UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

IDEMPOTENTES EN ANILLOS DE BURNSIDE

TESIS

PARA OBTENER EL TITULO DE:

LICENCIADO EN MATEMATICAS

PRESENTA

FAUSTO HUMBERTO MEMBRILLO HERNANDEZ

MEXICO D.F AGOSTO 1990.

INTRODUCCION

Los anillos de Burnside tienen una gran importancia dentro del álgebra y de las matemáticas en general, en donde han servido para el estudio de los grupos finitos, y de la teoría de los números. Los anillos de Burnside juegan un papel central dentro de la topología algebraica y de ciertas ramas de la combinatoria. Además son un ejemplo importante de anillos conmutativos con unidad. Los anillos de Burnside tienen más que justificado su derecho a permanecer como uno de los tópicos más interesantes e importantes de las matemáticas modernas.

En buena medida, este trabajo esta autocontenido, sin embargo, pensamos que es necesario para la lectura de este trabajo, conocimientos fundamentales de la teoría de grupos y anillos. Es recomendable también conocimientos de álgebra conmutativa, topología y fundamentos de la teoría de Categorías, aunque no son indispensables.

El objetivo primordial es demostrar el teorema de Yoshida, publicado en *Journal of algebra* **80**, *90-105 (1983)*. Cuyo titulo es *Idempotents of Burnside Rings and Dress Induction Theorem.*

Aunque el objetivo fundamental es este teorema, aproveche la oportinidad para desarrollar la teoría de los anillos de Burnside en los primeros tres capítulos, hasta el teorema de Dress 7.10 y sus corolarios.

Los primeros tres capítulos están basados en las conferencias dictadas por el Dr. Ernesto Vallejo en el Instituto de Matemáticas, y en el Seminario sobre anillos de Burnside ofrecido por el Dr. Andreas Dress durante su estancia en el Instituto de Matemáticas en marzo de 1990. Creo que es importante mencionar aquí que gran parte de los teoremas acerca de los anillos de Burnside que se enuncian en este trabajo, fueron descubiertos por el Dr. Andreas Dress.

En el primer capítulo se enuncian y demuestran todos los requisitos acerca de acciones de un grupo en un conjunto. En todo el desarrollo del tema, cuando mencionamos al grupo G, estamos pensando que G es finito. Además, introducimos todos los conceptos preliminares a la definición del anillo de Burnside y sus distintas propiedades que se enuncian en el capítulo 2.

En la primera sección trabajamos en algunos ejemplos importantes de G-conjuntos, que son muy interesantes en sí mismos. Introducimos métodos para construir nuevos conjuntos con nuevas acciones a partir de otros ya conocidos.

En la segunda sección se enuncian y demuestran algunas propiedades fundamentales de los $G-$ *conjuntos*. Uno de los teoremas más importantes de este capítulo es el teorema de "estructura" de los G-conjuntos, este teorema nos dice cuales son exáctamente los componentes básicos de cualquier G-conjunto.

En la tercera sección introducimos el concepto de marca de un subconjunto H en un G-conjunto X. Este concepto juega un papel central en el desarrollo de la teoría. La marca de H nos permitirá obtener un morfismo de anillos φ, del anillo de Burnside de G al anillo $\mathbb{Z}^n$, donde n es el número de clases de conjugación de subgrupos de G.

El segundo capítulo se compone de las secciones 4 y 5. En la primera hacemos la construcción formal del anillo de Burnside $\Omega(G)$ para cualquier grupo finito G. Las clases de G-isomorfismo de los G-conjuntos finitos forman un semianillo conmutativo con uno, tomando la unión ajena como la suma y el producto cartesiano como la multiplicación del anillo. El anillo de Grothendieck de este semianillo es el anillo de Burnside de G.

En este capítulo encontramos explícitamente el anillo de Burnside para ciertos grupos interesantes, como son los cuaternios y el grupo diédrico de orden 8, entre otros. Terminamos esta sección con la definición de la función φ de la que ablamos arriba. Resulta que la función φ es inyectiva, y podemos pensar al anillo de Burnside dentro de $\mathbb{Z}^n$. El teorema 5.5 nos da una condición necesaria y suficiente para que un elemento de $\mathbb{Z}^n$ pertenezca al anillo de Burnside de G.

En el tercer capítulo se estudian las propiedades del espectro primo del anillo de Burnside. Además, se hace una generalización de los resultados a anillos, que también llamaremos de Burnside: Sea π un conjunto de números primos, entonces $\Omega_\pi(G) := \mathbb{Z}_\pi \bigotimes_{\mathbb{Z}} \Omega(G)$. En esta parte se enuncian teoremas de Dress que son muy importantes.

En el último capítulo, aprovechamos todo lo que se ha desarrollado en la tesis para poder probar el teorema de *Yoshida*. En la parte final damos un teorema muy interesante: Si H, G son grupos que tienen su anillo de Burnside isomorfo, entonces tiene el mismo orden.

Recientemente ya se sabe un poco más sobre este tema, en 1989 los doctores Gerardo Raggi y Ernesto Vallejo descubrieron lo siguiente: Si H, G son grupos Hamiltonianos y $\Omega(G) \cong \Omega(H)$, entonces $G \cong H$.

Es dificil mejorar este teorema, ya que a últimas fechas se han encontrado p-grupos no isomorfos, con el mismo anillo de Burnside.

CONTENIDO

1

Preliminares

So much depends
upon
a red wheel
barrow
glazed with rain
water
beside the white
chickens

The red wheel barrow
Whilliam Carlos Williams (1883-1963)

§1 ACCION DE UN GRUPO EN UN CONJUNTO

Todos los grupos que se utilizarán en este trabajo son finitos, a menos que se especifique lo contrario, ésta será una hipótesis general. Sin embargo, las proposiciones que valen también para grupos infinitos tienen demostraciones que no utilizan la hipótesis de finitud. El lector podrá notar que cuando hablemos de subgrupos de un grupo finito, podemos sustituir la hipótesis de finitud del grupo por la del índice de algún subgrupo.

En la primera sección de este capítulo analizamos algunos ejemplos importantes de G-conjuntos, se introducen métodos para construir nuevos G-conjuntos a partir de otros ya conocidos. En la segunda sección trabajamos en las propiedades fundamentales de los G-conjuntos hasta llegar, en la tercera sección, al conocido lema de Cauchy-Frobenius-Burnside.

Un grupo G puede actuar en un conjunto X por medio de una "multiplicación" donde un elemento de G por cualquier elemento de X tiene como valor algún elemento de X. Formalmente tenemos la siguiente definición:

1.1 DEFINICION

Sean G un grupo y X un conjunto. Una *acción de G en X* es una regla de composición $\mu : G \times X \to X \ : (g, x) \longmapsto gx$, que cumple con:

i) Para el elemento identidad e de G se tiene que: $ex = x \ \ \forall x \in X$,

ii) $(gh)x = g(hx)$, siempre que $g, h \in G$ y $x \in X$.

Bajo estas condiciones decimos que X es un *G-conjunto* y que G *actúa* en X.

Dada una acción de G en X, se tiene una relación de equivalencia $\sim$ en X: $x \sim y$ si y sólo si existe g en G tal que $x = gy$. Sus clases de equivalencia se llaman *las órbitas* de la acción. Denotamos por $O(x)$ la órbita de x.

Analizaremos algunos ejemplos de G-conjuntos que serán importantes posteriormente para el desarrollo de la teoría de los anillos de Burnside.

1.2 EJEMPLO

Sea G un grupo y X cualquier conjunto, definimos la acción *trivial* de G en X como sigue: $gx := x$, para todo elemento g de G y todo x en X; entonces X es un G-conjunto.

A lo largo de este trabajo denotaremos el hecho de que H sea un subgrupo del grupo G por $H \leq G$. Como notación adicional: si A es un conjunto, $|A|$ representa la cardinalidad de A.

1.3 EJEMPLO

Sea G un grupo y $H \leq G$ un subgrupo de G, consideremos el conjunto de *clases laterales izquierdas* de H en G: $G/H = \{gH : g \in G\}$. Definimos una acción de G en G/H como sigue:

$$g_1(g_2H) := (g_1g_2)H, \quad \forall g_1 \in G \text{ y } \forall\, g_2H \in G/H.$$

Así el conjunto G/H es un G-conjunto.

Demostración: La acción de G está bien definida, ya que si $gH = g'H$ entonces $gh = g'$, para alguna $h \in H$. Sea $f \in G$, entonces $f(g'H) = f(ghH) = f(gH)$. Ahora bien, tenemos que: $e(gH) = (eg)H = gH$ y que $(kf)gH = (kfg)H = k(fgH) = k(f(gH))$, lo que demuestra la afirmación. ∎

1.4 EJEMPLOS

Sea $(X_i)_{i\in I}$ una familia de G-conjuntos. Entonces:

i) La *unión ajena* de la familia (ó *coproducto* de la familia), que denotaremos $\biguplus_{i\in I} X_i$, es un G-conjunto de manera natural. La acción está dada por la acción en cada componente.

ii) El *producto cartesiano* de la familia $\prod_{i\in I} X_i$ es un G-conjunto, con acción definida por coordenadas: $g\bar{x} = g(x_i)_{i\in I} := (gx_i)_{i\in I}$.

1.5 EJEMPLO

Sean X, Y dos G-conjuntos. Sea $Hom(X,Y)$ el *conjunto de funciones* con *dominio* X y *codominio* Y. Afirmamos que $Hom(X,Y)$ es un G-conjunto, definiendo la acción de G en $Hom(X,Y)$ como:

$$(gF): X \longrightarrow Y : x \longmapsto (gF)(x) := gF(g^{-1}(x)), \;\; \forall F \in Hom(X,Y), \; g \in G, \; x \in X.$$

Demostración: Sea $F \in Hom(X,Y)$ entonces

$$eF = F, \text{ ya que } eF(x) = eF(e^{-1}x) = F(x), \; \forall x \in X.$$

Por otra parte:

$$[(hg)F](x) = (hg)F((hg)^{-1}x) = (hg)F(g^{-1}h^{-1}x) = h(gF(g^{-1}h^{-1}x)) =$$

$$h[(gF)(h^{-1}x)] = [h(gF)](x), \; \forall x \in X,$$

por tanto $(hg)F = h(gF)$. ∎

Los tres ejemplos siguientes son una muestra importante de como construir nuevos conjuntos con nuevas acciones, a partir de conjuntos y acciones ya definidas.

1.6 EJEMPLO

Sean X un G-conjunto y Y un H-conjunto, entonces $Hom(X,Y)$ es un $G \times H$-conjunto, con la acción:

$$(g,h)F: X \longrightarrow Y : x \longmapsto ((g,h)F)(x) := hF(g^{-1}(x)), \; \forall F \in Hom(X,Y), \; g \in G, \; h \in H.$$

Demostración: Sea $F \in Hom(X,Y)$, entonces $eF(x) = ((e_G, e_H)F)(x) = e_H F(e_G^{-1}x) = F(x), \; \forall x \in X$. Tomemos ahora $(g_1,h_1),(g_2,h_2) \in G \times H$, $F \in Hom(X,Y)$ entonces:

$$((g_1,h_1)[(g_2,h_2)F])(x) = h_1([(g_2,h_2)F](g_1^{-1}x))$$

$$= h_1h_2F(g_2^{-1}g_1^{-1}x) = h_1h_2F((g_1g_2)^{-1}x) = ((g_1g_2, h_1h_2)F)(x)$$

$$= ([(g_1, h_1)(g_2, h_2)]F)(x), \ \forall x \in X. \ \blacksquare$$

1.7 EJEMPLO

Sean X un G-conjunto y Y un H-conjunto. Entonces $X \times Y$ es un $G \times H$-conjunto, con acción diagonal: $(g, h)(x, y) := (gx, hy)$, $\forall (g, h) \in G \times H, (x, y) \in X \times Y$.

1.8 EJEMPLO

Sean $H \leq G$, un subgrupo del grupo G, y X un H-conjunto, entonces: $G \times X$ es un H-conjunto, con acción: $h(g, x) = (gh^{-1}, hx)$, para todo elemento $h \in H$ y para todo $(g, x) \in G \times X$.

Demostración: El elemento identidad de H actúa trivialmente: $e(g, x) = (ge^{-1}, ex) = (g, x)$, $\forall (g, x) \in G \times X$. Por otra parte, si $f, h \in H$, entonces:

$$(hf)(g, x) = (g(hf)^{-1}, hfx) = (gf^{-1}h^{-1}, hfx) = h(f(g, x)). \ \blacksquare$$

Cuando X es un G-conjunto y existe un *homomorfismo de grupos* del grupo H en G, podemos hacer de X un H-conjunto aprovechando la acción de G y el homomorfismo.

1.9 EJEMPLO

Si X es G-conjunto, H es un grupo y $F: H \to G$ es un homomorfismo de grupos, entonces X es un H-conjunto con la acción: $hx := F(h)x$, $\forall h \in H$, $x \in X$. Denotaremos este nuevo H-conjunto por F^*X.

Demostración: Sea $e_H \in H$, el elemento identidad de H, entonces: $e_H x = F(e_H)x = e_G x = x$, $\forall x \in X$. Sean $h_1, h_2 \in H$, tenemos:

$$(h_1 h_2)(x) = F(h_1 h_2)x = (F(h_1)F(h_2))x = F(h_1)(F(h_2)x) = h_1(h_2 x). \ \blacksquare$$

1.10 EJEMPLO

Sean $H \leq G$, un subgrupo de G, y X un H-conjunto. Por el ejemplo 1.8, $G \times X$ es un H-conjunto. Sea $G \times_H X$ el conjunto $G \times X$ módulo la relación de equivalencia determinada por esa acción. Para cada $(g,x) \in G \times X$ denotamos por $[(g,x)]$ su órbita.

Así $G \times_H X$ resulta ser un G-conjunto con acción: $g'(g,x) := (g'g,x)$, $\forall g' \in G$.

Demostración: Veamos que la acción está bien definida: si $(g',x') \in [(g,x)]$ entonces $(g',x') = h(g,x)$ para alguna $h \in H$. Tomemos una $f \in G$, entonces

$$f[(g',x')] = f[h(g,x)] = f[(gh^{-1},hx)] = [(fgh^{-1},hx)] = [h(fg,x)] = [(fg,x)] = f[(g,x)],$$

por lo que la acción está bien definida.

Veamos ahora que $G \times_H X$ es G-conjunto:

$$e[(g,x)] = [(eg,x)] = [(g,x)],$$

$$(fk)[(g,x)] = [((fk)g,x)] = [(f(kg),x)] = f[(kg,x)] = f(k[(g,x)]). \quad \blacksquare$$

1.11 EJEMPLO

Sea X un conjunto. En X^n, el producto cartesiano de X consigo mismo n veces (es decir $X^n := X \times \cdots \times X$), actúa el grupo de permutaciones de n elementos $S(n)$ vía:

$$\sigma(x_1,\ldots,x_n) := (x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(n)}),\ \forall \sigma \in S(n),\ \forall (x_1,\ldots,x_n) \in X^n.$$

Demostración: Sea I la identidad de $S(n)$, tenemos que $I\bar{x} = (x_{I(1)},\ldots,x_{I(n)}) = \bar{x}$, $\forall \bar{x} \in X^n$.

Tomemos $\varphi, \sigma \in S(n)$ y $\bar{x} \in X^n$, entonces:

$$\varphi(\sigma(x_1,\ldots,x_n)) = \varphi(x_{\sigma^{-1}(1)},\ldots,x_{\sigma^{-1}(n)}) = (x_{\sigma^{-1}(\varphi^{-1}(1))},\ldots,x_{\sigma^{-1}(\varphi^{-1}(n))})$$

$$= (x_{(\varphi\sigma)^{-1}(1)},\ldots,x_{(\varphi\sigma)^{-1}(n)}) = (\varphi\sigma)(x_1,\ldots,x_n). \quad \blacksquare$$

1.12 EJEMPLO

Si X es un G-conjunto , entonces en X^n actúa $S(n) \times G$ vía:

$$(\sigma, g)(x_1, \ldots, x_n) := (gx_{\sigma^{-1}(1)}, \ldots, gx_{\sigma^{-1}(n)}), \quad \forall (\sigma, g) \in S(n) \times G.$$

Demostración: Veamos la acción del elemento identidad:

$$(I, e_G)\bar{x} = (e_G x_{I(1)}, \ldots, e_G x_{I(n)}) = \bar{x}, \ \forall \bar{x} \in X^n.$$

Si $(\sigma_1, g_1), (\sigma_2, g_2) \in S(n) \times G$, entonces:

$$(\sigma_1, g_1)((\sigma_2, g_2)(x_1, \ldots, x_n)) = (\sigma_1, g_1)(g_2 x_{\sigma_2^{-1}(1)}, \ldots, g_2 x_{\sigma_2^{-1}(n)}) =$$

$$(g_1 g_2 x_{\sigma_2^{-1}\sigma_1^{-1}(1)}, \ldots, g_1 g_2 x_{\sigma_2^{-1}\sigma_1^{-1}(n)}) = (g_1 g_2, \sigma_1 \sigma_2)(x_1, \ldots, x_n). \quad \blacksquare$$

1.13 EJEMPLO

Para $q \in \mathbb{N}^+ := \{1, 2, \ldots\}$ y X un conjunto, definimos:

$$\binom{X}{q} := \{Y \subseteq X : |Y| = q\}, \quad \text{aquí } |Y| \text{ denota el orden de } Y.$$

Si X es un G-conjunto, entonces $\binom{X}{q}$ también es un G-conjunto, vía

$$gY := \{gy : y \in Y\}, \quad \forall\, Y \in \binom{X}{q}.$$

Demostración: Como X es un G-conjunto, la transformación $F_g : X \to X \ : x \to gx$ es biyectiva $\forall g \in G$, en consecuencia la acción está bien definida. Además:

$$eY = \{ey : y \in Y\} = Y, \quad \text{y}$$

$$(fg)(Y) = \{(fg)y : y \in Y\} = f(\{gy : y \in Y\}) = f(gY). \quad \blacksquare$$

1.14 EJEMPLO

Sean X un conjunto, $q \in \mathbb{N}^+$ y $\mathbb{N} := \{0, 1, \ldots\}$, definimos

$$S_q(X) := \{f: X \longrightarrow \mathbb{N} : \sum_{x \in X} f(x) = q\}.$$

Está claro que si $f \in S_q(X)$, $f(x) = 0$ para casi toda $x \in X$. Si X es G-conjunto entonces también $S_q(X)$ es G-conjunto, vía la acción:

$$gf: X \longrightarrow \mathbb{N} : x \longmapsto gf(x) := f(g^{-1}x).$$

Demostración: Es claro que la acción está bien definida. Veamos como actúa la identidad de G, $ef(x) = f(e^{-1}x) = f(x)$, $\forall x \in X$, $\forall f \in S_q(X)$; además:

$$[(kh)f](x) = \quad f((kh)^{-1}x) = f(h^{-1}(k^{-1}x)) = (hf)(k^{-1}x) =$$

$$[k(hf)](x), \ \forall x \in X, \quad \text{por tanto } (kh)f = k(hf), \ \forall f \in S_q(X) \text{ y } k, h \in G. \quad \blacksquare$$

Los dos últimos ejemplos son casos particulares de construcciones más generales que vale la pena mencionar. Esas construcciones son "naturales" en G y dan lugar a operaciones que han sido objeto de estudio para muchos matemáticos (ver por ejemplo: [Boorman-75], [Morris & Wensley-84], [Rymer-77], [Siebeneicher-76], [Vallejo-90]).

Como vimos en el ejemplo 1.12, si X es un G-conjunto entonces X^n es un $S(n) \times G$-conjunto. Observemos que las acciones de $S(n)$ y de G en X^n conmutan; es decir

$$\sigma g(\bar{x}) = g\sigma(\bar{x}), \quad \forall \sigma \in S(n), g \in G, \bar{x} \in X.$$

Ahora, si $H \leq S(n)$, entonces por restricción (ver ejemplo 1.9 con F la inclusión) H actúa en X^n y su acción sigue conmutando con la acción de G. Así el conjunto de H-órbitas X^n/H es un G-conjunto, con acción:

$$g[(x_1, \ldots, x_n)] := [(gx_1, \ldots, gx_n)], \quad \forall g \in G \ \text{ y } \forall [(x_1, \ldots, x_n)] \in X^n/H.$$

Si H es igual a $S_n(X)$, entonces $X^n/S(n)$ coincide con $S(n)$. Más adelante en 2.3 definiremos qué significa que dos G-conjuntos sean *isomorfos*; sin embargo, adelantamos aquí que el G-*isomorfismo* τ entre $X^n/S(n)$ y $S_n(X)$ es el siguiente:

$$\tau : X^n/S(n) \longrightarrow S_n(X) : [(x_1, \ldots, x_n)] \longmapsto f\colon X \longrightarrow \mathbb{N},$$

donde, para toda $x \in X$, tenemos que $f(x)$ es el número de veces que aparece x como coordenada de $(x_1, \ldots, x_n)$.

Tomemos ahora el siguiente conjunto:

$$X^{[n]} := \{(x_1, \ldots, x_n) \in X^n \colon x_i \neq x_j \ \forall i \neq j\},$$

es decir, el conjunto formado por n-adas donde las componentes son distintas dos a dos.

Una vez más, de forma análoga al ejemplo 1.12, si X es un G-conjunto $X^{[n]}$ es un $S(n) \times G$-conjunto, y las acciones de $S(n)$ y de G en $X^{[n]}$ conmutan.

Además si $H \leq S(n)$, un grupo de permutaciones, H actúa por restricción en $X^{[n]}$ y el conjunto de H-órbitas $X^{[n]}/H$ es un G-conjunto, como hicimos antes, si $H = S(n)$ se tiene que:

$$X^{[n]}/S(n) \cong \binom{X}{n}.$$

Aquí un G-isomorfismo es:

$$\psi : X^{[n]}/S(n) \longrightarrow \binom{X}{n} : [(x_1, \ldots, x_n)] \longmapsto \{x_1, \ldots, x_n\}.$$

Como vimos, al introducir "cocientes" por H en un grupo de permutaciones se obtienen G-conjuntos nuevos, que también son interesantes desde el punto de vista de la combinatoria equivariante (ver [Vallejo-90]).

§2 G-CONJUNTOS

En esta sección se enuncian y demuestran algunas propiedades fundamentales de los G-conjuntos. Una de las más importantes es el teorema de "estructura" de los G-conjuntos, este teorema nos dice cuales son exactamente los componentes básicos de cualquier G-conjunto. Estos "ladrillos" fundamentales resultan ser G-conjuntos de la forma del ejemplo 1.3, es decir de la forma G/H.

2.1 DEFINICION

Sea X un G-conjunto y sea $x \in X$, definimos el siguiente subgrupo de G:

$$G_x := \{g \in G : gx = x\} \leq G,$$

y le llamaremos el *estabilizador* de x ó el *grupo de isotropía* de x.

El grupo de isotropía de x tiene una relación muy estrecha con la órbita de x en X. De hecho cada órbita de la acción de G en X resulta ser un G-conjunto, con la misma acción de G.

2.2 DEFINICION

Un G-conjunto X se llama *transitivo* si para cada par de elementos $x, y \in X$, existe un elemento g en G tal que $gx = y$.

Obsérvese que un G-conjunto es transitivo si y sólo si en X hay una sola órbita. Ahora definiremos los morfismos de G-conjuntos y, como consecuencia, definiremos cuando dos G-conjuntos son esencialmente iguales, es decir *isomorfos*.

2.3 DEFINICION

Una función $f: X \to Y$ con X, Y G-conjuntos, se llama *equivariante* ó *G-morfismo* si cumple que: $f(gx) = gf(x)$, $\forall g \in G, x \in X$.

2.4 EJEMPLO

Sea G un grupo y sean H, K subgrupos de G. Si $H \leq K$ entonces podemos definir un G-morfismo π, llamado *proyección canónica*, como sigue

$$\pi: G/H \longrightarrow G/K: \ fH \longmapsto fK.$$

Demostración: Si $fH = f'H$, entonces $f = f'h$, para alguna $h \in H$; de allí que

$$\pi(fH) = fK = f'hK = f'K, \quad \text{ya que } \ h \in K.$$

Entonces π está bien definida. Notemos que π es claramente suprayectiva. Veamos que π es equivariante:

$$l\pi(fH) = l(fK) = (lf)K = \pi(lfH), \quad \forall l \in G. \quad \blacksquare$$

Los G-morfismos son los morfismos de G-conjuntos. Denotaremos por $Hom_G(X,Y)$ el conjunto de morfismos de G-conjuntos de X en Y. Notemos que la composición de dos G-morfismos es de nueva cuenta un G-morfismo. Además, la función identidad también es un G-morfismo.

Decimos que dos G-conjuntos X, Y son *isomorfos*, denotado $X \cong_G Y$, si existe una función $f: X \to Y$ equivariante y biyectiva; f se llama entonces un *isomorfismo* de G-conjuntos ó un *G-isomorfismo*.

2.5 OBSERVACIONES

Sean G un grupo y $g \in G$. Sean, además, X un G-conjunto y x_0 un elemento de X. Entonces:

i) $G_{gx_0} = gG_{x_0}g^{-1}$.

ii) $O(x_0) \cong_G G/G_{x_0}$.

iii) G/H es transitivo $\forall H \leq G$.

iv) Si un G-conjunto X es transitivo, entonces:

$$X \cong_G G/H, \text{ para algún } H \leq G.$$

Demostración: Para el primer inciso sea $h \in G$, tenemos que:

$$h \in G_{gx_0} \iff h(gx_0) = gx_0 \iff (g^{-1}hg)x_0 = x_0 \iff g^{-1}hg \in G_{x_0} \iff h \in gG_{x_0}g^{-1}.$$

En el inciso dos el isomorfismo es $\phi\colon O(x_0) \to G/G_{x_0} : gx_0 \longmapsto gG_{x_0}$. Si $x = gx_0 = g'x_0$, entonces $g^{-1}g' \in G_{x_0}$, por tanto $gG_{x_0} = g'G_{x_0}$. Así ϕ está bien definida.

Además, ϕ es claramente suprayectiva: $\forall\, g \in G$, $gx_0 \longmapsto gG_{x_0}$. Por otra parte, ϕ es inyectiva: si $\phi(x) = \phi(x')$, tenemos que $gx_0 = x$, $g'x_0 = x'$, para algunas $g, g' \in G$. Entonces $gG_{x_0} = g'G_{x_0}$ y $g^{-1}g'x_0 = x_0$, por tanto $g'x_0 = gx_0$, y finalmente $x = x'$. Sólo resta ver que ϕ es equivariante: $\phi(gx) = \phi(gg'x_0) = gg'G_{x_0} = g(g'G_{x_0}) = g\phi(x)$.

El inciso tercero es claro, y el cuarto tiene una demostración sencilla: por hipótesis $X = O(x_0)$, por tanto $X = O(x_0) \cong_G G/G_{x_0}$, y por (iii), X es transitivo. ∎

Sea G un grupo, tomemos H y K subgrupos de G, decimos que H y K son *conjugados* si existe un elemento $g \in G$ tal que $H = gKg^{-1}$. En este caso escribimos $H \sim K$. Nótese que G actúa en el conjunto de sus subgrupos mediante conjugación, a la órbita de un subgrupo H de G se le denotará por (H) y se le llamará *la clase de conjugación* del subgrupo H. Llamemos $\mathcal{C}(G)$ al *conjunto de clases de conjugación* de G:

$$\mathcal{C}(G) := \{(H) : H \leq G\}.$$

2.6 LEMA

Sean $H, K \leq G$, subgrupos de G, entonces:

$$G/H \cong_G G/K \iff H, K \text{ son conjugados en } G.$$

Demostración: $(\Longleftarrow)$: Supongamos que $K = gHg^{-1}$, para cierto $g \in G$. Definimos:

$$\phi: G/H \to G/K : aH \longmapsto ag^{-1}K.$$

Veamos que ϕ es un isomorfismo de G-conjuntos, con inversa:

$$\psi: G/K \to G/H : bK \longmapsto bgH.$$

Si $aH = a'H$, entonces $\phi(aH) = ag^{-1}K = ag^{-1}(gHg^{-1}) = (aH)g^{-1}$; analogamente $\phi(a'H) = a'Hg^{-1}$. Entonces $\phi(aH) = \phi(a'H)$ y ϕ está bien definida. Veamos que ϕ es equivariante:

$$\phi(b(aH)) = (ba)g^{-1}K = b(ag^{-1}K) = b\phi(aH), \quad \forall\, b \in G.$$

De la misma forma se prueba que ψ está bien definida y es equivariante. Veamos que son inversas:

$$\psi\phi(aH) = \psi((ag^{-1})K) = ag^{-1}gH = aH,$$

$$\phi\psi(bK) = \phi((bg)H) = bgg^{-1}K = bK.$$

Por tanto ϕ y ψ son isomorfismos de G-conjuntos.

$(\Longrightarrow)$: Sea $\alpha : G/H \to G/K$ un G-isomorfismo. Si $\alpha(eH) = gK$, afirmamos que $H = gKg^{-1}$. Notemos que $\alpha(bH) = b\alpha(eH) = bgK$. Entonces, claramente, su inversa es:

$$\alpha^{-1} : G/K \to G/H : bK \longmapsto bg^{-1}H.$$

Entonces $gK = \alpha(eH) = \alpha(hH) = h\alpha(eH) = hgK$, $\forall h \in H$. De allí que $HgK = gK$, por tanto $(g^{-1}Hg)K = K$, y en consecuencia $g^{-1}Hg \subseteq K$.

Si realizamos este mismo análisis empezando con α^{-1}, de manera análoga, llegamos a que $gKg^{-1} \subseteq H$. Por tanto $H = gKg^{-1}$. ∎

2.7 LEMA

Si $f: X \to Y$ es un G-isomorfismo, entonces

$$f(O(a)) = O(f(a)). \quad ∎$$

En general, como consecuencia del lema anterior, si $f: X \to T$ es morfismo de G-conjuntos y T es transitivo, entonces f es suprayectiva.

La siguiente proposición es básica para la teoría de los anillos de Burnside.

2.8 PROPOSICION

Todo G-conjunto es isomorfo a una unión ajena de G-conjuntos de la forma G/H.

Demostración: Sea X un G-conjunto. Entonces: $X = \biguplus_{i\in I} O(x_i)$, unión ajena de órbitas de G en X, con representante x_i para cada órbita.

Además $O(x_i) \cong_G G/G_{x_i}$, por medio del isomorfismo ϕ_i de 2.5 (ii), para cada $i \in I$. Observemos que:

$$\Phi : \biguplus_{i\in I} O(x_i) \longrightarrow \biguplus_{i\in I} G/G_{x_i},$$

definida por $\Phi(x) = \phi_i(x)$ si y sólo si $x \in O(x_i)$, está bien definida y es claramente biyectiva. Como cada ϕ_i es equivariante, entonces Φ es equivariante, por tanto isomorfismo. ∎

Sea G un grupo, tomemos además dos subgrupos H, K de G. Si $gHg^{-1} \subseteq K$, para algún $g \in G$, decimos que H es *subconjugado* de K.

2.9 PROPOSICION

Sean H, K subgrupos de G. Entonces

$$Hom_G(G/H, G/K) \neq \emptyset \iff H \text{ es subconjugado de } K.$$

Demostración: $(\Longrightarrow)$: Si $f: G/H \to G/K$ es morfismo de G-conjuntos y tomamos $g \in G$ tal que $f(eH) = gK$, entonces $f(hH) = (hg)K$, $\forall h \in H$. Luego,

$$g^{-1}hgK = g^{-1}f(hH) = g^{-1}f(eH) = g^{-1}gK = eK.$$

De allí que $g^{-1}hg \in K$ $\forall h \in H$, y $g^{-1}Hg \subseteq K$.

$(\Longleftarrow)$: Si $gHg^{-1} \subseteq K$, existe un isomorfismo de G-conjuntos $\phi: G/H \longrightarrow G/gHg^{-1}$, dado por el lema 2.6. Además, por el ejemplo 2.4, existe π la proyección canónica, que es equivariante. Por tanto $\pi\phi \in Hom_G(G/H, G/K)$. ∎

Notemos que si H es subconjugado de K, entonces cualquier conjugado de H es subconjugado de cualquier conjugado de K. Tenemos así una relación entre los elementos de $C(G)$, que llamaremos también "subconjugado de".

Observemos que tenemos lo siguiente:

$$(H) \leq (K) \overset{\text{def}}{\iff} H \text{ es subconjugado de } K \iff Hom_G(G/H, G/K) \neq \emptyset.$$

2.10 PROPOSICION

La relación "subconjugado de", que denotaremos por $\leq$, es un orden parcial en $C(G)$.

Demostración: Es claro que $(H) \leq (H)$, para cada $H \leq G$. Luego $\leq$ es reflexiva. Si $(H) \leq (K)$ y $(K) \leq (M)$, existen (por 2.9) φ, ψ G-equivariantes, tales que:

$$G/H \xrightarrow{\varphi} G/K \xrightarrow{\psi} G/M.$$

Entonces $\psi\varphi \in Hom_G(G/H, G/M)$, y $(H) \leq (M)$. Tenemos entonces que $\leq$ es transitiva.

Sólo resta mostrar que si $(H) \leq (K)$ y $(K) \leq (H)$, entonces $(K) = (H)$. Sabemos que existen g_1, g_2 tales que: $g_1 H g_1^{-1} \subseteq K$, $g_2 K g_2^{-1} \subseteq H$. Por tanto

$$H \supseteq g_2 K g_2^{-1} \supseteq g_2 g_1 H (g_2 g_1)^{-1}, \text{ así } H = g_2 K g_2^{-1}. \text{ Por lo tanto } (H) = (K). \quad \blacksquare$$

Notemos que en $C(G)$ toda cadena creciente $(H_1) \leq (H_2) \ldots$ se estaciona, por ser G un grupo finito. De hecho lo mismo sucede si los H_i tienen todos índice finito. Además "$\leq$" sigue siendo un orden parcial en el conjunto de clases de conjugación de subgrupos de índice finito.

2.11 DEFINICION

Una *representación* de un grupo G por permutaciones es un homomorfismo de grupos: $\phi: G \to S(n)$. Donde $S(n)$ es el grupo de permutaciones de un conjunto de n elementos.

Dos tales representaciones ϕ, ψ son *equivalentes* cuando existe una permutación σ en $S(n)$ tal que:

$$\phi(g) = \sigma\psi(g)\sigma^{-1}, \ \forall g \in G.$$

En este caso escribiremos $\phi \sim \psi$.

Observemos que si $X = \{x_1, \ldots, x_n\}$ es un G-conjunto finito con n elementos, éste determina una representación:

$$\phi_X: G \longrightarrow S(n): g \longmapsto \phi_X(g),$$

donde $\phi_X(g)$ está definida como sigue: si $gx_i = x_j$ entonces $\phi_X(g)(i) = j$.

A la inversa, si tenemos una representación $\phi: G \to S(n)$, obtenemos un G-conjunto: $X_\phi := \{1, \ldots, n\}$, con acción: $gi := \phi(g)i$, $\forall i \in X_\phi$.

2.12 OBSERVACION

Sean X, Y dos G-conjuntos. Entonces:

$$X \cong_G Y \iff \phi_X \sim \phi_Y.$$

Demostración: $(\Longrightarrow)$: Sea $\psi: X \to Y$ un G-isomorfismo y supongamos que $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_n\}$.

Sea $\sigma \in S(n)$ definida como sigue: $\sigma(i) := j$, donde $\psi(x_i) = y_j$. Entonces

$$[\sigma^{-1}\phi_Y(g)\sigma](i) = \sigma^{-1}(\phi_Y(g)(\sigma(i))) =$$

$$\sigma^{-1}(\sigma(\phi_X(g)(i))) = [\phi_X(g)](i), \ \forall g \in G, i \in \{1, \ldots, n\}.$$

Por tanto $\phi_X \sim \phi_Y$.

$(\Longleftarrow)$: Sabemos que $\phi_Y(g)\sigma = \sigma\phi_X(g)$, para alguna $\sigma \in S(n)$. Para toda $\rho \in S(n)$ definimos

$$\psi_\rho: X \longrightarrow Y: x_i \longmapsto y_{\rho(i)}.$$

Nótese la biyectividad de ψ_ρ. Es fácil ver que ψ_σ es equivariante:

$$\psi_\sigma(gx_i) = \psi_\sigma(x_{\phi_X(g)(i)}) = y_{\sigma[\phi_X(g)(i)]} = y_{\phi_Y(g)(\sigma(i))} = gy_{\sigma(i)} = g\psi_\sigma(x_i), \ \forall g \in G. \ \blacksquare$$

§ 3 LA MARCA DE H EN X

El concepto de marca de un subgupo H en un G-conjunto X, nos permitirá obtener un morfismo de anillos, entre el anillo de Burnside de G y un anillo que es un producto de varias copias del anillo de los números enteros $\mathbb{Z}$. La noción de marca es fundamental para la teoría de los anillos de Burnside.

En esta sección demostramos un resultado importante: el *Lema de Cauchy-Frobenius-Burnside,* mejor conocido como el *Lema de Burnside.*

3.1 DEFINICION

Sea X un G-conjunto y $H \leq G$, un subgrupo de G. Se define *el conjunto de puntos fijos* de X bajo la acción de H como:

$$X^H := \{x \in X : hx = x, \ \forall h \in H\}.$$

La *marca* de H en X es: $\varphi_H(X) := |X^H|$.

Es decir, la marca de H en X es el número de elementos que deja fijos la acción del subgrupo H de G.

3.2 LEMA

Sean X, Y G-conjuntos y $H \leq G$, entonces:

(1) $\varphi_H(X \uplus Y) = \varphi_H(X) + \varphi_H(Y)$.

(2) $\varphi_H(X \times Y) = \varphi_H(X) \cdot \varphi_H(Y)$.

Demostración:

(1) $\varphi_H(X \uplus Y) = |(X \uplus Y)^H| = |(X^H \uplus Y^H)| = |X^H| + |Y^H| = \varphi_H(X) + \varphi_H(Y)$.

(2) $\varphi_H(X \times Y) = |(X \times Y)^H| = |(X^H \times Y^H)| = \varphi_H(X) \cdot \varphi_H(Y)$. ∎

3.3 LEMA

$H \sim H' \Longrightarrow \varphi_H = \varphi_{H'}$.

Demostración: Sean X un G-conjunto y $g \in G$ tal que $H = gH'g^{-1}$. Entonces:

$$x \in X^H \Longleftrightarrow hx = x,\ \forall h \in H \Longleftrightarrow gh'g^{-1}x = x,\ \forall h' \in H' \Longleftrightarrow$$

$$h'g^{-1}x = g^{-1}x,\ \forall h' \in H' \Longleftrightarrow g^{-1}x \in X^{H'} \Longleftrightarrow x \in gX^{H'}$$

Por tanto $X^H = gX^{H'}$. Así:

$$\varphi_H(X) = |X^H| = |gX^{H'}| = |X^{H'}| = \varphi_{H'}(X). \quad \blacksquare$$

3.4 LEMA

Sean $H, K \leq G$ subgrupos del grupo G. Hay una biyección entre:

$$(G/H)^K \text{ y } Hom_G(G/K, G/H).$$

Demostración: Si $(K) \not\leq (H)$, entonces $Hom_G(G/K, G/H) = \emptyset$, por otra parte:

$$(G/H)^K = \{gH : k(gH) = gH,\ \forall k \in K\} =$$

$$\{gH : g^{-1}kgH = H,\ \forall k \in K\} = \{gH : g^{-1}Kg \subseteq H\} = \emptyset.$$

Supongamos que $(K) \leq (H)$ y definamos:

$$\Gamma : (G/H)^K \longrightarrow Hom_G(G/K, G/H) : gH \longmapsto \Gamma(gH) := \Gamma_g,$$

donde $\Gamma_g : G/K \longrightarrow G/H : xK \longmapsto (xg)H$.

Veamos que Γ_g está bien definida: Si $xK = x'K$, entonces $x' = xk$, para alguna $k \in K$. Por tanto

$$\Gamma_g(x'K) = (x'g)H = (xkg)H = x(k(gH)) = x(gH) = (xg)H = \Gamma_g(xK).$$

Sea $f \in G$ un elemento del grupo G, entonces

$$\Gamma_g(f(xK)) = \Gamma_g((fx)K) = (fx)gH = f(xgH) = f\Gamma_g(xH),$$

así Γ_g es equivariante. Además, si $g'H = gH$, entonces $g' = gh$, para alguna $h \in H$. Entonces:

$$\Gamma_{g'}(xK) = (xg')H = (xgh)H = xgH = \Gamma_g(xK), \quad \forall xK \in G/K.$$

De allí que Γ está bien definida.

Sea $\Gamma': Hom_G(G/K, G/H) \longrightarrow (G/H)^K : \alpha \longmapsto \alpha(eK)$. Notemos que Γ' está bien definida, ya que: $k(\alpha(eK)) = \alpha((ke)K) = \alpha(eK)$, $\forall k \in K$.

Además $[\Gamma(\Gamma'(\alpha))](fK) = [\Gamma(\alpha(eK))](fK) = [\Gamma(gH)](fK) = \Gamma_g(fK) = fgH = f\alpha(K) = \alpha(fK)$, donde $\alpha(eK) = gH$. De allí que $\Gamma\Gamma' = Id_{Hom_G(G/K,G/H)}$.

Por otra parte, $\Gamma'(\Gamma(gH)) = \Gamma'(\Gamma_g) = \Gamma_g(eK) = (eg)H = gH$. Entonces $\Gamma'\Gamma = Id_{(G/H)^K}$, y se sigue que Γ es una biyección con inversa Γ'. ∎

Sea H un subgrupo del grupo G. Llamaremos *el normalizador de H en G* al siguiente subgrupo de G:

$$N_G(H) := \{g \in G : gHg^{-1} = H\}.$$

Ya que H es normal en $N_g(H)$, podemos considerar el grupo cociente

$$W(H) := N_G(H)/H,$$

el grupo $W(H)$ se llamará *el grupo de Weyl de H*.

3.5 LEMA

Sea $H \leq G$ un subgrupo del grupo G, entonces $(G/H)^H$ es un $N_G(H)$-conjunto. Además: $(G/H)^H \cong_{N_G(H)} W(H)$.

Demostración: Veamos primero que $(G/H)^H$ es un $N_G(H)$-conjunto. Como $N_G(H)$ es un subgrupo de G que contiene a H, y como G actúa sobre G/H vía: $f(gH) = (fg)H$, $\forall f \in G$, bastará verificar que $n(gH) \in (G/H)^H$, si $n \in N_G(H)$ y $gH \in (G/H)^H$.

Sea $h \in H$, como H es normal en $N_G(H)$, existe $h' \in H$ tal que:

$$h(n(gH)) = (hn)(gH) = (nh')(gH) = n(h'(gH)) = n(gH).$$

Por tanto $(G/H)^H$ es un $N_G(H)$-conjunto. Veamos ahora que:

$$\tau: (G/H)^H \longrightarrow \frac{N_G(H)}{H} : gH \longmapsto gH,$$

es un $N_G(H)$-isomorfismo.

Veamos que τ está bien definida: Sea $gH \in (G/H)^H$, entonces $hgH = gH$, $\forall h \in H$, por tanto $g^{-1}Hg \subseteq H$, así $g^{-1}Hg = H$, ya que H es finito. Por ello $g \in N_G(H)$. Esto muestra que τ es la función identidad.

Es claro que τ es de $N_G(H)$-conjuntos: $n\tau(gH) = n(gH) = \tau(ngH)$. ∎

3.6 COROLARIO

(1) $\varphi_H(G/H) = |W(H)|$.

(2) $\varphi_H(G/K) = 0 \iff (H) \not\leq (K)$ en el orden de $\mathcal{C}(G)$ (de 2.10).

Demostración: (1) $\varphi_H(G/H) = |(G/H)^H| = |N_G(H)/H| = |W(H)|$.

(2) Por (3.4), (3.3) y (2.9). ∎

3.7 LEMA (Cauchy-Frobenius-Burnside)

Sean G un grupo finito y X un G-conjunto. Para cada $g \in G$, sea $X^g := \{x \in X: gx = x\}$, y sea N el número de órbitas de X bajo la acción de G. Entonces:

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Demostración: Notemos que

$$\sum_{g\in G} |X^g| = \Big| \biguplus_{g\in G} \{x \in X: gx = x\} \Big| = \big|\{(g,x) \in G \times X: gx = x\}\big| =$$

$$\Big| \biguplus_{x\in X} \{g \in G: gx = x\} \Big| = \sum_{x\in X} |G_x| .$$

Supongamos que $X = G/H$, para algún subgrupo H de G. Entonces, usando que $G_{ga} = gG_a g^{-1}$, tenemos:

$$\sum_{fH \in G/H} |G_{fH}| = \sum_{fH \in G/H} |fG_{eH}f^{-1}| = \sum_{fH \in G/H} |fHf^{-1}| = |G:H|\,|H| = |G|\,.$$

El caso general se sigue de que todo G-conjunto X es isomorfo a una unión ajena de G-conjuntos de la forma G/H. ∎

2

El anillo de Burnside

No hay que confundir la opinión que aquí
enuncio con la afectación que tienen ciertas
gentes para evitar en apariencia los cálculos,
reemplazando por largas frases lo que puede
expresarse muy brevemente por el álgebra,
y agregando así a la longitud de las
operaciones la longitud de un lenguaje que no
está hecho para expresarlas.
Estas gentes están atrasadas en cien años.

Evariste Galois (1811-1832)

§4 EL ANILLO DE BURNSIDE DEL GRUPO G

En este capítulo definiremos el anillo de Burnside y probaremos algunas de sus propiedades fundamentales. Los ejemplos concretos que analizamos harán más claro este concepto.

Consideremos un grupo G, no necesariamente finito, y consideremos sus G-conjuntos finitos. Notemos que la relación $\sim$ definida en los G-conjuntos como: $X \sim Y \overset{\text{def}}{\Longleftrightarrow} X \cong_G Y$, es una relación de equivalencia. Las clases de equivalencia se llaman clases de G-isomorfismo. La clase del G-conjunto X se denota $[X]$.

Llamaremos $\Omega^+(G)$ al conjunto de clases de G-isomorfismo de G-conjuntos finitos,

$$\Omega^+(G) := \{[X]\colon X \text{ es un } G\text{-conjunto finito}\}.$$

En $\Omega^+(G)$ tenemos dos operaciones binarias: la unión ajena, que también llamaremos *suma*, y el producto cartesiano que llamaremos *multiplicación* :

$$X + Y := X \biguplus Y; \quad X \cdot Y := X \times Y$$

(A menudo, por simplicidad, abusamos del lenguaje y denotamos clases y representantes con las mismas letras).

4.1 TEOREMA

Las operaciones suma y multiplicación en $\Omega^+(G)$ están bien definidas y hacen de $\Omega^+(G)$ un semianillo* conmutativo con unidad.

* Para ser anillo lo único que falta es la propiedad de tener inversos aditivos para todos sus elementos.

Demostración: Sean $[X],[Y] \in \Omega^+(G)$ y supongamos que $[X'] = [X]$, $[Y'] = [Y]$. Sean $\alpha: X \longrightarrow X'$, $\beta: Y \longrightarrow Y'$ G-isomorfismos. Definamos la función:

$$\varphi: X \biguplus Y \longrightarrow X' \biguplus Y': \; z \longmapsto \varphi(z) = \begin{cases} \alpha(z), & \text{si } z \in X; \\ \beta(z), & \text{si } z \in Y. \end{cases}$$

Es claro que la función φ es un G-isomorfismo. Así, la suma en $\Omega^+(G)$ está bien definida.

Además, $X + Y = X \uplus Y \cong_G Y \uplus X = Y + X$, por lo que la suma es conmutativa. Por otra parte $(X \uplus Y) \uplus Z \cong_G X \uplus (Y \uplus Z)$, y la suma es asociativa. Obsérvese que $X + \emptyset = X \uplus \emptyset \cong_G X$, entonces el *conjunto vacío* es el elemento neutro para la suma en $\Omega^+(G)$.

Ahora sea ψ definida como sigue,

$$\psi: X \times Y \longrightarrow X' \times Y': \; (x, y) \longmapsto (\alpha(x), \beta(y)).$$

Entonces, ψ es una función biyectiva, ya que α y β lo eran. Además, como la acción de G es diagonal, ψ es un G-isomorfismo, por ello la multiplicación en $\Omega^+(G)$ está bien definida.

Por otra parte es claro que $X \times Y \cong_G Y \times X$, así la multiplicación es conmutativa. Como $(X \times Y) \times Z \cong_G X \times (Y \times Z)$, se sigue la asociatividad de la multiplicación. Más aun $X \times G/G \cong_G X$, $\forall X \in \Omega^+(G)$. Así la unidad de $\Omega^+(G)$ es G/G.

Como $\Omega^+(G)$ es conmutativo, sólo resta mostrar la distributividad derecha. Consideremos la función:

$$\tau: X \times (Y \biguplus Z) \longrightarrow X \times Y \biguplus X \times Z: \; (x, w) \longmapsto \begin{cases} (x, w) \in X \times Y, & \text{si } w \in Y; \\ (x, w) \in X \times Z, & \text{si } w \in Z. \end{cases}$$

Es claro que τ es G-isomorfismo. ∎

El semianillo $\Omega^+(G)$ es el primer paso para la construcción del anillo de Burnside de G. En el caso en que G sea el grupo trivial, veamos como luce $\Omega^+(G)$.

4.2 EJEMPLO

Sea $G = \{e\}$ el grupo trivial, Entonces: $\Omega^+(G) \cong \mathbb{N}$.

Demostración: Sea X un G-conjunto, entonces e actúa trivialmente en X, y por lo tanto su clase depende solamente de su orden. Así el isomorfismo de semianillos es claro:

$$\psi: \Omega^+(e) \longrightarrow \mathbb{N}: [X] \longmapsto |X|. \quad \blacksquare$$

4.3 LEMA

Vale la ley de la cancelación para la suma en $\Omega^+(G)$.

Demostración: Sean X, Y, Z G-conjuntos y supongamos que $[X] + [Z] = [Y] + [Z]$. Tenemos que demostrar que $[X] = [Y]$, es decir que X y Y son G-isomorfos.

Tomemos $\psi: X \uplus Z \longrightarrow Y \uplus Z$, un isomorfismo de G-conjuntos. Si restringimos ψ a una sola órbita de $X \uplus Z$, por el lema 2.7, la imagen de ψ será una órbita isomorfa en $Y \uplus Z$. Por tanto $X \uplus Z$ y $Y \uplus Z$ tienen órbitas isomorfas. Como las órbitas de Z son las mismas para las dos sumas, tenemos que las órbitas de X son isomorfas a las de Y, por lo tanto X es isomorfo a Y. Así pues $[X] = [Y]$. $\blacksquare$

El lema anterior nos permitirá construir un anillo "agregando los inversos aditivos" al semianillo $\Omega^+(G)$, de la misma manera como se construyen los números enteros a partir de los naturales.

4.4 PROPOSICON Y DEFINICION

Sea G un grupo. Consideremos el conjunto de expresiones formales:

$$\Delta := \{X - Y : X, Y \in \Omega^+(G)\},$$

y definimos una relación:

$$X - Y \sim W - Z \overset{\text{def}}{\Longleftrightarrow} X + Z = W + Y.$$

Entonces $\sim$ es una relación de equivalencia, y el conjunto cociente $\Delta/\sim$ admite de manera natural una estructura de anillo conmutativo. Si $[X],[Y] \in \Delta/\sim$, entonces

$$[X]+[Y] := [X+Y] \;,$$

$$[X][Y] := [XY] \;.$$

Este anillo es *el anillo de Grothendieck* de $\Omega^+(G)$, y lo denotaremos por $\Omega(G)$. Podemos definir ahora el anillo de Burnside: si el grupo G es finito, $\Omega(G)$ se llama *el anillo de Burnside* de G.

Observemos que $\psi : \Omega^+(G) \longrightarrow \Omega(G) : X \longmapsto [X]$ es un morfismo inyectivo de semianillos. Abusamos del lenguaje, y escribimos X por $[X]$, además de escribir $=$ por $\cong$.

El siguiente lema, aunque parece "técnico", nos permitirá construir homomorfismos de anillos, con dominio $\Omega(G)$, definiéndolos únicamente para los elementos de $\Omega^+(G)$, es decir, definiéndolos solamente para G-conjuntos.

4.5 LEMA

Sean R un anillo con unidad, G un grupo y $f: \Omega^+(G) \longrightarrow R$ una función aditiva y multiplicativa (i.e. f es un morfismo de semianillos). Entonces f se extiende de manera única a un morfismo de anillos
$F: \Omega(G) \longrightarrow R$.

Demostración: Definimos F en los elementos de $\Omega(G)$ como:

$$F(X-Y) := f(X) - f(Y).$$

Entonces F es claramente morfismo de anillos, y obviamente extiende a f.

Además la extensión es única: si ψ es un morfismo de anillos que extiende a f, entonces

$$\psi(X-Y) = \psi(X) - \psi(Y) = f(X) - f(Y) = F(X-Y). \quad \blacksquare$$

Si H, G son grupos y $F: H \longrightarrow G$ un homomorfismo de grupos, de acuerdo al ejemplo 1.9, podemos hacer de cualquier G-conjunto X, un H-conjunto $F^{\bullet}X$, que como conjunto es X, pero con la acción de H: $hx := F(h)x, \; \forall x \in F^{\bullet}X$.

Tenemos así una función:

$$F^{\bullet}: \Omega^{+}(G) \longrightarrow \Omega^{+}(H): \quad X \longmapsto F^{\bullet}X.$$

Es fácil ver que $F^{\bullet}$ es aditiva: Sean X, Y G-conjuntos, consideremos los H-conjuntos $F^{\bullet}(X \uplus Y)$ y $F^{\bullet}(X) \uplus F^{\bullet}(Y)$, que son iguales como conjuntos. Veamos que la acción es la misma: sea $h \in H$ arbitraria, en $F^{\bullet}(X \uplus Y), hx = F(h)x, hy = F(h)y$, para todo $x \in X, y \in Y$. Esta es la misma acción de H en $F^{\bullet}(X) \uplus F^{\bullet}(Y)$, y por lo tanto son isomorfos.

Veamos ahora que $F^{\bullet}$ es multiplicativa: consideremos los dos H-conjuntos $F^{\bullet}(X \times Y)$ y $F^{\bullet}(X) \times F^{\bullet}(Y)$. Estos son iguales como conjuntos, y la acción es la claramente la misma, en consecuencia son isomorfos. Por lo tanto $F^{\bullet}$ es multiplicativa y, por el lema anterior, se extiende de manera única a un morfismo de anillos $F^{\bullet}: \Omega(G) \longrightarrow \Omega(H)$.

4.6 LEMA

Ω es un funtor contravariante de la categoría de grupos $\mathcal{G}$ en la categoría de anillos conmutativos con unidad $\mathcal{R}$.

Demostración: Tenemos lo siguiente:

$$\begin{array}{cccc} \Omega: & \mathcal{G} & \longrightarrow & \mathcal{R} \\ & G & \longmapsto & \Omega(G) \\ & \varphi \downarrow & & \uparrow \varphi^{\bullet} \\ & H & \longmapsto & \Omega(H) \end{array}$$

Es claro que para cualquier grupo G, se tiene $(Id_G)^{\bullet} = Id_{\Omega(G)}$. Además si $\varphi: G \longrightarrow H$, y $\psi: H \longrightarrow K$, entonces $(\psi \circ \varphi)^{\bullet} = \varphi^{\bullet} \circ \psi^{\bullet}$, ya que si X es un K-conjunto, entonces $\psi^{\bullet}X$ es un H-conjunto. Adicionalmente $\varphi^{\bullet}(\psi^{\bullet}X)$ es un G-conjunto, con acción: $gx := \varphi(g)x := \psi(\varphi(g))x$. Que es la acción de G en $(\psi \circ \varphi)^{\bullet}X$. En consecuencia son iguales, y por tanto

$$(\psi \circ \varphi)^{\bullet} = \varphi^{\bullet} \circ \psi^{\bullet}. \quad \blacksquare$$

4.7 PROPOSICION

Como grupo abeliano $\Omega(G)$ es libre, generado por los elementos G/H_i, con $(H_i) \in \mathcal{C}(G)$.

Demostración: Todo G-conjunto X, se puede expresar como unión ajena de sus órbitas,

$$X = \biguplus_{(H)\in\mathcal{C}(G)} a_H \frac{G}{H}, \quad a_H \geq 0.$$

Es claro entonces que como *semigrupo** abeliano

$$\Omega^+(G) = \bigoplus_{(H)\in\mathcal{C}(G)} \mathbb{N}.$$

El anillo de Grothendieck de $\mathbb{N}$ es $\mathbb{Z}$, es claro ahora que $\Omega(G)$ "extiende los coeficientes a_H a los números enteros", por lo tanto, como grupo abeliano

$$\Omega(G) = \bigoplus_{(H)\in\mathcal{C}(G)} \mathbb{Z}. \quad \blacksquare$$

Obviamente $\Omega(G)$ es un $\mathbb{Z}$-módulo con base los elementos de $\mathcal{C}(G)$. Como corolario a la proposición anterior, si $G = \{e\}$, entonces $\Omega(G) \cong \mathbb{Z}$ como anillo.

Consideremos ahora otro ejemplo de anillo de Burnside.

4.8 EJEMPLO

Calculemos el anillo de Burnside de $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. Sean $a := \frac{\mathbb{Z}_2}{<\bar{0}>}, e := \frac{\mathbb{Z}_2}{\mathbb{Z}_2}$ los dos generadores de $\Omega(\mathbb{Z}_2)$. Entonces, como grupo abeliano

$$\Omega(\mathbb{Z}_2) = \mathbb{Z}a \bigoplus \mathbb{Z}e.$$

Consideremos la función

$$\frac{\mathbb{Z}_2}{<\bar{0}>} \times \frac{\mathbb{Z}_2}{<\bar{0}>} \xrightarrow{\psi} \frac{\mathbb{Z}_2}{<\bar{0}>} \biguplus \frac{\mathbb{Z}_2}{<\bar{0}>},$$

definida en cada elemento como sigue: $(\bar{1}, \bar{0}) \longmapsto \bar{1}$, $(\bar{0}, \bar{0}) \longmapsto \bar{0}$; $(\bar{0}, \bar{1}) \longmapsto \bar{1}'$, $(\bar{1}, \bar{1}) \longmapsto \bar{0}'$. Donde $\bar{1}, \bar{0}$ denotan los elementos de la primera componente de la unión ajena y $\bar{1}', \bar{0}'$ los

* Para ser Grupo, falta la propiedad de que todos los elementos tengan inverso.

correspondientes elementos de la segunda componente. Como ψ es un isomorfismo de G-conjuntos, tenemos que $aa = 2a$.

Tenemos que la tabla de multiplicar de los elementos básicos del anillo $\Omega(\mathbb{Z}_2)$ es:

$$\begin{array}{c|cc} & e & a \\ \hline e & e & a \\ a & a & 2a \end{array}$$

4.9 PROPOSICION

Sean H, K subgrupos del grupo G. Hay biyecciones canónicas entre los siguientes tres conjuntos:

(1) El conjunto de las G-órbitas de $G/H \times G/K$.

(2) El conjunto de las H-órbitas de G/K.

(3) El conjunto de las clases laterales dobles en G, de la forma HgK, $g \in G$.

Demostración: Si denotamos por $O_H(gK)$ la H-órbita de gK, claramente tenemos $O_H(gK) = O_H(g'K) \iff HgK = Hg'K$. Luego, la asignación $O_H(gK) \longmapsto HgK$ establece claramente una biyección entre (2) y (3).

Por otra parte, a cada G-órbita $O_G(fH, lK)$ de $G/H \times G/K$, le hacemos corresponder la H-órbita $O_H(f^{-1}lK)$ de G/K. Tenemos, $O_G(fH, lK) = O_G(f'H, l'K) \Longrightarrow$ existe $g \in G$ tal que $(fH, lK) = g(f'H, l'K) \Longrightarrow gf'H = fH$ y $lK = gl'K \Longrightarrow f^{-1}gf' \in H$ y $f^{-1}lK = f^{-1}gl'K \Longrightarrow f'^{-1}g^{-1}f \in H$. Por lo tanto $O_H(f^{-1}lK) = O_H(f^{-1}gl'K) = O_H(f'^{-1}l'K)$. Por ello, la asociación está bien definida.

Si $(fH, lK) \in G/H \times G/K$ entonces pertenecerá a la órbita $O_G(eH, f^{-1}lK)$, así toda G-órbita de $G/H \times G/K$ tiene un representante de la forma (eH, gK). Además, $(eH, gK) = g'(eH, g''K) \iff g' \in H$. Tenemos entonces que:

$$O_H(gK) = O_H(g'g''K) = O_H(g''K).$$

Así pues la asignación es inyectiva y suprayectiva, por lo tanto es biyección. ∎

La siguiente proposición será útil para el cálculo de la tabla de multiplicar de los elementos de la forma G/H de $\Omega(G)$. Por la proposición 4.7, esta tabla es suficiente para calcular cualquier producto entre los elementos de $\Omega(G)$, por ello, la tabla determina al anillo de Burnside de G.

4.10 PROPOSICION

Sean $H, K \leq G$ subgrupos de G. Sea $(aH, bK) \in G/H \times G/K$, entonces:

$$G_{(aH,bK)} = aHa^{-1} \bigcap bKb^{-1}.$$

Demostración: Si $g(aH) = aH$ entonces $a^{-1}ga \in H$, así $g \in aHa^{-1}$. Análogamente $g \in bKb^{-1}$. Luego, $G_{(aH,bK)} \subseteq aHa^{-1} \bigcap bKb^{-1}$, y la otra contención es inmediata. ∎

4.11 COROLARIO

Si H, K son subgrupos de G y R es un conjunto de representantes de la partición inducida en G por las clases laterales dobles de la forma HgK. Entonces:

$$G/H \times G/K = \biguplus_{g \in R} \frac{G}{H \bigcap gKg^{-1}}.$$

Demostración:

$$G/H \times G/K = \biguplus_{g \in R} O(eH, gK) = \biguplus_{g \in R} G/G_{(eH,gK)} = \biguplus_{g \in R} \frac{G}{H \bigcap gKg^{-1}}. \quad ∎$$

Los cálculos de la multiplicación de dos elementos $G/H, G/K$ de $\Omega(G)$ pueden facilitarse si H ó K es normal. En particular, cuando G es abeliano, el cálculo de la tabla de multiplicar de los elementos básicos de $\Omega(G)$, resulta muy sencillo.

4.12 COROLARIO

Sean $H, K \leq G$ subgrupos de G, y sea R un conjunto de representantes de la partición inducida en G por las clases laterales dobles de la forma HgK. Supongamos que K es normal, entonces:

$$G/H \times G/K = \biguplus_{g \in R} \frac{G}{H \bigcap K} = \left(\frac{|H \bigcap K| \; |G|}{|H| \; |K|} \right) \frac{G}{H \bigcap K}.$$

Demostración: Simplemente calcúlese el número de clases bilaterales de la forma HgK, con g en G (i.e. $|R|$). ∎

Obsérvese que pudimos haber supuesto que H es normal, en lugar de suponerlo para K, ya que $\Omega(G)$ es un anillo conmutativo.

Utilizando estos últimos resultados, calcularemos explícitamente la tabla de multiplicar de los elementos básicos en el anillo Burnside de algunos grupos interesantes, de esta manera estos anillos estarán completamente determinados.

4.13 EJEMPLO

Denotemos por $\mathbb{Z}_n$ al grupo cociente $\mathbb{Z}/n\mathbb{Z}$, que llamaremos *el grupo de los enteros módulo n*. Calcularemos el anillo de Burnside de $\mathbb{Z}_n$, para todo n en $\mathbb{N}$.

Todos los subgrupos de $\mathbb{Z}_n$ son de la forma $\lambda\mathbb{Z}_n := \{\lambda x : x \in \mathbb{Z}_n\}$, con λ un divisor del natural n.

Sean λ, μ divisores de n, como $\mathbb{Z}_n$ es abeliano, el número de clases bilaterales de los subgrupos $\lambda\mathbb{Z}_n, \mu\mathbb{Z}_n$ es $[\mathbb{Z}_n : \lambda\mathbb{Z}_n + \mu\mathbb{Z}_n]$. Así que:

$$\frac{\mathbb{Z}_n}{\lambda\mathbb{Z}_n} \times \frac{\mathbb{Z}_n}{\mu\mathbb{Z}_n} = [\mathbb{Z}_n : \lambda\mathbb{Z}_n + \mu\mathbb{Z}_n] \frac{\mathbb{Z}_n}{\lambda\mathbb{Z}_n \bigcap \mu\mathbb{Z}_n}.$$

Podemos mejorar esta fórmula observando que $\lambda\mathbb{Z}_n + \mu\mathbb{Z}_n = (\lambda, \mu)\mathbb{Z}_n$, donde (λ, μ) denota el máximo común divisor de λ y μ. Además, tenemos que $\lambda\mathbb{Z}_n \bigcap \mu\mathbb{Z}_n = [\lambda, \mu]\mathbb{Z}_n$, donde $[\lambda, \mu]$ es el mínimo común múltiplo de λ y μ. Así, la multiplicación de cualesquiera dos básicos en $\Omega(\mathbb{Z}_n)$ es:

$$\frac{\mathbb{Z}_n}{\lambda\mathbb{Z}_n} \times \frac{\mathbb{Z}_n}{\mu\mathbb{Z}_n} = (\lambda, \mu) \frac{\mathbb{Z}_n}{[\lambda, \mu]\mathbb{Z}_n}.$$

Denotemos por $\lambda|n$ el hecho de que λ divida a n, entonces $\Omega(\mathbb{Z}_n)$, como grupo abeliano, es:

$$\Omega(\mathbb{Z}_n) = \bigoplus_{\lambda|n} \mathbb{Z}\left(\frac{\mathbb{Z}_n}{\lambda\mathbb{Z}_n}\right). \quad ∎$$

Sea G un grupo y sean $a_1, \ldots, a_n \in G$. Denotaremos por $< a_1, \ldots, a_n >$ al subgrupo generado por $a_1, \ldots, a_n$.

4.14 EJEMPLO

Consideremos ahora el grupo de *permutaciones* de 3 elementos, denotado $S(3)$. Como sabemos este grupo es isomorfo al grupo *diédrico de orden* 6. Las clases de conjugación de $S(3)$ son:

$$C(S(3)) = \{(Id), (<(1\ 2)>), (<(1\ 2\ 3)>), (S(3))\}.$$

Sean $H_1 = S(3), H_2 = <(1\ 2\ 3)>, H_3 = <(1\ 2)>, H_4 = Id$, representantes de las clases de conjugación de $S(3)$. De éstos el único que no es normal en $S(3)$ es H_3. Como sabemos, $\Omega(S(3))$ considerado como grupo abeliano es:

$$\Omega(S(3)) = \mathbb{Z}\frac{S(3)}{H_1} \bigoplus \mathbb{Z}\frac{S(3)}{H_2} \bigoplus \mathbb{Z}\frac{S(3)}{H_3} \bigoplus \mathbb{Z}\frac{S(3)}{H_4}.$$

Usando el corolario 4.12, se calculan facilmente todos los productos de los $S(3)$-conjuntos básicos, excepto el producto $S(3)/H_3 \times S(3)/H_3$. Sea $R := \{e, (1\ 3)\}$ un conjunto de representantes de las clases bilaterales de la forma $<(1\ 2)>a<(1\ 2)>$, $a \in S(3)$. Entonces:

$$S(3)/H_3 \times S(3)/H_3 = \sum_{a \in R} \frac{S(3)}{<(1\ 2)> \bigcap a <(1\ 2)> a^{-1}}$$

$$= \frac{S(3)}{<(1\ 2)> \bigcap <(1\ 2)>} + \frac{S(3)}{<(1\ 2)> \bigcap (1\ 3) <(1\ 2)> (1\ 3)}$$

$$= S(3)/H_3 + S(3)/Id = S(3)/H_3 + S(3)/H_4.$$

Además $S(3)/H_1$ es el elemento identidad de $\Omega(S(3))$. Así, la tabla de multiplicar de $\Omega(S(3))$ es:

	$S(3)/H_1$	$S(3)/H_2$	$S(3)/H_3$	$S(3)/H_4$
$S(3)/H_1$	$S(3)/H_1$	$S(3)/H_2$	$S(3)/H_3$	$S(3)/H_4$
$S(3)/H_2$	$S(3)/H_2$	$2S(3)/H_2$	$S(3)/H_4$	$2S(3)/H_4$
$S(3)/H_3$	$S(3)/H_3$	$S(3)/H_4$	$S(3)/H_3 + S(3)/H_4$	$3S(3)/H_4$
$S(3)/H_4$	$S(3)/H_4$	$2S(3)/H_4$	$3S(3)/H_4$	$6S(3)/H_4$

4.15 EJEMPLO

Consideremos ahora el grupo de los *cuaternios*, definido por: $Q := \{\pm 1, \pm i, \pm j, \pm k\}$, con las reglas de multiplicar: $i^2 = j^2 = k^2 = 1; ij = k, jk = i, ki = j; ji = -k, kj = -i, ik = -j$; y las reglas usuales para la multiplicación por ± 1.

Todos los subgrupos de Q son normales y estos son:

$$H_1 = Q; H_2 =< i >; H_3 =< j >; H_4 =< k >; H_5 =< -1 >; H_6 = 1.$$

Si denotamos por $\mathbb{Z}^n$ el producto cartesiano de $\mathbb{Z}$ consigo mismo n veces, entonces $\Omega(Q) \cong \mathbb{Z}^6$ como grupo abeliano.

Mostramos a continuación la tabla de multiplicar de los Q-conjuntos básicos de $\Omega(Q)$.

	Q/H_1	Q/H_2	Q/H_3	Q/H_4	Q/H_5	Q/H_6
Q/H_1	Q/H_1	Q/H_2	Q/H_3	Q/H_4	Q/H_5	Q/H_6
Q/H_2	Q/H_2	$2Q/H_2$	Q/H_5	Q/H_5	$2Q/H_5$	$2Q/H_6$
Q/H_3	Q/H_3	Q/H_5	$2Q/H_3$	Q/H_5	$2Q/H_5$	$2Q/H_6$
Q/H_4	Q/H_4	Q/H_5	Q/H_5	$2Q/H_4$	$2Q/H_5$	$2Q/H_6$
Q/H_5	Q/H_5	$2Q/H_5$	$2Q/H_5$	$2Q/H_5$	$4Q/H_5$	$4Q/H_6$
Q/H_6	Q/H_6	$2Q/H_6$	$2Q/H_6$	$2Q/H_6$	$4Q/H_6$	$8Q/H_6$

4.16 EJEMPLO

Consideremos el *grupo diédrico de orden* 8, denotado D_4. Este grupo es un subgrupo del grupo de permutaciones de 4 elementos $S(4)$, formado por las permutaciones:

$$D_4 := \{Id, (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 3), (2\ 4), (1\ 3)(2\ 4)\}.$$

En D_4 existen 7 subgrupos normales:

$$H_1 := D_4, \quad H_8 := Id,$$

$$H_2 := \{Id, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\},$$

$$H_3 := \{Id, (1\ 3), (2\ 4), (1\ 3)(2\ 4)\},$$

$$H_4 := \{Id, (1\ 4)(2\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4)\},$$

$$H_5 := \{Id, (1\ 3)(2\ 4)\}.$$

Además existen otras dos clases de conjugación de subgrupos no normales. Los representantes de estas clases son:

$$H_6 := \{Id, (1\ 4)(2\ 3)\},\ H_7 := \{Id, (1\ 3)\}.$$

Por lo tanto $\Omega(D_4) \cong \mathbb{Z}^8$ como grupo abeliano. Utilizando los dos últimos corolarios obtenemos la tabla de multiplicar de los D_4-conjuntos básicos:

	D_4/H_1	D_4/H_2	D_4/H_3	D_4/H_4	D_4/H_5	D_4/H_6	D_4/H_7	D_4/H_8
D_4/H_1	D_4/H_1	D_4/H_2	D_4/H_3	D_4/H_4	D_4/H_5	D_4/H_6	D_4/H_7	D_4/H_8
D_4/H_2	D_4/H_2	$2D_4/H_2$	D_4/H_5	D_4/H_5	$2D_4/H_5$	D_4/H_8	D_4/H_8	$2D_4/H_8$
D_4/H_3	D_4/H_3	D_4/H_5	$2D_4/H_3$	D_4/H_5	$2D_4/H_5$	D_4/H_8	$2D_4/H_7$	$2D_4/H_8$
D_4/H_4	D_4/H_4	D_4/H_5	D_4/H_5	$2D_4/H_4$	$2D_4/H_5$	$2D_4/H_6$	D_4/H_8	$2D_4/H_8$
D_4/H_5	D_4/H_5	$2D_4/H_5$	$2D_4/H_5$	$2D_4/H_5$	$4D_4/H_5$	$2D_4/H_8$	$2D_4/H_8$	$4D_4/H_8$
D_4/H_6	D_4/H_6	D_4/H_8	D_4/H_8	$2D_4/H_6$	$2D_4/H_8$	$2D_4/H_6 + D_4/H_8$	$2D_4/H_8$	$4D_4/H_8$
D_4/H_7	D_4/H_7	D_4/H_8	$2D_4/H_7$	D_4/H_8	$2D_4/H_8$	$2D_4/H_8$	$2D_4/H_7 + D_4/H_8$	$4D_4/H_8$
D_4/H_8	D_4/H_8	$2D_4/H_8$	$2D_4/H_8$	$2D_4/H_8$	$4D_4/H_8$	$4D_4/H_8$	$4D_4/H_8$	$8D_4/H_8$

Consideremos ahora un grupo G finito cualquiera, por el lema 3.2, para cada clase de conjugación $(H) \in \mathcal{C}(G)$ tenemos que la función φ_H, definida en un G-conjunto X como $\varphi_H(X) = |X^H|$, es un homomorfismo de semianillos. Definimos la función:

$$\varphi : \Omega^+(G) \longrightarrow \prod_{(H)\in\mathcal{C}(G)} \mathbb{Z}$$

$$X \longmapsto (\varphi_H(X))_{(H)\in\mathcal{C}(G)}\,.$$

Como está definida φ resulta ser aditiva y multiplicativa, ya que en cada entrada las φ_H lo son. Por tanto φ se extiende de manera única a un homomorfismo de anillos, que también llamaremos φ :

$$\varphi : \Omega(G) \longrightarrow \prod_{(H)\in\mathcal{C}(G)} \mathbb{Z}.$$

4.17 LEMA

Sea G un grupo finito, entonces φ es inyectiva.

Notemos que en particular el conúcleo de φ, que es un grupo abeliano, es finito, φ es un homomorfismo inyectivo entre dos grupos abelianos libres finitamente gene: mismo rango.

Demostración: Sea $x \in \Omega(G)$, y $x \neq 0$. Podemos escribir el elemento x en de sus órbitas como :

$$x = \sum_{(K)\in C(G)} a_{(K)} \frac{G}{K}.$$

Escojamos una clase de conjugación $(H) \in C(G)$ maximal, con respecto al ord ducido en 2.10, tal que $a_{(H)} \neq 0$. Entonces, por (3.6) (2),

$$\varphi_H(x) = \varphi_H\Big(\biguplus_{(K)\in C(G)} a_{(K)}(G/K)\Big) = \sum_{(K)\in C(G)} a_{(K)}\varphi_H(G/K)$$

$$= a_{(H)}\big|(G/H)^H\big| = a_{(H)}\big|W(H)\big| \neq 0. \quad \blacksquare$$

4.18 COROLARIO

Sean X, Y G-conjuntos, entonces:

$$X \cong_G Y \iff \varphi_H(X) = \varphi_H(Y) \ \ \forall\, (H) \in C(G)\,. \quad \blacksquare$$

§5 LA MATRIZ DE φ

En la sección anterior definimos el homomorfismo de anillos $\varphi\colon \Omega(G) \longrightarrow \prod_{(H)\in C(G)} \mathbb{Z}$. Denotaremos al anillo $\prod_{(H)\in C(G)} \mathbb{Z}$ como $\widetilde{\Omega}(G)$.

En esta sección encontraremos la matriz del homomorfismo de anillos φ. Como φ es inyectiva, identificaremos la imagen de φ con $\Omega(G)$, de esta manera encontraremos las condiciones para que un elemento de $\widetilde{\Omega}(G)$ esté en $\Omega(G)$.

5.1 DEFINICION

Sea G un grupo y sean H, K subgrupos de G, definimos los siguientes números:

$$\alpha(H,K) = \left|\{E \leq G\colon (E) = (K), H \subseteq E\}\right| ,$$

$$\beta(H,K) = \left|\{E \leq G\colon (E) = (H), E \subseteq K\}\right| .$$

La definición anterior se puede expresar en palabras facilmente: $\alpha(H,K)$ es el número de conjugados de K que contienen a H, $\beta(H,K)$ es el número de conjugados de H que están contenidos en K.

5.2 PROPOSICION

Sean H, K subgrupos de G, entonces

$$\varphi_H(G/K) = |W(K)|\alpha(H,K).$$

Demostración:

$$\varphi_H(G/K) = \left|\{aK\colon h(aK) = aK,\ \forall h \in H\}\right| = \left|\{aK\colon a^{-1}Ha \subseteq K\}\right|$$

$$= \left|\{a : H \subseteq aKa^{-1}\}\right| \Big/ |K|$$

$$= \left(|N_G(K)| \Big/ |K|\right) \ \left|\{E \leq G : (E) = (K), H \subseteq E\}\right|$$

$$= |W(K)| \alpha(H,K). \ \blacksquare$$

5.3 COROLARIO

Si H, K son subgrupos de G, tenemos:

$$|N_G(K)| \ \alpha(H,K) = |N_G(H)| \ \beta(H,K).$$

Demostración: En la demostración anterior llegamos a que:

$$\varphi_H(G/K) = \left|\{a : a^{-1}Ha \subseteq K\}\right| / |K|$$

$$= (|N_G(H)| / |K|) \left|\{E \leq G : (E) = (H), E \subseteq K\}\right|$$

$$= (|N_G(H)| / |K|) \, \beta(H,K).$$

Por tanto $|N_G(K)| \ \alpha(H,K) = |N_G(H)| \ \beta(H,K)$. $\blacksquare$

En la sección anterior definimos un orden parcial en $C(G)$: K es subconjugado de H si y sólo si $(K) \leq (H)$. Este orden parcial lo refinamos a un orden total en $C(G)$:

$$(e) = (H_1) \leq (H_2) \leq \cdots \leq (H_m) = (G).$$

Usaremos el mismo símbolo "$\leq$" para el orden total. Sin embargo, debe notarse que $(H) \not\leq (K)$ en el orden refinado implica que $(H) \not\leq (K)$ en el orden introducido antes en 2.10.

Entonces podemos ordenar la base canónica, como $\mathbb{Z}$-módulo de $\Omega(G)$:

$$\mathbb{B} := \{G/H_1, \ldots, G/H_m\}.$$

Consideremos también para $\widetilde{\Omega}(G) = \prod_{(H_i) \in C(G)} \mathbb{Z}$, su $\mathbb{Z}$-base ordenada natural:

$$\mathbb{B}' = \{\bar{e}_1, \ldots, \bar{e}_m\},$$

donde $\bar{e}_i = (0,\ldots,0,1,0,\ldots,0)$, el uno aparece en la i-ésima coordenada.

Como φ es morfismo de anillos, entonces φ es morfismo de $\mathbb{Z}$-módulos, entonces podemos considerar la matriz de φ con respecto a estas bases:

$$[\varphi]_{\mathbb{B}}^{\mathbb{B}'} = \begin{pmatrix} \varphi_{H_1}(G/H_1) & \varphi_{H_1}(G/H_2) & \ldots & \varphi_{H_1}(G/H_m) \\ 0 & \varphi_{H_2}(G/H_2) & \ldots & \varphi_{H_2}(G/H_m) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \varphi_{H_m}(G/H_m) \end{pmatrix}$$

Como sabemos, $\varphi_{H_i}(G/H_j) = 0$ si $i > j$ (usé (3.6)(2)).

De la proposición 5.2, sabemos que:

$$\varphi_{H_i}(H_j) = |W(H_j)|\alpha(H_i,H_j);$$

usando ésto y el hecho de que $\alpha(K,K) = 1$, podemos expresar a la matriz de φ como producto de dos matrices:

$$\begin{pmatrix} 1 & \alpha(H_1,H_2) & \ldots & \alpha(H_1,H_m) \\ 0 & 1 & \ldots & \alpha(H_2,H_m) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} |W(H_1)| & 0 & \ldots & 0 \\ 0 & |W(H_2)| & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & |W(H_m)| \end{pmatrix}$$

La matriz de la izquierda, considerada como una transformación de $\widetilde{\Omega}(G)$ en sí mismo, corresponde a un isomorfismo de $\mathbb{Z}$-módulos, y por tanto tiene una transformación inversa, llamémosla ψ. Obtenemos así la siguiente composición:

$$\Omega(G) \xrightarrow{\varphi} \prod_{(H_i)\in\mathcal{C}(G)} \mathbb{Z} \xrightarrow{\psi} \prod_{(H_i)\in\mathcal{C}(G)} \mathbb{Z}\,.$$

Si identificamos a $\varphi(\Omega(G))$ con $\Omega(G)$, tenemos un isomorfismo de $\mathbb{Z}$-módulos $\bar{\psi}$ de la siguiente manera:

$$\frac{\prod_{(H_i)\in\mathcal{C}(G)}\mathbb{Z}}{\Omega(G)} \xrightarrow{\bar{\psi}} \frac{\prod_{(H_i)\in\mathcal{C}(G)}\mathbb{Z}}{\psi(\Omega(G))}.$$

Así, el codominio de $\bar{\psi}$ es isomorfo al anillo

$$\prod_{(H_i)\in\mathcal{C}(G)} \frac{\mathbb{Z}}{|W(H_i)|\mathbb{Z}},$$

ya que la matriz $(a_{i,j})$ de $(\psi \circ \varphi)$ es diagonal, con entradas $a_{i,i} = |W(H_i)|$.

Por esto, el orden del conúcleo de φ es igual a $\prod_{(H_i)\in C(G)} |W(H_i)|$.

La observación anterior y la definición del morfismo de Frobenius que damos a continuación, permitirán demostrar que una condición es necesaria y suficiente, para que un elemento de $\widetilde{\Omega}(G)$ pertenezca a $\Omega(G)$.

Consideremos un G-conjunto X y sea K un subgrupo de G, si restringimos la acción de G al subgrupo K, hacemos de X un K-conjunto. A este K-conjunto lo denotaremos por X_K. Supongamos ahora que H es un subgrupo normal de K, la notación es $H \trianglelefteq K$, entonces X_K^H (el conjunto de puntos fijos bajo la acción de H en X_K) es un K/H-conjunto, con acción:

$$(kH)\, x := k\, x, \quad \forall kH \in K/H \quad , x \in X_K^H.$$

Es claro que esta acción está bien definida y es una acción de K/H-conjuntos. Si X, Y son G-conjuntos entonces:

$$((X+Y)_K)^H = ((X \uplus Y)_K)^H = (X_K \uplus Y_K)^H = X_K^H \uplus Y_K^H,$$

$$((X \times Y)_K)^H = (X_K \times Y_K)^H = X_K^H \times Y_K^H.$$

Tenemos una asociación de G-conjuntos a K/H-conjuntos que respeta las operaciones del anillo, éste será el *morfismo de Frobenius.*

5.4 DEFINICION

Sean H, K subgrupos del grupo G, y supongamos que $H \trianglelefteq K$. Definimos el *morfismo de Frobenius* como el morfismo de anillos definido en G- conjuntos como:

$$Fr_{H,K}^G : \Omega(G) \longrightarrow \Omega(K/H), \quad X \longmapsto X_K^H, \quad \forall X \text{ } G\text{-conjunto}.$$

Para un subconjunto A de elementos del grupo G denotaremos por $< A >$ al subgrupo generado por los elementos de A.

5.5 TEOREMA

Sea $a \in \widetilde{\Omega}(G)$. Entonces $a \in \Omega(G)$ si y sólo si

$$\sum_{gH \in \frac{N_G(H)}{H}} \varphi_{<g,H>}(a) \equiv 0 \quad \left(mod \ \frac{|N_G(H)|}{|H|} \right), \quad \forall\, H \leq G\,.$$

Demostración: $(\Longrightarrow)$: Nótese que basta probar la afirmación para G-conjuntos $a = X$. Consideremos el caso $H = e$, sabemos que, (3.7),

$$(1) \qquad \sum_{g \in G} |X^g| \equiv 0 \quad (mod |G|)\,;$$

donde es fácil ver que $|X^g| = \varphi_{<g>}(X)$, y entonces la fórmula del enunciado vale. Ahora veamos el caso general. Sea H un subgrupo de G, puesto que H es normal en $N_G(H)$, podemos considerar el morfismo de Frobenius

$$\eta := Fr^G_{H, N_G(H)} \colon \Omega(G) \longrightarrow \Omega\left(\frac{N_G(H)}{H}\right).$$

Tenemos que $\eta(a) = a^H$. Utilizando (1) para el subgrupo trivial de $\frac{N_G(H)}{H}$, tenemos:

$$\sum_{gH \in \frac{N_G(H)}{H}} \varphi_{\frac{<g,H>}{H}}(a^H) \equiv 0 \quad \left(mod \frac{|N_G(H)|}{|H|} \right).$$

El resultado se sigue inmediatamente de que:

$$\varphi_{\frac{<g,H>}{H}}(a^H) = \varphi_{<g,H>}(a).$$

$(\Longleftarrow)$: Consideremos el conjunto S de todos los elementos de $\widetilde{\Omega}(G)$ que cumplen las congruencias del teorema, es decir:

$$S := \left\{ a \in \widetilde{\Omega}(G) : \sum_{gH \in \frac{N_G(H)}{H}} \varphi_{<g,H>}(a) \equiv 0 \quad \left(mod \ \frac{|N_G(H)|}{|H|} \right), \ \forall H \leq G \right\}.$$

Acabamos de demostrar que $\Omega(G) \subseteq S \subseteq \widetilde{\Omega}(G)$. Como grupos abelianos, el índice de $\Omega(G)$ en $\widetilde{\Omega}(G)$ es $\prod_{H_i \in \mathcal{C}(G)} \left| \frac{N_G(H_i)}{H_i} \right|$. Es claro que S es un subgrupo de $\widetilde{\Omega}(G)$. Así, es suficiente mostrar que:

$$\left[\widetilde{\Omega}(G) : S \right] = \prod_i \left| \frac{N_G(H_i)}{H_i} \right|.$$

Sean $e = (H_1) \leq (H_2) \ldots \leq (H_n) = G$ el conjunto totalmente ordenado de clases de conjugación de subgrupos de G. Consideremos la siguiente sucesión de $\mathbb{Z}$-módulos :

$$(2) \qquad 0 \longrightarrow S \xrightarrow{\psi} \left(\bigoplus_{H_i \in \mathcal{C}(G)} \mathbb{Z} \right) = \widetilde{\Omega}(G) \xrightarrow{\pi} \bigoplus_{H_i \in \mathcal{C}(G)} \frac{\mathbb{Z}}{m_i \mathbb{Z}} \longrightarrow 0 \,,$$

donde $m_i = \left|\frac{N_G(H_i)}{H_i}\right|$, π es la proyección canónica, y ψ está definida como sigue:

$$\psi(a) = \left(\sum_{gH_i \in \frac{N_G(H_i)}{H_i}} \varphi_{<g,H_i>}(a) \right)_i \quad , \ \forall a \in \widetilde{\Omega}(G).$$

Si probamos que la sucesión (2) es exacta, entonces

$$\left|\frac{\widetilde{\Omega}(G)}{S}\right| = \prod_i \left|\frac{N_G(H_i)}{H_i}\right|,$$

y como consecuencia tenemos que $\Omega(G) = S$, con lo que queda mostrada la afirmación.

El kernel de π es $\bigoplus_{H_i \in \mathcal{C}(G)} m_i \mathbb{Z} \leq \bigoplus_{H_i \in \mathcal{C}(G)} \mathbb{Z}$. Como los elementos de S cumplen las congruencias, tenemos que $\psi(S) \leq \bigoplus_i m_i \mathbb{Z} = \ker \pi$.

Para probar la otra contención, $\bigoplus_i m_i \mathbb{Z} \subseteq \psi(S)$, requerimos de algunos cálculos previos: sea $j \in \{1, \ldots, n\}$, entonces $\psi(G/H_j) = \mu_{H_j}$, donde

$$(\mu_{H_j})_i = \sum_{gH_i \in \frac{N_G(H_i)}{H_i}} \varphi_{<g,H_i>}(G/H_j).$$

Como $H_i \leq \, < g, H_i >$, cuando $i > j$ tenemos que $(H_i) \not\leq (H_j)$ y por tanto $(< g, H_i >) \not\leq (H_j)$, $\forall g \in G$. Por esto $(\mu_{H_j})_i = 0$, $\forall i > j$.

Si $i = j$, tenemos $(< g, H_l >) \leq (H_j)$ si y sólo si $g \in H_j$, por tanto

$$(\mu_{H_j})_j = \varphi_{H_j}(G/H_j) = |W(H_j)| = m_j.$$

Así pues:

$$\psi(G/H_1) = \mu_{H_1} = (m_1, 0, \ldots, 0, 0),$$

$$\psi(G/H_2) = \mu_{H_2} = ((\mu_{H_2})_1, m_2, 0, \ldots, 0, 0),$$

$$\vdots$$

$$\psi(G/H_n) = \mu_{H_n} = ((\mu_{H_n})_1, (\mu_{H_n})_2, \ldots, (\mu_{H_n})_{n-1}, m_n).$$

Para probar que $\psi(S) = \bigoplus_{H_i \in C(G)} m_i\mathbb{Z}$, basta ver que $\mu_{H_1}, \mu_{H_2}, \ldots, \mu_{H_n}$ generan a $\bigoplus_i m_i\mathbb{Z}$. Pero esta afirmación se sigue inmediatamente del hecho de que $\mu_{H_j} \in \bigoplus_i m_i\mathbb{Z}$, pues esta última implica que $m_i \mid (\mu_{H_j})_i$, $\forall j$. La inyectividad de ψ se sigue de que tanto su dominio como su imagen tienen el mismo rango n. ∎

3

El Espectro primo del anillo de Burnside

Nosotros, los hombres, tenemos un campo de acción mucho más vasto e intereses más amplios que los animales. Pero también nos hallamos inscritos en un círculo relativamente pequeño, y no podemos traspasarlo. Yo puedo fantasear muchas cosas, imaginarme, por ejemplo, que mi mayor deseo sería llegar al Polo Norte, o algo semejante; pero sólo podré quererlo así con suficiente intensidad y realizarlo cuando el deseo viva realmente en mí y todo mi ser se halle penetrado de él. Cuando así sucede, en cuanto intentas algo que te es ordenado desde el propio interior, acabas por conseguirlo, y puedes uncir tu voluntad como un buen animal de tiro.

Hermann Hesse (1877-1962)

§6 EL ANILLO $\Omega_\pi(G)$

En este capítulo seguiremos estudiando el anillo de Burnside para un grupo finito G. Como vimos en el capítulo anterior, las clases de isomorfismo de G-conjuntos finitos se transforman en un semianillo $\Omega^+(G)$ conmutativo con unidad, por medio de la unión ajena y del producto cartesiano.

El anillo de Grothendieck $\Omega(G)$ de $\Omega^+(G)$ es el anillo de Burnside de G.

El anillo $\Omega(G)$ es, como grupo abeliano, libre con base $\{G/H : (H) \in C(G)\}$, donde $C(G)$ es el conjunto de clases de conjugación de subgrupos de G.

Tomemos un conjunto de números primos cualquiera π, y consideremos el siguiente subconjunto del *campo* de los números racionales $\mathbb{Q}$:

$$\mathbb{Z}_\pi := \left\{ \frac{a}{b} : p \nmid b, \ \forall p \in \pi \right\}.$$

Es fácil ver que $\mathbb{Z}_\pi$ es un anillo conmutativo con unidad, que contiene a $\mathbb{Z}$.

Cualquier anillo que esté contenido en $\mathbb{Q}$ y contenga a $\mathbb{Z}$ es de la forma $\mathbb{Z}_\pi$, para un cierto conjunto de primos π.

6.1 DEFINICION

Para cualquier anillo conmutativo A, definimos el *espectro primo* de A como el conjunto de todos los ideales primos de A, y denotamos por $Spec(A)$ a este conjunto.

El espectro de un anillo A tiene estructura de espacio topológico, donde los conjuntos cerrados son: $V(I) := \{\wp \in Spec(A) \colon \wp \supseteq I\}$, con I ideal de A. En efecto, es fácil ver que: si I, J son ideales, $V(IJ) = V(I) \bigcup V(J)$; si $\{I_i\}$ es una familia de ideales, $V(\sum_i I_i) = \bigcap V(I_i)$.

6.2 LEMA

Sea π un conjunto de números primos, entonces:

(i) $Spec(\mathbb{Z}_\pi) = \{p\mathbb{Z}_\pi \colon p \in \pi\} \bigcup \{0\}$, donde: $p\mathbb{Z}_\pi := \{\frac{a}{b} \in \mathbb{Z}_\pi \colon p \mid a\}$.

(ii) Sea $p \in \pi$, entonces:

$$\frac{\mathbb{Z}_\pi}{p\mathbb{Z}_\pi} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}\,.$$

Demostración: (i) : Es claro que, para cada $p \in \pi$, $p\mathbb{Z}_\pi$ es un ideal de $\mathbb{Z}_\pi$. Además, si $(a/b)(c/d)$ es un elemento de $p\mathbb{Z}_\pi$, entonces $p \mid ac$, así $p \mid a$ ó $p \mid c$. Por tanto $p\mathbb{Z}_\pi$ es un ideal primo para todo $p \in \pi$.

Por otra parte, si $I \subsetneq \mathbb{Z}_\pi$ es un ideal primo de $\mathbb{Z}_\pi$, entonces $I \bigcap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$. Por ello $I \bigcap \mathbb{Z} = q\mathbb{Z}$, para algún primo $q \in \pi$ (si $q \notin \pi$ entonces $1 \in I$). Además, si $q \nmid a$ para algún $a/b \in I$, entonces $b(a/b) \in I \bigcap \mathbb{Z}$, lo cual es una contradicción. Por tanto $I = q\mathbb{Z}_\pi$, $q \in \pi$.

(ii) : Consideremos la siguiente sucesión:

$$0 \longrightarrow p\mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{\rho} \frac{\mathbb{Z}_\pi}{p\mathbb{Z}_\pi} \longrightarrow 0\,.$$

Donde i es inclusión, y ρ es incluir en $\mathbb{Z}_\pi$ y luego proyectar al cociente. Es suficiente mostrar que la sucesión es exacta. Es claro que $\rho(m) = 0$ si y sólo si $m \in p\mathbb{Z}$. Así, sólo resta mostrar la suprayectividad de ρ. Sea $[a/b]$ un elemento de $\mathbb{Z}_\pi/p\mathbb{Z}_\pi$. Como p y b son primos relativos, existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha p + \beta b = 1$. Entonces $a/b = a\alpha p/b + a\beta$, por tanto $\rho(a\beta) = [a/b]$. ∎

El anillo de Burnside $\Omega(G)$, es un $\mathbb{Z}$-módulo libre con base los elementos de $C(G)$. En esta sección generalizamos el concepto de anillo de Burnside, para considerarlo un $\mathbb{Z}_\pi$-módulo.

Sea π un conjunto de primos, definimos:

$$\Omega_\pi(G) := \mathbb{Z}_\pi \otimes_{\mathbb{Z}} \Omega(G)\ ,\ \text{y}$$

$$\widetilde{\Omega}_\pi(G) := \mathbb{Z}_\pi \otimes_{\mathbb{Z}} \widetilde{\Omega}\,(G)\,.$$

Notemos que

$$\widetilde{\Omega}_\pi(G) = \mathbb{Z}_\pi \otimes_{\mathbb{Z}} \widetilde{\Omega}\,(G) = \mathbb{Z}_\pi \otimes_{\mathbb{Z}} \left(\prod_{(H_i)\in\mathcal{C}(G)} \mathbb{Z} \right) = \prod_{(H_i)\in\mathcal{C}(G)} (\mathbb{Z}_\pi \otimes \mathbb{Z}) \cong \prod_{(H_i)\in\mathcal{C}(G)} \mathbb{Z}_\pi\,.$$

Es conveniente observar también que la función:

$$\psi : \mathbb{Z}_\pi \otimes_{\mathbb{Z}} \Omega(G) \longrightarrow \bigoplus_{(H_i)\in\mathcal{C}(G)} \mathbb{Z}_\pi G/H_i\,,$$

cuyo codominio es el $\mathbb{Z}_\pi$-módulo libre con base $\{G/H_i\}_{(H_i)\in\mathcal{C}(G)}$, y que está definida en los elementos básicos como $1 \otimes G/H_i \longmapsto G/H_i$, es un isomorfismo de $\mathbb{Z}_\pi$-módulos.

Si traducimos las operaciones del anillo $\Omega_\pi(G)$ a la suma directa por medio de ψ, resulta que los básicos G/H_i se multiplican en $\bigoplus_{(H_i)\in\mathcal{C}(G)} \mathbb{Z}_\pi G/H_i$ igual que en $\Omega(G)$. Abusando un poco del lenguaje, aprovechamos la posibilidad de ver los elementos de $\Omega_\pi(G)$ como combinaciones $\mathbb{Z}_\pi$-lineales formales de básicos G/H_i (ó de G-conjuntos) y de identificar a $\Omega(G) = \bigoplus_{(H_i)\in\mathcal{C}(G)} \mathbb{Z}G/H_i$ con el subanillo correspondiente de $\Omega_\pi(G)$.

Entonces:

$$\Omega(G) \leq \Omega_\pi(G) = \bigoplus_{(H_i)\in\mathcal{C}(G)} \mathbb{Z}_\pi G/H_i = \sum_{X\ G\text{–conjunto}} \mathbb{Z}_\pi X.$$

Cuando $\pi = \emptyset$, nuestra convención es $\mathbb{Z}_\pi = \mathbb{Q}$, y usamos la notación $\Omega_{\mathbb{Q}}$, $\widetilde{\Omega}_{\mathbb{Q}}$ respectivamente. Si π es el conjunto de todos los primos, entonces $\mathbb{Z}_\pi = \mathbb{Z}$, y $\Omega_\pi(G) = \Omega(G)$, $\widetilde{\Omega}_\pi(G) = \widetilde{\Omega}(G)$.

Recordemos que para cualquier subgrupo H de G y para cualquier G-conjunto X, X^H es el conjunto de puntos fijos de H. Tenemos un homomorfismo de anillos:

$$\varphi_H : \Omega_\pi(G) \longrightarrow \mathbb{Z}_\pi\,,$$

definido para cualquier G-conjunto X como $|X^H|$.

Como en 4.17, definimos el homomorfismo

$$\varphi\ :\ \Omega_\pi(G) \longrightarrow \widetilde{\Omega}_\pi(G)\ :\ X \longmapsto (\varphi_{H_i}(X))_{(H_i)\in\mathcal{C}(G)}.$$

6.3 TEOREMA

El homomorfismo de anillos φ es inyectivo.

Demostración: Se sigue inmediatamente de la inyectividad de

$$\varphi \; : \; \Omega(G) \longrightarrow \widetilde{\Omega}(G) \quad \blacksquare.$$

§7 EL ESPECTRO PRIMO DE $\Omega_\pi(G)$

En la sección anterior definimos el espectro primo de un anillo conmutativo. Ahora, encontraremos explícitamente el espectro primo del anillo de Burnside de cualquier grupo finito G, en términos del mismo grupo G.

7.1 PROPOSICION

Sea $f : \Omega_\pi(G) \longrightarrow R$ un homomorfismo de anillos, con R dominio entero. Entonces:

(i) Existe una única clase de conjugación (H) minimal, tal que $f(G/H) \neq 0$.

(ii) $f(X) = \varphi_H(X)\ Id_R$, $\forall X \in \Omega_\pi(G)$.

Demostración: (i) : Como $f(G/G) = f(1) = 1$, y el grupo G es finito, tenemos que existe una clase de conjugación (H) minimal con $f(G/H) \neq 0$. Supongamos ahora que (H) y (K) son clases minimales con la propiedad $f(G/H) \neq 0 \neq f(G/K)$. Como R es dominio entero, tenemos que $f(G/H) \cdot f(G/K) \neq 0$. Así, $f(G/H \cdot G/K) \neq 0$. Sea T un conjunto de representantes de las clases laterales dobles en G, de la forma HaK; del corolario 4.11, tenemos:

$$G/H \times G/K = \sum_{g\in T} \frac{G}{H \bigcap gKg^{-1}} = \sum_{\substack{(U)\leq(H)\\(U)\leq(K)}} a_U G/U ,$$

para algunos enteros a_U apropiados. Entonces existe U tal que $f(a_U G/U) \neq 0$. Por tanto $(U) = (H)$, ya que (H) es minimal. Análogamente $(U) = (K)$. Así, $(H) = (K)$.

(ii) : Como f y φ_H son homomorfismos de anillos, basta probar la afirmación para G-conjuntos X. Notemos que:

$$G/H \times X = \sum_{(K)\leq(H)} a_K G/K ,$$

para algunos enteros a_K apropiados. Así, $G/H \times X = a_H G/H + \sum_{(K)<(H)} a_K G/K$. Pero

$$\varphi_H(G/H)\varphi_H(X) = \varphi_H(G/H \times X) = a_H \varphi_H(G/H).$$

Por tanto, $\varphi_H(X) = a_H$. Entonces:

$$f(G/H) \cdot f(X) = f(G/H \times X) = f\left(\varphi_H(X)G/H + \sum_{(K)<(H)} a_K G/K\right) = \varphi_H(X) \cdot f(G/H).$$

Por lo tanto $f(X) = \varphi_H(X)\ Id_R$. ∎

El siguiente corolario es inmediato del resultado anterior.

7.2 COROLARIO

Sea R un dominio entero y sean $f, f' \colon \Omega_\pi(G) \longrightarrow R$, homomorfismos de anillos, con el mismo núcleo. Entonces $f = f'$. ∎

7.3 DEFINICION

Para cada subgrupo U de G, y para cada ideal primo $p^* := p\mathbb{Z}_\pi$, $p \in \pi$, de $\mathbb{Z}_\pi$, definimos:

$$\beta_\pi(U, p^*) := \{x \in \Omega_\pi(G) : \varphi_U(x) \in p^*\}.$$

Como φ_U es homomorfismo de anillos, $\beta_\pi(U, p^*) = \varphi_U^{-1}(p^*)$ es un ideal primo de $\Omega_\pi(G)$. Veremos que estos son todos los ideales primos de $\Omega_\pi(G)$.

7.4 PROPOSICION

Todo ideal primo de $\Omega_\pi(G)$ tiene la forma $\beta_\pi(U, p^*)$ para algún subgrupo U de G, y algún ideal primo p^* de $\mathbb{Z}_\pi$.

Demostración: Sea $\wp \subseteq \Omega_\pi(G)$ ideal primo. Entonces el anillo cociente $R := \Omega_\pi(G)/\wp$ es dominio entero, y la proyección canónica ρ es un morfismo de $\Omega_\pi(G)$ a un dominio entero; por la proposición 7.1, $\rho(x) = \varphi_U(x)\ Id_R$, $\forall x \in \Omega_\pi(G)$, para algún subgrupo $U \leq G$.

Sea p la característica de $\Omega_\pi(G)/\wp$. Entonces

$$x \in \wp \Longleftrightarrow x \in \mathrm{Ker}\rho \Longleftrightarrow \rho(x) = 0 \Longleftrightarrow \varphi_U(x)\ Id_R = 0 \Longleftrightarrow p \mid \varphi_U(x) \Longleftrightarrow \varphi_U(x) = \frac{pa}{b},$$

para algunos $a, b \in \mathbb{Z}$, y ningún primo de π divide a b. Esto último si y sólo si $\varphi_U(x) \in p\mathbb{Z}_\pi = p^*$. Entonces

$$x \in \wp \Longleftrightarrow x \in \beta_\pi(U, p^*).$$

Es claro que p es un elemento de π. ∎

El que todos los ideales primos de $\Omega_\pi(G)$ sean de la forma $\beta_\pi(U, p^*)$, nos permitirá obtener información acerca del espectro del anillo $\Omega_\pi(G)$.

7.5 LEMA

Sean $U, V \leq G$. Entonces:

(i) Si $\beta_\pi(U, p^*) \supset \beta_\pi(V, q^*)$ entonces $p^* = q^*$.

(ii) Si $\wp$ es un ideal primo de $\Omega_\pi(G)$, y $\beta_\pi(U, 0^*) \subseteq \wp$, entonces existe $p \in \pi$ tal que $\wp = \beta_\pi(U, p^*)$.

(iii) $\beta_\pi(U, p^*)$ es maximal en $Spec(\Omega_\pi(G)) \Longleftrightarrow p^* \neq 0^*$, con $\pi \neq \emptyset$.

(iv) $\beta_\pi(U, 0^*)$ es minimal en $Spec(\Omega_\pi(G))$.

Demostración: (i) : Como $p^* = p\mathbb{Z}_\pi$, $q^* = q\mathbb{Z}_\pi$, con $p, q \in \pi$. Entonces tenemos un morfismo γ sobre, de dominios enteros:

$$\frac{\Omega_\pi(G)}{\beta_\pi(V, q^*)} \xrightarrow{\gamma} \frac{\Omega_\pi(G)}{\beta_\pi(U, p^*)}.$$

Luego,

$$p = \mathrm{Char}\ \frac{\Omega_\pi(G)}{\beta_\pi(U, p^*)} \ \text{ divide a } \ \mathrm{Char}\ \frac{\Omega_\pi(G)}{\beta_\pi(V, q^*)} = q\ .$$

Por lo tanto $p = q$ y $p^* = q^*$.

(ii) : $\varphi_U(\wp)$ es un ideal primo de $\mathbb{Z}_\pi$, por tanto $\varphi_U(\wp) = p\mathbb{Z}_\pi$, $p \in \pi$. Así $\wp = \varphi_U^{-1}(p\mathbb{Z}_\pi) = \beta_\pi(U, p^*)$.

(iii) : Si $\pi \neq \emptyset$, tomamos $p^* \neq 0^*$, entonces

$$\frac{\mathbb{Z}_\pi}{p^*} = \frac{\mathbb{Z}_\pi}{p\mathbb{Z}_\pi} \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p,$$

ya que $\mathbb{Z}_p$ es un campo, tenemos que p^* es maximal en $Spec(\mathbb{Z}_\pi)$, y por tanto

$$\beta_\pi(U, p^*) = \varphi_U^{-1}(p^*)$$

es maximal en $Spec(\Omega_\pi(G))$. Además, es claro que si $p \in \pi$, entonces $\beta_\pi(U, 0^*) \subsetneq \beta_\pi(U, p^*)$.

(iv) : Supongamos que $\beta_\pi(V, q^*) \subseteq \beta_\pi(U, 0^*)$. Por (i) $q^* = 0^*$; por ello, tenemos que $\beta_\pi(V, 0^*) \subseteq \beta_\pi(U, 0^*)$. Pero por (ii), $\beta_\pi(U, 0^*) = \beta_\pi(V, k^*)$, para algún primo $k \in \pi$. Usando (i), tenemos que $\beta_\pi(V, 0^*) = \beta_\pi(U, 0^*)$. ∎

7.6 LEMA

Vale la equivalencia:

$$\beta_\pi(U, 0^*) = \beta_\pi(V, 0^*) \Longleftrightarrow V \sim U \Longleftrightarrow \varphi_U = \varphi_V \, .$$

Demostración: Si $V \sim U$, como en 3.3 tenemos que $\varphi_U = \varphi_V$, y por lo tanto

$$\beta_\pi(U, 0^*) = \mathrm{Ker}\varphi_U = \mathrm{Ker}\varphi_V = \beta_\pi(V, 0^*) \, .$$

Ahora bien, si $\beta_\pi(V, 0^*) = \beta_\pi(U, 0^*)$, por 7.2, $\varphi_U = \varphi_V$. En consecuencia $\varphi_V(G/U) = \varphi_U(G/V) \neq 0$. Por tanto $(U) \subseteq (V)$, y análogamente $(V) \subseteq (U)$, así $V \sim U$. ∎

Sea G un grupo y sea $O^p(G)$ el mínimo subgrupo normal de G tal que $G/O^p(G)$ es p-grupo. Este subgrupo es único: si los subgrupos $N_1 \trianglelefteq G$ y $N_2 \trianglelefteq G$ son normales, y cumplen que G/N_1, G/N_2 son p-grupos, entonces $N_1 \bigcap N_2$ es normal y la sucesión:

$$0 \longrightarrow N_1 \bigcap N_2 \xrightarrow{i} G \xrightarrow{\rho} \frac{G}{N_1} \times \frac{G}{N_2}$$

es exacta en G, por tanto $G/(N_1 \bigcap N_2)$ es p-grupo, ya que es isomorfo a un subgrupo del p-grupo $G/N_1 \times G/N_2$.

El subgrupo $O^p(G)$ de un grupo dado G, jugará un papel muy importante en la descripción del espectro del anillo de Burnside de G.

7.7 OBSERVACION

$O^p(G)$ es un subgrupo característico de G.

Demostración: Sea $f: G \longrightarrow G$ un automorfismo, entonces f induce un isomorfismo

$$\frac{G}{O^p(G)} \cong \frac{G}{f\,(O^p(G))}.$$

Como ambos grupos son p-grupos, tenemos, por la minimalidad de $O^p(G)$, que $O^p(G) \subseteq f\,(O^p(G))$, pero estos subgrupos tienen el mismo orden. Así $O^p(G) = f\,(O^p(G))$. ∎

Notemos que si dos subgrupos U y V de G son conjugados, es decir, existe $g \in G$ tal que $U = gVg^{-1}$, entonces el automorfismo $T_g: G \longrightarrow G : x \longmapsto gxg^{-1}$ induce un isomorfismo entre

$$\frac{U}{O^p(U)} \cong \frac{V}{T_g(O^p(U))} \quad .$$

De la misma forma construimos el automorfismo inverso $T^{-1} = T_{g^{-1}}$. Obtenemos así que:

$$O^p(V) \subseteq T_g(O^p(U)) \subseteq T_g^{-1}T_g(O^p(V)) = O^p(V).$$

Por ello, $O^p(U) \sim O^p(V)$. De hecho los grupos $O^p(U)$ y $O^p(V)$ son conjugados por la misma g que hacía que $U = gVg^{-1}$.

7.8 LEMA

Sean W, U subgrupos del grupo G. Si $W \trianglelefteq U$ y U/W es un p-grupo, entonces $O^p(U) = O^p(W)$. En particular $O^p(O^p(U)) = O^p(U)$.

Demostración: Tenemos que $O^p(U) \trianglelefteq W$, y que $W/O^p(U)$ es un p-grupo. Así, $O^p(U) \supseteq O^p(W)$.

Por otra parte $O^p(W) \trianglelefteq W \trianglelefteq U$, pero $O^p(W)$ es característico, así que $O^p(W) \trianglelefteq U$. Tenemos que:

$$\frac{W}{O^p(W)} \text{ es } p\text{-grupo y } \frac{U/O^p(W)}{W/O^p(W)} \text{ es } p\text{-grupo} \quad ,$$

entonces $U/O^p(W)$ es p-grupo. Por ello $O^p(U) \subseteq O^p(W)$. Así, $O^p(U) = O^p(W)$. ∎

Observemos que si X es un U-conjunto, entonces $X^U \subseteq X^{O^p(U)}$ y $U/O^p(U)$ actúa en $X^{O^p(U)}$. Por lo tanto, el $U/O^p(U)$-conjunto $X^{O^p(U)} - X^U$ tiene sólo órbitas no triviales. Pero $U/O^p(U)$ es p-grupo, así las órbitas tienen cardinalidad múltiplos de p. Por ello, para todo G-conjunto Y, tenemos que

$$\varphi_U(Y) \equiv \varphi_{O^p(U)}(Y) \quad (mod\, p).$$

Así llegamos a que

$$x \in \beta_\pi(U,p^*) \Longleftrightarrow \varphi_U(x) \in p^* \Longleftrightarrow p \mid \varphi_{O^p(U)}(x) \Longleftrightarrow x \in \beta_\pi(O^p(U),p^*).$$

Por lo tanto $\beta_\pi(U,p^*) = \beta_\pi(O^p(U),p^*)$.

7.9 LEMA

Sea p^* un ideal primo de $\mathbb{Z}_\pi$, entonces $\beta_\pi(U,p^*) = \beta_\pi(V,p^*)$ si y sólo si $O^p(U)$ es conjugado de $O^p(V)$ en G.

Demostración: $(\Longleftarrow)$: Si $O^p(U) \sim O^p(V)$ entonces:

$$\beta_\pi(U,p^*) = \beta_\pi(O^p(U),p^*) = \beta_\pi(O^p(V),p^*) = \beta_\pi(V,p^*).$$

$(\Longrightarrow)$: Si $\beta_\pi(U,p^*) = \beta_\pi(V,p^*)$, y la función $\rho_p: \mathbb{Z}_\pi \longrightarrow \mathbb{Z}_\pi/p\mathbb{Z}_\pi$ es la proyección canónica, entonces Ker $\rho_p\varphi_U =$ Ker $\rho_p\varphi_V$. Por el corolario 7.2, $\rho_p\varphi_U = \rho_p\varphi_V$. Tomemos una clase de conjugación (H) minimal tal que $\rho_p\varphi_U(G/H) \neq 0$. Además, tomemos P un p-subgrupo de Sylow de $N_G(O^p(U))/O^p(U)$ que contenga a $U/O^p(U)$. Definimos $O_p(U) := \rho^{-1}(P)$, donde ρ es la proyección canónica de $N_G(O^p(U))$ en $N_G(O^p(U))/O^p(U)$. Obtenemos así las siguientes correspondencias:

$$\begin{array}{ccc}
N_G(O^p(U)) & \overset{\rho}{\longrightarrow} & \frac{N_G(O^p(U))}{O^p(U)} \\
\cup| & & \cup| \\
O_p(U) & \longrightarrow & P \\
\cup| & & \cup| \\
U & \longrightarrow & \frac{U}{O^p(U)} \\
\cup| & & \cup| \\
O^p(U) & \longrightarrow & 0
\end{array}$$

Por el lema anterior tenemos que $O^p(U) = O^p(O_p(U))$. Entonces: $\varphi_U \equiv \varphi_{O^p(U)} \equiv \varphi_{O_p(U)}$ $(mod\ p)$. Por tanto $\rho_p\varphi_U = \rho_p\varphi_{O^p(U)} = \rho_p\varphi_{O_p(U)}$. Entonces $\varphi_{O_p(U)}(G/H) \neq 0$, y por tanto $(O_p(U)) \leq (H)$.

Como $p\dagger[\frac{N_G(O^p(U))}{O^p(U)} : P] = [N_G(O^p(U)) : O_p(U)]$, tenemos $p\dagger\varphi_{O_p(U)}(G/O_p(U))$. Por lo tanto:

$$\rho_p\varphi_U\left(\frac{G}{O_p(U)}\right) = \rho_p\varphi_{O_p(U)}\left(\frac{G}{O_p(U)}\right) \neq 0 \, .$$

Así, $(O_p(U)) = (H)$, por la minimalidad de (H). Por lo tanto $O_p(U) \sim H$. De forma análoga llegamos a que $O_p(V) \sim H$, así $O^p(O_p(U)) \sim O^p(O_p(V))$. Pero, usando el lema anterior, tenemos:

$$O^p(U) = O^p(O_p(U)) \sim O^p(O_p(V)) = O^p(V) \, . \quad \blacksquare$$

El teorema de Dress resume lo que hemos avanzado hasta ahora en el estudio del espectro primo de $\Omega_\pi(G)$.

7.10 TEOREMA (DRESS)

Todo ideal primo de $\Omega_\pi(G)$ es de la forma $\beta_\pi(U,p^*)$, con $U \leq G$ subgrupo del grupo G, y p^* ideal primo de $\mathbb{Z}_\pi$. Estos ideales primos satisfacen:

(1) Si $p^* \neq q^*$, entonces $\beta_\pi(U,p^*) \neq \beta_\pi(V,q^*)$;

(2) $\beta_\pi(U,0^*)$ es minimal y $\beta_\pi(U,0^*) = \beta_\pi(V,0^*) \Longleftrightarrow U \sim V$;

(3) Si $p^* \neq 0^*$, $\beta_\pi(U,p^*)$ es maximal, y $\beta_\pi(U,p^*) = \beta_\pi(V,p^*) \Longleftrightarrow O^p(U) \sim O^p(V)$;

(4) $\beta_\pi(V,0^*) \subseteq \beta_\pi(V,p^*)$. $\blacksquare$

Sea A un anillo conmutativo, los conjuntos cerrados del espectro primo son los conjuntos de la forma: $V(I) := \{\wp \in Spec(A) : I \subseteq \wp\}$, I ideal de A. Notemos que, si tomamos un punto del espectro de A, es decir un ideal primo $\wp$ de A, la cerradura $\overline{\{\wp\}}$ coincide con $V(\wp)$. Seguiremos estudiando el espectro primo del anillo de Burnside.

7.11 OBSERVACION

Dos ideales primos $\wp$, $\wp'$ de $\Omega_\pi(G)$ están en la misma componente conexa del espacio $Spec(\Omega_\pi(G))$ si y sólo si hay una sucesión de ideales primos minimales $\wp_1, \ldots, \wp_n$ en $\Omega_\pi(G)$ tal que:

$$\wp \in \overline{\{\wp_1\}}, \quad \wp' \in \overline{\{\wp_n\}}, \quad \overline{\{\wp_i\}} \bigcap \overline{\{\wp_{i+1}\}} \neq \emptyset, \quad \forall i\,.$$

Demostración: $(\Longleftarrow)$: Trivial.

$(\Longrightarrow)$: Sean $\{\wp_1, \ldots, \wp_m\}$ los ideales primos minimales en la componente conexa que contienen a $\wp$ y a $\wp'$, son un número finito porque $\Omega_\pi(G)$ es un anillo *noetheriano*, ya que es finitamente generado como $\mathbb{Z}_\pi$-módulo (ver [Kunz]). Como la unión de las cerraduras de los minimales forman la componente conexa, es claro que existe un subconjunto de $\{\wp_1, \ldots, \wp_m\}$, tal que, salvo ordenamiento y renumeración, $\overline{\{\wp_i\}} \bigcap \overline{\{\wp_{i+1}\}} \neq \emptyset$, $\forall i$, con $\wp \in \overline{\{\wp_s\}}$, $\wp' \in \overline{\{\wp_t\}}$, para algunas s, t. ∎

Sea H un grupo finito y π un conjunto de primos, decimos que H es π-soluble si y sólo si, por definición, tiene una serie normal cuyos grupos factores son cíclicos de orden p, para algún $p \in \pi$.

Si el grupo H es π-soluble, entonces su orden es un π-*número*, es decir, el orden de H sólo es divisible por primos de π.

Si G es un grupo finito cualquiera, podemos pensar en un subgrupo normal mínimo $O^\pi(G)$, tal que el grupo cociente $G/O^\pi(G)$ sea π-soluble. Veremos que el subgrupo $O^\pi(G)$ existe y es único.

7.12 LEMA

Sea G un grupo finito, entonces:

(i) $O^\pi(G)$ existe y es único;

(ii) $O^\pi(G)$ es característico en G;

(iii) Si $\pi = \emptyset$, entonces $O^\pi(G) = G$;

(iv) Si π es el conjunto de todos los primos, entonces $O^\pi(G)$ es el mínimo subgrupo normal de G tal que $G/O^\pi(G)$ es soluble;

(v) Si $\pi = \{p\}$, entonces $O^\pi(G) = O^p(G)$;

(vi) Si $f\colon G \longrightarrow K$ es un isomorfismo de grupos, entonces $f(O^\pi(U)) = O^\pi(f(U))$, para todo subgrupo $U \leq G$;

(vii) Dado π, existe un subconjunto finito $\pi' \subseteq \pi$, tal que $O^\pi(G) = O^{\pi'}(G)$;

$(viii)$ Si $\pi' \subseteq \pi$, entonces $O^\pi(O^{\pi'}(G)) = O^\pi(G)$;

(ix) Si $H \trianglelefteq K \leq G$, y K/H es π-soluble, entonces $O^\pi(K) = O^\pi(H)$;

(x) Dado π, existen $p_1, p_2, \ldots, p_n \in \pi$ tales que:

$$O^\pi(G) = O^{p_1} O^{p_2} \cdots O^{p_n}(G) \; .$$

Demostración: (i) : Como G/G es π-soluble, entonces $O^\pi(G)$ existe. Si G/U y G/V son π-solubles, con $U, V \leq G$, entonces la sucesión:

$$1 \longrightarrow U \bigcap V \xrightarrow{\;i\;} G \xrightarrow{\;\rho\;} \frac{G}{U} \times \frac{G}{V}$$

es exacta en G, donde i es la inclusión y ρ es la proyección canónica en cada coordenada. Por tanto, $G/U \bigcap V$ es π-soluble, ya que es isomorfo a un subgrupo del grupo π-soluble $G/U \times G/V$. Así, $O^\pi(G)$ es único.

(vi) : Si $f\colon G \longrightarrow K$ es un isomorfismo, entonces f induce un isomorfismo:

$$\bar{f}\colon \frac{U}{O^\pi(U)} \longrightarrow \frac{f(U)}{f(O^\pi(U))}$$

así, $O^\pi(f(U)) \leq f(O^\pi(U))$. Usando f^{-1} tenemos el resultado.

(ii) : Se sigue inmediatamente de (vi). Además los incisos (iii) y (iv) son claros.

(v) : Como $G/O^p(G)$ es p-grupo, y por lo tanto G-soluble. Así, $O^\pi(G) \leq O^p(G)$. Pero $G/O^\pi(G)$ es p-grupo , entonces $O^p(G) \leq O^\pi(G)$.

(vii) : Tomemos $\pi' = \{p \in \pi : p \mid |G|\}$.

$(viii)$: Como $O^\pi(O^{\pi'}(G)) \trianglelefteq O^{\pi'}(G) \trianglelefteq G$, y $O^\pi(O^{\pi'}(G))$ es característico en $O^{\pi'}(G)$. Luego $O^\pi(O^{\pi'})$ es subgrupo normal de G. Además, tenemos la siguiente sucesión exacta:

$$1 \longrightarrow \frac{O^{\pi'}(G)}{O^\pi(O^{\pi'}(G))} \xrightarrow{\;i\;} \frac{G}{O^\pi(O^{\pi'}(G))} \xrightarrow{\;\rho\;} \frac{G}{O^{\pi'}(G)} \longrightarrow 1 \; ,$$

donde i es la inclusión y ρ la proyección canónica. Por lo tanto, $G/O^\pi(O^{\pi'}(G))$ es π-soluble, así, $O^\pi(G) \leq O^\pi(O^{\pi'}(G))$. Además, $G/O^{\pi'}(G)$ es π'-soluble, entonces es π-soluble. Por ello $O^\pi(G) \trianglelefteq O^{\pi'}(G)$, ya que $O^\pi(G) \trianglelefteq G$.

Entonces $O^{\pi'}(G)/O^\pi(G) \leq G/O^\pi(G)$, así, $O^\pi(O^{\pi'}(G)) \leq O^\pi(G)$.

(ix) : Por hipótesis $O^\pi(K) \leq H$. Por ello, $H/O^\pi(K) \leq K/O^\pi(K)$. Así $H/O^\pi(K)$ es π-soluble. Entonces $O^\pi(H) \leq O^\pi(K)$. Por otra parte, la sucesión:

$$1 \longrightarrow \frac{H}{O^\pi(H)} \longrightarrow \frac{K}{O^\pi(H)} \longrightarrow \frac{K}{H} \longrightarrow 1\,,$$

es exacta, entonces $K/O^\pi(H)$ es π-soluble, ya que los extremos de la sucesión lo son. Por tanto $O^\pi(K) \leq O^\pi(H)$.

(x) : Como $G/O^\pi(G)$ es π-soluble, existe una serie:

$$O^\pi(G) = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G,$$

donde $|H_i/H_{i-1}| = p_i \in \pi$ para cada i. Entonces $O^{p_1}O^{p_2}\cdots O^{p_n}(G) = O^\pi(G)$, pués $O^{p_n}(G) \leq H_{n-1}$. Por tanto $O^{p_{n-1}}O^{p_n}(G) \leq O^{p_{n-1}}(H_{n-1}) \trianglelefteq H_{n-2}$. Continuando de esta manera llegamos a $O^{p_1}O^{p_2}\cdots O^{p_n}(G) \leq O^\pi(G)$.

Por otra parte, $O^{p_1}O^{p_2}\cdots O^{p_n}(G) \trianglelefteq (G)$, pues la propiedad de ser característico es transitiva. Es claro que $G/O^{p_1}O^{p_2}\cdots O^{p_n}(G)$ es soluble y su orden es un π-número. Por tanto $O^\pi(G) \leq O^{p_1}O^{p_2}\cdots O^{p_n}(G)$ ∎

Sea $H \leq G$ un subgrupo de G. Decimos que H es *π-perfecto* si cumple que $O^\pi(H) = H$.

Sean U, V subgrupos de G, observemos que $\overline{\beta_\pi(U,0^*)} \bigcap \overline{\beta_\pi(V,0^*)} \neq \emptyset$ si y sólo si existe un ideal primo $\wp$ de $\Omega_\pi(G)$ que es de la forma:

$$\wp = \beta_\pi(U, q^*) = \beta_\pi(V, q^*),$$

para algún ideal primo $q^* \in \mathbb{Z}_\pi$. Por el teorema 7.9, ésto sucede si y sólo si $O^q(U) \sim O^q(V)$.

7.13 LEMA

Si $\beta_\pi(U,p^*)$ y $\beta_\pi(V,q^*)$ están en la misma componente conexa del espectro de $\Omega_\pi(G)$, entonces $O^\pi(U) \sim O^\pi(V)$.

Demostración: Por la observación 7.11, existe una sucesión de ideales primos minimales $\beta_\pi(U_1,0^*),\ldots,\beta_\pi(U_n,0^*)$ de $\Omega_\pi(G)$, tal que:

$$\beta_\pi(U,p^*) \in \overline{\{\beta_\pi(U_1,0^*)\}},\ \beta_\pi(V,q^*) \in \overline{\{\beta_\pi(U_n,0^*)\}},\ \overline{\{\beta_\pi(U_i,0^*)\}} \bigcap \overline{\{\beta_\pi(U_{i+1},0^*)\}} \neq \emptyset,\ \forall i\,.$$

Utilizando el lema 7.12, tenemos:

$$O^\pi(U) = O^\pi(O^{p_1}(U)) \sim O^\pi(O^{p_1}(U_1)) \sim \ldots \sim O^\pi(O^{p_n}(U_n)) \sim O^\pi(O^{p_n}(V)) = O^\pi(V)\ . \quad \blacksquare$$

7.14 LEMA

Los ideales primos $\beta_\pi(U,q^*)$ y $\beta_\pi(O^\pi(U),0^*)$ están en la misma componente conexa del espectro.

Demostración: Sabemos que $U/O^\pi(U)$ es π-soluble, así que existe una serie de composición:

$$O^\pi(U) = U_0 \trianglelefteq U_1 \trianglelefteq \ldots \trianglelefteq U_n = U\ ,$$

donde U_i/U_{i-1} es un p_i-grupo cíclico, con $p_i \in \pi$, para toda i. Entonces:

$$\beta_\pi(O^\pi(U),0^*) \in \overline{\{\beta_\pi(U_0,0^*)\}},\ \ \beta_\pi(U,q^*) \in \overline{\{\beta_\pi(U_n,0^*)\}}\ ,$$

y veremos que $\overline{\{\beta_\pi(U_{i-1},0^*)\}} \bigcap \overline{\{\beta_\pi(U_i,0^*)\}} \neq \emptyset,\ \forall i$, con lo que queda demostrado el lema. Como U_i/U_{i-1} es un p_i-grupo, usando el lema 7.8, tenemos que $O^{p_i}(U_i) \sim O^{p_i}(U_{i-1})$. Simplemente aplicamos el teorema de Dress, y tenemos que $\beta_\pi(U_{i-1},p_i^*) = \beta_\pi(U_i,p_i^*)$. $\blacksquare$

7.15 TEOREMA

Dos ideales primos $\beta_\pi(U,p^*)$ y $\beta_\pi(V,q^*)$ están en la misma componente conexa del espectro si y sólo si $O^\pi(U) \sim O^\pi(V)$.

Demostración: $(\Longrightarrow)$: Lema 7.13.

$(\Longleftarrow)$: Por el lema anterior, los ideales primos $\beta_\pi(U,p^*)$ y $\beta_\pi(O^\pi(U),0^*)$ están en la misma componente conexa. De igual forma, $\beta_\pi(V,q^*)$ y $\beta_\pi(O^\pi(V),0^*)$ están en la misma componente. Si $O^\pi(U) \sim O^\pi(V)$, por el teorema de Dress tenemos que: $\beta_\pi(O^\pi(U),0^*) = \beta_\pi(O^\pi(V),0^*)$. ∎

Sea G un grupo, es claro que $O^\pi(O^\pi(U)) = O^\pi(U)$, para todo $U \leq G$. Así el grupo $O^\pi(U)$ es π-perfecto. Entonces hay una biyección entre las componentes conexas de $Spec(\Omega_\pi(G))$ y las clases de conjugación de subgrupos π-perfectos de G. Esto prueba la primera equivalencia del siguiente corolario.

7.16 COROLARIO

G es π-soluble $\Longleftrightarrow$ $Spec(\Omega_\pi(G))$ es conexo $\Longleftrightarrow$ 0 y 1 son los únicos idempotentes en $\Omega_\pi(G)$.

Demostración: Sólo probaremos la segunda equivalencia. $(\Longrightarrow)$: Supongamos que existe un idempotente $e \in \Omega_\pi(G)$ distinto de 0 y 1. Entonces

$$\Omega_\pi(G) = (e)\Omega_\pi(G) \bigoplus (1-e)\Omega_\pi(G) .$$

Así, $Spec(\Omega_\pi(G)) = V((e)\Omega_\pi(G)) \uplus V((1-e)\Omega_\pi(G))$.

$(\Longleftarrow)$: Supongamos que $Spec(\Omega_\pi(G)) = V(I_1) \uplus V(I_2)$, para algunos ideales I_1, I_2 de $\Omega_\pi(G)$. Los elementos de $I_1 \cap I_2$ son nilpotentes (porque están en la intersección de todos los ideales primos). Pero $\Omega_\pi(G)$ no tiene elementos nilpotentes distintos de 0. Entonces $I_1 \bigcap I_2 = 0$. Por otra parte, $\emptyset = (I_1) \bigcap (I_2) = V(I_1 + I_2)$, por tanto, $\Omega_\pi(G) = I_1 + I_2$. Luego, $\Omega_\pi(G) = I_1 \bigoplus I_2$, y tenemos que $1 = e_1 + e_2$ con $e_1 \in I_1$, $e_2 \in I_2$. Es claro que e_1, e_2 son idempotentes distintos de 0 y 1. ∎

4

Idempotentes en los Anillos de Burnside

La filosofía está escrita en este grandísimo libro que continuamente está abierto ante nuestros ojos (digo: el Universo), pero no puede entenderse si antes no se procura entender su lengua y conocer sus caracteres en los cuales está escrito. Este libro está escrito en lengua matemática, y sus caracteres son triángulos, círculos y otras figuras geométricas, sin las cuales es totalmente imposible entender humanamente una palabra, y sin las cuales nos agitamos vanamente en un oscuro laberinto.

Galileo Galilei (1564-1642)

§8 CONJUNTOS PARCIALMENTE ORDENADOS

En esta sección estableceremos propiedades fundamentales de los conjuntos parcialmente ordenados. El tema de esta sección parece apartado del objetivo principal de esta tesis, sin embargo, el teorema de inversión de Mõbius y otros resultados que estudiaremos serán muy importantes para la última y más importante sección de este trabajo.

8.1 DEFINICION

Un conjunto parcialmente ordenado es un conjunto P no vacío, junto con una relación "$\leq$" entre sus elementos, que cumple:

(i) : $a \leq a, \ \forall a \in P$;

(ii) : $a \leq b, \ b \leq c \implies a \leq c, \ \forall a, b, c \in P$;

(iii) : $a \leq b, \ b \leq a \implies a = b, \ \forall a, b \in P$.

Además, decimos que P es *localmente finito* si sus "intervalos" son finitos. Es decir, la cardinalidad $|\{x \in P : a \leq x \text{ y } \ x \leq b\}|$ es finita, para calquier $a, b \in P$.

Sean P un conjunto parcialmente ordenado localmente finito, y R un anillo conmutativo con uno. Definimos el conjunto:

$$a_R(P) = \{\vartheta : P \times P \longrightarrow R : \vartheta(x, y) = 0 \text{ si } x \not\leq y\}.$$

Este conjunto tiene estructura de anillo, con la suma usual de funciones $+$, y la multiplicación $*$ definida para toda $\vartheta, \varepsilon \in a_R(P)$ como:

$$(\vartheta * \varepsilon)(x, y) := \sum_{x \leq z \leq y} \vartheta(x, z)\varepsilon(z, y) = \sum_{z \in P} \vartheta(x, z)\varepsilon(z, y).$$

El lector puede verificar facilmente que estas operaciones cumplen las propiedeades requeridas para hacer de $a_R(P)$ un anillo.

Desafortunadamente $a_R(P)$ no es, en general, un anillo conmutativo. En cambio, $a_R(P)$ siempre tiene elemento identidad. El uno de $a_R(P)$ es la función δ, definida como:

$$\delta(x,y) := \delta_{x,y}\ ,\ \forall(x,y) \in P \times P.$$

Esto es fácil de comprobar: sea $\vartheta \in a_R(P)$, entonces

$$(\vartheta * \delta)(x,y) = \sum_{x \leq z \leq y} \vartheta(x,z)\delta(z,y) = \vartheta(x,y)\delta(y,y) = \vartheta(x,y),$$

$$(\delta * \vartheta)(x,y) = \sum_{x \leq z \leq y} \delta(x,z)\vartheta(z,y) = \delta(x,x)\vartheta(x,y) = \vartheta(x,y),\ \forall(x,y) \in P \times P.$$

Si R es un anillo, denotamos por $\mathcal{U}(R)$ al conjunto de elementos de R que tienen inverso derecho e izquierdo en el anillo, es decir, $\mathcal{U}(R)$ es el conjunto de las unidades del anillo R.

8.2 TEOREMA

Sean P un conjunto parcialmente ordenado localmente finito, y R un anillo conmutativo, entonces:

$$\vartheta \in \mathcal{U}(a_R(P)) \iff \vartheta(x,x) \in \mathcal{U}(R)\ \forall x \in P.$$

Demostración: $(\Longrightarrow)$: Por hipótesis, existe $\varepsilon \in a_R(P)$ tal que $\vartheta * \varepsilon = \delta$. Por tanto, si $x \in P$,

$$1 = \delta(x,x) = (\vartheta * \varepsilon)(x,x) = \sum_{x \leq z \leq x} \vartheta(x,z)\varepsilon(z,x) = \vartheta(x,x)\varepsilon(x,x).$$

Así, usando que R es conmutativo, $\vartheta(x,x) \in \mathcal{U}(R)$.

$(\Longleftarrow)$: Construyamos la función $\varepsilon = \vartheta^{-1}$, inversa de ϑ inductivamente. Para cada $x \in P$ definimos $\varepsilon(x,x) = (\vartheta(x,x))^{-1}$. También definimos $\varepsilon(x,y) = 0$ si $y \in P$ con $x \not\leq y$. Sean $x,y \in P$ y supongamos que para toda z tal que $x \leq z < y$, $\varepsilon(x,z)$ está definido (hipótesis de inducción). Supongamos por un momento que ya sabemos quién es ε y tratemos de calcular $\varepsilon(x,y)$:

$$(\varepsilon * \vartheta)(x,y) = \sum_{x \leq z \leq y} \varepsilon(x,z)\vartheta(z,y) = \sum_{x \leq z < y} \varepsilon(x,z)\vartheta(z,y) + \varepsilon(x,y)\vartheta(y,y).$$

Por lo anterior, tenemos que definir

$$\varepsilon(x,y) := \frac{-\sum_{x\leq z<y}\varepsilon(x,z)\vartheta(z,x)}{\vartheta(y,y)}.$$

De esta manera, $(\varepsilon * \vartheta)(x,y) = \delta(x,y)$, para todo $(x,y) \in P \times P$. De forma análoga podemos construir el inverso derecho de ϑ. Por tanto $\vartheta \in \mathcal{U}(a_R(P))$. ∎

Consideremos ahora la función ς de $a_R(P)$ definida como:

$$\varsigma(x,y) = \begin{cases} 1, & \text{si } x \leq y; \\ 0, & \text{si } x \not\leq y. \end{cases}$$

Llamaremos a ς la *función Zeta*. Nótese que, por el teorema anterior, $\varsigma \in \mathcal{U}(a_R(P))$. La *función de Mõbius* es por definición: $\mu := \varsigma^{-1}$.

8.3 LEMA

Sea P un conjunto parcialmente ordenado localmente finito. La función μ de Mõbius de P cumple que:

(1) $\mu(x,x) = 1, \ \ \forall x \in P$;

(2) $\sum_{x\leq z\leq y}\mu(x,z) = 0, \ \ \forall x,y \in P, \ x \neq y$;

(3) Sea P' un subconjunto parcialmente ordenado de P *pleno* (i.e. $x \leq y$ en P implica $x \leq y$ en P', para cada $x,y \in P'$). Denotemos por μ' la funcion de Mõbius de P'. Entonces:

$$\mu'(x,y) = \mu(x,y), \ \ \forall x,y \in P'.$$

Demostración: (1) Se sigue de la definición de μ: $\mu(x,x) = (\varsigma(x,x))^{-1} = 1, \ \ \forall x \in P$.

(2) Como $x \neq y$, tenemos que:

$$0 = \delta(x,y) = (\mu * \varsigma)(x,y) = \sum_{x\leq z\leq y}\mu(x,z)\varsigma(z,y) = \sum_{x\leq z\leq y}\mu(x,z).$$

(3) Se demuestra facilmente por inducción sobre la distancia de x a y usando (2). ∎

Definimos la *función de cadenas* η como: $\eta := \varsigma - \delta$. Es decir:

$$\eta(x,y) = \begin{cases} 0, & \text{si } x \not< y; \\ 1, & \text{si } x < y. \end{cases}$$

Si $x < y$, una *cadena* entre x y y es un conjunto $\{x_0, x_1, \ldots, x_n\}$ de elementos de P tales que $x = x_0 < x_1 < x_2 < \cdots < x_n = y$. El número n se denomina *el tamaño* de la cadena. Un n-simplejo es sencillamente una cadena de tamaño n.

La función η nos indicará el número de cadenas, de cierta longitud, que existen entre x y y.

8.4 TEOREMA

La función η cumple que:

$$\eta^n(x,y) = \left|\{x = x_0 < x_1 < x_2 < \cdots < x_n = y : x_i \in P\}\right|.$$

Es decir, $\eta^n(x,y)$ es el número de cadenas entre x y y de longitud n.

Demostración: Sin pérdida de generalidad, supongamos que $x < y$. La demostración se hará por inducción sobre k , la potencia de η. Para $k = 1$, $\eta^1(x,y) = 1$, por tanto, el resultado vale para el pie de la inducción.

Supongamos válido el resultado para $k = n-1$, y probaremos el resultado para $k = n$.

$$\eta^n(x,y) = (\eta * \eta^{n-1})(x,y) = \sum_{x \le z \le y} \eta(x,z)\eta^{n-1}(z,y)$$

$$= \sum_{x<z<y} \eta(x,z)\eta^{n-1}(z,y) = \sum_{x<z<y} \eta^{n-1}(z,y).$$

Utilizando la hipótesis de inducción tenemos que lo anterior coincide con:

$$\sum_{x<z<y} \left|\{z = x_0 < x_1 < \cdots < x_{n-1} = y : x_i \in P\}\right|,$$

que es precisamente el número de cadenas entre x y y de longitud n. ∎

El *complejo simplicial* C_P asociado a P es, por definición, el conjunto formado por todos los k-simplejos, para todo $k \in \mathbb{N}$.

Si P es finito, definimos la *característica de Euler* $\chi(P)$ de P como la característica de Euler del complejo simplicial C_P asociado a P. Esto es:

$$\chi(P) = \sum_{k=0}^{\infty} (-1)^k \alpha_k,$$

donde α_k es el número de k-simplejos del complejo simplicial C_P.

8.5 LEMA

Sea P un conjunto parcialmente ordenado finito, entonces:

$$\chi(P) = \sum_{x,y\in P} \mu(x,y).$$

Demostración: Por el teorema anterior, $\alpha_k = \sum_{x,y\in P} \eta^k(x,y)$, para cada $k \in \mathbb{N}$. Además, como sabemos, $\chi(P) = \sum_{k=0}^{\infty}(-1)^k\alpha_k$. Por tanto,

$$\chi(P) = \sum_{k=0}^{\infty}\sum_{x,y\in P}(-1)^k\eta^k(x,y) = \sum_{x,y\in P}\left(\sum_{k=0}^{\infty}(-1)^k\eta^k(x,y)\right).$$

Pero $[(\delta+\eta)*(\sum_{k=0}^{\infty}(-1)^k\eta^k)](x,y) = [(\sum_{k=0}^{\infty}(-1)^k\eta^k) + (\sum_{k=0}^{\infty}(-1)^k\eta^{k+1}](x,y) = \eta^0(x,y) = \delta(x,y)$, para cada $x,y \in P$. Por tanto,

$$\sum_{k=0}^{\infty}(-1)^k\eta^k = (\delta+\eta)^{-1} = \mu.$$

Por lo tanto $\chi(P) = \sum_{x,y\in P}\mu(x,y)$. ∎

8.6 LEMA

Si el conjunto parcialmente ordenado finito P tiene un único elemento minimal 0, y μ denota la función de Möbius de P, entonces:

$$\chi(P) = 1, \quad \text{y} \quad \chi(P-\{0\}) = 1 - \sum_{x\in P}\mu(0,x).$$

Demostración: Por el lema anterior y por el lema 8.3,

$$\chi(P) = \sum_{x,y\in P}\mu(x,y) = \sum_{y\in P}\left(\sum_{0\leq x\leq y}\mu(x,y)\right) = \mu(0,0) = 1. \text{ Además:}$$

$$1 = \chi(P) = \sum_{x,y\in P}\mu(x,y) = \sum_{\substack{x,y\in P\\ x\neq 0}}\mu(x,y) + \sum_{w\in P}\mu(0,w) = \chi(P-\{0\}) + \sum_{w\in P}\mu(0,w).$$

La última igualdad se tiene por el lema 8.3. Por lo tanto, $\chi(P-\{0\}) = 1-\sum_{x\in P}\mu(0,x)$.

∎

El lema anterior puede cambiarse facilmente, sustituyendo la hipótesis de tener un elemento minimal por la de tener un único elemento maximal.

8.7 TEOREMA (DE INVERSION DE MÖBIUS)

Sean P un conjunto parcialmente ordenado finito, R un anillo conmutativo, y $f, g: P \longrightarrow R$ dos funciones. Supongamos que existe $\alpha \in \mathcal{U}(a_R(P))$, con inverso β. Entonces:

$$f(x) = \sum_{y\in P}\alpha(y,x)g(y) \iff g(x) = \sum_{y\in P}\beta(y,x)f(y).$$

Demostración: Por la simetría de la proposición, es suficiente probar sólo una implicación:

$(\Longrightarrow)$: Tenemos que:

$$\sum_{y\in P}\beta(y,x)f(y) = \sum_{y\in P}\beta(y,x)\sum_{z\in P}\alpha(z,y)g(z) = \sum_{z\in P}\sum_{y\in P}\beta(y,x)\alpha(z,y)g(z)$$

$$= \sum_{z\in P}g(z)(\sum_{y\in P}\beta(y,x)\alpha(z,y)) = \sum_{z\in P}g(z)\delta(x,z) = g(x) \quad ∎$$

.

Sean P y T dos conjuntos parcialmente ordenados localmente finitos. Una función $f: P \longrightarrow T$ biyectiva se dice que es un isomorfismo de parcialmente ordenados si cumple que: $a \leq b \iff f(a) \leq f(b)$.

8.7 OBSERVACION

Sea $f : P \longrightarrow T$ un isomorfismo de conjuntos parcialmente ordenados, y denotemos por μ las funciones de Möbius de P y T. Entonces:

$$\mu(x,y) = \mu(f(x), f(y)). \quad ∎$$

§9 IDEMPOTENTES EN LOS ANILLOS DE BURNSIDE

En esta sección enunciaremos y demostraremos el teorema de Yoshida, que es el objetivo primordial de este trabajo.

Introducimos primero alguna notación: Sea G un grupo finito. El conjunto de subgrupos de G está parcialmente ordenado por la relación de contención. Llamemos a este conjunto el *la red de subgrupos* de G, denotado $S(G)$. Sea μ la función de Möbius de $S(G)$, y sea π un conjunto de números primos. $\mathbb{P}_\pi(G) \subseteq C(G)$ denotará el conjunto de clases de conjugación de subgrupos π-perfectos de G.

Para un subgrupo D de G y un subgrupo π-perfecto H de G, definimos:

$$\xi_\pi(H) := \xi_\pi(G,H) := \{S \subseteq G : O^\pi(S) = H\} ;$$

$$\lambda(D,H) := \sum_{S \in \xi_\pi(H)} \mu(D,S) .$$

Nótese que si $\lambda(D,H) \neq 0$, entonces existe $S \in \xi_\pi(H)$ tal que $\mu(D,S) \neq 0$, por lo tanto $D \leq S$. Así, $O^\pi(D) \leq O^\pi(S) = H$. De esto tenemos $D \leq N_G(H)$.

Ahora, para cada subgrupo π-perfecto H de G, definimos un elemento de $\Omega_{\mathbb{Q}}(G)$:

$$e^\pi_{G,H} := \frac{1}{|N_G(H)|} \sum_{D \leq N_G(H)} |D|\lambda(D,H)[G/D].$$

9.1 OBSERVACION

Si $(H) = (K)$, es decir, $H = g^{-1}Kg$ para alguna $g \in G$, entonces $e^\pi_{G,H} = e^\pi_{G,K}$.

Demostración: Tenemos que:

$$e^\pi_{G,H} = e^\pi_{G,g^{-1}Kg} = \frac{1}{|N_G(g^{-1}Kg)|} \sum_{D \leq N_G(g^{-1}Kg)} |D|\lambda(D,g^{-1}Kg)[G/D].$$

Pero, $N_G(g^{-1}Kg) = g^{-1}N_G(K)g$. Así:

$$e^{\pi}_{G,H} = \frac{1}{|g^{-1}N_G(K)g|} \sum_{D \le g^{-1}N_G(K)g} |D|\lambda(D, g^{-1}Kg)[G/D].$$

Tenemos $D \le g^{-1}N_G(K)g$ si y sólo si $gDg^{-1} \le N_G(K)$. Sea $D' = gDg^{-1}$. Entonces:

$$e^{\pi}_{G,H} = \frac{1}{|N_G(K)|} \sum_{D' \le N_G(K)} |D'|\lambda(g^{-1}D'g, g^{-1}Kg)[G/D'].$$

Pero:

$$\lambda(g^{-1}D'g, g^{-1}Kg) = \sum_{g^{-1}Sg \in \xi_\pi(g^{-1}Kg)} \mu(g^{-1}D'g, g^{-1}Sg).$$

Podemos escribir esto así, ya que la conjugación por un elemento de G es un isomorfismo de conjuntos parcialmente ordenados de $S(G)$ en $S(G)$. Por la última observación de la sección anterior tenemos:

$$\sum_{g^{-1}Sg \in \xi_\pi(g^{-1}Kg)} \mu(g^{-1}D'g, g^{-1}Sg) = \sum_{S \in \xi_\pi(K)} \mu(D', S) = \lambda(D', K).$$

Por tanto:

$$e^{\pi}_{G,H} = \frac{1}{|N_G(K)|} \sum_{D' \le N_G(K)} |D'|\lambda(D', K)[G/D'] = e^{\pi}_{G,K}. \quad \blacksquare$$

En particular, cuando $\pi = \emptyset$, tenemos que $\Omega_\pi(G) = \Omega_{\mathbb{Q}}(G)$, y que $\mathbb{P}_\pi(G) = \mathcal{C}(G)$. Además, $\xi_\pi(H) = \{H\}$ para todo subgrupo H de G. De esta manera:

$$e_{G,H} = e^{\emptyset}_{G,H} = \frac{1}{|N_G(H)|} \sum_{D \le H} |D|\mu(D, H)[G/D].$$

9.2 LEMA

Sea $e_D := (0, \ldots, 1, 0, \ldots, 0)$ donde el 1 aparece en la coordenada correspondiente a (D). Entonces

$$\frac{G}{H} = \sum_{D \le H} \frac{|N_G(D)|}{|H|} e_D.$$

Demostración: Tenemos que:

$$\frac{G}{H} = \sum_{(D)\in\mathcal{C}(G)} \varphi_D(G/H)e_D$$

$$= \sum_{(D)\in\mathcal{C}(G)} \frac{|N_G(D)|}{|H|}\beta(D,H)e_D = \sum_{D\le H} \frac{|N_G(D)|}{|H|}e_D \ .$$

Donde $\beta(D,H)$ está definido en 5.1 . ∎

Es claro que los $\{e_H\}_{H\in\mathcal{C}(G)}$ son todos los idempotentes primitivos de $\Omega_{\mathbb{Q}}(G)$.

9.3 LEMA

El conjunto $\{e_{G,H} : (H) \in \mathcal{C}(G)\}$ es el conjunto de todos los idempotentes primitivos de $\Omega_{\mathbb{Q}}(G)$.

Demostración: Sean $\ell(G)$ la red de subgrupos de G, $R := \Omega_{\mathbb{Q}}(G)$, y sean $f, g : \ell(G) \longrightarrow R$ definidas como: $f(H) = |H|G/H$, $\forall H \in \ell(G)$, y $g(H) = |N_G(H)|e_H$. Entonces:

$$f(H) = \sum_{D\le H} g(D) = \sum_{D\in\ell(G)} \varsigma(D,H)g(D),$$

por el teorema de inversión de Möbius, tenemos $g(H) = \sum_{D\in\ell(G)} \mu(D,H)f(D)$, por lo tanto:

$$|N_G(H)|e_H = \sum_{D\in\ell(G)} \mu(D,H)|D|\frac{G}{D} \ . \quad ∎$$

9.4 TEOREMA (YOSHIDA)

El conjunto $\{e^{\pi}_{G,H} : (H) \in \mathbb{P}_{\pi}(G)\}$ es el conjunto de todos los *idempotentes primitivos* de $\Omega_{\pi}(G)$. Así, en particular:

$$\sum_{(H)\in\mathbb{P}_{\pi}(G)} e^{\pi}_{G,H} = 1 \ ,$$

$$e^{\pi}_{G,H}e^{\pi}_{G,K} = \begin{cases} e^{\pi}_{G,K}, & \text{si } (H) = (K); \\ 0, & \text{otro caso.} \end{cases}$$

Demostración: Sean H un subgrupo π-perfecto de G, $N := N_G(H)$, y $\xi := \xi_{\pi}(G,H)$. Ya que H es un subgrupo característico de todo S en ξ, tenemos que $H \trianglelefteq N_G(S)$, así que $N_G(S)$ está contenido en N para cualquier S en ξ. Además, dos miembros S y T de ξ son conjugados en G si y sólo si son conjugados en N, ya que si $S = gTg^{-1}$, entonces $H = O^\pi(S) = gO^\pi(T)g^{-1} = gHg^{-1}$, así que $g \in N$.

Sea $\{S_1, S_2, \ldots\}$ un conjunto completo de representantes de clases de N-conjugación de ξ. Notemos que N actúa en ξ vía conjugación, entonces la órbita $O(S)$ de S son todos sus conjugados en ξ, y su orden es $|O(S)| = |N : N_S| = [N : N_G(S)]$. Entonces, tenemos la siguiente serie de igualdades en $\Omega_{\mathbb{Q}}(G)$:

$$\sum_i e_{G,S_i} = \sum_{S\in\xi} \frac{1}{[N : N_G(S)]} e_{G,S} = \sum_{S\in\xi} \frac{1}{[N : N_G(S)]} \frac{1}{|N_G(S)|} \sum_{D\leq S} |D|\mu(D,S)[G/D] =$$

$$\frac{1}{|N|} \sum_{S\in\xi} \sum_{D\leq S} |D|\mu(D,S)[G/D] = \frac{1}{|N|} \sum_{S\in\xi} \sum_{D\leq G} |D|\mu(D,S)[G/D] =$$

$$\frac{1}{|N|} \sum_{D\leq G} |D| \left(\sum_{S\in\xi} \mu(D,S) \right) [G/D] = \frac{1}{|N|} \sum_{D\leq G} |D|\lambda(D,H)[G/D] = e^\pi_{G,H}.$$

Entonces cada $e^\pi_{G,H}$ es un idempotente de $\Omega_{\mathbb{Q}}(G)$. Además $e^\pi_{G,H} = e^\pi_{G,K}$ si y sólo si $(H) = (K)$. En efecto: si $e^\pi_{G,H} = e^\pi_{G,K}$, entonces $e_{G,H}e^\pi_{G,H} = e_{G,H}$, y por otra parte $e_{G,H}e^\pi_{G,K} = e_{G,T}$, con $O^\pi(T) = K$; pero $e_{G,T} = e_{G,H}$ implica $T \sim H$; la reciproca es la observación 9.1.

Como sabemos, el número de idempotentes primitivos de $\Omega_\pi(G)$ es igual al rango del $\mathbb{Z}_\pi$-módulo libre $\Omega_\pi(G)$, es decir, es orden de $\mathbb{P}_\pi(G)$. Este es igual también al número de idempotentes de $\Omega_{\mathbb{Q}}(G)$ de la forma $e^\pi_{G,H}$. Lo que resta ahora es probar que los $e^\pi_{G,H}$ son justamente los idempotentes primitivos de $\Omega_\pi(G)$. Será suficiente mostrar la siguiente proposición:

Todo idempotente de $\Omega_\pi(G)$ es la suma en $\Omega_{\mathbb{Q}}(G)$ de algunos idempotentes (distintos) de la forma $e^\pi_{G,H}$.

Nótese que ésto implica que $e^\pi_{G,H} \in \Omega_\pi(G)$ y es idempotente primitivo. Sea $e \in \Omega_\pi(G)$ un idempotente. Para cada subgrupo H de G, vemos que $\varphi_H(e)$ es cero ó uno, ya que φ_H es un homomorfismo de anillos. Sea $\mathbb{H}$ el conjunto de subgrupos H de G tales que $\varphi_H(e) = 1$, y sean $H_1, \ldots H_t$ un conjunto de representantes de clases de conjugación de G en $\mathbb{H}$. Por el primer caso, si vemos a e en $\Omega_{\mathbb{Q}}(G)$, tenemos que $e = \sum_{i=1}^{t} e_{G,H_i}$. Describamos $\mathbb{H}$: Sea H un subgrupo de G, entonces es claro de la definición del ideal primo $\beta_\pi(H, p\mathbb{Z}_\pi)$, que $H \in \mathbb{H}$ si y sólo si $e \notin \beta_\pi(H, p\mathbb{Z}_\pi)$, para todo $p \in \pi \cup \{0\}$.

Sea $p \in \pi$. Ya que $\beta_\pi(H, p\mathbb{Z}_\pi) = \beta_\pi(O^p(H), p\mathbb{Z}_\pi)$, vemos que $H \in \mathbb{H}$ si y sólo si $O^p(H) \in \mathbb{H}$ para todo $p \in \pi \bigcup \{0\}$. Por el lema 7.12, existen $p_1, \ldots, p_n \in \pi$ tales que $O^\pi(H) = O^{p_1} O^{p_2} \cdots O^{p_n}(H)$. En consecuencia $H \in \mathbb{H}$ si y sólo si $O^\pi(H) \in \mathbb{H}$. Ya que $O^\pi(H)$ es siempre π-perfecto, esto significa que

$$\mathbb{H} = \bigcup \{\xi_\pi(H) : H \in \mathbb{H} \text{ y } H \text{ es } \pi\text{-perfecto}\} \qquad \text{(unión disjunta)}.$$

Para cada i, sean $H_{i_1}, H_{i_2}, \ldots$ un conjunto de representantes de clases de conjugación de G en $\xi_\pi(O^\pi(H_i))$, entonces

$$e = \sum_i e_{G,H_i} = \sum_i \sum_j e_{G,H_j} = \sum_i e^\pi_{G,O^\pi(H_i)}.$$

Esto prueba la afirmación, y como consecuencia, el teorema. ∎

Sea π un conjunto de primos, y n un entero, denotamos por $|n|_\pi$ al número que resulta del producto de los primos de π que aparecen en la descomposición de n, conservando sus potencias. Por ejemplo, si $\pi = \{2,3\}$, $n = 45$, entonces $|n|_\pi = 9$.

9.5 COROLARIO

Sean H un subgrupo normal π-perfecto de G, y D un subgrupo de G. Entonces:

$$\lambda(D,H) = \sum_{S \in \xi_\pi(H)} \mu(D,S) \equiv 0 \pmod{[N_G(D) : D]_\pi}.$$

Demostración: Consideremos el idempotente

$$e^\pi_{G,H} = \frac{1}{|G|} \sum_{E \leq G} |E| \lambda(E,H)[G/E].$$

El coeficiente de $[G/D]$ en la expresión única de $e^\pi_{G,H}$ en términos de la $\mathbb{Z}_\pi$-base canónica de $\Omega_\pi(G)$ es:

$$\frac{1}{|G|} |D| \lambda(D,H)[G : N_G(D)] \in \mathbb{Z}_\pi,$$

ya que el número de conjugados de D en G es $[G : N_G(D)]$. Por tanto

$$\lambda(D, H) \in [N_G(D) : D]_\pi \mathbb{Z}. \quad \blacksquare$$

9.6 COROLARIO

Sea ξ_p el conjunto de p-subgrupos no triviales del grupo finito G para un primo p. Este conjunto está parcialmente ordenado por contención. Su característica de Euler satisface:

$$\chi(\xi_p) \equiv 1 \pmod{|G|_p}.$$

Demostración: Sea $\mathfrak{A}_p := \{A \leq G : A \text{ es } p\text{-grupo}\}$. Entonces el elemento identidad e es el único elemento minimal de $\mathfrak{A}_p$. Por el lema 8.5, $\chi(\mathfrak{A}_p) = 1$, y también $\chi(\mathfrak{A}_p - \{e\}) = 1 - \sum_{x \in \mathfrak{A}_p} \mu(e, x)$.

Por el corolario 9.5, haciendo $\pi = \{p\}, H = D = e$, tenemos

$$\sum_{s \in \xi_\pi(e)} \mu(e, s) \equiv 0 \pmod{|G|_p},$$

pero $\xi_\pi(e) = \mathfrak{A}_p$, por tanto

$$\chi(\mathfrak{A}_p - \{e\}) \equiv 1 \pmod{|G|_p}. \quad \blacksquare$$

A continuación mencionamos algunas fórmulas sobre los idempotentes del anillo de Burnside.

9.7 OBSERVACIONES

(i) $\varphi_K(e_{G,H}) = 1,$ si $(H) = (K)$;

$= 0,$ otro caso.

(ii) $e_{G,H}x = \varphi_H(x)e_{G,H}$ para todo $x \in \Omega_{\mathbb{Q}}(G)$.

(iii) $e^\pi_{G,H} = \sum_{(S)} e_{G,S}$, donde (S) corre sobre $(S) \in C(G)$ con $O^\pi(S) = H$.

Demostración: Los incisos (i) y (iii) fueron probados en la demostración del teorema 9.4. Por otra parte, el inciso (ii) se sigue de la proposición 4.1. $\blacksquare$

9.8 COROLARIO

Si G, K son grupos finitos tales que: $\Omega(G) \cong \Omega(K)$, entonces $|G| = |K|$.

Demostración: Sea $f : \Omega(G) \longrightarrow \Omega(K)$ un isomorfismo de anillos. Entonces f se extiende de manera única a un isomorfismo $\bar{f} : \Omega_{\mathbb{Q}}(G) \longrightarrow \Omega_{\mathbb{Q}}(K)$.

Si $x \in \Omega_{\mathbb{Q}}(G)$, se define el *orden de* x como: $Ord(x) := \min\{n \in \mathbb{N}^+ : n\, x \in \Omega(G)\}$, este mínimo existe pues el producto de los denominadores de los factores de x multiplicado por x está en $\Omega(G)$. Ademas $Ord(e_{G,H})$ divide a $|N_G(H)|$. De esto, el orden de cada idempotente divide al orden del grupo correspondiente. Además, $\bar{f}$ manda idempotentes primitivos en idempotentes primitivos. Los ordenes son invariantes bajo el isomorfismo $\bar{f}$. Notemos además, que el orden del idempotente $e_{G,1} = (1/|G|)G/1$ es, claramente, el orden de G. Por esto $|G| = |K|$. ∎

B I B L I O G R A F I A

T. Tom Dieck, "Transformation Groups and representation Theory", *Lectures Notes in Mathematics No. 766*, Springer-Verlag, Berlin, 1979.

T.Yoshida, "Idempotents of Burnside Rings and Dress Induction Theorem", *Jurnal of Algebra* 80, 90-105(1983).

J.Thévenaz "Isomorphic Burnside Rings", *Communications in Algebra,* 16(9),1945-1947 (1988).

J.Thevenaz & C. Kratzer "Fonction de Möbius d'un groupe fini et anneau de Burnside", *Comment Math Helvetici* 59 (1984) 425-434

E.H.Boorman. "S-operation in representation theory", *Trans. Amer. Math. Soc.* 205 (1975) 127-149

I. Morris & C.B. Wensley "Adams operations and λ-operations in β-rings, *Discrete Math.* 50 (1984) 253-270

N.W.Rymer "Power operations on the Burnside ring", *J. London Math. Soc.* 15 (1977) 75-80.

C.Siebeneicher "λ-Ringstrukturen auf dem Burnsidering der Permutationsdarstellugen einer endlichen Gruppe", *Math. Z.* 146 (1976) 223-238.

E. Vallejo "Polynomial operations from Burnside rings to representation functors". *Journal of pure and Applied Algebra,* 1990.

E.Kunz "Introduction to Commutative Algebra and Algebraic Geometry". *Birkhäuser,* 1985.