un anillo (asociativo con unidad) entonces si existe una acción de

$$* : R \times M \longrightarrow M$$

diremos que M es un R-módulo izquierdo

Sea M un grupo abeliano y consideremos la siguiente situación:

$$* : \mathbf{Z} \times M \longrightarrow M \quad (n, m) \longrightarrow n * m$$

Donde $n * m = m + ... + m$ n veces. Observemos los siguiente sea $n_1, n_2 \in \mathbf{Z}$ y $m \in M$

$$\begin{aligned}
(n_1 n_2) * m_1 = &= (n_1 n_2) * m_1 \quad M \quad grupo \quad abeliano \\
&= n_1(n_2 m_1) \\
&= n_1(n_2 * m_1) \quad Como \quad n_2 * m_1 \in M \\
&= n_1 * (n_2 * m_1)
\end{aligned}$$

Además

$$e * m = em = m$$

De este modo por obtenemos el siguiente resultado

Proposición 1.1.1 *Todo grupo abeliano es un* $\mathbf{Z}$*-módulo es una acción*

Definición Un conjunto X con una acción de un grupo G se llama G-conjunto

Notemos lo siguiente, si X es un G-conjunto es decir

$$* : G \times X \longrightarrow X$$

Consideremos

$$S_X = f : X \longrightarrow X | fesbiyectiva$$

Definamos

$$\rho_* : G \longrightarrow S_X$$

$$\rho_*(g)(x) = g * x$$

Afirmación $\rho_*(g)$ así definida es biyectiva $\forall g \in G$.
Decimos $\rho_*(g^{-1})$ es la inversa de $\rho_*(g)$ ya que

$$\begin{aligned}(\rho_*(g) \circ \rho_*(g^{-1})(x) &= \rho_*(\rho_*(g^{-1}(x) \\ &= \rho_*(g^{-1} * x) \\ &= g * (g^{-1} * x) \\ &= (gg^{-1}) * x \\ &= e * x \\ &= x\end{aligned}$$

Además notemos ρ_* es morfismo de grupos:
Si $g_1, g_2 \in G$ entonces

$$\rho_*(g_1 g_2) : X \longrightarrow X$$

$$\begin{aligned}(\rho_*(g_1 g_2)(x) &= (g_1 g_2) * x \\ &= g_1 * (g_2 * x) \\ &= g_1 * (\rho_*(g_2)(x)) \\ &= \rho_*(g_1)(\rho_*(g_2)(x)) \\ &= (\rho_*(g_1) \circ \rho_*(g_2))(x)\end{aligned}$$

y también

$$(\rho_*(e)(x) = e * x = x$$

esto ultimo porque $*$ ya es acción.

Ahora supongamos tenemos

$$\rho_* : G \longrightarrow S_X$$

un morfismo,definimos una acción

$$*_\rho : G \times X$$

$$(g, x) \longrightarrow g *_\rho x = \rho(g)(x)$$

Afirmación $*_\rho$ es una acción de G en X

$$\begin{aligned}(g_1 g_2) *_\rho x &= \rho(g_1 g_2)(x) \\ &= \rho(g_1)\rho(g_2 x) \\ &= \rho(g_1)(g_2 *_\rho x) \\ &= g_1 *_\rho (g_2 *_\rho x)\end{aligned}$$

$$e *_\rho x = (\rho_*(e)(x) = e * x = x$$

Si $*: G \times X \longrightarrow X$ es una acción, entonces nos define un morfismo

$$\begin{aligned}(g_1g_2) *_\rho x &= \rho(g_1g_2)(x)\\ &= \rho(g_1)\rho(g_2x)\\ &= \rho(g_1)(g_2 *_\rho x)\\ &= g_1 *_\rho (g_2 *_\rho x)\end{aligned}$$

$\rho_* : G \longrightarrow S_X \; g \longrightarrow \rho(g) : X \longrightarrow X \; x \longrightarrow x$

Si $\rho : G \longrightarrow S_X$ es un morfismo entonces $*_\rho : G \times X \longrightarrow gX \; (g, x) \longrightarrow g\rho(g)(x) = g * x$ nos define una acción.

Esto nos lleva a lo siguiente:

Una acción $*$ sobre un grupo G y un conjunto X nos define morfismos biyectivos $\rho : G \longrightarrow gS_X$ y viceversa.

Si k es un campo y V un k-espacio vectorial $Gl(V) = \{T : V \to V \mid T\}$ es operador lineal invertible Notemos que $dim_k(V) = n < \infty$. Sea B una base de V. $B = v_1, ..., v_n$ en $[T]_B$ entonces $T(v_j) = \sum_{i=1}^{n} a_{ij}vj \longrightarrow g(a_{ij})$ Considerando $det(a_{ij}) \neq 0$

$Gl(V)$ es un grupo con la composición

Si $Gl(n, k) = m \in M_{n\times n}|det(m) \neq 0$ tenemos una función $\rho : Gl(V) \longrightarrow Gl(n, k) \; T \longrightarrow [T]_B$ Con la base B fija, veamos ρ es un isomorfismo.

Sean B base de V y $T_1, T_2 \in Gl(V)$ y $v \in V$ entonces

$$\begin{aligned}\rho((t_1 + T_2)(v)) &= [T_1 + T_2]_B(v)\\ &= ([T_1]_B + [T_2]_B)(v)\\ &= [T_1]_B(v) + [T_2]_B(v)\\ &= \rho(T_1(v)) + \rho(T_2(v))\end{aligned}$$

Entonces

$$Gl(V) \cong Gl(n, k)$$

$$*: Gl(n, k) \times V(A, v) \longrightarrow T_A(v) \tag{1.1}$$

notemos que tiene lo siguiente:

$$(I_n, v) \longrightarrow I_n * v = I_nv = v \tag{1.2}$$

Sean $A, B \in Gl(n, k)$ entonces

$$\begin{aligned}(AB) * v &= T_{AB}(v)\\ &= (T_A \circ T_B)(v)\\ &= A * (T_B)(v))\\ &= A * (B * v)\end{aligned}$$

De este modo concluimos que $Gl(n,k)$ actúa en V Además sea $A \in Gl(n,k)$ y $v, w \in V$

$$\begin{aligned}(A) * (v + w) &= T_A(v + w)\\ &= T_A(v) + T_A(w)\\ &= A * v + A * w\end{aligned}$$

y si $\lambda \in k$, $A \in Gl(n,k)$ tenemos

$$\begin{aligned}(A) * (\lambda v) &= T_A(\lambda v)\\ &= \lambda T_A(v)\\ &= \lambda(A * v)\end{aligned}$$

es decir, respeta la estructura e V la acción $*$, esto nos lleva a la siguiente:

Definición Sea G un grupo y V un k-espacio vectorial ($dim_k(V) < \infty$) una acción lineal de G en V es una función $* : G \times V \longrightarrow V$ tal que $*$ es una acción que cumple lo siguiente:

1) $e * v = v$
2) $(\sigma\tau) * v = \sigma * (\tau * v)$
3) $\sigma * (v + w) = \sigma * v + \sigma * w$
4) $\sigma * (\lambda v) = \lambda(\sigma * v)$

Para todo $\sigma, \tau \in G$, $\lambda \in k$ y $v \in V$. Se dice entonces que V es un G espacio vectorial de dimensión finita

Observación Si V es un espacio vectorial y G un grupo entonces diremos V es un G espacio

De este modo hemos obtenido un resultado que nos relaciona las acciones lineales con los isomorfismos de G en $Gl(V)$, es decir:

$$Acclin(G \times V, V) \cong Hom(G, Gl(V))$$

1.2 Puntos fijos

Si un grupo G actúa sobre un conjunto Y, interesa saber cómo ”mueve” G a los elementos de Y y para ésto suele ser útil estudiar los elementos de Y que no se ”mueven”, es decir, que permanecen fijos bajo la acción de G, para ello consideremos lo siguiente:

Definición Sea $\sigma \in G$, el conjunto Y^{σ} de los puntos fijos de σ está dado por $Y^{\sigma} := \{x \in Y : \sigma * x = x\} \subseteq Y$ Es decir, los elementos de Y que permanecen fijos bajo la acción σ

Definición Sea $x \in Y$, consideremos el subconjunto de elementos del grupo G que dejan fijos a x como $G_x := \{\sigma \in G : \sigma * x = x\} \subseteq G$ El conjunto G_x se llama el subgrupo de isotropía o estabilizador de x

En la definición mencionamos G_x es subgrupo este es un resultado que veremos en el siguiente lema:

Lema 1.2.1 *G_x es un subgrupo del grupo G*

Demostración: Claramente $e \in G_x$ ya que $e * x = x$.
Si $\sigma, \tau \in G_x$, entonces $(\sigma\tau) * x = \sigma * (\tau * x) = \sigma * x = x$ y por tanto $\sigma\tau \in G_x$.
Finalmente, si $\sigma \in G_x$, entonces $\sigma^{-1} * x = \sigma^{-1} * (\sigma * x) = (\sigma^{-1}\sigma) * x = e * x = x$ y así $\sigma^{-1} \in G_x$

1.3 Representaciones Lineales de Grupos Finitos

Definición Sea V un G-espacio vectorial una representación de G en V es un morfismo

$$\rho : G \longrightarrow Gl(V)$$

Observación

- Nuestros grupos serán finitos y nuestro espacio vectorial de $\mathbf{C}$-espacio vectorial.
- A la dimensión de V se le llama el grado de la representación
- Diremos V es un espacio de representación para G o que V es una representación de G.

Si fijamos una base de V $B = v_1, ..., v_n$ tenemos

$$\rho : G \longrightarrow Gl(V) \cong Gl(n, \mathbf{C})$$

y para todo $\sigma \in G$ tenemos $\rho(\sigma) \in Gl(n, \mathbf{C})$ Si tenemos dos representaciones $\rho : G \longrightarrow Gl(V)$ y $\rho' : G \longrightarrow Gl(V')$, un morfismo de representaciones es una transformación lineal

$$f : V \longrightarrow V'$$

tal que para todo $\sigma \in G$ tenemos

$$\begin{array}{ccc} V & \xrightarrow{f} & V' \\ {\scriptstyle \rho(\sigma)}\downarrow & & \downarrow{\scriptstyle \rho(\sigma)} \\ V & \xrightarrow{f} & V' \end{array}$$

el diagrama conmuta, es decir

$$\rho'(\sigma) \circ f = f \circ \rho(\sigma)$$

Diremos que ρ y ρ' son equivalentes o isomorfos si existe un isomorfismo $f : V \longrightarrow V'$ tal que f morfismo de representaciones

$$f : \rho \longrightarrow \rho'$$

Ejemplo
Si G es un grupo de dimensión finita, consideremos una representación de grado 1 es decir

$$\rho : G \longrightarrow Gl(1, \mathbf{C}) = \mathbf{C}^* = \mathbf{C} - 0$$

Como $|G| = 1$ tenemos que $\forall \sigma \in G \; \sigma^n = e$ entonces

$$\rho(\sigma)^n = \rho(\sigma^n) = \rho(e) = 1$$

De este modo $\rho(\sigma)$ es una raíz n-ésima de la unidad.

Ejemplo
Si G infinito definimos $\rho : G \longrightarrow \mathbf{C}^*$ tal que $\rho(g) := 1 \; \forall g \in G$ es una representación cuya acción es la trivial a esta la llamaremos la Representación Trivial

Ejemplo
Sea $G = \frac{\mathbf{Z}}{n\mathbf{Z}}$ si $\rho : \frac{\mathbf{Z}}{n\mathbf{Z}} \longrightarrow \mathbf{C}^*$ es de grado 1, por el primer ejemplo, nos lleva

$$Im\rho \subset M_n$$

Donde M_n={Grupo de raíces n-ésima de 1}. Como $\frac{\mathbf{Z}}{n\mathbf{Z}}$ es cíclico tiene un generador digamos $1 \in \frac{\mathbf{Z}}{n\mathbf{Z}}$ entonces $\rho_w(1) = w$ para cada $w \in M_n$
Si $k \in \frac{\mathbf{Z}}{n\mathbf{Z}}$ entonces $\rho_w(k) := w^k \; 0 \leq k < n$. Así $\rho_w : \frac{\mathbf{Z}}{n\mathbf{Z}} \longrightarrow M_n \subset \mathbf{C}^*$ es una representación.

Representación regular de grado n
Sea G finito $|G| = n$ y V un $\mathbf{C}$-espacio vectorial de $dim = n$ con base $B =$

$v_g|g \in G$ para cada $\sigma \in G$ $\rho(\sigma) : B \longrightarrow B$ definimos $\rho(\sigma)(v_g) = v_{\sigma g}$ y esto por linealidad $\rho(\sigma)$ se extiende a todo V es decir

$$\rho(\sigma) : V \longrightarrow V$$

Se define

$$\rho : G \longrightarrow Gl(V)$$

$$\sigma \longrightarrow \rho(\sigma)$$

es un morfismo ya que si consideramos

$$\rho(\sigma\tau) : V \longrightarrow V$$

$$\begin{aligned} \rho(\sigma\tau)(v_g) &= v_{\sigma\tau g} \\ &= \rho(\sigma)(v_{\tau g}) \\ &= \rho(\sigma)(\rho(\tau)(v_g)) \\ &= (\rho(\sigma) \circ \rho(\tau))(v_g) \end{aligned}$$

Notemos que si $g \in G$ entonces $\rho(g)(v_1) = v_g$ de este modo la imagen de v_1 forman la base

Ejemplo Sea $G = S_3 = (1), (12), (13), (23), (123), (132)$, si $\rho : S_3 \longrightarrow Gl(6, \mathbf{C})$ es la representación regular, veamos como es la representación de

$$\rho(12) = V_{\mathbf{C}} \longrightarrow V_{\mathbf{C}}$$

con $dim_{\mathbf{C}} = 6$. La base está dada por

$$B = v_{(1)}, v_{(12)}, v_{(13)}, v_{(23)}, v_{(123)}, v_{(132)}$$

Tenemos

$$\rho(12)(v_1) = v_{(12)(1)} = 0v_{(1)} + 1v_{(12)} + 0v_{(13)} + 0v_{(23)} + 0v_{(123)} + 0v_{(132)}$$

$$\rho(12)(v_{(12)}) = v_{(12)(12)} = 1v_{(1)} + 0v_{(12)} + 0v_{(13)} + 0v_{(23)} + 0v_{(123)} + 0v_{(132)}$$

$$\rho(12)(v_(13)) = v_{(12)(1)} = 0v_{(1)} + 0v_{(12)} + 0v_{(13)} + 0v_{(23)} + 0v_{(123)} + 1v_{(132)}$$

$$\rho(12)(v_(23)) = v_{(12)(1)} = 0v_{(1)} + 0v_{(12)} + 0v_{(13)} + 0v_{(23)} + 1v_{(123)} + 0v_{(132)}$$

$$\rho(12)(v_(123)) = v_{(12)(1)} = 0v_{(1)} + 0v_{(12)} + 0v_{(13)} + 1v_{(23)} + 0v_{(123)} + 0v_{(132)}$$

$$\rho(12)(v_(132)) = v_{(12)(1)} = 0v_{(1)} + 0v_{(12)} + 1v_{(13)} + 0v_{(23)} + 0v_{(123)} + 0v_{(132)}$$

De este modo transponiendo llegaremos a la matriz asociada siguiente:

$$\rho(12) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Definición
Si $\rho : G \longrightarrow Gl(V)$ es una representación de grado $n = dim_{\mathbf{C}}V$ y $W \leq V$, diremos que W es estable o invariante bajo G si para cualquier $\sigma \in G$, $w \in W$ se tiene que $\rho(\sigma)(w) \in W$ es decir W es $\rho(\sigma)$-invariante

Observación
Notemos las siguientes equivalencias a la anterior definición

- W es estable
- $\rho(\sigma)(W) \subset W \quad \forall \quad \sigma \in G$
- $\rho(\sigma)(W) \subset W \quad \forall \quad \sigma \in G$
- $\rho|_W(\sigma) : W \longrightarrow W$ es isomorfismo.
- $\rho|_W(\sigma) \in Gl(W)$

Ejemplo y V son G invariantes.

Ejemplo Sea $\rho : G \longrightarrow Gl(V)$ la representación regular de G, supongamos que V tienes base $B = v_g | g \in G$ y sea $W =< v >$ con $v \in B$ de este modo $v \neq 0$ entonces $W \neq 0$ y $dim_{\mathbf{C}}W = 1$,

Entonces W es G invariante.

Para este caso $\rho|_W(\sigma) : W \longrightarrow Gl(W) \cong Gl(1, \mathbf{C}) = \mathbf{C}^*$ entonces si $\rho(\sigma)(v) = v$ tenemos $\rho(\sigma) : G \longrightarrow Gl(1, \mathbf{C}) = \mathbf{C}^*$ a esta representación se le llama representación trivial cuando el el grado de ρ es 1.

Ejemplo Sea $\rho : G \longrightarrow Gl(V)$ la representación regular, supongamos que V tiene base $B = \{v_g | g \in G\}$.
Consideremos el subespacio W tal que $v_g \in W \Leftrightarrow g \neq 1$. De este modo W no es estable bajo G, pues $\rho(g^{-1})(v_g) = v_1 \notin W$ Si consideramos $W' =< v_1 >$ notemos que $V = W + W'$ mas aún $W \cap W' = 0$ entonces $V = W \oplus W'$.

Teorema 1.3.1 *Sea G un grupo finito y $\rho : G \longrightarrow Gl(V)$ la representación de grado $n < \infty$.Si $W \leq V$ es G-invariante entonces existe W^0 G-invariante de V tal que*
$$V = W \oplus W^0$$

Demostración: Como $W \subset V$ entonces existe un complemento W' tal que $V = W \oplus W'$, sea $p : V \longrightarrow W$ la proyección entonces tenemos $ker(p) = W'$ y $IM(W)$. Sea
$$p^0 = \frac{1}{|G|}\sum_{g\in G}\rho(g)\circ p\circ\rho(g^{-1}) : V \longrightarrow V$$

Como p manda V en W y W es G-invariante entonces p^0 manda V en W.
Si $w \in W$ entonces $p\rho(g^{-1})(w) \in W$ como p deja a w igual tenemos lo siguiente:

$$\begin{aligned} p\rho(g^{-1})(w) &= \rho(g^{-1})(w) \\ \rho(g)p\rho(g^{-1})(w) &= \rho(g)\rho(g^{-1})(w) \\ \rho(g)p\rho(g^{-1})(w) &= w \end{aligned}$$

Así sustituyendo en la definición de p^0 $p^0(w) = 0$ y $Im(p^0) = W$ entonces p^0 es una proyección y $ker(p^0) = W^0$. Así

$$V = W \oplus W^0$$

Mostremos que W^0 es G-invariante.
Si $\sigma \in G$ entonces $p^0(\sigma)(w^0) \in W^0$ $\forall w^0 \in W^0$
En efecto, por un la un lado

$$\begin{aligned} \rho(\sigma)p\rho(\sigma^{-1}) &= \rho(\sigma)(\frac{1}{|G|}\sum_{g\in G}\rho(g)\circ p\circ\rho(g^{-1}))\rho(\sigma^{-1}) \\ &= \frac{1}{|G|}\sum_{g\in G}\rho(\sigma)\rho(g)\circ p\circ\rho(g^{-1})\rho(\sigma^{-1}) \\ &= \frac{1}{|G|}\sum_{g\in G}\rho(\sigma g)\circ p\circ\rho((\sigma g)^{-1}) \\ &= p^0 \end{aligned}$$

De este modo tenemos $\rho(\sigma)p^0 = p^0\rho(\sigma)$ $\forall\sigma \in G$
Si $w \in W^0 = ker(p^0)$ y si $\sigma \in G$ entonces

$$p^0\rho(\sigma)(w) = \rho(\sigma)p^0(w) = \rho(\sigma)(0) = 0$$

, de este modo concluimos $\rho(\sigma)(w) \in ker(p^0) = W^0$ Si tenemos $W \leq V$ G-invariante, la

$$\rho|_W(\sigma) : W \longrightarrow Gl(W)$$

Se dice ser una subrepresentación de ρ.

1.4 Suma directa de Representaciones

Si $\rho(\sigma)p^0 = p^0\rho(\sigma)\ \forall\sigma \in G$ es una representación de grado $n = dim_{\mathbf{C}}V$ y si $W, W^0 \leq V$ invariantes tal que

$$V = W \oplus W^0$$

Tenemos para todo $v \in V$, $v = w + w^0$ y si $\sigma in G$ entonces

$$\rho(\sigma)(v) = \rho(\sigma)(w + w^0) = \rho(\sigma)(w) + \rho(\sigma)(w^0)$$

Donde $\rho(\sigma)(w) \in W$ y $\rho(\sigma)(w^0) \in W^0$, así

$$\rho|_W(\sigma) : W \longrightarrow W \qquad \rho|_{W^0}(\sigma) : W^0 \longrightarrow W^0$$

De este modo tenemos

$$\rho = \rho^W + \rho^{W^0}$$

Diremos que ρ es suma directa de sus representaciones.

Sea B y B^0 bases de W y W^0, y consideremos sus representaciones ρ^W, ρ^{W^0}, así $A = W \cup W^0$ es base de V. Entonces $\forall\sigma \in G$ se tiene

$$[\rho(\sigma)]_A = \begin{bmatrix} [\rho^W(\sigma)]_B & 0 \\ 0 & [\rho^{w^0}(\sigma)]_B \end{bmatrix} \tag{1.3}$$

En general, si $V = \bigoplus_{i=1}^n V_i$ con V_i G-invariantes, entonces

$$[\rho(\sigma)]_A = \begin{bmatrix} [\rho^{V_1}(\sigma)]_{B_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [\rho^{V_n}(\sigma)]_{B_n} \end{bmatrix} \tag{1.4}$$

Y por tanto

$$\rho = \bigoplus_{i=1}^n \rho_i^{V_i}$$

Observación Si el espacio V no tiene subespacios G-invariantes no triviales, diremos que la representación es irreducible o simple

Teorema 1.4.1 (Maschke) *Toda representación de un grupo finito es suma directa de representaciones irreducibles.*

Demostración: Sea $\rho : G \longrightarrow GL(V)$ una representación de grado $n = dim_{\mathbb{C}}V$. Haremos inducción sobre n. Si $n = 1$, entonces ρ es irreducible hemos terminado. Supongamos $n > 1$. Si ρ es irreducible hemos terminado. Si ρ es reducible, entonces existe un subespacio G-invariante $W \subseteq V$ con $1 < dim_{\mathbb{C}}W < n$ y por el Teorema 13.2) W tiene un complemento invariante W^0 tal que $V = W \oplus W^0$ y es claro que $1 < dim_{\mathbb{C}}W^0 < n$. Por hipótesis de inducción ρ^W y ρ^{W^0} se descomponen en sumas directas de irreducibles y así $\rho = \rho^W \oplus \rho^{W^0}$ también se descompone en suma de irreducibles.

La descomposición anterior no es necesariamente única. Por ejemplo la representación $\rho : G \longrightarrow GL(n, \mathbb{C})$, dada por $\rho(g) = I_n$ para toda $g \in G$, es tal que todos los subespacios de $\mathbb{C}^n$ son G-invariantes, en particular los de dimensión 1, es decir las rectas (que son irreducibles). Se sigue que cualquier subespacio unidimensional de $\mathbb{C}^n$ puede formar parte de una descomposición de ρ.

Consideremos ahora la representación regular del grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, $\rho : \mathbb{Z}/n\mathbb{Z} \longrightarrow GL(V)$ donde V tiene base $\{v_0, ..., v_{n-1}\}$ indexada por los elementos de $\mathbb{Z}/n\mathbb{Z}$. Por la definición de la representación regular $\rho(i)v_j = v_{i+j}$ donde la suma $i + j$ es en $\mathbb{Z}/n\mathbb{Z}$, es decir es módulo n.

Lema 1.4.2 *Si $W =< w >\subseteq V$ es un subespacio unidimensional, $w \neq 0$, entonces W es $\mathbb{Z}/n\mathbb{Z}$-invariante si y solo si $\rho(1)w = \lambda w$, para algún $\lambda \in \mathbb{C}^*$.*

Demostración: Si W es invariante, entonces $\rho(1)w \in W =< w >$ y así $\rho(1)w = \lambda w$, para algún $\lambda \in \mathbb{C}$, y $\lambda \neq 0$ porque de lo contrario $\rho(1)w = 0$ y así $\rho(1) : W \longrightarrow W$ sería la transformación lineal 0 contradiciendo que $\rho(1)$ es un isomorfismo. Recíprocamente, si $\rho(1)w = \lambda w$, con $\lambda \in \mathbb{C}^*$, entonces para cada $k \in \mathbb{Z}/n\mathbb{Z}$ se tiene que $\rho(k)w = \rho(1 + ... + 1)w = \rho(1)^k w = \lambda^k w \in< w >= W$, y así W es invariante.

Para detectar los subespacion $\mathbb{Z}/n\mathbb{Z}$-invariantes basta detectar...

Lema 1.4.3 (Lema de Schur) *Sean $\rho_1 : G \longrightarrow GL(V_1)$ y $\rho_2 : G \longrightarrow GL(V_2)$ dos representaciones irreducibles de G y sea $f : V_1 \longrightarrow V_2$ una representación lineal tal que $\rho_2(g) \circ f = f \circ \rho_1(g)$, para todo $g \in G$. Entonces,*

1. *Si $\rho_1 = \rho_2$ no son isomorfas, entonces $f = 0$.*
2. *Si $\rho_1 = \rho_2$ (en particular, $V_1 = V_2$), entonces f es una homotecia, i.e., es un múltiplo escalar de la identidad, $f = \lambda id_V$, con $\lambda \in \mathbb{C}$.*

Demostración: Para (1). Si $f = 0$ no hay nada que probar. Supongamos ahora $f \neq 0$ y sea $W_1 \subseteq V_1$ el núcleo de f. Si $w \in W_1$ es cualquier vector, como $f \circ \rho_1(g)w = \rho_2 \circ f(w) = 0$, entonces $\rho_1(g) \in kerf = W_1$, y así W_1 es ρ_1-invariante. Como V_1 es irreducible, entonces $W_1 = 0$ o $W_1 = V1$. Si $W_1 = V1$, entonces $f = 0$, lo cual contradice la suposición de que $f \neq 0$. Se sigue que $W_1 = 0$ y por lo tanto f es inyectiva.

Ahora supongamos $W_2 = imf \subseteq V_2$. Si $w \in W_2$, entonces $w = f(v)$ con $v \in V_1$ y así $\rho_2(g)w = \rho_2(g)f(v) = f\rho_1(g)v \in Imf \subseteq W_2$, por lo que W_2 es ρ_2-invariante. Como V_2 es irreducible, entonces $W_2 = 0$ o $W_2 = V_2$. El caso $W_2 = 0$ no es posible pues implicaría que $f = 0$. Se sigue que $W_2 = V_2$ y por lo tanto f es sobreyectiva. Hemos así demostrado que si $f \neq 0$, entonces f es un isomorfismo. Lo cual prueba (1).

Para (2), supongamos que $V = V_1 = V_2$ y $\rho_1 = \rho_2$. Sea λ un valor propio de f y supongamos $\tilde{f} := f - id_V$. Como λ es valor propio de f, entonces $ker\tilde{f} \neq 0$. Por otra parte,

$$\begin{aligned} \rho_2(g) \circ \tilde{f} &= \rho_2(g)(f - id_V) \\ &= \rho_2(g)f - \lambda\rho_2(g) \\ &= f\rho_1(g) - \lambda\rho_1(g) \\ &= (f - id_V)\rho_1(g) \\ &= \tilde{f} \circ \rho_1(g) \end{aligned}$$

En la tercera linea utilizamos el hecho de que $\rho_2(g) \circ f = f \circ \rho_1(g)$ y $\rho_1 = \rho_2$. Aplicando la parte (1) a $\tilde{f}$, y como $ker\tilde{f} \neq 0$, entonces $\tilde{f} = 0$. Se sigue que $f - \lambda id_V = 0$, como se quería.

1.5 Caracteres de grupos finitos

Sea $A \in M_{nxn}(\mathbb{C})$, su traza es el escalar dado por

$$Tr(A) = \sum_{i=1}^{n} a_{ii}$$

Observación Si $A, B \in M_{nxn}(\mathbb{C})$ entonces $Tr(AB) = Tr(BA)$, ademas considerando A invertible, considerar $A' = AB$ y $B' = A^{-1}$ entonces $A'B' = ABA^{-1}$ y $B'A' = B$ y obtendremos $Tr(ABA^{-1}) = Tr(B)$

Si consideramos una tranformación lineal $T : V \longrightarrow V$ sobre un espacio vectorial de dimensión n, podemos definir la traza del operador T usando la matriz asociada a T en cualquier base de V, porque las matrices asociadas a T en dos bases cualquiera de V son conjugadas (Matrices semejantes) y aplicando la observación antes mencionada.

Definición Sea $\rho : G \longrightarrow GL(V)$ una representación de grado n de un grupo finito G, para cada $g \in G$ sea $\rho(g) : V \longrightarrow V$ el isomorfismo correspondiente, podemos considerar su traza $Tr(\rho(g)) \in \mathbb{C}$ y así se tiene una función $\chi : G \longrightarrow \mathbb{C}$ definida como

$$\chi(g) := Tr(\rho(g))$$

La cual se le llama el carácter de la representación

Teorema 1.5.1 *Sea G u grupo finito y sea χ el carácter de una representación $\rho : G \longrightarrow GL(V)$ de grado n. Entonces:*

1. *La transformación $\rho(g) : V \longrightarrow V$ es diagonalizable, para todo $g \in G$.*
2. $\chi(1) = n$.
3. $\chi(tgt^{-1}) = \chi(g)$ *para todo* $g, t \in G$.
4. $\chi(g)$ *es la suma, con multiplicidades, de los valores propios de* $\rho(g)$.
5. $\chi(g)$ *es la suma de n raíces k-ésimas de la unidad, donde k es el orden de g*
6. $\chi(g^{-1}) = \overline{\chi(g)}$
7. $|\chi(g)| \leq \chi(1)$. *Donde* 1 *es la identidad de* G
8. $ker\rho = \{g \in G : \chi(g) = \chi(1)\}$

Demostración:

1. Sea $g \in G$ de orden k y consideremos el subgrupo cíclico $H =< g >\subseteq G$. La restricción de ρ a H es una representación $\rho : H \hookrightarrow G \longrightarrow GL(V)$ de H. Usando el teorema de Maschke (**??**), sea $V = W_1 \oplus ... \oplus W_r$ una descomposición de $\rho : H \longrightarrow GL(V)$ en irreducibles. Como H es abeliano, por el corolario **??** cada W_i es unidimencional, digamos $W_i =< u_i >$ y así $r = n$. Ahora, si $\rho_i : H \longrightarrow GL(V) \simeq GL(1, \mathbb{C}) \simeq \mathbb{C}^*$ es la subrepresentación correspondiente, por el ejemplo 1 del capitulo 2, $\rho_i(g)$ es una raíz k-ésima de la unidad, digamos w^{e_i} con $w = e^{\frac{2\pi i}{k}}$ una raíz primitiva.

Entonces, $\rho_i(g)u_i = w^{e_i}u_i$ y por lo tanto, la base $\{u_1, ..., u_r\}$ de V, como $\rho = \rho_1 \oplus \cdots \oplus \rho_n$, entonces

$$[\rho(g)] = \begin{pmatrix} [\rho_1(g)] & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [\rho_n(g)] \end{pmatrix} = \begin{pmatrix} w^{e_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & w^{e_n} \end{pmatrix}$$

Que es lo que queríamos probar.

2. Como $\rho(1) = id_V$, entonces $[\rho(1)] = I_n$ y así $\chi(1) = Tr(I_n) = n$.

3. Como $\rho(tgt^{-1}) = \rho(t)\rho(g)\rho(t^{-1})$, el resultado es consecuencia de $Tr(ABA^{-1}) = Tr(B)$.

4. Como $\rho(g)$ es diagonalizable, su traza es la suma de sus valores propios, por 1.

5. Si k es el orden de g, por la parte 1. en la diagonal de $[\rho(g)]$ aparecen raíces k-ésimas de la unidad.

6. Los valores propios del operador $\rho(g^{-1}) : V \longrightarrow V$ son los inversos λ_i^{-1} de los valores propios λ_i de $\rho : V \longrightarrow V$, y como por 4 los λ_i son raíces de la unidad, entonces $\lambda_i^{-1} = \overline{\lambda_i}$, por lo que
$$\chi(g^{-1}) = \sum_i \overline{\lambda_i} = \overline{\sum_i \lambda_i} = \overline{\chi(g)}$$

7. Por 4, $\chi(g) = \sum_{i=1}^n \lambda_i$ con los λ_i raíces de la unidad. De la desigualdad del triángulo se sigue que
$$|\chi(g)| \leq \sum_{i=1}^{n} |\lambda_i| \leq n \quad ya \quad que \quad |\lambda_i| = 1$$

8. Si g es tal que $\chi(g) = \chi(1) = n$, como $\chi(g)$ es la suma de sus n valores propios y cada uno de éstos tiene valor absoluto 1, entonces cada uno de éstos debe ser 1 y por lo tanto la matriz de $?`rho(g)$ debe ser la I_n, por lo que $\chi(g) = Tr(I_n) = n = \chi(1)$.

Proposición 1.5.2 *Si $\rho_1 : G \longrightarrow GL(V_1)$ y $\rho_2 : G \longrightarrow GL(V_2)$ son dos representaciones del grupo finito G, y si χ_1 y χ_2 son sus caracteres, entonces $\chi_{\rho_1 \oplus \rho_2} = \chi_1 + \chi_2$.*

Demostración: Si $V = V_1 \oplus V_2$ y si $\mathcal{B}_1$ y $\mathcal{B}_2$ son bases de V_1 y V_2 respectivamente, entonces $\mathcal{B}_1 \cup \mathcal{B}_2$ es base de V y la matriz asociada a $(\rho_1 \oplus \rho_2)(g)$ es de la forma

$$[(\rho_1 \oplus \rho_2)(g)_{\mathcal{B}} \quad = \quad \begin{pmatrix} [\rho_1(g)]_{\mathcal{B}_1} & 0 \\ 0 & [\rho_2(g)]_{\mathcal{B}_2} \end{pmatrix},$$

por lo que

$$\chi_{\rho_1 \oplus \rho_2}(g) = Tr[(\rho_1 \oplus \rho_2)]_{\mathcal{B}} = Tr[\rho_1(g)]_{\mathcal{B}_1} + Tr[\rho_2(g)]_{\mathcal{B}_2} = \chi_1(g) + \chi_2(g).$$

Ejemplo Si $\rho : G \longrightarrow \mathbb{C}^*$ es la representación trivial $\rho(g) = 1$, para todo $g \in G$, su carácter está dado por $\chi(g) := Tr[\rho(g)] = 1$, para todo $g \in G$. A éste carácter lo llamaremos el carácter principal de G y lo denotaremos por χ_1.

Ejemplo Si $\rho : G \longrightarrow GL(V)$ es la representación regular de G, $n = |G| = dim_{\mathbb{C}}V$, y si el espacio V tiene como base $\{v_g\}_{g \in G}$, por definición de la representación regular se tiene que $\rho(\sigma)v_g = v_{\sigma g}$ y notemos que $\rho(\sigma)v_g = v_g$ si y sólo si $\sigma g = g$, esto es $\sigma = 1$. Así, si $[\rho(\sigma)]$ es la matriz asociada a $\rho(\sigma)$ en la base regular, entonces:

1. Si $\sigma = 1$ (el neutro de G), la diagonal de $[\rho(\sigma)]$ consiste de ceros.

2. Si $\sigma = 1$, la diagonal de $[\rho(1)]$ consiste de unos.

Se sigue que el carácter χ de la representación regular está dado por:

$$\chi(\sigma) = \begin{cases} 0 & \text{si } \sigma \neq 1, \\ |G| & \text{si } \sigma = 1. \end{cases}$$

Ejemplo Generalizando el ejemplo anterior, sean G es finito y Y un G-conjunto finito, esto define la representación por permutaciones $\phi : G \longrightarrow GL(V)$, donde el espacio vectorial V tiene base $\{v_x : x \in Y\}$ indexada por Y y si $\sigma \in G$, $\phi(\sigma)v_x := v_\sigma x$, donde σx es la acción de σ en x.

Notemos que $\phi(\sigma)v_x = v_x$ si y sólo si $\sigma x = x$, es decir si y sólo si $x \in Y^\sigma$. En la diagonal de la matriz asociada a $\phi(\sigma)$ se tiene un 1 por cada $x \in Y^\sigma$ y por lo tanto la traza $Tr[\phi(\sigma)]$ cuenta los puntos $x \in Y^\sigma$, esto es, el carácter χ de la representación por permutaciones de G en Y está dado por $\chi(\sigma) = |Y^\sigma|$.

Corolario 1.5.3 *Sean $\rho_1 : G \longrightarrow GL(V_1)$ y $\rho_2 : G \longrightarrow GL(V_2)$ dos representaciones irreducibles de G y sea $h : V_1 \longrightarrow V_2$ una transformación lineal arbitraria. Pongamos*

$$h^0 := \frac{1}{|G|} \sum_{g \in G} \rho_2(g)^{-1} \circ h \circ \rho_1(g)$$

1. *Si ρ_1 y ρ_2 no son isomorfas, entonces $h^0 = 0$.*

2. *Si $\rho_1 = \rho_2$ (en particular $V := V_1 = V_2$), entonces h^0 es una homotecia de razón $\lambda = (1/n)Tr(h)$, donde $n = dim_{\mathbb{C}}V$.*

Demostración: La transformación lineal h^0 satisface $\rho_2(g) \circ h^0 = h^0 \circ \rho_1(g)$ ya que

$$\begin{aligned} \rho_2(\tau)^{-1}h^0\rho_1(\tau) &= \frac{1}{|G|}\sum_{g\in G}\rho_2(\tau)^{-1}\rho_2(g)^{-1} \circ h \circ \rho_1(g)\rho_1(\tau) \\ &= \frac{1}{|G|}\sum_{g\in G}\rho_2(g\tau)^{-1} \circ h \circ \rho_1(g\tau) \\ &= h^0. \end{aligned}$$

Entonces podemos aplicar el lema de Schur a $f = h^0$ y concluir (1) y (2), excepto por la identificación del escalar λ. Ahora, como $\rho_1 = \rho_2$, entonces

$$Tr(h^0) = \frac{1}{|G|}\sum_{g\in G} Tr(\rho_2(g)^{-1} \circ h \circ \rho_1(g)) = \frac{1}{|G|}\sum_{g\in G} Tr(h) = Tr(h)$$

Y como $h^0 = \lambda id_V$, etnonces $Tr(h^0) = \lambda Tr(id_V) = n\lambda$, por lo que $n\lambda = Tr(h)$ y así $\lambda = (1/n)Tr(h)$.

1.6 Ortogonalidad de Caracteres

Si $\phi, \psi : G \longrightarrow \mathbf{C}$ son dos funciones, pongamos

$$< \phi, \psi > := \frac{1}{|G|}\sum_{g\in G}\phi(g)\overline{\psi(g)}$$

y observemos que éste es un producto interno ya que:

1) Es lineal en ϕ ya que es aditivo y saca escalares.

2) Es aditivo en ψ.

3) $< \phi, \psi > = \overline{< \psi, \phi >}$

4) Saca escalares conjugados en ψ esto a partir de 3 y 1

5) $< \phi, \phi >$ es mayor que cero para toda $\phi \neq 0$.

En particular, si $\phi, \psi : G \longrightarrow \mathbf{C}$ son caracteres, como $\overline{\psi(g)} = \psi(g)^{-1}$, por **??**, la definición del producto interior su vuelve

$$< \phi, \psi > := \frac{1}{|G|} \sum_{g \in G} \phi(g)\psi(g)^{-1}$$

y observemos que

$$\sum_{g \in G} \phi(g)\overline{\psi(g)} = \sum_{g \in G} \phi(g)\psi(g)^{-1}$$

ya que g^{-1} recorre G cuando g lo hace. Se sigue que

$$< \phi, \psi > = < \psi, \phi >$$

cuando ϕ y ψ son caracteres.

Teorema 1.6.1
Sea G un grupo finito

1) *Si χ y χ' son caracteres de dos representaciones irreducibles no isomorfas de G, entonces son ortogonales, es decir, $< \chi, \chi' > = 0$.*

2) *Si χ es el carácter de una representación irreducible de G, entonces es de norma 1, es decir, $< \chi, \chi > = 1$.*

Demostración:

1) Sean $\rho : G \longrightarrow GL(V)$ y $\rho' : G \longrightarrow GL(V')$ dos representaciones irreducibles de G, con caracteres χ y χ' , respectivamente. Sean $[\rho(g)] = (a_{ij})$ y $[\rho'(g)] = (a'_{kl})$ sus matrices correspondientes respectos a bases fijas de V y V'. Si $h : V \longrightarrow V'$ es transformación lineal con matriz asociada $[h] = (x_{st})$ en las bases de V y V' usadas anteriormente como la matriz de $\rho(g^{-1})$ es de la forma $(a_{ij}(g^{-1}))$, entonces para el h^0 definido como

$$h^0 := \frac{1}{|G|} \sum_{g \in G} \rho(g)^{-1} \circ h \circ \rho'(g)$$

del corolario anterior su matriz asociad es

$$[h^0] = \frac{1}{|G|} \sum_{g \in G} [\rho(g)^{-1}][h][\rho'(g)]$$

ya que la matriz de una suma de aplicaciones lineales, es la suma de las matrices, y la matriz de una composición es el producto de las matrices, así, los coeficientes h^0_{ij} de $[h^0]$ son:

$$h^0_{ij} = \frac{1}{|G|}\sum_{g\in G}\sum_{k,t} a_{ij}(g^{-1})x_{st}a'_{kl}(g) \tag{1.5}$$

Ahora como ρ y ρ' no son isomorfas, se tiene que $h^0 = 0$ y así para toda i, j las $h^0_{ij} = 0$y de esto se sigue que es un sistema de ecuaciones lineales en las variables x_{sr} que se anula para cualquier $h : V \longrightarrow V'$, es decir, para todos los valores de x_{st}. Por lo tanto sus coeficientes tienen que ser todos cero para todo i, j, k, t:

$$\frac{1}{|G|}\sum_{g\in G}\sum_{k,t} a_{ij}(g^{-1})x_{st}a'_{kl}(g) = 0$$

Ahora, como $\chi(g) = \sum_i a_{ii}(g)$ y $\chi'(g) = \sum_i a'_{jj}(g)$, entonces

$$\begin{aligned} < \chi, \chi' > &=< \sum_i a_{ii}(g), \sum_i a'_{jj}(g) > \\ &= \sum_i < a_{ii}(g), a'_{jj}(g) > \\ &= \frac{1}{|G|}\sum_{g\in G}\sum_i < a_{ii}(g), a'_{jj}(g) > \end{aligned}$$

2) Con la misma notación para $\rho = \rho'$ y h, sólo que en este caso tenemos, por el corolario anterior, que $h^0 = \lambda id_V$, para un escalar λ de la forma $\lambda = (1/n)Tr(h)$, con $n = dim_{\mathbf{C}}V$, por lo que

$$h^0_{ij} = \begin{cases} 0 & i \neq j \\ \lambda & i = j \end{cases}$$

es decir, $h^0_{ij} = \lambda\delta_{ij}$, la delta de Kronecker, y comoλ es de la forma

$$\lambda\frac{1}{n}Tr(h) = \frac{1}{n}\sum_k x_{kk} = \frac{1}{n}\sum_{s,t} x_{s,t}\delta_{st}$$

entonces

$$h^0_{ij} = \lambda\delta_{st} = \frac{1}{n}\sum_{s,t} x_{s,t}\delta_{st}\delta_{ij}$$

por lo que la igualdad (1.5)

$$\frac{1}{n}\sum_{s,t} x_{s,t}\delta_{st}\delta_{ij} = \frac{1}{|G|}\sum_{i,s,t,j,g\in G} a_{is}(g^{-1})x_{st}a'_{tj}(g)$$

e igualando los coeficientes de las variables x_{st} se obtiene que

$$\frac{1}{|G|}\sum_{g\in G} a_{is}(g^{-1})a'_{tj}(g) = \frac{1}{n}\delta_{st}\delta_{ij} = \begin{cases} \frac{1}{n} & \text{si } i=j \text{ y } s=t \\ 0 & \text{en cualquier otro caso} \end{cases} \tag{1.6}$$

y como $\chi(g) = \sum_i a_{ii}(g)$, entonces

$$\begin{aligned} <\chi,\chi> &= <\sum_i a_{ii}(g), \sum_i a_{jj}(g)> \\ &= \sum_i <a_{ii}(g), a_{jj}(g)> \\ &= \sum_{i,j}\frac{1}{|G|}\sum_{g\in G} a_{ii}(g^{-1}), a_{jj}(g) \text{ por definición} \\ &= \sum_{i,j}\frac{1}{n}\delta_{ij} \text{ por } 1.6 \\ &= \sum_{i=1}^{n}\frac{1}{n} \\ &= 1 \end{aligned}$$

Observación
Note que la parte 2 del teorema es una condición necesaria para que una representación ρ sea irreducible: se requiere que $<\chi_\rho,\chi_\rho>= 1$.

Ejemplo Sea $G \neq 1$, $|G| = n$, $\rho : G \longrightarrow Gl(V)$ la representación regular de G y χ su carácter. Entonces

$$\chi(g) = \begin{cases} 0 & \text{si } g \neq 1 \\ n & \text{si } g = 1 \end{cases} \tag{1.7}$$

por lo que

$$<\chi,\chi>= \frac{1}{n}\sum_{g\in G}\chi(g)\chi(g^{-1}) = \frac{1}{n}\chi(1)\chi(1) = \frac{1}{n}(n)(n) = n \neq 1$$

y por lo tanto la representación regular de grado $n > 1$ no es irreducible.

Corolario 1.6.2
Sea G un grupo finito y se $\rho : G \longrightarrow Gl(V)$ una representación con carácter χ. Supongamos que la representación se descompone en suma directa de irreducibles como

$$V = W_1 \oplus \cdots \oplus W_k$$

Si W es una representación irreducible de G con carácter ψ, entonces $< \chi, \psi >$ es un entero que es igual al número de W_i isomorfo a W. Se sigue que el número de W_i isomorfas a W no depende de la descomposición de V

Demostración:
Si χ_i es el carácter de W_i, por (**??**) se tiene que $\chi = \chi_1 + \cdots + \chi_k$, por lo que

$$< \chi, \psi >=< \chi_1 + \cdots + \chi_k, \psi >=< \chi_1, \psi > + \cdots + \chi_k, \psi > \tag{1.8}$$

y por el teorema anterior tenemos

$$< \chi, \psi >= \begin{cases} 1 & \text{si } W_i \text{ es isomorfo a } W \\ 0 & \text{si } W_i \text{ no es isomorfo a } W \end{cases} \tag{1.9}$$

por lo que la suma (1.8) cuenta los W_i isomorfos a W. Para la segunda afirmación del corolario, note que el numero $< \chi, \psi >$ no depende de la descomposición.

Observación En el corolario anterior, diremos que $< \chi, \psi >$ es el número de veces que W ocurre en la descomposición en irreducibles de V.

Corolario 1.6.3
Dos representaciones ρ_1 y ρ_2 de G, son isomorfas si y sólo si sus caracteres son iguales.

Demostración: Si $\rho_1 : G \longrightarrow Gl(V)$ y $\rho_2 : G \longrightarrow Gl(V')$ son isomorfos, existe un isomorfismo lineal $f : V \longrightarrow V'$ tal que $f\rho_(g) = \rho_2(g)f$, para todo $g \in G$. Se sigue que $f\rho_1(g)f^{-1} = \rho_2(g)$ y por lo tanto

$$\chi_1(g) = Tr(\rho_1(g)) = Tr(f\rho_1(g)f^{-1}) = Tr(\rho_2(g)) = \chi_2(g)$$

para todo $g \in G$, y así $\chi_1 = \chi_2$. Recíprocamente, si $\chi_1 = \chi_2$, el corolario anterior nos dice que en este caso ρ_1 y ρ_2 contiene, cada una, una representación irreducible el mismo numero de veces.

Observación Si $\rho : G \longrightarrow Gl(V)$ es una representación de grado n con carácter χ, supongamos que $W_1, ..., W_r$ so todos los irreducibles no isomorfos que aparecen en una descomposición de ρ. Pongamos $m_i :=< \chi, \chi_i >$, donde χ_i es el carácter de W_i, recordando de (1.8) que los m_i son enteros ≥ 0, y denotemos con $m_i W_i$ a la suma directa de W_i consigo mismo m_i veces, es decir:

$$m_i W_i := \underbrace{W_1 \oplus \cdots \oplus W_i}_{m_i}$$

(con $0W_i := 0$).Al entero m_i lo llamaremos la multiplicidad de W_i. Entonces

$$V = m_i W_1 \oplus \cdots \oplus m_r W_r$$

y el carácter χ de ρ es una combinación lineal de los caracteres irreducibles $\chi_1, ..., \chi_r$, con coeficientes enteros [redacted]0:

$$\chi = m_1 \chi_1 + ... + m_r \chi_r$$

Corolario 1.6.4
Si χ es el carácter de una representación V de G, entonces

- $< \chi, \chi >= \sum_{i=1}^{r} m_i^2$
- $< \chi, \chi >$ *mayor que cero*
- $< \chi, \chi >= 1$ *si sólo si χ es irreducible.*

Demostración:
Para demostrar (1) se sigue del teorema (1.6.1) de ortogonalidad de los caracteres irreducibles, además notemos (2) es consecuencia de (1) y para (3) observemos que $< \chi, \chi >= \sum_{i=1}^{r} m_i^2 = 1$ si y solo si uno de los $m_i = 1$ y los otros son cero, es decir, si y solo si $V \simeq W_i$

Corolario 1.6.5 *Toda representación irreducibles ρ_i de un grupo finito G está contenida en la representación regular de G, con multiplicidad m_i igual al grado n_i de ρ_i*

Demostración: Sabemos el carácter χ_R de la representación regular de G está dada por

$$\chi_R(g) = \begin{cases} 0 & \text{si } g \neq 1 \\ |G| & \text{si } g = 1 \end{cases} \tag{1.10}$$

Ahora por el corolario (1.8) la multiplicidad m_i con que la representación irreducible W_i, con carácter χ_i, está contenida en la representación regular R de G es

$$m_i =< \chi_R, \chi_i >= \frac{1}{|G|} \sum_{g \in G} \chi_R(g^{-1}) \chi_i(g) = \frac{1}{|G|} \chi_R(1) \chi_i(1) = \frac{|G|}{|G|} (\chi_i(1)) = n_i$$

ya que $\chi_i(1) = n_i$ es el grado de la representación irreducible de W_i.

Corolario 1.6.6

1) *Si G es un grupo finito, entonces tiene sólo un número finito de representaciones irreducibles no isomorfas, con caracteres $\chi_1, ..., \chi_r$*

2) *Los grados n_i de los caracteres irreducibles χ_i de G satisfacen*

$$\sum_{i=1}^{r} n_i^2 = |G|$$

3) *Si $g \in G$, $g \neq 1$, entonces*

$$\sum_{i=1}^{r} n_i \chi_(g) = 0$$

Demostración: (1) Por el corolario anterior todas las representaciones irreducibles de G están contenidas en la representación regular V_R cuyo grado es $|G|$, y como V_R sólo tiene un número finito de subespacios no isomorfos, de esto se sigue (1). (2)Por el corolario anterior

$$\chi_R(g) = \sum_{i=1}^{r} n_i \chi_(g)$$

para todo $g \in G$. Poniendo $g = 1$ obtenemos

$$|G| = \chi_R(1) = \sum_{i=1}^{r} n_i \chi_(g) \sum_{i=1}^{r} n_i n_i = \sum_{i=1}^{r} n_i^2$$

lo cual prueba (2). Ahora poniendo $g \neq 1$ en (1.6) se obtiene

$$\sum_{i=1}^{r} n_i \chi_(g) = \chi_R(g) = 0$$

donde la última igualdad es porque $\chi_R(g)$ es el carácter de la representación regular y $g \neq 1$.

1.7 Funciones de clase

Si $\chi : G \longrightarrow \mathbf{C}$ es un carácter de G por **??**(2) sabemos que $\chi(tgt^{-1}) = \chi(g)$, para cualquier $g, t \in G$ y esto nos dice que todo carácter χ es constante en cada clase de conjugación de G. En general, una función $f : G \longrightarrow \mathbf{C}$ que es constante en cada clase de conjugación de G, es decir, tal que $f(tgt^{-1}) = f(g)$, para todo $g, t \in G$, se llamará una función de clases.Sea $\mathcal{F}$ el conjunto de todas las funciones de clases en G.Es claro que la suma de dos funciones de clase es una función de clases y que el producto de n escalar por una función de clases también es una función de clases. Como la función constante cero $0 : G \longrightarrow \mathbf{C}$ está en $\mathcal{F}$, se sigue que $\mathcal{F}$ es un $\mathbf{C}$-subespacio vectorial del espacio de todas las funciones de G en $\mathbf{C}$ y por lo tanto podemos considerar el producto escalar

$$< f, h >:= \frac{1}{|G|} \sum_{\sigma \in G} f(\sigma^{-1}) h(\sigma)$$

definido anteriormente, restringido a $\mathcal{F}$, por (1.6.1) los caracteres irreducibles $\chi_1, ..., \chi_r$ de G forman un sistema ortonormal en $\mathcal{F}$, y son un conjunto finito por (1.6.6). Mostraremos que forman una base y para ello es necesario el siguiente lema

Lema 1.7.1 *Sean $f : G \longrightarrow \mathbf{C}$ una función de clases y $\rho : G \longrightarrow Gl(V)$ una representación. Sea$\rho_f : V \longrightarrow V$ la función lineal dada por*

$$\rho_f := \sum_{\sigma \in G} f(\sigma) \rho(\sigma)$$

Si ρ es irreducible de grado n y carácter χ, entonces ρ_f es una homotecia de razón λ dada por

$$\lambda := \frac{1}{n} \sum_{\sigma \in G} f(\sigma) \chi(\sigma) = \frac{|G|}{n} < f, \overline{\chi} >$$

Demostración: Mostraremos que ρ_f satisface la condición del lema de Schur. En efecto, para todo $t \in G$

$$\rho(t^{-1}) \rho_f \rho(t) = \sum_{\sigma \in G} \rho(t)^{-1} f(\sigma) \rho(\sigma) \rho(t) = \sum_{\sigma \in G} f(\sigma) \rho(t^{-1} \sigma t)$$

(la ultima igualdad por linealidad, ya que $f(\sigma) \in \mathbf{C}$), y poniendo $u := t^{-1} \sigma t$, es decir, $\sigma = tut^{-1}$, y usando que f es función de clases, la igualdad anterior se vuelve

$$\rho(t^{-1}) \rho_f \rho(t) = \sum_{u \in G} f(tut^{-1}) \rho(u) = \sum_{u \in G} f(u) \rho(u) = \rho_f$$

es decir, $\rho_f \rho(t) = \rho(t) \rho_f$, y así, por la parte 2 del lema de Schur, se tiene que ρ_f es una homotecia, $\rho_f = \lambda id_V$. Calculando la traza en esta igualdad:

$$n\lambda = Tra(\lambda Id_V) = Tr(\rho_f) = \sum_{\sigma \in G} f(\sigma) Tr(\rho(\sigma)) = \sum_{\sigma \in G} f(\sigma) \chi(\sigma)$$

y así
$$\lambda = \frac{1}{n}\sum_{\sigma\in G} f(\sigma)\chi(\sigma)\frac{1}{n}|G| < f, \overline{\chi} >$$
la ultima igualdad por la definición del producto interno.

Capítulo 2

Aplicaciones de la teoría de caracteres

Para determinar la simpleza o solubilidad de un grupo necesitaremos los resultados siguientes:

Lema 2.0.1 *Sea G un grupo finito y $H \lhd G$ un subgrupo normal.*

1. *Si $\rho : G/H \longrightarrow GL(V)$ es una representación del cociente G/H, entonces la composición $\rho' : G \longrightarrow G/H \longrightarrow GL(V)$ es una represntación de G.*

2. *El carácter χ' de ρ' es la composición del caracter χ de ρ con el homomorfismo canónico $\pi : G \longrightarrow G/H$, i.e., $\chi' = \chi \circ \pi$.*

3. *Si $W \subseteq V$ es un subespacio, entonces W es G-invariante si y sólo si es G/H-invariante.*

Demostración:

1. Es trivial. Si $H \lhd G$, el conjunto G/H resulta un grupo llamado grupo cociente de G por H.

2. Si $g \in G$, como $\rho'(g) = \rho(gH)$, entonces $\chi'(g) = Tr(\rho'(g)) = Tr(\rho(gH)) = \chi(gH) = \chi(\pi(g)) = \chi \circ \pi(g)$.

3. Si $W \subseteq V$ es G-invariante, entonces para todo $gH \in G/H$ se tiene que $gH \cdot w = \{gh \cdot w : h \in H\} \subseteq W$ para todo $w \in W$ ya que $gh \in G$. Por lo tanto G/H es G-invariante.

   Recíprocamente, si W es G/H-invariante, entonces para todo $g \in G$ y para todo $w \in W$, por definición de la acción $(\rho'(g) = \rho(gH))$ tenemos $g \cdot w := (gH) \cdot w \in W$, así W es G-invariante.

Si G es un grupo finito y χ es un caracter de G, por **??**(7) el conjunto

$$K_\chi := \{g \in G : \chi(g) = \chi(1)\}$$

es un subgrupo normal de G, al que se le llama núcleo de χ ya que es el núcleo representación correspondiente por 14.1(7). Si χ_i son los caracteres irreducibles de G, escribiremos $K_i := K_{\chi_i}$.

Proposición 2.0.2 *Los subgrupos normales de G son los conjuntos de la forma $\cap_{i\in I} K_i$, para algún $I \in \mathbb{I}_r = \{1, 2, ..., r\}$.*

Demostración: Supongamos que $H \lhd G$ y sean $\rho' : G/H \longrightarrow GL(V)$ la representación regular de G/H y χ' su caracter. Consideremos $\rho : G \longrightarrow G/H \longrightarrow GL(V)$ y sea χ su caracter. Por el ejemplo 2 del capítulo 14,

$$\chi'(gH) = \begin{cases} 0, & \text{si } gH \neq H, \\ |G|, & \text{si } gH = H \end{cases}$$

y así, por el lema $\chi = \chi \circ \pi$, entonces

$$\chi(g) = \chi'(gH) = \begin{cases} 0, & \text{si } g \notin H, \\ |G|, & \text{si } g \in H \end{cases}$$

por lo que

$$\chi(g) = \chi(1) \iff g \in H.(*)$$

Se sigue que $K_\chi = H$. Ahora escribamos $\chi = \sum_i n_i \chi_i$, con $n_i \geq 0$ y χ_i los caracteres irreducibles de G. De 14.1(6) y por desigualdad triangular se tiene que

$$|\chi(g)| \leq \sum_i n_i |\chi_i(g)| \leq \sum_i n_i \chi_i(1) = \chi(1)$$

para todo $g \in G$. Se sigue que

$$g \in K_\chi \iff \chi(g) = \chi(1) \iff g \in K_i, \forall i, n_i > 0(\dagger)$$

(ya que $|\chi_i(g)| \leq \chi_i(g)$?? por 14.1(6)). Por lo tanto, de (*) y $(\dagger)$ se sigue que

$$g \in H \iff g \in K_i, \forall i, n_i > 0 \iff g \in \cap_{i\in I} K_i, I = \{i : 1 \leq i \leq r, n_i > 0\}.$$

Para el recíproco, como cada $K_i \lhd G$, para $i \in I$, entonces $\cap_{i\in I} K_i \lhd G$.

Usando la proposición anterior, es bastante sencillo, mirando la tabla de caracteres de un grupo finito, decidir si es o no simple:

Corolario 2.0.3 *Un grupo finito G es simple si y sólo si el único caracter irreducible χ_i de G para el cual $\chi_i(g) = \chi_i(1)$, para algún $g \neq 1$ en G, es el caracter principal χ_1.*

Demostración: Si G es simple y si sucediera que $\chi_i(g) = \chi_i(1)$ para algún $i > 1$ y algún $g \neq 1$, entonces $g \in K_i \lhd G$, una contradicción.

Recíprocamente, si G no fuera simple, entonces existiría un $H \lhd G$ propio y con $H \neq 1$, i.e., existiría $g \neq 1$ en H. Por la proposición anterior, $H \subseteq K_i$ para algún $i > 1$ y por lo tanto $\chi_i(g) = \chi_i(1)$, en contradicción con la hipótesis.

Corolario 2.0.4 *La tabla de caracteres de un grupo finito G se puede usar para determinar si G es o no soluble.*

Demostración: La tabla de caracteres de G nos da todos los núcleos de K_i y la proposición anterior nos da todos los subgrupos normales de G y todas las relaciones de inclusión entre ellos, en términos de esos núcleos. Por lo tanto, la tabla de caracteres nos permite determinar todas las series normales de G y los órdenes de los términos involucrados. En particular, nos permite determinar si G tiene o no una serie normal cuyos cocientes sean abelianos.

Lema 2.0.5 *Si χ es un caracter irreducible de un grupo finito G, entonces para todo $g \in G$ el número complejo $[G : C_G(g)]\chi(g)/\chi(1)$ es un entero algebraico.*

Demostración: Sea $\rho : G \longrightarrow GL(W)$ una representación irreducible con caracter χ. Sean $g \in G$ y C_g su clase de conjugación. Consideremos la función $f : W \longrightarrow W$ dada por $f = \sum_{s \in C_g} \rho(s)$ y observe que, para todo $\sigma \in G$ se tiene que $\rho(\sigma) \circ f = f \circ \rho(\sigma)$ ya que $\rho(\sigma)^{-1} f \rho(\sigma) = \sum_{s \in C_g} \rho(\sigma)^{-1}\rho(s)\rho(\sigma) = \sum_{s \in C_g} \rho(\sigma^{-1} s \sigma) = f$, la última igualdad por definición de f y porque $\sigma^{-1}s\sigma$ recorre C_g cuando s lo hace. Se sigue que $f\rho(\sigma) = \rho(\sigma)f$ como se quería. Podemos entonces aplicar el lema de Schur, 13.5(2), y así existe un escalar $\lambda \in \mathbb{C}$ tal que $f = \lambda \cdot id_W$. Tomando trazas en esta igualdad obtenemos:

$$\begin{aligned} \lambda \cdot \chi(1) = Tr(\lambda \cdot id_W) &= Tr(f) = Tr(\sum_{s \in C_g} \rho(s)) = \sum_{s \in C_g} \chi(s) \\ &= \sum_{s \in C_g} \chi(g), (\chi(s) = \chi(g), \forall a \in C_g) \\ &= |C_g|\chi(g) = [G : C_g(g)]\chi(g) \end{aligned}$$

y así $\lambda = [G : C_G(g)]\chi(g)/\chi(1)$.

Ahora sea $R : G \longrightarrow GL(V)$ la representación regular de G y recordemos que como $\rho : G \longrightarrow W$ es irreducible, la podemos ver como una subrepresentación (irreducible) de R (14.8). Ahora, si $h : V \longrightarrow V$ es la función lineal dada por $h = \sum_{s\in C_g} \rho(s)$, notamos que $h|_W = f$ y que $R(\sigma) \circ h = h \circ R(\sigma)$, para todo $\sigma \in G$ (se demuestra de forma análoga a como lo hicimos para f), y como $f = \lambda \cdot id_W$, entonces λ es un valor propio de h y así existe un $v \neq 0$ en $w \subseteq V$ tal que $h(v) = \lambda v$, por lo que si A es la matriz asociada a R con respecto a la base $\{v_g\}_{g\in G}$ de V, se tiene que $det(\lambda I_n - A) = 0$. Observamos ahora que, por el ejemplo 5 del capítulo 13, cada entrada de la matriz A de la representación regular es 0 ó 1. Se sigue que el polinomio característico $\phi(x) := det(xI_n - A)$ es mónico con coeficientes enteros y como λ es raíz de este polinomio, entonces λ es un entero algebraico, como se quería.

Una consecuencia importante es que el grado de cualquier representación irreducible divide al orden del grupo.

Teorema 2.0.6 *Si χ es un caracter irreducible de G, entonces $\chi(1)$ divide a $|G|$.*

Demostración: Sea $g_1, ..., g_r$ un conjunto completo de representantes de las clases de conjugación de G. Por el lema previo, $[G : C_G(g_i)]\chi(g_i)/\chi(1)$ es un entero algebraico para cada g_i, y por 14.1 (5) y (4) también cada $\overline{\chi(g_i)}$ es un entero algebráico. Ahora, usando ortogonalidad por renglones, se tiene que

$$\frac{|G|}{\chi(1)} = \frac{1}{\chi(1)} \sum_{i=1}^{r} [G : C_G(g_i)]\chi(g_i)\overline{\chi(g_i)} = \sum_{i=1}^{r} [G : C_G(g_i)] \frac{\chi(g_i)}{\chi(1)} \overline{\chi(g_i)}$$

donde cada sumando en el lado derecho es un entero algebraico. Se sigue que el número racional $|G|/\chi(1)$ es un entero algebraico y por A.11 está en $\mathbb{Z}$, i.e., $\chi(1)$ divide a $|G|$.

Para probar el teorema de Burnside, necesitaremos el lema siguiente:

Lema 2.0.7 *Sean χ un caracter de G y $g \in G$. Pongamos $\gamma := \chi(g)/\chi(1)$. Si γ es un enterno algebraico no nulo, entonces $|\gamma| = 1$.*

Demostración: Si n es el orden del elemento g, por 14.1(4), $\chi(g)$ es una suma de $\chi(1)$ raíces n-ésimas de la unidad, digamos $\chi(g) = \omega_1 + ... + \omega_{\chi(1)}$, y así

$$|\chi(g)| \leq |\omega_1| + ... + |\omega_{\chi(1)}| \leq 1 + ... + 1 = \chi(1)$$

y por lo tanto

$$|\gamma| = \frac{|\chi(g)|}{|\chi(1)|} \leq 1$$

y como $\gamma \neq 0$, entonces $0 < |\gamma|$. Si sucediera que $0 < |\gamma| < 1$, mostraremos que $\chi(g) = 0$. En efecto, sea $p(x) = x^t + a_{t-1}x^{t-1} + ... + a_1 t + a_0$ el polinomio mónico irreducible del cual γ es raíz. Por A.15, $p(x)$ tiene coeficientes en $\mathbb{Z}$. Ahora, como

$$\gamma = \frac{1}{d}(\omega_1 + ... + \omega_{\chi(1)})$$

con $d := \chi(1)$ y $\omega_i \in \mu_n$, entonces, por A.10, todo conjugado algebraico γ' de γ es de la forma

$$\gamma' = \frac{1}{d}(\omega'_1 + ... + \omega'_{\chi(1)}),$$

(donde los ω'_j son raíces de la unidad, porque son conjugados de ω_j que satisface $x^n - 1$), por lo que $0 < |\gamma| < 1$ implica que $0 < |\gamma'| \leq 1$ y así el producto de los conjugados algebraicos de γ (incluyendo a γ) satisface que

$$|\prod \gamma'| < 1,$$

ya que $|\gamma| < 1$. Pero, como los γ' son las raices de $p(x)$, entonces el producto de éstas raíces es $\pm a_0$ (término independiente de $p(x)$), i.e.m $|a_0| < 1$ con $a_0 \in \mathbb{Z}$, por lo que $a_0 = 0$, y como $p(x)$ es irreducible,ésto implica que $p(x) = x$ y por lo tanto $\gamma = 0$ es su única raíz, i.e., $\chi(g)/\chi(1) = 0$ y así $\chi(g) = 0$, una contradicción con la hipótesis del lema. Se sigue que $|\gamma| = 1$.

Teorema 2.0.8 *(Burnside) Sea G un grupo finito. Si G tiene una clase de conjugación cuyo orden es la potencia (no trivial) de un primo, entonces G no es simple.*

Demostración: Note que G no puede ser abeliano, y que si lo fuera todas sus clases de conjugación tendrían un único elemento, en contradicción con la hipótesis del teorema.

Ahora, por hipótesis existe un elemento $1 \neq g$ en G cuya case de conjugación es de orden p^t, para p un primo y $t \geq 1$ entero. De la ortogonalidad por columnas de la tabla de caracteres de G, se tiene que si $\chi_1, ..., \chi_r$ son los caracteres irreducibles de G, entonces

$$\begin{aligned} 0 &= \sum_{i=1}^{r} \chi_i(g)\overline{\chi_i(1)}, (g \neq 1, \delta_{ij} = 0) \\ &= \sum_{i=1}^{r} \chi_i(g)\chi_i(1), (Im(\chi_i(1)) = 0) \\ &= 1 + \sum_{i=2}^{r} \chi_i(g)\chi_i(1), (\chi_1(g) = \chi_1(1) = 1) \end{aligned}$$

Dividiendo entre el primo p obtenemos

$$-\frac{1}{p} = \sum_{i=2}^{r} \chi_i(g)\chi_i(1)/p$$

y como $-1/p$ no es un entero algebraico, entonces uno de los sumandos $\chi_i(g)\chi_i(1)/p$ no es un entero algebraico, para $2 \leq i \leq r$, y como $\chi_i(g)$ sí es un entero algebraico, esto implica que $p \nmid \chi_i(1)$ (y también que $\chi_i(g) \neq 0$).

Ahora, como $[G : C_G(g)] = p^t$ y como $p \nmid \chi_i(1)$, entonces $[G : C_G(g)]$ es coprimo con $\chi_i(1)$ y así el 1 es combinación lineal de estos dos enteros:

$$1 = a[G : C_G(g)] + b\chi_i(1)$$

para algunos enteros a, b. Se sigue que

$$\frac{\chi_i(g)}{\chi_i(1)} = \frac{a[G : C_G(g)]\chi_i(g)}{\chi_i(1)} + b\chi_i(1)$$

donde, por el lema 15.5, el primer sumando de la derecha es un entero algebraico y como el segundo sumando también lo es, entonces $\chi_i(g)/\chi_i(1)$ es un entero algebraico $\neq 0$ y así, por el lema previo se sigue que su módulo es 1 por lo que $|\chi_i(g)| = |\chi_i(1)| = \chi_i(1)$.

Ahora, sea $\rho_i : G \longrightarrow GL(W_i)$ la representación correspondiente al caracter χ_i. Observe que como, para $g \in G$, $\chi_i(g)$ es una suma de $\chi_i(1)$ raíces de la unidad, entonces

$$|\chi_i(g)| = \chi_i(1) \iff \rho_i(g) : W_i \longrightarrow W_i$$

tiene un único valor propio, digamos λ_g, ya que si $|\chi_i(g)| = \chi_i(1)$, como en la demostración del lema anterior, si n es el orden del elemento g, por 14.1(4), $\chi_i(g)$ es una suma de $\chi_i(1)$ raices n-ésimas de la unidad, digamos ω_j, y así

$$|\chi_i(g)| = |\omega_1 + ... + \omega_{\chi_i(1)}| = \chi_i(1)$$

y por desigualdad del triángulo, la igualdad anterior sólo puede suceder si todos los ω_i son iguales (a un ω, digamos, con módulo 1); se sigue que $\chi_i(g) = n_i\omega$, con $n_i = \chi_i(1)$, por lo que la matriz diagonal asociada a $\rho_i(g)$ tiene a ω en su diagonal n_i veces, y por lo tanto $\rho_i(g) = \omega id_{W_i}$. Recíprocamente, si $\rho_i(g) = \lambda_g$, entonces λ_g es una raíz de la unidad y

$$|\chi_i(g)| = |Tr(\lambda_g id_{W_i})| = |n_i\lambda_g| = n_i = \chi_i(1)$$

como se quería. Así, $\rho_i(g)v = \lambda_g v$, para todo $v \in W_i$. Sea $K_i = ker\rho_i \lhd G$. Como χ_i no es trivial, entonces $K_i \neq G$. Si $K_i \neq 1$, entonces G no sería simple y ya acabamos.

Si $K_i = 1$, entonces ρ_i es inyectivo y observando ahora que la matriz de $\rho_i(g)$, con respecto a cualquier base de W_i, es una matriz diagonal con el único valor propio λ_g de $\rho_i(g)$ en la diagonal, se sigue que esta matriz conmuta con todas las matrices de la imagen $\rho_i(G)$ de ρ_i y así

$$\rho_i(gh) = \rho_i(g)\rho_i(h) = \rho_i(h)\rho_i(g) = \rho_i(hg)$$

para todo $h \in G$, y como ρ_i es inyectiva, la igualdad anterior implica que $gh = hg$ para todo $h \in G$, i.e., $g \in Z(G)$ por lo que $Z(G) \neq 1$. Pero $Z(G) \neq G$, porque G no es abeliano. Se sigue que $1 \neq Z(G) \lhd G$ y por lo tanto G no es simple.

Teorema 2.0.9 *(Burnside) Si $|G| = p^r q^s$ con p, q primos, entonces G es soluble.*

Demostración: Por inducción sobre el orden de G (de hecho, sobre $r + s$). Si $r + s = 1$, entonces $r = 1$ y $s = 0$, o viceversa; en cualquier caso G sería de orden primo y por lo tanto soluble.

Supongamos ahora que $r + s > 1$ y que el teorema es válido para grupos G de orden $p^a q^b$ con $a + b < r + s$. Sea Q un q-subgrupo de Sylow de G. Si $Q = 1$, entonces G es un p-grupo y por lo tanto es soluble. Supongamos entonces que $Q \neq 1$; como Q es un q-grupo, su centro $Z(Q) \neq 1$ por 9.10, y así existe un $1 \neq g \in Z(Q)$, por lo que g conmuta con todos los elementos de Q y así $Q \subseteq C_G(g)$. Las inclusiones $Q \subseteq C_G(g) \subseteq G$ implican que $[G : Q] = [G : C_G(g)][C_G(g) : Q]$ y como $[Q] = q^s$ (por ser un q-subgrupo de Sylow), entonces

$$[G : Q] = \frac{|G|}{|Q|} = \frac{p^r q^s}{q^s} = p^r.$$

Se sigue que $[G : C_G(g)]$ divide a p^r y así $[G : C_G(g)] = p^t$ para algún $t \leq r$.

Caso 1: Si $t = 0$, $G = C_G(g)$ y así g conmuta con todos los elementos de G, or lo que $q \neq g \in Z(G)$ y por lo tanto $1 \neq Z(G) \lhd G$, y como G no es abeliano $Z(G) \neq G$, y así G no es simple.

Caso 2: Si $t > 0$, como $p^t = [G : C_G(g)]$ es el número de elementos en la clase de conjugación de g, por 8.2 y el ejemplo 12 del capítulo 8, entonces el teorema anterior implica que G no es simple.

En cualquiera de los dos casos hemos mostrado que G no es simple y así tiene un subgrupo normal propio $H \lhd G$ que, por el teorema de Lagrange, tienen orden de la forma $|H| = p^a q^b$ con $a + b < r + s$ y consecuentemente, por la hipótesis de inducción, H es soluble. El cociente G/H también tiene orden de la forma $p^\alpha q^\beta$ con $\alpha + \beta < r + s$, y por lo tanto también es soluble por la hipótesis de inducción. De 11.6(3) se sigue que G también es soluble.

2.1 Caracteres inducidos y grupos de Forbenius

En **??** mostramos que la teoría de caracteres se puede usar para determinar los subgrupos normales de un grupo finito dado, sencillamente examinando las soluciones de la ecuación

$$\chi(\sigma) = \chi(1)$$

para un carácter arbitrario χ de G. Usando ésto en esta última parte, probaremos un teorema de Frobenius que identifica un subgrupo normal de un grupo de permutaciones bajo ciertas condiciones y al final reformulamos este resultado en forma abstracta descomponiendo un grupo, bajo ciertas hipótesis en un producto. A diferencia del teorema $p^a q^b$ de Burnside, para este teorema de Frobenius no existe una demostración sin usar teoría de caracteres y es una aplicación hasta cierto punto mas sencillo (no usa la teoría de números algebraicos), de la teoría de caracteres para probar un resultado de teoría de grupos pura. Antes de proceder al teorema de Frobenius, necesitaremos algunos resultados sobre caracteres.

2.2 Representaciones y caracteres inducidos

Si G es un grupo y $H \subseteq G$ es un subgrupo de índice finito, dada una representación de H, $\rho : H \longrightarrow GL(k, \mathbf{C})$, Frobenius construye una representación de G que extiende a la representación de H dada como sigue:
Para extender ρ a G, primero se define $\rho(\sigma) = 0$ para $\sigma \in G - H$ y notamos que esta extensión de ρ en G no define una representación, tan solo por el hecho de que si $\sigma \in G - H$, $\rho(\sigma) = 0$ no es invertible. Lo que Frobenius hace, usando el subgrupo H, es considerar la partición de G en clases laterales (digamos izquierdas) de H

$$G = g_1 H \cup ... \cup g_n H$$

donde $n = [G : H]$ y los $g_1, ..., g_n$ son representantes dados de las clases laterales izquierdas de H en G. Luego, para cada $\sigma \in G$,define una matriz de tamaño knxkn como un arreglo de nxn bloques de tamaño kxk, donde cada bloque es la matriz $\rho(g_i^{-1}\sigma g_j)$, la cual es una matriz invertible si y solo si $g_i^{-1}\sigma g_j \in H$, y es la matriz cero de tamaño kxk si $g_i^{-1}\sigma g_j \notin H$. Así, se ha definido una función $\rho^G : H \longrightarrow GL(k, \mathbf{C})$ mediante

$$\rho^G(\sigma) = \begin{pmatrix} \rho(g_1^{-1}\sigma g_1) & \rho(g_1^{-1}\sigma g_2) & \cdots & \rho(g_1^{-1}\sigma g_n) \\ \rho(g_2^{-1}\sigma g_1) & \rho(g_2^{-1}\sigma g_2) & \cdots & \rho(g_2^{-1}\sigma g_n) \\ \vdots & \vdots & \ddots & \vdots \\ \rho(g_n^{-1}\sigma g_1) & \rho(g_n^{-1}\sigma g_2) & \cdots & \rho(g_n^{-1}\sigma g_n) \end{pmatrix}$$

Lema 2.2.1
La función $\rho^G : G \longrightarrow GL(kn, \mathbf{C})$ así definida es una representación de G.

Demostración: Queremos probar que $\rho^G(\sigma\tau) = \rho^G(\sigma)\rho^G(\tau)$, para $\sigma, \tau \in G$. Comparando el bloque (ij) en ambos lados de esta igualdad, el correspondiente al lado izquierdo es $\rho(g_i^{-1}\sigma g_j)$ y el correspondiente al lado derecho por definición de producto de matrices, es

$$\sum_{k=1}^{n} \rho(g_i^{-1}\sigma g_k)\rho(g_k^{-1}\sigma g_j)$$

Así, lo que queremos probar es

$$\rho(g_i^{-1}\sigma\tau g_j) = \sum_{k=1}^{n} \rho(g_i^{-1}\sigma g_k)\rho(g_k^{-1}\tau g_j) \tag{2.1}$$

y se tienen dos casos, dependiendo del lado izquierdo:

Caso 1 Supongamos que $g_i^{-1}\sigma\tau g_j \notin H$. Entonces, el lado izquierdo de (2.1) es la matriz cero, para el lado derecho de (2.1) veremos que, para cada k, ya sea que $g_i^{-1}\sigma g_k \notin H$ o que $g_k^{-1}\tau g_j \notin H$. En efecto, suponiendo lo contrario se tendría

$$g_i^{-1}\sigma\tau g_j = (g_i^{-1}\sigma g_k)(g_k^{-1}\tau g_j) \in H$$

Lo cual contradice lo que estamos asumiendo en este caso. Se sigue que cada sumando del lado derecho de (2.1) es cero y por lo tanto se tiene la igualdad deseada.

Caso 2 Supongamos ahora que $v := g_i^{-1}\sigma\tau g_j \in H$. Consideremos entonces al elemento τg_i, este pertenece a una única clase lateral, digamos $g_t H$. y así $\tau g_i = g_t u$ para algún $u \in H$. Entonces, $g_t^{-1}\tau g_j = u \in H$, y para $k \neq t$ se tiene que $\tau g_i \notin g_k H$ (solo puede estar en una clase lateral) por lo que $g_k^{-1}\tau g_j \notin H$ y así el sumando correspondiente en el lado derecho de (2.1) es cero; se sigue que el único sumando sobreviviente en el lado derecho de (2.1), es cuando $k = t$, es decir

$$(g_i^{-1}\sigma g_t)(g_i^{-1}\tau g_j)$$

donde para cada $v = g_i^{-1}\sigma\tau g_j \in H$ y $u = g_t^{-1}\tau g_j \in H$ se tiene que $vu^{-1} = g_i^{-1}\sigma g_t$ por lo que la igualdad (2.1) es equivalente a

$$\rho(v) = \rho(vu^{-1})\rho(u)$$

la cual es verdadera porque u, v, vu^{-1} pertenecen a H y ρ es un homomorfismo.

La representación $\rho^G : G \longrightarrow GL(kn, \mathbf{C})$ del lema (2.2.1), se dice que es inducida de la representación $\rho : H \longrightarrow GL(k, \mathbf{C})$ del subgrupo H. Ahora, si χ es el carácter de H asociado a ρ y si denotamos con χ^G al carácter de G correspondiente a ρ^G, se tiene que:

$$\chi^G(\sigma) = Tr\rho^G(\sigma) = \sum_{i=1}^{n} Tr\rho(g_i^{-1}\sigma g_j) = \sum_{i=1}^{n} \chi(g_i^{-1}\sigma g_j)$$

donde, si $g_i^{-1}\sigma g_j \notin H$ usamos la convención de que $\chi(g_i^{-1}\sigma g_j) = 0$ en conformidad de que $\rho(g_i^{-1}\sigma g_j)$ es la matriz cero.

Observación En la definición de ρ^G, y por lo tanto en la del carácter χ^G, usamos un sistema particular de representantes $g_1, ..., g_n$ de las clases laterales izquierdas de H en G. Veamos a continuación que el carácter χ^G no depende de la elección de estos representantes. Para esto, supongamos que $\sigma_1, ..., \sigma_n$ son otros representantes, digamos $\sigma_i \in g_iH$, es decir, $\sigma_i = g_ih_i$ con $h_i \in H$.Se tiene entonces que

$$\sigma_i^{-1}\sigma\sigma_i = h_i^{-1}(g_i^{-1}\sigma g_i)h_i$$

con $h_i \in H$ por lo que $\sigma_i^{-1}\sigma\sigma_i \in H$ si y solo si $g_i^{-1}\sigma g_i \in H$ y como estos son elementos conjugados en H por la ecuación anterior, entonces $\chi(\sigma_i^{-1}\sigma\sigma_i) = \chi(g_i^{-1}\sigma g_i)$ por lo que

$$\sum_{i=1}^{n} \chi(\sigma_i^{-1}\sigma\sigma_i) = \sum_{i=1}^{n} \chi(g_i^{-1}\sigma g_i) = \chi^G(\sigma)$$

como se quería.

Hay otra forma de escribir la formula para el carácter inducido χ^G. Por ejemplo, si $g_1H, ...g_nH$ son las clases laterales izquierdas de H en G, podemos elegir como representantes a elementos de la forma $\sigma_i = g_iu$ con $u \in H$ fijo. Se tiene entonces que

$$\chi^G(\sigma) = \sum_{i=1}^{n} \chi((g_iu)^{-1}\sigma(g_iu) = \sum_{i=1}^{n} \chi((u^{-1}g_i^{-1}\sigma g_iu) \tag{2.2}$$

y sumando sobre u en H, el lado izquierdo de (2.2) es constante y así queda multiplicado por $|H|$, mientras que el lado derecho de (2.2) al recorrer u en el subgrupo H, como $G = g_1H \cup ... \cup g_nH$, los productos g_iu recorren todo el grupo G exactamente una vez y por lo tanto (2.2) queda

$$|H|\chi^G(\sigma) = \sum_{\tau \in G} \chi(\tau^{-1}\sigma\tau)$$

y así

$$\chi^G(\sigma) = \frac{1}{|H|}\sum_{\tau\in G}\chi(\tau^{-1}\sigma\tau)$$

Ejemplo Si $H \subseteq G$ es un subgrupo de índice finito n y si $g_1H, ..., g_nH$ son las clases laterales izquierdas de H en G, consideremos el carácter trivial ξ del subgrupo H, es decir $\xi(h) = 1$ para todo $h \in H$;pero entonces, el carácter inducido ξ^G de G está dado por (2.2):

$$\xi^G(\sigma) = \sum_{i=1}^{n}\xi(g_i^{-1}\sigma g_i)$$

y para identificar este carácter de G, consideremos la presunción por permutaciones de G dada por la acción de G en el conjunto G/H de clases laterales izquierdas de H mediante traslación izquierdas, es decir

$$G \times G/H \longrightarrow g/H$$

$$(\sigma, g_iH) \longrightarrow (\sigma g_i)H$$

y se——a χ el carácter de esta representación de G.
Recordemos que $\chi(\sigma) = |(G/H)^\sigma|$ es el numero de elementos g_iH de G/H fijado por σ. Observamos ahora que $\sigma g_iH = g_iH$ si y solo si $g_i^{-1}\sigma g_i \in H$ por lo que el numero $\chi(\sigma)$ de clases de G/H fijadas por σ es igual al número de elementos de la forma $g_i^{-1}\sigma g_i$ que están en H y este número es $\sum_{i=1}^{n}\xi(g_i^{-1}\sigma g_i)$ ya que cada uno de estos sumandos es 1 cuando $g_i^{-1}\sigma g_i \in H$ porque ξ es el carácter trivial. Hemos identificado de este modo el carácter inducido ξ^G como el carácter χ

2.3 Caracteres virtuales

Si G es un grupo finito y si $\chi_1, ..., \chi_r$ son todos los caracteres irreducibles de G, tenemos que todos los caracteres irreducibles de χ de G son combinación lineales de la forma

$$\chi = a_1\chi + ... + a_r\chi \tag{2.3}$$

con los coeficientes a_i enteros no negativos, y en general, por (**??**) toda función de clases en G es una combinación lineal como la anterior pero con los coeficientes a_i en $\mathbf{C}$. Si ξ es una función de clases en G de la forma (2.3) pero con los coeficientes $a_i \in \mathbf{Z}$ enteros positivos, negativos o cero, diremos que ξ es un carácter virtual de G. Notemos que si hay coeficientes negativos, por la observación mencionada antes, la función ξ no es un carácter de G, es decir, no existe una representación de G cuya traza se ξ. Ahora, si $\xi = a_1\chi_1 + ... + a_r\chi_r$ es el carácter virtual de G, entonces usando el producto interno definido antes de **??** se tiene que

$$< \xi, \xi >= a_1^2 + ... + a_r^2$$

y por lo tanto, si $< \xi, \xi >= 1$ entonces exactamente uno de los coeficientes en $\xi = a_1\chi_1 + ... + a_r\chi_r$ es ± 1 y los otros son cero. Hemos así probado la siguiente proposición:

Proposición 2.3.1
Si ξ es un carácter virtual de G tal que $< \xi, \xi >= 1$, entonces $\xi = \pm\chi$, donde χ es un carácter irreducible de G. Si además $\xi(1) > 0$, entonces $\xi = \chi$ es un carácter irreducible de G

2.4 Grupo de Frobenius

A continuación probaremos, usando teoría de caracteres, un celebrado teorema de Frobenius que describe una clase importante de grupos, formulandolos en el lenguaje de acciones de grupos (grupos de permutaciones).

Teorema 2.4.1
Sea G un grupo finito que actúa transitivamente sobre un conjunto X de cardinalidad n. Si todas las permutaciones de G, excepto por la identidad, tienen a lo más un punto fijo, entonces el conjunto de elementos de G sin puntos fijos, junto con la identidad, es un subgrupo normal de G de orden n

Demostración: Por la transitividad de la acción, existen permutaciones $p_i \in G$ tales que $p_1(1) = 1, p_2(1) = 2, ..., p_n(1) = n$. Podemos suponer que $p_1 = 1$ es la identidad de G. Ahora, el estabilizador de $i \in \mathbf{I}_n$ es el grupo

$$H_i = p_i H_1 p_i^{-1}$$

donde h_1 es el estabilizador de $1 \in \mathbf{I}_n$. En efecto, como $H_i = \{\sigma \in G : \sigma i = i\}$, si $\sigma \in H_i$, entonces

$$\begin{aligned} p_i\sigma p_i^{-1}(i) &= p_i\sigma(1) \text{ ya que } p_i(1) = i \\ &= p_i(1) \text{ ya que } \sigma \in H_1 \\ &= i \text{ porque } p_i(1) = i \end{aligned}$$

y así $p_i\sigma p_i^{-1} \in H_i$. Recíprocamente, si $\tau \in H_i$ notemos que

$$p_i^{-1}\tau p_i(1) = p_i\tau(i) = p_i(i = 1)$$

y así $p_i^{-1}\tau p_i \in H_1$, digamos $p_i^{-1}\tau p_i = u \in H_1$ y por lo tanto $\tau = p_i u p_i^{-1} \in p_i H_1 p_i^{-1}$, como se quería.
Por otra parte, si σH_1 es cualquier clase lateral izquierda de H_1 en G y si el representante σ manda 1 en i, entonces $\sigma \in p_i H_i$ y recíprocamente. En efecto, si σ manda 1 en i, se $\tau \in H_1$ la permutación dada por $\tau(1) = 1$ y $\tau(j) = \sigma(j)$ si $j \neq 1$. Entonces, $\sigma = p_i\tau \in p_i H_i$, y el recíproco es claro.
Se sigue que $p_1 H_1, ..., p_n H_1$ son todas las clases laterales izquierdas de H_1 en G, y son diferentes entre sí porque si $p_i H_1 = p_j H_1$, entonces $p_i \in p_j H_1$ y así p_i manda 1 en i y también manda el 1 en j por lo que se debe tener que $i = j$. Entonces

$$G = p_1 H_1 \cup ... \cup p_n H_1$$

y $[G : H_1] = n$, por lo que el cardinal n de X (a veces se le llama el grado de G) divide a su orden, es decir, si $|G| = g$ y $|H| = h$, entonces $g = nh$.

Ahora la hipótesis de que excepto por la identidad, ninguna permutación de G tiene más de un punto fijo, en términos de estabilizadores quiere decir que $H_i \cap H_j = 1$ para $i \neq j$.
Consideremos $K^* := K - \{1\}$ los elementos distintos de 1 de un grupo K. Así, denotemos H_i^* el conjunto de permutaciones en G para las cuales i es el único punto fijo, y así, si W es la colección de permutaciones sin punto fijo, se tiene la participación de G

$$G = \{1\} \cup W \cup H_1^* \cup ... \cup H_n^*$$

Observe ahora que $p_1 = 1$ (la identidad) es la única permutación con n puntos fijos y las permutaciones que fijan exactamente un punto están en la unión

$$H_1^* \cup ... \cup H_n^*$$

y se tiene que $|H_i| = |H_1|$ ya que $H_i = p_i H_1 p_i^{-1}$, por lo que $|H_i^*| = h - 1$. Por lo tanto, G tiene $n(h-1)$ permutaciones que fijan un sólo punto y así el numero de permutaciones sin puntos fijos es

$$|W| = |G| - |\{1\}| - |H_1^* \cup ... \cup H_n^*| = g - 1 - n(h-1) = nh - 1 - nh + n = n - 1$$

Con esta información sobre la estructura del grupo G, es facil calcular el carácter inducido ψ^G de cualquier carácter ψ del subgrupo H_1. Recordemos que, por definición

$$\psi^G(\sigma) := \sum_{i=1}^{n} \psi(p_i^{-1}\sigma p_i) \tag{2.4}$$

porque $G = p_1H_1 \cup ... \cup p_nH_n$.
Ahora si $d = \psi(1)$ es el grado de ψ entonces usando 2.4 el grado de ψ^G es

$$\psi^G(1) = \sum_{i=1}^{n} \psi(p_i^{-1}(1)p_i) = \sum_{i=1}^{n} \psi(1) = nd \tag{2.5}$$

Tambien, si $u_j \in H_j^*$, como $H_j = p_jH_1p_j^{-1}$, escribamos $u_j = p_jup_j^{-1}$ con $u \in H_1$ y notemos $u \neq 1$ porque $u_j \neq 1$. Entonces

$$\psi^G(u_j) = \sum_{i=1}^{n} \psi(p_i^{-1}(u_j)p_i) = \sum_{i=1}^{n} \psi(p_i^{-1}p_j(u_j)p_j^{-1}p_i) \tag{2.6}$$

y el i-ésimo termino de esta suma es distinto de cero si y solo si $p_i^{-1}p_j(u_j)p_i^{-1}p_i \in H_1$ lo cual sucede si y solo si $p_j(u_j)p_i^{-1} \in p_iH_1p_i^{-1} = H_i$, es decir, si y solo si $H_J = H_i$ y esto pasa si y solo si $j = i$ por lo que 2.6 se reduce a

$$\psi^G(u_j) = \psi^G(p_i^{-1}(u)p_i) = \psi(u)$$

para $j = 1, ..., n$. Finalmente, si $w \in W$ entonces

$$\psi^G(w) = 0 \tag{2.7}$$

porque $p_i^{-1}wp_i \notin H_1$ para todo i ya que no fija a punto alguno.
Resumiendo, los valores del caracter ψ^G, en 1, $u_j \in H_j^*$ y $w \in W$ son

$$\psi^G(1) = nd \qquad \psi^G(u_j) = \psi(u) \qquad \psi^G(w) = 0$$

Ahora, para el carácter χ de la representación por permutaciones de G, recordemos que $\chi(\sigma)$ es el numero de puntos fijos de σ y así, para el carácter dado por $\theta(\sigma) = \chi(\sigma) - 1$, como para las permutaciones 1,u_j, w anteriores, los numeros de puntos fijos son n, 1 y cero respectivamente, los valores de θ son los siguientes

$$\theta(1) = n - 1 \qquad \theta(u) = 0 \qquad \theta(w) = -1$$

Ahora, para el caracter virtual ϵ dado por $\epsilon(\sigma) := \psi^G(\sigma) - d\theta(\Sigma)$, usando los calculos de ψ^G y θ anteriores se tiene que $\epsilon(1) = dn - d(n-1) = d$, $\epsilon(u_j) = \psi(u) - d(0) = \psi(u)$ y $\epsilon(w) = 0 - d(-1) = d$, por lo que

$$\epsilon(w) = \epsilon(1) \quad \forall w \in W \tag{2.8}$$

Notemos que la igualdad 2.8 parece identificar W con el núcleo de ϵ, sin embargo esto no es así porque

i) solo caracteres verdaderos identifican núcleos y ϵ es un carácter virtual.

ii) pueden haber otros elementos fuera de W que satisfacen la ecuación 2.8.

El primer problema se resuelve si en lugar de tener cualquier carácter ψ de H_1 se toma un carácter irreducible ρ de H_1, digamos de grado d, en la definición 2.4, observando entonces que el carácter virtual ϵ resulta en este caso un carácter irreducible de grado d. En efecto, como estamos suponiendo que $\rho(1) = d$ y que $< \psi, \psi >_{H_1} = 1$ porque es irreducible, entonces

$$\sum_{u \in H_1^*} |\psi(u)|^2 = \sum_{u \in H_1} |\psi(u)|^2 - |\psi(1)|^2 = \sum_{u \in H_1} < \psi(u), \psi(u) > -d^2 = h - d^2 \tag{2.9}$$

la ultima igualdad porque $< \psi(u), \psi(u) >= 1$ y $|H_1| = h$. Ahora, como $\epsilon(1) = d > 0$ para probar que ϵ es un carácter irreducible de G, de grado d, por 2.3.1, basta ver que $< \epsilon, \epsilon >= 1$. Ahora, como $G = \{1\} \cup W \cup (H_1^* \cup ... \cup H_n^*)$ entonces

$$\begin{aligned} \sum_{\sigma \in G} |\epsilon(\sigma)|^2 &= |\epsilon(1)|^2 + \sum_{w \in W} |\epsilon(w)|^2 + \sum_{j=1}^{n} (\sum_{u_j \in H_j^*} |\epsilon(u_j)|^2) \\ &= d^2 + (n-1)d^2 + n(h - d^2) \\ &= nh \\ &= g \end{aligned} \tag{2.10}$$

ya que $|W| = n - 1$, $\epsilon(w) = d$ para $w \in W$ y por 2.9, se sigue:

$$< \epsilon, \epsilon >= \frac{1}{|G|} \sum_{\sigma \in G} |\epsilon(\sigma)|^2 = \frac{1}{g}(g) = 1$$

y así por 2.3.1, ϵ es un caracter irreducible de G.
Para resolver el segundo problema, cambiaremos el carácer ϵ en 2.8 por otro carácter π para el cual $W \cup \{1\} = Ker\pi$. Para hacer esto, sean $\psi_1, ..., \psi_r$ todos los caracteres irreducibles de H_1 y sean $d_i = \psi_i(1)$ sus grados. Para el carácter ρ de la representación regular de H_1 sabemos que $\rho(1) = h$, $\rho(u) = 0$ para $u \neq 1$ y

$$\rho = \sum_{k=1}^{r} d_k \psi_k \tag{2.11}$$

Definiendo ahora carácteres ϵ_k de G en forma análoga a como se definió ϵ solo que ahora usando ψ_k en lugar de ψ, es decir $\epsilon_k = \psi_k^G - d_k\theta$ para $k = 1, ..., r$ notamos que los valores de ϵ_k son análogos a los de ϵ es decir:

$$\epsilon(1) = d_k \qquad \epsilon(1) = \psi_k(u) \qquad \epsilon(1) = d_k$$

Se define entonces el carácter π mediante

$$\phi := \sum_{k=1}^{r} d_k \epsilon_k$$

(es carácter porque los $d_k \geqslant 1$ son enteros) y sustituyendo los valores de ϵ_k se tiene que:
$\pi(1) = \sum_{k=1}^{r} d_k \epsilon_k(1) = \sum_{k=1}^{r} d_k^2 = h$
$\pi(1) = \sum_{k=1}^{r} d_k \epsilon_k(u_j) = \sum_{k=1}^{r} d_k \psi_k(u) = \rho(u) = 0$
$\pi w) = \sum_{k=1}^{r} d_k \epsilon_k(w) = \sum_{k=1}^{r} d_k^2 = h$
y por tanto $\pi(w) = \pi(1)$ si y solo si $w \in W$ por lo que para este carácter π se tiene que su núcleo es en efecto $\{1\} \cup W$ y de modo es un subgrupo normal de G de orden n como se quería.

Teorema 2.4.2 (Frobenius)
Si H es un subgrupo finito de un grupo G con la propiedad de que $\sigma H \sigma^{-1} \cap H = 1$, para todo $\sigma \in G - H$ entonces G tiene un subgrupo normal K tal que $G = KH$ y $H \cap K = 1$ (es decir, G es el producto semidirecto de K y H).

Demostración:
Para aplicar el teorema anterior lo primero que haremos sera ver al grupo abstracto como un grupo de permutaciones. Para esto consideremos la acción de G en el conjunto de clases laterales izquierdas G/H dada por $(\sigma, gH) \mapsto \sigma g H$ y la representación por permutaciones correspondiente $\rho : G \to Gl(n, \mathbf{C})$, donde $n = [G : H]$ y hemos elegido una partición de G en clases laterales de $H_1 G = g_1 H \cup ... \cup g_n H$ con $g_1 = 1$, recordemos que $\rho(\sigma)$ manda la clase $g_i H$ en $\sigma g_i H$, por lo que la clase $g_i H$ permanece fija bajo la acción de $\rho(\sigma)$ es decir $\sigma g_i H = g_i H$ si y solo si $g_i^{-1} \sigma g_i H = H$ es decir si y solo si $\sigma \in g_i H g_i^{-1}$.
Veremos que la representación es fiel es decir es inyectiva.
En efecto, si $\sigma \neq 1$ observe que $\rho(\sigma)$ no puede tener más de un punto fijo ya que si $g_i H$ y $g_j H$ quedan fijos bajo $\rho(\sigma)$, entonces $1 \neq \sigma \in g_i H g_i^{-1} \cap g_j H g_j^{-1}$ y por lo tanto $H \cap g_i^{-1} g_j H g_j^{-1} g_i \neq 1$ en contradicción con la hipótesis del teorema porque al estar suponiendo que $g_i H \neq g_j H$ se tiene que $g_i^{-1} g_j \notin H$. Esto nos dice que ρ es inyectiva y por lo tanto G es isomorfo a su imagen, que es el subgrupo de permutaciones de la forma

$$\begin{pmatrix} g_1 H & \cdots & g_n H \\ \sigma g_1 H & \cdots & \sigma g_n H \end{pmatrix}$$

y es claro que este grupo actúa transitivamente. También al probar la inyectividad de ρ mostramos que ningun elemento de G, con la excepción del anterior el conjunto $K1 \cup W$, con W la familia de elementos de G sin puntos fijos, es un subgrupo

normal de G de orden $n = [G : H]$.
Veremos ahora que los elementos de K estan en correspondecia biyectiva con las clases laterales en G/H. En efecto, como cada elemento de G pertenece a una única clase lateral, se tiene la función $K \to G/H$, la cual afirmamos es inyectiva. Para ver esto, supongamos que $w, w' \in K \cap g_i H$ y así $w^{-1}w' \in H$ y por lo tanto fija a la clase lateral $1H = H$. Pero como $w^{-1}w' \in K$, porque K es grupo, como el único elemento de K que fija algo es el 1 entonces $w^{-1}w' = 1$ es decir $w = w'$, por lo que la función $K \to G/H$ es inyectiva. Finalmente, como $|K| = n = |G/H|$, entonces la función inyectiva anterior debe ser suprayectiva. Podemos entonces denotar los elementos de K como $w_1 = 1$, w_2,...,w_n, donde $w_i \in g_i H$ de tal forma que los w_i se pueden usar como representantes de las clases laterales de H en G en lugar de los g_i. Se sigue que $G = KH$. Por otra parte, se tiene que $H \cap K = 1$ porque los elementos de K están en correspondencia biyectiva al 1 en K.
Cuando un grupo finito G tiene un subgrupo H que satisface el teorema anterior, se dice que G es un grupo de Frobenius y que H es un complemento de Frobenius; al subgrupo normal K cuya existencia asegura el teorema anterior, se le llama un núcleo de Frobenius

Capítulo 3

Teoría de categorías

3.1 Categorías

La teoría de categorías es una moderna manera de considerar la organización de las matemáticas permitiendo reunir en clases de objetos que tienen características similares para de esta forma su estudio sea más organizado y también para relacionar las diferentes clases con un proceso similar a construir funciones entre conjuntos. Así, $\mathcal{C}$ es una categoría si consta de lo siguiente:

1) Una clase $Ob(\mathcal{C})$, llamada clase de objetos de $\mathcal{C}$.

2) Para todo par de objetos $A, B \in Ob(\mathcal{A})$, un conjunto denotado por $Hom_{\mathcal{C}}(A, B)$ o $Mor_{\mathcal{A}}(A, B)$ (los subíndices pueden omitirse cuando está claro cuál es la categoría a la que se refieren). Los elementos de este conjunto se denominan morfismos de A a B. Un morfismo f de A a B se escribe también como $f : A \to B$.

3) Una operación binaria, denominada composición de morfismos y denotada por $\circ$. Dados tres objetos $A, B, C \in \mathcal{C}$, la composición define una aplicación $\circ : Hom(B, C) \times Hom(A, B) \to Hom(A, C)$. La composición de un morfismo $g : B \to C$ con un morfismo $f : A \to B$ se denota $g \circ f$. La operación composición satisface las siguientes propiedades:

    a) Asociativa: si $f : A \to B, g : B \to C$ y $h : C \to D$ son morfismos entre objetos $A, B, C, D \in \mathcal{C}$, entonces $h \circ (g \circ f) = (h \circ g) \circ f$.

    b) Existencia de identidad: para todo objeto $a \in \mathcal{C}$, existe un morfismo de A a sí mismo (es decir, un elemento de $Hom(A, A)$), denotado por I_A

denominado morfismo identidad, tal que, para morfismos cualesquiera $f : A \to B$ y $g : C \to A$, se tiene que $f \circ I_A = f$ y que $I_A \circ g = g$.

De este modo

$$\mathcal{C} = (\mathcal{C}, Hom(\mathcal{C}))$$

donde $Hom(\mathcal{C}) := \{Hom_{\mathcal{C}}(A, B) | A, B \in Ob(\mathcal{C})\}$. Si no existe confusión con respecto a la categoría podemos escribir $Hom(A, B)$ por $Hom_{\mathcal{C}}(A, B)$. Cuando se conoce el tipo de morfismos entre los objetos, nos referimos a la categoría simplemente como la colección de objetos que la conforma.

Ejemplo

- La categoría Set, cuyos objetos son los conjuntos y cuyos morfismos son las aplicaciones entre estos.
- La categoría Top, cuyos objetos son los espacios topológicos y cuyos morfismos son las aplicaciones continuas entre estos.
- La categoría Grp, cuyos objetos son los grupos y cuyos morfismos son los homomorfismos entre estos.
- La categoría Ab, cuyos objetos son los grupos abelianos y cuyos morfismos son los homomorfismos entre estos. Es subcategoría llena de Grp.
- La categoría Vec_K, cuyos objetos son los espacios vectoriales sobre un campo K y cuyos morfismos son las transformaciones lineales entre estos.

3.2 Funtores

Definición
Sean $\mathcal{C}$, $\mathcal{D}$ categorías, un **Funtor covariante** consta de la siguiente información:

$$F : \mathcal{C} \longrightarrow \mathcal{D}$$

1 Una asignación $F : Obj(\mathcal{C}) \longrightarrow Obj(\mathcal{D})$, es decir, para cada $C \in Obj(\mathcal{C})$ se tiene $F(C) \in Obj(\mathcal{D})$

2 Si $f : C \longrightarrow C'$ un morfismo en $\mathcal{C}$ entonces $F(C) \in Hom_{\mathcal{D}}(F(C), F(C'))$

3 Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ entonces $F(g \circ f) = F(g) \circ F(f)$

4 $\forall A \in Obj(\mathcal{C})$ se tiene $F(Id : A) = Id_{F(A)}$

Diremos F es **Funtor contravariantes** Si $f : C \longrightarrow C'$ un morfismo en $\mathcal{C}$ entonces $F(C) \in Hom_{\mathcal{D}}(F(C'), F(C))$

Ejemplo
Sea $\mathcal{C}$ una categoria, consideremos el funtor dado por

$$Id_{\mathcal{C}} : \mathcal{C} \longrightarrow \mathcal{C}$$

$$Id_{\mathcal{C}} : Obj(\mathcal{C}) \longrightarrow Obj(\mathcal{D})$$
$$C \longrightarrow C$$

y cada morfismo $f : C \longrightarrow C'$ en $\mathcal{C}$ tenemos $id = f$.
Caramente es un funtor.

Ejemplo Sean $\mathcal{C}, \mathcal{D}$ categorias, fijemos $D \in \mathcal{D}$ entonces se define $\overline{D} : \mathcal{C} \longrightarrow \mathcal{D}$ de la siguiente manera, a cada objeto de $C \in \mathcal{C}$ tenemos $\overline{D}(C) = D$ y si $f : C \longrightarrow C'$ morfismo en $\mathcal{C}$ entonces $id_D\overline{D}(f) : \mathcal{D} \longrightarrow \mathcal{D}$.
Por lo tanto $\overline{D}$ es funtor (Funtor constante).

Ejemplo
Sea $\mathcal{C}$ una categoria tal que $\forall \quad D, D' \in \mathcal{C}$ se tiene $Hom_{\mathcal{C}}(D, D') \in Con$ es decir D, D' son conjuntos con una estructura extra. Entonces tiene el siguiene funtor $\mathcal{U} : \mathcal{C} \longrightarrow Con$, (el funtor que olvida) donde $\mathcal{U}(C) = C$ es un conjunto y para $f : C \longrightarrow C'$ tenemos $\mathcal{U}(f) : C \longrightarrow C'$ es un morfismo de conjuntos.

Definición Sean $\mathcal{C} = R - Mod$ y $\mathcal{C}' = \mathbb{Z} - Mod$ y $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{C}'$ un funtor. Consideremos

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

una sucesión exacta corta en $\mathcal{C}$ diremos que un el funtor $\mathcal{F}$ es exacto izquierdo si

$$0 \longrightarrow \mathcal{F}(M') \xrightarrow{\mathcal{F}(f)} \mathcal{F}(M) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(M'')$$

es exacto izquierdo.
Dualmente diremos que $\mathcal{F}$ es exacto derecho si

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

una sucesión exacta corta en $\mathcal{C}$ entonces

$$\mathcal{F}(M') \xrightarrow{\mathcal{F}(f)} \mathcal{F}(M) \xrightarrow{\mathcal{F}(g)} \mathcal{F}(M'') \longrightarrow 0$$

es exacto derecho.

Proposición 3.2.1
Para todo $M \in R - Mo$ *el funtor* $H_*(M) := Hom(M, \_) : R - Mod \longrightarrow \mathbb{Z} - Mod$ *es exacto izquierdo.*

Demostración:
Consideremos la siguiente sucesión exacta corta de $R - Mod$

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

Así bajo H_* se tiene lo siguiente

$$H_*(M') \xrightarrow{H_*(f)} H_*(M) \xrightarrow{H_*(g)} H_*(M'')$$

PD $ImH_*(f) = KerH_*(g)$
Sabemos que $H_*(g)H_*(f) = H_*(gf) = H_*(0) = 0$ ya que la sucesion es exacta $gf = 0$ entonces $ImH_*(g) \subset KerH_*(f)$
Sea $\sigma \in KerH_*(g)$ tal que $H_*(g)(\sigma) = g\sigma = 0$ queremos encontrar $\alpha \in H_*(M')$ tal que $H_*(f)(\alpha) = \sigma$

$$\begin{tikzcd} & & N \arrow[dl, dashed, "\alpha"'] \arrow[d] \arrow[dr, "0"] & & \\ 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

Así $Im\sigma \subset Kerg \subset Imf$, esto nos dice $\forall y \in Im\sigma$, $y = \sigma(n)$ para algún $n \in N$ entonces $y = f(m')$ para algún $m' \in M'$ así definimos

$$\alpha : N \longrightarrow M$$
$$n \mapsto m'$$

tal que $\sigma(n) = f(m')$. Veamos que está bien definida para ello consideremos $m, m' \in M'$ tal que $\sigma(n) = f(m') = f(m)$ entonces $f(m - m') = 0$ por ser morfismo entonces $m - m' \in Kerf = \{0\}$ por ser inyectivo, por lo tanto $m = m'$.
Ahora para α morfismo, si $n, n' \in N$ con $\sigma(n') = f(m')$ y $\sigma(n) = f(m)$ entonces $\alpha(n + n') = m'' \in M'$ tal que

$$f(m'') = \sigma(n + n') = \sigma(n) + \sigma(n') = f(m) + f(m') = f(m + m')$$

Con f inyectiva tenemos $m'' = m + m'$ por lo tanto $\alpha(n + n') = m + m' = \alpha(n) + \alpha(n')$
Si $r \in R$, $n \in N$ tenemos $\alpha(rn) = m'$ y $r\alpha(n) = rm$ tal que $\sigma(rn) = f(m')$ y

$r\sigma(n) = rf(m) = f(rm)$, de este modo concluimos $m' = rm$.
Finalmente para ver $H_*(f)$ inyectivo consideremos $\sigma \in H_*M'$ tales que $H_*(f)(\sigma) = 0$ entonces $f \circ \sigma = 0$ esto implica $Im\sigma \subset Kerf = \{0\}$ por ser f inyectivo, de este modo $\sigma = 0$.
Por lo tanto $Hom(N, \_)$ es funtor exacto izquierdo.

Una pregunta importante es preguntarse cuando es exacto derecho, esto es cuando la sucesion es exacta derecha

$$0 \longrightarrow Hom(N, M') \longrightarrow Hom(N, M) \longrightarrow H_*(N, M'') \longrightarrow 0$$

Queremos para $\sigma : N \longrightarrow M''$ exista $\beta : N \longrightarrow M$ tal que $H_*(g)(\beta) = \sigma$ como se muestra en el diagrama

$$\begin{tikzcd} & & N \arrow[d, dashed, "\beta"'] \arrow[dr, "\sigma"] & & \\ 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

Esto es factoriza σ a través de g epimosfismo.

Definición
Un módulo $P \in R - Mod$ es proyectivo si el funtor $Hom(P, \_)$ es funtor exacto derecho.

Tomemos el funtor $Hom(\_, N)$ para todo $N \in R - Mod$ es contravariante.

Proposición 3.2.2
Para todo $N \in R - Mod$ tenemos $Hom(\_, N) : R - Mod \longrightarrow \mathbb{Z} - Mod$ es funtor exacto izquierdo.

Demostración:
Consideremos la siguiente sucesión exacta corta

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

Aplicando el funtor $Hom(\_, N)$ tenemos la siguiente sucesión

$$Hom(M'', N) \xrightarrow{H^*(g)} Hom(M, N) \xrightarrow{H^*(f)} H_*(M'', N)$$

$H^*(f)H^*(g) = H^*(gf) = H^*(0) = 0$ por ser la sucesión exacta. Por lo tanto $ImH^*(g) \subseteq KerH^*(f)$.

Ahora si $\sigma \in KerH^*(f)$ entonces $H^*(f)(\sigma) = \sigma f = 0$. De este modo existe $\alpha \in Hom(M'', N)$ tal que $H(g)(\alpha) = \sigma$, de este modo tenemos $Kerg = Imf \subseteq Ker\sigma$. Definamos

$$\begin{aligned} \overline{\sigma} : M'' &\longrightarrow N \\ m'' &\mapsto \sigma(m) \end{aligned}$$

Donde $m \in M$ es tal que $g(m) = m''$.
Supongamos existe $m' \in M$ tal que $g(m') = m''$ entonces $g(m') = g(m')$ esto implica $m' - m \in Kerg = Imf$ con lo cual $\sigma(m' - m) = 0$ por lo antes mencionado, de este modo $\sigma(m') = \sigma(m)$ y por lo tanto $\overline{\sigma} = \sigma(m') = \sigma(m)$,es decir, está bien definida.
Veamos ahora que $\overline{\sigma}$ es morfismo.
Si $m''_, m''_2 \in M''$ entonces $g(m_1) = m''_1$ y $g(m_2) = m''_2$ para algunos $m_1, m_2 \in M$, y $g(m_1 + m_2) = g(m_1) + g(m_2) = m''_1 + m''_2$. Así $\overline{\sigma}(m''_1 + m''_2) = \sigma(m)$ tal que $g(m_1 + m_2) = m''_1 + m''_2$ esto implica $\sigma(m) = \sigma(m_1 + m_2) = \sigma(m_1) + \sigma(m_2)$ y por lo tanto

$$\overline{\sigma}(m''_1 + m''_2) = \sigma(m_1) + \sigma(m_2) = \overline{\sigma}(m_1) + \overline{\sigma}(m_2)$$

Si $r \in R$, $m'' \in M''$ tal que $g(m) = m''$

$$\overline{\sigma}(rm) = \sigma(rm) = r\sigma(m) = r\overline{\sigma}(m)$$

Por tanto $\overline{\sigma}$ es morfismo

De acuerdo a la propician tenemos el funtor $Hom(\_, N)$ siempre es exacto izquierdo, y la pregunta que surge en este momento es ¿ cuando es exacto derecho?, para ello consideremos

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

Aplicando el funtor $Hom(\_, N)$ tenemos la siguiente sucesión

$$0 \longrightarrow Hom(M'', N) \xrightarrow{H^*(g)} Hom(M, N) \xrightarrow{H^*(f)} H_*(M'', N)$$

Se tendría que si $\sigma \in H_*(M'', N)$ entonces $\sigma : M'' \longrightarrow N$ entonces existe $\beta \in Hom(M, N)$ tal que $H^*(f)(\beta) = \sigma$, es decir $f\beta = \sigma$, como se muestra en el siguiente diagrama:

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\sigma"'] & M \arrow[r, "g"] \arrow[dl, dashed, "\beta"] & M'' \arrow[r] & 0 \\ & N & & & \end{tikzcd}$$

es decir β es una extensión de σ

Capítulo 4

Categoría R-Mod

En esta sección

4.1 Módulos

Sea G un grupo finito y V un k-espacio vectorial con una acción lineal

$$* := G \times V \longrightarrow V \Longleftrightarrow \rho := G \longrightarrow GL(V) \cong GL(dimV, k).$$

A continuación definamos el conjunto

$$K(G) = \{\sum_{\alpha}^{<\infty} a_\alpha g_\alpha : a_\alpha \in k, g_\alpha \in G\},$$

donde $a_\alpha = 0$ para casi todas las α.

Sean $\sum_\alpha a_\alpha g_\alpha, \sum_\beta b_\beta g_\beta \in K(G)$ y supongamos $\beta < \alpha$, entonces tenemos que $a_\beta = 0$ para cada $j > \beta$.

Definimos la suma $(+)$ en $K(G)$ como sigue:

$$\sum_\alpha a_\alpha g_\alpha + \sum_\beta b_\beta g_\beta \quad = \quad \sum_\alpha (a_\alpha + b_\alpha) g_\alpha$$

y el producto en $K(G)$ como sigue:

$$(\sum_\alpha a_\alpha g_\alpha)(\sum_\beta b_\beta g_\beta) \quad = \quad \sum_{\alpha'} c_{\alpha'} g_\alpha$$

considerando $c_{\alpha'} = (a_\alpha)(b_\beta)$ Mas aún $K(G)$ es un anillo conmutativo al que denominamos anillo de grupo.Notemos que considerando lo siguiente

$$\begin{aligned}(\sum_\alpha a_\alpha g_\alpha)v &= \sum_\alpha a_\alpha(g_\alpha \cdot v)\\ &= \sum_\alpha (a_\alpha g_\alpha)v\\ &= (\sum_\alpha a_\alpha g_\alpha v)\end{aligned}$$

$k(G) \times V \longrightarrow$ entonces

$$\begin{aligned}(\sum_\alpha a_\alpha g_\alpha)(v_1+v_2) &= \sum_\alpha a_\alpha(g_\alpha \cdot (v_1+v_2))\\ &= \sum_\alpha a_\alpha(g_\alpha \cdot v_1 + g_\alpha \cdot v_2)\\ &= \sum_\alpha (a_\alpha g_\alpha \cdot v_1 + a_\alpha g_\alpha \cdot v_2)\\ &= \sum_\alpha a_\alpha g_\alpha \cdot v_1 + \sum_\alpha a_\alpha g_\alpha \cdot v_2\end{aligned}$$

Por otro lado si $\sum_\alpha a_\alpha g_\alpha, \sum_\beta b_\beta g_\beta ink(G)$

$$\begin{aligned}(\sum_\alpha a_\alpha g_\alpha \sum_\beta b_\beta g_\beta)(v) &= (\sum_{\alpha\beta} a_\alpha b_\beta g_{\alpha\beta}) \cdot v\\ &= \sum_{\alpha\beta} a_\alpha b_\beta g_{\alpha\beta} \cdot v\\ &= \sum_\alpha a_\alpha g_\alpha \cdot (\sum_\beta b_\beta g_\beta v)\end{aligned}$$

Considerando $1_{k(G)} = 1_k \cdot e$ tenemos lo siguiente

$$\begin{aligned}(1_k \cdot e) \cdot v &= 1_k(e \cdot v)\\ &= 1_k \cdot v\\ &= v \quad \forall v \in V\end{aligned}$$

Además

$$(\sum_\alpha a_\alpha g_\alpha + \sum_\alpha b_\beta g_\beta)(v) = (\sum_{\alpha\beta} (a_\alpha + b_\beta) g_{\alpha\beta}) \cdot v$$

4.2 Submódulos

Tonemos la categoría de R-módulos izquierdos (resp. derechos).

Definición Sea M un R-módulo. Decimos que un subconjunto $N \subseteq M$ es un **submódulo** de M si $i : N \hookrightarrow M$ es un R-morfismo.

Equivalentemente las operaciones de M restringidas a N definen a N como R-módulo. Si $M \xrightarrow{f} N$ es un R morfismo entre R-módulos M, N. Entonces

$$\begin{aligned} ker(f) &= \{m \in M : f(m) = 0\} \\ Im(f) &= \{n \in N : \exists m \in M, f(m) = n\} \end{aligned}$$

son submódulos de M y N respectivamente.

Definición Sea M un R-módulo, $\lambda(M)$ un submódulo de M y notemos que si $\{N_\alpha : \alpha \in I\} \subseteq \lambda(M)$, entonces $\cap\{N_\alpha : \alpha \in I\} \subseteq \lambda(M)$. Si $S \subseteq M$, definimos $< S >$ como el **submódulo generado** por S.

$$\begin{aligned} < S > &= \cap\{K \in \lambda(M) : S \subseteq K\} \\ &= \{\sum_{i=1}^{n} s_i m_i : s_i \in S, m_i \in M\}. \end{aligned}$$

Definición Un morfismo $f : M \to N$ es un **monomorfismo** si para cualquier par de morfismos $h, g : L \rightrightarrows M$ tales que $fh = fg$ se tiene que $h = g$. Esto es (diagrama).

Proposición 4.2.1 *Sea $f : M \to N$, las siguientes afirmaciones son equivalentes:*

1. *f es monomorfismo*
2. *ker(f)={0}*
3. *f es inyectiva*

Demostración: $1 \Longrightarrow 2$) Supongamos que $ker(f) \neq \{0\}$ y supongamos que f es monomorfismo, sea $a \in ker(f)$ y tomemos $i, 0 : ker(f) \rightrightarrows M \xrightarrow{f} N$. Notemos que $(fi)(a) = f(a) = 0$ y $(f0)(a) = f(0) = 0$. Por lo tanto $(fi) = (f0) \Longleftrightarrow i = 0 \Longleftrightarrow ker(f) = \{0\}$.

$2 \Longrightarrow 3$) Supongamos $f(m) = f(n) \Longleftrightarrow f(m - n) = 0 \Longleftrightarrow m - n \in ker(f) = \{0\}$. Por lo tanto $m - n = 0 \Longleftrightarrow m = n$.

$3 \Longrightarrow 1$) Sean $f_1, f_2 : L \rightrightarrows M$ tales que $ff_1 = ff_2$ para cada $l \in L$. Sea $l \in L$ y supongamos $f(f_1(l)) = f(f_2(l))$, por inyecividad de f se tiene $f_1(l) = f_2(l)$, por lo tanto $f_1 = f_2$.

Definición Un morfismo $f : M \to N$ es un **epimorfismo** si para cualquier par de morfismos $h, g : N \rightrightarrows L$ tales que $hf = gf$ se tiene que $h = g$. Esto es (diagrama).

Proposición 4.2.2 *Sea $f : M \to N$, las siguientes afirmaciones son equivalentes:*

1. *f es epimorfismo*
2. *f es suprayectiva*
3. *im(f)=N*

Demostración: $1 \implies 2)$ Supongamos que f es un epimorfismo. Buscando una contradicción supongamos que f no es suprayectiva. Entonces existe $n_0 \in N$ tal que para cada $m \in M$ se tiene $f(m) \neq n_0$. A continuación definamos

$$\begin{aligned} f_1 &: N \to L, f_1(n) := n \\ f_2 &: N \to L, f_2(n) := \begin{cases} n, & \text{si } n \neq n_0 \ ; \\ 0, & \text{si } n = n_0. \end{cases} \end{aligned}$$

Por la construcción de f se tiene que $f_1 f = f_2 f$, sin embargo se tiene $f_1 \neq f_2$, por lo que f no puede ser epimorfismo. Por lo tanto f debe ser necesariamente suprayectiva.

$2 \implies 1)$ Sean $f_1, f_2 : N \rightrightarrows L$ tales que para cada $n \in N$ $f_1 f = f_2 f$. Como f es suprayectiva, para cada $n \in N$ existe $m \in M$ tal que $f(m) = n$. Por lo tanto $f_1(n) = f_2(n) \implies f_1(f(m)) = f_2(f(m))$, esto es f es epimorfismo.

$2 \iff 3)$ f suprayectiva $\iff \forall n \in N, \exists m \in M : f(m) = n \iff im(f) = N$.

Definición Una sucesión de R-morfismos $M \xrightarrow{f} N \xrightarrow{g} L$ es una **sucesión exacta** si $im(f) = ker(g)$.

Una sucesion exacta se dice que es una **sucesión exacta corta** si $0 \to M \xrightarrow{f} N \xrightarrow{g} L \to 0$ implica que f es monomorfismo y g es suprayectiva.

Una sucesión de A-morfismos $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \ldots \xrightarrow{f_n} M_{n+1}$ es **exacta en** i si $im(f_i) = ker(f_{i+1})$.

Proposición 4.2.3 *Sea $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta corta. Entonces para cada R-morfismo $h : M \to N$ tal que $hf = 0$ existe un único R-morfismo $\bar{h} : M'' \to N$ tal que $\bar{h}g = h$, es decir, el siguiente diagrama conmuta.*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] \arrow[dr, "0"'] & M \arrow[r, "g"] \arrow[d, "h"] & M' \arrow[r] \arrow[dl, "!\bar{h}"] & 0 \\ & & N & & \end{tikzcd}$$

Demostración: Sea $y \in M''$, como g es suprayectiva se tiene que para cada $y \in M''$ existe $x \in M$ tal que $g(x) = y$. Si $g(x') = y$ para algún $x' \in M$, entonces $g(x) = g(x') \iff g(x - x') = 0 \iff (x - x') \in ker(g) = im(f)$. Por la conmutatividad del diagrama $h(x - x') = 0 \iff h(x) = h(x')$. Por lo tanto la asignación

$$\begin{aligned} \bar{h} \ : \ & M'' \to N \\ & y \to h(x) \end{aligned}$$

, donde $g(x) = y$ está bien definida. Tenemos que $\bar{h} : M'' \to N$, y además $h = \bar{h}g$. Consideremos $\bar{h}(y + y') = h(x + x')$. Afirmamos que $\bar{h}$ es R-morfismo:

$$\begin{aligned} \bar{h}(g(x) + g(x')) &= \bar{h}(g(x + x')) \\ &= h(x + x') \\ &= h(x) + h(x') \\ &= \bar{h}(g(x)) + \bar{h}(g(x')) \\ &= \bar{h}(y) + \bar{h}(y') \end{aligned}$$

Similarmente, $\forall r \in R$ se tiene:

$$\begin{aligned} \bar{h}(ry) &= \bar{h}(g(ry)) \\ &= h(rx) \\ &= rh(x) \\ &= r\bar{h}(g(x)) \\ &= r\bar{h}(y). \end{aligned}$$

Corolario 4.2.4 (Primer teorema de isomorfía) *Si $h : M \to M''$ es un epimorfismo con nucleo M', entonces existe un isomorfismo $f : M/M' \to M''$ tal que $f\rho = h$.*

$$\begin{tikzcd}
 & & & & 0 \\
 & & & M/M' \arrow[ur] \arrow[d, leftrightarrow, "f"', "\cong"] & \\
0 \arrow[r] & M' \arrow[r, "i"] & M \arrow[ur, "\rho"] \arrow[dr, "h"'] & & \\
 & & & M'' \arrow[dr] & \\
 & & & & 0
\end{tikzcd}$$

Demostración: Por la proposición anterior existen $f' : M'' \to M/M'$ y $f : M/M' \to M''$ únicas tales que $f\rho = h$ (1) y $f'h = \rho$ (2), es decir que hacen conmutar el siguiente diagrama.

$$
\begin{tikzcd}
 & & & & 0 \\
 & & & M/M' \arrow[ur] \arrow[dd, bend left, "f"] & \\
0 \arrow[r] & M' \arrow[r, "i"] \arrow[urr, "0"] \arrow[drr, "0"'] & M \arrow[ur, "\rho"] \arrow[dr, "h"'] & & \\
 & & & M'' \arrow[uu, bend left, "f'"] \arrow[dr] & \\
 & & & & 0
\end{tikzcd}
$$

Entonces sustituyendo (1) en (2) obtenemos $ff'h = h = id_{M''}h$. Por lo tanto $ff' = id_{M''}$ y similarmente sustituyendo (2) en (1) obtenemos $f'f = id_{M/M'}$.

Proposición 4.2.5 (Segundo teorema de isomorfía) *Si $M, N \subseteq \lambda(M)$, entonces la composición*

$$N \xrightarrow{j} N + N' \xrightarrow{q} (N + N')/N'$$

es un epimorfismo con nucleo $N \cap N'$. De donde $N/(N \cap N') \cong (N + N')/N'$.

Demostración: Sea $y \in (N + N')/N'$, como q es suprayectiva, existen $n \in N$ y $n' \in N'$ tales que

$$
\begin{aligned}
y &= q(n + n') \\
&= q(n) + q(n') \\
&= q(j(n)) + q(n'),
\end{aligned}
$$

entonces $q(j(n)) = y$ pues $n' \in N$. Por lo tanto qj es epimorfismo.

Sea $x \in ker(qj)$, entonces

$$
\begin{aligned}
q(j(x)) &= 0 \\
q(x) &= 0,
\end{aligned}
$$

entonces $x + N' = N' \implies x \in N'$ y como $x \in N$ se sigue que $x \in N \cap N'$. Por lo tanto $ker(qj) = N \cap N'$, y la conclusión se sigue por el Primer teorema de isomorfía.

Proposición 4.2.6 (Tercer teorema de isomorfía) *Sea*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

una sucesión exacta corta.

1. *Si $N'' \leq M''$, entonces $g^{-1}(N'') \leq M$ tal que $M' \leq g^{-1}(N'')$.*

2. *Si $N \in \lambda(M)$ tal que $M' \leq N$, entonces $M \to M/M' \to M/M'/N/M'$ es un epimorfismo con nucleo N. Y así $M/N \cong M/M'/N/M'$.*

Demostración:

Definición
Sea $\mathcal{C}$ una categoria y sea $\{M_\alpha | \alpha \in \Omega\}$ una familia de objetos de $\mathcal{C}$, un **producto** para la familia anterior consiste de un objeto $P \in \mathcal{C}$ y una familia de flechas $\{p_\alpha : P \longrightarrow M_\alpha | \alpha \in \Omega\}$ donde $p_\alpha \in Mor(\mathcal{C}) \quad \forall \alpha \in \Omega$ tal que si se tiene otro objeto $X \in \mathcal{C}$ y una familia $\{f_\alpha : X \longrightarrow M_\alpha | \alpha \in \Omega\}$ donde $f_\alpha \in Mor(\mathcal{C})$ entonces existe un único morfismo $\varphi : X \longrightarrow P$ tal que $f_\alpha = p_\alpha \varphi \quad \forall$ es decir, el siguiente diagrama conmuta en $\mathcal{C}$:

$$\begin{tikzcd} X \arrow[rr, dashed, "\exists! \varphi"] \arrow[dr, "f_\alpha"'] & & P \arrow[dl, "p_\alpha"] \\ & M_\alpha & \end{tikzcd}$$

Proposición 4.2.7
La categoria **Con** *tiene producto*

Demostración:
Sea $\{X_i\}_{i \in I} \subset Con$, consideremos $P = X_1, ..., X_n$ y la familia de funciones $\{p_\alpha : P \longrightarrow X_\alpha | \alpha \in I\}$ donde p_α son las proyecciones al conjunto X_α y sea $X \in Con$ con $\{f_\alpha : X \longrightarrow X_\alpha | \alpha \in I\}$ entonces tenemos el siguiente diagrama

$$\begin{tikzcd} X \arrow[rr, dashed, "\exists! \varphi"] \arrow[dr, "f_\alpha"'] & & P \arrow[dl, "p_\alpha"] \\ & X_\alpha & \end{tikzcd}$$

Definamos $\varphi(x) = f_\alpha$ para cada $x \in X$.
Veamos el diagrama conmuta, sea $x \in X$

Proposición 4.2.8
Sea $\mathcal{C}$ una categoría y $(P, \{p_\alpha : P \longrightarrow M_\alpha | \alpha \in I\})$ un producto para la familia $\{M_\alpha | \alpha \in I\}$ entonces la propiedad universal del producto lo caracteriza.

Demostración:

Proposición 4.2.9
Si $\{M_\alpha | \alpha \in I\}$ una familia de objetos de $\mathcal{C}$, $(P, \{p_\alpha : P \longrightarrow M_\alpha | \alpha \in I\})$ es el producto de la familia y si $N \in \mathcal{C}$, $f, g \in Hom_{\mathcal{C}}(N, P)$ entonces

$$f = g \quad \Longleftrightarrow \quad p_\alpha f = p_\alpha g \quad \forall \alpha \in I$$

Demostración:
Si $f = g$ entonces $p_\alpha f = p_\alpha g \quad \forall \alpha \in I$ por definición de igualdad de funciones.
Reciprocamente, tenemos

Ejemplo
Sea R un anillo cualquiera entonces la categoria $R - Mod$ tiene producto.

Demostración:

Definición
Sea $\mathcal{C}$ una categoria y sea $\{M_\alpha | \alpha \in I\}$ una familia de objetos de $\mathcal{C}$, un **Coproducto** para la familia anterior consiste de un objeto $C \in \mathcal{C}$ y una familia de flechas $\{u_\alpha : M_\alpha \longrightarrow C | \alpha \in I\}$ donde $u_\alpha \in Mor(\mathcal{C}) \quad \forall \alpha \in \Omega$ tal que si se tiene otro objeto $X \in \mathcal{C}$ y una familia $\{f_\alpha : M_\alpha \longrightarrow X | \alpha \in I\}$ donde $f_\alpha \in Mor(\mathcal{C})$ entonces existe un único morfismo $\varphi : C \longrightarrow X$ tal que $f_\alpha = \varphi u_\alpha \quad \forall$ es decir, el siguiente diagrama conmuta en $\mathcal{C}$:

$$\begin{tikzcd} C \arrow[rr, dashed, "\exists!\,\varphi"] & & X \\ & M_\alpha \arrow[ul, "u_\alpha"] \arrow[ur, "f_\alpha"'] & \end{tikzcd}$$

Proposición 4.2.10
Sea $\mathcal{C}$ una categoria y $(C, \{u_\alpha : M_\alpha \longrightarrow C | \alpha \in I\})$ un coproducto para la familia $\{M_\alpha | \alpha \in I\}$ entonces la propiedad universal del coproducto lo caracteriza.

Demostración:
Supongamos tenemos otro objeto C' junto con una familia de morfismos μ_α :

$M_\alpha \longrightarrow C' \ \forall\alpha \in I$ que satisface las propiedades del coproducto, entonces tenemos lo siguiente: existen morfismos únicos $\psi : C \longrightarrow C'$ y $\psi' : C' \longrightarrow C$ tales que $\psi \circ u_\alpha = \mu_\alpha$ y $\psi' \circ u_\alpha = \mu_\alpha$, es decir lo siguientes diagramas conmutan:

$$\begin{tikzcd} C \arrow[rr, dashed, "\psi"] & & C' \\ & M_\alpha \arrow[ul, "u_\alpha"] \arrow[ur, "\mu_\alpha"'] & \end{tikzcd} \qquad \begin{tikzcd} C' \arrow[rr, dashed, "\psi'"] & & C \\ & M_\alpha \arrow[ul, "\mu_\alpha"] \arrow[ur, "u_\alpha"'] & \end{tikzcd}$$

Así tenemos $Id_{C'} = \psi \circ \psi'$ y $Id_C = \psi' \circ \psi$, es decir $C \cong C'$

Proposición 4.2.11
La categoria $\mathbf{Con}$ *tiene coproducto.*

Demostración: Sean $\{C_\alpha\}_{\alpha\in I} \subset Con$ y la una familia de morfismos (inclusiones) $i_\alpha : M_\alpha \longrightarrow C' \ \forall\alpha \in I$ tenemos la union de conjuntos es un conjunto, así considermeos $\cup_{\alpha\in I} C_\alpha \in Con$.
Sea $X \in Con$ con $u_\alpha : C_\alpha \longrightarrow X$ familia de funciones de conjuntos. Así si $x \in \cup_{\alpha\in I} C_\alpha$ entonces existe $\beta \in I$ tal que $x \in C_\beta$ y de este modo definimos $\varphi(x) = u_\beta(x)$ notemos que φ no es función ya que sea $x \in C_\beta \cap C_\gamma$ entonces $\varphi(x) = u_\beta(x)$ y $\varphi(x) = u_\gamma(x)$ y no necesariamente $u_\beta(x)$ y $u_\gamma(x)$ son iguales, es decir, no está bien definida. Para ello tomemos la unión disjunta $\sqcup_{\alpha\in I} C'_\alpha$ donde $C'_\alpha = C_\alpha \times \{\alpha\}$ y definamos $\varphi(x,\alpha) := u'_\alpha, u'_\alpha(x,\alpha) = u_\alpha(x)$ y $i'_\alpha(x,\alpha) = i_\alpha(x)$ como se muestra en el diagrama

$$\begin{tikzcd} \sqcup_{\alpha\in I} C'_\alpha \arrow[rr, dashed, "\varphi"] & & X \\ & C'_\alpha \arrow[ul, "i'_\alpha"] \arrow[ur, "u'_\alpha"'] & \end{tikzcd}$$

Consideremos $(y,\beta) \in \sqcup_{\alpha\in I} C'_\alpha$ tal que $\varphi(y,\alpha) := u'_\alpha(x) = u_\alpha(x)$ como está completamente definida por x tenemos φ está bien definida, además es morfismo porque u_α lo son.

Ejemplo
Sea R un anillo cualquiera entonces la categoría $R - Mod$ tiene coproducto.

Demostración:
Sean $\{M_\alpha\}_{\alpha\in I} \subset R - Mod$ una familia de R- módulos definimos

$$\oplus_{\alpha\in I} M_\alpha = \{f \in \Pi_{\alpha\in I} | f(\alpha) = 0 \text{ para casi toda } \alpha\}$$

Veamos $\oplus_{\alpha\in I}M_\alpha$ es un R-módulo. Consideremos $f_1, f_2 \in \bigoplus_{\alpha\in I} M_\alpha$ y $r_1, r_2 \in R$ arbitrarios.
$((r_1r_2)f_1)(\alpha) = r_1((r_2f_1)(\alpha)) = r_1(r_2(f_1(\alpha)))$ donde $f(\alpha) = 0$ para casi toda α
R es anillo asociativo con unidad, entonces $1 \cdot f_1(\alpha) = f_1(\alpha)$ donde $f(\alpha) = 0$ para casi toda α
$((r_1+r_2)f_1)(\alpha) = r_1f_1(\alpha)+r_2f_1(\alpha) = r_1(r_2(f_1(\alpha)))$ donde $f(\alpha) = 0$ para casi toda α
$(r_1(f_+f_2))(\alpha) = r_1f_1(\alpha) + r_1f_2(\alpha)$ entonces $\oplus_{\alpha\in I}M_\alpha$ es un R-módulo. Ahora consideremos $\{i_\beta : M_\beta \longrightarrow \oplus_{\alpha\in I}M_\alpha\}$ donde para cada $m \in M_\beta$ tenemos $i_\beta(m) : I \longrightarrow \cup_{\alpha\in I}M_\alpha$ tal que

$$i_\beta(m)(\alpha) = \begin{cases} 0 & \text{si } \alpha \neq \beta \\ m & \text{si } \alpha = \beta \end{cases}$$

Veamos es R-morfismo, consideremos $m_1, m_2 \in M_\beta$ y $r \in R$, entonces

$$i_\beta(m_1+m_2)(\alpha) = \begin{cases} 0 & \text{si } \alpha \neq \beta \\ m_1+m_2 & \text{si } \alpha = \beta \end{cases}$$

$$i_\beta(m_1)(\alpha) = \begin{cases} 0 & \text{si } \alpha \neq \beta \\ m_1 & \text{si } \alpha = \beta \end{cases} \quad i_\beta(m_2)(\alpha) = \begin{cases} 0 & \text{si } \alpha \neq \beta \\ m_2 & \text{si } \alpha = \beta \end{cases}$$

De este modo tenemos dos posibles casos:
Si $\alpha \neq \beta$ entonces $i_\beta(m_1) + i_\beta(m_2) = 0 + 0 = 0 = i_\beta(m_1 + m_2)$
Si $\alpha = \beta$ entonces $i_\beta(m_1) + i_\beta(m_2) = m_1 + m_2 = i_\beta(m_1 + m_2)$
Por lo tanto $i_\beta(m_1 + m_2) = i_\beta(m_1) + i_\beta(m_2)$

$$i_\beta(rm)(\alpha) = \begin{cases} 0 & \text{si } \alpha \neq \beta \\ rm & \text{si } \alpha = \beta \end{cases}$$

De este modo tenemos dos posibles casos:
Si $\alpha \neq \beta$ entonces $i_\beta(rm) = 0 = ri_\beta(m)$
Si $\alpha = \beta$ entonces $i_\beta(rm) = rm = ri_\beta(m)$
Por lo tanto $i_\beta(rm) = ri_\beta(m)$ Ahora consideremos X en $R-Mod$ y $u_\beta : M_\beta \longrightarrow \oplus_{\alpha\in I}X$ y definamos $\varphi : \oplus_{\alpha\in I}M_\alpha \longrightarrow X$ como $\varphi(i_\alpha(m)(\alpha)) = \sum_{\alpha\in I} u_\alpha(m)$.

$$\begin{tikzcd}
\oplus_{\alpha\in I}M_\alpha \arrow[rr, dashed, "\varphi"] & & X \\
& M_\alpha \arrow[ul, "i_\alpha"] \arrow[ur, "u_\alpha"'] &
\end{tikzcd}$$

Sean $r \in R$ y $m_1, m_2 \in M_\alpha$ tenemos:

$$\begin{aligned}\varphi(i_\alpha(m_1+m_2)(\alpha)) &= \sum_{\alpha\in I} u_\alpha(m_1+m_2)\\ &= \sum_{\alpha\in I}(u_\alpha(m_1)+u_\alpha(m_2))\\ &= \sum_{\alpha\in I} u_\alpha(m_1)+\sum_{\alpha\in I} u_\alpha(m_2)\\ &= \varphi(i_\alpha(m_1)(\alpha))+\varphi(i_\alpha(m_2)(\alpha))\end{aligned}$$

$$\begin{aligned}\varphi(i_\alpha(rm_1)(\alpha)) &= \sum_{\alpha\in I} u_\alpha(rm_1)\\ &= \sum_{\alpha\in I}(ru_\alpha(m_1) \text{ Ya que } u_\alpha \text{ son R-morfismos}\\ &= r\sum_{\alpha\in I} u_\alpha(m_1)\\ &= r\varphi(i_\alpha(m_1)(\alpha))\end{aligned}$$

Entonces φ es R-morfismo. Ademas tenemos que el diagrama conmuta ya que sea $m \in M_\alpha$ entonces $\varphi(i_\alpha(m)(\beta)) = \sum_{\alpha\in I} u_\alpha(m)$ y por definición de $i_\alpha(m) = m$ si $\alpha = \beta$ y cero si son distintos por lo tanto solo queda en la suma $u_\alpha(m)$.
Finalmente, supongamos existe $\psi : \oplus_{\alpha\in I} M_\alpha \longrightarrow X$ tal que el diagrama conmuta. Entonces

$$\psi(i_\alpha(m)(\alpha)) = \sum_{\alpha\in I} u_\alpha(m) = \psi(i_\alpha(m)(\alpha))$$

Proposición 4.2.12
La categoria **Top** *tiene coproducto.*

Demostración:

4.3 Módulos inyectivos y proyectivos

Definición
Un R-módulo E es inyectivo si $Hom(\_, N) : R - Mod \longrightarrow \mathbb{Z} - Mod$ es funtor exacto derecho(es decir, es exacto ya que siempre es exacto izquierdo). En general tenemos

$$Hom(\_,\_) : R - Mod \times R - Mod \longrightarrow \mathbb{Z} - Mod$$

es un bifuntor izquierdo en cada variable.

Proposición 4.3.1 *Si $\{M_\alpha | \alpha \in I\}$ es una familia de R-módulos entonces $\oplus_{\alpha\in I} M_\alpha$ es proyectivo si y solo si M_α es proyectivo para todo $\alpha \in I$.*

Demostración:
Supongamos M_α es proyectivo para todo $\alpha \in I$ y consideremos la siguiente sucesión exacta:

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

PD $\oplus_{\alpha\in I} M_\alpha$ es proyectivo es decir existe $\beta : \oplus_{\alpha\in I} M_\alpha \longrightarrow M$ tal que para todo morfismo $\sigma : \oplus_{\alpha\in I} M_\alpha \longrightarrow M''$ se tiene $g\beta = \sigma$ o el siguiente diagrama conmuta :

$$\begin{tikzcd}
 & & & \oplus_{\alpha\in I} M_\alpha \arrow[dl, dashed, "\beta"'] \arrow[d, "\sigma"] & \\
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0
\end{tikzcd}$$

Para ello, por hipótesis tenemos M_α es proyectivo entonces existen $\beta_\alpha : M_\alpha \longrightarrow M$ tales que $g\beta_\alpha = \sigma_\alpha$, es decir el siguiente diagrama conmuta:

$$\begin{tikzcd}
 & & & M_\alpha \arrow[dl, dashed, "\beta_\alpha"'] \arrow[d, "\sigma_\alpha"] & \\
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0
\end{tikzcd}$$

Así, por propiedad universal del coproducto $\exists!\beta : \oplus_{\alpha\in I} M_\alpha \longrightarrow M$ tal que $\beta_\alpha = \beta i_\alpha$ como se muestra en el diagrama

$$\begin{tikzcd}
\oplus_{\alpha\in I} M_\alpha \arrow[rr, "\exists!\beta"] & & X \\
 & M_\alpha \arrow[ul, "i_\alpha"] \arrow[ur, "\beta_\alpha"'] &
\end{tikzcd}$$

tal que conmuta. Así tenemos

$$g \circ \beta_\alpha = \sigma_\alpha = \sigma \circ i_\alpha \quad y \quad \beta \circ i_\alpha = \beta_\alpha$$

$$g \circ (\beta_\alpha \circ i_\alpha) = g \circ \beta_\alpha = \sigma \circ i_\alpha \quad \Rightarrow \quad g \circ \beta = \sigma$$

La existencia de β la garantiza la propiedad universal del coproducto y lo ultimo que se demostró es que el diagrama conmuta.

Supongamos $\oplus_{\alpha\in I} M_\alpha$ es proyectivo y consideremos la siguiente sucesión exacta:

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

PD M_α es proyectivo es decir existen $\beta_\alpha : M_\alpha \longrightarrow M$ tal que para todo morfismo $\sigma_\alpha : M_\alpha \longrightarrow M''$ se tiene $g\beta = \sigma$ o el siguiente diagrama conmuta:

$$\begin{tikzcd} & & & M_\alpha \arrow[dl, dashed, "\beta_\alpha"'] \arrow[d, "\sigma_\alpha"] & \\ 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

Para ello, por hipótesis tenemos M_α es proyectivo entonces existen $\beta_\alpha : M_\alpha \longrightarrow M$ tales que $g\beta_\alpha = \sigma_\alpha$, es decir el siguiente diagrama conmuta:

$$\begin{tikzcd} & & & M_\alpha \arrow[dl, dashed, "\beta_\alpha"'] \arrow[d, "\sigma_\alpha"] & \\ 0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0 \end{tikzcd}$$

Así, por propiedad universal del coproducto $\exists!\varphi : \oplus_{\alpha\in I} M_\alpha \longrightarrow M''$ tal que $\varphi \circ i_\alpha = \sigma$, es decir, el diagrama conmuta

$$\begin{tikzcd} \oplus_{\alpha\in I} M_\alpha \arrow[rr, "\exists!\varphi"] & & M'' \\ & M_\alpha \arrow[ul, "i_\alpha"] \arrow[ur, "\beta_\alpha"'] & \end{tikzcd}$$

y de este modo, como $\oplus_{\alpha\in I} M_\alpha$ es proyectivo existe $\beta_\alpha : \oplus_{\alpha\in I} M_\alpha \longrightarrow M$ tal que $g \circ \beta = \varphi$. De este modo aplicando la igualdad a i_α tenemos

$$\varphi(i_\alpha) = (g \circ \beta) \circ i_\alpha = g \circ (\beta \circ i_\alpha)$$

Y finalmente tomando $\beta_\alpha = \beta \circ i_\alpha$tenemos

$$g \circ \beta_\alpha = g \circ \beta \circ i_\alpha = \varphi \circ i_\alpha = \sigma_\alpha$$

Lo que se quería.

Proposición 4.3.2 *Si $\{M_\alpha | \alpha \in I\}$ es una familia de R-módulos entonces $\Pi_{\alpha\in I} M_\alpha$ es inyectivo si y solo si M_α es inyectivo para todo $\alpha \in I$.*

Demostración:
Supongamos M_α es inyectivo para todo $\alpha \in I$ y consideremos la siguiente sucesión exacta:

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

PD Dado un morfismo $\sigma : M' \longrightarrow \Pi_{\alpha\in I} M_\alpha$ existe $\beta : M \longrightarrow \Pi_{\alpha\in I} M_\alpha$ tal que $\beta_\alpha f = \sigma_\alpha$ es decir el siguiente diagrama conmuta :

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\sigma"'] & M \arrow[r, "g"] \arrow[dl, dashed, "\beta"] & M'' \arrow[r] & 0 \\
& \Pi_{\alpha\in I} M_\alpha & & &
\end{tikzcd}$$

Para ello, por hipótesis tenemos M_α es inyectivo entonces existen $\beta_\alpha : M \longrightarrow M_\alpha$ tales que $\beta_\alpha f = \sigma_\alpha$, es decir el siguiente diagrama conmuta:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\sigma_\alpha = p_\alpha \circ \sigma"'] & M \arrow[r, "g"] \arrow[dl, "\beta"] & M'' \arrow[r] & 0 \\
& M_\alpha & & &
\end{tikzcd}$$

Así, por propiedad universal del producto $\exists! \sigma : M \longrightarrow \Pi_{\alpha\in I} M_\alpha$ tal que $p_\alpha \beta = \beta_\alpha$. Así tenemos aplicando a f

$$(p_\alpha \circ \beta) \circ f = \beta_\alpha \circ f = \sigma_\alpha = p_\alpha \sigma \quad \Rightarrow \quad p_\alpha \circ (\beta \circ f) = (p_\alpha \circ \beta) \circ f = p_\alpha \circ \sigma$$

De este modo tenemos $\beta \circ f = \sigma$.

Supongamos $\Pi_{\alpha\in I} M_\alpha$ es inyectivo y consideremos la siguiente sucesión exacta:

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

PD Dado un morfismos $\sigma_\alpha : M' \longrightarrow M_\alpha$ existe $\beta_\alpha : M \longrightarrow M_\alpha$ tal que $\beta_\alpha f = \sigma_\alpha$ es decir el siguiente diagrama conmuta:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\sigma_\alpha"'] & M \arrow[r, "g"] \arrow[dl, dashed, "\beta_\alpha"] & M'' \arrow[r] & 0 \\
& M_\alpha & & &
\end{tikzcd}$$

Para ello, por hipótesis tenemos $\Pi_{\alpha\in I} M_\alpha$ es inyectivo entonces existe $\beta : M \longrightarrow \Pi_{\alpha\in I} M_\alpha$ tales que $\beta f = \sigma$, es decir el siguiente diagrama conmuta:

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "\sigma"'] & M \arrow[r, "g"] \arrow[dl, "\beta"] & M'' \arrow[r] & 0 \\
& \Pi_{\alpha\in I} M_\alpha & & &
\end{tikzcd}$$

Por la propiedad universal del producto existe $\sigma : M' \longrightarrow \Pi_{\alpha \in I} M_\alpha$ tal que $p_\alpha \circ \sigma = \sigma_\alpha$. Así tenemos

$$\sigma_\alpha = p_\alpha \circ \sigma = p_\alpha \circ (\beta \circ f) = (p_\alpha \circ \beta) \circ f$$

Y finalmente tomando $\beta = p_\alpha \beta$ tenemos $\sigma_\alpha = \beta \circ f$.

Definición
Si $\{M_\alpha\}_{\alpha \in I}$ es una familia de submódulos de un R-módulo M. Diremos que la familia es independiente

- Si $\sum_{\alpha \in I} N_\alpha = \oplus_{\alpha \in I} N_\alpha$
- Si $\{m_\alpha | \alpha \in I\} \subseteq M$ diremos que es independiente si $\{Rm_\alpha | \alpha \in I\}$ es una familia independiente

Diremos que la familia $\{m_\alpha | \alpha \in I\}$ es *linealmente independiente*:
si $0 = \sum_{\alpha \in I} r_\alpha m_\alpha \in_\alpha Rm_\alpha$ entonces r_α son cero para casi toda $\alpha \in I$

Proposición 4.3.3
Sea$\{M_\alpha\}_{\alpha \in I}$ es una familia de módulos y M R-módulo. Probar:

a) $Hom_R(\oplus_{\alpha \in I} M_\alpha, M) \cong \Pi_{\alpha \in I}(M_\alpha, M)$

b) $Hom_R(M, \Pi_{\alpha \in I} M_\alpha) \cong \Pi_{\alpha \in I}(M, M_\alpha)$

Definición
Sea $M \in R - Mod$ un subconjunto $B \subseteq M$ es base de M si

- $< B >= M >$
- B es linealmente independiente.

Definición
Un módulo M es libre si tiene una base.

Proposición 4.3.4
Sea $M \in R - Mod$ entonces
M es libre si y solo si $M \cong R^{(X)} = \oplus_{x \in X} R$ para algún conjunto X

Demostración:
Supongamos $R^{(X)}$ que es libre para cada $b \in X$, consideremos $e_b : X \longrightarrow R$ tomando

$$e_b(x) = \begin{cases} 1 & \text{si } x = b \\ 0 & \text{si } x \neq b \end{cases}$$

Afirmación $\{e_b|b \in X\}$ son base para $R^{(X)}$
Sea $\{x_b\}_{b\in X} \in R^{(X)}$ entonces $\sum_{b\in X} x_b e_b(x_b)$ trivialmente genera a $R^{(X)}$ además es linealmente independiente, por lo tanto es base.
Sea $\{m_\alpha|\alpha \in I\}$ una base para M, por cada $\alpha in I$ consideremos $f_\alpha : R \longrightarrow M$ $f_\alpha(r) = rm_\alpha$ es un R-morfismo (por propiedad del coproducto)como se muestra en el diagrama:

$$\begin{tikzcd} R \arrow[r, "f_\alpha"] \arrow[d, "\mu"'] & M \\ R^{(X)} \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

Afirmación, $f : R^{(X)} \longrightarrow M$ es isomorfismo. Tenemos $f\mu_\alpha = f_\alpha$.
Si $(r_\alpha) \in R^{(X)}$ tal que $f((r_\alpha)) = 0$ entonces $\sum_{\alpha\in I} r_\alpha m_\alpha = 0$ y de este modo $r_\alpha = 0 \quad \forall\alpha \in I$. Por lo tanto f es inyectiva.
Sea $x \in M$ entonces $x \in \sum_{\alpha\in I} r_\alpha m_\alpha$ ya que $f((r_\alpha)) = 0$, así f es sobre.

Proposición 4.3.5
Todo R-módulo es cociente de un módulo libre.

Demostración:
Sea $M \in R - Mod$, por cada $m \in M$, sea $f_m : R \longrightarrow M$ $f_m(r) = rm$ entonces existe un único morfismo $\varphi : R^{(X)} \longrightarrow M$, donde se tiene

$$Ker\varphi = \{(rm)|\varphi((rm)) = 0\} = \{(rm)|\sum r_m m = 0\}$$

que no es trivial en general ya que de serlo M seria módulo libre. Por otro lado, si $m \in M$ consideremos lo siguiente:

$$(m) = (0, ..., 1_m, ...) \in R^{(X)}$$

Por lo tanto se tiene $\varphi(m) = m$, y con ello φ es suprayectivo. Finalmente por el primer teorema de isomorfia se tiene

$$R^{(X)}/Ker\varphi \cong M$$

Proposición 4.3.6
Todo módulo libre es proyectivo.

Demostración:
Sea P un modulo libre, tenemos el siguiente diagrama:

$$\begin{tikzcd} & P \arrow[dl, dashed, "\overline{f}"'] \arrow[d, "f"] & \\ N \arrow[r, "g"] & N'' \arrow[r] & 0 \end{tikzcd}$$

Sea $B = \{m_\alpha\}_{\alpha \in I}$ una base de P. sea $\{n_\alpha\}_{\alpha \in I}$ los elementos de N tales que $g(n_\alpha) = f(m_\alpha)$ y consideremos $\overline{f} : B \longrightarrow N$ la función dada por $\overline{f}(m_\alpha) = n_\alpha$ dada por la igualdad anterior. Así extendemos $\overline{f}$ como sigue:
$\overline{f} : P \longrightarrow N$ tomamos un $m \in P$ entonces $m = \sum r_\alpha m_\alpha$ y aplicando la función tenemos

$$\overline{f}(m) = \overline{f}(\sum r_\alpha m_\alpha) = \sum r_\alpha \overline{f}(m_\alpha) = \sum r_\alpha n_\alpha$$

Definida de esta forma $\overline{f}$ es R-morfismo

$$\overline{f}(m+m') = \overline{f}(\sum r_\alpha m_\alpha + \sum r_\beta m_\beta) = \sum r_\alpha m_\alpha + \sum r_\beta m_\beta = \overline{f}(m) + \overline{f}(m')$$

$$\overline{f}(rm) = \overline{f}(\sum r_\alpha r m_\alpha) = \sum r r_\alpha n_\alpha = r \sum r_\alpha n_\alpha = r\overline{f}(rm)$$

Observación
La clase de módulos inyectivos en R-Mod es cerrada bajo productos directos, sumandos directos y extensiones.

Teorema 4.3.7 (Baer)
Sea $Q \in R - Mod$, tenemos
${}_RQ$ es inyectivo si y solo si $\forall I$ ideal izquierdo de R y todo morfismo $f : I \longrightarrow Q$ existe $\overline{f} : R \longrightarrow Q$ tal que $\overline{f}_{|1} = f$; es decir, el siguiente diagrama conmuta:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "i"] \arrow[d, "f"'] & R \arrow[dl, dashed, "\overline{f}"] \\ & Q & \end{tikzcd}$$

Demostración:
Si Q es inyectivo entonces es claro.
Recíprocamente, sea la siguiente sucesión exacta en R-Mod y $g : N' \longrightarrow Q$ un morfismo,

$$0 \longrightarrow N' \xrightarrow{f} N$$

Consideremos

$$\mathcal{J} = \{(H, \sigma) | N' \subseteq H \subseteq N \quad \sigma \in Hom(H, Q) \quad \sigma_{|N'} = g\}$$

Notemos $\mathcal{J} \neq \emptyset$ pues $(N', g) \in \mathcal{J}$. Además $\mathcal{J}$ tiene un orden dado por $(H, \sigma) \leqslant (H', \sigma')$ si $H \subseteq H'$ y $\sigma_{|H} = \sigma$ entonces $(\mathcal{J}, \leqslant)$ es un COPO.
Afirmación $(\leqslant)$ satisface las hipótesis del lema de Zorn.
Sea $\mathcal{C} = \{(N_\alpha, \sigma_\alpha)\}$ una cadena en $(\mathcal{J}, \leqslant)$. PD $\cup\mathcal{C} \in \mathcal{J}$.

Como $\mathcal{C}$ es una cadena de submódulos entonces $\cup N_\alpha$ es un submódulo, definamos $\varphi : \cup N_\alpha \longrightarrow Q$ para cada $m \in \cup N_\alpha$ existe $\alpha \in I$ tal que $m \in N_\alpha$ y $\sigma_\alpha : N_\alpha \longrightarrow Q$ con $\varphi(m) = \sigma_\alpha(m)$. Así φ es morfismo y $\varphi(m)_{|N'} = \sigma_\alpha(m)_{|N'} = g(m)$ por definición. Por lo tanto $\cup\mathcal{C} \in \mathcal{J}$,($\leqslant$) satisface las hipótesis del lema de Zorn y hay máximos.
Sea (H, h) uno de tales máximos. Afirmación $H = N$.
Supongamos que $H \neq N$, sea $m \in N - H$ y sea $I = (H : m) = \{r \in R | rm \in H\}$. Consideremos $\gamma : I \longrightarrow Q$ tal que $\gamma(r) = h(rm)$. Claramente γ es morfismo ya que h lo es, por hipótesis existe $\overline{\gamma} : R \longrightarrow Q$ dado por $\overline{\gamma}(r) = \gamma(r) \quad \forall r \in R$.
Notemos $H \subseteq H + Rm \subseteq N$.
Sea $\overline{h} : H + Rm \longrightarrow Q$ dado por $\overline{h}(x + rm) = h(x) + \overline{\gamma}(r)$, $\overline{h}$ está bien definida pues si $x+rm = x'+r'm$ entonces $x-x' = (r'-r)m \in H$ y por tanto $r'-r \in I$, así:

$$\begin{aligned}\overline{\gamma}(r' - r) = \gamma(r' - r) &= h((r' - r)m) = h(x - x') \\ &\Rightarrow h(r'm) - h(rm) = h(x) - h(x') \\ &\Rightarrow h(x) - h(rm) = h(x) - h(r'm) \\ &\Rightarrow h(x) - \gamma(r) = h(x) - \gamma(r')\end{aligned}$$

entonces $\overline{h}$ está bien definida y $\overline{h}_{|I} = h$ lo que implica $(H + Rm, \overline{h}) \in \mathcal{J}$, es decir $(H, h) \leqslant (H + Rm, \overline{h})$ lo cual es una contradicción ya que (H, h) es máximo, por lo tanto $H = N$.

Proposición 4.3.8
Sea $Q \in R$-Mod entonces
Q es inyectivo si y sólo si $\forall I \leqslant R$ ideal izquierdo y todo morfismo $f : I \longrightarrow Q$ existe $q \in Q$tal que $f(a) = aq \quad \forall a \in I$

Demostración:
Sean $I \leqslant R$ ideal izquierdo y $f \in Hom(I, Q)$ por hipótesis existe $\overline{f} : R \longrightarrow Q$ tal que $\overline{f}_{|I} = f$ por el teorema de Baer, sea $a \in I$ entonces $f(a) = \overline{f}(a) = \overline{f}(a\cdot) = a\overline{f}(1) = aq$ tomando $\overline{f}(1) = q$.
Ahora sean $I \leqslant R$ ideal izquierdo y $f \in Hom(I, Q)$ por hipótesis existe $q \in Q$ tal que $f(a) = aq \quad \forall a \in I$. Sea $\overline{f} : R \longrightarrow Q$ dada como $\overline{f}(r) = rq$, notemos que si $r \in I$ $\overline{f}(r) = r\overline{f}(1) = aq = f(a)$ y por el criterio de Baer R es inyectivo.

Definición
Sea $D \in \mathbb{Z}$-Mod diremos que D es un grupo abeliano divisible si para todo $d \in D$ y $a \in \mathbb{Z}$ tenemos existe $d' \in D$ tal que $ad' = d$

Corolario 4.3.9
Un grupo abeliano G es divisible si y sólo si G es inyectivo.

Demostración:
Supongamos G es inyectivo, sea $f : n\mathbb{Z} \longrightarrow G$ definido por $f(n) = g$, recordemos $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$. Como G inyectivo existe $\overline{f} : \mathbb{Z} \longrightarrow G$tal que $\overline{f}_{|n\mathbb{Z}} = f$ por Baer, entonces $g = f(n) = \overline{f}(n) = n\overline{f}(1) \quad \forall g \in G$
Entonces G es divisible. Ahora sea $I \subset \mathbb{Z}$ entonces $I = m\mathbb{Z}$ para algún $m \in \mathbb{Z}$ y sea $f : I \longrightarrow G$ un morfismo $f(m) \in G$. Consideremos $q \in G$ solución de $f(m) = mx$ y $\overline{f} : \mathbb{Z} \longrightarrow G$ dada por $\overline{f}(1) = q$ esta definición lo podemos considerar en un solo elemento ya que tenemos $\overline{f}(a) = a\overline{f}(1) = aq$. Así por la proposición anterior G es inyectivo.

Teorema 4.3.10
Todo grupo abeliano se puede sumergir en un grupo abeliano divisible.

Demostración:
Sea $G \in \mathbb{Z}$-Mod entonces tenemos el siguiente diagrama:

$$\begin{tikzcd}
0 \arrow[r] & Ker\varphi \arrow[r, "i"] \arrow[d, equal] & \mathbb{Z}^{(X)} \arrow[r, "\varphi"'] \arrow[d, "i"] & G \arrow[r] \arrow[d, "\psi"] & 0 \\
0 \arrow[r] & Ker\varphi \arrow[r, "i"] & \mathbb{Q}^{(X)} \arrow[r] & \mathbb{Q}^{(X)}/Ker\varphi \arrow[r] & 0
\end{tikzcd}$$

$\psi(g) = x + Ker\varphi$ donde x es tal que $\varphi(x) = g$, Claramente φ es Monomorfismo.

$$\psi(g) = \psi(g') \Leftrightarrow x + Ker\varphi = x' + Ker\varphi \Leftrightarrow x - x' \in Ker\varphi \Leftrightarrow \varphi(x - x') = 0$$

ademas

$$\varphi(x) - \varphi(x') = 0 \Leftrightarrow g - g' = 0 \Leftrightarrow g = g'$$

$$G \cong_{\psi} H \leqslant \mathbb{Q}^{(X)}/Ker\varphi$$

Por tanto $\mathbb{Q}^{(X)}/Ker\varphi$ es divisible ($\mathbb{Q}^{(X)}$ es producto de módulos inyectivos y $\mathbb{Q}^{(X)}/Ker\varphi$ es un cociente de módulos inyectivos).

Observación Sea $N \in R$-Mod derecho y $G \in \mathbb{Z}$-Mod consideremos $Hom_{\mathbb{Z}}(N, G)$, tiene estructura de R-módulo izquierdo con la siguiente operación:
Si $r \in R$, $f \in Hom_{\mathbb{Z}}(N, G)$ definimos

$$rf : N \longrightarrow G$$
$$rf(x) \mapsto f(xr)$$

Teorema 4.3.11
Sea D un grupo abeliano divisible entonces el R-Mod izquierdo $Hom_{\mathbb{Z}}(R, D)$ es inyectivo en R-Mod.

Demostración: Sea $I \leqslant R$ ideal izquierdo, $f : I \longrightarrow Hom_{\mathbb{Z}}(R, D)$ un R-morfismo. PD existe $\overline{f} : R \longrightarrow Hom_{\mathbb{Z}}(R, D)$ tal que el diagrama conmuta:

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d, "f"'] & R \arrow[dl, dashed, "\overline{f}"] \\
 & Hom_{\mathbb{Z}}(R, D) &
\end{tikzcd}$$

Si $a \in I$ entonces $f(a) : R \longrightarrow D$ y por tanto $f(a)(1) \in D$. Sea $g : I \longrightarrow D$ dado por $g(a) = f(a)(1)$ entonces g es $\mathbb{Z}$-morfismo ya que

$$g(a + a') = f(a + a')(1) = f(a)(1) + f(a')(1) = g(a) + g(a')$$

Así, como D es divisible existe $\overline{g} : R \longrightarrow D$ tal que $\overline{g}(a) = g(a) \quad \forall a \in I$ en $\mathbb{Z}$-Mod como se muestra en el diagrama

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[d, "g"'] & R \arrow[dl, dashed, "\overline{g}"] \\
 & D &
\end{tikzcd}$$

Sea $\overline{f} : R \longrightarrow Hom_{\mathbb{Z}}(R, D)$ dado por $\overline{f}(a) : R \longrightarrow D$ $\overline{f}(a)(r) = \overline{g}(ra)$.
Afirmación

1) $\forall a \in R \quad \overline{f}(a) \in Hom_{\mathbb{Z}}(R, D)$

2) $\overline{f}$ es R-morfismo.

3) $\overline{f}_{|I} = f$

1)

$$\begin{aligned}
\overline{f}(a)(r + r') &= \overline{g}((r + r')a) \\
&= \overline{g}(ra + r'a) \\
&= \overline{g}(ra) + \overline{g}(r'a) \\
&= \overline{f}(a)(r) + \overline{f}(a)(r')
\end{aligned}$$

2)

$$\begin{aligned}
\overline{f}(a+a')(r) &= \overline{g}(r(a+a')) \\
&= \overline{g}(r(a+a') \\
&= \overline{g}(ra+ra') \\
&= \overline{g}(ra)+\overline{g}(ra') \\
&= \overline{f}(a)(r)+\overline{f}(a')(r) \\
\text{Si } \alpha \in R \text{ entonces } \overline{f}(\alpha a)(r) &= \overline{g}(r(\alpha a)) \\
&= \overline{g}(r\alpha)a \\
&= \overline{f}(a)(r\alpha) \\
&= \alpha\overline{f}(a)(r) \text{ Por la observacion anterior}
\end{aligned}$$

3)Sea $a \in I$

$$\overline{f}(a)(r) = \overline{g}(ra) = g(ra) = f(ra) = rf(a)(1) = f(a)(r)$$

Definición
Un submodulo $0 \neq N \subseteq M$ es escencial si $\forall \quad K \subseteq N$ no cero

$$N \cap K \neq 0 \quad \Leftrightarrow \quad siK \neq 0 \text{ entonces } K = 0$$

Proposición 4.3.12
Sea $M \in R-Mod$ y sea $\sigma : M \to E$ un monomorfismo en un inyectivo E y $\rho : M \to C$ un monomorfismo tal que $Im\rho \subseteq C$ entonces existe un monomorfismo $\overline{\sigma} : C \to E$ tal que $\overline{\sigma}\rho = \sigma$.

Demostración:
Como E es inyectivo entonces existe $\overline{\sigma} : C \to E$ como en el siguiente diagrama:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\rho"] \arrow[d, "\sigma"'] & C \arrow[dl, dashed, "\overline{\sigma}"] \\
& E &
\end{tikzcd}$$

Sea $x \in Ker\overline{\sigma}$, si $x \neq 0$ notemos que $Ker\overline{\sigma} \neq 0$, $\overline{\sigma} \subseteq C$ entonces $Im\rho \cap \overline{\sigma} \neq 0$. Ahora consideremos el cíclico $Rx \neq 0$. Ahora $Rx \subseteq C$ entonces $Im\rho \cap Rx \neq 0$ y de este modo existe $\alpha \in R$ tal que $ax \in Im\rho$. Así existe $y \in M$ tal que $\rho(y) = \alpha x$ entonces $\overline{\sigma}(\rho(y)) = \sigma(y)$, de este modo sustituyendo tenemos $\overline{\sigma}(\alpha x) = \sigma(y)$ además tenemos $\alpha\overline{\sigma}(x) = 0$ esto implica $y \in Ker\sigma = \{0\}$ por hipotesis. De este modo $y = 0$ y por tanto $\alpha x = 0$ lo cual es una contradiccion ya que habiamos supuesto ambos eran distintos de cero.
Finalmente concluimos $x = 0$.

Definición
Sea M un R-módulo izquiedo entonces una capsula inyectiva para M en $R-Mod$ es una pareja (E,σ) donde E es inyectivo y $\sigma : M \to E$ es un morfismo tal que $Im \leqslant E$.

Proposición 4.3.13
Sea $M \in R-Mod$ entonces:

1) *La capsula inyectiva de M (si existe) es única salvo isomofismo.*

2) *Si (E,σ) es capsula inyectiva de M y Q es inyectivo que contiene a M entonces Q contiene una copia de E.*

Demostración:
Sea (E,σ) y (E',σ') capsulas inyectivas de M, por la proposición anterior $\overline{\sigma}$ es monomofismo entonces

$$M \simeq \sigma'(M) = \overline{\sigma}(\sigma(M)) \subseteq \overline{\sigma}(E) \simeq E$$

como en el siguiente diagrama:

$$\begin{tikzcd} & 0 \arrow[d] & \\ 0 \arrow[r] & M \arrow[r, "\sigma"] \arrow[d, "\sigma'"'] & E \arrow[dl, dashed, "\overline{\sigma}"] \\ & E' & \end{tikzcd}$$

Notemos que

$$E \simeq \overline{\sigma}(E) \leq E'$$

Así existe $\iota : E' \to E$ tal que $\overline{\iota}\iota = Id_E$ De este modo

$$0 \longrightarrow E' \xrightarrow{\iota} E \xrightarrow{P} \frac{E'}{E} \longrightarrow 0$$

Y por lo tanto $E' \simeq E \bigoplus E'/E$ ya que $\iota'\overline{\iota}$ es un isomorfsmo por el lema del cinco.

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[r, "\iota"] \arrow[d, equal] & E' \arrow[r, "P"] \arrow[d, "\iota'\overline{\iota}"] & \frac{E'}{E} \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & E \arrow[r, "\iota"] & E \bigoplus E'/E \arrow[r, "P'"] & \frac{E'}{E} \arrow[r] & 0 \end{tikzcd}$$

Entonces E es suma directa de E' en particular

$$E' = \overline{\sigma}(E) \bigoplus K$$

De este modo $\sigma'(M) \subset \overline{\sigma}(E)$ entonces $\sigma'(M) \cap K = \{0\}$ (es esencial). Por lo tanto $k = \{0\}$ ya que $\sigma'(M) \subseteq E$ Por lo tanto concluimos

$$E' = \overline{\sigma}(E)$$

Proposición 4.3.14
Todo R módulo izquierdo se sumerge en un módulo inyectivo.

Demostración: Sea $M \in R - Mod$ entonces M es un **Z**-módulo, sea D un grupo abeliano divisible tal que $M \hookrightarrow D$ entonces bajo $Hom_{\mathbf{Z}}(R,_)$ obtenemos lo siguiente:

$$0 \longrightarrow Hom_{\mathbf{Z}}(R, M) \longrightarrow Hom_{\mathbf{Z}}(R, D)$$

Donde $Hom_{\mathbf{Z}}(R, D)$ es inyectivo en $R - Mod$.
Afirmacion: $Hom_R(R, M)$ es un submódulo de $Hom_{\mathbf{Z}}(R, M)$.
Sea $f \in Hom_R(R, M)$, $\alpha \in R$ entonces $\alpha f \in Hom_R(R, M)$, así:

$$(\alpha f)(rx) = f(rx\alpha) = rf(x\alpha) = r(\alpha f)(x)$$

De este modo tenemos

$$Hom_R(R, M) \hookrightarrow Hom_{\mathbf{Z}}(R, M) \hookrightarrow Hom_R(R, D)$$

Finalmente, Observemos que $Hom_R(R, M) \simeq M$ bajo el isomorfismo

$$\begin{aligned} \lambda : Hom_R(R, M) &\to M \\ f &\mapsto \lambda(f) = f(1) \end{aligned} \tag{4.1}$$

Teorema 4.3.15
Todo módulo izquierdo M tiene una capsula inyectiva en $R - Mod$.

Demostración: Sea $M \in R-Mod$ y $Q \in R-Mod$ un inyectivo tal que $M \leqslant Q$.
Sea $\mathcal{F} = \{H \leqslant Q | M \leqslant H\}$. Notemos $\mathcal{F} \neq \emptyset$ ya que $M \in \mathcal{F}$, así consideremos $(\mathcal{F}, \subseteq)$ y veamos lo siguiente ($\mathcal{F}$ satisface Zorn).
Sea $\mathcal{C} \subseteq \mathcal{F}$ una cadena, entonces $\cup\mathcal{C} = \overline{H} \leqslant Q$.
Sea $x \in \overline{H}$, $x \neq 0$ entonces existe α tal que $x \in H_\alpha$ así $M \leqslant H_\alpha$ entonces existe $r \in R$ tal que $0 \neq rx \in M$ de este modo $M \leqslant \overline{H}$ y por Zorn existen los máximos, digamos E.
Afirmación: E no tiene extensión esencial en Q porque E es máximo obtenemos

que no existe $K \in R - Mod$ tal que $E \leqslant K$.
Notese si tal K existe entonces

$$\begin{tikzcd}
0 \arrow[r] & E \arrow[r, "\iota"] \arrow[d, "i"'] & K \arrow[dl, dashed, "\bar{\iota}"] \\
& Q &
\end{tikzcd}$$

donde $\bar{\iota}_{|E} = \iota$, $\bar{\iota}$ es monomorfismo y $M \leqslant E \leqslant \bar{\iota}(K) \leqslant Q$ lo cual no puede suceder ya que contradice la maximalidad de E entonces $E = \bar{\iota}(K)$ y de este modo $E = K$.
Afirmación: E es inyectivo.
Primero, sea $T \leqslant Q$ tal que $E \cap T = \emptyset$ y $E \bigoplus T \leqslant Q$ (T se le llama pseudocomplemento de E en Q).
De este modo $E \simeq (E \bigoplus T)/T \subseteq Q/T$ (equivalencia de los submódulos en el cociente).
De este modo al ser E máximo $E \simeq (E \bigoplus T)/T = Q/T$ entonces $E \bigoplus T = Q$ y por tanto E es inyectivo (suma directa de inyectivos es inyectivo). Finalmente E es capsula inyectiva (denotada $E(M)$).