Universidad de Valparaíso

Facultad de Ciencias

Departamento de Matemáticas

Álgebra de Solomon

Tesis presentada por **Ricardo Guajardo Flores**
para obtener el grado de Licenciado en Matemática.

Profesor Guía: Dr. Daniel Jiménez B.

Valparaíso, 2010.

Índice general

Simbología:

Símbolo	**Significado**
$\amalg$	Union disjunta
$\| \ \|$	Cardinalidad
$\mathbb{K}$	Cuerpo de caracteristica 0
V	$\mathbb{K}-$ espacio vectorial
$GL(V)$	Grupo de transformaciones lineales invertibles de V en V
$O(V)$	Grupo ortogonal
(W,S)	Sistema de Coxeter
c_S	Producto de todos los elementos de S en algún orden fijo
$W_J \ ; \ J \subseteq S$	Subgrupo parabólico estándar de W
w_V	Representación de w como transformación lineal de V en V
$W \diagup W_J$	$\{wW_J \mid w \in W\}$
$W_J \diagdown W$	$\{W_J w \mid w \in W\}$
$W_J \diagdown W \diagup W_{J'}$	$\{W_J w W_{J'} \mid w \in W\}$
$C(w) = W_J w W_K$	Doble clase que contiene a w
ℓ	Función largo
X_K	Sistema de representantes distinguidos de $W \diagup W_K$
X_J^{-1}	Sistema de representantes distinguidos de $W_J \diagdown W$
X_{JK}	Sistema de representantes distinguidos de $W_J \diagdown W \diagup W_K$
X_{JKL}	$\{x \in X_{JK} \mid x^{-1}Jx \cap K = L\}$
a_{JKL}	$\lvert X_{JKL} \rvert$
C_{JKL}	$\{C(x) \mid x \in X_{JKL}\}$
x_J	$\sum_{w \in X_J} w$
(V,ρ)	Representación lineal de grupo
$(\mathbb{C}, \mathbb{1})$	Representación trivial
$Ind_H^G(W,\theta)$	Representación de G inducida por (W,θ) representación de H
χ_ρ	Carácter de la representación de grupo ρ
$\chi_{\mathbb{1}}$	Carácter de la representación trivial
χ_θ^ρ	Carácter de la representación $\rho = Ind_H^G \theta$

φ_J	Carácter de W inducido por el carácter principal de W_J
$Asc(w)$	$\{s \in S \mid \ell(w) < \ell(ws)\}$
$Ann(M)$	Aniquilador del R-módulo M
$Rad(R)$	Radical de Jacobson del anillo R
$\mathbb{Z}[W]$	Anillo de grupo de un grupo de Coxeter W
$\mathbb{Q}[W]$	Álgebra de grupo de un grupo de Coxeter W
$\mathbb{A}$	$\mathbb{Z}$-Módulo generado por los x_J
$\mathbb{B}$	$\mathbb{Z}$-Módulo generado por los φ_J
$\mathbb{A}_{\mathbb{Q}}$	Álgebra de Solomon
$\mathbb{B}_{\mathbb{Q}}$	Álgebra de caracteres generada por los φ_J

Introducción:

El objetivo de este trabajo es construir el álgebra de Solomon para los grupos finitos de Coxeter, la cual es una *álgebra* sobre el cuerpo de los números racionales $\mathbb{Q}$, esta álgebra es una subalgebra del álgebra de grupo $\mathbb{Q}[W]$ de un grupo de Coxeter W. Siendo más preciso, el álgebra de Solomon $\mathbb{A}_{\mathbb{Q}} = \sum \mathbb{Q}x_J$ de un sistema finito de Coxeter (W, S) de rango n, es una 2^n-dimensional $\mathbb{Q}$-subálgebra del álgebra de grupo $\mathbb{Q}[W]$, generada por $\{x_J : J \subseteq S\}$, donde los elementos x_J son definidos en el capítulo 4.

El álgebra de Solomon fue introducida primeramente por Louis Solomon en 1976 [1], después que el notara una curiosa propiedad de ciertos elementos en el álgebra de grupo de un grupo de Coxeter, Solomon definió esta álgebra en términos de un sistema de representantes distinguidos (de largo mínimo) de los subgrupos parabólicos estándar de W. El probó que esos elementos forman una subálgebra y se multiplican acorde a la fórmula de Mackey para el producto de los caracteres φ_J inducidos por las representaciones triviales de los parabólicos estándar de W. Esto estableció un homomorfismo de anillos desde $\mathbb{A}_{\mathbb{Q}}$ al anillo de los caracteres inducidos φ_J, llamado el homomorfismo de Solomon, que se extiende a un homomorfismo de $\mathbb{Q}$-álgebras.

El tema principal de esta tesis está en el último capítulo, pero involucra variados conceptos que son desarrollados en los capítulos previos y están desarrollados con el fin de obtener la demostración del resultado principal. En el primer capítulo de este trabajo vemos las nociones básicas de estructuras algebraicas, es decir, grupos, anillos, módulos y álgebras, se presentan sus principales propiedades, teoremas y notaciones, que se usarán en el desarrollo de esta tesis. El segundo capítulo presenta la teoría de representaciones de grupos finitos, representación inducida y caracteres. En el tercer capítulo se estudian los sistemas de Coxeter finitos (W, S), y en particular los subgrupos parabólicos estándar W_J ; $J \subseteq S$ y a partir de ellos se construyen los elementos x_J como una suma formal de elementos de un sistema de representantes de las clases laterales, este sistema de representantes se obtiene usando la función largo y en cada clase lateral se escoge el elemento de largo mínimo, además se establece la correspondencia de los sistema de Coxeter finitos con los grupos de reflexiones en un espacio euclidiano. Finalmente en el cuarto capítulo se construye el álgebra de

Solomon $\mathbb{A}_{\mathbb{Q}}$. Mediante una secuencia de lemas se demuestra el Teorema de Solomon el cual define el producto de tal álgebra. Después se establece el homomorfismo de $\mathbb{Q}$-álgebras $\theta_{\mathbb{Q}}$ desde el álgebra de Solomon $\mathbb{A}_{\mathbb{Q}}$ al álgebra de caracteres principales $\mathbb{B}_{\mathbb{Q}}$ llamado homomorfismo de Solomon, tal homomorfismo se obtiene del hecho de que el $\mathbb{Z}$-módulo de Solomon $\mathbb{A}$ es libre, entonces existe θ el homomorfismo de $\mathbb{Z}$-módulos de $\mathbb{A}$ a $\mathbb{B}$, el cual mediante el producto tensorial se extiende a $\theta_{\mathbb{Q}}$. Luego a dicho homomorfismo se le calcula el kernel, y por el segundo Teorema de Solomon, se tiene que tal kernel coincide con el radical de Jacobson del anillo $\mathbb{A}_{\mathbb{Q}}$.

Capítulo 1

Estructuras Algebraicas

En esta tesis se usan conceptos matemáticos y estructuras algebraicas tales como grupos, anillos y módulos. Este capítulo incluye solamente los resultados que permiten entender el desarrollo de este trabajo.

1. Grupos

Definición 1. *Un grupo es un conjunto no vació G, con una operación binaria*

$$\begin{array}{rccc} * : & G \times G & \to & G \\ & (g,h) & \rightsquigarrow & g*h, \end{array}$$

tal que satisface:

i) Para todo $g,h,k \in G$ tenemos que $(g*h)*k = g*(h*k)$.
ii) Existe un único $e \in G$, tal que para todo $g \in G$ entonces se tiene $g*e = e*g = g$ El elemento e es llamado elemento neutro de G.
iii) Para todo $g \in G$, existe un único $h \in G$ tal que $g*h = h*g = e$, al elemento h se le dice inverso de g, y se denota por $h := g^{-1}$ ó $(-g)$ si es un grupo con la operación multiplicación o la operación adición respectivamente.

Además G es un grupo abeliano si cumple la propiedad conmutativa, es decir, para todo $g,h \in G$ entonces se tiene $g*h = h*g$.

Por ejemplo: $(\mathbb{R},+)$, $(\mathbb{Z},+)$, $(\mathbb{Z}_n,+)$, $(\mathbb{R}^*,\cdot)$, $(U(\mathbb{Z}_n),\cdot)$, $(\mathbb{Q}^*,\cdot)$, $(\{1,-1\},\cdot)$, $(\mathbb{Z}_p^*,\cdot)$ y $(S_n,\circ)$ son algunos grupos conocidos, donde $U(\mathbb{Z}_n)$ es el grupo de los elementos invertibles en $\mathbb{Z}_n$ bajo la multiplicación y p es un número primo.

En el grupo G, se define la potencia de g por $g^0 = e,\ g^{n+1} = g^n g,$ y $g^{-n} = (g^{-1})^n$ donde $n \in \mathbb{N}$, y se cumplen las siguientes propiedades.

PROPIEDADES 2. *Para todo $g, h \in G$, se tiene:*

1. $(g^{-1})^{-1} = g$.
2. $(gh)^{-1} = h^{-1}g^{-1}$.
3. $g^{m+n} = g^m g^n$ *para todo* $n, m \in \mathbb{Z}$.
4. $(g^n)^m = g^{nm}$ *para todo* $n, m \in \mathbb{Z}$.

Cualquier subconjunto H no vació de G, que cumpla las cuatro propiedades de grupo con la misma operación binaria de G, se dice que es un subgrupo de G y se denota $H \leq G$, podemos comprobar que $\{e\}$ es un subgrupo de G, llamado *grupo trivial*. También es fácil probar que si $K \leq H$ y $H \leq G$ entonces $K \leq G$, y que la intersección arbitraría de subgrupos de G es un subgrupo de G.

PROPOSICIÓN 3. *Sean G un grupo y H un subconjunto no vacío de G. Entonces H es un subgrupo de G si, y sólo si, para todo $g, k \in H$ se tiene que $gk^{-1} \in H$.*

Si X es un subconjunto del grupo G, entonces se define $\langle X \rangle$ como la intersección de todos los subgrupos de G que contienen a X y por lo anterior es un subgrupo de G llamado *subgrupo de G generado por X*, si X es un conjunto finito ($X = \{x_1, x_2, ..., x_n\}$) entonces el subgrupo generado por X se dice finitamente generado.

DEFINICIÓN 4. *Sea G un grupo, se dice que G es un grupo finito si, y sólo si, el cardinal del conjunto G es finito, en caso contrario se dice que el grupo es infinito. Si G es un grupo finito, se dice que el orden de G es n si el cardinal de G es n, y se denota $|G| = n \in \mathbb{N}$.*

Por ejemplo tenemos que $|S_n| = n!$, $|\mathbb{Z}_n| = n$ y $|U(\mathbb{Z}_n)| = \varphi(n),$ (*φ es la función de Euler*).

TEOREMA 5. *Sean G un grupo finito, y $H \leq G$, entonces $|H|$ divide a $|G|$.*

Sea $g \in G$, se dice que el orden de g es n si, y sólo si, $n \neq 0$ es el menor número natural tal que $g^n = e$.

1.1. Clases laterales: Sea $H \leq G$, para $g \in G$, denotamos por gH al conjunto de todos los productos gh con $h \in H$, y decimos que gH es la clase lateral izquierda de H conteniendo a g. Dos elementos g y g' de G se dicen ser congruentes módulo H si ellos pertenecen a la misma clase lateral izquierda, es decir, si $g^{-1}g' \in H$, entonces escribimos:

$$g' \equiv g \ (mod(H)).$$

El conjunto de todas las clases laterales izquierdas se denota por:

$$G/H := \{gH \mid g \in G\}.$$

Si escogemos un único elemento por cada clase lateral izquierda de H, obtenemos un subconjunto R de G llamado *sistema de representantes* de G/H, es decir, que cada $g \in G$ se puede escribir únicamente $g = rh$, donde $r \in R$ y $h \in H$. Con esto tenemos que:

$$G = \coprod_{r \in R} rH,$$

donde $\coprod$ simboliza la union disjunta.

Si $|G| = n$ y $|H| = m$ entonces

$$|G/H| = \frac{n}{m}.$$

El número natural $\frac{n}{m}$ es el *índice* de H en G y es denotado $[G : H]$.

Un resultado análogo se obtiene de las clases laterales derechas $Hg = \{hg \mid h \in H\}$, con $g \in G$.

Si k y g son elementos del grupo G, el conjugado de k por g es el elemento gkg^{-1}. Dos elementos g y g' de G son conjugados si existe algún $x \in G$ tal que $g' = xgx^{-1}$.

Sean G un grupo y H un subgrupo de G, si $g \in G$, el conjugado de H por g es el conjunto $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ que consiste de todos los elementos conjugados de H por g. Dos subgrupos K y H de G, son conjugados en G si $K = gHg^{-1}$, para algún $g \in G$.

PROPOSICIÓN 6. *Sea H un subgrupo cualquiera de G, entonces cualquier conjugado gHg^{-1} es también un subgrupo de G.*

Sea N un subgrupo de G, se dice que N es un *subgrupo normal* de G si, y sólo si, $gN = Ng$ para todo $g \in G$, o equivalentemente que $gNg^{-1} \subseteq N$ para todo $g \in G$, y se denota por $N \trianglelefteq G$. Todo grupo G tiene al menos dos subgrupos normales, que son $\{e\}$ y G. También se tiene que todos los subgrupos de un grupo abeliano son normales.

TEOREMA 7. *Si $N \trianglelefteq G$, entonces el conjunto G/N es un grupo con la operación binaria definida por:*

$$(gN)(g'N) = (gg')N.$$

Si $N \trianglelefteq G$, entonces G/N es llamado *grupo cociente* con la operación binaria definida en el teorema anterior, el elemento neutro es $eN = N$ y el elemento inverso de $gN \in G/N$ es $g^{-1}N$. Además se tiene que si G es un grupo abeliano, entonces G/N también lo es.

EJEMPLO 1. *Sea $\mathbb{Z}$ el grupo de los números enteros con la adición, el subgrupo $n\mathbb{Z}$ de $\mathbb{Z}$ es normal, pues es abeliano, luego $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ es un grupo con la adición de orden n, conocido como el grupo de los enteros módulo n.*

1.2. Homomorfismos: Sean $(G, \cdot)$ y $(K, *)$ dos grupos, y $f : G \to K$ una función. Se dice que f es un homomorfismo de grupo si, y sólo si:

$$(\forall\, g \in G)\,(\forall\, h \in G)(f(g \cdot h) = f(g) * f(h)).$$

El conjunto de todos los homomorfismos del grupo G al grupo K se denota:

$$Hom(G, K) := \{f : G \to K \mid f \text{ es un homomorfismo de grupo}\}.$$

Si $f \in Hom(G, K)$, entonces decimos que f es un monomorfismo si f es inyectivo, que f es un epimorfismo si f es epiyectiva y f es un isomorfismo si f es biyectiva. A f se le dice endomorfismo si $f \in End(G) := Hom(G, G)$ y automorfismo si $f \in End(G)$ y es biyectiva.

La función del grupo G al grupo K que envía todos los elementos de G en el elemento neutro de K, es decir, que para todo $g \in G$ la función f cumple que $f(g) = e_K$ es un homomorfismo de grupo, y es llamado *homomorfismo trivial* de G a K.

El conjunto de los automorfismos de un grupo G se denota:

$$Aut(G) := \{f \in End(G) \mid f \text{ es biyectiva}\}.$$

Si ϕ y $\psi \in Aut(G)$, tenemos que su composición $\phi \circ \psi \in Aut(G)$, con esta operación binaria $Aut(G)$ es un grupo, cuyo elemento neutro es la identidad Id, es decir, $Id(g) = g$ para todo $g \in G$.

Decimos que los grupos G y K son isomorfos si, existe un isomorfismo $f : G \to K$, y se denota por $G \cong K$.

Definición 8. *Sea $f \in Hom(G, K)$.*
El Kernel de f es:

$$Ker(f) := \{g \in G \mid f(g) = e_K\}.$$

y la Imagen de f es:

$$Im(f) := \{k \in K \mid (\exists\, g \in G)\,(f(g) = k)\,\} = f(G).$$

Si $f \in Hom(G, K)$ entonces $f(e) = e$ y $f(g^{-1}) = f(g)^{-1}$ para todo $g \in G$, esto permite verificar que $Ker(f)$ es un subgrupo normal de G y $Im(f)$ es un subgrupo de K.

Teorema 9. Teorema del homomorfismo
Si G y K son grupos y $f : G \to K$ es un homomorfismo de grupo, entonces existe un único isomorfismo $\widetilde{f} : G/Kerf \to Im(f)$ tal que $f = \widetilde{f} \circ \eta$ donde $\eta : G \to G/Ker(f)$ dada por $\eta(g) = g(Ker(f))$. Con esto se tiene que:

$$G/Ker(f) \cong Im(f).$$

Teorema 10. *Si X es un conjunto no vacío, entonces existe un grupo $F(X)$ generado por X tal que satisface:*

Para todo grupo G y $f : X \to G$ una función, entonces existe un único homomorfismo de grupos $\overline{f} : F \to G$ tal que $\overline{f} \circ i = f$, donde $i : X \hookrightarrow F$ es la función inclusión.

El grupo $F(X)$ es llamado el grupo libre sobre el conjunto X.

COROLARIO 11. *Todo grupo G es la imagen homomorfica de un grupo libre.*

DEFINICIÓN 12. *Sea G un grupo, se dice que el par $\langle X|Y\rangle$ es una presentación de G si, y sólo si, $G \cong F/N$, donde F es el grupo libre sobre X y N es el subgrupo normal minimal de F generado por Y.*

EJEMPLO 2. *Una presentación del grupo $\mathbb{Z}_n$ de los enteros módulo n es $\langle \{b\} \mid \{b^n\} \rangle$.*

2. Anillos y Módulos

2.1. Anillos.

DEFINICIÓN 13. *Un anillo es un conjunto no vació R junto con dos operaciones binarias (la adición $+$ y la multiplicación $\cdot$) tal que $(R,+)$ es un grupo abeliano, asociativo con la multiplicación, es decir,*

$$a(bc) = (ab)c \text{ para todo } a,b,c \in R,$$

y cumple la propiedad distributiva de izquierda y derecha, esto es:

i) $a(b+c) = ab + ac \quad$ *para todo* $\quad a,b,c \in R.$
ii) $(a+b)c = ac + bc \quad$ *para todo* $\quad a,b,c \in R.$

Se dice que este anillo es abeliano si sus elementos conmutan bajo la multiplicación esto es que $ab = ba$ para todo $a,b \in R$, y decimos que R es un anillo con unidad *si contiene un elemento 1_R tal que $1_R a = a1_R = a$, para todo $a \in R$.*

El conjunto de los números enteros $\mathbb{Z}$ es anillo abeliano con unidad.

DEFINICIÓN 14. *Sean G un grupo y R un anillo. El* anillo de grupos *de G sobre R, es un anillo, denotado por $R[G]$, en el cual sus elementos son de la forma: $\sum_{i=1}^{n} r_{g_i} g_i$ y sus operaciones son:*

1. $\sum_{i=1}^{n} r_{g_i} g_i + \sum_{i=1}^{n} s_{g_i} g_i := \sum_{i=1}^{n} (r_{g_i} + s_{g_i}) g_i$.
2. $(\sum_{i=1}^{n} r_{g_i} g_i)(\sum_{j=1}^{m} s_{h_j} h_j) := \sum_{i=1}^{n} \sum_{j=1}^{m} (r_i s_j)(g_i h_j)$.

Notamos que $(r_i s_j)$ es el producto en R y $(g_i h_j)$ en G.

$R[G]$ es conmutativo si R y G lo son, y si R es un anillo con unidad $R[G]$ también lo es, vemos que $1_{R[G]} = (1_R)e$, donde e es el elemento neutro de G.

Sean R un anillo y S un subconjunto no vació de R. Si S es un anillo con las mismas las operaciones de adición y multiplicación de R, se dice que S es un *subanillo* de R. Si I es un subanillo de R y si I satisface la siguiente propiedad:

$$\text{Para todo } r \in R \text{ y para todo } x \in I \text{ entonces } rx \in I.$$

Entonces I es llamado *ideal izquierdo*, y si I satisface que:

$$\text{Para todo } r \in R \text{ y para todo } x \in I \text{ entonces } xr \in I.$$

Entonces I llamado *ideal derecho*.

Si I es un ideal izquierdo y un ideal derecho, entonces I es llamado simplemente *ideal* del anillo R.

Un anillo R tiene al menos dos ideales, los cuales son R y $\{0\}$, también se tiene que la intersección arbitraria de ideales R es también un ideal de R. Un ideal M de un anillo R se dice maximal si $M \neq R$ y para todo ideal N de R tal que $M \subset N \subset R$ se tiene $N = M$ o $N = R$.

Si I es un ideal de R, dado que R es un grupo abeliano con la adición, podemos construir el grupo cociente R/I el cual es aditivo bajo la operación $(r+I)+(r'+I) = (r + r') + I$, para todo $r, r' \in R$.

Teorema 15. *Sean R un anillo y I un ideal de R. Entonces el grupo cociente R/I es un anillo bajo la operación:*

$$(r + I)(r' + I) = (rr') + I.$$

Si R tiene unidad y es abeliano también R/I tiene unidad y es abeliano.

Sean R y S anillos, y $f : R \to S$ una función. Se dice que f es un *homomorfismo de anillos* si, y sólo si:

i) $f(r+s) = f(r) + f(s)$ para todo $r, s \in R$.
ii) $f(rs) = f(r)f(s)$ para todo $r, s \in R$.

Se usa la misma terminología para monomorfismo, epimorfismo, endomorfismo y automorfismo de anillos como en la sección de grupos, ahora por ejemplo un monomorfismo de anillo es un homomorfismo de anillo inyectivo.

Ejemplo 3. *Sean G y H dos grupos multiplicativos y $f : G \to H$ un homomorfismo de grupos. Para todo anillo R, se tiene que:*

$$\begin{array}{rccc} \overline{f}: & R[G] & \longrightarrow & R[H] \\ & \sum_{i=1}^{n} r_i g_i & \rightsquigarrow & \sum_{i=1}^{n} r_i f(g_i), \end{array}$$

es un homomorfismo de anillos.

Teorema 16. *Sea $f : R \to S$ un homomorfismo de anillos, entonces existe un isomorfismo inducido por f desde $R/Ker(f)$ a $Im(f)$, donde $Ker(f) = \{r \in R \mid f(r) = 0_S\}$ y $Im(f) = \{f(r) \mid r \in R\}$.*

2.2. Módulos.

Definición 17. *Sea R un anillo con unidad. Un R-módulo izquierdo es un grupo abeliano aditivo M junto con una función $R \times M \to M$ donde $(r, m) \mapsto rm$, tal que satisface lo siguiente:*

i) $1m = m$ *para todo* $m \in M$.
ii) $r(m+n) = rm + rn$ *para todo* $r \in R$ *y* $m, n \in M$.
iii) $(r+s)m = rm + sm$ *para todo* $r, s \in R$ *y* $m \in M$.
iv) $r(sm) = (rs)m$ *para todo* $r, s \in R$ *y* $g \in M$.

Un R-módulo derecho M es análogo al izquierdo, pero el anillo multiplica por la derecha a M, y diremos solamente que M es un R-módulo si, y sólo si M es un R-módulo izquierdo y derecho a la vez o bien un R-bimódulo.

Ejemplo 4. *Todo grupo abeliano G (aditivo) es un $\mathbb{Z}$-módulo, bajo la acción del anillo $\mathbb{Z}$, dada por:*

$$nm = \underbrace{m + m + ... + m}_{n-veces}.$$

Para todo $n \in \mathbb{Z}$ y $m \in M$.

Ejemplo 5. *Si G es un grupo y R un anillo con unidad, entonces el anillo de grupo $R[G]$ es un R-módulo, bajo la ponderación:*

$$r \sum r_i g_i = \sum (r r_i) g_i.$$

Un R-módulo M es *finitamente generado* por $X \subset M$ si todo elemento de M puede ser escrito como una R-combinación lineal de elementos de algún subconjunto finito X de M, es decir, si $m \in M$ entonces $m = r_1 x_1 + ... + r_k x_k$ para $r_i \in R$ y $x_i \in X$, y se denota $M = \sum Rx$ donde $x \in X$ o bien $M = \langle X \rangle_R$.

Sean M un R-módulo y N un subgrupo de M, se dice que N es un R-submódulo (o solo submódulo) de M si $rn \in N$ para todo $r \in R$ y $n \in N$. Todo R-módulo tiene al menos dos submódulos, el submódulo $\{0\}$ y a sí mismo, el submódulo $\{0\}$ a veces es escrito por 0.

Un módulo que tiene como submódulos únicamente a si mismo y al 0 es un *Módulo Simple*. En particular un subespacio vectorial de un $\mathbb{K}$-espacio vectorial V es un K-submódulo de V.

Si N es un R-submódulo de M, dado que M es un grupo abeliano podemos construir el grupo cociente M/N que es un R-módulo bajo la acción de R dada por $r(m + N) = rm + N$ para $r \in R$ y $m + N \in M/N$, de esta manera el R-módulo M/N es llamado *módulo cociente*.

Sean N y L dos R-submódulos de M, la suma (interna) de N con L es definida como:

$$N + L = \{n + l \mid n \in N,\ l \in L\},$$

la cual es un R-submódulo de G bajo la acción $r(n + l) = rn + rl \ \in \ N + L$ para todo $r \in R$.

Cuando $N \cap L = \{0\}$ se dice que la suma $N + L$ es *directa* y se denota por $N \oplus L$.

La suma directa externa de N con L, es definida por:

$$N \times L = \{(n, l) \mid n \in N, l \in L\},$$

la cual es un R-módulo bajo la acción $r(n, l) = (rn, rl)$, para todo $r \in R$, también escribimos $N \oplus L$ en lugar de $N \times L$.

Sean M y N dos R-módulos. La función $f : M \to N$ es un homomorfismo de R-módulo o un R-lineal si, y sólo si:

i) $f(m + m') = f(m) + f(m')$; para todo $m, m' \in M$.
ii) $f(rm) = rf(m)$; para todo $r \in R$ y $m \in M$.

Se usa la misma terminología para monomorfismo, epimorfismo, endomorfismo y automorfismo de R-módulos como en la sección de grupos, ahora por ejemplo un epimorfismo R-lineal es un R-lineal epiyectivo.

Dos R-módulos M y N se dicen isomorfos si existe un isomorfismo R-lineal $f : M \to N$, y se escribe $M \cong_R N$.

El kernel y la imagen de un R-lineal $f : M \to N$ se definen análogos al de grupos, y tenemos que $Ker(f) := \{m \in M \mid f(m) = 0\}$ es un submódulo de M y $Im(f) := \{f(m) \mid m \in M\}$ es un submódulo de N.

Con esto el teorema fundamental del homomorfismo de módulos es análogo al de grupos, es decir:

$$M/Ker(f) \cong_R Im(f).$$

Sea M un R-módulo (izquierdo), definimos el aniquilador de M como

$$Ann(M) := \{r \in R \mid rm = 0 \text{ para todo } m \in M\}.$$

Podemos comprobar que es un ideal izquierdo del anillo R.

Sean R un anillo con unidad y M un R-módulo simple, para $m \in M$ no nulo definimos:

$$\begin{array}{rccc} f_m: & R & \to & M \\ & r & \mapsto & rm. \end{array}$$

Tenemos que f_m es un epimorfismo R-lineal y que $Ker(f_m) = Ann(\{m\})$, luego

$$R/Ann(\{m\}) \cong_R M.$$

PROPOSICIÓN 18. *R/I es un R-módulo simple si, y sólo si I es un ideal maximal.*

TEOREMA 19. *Sea R un anillo con unidad, entonces existe un ideal $Rad(R)$ de R tal que:*

1. *$Rad(R)$ es la intersección de todos los aniquiladores de los R-módulos simples.*
2. *$Rad(R)$ es la intersección de todos los ideales maximales de R.*

El ideal $Rad(R)$ es llamado *radical de Jacobson* del anillo R.

EJEMPLO 6.

1. $Rad(\mathbb{Z}) = 0$.
2. $Rad(\mathbb{Z}_8) = 2\mathbb{Z}/8\mathbb{Z}$.
3. *Si $\mathbb{K}$ es un cuerpo entonces $Rad(\mathbb{K}) = 0$.*

TEOREMA 20. *Sea R un anillo, entonces:*

Si I es un ideal de R, entonces $Rad(I) = I \cap Rad(R)$.

LEMA 21. SCHUR'S
Cualquier homomorfismo distinto del nulo entre R-módulos simples es un isomorfismo.

Un módulo M se dice *semisimple* si este es una suma directa de módulos simples.

LEMA 22. *Sea M un R-módulo semisimple, entonces todo submódulo y módulo cociente de M es semisimple.*

Un R-módulo M, se dice *libre* de rango n si, y sólo si,

$$M \cong_R \underbrace{R \times ... \times R}_{n-veces}.$$

TEOREMA 23. *Son equivalentes:*

1. *M es un R-módulo libre de rango n.*
2. *Existe un subconjunto B de M tal que $|B| = n$ que cumple lo siguiente:*
   - *i) M es finitamente generado por B.*
   - *ii) B es linealmente independiente, esto es que para todo $r_i \in R$,*

   $$r_1 m_1 + ... + r_n m_n = 0$$

   implica que $r_i = 0$, donde $m_i \in B$ para todo $i \in \{1, 2, ..., n\}$.
3. *Dado un R-módulo K y una función $f : B \to K$, existe un único homomorfismo de R-módulos $\widetilde{f} : M \to K$ tal que $\widetilde{f} \circ i = f$, donde i es la inclusión, es decir, que el siguiente diagrama conmute:*

$$\begin{array}{ccc} B & \overset{i}{\hookrightarrow} & M \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} & \\ K & & \end{array}$$

EJEMPLO 7. *Todo $\mathbb{K}$-espacio vectorial V es libre de dimensión n, en este caso se dice dimensión en lugar de rango. La dimensión de V se denota $dim(V)$.*

Si $\mathbb{K}$ es un cuerpo, entonces tenemos que la definición de un $\mathbb{K}$-módulo corresponde a la de un $\mathbb{K}$-espacio vectorial. Si V es un espacio vectorial sobre $\mathbb{K}$, entonces el grupo *General Lineal* $GL(V)$ de V se define como el grupo:

$$GL(V) := Aut(V) = \{f \in End(V) \mid f \text{es biyectiva}\},$$

es decir, el grupo formado por los $\mathbb{K}$-lineales biyectivos (transformaciones lineales biyectivas) de V a V, donde la operación binaria es la compuesta de funciones y el elemento neutro es la identidad. Si V es de dimensión n, entonces $V \cong \mathbb{K}^n$, luego tenemos que el grupo $GL(V)$ es isomorfo a $GL(n, \mathbb{K})$, donde $GL(n, \mathbb{K})$ es el grupo multiplicativo de las matrices invertibles de n por n con entradas en $\mathbb{K}$.

DEFINICIÓN 24. *Sean M, N, L tres R-módulos, una función $f : M \times N \to L$ es R-bilineal si las funciones $f_{1,n}$ y $f_{2,m}$ son R-lineales, donde:*

i) $f_{1,n} : M \to L$ *tal que* $m \mapsto f_{1,n}(m) = f(m,n)$ *para cada* $n \in N$.

ii) $f_{2,m} : K \to H$ *tal que* $k \mapsto f_{2,m}(n) = f(m,n)$ *para cada* $m \in M$.

PROPOSICIÓN 25. *Sean M y N dos R-módulos. Entonces existe un R-módulo T y una función R-bilineal $\mu : M \times N \to T$ con las siguientes propiedades:*

1. *Dado cualquier R-módulo L y cualquier función R-bilineal $f : M \times N \to L$, existe una única función R-lineal $\phi : T \to L$ tal que $f = \phi \circ \mu$, esto es que el siguiente diagrama conmute:*

$$\begin{array}{ccc} M \times N & \xrightarrow{\mu} & T \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle \phi} & \\ L & & \end{array}$$

2. *Si existen dos pares (T, μ) y (T', μ') con estas propiedades, entonces existe un único isomorfismo R-lineal $\psi : T \to T'$ tal que $\psi \circ \mu = \mu'$.*

Con esto el R-módulo T es llamado el producto tensorial de M y N, y es denotado $M \otimes_R N$ o simplemente $M \otimes N$ si no hay lugar a confusión. El producto tensorial es generado por los elementos $\mu(m,n)$ los cuales denotamos por $m \otimes n$.

PROPOSICIÓN 26. *Sean M y N dos R-módulos, entonces:*

1. $M \otimes N \cong N \otimes M$.
2. $R \otimes M \cong M$.

PROPOSICIÓN 27. *Sean R un subanillo de S y M un R-módulo, entonces $S \otimes M$ es un S-módulo bajo la acción $s(s' \otimes r) = (ss' \otimes r)$.*

TEOREMA 28. *Sean $f : M \to M'$ y $g : N \to N'$ funciones R-lineales. Entonces existe una única función R-lineal $f \otimes g : M \otimes N \to M' \otimes N'$ tal que:*

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n).$$

3. Álgebras

DEFINICIÓN 29. *Sea $\mathbb{K}$ un cuerpo. Un anillo R es una $\mathbb{K}$-álgebra si, y sólo si, se cumple lo siguiente:*

1. *R es un $\mathbb{K}$-espacio vectorial.*
2. *$k(rs) = (kr)s = r(ks)$ para todo $r, s \in R$ y para todo $k \in \mathbb{K}$.*

Ejemplo 8. *$\mathbb{K}$ es una $\mathbb{K}$-álgebra.*

Ejemplo 9. *Si $M_n(\mathbb{K})$ es el anillo de matrices de orden $n \times n$, entonces $M_n(\mathbb{K})$ es una $\mathbb{K}$-álgebra, pues el escalar actúa sobre las matrices multiplicando a cada coeficiente de la matriz, es decir, si $(a_{ij}) \in M_n(\mathbb{K})$ entonces $\alpha(a_{ij}) = (\alpha a_{ij})$, para todo $\alpha \in \mathbb{K}$.*

Ejemplo 10. *$\mathbb{C}$ es una $\mathbb{R}$-álgebra.*

Definición 30. *Sea G un grupo y $\mathbb{K}$ un cuerpo, entonces el anillo de grupo $\mathbb{K}[G]$ es llamado el* álgebra de grupo *de G sobre $\mathbb{K}$, y es una $\mathbb{K}$-álgebra bajo la acción dada por:*

$$k(\sum \alpha_i g_i) = \sum (k\alpha_i) g_i,$$

donde $k, \alpha_i \in \mathbb{K}$ y $g_i \in G$.

Si H es un subgrupo de G, entonces $\mathbb{K}[H]$ es un subanillo de $\mathbb{K}[G]$.

Sea R una $\mathbb{K}$-álgebra, una $\mathbb{K}$-subálgebra S de R, es un subanillo de R y es un $\mathbb{K}$-submódulo.

Un *ideal de álgebra* de la $\mathbb{K}$-álgebra R, es un ideal del anillo R que también es un $\mathbb{K}$-módulo.

Se dice que la $\mathbb{K}$-álgebra R es *simple* si sus únicos ideales son R y el $\{0\}$.

Se dice que la $\mathbb{K}$-álgebra R es semisimple si todos los R-módulos distintos del módulo $\{0\}$ son semisimples.

Lema 31. *La $\mathbb{K}$-álgebra R es semisimple si, y sólo si, el R-módulo R es semisimple.*

Un homomorfismos de $\mathbb{K}$-álgebras es un homomorfismo de anillos $\mathbb{K}$-lineal, es decir, si R y S son dos $\mathbb{K}$-álgebras, entonces la función $\psi : R \to S$ es un homomorfismo de álgebras si, y sólo si, para todo r y $r' \in R$ y todo $k \in \mathbb{K}$, se satisface lo siguiente:

i) $\psi(r + r') = \psi(r) + \psi(r')$.
ii) $\psi(rr') = \psi(r)\psi(r')$.
iii)$\psi(kr) = k\psi(r)$.

El $Ker(\psi) := \{r \in R \mid \psi(r) = 0\}$ es un ideal de álgebra de R y $Im(\psi) := \{\psi(r) \mid r \in R\}$ es un ideal de álgebra de S, con esto se mantiene el teorema del homomorfismo para álgebras, es decir, $R/Ker(\psi)$ es isomorfo a $Im(\psi)$.

Capítulo 2

Representaciones de Grupos Finitos

En este capítulo, $\mathbb{K}$ es un cuerpo de característica 0, G un grupo finito, V un $\mathbb{K}$-espacio vectorial de dimensión n y $GL(V)$ el grupo General Lineal sobre $\mathbb{K}$.

1. Representaciones Lineales de Grupos Finitos

Definición 32. *Sea G un grupo. Una representación lineal (V, ρ) de G es un homomorfismo ρ del grupo G al grupo $GL(V)$, es decir:*

$$\begin{array}{rccc} \rho: & G & \longrightarrow & GL(V) \\ & g & \rightsquigarrow & \rho(g) := \rho_g \end{array}$$

tal que $\rho_{gh} = \rho_g \rho_h$, para todo $g, h \in G$.

Se dice que el grado de la representación (V, ρ) es la dimensión de V.

Sea (V, ρ) una representación lineal de G. Un subespacio vectorial W de V se dice *estable* bajo G si, y sólo si, $\rho_g(W) = W$ para todo $g \in G$, es decir, que para cada $w \in W$ y para cada $g \in G$ se tiene que $\rho_g(w) \in W$.

Definición 33. *Sea $\rho : G \to GL(V)$ una representación lineal del grupo G. Se dice que (W, ρ) es una subrepresentación de (V, ρ) si, y sólo si:*

1. *W es un subespacio vectorial de V.*
2. *W es estable bajo G.*

Si los únicos subespacios estables de V son 0 y V, se dice que (V, ρ) es una *representación irreducible* de G, en caso contrario decimos que es una representación reducible.

TEOREMA 34. *Sea $\rho : G \to GL(V)$ la representación lineal de G en V, y supongamos que W es un subespacio vectorial de V estable bajo G, entonces existe un subespacio vectorial W' de V que es estable bajo G, y además $V = W \oplus W'$.*

1.1. Representación trivial. Sea G un grupo finito, la *representación trivial de G* es un homomorfismo dado por:

$$\begin{array}{rccc} \mathbb{1}: & G & \longrightarrow & GL(\mathbb{C}) \\ & g & \rightsquigarrow & \mathbb{1}_g = 1_{\mathbb{C}}. \end{array}$$

Con esto $(\mathbb{C}, \mathbb{1})$ es una representación lineal irreducible, ya que envía todo elemento de G a $1_{\mathbb{C}}$, donde $1_{\mathbb{C}}$ es la identidad de $GL(\mathbb{C})$, y a $GL(\mathbb{C})$ lo podemos identificar con $\mathbb{C}^*$.

1.2. Representación regular. Sean G un grupo de orden n y V un $\mathbb{K}$-espacio vectorial de dimensión n con base $\{e_g \mid g \in G\}$, la *representación regular* (V, ρ) de G es dada de manera que, para cada $g \in G$, se tiene que $\rho_g(e_h) = e_{gh}$, para todo $h \in G$.

Sean $\rho : G \to GL(V_1)$ y $\sigma : G \to GL(V_2)$ dos representaciones del grupo G. Estas representaciones son isomorfas si existe un $\mathbb{K}$-isomorfismo lineal $\phi : V_1 \to V_2$ tal que:

$$\sigma_g \circ \phi = \phi \circ \rho_g \quad \text{para todo} \quad g \in G.$$

DEFINICIÓN 35. *Sean $\rho : G \to GL(V)$ y $\psi : G \to GL(W)$ dos representaciones lineales del grupo G, tenemos que: La representación* suma directa *del grupo G de ρ con ψ es*

$$\rho \oplus \psi : G \to GL(V \oplus W),$$

donde $(\rho \oplus \psi)_g(v \oplus w) = \rho_g(v) \oplus \psi_g(w)$ para todo $g \in G$.

DEFINICIÓN 36. *Sean $\rho : G \to GL(V)$ y $\psi : G \to GL(W)$ dos representaciones lineales del grupo G, tenemos que: La representación* producto tensorial *del grupo G de ρ con ψ es*

$$\rho \otimes \psi : G \to GL(V \otimes W),$$

donde $(\rho \otimes \psi)_g(v \otimes w) = \rho_g(v) \otimes \psi_g(w)$ para todo $g \in G$.

Teorema 37. Maschke
Sea $\rho : G \to GL(V)$ una representación lineal del grupo finito G, y V un $\mathbb{K}$-espacio vectorial, entonces (V, ρ) es reducible y es una suma directa finita de representaciones irreducibles.

Teorema 38. *Toda representación irreducible del grupo G se encuentra en la representación regular.*

Teorema 39. *El número de representaciones irreducibles de un grupo finito G es igual al número de las clases de conjugación de G.*

Sea G es un grupo finito, si consideramos el álgebra de grupo $\mathbb{K}[G]$, podemos ver que hay un correspondencia entre módulos sobre el álgebra de grupo y las representaciones de grupo, es decir, que dada una representación (V, ρ) de G, podemos darle al $\mathbb{K}$-espacio vectorial V estructura de $\mathbb{K}[G]$-módulo, del siguiente modo:

$$\sum_{g \in G} \alpha_g g \cdot v := \sum_{g \in G} \alpha_g \rho_g(v) \quad ; \quad v \in V.$$

Recíprocamente, si V es un $\mathbb{K}[G]$-módulo, entonces V es un $\mathbb{K}$-espacio vectorial, pues $\lambda := \lambda 1_G \in \mathbb{K}[G]$, luego podemos definir la representación (V, ρ) de G, dada por $\rho_g(v) = gv$, para todo $g \in G$ y $v \in V$, donde g es lineal, es decir, $g \in GL(V)$.

Con esto se tiene que el estudio de las representaciones de grupos finitos es equivalente al estudio de módulos sobre algebras de grupo.

2. Representación Inducida

Sean G un grupo y H un subgrupo de G. A partir de una representación lineal de H se construirá una representación del grupo G.

Para lo anterior, sean $\rho : G \to GL(V)$ una representación lineal de G, W un subespacio de V que es estable bajo H y R un sistema de representantes de G/H.

Sea $g \in G$, el espacio vectorial $\rho_g(W)$ depende solamente de las clases laterales izquierdas gH, ya que si $h \in H$, entonces $\rho_{gh}W = \rho_g\rho_h W = \rho_g W$ pues $\rho_h W = W$.

Denotamos el subespacio $\rho_g(W) := W_r$ de V, para cualquier $g \in rH$, donde $r \in R$. Con esto podemos definir lo siguiente:

DEFINICIÓN 40. *La representación $\rho : G \to GL(V)$ es inducida por la representación $\theta : H \to GL(W)$, si V es igual a la suma directa de W_r, $r \in R$, es decir*

$$V = \bigoplus_{r \in R} W_r.$$

Con esto tenemos:

$$dim(V) = \sum_{r \in R} dim(\rho_r(W)) = [G : H]dim(W),$$

y denotamos por $V =: Ind_H^G W$ y $\rho =: Ind_H^G \theta$, cuando (V, ρ) es la representación de G inducida por (W, θ).

Como vimos en la sección anterior, una representación lineal (V, ρ) de un grupo G, es equivalente a un $\mathbb{K}[G]$-módulo, ahora mostraremos que la representación inducida es equivalente a un producto tensorial de módulos, del siguiente modo:

Sean H un subgrupo de G y L un $\mathbb{K}[H]$-módulo, el producto tensorial de $\mathbb{K}[H]$-módulos

$$\mathbb{K}[G] \otimes_{\mathbb{K}[H]} L := L^G,$$

es un $\mathbb{K}[G]$-módulo inducido por L, bajo la acción:

$$\alpha(u \otimes v) = (\alpha u \otimes v),$$

para todo $\alpha, u \in \mathbb{K}[G]$ y $v \in L$.

Con esto, si el $\mathbb{K}[H]$-módulo L es equivalente a (W, θ) entonces el $\mathbb{K}[G]$-módulo L^G es equivalente a (V, ρ), donde $V = Ind_H^G W$ y $\rho = Ind_H^G \theta$.

TEOREMA 41. *Sean H y K dos subgrupos de G, L_H un $\mathbb{K}[H]$-módulo y L_K un $\mathbb{K}[K]$-módulo y para $x \in G$, consideremos el grupo*

$$P := xHx^{-1} \cap K.$$

Entonces $L_H^{(x)} = x \otimes L_H$ y L_K son $\mathbb{K}[P]$-módulos, y el $\mathbb{K}[G]$-módulo inducido

$$(L_H^{(x)} \otimes_{\mathbb{K}[P]} L_K)^G,$$

depende solamente de las dobles clases $HxK \in H\diagdown G\diagup K$ *y*

$$L_H^G \otimes L_K^G = \sum_{x\in R}(L_H^{(x)} \otimes L_K)^G,$$

donde R *es un sistema de representantes del doble cociente* $H\diagdown G\diagup K$.

DEMOSTRACIÓN. Referencia [8], cap 7 sección 44. □

COROLARIO 42. *Sean* $(\mathbb{C}_H, \mathbb{1}_H)$ *la representación trivial de* H *y* $(\mathbb{C}_K, \mathbb{1}_K)$ *la representación trivial de* K*, entonces:*

$$Ind_H^G\mathbb{C} \otimes Ind_K^G\mathbb{C} = \sum_{x\in R} Ind_P^G((x \otimes \mathbb{C}) \otimes \mathbb{C}) = \sum_{x\in R} Ind_P^G\mathbb{C}.$$

Notamos que para este caso particular $x \otimes \mathbb{C} = \mathbb{C}x$.

3. Caracteres

Sean G un grupo y $f : G \to \mathbb{C}$ una función que es invariante bajo las clases de conjugación de G, es decir, $f(gxg^{-1}) = f(x)$ para todo $x, g \in G$. A la función f se le llama *función de clase*. El conjunto de todas las funciones de clase de un grupo es un $\mathbb{Z}$-módulo y más aún es un $\mathbb{K}$-espacio vectorial bajo la suma usual de funciones y $\alpha(f) = \alpha f$.

DEFINICIÓN 43. *Sea* $\rho : G \to GL(V)$ *una representación lineal de un grupo finito* G*. Se define el carácter de la representación* ρ*, como la función:*

$$\begin{array}{rccc} \chi_\rho : & G & \longrightarrow & \mathbb{C} \\ & g & \rightsquigarrow & \chi_\rho(g) = tr(\rho_g) \end{array} .$$

Donde tr *es la función traza.*

DEFINICIÓN 44. *Al carácter* $\chi_{\mathbb{1}}$ *de la representación trivial de* G *se le llama carácter principal de* G*, donde* $\chi_{\mathbb{1}}(g) = 1 \in \mathbb{C}$ *; para todo* $g \in G$.

PROPOSICIÓN 45. *Sea* χ *es el carácter de una representación* (V, ρ) *del grupo* G *de grado* n*, entonces:*

(i) $\chi_\rho(1) = n$.

(ii) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)} \in \mathbb{C}$; $g \in G$, *donde* $\overline{\chi_\rho(g)}$ *es el conjugado de* $\chi_\rho(g)$ *como número complejo.*
(iii) $\chi_\rho(tgt^{-1}) = \chi_\rho(g)$; $g, t \in G$, *es decir,* χ_ρ *es una función de clase.*

PROPOSICIÓN 46. *Si dos representaciones* ρ *y* σ *son equivalentes entonces* $\chi_\rho = \chi_\sigma$.

PROPOSICIÓN 47. *Sean* $\rho : G \to GL(V)$ *y* $\psi : G \to GL(V)$ *dos representaciones del grupo y* χ_ρ, χ_ψ *su respectivos caracteres, entonces se tiene:*

i) $\chi_{\rho\oplus\psi} = \chi_\rho + \chi_\psi$.
ii) $\chi_{\rho\otimes\psi} = \chi_\rho \cdot \chi_\psi$.

PROPOSICIÓN 48. *Sean* H *un subgrupo de* G *y* $\chi_\theta : H \to \mathbf{C}$ *el carácter de la representación* (W, θ) *de* H. *El carácter de la representación* $\rho = Ind_H^G\theta$ *de* G *es:*

$$\begin{array}{rccl} \chi_\theta^\rho : & G & \longrightarrow & \mathbb{C} \\ & g & \rightsquigarrow & \chi_\theta^\rho(g) = \dfrac{1}{|H|}\left(\displaystyle\sum_{\substack{hgh^{-1}\in H \\ h\in G}} \chi_\theta(hgh^{-1})\right). \end{array}$$

EJEMPLO 11. *Sea* $G = S_3$ *el grupo simétrico, con la notación de ciclos tenemos que*

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

Consideremos el subgrupo generado por $\{(1\,2)\}$ *el cual es* $\langle\{(1\,2)\}\rangle \cong S_2 = \{(1), (1\,2)\}$.

Luego, el carácter de S_3 *inducido por el carácter principal de* S_2 *es:*

$$\begin{array}{rccl} \chi_{\mathbb{1}_{S_2}}^\rho : & S_3 & \to & \mathbb{C} \\ & \sigma & \mapsto & \dfrac{1}{2}\left(\displaystyle\sum_{\substack{f\sigma f^{-1}\in S_2 \\ f\in S_3}} \chi_{\mathbb{1}_{S_2}}(f\sigma f^{-1})\right). \end{array}$$

Para $\sigma = (1)$, se tiene que:

$$\begin{aligned}
\chi^{\rho}_{\mathbb{1}_{S_2}}((1)) &= \frac{1}{2}\left(\sum_{\substack{f(1)f^{-1}\in S_2\\ f\in S_3}} \chi_{\mathbb{1}_{S_2}}(f(1)f^{-1})\right)\\
&= \frac{1}{2}\left(\sum_{\substack{ff^{-1}\in S_2\\ f\in S_3}} \chi_{\mathbb{1}_{S_2}}(ff^{-1})\right)\\
&= \frac{1}{2}(1+1+1+1+1+1)\\
&= 3.
\end{aligned}$$

Análogamente calculamos el carácter de los representantes de cada clase de conjugación de S_3 y obtenemos:

σ	$\chi^{\rho}_{\mathbb{1}_{S_2}}(\sigma)$
(1)	*3*
(1 2)	*1*
(1 2 3)	*0*

Proposición 49. *Sean G un grupo, $\rho = Ind_H^G\theta$ y $\rho' = Ind_K^G\theta'$. Si fijamos $x \in G$, entonces el subgrupo $P := x^{-1}Hx \cap K$ induce a una representación de G, cual es $\rho'' = Ind_P^G\theta''$ y además*

$$\chi^{\rho}_{\theta}\chi^{\rho'}_{\theta'} = \sum_{x\in R} a_{HKP}\chi^{\rho''}_{\theta''},$$

donde $a_{HKP} = |\{x \in R \mid x^{-1}Hx \cap K = P\}|$ y R es un sistema de representantes del doble cociente $H\backslash G/K$.

Demostración. Aplicamos proposición 47 del carácter de la representación producto tensorial, el cual nos muestra que $\chi_{\rho\otimes\rho'} = \chi_\rho\chi_{\rho'}$ donde ρ y ρ' son representaciones de algún grupo, y el teorema 41 del producto tensorial de módulos inducidos. Es decir, si $\rho = Ind_H^G\theta$ y $\rho' = Ind_K^G\theta'$ son representaciones inducidas del grupo G, entonces $\rho \otimes \rho'$ equivale a:

$$L_H^G \otimes L_K^G = \sum_{x\in R}(L_H^{(x)} \otimes L_K)^G.$$

Luego

$$\chi_{\rho\otimes\rho'} = \chi_\theta^\rho \chi_{\theta'}^{\rho'} = \sum_{x\in R} a_{HKP}\chi_{\theta''}^{\rho''},$$

donde $\rho'' = Ind_P^G\theta''$ y $P = x^{-1}Hx \cap K$. $\square$

Capítulo 3

Sistemas de Coxeter

1. Sistemas de Coxeter

DEFINICIÓN 50. *El par (W, S) es llamado sistema de Coxeter finito si, y sólo si, el grupo W tiene una presentación:*

$$W = \langle\, S \mid (ss')^{m_{ss'}} \,\rangle,$$

donde $m_{ss} = 1$ y $m_{ss'} \in \{2, 3, 4, ...\}$ si $s \neq s'$.

El grupo W es llamado grupo de Coxeter y el orden de S es llamado el rango de W.

En particular, la relación $m_{ss} = 1$ afirma que cada $s \in S$ es una involución, es decir, que $(ss)^1 = s^2 = 1$. También notamos que:

$$m_{ss'} = 2 \Leftrightarrow ss'ss' = 1 \Leftrightarrow ss' = s's.$$

Se dice que (W, S) y (W', S') son isomorfos si existe un isomorfismo de grupo

$$f : W \to W',$$

que envíe S a S'.

El sistema de Coxeter (W, S) es reducible si $W = W_1 \times W_2$ y $S = S_1 \coprod S_2$, tal que los S_i son distinto del vació y generan los W_i formando los sistemas de Coxeter (W_i, S_i) con $i \in \{1, 2\}$. En otro caso, se dice que el sistema de coxeter es irreducible.

EJEMPLO 12. *El grupo Diedral es un grupo de Coxeter de rango 2, pues tiene una presentación:*

$$D_n = \langle\, s_1, s_2 \mid s_1^2 = s_2^2 = (s_1 s_2)^n = 1 \,\rangle.$$

EJEMPLO 13. *El grupo de las simetrías del cubo B_3 es un grupo de Coxeter de rango 3, pues:*

$$B_3 = \langle s_1, s_2, s_3 | (s_1s_2)^3 = (s_1s_3)^4 = (s_2s_3)^3 = 1 \ ; \ s_1^2 = s_2^2 = s_3^2 = 1 \rangle.$$

Este grupo de orden 48 actúa en $\mathbb{R}^3$, permutando los vertices del cubo, es decir:

$$B_3 = \{ f \in O(\mathbb{R}^3) \,|\, f\{(\pm 1, \pm 1, \pm 1)\} = \{(\pm 1, \pm 1, \pm 1)\}\},$$

donde $O(\mathbb{R}^3) = \{T \in Aut(\mathbb{R}^3) \mid \forall \ x, y \in \mathbb{R}^3, \ B(T(x), T(y)) = B(x, y) \ \}$ y B es el producto interno sobre $\mathbb{R}^3$.

EJEMPLO 14. *El grupo simétrico $S_n = Biy(\{1, 2, ..., n\})$ es un grupo de Coxeter de rango $n-1$, pues tiene como conjunto generador $S = \{(i \ i+1) \,|\, 1 \leq i < n\}$, entonces los elementos $s_i := (i \ i+1)$, satisfacen las siguientes relaciones*

$$s_i^2 = 1, \ s_is_j = s_js_i \ con \ |i-j| > 1 \ y \ s_is_{i+1}s_i = s_{i+1}s_is_{i+1} \ \ \forall \, i, j,$$

es decir, una presentación de S_n es:

$$S_n = \langle S \mid s_i^2 = 1, \ s_is_j = s_js_i \ con \ |i-j| > 1 \ y \ s_is_{i+1}s_i = s_{i+1}s_is_{i+1} \ \ \forall \, i, j \rangle.$$

En general los grupos de reflexiones finitos sobre un espacio euclidiano son sistemas de Coxeter junto a su conjunto generador.

2. La Función Largo

Cada $w \in W$ puede ser escrito de la forma $w = s_1s_2...s_r$ con los s_i (no necesariamente distintos) en S. Si r es el menor número natural posible para el cual existen s_i tales que $w = s_1s_2...s_r$, llamamos a r el largo de w, y lo denotamos $\ell(w) = r \in \mathbb{N}$. Es decir, la función largo es definida de la siguiente manera:

$$\begin{array}{rccl} \ell: & W & \to & \mathbb{N} \\ & w & \rightsquigarrow & \ell(w) = r. \end{array}$$

Si $w = s_1s_2...s_r$ y $\ell(w) = r$, esta expresión se dice reducida. Por convención, $\ell(1) = 0$, y cuando $w = s_1s_2...s_r$ es reducida tenemos que $\ell(s_1s_2...s_{r-1}) = r-1$ y $\ell(s_2s_3...s_{r-1}) = r-2$, etc.

Ejemplo 15. *El grupo simétrico de 4 elementos* $S_4 = Biy(\{1,2,3,4\})$ *es generado por las transposiciones* $S = \{(i \;\; i+1) \mid 1 \leq i < 4\}$, *el 4-ciclo* $(1\ 4\ 3\ 2)$ *puede ser escrito usando la mínima cantidad de generadores posibles de la forma* $(3\ 4)(2\ 3)(1\ 2)$ *y con esto se tiene que* $\ell((1\ 4\ 3\ 2)) = \ell((3\ 4)(2\ 3)(1\ 2)) = 3$.

Lema 51. *Sea* (W, S) *un sistema de Coxeter, para todo* $w \in W$ *y* $s \in S$ *se tiene que:*

i) $\ell(w) = 1 \Leftrightarrow w = s \in S$.
ii) $\ell(w) = \ell(w^{-1})$.
iii) $\ell(ww') \leq \ell(w) + \ell(w')$.
iv) $\ell(ww') \geq \ell(w) - \ell(w')$.
v) $\ell(w) - 1 \leq \ell(ws) \leq \ell(w) + 1$.

Demostración.

i) Por definición.

ii) Dado que $w \in W$ entonces si $w = s_1...s_r$ donde $\ell(w) = r$ y $s_i \in S$, tenemos que $w^{-1} = s_r...s_1$, luego $\ell(w) \leq \ell(w^{-1})$, la otra desigualdad se obtiene de $\ell(w^{-1}) \leq \ell((w^{-1})^{-1})$.

iii) si $w = s_1...s_p$ y $w' = s'_1...s'_q$, entonces el producto $ww' = s_1...s_p s'_1 s'_1...s'_q$ tiene largo a los más $p + q$.

iv) Aplicamos parte del lema iii) al par ww', w'^{-1} es decir $\ell(ww'w'^{-1}) \leq \ell(ww') + \ell(w'^{-1})$ pero $\ell(ww'(w'^{-1})) = \ell(w)$ y $\ell((w')^{-1}) = \ell(w')$ reemplazando tenemos $\ell(w) - \ell(w') \leq \ell(ww')$.

v) Usamos partes i) iii) iv) anteriores.

□

Teorema 52. *Sea* $w = s_1...s_r\,(s_i \in S)$ *no necesariamente una expresión reducida. Supongamos existe* $t \in S$ *tal que* $\ell(wt) < \ell(w)$. *Entonces existe un índice* i *para el cual* $wt = s_1...\widehat{s_i}...s_r$ *(omitiendo* s_i*). Si* w *es una expresión reducida entonces el índice* i *es único.*

Teorema 53. Propiedad de cancelación de Matsumoto *Dado* $w \in W$, *si* $w = s_1 s_2...s_r$ *y* $\ell(w) < r$, *entonces existen* $1 \leq i \leq j < r$ *tal que:*

$$w = s_1...\widehat{s_i}...\widehat{s_{j+1}}...s_r.$$

LEMA 54. *Sean (W, S) un sistema de Coxeter, $w \in W$ y $s, s' \in S$.*

Si $\ell(sws') < \ell(sw)$ y $\ell(w) < \ell(ws')$, entonces $sw = ws'$.

3. Subgrupos Parabólicos

DEFINICIÓN 55. *Sean S el conjunto generador del grupo de Coxeter W, y $J \subset S$, entonces definimos el subgrupo parabólico estándar W_J de W como:*

$$W_J := \langle\, J \,\rangle \leq W,$$

como $\varnothing, S \subset S$, entonces se tiene que $W_\varnothing = \{1\} \ \wedge \ W_S = W$.

EJEMPLO 16. *El grupo simétrico $W = S_3 = Biy(\{1, 2, 3\})$, es generado por el conjunto de transposiciones*

$$S = \{(1\ 2), (2\ 3)\}.$$

Consideremos el conjunto

$$2^S = \{\varnothing, \{(1\ 2)\}, \{(2\ 3)\}, S\}.$$

Entonces los subgrupos parabólicos estándares de S_3 son:

1. $W_\varnothing = \{(1)\}$.
2. $W_{\{(1\ 2)\}} = \{(1\ 2),\ (1)\}$.
3. $W_{\{(2\ 3)\}} = \{(2\ 3),\ (1)\}$.
4. $W_S = S_3$.

TEOREMA 56.

i) Para cada $J \subseteq S$. El par (W_J, J) es un sistema de Coxeter.
ii) Sea $J \subseteq S$. Sea $w = s_1 ... s_r$ una expresión reducida con los $s_i \in S$. Si $w \in W_J$ entonces $s_i \in J$ para todo $i \in \{1, ..., r\}$, además $W_J \cap S = J$.
iii) La correspondencia entre $J \rightsquigarrow W_J$ define una función biyectiva entre 2^S y la colección de subgrupos parabólicos estándares W_J de W.

DEMOSTRACIÓN. Referencia [2] capítulo II, sección 5.5. □

4. Representación Geométrica de W

En esta sección veremos que un grupo de Coxeter W tiene una representación como un grupo generado por reflexiones en un espacio euclidiano.

Sean (W, S) un sistema de Coxeter finito de rango n y $V = \mathbb{R}^n$ un $\mathbb{R}$-espacio vectorial con base $\{e_s \mid s \in S\}$ y con producto interno dado por $B : V \times V \to \mathbb{R}$, tal que

$$B(e_s, e_{s'}) \ = \ -cos(\frac{\pi}{m_{ss'}}).$$

Notamos que $B(e_s, e_s) = 1$ y $B(e_s, e_{s'}) \leq 0$ si $s \neq s'$. Representamos a cada generador $s \in S$ como una reflexión en V, la cual es una transformación lineal que envía un vector distinto de cero a su negativo y deja fijo todos los puntos del hiperplano ortogonal al vector.

La geometría sobre V es impuesta de tal manera que el ángulo entre e_s y $e_{s'}$ es compatible con $m_{ss'}$. El vector e_s es ortogonal a un hiperplano

$$H_s = \{v \in V \mid B(e_s, v) = 0\},$$

luego la recta generada por e_s es el complemento ortogonal a H_s, es decir:

$$H_s \oplus \mathbb{R}e_s = \mathbb{R}^n,$$

donde $dim(H_s) \ = \ n - 1$, $dim(\mathbb{R}e_s) = 1$ y $\mathbb{R}e_s = \{re_s \mid r \in \mathbb{R}\}$.

Para cada $s \in S$, definimos la reflexión en $GL(V)$ como $s_V : V \to V$, tal que:

$$s_V(v) = v - 2B(e_s, v)e_s.$$

Con la definición anterior se tiene que $s_V(e_s) = -e_s$ y los elementos del subespacio H_s quedan fijos por s_V. También vemos que $s_V^2 = 1_V$ y que $B(s_V(v), s_V u) = B(v, u)$ para todo $u, v \in V$, esto nos muestra que todo elemento de $GL(V)$ generado por los s_V preserva el producto interno B.

Proposición 57. *Existe un único homomorfismo:*

$$\begin{array}{rccc} \rho : & W & \longrightarrow & GL(V) \\ & s & \mapsto & \rho(s) = s_V. \end{array}$$

Y además, el subgrupo $\rho(W)$ de $GL(V)$ preserva el producto interno B sobre V, o de otro modo, $\rho(W)$ es un subgrupo del grupo ortogonal $O(V)$.

Capítulo 4

Álgebra de Solomon

1. Sistemas de Representantes de Clases Laterales de W

PROPOSICIÓN 58. *Sean (W, S) un sistema de Coxeter finito y $J, K \subseteq S$. Cada doble clase $W_J w W_K \in W_J \backslash W / W_K$ posee un único elemento x de largo mínimo, y además cada elemento en $W_J w W_K$ tiene una expresión de la forma uxv donde $u \in W_J$, $v \in W_K$, tal que:*

$$\ell(uxv) = \ell(u) + \ell(x) + \ell(v).$$

DEMOSTRACIÓN. Supongamos que $x \in W_J w W_k$ es un elemento de largo mínimo m en la doble clase, y sea uxv otro elemento en la doble clase, donde $u \in W_J$ y $v \in W_K$.

Sean u, v y x elementos de W tales que $u \in W_J$ y $v \in W_K$. Si el producto uxv es una expresión reducida, entonces

$$\ell(uxv) = \ell(u) + \ell(x) + \ell(v).$$

Dado que $\ell(x) = m$, entonces debemos tener que $u = 1 = v$ entonces $x = uxv$. Ahora consideremos la otra opción, la cual es que el producto uxv no es una expresión reducida, entonces aplicamos el teorema de la cancelación, obtenemos

$$uxv = u'x'v'.$$

Donde u', x' y v' son expresiones reducidas a partir de u, x y v respectivamente, y mas aún, tenemos por el teorema de cancelación que $u' \in W_J$ y $v' \in W_K$, entonces $x' \in W_J x W_K$ con $\ell(x') \leq \ell(x)$, lo cual es una contradicción pues x es mínimo en la doble clase, entonces $x = x'$ y luego

$$uxv = u'xv'.$$

Por hipótesis tenemos:

$$\ell(u'xv') = m = \ell(x).$$

Entonces $u' = 1 = v'$ y por lo tanto $u'xv' = x$.

Por la propiedad de cancelación de Matsumoto obtenemos que cada elemento de la doble clase $W_J x W_K$ lo podemos expresar en su forma reducida uxv donde $u \in W_J$ y $v \in W_K$, entonces

$$\ell(uxv) = \ell(u) + \ell(x) + \ell(v).$$

□

Esta proposición permite definir un sistema de representante del doble cociente $W_J \backslash W / W_K$, tomando como representante de cada doble clase al elemento de largo mínimo. Lo llamaremos *sistema de representantes distinguidos* y lo escribiremos X_{JK}.

Notación: Sea $w \in W$, denotamos la doble clase de w como

$$C(w) := W_J w W_K \in W_J \backslash W / W_K.$$

Ejemplo 17. *Consideremos $J = \{(1\ 2)\}$ y $K = \{(2\ 3)\}$ subconjuntos de $S = \{(1\ 2), (2\ 3)\}$ conjunto de transposiciones generador del grupo de Coxeter $\mathbf{S}_3$, entonces:*

1. $C((1)) = \{(1), (1\ 2), (1\ 2)(2\ 3), (2\ 3)\}$.
2. $C((1\ 3\ 2)) = \{(2\ 3)(1\ 2), (1\ 2)(2\ 3)(1\ 2)\}$.

por lo tanto $X_{JK} = \{(1), (1\ 3\ 2)\}$, y verifica que $W = C((1)) \coprod C((1\ 3\ 2))$.

Notación: Consideremos X_{JK}, cuando se tiene que $J = \varnothing$, se denota X_K en lugar de $X_{\varnothing K}$, y denotamos $X_J^{-1} = \{x^{-1} \mid x \in X_J\}$.

Proposición 59. *Para cada $w \in W$, existen únicos $x \in X_K$ y $v \in W_K$ tal que $w = xv$.*

Además si $x \in X_K$ y $v \in W_K$ se tiene que $\ell(xv) = \ell(x) + \ell(v)$, y si $x \in X_J^{-1}$ y $u \in W_J$, se tiene que $\ell(ux) = \ell(u) + \ell(x)$.

DEMOSTRACIÓN. Aplicamos la Proposición 58 y el hecho que $W_\varnothing = \{1\}$.

Ahora sean $w \in W$ y $x \in X_J^{-1}$ entonces $x^{-1} \in X_J$, luego $w = x^{-1}u$ donde $u \in W_J$, pero sabemos que $\ell(x^{-1}) = \ell(x)$, entonces la demostración es análoga a la anterior considerando que $X_{J\varnothing} = X_J^{-1}$. □

PROPOSICIÓN 60. $X_{JK} = X_J^{-1} \cap X_K$.

DEMOSTRACIÓN. Sean $x \in X_J^{-1} \cap X_K$ y $w \in C(x) = W_J x W_K$, entonces $w = uxv$ donde $u \in W_J$ y $v \in W_K$. Luego,

$$u^{-1}w = xv \ \text{ y } \ wv^{-1} = ux.$$

Por la Proposición 59 tenemos que

$$\ell(u^{-1}w) = \ell(x) + \ell(v) \ \text{ y } \ \ell(wv^{-1}) = \ell(u) + \ell(x),$$

luego por las propiedades de la función *largo* se tiene que:

$$\ell(x) + \ell(v) \leq \ell(w) + \ell(u) \ \text{ y } \ \ell(u) + \ell(x) \leq \ell(w) + \ell(v),$$

ahora sumando ambas expresiones obtenemos que $\ell(x) \leq \ell(w)$, entonces x es de largo mínimo en la doble clase, por lo tanto $x \in X_{JK}$.

Ahora sean $x \in X_{JK}$ y $w \in W_J x$, entonces $w = ux = ux1 \in W_J x W_K$, donde $u \in W_J$, por Proposición 59 se tiene que $\ell(w) = \ell(u) + \ell(x)$, luego $\ell(x) \leq \ell(w)$, entonces $x \in X_J^{-1}$. Análogamente se tiene que $x \in X_K$, entonces $x \in X_J^{-1} \cap X_K$.

Por lo tanto $X_{JK} = X_J^{-1} \cap X_K$. □

TEOREMA 61. *Sea $x \in X_{JK}$. Entonces*

$$x^{-1}W_J x \cap W_K = W_L, \ \ \textit{donde} \ \ L = x^{-1}Jx \cap K.$$

DEMOSTRACIÓN. Sea $w \in x^{-1}W_J x \cap W_K$, probaremos que $w \in W_L$, y lo haremos mediante inducción sobre $\ell(w)$. La afirmación es clara cuando $\ell(w) = 0$, así que lo haremos para $\ell(w) \geq 1$, siendo así se tiene que $K \neq \varnothing$.

Si $\ell(w) < \ell(ws)$ para todo $s \in K$, entonces se tiene que $w \in W_K \cap X_K$ así que $w = 1$, y quedaría demostrado. Entonces sea $s \in K$ tal que $\ell(w) > \ell(ws)$, como $w \in x^{-1}W_J x$, podemos escribir $xw = vx$ para algún $v \in W_J$.

Dado que $x \in X_{JK} = X_J^{-1} \cap X_K$ y por Proposición 59 tenemos:

$$\ell(vxs) = \ell(xws) = \ell(x) + \ell(ws) < \ell(x) + \ell(w) = \ell(xw) = \ell(vx).$$

Sea $\ell(v) = p$ y $\ell(x) = q$ entonces escribimos

$$v = s_1...s_p \text{ y } x = s_{p+1}...s_{p+q},$$

donde $s_1, ..., s_p \in J$ y $s_{p+1}, ..., s_{p+q} \in S$.

Por la Proposición anterior tenemos $\ell(vx) = \ell(v) + \ell(x)$.

Por Teorema de la cancelación existe un entero j con $1 \leq j \leq p+q$, tal que

$$vxs = s_1...\hat{s_j}...s_{p+q}.$$

Si $j > p$ tenemos:

$$vxs = s_1...s_p...\hat{s_j}...s_{p+q},$$

ahora cancelando v a ambos lados obtenemos:

$$xs = s_{p+1}...\hat{s_j}...s_{p+q},$$

y dado que $C(xs) = C(x)$, se contradice la minimalidad de $\ell(x)$. Esto obliga a que $j \leq p$, así que

$$vxs = s_1...\hat{s_j}...s_p x,$$

y de esta manera $xsx^{-1} \in W_J$. Dado que $s \in W_J$, la Proposición 59 nos dice que:

$$1 + \ell(x^{-1}) = \ell(xs^{-1}) = \ell(x^{-1}xsx^{-1}) = \ell(x^{-1}) + \ell(xsx^{-1}),$$

entonces $\ell(xsx^{-1}) = 1$, luego $xsx^{-1} \in S$, con esto vemos que $xsx^{-1} \in S \cap W_J$, pero por el Teorema 56 de los subgrupos parabólicos tenemos que $xsx^{-1} \in J$ y esto es equivalente a que $s \in x^{-1}Jx$. Por lo tanto $s \in x^{-1}Jx \cap K = L$. Ahora aplicamos hipótesis de inducción sobre el largo de w.

Si $ws \in x^{-1}W_J x \cap W_K$ entonces $ws \in W_L$, de esta manera

$$w = (ws)s \in W_L.$$

Esto completa la inducción y prueba que

$$x^{-1}W_J x \cap W_K \subseteq W_L.$$

Sea $w \in W_L$ donde $L = x^{-1}Jx \cap K$. Luego $w = s_1...s_r$ con $s_i \in x^{-1}Jx$ y $s_i \in K$, para todo $i \in \{1, 2, ..., r\}$. Entonces $w \in W_K$, y además se tiene que:

$$xs_1x^{-1}xs_2x^{-1}...xs_rx^{-1} = xs_1s_2...s_{r-1}s_rx^{-1} \in W_J,$$

lo es equivalente a que $s_1s_2...s_r \in x^{-1}W_Jx$, pero $s_1s_2...s_r = w$, por lo tanto $w \in x^{-1}W_Jx \cap W_K$. □

Observación: Para todo $x \in X_{JK}$ se tiene que, para todo $z \in W$, existe un único $u \in W_J$, tal que $ux \in X_J^{-1}z$.

LEMA 62. *Sean $x \in X_{JK}$, $z \in W$ y u el único elemento de W_J tal que $zx^{-1} \in X_Ju$, entonces:*

$$X_J^{-1}z \cap X_K \cap C(x) = \{ux\} \ ; \ \textit{donde } ux \in X_K,$$

y la intersección es vacía si $ux \notin X_K$.

DEMOSTRACIÓN. Supongamos que $X_J^{-1}z \cap X_K \cap C(x) \neq \varnothing$.

Sea $w \in X_J^{-1}z \cap X_K \cap C(x)$, por la Proposición 58 se tiene que $w = u'xv$, donde $u' \in W_J$, $v \in W_K$ y $\ell(w) = \ell(u') + \ell(x) + \ell(v)$. Si $v \neq 1$, podemos escoger un $s \in K$ con $\ell(vs) < \ell(v)$, entonces

$$\ell(ws) = \ell(u'xvs) < \ell(u') + \ell(x) + \ell(v) = \ell(w),$$

lo que contradice el hecho que $w \in X_K$. De esta manera $v = 1$. Entonces

$$w = u'x \in X_J^{-1}z,$$

lo que equivale a que $zx^{-1} \in X_Ju'$. Por la unicidad de u se tiene que $u = u'$ y luego se tiene que $w = ux$, entonces $X_J^{-1}z \cap X_K \cap C(x) \subset \{ux\}$.

Si $ux \in X_K$, entonces $ux = ux1 \in C(x)$ y por hipótesis $zx^{-1} \in X_Ju$, por lo tanto $\{ux\} \subset X_J^{-1}z \cap X_K \cap C(x)$, esto completa la demostración.

□

LEMA 63. *Sean $s \in S$, $w \in W$ y $x \in X_J$.*

Si $\ell(ws) > \ell(w)$ y $wsw^{-1} \in W_J$, entonces $\ell(xws) > \ell(xw)$.

Demostración. Supongamos lo contrario, es decir que $\ell(xws) \leq \ell(xw)$ cuando $\ell(ws) > \ell(w)$ y $wsw^{-1} \in W_J$. Si $\ell(x) = p$ y $\ell(w) = q$, luego

$$x = s_1...s_p \text{ y } w = s_{p+1}...s_{p+q},$$

donde $s_i \in S$, entonces tenemos:

$$xw = s_1...s_p s_{p+1}...s_{p+q}.$$

Por hipótesis sabemos que existe un entero j con $1 \leq j \leq p+q$, tal que

$$xws = s_1...\hat{s_j}...s_{p+q}.$$

Si $j > p$ entonces $ws = s_{p+1}...\hat{s_j}...s_{p+q}$ contradice la hipótesis $\ell(ws) > \ell(w)$.

Entonces si $1 \leq j \leq p$, se tiene

$$xws = s_1...\hat{s_j}...s_p w \text{ entonces } xwsw^{-1} = s_1...\hat{s_j}...s_p.$$

Dado que $x \in X_J$ y $wsw^{-1} \in W_J$, la Proposición 59 nos da la contradicción, pues:

$$p > \ell(s_1...\hat{s_j}...s_p) = \ell(xwsw^{-1}) = \ell(x) + \ell(wsw^{-1}) > \ell(x).$$

□

Definición 64. *Sean (W, S) un sistema de Coxeter y $w \in W$.*

El conjunto

$$Asc(w) := \{s \in S \mid \ell(ws) > \ell(w)\},$$

es llamado ascendiente de w.

Lema 65. *Sean $s \in S$, $w \in W$ y $w' = sw$. Si $\ell(w') < \ell(w)$, entonces $Asc(w) \subset Asc(w')$.*

Demostración. Supongamos lo contrario, entonces existe $s' \in Asc(w)$ tal que $s' \notin Asc(w')$. De esta manera tenemos:

$$\ell(ws') > \ell(w) > \ell(w') > \ell(w's') = \ell(sws'),$$

así que $\ell(ws') > 1 + \ell(sws')$, esto contradice las propiedades de la función largo.

□

Definición 66. *Sean (W,S) un sistema de Coxeter finito y J,K,L subconjuntos de S, se definen*

$$X_{JKL} := \{x \in X_{JK} \mid x^{-1}Jx \cap K = L\},$$

y

$$C_{JKL} := \{C(x) \mid x \in X_{JKL}\}.$$

Lema 67. *Sean $z \in W$, $L \subset Asc(z)$, $x \in X_{JKL}$ y u el único elemento de W_J tal que $zx^{-1} \in X_J u$.*

Si $w = ux$ entonces $w \in X_J^{-1}z \cap X_K$ y $C(w) = C(x)$.

Demostración. Dado que $u \in W_J$, tenemos que $C(w) = C(x)$ pues

$$w = ux = ux1.$$

Como $zx^{-1} \in X_J u$, entonces $w = ux \in X_J^{-1}z$.

Sólo queda demostrar que $w \in X_K$ y lo haremos por inducción sobre $\ell(z)$.

Para $z = 1$, $x^{-1} \in X_J u$ si, y sólo si, $ux \in X_J^{-1}$, pero por hipótesis $x \in X_J^{-1}$, luego $u = 1$ por unicidad de x, luego $w = x \in X_K$.

Ahora si $\ell(z) > 1$, entonces podemos escoger $s \in S$ fijo, tal que $\ell(sz) < \ell(z)$. Sea $z' = sz$, el lema anterior nos muestra que $Asc(z) \subseteq Asc(z')$ entonces $L \subseteq Asc_(z')$. Por la hipótesis de inducción escribimos $z'x^{-1} = yu' \in X_J u'$, donde $y \in X_J$ y $u' \in W_J$ por inducción $w' \in X_K$, donde $w' = u'x$.

Supongamos que $sy \in X_J$, entonces

$$zx^{-1} = sz'x^{-1} = syu',$$

así que por unicidad de u tenemos que $u = u'$, de esta manera $w = w'$ y queda demostrado. Ahora supongamos que $sy \notin X_J$, es decir existe $s' \in J$ tal que $\ell(sys') < \ell(sy)$. Dado que $y \in X_J$, tenemos $\ell(y) < \ell(ys')$, entonces por Lema 54 obtenemos que $sy = ys'$, y de esta manera

$$zx^{-1} = sz'x^{-1} = syu' = ys'u'.$$

Dado que $s' \in J$ tenemos que $s'u' \in W_J$, luego $u = s'u'$ y de esta manera

$$z = yux = yw \text{ y } w = ux = s'u'x = s'w'.$$

Supongamos que $w \notin X_K$, entonces existe $s'' \in K$ tal que $\ell(ws'') < \ell(w)$. Luego

$$\ell(s'w's'') < \ell(s'w').$$

Pero $w' \in X_K$ así que $\ell(w') < \ell(w's'')$, luego nuevamente el Lema 54 nos dice que $w's'' = s'w'$. Esto puede ser reescrito como $u'xs'' = s'u'x$ y de esta manera

$$s''x^{-1} = x^{-1}(u'^{-1}s'u').$$

Dado que $x^{-1} \in X_J$ y $1 \neq u'^{-1}s'u' \in W_J$ la Proposición 59 nos muestra que no podemos tener $s''x^{-1} \in X_J$, luego existe $\tilde{s} \in J$ tal que $\ell(s''x^{-1}\tilde{s}) < \ell(s''x^{-1})$ y por propiedad de la función largo del inverso, tenemos $\ell(\tilde{s}xs'') < \ell(xs'')$, y por otro lado tenemos que $x^{-1} \in X_J$ y $\tilde{s} \in J$, así que $\ell(x^{-1}) < \ell(x^{-1}\tilde{s})$ es igual a tener que $\ell(x) < \ell(\tilde{s}x)$. Con todo esto podemos volver a aplicar el Lema 54, el cual nos dice $xs'' = \tilde{s}x$.

Ahora usando la hipótesis $L \subseteq Asc(z)$, se tiene que

$$s'' = x^{-1}\tilde{s}x \in x^{-1}Jx \cap K = L \subseteq Asc(z).$$

De esta manera $\ell(z) < \ell(zs'')$. Pero

$$zs'' = yws'' = yw' = ys'w = syw = sz.$$

Así que $\ell(z) < \ell(sz)$, contradiciendo nuestra elección de s. Por lo tanto $w \in X_K$. Esto completa la demostración.

□

Teorema 68. *Sean (W, S) un sistema de Coxeter y J y K subconjuntos de S. Para $w, z \in W$ la aplicación $w \to C(w)$ es una biyección de $X_J^{-1}z \cap X_K$ a $\bigcup_{L \subset Asc(z)} C_{JKL}$.*

Demostración. Sean

$$\begin{array}{rccc} f_z: & X_J^{-1}z \cap X_K & \to & \bigcup_{L \subset Asc(z)} C_{JKL} \\ & w & \mapsto & C(w) \end{array}$$

y $w \in X_J^{-1}z \cap X_K$ y $x \in X_{JK}$ con $C(x) = C(w)$, el Teorema 61 nos dice que $C(x) \in C_{JKL}$ donde $L = x^{-1}Jx \cap K$ y $W_L = x^{-1}W_J x \cap W_K$, sólo queda probar que $L \subseteq Asc(z)$.

Dado que $w \in X_J^{-1}z \cap X_K \cap C(x)$ por el Lema 62 se tiene que que $w = ux$ para algún $u \in W_J$. Sea $s \in L = x^{-1}Jx \cap K$, tenemos que $\ell(w) < \ell(ws)$ pues $w \in X_K$ y $s \in K$. Y además se tiene que

$$wsw^{-1} = uxsx^{-1}u^{-1} \in uJu^{-1} \subseteq W_J.$$

Aplicamos el Lema 63 a zw^{-1} en lugar de x, pues se cumplen todas las hipótesis del lema, luego tenemos:

$$\ell(zs) = \ell(zw^{-1}ws) > \ell(zw^{-1}w) = \ell(z).$$

Esto implica que $L \subseteq Asc(z)$, entonces f_z esta bien definida, es decir

$$Im(f_z) \subseteq \bigcup_{L \subset Asc(z)} C_{JKL}.$$

Sean $w, w' \in X_J^{-1}z \cap X_K$ y supongamos que $C(w) = C(w')$.

Tomando $x \in X_{JK} \cap C(w)$, se tiene que w y $w' \in X_J^{-1}z \cap X_K \cap C(x)$. Luego por el Lema 62 tenemos que

$$|X_J^{-1}z \cap X_K \cap C(x)| \leq 1,$$

entonces $w = w'$, por lo tanto f_z es inyectiva.

Finalmente mostraremos que f_z es epiyectiva. Sea $C \in C_{JKL}$ con $L \subseteq Asc(z)$, y para algún $x \in X_{JKl}$, sean $C = C(x)$ y w el elemento de $X_J^{-1}z \cap X_K$ dado por el Lema 67, entonces $f_z(w) = C(w) = C$, con lo que obtenemos la epiyectividad de f_z, por lo tanto f_z es biyectiva.

□

Corolario 69. *Sea $z \in W$, entonces:*

$$|X_J^{-1}z \cap X_K| = \sum_{L \subseteq Asc(z)} |X_{JKL}|.$$

Demostración. Dado que $X_{JKL} = \{x \in X_{JK} \mid x^{-1}Jx \cap K = L\}$, la igualdad es inmediata por la biyectividad de f, pues las dobles clases son disjuntas. □

Lema 70.

$$z \in X_L \text{ si, y sólo si, } L \subseteq Asc(z).$$

Demostración. $z \in X_L$ si, y sólo si, para todo $s \in L$, $\ell(z) < \ell(zs)$

luego $L \subseteq Asc(z)$.

□

Proposición 71. *Sea (W, S) un sistema de Coxeter finito. Si $K \subseteq S$, sea*

$$x_K = \sum_{w \in X_K} w,$$

entonces:

$$x_J x_K = \sum_{z \in W} |X_J^{-1} z \cap X_K| z.$$

Demostración. Dado que el grupo es finito, tenemos que

$$x_J = w_1 + ... + w_r,$$

con $w_i \in X_J$, para todo $i \in \{1, 2, ..., |J| = r\}$. Y

$$x_K = w'_1 + ... + w'_t,$$

con $w'_j \in X_K$ para todo $j \in \{1, 2, ..., |K| = t\}$. Entonces:

$$x_J x_K = w_1 w'_1 + w_1 w'_2 + ... + w_1 w'_t + w_2 w'_1 + ... + w_r w'_1 + ... + w_r w'_t.$$

Sea $z = w_i w'_j \Leftrightarrow w_i^{-1} z = w'_j$. Ahora el coeficiente de z en $x_J x_K$ es el número de pares (w_i, w'_j), con $w_i \in X_J$ y $w_j \in X_K$, el cual es $|X_J^{-1} z \cap X_K|$. Es decir:

$$x_J x_K = \sum_{z \in W} |X_J^{-1} z \cap X_K| z.$$

□

Teorema 72. Solomon

Sea (W, S) un sistema de Coxeter finito. Si $K, J, L \subseteq S$, sean

$$x_K = \sum_{w \in X_K} w,$$

y a_{JKL} el número de elementos $x \in X_{JK}$ tal que $x^{-1}W_J x \cap W_K = W_L$, entonces:

$$x_J x_K = \sum a_{JKL} x_L.$$

Demostración.

$$\begin{aligned}
\sum a_{JKL} x_L &= \sum_{L \in 2^S} |X_{JKL}| x_L \\
&= \sum_{L \in 2^S} |X_{JKL}| \sum_{w \in X_L} w \\
&= \sum_{L \in 2^S} \sum_{w \in X_L} |X_{JKL}| w \\
&= \sum_{w \in W} \sum_{L \subseteq Asc(w)} |X_{JKL}| w \\
&= \sum_{w \in W} |X_J^{-1} w \cap X_K| w \\
&= x_J x_K.
\end{aligned}$$

□

Ejemplo 18. *Consideremos el sistema de Coxeter (S_3, S) donde $S = \{(1\,2), (2\,3)\}$ y sean $J = \{(1\,2)\}$ y $K = \{(2\,3)\}$ en $2^S = \{\{(1\,2)\}, \{(2\,3)\}, S, \varnothing\}$. Entonces los sistemas de representantes distinguidos de los cocientes izquierdos para cada subgrupo parabólico estándar son:*

1. $X_\varnothing = \{(1), (1\,2), (2\,3), (1\,2\,3), (1\,3\,2), (1\,3)\} = S_3$ *dado que cada clase en* $W/\{(1)\}$ *tiene un único elemento.*
2. $X_J = \{(1), (2\,3), (1\,2\,3)\}$.
3. $X_K = \{(1), (1\,2), (1\,3\,2)\}$.
4. $X_S = \{(1)\}$.

Por el teorema de Solomon tenemos que:

$$x_J x_K = \sum_{L \in 2^S} a_{JKL} x_L,$$

donde

$$a_{JKL} = |X_{JKL}| = |\{x \in X_{JK} \,|\, x^{-1}Jx \cap K = L\}|,$$

y además se tiene que $X_{JK} = X_J^{-1} \cap X_K = \{(1), (1\,3\,2)\}$.

Sea $x \in X_{JK} = \{(1), (1\,3\,2))\}$, *calculando* $x^{-1}\{(1,2)\}x \cap \{(2\,3)\}$, *resulta:*

$$(1)\{(1\,2)\}(1) \cap \{(2\,3)\} = \varnothing.$$
$$(1\,2\,3)\{(1\,2)\}(1\,3\,2) \cap \{(2\,3)\} = \{(2\,3)\} = K.$$

Por lo tanto:

$$\begin{aligned} x_J x_K &= (a_{JKS})x_S + (a_{JKJ})x_J + (a_{JKK})x_K + (a_{JK\varnothing})x_\varnothing \\ &= |X_{JKS}|x_S + |X_{JKJ}|x_J + |X_{JKK}|x_K + |X_{JK\varnothing}|x_\varnothing \\ &= 0x_S + 0x_J + 1x_K + 1x_\varnothing = x_K + x_\varnothing. \end{aligned}$$

Calculamos de manera análoga los otros productos y obtenemos (los de la columna multiplican por la izquierda):

	x_S	x_J	x_K	$x_\varnothing$
x_S	x_S	x_J	x_K	$x_\varnothing$
x_J	x_J	$x_\varnothing + x_J$	$x_\varnothing + x_K$	$3x_\varnothing$
x_K	x_K	$x_\varnothing + x_J$	$x_\varnothing + x_K$	$3x_\varnothing$
$x_\varnothing$	$x_\varnothing$	$3x_\varnothing$	$3x_\varnothing$	$6x_\varnothing$

2. La $\mathbb{Q}$-álgebra de Solomon

El $\mathbb{Z}$-módulo $\sum \mathbb{Z}x_J$ generado por $\{x_J \mid J \in 2^S\}$ es un anillo bajo el producto $x_J x_K = \sum a_{JKL} x_L$ descrito en el teorema de Solomon, y en particular es un subanillo del anillo de grupos $\mathbb{Z}[W]$.

De aquí en adelante denotaremos al $\mathbb{Z}$-módulo $\sum \mathbb{Z}x_J =: \mathbb{A}$.

PROPOSICIÓN 73. *El $\mathbb{Z}$-módulo $\mathbb{A}$ es libre de rango $|2^S|$.*

DEMOSTRACIÓN. Dado que $\mathbb{A}$ es generado por $\{x_J \mid J \in 2^S\}$, sólo queda demostrar que este conjunto generador es linealmente independiente. Podemos caracterizar a X_K como el conjunto de todos los $x \in W$, tal que $\ell(x) < \ell(xs)$ para todo $s \in K$. Sea

$$Y_K = \{y \in W \mid \ell(y) < \ell(ys) \text{ y } \ell(y) > \ell(ys') \text{ para todo } s \in K, s' \in S - K\}.$$

Entonces se tiene que:

$$X_K = \coprod_{K \subseteq J} Y_J.$$

Luego

$$y_K = \sum_{w \in Y_K} w,$$

y con esto tenemos que

$$x_K = \sum_{K \subseteq J} y_J.$$

Luego por la inversión de *Mobious* ([7], pág 440), se tiene que

$$y_J = \sum_{J \subseteq K} (-1)^{|K-J|} x_K \quad \text{donde} \quad (-1)^{|K-J|} \quad \text{es la función de Mobious.}$$

Dado que los Y_J son disjuntos y los elementos y_J son linealmente independientes sobre $\mathbb{Z}$, entonces también lo son los x_J. Por lo tanto $\mathbb{A}$ es libre. □

Consideremos el $\mathbb{Z}$-módulo $C_W = \{f : W \mapsto \mathbb{Z} \mid f(w) = f(zwz^{-1}) \text{ para todo } z, w \in W\}$ de las funciones de clase de W, notamos que los caracteres de una representación de W pertenecen a C_W.

Sea φ_J el carácter de W, inducido por el carácter principal de W_J, el $\mathbb{Z}$-módulo $\sum \mathbb{Z}\varphi_J$ generado por el conjunto $\{\varphi_J \mid J \in 2^S\}$ es un anillo, pues por la Proposición 49 del producto de caracteres inducidos tenemos que $\varphi_J\varphi_K = \sum_{L\in 2^S} a_{JKL}\varphi_L$. En adelante denotaremos $\sum \mathbb{Z}\varphi_J =: \mathbb{B}$.

Dado que $\mathbb{A}$ es libre, existe una función $\mathbb{Z}$-lineal $\theta : \mathbb{A} \to \mathbb{B}$ tal que $\theta(x_J) = \varphi_J$.

PROPOSICIÓN 74. *$\theta : \mathbb{A} \to \mathbb{B}$ es un homomorfismo de anillo.*

DEMOSTRACIÓN. Dado que θ es $\mathbb{Z}$-lineal, tenemos que

$$\theta(x_J + x_K) = \theta(x_J) + \theta(x_K).$$

Sólo queda probar que $\theta(x_Jx_K) = \theta(x_J)\theta(x_K)$.

$$\begin{aligned}
(1) \qquad \theta(x_Jx_K) &= \theta\left(\sum_{L\in 2^S} a_{JKL}x_L\right) \\
(2) \qquad &= \sum a_{JKL}\theta(x_J) \\
(3) \qquad &= \sum a_{JKL}\varphi_L \\
(4) \qquad &= \varphi_J\varphi_K \\
(5) \qquad &= \theta(x_J)\theta(x_K).
\end{aligned}$$

La igualdad (1) se tiene por el Teorema 72 de Solomon, la (2) pues θ es $\mathbb{Z}$-lineal por hipótesis, (4) por la Proposición 49 y por último la tercera y quinta igualdad se tiene por la definición de θ. □

2.1. Álgebra de Solomon. El álgebra de Solomon se obtiene al extender el $\mathbb{Z}$-módulo $\mathbb{A}$ a una $\mathbb{Q}$-álgebra mediante el producto tensorial de módulos, de la siguiente manera:

$$\mathbb{A}_{\mathbb{Q}} := \mathbb{A} \otimes \mathbb{Q} = \sum \mathbb{Q}x_J.$$

Dado que $|S| = n$, el *álgebra de Solomon* $\mathbb{A}_{\mathbb{Q}}$, es una $\mathbb{Q}$-subálgebra de dimensión 2^n del álgebra de grupo $\mathbb{Q}[W]$ del grupo de Coxeter W.

Por lo tanto, podemos identificar a $\mathbb{A}$ con $\mathbb{A} \otimes \mathbb{Z}$ y a $\mathbb{B}$ con $\mathbb{B} \otimes \mathbb{Z}$ subanillos de $\mathbb{A}_{\mathbb{Q}}$ y $\mathbb{B}_{\mathbb{Q}}$ respectivamente. Entonces $\theta_{\mathbb{Q}} = \theta \otimes 1$ es un $\mathbb{Q}$-homomorfismo de $\mathbb{Q}$-álgebras, llamado el *homomorfismo de Solomon* el cual es una extensión de θ.

Lo podemos visualizar en el siguiente diagrama:

$$\begin{array}{rccc} i: & \mathbb{A} & \hookrightarrow & \mathbb{A}_{\mathbb{Q}} \\ & \downarrow \theta & & \downarrow \theta_{\mathbb{Q}} \\ i': & \mathbb{B} & \hookrightarrow & \mathbb{B}_{\mathbb{Q}} \end{array}$$

donde i y i' son inclusiones.

2.2. El Kernel de $\theta_{\mathbb{Q}}$.

Definición 75. *Si J es un subconjunto de S, definimos c_J como el producto de todos los elementos de J, tomados en algún orden fijo. Es decir, si $J = \{s_1, s_2, ..., s_r\}$, entonces*

$$c_J = s_{\sigma(1)} \cdot s_{\sigma(2)} \cdot ... \cdot s_{\sigma(r)},$$

para algún $\sigma \in S_r$.

Lema 76. *Sean c_J y c'_J dos productos de todos los elementos de J, tomados en algún orden fijo, pero con diferente orden uno del otro, entonces c_J y c'_J son conjugados, es decir, pertenecen a la misma clase de conjugación.*

Demostración. Ver Referencia [2], capítulo 1, sección 3.16. □

Definición 77. *Sea*

$$A(x) := \{w \in W \mid Ker(1 - w_V) \supseteq Ker(1 - x_V)\},$$

donde w_V denota la correspondiente transformación lineal sobre el espacio vectorial V de dimensión $|S|$, $1 = 1_V$ denota la transformación lineal identidad y

$$Ker(1 - w_V) = \{v \in V \mid (1 - w_V)(v)\} = \{v \in V \mid w_V(v) = v\}.$$

Es decir, $Ker(1 - w_V)$ son los puntos fijos de w_V.

PROPOSICIÓN 78. *Para todo $x \in W$ se tiene:*

1. *$A(x)$ es un subgrupo de W.*
2. *Si $w \in A(x)$ entonces $A(w)$ es subgrupo de $A(x)$.*
3. *$A(w^{-1}xw) = w^{-1}A(x)w$ para todo $w \in W$.*

DEMOSTRACIÓN.

1. Tenemos que $1 \in A(x)$ pues $Ker(1_V - 1_V) = Ker(0) = W$. Ahora si w y $w' \in A(x)$, entonces:

   $$Ker(1 - w_V) \supseteq Ker(1 - x_V) \text{ y } Ker(1 - w'_V) \supseteq Ker(1 - x_V).$$

   Luego, para todo $v \in Ker(1 - x_V)$ tenemos que $w_V(v) = v$ y $w'_V(v) = v$, y dado que $w_V(v) = v$, esto implica que $w_V^{-1}(v) = v$, entonces:

   $$w_V^{-1} \circ w'_V(v) = w_V^{-1}(w'_V(v)) = w_V^{-1}(v) = v,$$

   de esta manera, $v \in Ker(1 - (w^{-1}w')_V)$, luego $w^{-1}w' \in A(x)$, por lo tanto $A(x)$ es un subgrupo de W.
2. Sean $w \in A(x)$ y $w' \in A(w)$, luego

   $$Ker(1 - w'_V) \supseteq Ker(1 - w_V) \supseteq Ker(1 - x_V),$$

   entonces $w' \in A(x)$, por lo tanto $A(w) \subseteq A(x)$.
3. Sea $z \in w^{-1}A(x)w$, luego $z = w^{-1}yw$, con $y \in A(x)$.

   Para $v \in Ker(1 - w^{-1}xw)$ tenemos $(w^{-1}xw)_V(v) = v$ lo que implica $x_V(w_V(v)) = w_V(v)$, es decir, $w_V(v) \in Ker(1 - x_V)$, pero dado que $Ker(1 - x_V) \subseteq Ker(1 - y_V)$ tenemos que $y_V(w_V(v)) = w_V(v)$ lo que equivale a $(w^{-1}yw)_V(v) = v$ esto es $z_V(v) = v$, luego $v \in Ker(1 - z_V)$, por lo tanto

   $$Ker(1 - z_V) \supseteq Ker(1 - (w^{-1}xw)_V,$$

   y con esto se tiene $w^{-1}A(x)w \subseteq A(w^{-1}xw)$.

   La otra contención se tiene del hecho que $w^{-1}A(x)w \subseteq A(w^{-1}xw)$ y haciendo el cambio de variable a $x = zuz^{-1}$ y a $w = z^{-1}$, obtenemos $z^{-1}A(zuz^{-1})z \subseteq A(u)$ lo cual equivale a $A(zuz^{-1}) \subseteq zA(u)z^{-1}$, lo cual completa la demostración.

□

LEMA 79. *Para todo $J \subset S$ se tiene que $A(c_J) = W_J$.*

DEMOSTRACIÓN. Sean H_s, el hiperplano de V fijado por la reflexión s_V y

$$H_J := \bigcap_{s \in J} H_s.$$

Dado que cada $s \in J$ fija un H_s, el argumento dado en la Referencia [5] (sección 2, lema 2), nos muestra que

$$Ker(1 - (c_J)_V) = H_J.$$

Notamos que para todo $w \in W$ y $u \in H_J$, tenemos que $w_V(u) = u$ si, y sólo si, $w \in W_J$. Seguido de esto obtenemos $A(c_J) = W_J$ Referencia [2] capítulo I, sección 1.12 . □

LEMA 80. *Sea $J, K \subset S$. Si c_J es conjugado a un elemento de W_K, entonces W_J es conjugado a un subgrupo de W_K.*

DEMOSTRACIÓN. Por hipótesis tenemos que

$$w^{-1} c_J w \in W_K \text{ para algún } w \in W.$$

Luego por Lema 79, tenemos:

$$w^{-1} W_J w = w^{-1} A(c_J) w = A(w^{-1} c_J w) \subseteq A(c_K) = W_K.$$

□

TEOREMA 81. *El Kernel de $\theta : \mathbb{A} \to \mathbb{B}$ es $\sum_{J \sim K} \mathbb{Z}(x_J - x_K)$, tal que $J, K \subseteq S$, donde $J \sim K$ si, y sólo si, W_J es conjugado a W_K en W. Además*

$$Ker(\theta_{\mathbb{Q}}) = \sum_{J \sim K} \mathbb{Q}(x_J - x_K) = Rad(\mathbb{A}_{\mathbb{Q}}),$$

donde $Rad(\mathbb{A}_{\mathbb{Q}})$ es el radical de Jacobson del anillo $\mathbb{A}_{\mathbb{Q}}$.

DEMOSTRACIÓN. Probaremos las siguientes inclusiones:

$$\sum \mathbb{Q}(x_J - x_K) \subseteq Rad(\mathbb{A}_{\mathbb{Q}}) \subseteq Ker(\theta_{\mathbb{Q}}) \subseteq \sum \mathbb{Q}(x_J - x_K).$$

Sea ρ la representación regular del álgebra de grupo $\mathbb{Q}[W]$. Para $J, L \subseteq S$, y $w \in W$, tenemos:

$$x_J x_L = \sum a_{JLM} x_M.$$

Dado que $1 \in X_M$ para todo $M \subseteq S$, luego tenemos que:

$$\sum a_{JLM} = |W_J \backslash W / W_L|,$$

de esta manera:

$$\chi_\rho(x_J x_L) = \chi_\rho(\sum a_{JLM} x_M) = |W||W_J \backslash W / W_L|,$$

decir que W_J es conjugado a W_K en W es decir que existe un $z \in W$ tal que $zW_J z^{-1} = W_K$. Entonces $C \mapsto zC$ es una biyección desde $W_J \backslash W / W_L$ a $W_K \backslash W / W_L$.

Así que por lo tanto tenemos

$$|W_J \backslash W / W_L| = |W_K \backslash W / W_L|.$$

Luego concluimos que $\chi_\rho((x_J - x_K)x_L) = 0$. Dado que los elemento x_L generan $\mathbb{A}_\mathbb{Q}$ con $L \subseteq S$ podemos afirmar que $\chi_\rho((x_J - x_K)a) = 0$ para todo $a \in \mathbb{A}_\mathbb{Q}$. Dado que ρ es fiel(inyectiva) y que $\mathbb{Q}[W]$ es semisimple y contiene todas las representaciones irreducibles, se tiene que $x_J - x_K \in Rad(\mathbb{A}_\mathbb{Q})$. De esta manera tenemos la primera inclusión

$$\sum_{J \sim K} \mathbb{Q}(x_J - x_K) \subseteq Rad(\mathbb{A}_\mathbb{Q}).$$

Dado que $\theta_\mathbb{Q}(\mathbb{A}_\mathbb{Q}) \subseteq \mathbb{B}_\mathbb{Q}$ y la característica de $\mathbb{Q}$ es 0, entonces $\theta_\mathbb{Q}(\mathbb{A}_\mathbb{Q})$es semisimple. Luego por el Teorema del homomorfismo $\mathbb{A}_\mathbb{Q} / Ker(\theta_\mathbb{Q})$ es semisimple, de esta manera $Rad(\mathbb{A}_\mathbb{Q}) \subseteq Ker(\theta_\mathbb{Q})$.

Para la última inclusión, notemos la relación de equivalencia sobre los subconjuntos de S, dada por $J, K \subseteq S$ escribimos $J \sim K$ si, y sólo si, W_J es conjugado a W_K en W.

Sean $J_1, J_2, ..., J_r$ los representantes de cada una de las clases de equivalencia y los enumeramos de la manera que cumple con:

$$|W_{J_r}| \leq ... \leq |W_{J_1}|,$$

y en adelante escribiremos: $W_i := W_{J_i}$, $\varphi_i := \varphi_{J_i}$ y $c_i := c_{J_i}$, donde φ_i es el carácter principal de W_{J_i}.

Sea $a \in Ker(\theta_{\mathbb{Q}})$ entonces

$$a = \sum_{J \in 2^S} q_J x_J, \qquad \text{donde } \ q_J \in \mathbb{Q}.$$

Dado que los caracteres son constantes bajo las clases de conjugación, tenemos que, si $J \sim K$ entonces $\varphi_J = \varphi_K$, con esto tenemos que:

$$\sum_{i=1}^{r} \left(\sum_{J \sim J_i} q_j \right) \varphi_i = 0.$$

Si podemos probar que $\varphi_1, ..., \varphi_r$ son linealmente independiente sobre $\mathbb{Q}$, entonces por la expresión anterior tendríamos que $\sum_{J \sim J_i} q_J = 0$ y luego $a \in \sum \mathbb{Q}(x_J - x_K)$, con lo cual completaríamos la última inclusión.

Supongamos entonces que tenemos una relación $\sum_{i=1}^{r} l_i \varphi_i = 0$, donde $l_i \in \mathbb{Q}$. Argumentaremos que $l_j = 0$ por inducción sobre i. Supongamos que hemos mostrado que

$$l_1 = ... = l_{j-1} = 0 \quad \text{para algún } j \geq 1,$$

entonces:

$$\sum_{i \geq j} l_i \varphi_i(c_j) = 0.$$

Supongamos que $\varphi_i(c_j) \neq 0$, para algún $i \geq j$. Dado que el carácter inducido es constante sobre las clases de conjugación, se tiene que c_j es conjugado a un elemento de W_i y por el Lema 80, tenemos que W_j es conjugado a un subgrupo de W_i, en particular $|W_j| \leq |W_i|$, pero como $i \geq j$ entonces $|W_j| \leq |W_i|$ por nuestra elección de numeración hecha antes. De esta forma $|W_j| = |W_i|$, así que W_j es conjugado a W_i y luego $j = i$. De esta manera

$$l_j \varphi_j(c_j) = 0,$$

pero $c_j \in W_j$, así que $\varphi_j(c_j) \neq 0$. Con esto tenemos que $l_j = 0$, y esto prueba mediante la inducción la última contención, por lo tanto se tiene la segunda afirmación del teorema.

Podemos ver que también prueba que $Ker(\theta) \subseteq \sum \mathbb{Z}(x_J - x_K)$. Sea $a \in Ker(\theta)$ entonces $a \in Ker(\theta_{\mathbb{Q}})$ y luego las contenciones probadas anteriormente nos dice que $Ker(\theta_{\mathbb{Q}})$ es generado sobre $\mathbb{Q}$ por los elementos $x_J - x_{J_i}$, donde $i \in \{1, ..., r\}$ y $J \sim J_i$, de esta manera podemos escribir:

$$a = \sum_{i=1}^{r} \sum_{J \sim J_i} q_J (x_J - x_{J_i}),$$

donde $q_j \in \mathbb{Q}$. Dado que $a \in A$ y los elementos x_J con $J \subseteq S$ son una base con escalares en $\mathbb{Z}$ en A, entonces tenemos que $q_J \in \mathbb{Z}$ y esto completa la demostración. $\square$

Bibliografía

[1] Louis Solomon. A Mackey formula in the group ring of a Coxeter group, Journal Algebra 41 (1976), 255-264

[2] Humphreys. *Reflection groups and Coxeter groups*, Cambridge University Press, 1990.

[3] J.L. Alperin and Rowen B. Bell. *Groups and Representations*, Springer, 1995.

[4] J.P Serre. *Linear representations of finite groups*, Springer,1977.

[5] R.W Carter. Conjugacy classes in the Weyl group, Compositio Math. 25 (1967)

[6] Louis Solomon. A descomposition of the group algebra of a finite Coxeter group. New Mexico State University, 1967

[7] Steven Roman, *Coding and theory information*. Springer, 1992

[8] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associatives algebras*, Wiley, New York, 1962.